UAH

Análisis y estudio de comunicaciones industriales para implementar arquitectura de comunicaciones estándar en Planta Estándar de Ciclo Combinado.

Máster Universitario en

Departamento de Electrónica

Presentado por:

D. ROSENDO CALER RUBIO

Dirigido por:

Dra. SIRA E. PALAZUELOS CAGIGAS

D. José Luis Martín Sánchez

Alcalá de Henares, a 30 de Junio de 2015.

INDICE

I. RESUMEN

II. INTRODUCCIÓN

III. OBJETIVOS

IV. DESARROLLO

1. Redes Industriales

1.1. Introducción a las comunicaciones industriales.

1.1.1. Modelo de automatización CIM.

1.2. Niveles de una red industrial.

a) Nivel de control de factoría.
b) Nivel de control de planta.
c) Nivel de control de célula.
d) Nivel de control de campo.
e) Nivel de control de proceso.

1.3. Tipos de redes industriales.

a) Red de factoría.
b) Red de control o supervisión.
c) Red de célula/celda.
d) Red/Bus de campo.

1.4. Arquitecturas de comunicación.

a) Sistema de control cableado.
b) Sistemas de control cableados con red de supervisión.
c) Sistemas de control en red (NCS).
d) Sistemas de control Fieldbus (FCS).

1.5. Topologías de redes industriales.

a) BUS LINEAL.
b) ANILLO.
c) ARBOL.
d) ESTRELLA.

2. Buses de campo

2.1. Introducción.

a) Sustitución de la señal 4-20mA por señales digitales.
b) Aplicación a sistemas de control distribuido.
c) Interoperabilidad de dispositivos.
d) Sistemas abiertos.

2.2. Clasificación de los buses de campo.

2.3. Buses de alta velocidad y baja funcionalidad.

2.3.1. AS-i.
2.3.2. CAN.
2.3.2.1. CANOpen
2.3.3. SDS.

2.4. Buses de alta velocidad y funcionalidad media.

2.4.1. DeviceNet.
2.4.2. COMPOBUS.
2.4.2.1. COMPOBUS-S
2.4.2.2. COMPOBUS-D
2.4.3. LONWorks (Local Operating Networks).
2.4.4. MODBUS.
2.4.4.1. Modbus RTU
2.4.4.2. Mosbus ASCII
2.4.5. INTERBUS.
2.4.6. UNI-TELWAY.
2.4.7. BITBUS.

2.5. Buses de altas prestaciones.

2.5.1. PROFIBUS.
2.5.1.1. PROFIBUS-DP
2.5.1.2. PROFIBUS-PA
2.5.1.3. PROFIBUS-FMS
2.5.2. ControlNet.
2.5.3. Fieldbus Foundation.
2.5.3.1. Protocolo H1
2.5.3.2. HSE (High Speed Ethernet)
2.5.4. FIP/WorldFIP.

2.6. Comparativa general entre buses de campo actuales.

3. Redes LAN industriales

3.1. Modelo OSI (ISO7498/1984).

3.1.1. Aplicación del modelo OSI a redes industriales.

3.2. Tipos de redes LAN industriales

3.2.1. Modbus TCP
3.2.2. Ethernet/IP

3.2.2.1. CIP Sync
3.2.3. EtherCAT.
3.2.4. PROFINET
3.2.5. Fieldbus HSE
3.2.6. Comparativa entre buses basados en Ethernet

4. Comunicaciones OPC

5. Criterios de selección de un bus de campo

6. Ciberseguridad en monitorización de procesos industriales

6.1. Características de los sistemas de monitorización y control

6.2. La historia de Stuxnet

6.3. Algunas amenazas (actuales y futuras)

6.3.1. DDoS
6.3.2. Botnets
6.3.3. Zeus
6.3.4. Amenazas futuras

6.4. Organismos e instituciones Españolas con competencias en Ciberseguridad

6.5. Guías y estándares de Ciberseguiridad en relación a los sistemas SCADA

6.4.1. Guía CCN-STIC-480 en materia de Seguridad en Sistemas SCADA

6.4.2. IEEE PC37.1™ Draft Standard for SCADA and Automation Systems

6.4.3. ENISA “Protecting Industrial Control Systems. Recommendations for Europe and Member States”.

7. Planta estándar de Ciclo Combinado

7.1. Introducción

7.1.1. Definición termodinámica de un Ciclo Combinado
7.1.2. Planta de energía estándar 109FB-SS de GE Energy©
7.1.3. Filosofía de control de la Planta estándar de Ciclo Combinado
7.1.4. El Sistema de Control (PCS)
7.1.4.1. Diseño hardware de cabinas de control del PCS
7.1.5. Instrumentación de sistemas
7.1.5.1. Triple instrumentación redundante (sistemas críticos)

7.1.5.2. Doble instrumentación redundante (sistemas importantes)
7.1.5.3. Instrumentación HRSG
7.1.5.4. Instrumentación para sistemas no importantes
7.1.6. Instrumentos y dispositivos de control
7.1.7. Interfaz del operador
7.1.7.1. Avisos y alarmas
7.1.7.2. Presentación de los datos
7.1.8. Diseño a prueba de fallos
7.1.9. Circuitos de protección y alarma
7.1.10. Enclavamientos
7.2. Descripción de la arquitectura general de la Planta estándar
7.2.1. Elementos de campo
7.2.2. Elementos de control/supervisión del PCS
7.2.3. Elementos de control de sistemas paquete
7.3. Premisas para el diseño de la nueva arquitectura con redes de comunicaciones
7.4. Identificación de redes de comunicaciones en la Planta estándar
7.4.1. Red/Bus de campo
7.4.2. Red de célula
7.4.3. Red de control/supervisión
7.4.4. Red de factoría
7.5. Definición de los elementos que componen cada una de las redes de comunicaciones
7.5.1. Elementos de la red de campo
7.5.2. Elementos de la red de célula
7.5.3. Elementos de la red de control/supervisión
7.5.4. Elementos de la red de factoría
7.5.5. Definición de la especificación de bus empleado
7.6. Implementación práctica de las diferentes redes de la Planta estándar de Ciclo Combinado mediante especificación PROFIBUS
7.6.1. Diseño de la red de proceso y segmentos que la componen
7.6.1.1. Definición de segmentos de señales analógicas/digitales
7.6.1.2. Hardware para creación de segmentos de señales analógicas/digitales
a) Módulos ET200M
b) Módulos de interfaz IM153
c) Módulos de E/S

7.6.1.3. Rack de segmentos de señales analógicas/digitales
7.6.1.4. Definición de segmentos de válvulas motorizadas (MOV)
7.6.1.5. Comunicación entre segmentos. Optical Link Manager (OLM)
7.6.1.6. Cableado de redes PROFIBUS DP/PA
a) Redes eléctricas
b) Redes ópticas
7.6.1.7. Interconexión de segmentos y conexión de la red de campo con nivel superior
7.6.1.8. Consumos máximos por segmento
7.6.2. Diseño de la red de célula
7.6.3. Diseño de la red de control/supervisión
7.6.3.1. Topología empleada
7.6.3.2. Elementos de conexión a red
7.6.3.3. Interfaz de comunicación del Sistema de Control/Bus mediante OPC
7.6.3.4. Cableado Ethernet
7.6.4. Diseño de la red de factoría
7.6.4.1. Topología empleada
7.6.4.2. Elementos de conexión a red
7.6.5. Configuración del sistema y tipos de dispositivos.
7.7. Políticas de Ciberseguridad a aplicar para proteger la instalación
7.7.1. Principales orígenes de los ataques cibernéticos
7.7.2. Causa de las vulnerabilidades y amenazas o factores que los fomentan
7.7.3. Identificación y análisis de los principales riesgos y amenazas
7.7.4. Buenas prácticas aplicables
8. Conclusiones finales
9. Bibliografía y referencias de internet
ANEXO 1
ANEXO 2
ANEXO 3
ANEXO 4

I. RESUMEN.

Con el presente trabajo se realiza un análisis y estudio de las comunicaciones industriales actuales, con el fin de implementar una arquitectura de comunicaciones estándar para una Planta Estándar de Ciclo Combinado 109FB de GE Energy©.

En la primera parte del trabajo se realiza una recopilación de los diversos tipos de comunicaciones industriales más utilizadas en la actualidad, para incorporarlo al know-how de la Empresarios Agrupados AIE©, y en la segunda parte se define una arquitectura de comunicaciones estándar aplicando la filosofía de jerarquización de redes basada en el modelo CIM, para establecer las redes de comunicaciones de los diferentes sistemas de la planta.

Finalmente, una vez definidas las redes de comunicaciones de la Planta Estándar, se realiza una aplicación práctica del diseño de estas redes con tecnología PROFIBUS.

II. INTRODUCCIÓN.

La Planta estándar de Ciclo Combinado es un proyecto conjunto llevado a cabo por la Ingeniería española Empresarios Agrupados AIE© y empresa estadounidense General Electric GE©, con el fin de establecer un diseño modular estándar para una Planta de Ciclo Combinado basada en la Turbina monoeje de GE®.

La Ingeniería de Empresarios Agrupados AIE© cubre la realización de: diseño detalle de sistemas principales, definición de criterios de ingeniería y layouts eléctricos/mecánicos.

Con el presente trabajo se pretende la consecución de los siguientes objetivos:

1) Realizar un análisis y estudio de las comunicaciones industriales actuales para incorporarlo al Know-how de la empresa, que sirva como base para la formación en comunicaciones industriales de la plantilla del Departamento de I&C y que permita en proyectos futuros la incorporación de la ingeniería de las comunicaciones de la planta.

2) El diseño del Sistema de Control Distribuido basado en procesadores MARK VIe es una tecnología definida y propiedad de GE©, pero como el layout de cables y señales de campo es parte de la Ingeniería que aporta Empresarios Agrupados al proyecto de la Planta Estándar de Ciclo Combinado, con el presente trabajo se quiere implementar una arquitectura de comunicaciones estándar basada en buses de campo, entre los dispositivos de campo de los diferentes sistemas de la planta y el Sistema de Control Distribuido, así como la comunicación con la Sala de Control Central (CCR); proporcionando una solución alternativa a la incluida por GE©.

Para la definición de la arquitectura de comunicaciones se emplea la filosofía de jerarquización de redes basada en el modelo CIM, que permite establecer las redes de comunicaciones de los diferentes sistemas de la planta.

Finalmente, una vez definidas las redes de comunicaciones de la Planta Estándar se realiza una aplicación práctica con tecnología PROFIBUS para el diseño de estas redes.

III. OBJETIVOS.

El objetivo del presente trabajo es realizar un análisis y estudio de las comunicaciones industriales actuales, con el fin de implementar una arquitectura de comunicaciones estándar para una Planta Estándar de Ciclo Combinado, para lo cual se seguirá la siguiente metodología de desarrollo en el trabajo:

- Estudio de la filosofía de diseño de redes industriales:
  - Como se definen los diferentes niveles de automatización.
  - Modelo CIM para jerarquización de las redes.
- Estudio de las comunicaciones industriales más utilizadas en la actualidad basados en:
  - Buses de Campo.
  - Redes Ethernet.
- Recopilación de todas las comunicaciones comentadas en cuanto a:
  - Topologías de red.
  - Aplicaciones más frecuentes de cada uno de los buses.
  - Soporte físico y accesorios.
  - Distancias máximas.
  - Velocidad de la comunicación.
  - Número máximo de dispositivos.
  - Tipo de acceso al bus.
  - Normativa soporte.
- Aplicación práctica:
  - Realización de la arquitectura de comunicaciones para una Planta Estándar de Ciclo Combinado (PROFIBUS).
  - Aplicación del modelo CIM para la definición de redes de la Planta Estándar.
  - Definición de segmentos y topologías de red.
  - Definición de cableado y elementos de conexión.
- Conclusiones finales.

IV. DESARROLLO.

1. Redes Industriales.

1.1. Introducción a las comunicaciones industriales.

En cualquier industria es indispensable conocer el estado del proceso productivo, para lo cual se dispone en las distintas etapas del proceso de multitud de dispositivos de campo que permiten obtener información a los equipos de control y a los operadores de la planta, para mantener el proceso productivo tanto en unas condiciones óptimas de producción que permitan producir el máximo, como unas condiciones seguras tanto para los trabajadores de la planta como para el entorno en el que se encuentra ubicada la instalación.

1.1.1 Modelo de automatización CIM.

Un proceso productivo suele constar de diversas etapas automatizadas para su monitorización y control formando "islas automatizadas", que se definen como células de trabajo sin comunicación entre sí. En la industria moderna se utilizan diferentes redes de comunicación de acuerdo a diferentes niveles de automatización.

Para la definición de los diferentes niveles de automatización, en la actualidad está completamente aceptado el modelo denominado *Computer Integrated Manufacturing* (CIM), definido por el *National Bureau of Standards (NBS)* de los Estados Unidos. Este modelo es uno de los modelos más difundidos en la actualidad para determinar la jerarquización de las redes según el propósito para el que han sido diseñadas y aplicadas, considerando la factoría como un todo, y dividiendo las tareas de control en distintos niveles funcionales.

El modelo CIM busca incrementar la eficiencia de todos los componentes de la empresa, relacionados con la producción, con los siguientes objetivos [1]:

- Aumentar la flexibilidad.
- Mejorar la calidad del producto.
- Reducir los costos.
- Reducir el tiempo y el número de pasos empleados en la fabricación.
- Aumentar la confiabilidad del sistema.

Cada nivel lleva a cabo labores específicas, asociando a ello un tipo de información y de procesamiento diferente. De ahí, queda determinada la jerarquía a la cual pertenece una red. Cada red gobierna las funciones del nivel inferior y sirve de interfaz al nivel superior (integración del proceso automatizado). El flujo de la información fluye tanto en sentido horizontal (dentro de su propio nivel) como en sentido vertical (a un nivel superior o inferior). [1]

1.2. Niveles de una red industrial.

El modelo CIM se define los siguientes niveles dentro de una red industrial:

a. Nivel de control de factoría:

Es el nivel más elevado y se encarga de integrar el proceso productivo en el área de gestión. De este modo permite supervisar a los diversos departamentos de una compañía la evolución o estado del proceso productivo, obteniendo información del mismo pero nunca interviniendo en él. Se emplea una red de tipo LAN o WAN.

b. *Nivel de control de planta:*

A este nivel corresponden las funciones de planificación de la producción del conjunto de la factoría. Se generan órdenes de ejecución hacia el nivel de célula en base a las indicaciones del nivel de factoría. Se generan funciones de elaboración de secuencias de producción, secuenciamiento de tareas y coordinación de recursos en la planta. [1]

c. *Nivel de control de célula:*

En este nivel se realiza la coordinación de las máquinas pertenecientes a la célula de fabricación, y se subdivide el proceso productivo en distintas zonas o sistemas enlazados entre sí o con niveles superiores mediante autómatas de altas prestaciones u ordenadores dedicados al control o programación. [1]

d. *Nivel de control de campo:*

Este nivel integra pequeños automatismo (autómatas compactos, controladores PID, etc.) dentro de subredes o islas. En lo más alto de estas redes se suelen encontrar uno o varios autómatas modulares actuando como maestros o flotantes. En este nivel se suele emplear buses de campo tradicionales o actualmente está en auge el uso de Ethernet Industrial bajo una serie de pautas de ciberseguridad que eviten posible ataques cibernéticos en puedan dañar el proceso productivo o incluso al personal de la planta.

e. *Nivel de de control de proceso:*

Es el nivel más próximo al proceso, y a este nivel se sitúan los sensores y actuadores, encargados de manejar el proceso productivo y tomas las medidas necesarias para la correcta automatización y supervisión. Se trata de sustituir el sistema de cableado tradicional por buses de campo de prestaciones sencillas y sistemas de periferia descentralizada.

En las siguientes figuras se muestra el modelo CIM de 5 niveles aplicado a una arquitectura de aplicación típica en la industria [6].

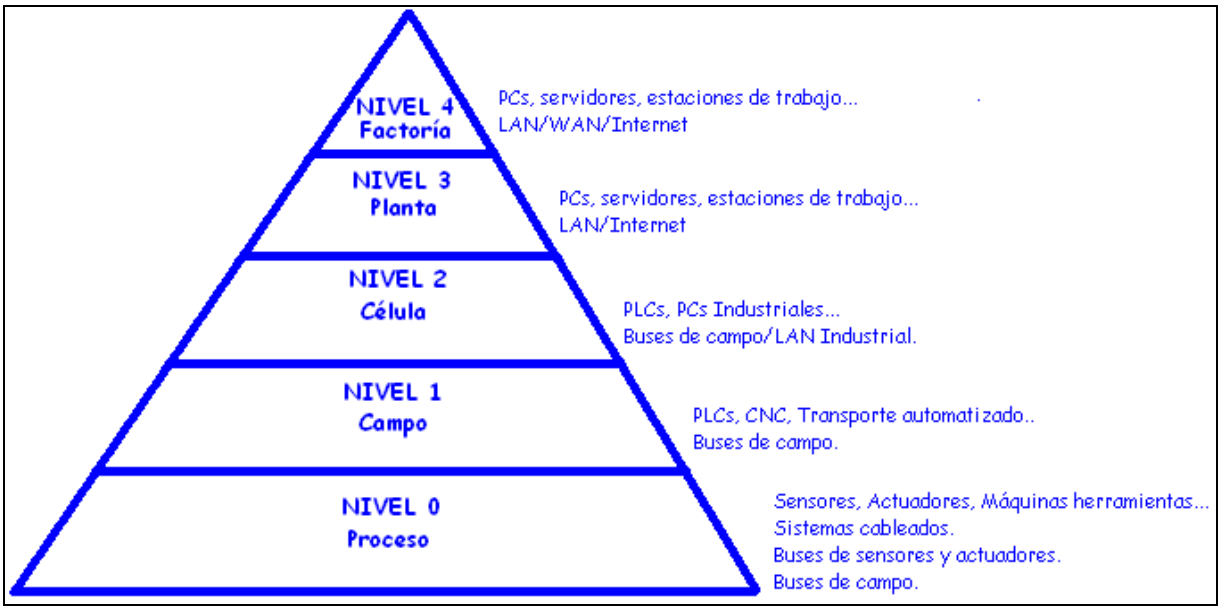


Figura 1.
Modelo CIM definido por NBS de los Estados Unidos [6].

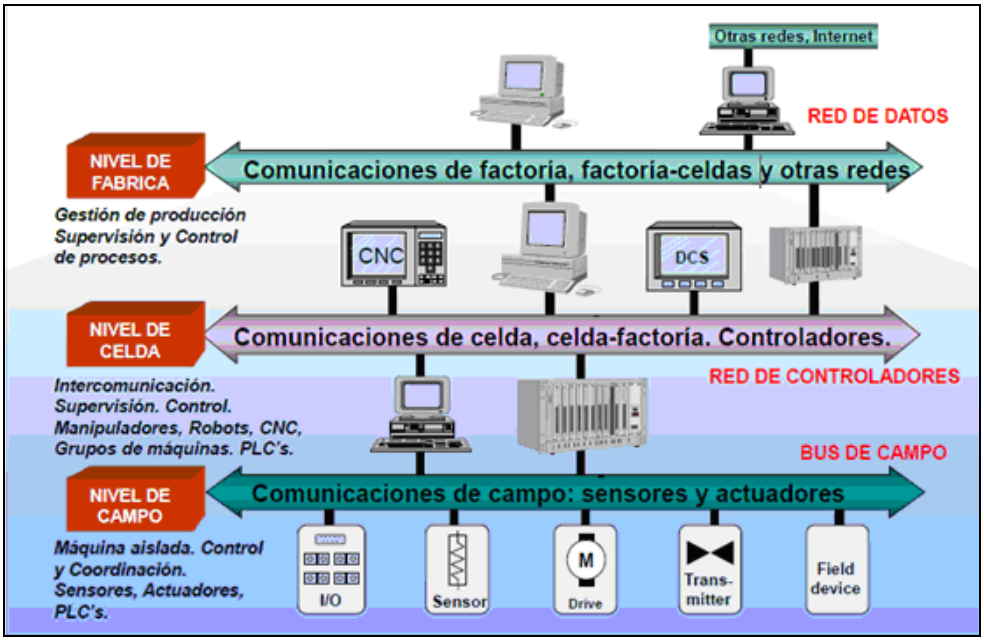


Figura 2.
Niveles de comunicación industrial. [2]

Lo habitual en las diversas etapas del proceso productivo es que interaccionen, por lo que suelen unirse mediante el empleo de redes y protocolos de comunicación:

a) El protocolo de comunicación es un conjunto de reglas que permiten la transferencia e intercambio de datos entre los distintos dispositivos que conforman una red.

b) Las redes permiten estructurar el proceso productivo dividiendo las diversas tareas que lo componen entre un grupo de procesadores jerárquicamente anidados, permitiendo la integración de las islas automatizadas en redes de comunicación que proporcionan importantes ventajas como: mayor disponibilidad de la información, diagnósticos remotos, menores costes de mantenimiento, etc. Esto da lugar a una estructura de redes industriales que se podrían agrupar en dos categorías [1], que posteriormente serán detalladas en el presente trabajo:

- *Redes/Buses de campo:* son las ubicadas en la parte más baja de la jerarquía CIM, y conectan distintos procesos de aplicación con el propósito de asegurar la explotación de la instalación (comando, supervisión, mantenimiento y gestión). Provee servicios bajo restricciones temporales (tiempo real) y están constituidas por protocolos capaces de gestionar estas restricciones (garantiza que las restricciones de tiempo serán respetadas con cierta probabilidad). A diferencia de las redes de información, están diseñadas para enfrentar un tráfico formado por un gran número de pequeños paquetes, intercambiados con frecuencia entre un alto número de estaciones que forman la red y que muchas veces trabajan en tiempo real. Los dispositivos típicos a conectar son PLCs, PC con tarjetas de red de campo, variadores de frecuencia, sensores, etc.

- *Redes de información (LAN/WAN):* se ubican en la parte más alta de la jerarquía CIM, y son redes orientas al transporte de grandes paquetes de datos y por tanto necesitan un amplio ancho de banda para poder permitir el envío rápido de información, y suelen ser redes basadas en tecnología IP. Los dispositivos típicos a conectar por estas redes son Computadores Personales (PC), servidores (Host) y MainFrames.

1.3. Tipos de redes industriales.

En base a los distintos niveles de una red industrial establecidos por el modelo CIM comentado en el punto 1.2, se hace la diferenciación de los siguientes tipos de redes:

a. *Red de factoría:*

Son redes que interconectan todos los sectores y servicios de la fábrica utilizando computadores: almacén, servicios generales, ingeniería, líneas de producción, etc.

Esta red conecta a los dispositivos con funciones correspondientes al nivel de control de factoría de la pirámide CIM.

b. Red de control o supervisión:

Transmite al operador los datos necesarios para conducir el proceso, y a su vez, el operador envía al proceso cambios de consigna.

Esta red conecta a los dispositivos con las funciones definidas en el nivel de control de planta de la pirámide CIM.

c. Red de célula/celda:

Conecta entre sí los equipos de comando y control pertenecientes a una isla de producción. Los equipos conectados son controladores.

Esta red conecta a los dispositivos con las funciones definidas en el nivel de control de célula de la pirámide CIM.

d. Red/ Bus de campo:

La idea es sustituir con este tipo de bus el cableado entre sensores-actuadores y los correspondientes elementos de control. Este tipo de buses son una red local industrial que conecta dispositivos de campo tipo: actuadores, sensores, transductores, elementos HMI, etc, con equipos que soportan procesos de aplicación como PLC, CPU de DCS, Robot, Sistemas HMI, etc. que necesitan acceder a los dispositivos de campo. Son buses de bajo coste, tiempo real y permiten las transmisión serie sobre un bus digital de datos, además de gestionar mensajes cortos eficientemente, tener capacidad de manejar tráfico de eventos discretos, poseer mecanismos de control de error, transmitir mensajes prioritarios, poder recuperarse de eventos anormales en la red y responder rápidamente a los mensajes recibidos. Por regla general estos buses tienen un tamaño pequeño (5 a 50 nodos), utilizan tráfico de mensajes cortos para control y sincronización entre los dispositivos, y la transferencia de ficheros es ocasional o inexistente.

Esta red conecta a los dispositivos con las funciones definidas en los niveles de control de campo y proceso de la pirámide CIM.

1.4. Arquitecturas de comunicación.

La forma de interconectar los diferentes elementos de una red es muy variada, lo que da lugar a muy diversas arquitecturas de comunicación, pero las arquitecturas de comunicación más utilizadas en entornos industriales son las siguientes:

a. Sistema de control cableado: los dispositivos de campo se cablean de forma individual a los controladores, comunicándose con las estaciones de supervisión a través de interfases serie punto a punto o protocolos propietarios.

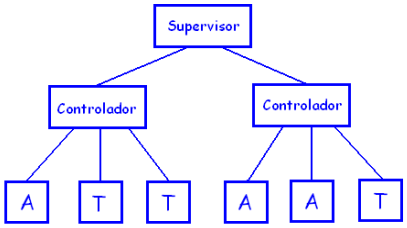


Figura 3. Sistema cableado tradicional.

b. Sistemas de control cableados con red de supervisión: ahora entre controladores y supervisores se establece una red propietaria o semiabierta a la que se define red de supervisión.

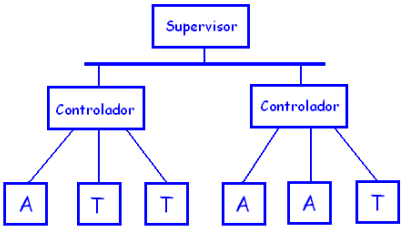


Figura 4. Sistema cableado con red de supervisión.

c. Sistemas de control en red (NCS): Los dispositivos de campo se cablean formando un bus de campo, y entre controladores y supervisores se establece un bus de campo o red abierta o semiabierta.

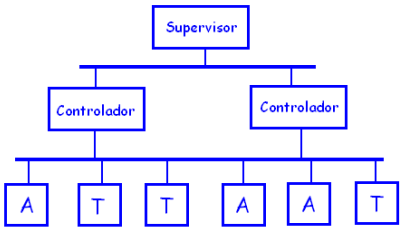


Figura 5. Sistema de control en red NCS.

d. Sistemas de control Fieldbus (FCS): Existe una única red que es el bus de campo y se elimina el controlador. Ahora la supervisión se hace directamente sobre los dispositivos de campo lo que requiere que éstos sean inteligentes (smart devices).

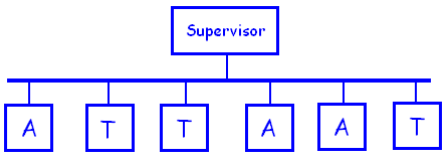


Figura 6. Fielbus.

1.5. Topologías de redes industriales.

La topología de red es la disposición física en la que se conecta una red de ordenadores. Las topologías más típicas son [1]:

a. BUS LINEAL: La estructura de Línea Troncal (bus) es muy clara y entraña muy poca complejidad, ya que todos los usuarios se comunican a través de una línea común. Los dispositivos se conectan con o sin derivaciones cortas, lo que en ocasiones conduce a cableados algo engorrosos.

b. ANILLO: Si se construye un anillo físico con varias conexiones de dos-puntos, se denomina estructura en anillo. Los mensajes se transmiten de un usuario al siguiente. El hecho de que la señal se amplíe cada vez que se transmite el mensaje permite a éste recorrer grandes distancias.

c. ARBOL: La estructura en árbol es similar a la lineal con la única diferencia de que varias derivaciones pueden converger en los nodos. Esta estructura permite conectar en red zonas muy amplias de una manera más fácil y más flexible.

d. ESTRELLA: Una estación central está conectada a todos los usuarios mediante conexiones a dos-puntos formando una estructura en estrella. Esta estación central puede actuar como Master y ser responsable del control de la red, o actuar como "acoplador en estrella", estableciendo simplemente la conexión entre el emisor y el receptor.

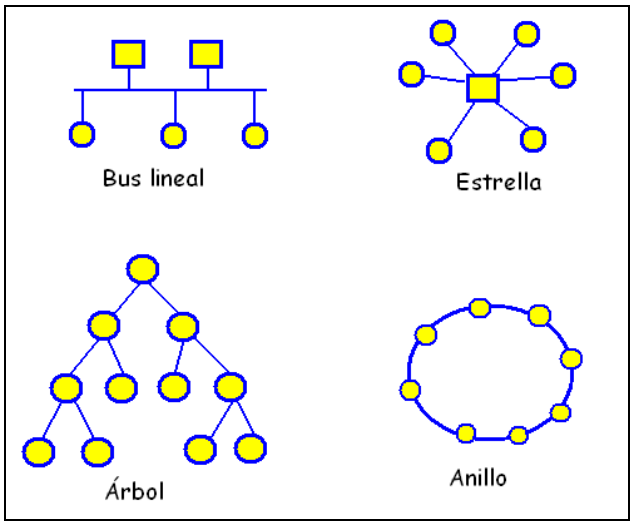


Figura 7.
Topologías de red.

Los buses de campo admiten la implementación de distintas topologías. Entre ellas, las más comunes podemos encontrar las siguientes:

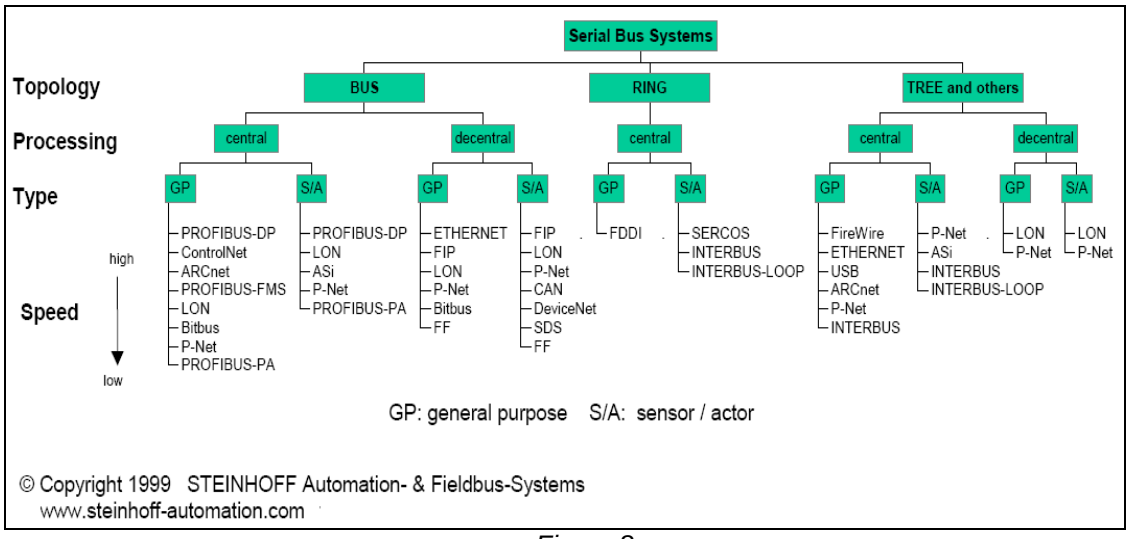


Figura 8.
Tipologías más usuales en buses de campo.

2. Buses de campo.

2.1. Introducción

Un bus de campo es un sistema de transmisión de datos con el objetivo de sustituir las conexiones punto a punto entre los elementos de campo y el equipo de control a través del tradicional lazo de corriente 4-20mA o 0-10VDC. Generalmente son redes digitales, bidireccionales o multipunto que van montadas sobre un bus serie y que conectan dispositivos de campo como: PLCs, transductores, actuadores, sensores, etc. Varios grupos han intentado generar e imponer una norma que permita la integración de equipos de distintos proveedores, sin embargo hasta la fecha no existe un bus de campo universal [4].

En las redes de campo se pueden destacar las siguientes cuatro características principales [1]:

a. Sustitución de la señal de 4-20mA por señales digitales:

La sustitución de las señales 4-20mA por señales digitales trae consigo sustanciales ventajas como son:

- **Mayor exactitud y confiabilidad de datos:** Debido a la comunicación digital, ya que los microprocesadores, por ejemplo en un transmisor y un controlador, pueden hablar directamente en lugar de pasar a través de conversiones D/A y A/D, de las cuales hay muchas en un lazo cerrado. El estado es enviado junto con los datos de medición y control. En consecuencia, es posible determinar si la información es confiable o no. Todos los datos son verificados y garantizados, libres de distorsión debido al ruido o a algún desajuste de impedancia, que en las señales analógicas no serian detectados.

- **Acceso multivariable:** Esto significa que un transmisor de presión, por ejemplo, no está limitado a una sola salida para presión, sino que también informa de la temperatura de proceso. Otro ejemplo es el acceso a la variable de setpoint y a la variable manipulada de un controlador en el mismo dispositivo, o los distintos canales de entrada en un transmisor de temperatura.

- **Configuración y diagnósticos remotos:** La comunicación digital permite modificar remotamente la configuración completa. La calibración se efectúa en funcionamiento sin tener que aplicar ninguna entrada o medir la salida. De manera similar se puede interrogar el estado de los autodiagnósticos.

- **Disminución y simplificación del cableado:** Se logra a través de la conexión de varios dispositivos sobre un solo par de cables. La conexión es una tarea sencilla, ya que todo se encuentra en paralelo y el número de terminales a utilizar es mínimo. Esto significa un bajo costo y un fácil reemplazo de viejos transmisores.

b. Aplicación a sistemas de control distribuido:

Los buses de campo permiten un control distribuido al incorporar esta función en los propios dispositivos. Sin embargo, también es posible configurar una arquitectura de control centralizada.

c. Interoperabilidad de dispositivos:

Los buses de campo tienen capacidad de interoperabilidad, que es la capacidad que tiene la red de reemplazar un dispositivo por otro del mismo tipo independientemente de la marca del fabricante.

d. Sistemas abiertos:

La interoperabilidad es posible debido a que la mayoría de los buses industriales son de estándares abiertos que son administrados por asociaciones internacionales integradas por empresas fabricantes. De esta manera, las especificaciones para producir hardware y software compatible con determinado bus, están disponibles para los desarrolladores de dispositivos.

2.2. Clasificación de los buses de campo.

Los buses de campo se pueden clasificar de muy diversas formas, y de acuerdo a la diversa documentación estudiada, los buses que se recogen en este trabajo se clasifican y agrupan en base al volumen de información que se puede transmitir, a la funcionalidad del dispositivo, velocidad de transmisión y tiempo de respuesta del mismo.

Además, según las funcionalidades del bus éste se ubicará en uno u otro nivel dentro de la pirámide CIM, y por tanto nos permitirá establecer qué tipo de red es la más adecuada para formar con este bus.

Por tanto, los buses de campo se van a clasificar en base a las siguientes premisas:

- Buses de alta velocidad y baja funcionalidad, conocidos como SENSORBUS.
- Buses de alta velocidad y funcionalidad media, conocidos como DEVICEBUS.
- Buses de altas prestaciones, conocidos como FIELDBUS.

En la siguiente figura se muestra de forma gráfica los tipos de redes empleados en la industrial actual:

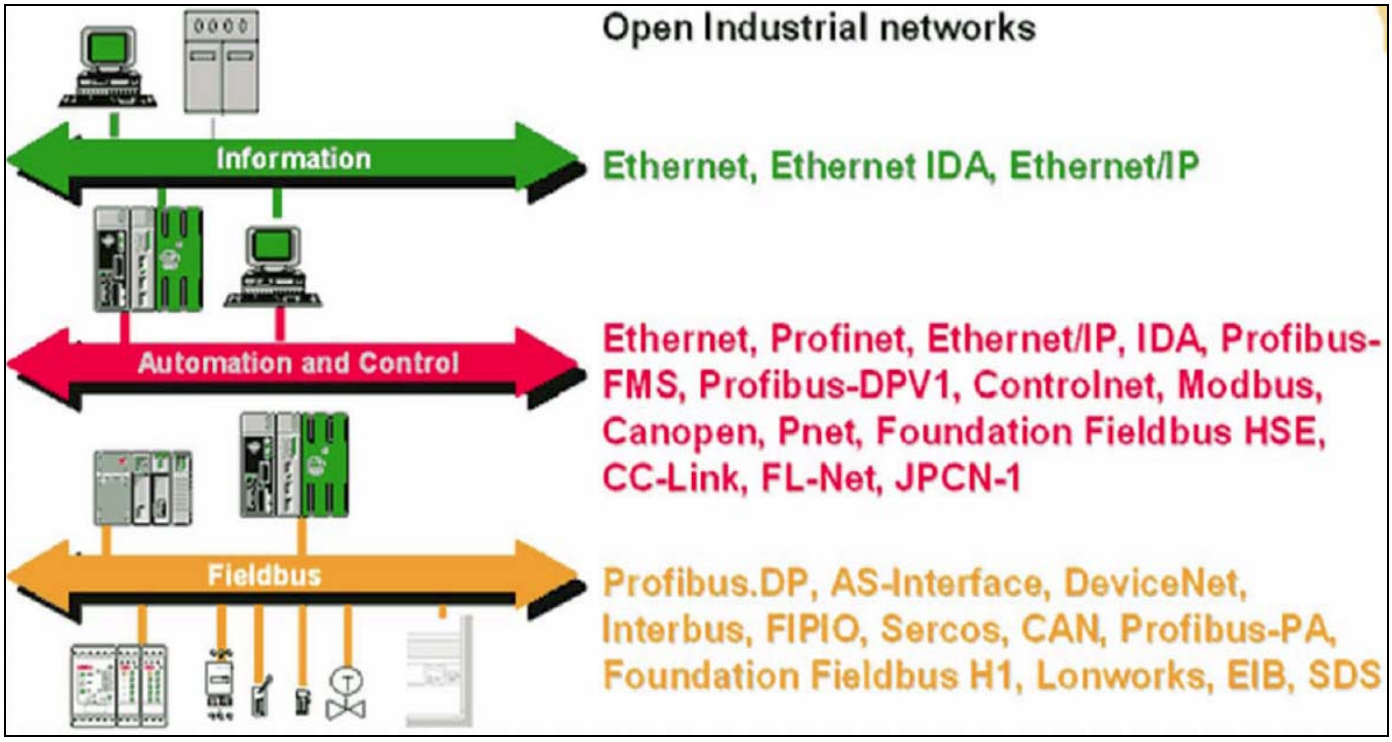


Figura 9.
Redes industriales más usuales [8].

2.3. Buses de alta velocidad y baja funcionalidad.

Los buses considerados con estas características son los situados en los niveles 1 y 2 de la pirámide CIM, correspondientes a los niveles de sensor/actuador y control de máquina, respectivamente. Por tanto su utilización va enfocada a la implementación de redes de campo.

A este tipo de buses de campo también se les conoce como SENSORBUS, y la información que transmiten es a nivel de bits mediante variables digitales. Suelen ser dispositivos de E/S digitales tales como: interruptores, botoneras, captadores, etc.

Los buses de este tipo más empleados en la industria actual son:

- AS-i (Actuator-Sensor Interface).
- CAN (Controller Area Network).
- SDS (Smart Distributed System).

2.3.1 AS-i.

El bus AS-i nació en 1990 como un intento de eliminar el cableado existente entre los sensores y actuadores binarios (todo-nada), con la característica añadida de proporcionar la tensión de alimentación sobre el mismo cable (hasta 8A). Posteriormente el bus ha evolucionado para comunicarse con elementos inteligentes para poder transmitir datos y parámetros, además de las señales binarias, formando redes sensor-actuador. El bus AS-i es considerado uno de los sistemas de comunicación más sencillos y con menos prestaciones, por lo que se emplea a nivel de proceso en la parte más baja de la pirámide de automatización. AS-i es un sistema abierto definido por el estándar europeo EN 50295 y el estándar IEC 62026-2.

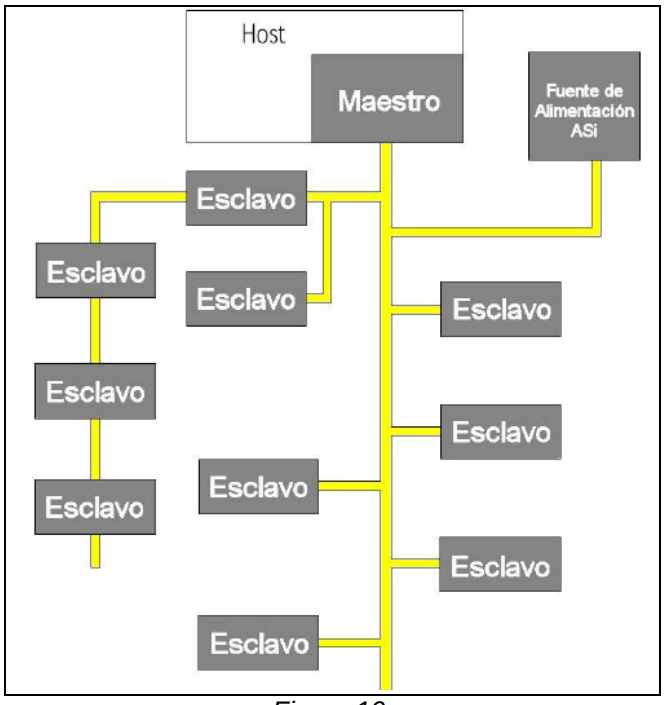


Figura 10.
Esquema de distribución de una red AS-i [6].

Las principales características que posee este bus son:

- Principio de funcionamiento basado en la técnica de sondeo, mediante un maestro y varios esclavos.
- Tiempo máximo de ciclo es 5 msg. En este tiempo se conoce el valor de todos los esclavos.
- Un maestro puede controlar a 31 esclavos, aunque puede llegar a 62 para la versión 2.1 del protocolo, y también es ampliable usando repetidores.
- Cada esclavo permite direccionar 4 entradas y 4 salidas digitales, y adicionalmente, 4 bits de parámetros por cada esclavo con un máximo de 248 entradas/salidas digitales.
- Es posible la comunicación con módulos analógicos.
- El direccionamiento de los esclavos es electrónico, mediante el maestro, o un dispositivo específico de direccionamiento.
- Permite la interconexión, mediante un único canal de comunicación, de un sistema de control (Autómata Programable, Control Numérico, Computador Industrial, Robot, etc.) y un máximo de 31 nodos que constituyen procesadores de comunicaciones, a cada uno de los cuales se pueden conectar, como máximo, 4 sensores y 4 actuadores todo/nada
- Admite cualquier topología de la red (incluyendo topologías mixtas), con longitud máxima de 100 metros sin repetidores y caída de tensión máxima de 3V.
- La tensión de operación de los esclavos debe estar entre 26,5V y 31,6V.
- Típicamente la corriente de consumo de cada esclavo es 200mA.

Los elementos esenciales en una red AS-i son:

Maestro de bus AS-i: suele estar conectado a un autómata programable o al elemento de control principal. También puede estar conectado a una pasarela que permita comunicarse con el bus AS-i desde diferentes dispositivos a través de una red de nivel superior.

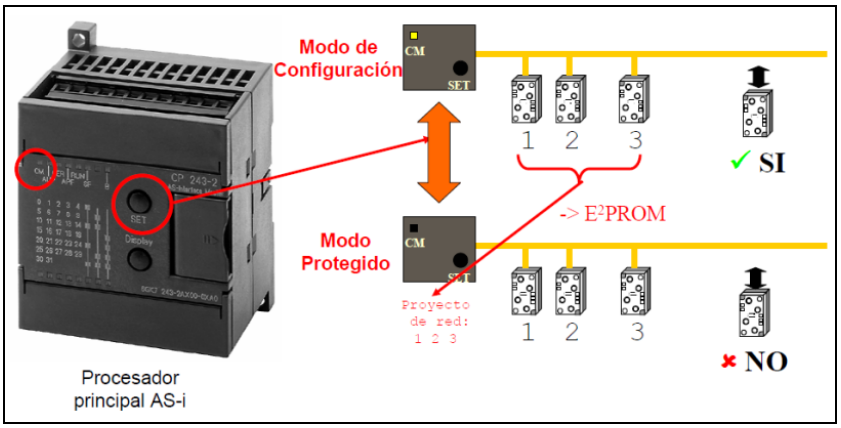


Figura 11.
Maestro de bus AS-i [6].

Fuente de alimentación AS-i: proporciona 30VDC y hasta 8A para alimentar a los elementos esclavos a través de un solo cable. Adicionalmente es posible conectar otro tipo de tensión de alimentación para proporcionar mayores corrientes si es necesario. Para ello se instalan fuentes de alimentación que proporcionan alimentación a través de cables adicionales de 24VDC (cable negro) y 230VAC (cable rojo).

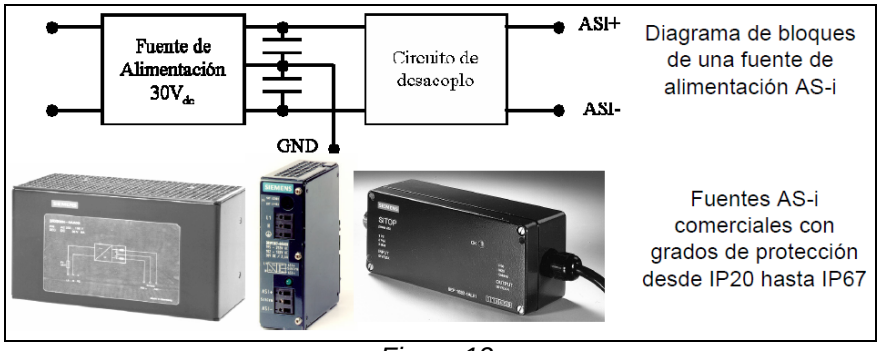


Figura 12.
Fuentes de alimentación AS-i [6].

Esclavos del bus AS-i: existen 2 tipos principales, unos los que integran el protocolo en el mismo elemento de entrada/salida mediante la inclusión de un chip ASIC (circuito integrado de aplicación específica), y otros son los módulos AS-i genéricos que disponen de 4 entradas/salidas de tensión para poder conectarles cualquier elemento sensor/actuados binario tradicional. Los módulos AS-i genéricos resultan aconsejables para las instalaciones existentes, ya que de esta forma no es necesario sustituir los elementos de la instalación, únicamente se sustituyen los cables de conexión.

Figura 13.
Módulos AS-i genéricos para integrar a la red sensores/actuadores tradicionales [6].

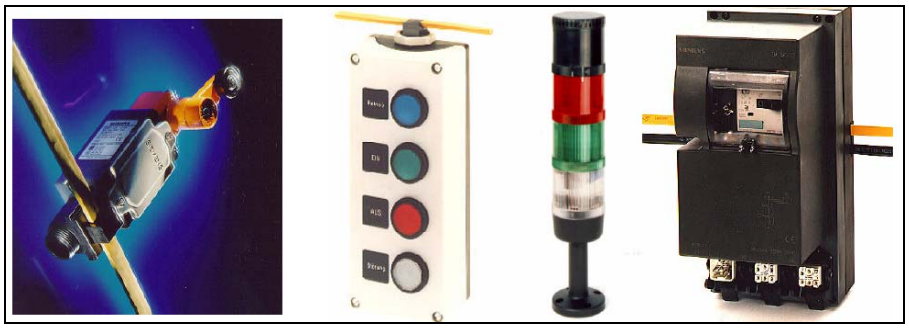


Figura 14.
Módulos AS-i sensores/actuadores inteligentes con chip ASIC [6].

Cable de conexión: generalmente es un cable plano de dos hilos no apantallado con guía de posicionamiento (DIN VDE 0295, clase 6) y un perfil especial que impide la inversión de polaridad en la conexión. Su color es amarillo y tiene una muesca en un lado para identificarlo y facilitar su instalación. También es admisible el uso de cable normal de dos hilos de 1,5mm2 de sección por hilo, tanto apantallado como no apantallado, pero en este caso es necesario ser cuidadoso en la instalación para no confundir polaridades. Además, para conectar el cable a los módulos electrónicos de usuario (esclavos) se utilizan módulos de interconexión que permiten la rápida conexión al cable AS-i amarillo y, opcionalmente, con la alimentación auxiliar.

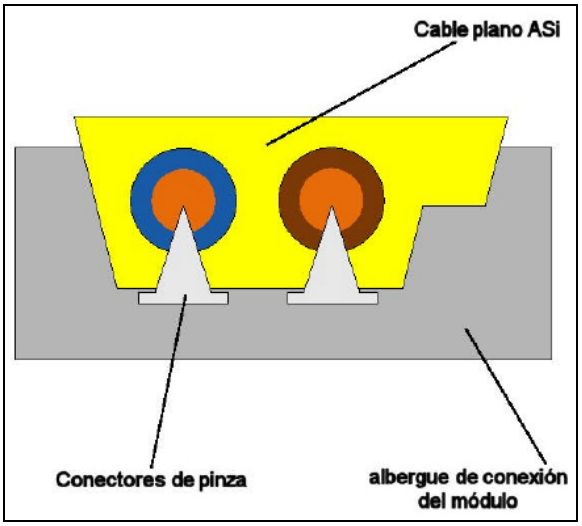


Figura 15.
Cable AS-i [4].

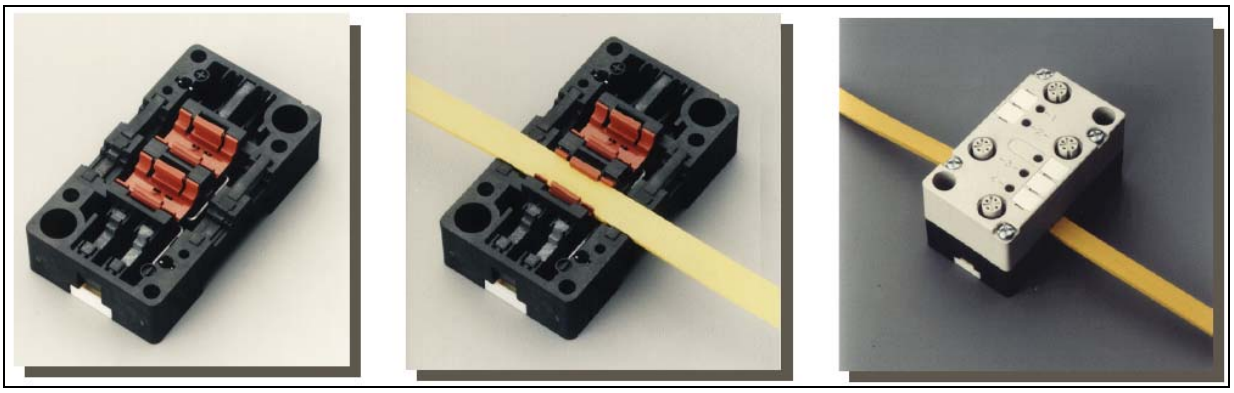


Figura 16.
Módulos de interconexión [6].

Existen algunos módulos esclavos que incorporan un watchdog que revisa continuamente la comunicación con el maestro y actúan en caso que ésta sea interrumpida o se produzca la detección de errores, poniendo en modo de seguridad las entradas/salidas controladas por él. Si no se reciben mensajes del maestro durante 40 msg, las salidas pasan a estar apagadas (off) o simulan un estado de reset continuo del sistema. Las causas habituales de una pérdida de comunicación pueden ser la rotura del cable, un fallo en el maestro (o su paso a estado de parada), o bien una falta de direccionamiento del módulo. La utilización de AS-i en entornos con fuertes interferencias (sistemas de soldadura, convertidores de frecuencia, etc) puede hacerse sin problemas.

También existen módulos específicos para la detección de fallos y protección de seguridad eléctrica llamado “monitor de seguridad”, encargado de monitorizar que las señales eléctricas transmitidas son adecuadas, y verifica la aparición de derivaciones a tierra o protección contra sobretensiones, en cuyo caso es posible enviar mensajes al módulo maestro para que permita ejecutar acciones de protección, o incluso controlar relés de protección directamente.

2.3.2 CAN.

Este tipo de bus se encuentra dentro de los considerados de bajo nivel, y aunque inicialmente no fue concebido para el sector industrial, se encuentra bastante popularizado en este sector por sus prestaciones, robustez y bajo coste.

Este bus está basado en el protocolo CAN que es un estándar que viene descrito en el estándar ISO 11898 e impulsado inicialmente por el fabricante alemán BOSCH para simplificar el cableado en los automóviles Mercedes-Benz. Por este motivo su aplicación más importante es en automoción, donde existe gran cantidad de electrónica asociada a los elementos instalados tanto en el motor como en el resto del vehículo (airbag, cinturones de seguridad, climatización, etc.) y es necesario el acceso distribuido, por lo que CAN proporciona una buena implementación para la comunicación entre estos elementos.

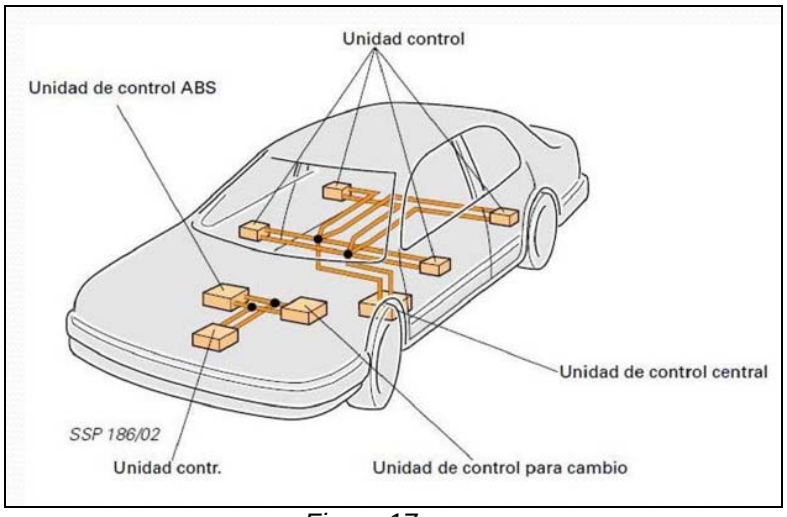


Figura 17.
Ejemplo red CAN [3].

Este protocolo esta basado en el principio “productor/consumidor” donde cada equipo está siempre a la escucha y las transmisiones se realizan bajo el control de un equipo especial (árbitro de bus). Las peticiones de información se construyen de acuerdo a una tabla de órdenes que contiene identificadores de variables. Al decodificar el nombre de la variable asociado a la información que él produce, un dispositivo transmite los valores actuales correspondientes. Esta información es consumida por todos los receptores que reconocen el nombre de la variable. Este modo de funcionamiento garantiza que todos los dispositivos consumidores actualizan su información del proceso de forma simultánea. Todos los nodos, incluido el transmisor están activos mientras hay actividad en el bus, revisan si existen errores (hasta cinco diferentes chequeos de error) y fuerzan la retransmisión en caso de error; todos los nodos deben aceptar el mensaje, en caso contrario se entiende que hay error. En el caso de los receptores, éstos envían un mensaje de “mensaje recibido” cuando el mensaje llega correctamente.

El bus CAN emplea un acceso al bus por prioridades mediante la técnica CSMA/CR (Carrier Sense Multiple Acess/Collition Resolution), resolviendo los conflictos de acceso al bus mediante técnicas no destructivas, permitiendo un tiempo de inactividad garantizado en el caso de colisión. CAN no utiliza direcciones físicas para el nodo, dado que todos los nodos reciben todos lo mensajes, cada uno de ellos decide si el mensaje va dirigido a él o no; esta decisión es tomada según la programación de cada nodo, o el hardware asociado. Pueden emplearse diferentes técnicas de gestión del bus como maestro/esclavo, multiplexado por división de tiempo (TDMA), o daisy Chain.

Como característica esencial del bus CAN está la necesidad del uso de un protocolo para capas más elevadas capaz de realizar la conexión de la aplicación. CAN constituye únicamente una especificación de bajo nivel, y sus posibilidades vienen determinadas en gran medida por el protocolo de las capas superiores elegido, que se elegirá dependiendo del mercado al que se oriente la aplicación, los requerimientos de tiempo real, etc. Por ejemplo, protocolos basados en CAN son: CANopen, DeviceNet y SDS.

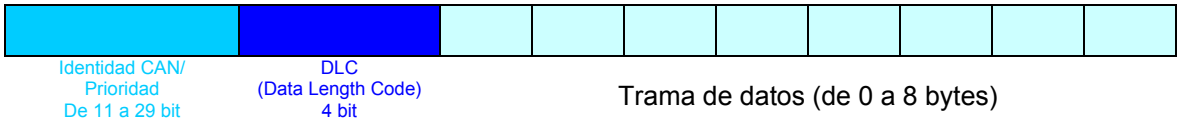


Figura 18. Formato trama de datos CAN [6].

Las principales características de este bus son:

- Velocidad: hasta 1 Mbit/s.
- Topología física: Bus.
- Topología lógica: mestro/esclavo, basado en el modelo productor/consumidor con árbitro de bus.
- Tipo comunicación: Distribuido.
- Número de dispositivos: 127 (limitado por la dirección de nodo) en la misma red física.
- Longitud de la red: 5000 metros, sujeto a velocidad de datos.
- Método de transmisión: bus CAN de par trenzado.

2.3.2.1 CANOpen:

Es un protocolo muy popular en Europa, que facilita el acceso a redes CAN paraa aplicaciones de protocolos de nivel superior, dado que simplifica su empleo al no ser necesario controlar detalles como la temporización, control a nivel de bits, etc. Existen diferentes objetos orientados para datos en tiempo real (process data objects), datos de configuración (service data objects) y funciones especiales (mensajes de emergencia, de sincronismo) y datos de gestión de la red (arranque, control de errores, etc.). Estas especificaciones incluyen diferentes perfiles predefinidos para dispositivos y entornos para aplicaciones industriales específicas, actualmente hay perfiles para módulos de entrada/salida genéricos, controladores de motores, medidas en dispositivos y control en lazo cerrado, encoders y válvulas hidráulicas. Las redes CANopen se han empleado en vehículos, equipos médicos y ferroviarios. La capa de aplicación que incorpora es muy flexible, permitiendo el desarrollo de aplicaciones a medida, pero en cambio, al tratarse de una capa estándar, permite compatibilizar muchos sistemas hardware.

Las principales ventajas de CANopen son:

- Es una especificación abierta, con el estándar europeo EN50325-4. La organización CiA (CAN in Automation) es la encargada de promover los estándares relacionados con el bus CAN.
- Permite interoperabilidad entre diferentes dispositivos.
- Dispone de capacidad en tiempo real.
- Es un sistema modular que engloba dispositivos sencillos y complejos.
- Existen numerosas herramientas de programación y verificación.

Las características principales de CANopen son:

- Velocidad: 1 Mbit/s.
- Topología física: Bus lineal.
- Topología lógica: centralizada, maestro/esclavo.

- El número máximo de dispositivos: 127 (limitado por la dirección de nodo) en la misma red física.
- Longitud de la red: 5000 metros, sujeto a velocidad de datos.
- Método de transmisión: bus CAN de par trenzado.

2.3.3 SDS.

Es uno de los buses basados en CAN más extendidos junto con DeviceNet y CANOpen.

Desarrollado por Honeywell en 1989, se utiliza sobre todo en aplicaciones de sistemas de almacenamiento, empaquetado y clasificación automática. Se define una capa física que incluye alimentación de dispositivos en las conexiones, y la capa de aplicación define autodiagnóstico de nodos, comunicación por eventos y prioridades de alta velocidad.

Al ser un bus basado en CAN, emplea para el acceso al bus la técnica CSMA/CR (Carrier Sense Multiple Acess/Collition Resolution).

Las características principales de este bus son:

- Velocidad: Desde 125 Kbit/s hasta 1 Mbit/s.
- Topología física: la capa física admite cualquier topología.
- Topología lógica: Maestro-esclavo, multicast y punto a punto.
- Número máximo de dispositivos: 64 nodos por red y hasta 124 con repetidores.
- Longitud de la red: Hasta 500 metros a 125Kbit/s. Se puede incrementar las longitudes mediante *Bridges*.
- Método de transmisión: mediante cable de 4 hilos apantallado (2 hilos para alimentación 12-24VDC y 2 hilos para comunicaciones).

2.4. Buses de alta velocidad y funcionalidad media.

Este tipo de buses transmiten información en bytes y se les conoce también como DEVICEBUS. Usan variables digitales y algunas analógicas, y se usan para conectar dispositivos, controladores y PCs con el objetivo de compartir dispositivos de campo entre varios equipos de control. Por tanto, son buses que están situados dentro del nivel control de célula de la pirámide CIM, y su utilización va enfocada a la implementación de redes de célula.

Los buses de este tipo más empleados en la industria actual son:

- DeviceNet.
- COMPOBUS.
- LONWorks.
- MODBUS.
- INTERBUS.
- UNI-TELWAY.
- BITBUS.

2.4.1 DeviceNet.

Desarrollado por Allen-Bradley en 1994 orientado a niveles de automatización medio-bajo, encuadrándose dentro de la pirámide de automatización en algunos casos en el Nivel de Planta y en otros en el Nivel de Célula. Es un sistema abierto y la ODVA (Open DeviceNet Vendor Association) es la encargada de gestionar y organizar la certificación de dispositivos DeviceNet e impulsar el empleo de esta tecnología dentro de la industria.

Las características principales de este bus son:

- Número máximo de nodos: 64.
- Distancia máxima entre 100 y 500 metros.
- Velocidad de transferencia de datos: 125, 250 y 500 Kbit/s. En función de la velocidad varía la distancia máxima.
- Estructura de comunicaciones en bus con línea principal y posibilidad de bifurcación de la línea hacia los nodos (a mayor número de bifurcaciones menor velocidad y distancia).
- Usa terminadores de línea con impedancia de 120Ω aprox.
- Utiliza dos pares trenzados: uno es para alimentación y otro para datos.
- Tamaño máximo del mensaje 8 bytes para cada nodo.
- Topología lógica: basado en modelo productor/consumidor, por ello admite modelo maestro/esclavo, multimaestro, igual a igual, etc., que se traduce en la transmisión de mensajes mediante diferentes métodos: sondeo, envío cíclico, etc.

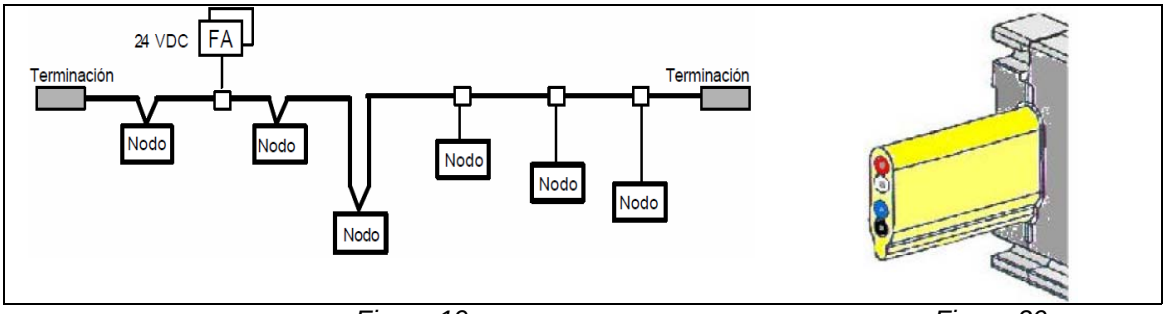


Figura 19.
Estructura general de una red DeviceNet [6].

Figura 20.
Cable DeviceNet [6].

La aplicación habitual de DeviceNet en buses de campo es por ejemplo en ensamblado de piezas, máquinas de soldadura, capitación de sensores distribuidos, sensores inteligentes, válvulas neumáticas, etc.

La principal ventaja de este protocolo es su bajo coste, alta fiabilidad, uso eficiente del ancho de anda e incorporación de tensión de alimentación de 24VDC en el mismo cable del bus. La desventaja más destacable es el ancho de banda limitado y el tamaño limitado de los mensajes.

DeviceNet usa las especificaciones del bus CAN, la capa 2 de DeviceNet es íntegramente CAN, por lo que son aplicables a este protocolo las características de robustez de CAN y añade las especificaciones eléctricas de RS-485. DeviceNet es un conjunto de funciones de alto nivel que incluyen mensajes CAN, donde dichas funciones están orientadas a facilitar las comunicaciones necesarias en procesos de automatización.

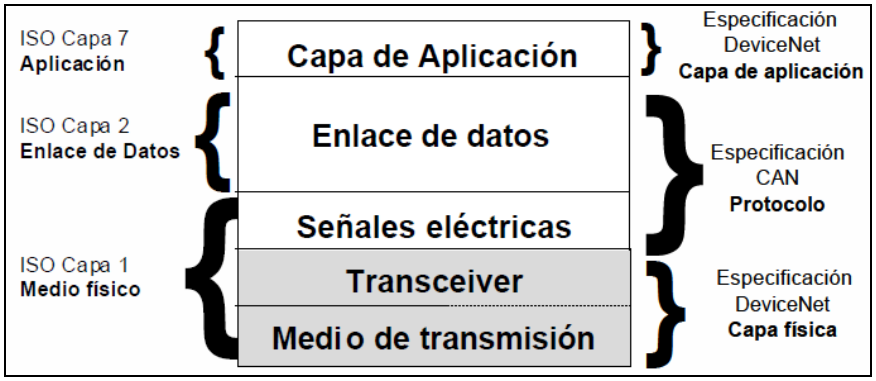


Figura 21.
Capa OSI de DeviceNet [6].

Las funciones que incorpora la capa de aplicación de DeviceNet son:

- Asignación de identificación CAN, estableciendo niveles de prioridad y permitiendo que cada nodo conozca qué mensajes van destinados a él. La configuración se puede realizar mediante software o micro-interruptores.
- Control del tipo de mensajes a transmitir.
- Detección de direcciones duplicadas. Antes de estar activos en la red debe chequearse la no duplicidad.
- Consistencia de datos en el dispositivo: datos de identidad tales como tipo de nodo, fabricante, nº de serie…, datos de enlace de comunicaciones tales como dirección del nodo, velocidad de transferencia…, y datos de configuración del nodo tales como velocidades, consumos…

Una de las principales particularidades de DeviceNet es la existencia de múltiples formatos de mensaje, lo que permite al bus operar de un modo u otro dependiendo del tipo de mensajes enviados, pudiendo mezclar diversos tipos de mensajes. Los tipos de mensajes que se definen son:

- Sondeo: el maestro interroga cada nodo uno a uno para enviar o recibir una actualización del estado del nodo. Este método requiere un mensaje saliente y otro mensaje entrante para cada nodo de la red. Es un método preciso y riguroso, pero poco eficiente a la hora de solicitar información a los dispositivos.
- Strobing: Un nodo solicita broadcast simultáneo a la actualización a todos los nodos. Cada nodo responde a este mensaje mediante en un orden predeterminado por una lista priorizada para permitir que los nodos más críticos sean los primeros en responder.
- Envío cíclico: Los dispositivos son configurados para enviar mensajes de forma regular según el tiempo programado. Este tipo de envío de mensajes se suele emplear juntamente con el modo de “cambio de estado”.
- Cambio de estado: Los nodos únicamente envían mensajes cuando su estado cambia, lo que implica una utilización mínima del bus. El principal problema radica en que el tiempo de recepción no es fijo ya que dependerá del tráfico del bus en el instante en que se desea acceder a él.
- Mensajes explícitos: Este método indica cómo un nodo debe interpretar los mensajes, y se emplea habitualmente en nodos con funcionalidad compleja para así poder enviar mensajes con numerosos parámetros de configuración que es necesario modificar regularmente, pero no tan a menudo como la lectura de datos del proceso que ese nodo realiza.

- Mensajes fragmentados: se emplea en los casos donde es necesario enviar más de 8 bytes de datos en un solo envío. En este caso, se envían varios mensajes de hasta 8 bytes donde viajan los datos fragmentados para posteriormente ser unidos de nuevo.
- Gestión de mensajes no conectados UCMM: la capacidad UCMM (Un Connected Message Manager) permite comunicación de igual a igual, es decir, que no es necesaria la gestión de un maestro en la red sino que dos nodos cualesquiera pueden comunicarse entre ellos de forma directa sin pasar por el nodo maestro. Para ello, los nodos UCMM deben poder conectar todos los mensajes CAN y realizar un filtrado de mensajes para conocer y aceptar únicamente aquello mensajes que van dirigidos a él. Este filtrado se realizar en la capa de software y requiere mayores recursos que un nodo que sólo admite mensajes procedentes de un maestro.

Existe otro modo de configuración similar a PROFIBUS que consiste en usar un fichero "modelo" para cada tipo de dispositivo, de modo que cada parámetro queda asignado a una ubicación concreta. De esta forma es posible intercambiar dispositivos de diferentes fabricantes con igual funcionalidad, aunque es necesario tener cuidado que la equivalencia sea completa para evitar problemas.

2.4.2 COMPOBUS.

Este bus es una particularización de DeviceNet, cuyo principal impulsor es OMROM, Y dispone de dos versiones que se detallan a continuación:

2.4.2.1 COMPOBUS-S:

Para interconectar con dispositivos DeviceNet existe COMPOBUS-S que está orientado a sustituir el cableado tradicional y los terminales múltiples, ideado como una solución para cableados de pequeños sistemas. Tiene la flexibilidad y la sencillez como principales características, aunque otras importantes son:

- Topología física: Bus
- Topología lógica: maestro-esclavo.
- Velocidad máxima: 700 Kbit/s.
- Número máximo de dispositivos: Sólo puede haber 1 maestro en la red y direcciona hasta 32 esclavos. Cada esclavo puede tener hasta 256 E/S.
- Medio de transmisión: Cable plano de 2 hilos. Par trenzado apantallado.
- Longitud: Hasta 100m de línea principal.
- No es compatible con Compobus-S.

2.4.2.2 COMPOBUS-D:

Esta versión de COMPOBUS se permite integrar fácilmente los dispositivos de dicho fabricante y cualquier dispositivo DeviceNet. Las principales características son:

- Topología física: Bus
- Topología lógica: maestro-esclavo.
- Número máximo de dispositivos: Hasta 50 nodos.
- Distancia máxima: 500m.

- Velocidad máxima: 0.5 Mbit/s.
- Medio de transmisión 3 ó 5 hilos.
- Posibilidad de almacenar tipo y número de esclavos en el maestro (lista de SCAN).
- Es un bus equiparable a AS-i aunque con una mayor funcionalidad.

2.4.3 LONWorks (Local Operating Networks).

Es un bus que está basado en el protocolo LONtalk, que consiste en una serie de protocolos que permiten la comunicación inteligente entre los dispositivos de la red. Este protocolo se incluyó en 1999 en el estándar ANSI/EIA 709.1, y el principal impulsor de este bus es Echelon Corporation.

LONworks define su red como una red de control, que en contraste con las redes de datos que tradicionalmente se conocen, está orientada a la transmisión de pocos datos de manera segura y en un tiempo restringido, de ahí que está más enfocado a la automatización de edificios que a la industria.

La comunicación LONworks entre los nodos puede hacerse por control distribuido de igual a igual o bien maestro/esclavo. Se usan nodos inteligentes que permiten distribuir la carga computacional para, por ejemplo, usarse en sensores inteligentes que sólo comunican en casos muy concretos. Esta distribución de las funciones de control permite un incremento muy significativo del rendimiento y la robustez. Para ello, un nodo incorpora lo que se denomina *neurona (neuron chip)*, que consiste en 3 procesadores de 8 bits en paralelo: dos para el protocolo de comunicaciones y el tercero para la ejecución de aplicaciones en el nodo. Esta técnica asegura que la complejidad de una aplicación no interfiera negativamente con el rendimiento de la red. Además, dado que toda la neurona queda incorporada en el mismo chip el coste económico no es significativamente elevado, o incluye funciones específicas dentro del mismo dispositivo como: temporizadores, memoria o incluso funciones específicas realizadas por hardware; facilitando así el desarrollo del software.

LONworks es capaz de funcionar en múltiples medios físicos de transmisión, utilizando los transceiver adecuados para cada uno de ellos. Se puede emplear como medio físico la línea eléctrica de potencia y la topología de red no influye siempre que no se superen los límites marcados.

Las principales características de este bus son:

- Velocidad: Normalmente 78 Kbit/s.
- Topología física: Bus o libre.
- Topología lógica: Maestro/esclavo, punto a punto.
- Número máximo de dispositivos: 248 dominios x 255 subredes x 127 (limitado a 127 en el mismo cable físico).
- Longitud de la red: 2200 metros con topología de bus y con topología libre hasta 500 metros (posible ampliarla con repetidores o hubs).
- Método de transmisión: existen varios pero típicamente par trenzado; la transmisión de alimentación también es posible.

2.4.4 MODBUS.

Modbus es un protocolo de transmisión para sistemas de control y supervisión de procesos (SCADA) con control centralizado, que puede comunicarse con una o varias estaciones remotas (RTU), con la finalidad de obtener datos de campo para la supervisión y control de un proceso. La interfaces de capa física pueden estar configuradas en: RS-232, RS-422 o RS-485.

MODBUS es un protocolo de tipo Petición/Respuesta, por lo que en una transacción de datos se puede identificar al dispositivo que realiza una petición como el cliente o maestro, y al que devuelve la respuesta como el servidor o esclavo de la comunicación. En una red MODBUS se dispone de un equipo maestro que puede acceder a varios equipos esclavos. Cada esclavo de la red se identifica con una dirección única de dispositivo.

En Modbus los datos pueden intercambiarse en 3 modos de transmisión: RTU, ASCII y TCP. Los dos primeros están pensados para ser utilizadas directamente sobre un medio físico serie asíncrono, como por ejemplo RS-232, RS-485, o RS-422. En cambio el modo TCP está desarrollado para funcionar sobre redes que utilizan la arquitectura TCP/IP, lo que permite usar MODBUS sobre redes como Ethernet o WiFi.

2.4.4.1 Modo RTU:

Desarrollado por Modicon para la comunicación de PLC, pero también se utiliza para el control básico de parámetros en las unidades, es uno de los estándares de bus de campo más utilizados y aceptados desde finales de 1970.

Modbus RTU funciona sobre RS-485 y está basado en un sistema maestro/esclavo, funcionando a velocidades de transmisión de hasta 115Kbit/s. Estaba inicialmente pensado para comunicaciones en bus serie y como ventaja principal tiene el buen aprovechamiento del canal de comunicación, mejorando la velocidad de la transmisión de los datos. El inconveniente es que requiere una gestión de tiempos entre bytes recibidos para saber cuando empiezan y terminan las tramas.

Las principales características de este bus son:

- Velocidad: dependiendo de la velocidad de transmisión de enlace serie.
- Topología física: Punto a punto o bus.
- Topología lógica: centralizada maestro/esclavo, sobre RS-485.
- Número máximo de dispositivos: 247.
- Longitud máxima de red: se basa en estándares RS-485, que es 1200 metros. Su pueden lograr longitudes mayores mediante el empleo de repetidores. Número máximo de nodos es 247 en una sola red.
- Medio de transmisión: par trenzado.

2.4.4.2 Modo ASCII:

Los datos se codifican como caracteres ASCII entre el “0” (16#30) y el “9” (16#39) y entre “A” (16#41) y “F” (16#46), además de utilizar 3 caracteres especiales: carácter “:” (16#3ª) para marcar el comienzo de la trama y el par de caracteres no imprimibles “CRLF” (16#0D, retorno de carro, y 16#0A, salto de línea) como delimitadores de fin de la trama.

Este formato tiene dos grandes ventajas:

- Ofrece una facilidad de detección del principio y del fin de trama gracias a los campos de inicio y fin (caracteres ":" y "CRLF"), con independencia de los tiempos de la transmisión del canal de comunicación.

- Permite trabajar con equipos de procesamiento lento sin tener que bajar la velocidad de comunicación siempre que tengan buffers de almacenamiento de los datos recibidos.

Los inconvenientes son que requiere un mayor ancho banda que MODBUS RTU para el envío de la misma petición o respuesta, o visto de otra manera, para el mismo ancho de banda el envío de una trama con ASCII es más lento que con RTU.

2.4.5 INTERBUS.

Interbus o Interbus-S, es un protocolo desarrollado a mediados de los años 80 por Phoenix Contact y varias instituciones técnicas alemanas, con el objetivo de simplificar el cableado de señal en aplicaciones industriales. En 1990 Phoenix Contact decidió revelar las especificaciones de Interbus, y como tal, este protocolo se convirtió en el primer sistema de bus de campo independiente de fabricante.

El protocolo Interbus ha seguido desarrollándose desde entonces, y ahora está controlado por el Interbus Club, una organización dirigida por los usuarios del protocolo.

Interbus ha sido normalizado mediante la norma europea EN 50254 y según DIN 19258.

La capa física está basada en RS-485 y cada dispositivo actúa como repetidor. En la capa de transporte la información se encapsula en tramas sin incluir en los mensajes información de direccionamiento, por lo que los datos se hacen circular por la toda la red.

Es un bus de alta eficiencia y velocidad, para aplicaciones con pocos nodos y pequeños conjunto de entradas/salidas por nodo. Poco buses son tan rápidos y eficientes como INTERBUS, aunque es muy sensible al corte de comunicación por apertura del anillo en cualquiera de los nodos.

Las principales características de este bus son:

- Velocidad: 500Kbit/s y 2Mbit/s.
- Topología física: anillo.
- Topología lógica: centralizada, sobre RS-485.
- Número máximo de dispositivos: hasta 512, con 4096 puntos de E/S.
- Longitud de la red: 400 metros entre dispositivos y hasta 13 kilómetros de longitud de red.
- Método de transmisión: par trenzado o de fibra óptica.

2.4.6 UNI-TELWAY.

Es un estándar para la comunicación entre componentes del sistema de control (PLC, terminales MMI, variadores de velocidad, controles numéricos, equipos de pesaje, etc), que ofrece fácil comunicación con dispositivos tales como la supervisión y equipos de gestión.

Este bus requiere de:

- Una estación maestra que supervisa el enlace de datos y controla su funcionamiento, y además gestiona los derechos de comunicación de las distintas estaciones conectadas.

- De 1 a 27 estaciones esclavas que procesan los diferentes datos transportados a través de la red. Cabe señalar que una estación puede tener varias direcciones de enlace de datos (direcciones lógicas definidas por el hardware o el software en función del tipo de dispositivo).

Una estación maestra siempre tiene la dirección de enlace de datos 0. No puede haber hasta 27 dispositivos esclavos que comparten 98 direcciones de enlace de datos. Es aconsejable el uso de direcciones de enlace de datos consecutivos por razones de rendimiento.

UNI-TELWAY utiliza comunicación a niveles iguales y envía mensajes de:

- Maestro a esclavo (1).
- Esclavo a maestro (2).
- Esclavo a esclavo (3).

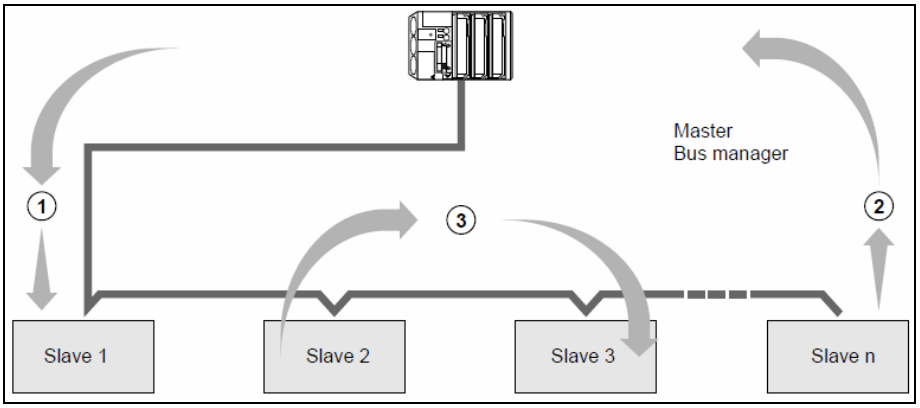


Figura 22.
Comunicación UNITEL-WAY [19].

La comunicación esclavo a esclavo, que están unidos entre sí, se realiza en dos pasos de forma automática sin que sea necesaria ningún tipo de acción del procesador o el programa de aplicación de la estación PLC maestra:

- El enrutamiento del mensaje al módulo principal (esclavo n ° 2 para el módulo de UNI-TELWAY del maestro).

- Dirección automática de este mensaje a la estación de destino (esclavo n ° 3).

El bus UNI-TELWAY y su protocolo de aplicación UNI-TE coordinan la actividad entre dispositivos inteligentes y permiten:

- La comunicación de una aplicación a otra, por ejemplo, entre los PLC.

- La comunicación desde una aplicación para el sistema de un dispositivo (por ejemplo: la lectura de bits, palabras, la gestión de los modos de funcionamiento, etc).

Las principales características de este bus son:

- Velocidad: Desde 1,2Kbit/s a 19,2Kbit/s.
- Topología física: Anillo.
- Topología lógica: paso de testigo, sobre RS-232/485.
- Número máximo de dispositivos: 28 (1 maestro y 27 esclavos).
- Longitud máxima de la red: 1000m sin repetidores.
- Método de transmisión: par trenzado apantallado.

2.4.7 BITBUS.

Introducido por Intel a principios de los 80, es un bus maestro-esclavo soportado sobre RS-485 y normalizado en IEEE-1118. Debido a su sencillez ha sido adoptado en redes de pequeños fabricantes e integradores. En su capa de aplicación se contempla la gestión de tareas distribuidas.

Este bus esta soportado por la organización europea *"Bitbus European User's Group"*.

Las características principales de este bus son:

- Velocidad: Desde 62,5 Kbit/s hasta 2,4Mbit/s.
- Topología física: Bus lineal.
- Topología lógica: Maestro-esclavo sobre RS-232/485.
- Número máximo de dispositivos: 28 por segmento y hasta 250 con repetidores.
- Longitud de la red: 300 metros a 375Kbit/s y 1200 metros a 62,5Kbit/s.
- Método de transmisión: par trenzado apantallado con conector tipo-D 9 pines.

2.5. Buses de altas prestaciones:

La información que transmiten este tipo de buses es en palabras o tablas entre dispositivos y controladores o PCs, y por tanto están situados en el nivel de planta de la pirámide CIM ya que su misión es generar órdenes de ejecución hacia el nivel de célula en base a la información recibida. Por tanto, estos buses se emplean para la creación de redes de control o supervisión que permiten transmitir al operador los datos necesarios para conducir el proceso, así como el envío de cambios de consigna en el mismo.

A este tipo de buses se le conoce como FIELDBUS y los más empleados en la actualidad son:

- PROFIBUS.
- ControlNet.
- Fieldbus Foundation.
- WorldFIP/FIP.

2.5.1 PROFIBUS.

Desarrollada en el año 1987 por empresas alemanas (ABB, Bosch, Klöckner Möller, Siemens…) y 5 institutos de investigación alemanes, es el bus de campo más usado con más de 20 millones de nodos instalados.

En 2002 se añade PROFINET, que es la versión de PROFIBUS para Ethernet.

Este tipo de bus trabaja con nodos maestros y nodos esclavos. Los nodos maestros se llaman también activos y los esclavos pasivos.

Existen tres perfiles para este bus:

2.5.1.1 PROFIBUS-DP:

- Orientado a sensores/actuadores enlazados a procesadores (PLCs) o terminales, por tanto aplicable al nivel de campo del modelo CIM.
- La capa física está basada en RS-485.
- Se distingue entre maestro clase 1 (monitorización y diagnóstico), maestro clase 2 (centralizadores de información) y esclavos (sensores y actuadores).
- El transporte se realiza mediantes tramas, enviando datagramas en modo broadcast o multicast.
- Implementa las capas 1, 2 y 7 según niveles del modelo OSI. La capa de aplicación es compleja debido a la necesidad de mantener la integridad en el proceso de paso de testigo.

2.5.1.2 PROFIBUS-PA:

- Para control de proceso y cumpliendo normas especiales de seguridad para la industria química (seguridad intrínseca). Este perfil está orientado para su aplicación al nivel de proceso del modelo CIM.
- Utiliza la norma IEC 11158-2 para la comunicación síncrona entre sensores de campo que utiliza modulación sobre la propia línea de alimentación de los dispositivos y puede utilizar los antiguos cableados de instrumentación 4-20mA, y para el nivel de proceso se tiende a la utilización de Ethernet.

2.5.1.3 PROFIBUS-FMS:

- Para comunicación entre células de proceso o equipos de automatización. La evolución de PROFIBUS hacia la utilización de protocolo TCP/IP para enlace al nivel de proceso hace que este perfil esté perdiendo importancia. Este perfil está dirigido a su aplicación en niveles de célula y planta del modelo CIM.
- Es una compleja capa de aplicación que permite la gestión distribuida de procesos al nivel de relación entre células con posibilidad de acceso a objetos, ejecución remota de procesos, etc.
- Los dispositivos se definen como dispositivos de campo virtuales (VFDs).
- Los servicios disponibles definidos en MMS (Manufacturing Message Specification ISO 9506).

Las características generales resumidas de este bus son:

- Velocidades de transmisión: Desde 9.6Kbit/s hasta 12 Mbit/s.
- Número máximo de estaciones: 127 (32 sin utilizar repetidores).
- Distancias máximas alcanzables (cable de 0.22 mm de diámetro) a 93.75 Kbit/s 1200 metros; a 187.5 Kbit/s 600 metros; a 500 Kbit/s 200 metros.
- Estaciones pueden ser activas (maestros) o pasivas (esclavos). Además, se pueden configurar sistemas multimaestro o más simples maestro-esclavo.
- Acceso al medio entre maestros se arbitra mediante paso por testigo.
- La comunicación maestro-esclavo se realiza mediante polling.

2.5.2 ControlNet.

Es un bus de alta velocidad, muy seguro, robusto y para grandes distancias; promovido por Allen-Bradley. No está soportado por muchos fabricantes y resulta de elevado precio por nodo. Se suele utilizar para interconexión de redes de PLC y computadores industriales en aplicaciones de alta velocidad y ambientes muy críticos.

ControlNet es una red productor/consumidor que soporta la comunicación de múltiples jerarquías y la priorización de mensajes.

Para acceso al bus emplea la técnica CTDMA (Concurrent Time Domain Multiple Access).

ControlNet define una única capa física basada en cable RG6/U (utilizado en televisión por cable) y se basa en un controlador ASIC de Rockwell.

Las características que distinguen a ControlNet de otros buses de campo es que incluye el soporte para cables totalmente redundantes, y que toda la comunicación en ControlNet es estrictamente planificada y altamente determinista.

La capa de aplicación de ControlNet está basada en la capa CIP que también se utiliza en DeviceNet y EtherNet/IP; y por tanto se rige por los estándares de dichos protocolos.

Las principales características de este bus son:

- Velocidad: 5Mbit/s.
- Topología física: Estrella, árbol o bus. También admite topología en anillo pero para ello se necesitan repetidores especiales.
- Topología lógica: maestroo/esclavo basado en modelo productor/consumidor.
- Número máximo de dispositivos: Hasta 48.
- Longitud de la red: Desde 250 a 1000 metros. Se puede llegar hasta 20Km usando repetidores.
- Método de transmisión: cable coaxial mediante conectores BNC, y recientemente se han introducido conectores TNC.

2.5.3 Fieldbus Foundation.

Un bus orientado sobre todo a la interconexión de dispositivos en industrias de proceso continuo, creado por la Sociedad de Instrumentación, Sistemas y Automatización (ISA) con el objetivo de sustituir el habitual bucle de corriente 4-20 mA, de la conexión punto a punto entre los elementos y el equipo de control.

Este bus se normalizó como ISA SP50 e IEC-ISO 61158, y en la actualidad existe la asociación *"Fieldbus Foundation"* formada por varios fabricantes que gestionan su normalización.

En 1996 lanzaron el protocolo H1 (31.25 Kbit/s) y en 1999 lanzaron el protocolo HSE (High Speed Ethernet):

2.5.3.1 Protocolo H1 (nivel 1):

La capa física sigue la norma IEC 11158-2 para comunicación a 31,25 Kbit/s, y por tanto, compatible con Profibus-PA, su principal contendiente. Presta especial atención a las versiones que cumplen normas de seguridad intrínseca para industrias de proceso en ambientes combustibles o explosivos. Utiliza par trenzado y es posible la reutilización de antiguos cableados de instrumentación analógica 4-20 mA.

En su capa de transporte utiliza un protocolo sofisticado orientado a objetos con múltiples formatos de mensaje, y se distinguen dispositivos con capacidad de arbitración (Link Master) y normales.

Existen servicios para configuración, gestión de diccionario de objetos en nodos, acceso a variables, eventos, carga descarga de ficheros y aplicaciones, ejecución de aplicaciones, etc.

Foundation Fieldbus no soporta medios redundantes a nivel H1. La redundancia puede ser realizada mediante el planificador activo de enlace (LAS).

Sus características principales son:

- Diseñado para control de procesos, comunicaciones a nivel de campo e integración de dispositivos.
- Velocidad de comunicación: 31,25 Kbit/s.
- Tipos de comunicación: paso por testigo, cliente-servidor, productor-consumidor…
- Puede operar con un par trenzado, llevando señal y alimentación en los mismos hilos.
- Puede usar fibra óptica.
- Soporta aplicaciones de seguridad intrínseca "Intrinsic Safety (IS)".
- No soporta redundancia.

2.5.3.2 Nivel 2, HSE (High Speed Ethernet):

Está basado en Ethernet de alta velocidad (100 Mbit/s) y orientado al nivel de control de la red industrial.

Sus características principales son:

- Velocidad hasta 100 Mbit/s.
- Integración de dispositivos diversos.
- Integra subsistemas e información empresarial.

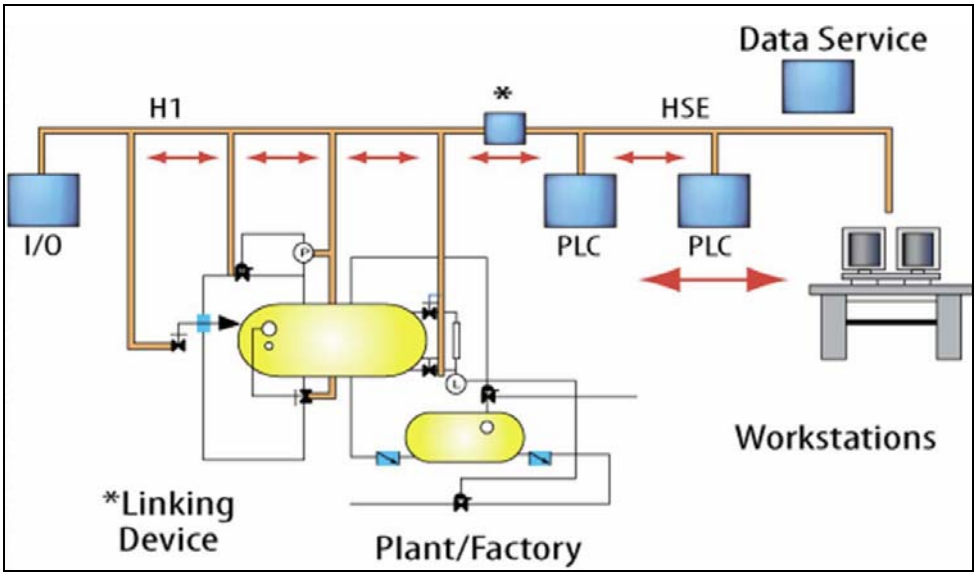


Figura 23.
Ejemplo protocolo H1 y HSE [8].

2.5.4 FIP/WorldFIP.

WorldFIP fue desarrollado como una ampliación del protocolo FIP original, en un intento de cumplir los requisitos para un bus de campo internacional. Originalmente desarrollado por un conglomerado de instituciones francesas y ahora gestionado y mantenido por la Organización WorldFIP. Al igual que PROFIBUS, fue uno de los primeros buses de campo de pleno derecho a desarrollar y se registra en la norma EN 50170, IEC 61158 e IEC 61784. WorldFIP es notable en que fue el primer bus de campo para poner en práctica un modelo productor-consumidor y contiene incorporado apoyo para el cableado redundante. También es bastante único porque consta de una sola variante diseñada para su uso tanto a nivel H1 y H2, pudiendo operar en cualquiera de las velocidades: 31,25 Kbit/s, 1 Mbit/s o 2,5 Mbit/s dependiendo de los requisitos.

WorldFIP difiere de los otros sistemas de buses de campo entre otras cosas por el uso de un protocolo único y sencillo que cubre tanto la información en tiempo real como la de control de los sistemas de instrumentación.

Único: porque solo se necesita un protocolo mientras que otros buses necesitan dos o tres clases de protocolos haciéndolos más difícil de aprender, aparte de tener que utilizar interfaces extras dentro del sistema para realizar conversiones.

Sencillo: porque es fácil de aprender, los términos utilizados se ajustan a formatos del estándar internacional como el MMS (Manufacturing Message Specification) con lo que se adapta también a los estándares internacionales de buses de campo.

Las características principales de este bus son:

- Velocidades de los datos de 31.25Kbit/s, 1 Mbit/s o 2.5 Mbit/s sobre par trenzado y 5 Mbit/s en fibra óptica.
- Topología física: bus lineal.
- Número máximo de dispositivos: 64 nodos por segmento de cable, hasta 4 segmentos a través de repetidores.

- Longitud de Segmento: 1 Km o más dependiendo de la velocidad de los datos, cable y número de nodos.
- Método de transmisión: cable troncal con cables laterales conectados a cada nodo de las dos siguientes maneras: conector sub-miniatura “9-pin D-type” para entornos normales o conector circular para entornos con condiciones extremas.
- Topología lógica: modelo “productor-consumidor” con un planificador de bus centralizado.
- La impedancia característica de los cables es de 150 Ω. El cable troncal requiere terminación para adaptarse a la impedancia de los cables y no producir reflexiones.

2.6. Comparativa general entre buses de campo actuales.

De acuerdo a lo comentado hasta ahora, a continuación se presenta un cuadro resumen de las características principales de los diferentes buses recogidos en este trabajo, a fin de realizar una comparativa entre los mismos que nos permitan evaluar que bus es más adecuado para la aplicación en las comunicaciones de la Planta estándar de Ciclo Combinado.

En la Tabla 1 sólo se incluyen los buses “tradicionales”, ya que los basados en Ethernet se analizan más adelante:

BUS	PROPIETARIO/ SOPORTE	VARIANTES	TOPOLOGIA FÍSICA	TIPO COMUNICACIÓN	MEDIO FISICO	VELOCIDAD	DISTANCIAC ABLEADO	NODOS/ Nº DISPOSITIVOS	ACCESO AL BUS	NORMA
Buses de alta velocidad y baja funcionalidad										
AS-i	Siemens (Alemania)	-	Cualquiera	Sondeo maestro/ esclavo.	Cable especial DIN VDE 0295	Ciclo de 5ms del maestro, para conocer estado de todos esclavos.	100 m	Un maestro direcciona hasta 31 esclavos. Cada esclavo puede conectar hasta 4 sensores y 4 actuadores todo/nada.	-	IEC 62026-2 EN 50295
CAN	Bosch y CiA (Alemania)		Bus	Productor/ consumidor.	Par trenzado	De 50 Kbit/s a 1 Mbit/s.	5000 m	Hasta 127	CSMA/ CD	ISO 11898 ISO 11519 EN 50325-4
SDS	Honeywell		Cualquiera	Maestro/esclavo. Multicast. Punto-punto.	Cable de 4 hilos	De 125 Kbit/s a 1 Mbit/s.	500 m	64 nodos	CSMA/ CD	ISO 11898 (Basado CAN)
Buses de alta velocidad y funcionalidad media										
DeviceNet	Allen Brandley (Rockwell)		Bus	Productor/consumidor. Maestro/esclavo. Multicast. Punto-punto.	Par trenzado	125 Kbit/s 250 Kbit/s 500 Kbit/s	500 m 250 m 100 m	64	CSMA/ CD	ISO 11898 ISO 11519 Basado en CAN
COMPOBUS	OMRON	COMPOBUS-D COMPOBUS-S	Cualquiera	Sondeo maestro/ esclavo.	Cable plano. Par trenzado.	500 Kbit/s 750 Kbit/s	500 m	Hasta 50 nodos Un maestro direcciona hasta 32 esclavo que direcciona hasta 256 E/S	-	-
LONWorks	Echelon Corporation	-	Bus	Maestro/ esclavo. Punto a punto.	Par trenzado. Posibilidad de alimentación.	78 Kbit/s	De 300 m a 2200 m	127	-	ANSI/EAI 709.1
MODBUS	Modicon (EEUU)	Modbus-RTU ModBus-ASCII	Bus	Productor/ consumidor. Unicast/Broadcast.	Par trenzado.	De 300 bps A 19,2 Kbit/s	1000 m	248	-	ANSI/ TIA/ EIA-232-F-1997. ANSI/ TIA/ EIA-485-A-1998.
INTERBUS	Phoenix Contact (Alemania)	INTERBUS-S	Anillo	Paso de testigo.	Par trenzado.	De 500 Kbit/s a 2 Mbit/s	De 400 m a 13 Km	512 (4096 de E/S)	-	DIN 19258 IEC 61158
UNI-TELWAY	-	-	Anillo	Paso de testigo.	Par trenzado (RS-232/485).	De 1,2 Kbit/s A 19,2 Kbit/s	1000 m	28 (1 maestro y 27 esclavos)	-	-
BITBUS	Intel (EEUU)	-	Bus lineal	Maestro-esclavo.	Par trenzado.	De 62,5 Kbit/s A 2,4 Mbit/s	300 m 1200 m	28	-	IEEE-1118

Buses de altas prestaciones										
PROFIBUS	Industria (Alemania)	PROFIBUS-DP (Siemens)	Bus	Paso de testigo	Par trenzado apantallado.	9,6Kbit/s	1200 m	32		EN50170 Vol.2
				Sondeo Activo-pasivo		19,2Kbit/s	1200 m			DIN STD 19245
				-		93,75Kbit/s	1200 m			
				-		187,5Kbit/s	600 m			
				-		500Kbit/s	200 m			
ControlNet	ODVA	-	Cualquiera	Productor/ consumidor	Cable coaxial con conector BNC. Fibra óptica.	5 Mbit/s	De 250 m a 3000 m	48	CTDMA	Basado en CAN
Fieldbus Foundation	ISA	H1	Bus lineal		Par trenzado. Fibra óptica.	31,25 Kbit/s			-	IEC 11158-2 IEC 61158
WorldFIP	Industria Francia	FIPIO (Scheneider)	Bus lineal		Par trenzado apantallado	31,25Kbit/s	1900 m	32	Centralizado (árbitro de bus)	EN 50117 Vol.3 NFC46 (601-605) IEC 1158-2
		FIPway (Scheneider)			Fibra óptica	1 Mbit/s 2,5 Mbit/s 5 Mbit/s	750 m 500 m			

TABLA 1.
Comparativa general entre buses de campo actuales.

3. Redes LAN industriales:

3.1. Modelo OSI (ISO7498/1984).

El modelo OSI (Open System Interconnection) de ISO (International Standars Organization) fue una propuesta para la estandarización de las redes de ordenadores que permite interconectar sistemas abiertos y ofrece al usuario la posibilidad de garantizar la interoperatividad de los productos entre sí.

El modelo OSI por si mismo no es una arquitectura de red, puesto que no especifica el protocolo que debe usarse en cada capa. Posteriormente, estos protocolos fueron implementados por los fabricantes de software de comunicaciones ajustándose a las funciones de cada una de las capas.

Este modelo establece siete niveles en los cuales se definen siete capas cuyas funciones son las siguientes:

- NIVEL 1: en este nivel se define la Capa Física que proporciona las condiciones físicas como son los niveles de corriente, tensión, modulación, frecuencia, etc. que son necesarias para hacer efectiva la comunicación sobre un medio de transmisión cableado o aéreo.

- NIVEL 2: en este nivel se define la Capa de Enlace que establece el mecanismo de acceso al medio de transmisión y el direccionamiento de las estaciones, de forma que durante un tiempo definido sólo una estación podrá enviar datos a través del medio de transmisión que se utilice. Los datos se estructuran en tramas para su correcta interpretación y se comprueba la transmisión sin errores de los mismos.

- NIVEL 3: en este nivel se define la Capa de Red cuya su misión es encaminar los datos que han de viajar a través de varias subredes, así como controlar los posibles problemas de congestión de la red.

- NIVEL 4: en este nivel se define la Capa de Transporte, encargada de garantizar la seguridad en el transporte y la coherencia de los datos transmitidos. Es el encargado de coordinar tareas con el control de flujo, la segmentación en bloques y la confirmación de acuse de recibo correcto de los datos. Para realizar estas funciones se establecen conexiones que garantizan que ambos extremos están preparados para el intercambio de datos.

- NIVEL 5: en este nivel se define la Capa de Sesión que se encarga del control de comunicación y su sincronización, junto con el control del uso que hace cada usuario de la red.

- NIVEL 6: en este nivel se define la Capa de Presentación que se codifican los datos en lenguaje de programación.

- NIVEL 7: en este nivel se define la Capa de Aplicación con los servicios, es decir, aplicaciones de comunicación a las que el usuario puede acceder directamente o a través de un interfaz de usuario.

3.1.1 Aplicación del modelo OSI a redes industriales.

Durante muchos años se ha considerado Ethernet para aplicaciones industriales, pero el rendimiento no determinista ha excluido en gran parte su uso generalizado en industria.

Ethernet ha evolucionado hasta convertirse en variantes dirigidas específicamente a abordar las cuestiones principales relacionadas con el rendimiento.

La mayoría de los usuarios finales espera que Ethernet sea la respuesta para la estandarización y la interoperabilidad entre productos de diferentes fabricantes. Sin embargo, el estándar Ethernet fue diseñada para redes de TI y generalmente no es adecuado para el control preciso en tiempo real tales como para el control de movimiento y posición. Organizaciones de bus de campo se han enfrentado al reto de hacer a Ethernet adecuado para aplicaciones industriales mediante la incorporación de una versión de su protocolo estándar sobre la una trama Ethernet.

Los dispositivos Ethernet habilitados son capaces de proporcionar fácil acceso a las interfaces de páginas web, generación de e-mail y hacer uso de las funciones de red Ethernet estándar, tales como la obtención de información de la hora, el direccionamiento de red, etc.

Ethernet ha evolucionado a un punto en el que se puede controlar de una manera que permita la entrega determinista y se pueda llevar a cabo un control distribuido en tiempo real. Esto se ha hecho mediante la adopción de las especificaciones originales de Ethernet y la adición de protocolos/controles de transmisión, lo que significa que esto ya no es Ethernet "estándar". La interoperabilidad con Ethernet estándar sigue siendo relativamente fácil de lograr con la eliminación de las restricciones, mientras que mantiene los beneficios de la plataforma original de Ethernet.

En los buses de redes industriales únicamente están implementadas las capas de los niveles 1, 2 y 7 del modelo OSI, aunque últimamente con los buses basados en Ethernet se está implementando protocolos en los niveles 3 y 4.

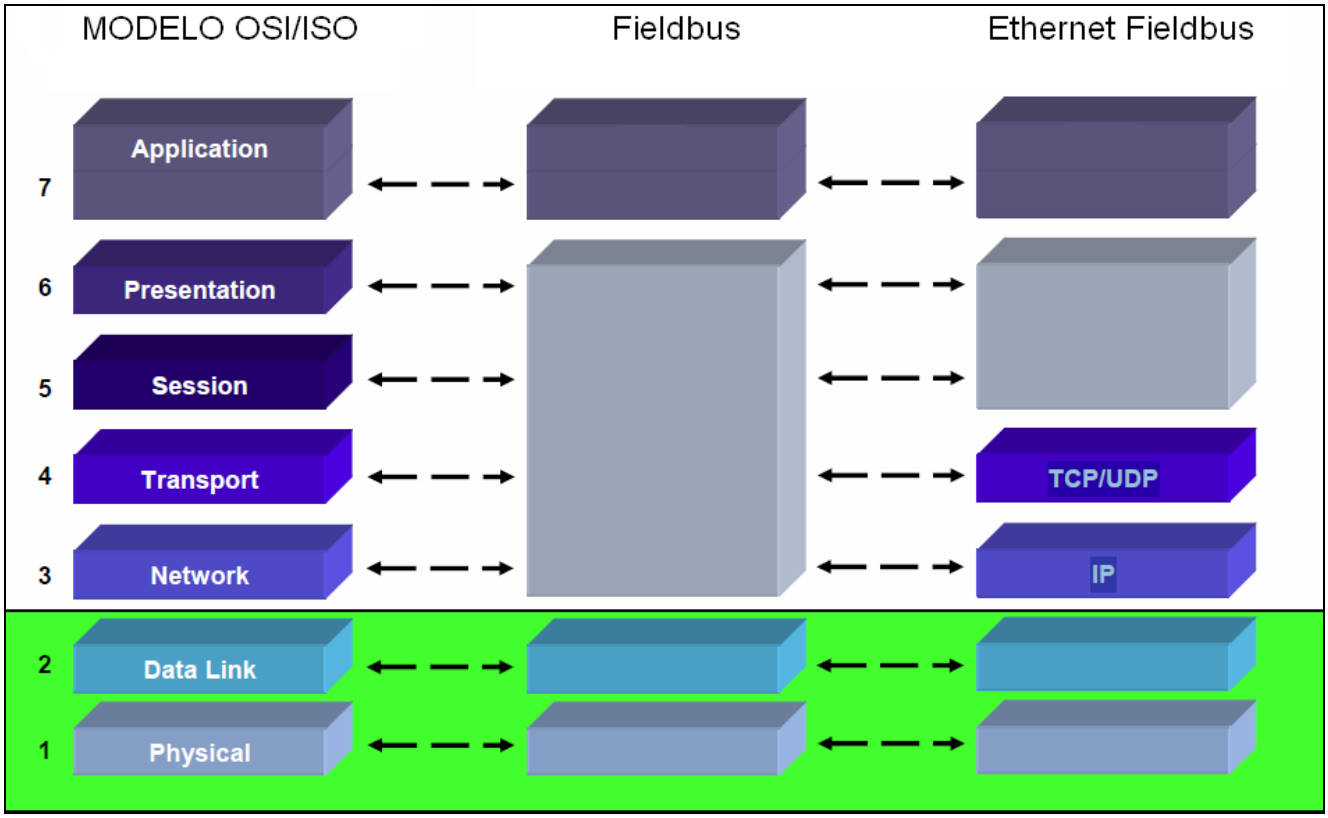


Figura 24.
Comparativa niveles OSI/ Fieldbus [11].

3.2. Tipos de redes LAN industriales:

La mayoría de buses tradicionales han evolucionado para ser utilizados sobre redes Ethernet, para lo cual han desarrollado especificaciones a nivel de la capa de transporte del nivel OSI manteniendo en las capas inferiores su especificación original.

Suelen ser redes situadas en los niveles más altos de la pirámide CIM.

Las buses tradicionales con especificaciones basadas en Ethernet que actualmente se están comenzando a utilizar son:

- Modbus TCP.
- Ethernet/IP.
- CYP Sync.
- EtherCAT.
- PROFINET.
- FieldBus HSE.

3.1.2 Modbus TCP.

La especificación MODBUS TCP/IP fue desarrollada en 1999 para encapsular el paquete MODBUS estándar dentro de la estructura de mensajería TCP/IP.

Modbus TCP/IP es actualmente el protocolo Ethernet industrial más popular debido a la sencillez de la aplicación utilizando el estándar Ethernet.

Las características principales de este protocolo son:

- Velocidad: 10 Mbit/s, 100 Mbit/s, 1 Gbit/s.
- Topología física: En general en estrella pero también se emplean topologías en bus, anillo o árbol.
- Tipo comunicación: centralizada, maestro/esclavo.
- Longitud de la red: número teóricamente ilimitado de nodos y distancia aunque siendo realista limitado por la velocidad de transmisión.
- Método de transmisión: utiliza Ethernet estándar.

3.1.3 Ethernet/IP.

Es un protocolo basado en Ethernet para aplicaciones de automatización industrial utilizando el conjunto de protocolos Ethernet IP/UDP/TCP estándar.

Ethernet/IP también ha sido desarrollado para ofrecer características de seguridad y funcionalidad en tiempo real, son los llamados CIPSafe y CIPSync.

Ethernet/IP tiene una base instalada grande y creciente debido a la simplicidad de la aplicación utilizando el estándar Ethernet, su compatibilidad con las normas anteriores de la CIP y su longevidad en el mercado.

Sus características principales son:

- Velocidad: 10 Mbit/s, 100 Mbit/s, 1 Gbit/s.
- Topología física: Generalmente en estrella pero también se puede usar topologías en bus o árbol.
- Tipo comunicación: centralizada, maestro/esclavo.
- Longitud de la red: teóricamente ilimitada, sin embargo los tiempos de ciclo y red son un factor limitante del rendimiento.
- Método de transmisión: Utiliza la norma Ethernet.

3.1.3.1 CIP Sync:

CIP Sync es una extensión del protocolo industrial común (CIP), y por tanto proporciona funcionalidad de sincronización para redes basadas en CIP, como Ethernet/IP, y es una implementación de IEEE1588.

El CIP estándar fue desarrollado originalmente por Rockwell Automation, pero ahora es mantenido por ODVA (Open DeviceNet Vendors Association). El estándar CIP Sync parece ser una adición muy reciente.

El estándar IEEE1588 proporciona un medio para sincronizar el número de relojes de los diversos dispositivos presentes en una red. En lugar de garantizar que los datos de proceso se transmiten por un maestro con una pequeña fluctuación del mensaje, CIP Motion proporciona un medio para hacer una marca de tiempo en los datos de proceso, a fin de compensar las variaciones de tiempo de transmisión.

Las características principales de este protocolo son:

- Velocidad: 100Mbit de Ethernet actual.
- Topología física: Generalmente estrella pero puede ser bus o árbol.
- Tipo comunicación: distribuido (IEEE1588 proporciona un medio para que los esclavos recojan el mejor reloj maestro en la red).
- Número máximo de dispositivos: teóricamente ilimitado, aunque los tiempos de ciclo en última instancia lo limitan.
- Longitud de la red: teóricamente ilimitada, sin embargo los tiempos de ciclo y red son un factor limitante del rendimiento.
- Método de transmisión: Ethernet estándar.
- Admite redundancia de redes.

3.1.4 EtherCAT.

Es un bus de campo en tiempo real para Ethernet industrial que ha sido desarrollado por Beckhoff y entregado posteriormente al Grupo de Tecnología abierto EtherCAT, para mantener y desarrollar la norma. El sistema de bus modifica el hardware Ethernet estándar y utiliza una estructura de tipo de bus repetitiva para pasar los datos de dispositivo a dispositivo. La eficiencia del protocolo se obtiene mediante la incorporación de los datos para muchos dispositivos dentro de una trama de Ethernet, para obtener un rendimiento del 90% del ancho de banda disponible.

Las características principales de este bus son:

- Velocidad: 100 Mbit/s.
- Topología física: bus replicado.
- Tipo comunicación: típicamente estrella pero también admite bus o árbol.
- Número máximo de dispositivos: 65.536, sin embargo la tasa de actualización de red se verá afectada.
- Longitud de la red: En teoría ilimitada, sin embargo la velocidad de actualización lo limita.
- Método de transmisión: la tecnología Ethernet estándar, con gestión de tiempo.
- Admite redundancia de redes.

3.1.5 PROFINET.

Es un estándar de Ethernet industrial para la automatización que incluye la comunicación de bus de campo en toda la planta. PROFINET puede manejar transmisiones Ethernet estándar y transmisiones en tiempo real a velocidades por debajo de milisegundos.

La comunicación PROFINET es escalable en tres niveles:

- *Comunicación basada en TCP/IP:* que permite tiempos de ciclo del orden de 100 ms. Es la preferida para la comunicación entre los controladores.
- *Comunicación en tiempo real (RT):* permite tiempos de ciclo del orden de 10 ms y es muy adecuado para su uso E/S distribuidas.
- *Comunicación asíncrona en tiempo real (IRT):* permite tiempos de ciclo de menos de 1 ms y es por tanto muy adecuado para su uso en aplicaciones de control de movimiento.

Todos estos niveles de comunicación pueden coexistir en la misma línea de bus junto con las comunicaciones de Ethernet estándar.

Profinet está algo por detrás de Modbus TCP/IP y Ethernet IP en términos de instalaciones efectuadas, ya que no ha estado en el mercado durante el mismo tiempo, sin embargo la popularidad de PROFIBUS asegura que esta tendencia vaya en aumento a medida que los nuevos productos se van sacando al mercado.

- Velocidad: 100 Mbit/s y superior.
- Topología física: Generalmente estrella y también puede ser bus, árbol o malla.
- Tipo comunicación: centralizada.
- Número máximo de dispositivos: hasta 200 puntos de E/S. Una de las principales ventajas de PROFINET en comparación con PROFIBUS es que se puede tener más nodos en la red.
- Longitud de red: la longitud, la velocidad y la topología de la red dependen de los componentes que se eligen para la red. Con componentes externos de fibra óptica se puede llegar hasta 26 kilómetros. En una red eléctrica la distancia máxima entre dos dispositivos es de 100 metros.
- Método de transmisión: Ethernet basada en VLAN.
- Admite redundancia de redes.

3.1.6 Fieldbus HSE.

La tecnología de la *Foundation Fieldbus Ethernet de Alta Velocidad (HSE)* proporciona una rentable alta velocidad, como columna vertebral de todos los procesos de automatización de la planta integrando las aplicaciones de control con los servidores de datos optimizadas como OLE for Process Control (OPC).

HSE soporta todo el ámbito de la tecnología FOUNDATION Fieldbus, incluyendo los bloques de función estándar y descripciones de dispositivos, y aprovecha al máximo el bajo coste y fácil disponibilidad de los componentes Ethernet.

HSE complementa, más que sustituye, al bus de campo H1 de 31,25 Kbit/s, y por lo tanto cumple con la demanda del mercado en todo el mundo para una solución de red de control unificado.

HSE integra H1 para aplicaciones de control de procesos distribuidos con una alta velocidad (100 Mbit/s) y la integración de la información con los sistemas de gestión de la planta.

Los protocolos de señalización de capa de enlace de datos y física HSE se especifican en la norma IEEE 802.3 e ISO/IEC 8802-3 normas. Sin embargo, HSE incluye 11 nuevas especificaciones por encima de la capa física IEEE 802 y la "pila" comunicación para cumplir con los requisitos de Ethernet en aplicaciones industriales.

3.1.7 Comparativa entre buses basados en Ethernet.

Bus tradicional	Bus Ethernet	Protocolo	Normativa
Modbus-RTU	Modbus-TCP	TCP/IP	IEC 61158 / IEC 61784
PROFIBUS	PROFINET	TCP/IP, UDP/IP	IEC 61158 / IEC 61784
DeviceNet ControlNet	Ethernet/IP (CIP)	TCP/IP, UDP/IP	IEC 61158 / IEC 61784 Estándar ODVA Ethernet/IP
Foundation Fieldbus H1	Foundation Fielbus High Speed Ethernet (HSE)		
CANopen	EtherCAT	EtherCAT, EtherCAT/UDP	IEC 61158 / IEC 61784-3 IEC/PAS 62407 ISO 15745-4

TABLA 2.
Comparativa entre buses basados en Ethernet.

4. Comunicaciones OPC.

Aunque no es un protocolo de bus de campo, OLE for Process Control (OPC) forma parte de muchas redes industriales en los niveles superiores proporcionando una interfaz estandarizada para la comunicación de datos industriales. Mantenido por la Fundación OPC, el estándar OPC originales (ahora denominado OPC Data Access) utiliza RPC y DCOM para permitir la comunicación en tiempo real de los valores de proceso a través de Ethernet con un modelo cliente-servidor. Varias otras variantes de OPC también se han desarrollado, incluyendo OPC de acceso a datos históricos que permite la recuperación de los valores almacenados, OPC de intercambio de datos para la comunicación de dos vías usando un modelo de servidor-servidor y OPC XML de acceso a datos que utiliza XML para la comunicación. OPC se combina generalmente con el software túnel que lleva a cabo las transacciones locales con la interfaz OPC y las transmite a través de una red privada virtual segura.

5. Criterios de selección de un bus de campo.

Al diseñar una aplicación concreta de bus de campo lo habitual es preguntarse tanto qué tipo de bus elegir como cual el más adecuado, y el criterio de selección suele girar siempre entorno a los siguientes aspectos:

Coste:

Lo primero que lleva a la elección del bus de campo es la posibilidad de ahorro en los costes. La primera pregunta de todas las que el técnico en automatismos ha de responder es si económicamente es ventajosa o no la utilización de un bus de campo.

Prestaciones:

Se trata ante todo de una exigencia, ya que si se decide que un determinado bus de campo es económicamente ventajoso, hay que asegurarse de que sus prestaciones satisfarán las exigencias de la aplicación.

Interoperatividad:

Si la respuesta al análisis de las dos cuestiones anteriores es positiva, hay que estar seguro que los diversos elementos del automatismo necesarios para un montaje concreto, son realmente capaces de funcionar conjuntamente según las necesidades del trabajo.

Perennidad:

Por último, una vez aceptada la validez y la versatilidad de la instalación de un bus de campo, no conviene olvidar la duración requerida para este tipo de instalación: la rentabilidad de las inversiones necesita una cierta prudencia ante las nuevas tecnologías. Aunque actualmente la tecnología de este tipo de bus de campo está perfectamente consolidada, el multiplicarlos excesivamente puede no garantizar siempre la rentabilidad de las inversiones que requiere.

Los dos primeros criterios, coste y prestaciones, sirven para realizar un análisis técnico-económico de las instalaciones con bus de campo. Los dos siguientes, interoperatividad y perennidad, reflejan sobre todo la confianza de los usuarios ya que hay que tener en cuenta el análisis del mercado, las estrategias de los fabricantes y su respeto a las normas.

6. Ciberseguridad en monitorización de procesos industriales.

6.1. Características de los sistemas de monitorización y control.

Hoy en día, al hablar de sistemas de monitorización y control en tiempo real el término que mayor aceptación tiene es el de SCADA. Sin embargo, históricamente existían diferentes catalogaciones de este tipo de sistemas, siendo las principales de ellas las siguientes:

- **Industrial Control System (ICS):** Este término, sistemas de control industrial, se puede considerar como una categoría que englobaría los sistemas SCADA, los DCS, así como los basados en PLCs. En general el término ICS se aplica a sistemas de monitorización y control orientados principalmente a usos industriales, por lo que en él se engloban los sistemas empleados en los sectores de electricidad, agua, petróleo, gas, química, etc.

- **Supervisory Control And Data Acquisition (SCADA):** Los sistemas SCADA, o sistemas de control de supervisión y adquisición de datos, son un caso particular de ICS, cuya principal característica respecto a las otras dos categorías (DCS y sistemas basados en PLCs) es la gestión centralizada de todo el sistema. Hoy en día, el término SCADA ha alcanzado un significado más amplio, englobando a cualquier sistema que monitoriza y/o gestiona de forma centralizada y en tiempo real un conjunto de dispositivos finales.

- **Distributed Control System (DCS):** Los DCS, o sistemas de control distribuido, son otro caso concreto de ICS, cuya principal diferencia respecto a los SCADA es que el control en este caso está repartido geográficamente, ubicándose en diferentes instalaciones donde se encuentran desplegados los elementos controlados. Es decir, un DCS podría considerarse como un conjunto de sistemas SCADA locales, que conforman un único sistema de monitorización sin ningún puesto de control central.

- **Sistemas basados en Programmable Logic Controllers (PLC):** Los sistemas de control basados en PLCs, o controladores lógicos programables, son en esencia sistemas SCADA de tamaño y complejidad reducidos. Dado que los programas informáticos que monitorizan y controlan los actuadores residen en estos dispositivos, en los casos en los que el proceso no es muy complejo estos PLCs se emplean como componentes principales del sistema.

Todos estos sistemas de monitorización y control tienen tres necesidades fundamentales que cubrir:

- **Confidencialidad:** Es la propiedad de la información por la que se garantiza que es accesible únicamente para las personas autorizadas. Por ejemplo, proteger un ordenador con una contraseña es una buena medida para aumentar la confidencialidad de los datos almacenados en él.

- **Integridad:** Se refiere a la exactitud de los datos, concretamente a la necesidad de asegurar que éstos no han sido manipulados o alterados. Por ejemplo, un error en las comunicaciones puede suponer una pérdida o una distorsión de la información transmitida, por lo que para evitarlo se pueden emplear mecanismos que comprueben la integridad de dicha información.

- **Disponibilidad:** Es la capacidad de un sistema de estar operativo para realizar las funciones para las que ha sido diseñado. Por ejemplo, cuando una página web no puede ser visitada, se puede decir que ese sistema tiene un problema de disponibilidad.

Mientras que en un sistema informático tradicional la prioridad suele ser la confidencialidad, seguida de la integridad y finalmente de la disponibilidad, en un sistema de monitorización y control en tiempo real lo primordial es garantizar la disponibilidad del servicio y del sistema. Esto es debido

principalmente a que su objetivo esencial es mantener en funcionamiento el proceso para el que ha sido creado, además de considerarse como tareas vitales para las empresas e incluso en algunos casos Infraestructuras Críticas para la sociedad.

Este enfoque de prioridades se ha mantenido desde la aparición de estos sistemas hasta la actualidad: los sistemas de monitorización y control en tiempo real son muy robustos funcionalmente, ofreciendo un servicio casi ininterrumpido. Sin embargo, esta desproporcionada priorización de la disponibilidad, unida a otras causas, ha generado una ausencia de seguridad notable en algunos aspectos. Por ejemplo, se puede tender a no cifrar la información, consiguiendo así mayor rapidez ya que el cifrado y descifrado de la información puede influir negativamente en la disponibilidad. Pero en contrapartida se penalizaría la seguridad, ya que cualquier individuo podría capturar la información en un formato comprensible.

De entre las diferentes clases de sistemas de monitorización y control existentes, los más utilizados son los denominados SCADA. El acrónimo SCADA (Supervisory Control And Data Acquisition) se puede traducir como control de supervisión y adquisición de datos.

Es decir, se denomina sistema SCADA a aquel conjunto de redes, equipos y programas que monitorizan en tiempo real procedimientos industriales y tareas complejas, a partir de la información obtenida a través de sensores, comunicándose con los dispositivos actuadores para transmitirles las órdenes adecuadas y pudiendo controlar el proceso de forma automática mediante un software especializado.

Estos sistemas reciben y envían información. Cuando en respuesta a una señal de salida del sistema, nueva información vuelve al mismo como entrada, se produce lo que se llama retroalimentación (feedback). La finalidad de esta continua comunicación es optimizar, vigilar, y en su caso, verificar la modificación de diversos aspectos del funcionamiento del sistema.

Toda la información que se genera con estos procedimientos puede estar disponible tanto para los usuarios directamente implicados en los procesos productivos, como para otros usuarios supervisores dentro de la organización (control de calidad, control de producción, almacenamiento de datos, etc.).

Esta definición puede resultar ambigua, pero esto se debe a que la variedad de sistemas SCADA es muy amplia, tanto en tipología como en funcionalidad, alcance y otras características. Puede referirse desde a sistemas que monitorizan y gestionan los procesos de una planta nuclear hasta a una red de control y seguimiento del estado de unas escaleras mecánicas.

Así pues, la frontera entre un sistema SCADA y un sistema de control remoto es muy difusa, pudiéndose incluir en esta denominación los ICS (Industrial Control System, sistema de control industrial), los DCS (Distributed Control System, sistema de control distribuido) o sistemas basados directamente sobre PLCs (Programmable Logic Controllers, controladores lógicos programables). Ofreciendo una descripción genérica que englobe a todos ellos, se les puede denominar sistemas de monitorización y/o control en tiempo real de forma, en mayor o menor medida, centralizada.

En definitiva, son sistemas que cuentan con un control central desde el que se puede conocer lo que ocurre en distintos puntos a través de la medición y transmisión de diferentes parámetros, pudiendo actuar desde este puesto central para modificar o ajustar estos parámetros en los puestos remotos. Este control puede ejercerse de forma automatizada estableciendo unas reglas de actuación para el sistema ante las posibles situaciones y valores de los parámetros.

Tradicionalmente, los sistemas SCADA se referían a aquellos que supervisaban y controlaban procesos industriales, ciñéndose la gestión principalmente a válvulas, bombas, sensores, interruptores y demás elementos mecánicos. Se trataba de sistemas aislados que permitían una

gestión centralizada y eficiente, ya que al conocer el estado de todos los elementos del proceso industrial, la toma de decisiones se simplificaba de manera notable.

En cambio hoy en día los sistemas SCADA suelen ser sistemas instalados en Sistemas de Control situados en la parte más alta de las redes de comunicación industrial, con interacción con PC/servidores de diferentes zonas de red de la planta industrial mediante el uso de Ethernet, para consulta de información del proceso productivo por las diferentes áreas de la compañía, con las consiguientes repercusiones que podría tener cualquier incidente de seguridad en el funcionamiento general de la planta y del proceso productivo.

A continuación, se exponen las diferentes amenazas a las que puede estar expuesto el sistema de control, dando previamente unas pinceladas a lo que se ha considerado el ataque cibernético más importante de la historia (Stuxnet), que ha dado origen a esta revolución en el campo de la ciberseguridad:

6.2. La historia de Stuxnet.

Tras el ataque cibernético más grande de la historia que Irán sufrió el 27 de septiembre de 2010, en el cual se vieron afectados por un virus de una potencia sin precedentes, denominado Stuxnet, los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, los diferentes paises han comenzado a establecer las estrategias de Ciberseguridad Nacional en un documento estratégico, que sirve de fundamento a los diferentes Gobiernos para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas [34]. Los expertos consultados afirman que el 60% de los ordenadores iraníes se podrían haber visto afectados, igual que el 20% en Indonesia y el 8% en India. El virus Stuxnet se convierte en agente durmiente y se puede accionar a distancia en el momento que su creador lo desee sin que el usuario sea consciente.

Dada su complejidad sin precedentes es imposible que haya sido creado por un hacker en solitario. Todo apunta a un equipo de profesionales que han dispuesto de medios y dinero suficiente y al menos seis meses de tiempo para prepararlo.

Los expertos consideran que el Stuxnet es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas como centrales eléctricas y nucleares, presas e industrias químicas.

La complejidad del programa es tal que los especialistas en seguridad informática que lo han examinado están convencidos de que no puede ser obra de un mero pirata informático. La mayoría opina que hay un Estado detrás y que es el primer ejemplo de guerra cibernética.

6.3. Algunas amenazas (actuales y futuras).

La valoración de las amenazas actuales y futuras es una parte importante de la evaluación de las prioridades a tener en cuenta en las crecientes medidas de seguridad. Será preciso tener presente la prevención, detección, respuesta, mitigación y recuperación junto con la cooperación internacional en su caso. A continuación se describe brevemente, algunas de las amenazas que se han hecho más populares en los últimos tiempos por las repercusiones e impacto que han tenido en aquellos lugares y equipos donde se han producido [35].

6.3.1 DDoS.

Los ataques DDoS (Distributed Denial of Service) son una forma relativamente sencilla y efectiva de hacer caer a una Web. Las acciones se pueden realizar de forma voluntaria

siguiendo las instrucciones dadas para iniciar el ataque a una hora señalada en una convocatoria mediante foros en la Red o utilizando redes de ordenadores previamente infectados por virus (botnet) de forma que los usuarios ni siquiera son conscientes de que participan.

Los ataques DDoS no siempre tienen un trasunto ideológico. Cada vez más responden a puras extorsiones.

6.3.2 Botnets.

Los botnets (robots de la Red) son redes de ordenadores zombis. Las redes han aumentado de modo exponencial, y se emplean para realizar ataques, envíos masivos de correo basura y espionaje contra empresas. Un botnet se crea infectando ordenadores sin que sus propietarios lo sepan. Cada máquina reclutada por el virus se pone en contacto sigilosamente con el cibercriminal a la espera de sus órdenes.

Los ciberdelincuentes bien, de modo aislado, o en una organización, construyen sus botnets y los venden o alquilan a empresas que desean mandar correo basura, bombardear o espiar a otras empresas, o robar datos bancarios. El virus puede enviarse por correo electrónico aunque lo habitual es ponerlo en páginas web, fundamentalmente que tengan muchas visitas. Una vez dentro del ordenador, el virus descargará un programa y lo instalará, es el bot, el lazo entre el ordenador infectado y la net, la red que permite su control remoto.

6.3.3 Zeus.

Zeus es un virus de tipo botnet (troyano) que se propaga por los navegadores, tanto Explorer como Firefox. El malware recopila información del usuario y contraseñas de internet y redes sociales, utilizándolas para suplantar la identidad y realizar robo de datos bancarios, datos de tarjetas de crédito o enviar spam. Miles de empresas de todo el mundo han caído en esta pandemia digital. Además a primeros de noviembre de 2010 se ha detectado que el virus Zeus ha afectado a dispositivos móviles.

6.3.4 Amenazas futuras.

El futuro de las amenazas se centran en dos grandes áreas: ingeniería social (manipulación de formularios, llamadas no solicitadas, mensajes,…) y ataques multivectoriales donde se combinan diferentes tipos de soporte (correo electrónico, mensajes en blogs, redes sociales, wikis,…., voz, vídeo, audio, etc.) [35].

6.4. Organismos e instituciones Españolas con competencias en Ciberseguridad.

La ciberseguridad en España, a diferencia de otros países, no ha sido definida todavía en una legislación específica y completa en materia de ciberseguridad aunque si existe legislación distribuida en distintos ámbitos ministeriales pero no se desarrollado todavía una política común que refleje el ámbito nacional y estratégico de la ciberseguridad. El Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica fue regulado en el Real Decreto 2/2010, de 8 de enero, pero cubre únicamente las administraciones públicas.

Existen otras leyes nacionales, europeas e internacionales que abordan la seguridad, tales como: Ley Orgánica de Protección de Datos (LOPD), la Ley General de las Telecomunicaciones (LOT) y la Ley de la Sociedad de la Información y Comercio Electrónico (LSI-CE).

Es necesaria la gestión de la ciberseguridad, además de en la administración pública, en otros sectores importantes de organizaciones, empresas, infraestructuras críticas y los ciudadanos. Los organismos e instituciones más sobresalientes que tienen competencias en la gestión de la ciberseguridad son [35]:

- El Centro Criptológico Nacional (CCN) dependiente del Centro Nacional de Inteligencia (CNI) que tiene a su cargo la gestión de la seguridad del ciberespacio en las tres administraciones del Estado.

- El CCN-CERT es el Centro de alerta nacional que coopera con todas las administraciones públicas para responder a los incidentes de seguridad en el ciberespacio y vela también por la seguridad de la información nacional clasificada.

- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) que depende del Ministerio del Interior.

- El Instituto Nacional de Tecnologías de la Comunicación (INTECO) dependiente del Ministerio de Industria, Turismo y Comercio, encargado de velar por la ciberseguridad de las PYMES y los ciudadanos en el ámbito doméstico.

- El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional, responsables de combatir la iberdelincuencia.

- La Agencia Española de Protección de Datos, dependiente del Ministerio de Justicia, así como las Agencias de Protección de Datos de la Comunidad de Madrid y de la Generalitat de Cataluña.

6.5. Guías y estándares de Ciberseguiridad en relación a los sistemas SCADA.

Al margen de las normativas de carácter legal y de obligado cumplimiento, existen algunas guías y estándares de carácter orientativo en relación a los sistemas SCADA.

Principalmente son:

6.5.1 Guía CCN-STIC-480 en materia de Seguridad en Sistemas SCADA.

El Centro Nacional de Inteligencia (CNI) a través de su Centro Criptológico Nacional (CCN), realiza diversas actividades relacionadas con la seguridad de las TIC. Una de las funciones más destacables del CCN en esta materia es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC de la Administración, materializada en la existencia de la serie de documentos “CCN-STIC”, que se elaboran para dar cumplimiento a los cometidos del CCN y a lo reflejado en el ENS.

La guía CCN-STIC-480 en materia de sistemas SCADA es de aplicación a todos los sistemas SCADA, aunque cobra especial importancia en las industrias que trabajen con Infraestructuras Críticas, y está orientada a cualquier organismo, institución, industria o empresa que cuente con sistemas SCADA. Sus objetivos son los siguientes:

- Presentar la problemática planteada por los sistemas SCADA y sus vulnerabilidades, su impacto y la necesidad imperativa de controlar su seguridad.

- Describir las técnicas necesarias para analizar los riegos derivados de dichos sistemas.

- Enumerar todos los elementos, sean estos técnicos o no, que tienen un papel en la seguridad de los sistemas SCADA, estableciendo los ámbitos en los que intervienen y presentando los mecanismos adecuados para que su actuación sea efectiva.

- Presentar algunas soluciones técnicas ante determinadas amenazas, referenciando los documentos donde se puede encontrar más información de cada una de ellas.

6.5.2 IEEE PC37.1™ Draft Standard for SCADA and Automation Systems.

El Institute of Electrical and Electronics Engineers (IEEE) es una asociación técnico-profesional de ámbito internacional dedicada, entre otras materias, a la estandarización. Sus principios inspiradores son promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.

Entre otros estándares, el IEEE ha publicado el IEEE PC37.1 Standard for SCADA and Automation Systems (IEEE PC37.1), estándar de referencia en materia de definición, especificación, análisis e implementación de sistemas SCADA y sistemas de automatización en las subestaciones eléctricas.

El IEEE PC37.1 va dirigido a ingenieros y su objetivo no es otro que facilitarles las pautas necesarias para diseñar los sistemas SCADA y los sistemas de automatización de las subestaciones eléctricas y fijar sus especificaciones.

6.5.3 ENISA “Protecting Industrial Control Systems. Recommendations for Europe and Member States”.

ENISA (European Network and Information Security Agency) es la agencia europea dedicada a la seguridad de las redes y de la información, entre cuyos objetivos está reforzar la capacidad de la UE y de los Estados miembros y, en consecuencia, la de la comunidad empresarial para prevenir, tratar y dar respuesta a los problemas de seguridad de las redes y de la información, proporcionando asistencia y asesoramiento, generando conocimiento especializado y fomentando la cooperación entre los sectores público y privado.

Para la consecución de estos objetivos reúne a diferentes expertos en referencia a muy diversos aspectos, publicando los resultados de sus investigaciones y colaboraciones. Uno de estos informes, “Protecting Industrial Control Systems. Recommendations for Europe and Member States”, es de especial relevancia en lo referente a los sistemas de monitorización y control en tiempo real. Este informe incluye un exhaustivo anexo (Anexo III, “ICS Security Related Standards, Guidelines and Policy Documents”) en el cual se exponen los diferentes estándares y normas de seguridad establecidas por diferentes organizaciones.

7. Diseño de arquitectura de comunicaciones de la Planta estándar de Ciclo Combinado.

La Planta estándar de Ciclo Combinado es un proyecto conjunto llevado a cabo por la Ingeniería española Empresarios Agrupados AIE© y empresa estadounidense General Electric GE©, con el fin de establecer una Planta de Ciclo Combinado estándar (109FB), que integra la turbina monoeje 9FB de GE®, con el fin de ofrecer un diseño modular para una Planta de Ciclo Combinado a coste bajo y un alto rendimiento de funcionamiento.

7.1. Introducción.

7.1.1 Definición termodinámica de un Ciclo Combinado.

Un Ciclo Combinado no es más que la integración de dos o más ciclos termodinámicos de producción de potencia de modo que interactúen para obtener una mejora sustancial del rendimiento.

El nombre de ciclo combinado surge al unir en cascada el ciclo Brayton abierto y Rankine cerrado y han de situarse en una ubicación donde confluya la cercanía de un gasoducto y una línea eléctrica de alta tensión, ambos con capacidad suficiente.

El tiempo de construcción es 2 a 3 años y una de las ventajas de las centrales de ciclo combinado es la flexibilidad.

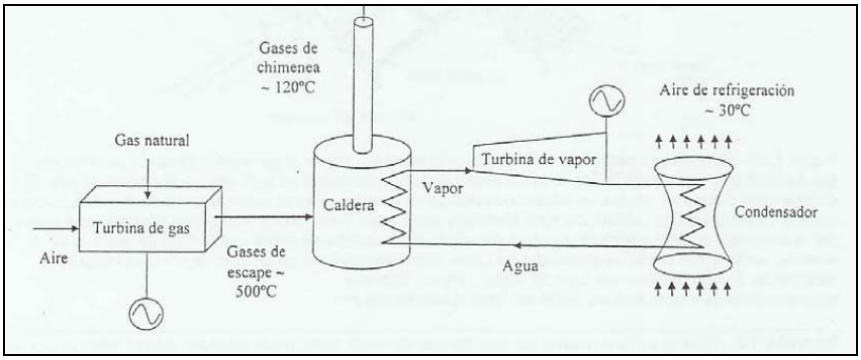


Figura 25.
Esquema general de un Ciclo Combinado.

El rendimiento del ciclo combinado es superior al que se obtendría por separado de cada uno de los ciclos que lo componen, y en todos los casos el ciclo de mayor temperatura (A) cede calor al de menor temperatura (B). De una forma muy simplificada, si se supone el rendimiento de los ciclos de Carnot que funcionen a temperaturas T_A y T_B y que el ciclo superior cede calor a la misma temperatura a la que lo absorbe el interior T_{AB}, se obtiene el máximo rendimiento (η_{max}) que podría alcanzar la planta de ciclo combinado:

$$\eta_{\max} = \left(1 - \frac{T_{AB}}{T_B}\right) + \left(1 - \frac{T_A}{T_{AB}}\right) - \left(1 - \frac{T_{AB}}{T_B}\right) \cdot \left(1 - \frac{T_A}{T_{AB}}\right)$$

Con la tecnología actual, el ciclo Brayton alcanza temperaturas de más de 1500K en el foco caliente y cede calor al foco frío a 700-900 K. El ciclo Rankine puede alcanzar temperaturas de más de 800 K en el foco caliente y casi temperaturas ambientales en el frío. La combinación de dos ciclos de Carnot entre dichas temperaturas conduciría a rendimientos en torno al 75 %. El empleo de ciclos reales distintos al de Carnot y presentando pérdidas, reduce notablemente dicho valor, pero se pueden conseguir rendimientos en torno al 60% en algunas configuraciones actuales.

De entre todas las alternativas de posibles ciclos combinados, en la práctica la configuración usada casi universalmente en la actualidad es el ciclo compuesto por un ciclo de gas y uno de vapor Brayton y Rankine respectivamente, acoplados mediante una caldera de recuperación de calor (HRSG). Este tipo de instalaciones se emplean fundamentalmente para la producción de energía eléctrica y constituyen, de entre todas las que evolucionan siguiendo ciclos termodinámicos, las que alcanzan mejores rendimientos, aunque el coste del kWh producido queda afectado por la necesidad de emplear combustibles ligeros de buena calidad,

generalmente gas natural. Básicamente, la integración de estos dos ciclos consiste en intercambiar calor en la caldera de recuperación, de forma que el ciclo de mayor temperatura cede el calor no convertido en trabajo al de menor temperatura; es decir, se aprovecha parte del calor de los gases de escape de la turbina de gas, que se cedería al ambiente como energía residual si dicho ciclo se emplease aislado, para producir trabajo en el ciclo de la turbina de vapor.

El esquema simplificado es el que se representa en la siguiente Figura 26:

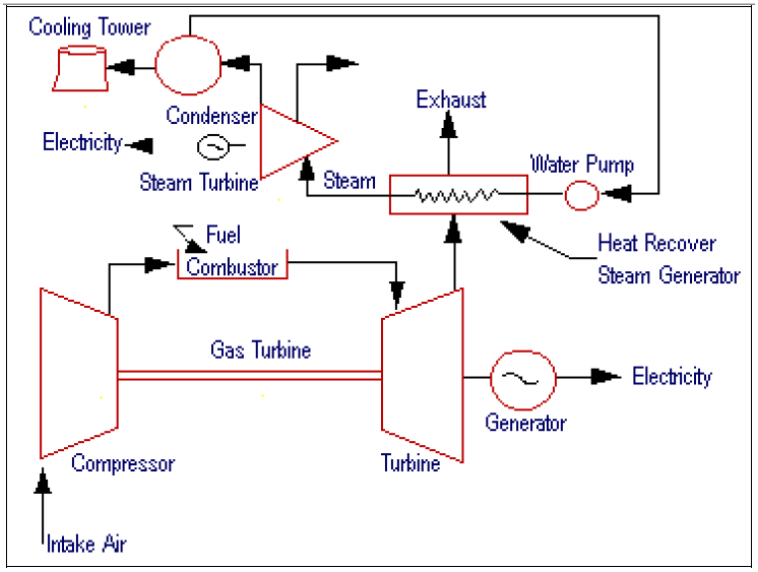


Figura 26.
Esquema simplificado de un ciclo combinado de gas y vapor.

En la Figura 27 se muestra una implantación típica actual, compuesta de un eje único sobre el que las turbinas de gas (GT) y vapor (ST) se disponen a ambos lados del alternador. El condensador se coloca axialmente en el mismo nivel que la turbina de vapor y la caldera de recuperación (HRGS) es de circulación natural, con los gases circulando horizontalmente y los bancos de tubos verticales:

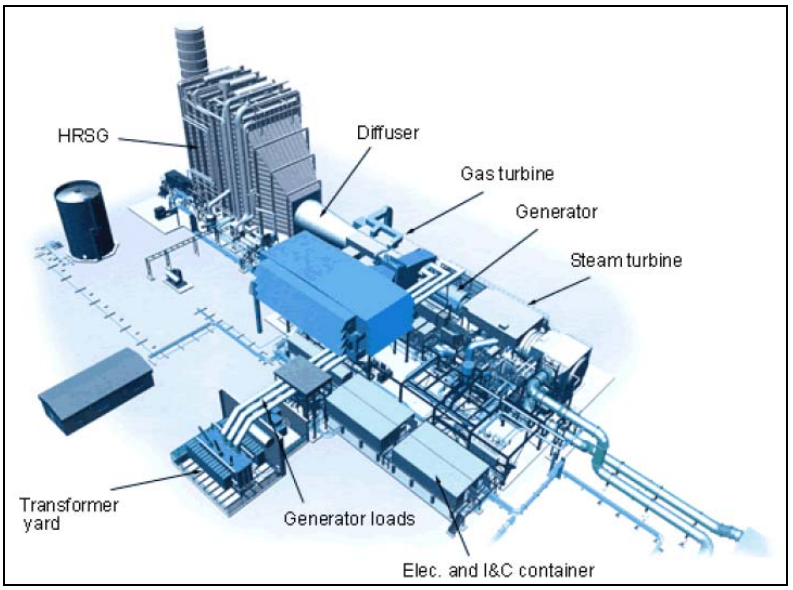


Figura 27.
Implantación de un ciclo combinado de gas y vapor con montaje en eje único [30].

La turbina de gas es el ciclo de alta temperatura y al que se le va a aportar todo el combustible como fuente de calor (salvo cuando haya post-combustión). En su integración dentro del ciclo combinado, se encarga de la mayor parte de la potencia y de ceder a la caldera los gases de combustión a una temperatura lo suficientemente elevada como para producir vapor. La caldera de recuperación es el principal nexo entre ambos ciclos. Los gases de escape de la turbina de gas transfieren el calor al agua en una serie de intercambiadores para producir vapor en las condiciones deseadas. Finalmente, el ciclo de vapor aprovecha el calor recuperado en la caldera para la producción de potencia.

La central de ciclo combinado también cuenta con una chimenea de by-pass a la salida de cada turbina de gas que permite que la central trabaje como ciclo simple (sólo actuando las turbinas de gas) o como ciclo combinado. En este segundo caso es cuando actúa la caldera de recuperación de calor y la chimenea para expulsar los gases sobrantes. Hay una caldera de recuperación de calor por cada turbina de gas.

En los primeros diseños de ciclos combinados la potencia que generaba la turbina de vapor suponía un tercio de la total, aportando el ciclo de gas otros dos tercios. De esa forma se conseguían rendimientos superiores al 40%. Con la evolución de las tecnologías de ha conseguido incrementar el rendimiento de las turbinas de gas y se ha mejorado la integración de ambos ciclos, elevándose la aportación del de vapor a casi el 40% del total, recuperándose mucho más calor.

Actualmente la tendencia de las plantas de ciclo combinado es a la modularización, ya que permite reducir el coste de producción, reduciendo el coste de mantenimiento a lo largo del ciclo de vida de la planta, y un aumentando el rendimiento termodinámico.

La tecnología fundamental empleada en la actualidad es suministrada por la empresa GE (General Electric) que es uno de los fabricantes a nivel mundial más importantes de todo tipo de tecnología para la generación de energía eléctrica (turbinas, generadores, centrales nucleares de nueva generación, etc).

7.1.2 Planta de energía estándar 109FB-SS de GE Energy©.

El STAG (Steam and Gas) 109FB-SS de planta de energía estándar integra las tres tecnologías principales de GE, optimizadas en una única planta de energía. Gracias al alto rendimiento y la fiabilidad de las turbinas de gas 9FB de tecnología de clase F, probadas en todo el mundo, se ha realizado un último paso evolutivo para mejorar aún más el rendimiento de dicha turbina como centro del sistema de ciclo combinado.

El diseño del STAG 109 FB-SS de ciclo combinado consta de los siguientes componentes [30]:

a. Turbina de gas 9FB:

Es la última evolución de la tecnología de turbinas de gas de clase F para aplicaciones con ciclos combinados de alta eficiencia, y cuyas características han sido probadas durante más de 12 millones de horas de funcionamiento.

b. Tecnología avanzada HEAT (High Efficiency Advanced Technology):

La tecnología avanzada HEAT que incorpora la turbina de vapor, está diseñada para un máximo rendimiento y eficiencia en los sistemas de ciclo combinado GE. Las características incluyen la tecnología de alta reacción del rotor de tambor HP, una alta eficiencia de campana y difusor LP, y una amplia gama de LSB con capacidad para condiciones de contrapresión específicas del sitio.

c. Enfriador de hidrógeno 450H:

El diseño compacto del enfriador de hidrógeno 450H le permite ser configurado para su colocación entre la turbina de vapor y turbina de gas. Además de su diseño robusto para una mayor eficiencia, el enfriador tiene una estructura de estator sellada herméticamente para prevenir fugas de gas y fuel, lo que reduce el mantenimiento y aumenta la fiabilidad.

d. Heat Recovery Steam Generator (HRSG):

La caldera de recuperación de calor (HRSG) está construida con una especificación rigurosa y contrastada por GE, que contribuye a la optimización del sistema de ciclo combinado y ayuda a ofrecer un menor coste de electricidad.

e. Mark VI DCS (Sistema de Control Distribuido).

Este sistema de control de tecnología avanzada integra un control proporcional completo para la planta de energía desde una plataforma única. Al integrar el control total de la planta de las turbinas de gas y vapor, HRSG y todos los subsistemas; el Mark VI DCS mejora la operación de la planta y reduce los costes.

f. Equipamiento para Balance of Plant (BoP).

El Balance Of Plant (BoP) se diseña y proporciona para dar cabida a las opciones de los clientes y las opciones específicas del sitio, incluyendo todos los aspectos eléctricos de una planta de energía desde la evacuación de calor al control. El sistema integrado es escalable, flexible y está diseñado para responder a las necesidades del cliente, ya sea como un paquete de equipamiento completo o como una solución modular mediante componentes individuales.

El BoP suministrado por GE© incluye los siguientes elementos:

- Equipamiento de Alta, Media y Baja Tensión, incluyendo Protección y Sistemas de Control.
- Sistemas de monitorización y diagnóstico de transformadores y motores.
- Protección de Generador.
- Transformador de generación.
- Sistemas de medición de potencia.
- Sistemas de comunicaciones.
- Sistema de Control de Plantas.

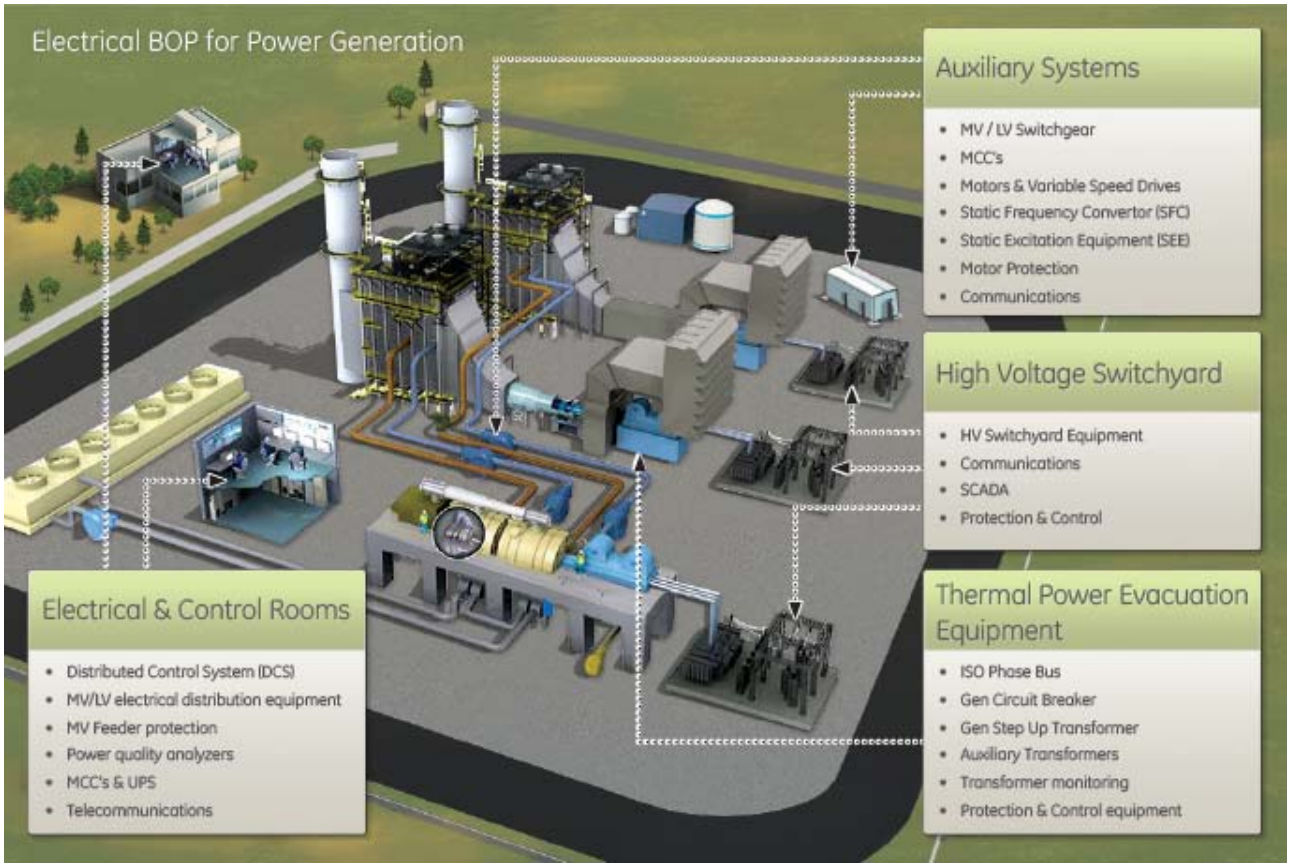


Figura 28.
Componentes del Balance Of Plant (BoP) suministrado por GE© en plantas de energía [30].

Los mismos procesos de diseño rigurosos utilizados para desarrollar la tecnología de turbinas, fiable y eficiente de GE, también se utilizan para diseñar este sistema de ciclo combinado modular.

La planta de energía estándar 109FB-SS está diseñada para alta fiabilidad y eficiencia, lo que hace que el proyecto de un ciclo resulte en mayor producción y en un menor coste de la electricidad.

7.1.3 Filosofía de control de la Planta Estándar de Ciclo Combinado.

El sistema de control de la Planta Estándar (PCS-Plant Control System) está basado en un control proporcional completo mediante procesadores Mark VIe, e incluye las facilidades necesarias para operar la central eléctrica de forma segura con tecnología de última generación, mediante sistemas de control tanto analógico como digital. La operación de la planta se realiza desde de la Sala de Control Central (CCR), y el modo de control principal de la instalación es automático con capacidad para el control manual de la Unidad de Visualización de video (VDU) utilizada como unidad de interfaz de operación.

La operación del sistema de control se basa en el arranque y parada remoto de los sistemas de la planta por los operadores en las estaciones de Operación del PCS, situadas en la CCR.

Las unidades de procesamiento del PCS, estaciones de ingeniería/operación, y dispositivos periféricos son completamente funcionales tras la restauración de la alimentación sin necesidad de cargar desde discos, cinta u otro dispositivo de nivel de red. La puesta en marcha, incluido reset, de cada estación se realiza sin ayuda de dispositivos de nivel superior.

Las variables de proceso de lazos críticos con triple redundancia emplearán tres transmisores con función de selección de la medida. La falta de cualquier transmisor se avisará mediante alarma y el control basará la medida en la media de los dos restantes. Si se produjera una desviación entre los dos transmisores que hacen la media, entonces el lazo de control será rechazado hasta que el operador seleccione sólo el transmisor que funciona correctamente. Si dos entradas están en estado de fallo, se utilizará el último valor. Una desviación excesiva entre los tres valores se avisará mediante alarma. Tras la aparición de un fallo en el proceso de generación, la protección de éste se inicia desde el PCS seleccionando: valor, mediana, media u otro dispositivo.

En interruptores de proceso con protección triple redundante, se realiza la protección mediante lógica 2 de 3 de modo que un fallo de un dispositivo no inicie un disparo.

En general, la pérdida de cualquier módulo o módulos redundantes no tiene como resultado la pérdida de control automático para procesos controlados por otros módulos.

La pérdida de algún módulo de E/S esclavos asociados o analógicos, se avisa mediante alarma en la CCR, y se inicia automáticamente la transferencia a un modo de control alternativo o manual.

7.1.4 El Sistema de Control (PCS).

El sistema de control de planta (PCS- Plant Control System) está basado en un sistema de control distribuido mediante procesadores MARK VIe, diseñado con un alto grado de disponibilidad y una arquitectura de sistema tolerante a fallos. El esquema de redundancia para el sistema está diseñado de forma el fallo de un solo componente, excepto para de E/S no-redundantes, no provoque fallo o interrupción del control normal ni de las funciones de supervisión.

El fallo único de un solo dispositivo de entrada no causará daños al equipamiento ni a la lógica de control, y se iniciarán sistemas de reserva alternativos con estrategias de control que permitan minimizar en la medida de lo posible perturbaciones en la planta.

Los sistemas principales controlados y monitorizados por el PCS son los siguientes:

- Caldera de recuperación de calor (HRSG).
- Sistema de purga de HRSG (HRSG Blowdown System).
- Sistema de Bypass y vapor de alta presión (High Pressure (HP) Steam & Bypass System).
- Sistema de Bypass y vapor de presión intermedia (IP-Intermediate Pressure Steam&Bypass system).
- Sistema de vapor recalentado (RH-Reheat Steam System)
- Sistema de Bypass y vapor de baja presión (LP-Low Pressure Steam & Bypass System).
- Sistema de vapor auxiliar (Auxiliary Steam System).
- Drenajes y venteos del sistema de vapor (Steam System Vents and Drains).
- Sistema de sellado de la turbina de vapor (Steam Turbine Seal System).
- Sistema cerrado de agua de refrigeración (Closed Cycle Cooling Water System Feedwater System).
- Sistema de condensado (Condensate System).

- Sistema de drenajes de planta (Plant Drains System).
- Sistema de distribución de aire comprimido (Compressed Air Distribution System).
- Sistema de agua bruta (Raw Water System).
- Sistema de agua de servicio (Service Water System).
- Sistema de agua potable (Potable Water System).
- Sistema de muestreo de agua y vapor (Steam and Water Sampling System: monitoring only, input via Profibus DP VO Datalink).
- Sistema de gas (Fuel Gas System).
- Sistema de gasoil (Fuel Oil System,if applicable).
- Sistema de extracción de aire del condensador (Condenser Air Extraction System).
- Sistema de agua de circulación (Circulating Water System, if applicable).
- Sistema abierto auxiliar de agua de refrigeración (Open Cycle Auxiliary Cooling Water System).
- Torres de refrigeración (Cooling Tower, if applicable).
- Sistema de protección de la unidad de balance de planta (BOP Unit Protection System).
- Sistemas eléctricos auxiliares (Electrical Auxiliaries System).

7.1.4.1 Diseño hardware de cabinas de control del PCS:

El sistema PCS utiliza E/S remotas dispuestas en cabinas que incluyen fuentes de alimentación, tarjetas de E/S y unidades de terminación de campo con bloques de terminales de campo cableados.

Las cabinas cumplen con la siguientes clasificación: IEC IP 42 o NEMA 12 para las cabinas situadas dentro del edificio eléctrico o IEC IP 54 para cabinas de E/S remotas situadas al aire libre o fuera del edificio eléctrico.

Los cuadros de E/S remotas cumplen con la clasificación NEMA 4.

La ubicación de las diferentes zonas de E/S son las siguientes:

- Entradas/salidas de la turbina de gas (GT), situadas en el edificio eléctrico.
- Entradas/salidas de la turbina de vapor (ST), situadas en el edificio eléctrico.
- Cuadro de entradas/salidas remotas mecánicas de BOP, situado en el edificio de servicios generales.
- Cuadro de entradas/salidas situado cerca de las bombas de agua de alimentación.
- Cuadro de entradas/salidas situado encima de HSRG.
- Cuadro de entradas/salidas de HRSG, situado en el edificio eléctrico.
- Entradas/salidas remotas de agua de circulación y/o torres de refrigeración, situadas en el edificio eléctrico de agua de circulación.
- Los procesadores de E/S remotas del edificio eléctrico, van ubicados dentro de cabinas con clasificación IEC IP42 que incluyen junto con el controlador tarjetas para bus de comunicaciones y fuentes de alimentación.

La alimentación de controlador, las tarjetas de red de comunicaciones y las redes de comunicaciones son redundantes. En cambio las tarjetas de entradas/salidas remotas y las unidades de terminación no son redundantes.

La alimentación de energía a las cabinas de control y las cabinas remotas de E/S es mediante dos UPS de 230 VAC 50 Hz. La alimentación de energía para la VDUs es mediante una única UPS de 230 VAC 50 Hz. La VDUs de la sala de control se alimentan de diferentes fuentes de UPS, para que una pérdida de alimentación de energía no de lugar a la pérdida de todos los VDUs.

7.1.5 Instrumentación de sistemas.

Se establecen tres niveles de protección y control en la filosofía en el diseño de la planta, y cada nivel tiene unos requisitos mínimos de redundancia.

Los diferentes niveles de instrumentación que se establecen y el nivel de redundancia correspondiente, son los siguientes:

- Sistemas críticos (triple instrumentación redundante).
- Sistemas importantes (doble instrumentación redundante).
- Sistemas no importantes (simple instrumentación).

A continuación se describen los sistemas con el nivel de redundancia que se les establece:

7.1.5.1 Triple instrumentación redundante (sistemas críticos):

Los sistemas críticos son los más importantes, ya que si se operan fueran de los límites para los que están diseñados se pueden causar una pérdida de la generación de energía, o daños catastróficos a los principales equipos de la planta, personas o medio ambiente. Dentro de estos sistemas críticos se incluyen las turbinas de gas y vapor, así como la caldera de recuperación de calor (HRSG), y las medidas de proceso de estos sistemas a las que se les requiere triple instrumentación redundante son las siguientes:

- Nivel de calderines HP, IP y LP.
- Presión de calderines HP, IP y LP.
- Presión de vapor HP, HRH y LP (controles ST).
- Temperatura de vapor HP, HRH y LP (controles ST).
- Temperatura de vapor de HP, HRH y CRH.
- Temperatura del bypass de vapor HP.
- Temperatura del bypass de vapor HRH.
- Presión de escape de la turbina de gas (controles GT).
- Presión del conducto HRSG (si se requiere por diseño).
- Compuerta de la chimenea de entrada de HRSG.
- Nivel del condensador.
- Vacío del condensador.
- Detección de conductividad en las fugas del condensador.
- Nivel del tanque receptor de drenajes de condensados.

- Nivel del tanque de expansion del condensador.
- Nivel del tanque de agua fría del ciclo cerrado.
- Cuna de filtro duplex coalescente de gas del separador de nivel HI HI (controles GT).
- Nivel liquido de la carcasa del calentador de gas HI HI (controles GT).

7.1.5.2 Doble instrumentación redundante (sistemas importantes):

Para los controles de sistemas y equipos para los cuales funcionar fuera de los límites establecidos puede afectar a la operación de planta o causar daño al equipamiento, se emplea instrumentación redundante doble.

Esta instrumentación redundante como mínimo se incluye en las medidas de proceso de los sistemas de presión de vapor (HP, HRH, IP and LP steam pressure):

- Caudal de vapor de HP, IP y LP.
- Presión del bypass deHP, HRH y LP.
- Temperatura del bypass de LP.
- Termopozo del colector de vapor de HP y LP.
- Termopozo de HRH (ST IP inlet) y CRH (ST HP outlet).
- Presión muestras de entrada de admisión ST, LP.
- Nivel de goteo de vapor.
- Caudal de condensados.
- Nivel de detección de fugas de gas condensado.
- Caudal de descarga de la bomba alimentación de la caldera HP y IP.
- Presión de la realimentación de la caldera de HP.
- HP BFP.
- Caudal de realimentación del economizador de HP.
- Caudal de realimentación del economizador de IP.
- Caudal de realimentación del economizador de LP.
- Nivel del tanque de almacenamiento de gasoil sin tratar.
- Nivel del tanque de almacenamiento de gasoil limpio.
- Nivel del tanque de almacenamiento de agua desmineralizada.
- Nivel del tanque de almacenamiento de condensados.
- Nivel de la balsa de la torre de refrigeración.

7.1.5.3 Instrumentación HRSG:

La caldera de recuperación deberá estar provista de una indicación electrónica independiente en la CCR para los calderines de vapor de HP, IP y LP. Estas indicaciones sirven al operador como método independiente para verificar el nivel de los calderines HRSG.

7.1.5.4 Instrumentación para sistemas no importantes.

Para los sistemas para los cuales un fallo del sistema de control puede ser fácilmente corregido sin que la operación de la planta se vea afectada, se suele emplear instrumentación simple con un único instrumento. Un fallo en este único instrumento causa un fallo o interrupción de las funciones normales de control o monitorización. Por tanto, este tipo de instrumentación se aplica al resto de sistemas que no correspondan a las turbinas de gas y vapor, a la HRSG o a los sistemas de presión vapor (HP, LP e IP).

7.1.6 Instrumentos y dispositivos de control.

Los dispositivos e instrumentos de proceso con los que se equipa y define la planta estándar son: señales analógicas 4-20mA y temperatura (Termopares y Pt-100), señales binarias y válvulas de control motorizadas (MOV) [ver 10.11 y 10.14].

7.1.7 Interfaz del Operador.

La interfaz del operador para el control de la planta será principalmente mediante VDUs de procesado de gráficos.

En pantallas adicionales a las VDUs se proporcionan, incluyendo agrupaciones de controlador de la placa frontal, datos tabulados y registros, y el tiempo frente a gráficos de tendencias de valor. Los gráficos de proceso serán proporcionados para el detalle de los sistemas de proceso y diseños de equipos, y proporcionar datos de procesos dinámicos para el seguimiento y control del operador.

Las placas frontales para permisivos y disparos se proporcionan para la operación de cada unidad de control. Estas placas frontales indican que permisivo es, que permisivos están impidiendo el control de la unidad, y que condiciones mecánicas son los responsables del disparo de la unidad.

7.1.7.1 Avisos y alarmas:

El PCS proporciona la monitorización de alarmas en la CCR para toda la planta. Como diseño básico, sistemas con autocontrol proporcionarán al menos una alarma común.

El anuncio de alarma se mostrará al operador a través del display de alarmas a pantalla completa del VDU, con impresión del mensaje de alarma, y con indicación en el gráfico del proceso

También se proporcionará indicación de alarmas de grupo por el sistema o por prioridad y un medio de acceso inmediato a las pantallas de alarma. Desde la pantalla de alarma, será posible llamar de inmediato a las pantallas de control aplicables a las variables que se encuentran en el estado de alarma.

Las alarmas generadas por valores analógicos, contarán con valores de alarma incrementales apropiadas bandas muertas para avisar al operador del deterioro o la mejora de las condiciones del proceso.

Se proporcionarán medios para que suene una alarma audible, y al silencio, reconocer y restablecer las alarmas.

7.1.7.2 Presentación de los datos:

El PCS permite al operador definir grupos de puntos para la visualización, ya sea en forma de tabla o gráfico, y permite múltiples grupos para ser guardados en la memoria.

Además, el PCS incluye servicios públicos para la preparación e impresión de registros periódicos, y además permite al operador seleccionar un subconjunto de la base de datos de la planta para su visualización como un grupo.

7.1.8 Diseño a prueba de fallos.

En general, los sistemas de la planta están diseñados para ser a prueba de fallos. Ante la pérdida de la señal de control o, control o alimentación, el sistema de control y dispositivos tomarán una posición segura que no cause daños a los equipos.

7.1.9 Circuitos de protección y alarma.

En general, los contactos de alarma están abiertos y los circuitos de protección están desenergizados para disparar. Una excepción a esto son los circuitos de control donde la energización provoca el disparo. El control de apertura de circuito se considera altamente fiable porque la alimentación del control es un desde un sistema de baterías. Sin embargo, la decisión de utilizar los contactos de apertura o cierre de alarma, energizando o desenergizando para disparar, depende de la configuración y de los equipos del sistema, las prioridades del sistema y el control, incluida la instrumentación. Por ejemplo, si es más importante mantener un equipo en funcionamiento que evitar daños por detenerlo; la energización para disparar puede ser más apropiada que la desenergización. Un buen juicio de ingeniería y conocimiento del sistema se utiliza para hacer esta determinación en base a caso por caso.

7.1.10 Enclavamientos.

Los enclavamientos serán incorporados para asegurar funcionamiento, arranque secuencial y apagado de los equipos del sistema. Enclavamientos, temporizaciones, circuitos y vigilancias serán provistos para asegurar el funcionamiento correcto, con la máxima seguridad y fiabilidad en todos los modos de operación, y para minimizar las acciones del operador o fallos en los equipos.

7.2. Descripción de la arquitectura general de la Planta estándar.

La arquitectura general de los diferentes sistemas de la Planta Estándar es la definida por General Electric que se recoge en el plano *129E3625 Rev.B (incluido en el documento 496-11-D-I-00300) [10.12]*, que se muestra a continuación en el Figura 29.

Está arquitectura corresponde a una arquitectura de sistemas de control cableados con red de supervisión según lo indicado en el punto 1.4.

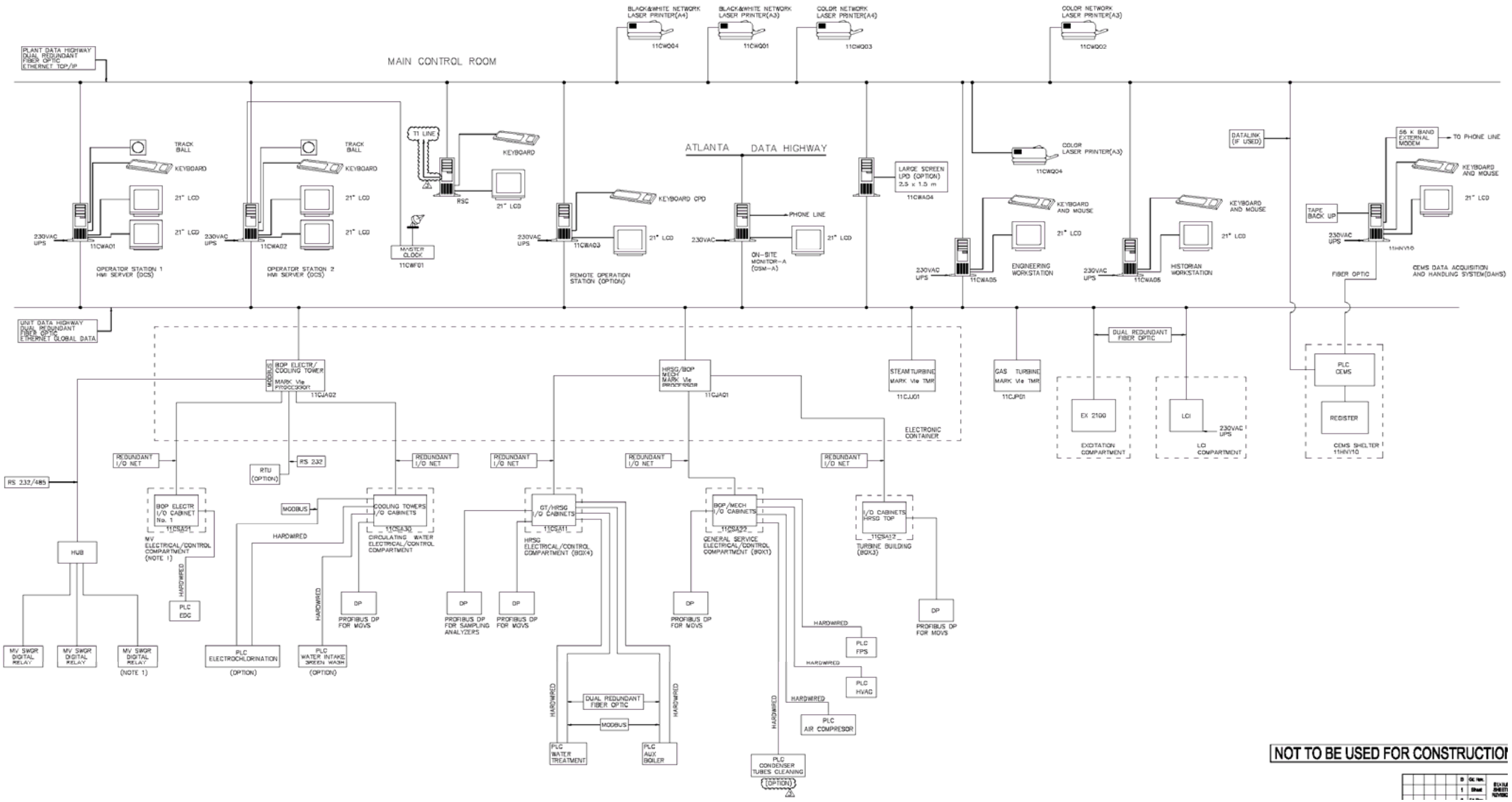


Figura 29. Arquitectura general de la Planta estándar [10.12].

La arquitectura general mostrada en la Figura 29, se compone los siguientes elementos:

7.2.1 Elementos de campo.

En los documentos de partida 496-11-LE-I-40100 (Instrument List)*[10.11]* y el 496-11-LE-I-40300_02 (Control Valve List) *[10.14]*, ambos de GE Energy©, se identifican el número de señales de dispositivos analógicos (AI, TC, Pt-100 y AO) y digitales (DI y DO), así como las válvulas de control (MOVs) con los que se equipa la planta estándar y son alcance del layout realizado Empresarios Agrupados AIE©.

El número total de señales son las indicadas en la siguiente Tabla 3:

	AI (Analog Input)	**TC-E** (Thermocople)	**PT-100**	**AO** (Analog Output)	**DI** (Digital Input)	**DO** (Digital Output)	**MOVs** (Válvula de Control)
Procesador 11CJA01	187	85	10	34	223	142	50
Procesador 11CJA02	16	0	2	2	30	30	3
TOTAL	**203**	**85**	**12**	**36**	**280**	**174**	**53**

Tabla 3.
Total señales alcance layout de EA AIE©

Todas las señales procedentes de campo se centralizan en cabinas de interconexión, que actúan como armarios concentradores de señales, para desde dichas cabinas conectar las señales con los elementos de control que consisten en dos procesadores MARK VIe (11CJA01 y 11CJA02).

Las cabinas de interconexión son las siguientes:

- Cabina de entradas/salidas de HRSG y de la turbina de gas (GT).
- Cabina de entradas/salidas de encima de HRSG.
- Cabina de entradas/salidas remotas eléctricas de BOP.
- Cabina de entradas/salidas remotas mecánicas de BOP.
- Cabina de entradas/salidas remotas de agua de circulación y/o torres de refrigeración.

Estas cabinas colectores recogen todas las señales de la instrumentación analógica y digital, así como de válvulas motorizadas (MOVS) de todos los sistemas que equipan la Planta Estándar.

7.2.2 Elementos de control/supervisión del PCS.

El PCS se compone de cuatro procesadores MARK VIe que se encargan de gestionar todas las señales de los diferentes sistemas de la planta, que no sean paquete, para llevar a cabo el control del proceso del ciclo combinado para la generación eléctrica. Estos procesadores se identifican como:

- *Procesador MARK VIe, HRSG*/BOP MECH (11CJA01).
- *Procesador MARK VIe, BOP* Electr/cooling Tower (11CJA02).
- *Procesador MARK VIe, STEAM* TURBINE (11CJJ01).
- *Procesador MARK VIe,* GAS TURBINE (11CJP01).

La labor de la Ingeniería de Empresarios Agrupados en el proyecto de la Planta Estádar 109FB es el layout de las señales conectadas a los procesadores 11CJA01 y 11CAJ02, y todas las señales de los diferentes sistemas que conectan con los procesadores están centralizadas en varias cabinas de E/S.

La identificación de las cabinas centralizadoras y sus ubicaciones en planta, con las señales a las que aplica la ingeniería de layout, es la siguiente:

- **11CSA11:** Cabina de entradas/salidas de HRSG y de la turbina de gas (GT), situado en el edificio eléctrico.
- **11CSA12:** Cabina de entradas/salidas de encima de HRSG, situado en el edifico de turbina.
- **11CSA21:** Cabina de entradas/salidas remotas eléctricas de BOP, situado en el edificio eléctrico.
- **11CSA22:** Cabina de entradas/salidas remotas mecánicas de BOP, situado en el edificio de servicios generales.
- **11CSA30:** Cabina de Entradas/salidas remotas de agua de circulación y/o torres de refrigeración, situadas en el edificio eléctrico de agua de circulación.

El PCS dispone de dos puestos en la Sala de Control (CWA01/02) para que el operador pueda supervisar/controlar todos los sistemas de la planta.

Además para supervisión/control del PCS, éste se completa con los siguientes puestos:

- **CWA03:** es opción a petición del cliente, y sirve para conexiones remotas.
- **CWA05:** es la estación de ingeniería, desde donde se pueden configurar parámetros de la lógica, modificar setpoints, etc.
- **CWA06:** es el histórico, donde se almacenan los datos de operación y se pueden ver curvas de tendencias, etc.

Por último, en Sala de Control se sitúa un puesto para el sistema de monitorización de emisiones contaminantes (CEMS) que sólo monitoriza y genera informes de emisiones contaminantes sin ningún control sobre el sistema.

La conexión entre todos los puestos de supervisión/control comentados y los dos procesadores de control (11CJA01/02), se realiza mediante redes de comunicaciones.

7.2.3 Elementos de control de sistemas paquete.

La planta estándar de ciclo combinado se equipa con un número de sistemas denominados “paquete” que no están incluidos con el suministro de GE Energy©. Estos sistemas “paquete” son funcionalmente independientes y no se requiere ningún control del DCS sobre ellos, aunque si proporcionan información de su estado mediante señales E/S digitales.

Estos sistemas “paquete” son los mostrados en el plano *129E3625 Rev.B* [10.12] y van equipados con su propio sistema de control que funciona de forma autónoma e independiente, formando islas de automatización, y únicamente interaccionan con el PCS proporcionando

información de su estado mediante señales binarias. Estas señales binarias de estado pueden ir cableadas directamente desde el PLC del sistema paquete a las cabinas centralizadoras, o bien usar bloques de contactos con comunicación mediante bus de campo como es el caso del interfaz de relés cuadros media tensión (MV SWGR DIGITAL RELAY), que comunica con el procesador 11CJA01 mediante una tarjeta de comunicación MODBUS.

Los sistemas "paquete" son los siguientes:

- Interfaz de relés cuadros media tensión (MV SWGR DIGITAL RELAY).
- Toma de agua de limpieza de rejillas (opcional).
- Sistema de electrocloración.
- Toma de muestras de analizadores.
- Sistema de tratamiento de aguas.
- Caldera auxiliar.
- Generadores diesel de emergencia (EDG).
- Sistema de limpieza de tubos del condensador.
- Aire de instrumentos.
- Sistema de ventilación, aire acondicionado y calefacción (HVAC).
- Sistema de protección contra-incendios (FPS).
- Sistema de monitorización de emisiones contaminantes (CEM).

La definición de criterios de diseño y definición/resolución de interfaces eléctricos/mecánicos para conectar los sistemas paquete a los sistemas diseñados por GE Energy©, es alcance de la ingeniería de Empresarios Agrupados AIE©.

7.3. Premisas para el diseño de la nueva arquitectura con redes de comunicaciones.

Una vez descrita la arquitectura general de la Planta estándar de Ciclo Combinado, como la interconexión de todos los elementos de campo al DCS se realiza mediante cableado tradicional y la comunicación entre los procesadores puestos de control/supervisión y sistemas paquete está excluida del alcance de la ingeniería de Empresarios Agrupados, se pretende con el presente trabajo establecer un diseño básico conceptual para todas las comunicaciones entre los elementos de la arquitectura de la Planta Estándar, que permita el empleo de buses de campo, para posteriormente hacer un diseño en detalle e incluirlo en el alcance de la ingeniería de Empresarios Agrupados para nuevos proyectos de Planta Estándar de Ciclo Combinado.

Por tanto, como la Planta Estandar 109FB es un estándar de Planta de Ciclo Combinado con un Sistema de Control ya definido, en cuanto al número de señales y dispositivos de control, el objetivo es establecer una arquitectura de comunicaciones basada en redes de comunicación que permita integrar las señales de los dispositivos de campo y sistemas paquete, de manera totalmente compatible con el DCS y que no implique tener que cambiar el software del mismo.

7.4. Identificación de redes de comunicaciones en la Planta Estándar.

En el siguiente punto se aplica la filosofía de diseño propuesto con el modelo CIM, para la definir las redes de comunicaciones de la Planta Estándar de acuerdo a la funcionalidad de los diferentes instrumentos/dispositivos de control, que se ha explicado en el punto 7.2 anterior.

7.4.1 Red/bus de campo:

Esta red corresponde a la situada en el nivel más bajo de la jerarquía de automatización, que es donde se sitúan los diferentes instrumentos analógicos y digitales de la planta estándar necesarios para manejar el proceso de generación eléctrica. Como se ha comentado anteriormente los elementos de campo son dispositivos analógicos (AI, TC, Pt-100 y AO) y digitales (DI y DO), así como válvulas de control motorizadas (MOVs). Estos dispositivos tienen que envíar sus señales a los dos procesadores de control para gobernar el proceso.

La instrumentación actualmente empleada en la Planta Estándar son instrumentos cuyas señales van cableadas desde campo hasta las cabinas centralizadoras de señales, y por tanto para poder establecer una/s red/es de campo es necesario integrar dichas señales en el bus con módulos de adquisición basados en tecnologías de bus de campo de prestaciones sencillas y sistemas de periferia descentralizada.

Sobre la Figura 30 se marca en color naranja las diferentes redes/buses de campo que se establecen.

7.4.2 Red de célula:

En esta red se sitúan los dispositivos de control pertenecientes a diversas islas de producción (sistemas de planta). La Planta estándar los únicos elementos de control que tiene son los procesadores 11CJA01 y 11CJA02, que además funcionan como elementos de supervisión de todos los sistemas de la planta, por lo que su ubicación debe estar por encima de los dispositivos de control de los diferentes sistemas que no controle directamente, y estos son los sistemas de control de los sistemas paquete. Por tanto, las redes de célula que se definen para la Planta Estándar de Ciclo Combinado son las formadas entre el sistema de control del sistema paquete y los procesadores 11CJA01 y 11CJA02.

Sobre la Figura 30 se marca en color azul oscuro las diferentes redes de célula de los sistemas paquete.

7.4.3 Red de control/supervisión:

La Planta Estándar para su funcionamiento se compone de diferentes sistemas, que a su vez tienen relación entre sí para poder llevar a cabo una funcionalidad o tarea concreta. Los elementos de control de la Planta estándar son los procesadores 11CJA01 y 11CJA02 que se encargan de gobernar todos los sistemas “importantes” de la planta, y éstos vez envían información a nivel superior a la CCR para que el Operador tenga los datos necesarios para conocer el estado del proceso, y a su vez enviar cambios de consigna para poder mantenerlo dentro de los criterios de funcionamiento.

Por tanto, la única red de control/supervisión que se establece en la Planta Estándar es la formada entre los procesadores del PCS (MARK VIe) y los diferentes puesto de supervisión/control en Sala de Control (CW03, CW04, CW05, etc). Está red se marca sobre la Figura 30 en color verde.

Para el intercambio de información de los procesadores del Sistema de Control y los puestos de supervisión/control, se precisa del uso de un OPC que facilite el intercambio de datos entre las aplicaciones gráficas de los puestos de supervisión y el procesador de control. Ya que el volumen de datos a manejar en esta red es muy elevado, el bus de campo que a emplear será basado en Ethernet ya que de este modo prácticamente la información en los puestos de supervisión estará disponible de forma instántanea, según esté disponible en las redes de las capas inferiores.

7.4.4 Red de factoría:

Esta red pretende permitir la comunicación de todos los equipos tipo PCs de las diferentes áreas de la planta, que estén habilitados para visualizar la información de los sistemas desde el Sistema de Control, para su consulta y/o impresión de datos.

Esta red como está situada en la parte más alta de la jerarquía de redes de la Planta Estándar y con acceso desde PC personales, es muy importante tener una política de Ciberseguridad muy bien definida que evite que mediante conexiones externas a dichos PCs personales o por el uso de dispositivos de almacenamiento personal tipo USB, se puedan facilitar el acceso de software malicioso en la infraestructura de red de la planta, que le daría total libertad para acceder a cualquier dispositivo de red para falsear la información de proceso, y dañar el proceso de producción eléctrica o incluso daños irreparables en la integridad de la planta, del personal o entorno de la misma.

Está red se marca sobre la Figura 30 en color rojo.

Por tanto, de acuerdo a lo comentado la arquitectura de la planta estándar queda dividida en las redes de comunicación que se representan en la siguiente Figura 30:

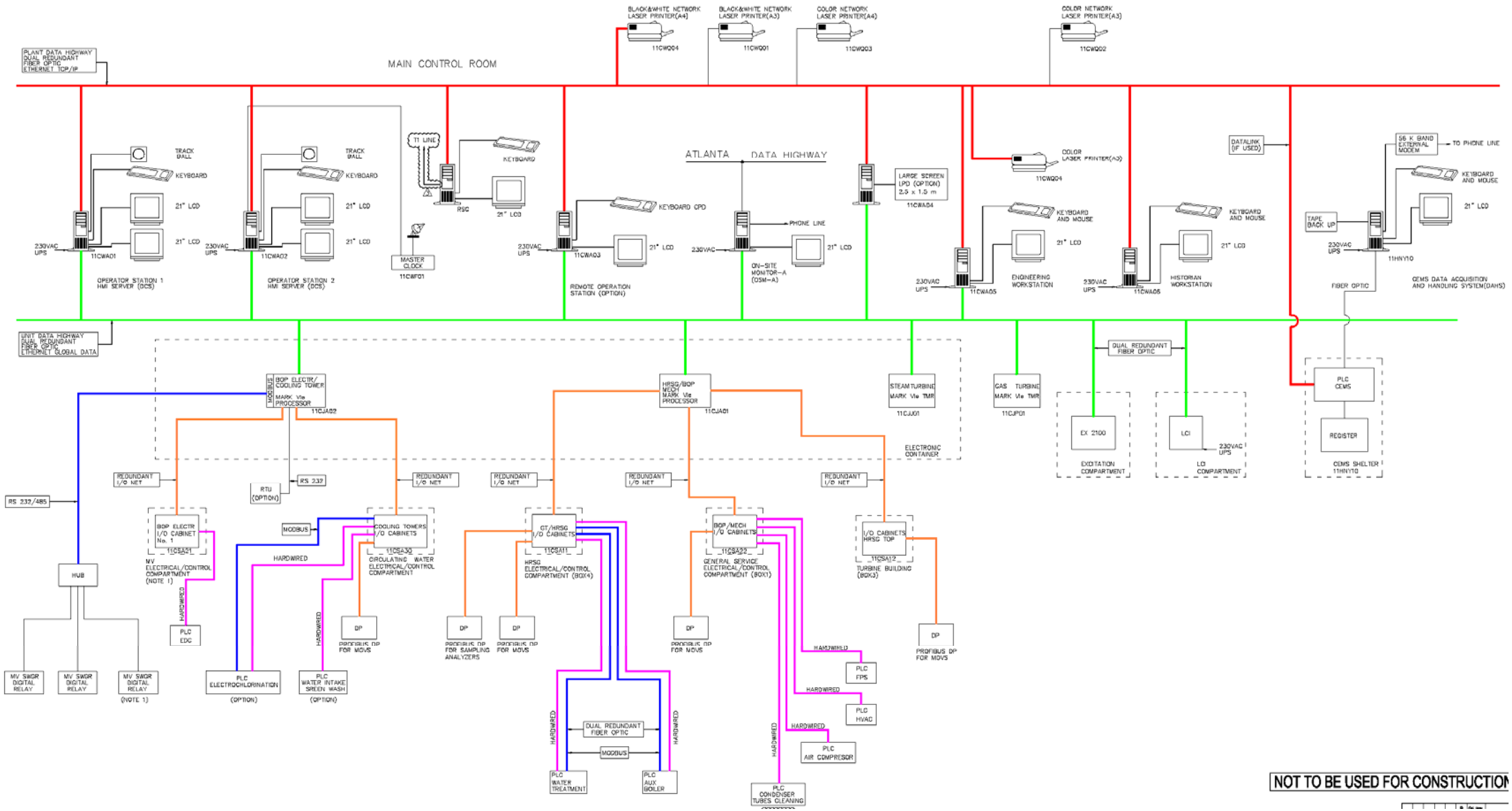


Figura 30. División en niveles de red de la arquitectura de la Planta estándar.

7.5. Definición de los elementos que componen cada una de las redes de comunicaciones.

Una vez definidas las diferentes redes de comunicación de la arquitectura de la Planta Estándar 109FB, el siguiente paso es estudiar y analizar que elementos componen dichas redes para poder establecer la infraestructura de las diferentes redes y los diferentes elementos que la componen.

7.5.1 Elementos de la red de campo.

La instrumentación de los sistemas principales, controlados y monitorizados por el PCS con los que se equipa la Planta Estándar de Ciclo Combinado, a fin de tener la idea del número de dispositivos/señales que vamos a tener que manejar para dimensionar la red de comunicaciones, son los indicados en los documentos de partida 496-11-LE-I-40100 *[10.11]* y el 496-11-LE-I-40300_02 *[10.14]*.

En dichos documentos se identifican los dispositivos y el número de señales asocidas, que pueden ser tipo analógicas (AI, TC, Pt-100 y AO) o binarias (DI y DO). Además se definen las válvulas de control motorizadas denominadas MOV, que están definidas para controlarse mediante bus de campo.

En la siguiente Tabla 4 se refleja el número total de señales y MOV con lo que se equipa la Planta estándar:

	AI (Analog Input)	**TC-E** (Thermocople)	**PT-100**	**AO** (Analog Output)	**DI** (Digital Input)	**DO** (Digital Output)	**MOV** (Válvula de Control)
Procesador 11CJA01	187	85	10	34	223	142	50
Procesador 11CJA02	16	0	2	2	30	30	3
TOTAL	**203**	**85**	**12**	**36**	**280**	**174**	**53**

Tabla 4.
Número de señales por procesador MARK VIe.

Todas las señales comentadas están centralizadas en cinco cabinas colectoras (I/O cabinet), que están identificadas y situadas como a continuación se indica (ver Anexo 3):

- Cabina 11CSA11 de entradas/salidas de HRSG y de la turbina de gas (GT), situado en el edificio eléctrico.
- Cabina 11CSA12 de entradas/salidas de encima de HRSG, situado en el edifico de turbina.
- Cabina 11CSA21 de entradas/salidas remotas eléctricas de BOP, situado en el edificio eléctrico.
- Cabina 11CSA22 de entradas/salidas remotas mecánicas de BOP, situado en el edificio de servicios generales.
- Cabina 11CSA30 de entradas/salidas remotas de agua de circulación y/o torres de refrigeración, situadas en el edificio eléctrico de agua de circulación.

Estas cabinas colectoras además de las señales indicadas en la Tabla 4, recogen señales de los PLC's de los diferentes sistemas paquete indicados en el punto 7.2.3, tanto mediante cableado tradicional como bus de campo, según se recogen en la arquitectura general [10.12].

Los buses de campo del tipo SENSORBUS no son adecuados para este tipo de red, ya que están enfocados para su uso en redes que se manejen datos a nivel de bit (variables

digitales de E/S), y por tanto se descarta su uso en el diseño de la red de campo ya que se manejan señales analógicas y de control de válvulas de control.

7.5.2 Elementos de la red de célula.

En esta red se sitúan los dispositivos de control pertenecientes a diversas islas de producción, que básicamente son elementos de control de los diferentes sistemas, y como se verá más adelante conforman una subred o segmento con los PLCs de los sistemas paquete de la planta estándar. A continuación se indica los PLCs de los sistemas paquete definidos en la Planta estándar, que en algunos casos conectan con el sistema de control mediante bus de campo, y en otros sólo llevan cableada alguna señal digital de estado:

Identificación	Sistema paquete	Procesador/ Cabina interconexión	Comunicación mediante bus	Cableado hardware de señales
MV SWGR DIGITAL RELAY	Interfaz de relés cuadros media tensión	11CJA02 11CSA21	SI	NO
PLC WATER INTAKE SCREEN WASH	Toma de agua de limpieza de rejillas	11CJA02 11CSA30	NO	SI
PLC ELECTROCHLORINATION	Sistema de electrocloración	11CJA02 11CSA30	SI	SI
PLC EDG	Equipos diesel de emergencia	11CJA02 11CSA21	NO	SI
PLC WATER TREATMENT	Sistema de tratamiento de aguas	11CJA01 11CSA11	SI	SI
PLC AUX BOILER	Caldera auxiliar	11CJA01 11CSA11	SI	SI
PLS CONDENSER TUBES CLEANING	Sistema de limpieza de tubos del condensador	11CJA01 11CSA22	NO	SI
PLC AIR COMPRESOR	Aire de instrumentos	11CJA01 11CSA22	NO	SI
PLC HVAC	Sistema de ventilación, aire acondicionado y calefacción	11CJA01 11CSA22	NO	SI
PLC FPS	Sistema de protección contra-incendios	11CJA01 11CSA22	NO	SI
PLC CEMS	Sistema de monitorización de emisiones contaminantes	Sala de Control (CCR)	SI	NO

Tabla 5.
Identificacion de conexión de PLCs paquete con cabinas colectoras.

7.5.3 Elementos de la red de control/supervisión.

Todos los elementos de campo comentados en el punto anterior son gobernados a nivel superior por cuatro procesadores MARK VIe, que se encargan de procesar las señales de las cabinas colectores de señales de los diferentes elementos de campo, y gobernar el proceso del ciclo combinado para la generación eléctrica, por lo que envían órdenes tanto a los elementos de campo de la *red de campo* situada a “nivel inferior”, como a los operadores situados en la CCR en el “nivel superior” de la *red control/supervisión*.

Los procesadores que componen la planta estándar son cuatro MARK VIe, pero en este trabajo sólo se implementa la comunicación para las señales de campo conectadas a los procesadores 11CJA01 y 11CAJ02, ya que son alcance de la ingeniería de layout que hace Empresarios Agrupados AIE © para la Planta estándar.

Los cuatro procesadores que gobiernan la Planta Estándar son los siguientes:

- *Procesador MARK VIe, HRSG*/BOP MECH (11CJA01).
- *Procesador MARK VIe, BOP* Electr/cooling Tower (11CJA02).
- *Procesador MARK VIe, STEAM* TURBINE (11CJJ01).
- *Procesador MARK VIe,* GAS TURBINE (11CJP01).

Por tanto, según lo indicado en el documento *List Hardwired & Datalinked* [10.11], los procesadores 11CJA01 y 11CJA02 gobiernan todas las señales que se recogen en el Anexo 1 de las cabinas que a continuación se indican. En el Anexo 03 se muestra la ubicación de las cabinas electrónicas donde se ubican los procesadores:

a) Procesador **11CJA01** gobierna las señales analógicas, digitales y de MOVs, centralizadas en las cabinas 11CSA11, 11CSA22 y 11CSA12.

b) Procesador **11CJA02** gobierna las señales analógicas, digitales y de MOVs, centralizadas en las cabinas 11CSA21 y 11CSA30.

c) Procesador **11CJJ01**: gobiernan las señales del control de la turbina de vapor (ST), y como no es alcance de la Ingeniería de Empresarios Agrupados AIE© para la planta estándar, no se incluyen en el análisis de este trabajo.

d) Procesador **11CJP01**: gobiernan las señales del control de la turbina de gas (GT), y como no es alcance de la Ingeniería de Empresarios Agrupados AIE© para la planta estándar, no se incluyen en el análisis de este trabajo.

De acuerdo con lo comentado, en esta red de supervisión/control se van a manejar variables digitales y analógicas entre los dispositivos de campo y los procesadores de control MARK VIe. Por tanto, como se comentó en el punto 2.4 los buses a emplear en esta red corresponden a los situados dentro del nivel de proceso de la pirámide CIM, que van enfocados a la implementación de buses de campo de alta velocidad y funcionalidad media (DEVICEBUS).

Además, en este nivel es necesaria la utilización de un OPC que proporcione una interfaz estandarizada para la comunicación de datos entre la red de factoría y la red de campo.

7.5.4 Elementos de la red de factoría.

El Sistema de Control de Planta (PCS) monitoriza las alarmas de toda la planta en la CCR, además de permitir que el operador envíe cambios de consigna para conducir el proceso. La interfaz del operador para el control de la planta es mediante VDUs de procesado de gráficos, que incluyen pantallas que proporcionan la información suficiente para el seguimiento y control de la Planta. Por tanto, la Planta Estándar se equipa con dos Estaciones de Operación denominadas: OPERATOR STATION 1 (11CWA01) y OPERATOR STATION 2 (11CWA02), asi como opción a petición del cliente se puede incluir en el suministro una Estación Remota de Operación (11CW03) para conexiones remotas.

Para configuración/modificación de estas Estaciones de Operación y de los procesadores MARK VIe, se dispone de una Estación de Ingeniería (11CWA05) que permite modificar la configuración de todos los equipos conectados en la *red de control/supervisión.*

Además para visualización de datos de proceso por parte de las secciones autorizadas, se dispone de una Estación de Históricos (11CW06) donde pueden acceder de forma remota a consultar información de proceso, sin posibilidad de enviar datos de consigna al proceso.

Por último, se dispone de un servidor de datos externos (OSM-A) que permite desde el exterior de la planta acceder a datos de la misma, con las correspondientes medidas de Ciberseguridad para evitar posibles ataques cibernéticos que puedan dañar la planta. Lo habitual es que este tipo de servidores sólo permitan la "salida" de datos al exterior y nunca el admitan el envío de datos desde el exterior hacia el interior de la red.

Por tanto, la red de control/supervisión de la Planta Estándar de Ciclo Combinado está compuesta por todos los elementos comentados, y la información que se maneja en esta red son palabras o tablas entre dispositivos controladores, ya que se trabaja con entornos gráficos con la misión de generar órdenes de ejecución hacia el nivel de supervisión/control, en base a la información recibida, así como almacenar y monitorizar la información de proceso. Por tanto, en esta red de debe emplear buses que manejen un gran volumen de datos, por lo que los buses de campo adecuados para este tipo de red son clasificados como tipo FIELDBUS o bien si los equipos que forman esta red los permite se puede utilizar redes LAN/WAN.

7.5.5 Definición de la especificación de bus empleado.

Primeramente es muy importante definir qué especificación de bus se va a emplear para implementar las redes de comunicaciones, ya que en función de esto se condiciona la arquitectura de comunicación de las redes de planta, tanto para definir los segmentos de la red de campo como para la definición de los diferentes elementos que interconecten las diferentes redes y dispositivos, que componen la arquitectura de la Planta Estándar de Ciclo Combinado desde el nivel más bajo de campo al nivel elevado de factoría.

Para la definición de la especificación de bus es necesario tener una visión global de la arquitectura para aplicar una solución de comunicación totalmente fiable y compatibible entre los elementos situados a más bajo nivel en campo (red de campo), y los elementos situados a más alto nivel situados en Sala de Control Central (CCR).

Como se ha comentado en puntos anteriores, la arquitectura de comunicaciones de la Planta Estándar de Ciclo Combinado se compone de cuatro niveles de red: red de campo, red de célula, red de control y red de factoría; es decir, se está dando una solución completa de automatización a la planta.

Si para dar una solución completa a la comunicación de la planta nos vamos al mercado a buscar un fabricante que nos la proporcione, nos encontraremos con multitud de posibilidades. La limitación fundamental que nos podemos encontrar radica en la selección de dispositivos de campo (sensores, válvulas, etc), ya que aunque todos los dispositivos definidos bajo una misma especificación de bus hablan el mismo "lenguaje" y son compatibles entre sí, los productos de software de la capa de aplicación ofertados por los fabricantes ya incluyen una serie de librerías estándar con los productos seleccionados por ellos mismos, con total garantía de funcionamiento con sus productos, y por tanto esto nos limita que la selección de la instrumentación de la planta se adecue a lo definido por el fabricante, así como su mantenimiento a lo largo de la vida de la planta.

En el caso de la Planta Estándar de Ciclo Combinado el inconveniente comentado no lo vamos a tener, ya que la arquitectura que se implementa es una arquitectura de control con red de supervisión, de modo que en campo tendremos las instrumentación que más nos interese con todas sus señales analógicas y digitales cableadas hasta las cabinas centralizadoras, a excepción de las señales de las válvulas motorizadas (MOV) que se conectan mediante bus, para que mediante módulos de comunicaciones adecuados integrarlas en la red de campo, desde donde ya conectan por bus con los procesadores de control MARK VIe.

De este modo como las señales de proceso de los instrumentos de campo son señales eléctricas en corriente y/o tensión, hace que el tipo de instrumento a usar en nuestra red de comunicaciones sea independiente del tipo de fabricante y tecnología, y por tanto seleccionar el instrumento de campo del fabricante que más nos convenga, de acuerdo al número y tipo de señales eléctricas que necesitemos para el correcto control del proceso.

7.6. Implementación práctica de las diferentes redes de la Planta estándar de Ciclo Combinado mediante especificación PROFIBUS©.

A continuación se desarrolla de forma práctica el diseño de las diferentes redes de comunicaciones de la Planta Estandar de Ciclo Combinado, definidas en la arquitectura de comunicaciones.

Primeramente se definirán los diferentes segmentos de la red de campo, teniendo en cuenta la disposición de señales en las cabinas centralizadoras (11CSA11, 11CSA12, 11CSA21, 11CSA22 y 11CSA30), para después definir todos los elementos de interconexión de la red de campo a niveles superiores así como el tipo de comunicación y el tipo de cable a emplear.

De forma esquemática, la arquitectura de redes de comunicaciones de la Planta Estándar que se ha definido es la siguiente:

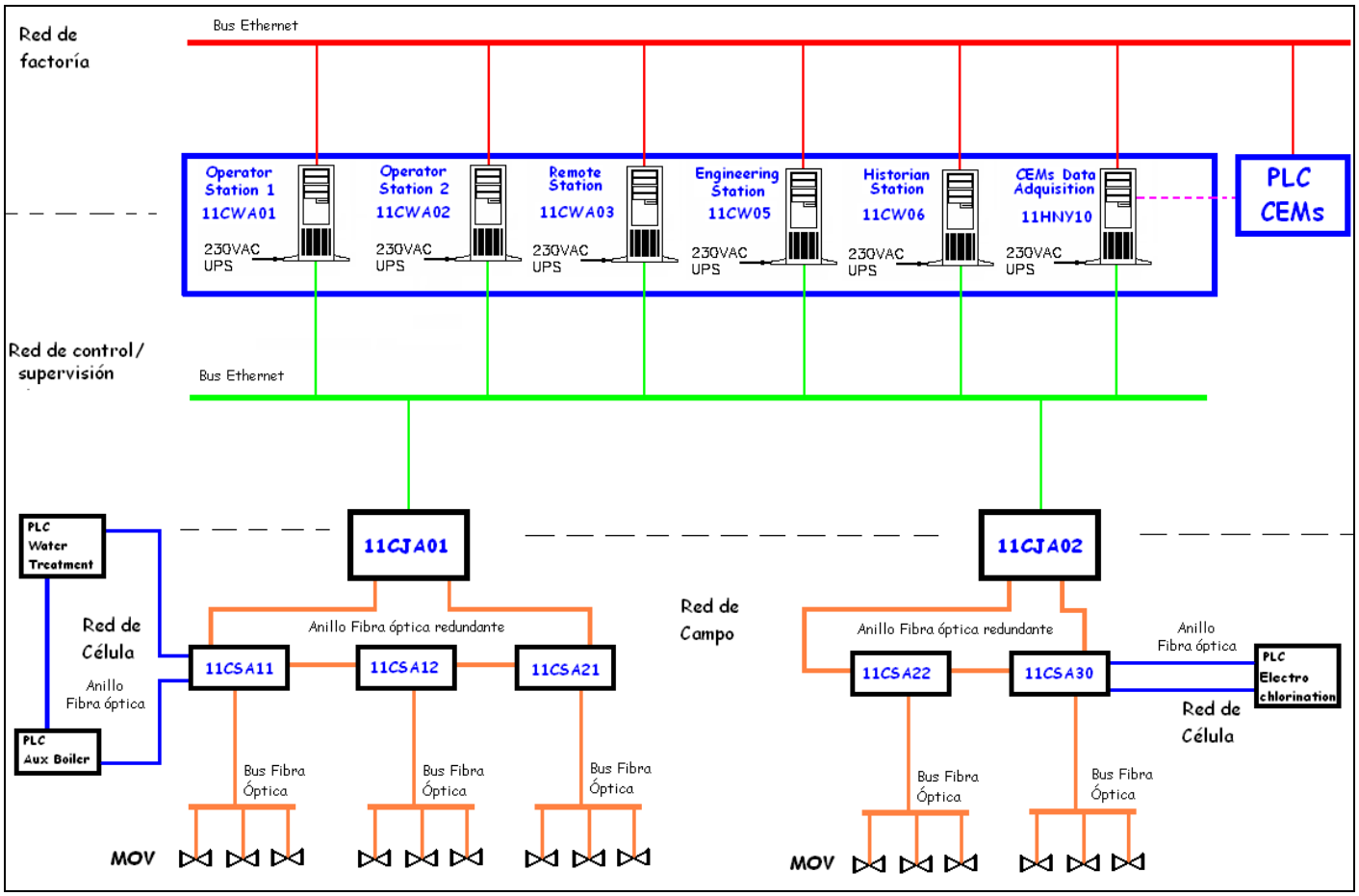


Figura 31.
Esquema general de redes de Planta Estándar.

Como se puede ver en la Figura 31, la arquitectura de la planta Estandar tiene varias redes de comunicación:

- Las redes de campo, marcadas en color naranja, que interconectan todas las señales de los dispositivos situados en campo con el procesador de control.
- Las redes de célula, marcadas en color azul, las cuales comunican los diferentes elementos de control de los sistemas paquete que funcionan totalmente independientes del control realizado por los procesadores de control del PCS.
- La red de control/supervisión, marcada en color verde, que comunica los procesadores de control con las estaciones de control de la CCR para que los operadores gobiernen el proceso de producción eléctrica, y otras estaciones de monitorización/configuración.
- La red de factoría, marcada en color rojo, que permite la comunicación de las diferentes secciones de la planta con las estaciones de monitorización para la visualización de parámetros del proceso, que les sean necesarios para la gestión de la planta.

7.6.1 Diseño de la red de proceso y segmentos que la componen.

Para la comunicación de los dispositivos de campo con el procesador de control, en cada una de las cabinas centralizadoras se hace una división de los dispositivos de los diferentes sistemas por segmentos de red, creando subredes de sistemas con sus correspondientes elementos de control.

La arquitectura de red de campo que se propone está basada en una topología mixta de bus líneal, para conectar los elementos de campo al segmento del sistema, y bus en anillo para conexión de los diferentes segmentos con el procesador de control. Gráficamente esto es:

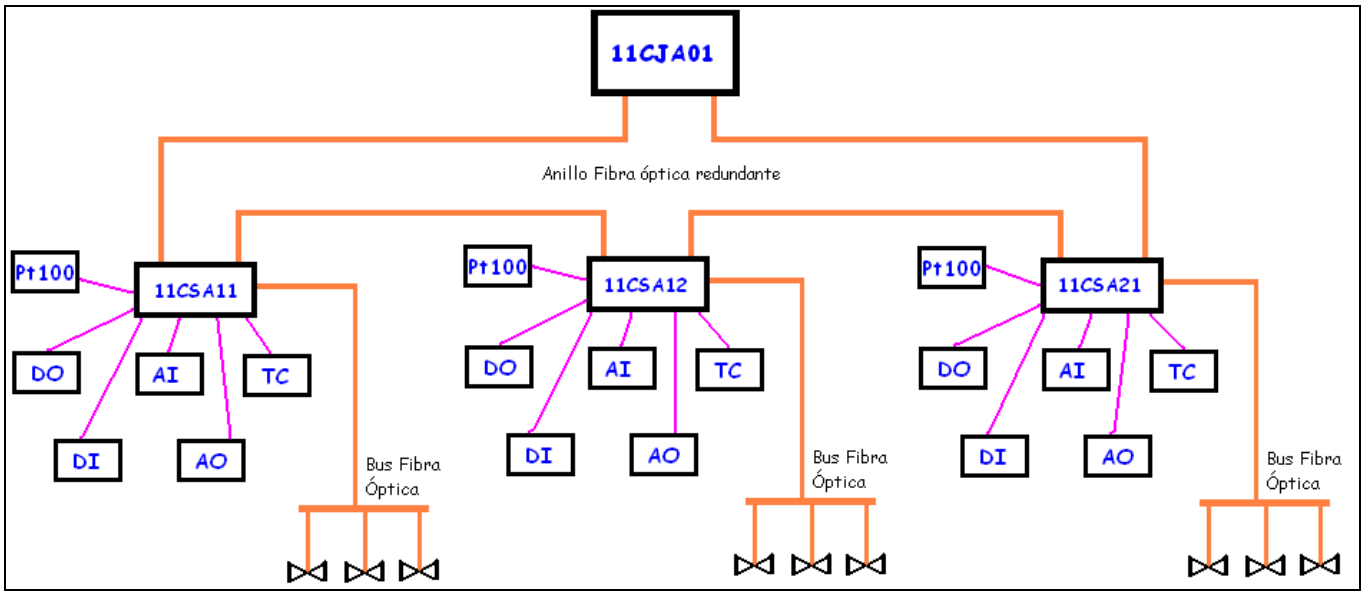


Figura 32.
Esquema general conexionado elementos de la red de campo del procesador 11CJA01.

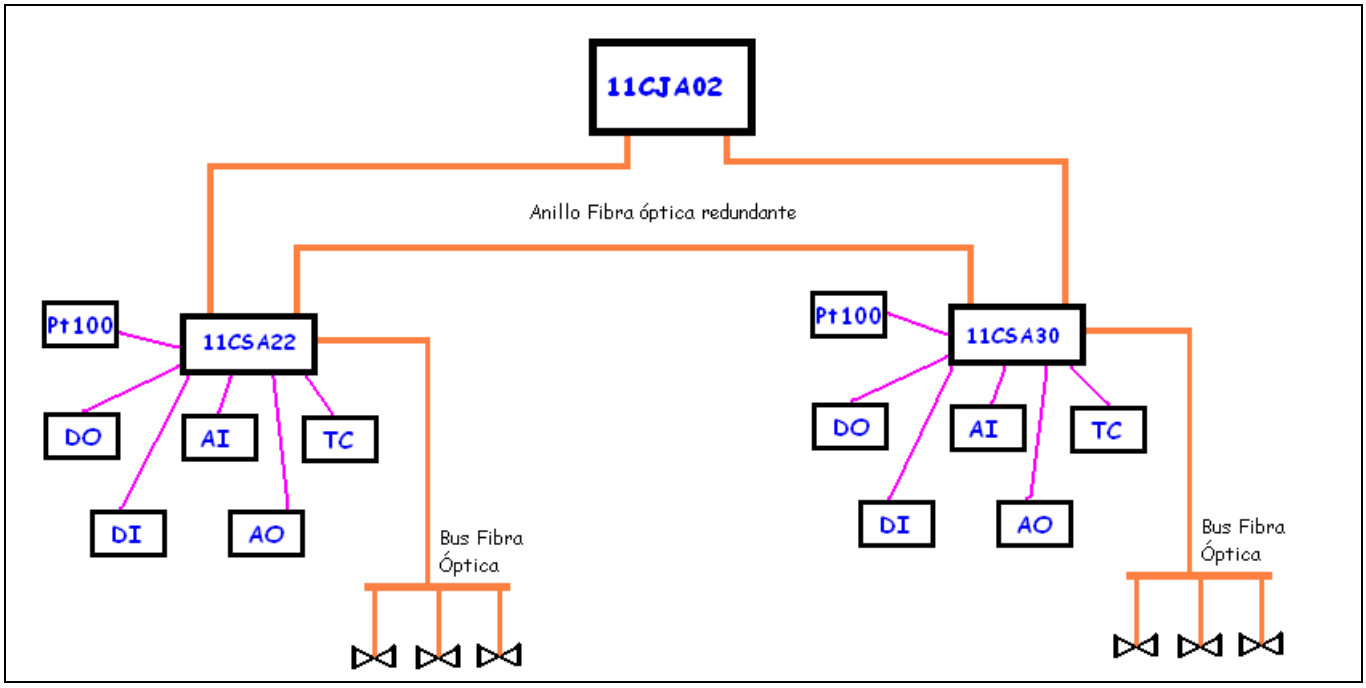


Figura 33.
Esquema general conexionado elementos de la red de campo del procesador 11CJA02.

7.6.1.1 Definición de segmentos de señales analógicas/digitales.

Para la integración de las señales (analógicas, digitales y MOV) procedentes de los dispositivos de campo en la red de campo, previamente se hace una división de ellas por sistemas en cada una de las cabinas centralizadoras, de forma que cada uno de estos conjuntos de señales representará un segmento de la red de campo. De este modo en caso de fallo o intervención por mantenimiento en un sistema concreto, se evita que interferir en segmentos de otros sistemas que pudiera ocasionar una malfunción en un sistema totalmente independiente al intervenido.

Para la comunicación de todos los elementos de la red de campo se emplean las versiones DP y PA de PROFIBUS:

- PROFIBUS-DP: esta versión de bus de campo está optimizada para alta velocidad y conexiones sencillas y baratas, con el objetivo de comunicar los sistemas de control y las entradas/salidas distribuidas. Por tanto, con esta versión de bus se conectan las señales analógicas y digitales a la red de campo mediante el empleo de elementos de periferia descentralizada

- PROFIBUS-PA: esta versión de bus de campo permite la conexión de sensores y actuadores a una línea de bus común incluso en áreas especialmente protegidas. Por tanto, esta versión del bus se utilizará para conectar las válvulas motorizadas (MOV) a la red de campo.

A continuación se definen los segmentos por cabina, indicando el número de señales y su tipo. Una vez definidos los segmentos y señales asociadas, se pasará a definir los módulos de interconexión necesarios para integrar las señales en la red de proceso, así como el bastidor de hardware necesario que conforma cada segmento.

Los segmentos que componen la red de campo por cabina, recogidos en el Anexo 2, son los siguientes:

- CABINA 11CSA11 (GT/HRSG).

Todas las señales centralizadas en esta cabina se distribuyen en un total de 16 segmentos, de la siguiente forma:

a) SEGMENTO CSA11-1 (HRSG System): de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:
   - 13 Entradas analógicas 4-20mA (AI).
   - 34 Entradas analógicas de termopar en mV (AI TC-E).
   - 5 Salidas analógicas 4-20mA (AO).
   - 40 Entradas digitales (DI).
   - 18 Salidas digitales (DO).
   - 14 Válvulas motorizadas (MOV).

b) SEGMENTO CSA11-2 (Auxiliary Steam System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:
   - 5 Entradas digitales (DI).
   - 2 Salidas digitales (DO).

c) SEGMENTO CSA11-3 (Compressed Air System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:
   - 1 Entradas analógicas 4-20mA (AI).
   - 5 Entradas digitales (DI).
   - 5 Salidas digitales (DO).

d) SEGMENTO CSA11-4 (Condensate System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:
   - 1 Entradas digitales (DI).
   - 2 Válvulas motorizadas (MOV).

e) SEGMENTO CSA11-5 (Desmineralised Water Storage & distribution System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:
   - 5 Entradas analógicas 4-20mA (AI).
   - 1 Salidas analógicas 4-20mA (AO).
   - 7 Entradas digitales (DI).
   - 6 Salidas digitales (DO).

f) SEGMENTO CSA11-6 (Feedwater System, IP/HP interstage bleed) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:
   - 26 Entradas analógicas 4-20mA (AI).
   - 3 Entradas analógicas de termopar en mV (AI TC-E).

- 8 Entradas analógicas de Pt-100 en Ω (AI Pt-100).
- 3 Salidas analógicas 4-20mA (AO).
- 13 Entradas digitales (DI).
- 11 Salidas digitales (DO).
- 4 Válvulas motorizadas (MOV).

g) SEGMENTO CSA11-7 (Fire Protection System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 2 Entradas digitales (DI).

h) SEGMENTO CSA11-8 (Fuel Gas System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 1 Entradas analógicas 4-20mA (AI).
- 1 Entradas analógicas de termopar en mV (AI TC-E).
- 10 Entradas digitales (DI).
- 2 Salidas digitales (DO).

i) SEGMENTO CSA11-9 (Gas Turbine Auxiliaries) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 1 Entradas analógicas 4-20mA (AI).

j) SEGMENTO CSA11-10 (HSRG Drains System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 3 Entradas analógicas 4-20mA (AI).
- 3 Entradas analógicas de termopar en mV (AI TC-E).
- 3 Salidas analógicas 4-20mA (AO).
- 4 Entradas digitales (DI).
- 4 Salidas digitales (DO).
- 4 Válvulas motorizadas (MOV).

k) SEGMENTO CSA11-11 (HVAC System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 4 Entradas digitales (DI).

l) SEGMENTO CSA11-12 (Plant Drains System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 14 Entradas digitales (DI).
- 8 Salidas digitales (DO).

m) SEGMENTO CSA11-13 (Sampling System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 26 Entradas analógicas 4-20mA (AI).

n) SEGMENTO CSA11-14 (Seal Steam System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 1 Entradas analógicas 4-20mA (AI).
- 3 Entradas analógicas de termopar en mV (AI TC-E).
- 2 Salidas analógicas 4-20mA (AO).
- 11 Entradas digitales (DI).
- 7 Salidas digitales (DO).

o) SEGMENTO CSA11-15 (Steam & bypass System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 17 Entradas analógicas 4-20mA (AI).
- 8 Entradas analógicas de termopar en mV (AI TC-E).
- 8 Salidas analógicas 4-20mA (AO).
- 4 Entradas digitales (DI).
- 5 Salidas digitales (DO).
- 2 Válvulas motorizadas (MOV).

p) SEGMENTO CSA11-16 (Steam Turbine Drains System) : de acuerdo con lo indicado en la Tabla 1 del Anexo 1, este segmento se compone de las siguientes señales:

- 6 Entradas analógicas 4-20mA (AI).
- 5 Entradas analógicas de termopar en mV (AI TC-E).
- 6 Entradas digitales (DI).
- 3 Salidas digitales (DO).

- <u>CABINA 11CSA22 (BOP/MECH).</u>

Todas las señales centralizadas en esta cabina se distribuyen en un total de 16 segmentos de la siguiente forma:

a) SEGMENTO CSA22-1 (HRSG System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 1 Entradas analógicas de termopar en mV (AI TC-E).
- 6 Entradas digitales (DI).
- 2 Salidas digitales (DO).
- 3 Válvulas motorizadas (MOV).

b) SEGMENTO CSA22-2 (Auxiliary Steam System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 3 Entradas analógicas 4-20mA (AI).
- 2 Entradas analógicas de termopar en mV (AI TC-E).
- 1 Salidas analógicas 4-20mA (AO).

- 8 Entradas digitales (DI).
- 2 Salidas digitales (DO).
- 1 Válvulas motorizadas (MOV).

c) SEGMENTO CSA22-3 (Circulating Water System/Cooling Tower): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 3 Entradas analógicas 4-20mA (AI).
- 4 Entradas analógicas de termopar en mV (AI TC-E).
- 21 Entradas digitales (DI).
- 11 Salidas digitales (DO).
- 4 Válvulas motorizadas (MOV).

d) SEGMENTO CSA22-4 (Condensate System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 14 Entradas analógicas 4-20mA (AI).
- 8 Entradas analógicas de termopar en mV (AI TC-E).
- 2 Entradas analógicas de Pt-100 en Ω (AI Pt-100).
- 4 Salidas analógicas 4-20mA (AO).
- 8 Entradas digitales (DI).
- 7 Salidas digitales (DO).

e) SEGMENTO CSA22-5 (Close Cooling Water System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 8 Entradas analógicas 4-20mA (AI).
- 2 Entradas analógicas de termopar en mV (AI TC-E).
- 2 Entradas digitales (DI).
- 1 Salidas digitales (DO).
- 6 Válvulas motorizadas (MOV).

f) SEGMENTO CSA22-6 (Condensate Vacuum System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 3 Entradas analógicas 4-20mA (AI).
- 16 Entradas digitales (DI).
- 10 Salidas digitales (DO).
- 1 Válvulas motorizadas (MOV).

g) SEGMENTO CSA22-7 (Fire Protection System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 1 Entradas analógicas de termopar en mV (AI TC-E).

h) SEGMENTO CSA22-8 (Chemical Injection System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 3 Entradas digitales (DI).
- 8 Salidas digitales (DO).

i) SEGMENTO CSA22-9 (Gas Turbine Auxiliaries): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 3 Entradas analógicas 4-20mA (AI).

j) SEGMENTO CSA22-10 (Fuel Oil System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 6 Entradas analógicas 4-20mA (AI).
- 1 Salidas analógicas 4-20mA (AO).
- 6 Entradas digitales (DI).
- 6 Salidas digitales (DO).

k) SEGMENTO CSA22-11 (H2, CO2 & N2 storage & distribution System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 1 Entradas digitales (DI).

l) SEGMENTO CSA22-12 (Plant Drains System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 14 Entradas digitales (DI).
- 8 Salidas digitales (DO).

m) SEGMENTO CSA22-13 (Open Cooling Water System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 5 Entradas analógicas 4-20mA (AI).
- 2 Entradas digitales (DI).
- 2 Salidas digitales (DO).
- 1 Válvulas motorizadas (MOV).

n) SEGMENTO CSA22-14 (Anti-Icing System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 1 Válvulas motorizadas (MOV).

o) SEGMENTO CSA22-15 (Steam & bypass System): de acuerdo con lo indicado en la Tabla 3 del Anexo 1, este segmento se compone de las siguientes señales:

- 18 Entradas analógicas 4-20mA (AI).
- 11 Entradas analógicas de termopar en mV (AI TC-E).
- 1 Salidas analógicas 4-20mA (AO).
- 31 Entradas digitales (DI).

- 9 Salidas digitales (DO).
- 8 Válvulas motorizadas (MOV).

- CABINA 11CSA12 (HSRG TOP).

Todas las señales centralizadas en esta cabina se distribuyen en un único segmento de la siguiente forma:

a) SEGMENTO CSA12-1 (HRSG System): de acuerdo con lo indicado en la Tabla 2 del Anexo 1, este segmento se compone de las siguientes señales:
   - 23 Entradas analógicas 4-20mA (AI).
   - 4 Salidas analógicas 4-20mA (AO).
   - 2 Entradas digitales (DI).
   - 4 Salidas digitales (DO).
   - 2 Válvulas motorizadas (MOV).

- CABINA 11CSA21 (BOP ELECTR).

Todas las señales centralizadas en esta cabina se distribuyen en un total de 16 segmentos de la siguiente forma:

a) SEGMENTO CSA21-1 (Close Cooling Water System): de acuerdo con lo indicado en la Tabla 4 del Anexo 1, este segmento se compone de las siguientes señales:
   - 4 Entradas digitales (DI).
   - 4 Salidas digitales (DO).

b) SEGMENTO CSA21-2 (Open Cooling Water System): de acuerdo con lo indicado en la Tabla 4 del Anexo 1, este segmento se compone de las siguientes señales:
   - 2 Entradas digitales (DI).
   - 2 Salidas digitales (DO).

c) SEGMENTO CSA21-3 (Feedwater System/IP-HP intestage bleed): de acuerdo con lo indicado en la Tabla 4 del Anexo 1, este segmento se compone de las siguientes señales:
   - 4 Entradas digitales (DI).
   - 4 Salidas digitales (DO).

d) SEGMENTO CSA21-4 (Condensate System): de acuerdo con lo indicado en la Tabla 4 del Anexo 1, este segmento se compone de las siguientes señales:
   - 4 Entradas digitales (DI).
   - 4 Salidas digitales (DO).

- CABINA 11CSA12 (HSRG TOP).

Todas las señales centralizadas en esta cabina se distribuyen en un único segmento de la siguiente forma:

b) SEGMENTO CSA30-1 (Circulating Water System): de acuerdo con lo indicado en la Tabla 5 del Anexo 1, este segmento se compone de las siguientes señales:

- 16 Entradas analógicas 4-20mA (AI).
- 2 Entradas analógicas de Pt-100 en Ω (AI Pt-100).
- 2 Salidas analógicas 4-20mA (AO).
- 18 Entradas digitales (DI).
- 18 Salidas digitales (DO).
- 2 Válvulas motorizadas (MOV).

7.6.1.2 Hardware para creación de segmentos de señales analógicas/digitales.

Como se ha analizado en el punto anterior, los buses adecuados para la comunicación entre los elementos de la Planta Estándar en estas redes de campo son los denominados DEVICEBUS.

Los elementos de interconexión usados entre los diferentes dispositivos y redes son del fabricante SIEMENS, debido a que ofrece una gama completa de productos totalmente probados y garantizados desde el nivel más bajo hasta el más alto de una red de comunicaciones, lo que se traduce en una alta interoperabilidad de todos los elementos de la red de comunicaciones unido con altas prestaciones. Quizá la nota negativa de usar productos SIEMENS sea el coste algo más elevado de sus productos frente a los de otros fabricantes, pero a la larga queda compensado con el gran soporte técnico que proporcionan para el mantenimiento de la instalación. Además, es el fabricante que más volumen de equipos tiene instalados y ofrecen una gran variedad de pasarelas que permiten integrar dispositivos basados en otro tipo de protocolo que no sea PROFIBUS, lo que facilita la integración de posibles nuevos sistemas futuros que mejoren la producción de la planta.

La comunicación de todos los elementos de la red de campo se realiza mediante PROFIBUS DP, y las señales analógicas y digitales se integran en la red de campo mediante el empleo de elementos de periferia descentralizada de la familia ET200 de SIEMENS [29], que se instalan en bastidores interiores de las cabinas centralizadoras. Como la conexión de todos los dispositivos analógicos y digitales de campo es mediante cableado tradicional, y las retricciones en cuanto a distancias vendrán definidas por los módulos de E/S empleados para la adquisición de las señales, así como las distancias máximas recomendadas por los fabricantes de los diferentes dispositivos de campo que se seleccionen.

a) Módulos ET200M [29]:

Los productos ET200 son elementos de periferia descentralizada (E/S remotas) muy diversos, tanto para soluciones en armario eléctrico o sin él, directamente en la máquina, así como para su uso en atmósferas potencialmente explosivas. La estructura modular permite escalar y ampliar los sistemas ET 200 de forma sencilla y en pequeños pasos. Más concretamente se va a utilizar las ET200M (Figura 34), ya que son módulos instalables de entradas y salidas analógicas y digitales ampliables, y también tienen la posibilidad de poder usarse para atmósferas explosivas (Ex).

Figura 34.
Periferia descentralizada ET200M [29].

Las características principales son:

- Diseño modular con módulos estándar del SIMATIC S7-300, también en configuración redundante.
- Módulos de E/S de seguridad positiva.
- Uso en atmósferas potencialmente explosivas hasta zona 2; sensores y actuadores hasta zona 1.
- Mayor disponibilidad de la instalación gracias a redundancia y a la posibilidad de cambio en caliente (hot swapping) o de modificar la configuración durante el servicio.

b) <u>Módulo de interfaz IM 153:</u>

El módulo de interfaz IM153 sirve para conectar la ET200 al sistema de bus, ya sea al bus de campo PROFIBUS o PROFINET. Se puede elegir entre diferentes módulos de interfaz, todos ellos con capacidad de diagnóstico granular por canales.

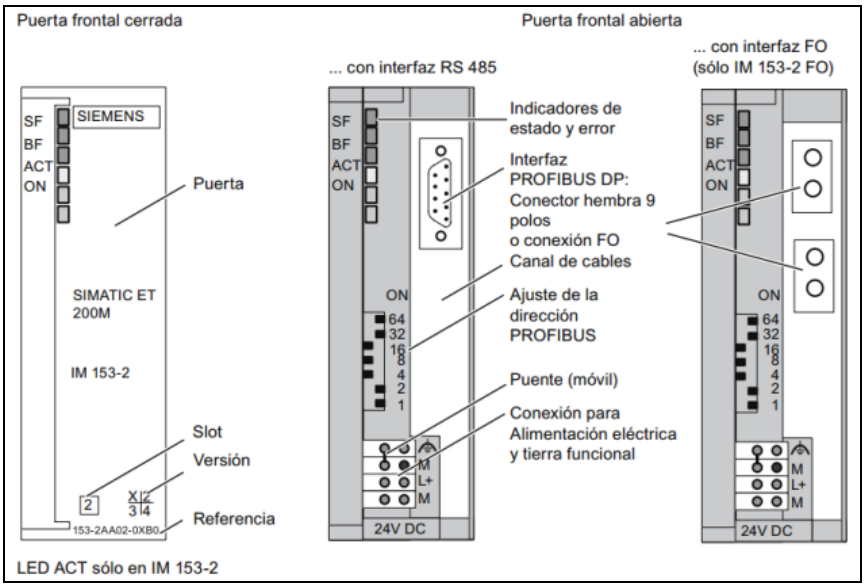


Figura 35.
Módulos de interfaz IM 153-1 e IM153-2 [29].

Los IM 153-x son módulos interfaz para módulos de señales (SM), módulos de función (FM) y procesadores de comunicaciones (CP). Disponen de una interfaz RS-485 (IM 153-2 o una interfaz para cable de fibra óptica) y ofrecen una serie de

funciones escalonadas. Las variantes de los módulos interfaz IM 153-2 correspondientes en cada caso con RS-485 o interfaz para cable de fibra óptica cuentan con las mismas funciones. De ello resultan las ventajas siguientes:

- Descarga del controlador central.
- Reducción de los tiempos de reacción ante señales críticas in situ.
- Programas más claros y cortos.
- Simplificación de la búsqueda de errores.
- Descarga del sistema de bus.
- Modularización de la máquina o instalación y puesta en marcha anticipada de los módulos, también en emplazamientos distintos.

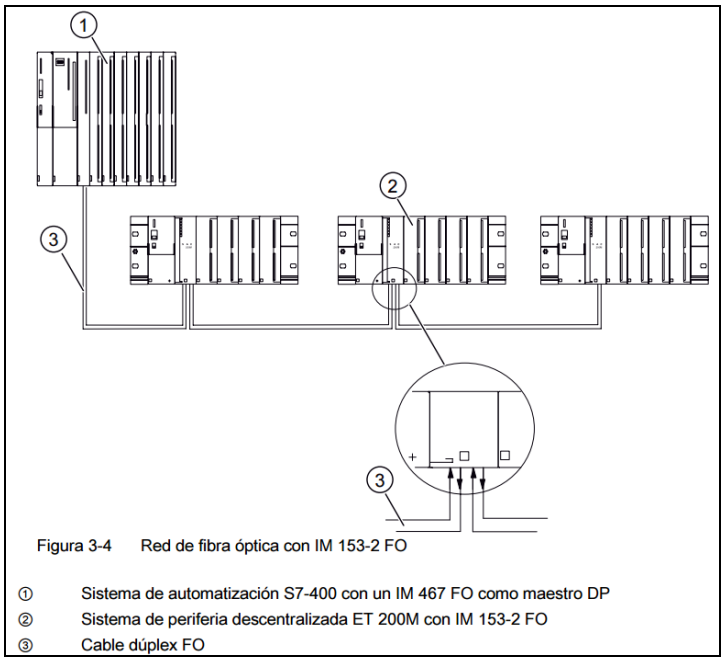


Figura 36.
Ejemplo conexión IM 153-2 y ET200M en red de fibra óptica [29].

Para conectar las señales analógicas y digitales a la ET200M se precisa de módulos de E/S analógicos y digitales.

c) <u>Módulos E/S:</u> para conectar a la ET200M las señales analógicas y digitales de campo se necesario el empleo de módulos de entrada/salida tipo SM. Los diferentes tipo de módulo SM son los siguientes:

- SM321: módulo de 16/32 entradas digitales.
- SM322: módulo de 8/16 salidas digitales tipo relé.
- SM323: módulo de 16 entradas/salidas digitales.
- SM331: módulo de 8 entradas analógicas (admite tipo de señal 4-20mA, termopares y Pt-100).
- SM332: módulo de 8 salidas analógicas.
- SM334: módulo de 4 entradas/4 salidas analógicas (no admite Pt-100).

Los módulos de E/S digitales tienen restricción en cuanto distancia máxima de 1000 metros, mientras que para los módulos de E/S analógicos la restricción es de 200 metros.

La ET200M junto con el módulo interfaz IM153 integra todas las señales conectadas a sus módulos de E/S en la red de proceso, permitiendo conectar las señales de campo al procesador de control MARK VIe.

La ET200M y el interfaz IM153 van instalados sobre un mismo rack (perfil soporte) que se alimenta mediante una fuente de alimentación PS307.

Por tanto, un segmento de sistema que integra las señales analógicas y digitales de campo se compone de: ET200M, Módulos de E/S analógicas, interfaz IM153 y fuente de alimentación PS307.

7.6.1.3 Rack de segmentos de señales analógicas/digitales.

Todas las las señales analógicas y digitales de la Planta Estándar están centralizadas en las cabinas 11CSA11/12/21/22/30, las cuales están situadas en diferentes ubicaciones de la planta con el objeto de centralizar las señales de los dispositivos de los diferentes sistemas, optimizando las distancias máximas para su cableado teniendo en cuenta las distancias recomendados por el fabricante del dispositivo seleccionado, además de tener en cuenta las distancias máximas recomendadas por SIEMENS para cada uno de sus módulos de E/S, referenciadas en el punto anterior.

Cada cabina de centralización lleva sus bastidores correspondientes para permitir la instalación de los elementos de conexión comentados en el punto anterior y así integrar las señales a la red de proceso. La configuración típica para un bastidor mediante ET200 es la siguiente:

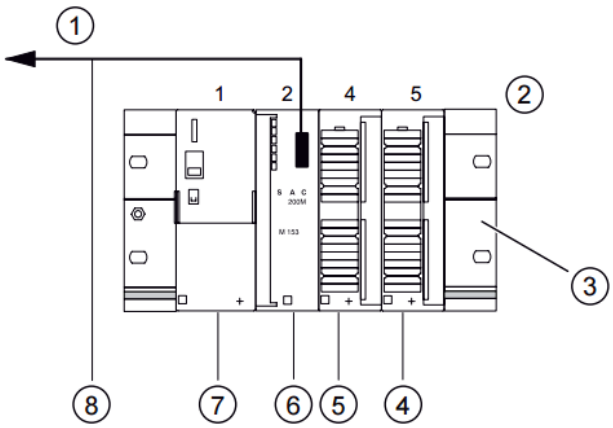


Figura 2-1 Componentes del ET 200M para la configuración de ejemplo

①	al maestro DP	⑤	SM 321
②	Slot	⑥	IM 153-2
③	Perfil soporte	⑦	Fuente de alimentación PS 307
④	SM 322	⑧	Cable PROFIBUS con conector de bus

Figura 37.
Ejemplo bastidor ET-200M [29].

Por tanto, de acuerdo con la definición de segmentos realizada en el punto anterior a continuación se definen los rack de cada uno de los segmentos de señales analógicas/digitales representados en el Anexo 2:

SEGMENTO CSA11-1

	Nº SEÑALES/ TIPO	Fibra Optica	13 AI (4-20mA)	32 DI	4 DI	15 DO			
CABINA CSA11 RACK 1	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	32 Entradas digitales SIM 321	16 Salidas digitales (relé) SIM 322	16 Salidas digitales (relé) SIM 322	Acoplador DP/PA	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	2	1	1	1	1		1

SEGMENTO CSA11-2

	Nº SEÑALES/ TIPO	Fibra Optica	5 DI	5 DO					
CABINA CSA11 RACK 2	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 Entradas digitales SIM 321	16 Salidas digitales (relé) SIM 322	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1					1

SEGMENTO CSA11-3

	Nº SEÑALES/ TIPO	Fibra Optica	1 AI (4-20mA)	5 DI	5 DO				
CABINA CSA11 RACK 3	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	16 Entradas digitales SIM 321	16 Salidas digitales (relé) SIM 322	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1				1

SEGMENTO CSA11-4

	Nº SEÑALES/ TIPO	Fibra Optica	1 DI						
CABINA CSA11 RACK 4	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 Entradas digitales SIM 321	Acoplador DP/PA	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1					1

SEGMENTO CSA11-5

	Nº SEÑALES/ TIPO	Fibra Optica	5 AI (4-20mA)	34 AI (termopar)	1 AO (4-20mA)	7 DI/ 6 DO			
CABINA CSA11 RACK 5	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	5	1	1			1

SEGMENTO CSA11-6

	Nº SEÑALES/ TIPO	Fibra Optica	24 AI (4-20mA)	8 AI (Pt-100)	34 AI (termopar)	8 DI/ 8DO			
CABINA CSA11 RACK 6	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Entradas analógicas SIM 331	8 Entradas analógicas SIM 331	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	3	1	1	1	1		1

SEGMENTO CSA11-7

	Nº SEÑALES/ TIPO	Fibra Optica	2 DI						
CABINA CSA11 RACK 7	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 Entradas digitales SIM 321	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA11-8

	Nº SEÑALES/ TIPO	Fibra Optica	1 AI/ 2AI (4-20mA)/ (termopar)	10 DI/ 2DO					
CABINA CSA11 RACK 8	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1					1

SEGMENTO CSA11-9

Nº SEÑALES/ TIPO		Fibra Optica	1 AI (4-20mA)						
CABINA CSA11 RACK 9	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA11-10

Nº SEÑALES/ TIPO		Fibra Optica	3 AI/ 3AI (4-20mA)/ (termopar)	3 AO	4 DI/ 4DO				
CABINA CSA11 RACK 10	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1	1			1

SEGMENTO CSA11-11

Nº SEÑALES/ TIPO		Fibra Optica	4 DI						
CABINA CSA11 RACK 11	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 Entradas digitales SIM 321	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA11-12

Nº SEÑALES/ TIPO		Fibra Optica	8 DO						
CABINA CSA11 RACK 12	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Salidas digitales SIM 322	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA11-13

Nº SEÑALES/ TIPO		Fibra Optica	26 AI (4-20mA)						
CABINA CSA11 RACK 13	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	4						1

SEGMENTO CSA11-14

Nº SEÑALES/ TIPO		Fibra Optica	1 AI/ 3AI (4-20mA)/ (termopar)	2 AO	11 DI	7 DO			
CABINA CSA11 RACK 14	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 Entradas digitales SIM 321	8 Salidas digitales SIM 322	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1	1			1

SEGMENTO CSA11-15

Nº SEÑALES/ TIPO		Fibra Optica	17AI/ 8AI (4-20mA)/ (termopar)	8 AO	4 DI/ 5DO				
CABINA CSA11 RACK 15	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	5	1	1	1			1

SEGMENTO CSA11-16

Nº SEÑALES/ TIPO		Fibra Optica	6AI/ 5AI (4-20mA)/ (termopar)	1 AO	8 DI/ 4DO				
CABINA CSA11 RACK 16	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	2	1	1				1

SEGMENTO CSA12-1

Nº SEÑALES/ TIPO		Fibra Optica	23 AI (4-20mA)	4 AO	2 DI/ 4DO				
CABINA CSA12 RACK 1	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	3	1	1	1			1

SEGMENTO CSA21-1

Nº SEÑALES/ TIPO		Fibra Optica	4 DI/ 4DO						
CABINA CSA21 RACK 1	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA21-2

Nº SEÑALES/ TIPO		Fibra Optica	2 DI/ 2DO						
CABINA CSA21 RACK 2	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA21-3

Nº SEÑALES/ TIPO		Fibra Optica	4 DI/ 4DO						
CABINA CSA21 RACK 3	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA21-4

Nº SEÑALES/ TIPO		Fibra Optica	4 DI/ 4DO						
CABINA CSA21 RACK 4	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA22-1

Nº SEÑALES/ TIPO		Fibra Optica	1 AI (termopar)	6 DI/ 2DO					
CABINA CSA22 RACK 1	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1				1

SEGMENTO CSA22-2

Nº SEÑALES/ TIPO		Fibra Optica	3AI/ 2AI (4-20mA)/ (termopar)	1 AO	8 DI/ 2DO				
CABINA CSA22 RACK 2	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1	1			1

SEGMENTO CSA22-3

Nº SEÑALES/ TIPO		Fibra Optica	3AI/ 4AI (4-20mA)/ (termopar)	18 DI	11 DO				
CABINA CSA22 RACK 3	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	32 Entradas digitales SIM 321	16 Salidas digitales SIM 322	Acoplador DP/PA	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1	1			1

SEGMENTO CSA22-4

	Nº SEÑALES/ TIPO	Fibra Optica	16 AI (4-20mA)	2AI/10AI (Pt-100)/ (termopar)	4 AO	8 DI/ 7DO			
CABINA CSA22 RACK 4	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	2	2	1	1			1

SEGMENTO CSA22-5

	Nº SEÑALES/ TIPO	Fibra Optica	8AI/ 2AI (4-20mA)/ (termopar)	2 DI/ 1DO					
CABINA CSA22 RACK 5	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	2	1	1				1

SEGMENTO CSA22-6

	Nº SEÑALES/ TIPO	Fibra Optica	2 AI (4-20mA)	16 DI	10 DO				
CABINA CSA22 RACK 6	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	16 Entradas digitales SIM 321	16 Salidas digitales SIM 322	Acoplador DP/PA	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	2	1	1	1			1

SEGMENTO CSA22-7

	Nº SEÑALES/ TIPO	Fibra Optica	1AI/ 1AI (4-20mA)/ (termopar)						
CABINA CSA22 RACK 7	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA22-8

	Nº SEÑALES/ TIPO	Fibra Optica	3 DI/ 8DO						
CABINA CSA22 RACK 8	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA22-9

	Nº SEÑALES/ TIPO	Fibra Optica	1 AI (4-20mA)						
CABINA CSA22 RACK 9	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA22-10

	Nº SEÑALES/ TIPO	Fibra Optica	6AI (4-20mA)	1 AO	6 DI/ 6DO				
CABINA CSA22 RACK 10	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1				1

SEGMENTO CSA22-11

	Nº SEÑALES/ TIPO	Fibra Optica	1 DI						
CABINA CSA22 RACK 11	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 E/S digitales SIM 323	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA22-12

	Nº SEÑALES/ TIPO	Fibra Optica	14 DI	8 DO					
CABINA CSA22 RACK 12	Fuente Alimentación PS307	Módulo intefaz IM153-2	16 Entradas digitales SIM 321	16 Salidas digitales SIM 322	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1					1

SEGMENTO CSA22-13

	Nº SEÑALES/ TIPO	Fibra Optica	5AI (4-20mA)	2 DI/ 2DO					
CABINA CSA22 RACK 13	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	16 E/S digitales SIM 323	Acoplador DP/PA	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1	1	1				1

SEGMENTO CSA22-14

	Nº SEÑALES/ TIPO	Fibra Optica							
CABINA CSA22 RACK 12	Fuente Alimentación PS307	Módulo intefaz IM153-2	Acoplador DP/PA	LIBRE	LIBRE	LIBRE	LIBRE	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	1						1

SEGMENTO CSA22-15

	Nº SEÑALES/ TIPO	Fibra Optica	18AI/ 11AI (4-20mA)/ (termopar)	1 AO	16 DI	9 DO			
CABINA CSA22 RACK 15	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	16 Entradas digitales SIM 321	16 Salidas digitales SIM 322	Acoplador DP/PA	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	4	1	1	1	1		1

SEGMENTO CSA30-1

	Nº SEÑALES/ TIPO	Fibra Optica	16AI/2AI (4-20mA)/ (Pt-100)	2 AO	18 DI	18 DO			
CABINA CSA30 RACK 1	Fuente Alimentación PS307	Módulo intefaz IM153-2	8 Entradas analógicas SIM 331	8 Salidas analógicas SIM 332	32 Entradas digitales SIM 321	16 Salidas digitales SIM 322	Acoplador DP/PA	LIBRE	Perfil soporte/ Slot
CANTIDAD	1	1	2	1	1	2	1		1

7.6.1.4 Definición de segmentos de válvulas motorizadas (MOV):

Una vez definidos todos los segmentos que permitirán integrar las señales analógicas/digitales de los dispositivos de campo en el bus mediante PROFIBUS-DP, para completar la red de campo es necesario conectar también al bus las válvulas motorizadas (MOV).

Al igual que las señales analógicas y digitales, cada válvula motorizada está asignada a un sistema en concreto, como se puede ver en la Tablas de señales del Anexo 1, por lo que se debe conectar cada MOV a su segmento de sistema adecuado.

La topología que se ha establecido para la red de campo es una topología mixta basada en bus lineal para los elementos que forman cada segmento, y una topología en anillo para comunicar los segmentos con el procesador de control MARK VIe.

Por tanto, asociado a cada rack de segmentos se establece un bus lineal que conecta cada una de las MOVs a su segmento, mediante la versión PROFIBUS-PA, y a su vez este bus lineal se conecta a la red de campo con enlaces ópticos PROFIBUS OLM® que más adelante se detallan.

Para conectar las MOVs a su segmento, se empleará un tramo de cable común para conexión tipo RS-485 de PROFIBUS definido más adelante. Dicho tramo de cable comenzará en un acoplador DP/PA y finalizará en un terminador de bus (ver Figura 43), de modo que se irán conectando las MOV al mismo empleando conectores SpliTConnect Tap (Figura 38), mediante tramos de cable tipo FC que irán conectados a las MOV mediante conectores tipo M12 [26].

Finalmente, para conectar este segmento PROFIBUS-PA a la red de campo, se conecta el puerto DB-9 (RS-485) del acoplador DP/PA al módulo OLM correspondiente, alimentándolo desde la fuente PS307 del bastidor de su segmento asociado (ver Figura 40).

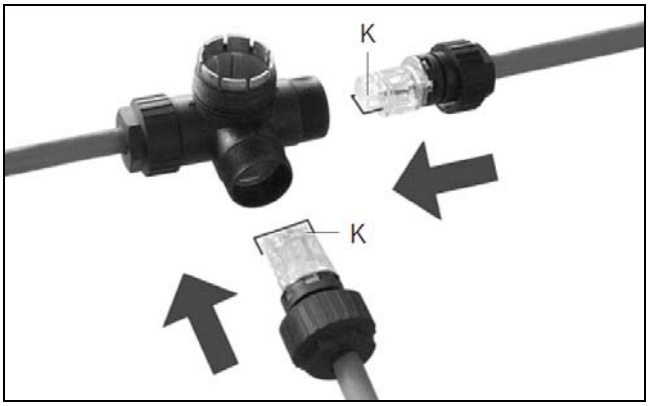


Figura 38.
SpliTconnect Fast [31].

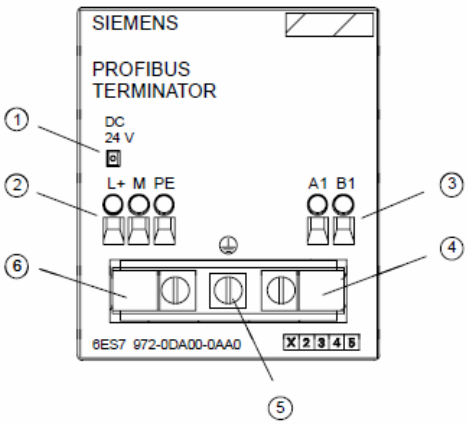
Design of the PROFIBUS Terminator	No.	Function
	①	LED 24 V power supply
	②	Connection for power supply 24 V DC
	③	PROFIBUS attachment
	④	Shield clamp grounding the braid shield and for strain relief of the LAN cable
	⑤	Ground screw
	⑥	Cable clamp for strain relief of the power supply cable

Figura 39.
Terminador PROFIBUS [31].

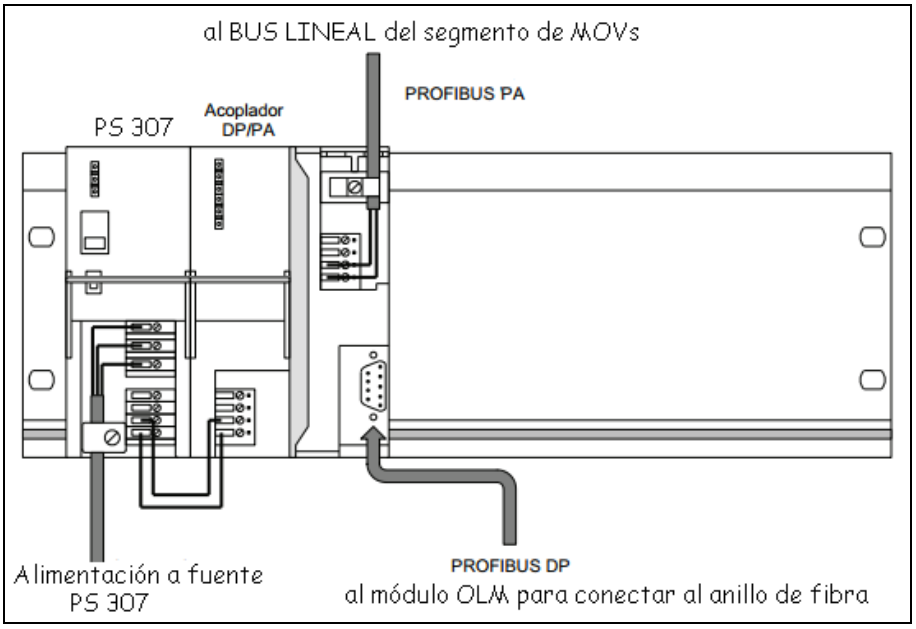


Figura 40.
Acoplador PROFIBUS-PA [33].

7.6.1.5 Comunicación entre segmentos. Optical Link Manager (OLM).

Como comunicación entre segmentos se optan por fibra óptica, ya evita que la presencia de interferencias electromagnéticas afecte a la comunicación si no se puede asegurar una conexión equipotencial fiable, o si las instalaciones son al aire libre o bien si no se desea que se emitan radiaciones electromagnéticas. Para construir topologías de red ópticas se utilizan cables de fibra óptica de vidrio (FO de vidrio) para cubrir grandes distancias, mientras que para las distancias cortas se emplean cables de fibra óptica de plástico compuestos por materiales conductores de luz, como la fibra óptica de plástico (Polymer Optic Fiber, POF) o bien las fibras de vidrio con recubrimiento plástico (Polymer Cladded Fiber, PCF).

Para definir las topologías de red comentadas en la red de proceso, se utilizan módulos PROFIBUS OLM diseñados para su uso en redes de bus de campo PROFIBUS ópticas. Los módulos denominados Optical Link Modules (OLMs) permiten construir fácilmente una red óptica con topología en línea, anillo y/o estrella. Dos OLMs pueden estar distanciados hasta 15 km y la velocidad de transmisión puede ajustarse en escalones de 9,6 kbit/s a 12 Mbit/s. Además, permiten la conversión de interfaces PROFIBUS eléctricas (RS-485) en el nivel de las interfaces PROFIBUS ópticas y viceversa.

Los módulos se pueden integrar en las redes de bus de campo PROFIBUS configurados para topologías: lineal (bus), estrella o anillo. Además, para aumentar la fiabilidad de la red de bus de campo en caso de fallo, se pueden configurar anillos redundantes [28].

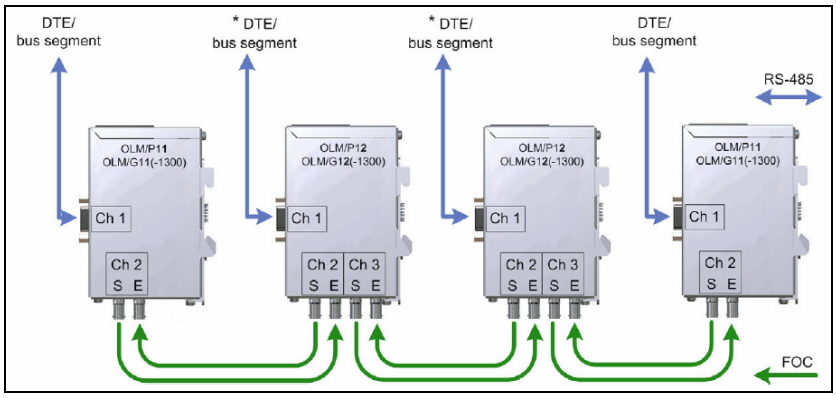


Figura 41.
Configuración OLM para topología en bus lineal [28].

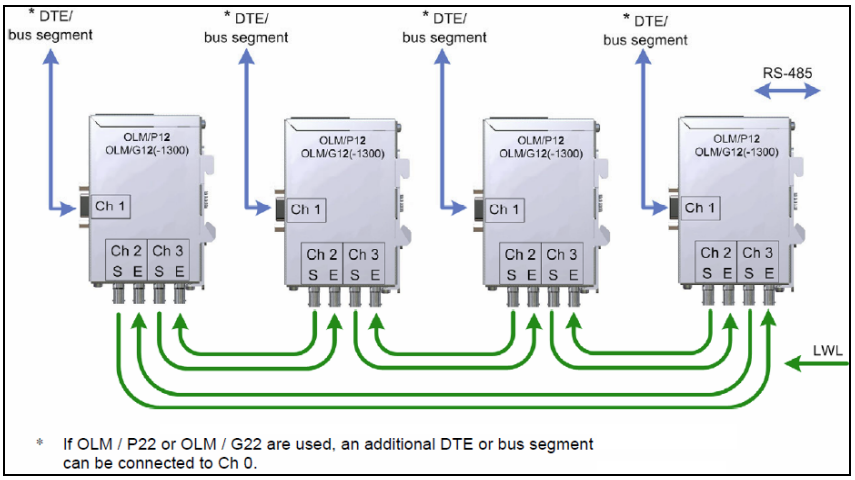


Figura 42.
Configuración OLM para topología con anillo redundante [28].

Por tanto, un segmento estándar de la red de proceso tiene la siguiente configuración:

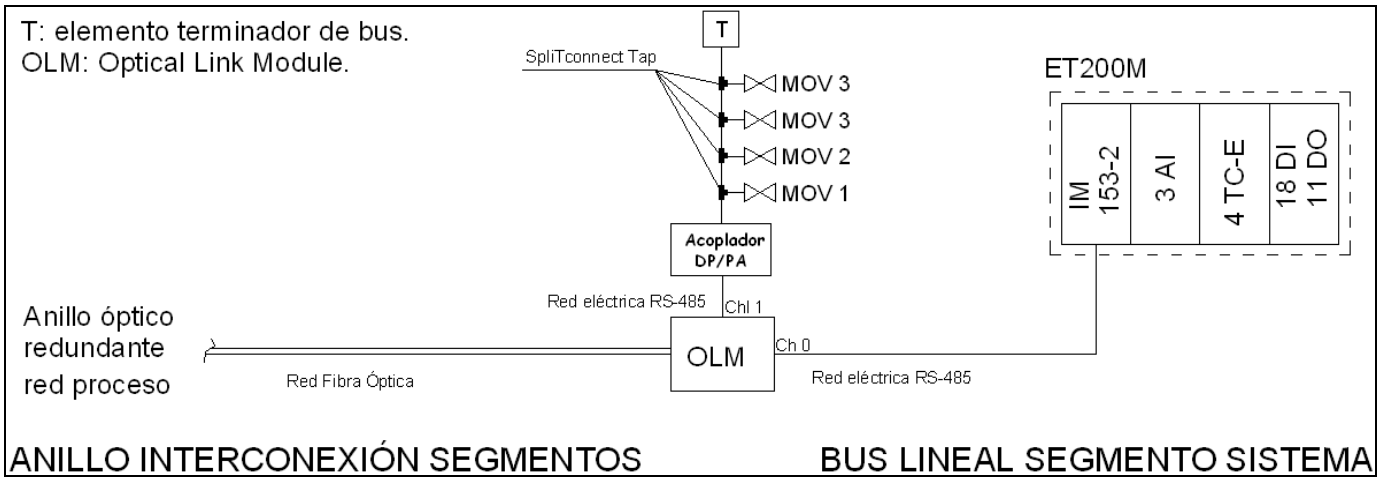


Figura 43.
Configuración segmento estándar de la red de proceso.

Todos lo elementos OLM y el conjunto del bastidor que forman cada segmento indicado en el punto anterior, van instalados en las cabinas centralizadores de señales sobre rack de bastidores.

Como se puede observar en la Figura 43, el módulo OLM es el módulo "frontera" entre las topologías de red conectando mediante RS-485 los elementos de campo que componen el segmento, para conectar al anillo de fibra óptica encargado de conectar todos los segmentos de la red de proceso al procesador de control.

Por tanto, según lo definido la red de proceso de la Planta Estándar de Ciclo combinado queda como se representa en el Anexo 2.

En dicho Anexo 2, además de la topología de los segmentos de la red de campo se representa la conexión de las MOV mediante conexión eléctrica RS-485, usando acopladores DP/PA y conectores SpliTconnect, para hacer el bus lineal que se conecta al OLM (Ch 0) y hacer la conversión de medio a Fibra Óptica. Las ET200M también se conectan con módulos de interfaz IM mediante RS-485 en lugar del IM153-2 de FO definida incialmente, ya que de este modo es posible utilizar los puertos RS-485 (Ch0 y Ch1) de los módulos OLM. Además los módulos interfaz IM153-2 FO para la conexión de Fibra Óptica de las ET200M no son redundantes, y el anillo de la red de campo se ha definido con comunicación redundante.

Los módulos OLM manejan todo el rango de velocidad de transmisión admitido por la especificación PROFIBUS (de 9,6Kbps hasta 12Mbps) y detectan automáticamente el baudrate del bus en todo momento, transmitiendo a esa velocidad.

La alimentación de los módulos OLM es a +24VDC, y se realiza desde las mismas fuentes de alimentación PS307 de los módulos que alimentan las ET200M y el acoplador DP/PA del mismo segmento.

7.6.1.6 Cableado de redes PROFIBUS DP/PA.

Para establecer diferentes topologías de red mediante el uso PROFIBUS DP y PA, existen dos tipos de cableado en función del tipo de señal de la red que conectan:

a) Redes eléctricas: este tipo de redes están basadas en el estádar RS-485 y emplean cables de par trenzado y apantallado. Para zonas sujetas a riesgo de explosión se emplea cable de par trenzado según IEC 1158-2.

Las características de los cables para este tipo de redes son [26]:

- Admite topologías en línea o árbol.
- Ahorro de tiempo mediante un rápido y fácil montaje de los conectores con cables FastConnect.
- Para diferentes aplicaciones a través de cables de bus especiales.
- Red insensible a interferencias mediante doble apantallado.
- Cable de bus para sistemas de bus según IEC 61158- 2, p.e. PROFIBUS-PA.
- Distintas variantes para diferentes aplicaciones (Ex, No Ex).
- Alta seguridad ante interferencias mediante un buen apantallamiento.
- Fácil estimación de longitud mediante marcación por metros.
- Es posible realizar estructuras mixtas ópticas y eléctricas mediante el empleo de OLM.

Para el caso de nuestra aplicación en la red de comunicaciones de la Planta Estándar de Ciclo Combinado, se utiliza este tipo de cable para conectar al módulo OLM el segmento de bus lineal compuesto por la ET200M y/o válvulvas motorizadas MOV (según aplique). El cable seleccionado para este tipo de redes eléctricas es de 3 tipos: Un cable estándar para recorridos por zonas con condiciones ambientales normales y recorridos interiores, otro cable más robusto para recorridos por zonas con condiciones ambientales más agresivas e interiores, y por último un cable para exteriores.

- FC robust cable 6XV1 830-0JH10: que con su cubierta PUR cumple con la especificación EN 50170 (tipo de cable A); con las siguientes características técnicas respecto al standar:
  - Retardante de llama.
  - Autoextinguible en caso de incendio.
  - Resistente a ciertas grasas y aceites minerales.
  - Material de la cubierta no libre de halógenos.

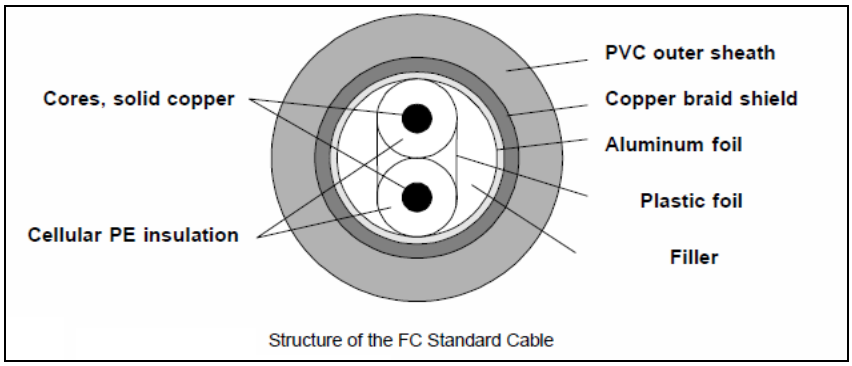


Figura 44.
Estructura cable estándar para RS-485 en interiores [26].

- FC robust cable 6XV1 830-0JH10: que con su cubierta PUR cumple con la especificación EN 50170 (tipo de cable A); con las siguientes características técnicas respecto al standar:
  - Hilos de cobre rígidos.
  - Mayor resistencia a la abrasión.
  - Resistente a la radiación ultravioleta.
  - Cubierta retardante de llama.
  - Mayor resistencia a grasas y aceites minerales.

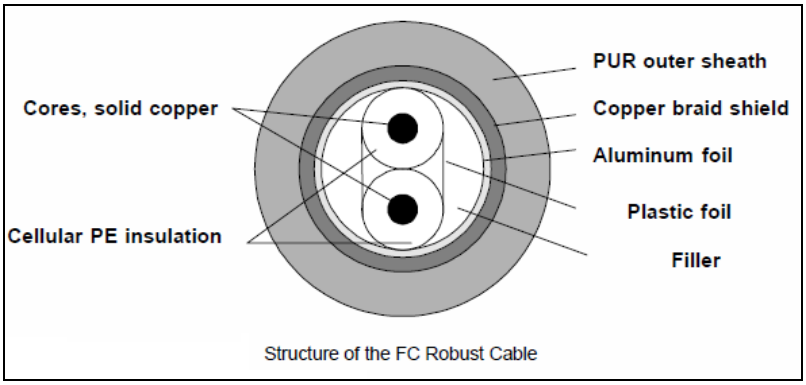


Figura 45.
Estructura cable robusto para RS-485 en interiores [26].

- FC Underground Cable 6GK1 830-3FH10: es un cable cuya estructura interna y características eléctricas son idénticas a las del cable estándar con la diferencia que la cubierta exterior se fabrica en materiales que permiten su tendido por zonas exteriores.

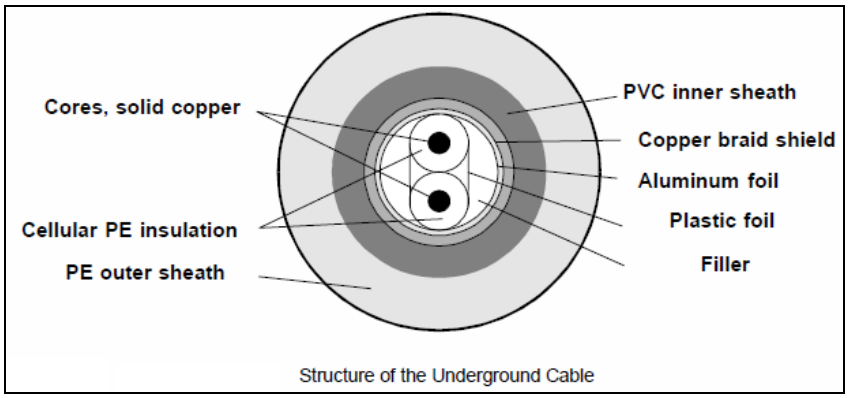


Figura 46.
Estructura cable para RS-485 en exteriores [26].

Estos tipos de cables seleccionados son cables considerados estándar para realizar el cableado de las comunicaciones de la Planta Estandar, pero para recorridos especialmente por zonas “delicadas” debería tratarse particularmente con SIEMENS o incluso elaborar un especificación para la búsqueda del cable en el mercado. Para recorridos por zonas ATEX deben emplearse cables especificados para PROFIBUS PA.

Las características técnicas de los dos cables seleccionados se recogen en la siguiente Tabla 6:

Technical Specifications [1)] Cable Type	**FC Standard Cable**	**FC FRNC Cable**	**FC Food Cable**	**FC Robust Cable**	**FC Under-ground Cable**
Order Number	6XV1 830 -0EH10	6XV1 830 -0LH10	6XV1 830 -0GH10	6XV1 830 -0JH10	6XV1 830 -3FH10
Attenuation at 16 MHz at 4 MHz at 38.4 kHz at 9.6 kHz	 < 42 dB/km < 22 dB/km < 4 dB/km <2.5 dB/km	 < 42 dB/km < 22 dB/km < 4 dB/km <2.5 dB/km	 < 42 dB/km < 22 dB/km < 4 dB/km <2.5 dB/km	 < 42 dB/km < 22 dB/km < 4 dB/km <2.5 dB/km	 < 42 dB/km < 22 dB/km < 4 dB/km <2.5 dB/km
Characteristic impedance at 9.6 kHz at 31.25 kHz at 38.4 kHz at 3 to 20 MHz Rated value	 270 ± 27 Ω - 185 ± 18.5 Ω 150 ± 15 Ω 150 Ω	 270 ± 27 Ω - 185 ± 18.5 Ω 150 ± 15 Ω 150 Ω	 270 ± 27 Ω - 185 ± 18.5 Ω 150 ± 15 Ω 150 Ω	 270 ± 27 Ω - 185 ± 18.5 Ω 150 ± 15 Ω 150 Ω	 270 ± 27 Ω - 185 ± 18.5 Ω 150 ± 15 Ω 150 Ω
d.c. loop resistance	≤ 110 Ω /km	≤ 110 Ω /km	≤ 110 Ω /km	≤ 110 Ω /km	≤ 110 Ω /km
Shield resistance	≤ 9.5 Ω /km	≤ 9.5 Ω /km	≤ 9.5 Ω /km	≤ 9.5 Ω /km	≤ 9.5 Ω /km
Effective capacitance at 1 kHz	approx. 28.5 nF/km	approx. 28.5 nF/km	approx. 28.5 nF/km	approx. 28.5 nF/km	approx. 28.5 nF/km
Operating voltage (effective)	≤ 100 V	≤ 100 V	≤ 100 V	≤ 100 V	≤ 100 V
Cable type standard code	02YY(ST)CY 1x2x0.64/2.55-150 KF 40 FRNC VI	02YSH(ST)CH 1x2x0.64/2.55-150 VI KF25 FRNC	02YSY(ST)C2Y 1x2x0.64/2.55-150 KF40	02YSY(ST)C11Y 1x2x0.64/2.5-150 KF40 FRNC VI	02YSY(ST)CY2Y 1x2x0.64/2.5-150 KF 40 SW
Sheath Material Color Diameter	 PVC violet 8.0 ± 0.4 mm	 FRNC light violet 8.0 ± 0.4 mm	 PE black 8.0 ± 0.4 mm	 PUR violet 8.0 ± 0.4 mm	 PE/PVC black 10.8 ± 0.5 mm [3)]
Permitted ambient conditions – Operating temperature – Transport/storage temperature – Installation temperature	 -40°C + 60°C -40°C + 60°C -40°C + 60°C	 -25°C + 60°C -25°C + 60°C -25°C + 60°C	 -40°C + 60°C -40°C + 60°C -40°C + 60°C	 -40°C + 60°C -40°C + 60°C -40°C + 60°C	 -40°C + 60°C -40°C + 60°C -40°C + 60°C
Bending radii One-time bending Repeated bending	 ≥ 75 mm ≥ 150 mm	 ≥ 75 mm ≥ 150 mm	 ≥ 75 mm ≥ 150 mm	 ≥ 75 mm ≥ 150 mm	 ≥ 80 mm ≥ 150 mm
Max. tensile load	100 N	100 N	100 N	100 N	100 N
Weight approx.	76 kg/km	67 kg/km	67 kg/km	73 kg/km	117 kg/km
Halogen free	no	yes	no	no	no
Behavior in fire	flame-retardant according to VDE 0472 T804 test type C	flame-retardant according to VDE 0472 T804 test type C	flammable	flame-retardant according to VDE 0472 T804 test type B	flammable
Oil resistance	Conditionally resistant to mineral oil and greases	Conditionally resistant to mineral oil and greases	Conditionally resistant to mineral oil and greases	good resistance to mineral oil and greases	Conditionally resistant to mineral oil and greases

Tabla 6.
Comparativa cables PROFIBUS eléctrico [26].

Para el conexionado de estos cables a las ET200M y puertos DB9 de las OLM, al igual que para el acoplador DP/PA, se emplean conectores *FastConnect Bus Connector* que básicamente son conectores DB9 con grado de protección IP20, de fácil instalación en los cables seleccionados mediante sistema FastConnect (FC) desarrollado por SIEMENS, para una conexión rápida de cables PROFIBUS que incluyan la etiqueta FC como los de la Tabla 6.

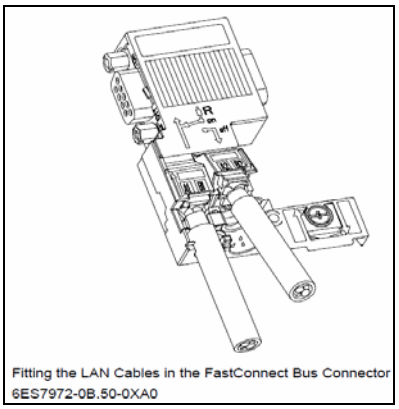


Figura 47.
FastConnect Bus Connector [26].

La definición de los pines del conector FastConnect Bus Connector es la siguiente:

Pin no.	Signal name	Meaning
1	-	-
2	-	-
3	RxD/TxD-P	Data line B
4	-	-
5	M5V2	Data reference potential (from station)
6	P5V2	Power supply plus (from station)
7	-	-
8	RxD/TxD-N	Data line A
9	-	-

Figura 48.
Definición de pines FastConnect Bus Connector [26].

En cambio para conectar los cables RS-485 a las válvulas de control (MOV) se emplean conectares M12 como los mostrados en la Figura 49.

Figura 49.
Conector M12 para MOVs [26].

b) Redes ópticas: para confeccionar estas redes se puede emplear cables de fibra óptica de cristal, plástico o PFC. La diferencia entre un tipo u otro radica en las longitudes del tramo de cable que se pueden alcanzar: con fibra óptica de plástico hasta máximo de 80 metros. Con los cables tipo PFC hasta un máximo de 400 metros, mientra que con fibra óptica de cristal se pueden alcanzar distancias máximas de Kms.

Las características de los cables para este tipo de redes son [26]:

- Insensible a la influencia de interferencias electromagnéticas (EMV).
- Adecuado para cubrir ampliadas distancias.
- Separación galvánica.
- Existe la posibilidad de realizar configuraciones mixtas entre ópticas y eléctricas mediante el uso de OLM.

Este tipo de cable se emplea en la red de comunicaciones de la planta estándar, para realizar el anillo de Fibra Óptica que conecta todos los segmentos de las redes de proceso y los PLCs de los sistemas paquete de la red de célula. El cable seleccionado es el SIEMENS SIMATIC NET FIBER-OPTIC 6XV1820-5AH10 con las siguientes características técnicas [28]:

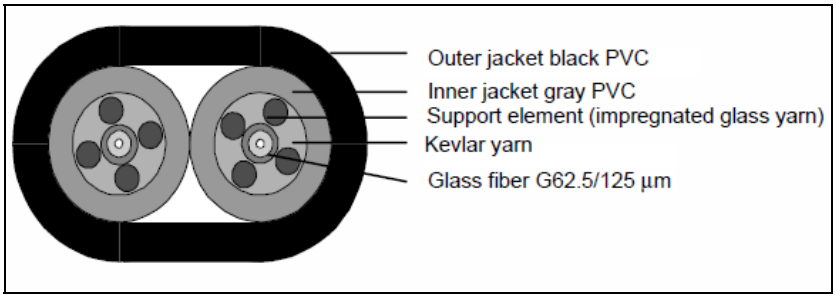


Figura 50.
Estructura cable estándar de fibra de vidrio [28].

- Para uso en interior y exterior.
- Retardante de llama de acuerdo a IEC 60332-3 cat CF.
- No es libre de halógenos.
- Para longitudes máximas de 4000 metros.
- Tipo de fibra multimodo (62.5/125µm).
- Numero de fibras: 2.
- Dimensiones interiores: (3.5 ± 0.2) mm Φ.
- Dimensiones exteriores: (6.3 x 9.8)± 0.4 mm.
- Peso approx. 74 kg/km.
- Temperatura ambiente: -5°C to +50°C
- Temperatura de operación: -25°C to +60°C

Para conectar los cables de fibra óptica a módulos OLM se emplean conectores tipo BFOC para cables de fibra de vidrio, como los de la siguiente Figura 51:

BFOC Connectors for Glass Fiber-Optic Cables

In PROFIBUS, only BFOC connectors are used for glass fiber-optic cables.

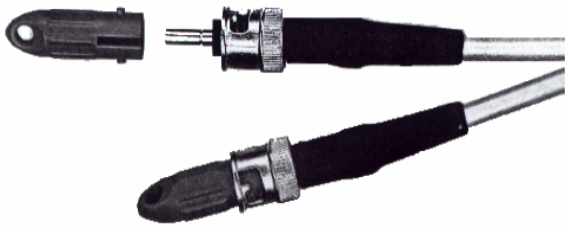


Figura 51.
Conector para fibra de vidrio [28].

Por último, es importante tener en cuanta que la longitud del tramo de cable del segmento influye completamente en la velocidad de transmisión de los datos. En la siguiente Figura 52, se muestra las longitudes máximas recomendadas por el fabricante SIEMENS para las diferentes velocidades de comunicación de PROFIBUS:

Transmission Rate in Kbps	Segment Length for Cable Type	
	– FC Standard Cable – FC Robust Cable – FC FRNC Cable – FC Food Cable – FC Underground Cable – SIENOPYR–FR Marine Cable	– FC Trailing Cable – PROFIBUS Flexible Cable – PROFIBUS Festoon Cable
9.6	1000 m	900 m
19.2	1000 m	900 m
45.45	1000 m	900 m
93.75	1000 m	900 m
187.5	1000 m	700 m
500	400 m	400 m

Figura 52.
Comparativa velocidad Vs tipo de cable PROFIBUS [24].

7.6.1.7 Interconexión de segmentos y conexión de la red de campo con nivel superior.

Una vez que está definida la red de proceso y todos sus componentes de red que conforman su infraestructura, es necesario conectarla a los procesadores del sistema de control (MARK VIe). Para ello lo que se realiza es conectar los anillos de Fibra Óptica de las diferentes redes de proceso asociadas a un mismo procesador, y cerrar el anillo mediante un tarjeta CP 5614 FO instalada en un slot PCI del propio procesador, según se muestra en el Anexo 2.

7.6.1.8 Consumos máximos de elementos por segmento.

Es muy importante a la hora de dimensionar un segmento de versión PROFIBUS-PA, tener en cuenta los consumos de los dispositivos que lo conforman, así como las velocidades de transmisión que se van a utilizar, ya que estos parámetros son críticos para definir la longitud máxima admitida para el segmento (velocidad) y además para definir el número máximo de dispositivos admitido por un segmento (consumo).

Por tanto, primeramente de acuerdo a los datos técnicos de consumos de los elementos del segmento PROFIBUS-PA (MOV y terminador de bus) se va a calcular el número máximo de dispositivos que admite un segmento alimentado desde el mismo acoplador DP/PA.

Datos técnicos elementos segmento PROFIBUS-PA:

Acoplador DP/PA [33].
(Versión atmósfera no explosiva).

Tensión salida acoplador:	31 VDC
Intensidad max.salida:	1000mA

Válvulas motorizadas MOV:

Tensión de alimentación:	De 9 a 32 VDC
Consumo máximo:	$\leq$ 1 Watio (aprox. 32mA).

Terminador de bus [31]:

Tensión nominal:	24 VDC
Intensidad máxima:	25 mA

Por tanto, aplicando el consumo más desfavorable que es 32mA de la válvula motorizada el número máximo de dispositivos por segmento será:

$$\text{Nº máximo dispositivos PA por segmento} = \frac{\text{Intensidad a la salida del acoplador (mA)}}{\text{Consumo más desfavorable dispositivo PA (mA)}} = \frac{1000}{32} = 31 \text{ dispositivos}$$

Una vez obtenido que el número máximo de dispositivos por segmento PROFIBUS-PA es 31, comprobamos que se está cumpliendo este requisito en los segmentos definidos anteriormente. El caso más desfavorable que tenemos es el correspondiente al segmento 11CSA11-1 que contiene 15 MOV más el elemento terminador de bus (en total 16 dispositivos), y por tanto cumple la restricción de número de dispositivos máximos por segmento.

Además como es importante calcular la longitud máxima del tramo de cable del segmento PROFIBUS-PA, que es función del número máximo de dispositivos por segmento, a continuación se calcula la longitud de cable referida al número máximo de dispositivos PA por segmento:

$$\text{Long. cable por segmento(km)} = \frac{\text{Tensión salida acoplador (V)} - \text{Tensión alim. min. dispositivo PA (V)}}{\Sigma\text{consumo dispositivos PA (A)} \times \text{resistencia de línea } (\Omega/\text{km})}$$

$$\text{Long. cable por segmento(km)} = \frac{(31-9)\text{ V}}{\frac{[(15\times32)+25]}{1000}\text{ (A)} \times 110\,(\Omega/\text{km})} = 0{,}396 \text{ km}$$

Por tanto, la longitud máxima del segmento PROFIBUS-PA con cable tipo FC para red eléctrica RS-485, en el caso más desfavorable del segmento 11CSA11-1, debería ser 396 metros. Según la ubicación de las cabinas centralizadoras mostrada en el Anexo 03 dicha longitud no es superada, ya que la distancia entre la cabina CSA11 y la turbina de vapor es muy inferior como se puede comprobar.

7.6.2 Diseño de la red de célula.

Las redes de célula que conforman los PLCs de sistemas paquete definidos en la Planta estándar tienen que conectarse a la red de comunicaciones de la planta mediante bus, para poder proporcionar la información del proceso que controlan.

Por tanto, lo que se requiere al sistema de control de estos sistemas paquete es un PLC que sea capaz de conectarse mediante PROFIBUS DP (eléctrico) a un módulo OLM asociado, y de este modo conectarlos al anillo de Fibra Óptica redundante de la red de proceso, de forma idéntica a lo definido en el punto 7.6.1.5. Lo recomendable sería utilizar un PLC Simatic S7 de SIEMENS, que facilitaría la configuración del bus así como ser totalmente compatible con los módulos OLM.

7.6.3 Diseño de la red de control/supervisión.

Para el diseño de esta red de comunicación se va a utilizar un bus basado en ETHERNET, para aprovechar las características que proporciona la capa de Ethernet, y entre ellas la velocidad casi en tiempo real de Mbps.

Para la especificación PROFIBUS, el bus basado en Ethernet es PROFINET y será el bus que vamos a utilizar para la comunicación de la red de control/supervisión, así como las situadas en el nivel superior y que corresponde a la red de factoría.

PROFINET admite varias tecnologías que, utilizándose de forma combinada, aumentan el rendimiento de la red unas 50 veces e incluso más en comparación con la tecnología original de 10 Mbits/s. Estas tecnologías son [27]:

- Fast Ethernet con 100 Mbits/s: En comparación con Ethernet, los telegramas se transportan a 10 Mbits/s, una velocidad considerablemente superior, por lo cual ocupan el bus sólo durante muy poco tiempo.

- Gigabit Ethernet con 1 Gbit/s: Frente a Fast Ethernet, Gigabit Ethernet es aún más rápido en el factor 10; la ocupación del bus se reduce a 1/10 del tiempo.

- Full Duplex excluye el riesgo de colisiones: el volumen de transmisión de datos aumenta enormemente, dado que se evitan las usuales repeticiones de telegramas. Entre dos estaciones se puede transmitir y recibir datos de forma simultánea. El volumen de transmisión de datos de una comunicación Full Duplex aumenta así a 200 Mbits/s con Fast Ethernet y a 2 Gbits/s con Gigabit Ethernet.

- Switching posibilita la comunicación paralela: la división de una red en varios segmentos mediante un switch o la conexión de estaciones individuales directamente a un switch permiten desacoplar las cargas. En cada segmento es posible intercambio de datos local, independiente de otros segmentos. En consecuencia pueden circular por la red global varios telegramas a la vez. Por lo tanto, el aumento de rendimiento radica en la simultaneidad de varios telegramas.

- Autocrossover: permite el cruce automático de las líneas de transmisión y de recepción en puertos de par trenzado • Autosensing describe la característica de nodos de red (equipos terminales y componentes de red) que detectan automáticamente la velocidad de transferencia de una señal (10 Mbits/s, 100 Mbits/s ó 1 Gbit/s) y soportan la función de Autonegotiation.

- Autonegotiation: es un protocolo de configuración en Fast Ethernet. Los dispositivos en la red acuerdan antes de la verdadera transferencia de datos un modo de

transferencia, el cual controla cualquier dispositivo participante (100 Mbits o 10 Mbits/s, full dúplex o semidúplex)

- Sistema de cableado Gigabit: El sistema de cableado FastConnect de 8 hilos de SIMATIC NET permite velocidades de transferencia de hasta 1 Gbit/s.

7.6.3.1 Topología empleada.

PROFINET admite cualquier tipo de topologías de red (estrella, árbol, anillo, …). Concretamente para la red de control/supervisión de la Planta Estándar de Ciclo Combinado se elige una topología mixta con la siguiente configuración:

a) Doble anillo de alta velocidad: se utiliza para conectar los dispositivos situados en diferentes áreas o localizaciones, de modo que se situará un switch de cada área que permita la conexión de los equipos de la misma localización, y entre todas las zonas se establece el anillo redundante. De este modo el uso de un segundo anillo redundante, conectando los mismos dispositivos, incrementa la fiabilidad y flexibilidad de la red, ya que si aparece un problema de comunicación por fallo en un anillo o una ruptura del cable, automáticamente se reconfigura el anillo y continúa la transmisión evitando la interrupción de la comunicación.

b) Conexión en estrella: esta conexión según lo comentado anteriormente se realizará desde cada equipo hasta el switch de red situado en su zona.

Gráficamente lo comentado es:

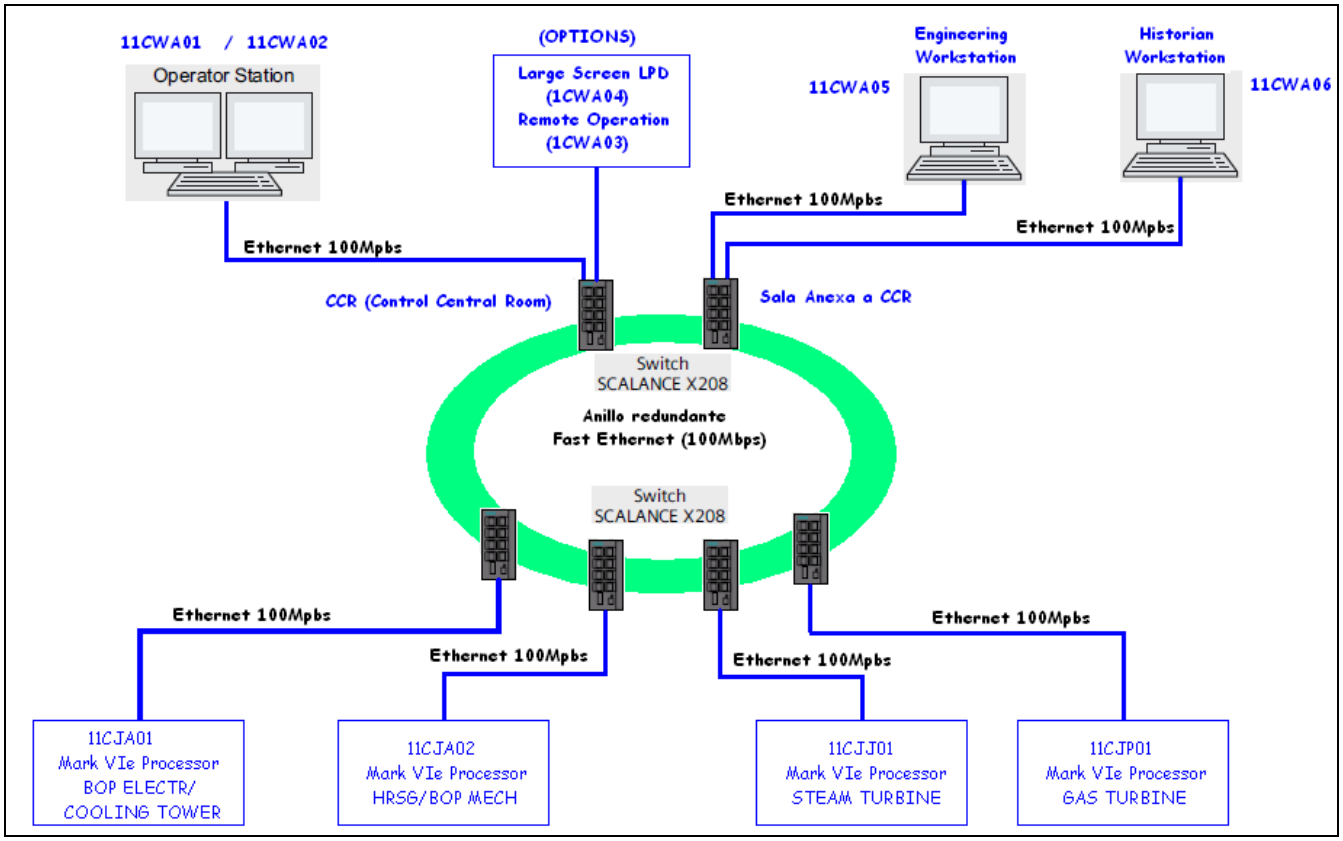


Figura 53.
Topología Red control/supervisión.

7.6.3.2 Elementos de conexión a red.

PROFINET admite cualquier tipo de topologías de red (estrella, árbol, anillo, …). Concretamente para la red de control/supervisión de la Planta Estándar de Ciclo Combinado se elige una topología mixta con la siguiente configuración:

a) Procesadores MARK VIe: para la conexión a la red Ethernet de control, se emplearán tarjetas CP1616 para conexión a puerto PCI del procesador. Para el correcto funcionamiento de la tarjeta comentada serán necesarios drivers y software de control. La definición de los elementos necesarios es la siguiente:

- **CP 1616:** Tarjeta PCI para conectar PG/PC a Industrial Ethernet con ASIC ERTEC 400 y switch de 4 puertos de tiempo real integrado. Utilización como IO Controller y como IO Device.
- **Development Kit DK-16xx PN IO:** Software Development Kit para CP 1616 y CP 1604 con driver LINUX como código fuente para la migración a sistemas operativos basados en PC.
- **SOFTNET PN IO:** Software de comunicaciones para el funcionamiento de un PC/estación de trabajo como IO Controller.

Figura 54.
Tarjeta CP1616 para PCI [26].

b) Puestos de supervisión/control: para la conexión a la red Ethernet de control de cualquier puesto de supervisión/control (11CWA01, 11CWA02, 11CWA03…) también se emplearán tarjetas CP1616 para conexión a puerto PCI del PC, con sus correspondientes drivers y software de control de igual modo que los procesadores MARK VIe del sistema de control.

c) Switches de conexión a red de control/supervisión: se emplean switches industriales Ethernet y el modelo seleccionado es el SCALANCE X-200 managed, de uso universal desde aplicaciones a pie de máquina hasta secciones de instalación interconectadas. Los equipos ofrecen alto grado de protección, lo que permite instalarlos sin necesidad de armario eléctrico.

Figura 55.
Gama switches SCALANCE X-200 [26].

Más concretamente se va a utilizar el switch SCALANCE X208 / SCALANCE X208PRO (grado de protección IP65) que tiene las siguientes características [27]:

- Para la construcción de Industrial Ethernet en topología en línea, estrella o anillo (8 puertos eléctricos): SCALANCE X208 para el montaje en el armario eléctrico y SCALANCE X208PRO especialmente para el uso fuera del armario eléctrico.
- Diagnóstico del equipo mediante LEDs (Power, estado del link, tráfico de datos).
- Diagnóstico remoto por contacto de señalización (con SCALANCE X208: máscara de señalización ajustable localmente con pulsador), PROFINET, SNMP y navegador Web.
- Aptos para la industria, los ocho conectores RJ45 del SCALANCE X208 están fabricados con collares de retención para fijar los conectores IE FC RJ45 Plug 180.
- Los ocho conectores M12 conformes con PROFINET del SCALANCE X208PRO están fabricados en grado de protección IP65, para la conexión del IE M12 Plug PRO o del cable IE M12 Connecting Cable ya conectorizado.
- El SCALANCE X208PRO puede fijarse sobre un perfil DIN/S7-300 o, ahorrando espacio, directamente en la instalación o máquina, tanto tumbado como de pie; la banda de LEDs oblicua permite leer la información de estado con independencia de la posición de montaje.
- Fuera del armario eléctrico, el SCALANCE X208PRO puede alimentarse con la fuente PS791-1PRO también con 230 V AC.

Con este tipo de switch a la hora de configurar la red deben respetarse las condiciones siguientes [27]:

- **Longitud de cable de par trenzado entre dos switches SCALANCE X:**
  - máx. 100 m con cable IE FC y conector IE FC RJ45 Plug 180 ó IE M12 Plug PRO.
  - máx. 10 m con latigillos TP Cord.

- **Longitud de los cables ópticos:**
  - máx. 3000 m con FO de vidrio Industrial Ethernet (multimodo).
  - máx. 26000 m con FO de vidrio Industrial Ethernet (monomodo).

- **Dirección IP:** La dirección IP se asigna a través del DHCP (Dynamic Host Configuration Protocol). Si en la red no está disponible ningún servidor, entonces la dirección IP se puede asignar con una herramienta software facilitada por el fabricante. La configuración de equipos y de tiempo real de los switches SCALANCE X-200IRT se realiza con STEP 7.

Una vez que ya tenemos todos los elementos de la red de control/supervisión conectados a la misma, ya es posible visualizar los datos de campo en las estaciones de supervisión y control. Para ello será necesaria la instalación de un servidor OPC, que proporcione al Sistema de Control una interfaz estandarizada de intercambio de datos para leer la información del bus. Además, este servidor OPC permite al Sistema de Control de la Planta Estándar, definido y programado por GE©, obtener la información mediante la modificación "sencilla" del software mediante compiladores habitualmente usados en el desarrollo de aplicaciones para la industria como son Microsoft Visual C++/.NET, Visual Basic,…

7.6.3.3 Interfaz de comunicación del Sistema de Control/Bus mediante OPC.

Como se ha comentado anteriormente, para poder visualizar los datos de proceso desde cualquier estación de supervisión/control es necesario tener un servidor OPC (OLE for Process Control), para ser utilizado como interfaz estándar de comunicación entre el bus y el software del Sistema de Control.

El principio básico de OPC es que las aplicaciones cliente OPC, se comunican con el servidor OPC por una interfaz estandarizada/abierta y, en consecuencia, no propietaria. Los clientes OPC, para conectar con el servidor OPC, pueden emplear aplicaciones Windows aptas para OPC ya disponibles en el mercado (Microsoft-Office o sistemas HMI).

Para PROFIBUS están disponibles los siguientes accesos de comunicación vía OPC [27]:

- Comunicación DP para PROFIBUS DP.
- DP-V0 maestro clase 1 y maestro clase 2.
- DP-V1 maestro clase 1 y maestro clase 2.
- Interfaz PROFIdrive V3 para servidores de perfil.
- Comunicación FMS para PROFIBUS FMS.
- Comunicación S7.
- Comunicación compatible con S5 (SEND/RECEIVE) sobre la base de la interfaz FDL.
- Los servidores OPC ofrecen:
  - Interfaz Data Access 2.05
  - Interfaz Alarm&Event 1.1
  - Interfaz OPC XML-DA 1.0
  - Homogeneidad entre productos de automatización de distintos fabricantes.

- Interfaz de usuario idéntica de fácil manejo para distintos componentes.
- Accesible desde cualquier ordenador en la LAN.
- Acceso de datos de alto rendimiento a través de Custom Interface (C++, .NET).
- Fácil de uso por la "Automation Interface" (VB, .NET) o el OCX Data Control adjunto.
- Agrupación de variables (items) para procesar gran volumen de datos en poco tiempo.
- Otros compiladores pueden usarse a través del servidor OPC; sin embargo, el compilador tiene que soportar la interfaz COM (modelo de componentes de Microsoft).

▪ Funciones:

- Estandarización abierta del direccionamiento a través de nombres lógicos para objetos de un componente o sistema de automatización.
- Soporta los símbolos de STEP 7.
- Intercambio de datos eficiente de un componente de proceso con una aplicación postprocesadora.
- Uso simultáneo de varios servidores por parte de una aplicación de cliente.
- Posibilidad de ejecución de varios clientes en un servidor OPC.
- Posibilidad de uso paralelo de los protocolos de comunicación.

▪ Interfaces:

- "Custom Interface" para aplicaciones C++/.NET de altorendimiento.
- "Automation Interface" para aplicaciones Visual Basic o comparables de fácil creación.
- OCX Data Control conexión sencilla a aplicaciones Windows que soportan COM/DCOM.
- XML-DA-Interface; esta función permite el acceso de datos a CPUs S7 por Internet.

▪ Configuración:

- La configuración completa de los parámetros de comunicación se realiza con las herramientas del software instalado Advanced PC Configuration (consola de configuración, SIMATIC NCM PC o STEP 7, V5.1 + SP2 o superior).

Por tanto, en cada uno de los Procesadores de control MARK VIe con lo que se equipa la Planta Estándar, se instala el servidor OPC para que de este modo toda la información del proceso incorporada a las redes de comunicación PROFIBUS, esté disponible en un interfaz conocido y abierto. Así el Sistema de Control puede leer la información mediante funciones software como si fueran entradas/salidas, y de este mdoo realizar el control de la planta o la visualización en los diferentes puestos de supervisión y control de la información de proceso.

Por tanto, gracias al servidor OPC la infraestructura de comunicaciones que se ha establecido mediante redes de comunicación para la Planta Estándar de Ciclo Combinado, tiene la ventaja que es fácil de implantar junto con el Sistema de Control ya diseñado por GE©, ya que el software de control sólo tendrá que implementar en su código, usando funciones estándar dadas por del fabricante del servidor OPC, la lectura de las variables de memoria donde se almacenan los datos de procesos deseados. De este modo el servidor OPC permite que el diseño del software del Sistema de Control sea totalmente independiente de la tecnología del bus de campo utilizada.

Para la Planta Estándar de Ciclo Combinado se puede establecer como servidor OPC adecuado, la versión de producto **OPC-Server DP-5613 para PROFIBUS DP de SIEMENS**.

7.6.3.4 Cableado Ethernet.

La restricción más importante en las redes Ethernet de la Planta estándar (red de control y red de factoría), la encontramos en la longitud de cable de par trenzado entre los switches SCALANCE X, que se deberá respetar en la instalación definitiva:

- Máx. 100 m con cable IE FC y conector IE FC RJ45 Plug 180 ó IE M12 Plug PRO.
- Máx. 10 m con latigillos TP Cord.

De acuerdo a la topología de red de control/supersión definida anteriormente los switches SCALANCE X-208 que hay y sus ubicaciones son la siguientes:

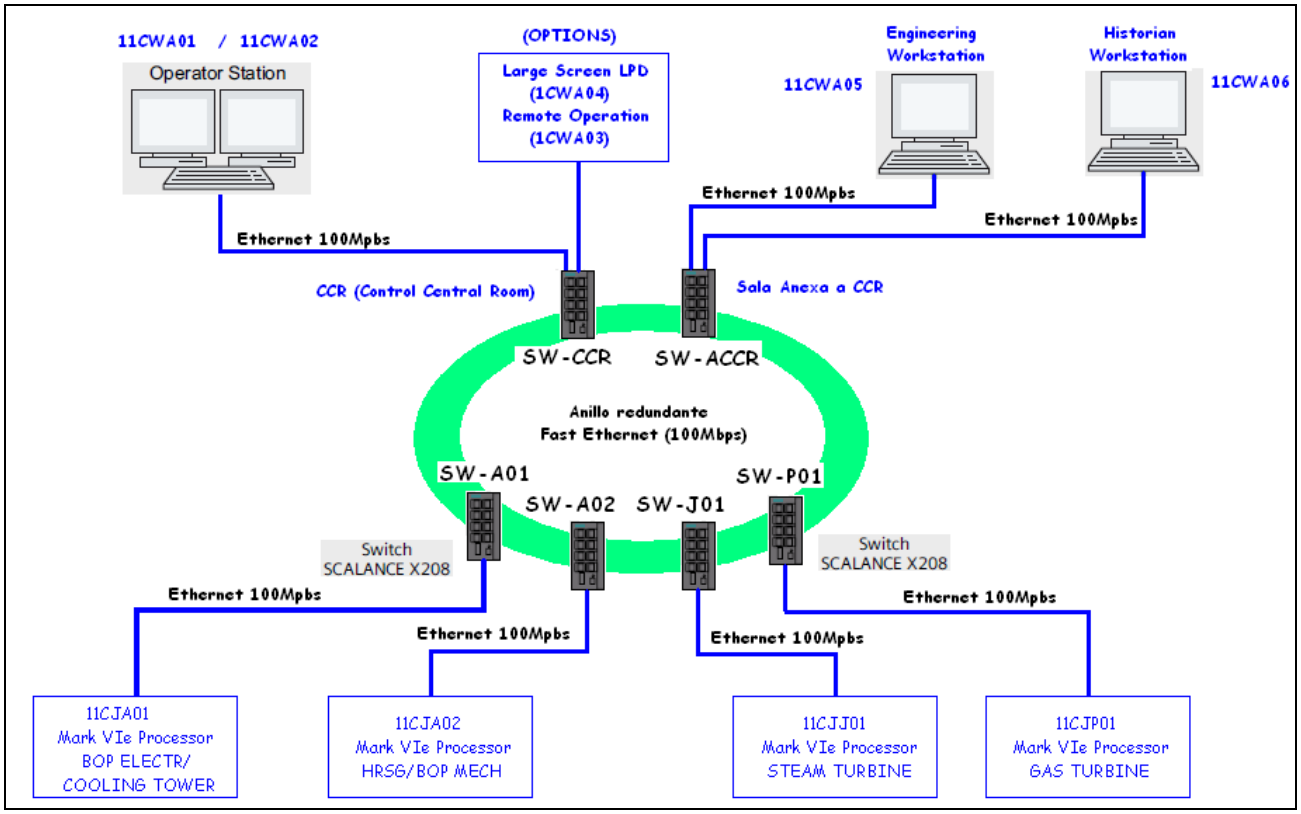


Figura 56.
Switches SCALANCE X-200 red control/supervisión.

SW-A01: switch que conecta el procesador MARK VIe 11CJA01 a la red de control/supervisión, y su instalación se realiza en la misma cabina que él.

SW-A02: switch que conecta el procesador MARK VIe 11CJA02 a la red de control/supervisión, y su instalación se realiza en la misma cabina que él.

SW-J01: switch que conecta el procesador MARK VIe 11CJJ01 a la red de control/supervisión, y su instalación se realiza en la misma cabina que él.

SW-P01: switch que conecta el procesador MARK VIe 11CJP01 a la red de control/supervisión, y su instalación se realiza en la misma cabina que él.

SW-CCR: switch que conecta los puestos de supervisión/control situados en la Sala de Control (puestos de operadores) a la red de control/supervisión, y su instalación se realiza en la mesa del Jefe de Turno.

SW-ACCR: switch que conecta los puestos de supervisión/control situados en la Sala de Control, a la red de control/supervisión y su instalación se realiza dicha sala en cabina o sobremesa.

a) Tipo de cable: el tipo de cable empleado para implementar el anillo redundantes Ethernet, es un **cable tipo IE FC TP 2x2** que conecta los switches mediante conexión doble en anillo para hacerlo redundante según se muestra en la Figura 57. Las características de este tipo de cable son [27]:

- Fácil pelado con la herramienta FastConnect Stripping que permite recortar la cubierta exterior y la malla de pantalla a la medida exacta en una sola operación.
- En los productos FastConnect la conexión es por desplazamiento del aislamiento.
- Supera la categoría 5 (Cat5e) de las normas de cableado internacionales ISO/IEC 11801 y EN 50173.
- Conforme con PROFINET.
- Homologación UL.
- Distintas variantes para diversos campos de aplicación:
  - IE FC TP Standard Cable GP.
  - IE FC TP Flexible Cable GP.
  - IE FC TP FRNC Cable GP.
  - IE FC TP Trailing Cable GP.
  - IE FC TP Trailing Cable.
  - IE TP Torsion Cable.
  - IE FC TP Marine Cable.
- Alta inmunidad contra perturbaciones gracias al apantallamiento doble.
- Determinación fácil de la longitud por marcas impresas cada metro.

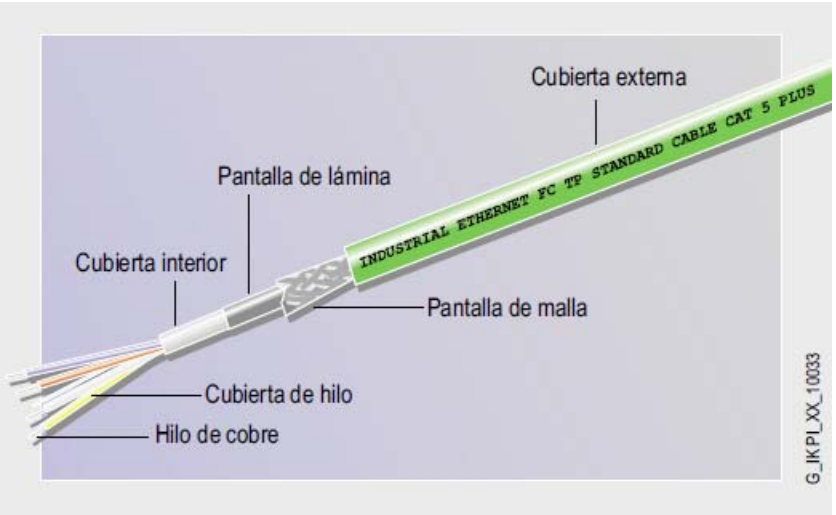


Figura 57.
Cable IE FC TP 2x2 [27].

De las variantes del tipo de cable IE FC TP, el empleado para cablear redes Ethernet de la Planta Estándar de Ciclo Combinado es el **IE FC TP FRNC Cable GP 22**, que es un cable flexible libre de halógenos para aplicación en edificios (FRNC= Flame Retardent Non Corrosive) y cuatro hilos (flexible) cableado en cuarteto para movimientos ocasionales.

b) Tipo de conectores: para conectar el tipo de cable empleado IE FC TP a los switches y tarjetas PCI de los procesadores, se utiliza un conector IE FC RJ45 Plug 180. Hay que tener en cuenta que este tipo de conector tiene limitaciones de distancias máximas del tramo de cable que conectar, la cuál no superará los 100 metros. Por tanto, si al conectar los switches según se muestra en la Figura 57, algún tramo tiene una distancia mayor a 100 metros, se tendrá que hacer un anillo de Fibra Óptica en lugar del anillo Fast Ethernet. Esto también implicará la sustitución de los switches SCALANCE X-208 de Ethernet por switches SCALANCE X-20,4 que permiten topologías en línea o en anillo con 2 puertos ópticos y 4 puertos eléctricos (RJ-45).

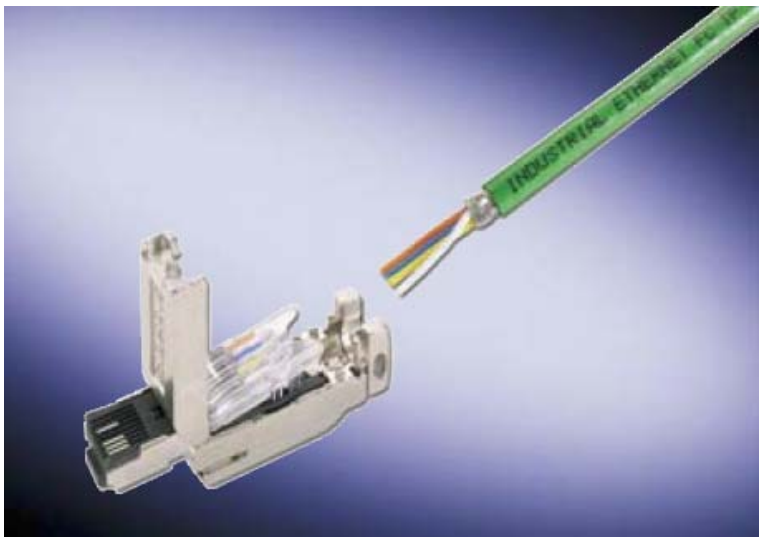


Figura 58.
Conector IE FC RJ45 Plug 180 [27].

Las características de este tipo de conector son [27]:

- Permite implementar conexiones directas entre equipos salvando hasta 100 metros usando cable Industrial Ethernet FC 2 x 2 sin necesidad de latigillos.
- Conexión simple (contactos de desplazamiento de aislamiento) para cables de par trenzado de 4 hilos (100 Mbits/s) sin necesidad de herramientas especiales.
- Sistema de conexión que evita errores gracias a zona de conexionado visible así como contactos de desplazamiento de aislamiento codificados por colores.
- Diseño apto para ambiente industrial (robusta caja metálica, ausencia de piezas perdibles).
- Alta compatibilidad electromagnética (caja metálica).
- Elemento de alivio de tracción para cables.
- Compatible con la norma EN 50173 (RJ45) / ISO IEC 11801.
- Posibilidad de alivio de tracción y de flexión adicional de la unión por conector por enganche de conector en la caja del aparato, p.ej. con SCALANCE X, SCALANCE S, ET 200S.

7.6.4 Diseño de la red de factoría.

Para el diseño de esta red de comunicación se va a utilizar un bus basado en ETHERNET, para aprovechar las características que proporciona la capa de Ethernet, y entre ellas la velocidad casi en tiempo real de Mbps.

Como la implementación de esta red de factoría tiene como objetivo compartir la información del proceso productivo que permita supervisar a los diversos departamentos de la compañía la evolución o estado del proceso productivo, se establece como tecnológia de comunicación el establecimiento de una red LAN típica.

7.6.4.1 Topología empleada.

La topología en estrella es la elegida para esta red de factoría, ya que los equipos de esta red se conectan directamente entre sí mediante el empleo de switches y tarjetas de red LAN adecuadas.

7.6.4.2 Elementos de conexión a red.

Para la conexión de todos los elementos de esta red se utilizan tarjetas de red LAN, así como switches para interconexión de equipos y router de comunicaciones para conexiones externas a la red.

Todos los elementos para interconexión de los diferentes equipos que conforman esta red, serán para montaje en rack de 19” de una cabina armario rack profesional de redes y servidores, similar al mostrado en la Figura 59. Este armario se instalará en la Sala de Control Central (CCR), y por tanto todos los elementos de esta red se conectarán a los switches instalados en este armario, mediante cable Ethernet **IE FC TP FRNC Cable GP 22** con sus conectores RJ45 correspondentes.

Figura 59.
Ejemplo de Armario rack 19" para 42U.

Como en esta red de factoría hay equipos que hacen conexiones hacia el exterior, será fundamental establecer las correspondientes medidas de Ciberseguridad que eviten posibles ataques cibernéticos que puedan dañar la planta. Lo habitual es que este tipo de servidores sólo permitan la "salida" de datos al exterior y nunca admitan el envío de datos desde el exterior hacia el interior de la red de planta.

Por tanto, la arquitectura general para los equipos que componen la red de factoría se define del siguiente modo:

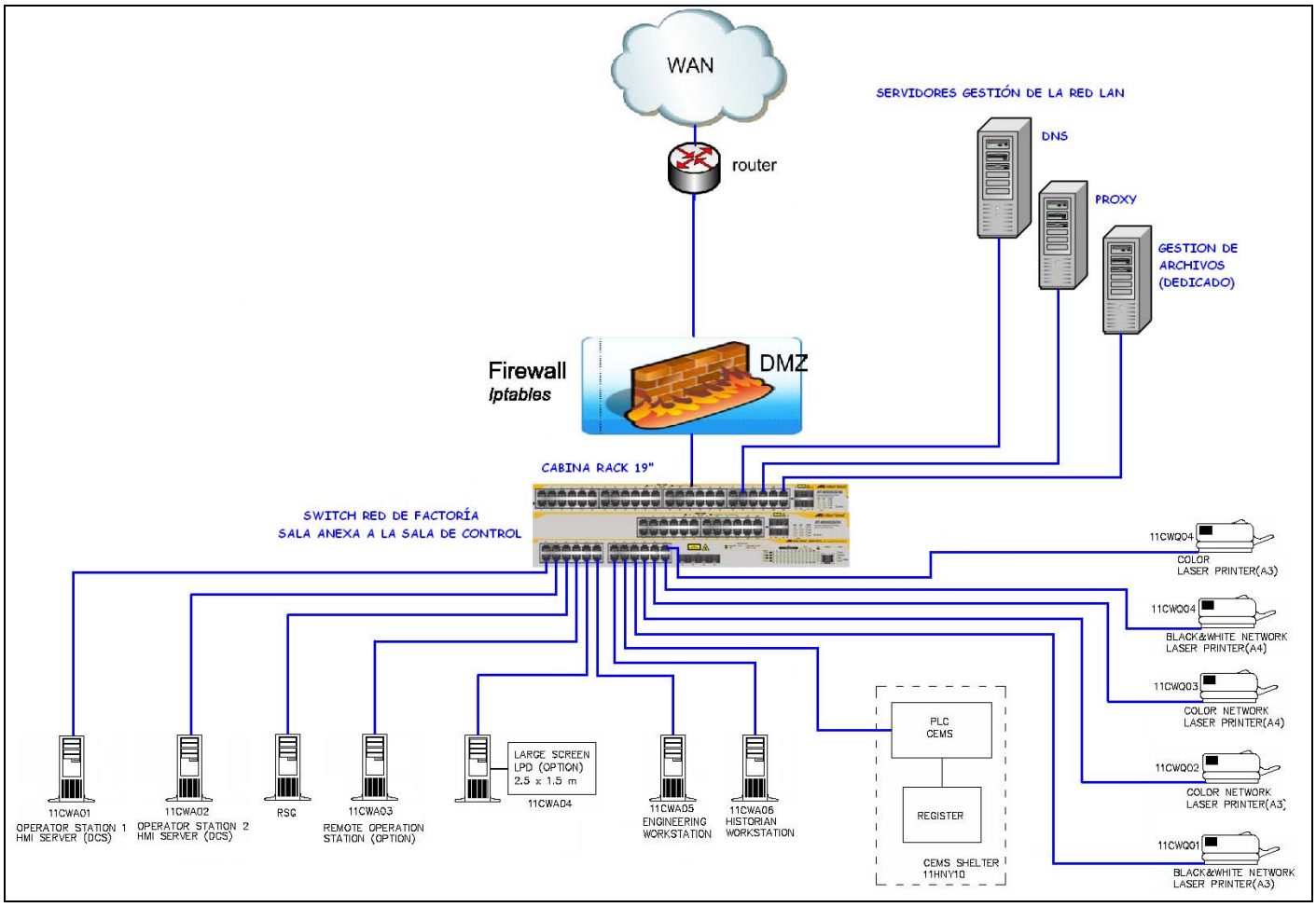


Figura 60.
Arquitectura general red de factoría.

Donde los diferentes servidores tienen las siguientes misiones:

Servidor DMZ: La intención de este servidor es asegurar que desde servidores externos a nuestra red, no se puedan comunicar con otros segmentos de la red interna. Un firewall es muy relevante en la implementación de DMZ, ya que es responsable de garantizar que las políticas adecuadas para proteger a las redes locales de DMZ se encuentren habilitadas, mientras que se mantiene la accesibilidad a la zona desmilitarizada (DMZ).

Servidor PROXY: actúa de intermediario entre un explorador web (como Internet Explorer) e Internet, y además de mejorar el rendimiento en Internet almacenando una copia de las páginas web más utilizadas, tiene funciones de seguridad filtrando algunos contenidos web y software malintencionado.

Servidor gestión archivos: Para permitir alojar páginas web o realizar venta de alojamientos web, es necesario instalar diversos programas o componentes del propio sistema operativo, para la gestión de DNS, gestión de archivos, asignación de usuarios y de permisos.

Servidor DNS: es un servidor que permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio. Las entradas existentes en nuestro DNS no serán visibles en Internet, solamente servirán a los equipos de nuestra red local. De esta forma, cuando un usuario de nuestra red intente acceder a un recurso local, podrá utilizar nombres en lugar de direcciones IP. Si el usuario desea acceder fuera de nuestra red local a algún recurso en Internet, el DNS local nunca podrá llevar a cabo dicha resolución y se la traslada al siguiente servidor DNS (que sí estará en Internet) en su jerarquía de servidores DNS, hasta que la petición sea satisfecha.

7.6.5 Configuración del sistema y tipos de dispositivos.

La descripción de la configuración del sistema consiste en el número de estaciones, la asignación entre la dirección de la estación y las direcciones de las entradas/salidas, el formato de los datos de entrada/salida, el formato de los mensajes de diagnóstico y los parámetros del bus usados.

Cada sistema PROFIBUS DP puede contener 3 tipos diferentes de dispositivos:

- DP Maestro Clase 1 (DPM1): es el controlador central que intercambia información con las estaciones descentralizadas (DP esclavos) con un ciclo de mensaje específico. Los dispositivos típicos controladores de la Planta Estándar son los procesadores MARK VIe.

- DP Maestro Clase 2 (DPM2): Son programadores, dispositivos de configuración y operadores. Se usan para la identificación de la configuración del sistema DP o para el funcionamiento y supervisión de operaciones. Este tipo de dispositivos corresponden a las estaciones de supervisión/control CWAxx situadas en la Sala de Control.

- DP esclavo: Es un dispositivo periférico (entradas/salidas, válvulas, etc.) que recoge información de entrada y/o manda información de salida. Estos dispositivos son todos los dispositivos de campo con los que se equipa la Planta Estándar de Ciclo Combinado.

Como la topología lógica de la red de comunicaciones de la Planta Estándar de Ciclo Combinado es la correspondiente a un sistema mono-maestro, sólo se encuentra activo un maestro en el bus durante la fase de operación, siendo el procesador MARK VIe. Los DP

esclavos correspondientes a los dispositivos de campo, son enlazados mediante el bus. Estos sistemas presentan el tiempo de ciclo más corto.

El comportamiento del sistema es determinado principalmente por el estado de los procesadores de control MARK VIe (DPM1), y podemos encontrar 3 estados principales:

- Stop: No se produce ningún tipo de transmisión entre procesador de control MARK VIe y los dispositivos de campo.
- Clear: el procesador de control MARK VIe lee la información de entrada de los dispositivos de campo y mantiene las salidas en estado de espera (seguridad).
- Operate: el procesador de control MARK VIe se encuentra en la fase de transferencia de datos. En una comunicación cíclica, se leen las entradas de los dispositivos de campo y se escribe la información de salida en éstos.

El procesador de control MARK VIe envía de forma cíclica su estado a todos los dispostivos de campo que tiene asignados mediante un comando Multicast a intervalos de tiempo configurables. La reacción del sistema a un error durante la fase de transferencia de datos del MARK VIe (p. ej. error en un sensor) se determina por un parámetro de configuración "autoborrado". Si este parámetro pasa a un estado true (verdadero), el MARK VIe pone todas las salidas de sus dispositivos de campo asignados a un estado de espera (seguridad) hasta que se cumplan de nuevo todas las condiciones para una transmisión correcta.

La transmisión de datos entre los procesadores de control y sus dispositivos asignados es ejecutada de forma automática por MARK VIe en un orden definido. Al configurar el sistema del bus, el usuario especifica la asignación de un dispositivo a un procesador de control MARK VIe y cuales de estos dispositivos esclavos se incluirán o se excluirán de la transmisión de datos de usuario. La transmisión de datos de usuario entre procesador y dispositivo se divide en 3 fases:

- Parametrización.
- Configuración.
- Transferencia de datos.

Durante las fases de parametrización y configuración cada dispositivo esclavo compara su configuración real (tipo de dispositivo, formato y longitud de la innformación), con la configuración esperada que es la que tiene el procesador de control, y sólo será incluido en la fase de transferencia de datos si coinciden las dos configuraciones. Estas pruebas garantizan al usuario una protección adecuada contra los errores de parametrización.

7.7. Políticas de Ciberseguridad a aplicar para proteger la instalación.

De acuerdo con la *"Guía para empresas: seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA)"* elaborada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO) [36], a continuación se identifican los principales orígenes de los ataques cibernéticos, las principales vulnerabilidades para que estos ataques cibernéticos tengan éxito, y por último se expone un manual de buenas prácticas con el fin de usarlo como base para la elaboración de Informes de Ciberseguridad específicos para la instalación de la Planta Estándar de Ciclo Combinado.

7.7.1 Principales orígenes de los ataques cibernéticos.

A continuación se describen tanto los principales orígenes de los ataques como algunas de las motivaciones de los mismos. Los posibles orígenes son:

a) Empleados descontentos:

Estos incidentes cobran especial relevancia debido al conocimiento que tienen dichos empleados sobre el sistema, así como los permisos que tienen asignados para su trabajo diario. Hay que incluir en este caso la posibilidad de acceso por parte de ex-empleados al contar con conocimientos similares.

b) Espionaje industrial:

Aunque este tipo de incidentes son inusuales, una compañía rival podría por ejemplo suministrar al empleado de una empresa algún tipo de software malicioso que produzca acciones no autorizadas sobre el sistema de monitorización y control en tiempo real, ya sea alteración de las comunicaciones, robo de información, o realización de operaciones arbitrarias. Este software podría encontrarse, por ejemplo, en un dispositivo de almacenamiento USB a la espera de ser conectado a un equipo del sistema SCADA para infectarlo.

c) Hackers:

Genéricamente, bajo este término se engloba a cualquier persona con conocimientos técnicos avanzados que realice acciones que vulneren la seguridad de un sistema. Las motivaciones de este tipo de personas pueden ser muy variadas, desde la depuración y resolución de errores en los sistemas, hasta la intrusión con fines maliciosos, pasando por aspiraciones como comprobar el nivel de conocimientos y las habilidades de intrusión.

d) Activismo ideológico:

Pueden existir grupos u organizaciones que, por motivos ideológicos, se marquen como objetivo los sistemas de monitorización y control en tiempo real de alguna compañía o administración. Entre estas motivaciones ideológicas se pueden encontrar razones políticas, medioambientales, sanitarias, éticas, etc.

e) Terrorismo:

Debido a la criticidad de las instalaciones o servicios controlados por algunos de estos sistemas, se pueden convertir en el objetivo de ataques terroristas.

f) Incidencias accidentales:

Como en todo sistema, muchos de los riesgos podrían tener como causa simples accidentes, desde desastres naturales a incendios de pequeño alcance.

Es importante señalar que las motivaciones y amenazas no son idénticas para todos los sistemas de monitorización y control, sino que dependen en gran medida de su criticidad y la relevancia del proceso asociado, por lo que el nivel de seguridad a aplicar dependerá de la importancia del sistema.

7.7.2 Causa de las vulnerabilidades y amenazas o factores que los fomentan.

Por otro lado, existen ciertas circunstancias que podrían considerarse como causa de las vulnerabilidades y amenazas o al menos como factores que pueden fomentar dichos problemas. Las principales son:

a) Exceso de confianza en la "seguridad por oscuridad":

Una idea extendida entre algunos profesionales de la seguridad en estos sistemas es que la ausencia de conocimiento y de información sobre una tecnología o producto ofrece altos niveles de seguridad al mismo. Esta concepción es especialmente aplicable a los sistemas de monitorización y control en tiempo real, ya que los elementos empleados en ellos tradicionalmente se han basado en tecnologías propietarias y especializadas, y cuyo acceso estaba restringido a un número reducido de usuarios.

Sin embargo, el desconocimiento general de la tecnología empleada no puede considerarse un mecanismo de seguridad aceptable. Una persona interesada en atacar un sistema de monitorización y control en tiempo real siempre podría estudiar y analizar una instalación, desarrollando y empleando diversas técnicas de recopilación de información. Por ello, un exceso de confianza en el modelo de seguridad por oscuridad puede generar o agravar ciertas amenazas.

b) Minimización o desestimación de riesgos y amenazas:

Muchos responsables de sistemas de monitorización y control en tiempo real consideran que sus instalaciones carecen de interés para potenciales atacantes, lo que a su juicio reduce la necesidad de seguridad de las mismas. Este hecho no se corresponde con la realidad, ya que un sistema que supervisa y gestiona procesos en tiempo real siempre va a ser un objetivo en potencia para atacantes. Por otro lado, no hay que olvidar que buena parte de los ataques proceden del interior de la propia compañía u organización (empleados descontentos o antiguos trabajadores/colaboradores).

c) Interconexión creciente:

Los sistemas de monitorización y control en tiempo real, desde sus orígenes, fueron diseñados para permanecer aislados del exterior, situación que actualmente se ha modificado en muchas ocasiones. Un claro ejemplo de este hecho es que no fueron pensados para estar interconectados con redes como Internet o las redes corporativas. Esto ha provocado la aparición de nuevos riesgos o amenazas para los que no estaban diseñados al incorporarse este tipo de conexiones.

d) Arquitecturas de red poco seguras:

Muy relacionado con los demás factores. En algunas ocasiones se han incorporado sistemas de comunicación poco seguros que posibilitan la intrusión en el sistema o la intercepción, falsificación y/o bloqueo de las transmisiones entre los dispositivos.

e) Configuraciones por defecto:

No modificar las configuraciones con las que cuentan los equipos y dispositivos desde su fabricación facilita enormemente la intrusión y manipulación de los mismos.

f) Ausencia de concienciación del personal:

Debido al nuevo escenario en el que se encuentran los sistemas de monitorización y control en tiempo real, la labor de concienciación del personal, tanto del operativo como de la alta dirección, se ha hecho más necesaria. Un punto en el que debe ahondar esta concienciación son los cambios que han sufrido este tipo de sistemas, el detrimento en seguridad que esto puede producir y la importancia del cumplimiento de las medidas que solventen o mitiguen estos inconvenientes.

g) Uso de tecnologías y soluciones de propósito general:

El uso de tecnologías de propósito general ofrece mayor flexibilidad y supone una reducción de costes considerable, aunque por otro lado implica que, debido a que los ataques contra este tipo de tecnología son bastante comunes, los sistemas de monitorización y control pasen a ser un objetivo más fácil.

h) Escasa evolución:

Debido a que el objetivo principal es su disponibilidad, los sistemas de monitorización y control en tiempo real suelen sufrir muy pocas modificaciones a lo largo del tiempo, ya que se consideran peligrosas: cualquier cambio puede introducir algún fallo o problema que afecte negativamente en su rendimiento o incluso paralizar el proceso al que se dedica. Asimismo, estos cambios suelen acarrear un alto coste económico, debido en buena medida a la especialización de los componentes y al amplio ámbito geográfico en el cual suelen estar desplegados.

7.7.3 Identificación y análisis de los principales riesgos y amenazas.

Una vez descritas las fuentes de amenaza que pueden encontrarse respecto a los sistemas de monitorización y control en tiempo real, se presentan los principales riesgos, ya sean estos técnicos o de gestión.

a) Usos inadecuados:

La concienciación en cuanto a la seguridad relativa a los sistemas de monitorización y control en tiempo real se ha focalizado tradicionalmente en su vertiente física, no lógica o informática. Esta es una de las principales causas de la inseguridad en estos sistemas. El desconocimiento de los riesgos reales posibilita en muchas ocasiones que los propios empleados, sin ánimo de poner en riesgo el sistema, realicen acciones que podrían comprometer la seguridad. Ejemplos de estas prácticas podrían ser la conexión de dispositivos no asegurados, utilizando los puertos USB, o simples conexiones a través de Internet.

b) Bloqueo/Intercepción/Falsificación de las comunicaciones:

Las comunicaciones entre los dispositivos o de éstos con el puesto de control, en caso de no realizarse mediante un canal modo seguro, podrían ser bloqueadas, interceptadas o falsificadas. En el caso de un bloqueo, la principal consecuencia sería la pérdida de contacto y por tanto de control de algún dispositivo de campo. En cambio, una intercepción de las comunicaciones supondría un riesgo para la privacidad, pudiendo poner al descubierto información sensible respecto al funcionamiento del sistema. Pero sin duda el mayor riesgo sería la falsificación de las comunicaciones, que podría utilizarse para forzar un error inducido.

Los errores inducidos son consecuencia del refinamiento de un ataque, en el cual el objetivo es provocar que se cometan errores al tomar decisiones, automáticamente

por el sistema o personalmente por los trabajadores, que provoquen un mal funcionamiento en los procesos controlados.

Este ataque suele realizarse mediante el envío de información errónea, haciendo creer que se ha producido un cambio frente al que hay que actuar, de modo que se trate de solucionar un problema inexistente generando otro. De esta forma, el atacante lograría su objetivo de una forma más sutil, ya que el incidente parecería haber sido producido por un error humano.

Este modelo de ataque también puede utilizarse para encubrir una manipulación, enviando información que indique que no se producen cambios de relevancia cuando sí están ocurriendo. De este modo se trataría de evitar las posibles acciones correctoras que inutilizasen la manipulación.

c) Virus informáticos o malware:

Debido a lo usual de la existencia de software desactualizado y/o configuraciones por defecto, estos sistemas pueden ser vulnerables a los virus informáticos y demás malware que son conocidos desde hace tiempo y para los que ya existen soluciones de prevención. Además del malware de ámbito genérico, hay que señalar la posibilidad de generación de nuevos códigos maliciosos específicos para este tipo de sistemas.

d) Accesos no autorizados:

El desconocimiento de la conectividad del sistema, la utilización de configuraciones por defecto en los mecanismos de acceso y las arquitecturas de red poco seguras, pueden facilitar el acceso no autorizado al sistema de monitorización y control. Este acceso puede comprometer la privacidad de la información acerca del sistema, pero de manera muy especial puede ser un riesgo de importancia en caso de lograr controlar el sistema, pudiendo modificar en el acto el proceso controlado o cambiar las órdenes y protocolos establecidos para su funcionamiento automático, de modo que las consecuencias de estas modificaciones podrían darse tiempo después de la intrusión.

Todo ello da lugar a un riesgo muy importante, ya que cualquier persona con un nivel de conocimiento técnico medio, podría al menos detectar los dispositivos y equipos de este tipo de sistemas. Por ello es necesario diseñar una arquitectura de red segura que permita evitar estas prácticas.

e) Ataques externos:

Mediante este tipo de ataques, usuarios malintencionados pueden hacer uso de distintas herramientas que se encuentran publicadas en Internet para tomar el control, desestabilizar o dañar los sistemas de una organización. No es necesario, por tanto, contar con grandes conocimientos técnicos, ni equipamiento específico, para perpetrar este tipo de ataques.

Debido a que la tendencia actual de las redes SCADA es la de interconectarse a través de redes como Internet o las redes corporativas, es posible realizar ataques desde redes externas a la organización.

Uno de los ataques externos más dañinos para los sistemas SCADA son los conocidos como de Denegación de Servicio (ataques DoS), mediante los cuales un recurso deja de ser accesible para los usuarios legítimos. Normalmente, el objetivo de este tipo de ataques es agotar los recursos disponibles de la red, de tal manera que se provoca una pérdida de la conectividad con los sistemas.

f) Sabotaje:

La mayoría de los ataques notorios son internos. Muchas organizaciones consideran que adoptar unas medidas de seguridad perimetrales robustas es suficiente para mantener un nivel de seguridad adecuado, protegiéndose así de ataques externos pero manteniendo las vulnerabilidades internas.

Igualmente, en muchas ocasiones se considera que los empleados, o bien no tienen los suficientes conocimientos técnicos para perpetrar un ataque, o bien no tienen motivaciones para consumarlos. Esta creencia da lugar a que no se tomen medidas de seguridad que contemplen la posibilidad de ataques por parte de empleados descontentos o motivadas por el espionaje industrial.

Es importante recalcar que este tipo de ataques pueden perpetrarse sobre la infraestructura de soporte de las organizaciones, tales como el soporte energético y la climatización de sistemas, y no únicamente sobre el sistema SCADA de forma directa.

g) Problemas en los sistemas de soporte:

Estos riesgos afectan a los sistemas de monitorización y gestión en tiempo real del mismo modo que al resto de sistemas TIC, pudiendo afectar especialmente al suministro eléctrico o a las comunicaciones. En el caso de estos sistemas, la redundancia de estos servicios es más habitual al ser prioritario su funcionamiento, por lo que suele existir mayor concienciación al respecto.

7.7.4 Buenas prácticas aplicables.

A continuación se incluye de forma genérica un conjunto de buenas prácticas para el sistemas de monitorización y control, destacando que no todas ellas son necesariamente de aplicación para cualquier sistema, ya que dependerá, entre otros factores, de su tamaño, alcance, naturaleza y objetivos.

Para detallar la aplicación de medidas de Ciberseguridad a adoptar de forma particular en la Planta de Estándar de Ciclo Combinado, se eleborarán informes de Ciberseguridad que hagan un análisis de riesgos y las medidas a llevar a cabo para evitar daños en la instalación.

a) Desarrollar un Plan de Continuidad de Negocio y un Plan de Recuperación ante Desastres para el sistema de monitorización y control.

Para garantizar la disponibilidad de estos sistemas, es muy recomendable definir y aprobar un Plan de Continuidad de Negocio (PCN) y un Plan de Recuperación ante Desastres (PRD) propios para el sistema de monitorización y control.

Como base se pueden emplear los PCN y PRD definidos para el conjunto de la empresa, siempre y cuando se recojan las necesidades específicas de este tipo de sistemas.

Estos planes contienen las pautas a seguir en caso de incidente, para, en primer lugar, mantener en funcionamiento los procesos productivos del negocio y, por otro lado, tomar las medidas necesarias para volver a la normalidad.

b) Desarrollar e implantar adecuadamente políticas de seguridad y procedimientos al respecto.

Dado que la seguridad no es exclusivamente un problema técnico, sino también de negocio, resulta necesario desarrollar e implantar un conjunto de políticas y

procedimientos. Este conjunto de documentos debe abarcar todos los aspectos que afectan al sistema.

c) Concienciación y formación del personal en seguridad.

Una de las principales medidas en el ámbito de la seguridad que todas las empresas deberían implementar, especialmente aquellas que emplean algún tipo de sistema de monitorización y/o control en tiempo real, es la planificación de cursos o talleres de concienciación sobre seguridad para sus empleados. De este modo se trata de situar la seguridad entre las prioridades de trabajo. Esta concienciación es clave.

De forma complementaria, es recomendable ofrecer sesiones periódicas de formación, en las que se muestren con ejemplos prácticos qué medidas pueden y deben tomarse para obtener un nivel de seguridad razonable y evitar posibles errores que impacten en el funcionamiento de la empresa.

Con estas medidas se podría evitar gran parte de los problemas debidos a errores humanos, al contar el personal con los suficientes conocimientos técnicos a la hora de afrontar situaciones inusuales.

d) Creación de equipos multidisciplinares.

Es recomendable que los equipos encargados de mantener los sistemas de gestión y supervisión sean multidisciplinares, es decir, que los miembros de dicho equipo abarquen los campos de conocimiento de seguridad (física y lógica), informática, telecomunicaciones o industria. De este modo, se evita la toma de decisiones en base a premisas incompletas por falta de conocimientos.

e) Seguridad integral.

Para maximizar los esfuerzos orientados a garantizar la seguridad, éstos se deben realizar utilizando un enfoque integral en el cual se aúnen tanto la visión física como la visión lógica o informática de la misma, ya que los riesgos suelen poseer ambos componentes. Por ello deben ser gestionados desde un punto de vista omnicomprensivo.

f) Definición y aplicación de roles y responsabilidades.

El objetivo principal de la definición y aplicación de responsabilidades es establecer un reparto de funciones que sea adecuado a la empresa y su funcionamiento, y que se base en el principio de mínimos privilegios.

Así, los empleados deben tener asignadas única y exclusivamente las funciones y responsabilidades propias de su puesto. Esto ayudará a minimizar las posibilidades de que ocurra un error humano.

Junto a esta medida es recomendable implantar un sistema de trazabilidad que guarde un registro de los cambios y acciones que cada trabajador ha realizado. De este modo, además de facilitar la investigación en caso de incidencias, se contará con una medida disuasoria de cara a posibles ataques internos.

g) Realización periódica de simulacros.

La realización periódica de simulacros ofrece garantías razonables que, en caso de contingencia, el personal operativo pueda asegurar la disponibilidad del servicio. Estos simulacros hacen que, además de reforzar y perfeccionar los conocimientos y

habilidades necesarias para estas tareas, se ejerciten en condiciones similares a las presentes en los casos de incidentes.

h) Realizar periódicamente auditorías de seguridad.

Con el objetivo de analizar y evaluar el nivel de seguridad real de los sistemas SCADA, se recomienda realizar de forma periódica auditorías de seguridad, tanto física como lógica o informática.

i) Prueba preliminar de cambios.

Se considera recomendable contar, al menos, con un entorno de producción y otro de preproducción para poder probar los cambios, actualizaciones y demás actuaciones sobre el sistema que se planifiquen. El entorno de preproducción tendría como finalidad probar los cambios que se deseen realizar en el entorno de producción, que será en el que realmente se encuentren en funcionamiento los procesos productivos. De este modo se podrán detectar las posibles disfunciones, inconsistencias o errores derivados de su instalación.

j) Restringir el acceso físico al centro de control y a los puestos de campo.

Un acceso físico no autorizado podría comprometer el sistema, por lo que deben establecerse los mecanismos de protección físicos que se consideren adecuados, combinándolos con medidas de protección lógica o informática cuando sea posible. Dependiendo de la criticidad y ubicación de los dispositivos a proteger se deben tomar las medidas acordes a su importancia.

k) Restringir la conexión entre el sistema y otras redes.

Debido a la ausencia de seguridad característica de redes públicas como Internet, las conexiones entre el sistema de monitorización y control y estas redes se deben limitar al mínimo imprescindible, con el objetivo de reducir el origen de posibles ataques.

Para ayudar a esta tarea, hay que definir una arquitectura de red segura, así como instalar elementos y herramientas de seguridad siempre y cuando sea posible.

l) Redundar aquellos componentes cuya disponibilidad se considere esencial.

Dado que la disponibilidad es el atributo principal en este tipo de sistemas, es aconsejable redundar o duplicar, ya sea física o informáticamente, aquellos componentes que se consideren críticos. El objetivo de esta redundancia es eliminar los denominados puntos únicos de fallo, de modo que la funcionalidad quede garantizada en caso de que un fallo lógico o físico ocurra.

m) Aseguramiento de los accesos remotos.

Aunque idealmente estos sistemas deberían permanecer aislados, en la mayoría de las ocasiones esto no es posible, ya sea por requerimientos de negocio, funcionales o de disponibilidad. En el caso de necesitar accesos remotos, es aconsejable establecer mecanismos de seguridad y autenticación robustos que eviten accesos no autorizados y robos de información. Pero el factor principal es la decisión de qué conexiones son realmente necesarias y cuáles no lo son.

n) Utilizar preferentemente enlaces de comunicación cableados.

Es apropiado utilizar, en la medida en que sea posible, enlaces de comunicación físicos, tanto por motivos de seguridad, al ser más difíciles de interceptar y suplantar las comunicaciones a través de redes cableadas que en el caso de utilizar dispositivos inalámbricos, como por cuestiones de disponibilidad, ya que las redes cableadas suelen ser más robustas frente a problemas de interferencias.

o) Bastionar aplicaciones, sistemas operativos y equipos.

Una práctica que se debería llevar a cabo antes de incorporar una aplicación, sistema operativo o equipo en el entorno productivo, es la realización de un bastionado de dicho elemento. El bastionado es la configuración de un nuevo elemento aplicando todas las medidas de seguridad que sea posible, de modo que se eliminen o mitiguen todas las vulnerabilidades conocidas. El objetivo es que ese elemento cuente con un nivel de seguridad razonable, sin que por ello su funcionalidad se vea afectada. Algunos de los pasos que se deberían seguir durante el bastionado son:

- Sustitución de cuentas por defecto por cuentas personales.
- Modificación de la configuración por defecto por una que se ajuste a las necesidades de la empresa y cumpla unos requisitos de seguridad.
- Activación de mecanismos y controles de seguridad, como puede ser el establecimiento de una política de contraseñas robustas.
- Configuración de la ejecución de actualizaciones automáticas, cuando sea posible.

p) Mantener el software y las herramientas de seguridad actualizadas.

Debido a la constante evolución que sufren los sistemas de información, especialmente y las amenazas relativas a la infección con virus y otros tipos de malware, la necesidad de mantener al día las firmas de los antivirus y demás herramientas de seguridad cobra gran relevancia. También es especialmente importante mantener actualizado el software, tanto programas como sistemas operativos, para corregir los fallos de seguridad que se descubren.

q) Realización periódica de copias de seguridad.

La realización de copias de seguridad de los activos de información de los sistemas es una tarea vital para garantizar su disponibilidad en caso de incidente. Estas copias de seguridad deben realizarse con la suficiente periodicidad, atendiendo a la importancia del activo sobre el que se está generando la copia de respaldo, así como a la frecuencia con la que se realizan cambios sobre el mismo.

También es necesario realizar pruebas periódicas de restauración de copias de seguridad, con el objetivo de verificar que la información de dichas copias es integra y correcta, y que el personal conoce el procedimiento a seguir para que, en caso de necesitarlo, estén preparados para utilizar estas copias.

r) Evaluar la opción de externalizar el mantenimiento y seguridad del sistema.

La posibilidad de contratar los servicios relativos al mantenimiento funcional y de seguridad de los sistemas de monitorización y control en tiempo real a empresas especializadas es una solución que debería analizarse y evaluarse, especialmente

por parte de las pymes que no controlen infraestructuras catalogadas como críticas. Debido a la complejidad de este tipo de sistemas, para algunas empresas puede resultar muy costoso y difícil contar con personal especializado que se encargue de dichas tareas, así como proporcionarle los recursos necesarios para su labor.

La externalización, en función de la empresa y del sistema, puede llegar a ser una solución a tener en cuenta, ya que provee flexibilidad, servicio continuo en cualquier momento y personal especializado, entre otros aspectos.

s) Seguimiento de estándares y organismos de referencia.

Debido a la especialización de este tipo de sistemas, así como de la tendencia actual hacia la convergencia en ciertos estándares, ya sean reconocidos o de facto, resulta altamente recomendable realizar un seguimiento de organismos de referencia, tanto a nivel nacional (CCN, CNPIC), como internacional (IEEE, JEC, CPNI, NIST, NERC, AGA, etc.).

t) Contratación del personal operador.

La aplicación de esta recomendación se circunscribe principalmente a aquellos sistemas de monitorización y control que gestionen Infraestructuras Críticas, o cuyo alcance sea considerable.

Para estos casos, es recomendable solicitar referencias en anteriores puestos de trabajo así como tratar de comprobar la veracidad de las mismas. Esto es debido a que una vez contratados, su capacidad de actuación sobre el sistema puede ser considerable, en función del rol que le sea asignado.

8. Conclusiones finales.

Con el presente trabajo se lleva a cabo la consecución de los siguientes objetivos:

a) Se ha realizado un estudio de las comunicaciones industriales actuales, para incorporarlo al Know-how de la empresa como base para la formación en comunicaciones industriales de la plantilla del Departamento de I&C, para permitir en proyectos futuros la incorporación de la ingeniería de las comunicaciones de la planta.

b) Con el presente trabajo se han puesto las bases para la implementación de una red de comunicaciones "estándar", basada en la especificación de bus de campo PROFIBUS mediante equipos de SIEMENS, para la Planta Estandar 109FB de General Electric ©, estableciendo una arquitectura de comunicaciones basada en bus de campo totalmente flexible, escalable y adaptable a la estructura modular que ofrece la Planta Estándar, sin entrar en detalles de configuración software de los diferentes equipos ni de las redes.

c) Para la definición de la arquitectura de comunicaciones se ha empleado la filosofía de jerarquización de redes basada en el modelo CIM, con el fin de implementar las redes de comunicaciones de los diferentes sistemas de la Planta Estándar de Ciclo Combinado, la cual se concluye que consta de: redes de campo, célula, control/supervisión y factoría.

d) Para la comunicación de todos los elementos de las redes de comunicaciones de la Planta Estándar de Ciclo Combinado se emplean las especificación de bus de campo PROFIBUS y la versión de éste para Ethernet, PROFINET.

e) PROFIBUS es un bus de campo standard que acoge un amplio rango de aplicaciones en fabricación, procesado y automatización bajo la norma EN 50 170, con PROFIBUS los componentes de distintos fabricantes pueden comunicarse sin necesidad de ajustes especiales de interfaces, por lo que es posible integrar en la arquitectura definida nuevos componentes de fabricantes diferentes.

f) Las diferentes redes de campo de la Planta Estandar de Ciclo Combinado se forman mediante las versiones DP y PA de PROFIBUS.

g) Las señales de los diferentes instrumentos analógicos y digitales de la planta necesarios para manejar el proceso de generación eléctrica, que son: dispositivos analógicos (AI, TC, Pt-100 y AO) y digitales (DI y DO); se "empaquetan" en la red de campo mediante sistemas de periferia descentralizada, formando segmentos PROFIBUS-DP compuestos de: módulo de periferia descentralizada ET200M, Módulos SIM de E/S analógicas y/o digitales, interfaz de comunicaciones IM153 y fuente de alimentación PS307.

h) Las válvulas motorizadas (MOV) se integran en la red de campo con la versión de PROFIBUS-PA, formando segmentos que se conectan a dicha red mediante acopladores DP/PA.

i) La topología de la red de campo está compuesta de una topología mixta de bus líneal y bus en anillo redundante. En cada rack de segmentos se forman dos buses lineales: un bus lineal que conecta cada una de las MOVs a su segmento, mediante la versión PROFIBUS-PA, y otro bus lineal que conecta el segmento de PROFIBUS-DP con las señales analógicas y digitales. Finalmente un bus en anillo redundante conecta los diferentes segmentos con el procesador de control MARK VIe.

j) La red de célula la forman los dispositivos de control pertenecientes a diversas islas de producción (sistemas de planta), correspondientes a los sistemas de control de los sistemas paquete con los procesadores MARK VIe situados en las cabinas 11CJA01 y 11CJA02.

Como recomendación se indicará a los suministradores de los sistemas paquete que el PLC de su sistema de control sea Simatic S7 de SIEMENS, que facilita la configuración del bus así como garantiza que sea totalmente compatible con los módulos de comunicación OLM.

k) La red de control/supervisión de la Planta estándar de Ciclo combinado es única, y la forman los procesadores 11CJA01 y 11CJA02 del PCS (MARK VIe) con los diferentes puestos de supervisión/control en Sala de Control (CW03, CW04, CW05, etc). El diseño de esta red de comunicación se basa en un bus basado en ETHERNET, para aprovechar las características que proporciona la capa de Ethernet, y entre ellas la velocidad casi en tiempo real de Mbps. Por tanto, como las capas inferiores son PROFIBUS el bus basado en Ethernet para esta especificación de bus es PROFINET que admite cualquier tipo de topologías de red (estrella, árbol, anillo, …).

l) Para la red de control/supervisión de la Planta Estándar de Ciclo Combinado se elige una topología mixta de doble anillo de alta velocidad que conecta los dispositivos situados en diferentes áreas o localizaciones, mediante switches situados en cada área para permitir la conexión de los equipos de la misma localización en estrella, y entre todas las zonas se establece el anillo redundante para incrementar la fiabilidad y flexibilidad de la red.

m) Los elementos de conexión a la red de control/supervisión de los procesadores de control MARK VIe y de PCs de los puestos de supervisión/control (11CWA01, 11CWA02, 11CWA03…), son tarjetas CP1616 de SIEMENS “pinchadas” al puerto de cada PC que conectan con el switch de conexión situado en su zona.

n) La red de factoría permite la comunicación de todos los equipos tipo PCs de las diferentes áreas de la planta, que estén habilitados para visualizar la información de los sistemas desde el Sistema de Control, para la consulta y/o impresión de datos que permita seguir la evolución o estado del proceso de generación eléctrica.

o) Para el intercambio de información de los procesadores del Sistema de Control y los puestos de supervisión/control se precisa del uso de un OPC que facilite el intercambio de datos entre las aplicaciones gráficas de los puestos de supervisión y el procesador de control. Ya que el volumen de datos a manejar en esta red es muy elevado. El bus de campo (PROFINET) empleado al estar basado en Ethernet permite que la información en los puestos de supervisión esté disponible de forma instántanea, según esté disponible en las redes de las capas inferiores.

p) La red de factoría está situada en la parte más alta de la jerarquía de redes de la Planta Estándar y con acceso desde PC personales. Por tanto, es muy importante tener una política de Ciberseguridad muy bien definida que evite tanto conexiones externas maliciosas a dichos PCs personales, como que eviten el acceso de software malicioso a la infraestructura de red de la planta que falsee la información de proceso, dañando el proceso de producción eléctrica o incluso daños irreparables en la integridad de la planta, del personal o entorno de la misma. Para ello se ha definido un conjunto de buenas prácticas para su uso como base en la elaboración de informes de Ciberseguridad, que analicen los riesgos de la instalación y definan las medidas a llevar a cabo para evitar poner en peligro la integridad de la planta.

9. Bibliografía y referencias en internet.

[1] Capítulo I. El modelo CIM y jerarquía de Redes de Comunicación en la Industria.
www.infoplc.com

[2] PIRAMIDE CIM MANUFACTURA INTEGRADA POR COMPUTADOR.
http://autycontrol.blogspot.com.es/2014/04/piramide-cim-manufactura-integrada-por.html

[3] COMUNICACIONES INDUSTRIALES.
http://www.infoplc.net/files/documentacion/comunicaciones/infoplc_net_UC3M_OWC_AI_Comunicaciones_Industriales.pdf

[4] COMUNICACIONES INDUSTRIALES. Universidad de Oviedo.
http://isa.uniovi.es/docencia/iea/teoria/comunicacionesindustrialesdocumento.pdf

[5] "Bus CAN: estado de buses industriales y aplicaciones". Curso de Doctorado: Protocolos de Comunicación entre sistemas de Información (UNED).
http://www.infoplc.net/files/documentacion/comunicaciones/infoPLC_net_Busses%20de%20campo.pdf

[6] Instalación de Sistemas de Automatización y Datos. Universidad de Vigo.
http://tv.uvigo.es/uploads/material/Video/1567/ISAD_Tema6.pdf

[7] Sistemas Industriales Distribuidos. Universidad de Valencia.
http://www.uv.es/rosado/courses/sid/Capitulo3_rev0.pdf

[8] Comunicaciones Industriales. Universidad Carlos III.
http://www.infoplc.net/files/documentacion/comunicaciones/infoplc_net_UC3M_OWC_AI_Comunicaciones_Industriales.pdf

[9] Instrumentation and Controls. GE Design Basis Document Vol I [S109FB-SS B2/B3].

[10] GE Reference Specifications. Instruments and control devices:

[10.1] GE Specification R151, Standard Requirements for Temperature Sensors and "Thermocouple Assemblies".
[10.2] GE Specification R201, Standard Requirements for "Flow Measuring Elements (Nozzles and Venturies)".
[10.3] GE Specification R202, Standard Requirements for "Flow Measuring Elements (Orifices)".
[10.4] GE Specification R251, Standard Requirements for "Electronic Process Transmitters".
[10.5] GE Specification R301, Standard Requirements for "Pressure Switches".
[10.6] GE Specification R351, Standard Requirements for "Local Pressure Transmitters and Gauges".
[10.7] GE Specification R352, Standard Requirements for "Local Temperature Transmitters and Gauges".
[10.8] GE Specification R353, Standard Requirements for "Level Gauges".
[10.9] GE Specification R354, Standard Requirements for "Local Flow Idicators".
[10.10] GE Specification R371, Standard Requirements for "Pneumatic Operated Control Valves".
[10.11] 496-11-LE-I-40200 "List: ICS hardwired and datalinked i/o signals (mechanical systems)".
[10.12] 129E3625 Rev.B "109FB "Control System Architecture".
[10.13] 238A7161 Rev.A "MOV Profibus Architecture".
[10.14] 496-11-LE-I-40300_02 "Control Valve List".

[11] "A Guide to Popular Fieldbus Systems for use with Variable Speed Drives". EMERSON INDUSTRIAL AUTOMATION.
http://www.emersonindustrial.com/en-EN/controltechniques/downloads/referencematerial/Pages/referencematerial.aspx

[12] “MODBUS over Serial Line Specification & Implementation guide v1.0”.
http://www.modbus.org/

[13] “Profibus and Profinet International”.
http://www.profibus.org/

[14] “The Common Industrial Protocol (CIP™) — EtherNet/IP™, DeviceNet™, CompoNet™, and ControlNet™”. ODVA Organization.
http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00123R0_Common%20Industrial_Protocol_and_Family_of_CIP_Netw.pdf

[15] “CiA nonprofit organization: CAN, CANOpen and DEVICENet busses”.
http://www.can-cia.org/

[16] INTERBUS Club.
http://www.interbus.de/index_en.html

[17] LonMark International. “LONWorks Bus”.
http://www.lonmark.org/

[18] Protocolo WorldFIP. IUMA-Universidad de Las Palmas de Gran Canaria.
http://www.iuma.ulpgc.es/~avega/int_equipos/trab9899/busescampo_2/worldfip/protocol.htm

[19] Unitel-Way characteristics. SCHNEIDER ELECTRIC.
http://www.global-download.schneider-electric.com/mainRepository/EDMS_CORP5.nsf/69f5d72c7a0cf811c12573d800389503/417791985ccbbcf08525786b006997ac/$FILE/W913293610301A_K01_000_01.pdf

[20] Smart Distribuided System (SDS). HONEYWELL.
http://www.honeywell.com/sensing/prodinfo/sds

[21] Bitbus characteristics. HOEBEN ELECTRONICS (Members of Bitbus European Users Group).
http://www.hoeben.com/electronics.html

[22] BITBUS specification overview.
http://www.bitbus.org/fprimer.htm

[23] Guía rápida de COMPOBUS-S.
http://www.sainel.es/intraweb/buscadocman/lanzar.php?idarch=289

[24] Guía rápida de COMPOBUS-D.
http://www.sainel.es/intraweb/buscadocman/lanzar.php?idarch=288

[25] ControlNet Protocol.
http://www.controlnet.org/

[26] SIMATIC NET PROFIBUS Networks Manual (6GK1970–5CA20–0AA1 Release 2).

[27] PROFIBUS. Siemens IK PI · 2004.

[28] SIMATIC NET PROFIBUS (Optical Link Module).

[29] Sistema de periferia descentralizada ET 200 de SIMATIC (A5E00172812-08).

[30] STAG ™ 109FB-Single Shaft. STANDARD POWER PLANT.
http://site.ge-energy.com/prod_serv/products/gas_turbines_cc/en/downloads/stag_109fb.pdf

[31] Catálogo de productos SIEMENS para comunicación industrial.
https://mall.industry.siemens.com/mall/es/es/Catalog/Products/9309999?tree=CatalogTree

[32] SIMATIC S7-300 S7-300 Module data Manual.
https://cache.industry.siemens.com/dl/files/629/8859629/att_55794/v1/s7300_module_data_manual_en-US_en-US.pdf

[33] Acoplamientos de bus Acoplador DP/PA, distribuidores de campo activos, DP/PA-Link e YLink. Instrucciones de servicio.
https://cache.industry.siemens.com/dl/files/696/1142696/att_31155/v1/dppa_coupler_afdis_dppa_link_y_link_manual_es-ES_es-ES.pdf

[34] Estrategias de ciberseguridad en el mundo.
http://www.thiber.org/estrategias-nacionales-de-ciberseguridad-en-el-mundo/

[35] CIBERSEGURIDAD. Retos y amenazas a la seguridad nacional en el Ciberespacio. (Catálogo general de publicaciones oficiales).
http://www.publicacionesoficiales.boe.es

[36] Guía para empresas: Seguridad de los sistemas de monitorización y control de los procesos e infraestructuras (SCADA). *Instituto Nacional de Tecnologías de la Comunicación (INTECO).*
https://www.incibe.es/

ANEXO 1.

"Listado de señales de dispositivos de campo."

Tabla 1. SEÑALES CABINA 11CSA11

Tipo INS	Identificación señal	Descripción de la señal	PID	SISTEMA	Tipo señal
1046	11GHA10AC001	Auxiliary boiler	496-11-DT-M-13300 Sh 1	Auxiliary Steam System	5DI x 2DO
110	11SCA20CP001	Dry tank pressure	496-11-DT-M-13400 Sh 2	Compressed Air System	AI
994	11SCA10GH002	Comp air dryer	496-11-DT-M-13400 Sh 1	Compressed Air System	2DI x 2DO
995	11SCA10GH001	Comp air compressor	496-11-DT-M-13400 Sh 1	Compressed Air System	3DI x 3DO
167	11LCP01CP301	Conden stor tank filter dp switch	496-11-DT-M-10400 Sh 2	Condensate System	DI
400	11LCA30AA301	LP economizer isolation MOV	496-11-DT-M-10400 Sh 1	Condensate System	PROFIBUS MOV
450	11LCA30AA302	LP economizer isolation bypass MOV	496-11-DT-M-10400 Sh 1	Condensate System	PROFIBUS MOV
110	11GHC10CL001A	Demineralized water tank level	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	AI
110	11GHC10CL001B	Demineralized water tank level	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	AI
110	11GHC30CP001	Demin wtr inj pmp disch press	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	AI
110	11GHC43CP001	Demin water pumps disch pressure	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	AI
110	11GHC70CP002	Water injection skid inl press	496-11-DT-M-13500 Sh 2	Demineralised Water Storage & Distribution System	AI
152	11GHC10CP301	Demin water tk CO2 absorber press	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	DI
302	11GHC70AA201	Demin wtr to wtr injection skid CV	496-11-DT-M-13500 Sh 2	Demineralised Water Storage & Distribution System	AO
500	11GHC30AP001	Water injection pump	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	2DI x 2DO
500	11GHC41AP001	Demineralized water pump 1	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	2DI x 2DO
500	11GHC42AP001	Demineralized water pump 2	496-11-DT-M-13500 Sh 1	Demineralised Water Storage & Distribution System	2DI x 2DO
110	11LAB10CF001A	FWP 1 interstage bleed flow	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB10CF001B	FWP 1 interstage bleed flow	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB10CP006	FWP 1 interstage bleed press	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB20CF001A	FWP 2 interstage bleed flow	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB20CF001B	FWP 2 interstage bleed flow	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB30CP001	IP econom inlet feed water press	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB50CF001A	FWP 1 discharge feed water flow	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB50CF001B	FWP 1 discharge feed water flow	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB50CP001	FWP 1 suction filter dif press	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB50CP002	FWP 1 discharge feed water press	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI

110	11LAB60CF001A	FWP 2 discharge feed water flow	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB60CF001B	FWP 2 discharge feed water flow	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB60CP001	FWP 2 suction filter dif press	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB60CP002	FWP 2 discharge feed water press	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB70CF001A	HP econom inl feed wtr fl Full rng	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB70CF001B	HP econom inl feed wtr fl Full rng	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB70CF001C	HP econom inl feed wtr fl Low rng	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB70CP001	HP econom inlet feed water press	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB70CP002A	HP drum lvl CV dif pres Full range	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
110	11LAB70CP002B	HP drum lvl CV dif pres Low range	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
147	11LAB70CT002	HP econom inl feed water temp	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI (TC-E)
147	11LAB80CT001	HP feedwater pmps suction temp	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI (TC-E)
304	11LAB70AA201	HP drum level CV	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	DO x DI x AO
308	11LAB50AA202	HP/IP FWP 1 recirculation CV	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	DO x DI x AO
308	11LAB60AA202	HP/IP FWP 2 recirculation CV	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	DO x DI x AO
400	11LAB30AA301	IP economizer isolation MOV	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	PROFIBUS MOV
400	11LAE01AA301	SH attemperator isolation MOV	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	PROFIBUS MOV
400	11LAF10AA301	RH attemperator isolation MOV	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	PROFIBUS MOV
450	11LAB30AA302	IP economizer pre fill MOV	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	PROFIBUS MOV
500	11LAC10AC001	HP FWP1 lube oil heater	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	2DI x 2DO
500	11LAC10AP002	HP FWP1 aux lube oil pump	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	2DI x 2DO
500	11LAC20AC001	HP FWP2 lube oil heater	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	2DI x 2DO
500	11LAC20AP002	HP FWP2 aux lube oil pump	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	2DI x 2DO
560	11LAC10CT001	HP/IP FWP1 temperature	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI (PT-100)
560	11LAC20CT001	HP/IP FWP2 temperature	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI (PT-100)
562	11LAC10CY001	HP/IP FWP1 vibration	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
562	11LAC20CY001	HP/IP FWP2 vibration	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
1014	11LAC10CT003	HP/IP FWP1 speed var temp	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	3AI (PT-100)
1014	11LAC20CT003	HP/IP FWP2 speed var temp	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	3AI (PT-100)
1015	11LAC10CS001	HP/IP FWP1 speed var vel	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	DI x AI
1015	11LAC20CS001	HP/IP FWP2 speed var vel	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	DI x AI
1051	11LAE01CF001	SH attemperation flow	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	AI
1051	11LAF10CF001	RH attemperation flow	496-11-DT-M-10301 Sh 1	Feedwater System (IP/HP Interstage Bleed)	AI
989	11SGA10GH001	Fire protection system	496-11-DT-M-15100 Sh 1	Fire Protection System	2DI

110	11EKG01CL002	Drain collection tank level	496-11-DT-M-13100 Sh 2	Fuel Gas System	AI
147	11EKG80CT001	Gas temperature	496-11-DT-M-13100 Sh 2	Fuel Gas System	AI (TC-E)
167	11EKG01CL301	Stand pipe level switch	496-11-DT-M-13100 Sh 2	Fuel Gas System	DI
1001	11EKA10AA201	Fuel gas inlet AOV	496-11-DT-M-13100 Sh 1	Fuel Gas System	2DI x 2DO
1019	11EKD01GH001	Regulation & metering station	496-11-DT-M-13100 Sh 1	Fuel Gas System	7DI
110	11GMB01CL001	Water wash drains tank level	496-11-DT-M-11600 Sh 2	Gas Turbine Auxiliaries	AI
300	11HAC20AA201	LP cond prehtr AOV	218D3479 Sh 5	HRSG	2DI x DO
300	11HAC50AA201	IP economizer outlet vent AOV	218D3479 Sh 4	HRSG	2DI x DO
300	11HAD50AA201	IP cont blwdn AOV	218D3479 Sh 4	HRSG	2DI x DO
300	11HAD50AA251	IP drum start-up blowdown AOV	218D3479 Sh 4	HRSG	2DI x DO
300	11HAD70AA251	HP drum start-up blowdown AOV	218D3479 Sh 3	HRSG	2DI x DO
300	11HAH20AA201	LP superheater drain AOV	218D3479 Sh 5	HRSG	2DI x DO
300	11HAH50AA201	IP superheater drain AOV	218D3479 Sh 4	HRSG	2DI x DO
301	11LAB50AA201	IP economizer start-up line AOV	218D3479 Sh 4	HRSG	2DI x DO
301	11LBA50AA201	IP superhtr outlet drain pot AOV	218D3479 Sh 4	HRSG	2DI x DO
301	11LBA50AA202	IP st line vent AOV	218D3479 Sh 4	HRSG	2DI x DO
301	11LBA50AA203	IP superhtr outlet drain pot AOV	218D3479 Sh 4	HRSG	2DI x DO
301	11LBA50AA204	IP superhtr outlet drain pot AOV	218D3479 Sh 4	HRSG	2DI x DO
301	11LBC60AA201	CRS line drain pot drain line AOV	218D3479 Sh 4	HRSG	2DI x DO
1048	11HNE20AA301	Stack damper	218D3479 Sh 2	HRSG	4DI x 2DO
110	11HAC20CF001A	LP feedwater flow	218D3479 Sh 5	HRSG	AI
110	11HAC20CF001B	LP feedwater flow	218D3479 Sh 5	HRSG	AI
110	11HAC20CP001	LP preheaters diff press	218D3479 Sh 5	HRSG	AI
110	11HAC50CF001A	IP econom feedwater flow	218D3479 Sh 4	HRSG	AI
110	11HAC50CF001B	IP econom feedwater flow	218D3479 Sh 4	HRSG	AI
110	11HAH70CP001	HP superhtr 1 after attemp press	218D3479 Sh 3	HRSG	AI
110	11HAJ50CP001	Reheat steam after attemp press	218D3479 Sh 4	HRSG	AI
110	11HAN10CL001	HRSG blowdown tank level	218D3479 Sh 5	HRSG	AI
110	11LBA50CF001A	IP steam line to CR flow	218D3479 Sh 4	HRSG	AI
110	11LBA50CF001B	IP steam line to CR flow	218D3479 Sh 4	HRSG	AI
110	11LBA50CP001A	IP steam line to CR press 1	218D3479 Sh 4	HRSG	AI
110	11LBA50CP001B	IP steam line to CR press 2	218D3479 Sh 4	HRSG	AI
1052	11LCA40CF001	LP econom recirc pmp discharge fl	218D3479 Sh 5	HRSG	AI
147	11HAC20CT001	LP economizers outlet temp	218D3479 Sh 5	HRSG	AI (TC-E)
147	11HAC20CT002	LP feedwater temp	218D3479 Sh 5	HRSG	AI (TC-E)
147	11HAC50CT001	IP econom outlet temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11HAC70CT001	HP economizer 1/2 temp	218D3479 Sh 3	HRSG	AI (TC-E)
147	11HAC70CT002	HP economizer 2/2 temp	218D3479 Sh 3	HRSG	AI (TC-E)
147	11HAH70CT001	HP superhtr 2 after attemp temp	218D3479 Sh 3	HRSG	AI (TC-E)

147	11HAH70CT002	HP shr 2 after attemp dr pot temp	218D3479 Sh 3	HRSG	AI (TC-E)
147	11HAH70CT003	HP shr 1 after attemp dr pot temp	218D3479 Sh 3	HRSG	AI (TC-E)
147	11HAH70CT004A	HP superhtr 1 after attemp temp 1	218D3479 Sh 3	HRSG	AI (TC-E)
147	11HAH70CT004B	HP superhtr 1 after attemp temp 2	218D3479 Sh 3	HRSG	AI (TC-E)
147	11HAJ50CT001	Rhd steam bfr attempn dr pot temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11HAJ50CT002	Reheat steam before attemp temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11HAJ50CT003	Rhd steam aft attempn dr pot temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11HAJ50CT004A	Reheat steam after attemp temp 1	218D3479 Sh 4	HRSG	AI (TC-E)
147	11HAJ50CT004B	Reheat steam after attemp temp 2	218D3479 Sh 4	HRSG	AI (TC-E)
147	11HAN10CT001	HRSG blowdown tank cond temp	218D3479 Sh 5	HRSG	AI (TC-E)
147	11HAN10CT003	HRSG blowdown tank temp	218D3479 Sh 5	HRSG	AI (TC-E)
147	11HNA10CT001A	Gas turbine exhaust temp	218D3479 Sh 2	HRSG	AI (TC-E)
147	11HNA10CT001B	Gas turbine exhaust temp	218D3479 Sh 2	HRSG	AI (TC-E)
147	11HNA10CT001C	Gas turbine exhaust temp	218D3479 Sh 2	HRSG	AI (TC-E)
147	11HNE20CT001	Stack temp	218D3479 Sh 2	HRSG	AI (TC-E)
147	11LAB50CT002	IP feed water to IP econom temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11LAB70CT003	HP econom 2/2 inl feed water temp	218D3479 Sh 3	HRSG	AI (TC-E)
147	11LBA50CT001	IP steam line to CR temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11LBA70CT001A	Main steam line to HPST temp 1	218D3479 Sh 3	HRSG	AI (TC-E)
147	11LBA70CT001B	Main steam line to HPST temp 2	218D3479 Sh 3	HRSG	AI (TC-E)
147	11LBA70CT001C	Main steam line to HPST temp 3	218D3479 Sh 3	HRSG	AI (TC-E)
147	11LBA70CT004	Main steam line to HPST drain temp	218D3479 Sh 3	HRSG	AI (TC-E)
147	11LBB50CT001A	HRS line to IPT temp 1	218D3479 Sh 4	HRSG	AI (TC-E)
147	11LBB50CT001B	HRS line to IPT temp 2	218D3479 Sh 4	HRSG	AI (TC-E)
147	11LBB50CT001C	HRS line to IPT temp 3	218D3479 Sh 4	HRSG	AI (TC-E)
147	11LBB50CT004	HRS line to IPT drain pot temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11LBC60CT002	CR to reheater 2 temp	218D3479 Sh 4	HRSG	AI (TC-E)
147	11LCA20CT001	LP economizer inlet temp	218D3479 Sh 5	HRSG	AI (TC-E)
167	11LBA50CL301	IP steam line to CR dr pot 1 lvl	218D3479 Sh 4	HRSG	DI
167	11LBA50CL302	IP steam line to CR dr pot 1 lvl	218D3479 Sh 4	HRSG	DI
167	11LBA50CL303	IP steam line to CR dr pot 2 lvl	218D3479 Sh 4	HRSG	DI
167	11LBA50CL304	IP steam line to CR dr pot 2 lvl	218D3479 Sh 4	HRSG	DI
167	11LBC60CL301	CR to reheater 2 drain pot 3 level	218D3479 Sh 4	HRSG	DI
167	11LBC60CL302	CR to reheater 2 drain pot 3 level	218D3479 Sh 4	HRSG	DI
351	11LCA20AA251	LP econom bypass temp CV	218D3479 Sh 5	HRSG	DI x AO
351	11LCA40AA251	LP econom recirc pump disch CV	218D3479 Sh 5	HRSG	DI x AO

303	11LBA50AA251	IP superhtr to reheater IV	218D3479 Sh 4	HRSG	DO x AO
304	11LAE70AA251	HP desuperhtr wtr supply CV	218D3479 Sh 3	HRSG	DO x DI x AO
304	11LAF50AA251	RH desprhtr water line supply CV	218D3479 Sh 4	HRSG	DO x DI x AO
400	11HAC70AA301	HP econom vent MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
400	11HAD50AA301	IP drum start-up blowdown MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV
400	11HAD70AA301	HP drum continuous blowdown MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
400	11HAD70AA302	HP drum start-up blowdown MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
400	11HAJ50AA301	Rhd steam 2/2 after attemp dr MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV
400	11HAJ50AA302	Rhd steam 1/2 after attemp dr MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV
400	11HAJ50AA303	Rhd steam 1/2 bfr attemp dr MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV
400	11HAJ50AA304	Rhd steam 2/2 bfr attemp dr MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV
400	11LBA50AA301	IP steam to cold reheater MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV
400	11LBB50AA301	HRH steam line to IPT dr pot MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV
450	11HAH70AA301	HP sprhtr 3/3 dr to blwdwn tk MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
450	11HAH70AA302	HP sphtr aft attemp drn blwdwn MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
450	11HAH70AA303	HP sphtr aft attemp drn blwdwn MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
450	11HAH70AA304	HP sprhtr 1/3 drn to blwdwn tk MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
500	11HAN91AP001	Normal blowdown pump 1	496-11-DT-M-11100 Sh 1	HRSG Drains System	2DI x 2DO
500	11HAN92AP001	Normal blowdown pump 2	496-11-DT-M-11100 Sh 1	HRSG Drains System	2DI x 2DO
110	11HAN20CL001A	Intermitent blowdown tank level	496-11-DT-M-11100 Sh 1	HRSG Drains System	AI
110	11HAN20CL001B	Intermitent blowdown tank level	496-11-DT-M-11100 Sh 1	HRSG Drains System	AI
110	11HAN93CP001	Normal blowndown pmps disch pres	496-11-DT-M-11100 Sh 1	HRSG Drains System	AI
147	11HAN20CT001A	Intermitent blowdown tank temp	496-11-DT-M-11100 Sh 1	HRSG Drains System	AI (TC-E)
147	11HAN20CT001B	Intermitent blowdown tank temp	496-11-DT-M-11100 Sh 1	HRSG Drains System	AI (TC-E)
147	11HAN97CT001	NBD drains to effluent basin temp	496-11-DT-M-11100 Sh 1	HRSG Drains System	AI (TC-E)
302	11HAN80AA201	IBD tk disch plant drs attempn CV	496-11-DT-M-11100 Sh 1	HRSG Drains System	AO
302	11HAN81AA201	Intmt blowdown tk attemperation CV	496-11-DT-M-11100 Sh 1	HRSG Drains System	AO
302	11HAN93AA201	Intmt blowdown tank level CV	496-11-DT-M-11100 Sh 1	HRSG Drains System	AO
400	11HAN93AA301	NBD drs to effluent basin isol MOV	496-11-DT-M-11100 Sh 1	HRSG Drains System	PROFIBUS MOV
400	11HAN94AA301	NBD drs to clg twr basin isol MOV	496-11-DT-M-11100 Sh 1	HRSG Drains System	PROFIBUS MOV
1009	11SAA10GH001	HVAC sytem	496-11-DT-M-15300 Sh 1	HVAC System	4DI
159	11GMB03CL301	Sewage trtmt pit level	496-11-DT-M-14500 Sh 2	Plant Drains System	3DI
159	11GMB06CL301	Fuel oil stor pit level	496-11-DT-M-14500 Sh 2	Plant Drains System	3DI
500	11GMB03AP001	Sewage treatment plant sump pump 1	496-11-DT-M-14500 Sh 2	Plant Drains System	2DI x 2DO
500	11GMB03AP002	Sewage treatment plant sump pump 2	496-11-DT-M-14500 Sh 2	Plant Drains System	2DI x 2DO

500	11GMB06AP001	Fuel Oil storage area sump pump 1	496-11-DT-M-14500 Sh 2	Plant Drains System	2DI x 2DO
500	11GMB06AP002	Fuel Oil storage area sump pump 2	496-11-DT-M-14500 Sh 2	Plant Drains System	2DI x 2DO
1044	11QU_10CQ001	LP drum wtr cationic conductivity	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_10CQ006	LP drum water pH	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_11CQ003	IP drum blowdown spec conductivity	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_11CQ006	IP drum blowdown pH	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_12CQ003	HP drum blowdown spec conductivity	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_12CQ005	HP drum blowdown sodium	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_12CQ006	HP drum blowdown pH	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_13CQ001	LP sat steam cationic conductivity	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_14CQ001	IP sat steam cationic conductivity	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_15CQ001	HP sat steam cationic conductivity	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_15CQ004	HP saturated steam silicon dioxide	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_16CQ001	Reheat steam cationic conductivity	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_16CQ005	Reheat steam sodium	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_17CQ001	HP superheated steam cationic cndt	496-11-DT-M-14300 Sh 1	Sampling System	AI
1044	11QU_21CQ003	Aux boiler water spec conductivity	496-11-DT-M-14300 Sh 2	Sampling System	AI
1044	11QU_21CQ006	Aux boiler water pH	496-11-DT-M-14300 Sh 2	Sampling System	AI
1044	11QU_22CQ001	Aux boiler steam cationic cndt	496-11-DT-M-14300 Sh 2	Sampling System	AI
1044	11QU_30CQ003	Mkup dmnrld wtr spec cndt	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_30CQ004	Mkup dmnrld wtr silicon dioxide	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_31CQ003	Cond make-up wtr spec conductivity	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_31CQ006	Condenser make-up water pH	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_32CQ001	Cnds pmps discharge cationic cndt	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_32CQ002	Condensate pumps discharge O2	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_32CQ005	Condensate pumps discharge sodium	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_33CQ001	LP economizer inl cationic cndt	496-11-DT-M-14300 Sh 3	Sampling System	AI
1044	11QU_33CQ006	LP economizer inlet pH	496-11-DT-M-14300 Sh 3	Sampling System	AI
147	11MAW01CT001	Electric Heater temp	496-11-DT-M-11200 Sh 1	Seal Steam System	AI (TC-E)
147	11MAW01CT004A	Electric heater out steam temp	496-11-DT-M-11200 Sh 1	Seal Steam System	AI (TC-E)
147	11MAW01CT004B	Electric heater out steam temp	496-11-DT-M-11200 Sh 1	Seal Steam System	AI (TC-E)
167	11MAW01CL301	Aux st header drn pot lvl	496-11-DT-M-11200 Sh 1	Seal Steam System	DI
300	11MAW01AA203	Aux steam to condensate rcvr IV	496-11-DT-M-11200 Sh 1	Seal Steam System	2DI x DO
300	11MAW01AA204	Aux steam to LP steam header IV	496-11-DT-M-11200 Sh 1	Seal Steam System	2DI x DO
300	11MAW01AA205	Aux steam to condensate rcvr IV	496-11-DT-M-11200 Sh 1	Seal Steam System	2DI x DO
500	11MAL31AP001	Condensate receiver drain pump	496-11-DT-M-11200 Sh 1	Seal Steam System	2DI x 2DO

990	11MAW01AC001	Electric heater	496-11-DT-M-11200 Sh 2	Seal Steam System	2AO x 2DI x 2DO
1051	11MAW01CF001	Electric heater outlet steam flow	496-11-DT-M-11200 Sh 1	Seal Steam System	AI
110	11LBB50CP001A	HRH pressure	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI
110	11LBB50CP001B	HRH pressure	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI
110	11MAP10CP001A	LP dump tube pres	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11MAP10CP001B	LP dump tube pres	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11MAP20CP001B	Hot reheat dump tube pressure	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI
110	11MAP30CP001A	HP bypass discharge pressure	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
110	11MAP30CP001B	HP bypass discharge pressure	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
147	11MAP10CT001A	LP bypass discharge temperature	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI (TC-E)
147	11MAP10CT001B	LP bypass discharge temperature	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI (TC-E)
147	11MAP20CT001A	Hot reheat bypass disch temp	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI (TC-E)
147	11MAP20CT001B	Hot reheat bypass disch temp	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI (TC-E)
147	11MAP20CT001C	Hot reheat bypass disch temp	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI (TC-E)
147	11MAP30CT001A	HP bypass discharge temperature	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI (TC-E)
147	11MAP30CT001B	HP bypass discharge temperature	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI (TC-E)
147	11MAP30CT001C	HP bypass discharge temperature	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI (TC-E)
300	11LBG20AA202	LP steam cooling bypass IV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	2DI x DO
303	11LBG20AA201	LP steam cooling CV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DO x AO
350	11MAN10AA201	LP By-pass Valve	496-11-DT-M-10200 Sh 4	Steam & Bypass System	2AI x AO x DO
350	11MAN20AA201	HRH By-pass Valve	496-11-DT-M-10200 Sh 2	Steam & Bypass System	2AI x AO x DO
350	11MAN30AA201	HP By-pass Valve	496-11-DT-M-10200 Sh 1	Steam & Bypass System	2AI x AO x DO
351	11LCE10AA202	LP by-pass attemp water CV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DI x AO
351	11LCE20AA202	IP by-pass attemp water CV	496-11-DT-M-10200 Sh 2	Steam & Bypass System	DI x AO
400	11LCE10AA301	LP bypass attemperation MOV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	PROFIBUS MOV
400	11LCE20AA301	HRH bypass attemperation MOV	496-11-DT-M-10200 Sh 2	Steam & Bypass System	PROFIBUS MOV
1016	11LAC10AV001	FWP1 speed variator	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI x AO
1016	11LAC20AV001	FWP2 speed variator	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI x AO
1051	11LCE10CF001	LP bypass attemperation flow	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
1051	11LCE20CF001	IP bypass attemperation flow	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI
110	11MAL31CL001A	Condenser receiver tank level	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	AI
110	11MAL31CL001B	Condenser receiver tank level	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	AI
110	11MAL31CL001C	Condenser receiver tank level	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	AI
110	11MAL31CP001	Cond receiver dr pmp inl press	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	AI
110	11MAL60CL001	Condenser expansion tank level	496-11-DT-M-11300 Sh 2	Steam Turbine Drains System	AI
110	11MAL60CP001	Condenser expansion tank pressure	496-11-DT-M-11300 Sh 2	Steam Turbine Drains System	AI

147	11MAL31CT001	Condenser receiver tk temp	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	AI (TC-E)
147	11MAL32CT001	Condenser receiver vent temp	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	AI (TC-E)
147	11MAL65CT001	Condenser expansion tk vent temp	496-11-DT-M-11300 Sh 2	Steam Turbine Drains System	AI (TC-E)
147	11MAL66CT001	HP evacuation line attemp temp	496-11-DT-M-11300 Sh 2	Steam Turbine Drains System	AI (TC-E)
147	11MAL66CT002	HP evacuation line attemp temp	496-11-DT-M-11300 Sh 2	Steam Turbine Drains System	AI (TC-E)
301	11LCE60AA201	Condenser receiver spray water AOV	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	2DI x DO
301	11LCE60AA202	Condenser receiver attemp wtr AOV	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	2DI x DO
301	11LCE70AA201	Condenser exp tank spray water AOV	496-11-DT-M-11300 Sh 2	Steam Turbine Drains System	2DI x DO
301	11LCE71AA201	Condenser attemp water AOV	496-11-DT-M-11300 Sh 2	Steam Turbine Drains System	2DI x DO
302	11MAL30AA201	Condenser receiver level CV	496-11-DT-M-11300 Sh 1	Steam Turbine Drains System	AO

Tabla 2. SEÑALES CABINA 11CSA12

Tipo INS	Identificación señal	Descripción de la señal	PID	SISTEMA	Tipo señal
110	11HAD20CL001A	LP drum level 1	218D3479 Sh 5	HRSG	AI
110	11HAD20CL001A	LP drum level 1	218D3479 Sh 5	HRSG	AI
110	11HAD20CL001B	LP drum level 2	218D3479 Sh 5	HRSG	AI
110	11HAD20CL001C	LP drum level 3	218D3479 Sh 5	HRSG	AI
110	11HAD20CL002	LP drum level	218D3479 Sh 5	HRSG	AI
110	11HAD20CP001A	LP drum press 1	218D3479 Sh 5	HRSG	AI
110	11HAD20CP001C	LP drum press 3	218D3479 Sh 5	HRSG	AI
110	11HAD20CP002	LP drum press	218D3479 Sh 5	HRSG	AI
110	11HAD50CL001A	IP drum level 1	218D3479 Sh 4	HRSG	AI
110	11HAD50CL001B	IP drum level 2	218D3479 Sh 4	HRSG	AI
110	11HAD50CL001C	IP drum level 3	218D3479 Sh 4	HRSG	AI
110	11HAD50CL002	IP drum level	218D3479 Sh 4	HRSG	AI
110	11HAD50CP001	IP drum press 1	218D3479 Sh 4	HRSG	AI
110	11HAD50CP002A	IP drum press 1	218D3479 Sh 4	HRSG	AI
110	11HAD50CP002B	IP drum press 2	218D3479 Sh 4	HRSG	AI
110	11HAD50CP002C	IP drum press 3	218D3479 Sh 4	HRSG	AI
110	11HAD70CL001A	HP drum level 1	218D3479 Sh 3	HRSG	AI
110	11HAD70CL001B	HP drum level 2	218D3479 Sh 3	HRSG	AI
110	11HAD70CL001C	HP drum level 3	218D3479 Sh 3	HRSG	AI
110	11HAD70CL002	HP drum level	218D3479 Sh 3	HRSG	AI

110	11HAD70CP001	HP drum press	218D3479 Sh 3	HRSG	AI
110	11HAD70CP002A	HP drum press 1	218D3479 Sh 3	HRSG	AI
110	11HAD70CP002B	HP drum press 2	218D3479 Sh 3	HRSG	AI
110	11HAD70CP002C	HP drum press 3	218D3479 Sh 3	HRSG	AI
304	11HAD40AA251	LP drum pegging from IP drum CV	218D3479 Sh 5	HRSG	DI x DO x AO
304	11HAD60AA251	IP drum pegging from HP drum CV	218D3479 Sh 4	HRSG	DI x DO x AO
303	11HAC20AA251	LP drum level CV	218D3479 Sh 5	HRSG	DO x AO
303	11HAC50AA251	IP drum level CV	218D3479 Sh 4	HRSG	DO x AO
400	11HAD40AA301	LP drum pegging from IP drum MOV	218D3479 Sh 5	HRSG	PROFIBUS MOV
400	11HAD60AA301	IP drum pegging from HP drum MOV	218D3479 Sh 4	HRSG	PROFIBUS MOV

Tabla 3. SEÑALES CABINA 11CSA22

Tipo INS	Identificación señal	Descripción de la señal	PID	SISTEMA	Tipo señal
807	11LCB10CY001	CP1 vibration	496-11-DT-M-10400 Sh 1	Condensate System	2AI
1	11QJA20AA601	N2 supply pressure PCV	496-11-DT-M-13600 Sh 2	H2, CO2 & N2 Storage & Distribution System	N/A
500	11EGA20AP001	Fuel oil unloading pump 2	496-11-DT-M-13200 Sh 1	Fuel Oil System	2DI x 2DO
500	11EGC60AP001	Aux gas-oil forwarding pump 1	496-11-DT-M-13200 Sh 2	Fuel Oil System	2DI x 2DO
500	11EGC70AP001	Aux gas-oil forwarding pump 2	496-11-DT-M-13200 Sh 2	Fuel Oil System	2DI x 2DO
110	11EGA30CF001	Fuel oil flow	496-11-DT-M-13200 Sh 1	Fuel Oil System	AI
110	11EGB10CL002A	Untreated fuel oil storage tk lvl	496-11-DT-M-13200 Sh 1	Fuel Oil System	AI
110	11EGB10CL002B	Untreated fuel oil storage tk lvl	496-11-DT-M-13200 Sh 1	Fuel Oil System	AI
110	11GHA10CL001	Fire protection water tank level	496-11-DT-M-15100 Sh 1	Fire Protection System	AI
110	11GMA01CL001	GT drains tank level	496-11-DT-M-11600 Sh 2	Gas Turbine Auxiliaries	AI
300	11LAF30AA201	MS bypass attemperation AOV	496-11-DT-M-10200 Sh 1	Steam & Bypass System	2DI x DO
301	11LBC13AA201	CRH drains pot 6 IV	496-11-DT-M-10200 Sh 3	Steam & Bypass System	2DI x DO
301	11LBC14AA201	CRH drains pot 7 IV	496-11-DT-M-10200 Sh 3	Steam & Bypass System	2DI x DO
301	11LBC15AA201	CRH drains pot 8 IV	496-11-DT-M-10200 Sh 3	Steam & Bypass System	2DI x DO
301	11LBC18AA201	CRH drains pot 9 AOV	496-11-DT-M-10200 Sh 3	Steam & Bypass System	2DI x DO
301	11LBD11AA201	LP steam drain pot 10 IV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	2DI x DO
301	11LBD13AA201	LP steam drain pot 11 IV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	2DI x DO
301	11LBD14AA201	LP steam drain pot 12 IV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	2DI x DO
110	11LBA10CF001A	Main steam flow	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
110	11LBA10CF001B	Main steam flow	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI

110	11LBA10CP001A	Main steam pressure	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
110	11LBA10CP001B	Main steam pressure	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
110	11LBA10CP003A	HP steam 1 stage pressure 1	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
110	11LBA10CP003B	HP steam 1 stage pressure 2	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
110	11LBA10CP003C	HP steam 1 stage pressure 3	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
110	11LBC12CP001A	HP ST CRH line press 1	496-11-DT-M-10200 Sh 3	Steam & Bypass System	AI
110	11LBC12CP001B	HP ST CRH line press 2	496-11-DT-M-10200 Sh 3	Steam & Bypass System	AI
807	11LCB20CY001	CP2 vibration	496-11-DT-M-10400 Sh 1	Condensate System	2AI
300	11GHC88AA202	Condensate filling line CV	496-11-DT-M-10400 Sh 2	Condensate System	2DI x DO
300	11LCP10AA201	Condenser gravity make up CV	496-11-DT-M-10400 Sh 2	Condensate System	2DI x DO
300	11LCP20AA201	Cond Altnv mkup pmp disch CV	496-11-DT-M-10400 Sh 2	Condensate System	2DI x DO
301	11LCA45AA201	Water curtain CV	496-11-DT-M-10400 Sh 1	Condensate System	2DI x DO
110	11LCA10CP001	Condensate pump 1 suction fiter DP	496-11-DT-M-10400 Sh 1	Condensate System	AI
110	11LCA20CP001	Condensate pump 2 suction fiter DP	496-11-DT-M-10400 Sh 1	Condensate System	AI
110	11LCA30CF001B	Gland steam outlet flow	496-11-DT-M-10400 Sh 1	Condensate System	AI
110	11LCA30CP001	Condenser pumps disch pressure	496-11-DT-M-10400 Sh 1	Condensate System	AI
110	11LCP01CL002A	Condensate storage tank level	496-11-DT-M-10400 Sh 2	Condensate System	AI
500	11PAB80AP001	Water box priming pump	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	2DI x 2DO
500	11PAB90AP001	Water box priming pump	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	2DI x 2DO
500	11MAJ10AP001	Vacuum pump 1	496-11-DT-M-12400 Sh 2	Condenser Vacuum System	2DI x 2DO
500	11MAJ10AP002	Vacuum pmp 1 seal pump	496-11-DT-M-12400 Sh 2	Condenser Vacuum System	2DI x 2DO
500	11MAJ20AP001	Vacuum pump 2	496-11-DT-M-12400 Sh 3	Condenser Vacuum System	2DI x 2DO
300	11PAB83AA201	sep 1 Wtr box priming pmp inl AOV	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	2DI x DO
110	11PCB00CP001	OC booster pump inlet pressure	496-11-DT-M-12150 Sh 1	Open Cooling Water System	AI
110	11PCB01CP001	OC cooling pump disch pressure	496-11-DT-M-12150 Sh 1	Open Cooling Water System	AI
110	11PCB30CP001	OC booster pump filter 1 DP	496-11-DT-M-12150 Sh 1	Open Cooling Water System	AI
110	11PCB30CP002	OC booster pump filter 2 DP	496-11-DT-M-12150 Sh 1	Open Cooling Water System	AI
110	11PCB40CP001	Heat exchangers clng wtr inl pres	496-11-DT-M-12150 Sh 1	Open Cooling Water System	AI
110	11PGB01CL001A	Suge tank level	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI
110	11PGB01CL001B	Suge tank level	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI
110	11PGB01CL001C	Suge tank level	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI
110	11PGB10CP001	CCCW pump 1 disch pressure	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI
110	11PGB10CP002	CCCW pump 1 filter DP	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI
110	11PGB20CP001	CCCW pump 2 disch pressure	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI

110	11PGB20CP002	CCCW pump 2 filter DP	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI
110	11PGB40CP003	CCCW heat exchangers out pressure	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI
301	11QLB12AA201	Auxiliary steam pot 2 drain IV	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	2DI x DO
110	11LCP01CL002B	Condensate storage tank level	496-11-DT-M-10400 Sh 2	Condensate System	AI
301	11QLB13AA201	Auxiliary steam pot 1 drain IV	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	2DI x DO
147	11GHA10CT001	Fire protection water tk temp	496-11-DT-M-15100 Sh 1	Fire Protection System	AI (TC-E)
110	11LBC12CP001C	HP ST CRH line press 3	496-11-DT-M-10200 Sh 3	Steam & Bypass System	AI
110	11LBD10CF001A	HRSG outlet LP steam flow	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11LBD10CF001B	HRSG outlet LP steam flow	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11LBD10CP001A	HRSG outlet LP steam pressure	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11LBD10CP001B	HRSG outlet LP steam pressure	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11LBD10CP002	LP steam admission pressure	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11LBD10CP007A	Condenser to LP ST DP	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
110	11LBD10CP007B	Condenser to LP ST DP	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI
1051	11LAF30CF001	HP bypass attemperation flow	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI
147	11LBA10CT002	Main steam temperature	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI (TC-E)
147	11LBA12CT001	Main steam drain pot 1 temp	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI (TC-E)
301	11LBD20AA202	LP superhtr outlet vent AOV	218D3479 Sh 5	HRSG	2DI x DO
110	11LCP20CP002	Alternative make-up pmp disch pres	496-11-DT-M-10400 Sh 2	Condensate System	AI
110	11MAG01CL001A	Condenser level	496-11-DT-M-10400 Sh 1	Condensate System	AI
110	11MAG01CL001B	Condenser level	496-11-DT-M-10400 Sh 1	Condensate System	AI
110	11MAG01CL001C	Condenser level	496-11-DT-M-10400 Sh 1	Condensate System	AI
110	11QLB10CP004	Sparging steam pressure	496-11-DT-M-10400 Sh 1	Condensate System	AI
1051	11GHC88CF001	Demin water make-up flow	496-11-DT-M-10400 Sh 2	Condensate System	AI
804	11LCB10CT001	CP1 temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (PT-100)
804	11LCB20CT001	CP2 temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (PT-100)
300	11PAB93AA201	sep 2 Wtr box priming pmp inl AOV	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	2DI x DO
301	11PAB80AA201	Wtr boxes priming pump 1 inlet AOV	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	2DI x DO
301	11PAB90AA201	Wtr boxes priming pump 2 inlet AOV	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	2DI x DO
1045	11PAH30GH001	Condenser cleaning system	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	6DI x 3DO
147	11PGB40CT001	CCCW heat exchangers out temp	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI (TC-E)
147	11PGB50CT011	CCCW pumps inlet temperature	496-11-DT-M-12200 Sh 1	Close Cooling Water System	AI (TC-E)
110	11QLB10CP002	Auxiliary steam pressure	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	AI
110	11QLB50CP001	IP Saturated steam pressure	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	AI

500	11MAJ20AP002	Vacuum pmp 2 seal pump	496-11-DT-M-12400 Sh 3	Condenser Vacuum System	2DI x 2DO
301	11MAJ10AA201	Vacuum pump 1 make-up AOV	496-11-DT-M-12400 Sh 2	Condenser Vacuum System	2DI x DO
110	11MAG01CL009	Upper water box outlet level	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	AI
110	11MAG01CL010	Upper water box outlet level	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	AI
159	11GMA05CL301	Cond pmp sump pit level	496-11-DT-M-14500 Sh 1	Plant Drains System	3DI
159	11GMB04CL301	Xfmr sump pit level	496-11-DT-M-14500 Sh 2	Plant Drains System	3DI
147	11LBA13CT001	Main steam drain pot 2 temp	496-11-DT-M-10200 Sh 1	Steam & Bypass System	AI (TC-E)
147	11LBB11CT001	Hot reheat drain pot 3 temp	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI (TC-E)
147	11LBB21CT001	Hot reheat drain pot 4 temp	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI (TC-E)
147	11LBB31CT001	Hot reheat drain pot 5 temp	496-11-DT-M-10200 Sh 2	Steam & Bypass System	AI (TC-E)
147	11LBC10CT001A	CRH steam temp	496-11-DT-M-10200 Sh 3	Steam & Bypass System	AI (TC-E)
147	11LBC10CT001B	CRH steam temp	496-11-DT-M-10200 Sh 3	Steam & Bypass System	AI (TC-E)
147	11LBC10CT001C	CRH steam temp	496-11-DT-M-10200 Sh 3	Steam & Bypass System	AI (TC-E)
301	11LBD20AA203	LP superhtr outlet steam drain AOV	218D3479 Sh 5	HRSG	2DI x DO
147	11LBD20CT001	LP superheater outlet temperature	218D3479 Sh 5	HRSG	AI (TC-E)
301	11MAJ20AA201	Vacuum pump 2 make-up AOV	496-11-DT-M-12400 Sh 2	Condenser Vacuum System	2DI x DO
110	11MAG01CP001A	Condenser pressure	496-11-DT-M-12400 Sh 1	Condenser Vacuum System	AI
110	11PAB01CP001	wtr boxes priming vacuum tk press	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	AI
1051	11QLB50CF001	IP Saturated steam flow	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	AI
147	11QLB10CT002	Auxiliary steam temperature	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	AI (TC-E)
147	11QLB50CT001	IP Saturated steam temperature	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	AI (TC-E)
302	11QLB50AA201	IP saturated steam to aux steam CV	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	AO
147	11LCA30CT001	Condenser pumps disch temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
300	11GHC89AA201	Make-up demin water to surge tk CV	496-11-DT-M-12200 Sh 1	Close Cooling Water System	2DI x DO
147	11LBD10CT001	HRSG outlet LP steam temperature	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI (TC-E)
147	11LCA30CT003	Gland steam outlet temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
147	11MAG01CT001A	Condenser temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
147	11PAB31CT002	Upper water box inlet temperature	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	AI (TC-E)
147	11PAB31CT005	Upper water box outlet temperature	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	AI (TC-E)
147	11LBD10CT003	LP steam admission temperature	496-11-DT-M-10200 Sh 4	Steam & Bypass System	AI (TC-E)
167	11LBC13CL301	CRH drain pot 6 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI
167	11LBC14CL301	CRH drain pot 7 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI
167	11LBC15CL301	CRH drain pot 8 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI
167	11LBC18CL301	CRH drain pot 9 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI

167	11LBD11CL301	CRH drain pot 10 level	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DI
167	11LBD13CL301	CRH drain pot 11 level	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DI
167	11LBD20CL301	LP shd out dr pot no hi lvl	218D3479 Sh 5	HRSG	DI
167	11LBD20CL302	LP superhtd out dr pot no hh lvl	218D3479 Sh 5	HRSG	DI
147	11MAG01CT001B	Condenser temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
110	11MAG01CP001B	Condenser pressure	496-11-DT-M-12400 Sh 1	Condenser Vacuum System	AI
110	11MAG01CP001C	Condenser pressure	496-11-DT-M-12400 Sh 1	Condenser Vacuum System	AI
147	11PAB32CT002	Lower water box inlet temperature	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	AI (TC-E)
147	11PAB32CT005	Lower water box outlet temperature	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	AI (TC-E)
167	11QLB12CL301	Auxiliary steam drain pot 2 LS	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	DI
167	11QLB12CL302	Auxiliary steam drain pot 2 LS	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	DI
110	11EGB20CL002A	Treated fuel oil storage tk level	496-11-DT-M-13200 Sh 2	Fuel Oil System	AI
147	11MAG01CT001C	Condenser temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
167	11QLB13CL301	Auxiliary steam drain pot 3 LS	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	DI
147	11MAG01CT002A	Condenser temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
147	11MAG01CT002B	Condenser temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
167	11LBD14CL301	CRH drain pot 12 level	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DI
147	11MAG01CT002C	Condenser temperature	496-11-DT-M-10400 Sh 1	Condensate System	AI (TC-E)
1049	11LBC13CL302	CRH drain pot 6 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI
1049	11LBC14CL302	CRH drain pot 7 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI
400	11LBA70AA302	Main steam vent to silencer MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
400	11LBA70AA311	MS bfr fl nozzle bypass isol MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
1049	11LBC15CL302	CRH drain pot 8 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI
1049	11LBC18CL302	CRH drain pot 9 level	496-11-DT-M-10200 Sh 3	Steam & Bypass System	DI
1049	11LBD11CL302	CRH drain pot 10 level	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DI
1049	11LBD13CL302	CRH drain pot 11 level	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DI
1049	11LBD14CL302	CRH drain pot 12 level	496-11-DT-M-10200 Sh 4	Steam & Bypass System	DI
304	11LAF30AA202	MS bypass attemperation CV	496-11-DT-M-10200 Sh 1	Steam & Bypass System	DI x DO x AO
152	11MAJ10CF301	Vacuum pump 1 seal wtr flow switch	496-11-DT-M-12400 Sh 2	Condenser Vacuum System	DI
152	11PAB81CF301	WB priming pump 1 flow switch	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	DI
152	11PAB91CF301	WB priming pump 2 flow switch	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	DI
167	11PAB01CL301	WB priming vac tk lvl switch	496-11-DT-M-12100 Sh 3	Circulating Water System (Cooling Tower)	DI
400	11PAB31AA301	Upper water box inlet isol MOV	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	PROFIBUS MOV
400	11PCB01AA301	OC cool wtr shut down pmp isol MOV	496-11-DT-M-12150 Sh 1	Open Cooling Water System	PROFIBUS MOV

400	11PCB40AA301	clg wtr heat exchr1 to CW isol MOV	496-11-DT-M-12200 Sh 1	Close Cooling Water System	PROFIBUS MOV
400	11PCB40AA302	clg wtr heat exchr2 to CW isol MOV	496-11-DT-M-12200 Sh 1	Close Cooling Water System	PROFIBUS MOV
400	11PGB40AA301	Em opn Lube Oil Coolers wtr MOV	496-11-DT-M-12200 Sh 2	Close Cooling Water System	PROFIBUS MOV
400	11PGB46AA302	Closed Circuit Cooling isol MOV	496-11-DT-M-12200 Sh 2	Close Cooling Water System	PROFIBUS MOV
400	11PGB46AA303	LO Coolers to Raw wtr tk isol MOV	496-11-DT-M-12200 Sh 2	Close Cooling Water System	PROFIBUS MOV
400	11PGB46AA304	LO Coolers to dr wtr Sys isol MOV	496-11-DT-M-12200 Sh 2	Close Cooling Water System	PROFIBUS MOV
400	11QLB10AA302	Aux steam to exchanger MOV	496-11-DT-M-11650 Sh 1	Anti-Icing System	PROFIBUS MOV
167	11QLB13CL302	Auxiliary steam drain pot 3 LS	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	DI
450	11LBA70AA303	Main steam line to HPST drain MOV	218D3479 Sh 3	HRSG	PROFIBUS MOV
110	11EGB20CL002B	Treated fuel oil storage tk level	496-11-DT-M-13200 Sh 2	Fuel Oil System	AI
110	11EGD25CP001	Aux gofps disch press	496-11-DT-M-13200 Sh 2	Fuel Oil System	AI
302	11EGD23AA201	Treated fuel oil storage tk inl CV	496-11-DT-M-13200 Sh 2	Fuel Oil System	AO
500	11GMA05AP001	Condenser pump sump pump 1	496-11-DT-M-14500 Sh 1	Plant Drains System	2DI x 2DO
500	11GMA05AP002	Condenser pump sump pump 2	496-11-DT-M-14500 Sh 1	Plant Drains System	2DI x 2DO
500	11GMB04AP001	Transformer sump pump 1	496-11-DT-M-14500 Sh 2	Plant Drains System	2DI x 2DO
500	11GMB04AP002	Transformer sump pump 2	496-11-DT-M-14500 Sh 2	Plant Drains System	2DI x 2DO
152	11MAJ20CF301	Vacuum pump 1 seal wtr flow switch	496-11-DT-M-12400 Sh 3	Condenser Vacuum System	DI
167	11MAJ10CL301	Air / Steam trap 1 level switch	496-11-DT-M-12400 Sh 2	Condenser Vacuum System	DI
167	11MAJ20CL301	Air / Steam trap 2 level switch	496-11-DT-M-12400 Sh 3	Condenser Vacuum System	DI
400	11MAJ04AA301	Vacuum Breaker Valve	496-11-DT-M-12400 Sh 1	Condenser Vacuum System	PROFIBUS MOV
400	11PAB31AA302	Upper water box outlet isol MOV	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	PROFIBUS MOV
400	11PAB32AA301	Lower water box inlet isol MOV	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	PROFIBUS MOV
500	11PCC01AP001	OC cooling water shut down pump	496-11-DT-M-12150 Sh 1	Open Cooling Water System	2DI x 2DO
302	11QLB10AA202	Sparging steam CV	496-11-DT-M-10400 Sh 1	Condensate System	AO
303	11GHC88AA201	Condenser level CV	496-11-DT-M-10400 Sh 2	Condensate System	DO x AO
303	11LCA50AA201	Condensate spill over CV	496-11-DT-M-10400 Sh 2	Condensate System	DO x AO
307	11LCA60AA201	Condensate minimum flow CV	496-11-DT-M-10400 Sh 1	Condensate System	DO x AO
400	11PAB32AA302	Lower water box outlet isol MOV	496-11-DT-M-12100 Sh 1	Circulating Water System (Cooling Tower)	PROFIBUS MOV
1047	11QCA10GH001	Chemical injection system	496-11-DT-M-14400 Sh 1	Chemical Injection System	3DI X 8DO
400	11LBA12AA301	MS before flow nozzle dr pot 1 MOV	496-11-DT-M-10200 Sh 1	Steam & Bypass System	PROFIBUS MOV
400	11LBA13AA301	MS before MSCV drain pot 2 MOV	496-11-DT-M-10200 Sh 1	Steam & Bypass System	PROFIBUS MOV
400	11LBB11AA301	HRH drain pot 3 MOV	496-11-DT-M-10200 Sh 2	Steam & Bypass System	PROFIBUS MOV
400	11LBB21AA301	HRH drain pot 4 MOV	496-11-DT-M-10200 Sh 2	Steam & Bypass System	PROFIBUS MOV
400	11LBB31AA301	HRH drain pot 5 MOV	496-11-DT-M-10200 Sh 2	Steam & Bypass System	PROFIBUS MOV

400	11LBD10AA301	LP steam to LP ST isolation MOV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	PROFIBUS MOV
400	11LBD15AA301	LP steam to cond exp tnk MOV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	PROFIBUS MOV
1050	11QJB10AA601	H2 supply AOV	496-11-DT-M-13600 Sh 1	H2, CO2 & N2 Storage & Distribution System	DI
1	11LCA80AA601	Sealing Header PCV	496-11-DT-M-10400 Sh 2	Condensate System	N/A
400	11LBD16AA301	LP steam to cond exp tnk MOV	496-11-DT-M-10200 Sh 4	Steam & Bypass System	PROFIBUS MOV
400	11QLB50AA301	Aux boiler isolation valve	496-11-DT-M-13300 Sh 2	Auxiliary Steam System	PROFIBUS MOV

Tabla 4. SEÑALES CABINA 11CSA21

Tipo INS	Identificación señal	Descripción de la señal	PID	SISTEMA	Tipo señal
600	11PCC10AP001	Open circuit booster pump 1	496-11-DT-M-12150 Sh 1	Open Cooling Water System	2DO x 2DI
600	11PCC10AP001	Open circuit booster pump 1	496-11-DT-M-12150 Sh 1	Open Cooling Water System	2DO x 2DI
600	11PGC10AP001	Closed circuit cooling wtr pump 1	496-11-DT-M-12200 Sh 1	Close Cooling Water System	2DO x 2DI
600	11PGC20AP001	Closed circuit cooling wtr pump 2	496-11-DT-M-12200 Sh 1	Close Cooling Water System	2DO x 2DI
700	11LAC10AP001	Boiler HP/IP Feedwater pump 1	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	2DO x 2DI
700	11LAC20AP001	Boiler HP/IP Feedwater pump 2	496-11-DT-M-10301 Sh 2	Feedwater System (IP/HP Interstage Bleed)	2DO x 2DI
700	11LCB10AP001	Condensate pump 1	496-11-DT-M-10400 Sh 1	Condensate System	2DO x 2DI
700	11LCB20AP001	Condensate pump 2	496-11-DT-M-10400 Sh 1	Condensate System	2DO x 2DI

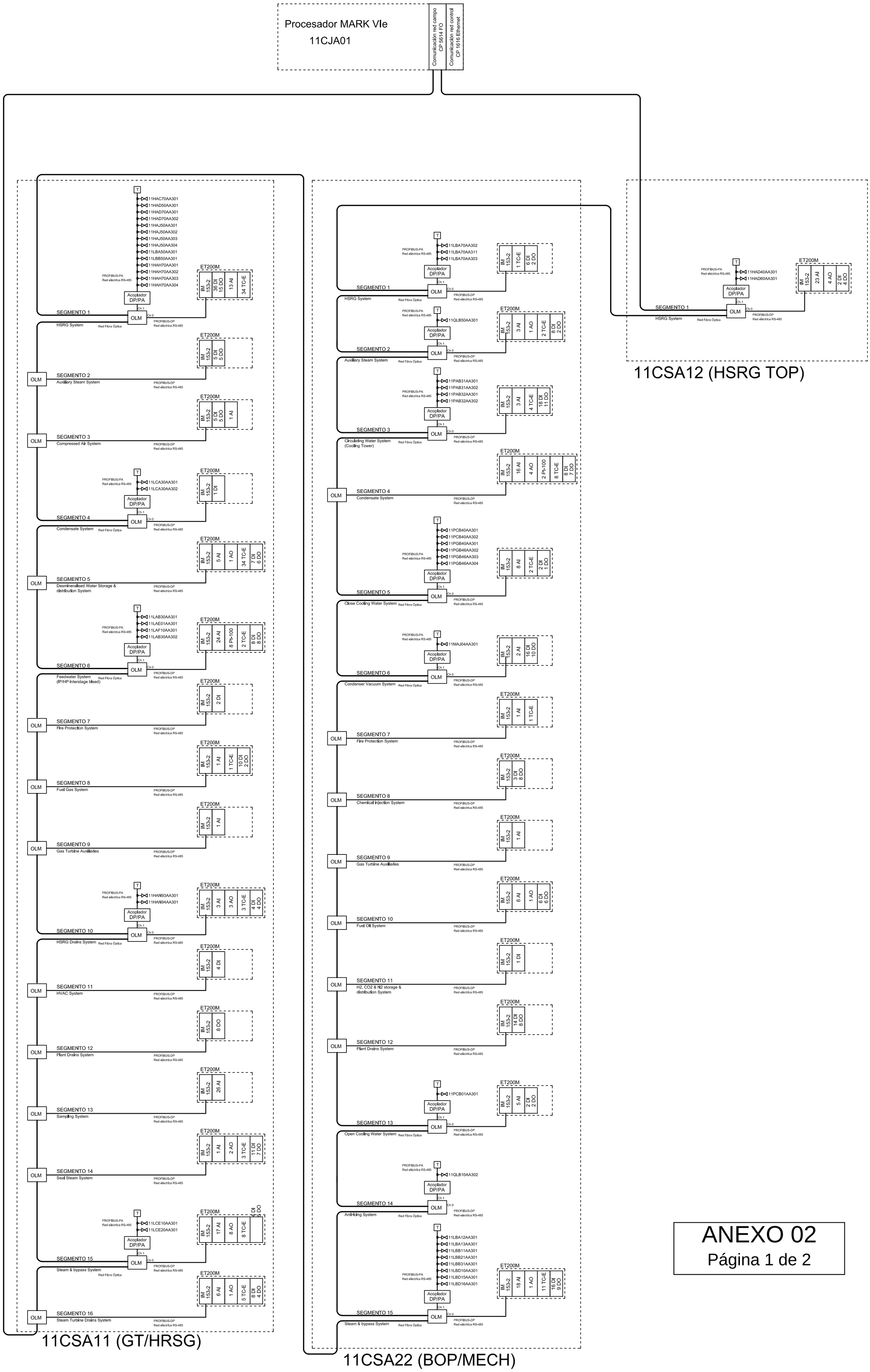
Tabla 5. SEÑALES CABINA 11CSA30

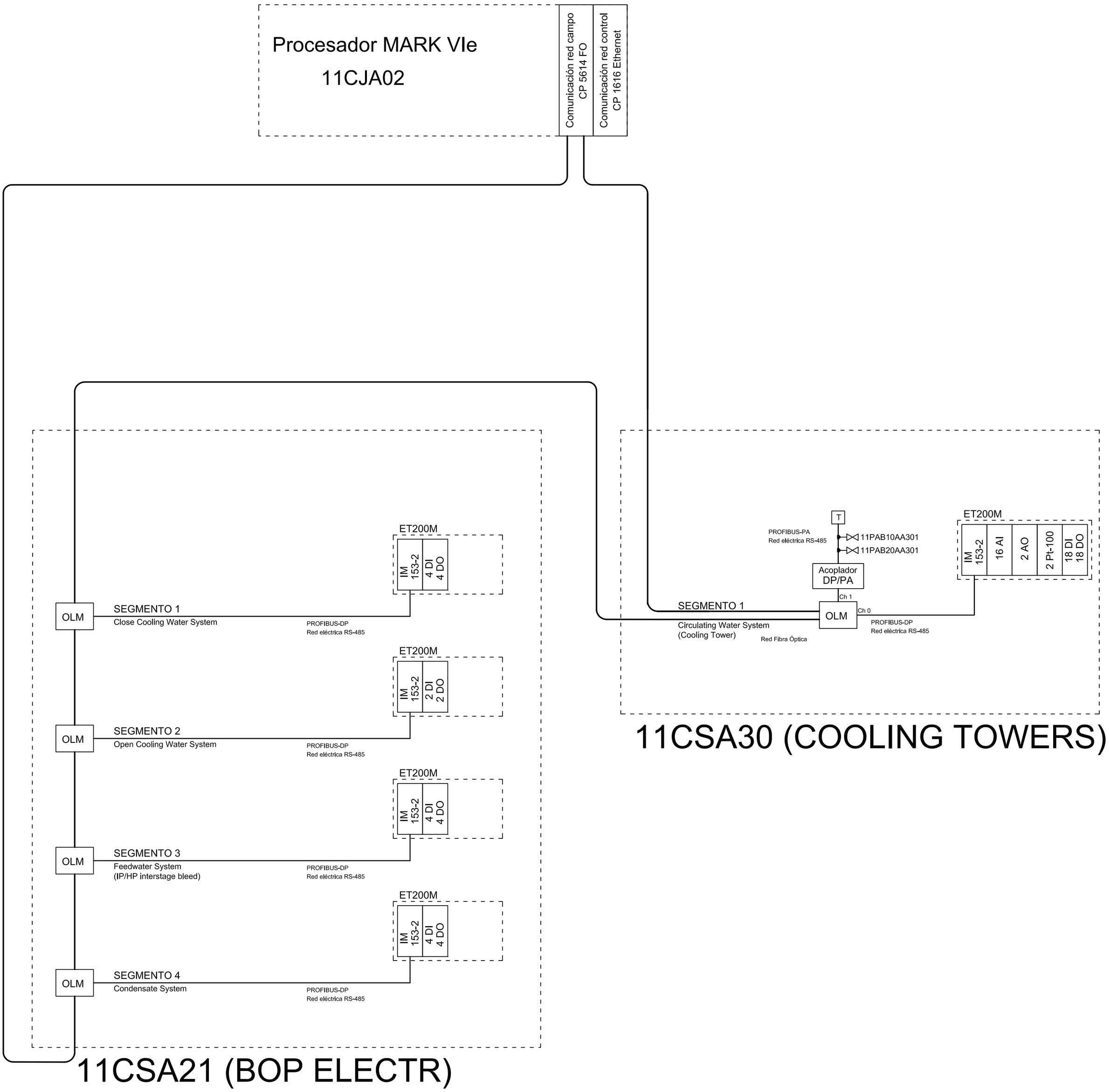
Tipo INS	Identificación señal	Descripción de la señal	PID	SISTEMA	Tipo señal
807	11PAC10CY001	CWP1 vibration	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2AI
807	11PAC20CY001	CWP2 vibration	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2AI
600	11PAE10AN001	Cooling tower fan 1	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
600	11PAE10AN002	Cooling tower fan 2	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
600	11PAE10AN003	Cooling tower fan 3	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
600	11PAE10AN004	Cooling tower fan 4	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
600	11PAE10AN005	Cooling tower fan 5	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
600	11PAE10AN006	Cooling tower fan 6	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
600	11PAE10AN007	Cooling tower fan 7	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
700	11PAC10AP001	Circulating pump 1	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
700	11PAC20AP001	Circulating pump 2	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	2DI x 2DO
110	11PAB10CP002	Circulating water pump 1 out press	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
110	11PAB20CP002	Circulating water pump 2 out press	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
110	11PAC10CL001A	CW1 water pool level	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
110	11PAC10CL001B	CW1 water pool level	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
110	11PAC20CL001A	CW2 water pool level	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
110	11PAC20CL001B	CW2 water pool level	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI

110	11PAE10CL001	Cooling towers pool level	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
1044	11PAE10CQ003A	Cooling towers pool wtr spec cond	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
1044	11PAE10CQ003B	Cooling towers pool wtr spec cond	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
1044	11PAE10CQ004	Cooling towers pool water pH	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
1044	11PAE10CQ005	Cooling towers pool water clorine	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
1044	11PAR10CQ003	CT pool wtr spec cond anal xmtr	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI
804	11PAC10CT001	CWP1 temperature	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI (PT-100)
804	11PAC20CT001	CWP2 temperature	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AI (PT-100)
302	11PAB72AA201	Cooling tower purge CV	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AO
302	11PAR10AA201	Cooling tower make up CV	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	AO
450	11PAB10AA301	Circulating pump 1 outlet isol MOV	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	PROFIBUS MOV
450	11PAB20AA301	Circulating pump 2 outlet isol MOV	496-11-DT-M-12100 Sh 2	Circulating Water System (Cooling Tower)	PROFIBUS MOV

ANEXO 2.

"Definición y topología de segmentos"


Procesador MARK VIe
11CJA01
Comunicación red campo CP 5614 FO
Comunicación red control CP 1616 Ethernet
11CSA11 (GT/HRSG)
SEGMENTO 1 HSRG System
SEGMENTO 2 Auxiliary Steam System
SEGMENTO 3 Compressed Air System
SEGMENTO 4 Condensate System
SEGMENTO 5 Desmineralised Water Storage & distribution System
SEGMENTO 6 Feedwater System (IP/HP interstage bleed)
SEGMENTO 7 Fire Protection System
SEGMENTO 8 Fuel Gas System
SEGMENTO 9 Gas Turbine Auxiliaries
SEGMENTO 10 HSRG Drains System
SEGMENTO 11 HVAC System
SEGMENTO 12 Plant Drains System
SEGMENTO 13 Sampling System
SEGMENTO 14 Seal Steam System
SEGMENTO 15 Steam & bypass System
SEGMENTO 16 Steam Turbine Drains System
11CSA22 (BOP/MECH)
SEGMENTO 1 HSRG System
SEGMENTO 2 Auxiliary Steam System
SEGMENTO 3 Circulating Water System (Cooling Tower)
SEGMENTO 4 Condensate System
SEGMENTO 5 Close Cooling Water System
SEGMENTO 6 Condenser Vacuum System
SEGMENTO 7 Fire Protection System
SEGMENTO 8 Chemical injection System
SEGMENTO 9 Gas Turbine Auxiliaries
SEGMENTO 10 Fuel Oil System
SEGMENTO 11 H2, CO2 & N2 storage & distribution System
SEGMENTO 12 Plant Drains System
SEGMENTO 13 Open Cooling Water System
SEGMENTO 14 Anti-Icing System
SEGMENTO 15 Steam & bypass System
11CSA12 (HSRG TOP)
SEGMENTO 1 HSRG System
ANEXO 02
Página 1 de 2



ANEXO 02

Página 2 de 2

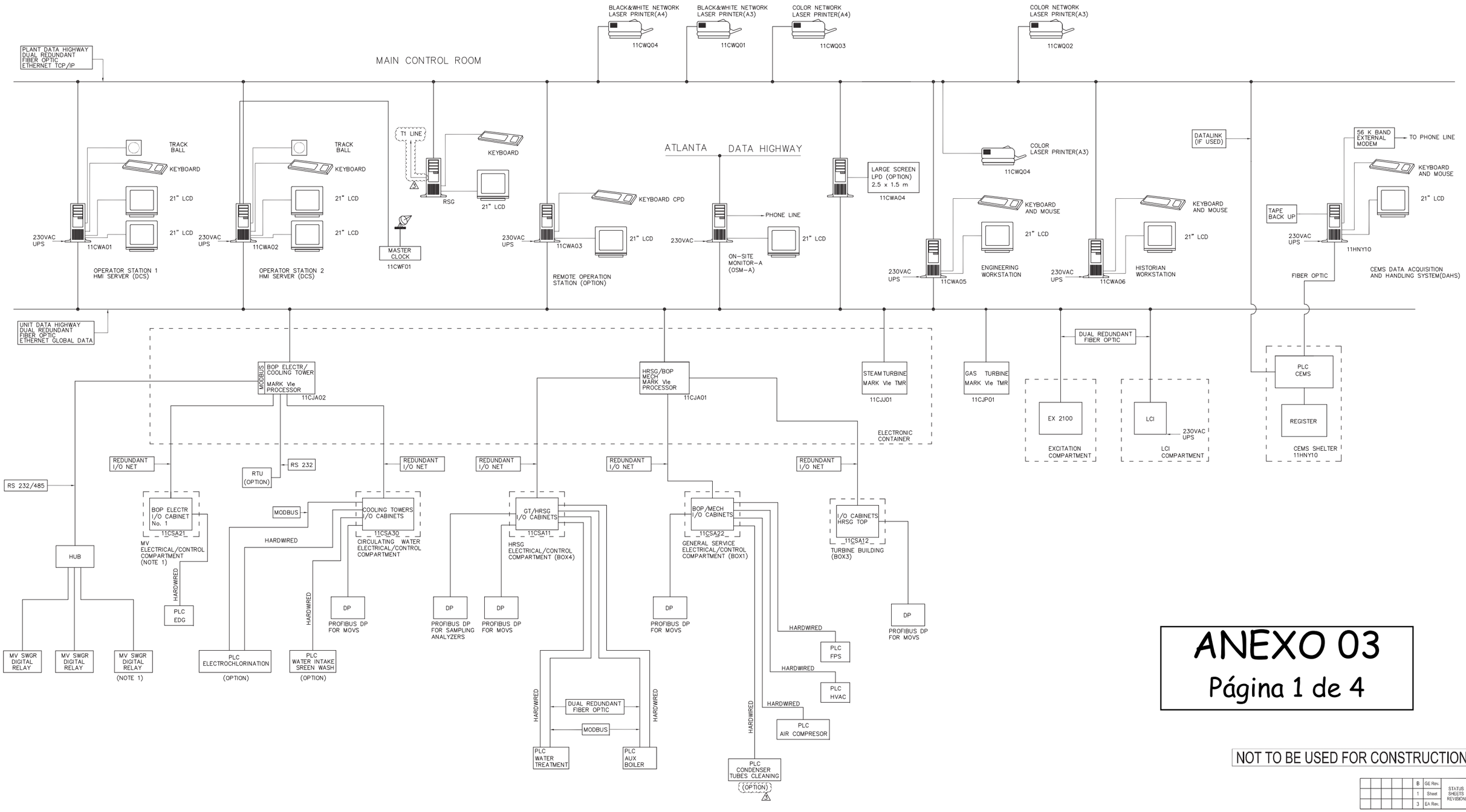
ANEXO 3.

"Disposición general de elementos de la arquitectura general de Planta Estandar de Ciclo Combinado"

REVISIONS		
EA Rev	DESCRIPTION	APPROVED/DATE
1	INFORMATION	AHA 2010-06-18
2	INFORMATION	AHA 2010-07-19
3	INFORMATION	

NOTES

1.- NUMBER OF I/O MV SWITCHGEAR DIGITAL RELAYS PENDING..



ANEXO 03

Página 1 de 4

NOT TO BE USED FOR CONSTRUCTION

B	GE Rev.	STATUS SHEETS REVISION
1	Sheet	
3	EA Rev.	

© COPYRIGHT 2010 GENERAL ELECTRIC COMPANY

PROPRIETARY INFORMATION-THIS DOCUMENT CONTAINS PROPRIETARY INFORMATION OF GENERAL ELECTRIC COMPANY AND OF EMPRESARIOS AGRUPADOS INTERNACIONAL S.A. AND MAY NOT BE USED BY OR DISCLOSED TO OTHERS, EXCEPT WITH THE WRITTEN PERMISSION OF GENERAL ELECTRIC COMPANY OR EMPRESARIOS AGRUPADOS INTERNACIONAL S.A.

EMPRESARIOS AGRUPADOS

EA DWG NO 496-11-D-I-00300

KKS DWG NO 496-11-11-CJ-YDE-EA-300

UNLESS OTHERWISE SPECIFIED
DIMENSIONS ARE IN MILLIMETERS
TOLERANCES ON:
DECIMALS ±
ANGLES ±
FRACTIONS ±

PROJECT GE STANDARD CC POWER PLANT

MADE FOR S109FB SINGLE SHAFT

SIGNATURES		DATE
DRAWN	AAB	10-09-06
CHECKED	CAB	10-09-06
PROJ ENG	FRP	10-09-06
ISSUED		
CIVIL		
ELECTRICAL		
MECHANICAL		
CONTROLS		

GE ENERGY

GENERAL ELECTRIC COMPANY
GENERAL ELECTRIC INTERNATIONAL, INC.
POWER GENERATION-POWER PLANT SYSTEMS

CONTROL SYSTEM ARCHITECTURE

FIRST MADE FOR ML-IPS#711391 MDL:R474

SIZE A0 | CAGE CODE | DWG NO 129E3625

SCALE NONE | GE Rev B | SHEET 1 OF 1

FIRST ANGLE PROJECTION

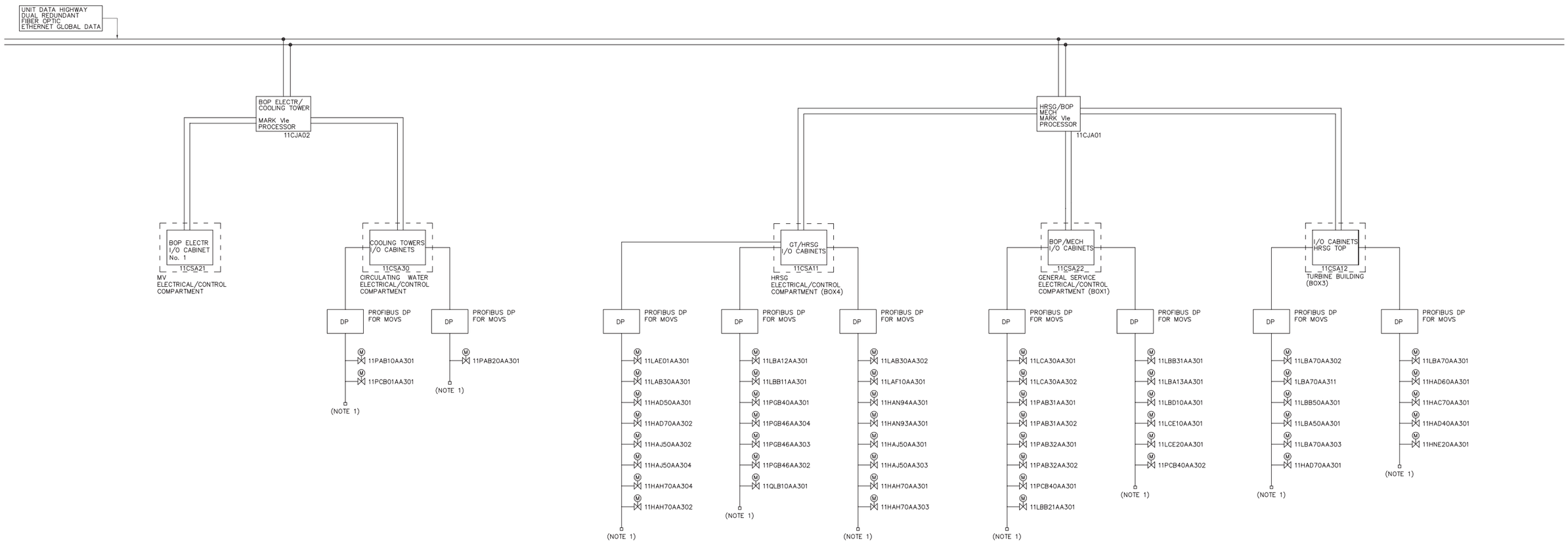
EMPRESARIOS AGRUPADOS

THIS DWG. CONTAINS INFORMATION FOR STRUCTURES, SYSTEMS OR COMPONENTS DESIGN ..... YES ☒ NO ☐

VERIFICATION: N/A ☐ HOU/SUP. ☐ VERIFIER L1 ☐ L2 ☒

496-11-D-I-00300-001-03

REVISIONS		
EA Rev	DESCRIPTION	APPROVED/DATE
1	INFORMATION	AHA 2010-06-18
2	INFORMATION	



ANEXO 03

Página 2 de 4

NOT TO BE USED FOR CONSTRUCTION

						A	GE Rev.
						1	Sheet
						2	EA Rev.

STATUS SHEETS REVISION

© COPYRIGHT 2010 GENERAL ELECTRIC COMPANY

PROPRIETARY INFORMATION–THIS DOCUMENT CONTAINS PROPRIETARY INFORMATION OF GENERAL ELECTRIC COMPANY AND OF EMPRESARIOS AGRUPADOS INTERNACIONAL S.A. AND MAY NOT BE USED BY OR DISCLOSED TO OTHERS, EXCEPT WITH THE WRITTEN PERMISSION OF GENERAL ELECTRIC COMPANY OR EMPRESARIOS AGRUPADOS INTERNACIONAL S.A.

EMPRESARIOS AGRUPADOS

EA DWG NO 496-11-DJ-00305

KKS DWG NO 496-11-CJ-YDE-EA-305

UNLESS OTHERWISE SPECIFIED
DIMENSIONS ARE IN MILLIMETERS
TOLERANCES ON:
DECIMALS ±
ANGLES ±
FRACTIONS ±

PROJECT GE STANDARD CC POWER PLANT

MADE FOR S109FB SINGLE SHAFT

SIGNATURES		DATE
DRAWN	CAB	10-07-05
CHECKED	CAB	10-07-05
PROJ ENG	FRP	10-07-05
ISSUED		
CIVIL		
ELECTRICAL		
MECHANICAL		
CONTROLS		

GE ENERGY

GENERAL ELECTRIC COMPANY
GENERAL ELECTRIC INTERNATIONAL, INC.
POWER GENERATION–POWER PLANT SYSTEMS

MOV PROFIBUS ARCHITECTURE

FIRST MADE FOR ML - IPS#711391 MDL: N836

SIZE A0 | CAGE CODE | DWG NO **238A7161**

SCALE NONE | GE Rev A | SHEET 1 OF 1

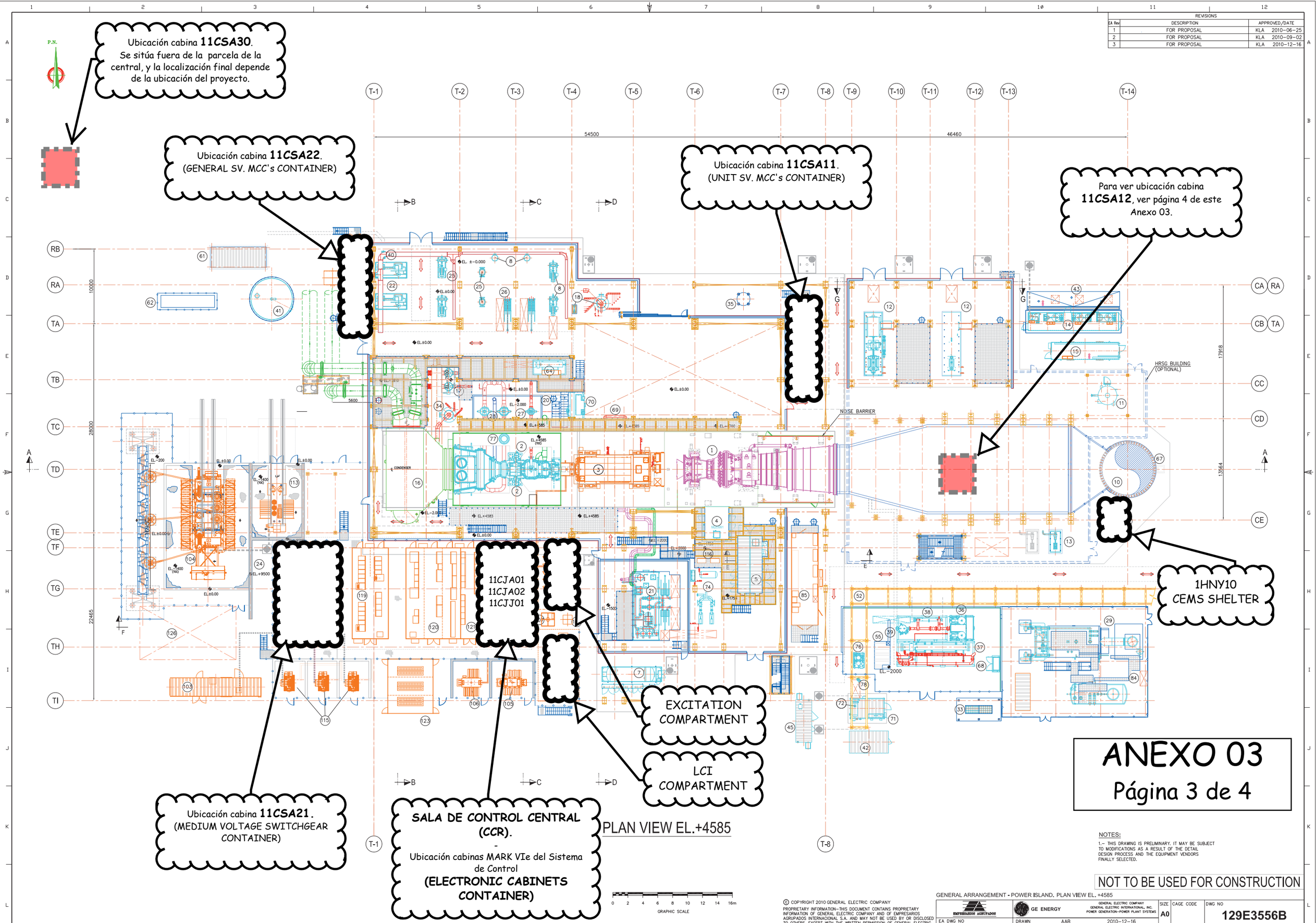
FIRST ANGLE PROJECTION

EMPRESARIOS AGRUPADOS

THIS DWG. CONTAINS INFORMATION FOR STRUCTURES, SYSTEMS OR COMPONENTS DESIGN ..... YES ☐ NO ☒
VERIFICATION: N/A ☐ HOU/SUP. ☒ VERIFIER L1 ☐ L2 ☐

496-11-D-I-00305-001-02

REVISIONS		
EA Rev	DESCRIPTION	APPROVED/DATE
1	FOR PROPOSAL	KLA 2010-06-25
2	FOR PROPOSAL	KLA 2010-09-02
3	FOR PROPOSAL	KLA 2010-12-16



ANEXO 03

Página 3 de 4

NOTES:

1.- THIS DRAWING IS PRELIMINARY. IT MAY BE SUBJECT TO MODIFICATIONS AS A RESULT OF THE DETAIL DESIGN PROCESS AND THE EQUIPMENT VENDORS FINALLY SELECTED.

NOT TO BE USED FOR CONSTRUCTION

GENERAL ARRANGEMENT - POWER ISLAND. PLAN VIEW EL. +4585

© COPYRIGHT 2010 GENERAL ELECTRIC COMPANY
PROPRIETARY INFORMATION-THIS DOCUMENT CONTAINS PROPRIETARY INFORMATION OF GENERAL ELECTRIC COMPANY AND OF EMPRESARIOS AGRUPADOS INTERNACIONAL S.A. AND MAY NOT BE USED BY OR DISCLOSED TO OTHERS, EXCEPT WITH THE WRITTEN PERMISSION OF GENERAL ELECTRIC COMPANY OR EMPRESARIOS AGRUPADOS INTERNACIONAL S.A.

EMPRESARIOS AGRUPADOS
EA DWG NO 496-11-D-M-00601B

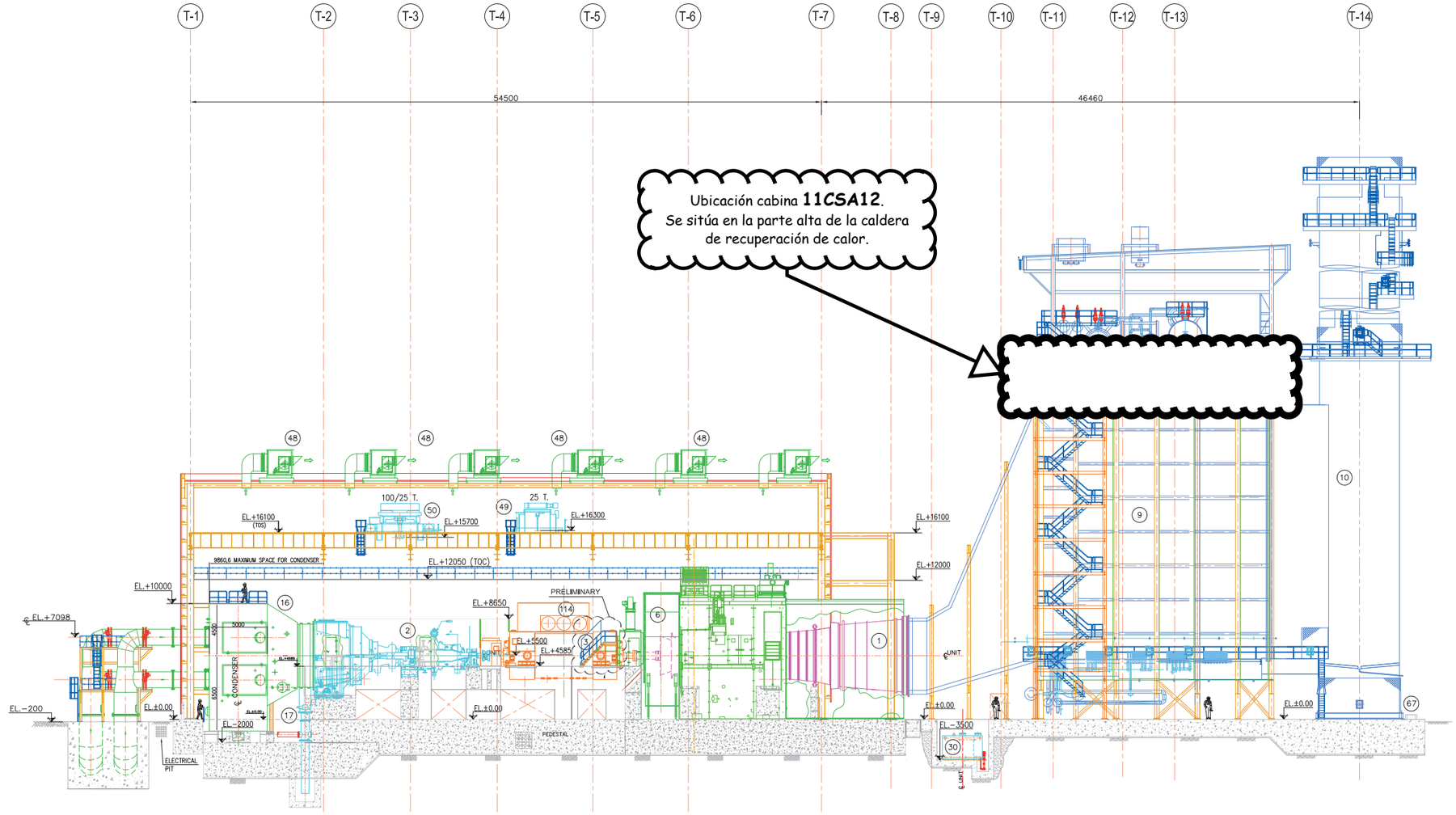
GE ENERGY
GENERAL ELECTRIC COMPANY
GENERAL ELECTRIC INTERNATIONAL, INC.
POWER GENERATION-POWER PLANT SYSTEMS

DRAWN	AAB	2010-12-16	
ISSUED	AZJ	2010-12-16	

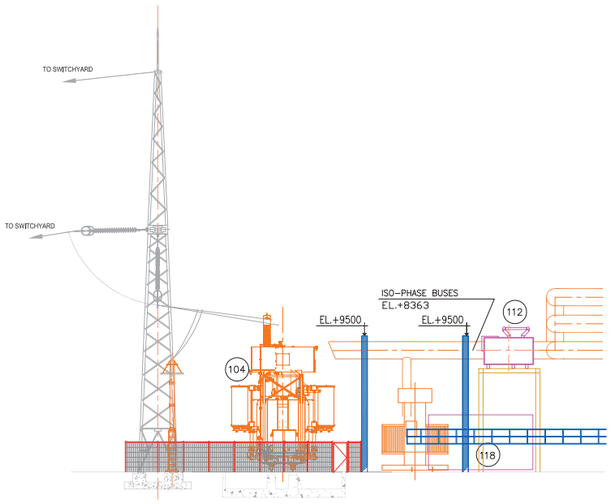
SIZE A0 | CAGE CODE | DWG NO 129E3556B
SCALE 1/150 | GE Rev B | SHEET 3 OF 8

496-11-D-M-00601B-003-02

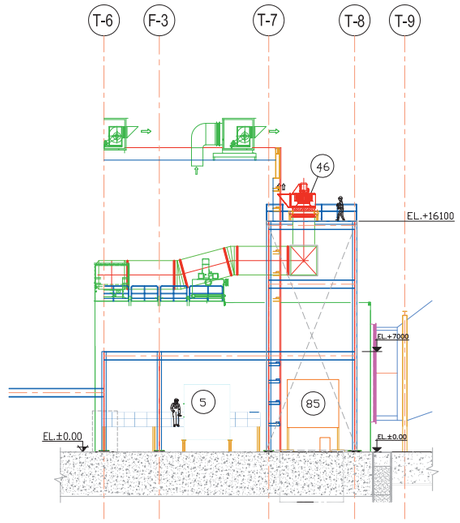
REVISIONS		
EA Rev	DESCRIPTION	APPROVED/DATE
1	FOR PROPOSAL	KLA 2010-06-25
2	FOR PROPOSAL	KLA 2010-09-02
3	FOR PROPOSAL	KLA 2010-12-16



SECTION A-A



SECTION F-F



SECTION E-E

ANEXO 03

Página 4 de 4

NOTES:

1.- THIS DRAWING IS PRELIMINARY. IT MAY BE SUBJECT TO MODIFICATIONS AS A RESULT OF THE DETAIL DESIGN PROCESS AND THE EQUIPMENT VENDORS FINALLY SELECTED.

NOT TO BE USED FOR CONSTRUCTION

© COPYRIGHT 2010 GENERAL ELECTRIC COMPANY
PROPRIETARY INFORMATION-THIS DOCUMENT CONTAINS PROPRIETARY INFORMATION OF GENERAL ELECTRIC COMPANY AND OF EMPRESARIOS AGRUPADOS INTERNACIONAL S.A. AND MAY NOT BE USED BY OR DISCLOSED TO OTHERS, EXCEPT WITH THE WRITTEN PERMISSION OF GENERAL ELECTRIC COMPANY OR EMPRESARIOS AGRUPADOS INTERNACIONAL S.A.

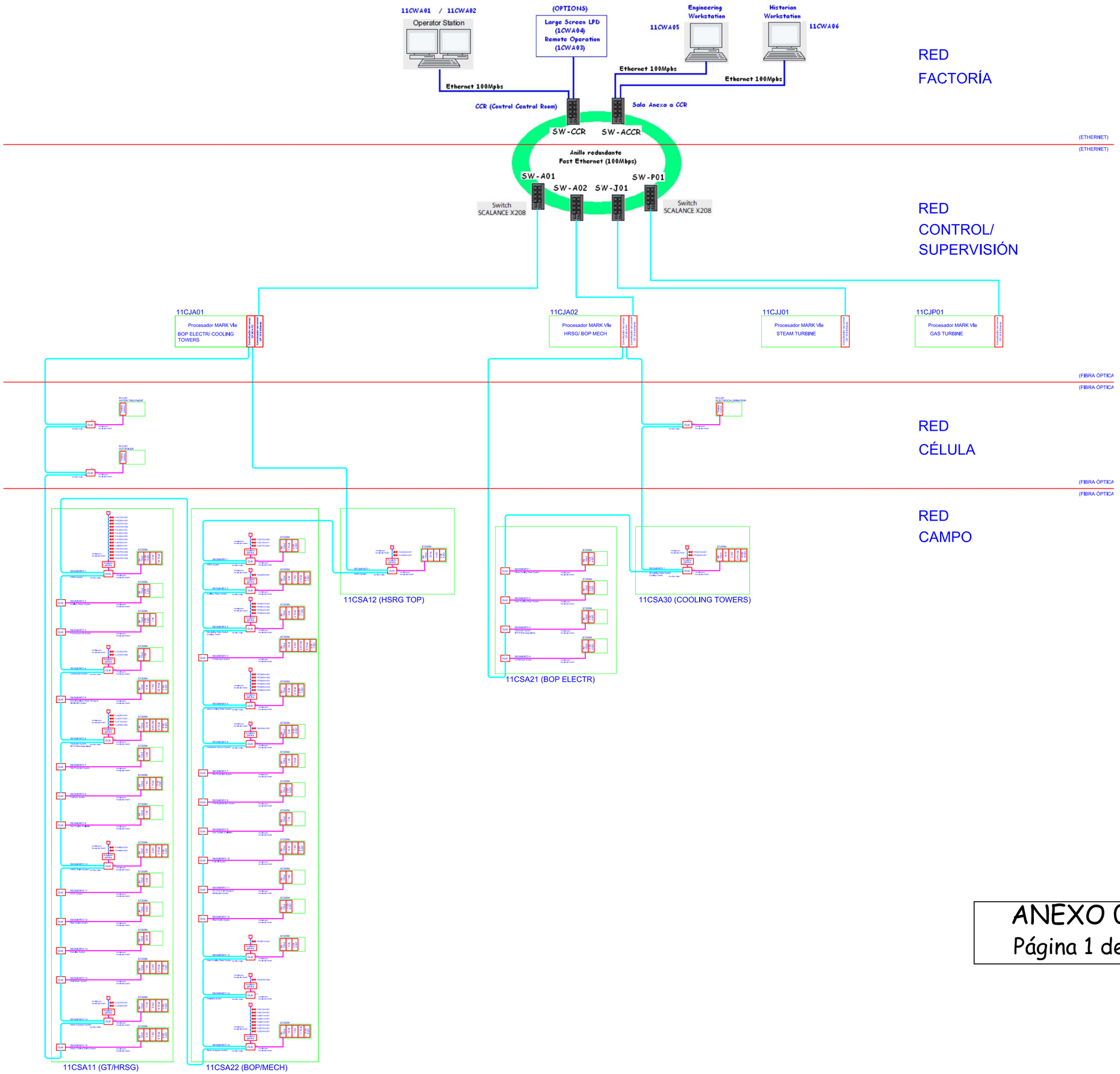
GENERAL ARRANGEMENT - POWER ISLAND. SECTION A-A/E-E/F-F

EMPRESARIOS AGRUPADOS	GE ENERGY — GENERAL ELECTRIC COMPANY, GENERAL ELECTRIC INTERNATIONAL, INC., POWER GENERATION-POWER PLANT SYSTEMS		SIZE A0	CAGE CODE	DWG NO 129E3556B
EA DWG NO 496-11-D-M-00601B	DRAWN AAB	2010-12-16			
	ISSUED AZJ	2010-12-16	SCALE 1/150	GE Rev B	SHEET 7 OF 8

496-11-D-M-00601B-007-03

ANEXO 4.

"Esquema general de comunicaciones diseñado para Planta Estandar de Ciclo Combinado"



ANEXO 04
Página 1 de 1