DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD COMPUTACIONAL PARA LOS EQUIPOS DE LOS SISTEMAS DE CONTROL DE UNA REFINERÍA

MANUEL JOSÉ RÍOS ARRIETA
ÁNGEL EDUARDO URUETA PUELLO

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y MECATRÓNICA
CARTAGENA DE INDIAS D.T. Y C.
2003.

DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD COMPUTACIONAL PARA LOS EQUIPOS DE LOS SISTEMAS DE CONTROL UNA REFINERÍA

MANUEL JOSÉ RÍOS ARRIETA
ÁNGEL EDUARDO URUETA PUELLO

Monografía presentada como requisito parcial para optar el título de Ingeniero de Electrónico

Director
JAIME ARCILA IRIARTE

Ing. Electricista
M.S.C. Ciencias Computacionales

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y MECATRÓNICA
CARTAGENA DE INDIAS D.T. Y C.
2003

Nota de aceptación

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Cartagena, 28 de Mayo de 2003

Dedico la culminación de este logro

A el de arriba, por existir.

A mi madre YADIRA ARRIETA RODELO, a mi padre MANUEL RIOS VARGAS y a mis hermanas EVELIN PAOLA y KAROL LICETH por su apoyo, comprensión y por ser la inspiración que me lleva a soportar todo tipo de sacrificio.

A mi abuela CARMEN RODELO por su demostración de cariño y humildad todo el tiempo que nos acompañó.

A mi compañero de monografía ANGEL EDUARDO URUETA por su amistad y compañerismo.

A ONIX y a toda la comunidad riverplatense de la CUTB.

Manuel José Ríos Arrieta

Dedico la culminación de este logro

A Dios,

A mis padres MIGUEL URUETA MENDOZA Y MARIBEL PUELLO DE URUETA y a mi hermano, JOSE URUETA PUELLO, por ser pilares en mi vida, por su sacrificio y apoyo constante y por darme la fuerza para luchar y seguir adelante. Gracias por ayudarme a culminar este logro que también es suyo.

A mis amigos, por estar siempre allí y por su amistad incondicional.

A mi Universidad y a mis maestros, por la formación personal y profesional que me entregaron.

Ángel Eduardo Urueta Puello

AGRADECIMIENTOS

Los autores expresan su agradecimiento a:

Jaime Arcila Iriarte, Ingeniero electricista profesor de la Corporación Universitaria Tecnológica de Bolívar, por su apoyo y su orientación.

Cartagena de Indias, 28 de Mayo del 2003.

Señores

Corporación Universitaria Tecnológica de Bolívar

Facultad de Ingeniería Eléctrica, Electrónica y Mecatrónica

Atn: Ing. Oscar S. Acuña

Decano Facultad

Ciudad

Respetados señores

Comedidamente nos dirigimos a usted con el fin de presentar a consideración para su estudio y aprobación la monografía titulada ***"Desarrollo de las políticas de seguridad computacional para los equipos de los sistemas de control una Refinería"***, con el objeto de optar el título de Ingeniero de Electrónico.

Atentamente,

Manuel J. Ríos Arrieta

Ángel E. Urueta Puello

Cartagena de Indias, 28 de Mayo del 2003.

Señores

Corporación Universitaria Tecnológica De Bolívar

Facultad de Ingeniería Eléctrica, Electrónica y Mecatrónica

Atn. Comité de Evaluación de Proyectos

Ciudad

Respetados Señores,

Con la presente me dirijo a ustedes, con ocasión a la petición de los señores **Manuel J. Ríos Arrieta** y **Ángel E. Urueta Puello**, estudiantes matriculados en el programa de Ingeniería electrónica, quienes han manifestado su determinación de presentar su proyecto titulado ***"Desarrollo de las políticas de seguridad computacional para los equipos de los sistemas de control una Refinería"***, requisito este indispensable para optar el titulo de Ingeniero de Electrónico.

Al respecto me permito comunicar que he dirigido el citado proyecto, el cual considero de gran importancia y utilidad.

Atentamente,

_____

Ing. Jaime Arcila Iriarte.
Director de Monografía

Cartagena de Indias, 28 de Mayo del 2003.

Señores

Corporación Universitaria Tecnológica de Bolívar

Facultad de Ingeniería Eléctrica, Electrónica y Mecatrónica

Atn. Comité de Evaluación de Proyectos

Ciudad

Respetados Señores,

Por medio de la presente nos permitimos hacer entrega formal de la monografía ***"Desarrollo de las políticas de seguridad computacional para los equipos de los sistemas de control una Refinería"***, como requisito parcial para optar al título de Ingeniero de Electrónico.

Atentamente,

Manuel J. Ríos Arrieta

Ángel E. Urueta Puello

REGLAMENTO ACADEMICO

(ARTICULO 105)

La Corporación Universitaria Tecnológica De Bolívar se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados y no pueden ser explotados comercialmente sin su autorización.

CONTENDIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACCESO REMOTO A LA RED: se refiere al acceso que se realiza a la red fuera de las instalaciones de la empresa o fuera de la red corporativa.

ADMINISTRADOR DE LA RED: es el encargado dirigir, guiar, organizar y manejar la red de planta de sistema de control distribuido de la refinería.

AREA CRÍTICA: es el área física donde se encuentra instalado el equipo o equipos que requieren de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la red de planta del DCS.

BASES DE DATOS: es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

BUG: error de programación.

CONTRASEÑA: conjunto de caracteres que permite el acceso de un usuario a un recurso informático.

CCB: Central Control Bulding, edificio donde su ubican los equipos principales de cómputo del sistema de control distribuido de la refinería.

DCS: Distribuided Control System. Sistema de control distribuido.

ESD: Estación de ShutDown. Estas estaciones realizan las tareas especificas de apagado de los dispositivos del sistema de control distribuido.

FCCU: Fluid Catalytic Cracking Unit

LCB: Local Control Building. En ellos se ubican las consolas de operación local de las distintas áreas que maneja el sistema de control distribuido.

MASTERBUS 300: red de campo de protocolo propietario ABB. Esta es la red de control que utiliza el DCS de la refinería.

RTDM-BDTR: Real Time Data Magnement. Base de Datos en Tiempo Real.

SIH: también son llamados cuartos satélites, en ellos se ubican los equipos necesarios en campo para realizar el control del proceso y la comunicación del mismo con el sistema de control distribuido.

STARCOUPLER: tipo de hub perteneciente al protocolo propietario de red de ABB MasterBus300.

RESUMEN

El objetivo de esta monografía es desarrollar las políticas de seguridad computacional de los sistemas de control de una refinería; de tal manera que garanticen la integridad, confidencialidad y disponibilidad de la información, plantas y equipos; lo cual se realizó mediante un estudio de la red y el análisis de posibles riesgos y ataques.

La metodología utilizada para la elaboración de estas políticas fue la realización de talleres en conjunto con el administrador de red, con el cual se efectuó el análisis de la base de datos de la administración de la red y de otros tipos de archivos confidenciales. También se realizó la evaluación de varios estudios sobre políticas de seguridad informática realizadas en redes corporativas a nivel mundial y se tomaron los puntos más importantes para poder adaptarlas a una red de planta.

La formulación de las políticas de seguridad computacional y de las respectivas recomendaciones deja claro que no importa que me medidas se tomen para la seguridad de una red de control, la medida principal es la de la adopción de una cultura de seguridad de la red por parte de todos los usuarios. Además las recomendaciones están centradas principalmente en como debe ser la restricción de los accesos y servicios en las estaciones que hacen parte de la red.

INTRODUCCIÓN

Aproximadamente un año atrás la refinería terminó de implementar casi en su totalidad un nuevo sistema de control distribuido con el objetivo de automatizar las áreas operativas que no encontraban automatizadas. En esta implementación no se contempló la realización de políticas de seguridad computaciones para los equipos que hacen parte de la red de planta este sistema de control distribuido, por lo tanto no se tienen bases, ni herramientas para considerar ni mucho menos implementar estrategias de seguridad que permitan trabajar en un ambiente más seguro, garantizando la continuidad de los procesos.

El objetivo de nuestro proyecto es desarrollar las políticas de seguridad para los equipos que hacen parte de la red de planta del sistema de control distribuido de una refinería, que vayan acorde con los objetivos generales de la organización. Además de esto se emitirán las recomendaciones necesarias de tal manera que se puedan implementar las estrategias de seguridad o las barreras de protección requeridas por este tipo de sistemas. Este proyecto también pretende dejar unas bases sólidas para posteriores estudios de seguridad en redes de control, ya que en la actualidad la bibliografía hacia seguridad de este tipo de redes ya sean redes de interconexión abierta o redes propietarias es muy escasa. Es importante destacar que esto es un ejercicio netamente académico, en el cual se tomó como marco de referencia información básica de la red de control de una refinería guardando discreción con los aspectos que pudieran comprometer la seguridad de la empresa. Por lo cual, las políticas, conclusiones y recomendaciones obtenidas no tienen ninguna acción de implantación inmediata en esta empresa, mas bien son resultados de un ejercicio académico de acuerdo a una conceptualización teórica y metodología aplicada que servirá como base para el

desarrollo de las políticas a implementar. Vale la pena resaltar que por razones de seguridad las IP's y nombres de HOSTS no son reales.

Para la elaboración de este proyecto se trabajó conjuntamente con el administrador del sistema de control distribuido de la refinería, con el cual se realizaron distintos talleres para realizar análisis a la base de datos de la administración de la red y de otros tipos de archivos confidenciales que se mencionaran en el desarrollo de la investigación. Para el análisis final también se tomó como base varios estudios sobre políticas de seguridad informática realizadas en redes corporativas a nivel mundial y se tomaron los puntos más importantes para poder adaptarlas a una red de planta, como es el caso de la red de planta del sistema de control distribuido de refinería.

1. DESCRIPCIÓN DEL SISTEMA

1.1. DESCRIPCIÓN GENERAL

Hace poco tiempo la refinería implementó un nuevo sistema de control distribuido. Este proyecto de automatización es el más grande realizado por la empresa en el cual se integraron tecnologías de diferentes fabricantes: ABB, Foxboro, Honeywell y Siemens. Este proyecto involucra las cuatro áreas operativas en que se divide la refinería: servicios industriales, crudo, cracking, y elementos externos, éste último aun en etapa de implementación. El área de servicios industriales se encarga del sistema de la generación eléctrica, subestaciones, calderas y aire de compresores; en esta área se utiliza la tecnología Siemens TXT para manejar la generación eléctrica, monitoreo y maniobra de las subestaciones. La tecnología Foxboro se utiliza para manejar las calderas y el aire de los compresores. Las demás áreas (crudo, cracking y elementos externos) son manejadas por el sistema de control distribuido ABB Advant, colocando seis cuartos de control satélite (Crudo y viscoreductora, Merox y tratamiento, FCCU y POLY, Azufre, elementos externos de refinería y elementos externos TNP), donde se ubican los equipos de control de procesos específicos de cada área, y un cuarto de control central donde se puede hacer la supervisión de cada uno de los cuartos satélites y de la refinería en general. En la actualidad, para el caso específico de la telemetría de tanques del área de elementos externos, se cuenta con un sistema HoneyWell TDC3000. La principal característica de este nuevo sistema de control distribuido es su gran interconexión, lo que permite realizar operaciones de una determinada área desde diferentes sitios en la planta.

1.2. ARQUITECTURA GENERAL

El sistema ABB advant de la refinería esta distribuido en varios cuartos de control satélite donde se alojan los distintos equipos que controlan y supervisan las distintas áreas. Además, se tiene un cuarto de control central donde se encuentran las consolas desde las cuales se manejan y supervisan los cuartos satélites remotamente. Este cuarto de control central concentra la información de los cuartos satélites a través de tres hubs(starcouplers) los cuales reciben, de manera redundante, la información proveniente de los hubs starcoupler ubicados en cada cuarto satélite. El primer hub de este cuarto de control central recibe la información del área de crudo. El segundo hub recibe la información del área de cracking. Y el tercer hub recibe la información del área de elementos externos.

Cada uno de estos hub se enlaza de manera redundante con dos grupos de consolas. El primer grupo esta conformado por las consolas aplicación quienes a su vez se dividen en estaciones de información, que se encargan de llevar el registro de eventos, datos históricos por un corto periodo de tiempo (2 meses) e interfase con la Base de Datos en Tiempo Real; y estaciones de ingeniería, estás son utilizadas para realizar cambios de las aplicaciones de control y gráficos. El segundo grupo esta compuesto por seis estaciones, que son llamadas consolas de operador, desde las cuales se realiza la modificación de parámetros de los procesos y la supervisión de la planta.

Paralelamente a la red MasterBus descrita anteriormente se tiene una red ethernet con protocolo TCP-IP que se encarga de interconectar cada una de las consolas utilizadas en el sistema de control. Esto incluye las estaciones de operación ubicadas en los cuartos satélites, las consolas de información, ingeniería y de operador ubicadas en el cuarto de control central y las consolas de

entrenamiento. Para esta interconexión se utilizan 4 hubs 3com superstack II HUB 10 conectados en cascada.

Este grupo de hubs es conectado a un Switch Nivel 3 superstack II 3800, el cual tiene acceso a:

- Un grupo de hubs que se encarga de concentrar la información proveniente del cuarto de computadoras en el cual se realizan las tareas de mantenimiento, optimización, reconciliación y otras tareas.
- Un switch ATM que comunica la red control con la red de corporativa ya existente.
- Un switch que enlaza este sistema con los sistemas HoneyWell, Siemens y Foxboro.

En la Figura 1 se muestra el diagrama simplificado de todo el sistema, donde la línea roja representa la red de control (MasterBus 300) y la línea verde representa la red de planta (TCP-IP).

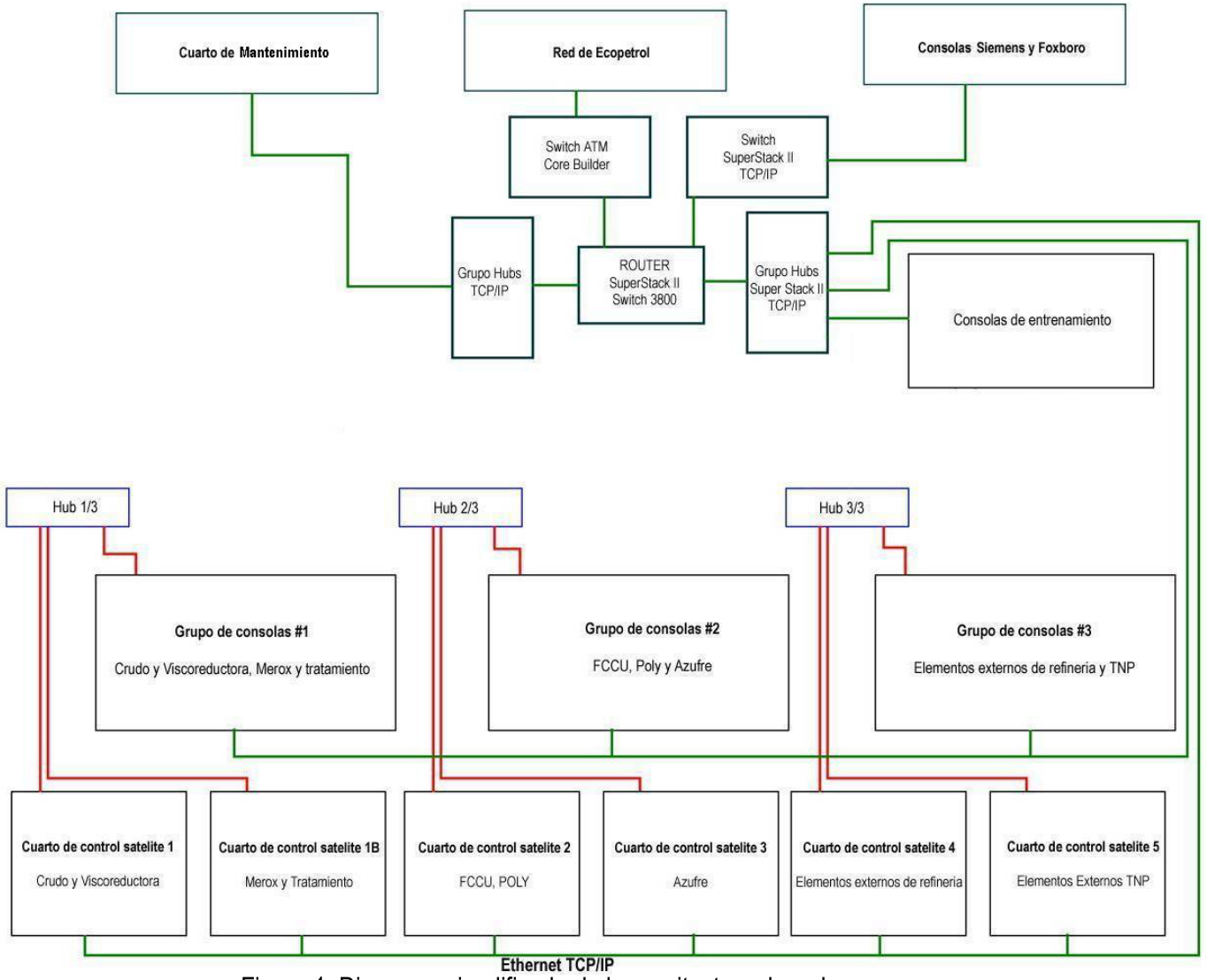

Figura 1. Diagrama simplificado de la arquitectura de red.

1.3. LOCALIZACIONES

El proyecto implementado se realizó con el propósito de automatizar las áreas operativas que no se encontraban automatizadas, estas áreas eran: crudo, cracking, y elementos externos, éste último aun en etapa de implementación. El área de servicios industriales no fue incluida en el proyecto, ya que ésta fue automatizada años atrás, sin embargo, en el proyecto si se tuvo en cuenta su interconexión con el nuevo sistema. El proyecto fue realizado utilizando productos ABB, implementando el sistema de control distribuido advant.

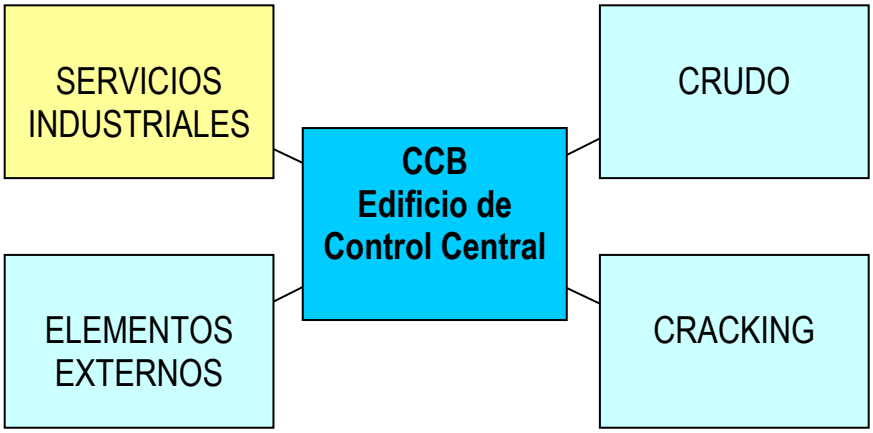

Figura 2. Diagrama de bloques de las áreas de operación de la refinería

Cada una de estas áreas, como se muestra en el esquema de la Figura 2, se comunica con el edificio de control central de tal manera que se puede realizar la supervisión y el monitoreo de manera remota, por lo que es posible realizar las misma operaciones que se realizan en los cuartos satélites.

Como se observa en la Figura 1 de la arquitectura simplificada del sistema cada área esta conformada por diferentes zonas (SIH, CCB) y éstas a su vez pueden estar formadas por diferentes grupos de equipos, cada uno con su respectiva localización.

El área de crudo está formada por las localizaciones de:

- Consola de aplicación de crudo en el edificio de control central, que está formada por una estación de ingeniería, dos de información y un Xterm.

- Consola de operación de crudo en el edificio de control central, éstas consolas se encuentran en el cuarto de control central del CCB y están formadas por seis consolas de operación, dos estaciones de shutdown y dos impresoras.

- Cuarto Satelite #1 Crudo, éste hace referencia a los sistemas de alimentación de respaldo que alimentan a los equipos de los cuartos satélites de esta área. Éstas son dos UPS.

- Cuarto Satelite #1 Crudo - Consola de Operación, contiene dos consolas para operación local de los sistemas de tratamiento y crudo y una estación de shutdown.

- Cuarto Satelite #1 Crudo - Racks del DCS, esta localización sólo posee un hub MB300 utilizado para enviar la información de esta área al CCB.

- Cuarto Satelite #1b Tratamiento - Racks del DCS, aquí se encuentra un módulo de E/S del DCS utilizado para recolectar información recolectar información de campo.

El área de cracking está formada por las localizaciones de:

- Consola de aplicación de cracking en el edificio de control central, que está formada por una estación de ingeniería, dos de información, un xterm, una estación de optimización del proceso de cracking y una impresora.

- Consola de operación de cracking en el edificio de control central, están formadas por seis consolas de operación, dos estaciones de shutdown y tres impresoras, las cuales se encuentran ubicadas en el cuarto de control central del CCB.

- Cuarto Satélite #2 Cracking, aquí se encuentran los sistemas de alimentación de respaldo que alimentan a los equipos de los cuartos satélites de esta área. Está constituido por dos UPS.

- Cuarto Satélite #2 Cracking - Racks del DCS, posee un hub MB300 utilizado para enviar la información de esta área al CCB.

- Cuarto de control local #2 cracking - consola de operación, se encuentra una estación de operación y una estación de shutdown.

- Cuarto Satélite #3 Azufre, contiene las UPS para respaldo de la alimentación de los equipos de esta área.

- Cuarto Satelite #3 Azufre - Racks del DCS, contiene un hub MB300.

- Cuarto de control local #2 Azufre - consola de operación, se encuentra una estación de operación y una estación de shutdown.

El área de elementos externos está formada por las localizaciones de:

- Consola de aplicación de Blending en el edificio de control central, que está formada por una estación de ingeniería, dos de información y un Xterm.

- Consola de operación de cracking en el edificio de control central, están formadas por seis consolas de operación, dos impresoras, una estación de control avanzado de blending y una estación star blend para optimización del proceso.

- Cuarto Satélite #4 Blending - Racks del DCS, posee un hub MB300 utilizado para enviar la información de esta área al CCB.

- Cuarto de control local #4 Blending- consola de operación, se encuentra una estación de operación local para el área de blending.

- Cuarto Satelite #5 Blenndig- Racks del DCS, contiene un hub MB300.

- Cuarto de control local #5 Blending- consola de operación, contiene una estación de operación local para el área de blending.

Otras localizaciones dentro del edificio de control central:

- Cuarto de Entrenamiento Edificio de Control Central, se encuentran 5 estaciones de operación, una de información y una impresora.
- Consola de Mantenimiento Edificio de Control Central, aquí se encuentran 8 equipos utilizados para el mantenimiento de instrumentación en el campo.

- Cuarto de comunicaciones Consola 1 Edificio de Control Central, se encuentra una estación de información, una de ingeniería, una estación para control avanzando y dos impresoras.

- Rack de Pi Edificio de Control Central, contiene las estaciones para realizar la interfase entre el sistema ABB y el Siemens.

- Gabinete de comunicaciones Edificio de Control Central, se encuentran todos los concentradores y dispositivos de enrutamiento tanto para la red TCP/IP como para la red MasterBus.

- Oficinas Edificio de Control Central

- Administrador del sistema Edificio de Control Central, se encuentra una estación para reconciliación de datos, una estación short term schedulling y una impresora.

- Cuarto de UPS del Edificio de Control Central, se encuentran las tres UPS para la alimentación de cada uno de los equipos que hacen parte del CCB.

La Tabla 1 que se encuentra a continuación, contiene un resumen de las localizaciones descritas anteriormente.

Tabla 1. Localizaciones del sistema de control distribuido

Código localización	Descripción localización
CCB-APLICACION1	CUARTO DE CONTROL CENTRAL - CONSOLA DE APLICACIÓN - CRUDO
CCB-APLICACION2	CUARTO DE CONTROL CENTRAL - CONSOLA DE APLICACIÓN - CRACKING
CCB-APLICACION3	CUARTO DE CONTROL CENTRAL - CONSOLA DE APLICACIÓN - BLENDING
CCB-COMUNIC-1	CUARTO DE CONTROL CENTRAL - CUARTO DE COMUNICACIONES CONSOLA 1
CCB-COMUNIC-2	CUARTO DE CONTROL CENTRAL - CUARTO DE COMUNICACIONES CONSOLA 2

Código localización	Descripción localización
CCB-COMUNIC-PI	CUARTO DE CONTROL CENTRAL - RACK DE PI
CCB-COMUNIC-RACK	CUARTO DE CONTROL CENTRAL - GABINETE DE COMUNICACIONES
CCB-CONSOLA1	CUARTO DE CONTROL CENTRAL - CONSOLA 1 - CRUDO
CCB-CONSOLA2	CUARTO DE CONTROL CENTRAL - CONSOLA 2 - CRACKING
CCB-CONSOLA3	CUARTO DE CONTROL CENTRAL - CONSOLA 3 - BLENDING
CCB-CONSOLA4	CUARTO DE CONTROL CENTRAL - CONSOLA 4 - UTILITIES
CCB-ENTRENAMIENTO	CUARTO DE CONTROL CENTRAL - CUARTO DE ENTRENAMIENTO
CCB-MANTENIMIENTO	CUARTO DE CONTROL CENTRAL - CONSOLA DE MANTENIMIENTO
CCB-OFICINAS	CUARTO DE CONTROL CENTRAL - OFICINAS
CCB-SISTEMA	CUARTO DE CONTROL CENTRAL - ADMINISTRADOR DEL SISTEMA
CCB-UPS	CUARTO DE CONTROL CENTRAL - CUARTO DE UPSs
LCB#2-CONSOLA	CRACKING - CUARTO DE CONTROL LOCAL #2 - CONSOLA DE OPERACIÓN
LCB#3-CONSOLA	AZUFRE - CUARTO DE CONTROL LOCAL #3 - CONSOLA DE OPERACIÓN
LCB#4-CONSOLA	BLENDING - CUARTO DE CONTROL LOCAL #4 - CONSOLA DE OPERACIÓN
LCB#5-CONSOLA	BLENDING - CUARTO DE CONTROL LOCAL #5 - CONSOLA DE OPERACIÓN
SIH#1	CRUDO - CUARTO SATELITE#1
SIH#1B-DCS	TRATAMIENTO - CUARTO SATELITE #1B - RACKS DEL DCS
SIH#1-CONSOLA	CRUDO - CUARTO SATELITE #1 - CONSOLA DE OPERACIÓN
SIH#1-DCS	CRUDO - CUARTO SATELITE #1 - RACKS DEL DCS
SIH#2	CRUDO - CUARTO SATELITE#2
SIH#2-DCS	CRACKING - CUARTO SATELITE #2 - RACKS DEL DCS
SIH#3	CRUDO - CUARTO SATELITE#3
SIH#3-DCS	AZUFRE - CUARTO SATELITE #3 - RACKS DEL DCS
SIH#4-DCS	BLENDING - CUARTO SATELITE #4 - RACKS DEL DCS
SIH#5-DCS	BLENDING - CUARTO SATELITE #5 - RACKS DEL DCS

1.4. TIPOS DE EQUIPOS

Dentro de la implementación del nuevo sistema de control distribuido de la refinería se realizó la instalación de diferentes tipos de equipos, que van desde varios tipos de computadora; por ejemplo IMS530, PC, etc ; hasta equipos de interconexión ethernet y MasterBus, e impresoras y UPS. En la Tabla 2 se encuentra un resumen con los tipos de equipo y el código respectivo para cada tipo.

Tabla 2. Tipos de equipos

Código tipo equipo	Descripción tipo equipo	Sistema Operativo
AW51	AW51 FOXBORO	UNIX SOLARIS
ETHERNET	HUB / SWITCH ETHERNET TCP/IP	N.A.
IMS530	ESTACION ABB ADVANT 530	UNIX HP UX
LCP	IMPRESORA LASER COLOR	N.A.
LP	IMPRESORA LASER BLANCO Y NEGRO	N.A.
MB300	EQUIPO DE COMUNICACIÓN MB300	N.A.
MP	IMPRESORA MATRIZ DE PUNTO	N.A.
MX	MULTIPLEXER	N.A.
OS520	ESTACION ABB ADVANT 520	UNIX HP UX
OT	ESTACION DE OPERACION SIEMENS	UNIX SCO
PC	PERSONAL COMPUTER	Windows 2000/NT
PORTATIL	COMPUTADOR PORTATIL	Windows
UNIX	ESTACION UNIX	
UPS	SISTEMA ININTERRUMPIDO DE POTENCIA	N.A.
XU	ESTACION GATEWAY SIEMENS	UNIX SCO

Los códigos de la Tabla 2 se refieren a las siglas en inglés del tipo de equipo donde:

AW51 : Estación de trabajo del DCS IA de FOXBORO.

IMS530: *Information Managment Station*, en español Estación de Manejo de Información.

LCP: *Laser Color Printer.*

LP: *Laser Printer.*

MB300: *Master Bus.*

MP: *Matriz Printer*.

OS520: *Operation Station*.

OT: *Operation Terminal.*

PC: *Personal Computer*.

UPS: *Uninterrupted Power Supply.*

XU: es un modelo del DCS TELEPERM XP de SIEMENS.

2. DIAGNÓSTICO DEL SISTEMA DE CONTROL DISTRIBUIDO

2.1. ÁREA DE CRUDO

Esta área esta constituida por los cuartos satélites de Crudo y viscoreductora(Satélite 1) y de Merox y tratamiento(satélite 1B) y por un grupo de consolas ubicadas en el cuarto de control.

2.1.1. Cuartos satélites. En la arquitectura final del sistema de control distribuido esta área, en cuanto a los cuartos satélites, quedó dividida en tres secciones(ver Figura 3):

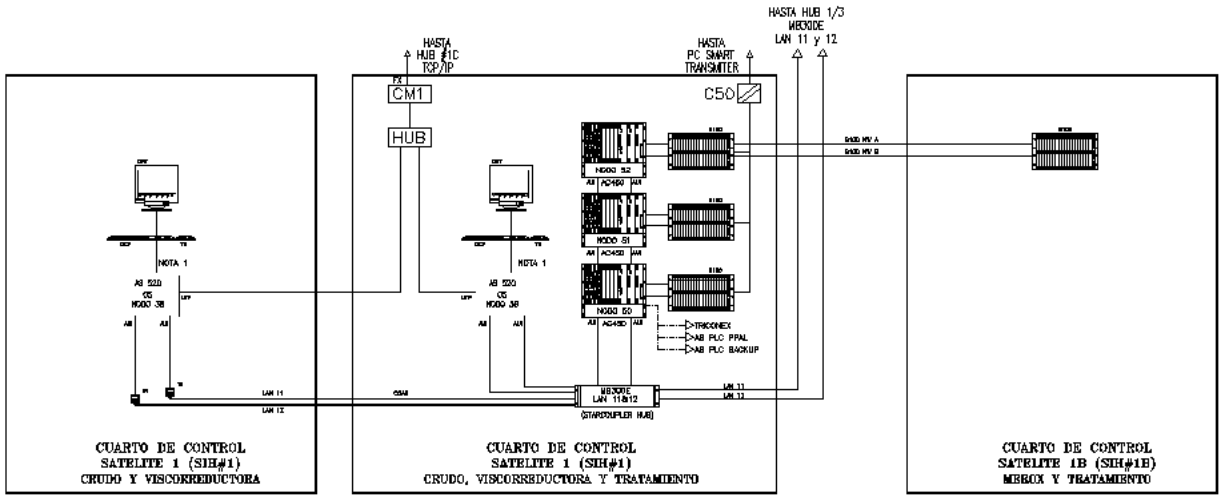

Figura 3. Cuartos satélites de área de crudo

a. Sección 1: Cuarto de control satélite 1(LCB-Local control building) Crudo y viscoreductora:

Aquí, como se muestra en la Figura 4, se encuentra una estación de trabajo (AS520) que se encarga de realizar la supervisión y monitoreo tanto del proceso de crudo y viscoreductora como de merox y tratamiento. En ésta se pueden realizar los cambios de los parámetros del proceso correspondientes a esta área.

La CPU está conectada de manera redundante (dos cables) a un hub starcoupler MasterBus 300 localizado en la sección 2 de ésta área. Esta conexión se realiza a través de dos transceptores que se encargan de convertir la señal de cable coaxial a AUI(cable utilizado para la red MasterBus). De la misma manera se encuentra conectada a un HUB TCP/IP de la sección 2 a través de UTP.

En este edificio de control local también se encuentra una estación de shutdown ESD PC1C que no aparece en los planos, ya que no está relacionada con la operación y monitoreo de los procesos de esta área. Esta estación de shutdown se encuentra conectada al Switch#5 a través de fibra óptica.

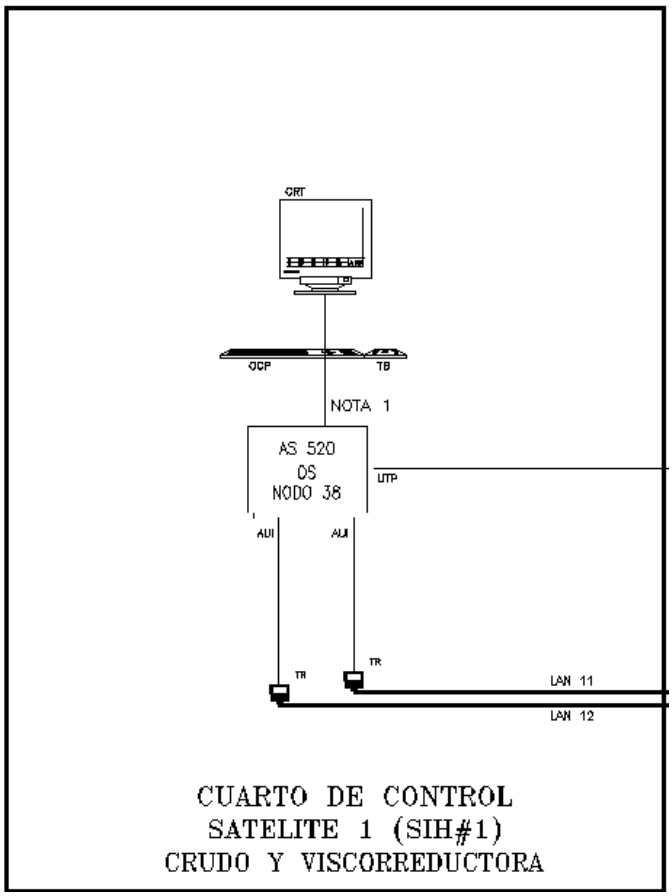

Figura 4. LCB #1 Crudo y Viscoreductora

b. Sección 2: Cuarto de control satélite 1(SIH#1) Crudo, viscoreductora y tratamiento.

Ésta es la más compleja de las tres secciones(Véase Figura 5). Esta formada por:

- Tres módulos de E/S(S100), que se encargan de concentrar todas las señales de entrada o salida del campo. Cada módulo está conectado individualmente de manera redundante a un controlador. También existe una conexión entre cada módulo E/S y un conversor(C50) de RS232 a fibra óptica monomodo, con el

propósito de enviar información al PC smart transmiter ubicado en el cuarto de computadoras descrito más adelante.

- Tres controladores avanzados (AC450) que reciben las señales de los módulos de entrada salida. Estos controladores se encuentran interconectados con el propósito de compartir datos de procesos, y de llevar los datos hasta el Hub Starcoupler. Se debe destacar que cada controlador tiene un controlador de respaldo, para hacer de éste un sistema redundante, por lo tanto en esta sección no se encontraría físicamente tres controladores sino seis. El controlador nodo 50 se encarga del proceso de crudo, el controlador nodo 51 del proceso de viscoreductora y el nodo 52 del proceso de merox y tratamiento.

- Un Hub StarCoupler MB300E que se encarga de realizar la interfase entre la estación de operación (AS520) y los controladores avanzados. De igual manera se encarga de enviar de manera redundante toda la información de proceso al HUB 1/3 de la red de control MB300E, ubicado en el cuatro de comunicaciones, utilizando la red MasterBus 300.

- Una estación de operación (AS520) en la que se pueden realizar las mismas operaciones que se realizan en la estación de operación del LCB(sección 1). Ésta se encuentra conectada de manera redundante al Hub MB300E y con UTP al Hub TCP/IP, ambos en esta misma sección.

- Un Hub TCP/IP que concentra la información de las dos estaciones de operación de esta área operativa y que envía la información a un conversor de UTP a fibra. La información en fibra es enviada al Hub #1C TCP/IP ubicado en el cuarto de comunicaciones descrito más adelante.

- Dos UPS para alimentación eléctrica y respaldo de los equipos anteriores. Las UPSs, que se encuentran conectadas al Switch#5 de la red TCP/IP, no aparecen en los planos de la arquitectura del sistema de control debido a que son equipos eléctricos.

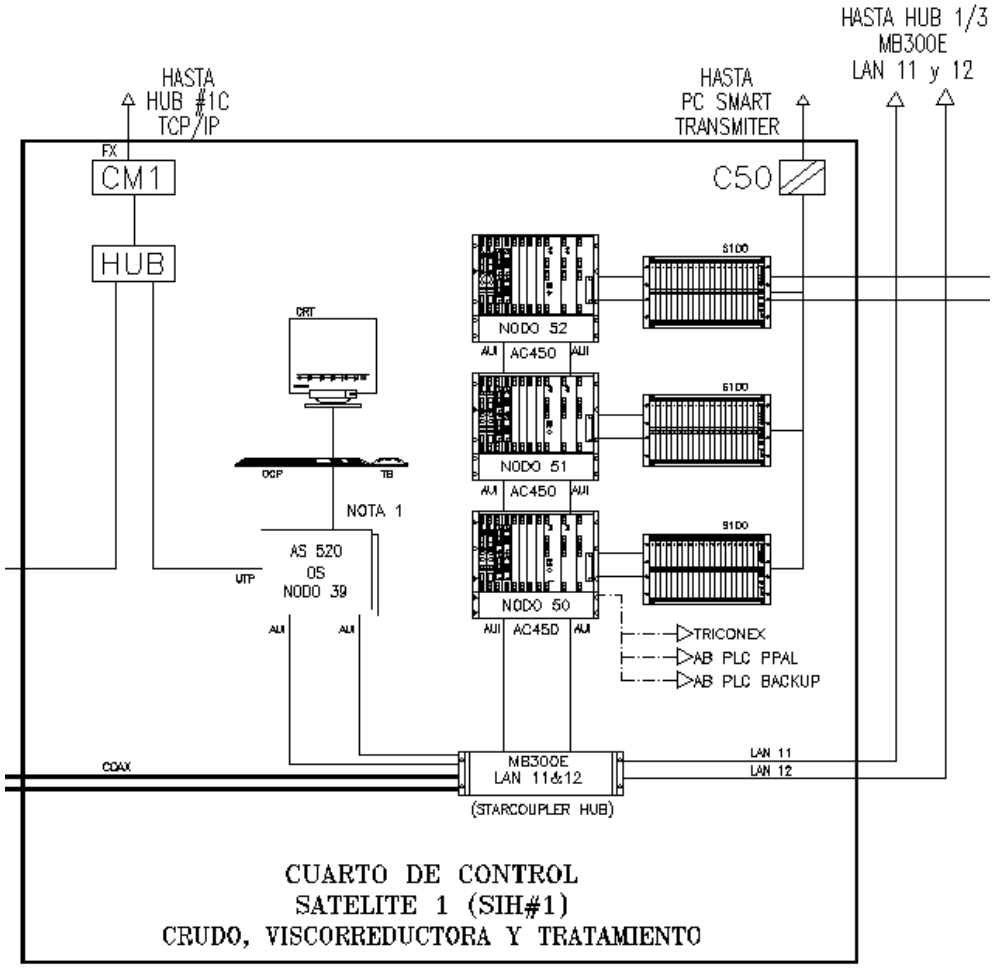

Figura 5. SIH #1 Crudo, Viscoreductora y Tratamiento

c. <u>Sección 3: Cuarto de control satélite 1B(SIH#1B) Merox y tratamiento</u>

Esta sección está conformada solamente por un módulo de E/S(S100) que envía la información de manera redundante a uno de los módulos E/S ubicado en la sección 2. Véase Figura 6.

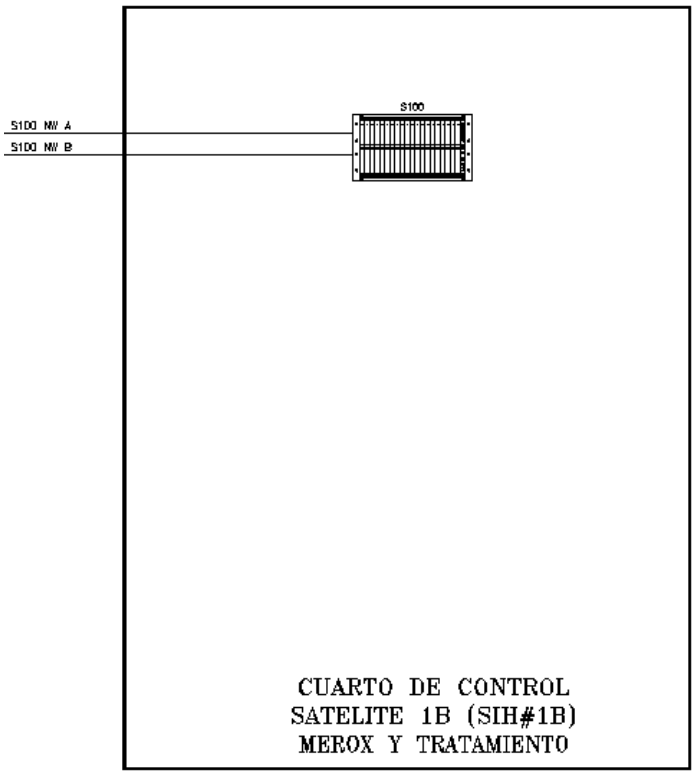

Figura 6. SIH#1B Merox y Tratamiento

2.1.2. Cuarto de aplicaciones y cuarto de control central. En el cuarto comunicaciones, cercano al cuarto de control central, se encuentra el Hub 1/3 MB300E que se encarga de recibir de manera redundante la información proveniente de los cuartos satélites 1 y 1B y enviarla, también de manera redundante a través de cable coaxial, al grupo de consolas correspondiente de esta área utilizando una topología tipo bus(ver Figura 7). Paralelamente a la red MasterBus, cada una de las computadoras de este grupo están conectadas a la red TCP/IP mediante UTP al Hub#1A ubicado en el cuarto de comunicaciones.

Este grupo de consolas está conformado por dos subgrupos: consolas de aplicación y las consolas de operador. Las primeras ubicadas en el cuarto de aplicaciones y las segundas ubicadas en el cuarto de control central.

Las consolas de operación son un grupo de seis estaciones de operación (AS520) encargadas de realizar la supervisión y monitoreo de los procesos de la zona de crudo de manera remota. Ésta, al igual que en la consola de los cuartos satélites, permite realizar cambios en los parámetros del proceso.

Cerca a las estaciones de operación se encuentran dos estaciones de shutdown ESD PC1A y PC1B para el área de crudo. Éstas, al igual que la estaciones de shutdown de los cuartos satélites, no aparecen en los planos de la arquitectura del sistema de control.

Las consolas de aplicación son un grupo de 4 computadoras, donde 2 son estaciones de administración de información (una estación NT y una estación AS530), una es una estación de ingeniería (AS520) y la restante es un PC Xterm.

Las estaciones de administración de información se encargan de llevar el registro de eventos, datos históricos por un tiempo corto (2 meses) e interfases con la base de datos en tiempo real. La estación de ingeniería es utilizada para realizar cambios en las aplicaciones de control y gráficos, mientras que el PC Xterm se utiliza para poder acceder a las estaciones de operación desde el cuarto de aplicación, utilizando la red TCP/IP. Es importante destacar que esta última computadora no está conectada a la red MasterBus 300.

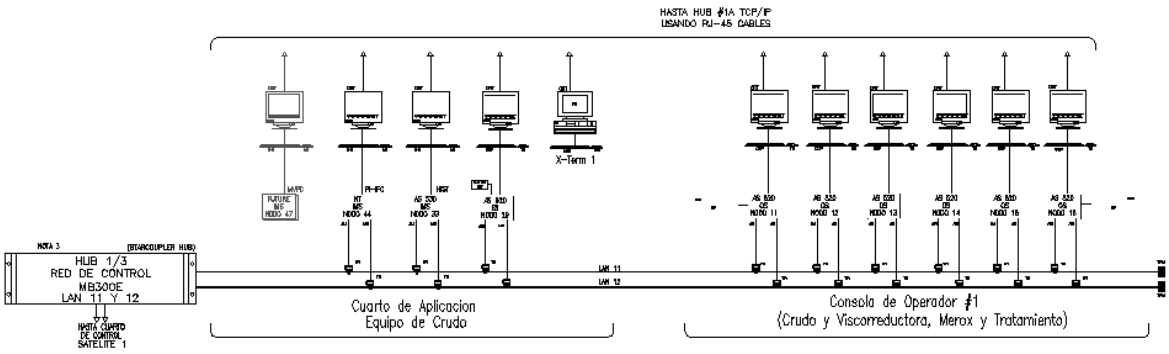

Figura 7. Consolas de Aplicación y operación del área de crudo

Integrando los cuartos satélites y el grupo de consolas del cuarto de control central, la arquitectura del sistema de control del área de crudo se vería de como se muestra en la Figura 8.

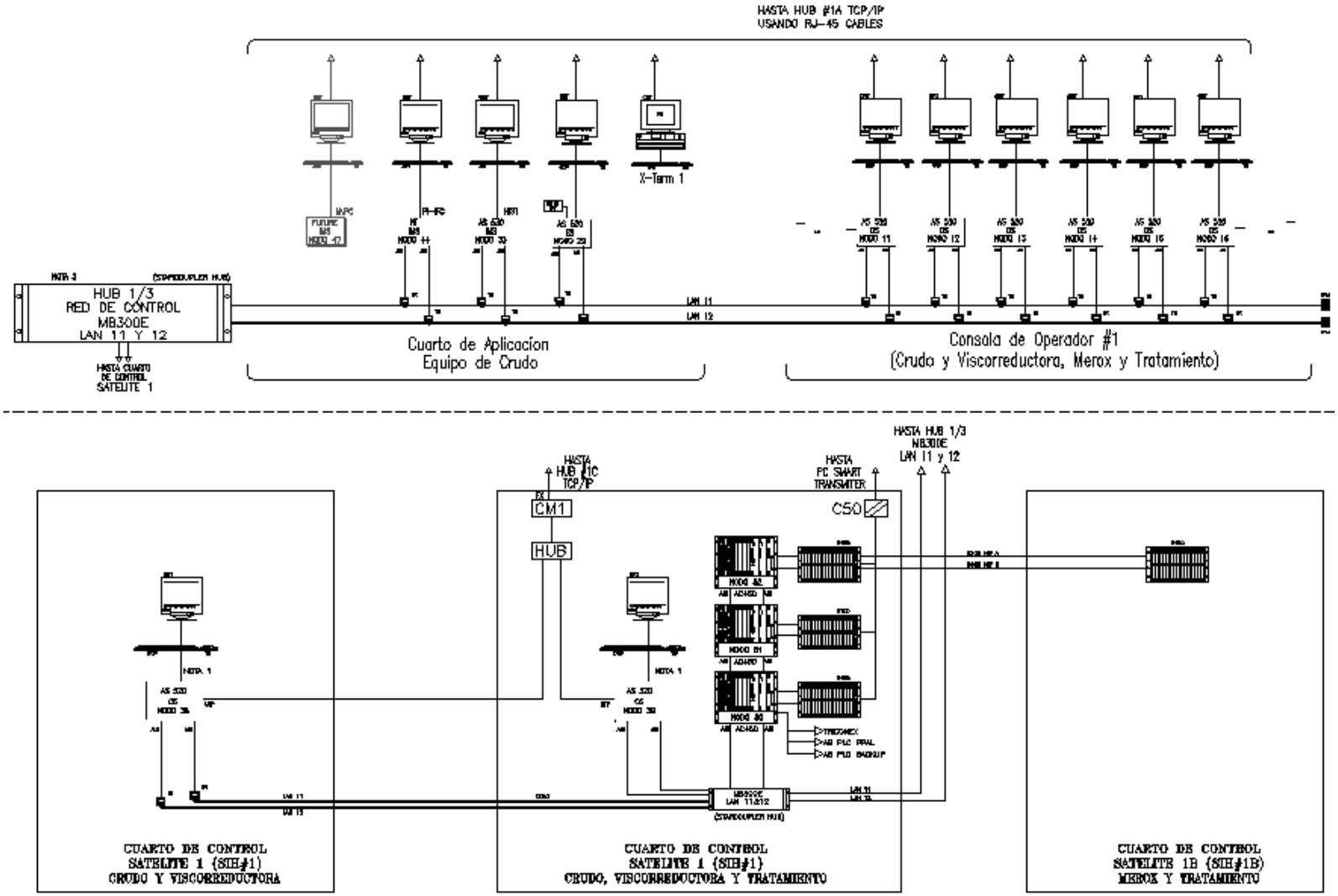

Figura 8. Arquitectura del sistema de control del área de crudo

2.2. ÁREA DE CRACKING

2.2.1. Cuartos satélites. Esta área esta constituida por los cuartos satélites de FCCU y POLY (Satélite 2) y de Azufre y asfalto (satélite 3) y el grupo de consolas ubicadas en el cuarto de control central. En la arquitectura final del sistema esta área quedó dividida en cinco secciones, como se ve en la Figura 9.

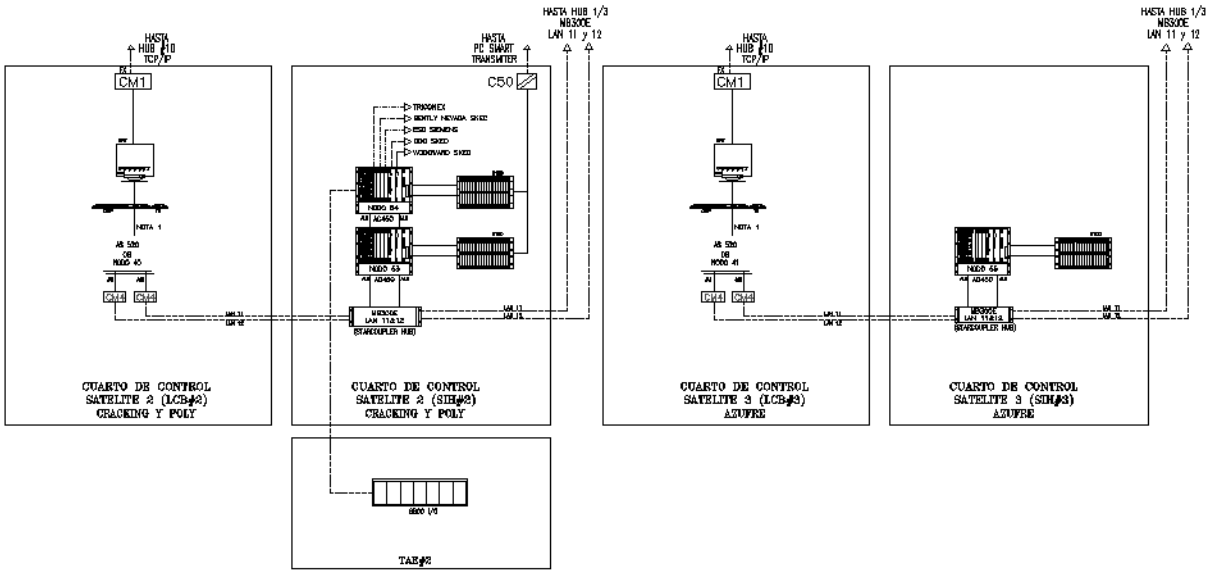

Figura 9. Cuartos satélites del área de crácking

a. Sección 1: Cuarto satélite 2(LCB#2) Cracking y Poly.

Como se muestra en la Figura 10, en esta sección existe una estación de trabajo (AS520) que se encarga de realizar la supervisión y monitoreo del proceso de cracking y Poly. En ésta se pueden realizar los cambios de los parámetros del proceso correspondientes a esta área.

La CPU está conectada de manera redundante (dos cables) a un hub starcoupler MasterBus 300 localizado en la sección 2 de ésta área, la comunicación se realiza vía fibra óptica por lo que se utilizan dos conversores(CM4) de AUI a fibra óptica multimodo. De la misma manera se encuentra conectada a un conversor de UTP a fibra óptica multimodo con el propósito de enviar la información al HUB #1D TCP/IP ubicado en el cuarto de comunicaciones.

En este edificio de control local también se encuentra una estación de shutdown ESD PC2C que no aparece en los planos, ya que no esta relacionada con la operación y monitoreo de los procesos de esta área. Esta estación de shutdown se encuentra conectada al Switch#5 a través de fibra óptica.

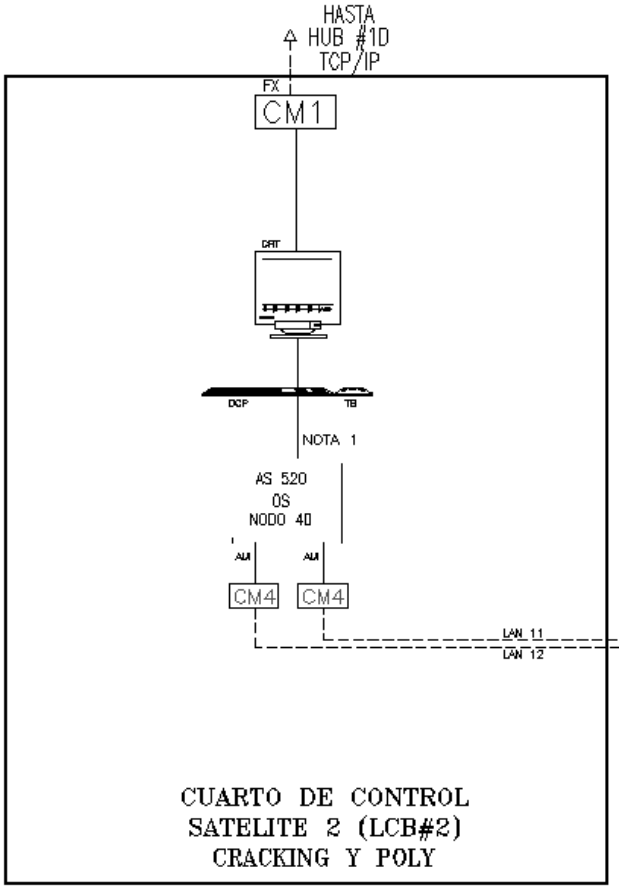

Figura 10. LCB #2 Cracking y Poly

b. Sección 2: Cuarto de control satélite 2(SIH#2) Cracking y poly.

Como se muestra en la Figura 11 está conformado por:

- Dos módulos de E/S (S100) conectados individualmente y de manera redundante a cada controlador. Existe una conexión entre cada módulo E/S y un conversor (C50) que pasa de Rs232 a fibra óptica multimodo, con el fin de enviar información al PC smart transmiter ubicado en el cuarto de computadoras.

- Dos controladores avanzados (AC450) conectados a los módulos E/S. Estos controladores se encuentran interconectados con el propósito de compartir datos de procesos y de llevar los datos hasta el Hub Starcoupler de la sección.

- Un Hub StarCoupler MB300E que se encarga de realizar la interfase entre la estación de operación (AS520) de la sección 1 y los controladores avanzados. También se encarga de enviar de manera redundante toda la información de proceso al HUB 2/3 de la red de control MB300E ubicado en el cuarto de comunicaciones, cerca al cuarto de control central, utilizando la red 300. Uno de estos controladores posee 5 entradas *modbus* provenientes de sistemas específicos dentro del proceso de cracking, por ejemplo: el *tricomex* es el sistema de *shutdown* del compresor y el *Bently Nevada Skec* es una señal de monitoreo de vibraciones del compresor.

- Dos UPS utilizadas para la alimentación y respaldo de los equipos de los equipos antes mencionados, los cuales van conectados al Switch#5 de la red TCP/IP. Éstas al igual que las UPS del SIH#1 no aparecen en los planos.

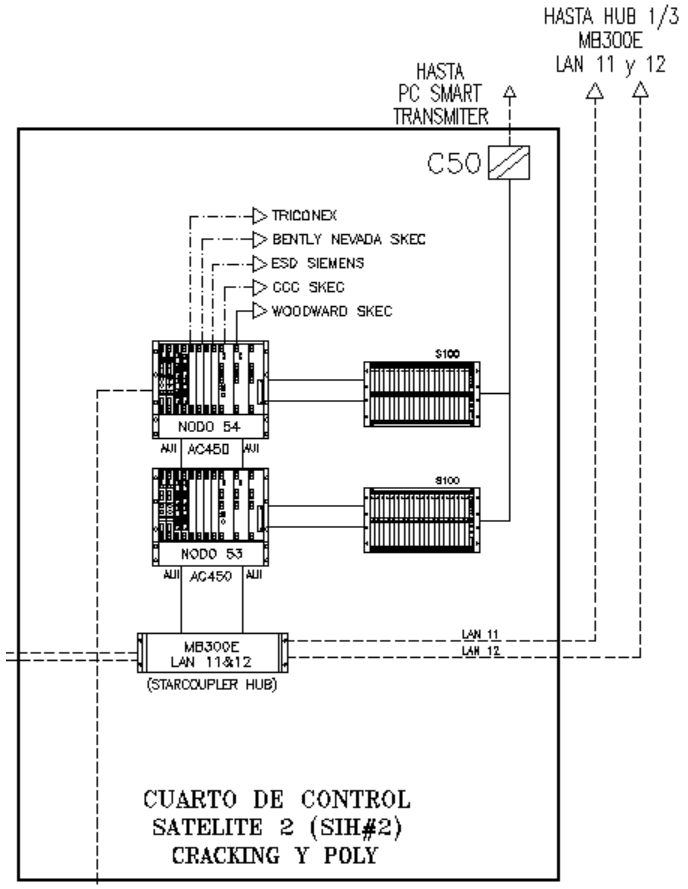

Figura 11. SIH #2 Cracking y Poly

c. Sección 3:Cuarto de control satélite 3(LCB#3) Azufre.

Contiene una estación de trabajo (AS520) que se encarga de realizar la supervisión y monitoreo del proceso de Azufre y asfalto(Ver Figura 12). La CPU está conectada de manera redundante a un hub starcoupler MasterBus 300 localizado en la sección 4 de esta área, está comunicación se realiza vía fibra óptica por lo que se utilizan dos conversores(CM4) de AUI a fibra óptica multimodo. De la misma manera se encuentra conectada a un conversor de UTP a fibra óptica multimodo con el propósito de enviar la información al HUB #1D TCP/IP ubicado en el cuarto de comunicaciones.

También se encuentra una estación de shutdown ESD PC2D que no aparece en los planos, ya que no está relacionada con la operación y monitoreo de los procesos de esta área. Esta estación de shutdown se encuentra conectada al Switch#5 a través de fibra óptica.

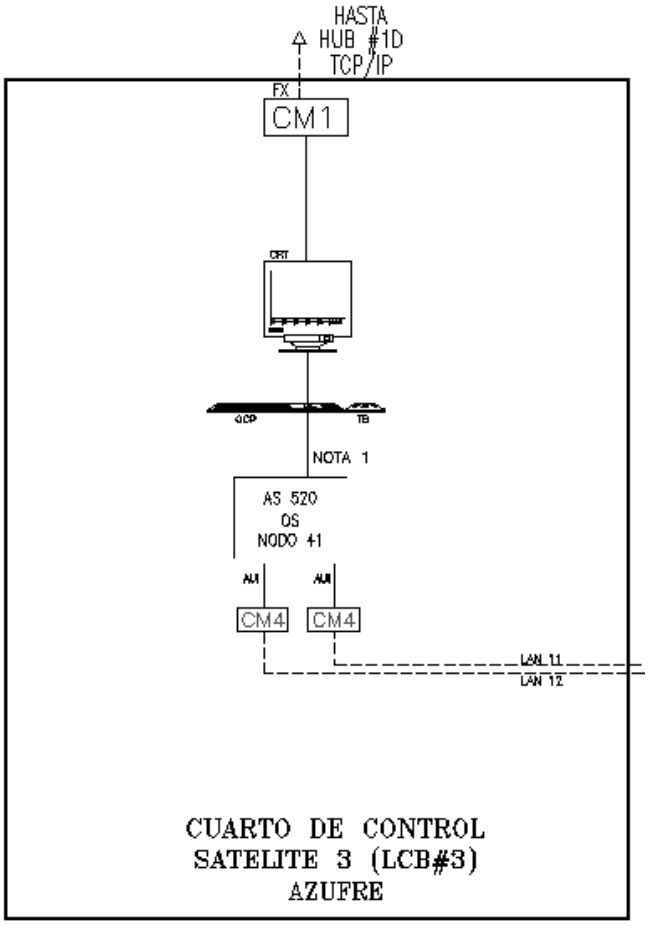

Figura 12. LCB #3 Azufre

d. Sección 4: Cuarto de control satélite 3(SIH#3) Azufre.

Como se observa en la Figura 13, en esta sección se encuentra:

- Un módulo de E/S (S100) conectado de manera redundante al controlador. Existe una conexión entre el módulo E/S y un conversor (C50) que pasa de Rs232 a fibra óptica multimodo, con el fin de enviar información al PC smart transmiter ubicado en el cuarto de computadoras.

- Un controlador avanzado (AC450) conectado al módulo E/S y al Hub Starcoupler de la sección.

- Un Hub StarCoupler MB300E que se encarga de realizar la interfase entre la estación de operación (AS520) de la sección 3 y el controlador avanzado. También se encarga de enviar de manera redundante toda la información de proceso al HUB 2/3 de la red de control MB300E ubicado en cuarto de comunicaciones, muy cerca al cuarto de control central, utilizando la red MasterBus 300.

- Dos UPS que se encuentran conectadas al Switch#5 de la red TCP/IP.

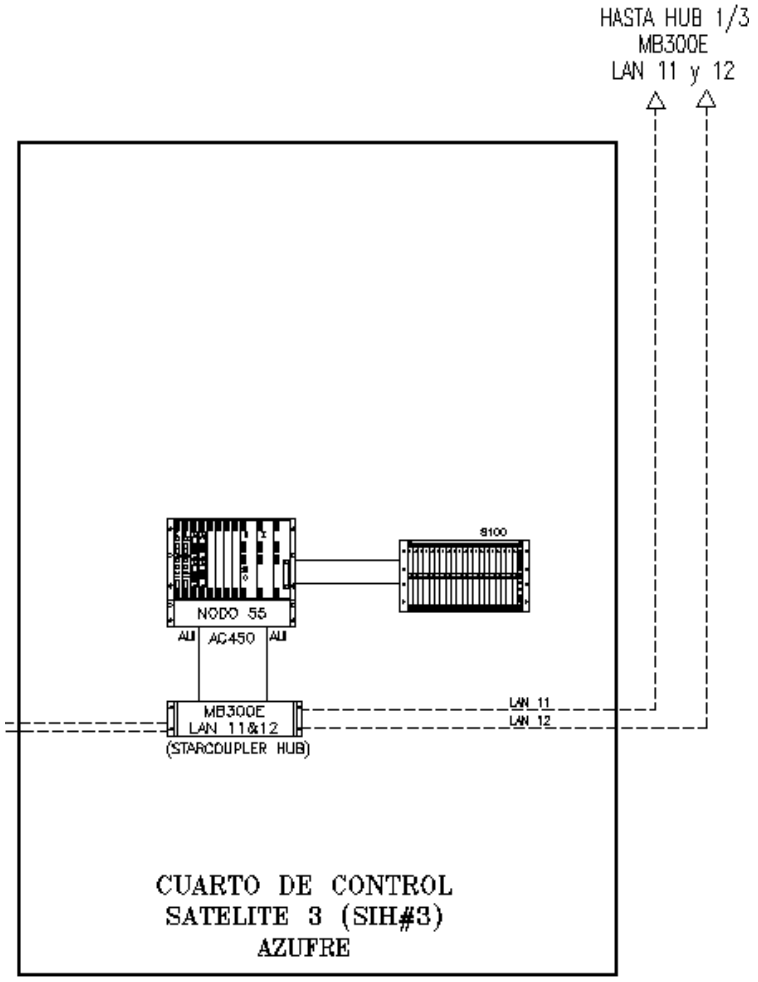

Figura 13. SIH #3 Azufre

e. Sección 5: TAE#2.

Esta conformada por un módulo de entrada salida (S800) que va conectado a uno de los controladores avanzados de la sección 2 vía fibra óptica(véase Figura 14).

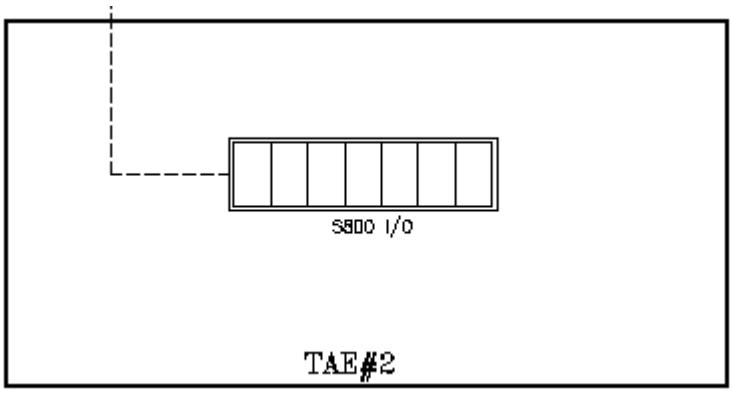

Figura 14. TAE #2

2.2.2. Cuarto de aplicaciones y cuarto de control central. En el cuarto de comunicaciones se encuentra el Hub 2/3 MB300E que se encarga de recibir de manera redundante la información proveniente de los cuartos satélites 2 y 3 y enviarla, también de manera redundante a través de cable coaxial, al grupo de consolas correspondiente de esta área utilizando una topología tipo bus. Paralelamente a la red MasterBus, cada una de las computadoras de este grupo están conectadas a la red TCP/IP mediante UTP al Hub#1A ubicado en el cuarto de comunicaciones(ver Figura 15).

Este grupo de consolas conformado por dos subgrupos: consolas de aplicación, ubicadas en el cuarto de aplicaciones; y las consolas de operador, localizadas en el cuarto de control central.

Las consolas de operador son un grupo de seis estaciones de operación (AS520) encargadas de realizar la supervisión y monitoreo de los procesos de la zona de cracking de manera remota. Ésta, al igual que en la consola de los cuartos satélites, permite realizar cambios en los parámetros del proceso.

Adyacentes a las estaciones de operación, se encuentran dos estaciones de shutdown ESD PC2A y PC2B para el área de cracking. Éstas, al igual que la estaciones de shutdown de los cuartos satélites, no aparecen en los planos de la arquitectura del sistema de control.

Las consolas de aplicación son un grupo de 4 computadoras, donde 2 son estaciones de administración de información (una estación NT y una estación AS530), una es una estación de ingeniería (AS520) y la restante es un PC Xterm 2. Al igual que en el área de crudo, esta computadora no está conectado a la red MasterBus 300.

En área también se incluye el PC FCCU optimizer & modelling que se utiliza para realizar la optimización del proceso de cracking, sin embargo su ubicación física no es el cuarto de control central sino el cuarto de aplicación. Este computador no se conecta a través de la red masterBus sino a la red de planta a través del Hub #3 TCP/IP.

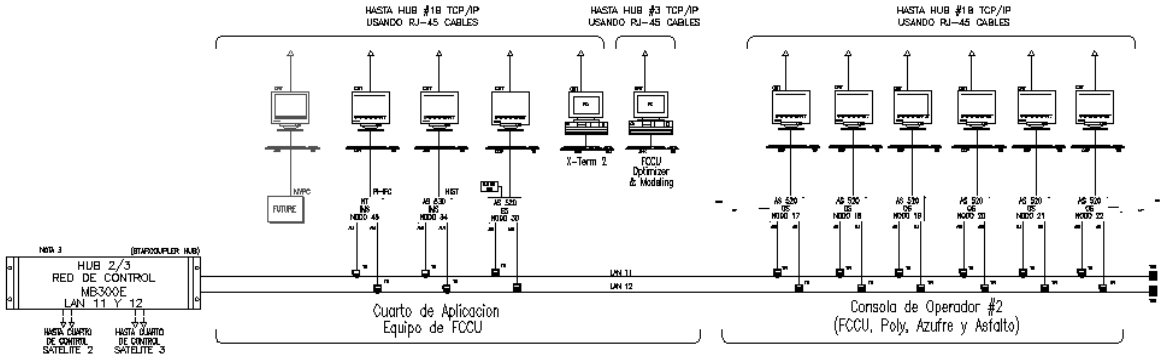

Figura 15. Consolas de Aplicación y Operación del área de Cracking

Integrando los cuartos satélites y el grupo de consolas del cuarto de control central, la arquitectura del sistema de control del área de cracking se vería como en la Figura 16.

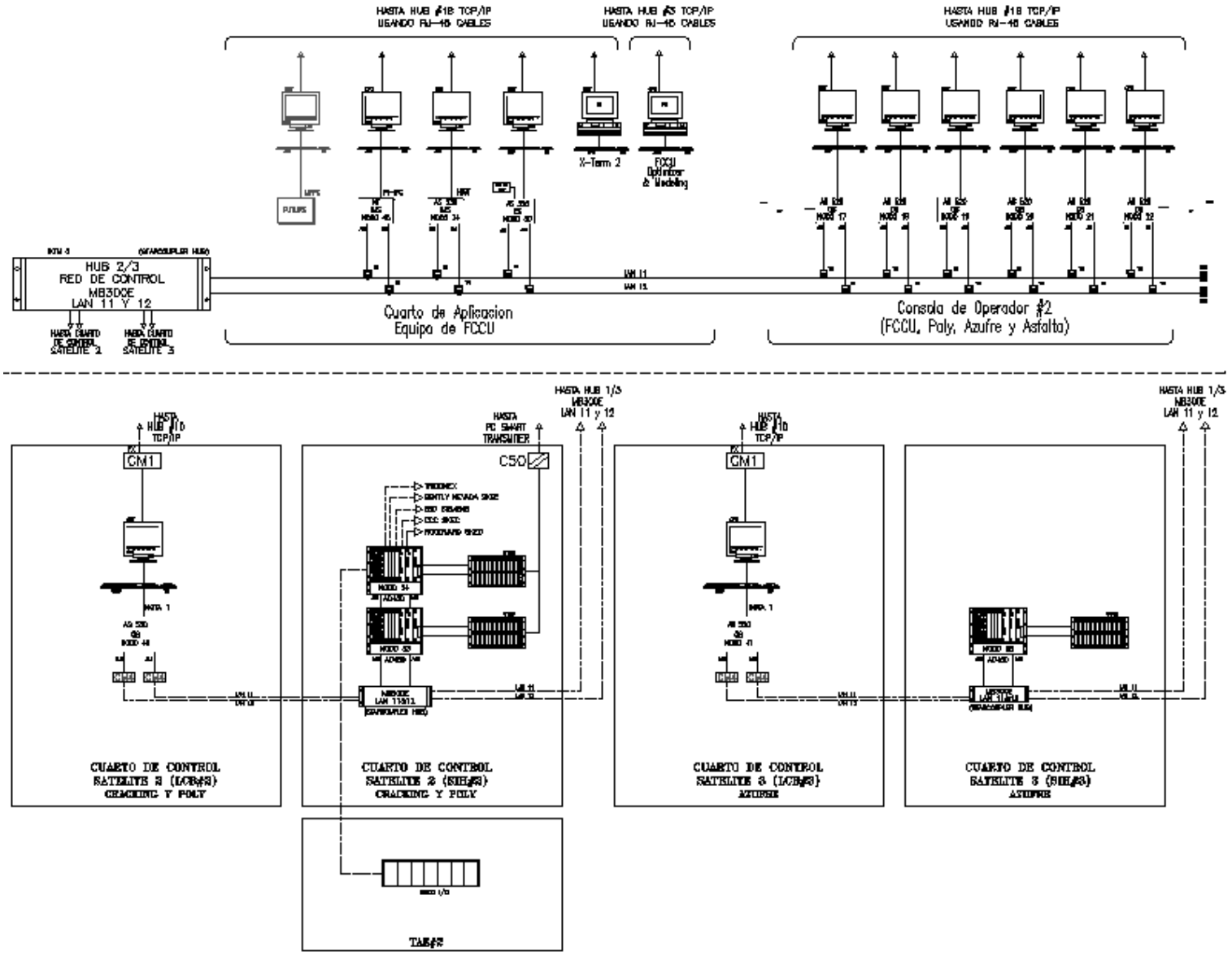

Figura 16. Arquitectura del sistema de control para el área de Cracking

2.3. ÁREA DE ELEMENTOS EXTERNOS

2.3.1. Cuartos satélites. Esta área esta constituida por los cuartos satélites de elementos externos de refinería (Satélite 4) y de elementos externos TNP (satélite 5) y el grupo de consolas ubicadas en el cuarto de control central. En la arquitectura final del sistema esta área quedó dividida en cuatro secciones, como se muestra en la Figura 17.

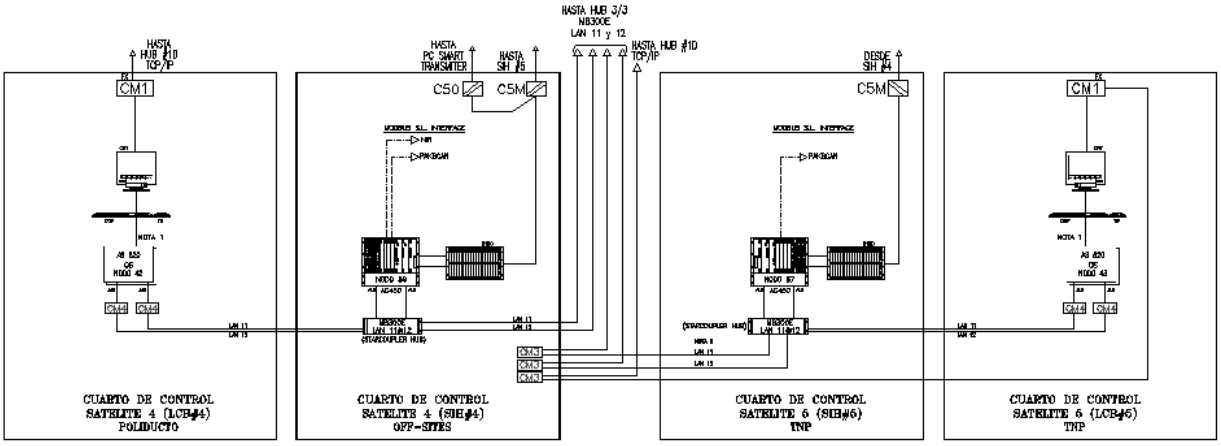

Figura 17. Cuartos satélites del área de elementos externos

a. Sección 1:Cuarto de control satélite 4(LCB#4) Poliducto.

Aquí se ubica una estación de trabajo (AS520) que se encarga de realizar la supervisión y monitoreo de toda el área de elementos externos. En ella se pueden realizar los cambios de los parámetros del proceso correspondientes a esta área(Ver Figura 18).

La CPU está conectada de manera redundante (dos cables) a un hub starcoupler MasterBus 300 localizado en la sección 2 de ésta área, esta comunicación se realiza vía fibra óptica por lo que se utilizan dos conversores(CM4) de AUI a fibra óptica multimodo. De la misma

manera se encuentra conectada a un conversor de UTP a fibra óptica multimodo con el propósito de enviar la información al HUB #1D TCP/IP ubicado en el cuarto de comunicaciones.

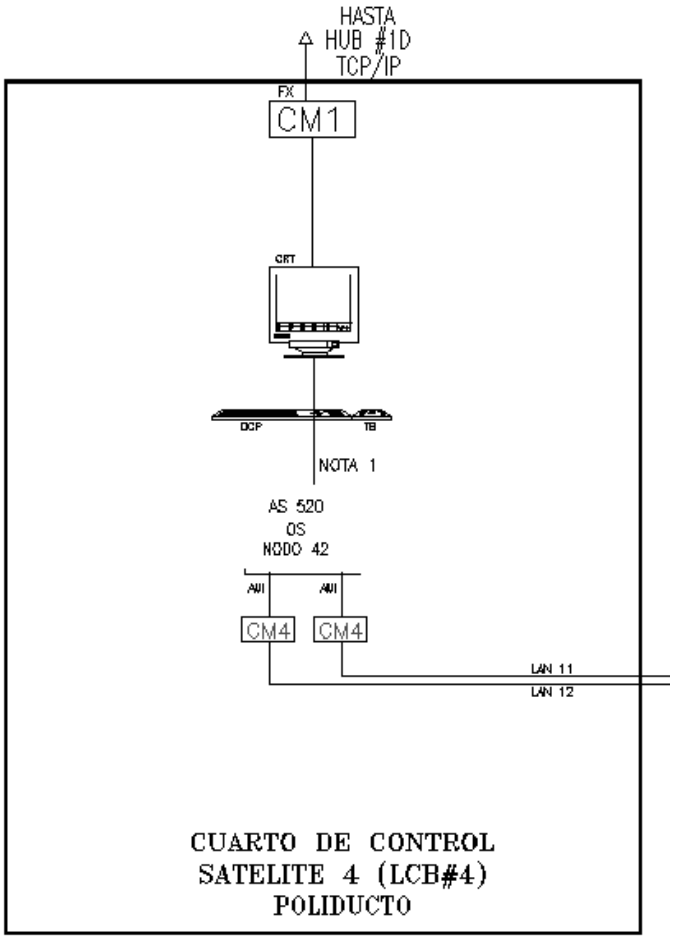

Figura 18. LCB #4 Poliducto

b. Sección 2:Cuarto de control satélite 4(SIH#4) Off-sites.

Como se ve en la Figura 19, en esta sección están ubicados:

- Un módulo de E/S (S100) conectado de manera redundante a un controlador avanzado. Existe una conexión entre el módulo E/S y dos conversores: el primero

es un conversor (C50) que pasa de Rs232 a fibra óptica multimodo, con el fin de enviar información al PC smart transmiter ubicado en el cuarto de computadoras; el segundo es un conversor (C5M) de RS485 a fibra óptica monomodo con el fin de enviar información al cuarto satélite SIH#5.

- Un controlador avanzado (AC450) conectado al módulo E/S y al Hub Starcoupler de la sección.

- Un Hub StarCoupler MB300E que se encarga de realizar la interfase entre la estación de operación (AS520) de la sección 3 y el controlador avanzado. También se encarga de enviar de manera redundante toda la información de proceso al HUB 3/3 de la red de control MB300E ubicado en el cuarto de comunicaciones, al lado cuarto de control central, utilizando la red MasterBus 300.

- Tres conversores (CM3) de Fibra óptica multimodo a monomodo, que reciben la información del Starcoupler de la sección 3 y del conversor de UTP a fibra (CM1) ubicado en la sección 4. Éstos se encargan de enviar esta información hasta el Hub 3/3 MB300E y al Hub #1D TCP/IP ubicados en el cuarto de comunicaciones.

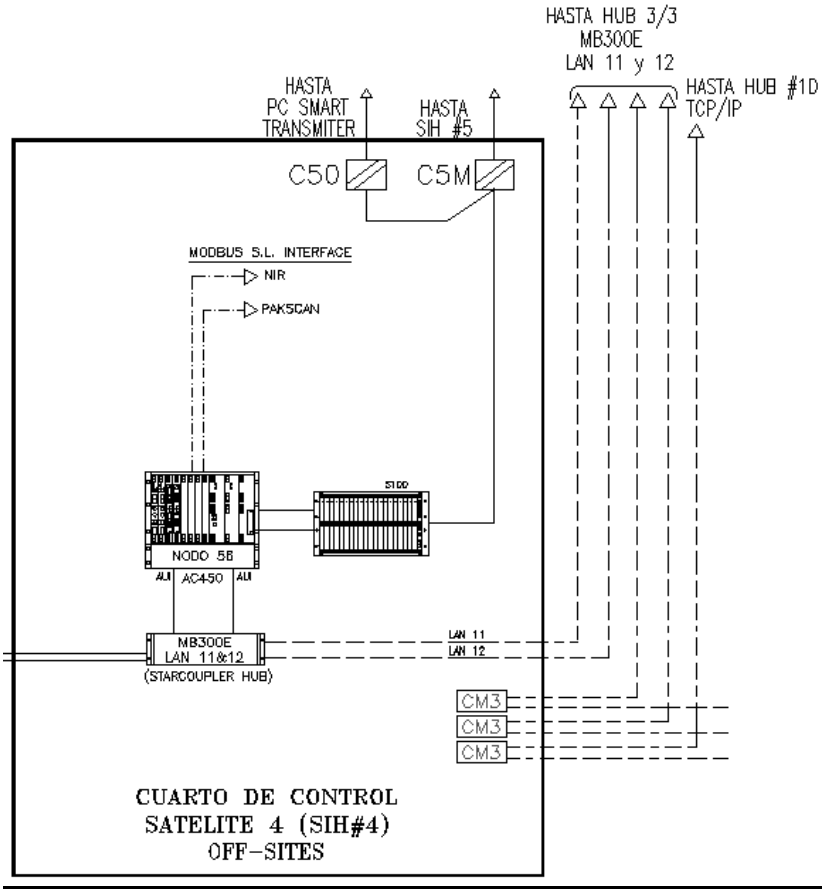

Figura 19. SIH #4 Off Sites

c. Sección 3: Cuarto de control satélite 5(SIH#5) TNP

En esta sección están ubicados(véase Figura 20):

- Un módulo de E/S (S100) conectado de manera redundante al controlador. Existe una conexión entre el módulo E/S y un conversor (C5M) de RS485 a fibra óptica monomodo con el fin de recibir información proveniente de la sección 2(SIH#4).
- Un controlador avanzado (AC450) conectado al módulo E/S y al Hub Starcoupler de la sección.

- Un Hub StarCoupler MB300E que se encarga de realizar la interfase entre la estación de operación (AS520) de la sección 4 y el controlador avanzado. También se encarga de enviar de manera redundante toda la información de proceso al HUB 3/3 de la red de control MB300E ubicado en el cuatro de control central pasando primero por los conversores CM3 ubicados en la sección 2.

- Tres conversores (CM3) de Fibra óptico multimodo a monomodo, que reciben la información del Starcoupler de la sección 3 y del conversor de UTP a fibra (CM1) ubicado en la sección 4. Éstos se encargan de enviar esta información hasta el Hub 3/3 MB300E y al Hub #1D TCP/IP ubicados en el cuarto de comunicaciones.

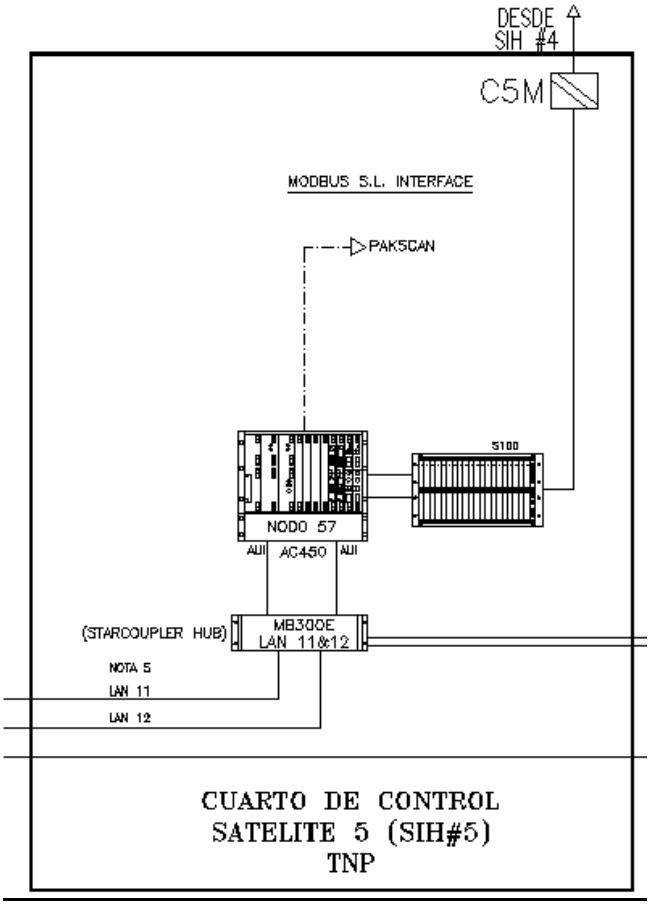

Figura 20. SIH #5 TNP

d. Sección 4: Cuarto de control satélite 5(LCB#5) TCP.

Aquí se ubica una estación de trabajo (AS520) que se encarga de realizar la supervisión y monitoreo de TNP. En ésta se pueden realizar los cambios de los parámetros del proceso correspondientes a este cuarto satélite(Véase Figura 21).

La CPU está conectada de manera redundante (dos cables) a un hub starcoupler MasterBus 300 localizado en la sección 3 de ésta área, esta comunicación se realiza vía fibra óptica por lo que se utilizan dos conversores(CM4) de AUI a fibra óptica multimodo. De la misma

manera se encuentra conectada a un conversor (CM1) de UTP a fibra óptica multimodo con el propósito de enviar la información al HUB #1D TCP/IP ubicado en el cuarto de comunicaciones, sin embargo, esta información no se envía directamente al cuarto de control central sino que pasa primero a través de uno del los conversores multimodo monomodo ubicados en las sección 2.

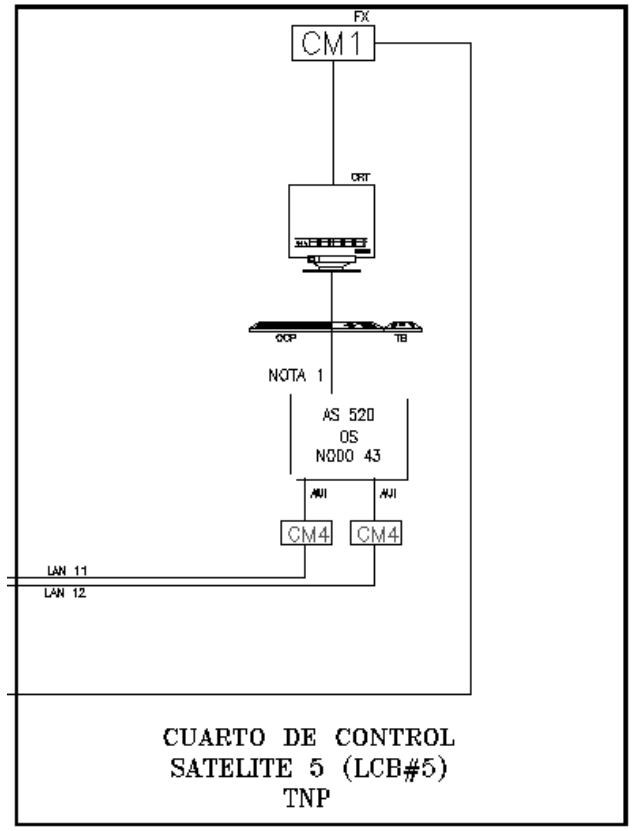

Figura 21. LCB #5 TNP

2.3.2. Cuarto de aplicaciones y cuarto de control central. El Hub 3/3 MB300E ubicado en el cuarto de comunicaciones se encarga de recibir de manera redundante la información proveniente de los cuartos satélites 4 y 5 y enviarla, también de manera redundante a través de cable coaxial, al grupo de consolas correspondiente de esta área utilizando una topología tipo bus. Paralelamente a la red MasterBus, cada una de las computadoras de este grupo están conectadas a la red TCP/IP mediante UTP al Hub#1B ubicado en el cuarto de comunicaciones. Estas consolas se pueden ver en la Figura 22.

Este grupo de consolas conformado por dos subgrupos: consolas de aplicación y las consolas de operador, estando las primeras en el cuarto de aplicaciones y las segundas en el cuarto de control central.

Las consolas de operador son un grupo de seis estaciones de operación (AS520) encargadas de realizar la supervisión y monitoreo de los procesos del área de elementos externos de manera remota. Ésta, al igual que en la consola de los cuartos satélites, permite realizar cambios en los parámetros del proceso.

Las consolas de aplicación son un grupo de 4 computadoras, donde 2 son estaciones de administración de información (AS530), 1 es una estación de ingeniería (AS520) y la restante es un PC Xterm 3. Al igual que en las demás áreas, esta computadora no esta conectado a la red MasterBus 300.

En el área también se incluyen el PC Star Blend, que se utiliza para realizar los modelos de optimización de blending; y el PC ABC, que se utiliza para realizar el control avanzado de esta área.

Su ubicación física es el cuarto de control central. Estos PCs no se conectan a través de la red masterBus sino mediante el Hub #2 TCP/IP.

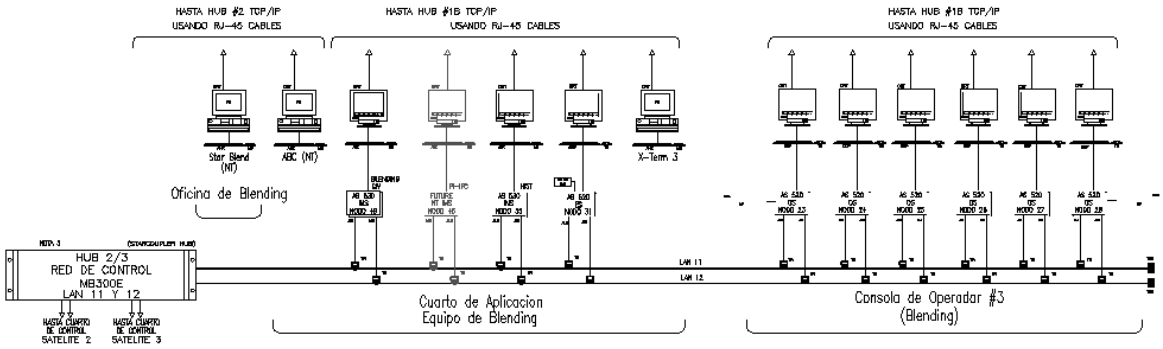

Figura 22. Consolas de aplicación y operación del área de elementos externos

Integrando los cuartos satélites y el grupo de consolas del cuarto de control central, la arquitectura del sistema de control del área de elementos externos se muestra en la Figura 23.

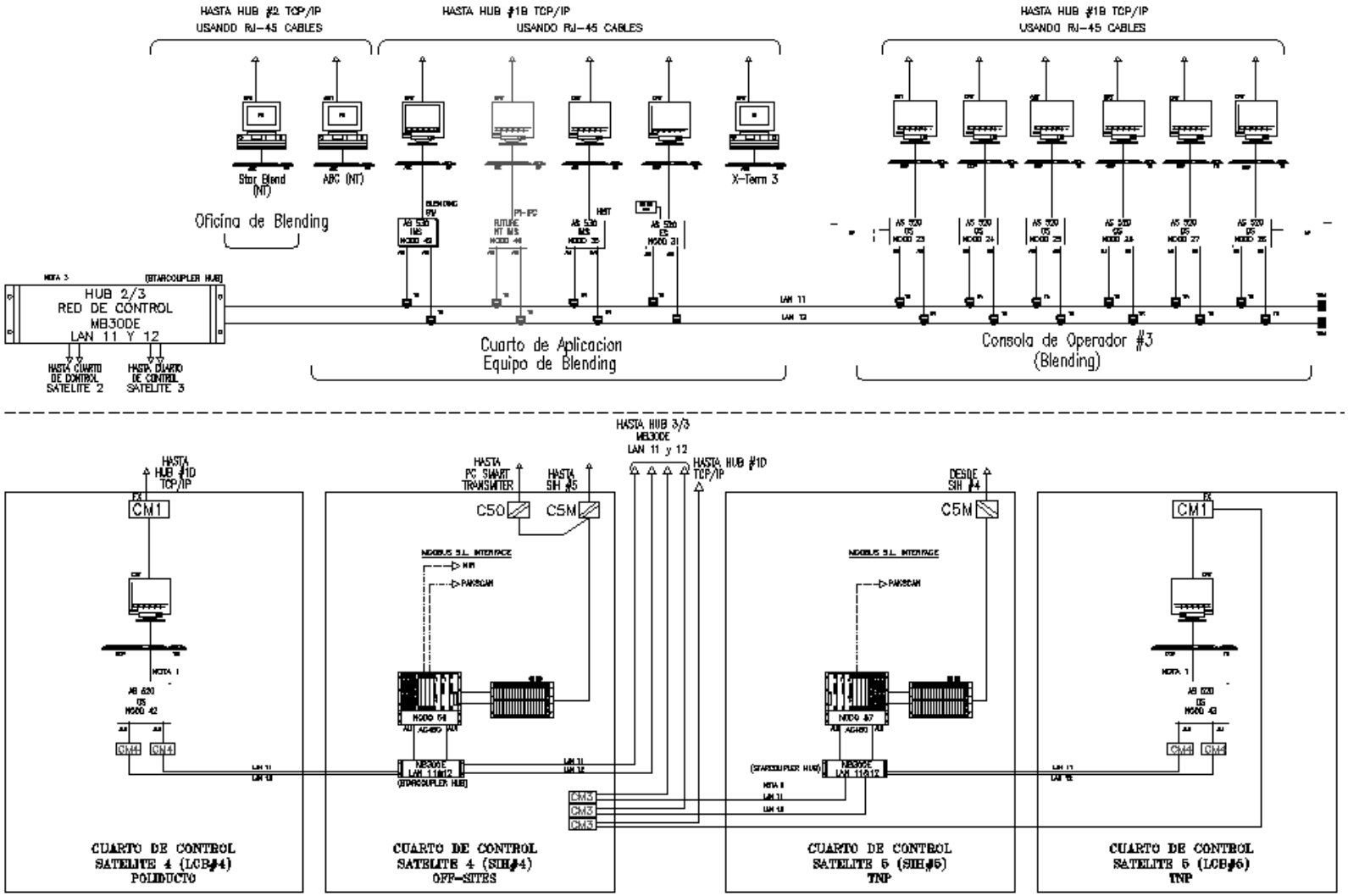

Figura 23. Arquitectura del sistema de control para el área de Elementos externos

2.4. ÁREA SERVICIOS INDUSTRIALES

2.4.1. Consolas Honeywell, Siemens y Foxboro. Este grupo constituye el grupo de consolas de los sistemas de control que se encontraban antes del montaje del nuevo sistema de control distribuido y que se han incluido en él. Estas consolas están conectadas a la red de planta a través del switch#4 TCP/IP. Cabe destacar que las consolas honeywell a un no han sido instaladas, por lo tanto, no se tendrán en cuenta ni para la descripción ni el análisis.

2.4.2. Sistema Utilities Siemens TELEPERM XPS. El sistema comienza en el cuarto satélite 6, donde se ubican dos módulos de fibra óptica conectados a una splice box, donde se reciben las señales ópticas. Esta splice box va comunicada con otra similar la cual va conectada a un hub OLM, que su vez conecta también a cada una de las terminales de operación del sistema de utilidades de siemens y a una computadora XU ubicada en el cuarto de comunicaciones en el rack de RTDM. En total son cuatro computadoras en el sistema siemens que van conectadas a manera de estrella y de forma redundante al OLM, las cuales también están conectadas a una red TCP/IP independientes de la del DCS ABB ADVANT. Estas cuatro computadoras están ubicadas en el CCB en el cuarto de control central junto a las consolas de operación de la demás áreas. En el cuarto de comunicaciones el XU es un equipo del DCS siemens que se conecta a la red siemens y posee una interfase TCP/IP. El XU tiene una conexión con el switch#4 y además va comunicado con un PC intermedio en el cual se corre el programa de la interfase con PI (Base de datos en tiempo real). En

este mismo rack RTDM se encuentra el servidor RDTM (HP9000) que tiene una conexión con el switch#4 y va conectado a un PC a través de PI IFC(Ver Figura 24).

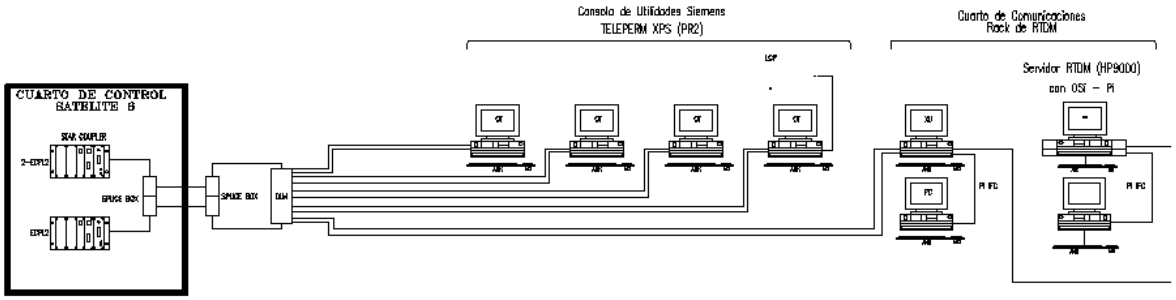

Figura 24. Sistema Utilities Siemens

2.4.3. Consola de utilidades Foxboro I/A PR3. Se tienen dos Módulos de fibra óptica (FONBE) conectados entre si a través de RG-75 y cada módulo va conectado una splice box. Esta splice box se comunica con una segunda splice box desde donde se distribuye la información a dos FONBE y estos a su vez se comunican a un computador a través de DNBT (Módulo de comunicaciones). Estos computadores(AW-51D) ubicadas en el cuarto de control central van conectados al switch#4, donde el primer computador es una consola de operación y el segundo es la interfase con la base de datos en tiempo real. Véase Figura 25.

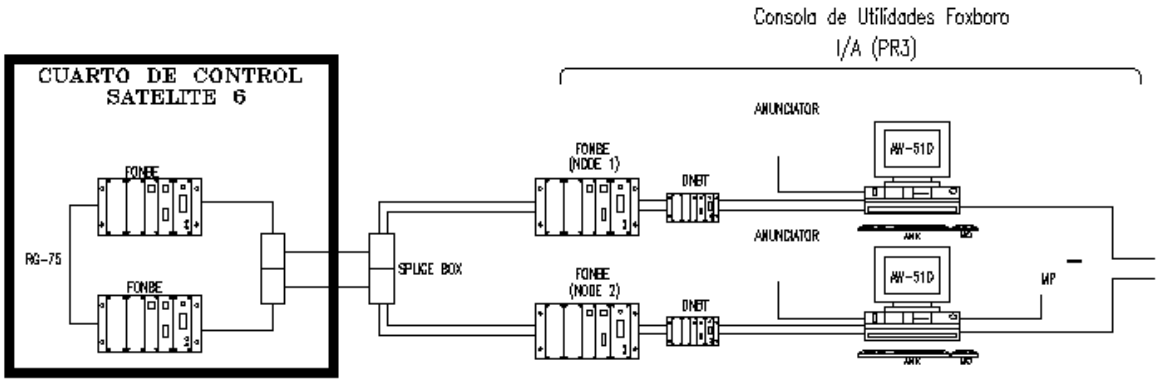

Figura 25. Consola de utilidades Foxboro I/A

El área completa de servicios industriales queda como se muestra en la Figura 26.

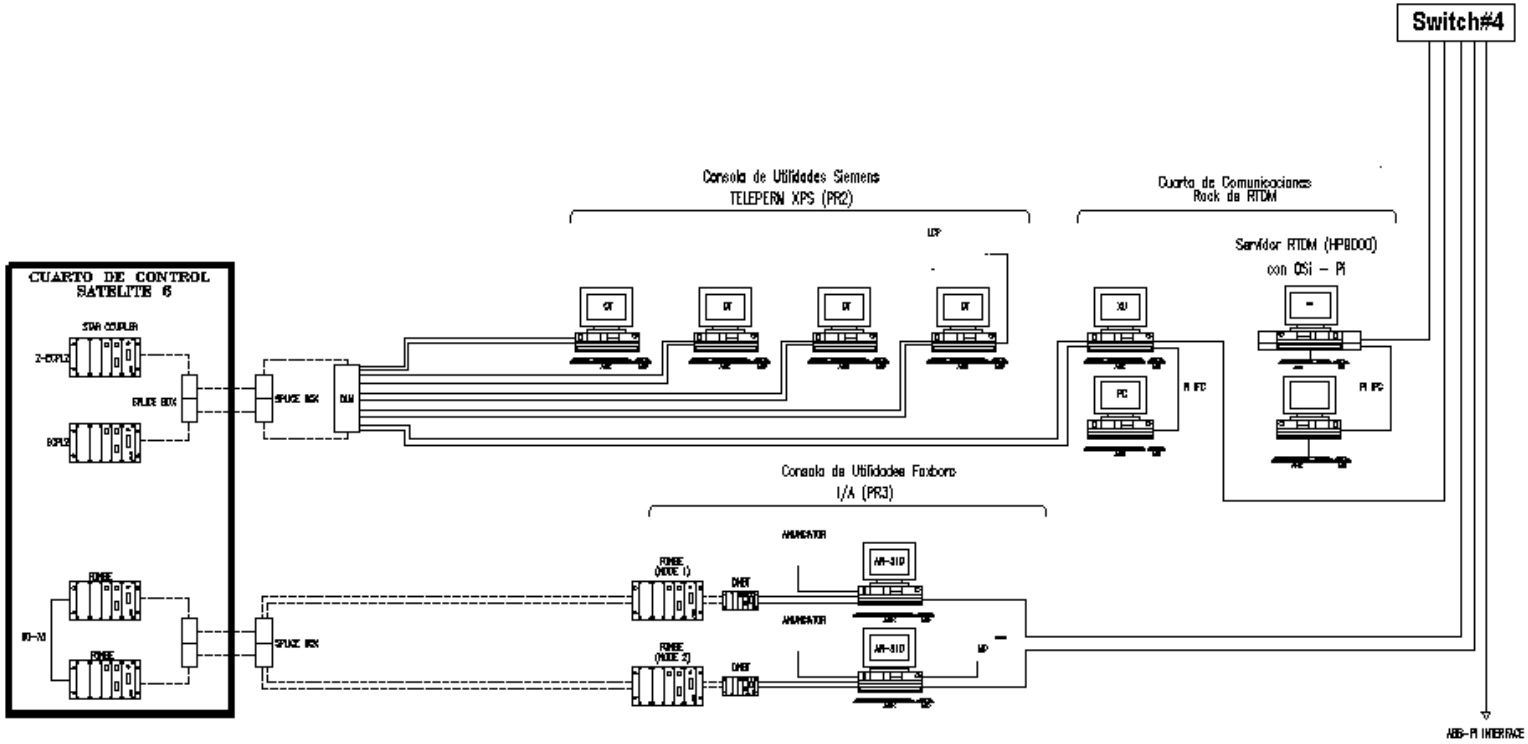

Figura 26. Arquitectura del sistema de control del área de Servicios industriales

2.5. EQUIPOS EN EL EDIFICIO DE CONTROL CENTRAL

Dentro del sistema de control distribuido además de los equipos de las áreas operativas de la empresa se encuentran otros grupos de equipos que cumplen funciones específicas, estos grupos son:

- Consolas de entrenamiento.
- Cuarto de mantenimiento.
- Computadores de la red Existente.
- Cuarto de comunicaciones.
- Cuarto eléctrico.

2.5.1. Consolas de entrenamiento. Esta conformado por seis consolas (AS520) distribuidas en 5 estaciones de operación y una de información. Estas consolas se utilizan para capacitación y para realizar simulaciones. Se conectan a través del hub#1B utilizando cables UTP. Véase Figura 27.

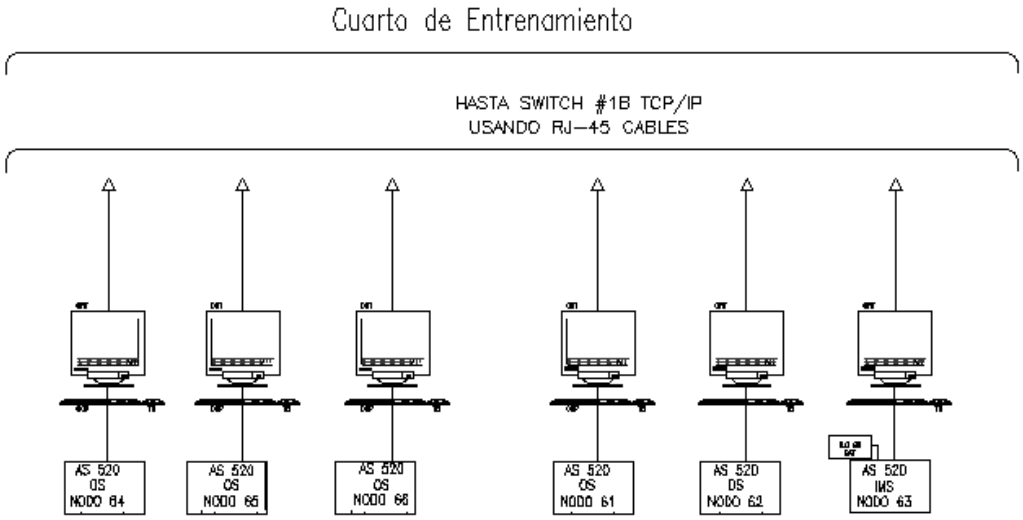

Figura 27. Consolas Cuarto de entrenamiento

2.5.2. Cuarto de mantenimiento. Los PCs del cuarto de mantenimiento(diríjase a la Figura 28) no están conectados a la red de planta TCP/IP, estos son:

- Smart transmiter interface: encargado de realizar el mantenimiento de la instrumentación HART.
- Multiplexer Ams Smart Transmitter Interface.
- NIR analizer system: que es un analizador infrarojo.
- VistaNet AMS (Analizer management system): que se utiliza para realizar analisis y mantenimiento.
- Bentley Nevada VMS2000: que monitorea las vibraciones de equipos críticos.

- Pc Portatil HVAC.

Estos computadores están conectados al hub 3.

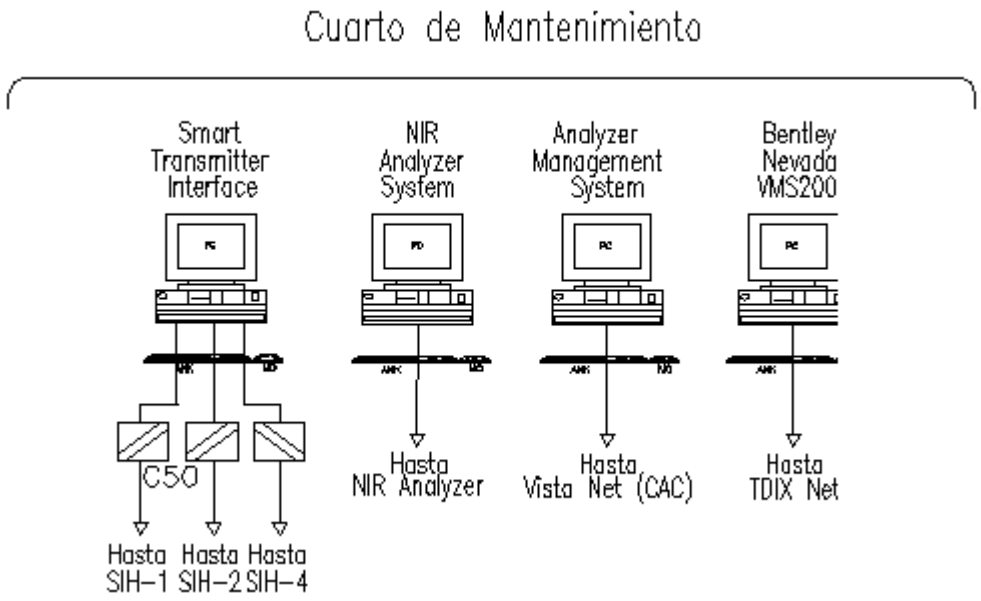

Figura 28. Consolas Cuarto de Mantenimiento

2.5.3. Computadores de la red existente. La Red existente (ver Figura 29) es en realidad la red de planta (red corporativa) que se encontraba antes del montaje del nuevo sistema de control distribuido. Esta compuesta por un grupo de computadoras conectadas a un switch ATM, utilizando protocolo TCP/IP. Los equipos más destacados de esta red son:

- SILabs - Sistema de información de laboratorios.

- RIS. - Base de datos que integra todos los sistemas de la refinería.

- SIO - Sistema de información de operaciones.

- PC Client - Para acceder a la información de la Base de datos en tiempo real.

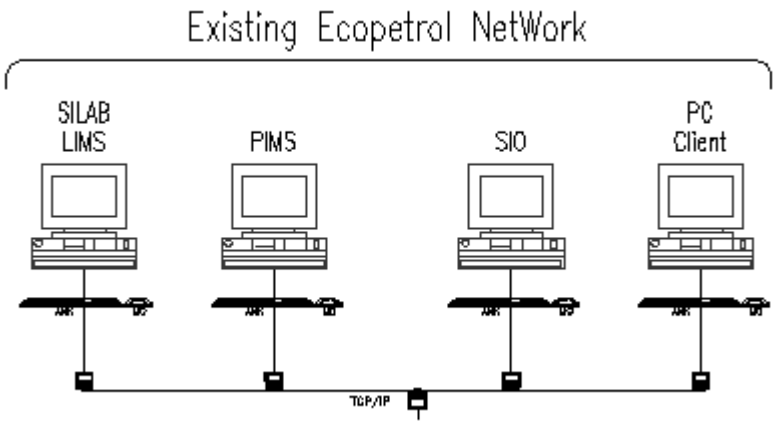

Figura 29. Computadoras de la red existente

2.5.4. Cuarto de comunicaciones. En este cuarto se realiza toda la interconexión del sistema de control distribuido. Aquí se realiza tanto la interconexión de la red de control (MasterBus) como de la red de planta (TCP/IP). Además de los hubs, switches, router y hubs starcoupler se encuentran otros equipos como:

- Servidor RTDM (HP9000) y PC.
- XU y PC del sistema de utilidades de SIEMENS.
- Estación Gateway PI-ABB.
- Estación de ingeniería sistema ABB.
- Estación de control avanzado ABC.

2.5.5. Cuarto eléctrico. En este se encuentran las tres UPS encargadas del respaldo eléctrico de los equipos del edificio de control central. En este edificio se encuentra: el cuarto de comunicaciones, cuarto de entrenamiento, cuarto de control central, cuarto de aplicación, el cuarto de mantenimiento y oficinas. Estas UPS ven conectadas a través de TCP/IP al switch#5.

2.5.6. Oficina del Administrador. Formado por:

- Short term scheduling and target setting: para realizar la planeación de la produccón.
- Data reconciliation: que se utiliza para determinar el balance de masa y reconciliación.

2.6. INTERCONEXION DE LA RED DE CONTROL

La red de control implementada en el sistema de control distribuido de la refinería es una MasterBus 300. Ésta es una red tipo propietaria utilizada para la interconexión de los equipos (controladores avanzados, estación de operación y aplicación, etc.) de control de la marca ABB.

Específicamente, en la refinería se colocó un hub starcoupler MB300E en cada cuarto satélite, de tal manera que sirviera de concentrador para el controlador avanzado y la estación de operación del satélite.

A través de este Hub se establece comunicación redundante con el Hub(MB300E) encargado del área de operación respectiva y localizado en el cuarto de comunicaciones. Con este último hub se

establece comunicación con las distintas consolas de operación y aplicación del área, ubicadas en el cuarto de control central.

En la Figura 30 se muestra un diagrama simplificado de la red de control.

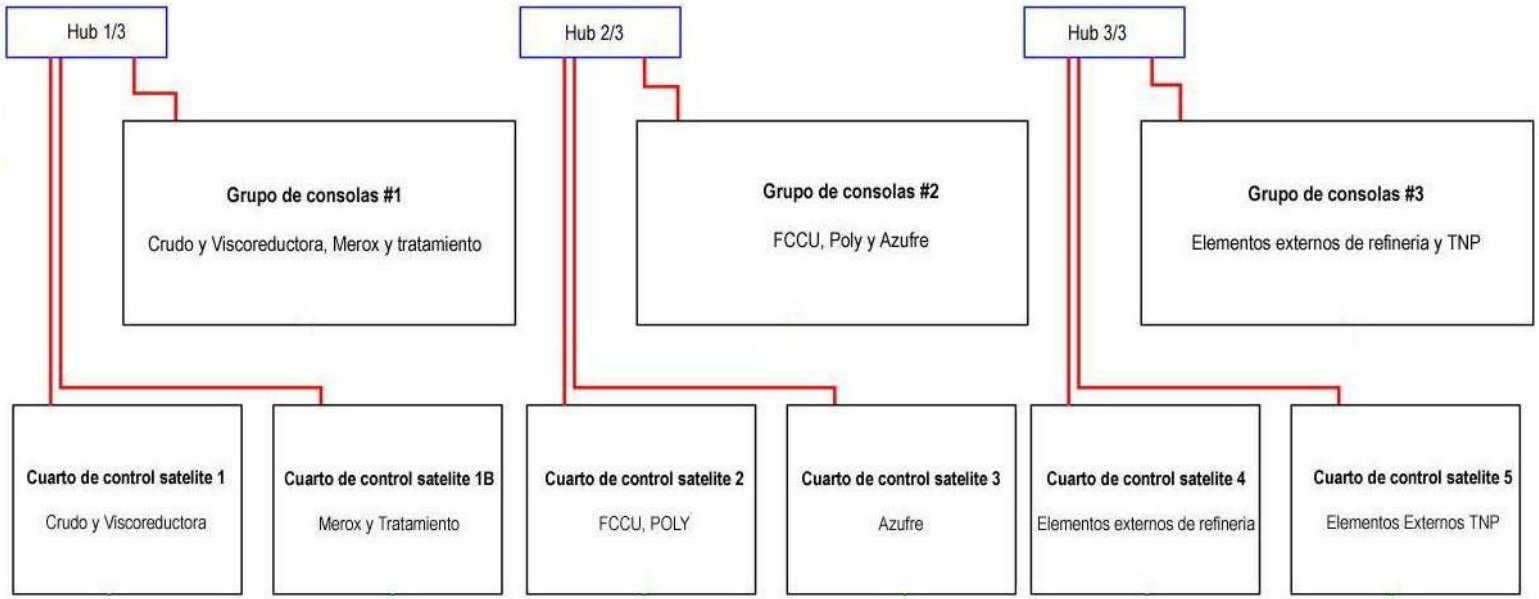

Figura 30. Arquitectura de la red de control MasterBus 300

Es importante destacar que en las políticas de seguridad a desarrollar no se tendrá en cuenta la red de control MasterBus 300. Esto se debe a que es una red muy segura, ya que es una red de protocolo propietario de ABB. Además de esto la red de control se encuentra dividida con respecto a las áreas en tres segmentos aislados, ya que no existe comunicación entre los tres hubs, por lo tanto, los servicios de un área no pueden ser accedidos por otra a través de esta red.

2.7. RED DE PLANTA

La interconexión de la red de planta se realiza con los equipos ubicados dentro del cuarto de comunicaciones. La interconexión de todo el sistema se realiza a través de un switch nivel 3 superstack II 3800 al que se conectan todos los hubs y switchs de la red la red planta. Esto se muestra en la Figura 31.

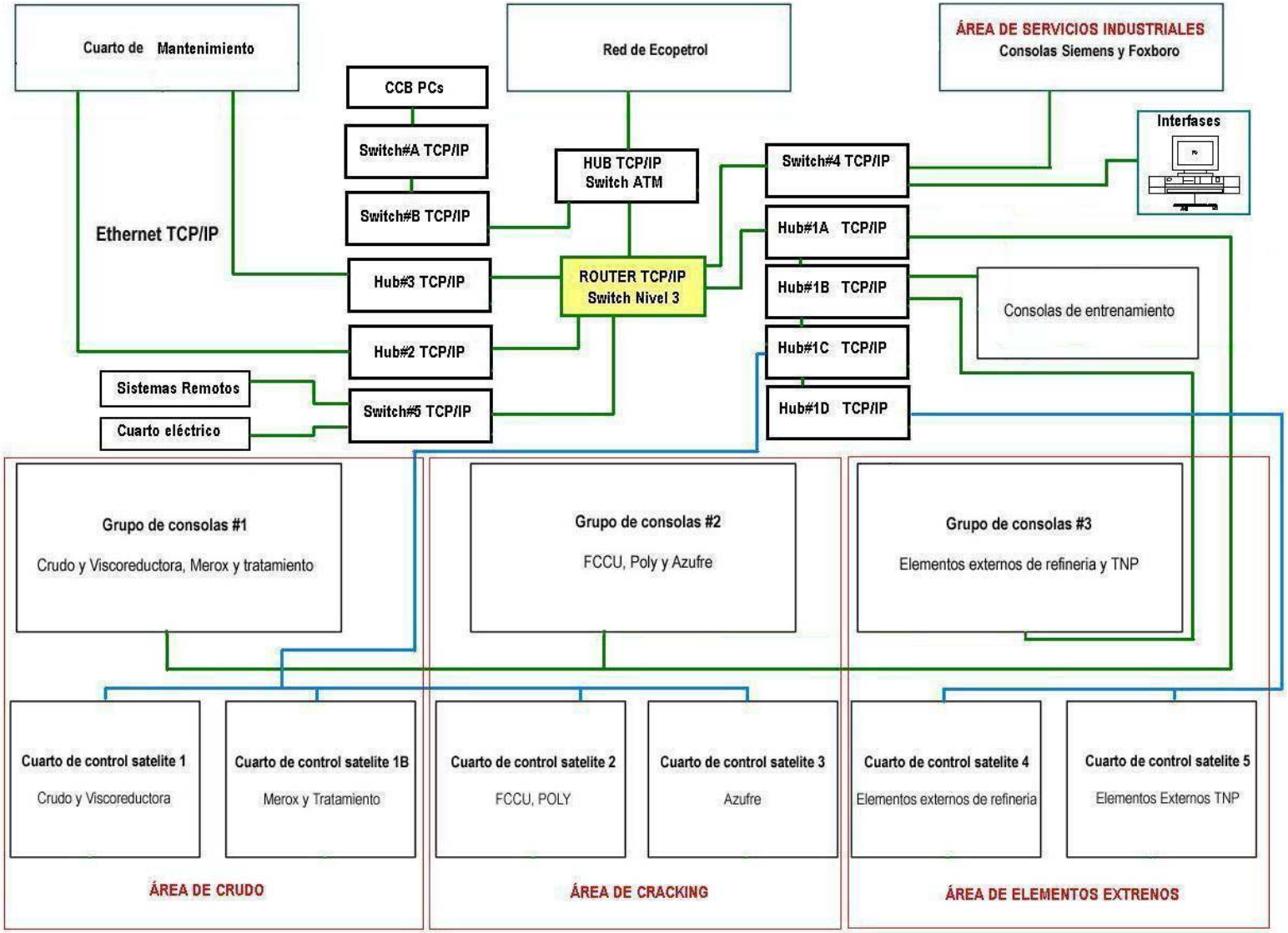

Figura 31. Arquitectura de la red de Planta TCP/IP

Los equipos del *cuarto de computadoras* se comunican con el router (switch nivel 3) a través de los hubs 3Com Superstack II Hub #3 y #2. Los equipos que se conectan al Hub#3 son: FCCU optimizer & Modelling, Short term scheduling and target setting, Data reconciliation. Los equipos que se conectan al Hub#2 son: Star Blend y ABC.

La *Red existente* antes del montaje del nuevo DCS se comunica con el router a través del switch ATM Core Builder 7000.

Los PCs de las oficinas del CCB(Central control building) se conectan al Switch#A y se comunican con el Switch ATM a través del Switch#B. Tanto el switch #A como el #B tienen como referencia 3Com Superstack II 3300.

El *área de servicios industriales* (consolas Foxboro, Siemens y Honeywell) al igual que el servidor RTDM HP9000 y todas las demás interfases tienen acceso a la red a través del Switch#4 que es un 3Com Superstack II switch.

Las consolas tanto de operador como de aplicación del *área de crudo* se conectan a la red a través del hub 1A 3Com Superstck hub 10 de igual manera que lo hacen las consolas de entrenamiento.

Las consolas de las *área de cracking y elementos externos* van conectadas a través del hub#1B 3Com Superstck hub 10.

Las consolas de los *cuartos satélites #1, #1B, #2 y #3* van conectadas a través de fibra óptica al Hub#1C 3Com Superstck hub 10, mientras que las de los *cuartos satélites #4 y #5* van conectadas al Hub#1D.

Como se muestra en la gráfica estos últimos 4 hubs están conectados en cascada por lo que el acceso al router se realiza a través del Hub#1A.

Los *sistemas remotos y el cuarto eléctrico* se conectan al router a través del switch#5.

2.8. LISTADO DE EQUIPOS

Para reconocer la cantidad de los equipos a analizar (véase Tabla 3), basados en la base de datos del administrador del sistema y en el esquema de configuración de la red de planta(Ver Anexo A), se realiza una lista con sus principales características como son localización, descripción, nodo equivalente en la red de control, tipo de equipo, nombre del host, dirección IP y sus conexión con la red de planta. Esta tabla será de mucha ayuda ya que servirá de soporte para realizar el análisis de la red TCP/IP para luego realizar recomendaciones al respecto.

Tabla 3. Listado de Equipos conectados a la red de planta.

Código localización	Descripción equipo	Dirección MB300	Código tipo equipo	Nombre host	Dirección TCP-IP	Conexión Red de Planta
CCB-CONSOLA3	ESTACION DE CONTROL AVANZADO DE BLENDING	0	PC	Eabc	150.67.13.6	Hub#2
CCB-COMUNIC-1	ESTACION DE CONTROL AVANZADO		PC	Eabc10	150.67.13.11	Hub#2
CCB-CONSOLA1	ESTACION DE OPERACIÓN #1 CONSOLA DE CRUDO	11	OS520	Eas110	150.67.14.11	Hub#1A
CCB-CONSOLA1	ESTACION DE OPERACIÓN #2 CONSOLA DE CRUDO	12	OS520	Eas120	150.67.14.12	Hub#1A
CCB-CONSOLA1	ESTACION DE OPERACIÓN #3 CONSOLA DE CRUDO	13	OS520	Eas130	150.67.14.13	Hub#1A
CCB-CONSOLA1	ESTACION DE OPERACIÓN #4 CONSOLA DE CRUDO	14	OS520	Eas140	150.67.14.14	Hub#1A
CCB-CONSOLA1	ESTACION DE OPERACIÓN #5 CONSOLA DE CRUDO	15	OS520	Eas150	150.67.14.15	Hub#1A
CCB-CONSOLA1	ESTACION DE OPERACIÓN #6 CONSOLA DE CRUDO	16	OS520	Eas160	150.67.14.16	Hub#1A
CCB-CONSOLA2	ESTACION DE OPERACIÓN #1 CONSOLA DE CRACKING	17	OS520	Eas170	150.67.14.17	Hub#1A
CCB-CONSOLA2	ESTACION DE OPERACIÓN #2 CONSOLA DE CRACKING	18	OS520	Eas180	150.67.14.18	Hub#1A
CCB-CONSOLA2	ESTACION DE OPERACIÓN #3 CONSOLA DE CRACKING	19	OS520	Eas190	150.67.14.19	Hub#1A
CCB-CONSOLA2	ESTACION DE OPERACIÓN #4 CONSOLA DE CRACKING	20	OS520	Eas200	150.67.14.20	Hub#1A
CCB-CONSOLA2	ESTACION DE OPERACIÓN #5 CONSOLA DE CRACKING	21	OS520	Eas210	150.67.14.21	Hub#1A
CCB-CONSOLA2	ESTACION DE OPERACIÓN #6 CONSOLA DE CRACKING	22	OS520	Eas220	150.67.14.22	Hub#1A
CCB-CONSOLA3	ESTACION DE OPERACIÓN #1 CONSOLA DE BLENDING	23	OS520	Eas230	150.67.14.23	Hub#1B
CCB-CONSOLA3	ESTACION DE OPERACIÓN #2 CONSOLA DE BLENDING	24	OS520	Eas240	150.67.14.24	Hub#1B
CCB-CONSOLA3	ESTACION DE OPERACIÓN #3 CONSOLA DE BLENDING	25	OS520	Eas250	150.67.14.25	Hub#1B
CCB-CONSOLA3	ESTACION DE OPERACIÓN #4 CONSOLA DE BLENDING	26	OS520	Eas260	150.67.14.26	Hub#1B
CCB-CONSOLA3	ESTACION DE OPERACIÓN #5 CONSOLA DE BLENDING	27	OS520	Eas270	150.67.14.27	Hub#1B
CCB-CONSOLA3	ESTACION DE OPERACIÓN #6 CONSOLA DE BLENDING	28	OS520	Eas280	150.67.14.28	Hub#1B
CCB-APLICACION1	ESTACION DE INGENIERIA SISTEMA DE CRUDO	29	OS520	Eas290	150.67.14.29	Hub#1A
CCB-APLICACION2	ESTACION DE INGENIERIA SISTEMA DE CRACKING	30	OS520	Eas300	150.67.14.30	Hub#1A
CCB-APLICACION3	ESTACION DE INGENIERIA SISTEMA DE BLENDING	31	OS520	Eas310	150.67.14.31	Hub#1B
SIH#1-CONSOLA	ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRUDO	38	OS520	Eas380	150.67.14.38	Hub#1C
SIH#1-CONSOLA	ESTACION DE OPERACIÓN LOCAL SISTEMA DE TRATAMIENTO	39	OS520	Eas390	150.67.14.39	Hub#1C
LCB#2-CONSOLA	ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRACKING	40	OS520	Eas400	150.67.14.40	Hub#1C
LCB#3-CONSOLA	ESTACION DE OPERACIÓN LOCAL SISTEMA DE AZUFRE	41	OS520	Eas410	150.67.14.041	Hub#1C
LCB#4-CONSOLA	ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING REFINERIA	42	OS520	Eas420	150.67.14.042	Hub#1D
LCB#5-CONSOLA	ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING TNP	43	OS520	Eas430	150.67.14.43	Hub#1D
CCB-ENTRENAMIENTO	ESTACION DE OPERACIÓN #1 SISTEMA DE ENTRENAMIENTO	61	OS520	Eas610	150.67.14.61	Hub#1B Hub of-Con
CCB-ENTRENAMIENTO	ESTACION DE OPERACIÓN #2 SISTEMA DE ENTRENAMIENTO	62	OS520	Eas620	150.67.14.62	Hub#1B Hub of-Con

Código localización	Descripción equipo	Dirección MB300	Código tipo equipo	Nombre host	Dirección TCP-IP	Conexión Red de Planta
CCB-ENTRENAMIENTO	ESTACION DE OPERACIÓN #5 SISTEMA DE ENTRENAMIENTO	64	OS520	Eas640	150.67.14.64	Hub#1B Hub of-Con
CCB-ENTRENAMIENTO	ESTACION DE OPERACIÓN #4 SISTEMA DE ENTRENAMIENTO	65	OS520	Eas650	150.67.14.65	Hub#1B Hub of-Con
CCB-ENTRENAMIENTO	ESTACION DE OPERACIÓN #3 SISTEMA DE ENTRENAMIENTO	66	OS520	Eas660	150.67.14.66	Hub#1B Hub of-Con
CCB-CONSOLA4	ESTACION DE OPERACION Y GATEWAY #1 FOXBORO	0	AW51	Eaw030	150.67.14.121	Switch#4
CCB-CONSOLA4	ESTACION DE OPERACION Y GATEWAY #1 FOXBORO	0	AW51	Eaw040	150.67.14.122	Switch#4
CCB-COMUNIC-PI	ESTACION DE BASE DE DATOS EN TIEMPO REAL	0	UNIX	Ebdtr	150.67.13.1	Switch#4
CCB-MANTENIMIENTO	ESTACION BENTLY NEVADA	0	PC	Ebn	150.67.13.13	Hub#3
CCB-MANTENIMIENTO	ESTACION DE ANALIZADORES VISTANET	0	PC	Ecac	150.67.13.10	Hub#3
CCB-COMUNIC-1	ESTACION DE INGENIERIA SISTEMA ABB		PC	Ees00	150.67.14.10	Hub#1A
CCB-CONSOLA1	ESTACION #1 SISTEMA DE SHUTDOWN DE CRUDO	0	PC	Eesd10a	150.67.16.51	Switch#5
CCB-CONSOLA1	ESTACION #2 SISTEMA DE SHUTDOWN DE CRUDO	0	PC	Eesd10b	150.67.16.52	Switch#5
SIH#1-CONSOLA	ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRUDO	0	PC	Eesd10c	150.67.16.53	Switch#5
CCB-CONSOLA2	ESTACION #1 SISTEMA DE SHUTDOWN DE CRACKING	0	PC	Eesd20a	150.67.16.55	Switch#5
CCB-CONSOLA2	ESTACION #2 SISTEMA DE SHUTDOWN DE CRACKING	0	PC	Eesd20b	150.67.16.56	Switch#5
LCB#2-CONSOLA	ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRACKING	0	PC	Eesd20c	150.67.16.57	Switch#5
LCB#3-CONSOLA	ESTACION LOCAL SISTEMA DE SHUTDOWN DE AZUFRE	0	PC	Eesd20d	150.67.16.58	Switch#5
CCB-MANTENIMIENTO	MULTIPLEXER AMS SMART TRANSMITTER INTERFACE	0	MX	Ihmux	150.67.13.8	Hub#3
CCB-MANTENIMIENTO	ESTACION AMS SMART TRANSMITTER INTERFACE - HART	0	PC	Ehpc	150.67.13.7	Hub#3
CCB-COMUNIC-RACK	ROUTER SUPER STACK 3800	0	ETHERNET	Ehub	150.67.16.1	
CCB-COMUNIC-RACK	HUB 24 PUERTOS UTP RED DE PLANTA ABB	0	ETHERNET	Ehub10	150.67.16.2	
CCB-COMUNIC-RACK	HUB 24 PUERTOS UTP RED DE PLANTA ABB	0	ETHERNET	Ehub10	150.67.16.2	
CCB-COMUNIC-RACK	HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	0	ETHERNET	Ehub10	150.67.16.2	
CCB-COMUNIC-RACK	HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	0	ETHERNET	Ehub10	150.67.16.2	
CCB-COMUNIC-RACK	HUB 24 PUERTOS UTP BLENDING	0	ETHERNET	Ehub20	150.67.16.3	
CCB-COMUNIC-RACK	HUB 24 PUERTOS UTP CONTROL AVANZADO	0	ETHERNET	Ehub30	150.67.16.4	
CCB-COMUNIC-RACK	SWITH 12 PUERTOS UTP BASE DE DATOS EN TIEMPO REAL	0	ETHERNET	Ehub40	150.67.16.5	
CCB-COMUNIC-RACK	SWITH 24 PUERTOS UTP ESD Y UPS	0	ETHERNET	Ehub50	150.67.16.6	
CCB-MANTENIMIENTO	PC PORTATIL HVAC	0	PORTATIL	Ehvac	150.67.13.12	Hub#3
CCB-APLICACION1	ESTACION DE HISTORIA SISTEMA DE CRUDO	33	IMS530	Eims330	150.67.14.33	Hub#1A
CCB-APLICACION2	ESTACION DE HISTORIA SISTEMA DE CRACKING	34	IMS530	Eims340	150.67.14.34	Hub#1A
CCB-APLICACION3	ESTACION DE HISTORIA SISTEMA DE BLENDING	35	IMS530	Eims350	150.67.14.35	Hub#1B
CCB-APLICACION1	ESTACION GATEWAY PI SISTEMA DE CRUDO	44	IMS530	Eims440	150.67.14.44	Switch#4
CCB-APLICACION2	ESTACION GATEWAY PI SISTEMA DE CRACKING	45	IMS530	Elms450	150.67.14.45	Switch#4
CCB-APLICACION3	ESTACION GATEWAY PI SISTEMA DE BLENDING	46	IMS530	Elms460	150.67.14.46	Switch#4
CCB-COMUNIC-1	ESTACION GATEWAY PI-ABB	47	IMS530	Eims470	150.67.14.47	Switch#4

Código localización	Descripción equipo	Dirección MB300	Código tipo equipo	Nombre host	Dirección TCP-IP	Conexión Red de Planta
CCB-ENTRENAMIENTO	ESTACION DE HISTORIA SISTEMA DE ENTRENAMIENTO	63	IMS530	Eims630	150.67.14.63	Hub#1B Hub of-Con
CCB-ENTRENAMIENTO	IMPRESORA LASER A COLOR SISTEMA DE ENTRENAMIENTO	0	LCP	ILcp10	150.67.15.1	
CCB-CONSOLA4	IMPRESORA LASER A COLOR OPERADORES DE CONSOLA	0	LCP	ILcp20	150.67.15.2	
CCB-SISTEMA	IMPRESORA LASER A COLOR ADMINISTRADOR DEL SISTEMA	0	LCP	Ilcp30	150.67.15.3	
CCB-MANTENIMIENTO	IMPRESORA LASER A COLOR CUARTO DE MANTENIMIENTO	0	LCP	Ilcp40	150.67.15.4	
CCB-APLICACION2	IMPRESORA LASER A COLOR SISTEMA DE INGENIERIA	0	LCP	Ilcp50	150.67.15.5	Hub#1A
CCB-COMUNIC-1	IMPRESORA LASER BLANCO Y NEGRO ADMINISTRADOR PI	0	LP	ILip60	150.67.15.6	Hub#3
CCB-COMUNIC-RACK	HUB MB300 PARA SISTEMA DE CRUDO	0	MB300			
CCB-COMUNIC-RACK	HUB MB300 PARA SISTEMA DE CRACKING	0	MB300			
CCB-COMUNIC-RACK	HUB MB300 PARA SISTEMA DE BLENDING	0	MB300			
SIH#1-DCS	STAR COUPLER MB300 PARA SISTEMA DE CRUDO	0	MB300			
SIH#1B-DCS	STAR COUPLER MB300 PARA SISTEMA DE TRATAMIENTO	0	MB300			
SIH#2-DCS	STAR COUPLER MB300 PARA SISTEMA DE CRACKING	0	MB300			
SIH#3-DCS	STAR COUPLER MB300 PARA SISTEMA DE AZUFRE	0	MB300			
SIH#4-DCS	STAR COUPLER MB300 PARA SISTEMA DE BLENDING REFINERIA	0	MB300			
SIH#5-DCS	STAR COUPLER MB300 PARA SISTEMA DE BLENDING TNP	0	MB300			
CCB-COMUNIC-RACK	SWITCHE MB300 MULTILAN PARA RED 11	0	MB300			
CCB-COMUNIC-RACK	SWITCHE MB300 MULTILAN PARA RED 12	0	MB300			
CCB-COMUNIC-1	IMPRESORA MATRIZ DE PUNTO CONSOLA DE CRUDO 1	0	MP			
CCB-CONSOLA1	IMPRESORA MATRIZ DE PUNTO CONSOLA DE CRUDO 2	0	MP			
CCB-CONSOLA2	IMPRESORA MATRIZ DE PUNTO CONSOLA DE CRACKING 1	0	MP			
CCB-CONSOLA2	IMPRESORA MATRIZ DE PUNTO CONSOLA DE CRACKING 2	0	MP			
CCB-CONSOLA3	IMPRESORA MATRIZ DE PUNTO CONSOLA DE BLENDING 1	0	MP			
CCB-CONSOLA3	IMPRESORA MATRIZ DE PUNTO CONSOLA DE BLENDING 1	0	MP			
CCB-MANTENIMIENTO	IMPRESORA MATRIZ DE PUNTO A COLOR BENTLY NEVADA	0	MP			
CCB-CONSOLA1	IMPRESORA MATRIZ DE PUNTO SISTEMA ESD DE CRUDO	0	MP			
CCB-CONSOLA2	IMPRESORA MATRIZ DE PUNTO SISTEMA ESD DE CRACKING	0	MP			
CCB-MANTENIMIENTO	ESTACION NIR	0	PC	Enir	150.67.13.9	Hub#3
CCB-APLICACION2	ESTACION DEL OPTIMIZADOR DE CRACKING	0	PC	Eopti	150.67.13.4	Hub#3
CCB-SISTEMA	ESTACION DE RECONCILIACION DE DATOS	0	PC	EReda	150.67.13.3	
CCB-CONSOLA4	ESTACION DE OPERACION #1 SIEMENS	0	OT	Esie010	150.67.14.123	N.A.
CCB-CONSOLA4	ESTACION DE OPERACION #2 SIEMENS	0	OT	Esie020	150.67.14.124	N.A.
CCB-CONSOLA4	ESTACION DE OPERACION #3 SIEMENS	0	OT	Esie030	150.67.14.125	N.A.
CCB-CONSOLA4	ESTACION DE OPERACION #4 SIEMENS	0	OT	Esie040	150.67.14.126	N.A.
CCB-COMUNIC-PI	ESTACION GATEWAY SIEMENS	0	XU	Esie050	150.67.14.127	Switch#4

Código localización	Descripción equipo	Dirección MB300	Código tipo equipo	Nombre host	Dirección TCP-IP	Conexión Red de Planta
CCB-COMUNIC-PI	ESTACION PC ESCLAVO SIEMENS	0	PC	Esie060	150.67.14.128	
CCB-CONSOLA3	ESTACION DE STAR BLEND	0	PC	Estarb	150.67.13.5	Hub#2
CCB-SISTEMA	ESTACION DE SHORT TERM SCHEDULLING	0	PC	Ests	150.67.13.2	Hub#3
CCB-UPS	UPS No.1 CCB	0	UPS		150.67.16.101	Switch#5
CCB-UPS	UPS No.2 CCB	0	UPS		150.67.16.102	Switch#5
CCB-UPS	UPS No.3 CCB	0	UPS		150.67.16.103	Switch#5
SIH#1	UPS No.1 SIH#1	0	UPS		150.67.16.104	Switch#5
SIH#1	UPS No.2 SIH#1	0	UPS		150.67.16.105	Switch#5
SIH#2	UPS No.1 SIH#2	0	UPS		150.67.16.106	Switch#5
SIH#2	UPS No.2 SIH#2	0	UPS		150.67.16.107	Switch#5
SIH#3	UPS No.1 SIH#3	0	UPS		150.67.16.108	Switch#5
SIH#3	UPS No.2 SIH#3	0	UPS		150.67.16.109	Switch#5
CCB-APLICACION1	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRUDO	0	PC	EXterm10	150.67.14.130	Hub#1A
CCB-APLICACION2	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRACKING	0	PC	EXterm20	150.67.14.131	Hub#1A
CCB-APLICACION3	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE BLENDING	0	PC	EXterm30	150.67.14.132	Hub#1B

2.9. LISTA DE SERVICIOS

La lista de servicios ofrecidos en los equipos del sistema de control distribuido de estará organizada según el tipo de equipo. Para esta lista de servicios no se tendrán en cuenta los equipos que prestan servicios básicos tales como impresoras y multiplexores. La lista de servicios por equipos es la siguiente:

2.9.1. Equipos Ethernet. Estos equipos están conformados por los hubs, switchs y el router utlizados para el enrutamiento de la red ethernet. El único servicio que puede ejecutarse es Telnet, el cual es utilizado para la configuración de los mismos.

2.9.2. OS520, IMS530. Están conformados por las distintas estaciones de información, operación e ingeniería de cada área. En estas estaciones se corren servicios básicos tales como telnet, ftp, smtp, http y pop3. Además se tienen otro gran número de servicios que no serán listados por confidencialidad de ésta información, por lo tanto sólo se emitirán recomendaciones de manera general en el capítulo V.

2.9.3. PCs y Portátiles. Son equipos de soporte que se utilizan en las distintas oficinas del edificio de control central que utilizan los ingenieros para realizar las labores diarias. Estos equipos como tales no corren servicios directos que puedan comprometer la seguridad del sistema, sin embargo, pueden ser instaladas herramientas que permitan tener acceso remoto a partes críticas del sistema de control, tales como:

- Exceed: con este software es posible acceder remotamente a través de TCP/IP a las estaciones de operación e ingeniería que tengan estos servicios instalados.

- Software de UPS: las UPS poseen un software que permite el monitoreo remoto y en algunos casos funciones de operación de las mismas, por lo cual pueden efectuarse cambios en sus modos de operación y maniobras de encendido y apagado.

2.9.4. Estación UNIX de la base de datos en tiempo real. Se refiere al equipo que contiene la base de datos en tiempo real localizado en el cuarto de comunicaciones. Tiene instaladas dos tarjetas de red, una para realizar la interfase con el sistema de control y otra para que los clientes de refinería puedan acceder a la base de datos.

2.9.5. UPS. Los servicios que pueden brindar estas UPSs son monitoreo y operación remota. Cabe destacar que para realizar el monitoreo y operación es necesario tener instalado el software en un computador que esté conectado a la red.

2.9.6. ESD. Están se encuentran clasificadas dentro del tipo de equipos PC, sin embargo, por realizar servicios específicos de shutdown se mencionan de manera separada. Corren bajo el sistema operativo Windows 2000. En estos se ejecutan los siguientes programas:

- I/O Server: se utiliza para conectar al PC con la red Modbus y establecer comunicación con los PLCs del sistema.

- Software Intouch: se utiliza para visualizar desplegables de los datos recogidos por el I/O Server a través de TCP/IP. Además se puede realizar el diseño de estos desplegables.

2.10. USUARIOS

Los usuarios, al igual que los servicios, se clasificarán de acuerdo al tipo de equipo. Los usuarios según los tipos de equipos son los siguientes:

2.10.1. Ethernet y OS520 IMS530. Los usuarios que tienen habilitados estos equipos son los usuarios por defecto con los que viene de fábrica. Para la realización de las políticas se analizó el archivo etc/passwd, que se encuentra en las OS520 e IMS530. Por cuestiones de confidencialidad no se listará la información contenida en este archivo, sin embargo, en el capítulo IV se emitirán recomendaciones basadas en el análisis de esta información.

2.10.2. PCs y portátiles. Tiene habilitados lo usuarios que hayan creado una sesión en el entorno Windows.

2.10.3. Estación Unix de la base de datos en tiempo real. Tiene como usuarios principales (con mayores privilegios) a los administradores de la red del sistema de control, los cuales acceden a

través de una de la tarjeta de red encargada de la interfase para el sistema de control. También, cada cliente es usuario de este sistema pero sólo puede acceder por la conexión de la red del sistema de datos de la refinería, a través de la otra tarjeta de red para los clientes de refinería.

2.10.4. UPS. Para el manejo de las UPSs no se tienen usuarios definidos.

2.10.5. ESD. El único usuario que tienen habilitado es el administrador.

3. POLÍTICAS DE SEGURIDAD

3.1. RESEÑA HISTÓRICA DE LA SEGURIDAD COMPUTACIONAL

Desde los comienzos de la computación, los sistemas han estado expuestos a una serie de peligrosos riesgos que han aumentando conforme se globalizan más las comunicaciones entre estos sistemas. Inicialmente la seguridad fue enfocada al control de acceso físico ya que para acceder a un computador se requería la presencia física del usuario frente al sistema.

Posteriormente comienzan a proliferar los sistemas multiusuario en los cuales un recurso computacional era compartido por varios usuarios, surgen nuevos riesgos como la utilización del sistema por personas no autorizadas, manipulación de información o aplicaciones por suplantación de usuarios, aparece un primer esquema de protección basado en códigos de usuarios y contraseñas (passwords) para restringir el acceso al sistema, además se establecen distintas categorías de control de acceso a los recursos.

Siguen evolucionando los sistemas y se inicia la computación en red, en la cual además de los riesgos asociados a los sistemas multiusuarios, aparece un nuevo tipo de vulnerabilidad, básicamente en el proceso de transmisión de la información; aunque las primeras redes estaban aisladas del mundo exterior a la empresa, estaban expuestas a los posibles atacantes internos.

La evolución tecnológica continúa y comienza el proceso de interconexión de las distintas redes aisladas de una empresa para configurar redes corporativas, donde aumentan considerablemente los riesgos ya que es más difícil controlar la totalidad de la red. Quizás hoy en día las redes

empresariales están siendo conectadas a redes públicas como Internet, CompuServer, BitNet, etc., en las cuales la seguridad se ha convertido en un problema realmente serio, pero a pesar que nuestro horizonte de oportunidades ha sido ampliado a millones de potenciales clientes, los posibles atacantes también han crecido en forma considerable.

Es responsabilidad de los diseñadores y administradores de los sistemas computacionales, proveer la suficiente garantía y confiabilidad que permita operar en las mejores condiciones y lograr un funcionamiento continuo de los sistemas bajo el mejor clima de confianza de los usuarios, garantizando el respeto por niveles adecuados de confidencialidad e integridad de la información que se procesa. Aunque inicialmente el interés de entrar ilegalmente a los sistemas fue el reto técnico de lograrlo, el número de incidentes y ganancias por la entrada ilegal ha aumentado considerablemente. Incidentes como el robo de información, espionaje industrial, estafas, extorsión, daño de sistemas, terrorismo, etc. se cuentan como los nuevos objetivos de ataques a nuestros sistemas. Entre los aspectos más relevantes de preocupación en los sistemas de seguridad se encuentra todo lo relacionado con:

- Los típicos servidores con sistemas operativos como UNIX, DEC, NT, Netware, etc. los cuales, de alguna forma, representan grandes riesgos.
- Los protocolos de comunicaciones representan uno de los puntos de vulnerabilidad más utilizado en las redes.
- Las aplicaciones del sistema o de los usuarios.
- Bases de datos, entre otros tópicos.

Definitivamente si se quieren minimizar los riesgos (nunca hay un sistema 100% protegido), se debe tomar conciencia del problema y adoptar una metodología o guías para enfrentarlo. Esto comienza con el conocimiento profundo de nuestra red, un análisis de amenazas y riesgos, la adopción de políticas de seguridad y finalmente la utilización de las tecnologías adecuadas para implantar un sistema de seguridad, el cual incorpora herramientas de criptografía, cortafuegos (Firewalls), monitoreo, auditoría y hasta esquemas proactivos que permita adelantarse a los ataques y prevenirlos.

3.2. INTERCONEXIÓN DE LAS REDES CORPORATIVAS CON LAS REDES DE CONTROL[1]

La mayoría de las redes de instalaciones empresariales involucran a los sistemas de control distribuido(DCS) y sistemas de monitoreo como los sistemas SCADA. Estos varían en complejidad, pero de manera típica, todos recolectan los datos de medición, manejan interruptores de potencia o ajustan válvulas de proceso que llevan agua, aceita y gas, examinan los datos que llegan y gobiernan múltiples dispositivos de red.

Las redes de proceso en una empresa a menudo están basadas en telemetría y en adquisición simple de datos y típicamente están provistas de pocas o ninguna medida de seguridad cuando se compara con las infraestructuras de las redes corporativas de hoy. Los grupos de ingenieros y las personas que toman las decisiones corporativas tienden a realizar la conexión entre la red corporativa y las redes SCADA o del DCS para obtener acceso en tiempo real a los datos críticos de operación del sistema. Por el hecho de que las medidas de seguridad y los protocolos están muy

[1] Utility Network Security, Protecting DCS and SCADA networks from damaging cyber-attacks. Pag. 1

ligados, algunos estudios recientes han identificado que muy pocos protocolos son realmente seguros a la hora de proteger el acceso a equipos de control del sistema de la red de control.

Debido a la gran complejidad de integrar sistemas que contrastan, dicho grupo de ingenieros a menudo falla en el intento de proveer controles adecuados de acceso para proteger los sistemas o equipos de la red de control en contra de accesos no autorizados, ya sea desde intentos internos o externos. Se recomienda el uso de firewalls internos y sistemas de detección de intrusos(IDS) combinados con políticas robustas de passwords desde el perímetro de una red sensible, pero pocas organizaciones protegen todos lo puntos de entrada al sistema de la red de control.

También, los sistemas de control tienden a depender de la relación con socios estratégicos y consultores externos. Estas relaciones resultan en que se incrementa tanto el número de individuos con estatus de nivel de administrador como el número de puntos de accesos a esta infraestructura. Los usuarios de la clase administrativa (o superusuarios) procesan passwords para efectuar las operaciones de configuración y mantenimiento de sistemas tales como servidores centrales, switches y routers IP los cuales trasportan los datos a lo largo de la red interna de la compañía; y de otros sistemas que controlan potencia, agua o gas. Para hacer más eficiente el uso de los sistemas distribuidos de control, la información a los largo de la arquitectura de la red ha sido desarrollada de manera abierta incrementado la posibilidad de ataques provenientes de entidades externas o de internos con intenciones malignas.

3.3. CONCEPTOS SOBRES POLÍTICAS DE SEGURIDAD[2]

3.3.1. Definición. Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan cómo una organización maneja, protege y distribuye información sensitiva. Este documento se convierte en el primer paso para construir barreras de protección efectivas. Es importante tener una política de seguridad de red efectiva y bien pensada que pueda proteger la inversión y recursos de información de su compañía. Sobre todo es importante que la organización defina claramente y valore qué tan importantes son los recursos e información que se tienen en la red corporativa y dependiendo de esto justificará si es necesario que se preste la atención y esfuerzos suficientes para lograr un nivel adecuado de protección. La mayoría de las organizaciones poseen información sensible y secretos importantes en sus redes, esta información debería ser protegida contra el vandalismo del mismo modo que otros bienes valiosos como propiedades de la corporación y edificios de oficinas.

La definición de una política de seguridad de red no es algo en lo que se pueda establecer un orden lógico o secuencia aceptada de estados debido a que la seguridad es algo muy subjetivo, cada empresa tiene diferentes expectativas, diferentes metas, diferentes formas de valorar lo que va por su red, cada negocio tiene distintos requerimientos para almacenar, enviar y comunicar información de manera electrónica; por esto nunca existirá una sola política de seguridad aplicable a 2 organizaciones diferentes. Además, así como los negocios evolucionan para adaptarse a los cambios en las condiciones del mercado, la política de seguridad debe evolucionar para satisfacer las condiciones cambiantes de la tecnología. Una política de seguridad de red efectiva es algo que todos los usuarios y administradores pueden aceptar y están dispuestos a reforzar, siempre y

[2] MONTOYA, Edwin. CAÑÓN, Jorge Alonso. Riesgos, Políticas y Herramientas de seguridad en redes.

cuando la política no disminuya la capacidad de la organización, es decir la política de seguridad debe ser de tal forma que no evite que los usuarios cumplan con sus tareas en forma efectiva.

3.3.2. Importancia. Existen muchos factores que justifican el establecimiento de políticas de seguridad para un sitio específico, pero los más determinantes son:

- Ayudan a la organización a darle valor a los recursos que posee.
- Es una infraestructura desde la cual otras estrategias de protección pueden ser desarrolladas.
- Proveen unas claras y consistentes reglas para los usuarios de la red y su interacción con el entorno.
- Contribuyen a la efectividad y direccionan la protección total de la organización.
- Pueden ayudar a responder ante requerimientos legales.
- Ayudan a prevenir incidentes de seguridad.
- Proveen una guía cuando un incidente ocurre.
- Es una planeación estratégica del papel que juega la arquitectura de red al interior de la organización.

Pág.8 y 9

- Ayuda en la culturización de los usuarios para el uso de servicios de red e inculca el valor real que ellos representan.

3.3.3. Características. Una política de seguridad es un plan elaborado de acuerdo con los objetivos generales de la organización y en el cual se ve reflejados los intereses de la empresa a cerca de los servicios de red y recursos que se desean proteger de manera efectiva y que representan activos importantes para el normal cumplimiento de la misión institucional. Por esto, la política de seguridad debe cumplir con ciertas características propias de este tipo de planes, como son:

- Debe ser simple y entendible (específica).
- Debe estar siempre disponible.
- Se puede aplicar en cualquier momento a la mayoría de situaciones contempladas.
- Debe ser practicable y desarrollable.
- Se debe poder hacer cumplir.
- Debe ser consistente con otras políticas organizacionales.
- Debe ser estructurada.
- Se establece como una guía, no como una cadena a la cual se tenga que atar para siempre.
- Debe ser cambiante con la variación tecnológica.

- Una política debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas.

3.3.4. Pasos para desarrollar una política de seguridad.[3] El objetivo perseguido para desarrollar una política de seguridad de red es definir las expectativas de la empresa acerca de su uso y definir procedimientos para prevenir y responder a incidentes de seguridad provenientes del cada día más avanzado mundo de la comunicación global.

Definir una política de seguridad de red significa desarrollar procedimientos y planes que salvaguarden los recursos de la red contra pérdidas y daños, por lo tanto es muy importante analizar entre otros los siguientes aspectos:

- Determinar los objetivos y directrices de la organización.

- La política de seguridad debe estar acorde con otras políticas, reglas, regulaciones o leyes ya existentes en la organización; por lo tanto es necesario identificarlas y tenerlas en cuenta al momento de desarrollar la política de seguridad de redes.

- Identificación de los recursos disponibles.

- ¿Qué recursos se quieren proteger?

- ¿De quién necesita proteger los recursos?

[3] MONTOYA, Edwin. CAÑÓN, Jorge Alonso. Riesgos, Políticas y Herramientas de seguridad en redes. Pág. 11

- Identificación de posibles amenazas.

- ¿Qué tan reales son las amenazas?

- ¿Qué tan importante es el recurso?

- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

- Verificación frecuente de la política de seguridad de red para ver si los objetivos y circunstancias han cambiado.

En general, el costo de proteger las redes de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad. La política de seguridad debe ser comunicada a cada quien que usa un computador en la red con el fin de que sea ampliamente conocida y se pueda obtener una retroalimentación de los usuarios de la misma para efectos de revisiones periódicas y detección de nuevas amenazas o riesgos.

4. POLÍTICAS DE SEGURIDAD DEL SISTEMA DE CONTROL DISTRIBUIDO DE LA REFINERÍA

4.1. EXPOSICIÓN DE MOTIVOS

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento, ya que cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

La tendencia actual es la de integrar los sistemas de control con los sistemas de información y de gestión de las organizaciones. Esto representa grandes ventajas como son: la rápida toma de decisiones y mayor eficiencia en el trabajo del personal; pero se tiene el gran inconveniente de que personas no autorizadas puedan acceder a una determinada información, aplicación o recurso de los sistemas de control incluso desde la misma red de información. Un ejemplo de esta tendencia es la red de la refinería, donde los sistemas de control están conectados de cierta manera a la red de planta.

Las políticas de seguridad conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos. Estas políticas

constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad.

El objetivo perseguido para desarrollar una política de seguridad de una red es definir las expectativas de la organización acerca del uso de la red y definir procedimientos para prevenir y responder a incidentes de seguridad provenientes tanto de interior de la organización como de del exterior.

Para el caso particular del sistemas de control distribuido de la refinería, es necesario proveer la suficiente garantía y confiabilidad que permita operar en las mejores condiciones y lograr un funcionamiento continuo de los sistemas bajo el mejor clima de confianza de los usuarios, garantizando el respeto por niveles adecuados de confidencialidad e integridad de la información que se procesa, garantizando la disponibilidad de los servicios requeridos. En estos sistemas de control todos los elementos son susceptibles a ser atacados y aun más si no se han adoptado metodologías para enfrentar este tipo de ataques. Por lo tanto es de necesidad realizar un análisis de amenazas y riesgos y la adopción de políticas de seguridad, que permitan acoger las recomendaciones de mejora adecuadas para garantizar la confidencialidad, integridad, disponibilidad y uso legítimo de los sistemas de control.

4.2. RESUMEN

El presente es una propuesta de las políticas de seguridad que en materia de informática y de comunicaciones digitales ha elaborado la administración de la red del sistema de control distribuido

de la refinería en colaboración con la CUTB, para normar a la institución en estos rubros. La propuesta ha sido detenidamente planteada, analizada y revisada a fin de no contravenir con las garantías básicas del individuo, y no pretende ser una camisa de fuerza, y más bien muestra una buena forma de operar el sistema con seguridad, respetando en todo momento estatutos y reglamentos vigentes de la Institución.

4.3. INTRODUCCIÓN

Las políticas de seguridad computacional para los equipos de los sistemas de control emergen como un instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la empresa cumplir con su misión. El proponer esta política de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

Para la implantación y cumplimiento de las siguientes políticas de seguridad es necesario el apoyo de todo el personal de la refinería, y en especial de los operadores e ingenieros del edificio de control central. Todos deben tener conocimiento de las políticas de seguridad y del uso adecuado de todos los dispositivos del sistema de control distribuido de los cuales estén encargados, con el fin de crear una cultura de seguridad para buenos usos de los recursos y protección de ataques hostiles.

4.4. ÁMBITO DE APLICACIÓN

Estas políticas serán la base para crear una cultura de seguridad dentro de los usuarios y operadores de las redes y equipos del sistema de control distribuido. Al momento de su realización, no existen lineamentos ni reglas de uso para estos equipos, por lo tanto, cualquier regla o política para el sistema de control deberá estar de acuerdo con las políticas recomendadas en este documento.

Estas políticas incluyen a todos los equipos pertenecientes al sistema de control distribuido ABB advant, tanto los cuartos satélites como el edificio de control central, incluyendo estaciones de operación, ingeniería, al igual que las PC y portátiles de las oficinas del CCB.

4.5. ANÁLISIS DE RIESGOS

Al crear una política de seguridad de red, es importante entender que la razón para crear tal política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables[4]. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger y que algunos recursos son más importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. El análisis de riesgos implica determinar lo siguiente:

- Qué se necesita proteger.
- De quién protegerlo.
- Cómo protegerlo.

[4] ArCERT, Manual de Seguridad en redes. Pág. 31

Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

En el análisis de los riesgos, es necesario determinar los siguientes factores:

- Estimación del riesgo de pérdida del recurso (lo llamaremos Ri).
- Estimación de la importancia del recurso (lo llamaremos Wi).

Como un paso hacia la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico. Por ejemplo, al riesgo (Ri) de perder un recurso, se le asigna un valor de cero a diez, donde cero, significa que no hay riesgo y diez es el riesgo más alto. De manera similar, a la importancia de un recurso (Wi) también se le puede asignar un valor de cero a diez, donde cero significa que no tiene importancia y diez es la importancia más alta. La evaluación general del riesgo será entonces el producto del valor del riesgo y su importancia (también llamado el peso). Esto puede escribirse como:

$$\mathbf{WRi = Ri * Wi}$$

Donde:

WRi : es el peso del riesgo del recurso “i” (también lo podemos llamar ponderación).

Ri : es el riesgo del recurso “i”.

Wi : es la importancia del recurso “i”.

Para el sistema de control distribuido de la refinería se diligenció la tabla del análisis de riesgos que se muestra en el Anexo A. La Tabla 4 contiene todos los elementos involucrados en las políticas de seguridad y sus respectivos pesos del riesgo del recurso, el riesgo del recurso y la importancia del recurso.

Tabla 4. Recursos del sistema ordenados según Riesgo evaluado.

Recurso del sistema		Riesgo(Ri)	Importancia (Wi)	Riesgo Evaluado (Ri* Wi)
Numero	**Nombre**			
	ESTACIONES SISTEMA DE SHUTDOWN DE CRUDO	**8**	**10**	**80**
	ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRUDO	**8**	**10**	**80**
	ESTACIONES SISTEMA DE SHUTDOWN DE CRACKING	**8**	**10**	**80**
	ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRACKING	**8**	**10**	**80**
	ESTACION LOCAL SISTEMA DE SHUTDOWN DE AZUFRE	**8**	**10**	**80**
	UPS SIH#2	**7**	**10**	**70**
	UPS SIH#3	**7**	**10**	**70**
	ESTACION DE CONTROL AVANZADO DE BLENDING	**8**	**6**	**48**
	ESTACION DE CONTROL AVANZADO	**8**	**6**	**48**
	ESTACIONES DE OPERACION Y GATEWAY #1 FOXBORO	**6**	**8**	**48**
	ESTACION DE BASE DE DATOS EN TIEMPO REAL	**6**	**8**	**48**
	ESTACION DE INGENIERIA SISTEMA ABB	**8**	**6**	**48**
	ESTACION AMS SMART TRANSMITTER INTERFACE – HART	**8**	**6**	**48**
	ESTACION GATEWAY PI SISTEMA DE CRUDO	**8**	**6**	**48**
	ESTACION GATEWAY PI SISTEMA DE CRACKING	**8**	**6**	**48**
	ESTACION GATEWAY PI SISTEMA DE BLENDING	**8**	**6**	**48**
	ESTACION GATEWAY PI-ABB	**6**	**6**	**48**
	ESTACION DEL OPTIMIZADOR DE CRACKING	**8**	**6**	**48**
	ESTACION DE STAR BLEND	**8**	**6**	**48**
	ESTACION DE SHORT TERM SCHEDULLING	**8**	**6**	**48**
	ESTACION DE INGENIERIA SISTEMA DE CRUDO	**6**	**6**	**36**
	ESTACION DE INGENIERIA SISTEMA DE CRACKING	**6**	**6**	**36**
	ESTACION DE INGENIERIA SISTEMA DE	**6**	**6**	**36**

	BLENDING			
	ESTACION DE HISTORIA SISTEMA DE CRUDO	**6**	**6**	**36**
	ESTACION DE HISTORIA SISTEMA DE CRACKING	**6**	**6**	**36**
	ESTACION DE HISTORIA SISTEMA DE BLENDING	**6**	**6**	**36**
	ESTACIONES DE OPERACIÓN CONSOLA DE CRUDO	**4**	**8**	**32**
	ESTACIONES DE OPERACIÓN CONSOLA DE CRACKING	**4**	**8**	**32**
	ESTACIONES DE OPERACIÓN CONSOLA DE BLENDING	**4**	**8**	**32**
	ESTACION BENTLY NEVADA	**8**	**4**	**32**
	ESTACION DE ANALIZADORES VISTANET	**8**	**4**	**32**
	PC PORTATIL HVAC	**8**	**4**	**32**
	ESTACION NIR	**8**	**4**	**32**
	ESTACION DE RECONCILIACION DE DATOS	**8**	**4**	**32**
	ESTACIONES DE OPERACION #1 SIEMENS	**4**	**8**	**32**
	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRUDO	**8**	**4**	**32**
	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRACKING	**8**	**4**	**32**
	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE BLENDING	**8**	**4**	**32**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRUDO	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE TRATAMIENTO	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRACKING	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE AZUFRE	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING REFINERIA	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING TNP	**6**	**4**	**24**
	MULTIPLEXER AMS SMART TRANSMITTER INTERFACE	**4**	**6**	**24**
	ROUTER SUPER STACK 3800	**4**	**6**	**24**
	HUB 24 PUERTOS UTP RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 24 PUERTOS UTP RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 24 PUERTOS UTP BLENDING	**4**	**6**	**24**
	HUB 24 PUERTOS UTP CONTROL AVANZADO	**4**	**6**	**24**
	SWITH 12 PUERTOS UTP BASE DE DATOS EN TIEMPO REAL	**4**	**6**	**24**
	SWITH 24 PUERTOS UTP ESD Y UPS	**4**	**6**	**24**
	ESTACION GATEWAY SIEMENS	**4**	**6**	**24**
	ESTACION PC ESCLAVO SIEMENS	**4**	**6**	**24**

	UPS CCB	**2**	**10**	**20**
	UPS SIH#1	**2**	**10**	**20**
	ESTACIONES DE OPERACIÓN SISTEMA DE ENTRENAMIENTO	**6**	**0**	**0**
	ESTACION DE HISTORIA SISTEMA DE ENTRENAMIENTO	**6**	**0**	**0**

Los estudios de seguridad realizados a nivel mundial en un gran número de empresas demuestran que el 80% de los problemas provienen de clientes internos y el restante 20% proviene de elementos externos a la organización.

Una aproximación acerca de cómo proteger los recursos de los problemas originados por el cliente interno consiste en la identificación del uso correcto de los mismos por parte de éstos. Pero primero, deberemos saber quiénes son los que van a hacer uso de los recursos. Es decir se debe contar, previamente, con un conocimiento cabal de todos los usuarios que tenemos en el sistema. Esta lista no es obligatoriamente individual, sino que puede ser, en efecto, una lista por grupos de usuarios y sus necesidades en el sistema. Esta es, con seguridad, la práctica más extendida pues, definida la necesidad de un grupo de usuarios, lo más efectivo es englobarlos a todos en un mismo grupo.

En la refinería no se tienen definidos los esquemas de grupo de usuarios para el acceso a los recursos de la red de planta del sistema de control distribuido. Contrario a esto se tienen los usuarios por defecto de los sistemas computacionales. La Tabla 5 muestra como es el acceso a cada uno de los recursos de la red, con sus tipos de acceso y permisos otorgados.

Tabla 5. Tipos de acceso por usuario de los equipos de la red de planta del DCS.

Recurso del sistema	**Identificación Del Usuario**	**Tipo de Acceso**	**Permisos otorgados**
Nombre			
ESTACION DE CONTROL AVANZADO DE BLENDING	Usuario Local por defecto	Local	Lectura y escritura
ESTACION DE CONTROL AVANZADO	Usuario Local por defecto	Local	Lectura y escritura
ESTACIONES DE OPERACIÓN CONSOLA DE	Usuario de acceso	Local	Lectura y

CRUDO	de operación(por defecto del sistema)		escritura
ESTACIONES DE OPERACIÓN CONSOLA DE CRACKING	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACIONES DE OPERACIÓN CONSOLA DE BLENDING	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA DE CRUDO	Usuario de acceso de ingeniería(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA DE CRACKING	Usuario de acceso de ingeniería(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA DE BLENDING	Usuario de acceso de ingeniería(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRUDO	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE TRATAMIENTO	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRACKING	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE AZUFRE	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING REFINERIA	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING TNP	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACIONES DE OPERACIÓN SISTEMA DE ENTRENAMIENTO	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE ENTRENAMIENTO	Usuario de acceso de ingeniería(por defecto del sistema)	Local	Lectura y escritura
ESTACIONES DE OPERACION Y GATEWAY FOXBORO	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION DE BASE DE DATOS EN TIEMPO REAL	Clientes DCS y Refinería	Remoto	Lectura
ESTACION BENTLY NEVADA	Superuruario Windows NT Administrador	Local	Lectura y escritura
ESTACION DE ANALIZADORES VISTANET	Superuruario Windows NT Administrador	Local	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA ABB	Superuruario	Local	Lectura y

	Windows NT Administrador		escritura
ESTACIONES SISTEMA DE SHUTDOWN DE CRUDO	Superuruario Windows 2000 Administrador	Local	Lectura y escritura
ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRUDO	Superuruario Windows 2000 Administrador	Local	Lectura y escritura
ESTACIONES SISTEMA DE SHUTDOWN DE CRACKING	Superuruario Windows 2000 Administrador	Local	Lectura y escritura
ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRACKING	Superuruario Windows 2000 Administrador	Local	Lectura y escritura
ESTACION LOCAL SISTEMA DE SHUTDOWN DE AZUFRE	Superuruario Windows 2000 Administrador	Local	Lectura y escritura
MULTIPLEXER AMS SMART TRANSMITTER INTERFACE	Superuruario Windows NT Administrador	Local	Lectura y escritura
ESTACION AMS SMART TRANSMITTER INTERFACE – HART	Superuruario Windows NT Administrador	Local	Lectura y escritura
PC PORTATIL HVAC	Superuruario Windows NT Administrador	Local	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE CRUDO	Usuario Local por defecto	Local	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE CRACKING	Usuario Local por defecto	Local	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE BLENDING	Usuario Local por defecto	Local	Lectura y escritura
ESTACION GATEWAY PI SISTEMA DE CRUDO	Usuario Local por defecto	Local	Lectura y escritura
ESTACION GATEWAY PI SISTEMA DE CRACKING	Usuario Local por defecto	Local	Lectura y escritura
ESTACION GATEWAY PI SISTEMA DE BLENDING	Usuario Local por defecto	Local	Lectura y escritura
ESTACION GATEWAY PI-ABB	Usuario Local por defecto	Local	Lectura y escritura
ESTACION NIR	Superuruario Windows NT Administrador	Local	Lectura y escritura
ESTACION DEL OPTIMIZADOR DE CRACKING			
ESTACION DE RECONCILIACION DE DATOS			
ESTACIONES DE OPERACION SIEMENS	Usuario de acceso de operación(por defecto del sistema)	Local	Lectura y escritura
ESTACION GATEWAY SIEMENS	Usuario Local por defecto	Local	Lectura y escritura
ESTACION PC ESCLAVO SIEMENS			
ESTACION DE STAR BLEND			
ESTACION DE SHORT TERM SCHEDULLING			

ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRUDO			
ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRACKING			
ESTACION DE INGENIERIA XTERMINAL SISTEMA DE BLENDING			

Además de estos usuarios por defecto, el administrador del sistema tiene acceso tanto local como remoto a todos los recursos.

Para identificar los usuarios (o grupos de usuarios), se puede realizar la determinación de los recursos de que harán uso y de los permisos que tendrán. La identificación de los tipos de acceso por usuarios para la red de planta de la refinería se muestra en la Tabla 6.

Tabla 6. Grupos de usuarios vs. Tipos de acceso de los equipos del DCS

Recurso del sistema	**Identificación Del Usuario**	**Tipo de Acceso**	**Permisos otorgados**
Nombre			
ESTACION DE CONTROL AVANZADO DE BLENDING	Grupo Operadores Blending	Local	Lectura y escritura
ESTACION DE CONTROL AVANZADO	Grupo de aplicación	Local	Lectura y escritura
ESTACIONES DE OPERACIÓN CONSOLA DE CRUDO	Grupo Operadores Crudo	Local	Lectura y escritura
	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACIONES DE OPERACIÓN CONSOLA DE CRACKING	Grupo Operadores Cracking	Local	Lectura y escritura
	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACIONES DE OPERACIÓN CONSOLA DE BLENDING	Grupo Operadores Blending	Local	Lectura y escritura
	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA DE CRUDO	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA DE CRACKING	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA DE BLENDING	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRUDO	Grupo Operadores Crudo	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE TRATAMIENTO	Grupo Operadores Crudo	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE	Grupo Operadores	Local	Lectura y

CRACKING	Cracking		escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE AZUFRE	Grupo Operadores Cracking	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING REFINERIA	Grupo Operadores Blending	Local	Lectura y escritura
ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING TNP	Grupo Operadores Blending	Local	Lectura y escritura
ESTACIONES DE OPERACIÓN SISTEMA DE ENTRENAMIENTO	Grupo de entrenamiento	Local	Lectura y escritura
	Grupo de aplicación	Local	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE ENTRENAMIENTO	Grupo de entrenamiento	Local	Lectura y escritura
	Grupo de aplicación	Local	Lectura y escritura
ESTACIONES DE OPERACION Y GATEWAY FOXBORO	Grupo de operación Servicios Industriales	Local	Lectura y escritura
ESTACION DE BASE DE DATOS EN TIEMPO REAL			
ESTACION BENTLY NEVADA	Grupo Mantenimiento	Local	Lectura y escritura
ESTACION DE ANALIZADORES VISTANET	Grupo Mantenimiento	Local	Lectura y escritura
ESTACION DE INGENIERIA SISTEMA ABB	Grupo de aplicación	Local	Lectura y escritura
ESTACIONES SISTEMA DE SHUTDOWN DE CRUDO	Grupo Operadores Crudo	Local	Lectura y escritura
ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRUDO	Grupo Operadores Crudo	Local y remoto	Lectura y escritura
ESTACIONES SISTEMA DE SHUTDOWN DE CRACKING	Grupo Operadores Cracking	Local	Lectura y escritura
ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRACKING	Grupo Operadores Cracking	Local y remoto	Lectura y escritura
ESTACION LOCAL SISTEMA DE SHUTDOWN DE AZUFRE	Grupo Operadores Cracking	Local y remoto	Lectura y escritura
MULTIPLEXER AMS SMART TRANSMITTER INTERFACE	Grupo Mantenimiento	Local	Lectura y escritura
ESTACION AMS SMART TRANSMITTER INTERFACE – HART	Grupo Mantenimiento	Local	Lectura y escritura
ROUTER SUPER STACK 3800	Administrador del sistema	Local y remoto	Lectura y escritura
HUB 24 PUERTOS UTP RED DE PLANTA ABB	Administrador del sistema	Local	N.A.
HUB 24 PUERTOS UTP RED DE PLANTA ABB	Administrador del sistema	Local	N.A.
HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	Administrador del sistema	Local	N.A.
HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	Administrador del sistema	Local	N.A.
HUB 24 PUERTOS UTP BLENDING	Administrador del sistema	Local	N.A.
HUB 24 PUERTOS UTP CONTROL AVANZADO	Administrador del	Local	N.A.

	sistema		
SWITCH 12 PUERTOS UTP BASE DE DATOS EN TIEMPO REAL	Administrador del sistema	Local	N.A.
SWITCH 24 PUERTOS UTP ESD Y UPS	Administrador del sistema	Local	N.A.
PC PORTATIL HVAC	Grupo Mantenimiento	Local	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE CRUDO	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE CRACKING	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION DE HISTORIA SISTEMA DE BLENDING	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION GATEWAY PI SISTEMA DE CRUDO	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION GATEWAY PI SISTEMA DE CRACKING	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION GATEWAY PI SISTEMA DE BLENDING	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION GATEWAY PI-ABB	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION NIR	Grupo Mantenimiento	Local	Lectura y escritura
ESTACION DEL OPTIMIZADOR DE CRACKING	Administrador	Local	Lectura y escritura
ESTACION DE RECONCILIACION DE DATOS	Administrador	Local	Lectura y escritura
ESTACIONES DE OPERACION SIEMENS	Grupo de operación Servicios Industriales	Local	Lectura y escritura
ESTACION GATEWAY SIEMENS	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION PC ESCLAVO SIEMENS	Grupo de operación Servicios Industriales	Local	Lectura y escritura
ESTACION DE STAR BLEND	Grupo de operación Blending	Local	Lectura y escritura
ESTACION DE SHORT TERM SCHEDULLING	Grupo de operación Blending	Local	Lectura y escritura
UPS CCB	Grupo Operadores Crudo	Local y remoto	Lectura y escritura
	Grupo operadores Cracking	Local y remoto	Lectura y escritura
UPS SIH#1	Grupo operadores Crudo	Local y remoto	Lectura y escritura
UPS SIH#2	Grupo operadores Cracking	Local y remoto	Lectura y escritura
UPS SIH#3	Grupo operadores Cracking	Local y remoto	Lectura y escritura
ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRUDO	Grupo de aplicación	Local y remoto	Lectura y escritura
ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRACKING	Grupo de aplicación	Local y remoto	Lectura y escritura

ESTACION DE INGENIERIA XTERMINAL SISTEMA DE BLENDING	Grupo de aplicación	Local y remoto	Lectura y escritura

Como se observa en la tabla del análisis de riesgo (Tabla 4) las Estaciones de shutdown son las estaciones más críticas dentro de la red de planta del sistema de control de la refinería. Esto se debe a que estas estaciones tienen un riesgo muy alto, ya que presentan una de las mayores vulnerabilidades del sistema, el usuario por defecto es el administrador y por lo tanto se tienen todos los privilegios del sistema. Además, son de gran importancia ya que a través de ellas se puede realizar el encendido o apagado de los equipos de las plantas de cada una de las áreas. Otros equipos críticos del sistema de control son las UPS, en especial las del SIH#2 y SIH#3. También se observa, como se esperaba, que los equipos con menor riesgo evaluado son las estaciones de entrenamiento, puesto que ellas no son trascendentes para la continuidad del funcionamiento del sistema de control.

4.6. ENUNCIADOS DE POLÍTICAS

4.6.1. Generales.

- La red de planta del sistema de control distribuido de la refinería tiene como propósito principal interconectar todos los elementos que constituyen el DCS, para transferencia de información entre las diferentes áreas operativas.

4.6.2. De los equipos.

4.6.2.1. Instalación.

- Todo el equipo del sistema de control distribuido ya sea estación de operación, estaciones de aplicación, estación de shutdown, UPS, interfase, etc. que esté o sea conectado a la **red de planta** o aquel que en forma autónoma se tenga y que sea propiedad de la empresa debe de sujetarse a las normas y procedimientos de instalación que emite su fabricante y la empresa.

- El administrador del sistema de planta deberá tener un registro actualizado de todos los equipos que hacen parte de ella, incluyendo sus principales característica y su localización.

- El equipo de la empresa que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de

seguridad física, condiciones ambientales y alimentación eléctrica que permitan su correcta operación

- Los responsables de las áreas operacionales en conjunto con el administrador del sistema deben velar y dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en la ubicación de los equipos.

- La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan al administrador del sistema.

4.6.2.2. Mantenimiento.

- Al grupo de control le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Esto se realiza a partir del momento en que sean autorizados por el administrador del sistema.

- Corresponde al administrador del sistema dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico.

- Queda estrictamente prohibido realizar el mantenimiento a equipos del DCS por personas no autorizados según lo estipula la normatividad de la empresa.

4.6.2.3. Actualización.

- Todo el equipo computacional del DCS advant (PC, estaciones de operacion, ingeniería demás relacionados), que sean propiedad del la refinería debe procurarse sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

4.6.2.4. Reubicación.

- La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que el administrador del sistema disponga, esto quiere decir que cualquier cambio en la ubicación de un equipo debe ser autorizado por el administrador del sistema.

- La reubicación de un equipo no debe perjudicar la capacidad de producción de empresa.

4.6.3. Del Control de Acceso.

- El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta la dirección de la refinería.

- La Dirección de la empresa deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

- Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas críticas estará sujeto a las que especifiquen las autoridades superiores de la institución.

- Las cuentas de usuario son las que permiten a los usuarios utilizar los equipos del DCS. A través de la cuenta el usuario cada uno se conecta.

- Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos.

- Una cuenta estará conformada por un nombre de usuario y su respectiva contraseña.

- Todos y cada uno de los equipos son asignados a un responsable o grupo responsable, por lo que es de su competencia hacer buen uso de los mismos.

- El acceso a cada uno de los cuartos en donde se encuentren ubicados los equipos del DCS, estará restringido como lo indica la Tabla 6. En caso que personal distinto al mencionado en la tabla necesite ingresar a estos cuartos, deberá ser autorizado por el jefe encargado de cada cuarto o área.

- Está prohibido acceder a los equipos del DCS con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.

- Al momento de ingresar al sistema, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual permitirá detectar fácilmente el uso no autorizado del los equipos.

4.6.3.1. Acceso a las estaciones de operación.

- El acceso a estas estaciones esta reservado al grupo de operadores correspondiente a cada área. El grupo de operadores debe velar por el buen uso de estos equipos y en caso de alguna falla debe dirigirse inicialmente al administrador del sistema.

- El uso de estos computadores debe estar protegido por un sistema de autenticación(sólo usuarios autorizados).

- Los operadores se colocarán en línea con su login y password, de tal manera que todos lo eventos que realice queden registrados en los archivos logs de las consolas.

- Los operadores tendrán acceso a los datos de monitoreo y supervisión y podrán realizar las maniobras necesarias para mantener los equipos de la refinería en operación normal.

- Los ingenieros tendrán los mismos privilegios que los operadores, además, podrán ejecutar el software para reconfigurar la aplicación de los sistemas instalados en las consolas de operador.

- El administrador asignará a cada usuario o grupo de usuarios un login y un password.

- Cualquier acceso remoto a estas consolas deberá efectuarse de manera autentificada utilizando filtrado IP. Debe ser posible leer la información de monitoreo y supervisión para todo aquel que tenga acceso a estas consolas. El administrador y los ingenieros habilitados por el administrador son lo únicos con privilegios suficientes para escribir o modificar algún

parámetro de la planta de manera remota. La información de configuración de las consolas sólo estará disponible para el administrador del DCS.

- Si el operador o el ingeniero abandona la consola deberá ya sea salir de su sesión o proteger de alguna manera la manipulación del equipo.

- Está totalmente prohibido realizar otras tareas distintas a las del monitoreo y supervisión de las áreas en las consolas de operador del DCS.

- Esta totalmente prohibido realizar tareas distintas a la de la realización de la ingeniería en las consolas de ingeniería.

- El acceso remoto a las estaciones de operación está habilitado sólo al administrador del sistema.

4.6.3.2. Acceso a las estaciones de ingeniería.

- El acceso a estas estaciones esta reservado al grupo de ingeniería. El grupo de ingenieros debe velar por el buen uso de estos equipos y en caso de alguna falla debe dirigirse inicialmente al administrador del sistema o el respectivo jefe de área.

- El uso de estos computadores debe estar protegido por un sistema de autenticación(sólo usuarios autorizados).

- Los usuarios del grupo de aplicación se colocarán en línea con su login y password, de tal manera que todos lo eventos que realice queden registrados en los archivos logs de las consolas.

- Los usuarios podrán ejecutar el software para reconfigurar la aplicación de los sistemas instalados en las consolas de ingeniería.

- El administrador asignará a cada usuario del grupo de usuarios un login y un password.

- Cualquier acceso remoto a estas consolas deberá efectuarse de manera autentificada utilizando filtrado IP. La información de configuración de las consolas sólo estará disponible para el administrador del DCS.

- Si el ingeniero abandona la consola deberá ya sea salir de su sesión o proteger de alguna manera la manipulación del equipo.

- Está totalmente prohibido realizar otras tareas distintas a las del monitoreo y supervisión de las áreas en las consolas de operador del DCS.

- Esta totalmente prohibido realizar tareas distintas a la de la realización de la ingeniería en las consolas de ingeniería.

4.6.3.3. Acceso a las estaciones de shutdown.

- El acceso a estas estaciones esta reservado al grupo de operadores correspondiente a cada área.

- Las estaciones de shutdown deben ser utilizadas especificamente para realizar funciones de monitoreo y alarma de los sistemas de emergencia de cada una de las áreas del DCS. También se puede hacer apagado de la planta a criterio del operador. Está totalmente prohibido realizar otras tareas distintas a estas en estos equipos.

- El uso de estos computadores debe estar protegido por un sistema de autenticación.

- Si el personal que se encuentra utilizando estos equipos abandona la consola deberá ya sea salir de su sesión o proteger de alguna manera la manipulación del equipo.

4.6.3.4. Acceso a las UPS.

- El acceso a las UPS de los cuartos satélites está reservado al grupo de operadores de cada área.
- El acceso a las UPS del CBB se reserva para todos los grupos de operadores.

4.6.3.5. Acceso a los equipos Ethernet.

- El acceso a estos equipos esta reservado al Administrador del sistema.

- El acceso telnet a estos equipos deberá estar protegido por un login y una contraseña que sólo debe conocer el administrador del sistema.

- Sólo se accederá a estos equipos en caso de reconfiguración o de pérdida de la configuración anterior.

- Para acceder a ellos se deben utilizar computadores autorizados, como por ejemplo los de los administradores de red.

- Cualquier cambio en la configuración debe anotarse en un registro de cambios de los equipos pertenecientes al grupo ethernet.

- Los gabinetes en los que se encuentran estos equipos, estarán asegurados bajo llave para evitar conexiones no autorizadas a la red de planta.

4.6.3.6. Acceso a la base de datos.

- El acceso a la base de datos está reservado al grupo de clientes de refinería y para el administrador del sistema.

4.6.3.7. Acceso a las consolas de entrenamiento.

- Estas consolas están reservadas exclusivamente para el entrenamiento de los del personal del DCS. Está totalmente prohibido realizar otras tareas distintas a las de aprendizaje y entrenamiento en estos equipos.

- El uso de estos computadores debe estar protegido por un sistema de autenticación(sólo usuarios autorizados).

- Las actividades que se realicen en estas consolas no debe estar ligadas en ningún momento con los procesos de cada una de las áreas, esto quiere decir que su manipulación no debe alterar los paramentos de los procesos.

- Si el personal que se encuentra utilizando estos equipos abandona la consola deberá ya sea salir de su sesión o proteger de alguna manera la manipulación del equipo.

4.6.3.8. Acceso local a la red.

- El Administrador del sistema es responsable de proporcionar a los usuarios el acceso a la red y a los recursos del sistema de control distribuido.

- El Administrador del sistema es la responsable de establecer y difundir el reglamento para el uso de la red del DCS y de procurar su cumplimiento.

- El acceso lógico a los equipo de interconexión del DCS conectados a la red (servidores, ruteadores, bases de datos, concentradores, etc.) son administrados por el Administrador del sistema.

- Todo el equipo de del sistema de control distribuido que esté o sea conectado a la red de planta, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe sujetarse a los procedimientos de acceso establecidos.

- Los servicios que se utilicen en los equipos de la red planta del sistema de control distribuido deben ser los estrictamente necesarios para realizar las funciones que le competen al DCS. Estos servicios deben escogerse de tal manera que no afecten la seguridad de la red o de alguno de sus equipos. La habilitación de un nuevo servicio dependerá de la autorización del administrador del sistema.

4.6.3.9. Acceso remoto a la red.

- El servicio de acceso remoto para asistencia a la red del sistema de control distribuido estará autentificado mediante dirección IP, identificación del número telefónico y clave de acceso por cada proveedor.

4.6.4. De Contraseñas.

- La longitud de la contraseña deberá siempre se verificada de manera automática al ser construida por el usuario. Todas las contraseñas deberán contar con al menos ocho caracteres.

- Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.

- Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.

- Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.

- La cuenta de un usuario es personal e intransferible, por lo cual no se permite que se comparta ni cuenta ni contraseña con persona alguna, aún si acredita la confianza del usuario.

4.6.5. De utilización de recursos de la red del DCS.

- Los recursos disponibles a través de la red del sistema de control distribuido serán de uso exclusivo para asuntos relacionados con las actividades de la refinería.

- El administrador del sistema es el responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.

- Corresponde al administrador del sistema administrar, mantener y actualizar la infraestructura de la red de planta del sistema de control distribuido.

- Dado el carácter confidencial que involucra el correo electrónico la reglamentación para su uso dentro de la red de planta del sistema de control, debe ser la misma que la de la red existente.

4.6.6. De Software.

- En los equipos del sistema de control distribuido, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

- La instalación de software que desde el punto de vista del administrador pudiera poner en riesgo los recursos del sistema de control distribuido no está permitida.

- Esta prohibida la instalación y desinstalación del software. El único que podrá autorizar la instalación y desintalación del software en los equipos del sistema de control distribuido es el administrador del sistema. Esto incluye el software de supervisión y operación de las estaciones, UPSs, estaciones de shutdown y demás.

- Con el propósito de proteger la integridad de los equipos de cómputo del sistema de control distribuido, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).

- Corresponde al administrador del sistema autorizar cualquier adquisición y actualización del software.

- El administrador del sistema deberá tener un registro de todos los paquetes de software propiedad de la refinería que sean utilizados en el sistema de control distribuido.

- Todos las aplicaciones (programas, bases de datos, interfases gráficas) desarrollados con o a través de los recursos de la empresa pertenecientes al DCS, se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.

- Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

- Los datos, las bases de datos, la información generada por los usuarios del DCS y los recursos informáticos del mismo deben estar resguardados.

- El administrador del sistema manejará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

- Está terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas. La utilización de estos programas esta restringido únicamente al administrador del sistema.

- Esta prohibido hacer uso de herramientas de delincuencia informática, tales como programas que rastrean y explotan vulnerabilidades en los equipos, para proporcionar privilegios no otorgados explícitamente por el administrador del sistema.

4.6.7. Supervisión y Evaluación.

- Cada uno de los Jefes de área en las cuales esté en riesgo la seguridad en la operación, servicio y funcionalidad, deberá emitir las normas y los procedimientos que correspondan.

- Para efectos de que el sistema de control disponga de una red de planta con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que se presten en ella.

- Los equipos considerados críticos, deberán estar bajo monitoreo permanente.

- Cada una de las áreas deberá emitir los planes de contingencia que correspondan a las actividades críticas que realicen.

4.6.8. Sanciones.

- Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento vigente.

- Las sanciones pueden ser desde una llamada de atención o informar al usuario el despido dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

- Corresponderá a un comité, encabezado por el administrador del sistema y los jefes de área, hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática del DCS.

5. RECOMENDACIONES PARA IMPLEMENTAR ESTRATEGIAS DE SEGURIDAD

- Para un mejor entendimiento de las políticas se seguridad enunciadas en capítulo IV, se recomienda extrae dicho capítulo en otro documento que permita la fácil divulgación de las mismas a los cada una de las personas involucradas en la red de planta del DCS de la refinería.

- El administrador debe realizar una evaluación periódica de los registros LOGs generados por el sistema. Por lo tanto, se debe activar al máximo la generación de estos reportes.

- Remplazar el Switch Nivel 3 por un Gateway Nivel 7, con esto se logra realizar un filtrado más estricto a niveles superiores al IP.

5.1. PARA LAS ESD

- Crear cuentas para cada operador encargado del manejo de la estaciones de shutdown, ya que actualmente se operando sobre la cuenta del administrador. Con esto se lograría limitar los privilegios de los operadores y limitar el acceso a estas estaciones, además de tener un registro de cual operador realiza una acción.

- Se debe restringir el acceso remoto a las estaciones ESD a través de un filtrado IP. Esto garantiza que las ESD estarán habilitadas sólo para el personal autorizado.

5.2. PARA LAS UPS

- Se debe restringir el acceso remoto a las UPS a través de un filtrado IP. Esto garantiza que las UPS estarán habilitadas sólo para el personal autorizado.

5.3. PARA LAS ESTACIONES UNIX

- **Eliminar las cuentas de invitado**. Existen dos esquemas para romper la seguridad de los sistemas Unix: La primera, un usuario puede obtener acceso sobre una máquina usando una cuenta de "invitado" o por cualquier otro medio, y corriendo después un programa para probar claves sobre esa máquina. El atacante debe ser capaz de probar miles de claves consumiendo una cantidad de recursos limitada. Además si el oponente es capaz de obtener una copia del archivo de claves, entonces puede seguir obteniendo nuevas claves para otras máquinas desde las máquinas para las cuales ya posee las claves.

- En los equipos de computo del DCS de la refinería, todos lo equipos se encuentran funcionando con las cuentas preinstaladas o por defecto. Es importante cambiar las contraseñas de dichas cuentas.

- Se deben eliminar las cuentas que no han sido usadas por mucho tiempo, las cuales pueden ser muy peligrosas.

- Se debe restringir a un número mínimo los superusuarios configurados. En el caso específico de este DCS sólo debe estar habilitado el superusuario utilizado por el administrador.

- Debido a que en UNIX los passwords encriptados residen en el archivo /etc/passwd es necesario separar estas contraseñas de las estaciones ABB, esto con el objetivo de que intrusos ya sea internos o externos no obtengan una copia de los passwords encriptados para intentar descifrarlos.

- Es posible especificar desde que terminales distintas a la consola de la estación de trabajo puede conectarse el superusuario. Cuando se deshabilitan conexiones remotas, la única forma de conectarse como superusuario desde una estación remota es conectándose inicialmente con el login de algún usuario distinto del superusuario, y después usar el comando su, en caso de que esté disponible. Distintas versiones de Unix tienen diferentes métodos para deshabilitar conexiones remotas de superusuario. En algunas versiones esta deshabilitación se realiza en el archivo /etc/ttys y en otras en el /etc/default/login.

- En importante revisar registros de monitoreo en donde se puede visualizar si existe algún usuario no autorizado que esté conectado como root o que trate de capturar el password. Siempre que se usa el comando su una entrada es colocada en el archivo llamado sulog. En este archivo puede verse desde la fecha que están conectados los usuarios y se puede verificar si cuentas durmientes están siendo accesadas.

- Se deben guardar las últimas conexiones ejecutadas por los usuarios en el archivo /var/adm/lastlog o /usr/adm/lastlog. Se puede preguntar a los usuarios si reconocen conexiones efectuadas a sus cuentas.

- El comando pwconv debe estar protegido contra lectura para usuarios distintos al superusuario.

- Realizar continuo monitoreo verificando la integridad de archivos importantes, corriendo los programas ISS, Satan.

- Se recomienda utilizar las versiones más recientes de programas de chequeo de la seguridad de los passwords elegidos por los usuarios.

- Instalar parches donde se encuentren problemas de seguridad.

- Utilizar periódicamente el comando pwck para chequear la integridad y consistencia de los archivos /etc/passwd y /etc/shadow. Con esto se puede tener conocimiento de las cuentas que tienen login en blanco, lo que podría ocasionar que alguien pudiera conectarse sin tener un login válido.

- Llevar un registro de conexiones falsas para rastrear los intentos de conexiones no exitosas al sistema. Esto se realiza en el archivo /var/adm/loginlog, donde después de 5 intentos consecutivos sin éxito se almacena el nombre del usuario. El administrador del sistema debe chequear este archivo periódicamente.

5.4. DE CONTRASEÑAS

- Combinar mayúsculas y minúsculas en los passwords y exigir el cambio periódico de los mismos.

5.5. DE LOS SERVICIOS

- Debe hacerse una evaluación de los servicios que deben correr.

- Es importante tener mecanismos de filtrado de paquetes, tales como Tcp Wrappers, lo cual puede realizarse sobre todos los sistemas críticos, como por ejemplo las estaciones de shutdown y para otros equipos importantes para el proceso como las estaciones de operación y las estaciones de ingeniería.

- Verificar que se dispone de una versión de ftpd posterior a diciembre de 1988 ya que un bug (error de programación) de versiones anteriores permitía entrar como root vía ftp anónimo.

- Deben evitarse correr daemons que no se utilizan.

- Intentar evitar servicios de rlogin y rsh pues son inseguros.

- El administrador debe comprobar que no haya programas inseguros instalados como setuid y setgid.

- Realizar un estudio detallado de los servicios que de una u otra forma pueda afectar al funcionamiento del DCS. Dicho estudio se puede realizar utilizando las consolas de entrenamiento y dependiendo de sus resultados, se deben deshabilitar en el archivo /etc/inetd.conf los servicios que no sean necesarios.

- Se debe deshabilitar el servicio finger, ya que a través de este se pueden obtener información del usuario de una máquina remota, tales como login, nombre completo, nombre de la terminal, derechos de escritura, tiempo sin actividad, etc.

- Deben deshabilitarse los servicios rlogin y rsh, ya que cumplen las mismas funciones de telnet pero son muy inseguros ya que pueden ser configurados para que no se requiera iformación de login y password.

- Verificar la versión de FTP que se está corriendo, puesto que existen algunas versiones con huecos de seguridad.

- El servicio TFTP, en lo posible, debe estar siempre deshabilitado ya que permite la trasferencia de archivo sin ningún tipo de seguridad.

- El servicio X-windows sólo debe ser habilitado para las X-TERM y para el administrador.

CONCLUSIONES

Con los avances de las redes, de los equipos de cómputo y de los sistemas de control distribuido, se ha mejorado el desempeño de estos sistemas interconectándolos en una sola red. Esto trae muchas ventajas, como son: el manejo de bases de datos en tiempo real generalizadas tanto para los sistemas de control como para los grupos administrativos de la empresa encargados de la toma decisiones. De esta manera, también se abre una brecha de seguridad, se abre un camino desde la red de planta hacia la red de control que podría aprovechar cualquiera que quiera acceder de manera infructuosa, ya sea de manera interna o externa.

Aun existe una gran diferencia entre las redes de control y las redes corporativas, es decir, las redes de control típicas pueden ser modbus, controlnet o como es el caso de la refinería una red propietaria MB300, y típicamente los equipos de cómputo, sean del sistema operativo que sean, utilizan la pila de protocolos TCP/IP para comunicarse. Sin embargo, la amenaza real radica en que los equipos de control están conectados tanto a la red de control como a la red de planta, y si alguien accede desde la red de planta a uno de estos equipos, y tiene el conocimiento suficiente de la red de control, puede acceder fácilmente a estos equipos.

No importa que medidas se tomen para la seguridad de una red de control, la medida principal es la de la adopción de una cultura de seguridad de la red por parte de todos los usuarios. Esta cultura inicia por el conocimiento de las políticas de seguridad y por la puesta en práctica de las recomendaciones que permitan adoptar estrategias de seguridad o barreras de protección requeridas para este tipo de sistemas.

La restricción número uno a los equipos de cómputo del DCS, en cuanto acceso local y remoto se refiere, se centra en las asignación de conjuntos login-passwords adecuados para cada uno de los usuarios y para los grupos de usuarios. Esta es la primera medida y en algunos casos la mayor garantía que se tiene a la hora de mantener la seguridad de un sistema de control.

La utilización de filtrado es algo muy conveniente a la hora de disminuir las brechas de seguridad de una red de control. Este filtrado se puede realizar ya sea desde el mismo servidor o utilizando switches, routers y gateways. A través de ellos se pueden realizar desde filtrados a través de máscaras para grupos de IPs o filtrados explícitos de un equipo origen a un servicio de un equipo destino. El filtrado a través de MAC no se recomienda ya que puede llegar a ser muy complicado y no tan efectivo como el IP.

Una buena opción para garantizar la seguridad en redes de control consiste en restringir de manera adecuada los servicios TCP/IP que se corren sobre la red, cualquiera que sea el sistema operativo. De manera esencial, todos los servicios TCP/IP no son necesarios para que funcionen los equipos del sistema de control, por lo tanto se debe realizar una evaluación que permita sólo los servicios que realmente se necesitan. El resultado de la evaluación debe buscar un equilibrio entre la funcionalidad de los equipos de la red de control y la seguridad de dicha red.

En el sistema de control de la refinería se encuentran muy bien segmentados algunos sectores de la red. Esto se observa, por ejemplo, en que las UPS y las estaciones de shutdown tienen un switch propio y la interfases van a un hub sólo para ellas. Esto puede ser útil para realizar restricciones de acceso a través de la misma conexión de cableado estructurado, haciendo posible el acceso a estos equipos sólo si se tiene una conexión directa con el elemento con que se conectan a la red.

De la arquitectura del sistema de control, se puede ver que tiene un punto central, el cual es el switch capa 3 que desempeña las funciones de un router, que interconecta a todos los segmentos establecidos por los demás hubs y switches. La pérdida de este router no es de gran relevancia, ya que las operaciones de control se realizan a través de la red MB300, sin embargo un daño que deshabilite el funcionamiento de este router dejaría incomunicadas las áreas operativas del la refinería y podría afectar en cierta manera las tareas que se deban realizar. También se puede observar que si se desea realizar filtrado IP a la gran cantidad de equipos que constituyen el DCS, el router no tendrá la capacidad esperada. La mejor opción es que la empresa coloque un gateway/firewall en su lugar, los cuales permitan la restricción hasta niveles de aplicación y no sólo hasta el nivel de transporte como lo hacen los routers.

BIBLIOGRAFÍA

- Planos, manuales y documentos del proyecto de automatización de la refinería.

- MONTOYA, Edwin. CAÑÓN, Jorge Alonso. Revista Universidad Eafit. Julio - Agosto - Septiembre 1997.Páginas 69-86. Artículo: Riesgos, políticas y herramientas de seguridad en redes. http://www.eafit.edu.co/revista/107/montoya.pdf. (Consulta: 25 de Abril de 2003).

- ArCERT. Coordinación de emergencias en redes teleinformáticas. Manual de seguridad. Seguridad en redes. http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf (Consulta: 26 de Abril de 2003).

- VILLALÓN HUERTA, Antonio. Seguridad en Unix y Redes. Versión 2.1. Julio 2002. http://andercheran.aiind.upv.es/toni/personal/unixsec.pdf (Consulta: 27 de Abril de 2003).

- AMADOR DONADO, Siler. AGREDO MÉNDEZ, Guefry L., CARRASCAL REYES, Carolina A. Políticas de Seguridad Computacional. Material de referencia. Universidad del Cauca. http://www.criptored.upm.es/descarga/pol_seg_com.zip (Consulta: 20 de Mayo de 2003).

- PONS MARTONELL, Manuel. Control de Accesos. Departament de Telecomunicacions. Escola Universitària Politècnica de Matarò. ants.dif.um.es/~humberto/asignaturas/v30/docs/Accesos.pdf (Consulta: 20 de Mayo de 2003).

ANEXOS

Anexo A. Tabla del análisis de riesgos diligenciada por el administrador del sistema.

Recurso del sistema		Riesgo(Ri)	Importancia (Wi)	Riesgo Evaluado (Ri* Wi)
Numero	**Nombre**			
	ESTACION DE CONTROL AVANZADO DE BLENDING	**8**	**6**	**48**
	ESTACION DE CONTROL AVANZADO	**8**	**6**	**48**
	ESTACIONES DE OPERACIÓN CONSOLA DE CRUDO	**4**	**8**	**32**
	ESTACIONES DE OPERACIÓN CONSOLA DE CRACKING	**4**	**8**	**32**
	ESTACIONES DE OPERACIÓN CONSOLA DE BLENDING	**4**	**8**	**32**
	ESTACION DE INGENIERIA SISTEMA DE CRUDO	**6**	**6**	**36**
	ESTACION DE INGENIERIA SISTEMA DE CRACKING	**6**	**6**	**36**
	ESTACION DE INGENIERIA SISTEMA DE BLENDING	**6**	**6**	**36**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRUDO	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE TRATAMIENTO	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE CRACKING	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE AZUFRE	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING REFINERIA	**6**	**4**	**24**
	ESTACION DE OPERACIÓN LOCAL SISTEMA DE BLENDING TNP	**6**	**4**	**24**
	ESTACIONES DE OPERACIÓN SISTEMA DE ENTRENAMIENTO	**6**	**0**	**0**
	ESTACION DE HISTORIA SISTEMA DE ENTRENAMIENTO	**6**	**0**	**0**
	ESTACIONES DE OPERACION Y GATEWAY #1 FOXBORO	**6**	**8**	**48**
	ESTACION DE BASE DE DATOS EN TIEMPO REAL	**6**	**8**	**48**
	ESTACION BENTLY NEVADA	**8**	**4**	**32**
	ESTACION DE ANALIZADORES VISTANET	**8**	**4**	**32**
	ESTACION DE INGENIERIA SISTEMA ABB	**8**	**6**	**48**
	ESTACIONES SISTEMA DE SHUTDOWN DE CRUDO	**8**	**10**	**80**
	ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRUDO	**8**	**10**	**80**
	ESTACIONES SISTEMA DE SHUTDOWN DE CRACKING	**8**	**10**	**80**
	ESTACION LOCAL SISTEMA DE SHUTDOWN DE CRACKING	**8**	**10**	**80**
	ESTACION LOCAL SISTEMA DE SHUTDOWN DE	**8**	**10**	**80**

	AZUFRE			
	MULTIPLEXER AMS SMART TRANSMITTER INTERFACE	**4**	**6**	**24**
	ESTACION AMS SMART TRANSMITTER INTERFACE – HART	**8**	**6**	**48**
	ROUTER SUPER STACK 3800	**4**	**6**	**24**
	HUB 24 PUERTOS UTP RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 24 PUERTOS UTP RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 6 PUERTOS FIBRA OPTICA RED DE PLANTA ABB	**4**	**6**	**24**
	HUB 24 PUERTOS UTP BLENDING	**4**	**6**	**24**
	HUB 24 PUERTOS UTP CONTROL AVANZADO	**4**	**6**	**24**
	SWITH 12 PUERTOS UTP BASE DE DATOS EN TIEMPO REAL	**4**	**6**	**24**
	SWITH 24 PUERTOS UTP ESD Y UPS	**4**	**6**	**24**
	PC PORTATIL HVAC	**8**	**4**	**32**
	ESTACION DE HISTORIA SISTEMA DE CRUDO	**6**	**6**	**36**
	ESTACION DE HISTORIA SISTEMA DE CRACKING	**6**	**6**	**36**
	ESTACION DE HISTORIA SISTEMA DE BLENDING	**6**	**6**	**36**
	ESTACION GATEWAY PI SISTEMA DE CRUDO	**8**	**6**	**48**
	ESTACION GATEWAY PI SISTEMA DE CRACKING	**8**	**6**	**48**
	ESTACION GATEWAY PI SISTEMA DE BLENDING	**8**	**6**	**48**
	ESTACION GATEWAY PI-ABB	**6**	**6**	**48**
	ESTACION NIR	**8**	**4**	**32**
	ESTACION DEL OPTIMIZADOR DE CRACKING	**8**	**6**	**48**
	ESTACION DE RECONCILIACION DE DATOS	**8**	**4**	**32**
	ESTACIONES DE OPERACION #1 SIEMENS	**4**	**8**	**32**
	ESTACION GATEWAY SIEMENS	**4**	**6**	**24**
	ESTACION PC ESCLAVO SIEMENS	**4**	**6**	**24**
	ESTACION DE STAR BLEND	**8**	**6**	**48**
	ESTACION DE SHORT TERM SCHEDULLING	**8**	**6**	**48**
	UPS CCB	**2**	**10**	**20**
	UPS SIH#1	**2**	**10**	**20**
	UPS SIH#2	**7**	**10**	**70**
	UPS SIH#3	**7**	**10**	**70**
	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRUDO	**8**	**4**	**32**
	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE CRACKING	**8**	**4**	**32**
	ESTACION DE INGENIERIA XTERMINAL SISTEMA DE BLENDING	**8**	**4**	**32**