



REPÚBLICA DEL ECUADOR

Escuela Politécnica Nacional

" E SCIENTIA HOMINIS SALUS "

La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del (los) autor(es).

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.
- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.
- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

“DISEÑO, IMPLEMENTACIÓN Y PRUEBAS DE LABORATORIO DEL SISTEMA DE SEGURIDAD FÍSICA INTEGRAL DE REFINERÍA ESMERALDAS”

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
ELECTRÓNICA Y CONTROL

ANDRÉS BENJAMÍN CAJO CRESPO

andrezk777@hotmail.com

MARTHA GRACIELA GUIJARRO ALTAMIRANO

m.guijarro17@gmail.com

DIRECTOR: ING. PATRICIO RAÚL FUSTILLOS PROAÑO

pfustillos@siaproci.com

CODIRECTOR: LUIS ANÍBAL CORRALES PAUCAR, PHD

luis.corrales@epn.edu.ec

Quito, diciembre 2014

DECLARACIÓN

Nosotros, Andrés Benjamín Cajo Crespo y Martha Graciela Guijarro Altamirano, declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Cajo Crespo Andrés Benjamín

Guijarro Altamirano Martha Graciela

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Andrés Benjamín Cajo Crespo y Martha Graciela Guijarro Altamirano y Andrés Benjamín Cajo, bajo mi supervisión.

Ing. Patricio Raúl Fustillos Proaño

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A Dios por darme la salud y perseverancia necesarias para luchar día a día y conseguir cumplir esta meta.

A mi madre, por su amor y apoyo incondicional durante toda mi vida.

A mis hermanos John y Joffre por el apoyo y cariño brindados sin ser su responsabilidad.

A mí querida novia Gabriela M. quien supo brindarme su apoyo y amor en el momento justo para finalizar la meta propuesta.

A mis queridas amigas Fernandita, Diana, Marjury y Jéssica que durante mi carrera fueron un apoyo importante y compartimos hermosos momentos que nunca olvidaré.

A la E.P.N por darme las enseñanzas necesarias para poder desarrollarme profesionalmente y humanamente.

Al departamento de CAC de Siaproci Cia. Ltda. en especial a Miguel Sempertegui y Anita Granizo quienes me brindaron sus conocimientos desinteresadamente cuando lo necesité.

Andrés Cajo.

AGRADECIMIENTO

Primero agradezco a Dios por haberme dado fuerza y valor para afrontar todos los obstáculos que se presentaron y haberlos superado.

A mis padres que son mi soporte, que aunque estando a la distancia siempre están pendientes de mí, por haberme impulsado a seguir adelante con sus consejos y guiarme por el camino correcto.

A mis hermanos que con su ejemplo me motivan a superarme y ser cada vez mejor.

A mis amigos que compartieron todo este proceso para llegar a esta meta, con su apoyo y momentos vividos durante nuestro tiempo de estudio así como hasta el momento.

A la empresa Siaproci por darnos la oportunidad de aprender y brindarnos el apoyo necesario para haber logrado esta meta, en especial a mis jefes y compañeros del proceso de consultoría y del proceso de construcciones que han compartido conmigo sus conocimientos para poder crecer profesionalmente además de enseñarme a trabajar en equipo en un ambiente de amistad.

Martha Guijarro.

DEDICATORIA

A mi madre Ana Luisa Crespo Abad que con su amor, apoyo y sacrificio incondicional me enseñó a amar y valorar el estudio, así como el significado de ser un buen ser humano para la sociedad.

A mis hermanos Joffre Bayas y John Bayas quienes con su cariño e inteligencia me han apoyado en todos los sentidos necesarios para culminar con éxito esta hermosa etapa de mi vida.

Andrés Cajo.

DEDICATORIA

A mis padres Carlos Guijarro y Enriqueta Altamirano que nos han guiado a todos sus hijos y han logrado que seamos unos profesionales y buenas personas, sin ellos esto no sería posible.

A mis hermanos Inés, Carlos, Yolanda y Jorge con los que he compartido nuevas experiencias estando lejos de nuestros padres.

Al ingeniero Patricio Fustillos y al Dr. Luis Corrales, por brindarnos su ayuda para culminar con nuestro proyecto de titulación.

Martha Guijarro.

CONTENIDO

RESUMEN	I
PRESENTACIÓN.....	II
CAPÍTULO 1.....	1
DESCRIPCIÓN Y DISEÑO CONCEPTUAL DE LOS SUBSISTEMAS QUE INTEGRAN LA SEGURIDAD FÍSICA	1
1.1 SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)	1
1.1.1 CONCEPTOS BÁSICOS DE UN CCTV.....	3
1.1.1.1 Tecnologías de sensores de imagen	3
<i>1.1.1.1.1 Tecnología CMOS</i>	<i>4</i>
<i>1.1.1.1.2 Tecnología CCD.....</i>	<i>4</i>
1.1.1.2 Tecnología POE	5
1.1.1.3 Tecnología megapíxel	6
1.1.1.4 Técnicas de barrido de imágenes	7
<i>1.1.1.4.1 Barrido entrelazado.....</i>	<i>7</i>
<i>1.1.1.4.2 Barrido progresivo</i>	<i>8</i>
1.1.1.5 Lentes	9
<i>1.1.1.5.1 Tipos de lentes</i>	<i>11</i>
<i>1.1.1.5.2 Criterio de selección del lente.....</i>	<i>13</i>
<i>1.1.1.5.3 Montaje de lente</i>	<i>14</i>
1.1.1.6 Sistema de CCTV analógico vs digital.....	15
<i>1.1.1.6.1 Cámara análoga.....</i>	<i>16</i>
<i>1.1.1.6.2 Cámara IP.....</i>	<i>17</i>
1.1.2 CRITERIO DE DISEÑO DE UN SISTEMA DE CCTV	18
1.1.2.1 Selección de cámaras.....	19
1.1.3 ELEMENTOS QUE CONFORMAN EL SUBSISTEMA	19
1.1.3.1 Cámaras	20
1.1.3.2 Grabador de video en red (NVR).....	22

1.1.3.3	Servidor web de video o encoder.....	23
1.1.3.4	Servidor de almacenamiento de video.....	24
1.1.3.5	Fuente de alimentación UPS.....	25
1.2	SUBSISTEMA DE CONTROL DE ACCESOS	26
1.2.1	CONCEPTOS BÁSICOS DE CONTROL DE ACCESOS	26
1.2.1.1	Tecnologías de reconocimiento	27
1.2.1.1.1	<i>Sistemas de uso de tarjetas de proximidad</i>	27
1.2.1.1.2	<i>Sistemas biométricos</i>	28
1.2.1.2	Protocolo Wiegand.....	28
1.2.1.3	Tipos de accesos controlables.....	29
1.2.1.4	Seguridad en puertas	30
1.2.1.5	Paneles de control de accesos	31
1.2.2	ELEMENTOS QUE CONFORMAN EL SISTEMA.....	32
1.2.2.1	Lectores	32
1.2.2.2	Entradas de seguridad.....	39
1.2.2.3	Dispositivos para seguridad en puertas	42
1.2.2.4	Dispositivos de carnetización	44
1.2.2.5	Tarjetas controladoras	46
1.2.2.5.1	<i>LNL-2220 (Controlador inteligente de lectora dual)</i>	46
1.2.2.5.2	<i>LNL-1320 (Módulo de interfaz de lectora dual)</i>	47
1.2.2.5.3	<i>LNL-500B (Interfaz puerta de enlace de lector biométrico)</i>	48
1.2.2.5.4	<i>LNL-1100 (Módulo de control de entradas)</i>	49
1.2.2.6	Software OnGuard	49
1.3	SUBSISTEMA DE SEGURIDAD PERIMETRAL POR CABLE SENSOR DE VIBRACIÓN	50
1.3.1	CONCEPTOS BÁSICOS DE SEGURIDAD PERIMETRAL.....	51
1.3.1.1	Etapas del sistema de seguridad perimetral.....	51
1.3.1.2	Tipos y configuraciones del sensor	52

1.3.1.2.1	<i>Sensores electromecánicos</i>	52
1.3.1.2.2	<i>Sensores piezoeléctricos</i>	53
1.3.1.3	Monitoreo local de alarma.....	53
1.3.1.4	Consideraciones ambientales.....	53
1.3.2	ELEMENTOS QUE CONFORMA EL SISTEMA.....	54
1.3.2.1	Sensor de vibración MDS-2.....	55
1.3.2.2	Cable multisensor de choque con sensores de vibración RB-SL3.....	55
1.3.2.3	Cable de comunicación y alimentación RB-4C.....	56
1.3.2.4	Unidades de procesamiento inteligente de campo SPU-2004.....	57
1.3.2.5	Terminación de zona RB-SLT.....	58
1.3.2.6	Unidad Meteorológica RB-VX25.....	59
1.3.2.7	Unidad Interfaz de control (IA-6500).....	60
1.3.2.8	Software VIDALERT.....	60
1.4	SISTEMA DE TRANSMISIÓN DE DATOS.....	61
1.4.1	Sistema CANOPY.....	62
1.4.1.1	<i>Configuración Punto a multipunto (PMP)</i>	63
1.4.1.2	<i>Elementos del sistema de comunicación CANOPY</i>	64
	CAPÍTULO 2	68
	DISEÑO DE LAS REDES DE LOS SUBSISTEMAS QUE INTEGRAN LA SEGURIDAD FÍSICA	68
2.1	DISEÑO DE LAS REDES DEL SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN.....	69
2.1.1	SELECCIÓN DE LENTE DE CÁMARA.....	70
2.1.2	CARACTERÍSTICAS TÉCNICAS DE EQUIPOS SELECCIONADOS.....	75
2.1.3	DESCRIPCIÓN DE LOS EQUIPOS DE CCTV.....	78
2.1.3.1	Cámara domo megapíxel fija.....	78
2.1.3.2	Cámara analógica PTZ.....	79
2.1.3.3	Inyector PoE.....	81

2.1.3.4	Grabador de video NVR.....	81
2.1.3.5	Servidor web de video.....	81
2.1.3.6	Switch de 8 puertos no administrable y fuente	82
2.1.3.7	Switch de 24 puertos PoE.....	83
2.1.4	DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE CCTV EN LAS AREAS A MONITOREAR.....	84
2.1.4.1	Cámara domo fija megapíxel (PoE).....	84
2.1.4.2	Cámara domo PTZ presurizada (análoga).....	86
2.2	DISEÑO DE LAS REDES DEL SUBSISTEMA DE CONTROL DE ACCESOS	88
2.2.1	DISEÑO DEL CONTROL DE ACCESOS DE CADA ÁREA.....	90
2.2.1.1	Garita peatonal.....	90
2.2.1.2	Garita vehicular.....	91
2.2.1.3	Sala de control (Bunker).....	92
2.2.2	CARACTERÍSTICAS TÉCNICAS DE EQUIPOS.....	93
2.2.3	DESCRIPCIÓN DE LOS EQUIPOS DE CONTROL DE ACCESOS.....	102
2.2.3.1	Lector de geometría de mano (handkey).....	102
2.2.3.2	Lectora de proximidad.....	104
2.2.3.3	Tarjetas de proximidad.....	104
2.2.3.4	Lector biométrico.....	105
2.2.3.5	Lectora vehicular de largo alcance.....	106
2.2.3.6	Tag vehicular (booster).....	107
2.2.3.7	Torniquetes simples y dobles.....	108
2.2.3.8	Puerta motorizada para personas con capacidades especiales	111
2.2.3.9	Molinete.....	111
2.2.3.10	Barrera vehicular.....	112
2.2.3.11	Luces indicadoras de acceso para handkey	114

2.2.3.12	Cerradura electromagnética	114
2.2.3.13	Contacto magnético.....	115
2.2.3.14	Panel de control de accesos	115
2.2.3.15	Tarjeta electrónica controladora LNL-2220	116
2.2.3.16	Tarjeta electrónica esclava LNL-1320	118
2.2.3.17	Tarjeta electrónica puente LNL-500B.....	119
2.2.3.18	Fuente electrónica de 24 VDC @ 2.5A.....	121
2.2.4	DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE CONTROL DE ACCESOS EN LAS ÁREAS DISEÑADAS	121
2.2.4.1	Diseño de diagramas de conexión del sistema de control de accesos en la garita peatonal	121
2.2.4.2	Diseño de diagramas de conexión del sistema de control de accesos en la garita vehicular	123
2.2.4.3	Diseño de diagramas de conexión del sistema de control de accesos en la sala de control de procesos (Bunker)	125
2.3	DISEÑO DE LAS REDES DEL SUBSISTEMA DE SEGURIDAD PERIMETRAL.....	126
2.3.1	DISEÑO DEL SUBSISTEMA POR ZONAS DE COBERTURA	127
2.3.2	CARACTERÍSTICAS TÉCNICAS DE EQUIPOS.....	129
2.3.3	DESCRIPCIÓN DE LOS EQUIPOS DE CABLEADO PERIMETRAL. ..	133
2.3.3.1	Cable sensor de vibración – 6C	133
2.3.3.2	Cable de datos y energía RB – 4C	133
2.3.3.3	Extensor de comunicación RS-485	134
2.3.3.4	Terminación de zona	134
2.3.3.5	Unidad inteligente SPU-2004	134
2.3.3.6	Tarjeta de protección contra descargas eléctricas	135
2.3.3.7	Unidad supresora de descargas eléctricas (E-CLIP)	136
2.3.3.8	Unidad meteorológica VX-25.....	136
2.3.3.9	Unidad interfaz de respaldo y control IA-6500	137

2.3.4	DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL EN LAS ÁREAS DISEÑADAS	138
2.4	DISEÑO DEL SISTEMA DE TRANSMISIÓN DE DATOS.....	140
2.4.1	DISEÑO DE LA COMUNICACIÓN DE EQUIPOS DE CADA ÁREA...	142
2.4.1.1	Garita peatonal.....	142
2.4.1.2	Garita vehicular.....	142
2.4.1.3	Sala de control de procesos (Bunker).....	142
2.4.1.4	Perímetro	142
2.4.1.5	Correspondencia de módulos suscriptores	143
2.4.2	CARACTERÍSTICAS TÉCNICAS DE EQUIPOS	144
2.4.3	DESCRIPCIÓN DE LOS EQUIPOS DE COMUNICACIONES.....	146
2.4.3.1	Módulo de administración de clúster (CMM)	146
2.4.3.2	Access point con AES y antena	146
2.4.3.3	Backhaul y fuente de poder	147
2.4.3.4	Módulo suscriptor	147
2.4.4	CUARTO DE CONTROL Y DATA CENTER.....	147
2.4.5	DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL EN LAS ÁREAS DISEÑADAS	154
CAPÍTULO 3.....		155
DISEÑO CONSTRUCTIVO E IMPLEMENTACIÓN DE LOS MÓDULOS DE SIMULACIÓN DE FUNCIONAMIENTO DE LOS SUBSISTEMAS QUE INTEGRAN LA SEGURIDAD FÍSICA		155
3.1	DISEÑO CONSTRUCTIVO E IMPLEMENTACION DE LOS MÓDULOS DE PRUEBAS DEL SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV) 155	
3.1.1	INSTALACIÓN DE LAS CÁMARAS Y ELEMENTOS COMPLEMENTARIOS PARA LAS PRUEBAS DE LABORATORIO	156
3.1.1.1	Instalación de la cámara PTZ.....	156
3.1.1.2	Instalación de las cámaras fijas.....	157
3.1.1.3	Instalación del grabador de video	158

3.1.2	CONFIGURACIÓN DEL SUBSISTEMA DE CCTV.....	158
3.1.2.1	Configuración del grabador de video (LNVR).....	160
3.1.2.2	Configuración de cámaras fijas.....	162
3.1.2.3	Configuración de la cámara PTZ.....	169
3.1.2.3.1	<i>Configuración del enlace inalámbrico</i>	<i>169</i>
3.2	DISEÑO CONSTRUCTIVO E IMPLEMENTACION DE LOS MODULOS DE PRUEBAS DEL SUBSISTEMA DE CONTROL DE ACCESOS.....	179
3.2.1	INSTALACION DE EQUIPOS DE CONTROL DE ACCESOS Y ELEMENTOS COMPLEMENTARIOS PARA ELABORAR LAS PRUEBAS DE LABORATORIO.....	180
3.2.2	CONFIGURACION DEL SUBSISTEMA DE CONTROL DE ACCESOS....	182
3.2.2.1	Configuración de la controladora LNL – 2220.....	182
3.2.2.2	Configuración de la tarjeta de doble interfaz LNL – 1320.....	187
3.2.2.3	Configuración de la tarjeta de enlace de handkeys LNL – 500B	193
3.2.2.4	Configuración de lectoras de proximidad R10	195
3.2.2.5	Configuración de handkeys (lectores de geometría de mano).....	200
3.2.2.6	Configuración de lectoras vehiculares.....	204
3.2.2.7	Configuración del biométrico de huellas digitales.....	208
3.2.2.8	Diseño constructivo e implementación de la espina de pescado	210
3.2.2.9	Diseño constructivo e implementación de la puerta motorizada de discapacitados.....	212
3.2.2.10	Diseño constructivo e implementación de las barreras vehiculares.....	214
3.2.2.11	Diseño constructivo e implementación del molinete	215
3.2.2.12	Diseño constructivo e implementación de la puerta de bunker	216
3.2.2.13	Creación y configuración de áreas de interés	217
3.2.2.14	Creación y configuración de zonas de tiempo	219
3.2.2.15	Creación y configuración de niveles de acceso	222
3.2.2.16	Creación y configuración de usuarios (tarjerahabientes)	226

CAPÍTULO 4	231
PRUEBAS Y RESULTADOS DEL FUNCIONAMIENTO DE LOS MÓDULOS ARMADOS	231
4.1 PRUEBAS Y RESULTADOS DEL SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)	231
4.1.1 PRUEBAS DE FUNCIONAMIENTO	231
4.1.2 RESULTADOS.....	243
4.2 PRUEBAS Y RESULTADOS DEL SUBSISTEMA DE CONTROL DE ACCESOS	243
4.2.1 PRUEBAS DE FUNCIONAMIENTO	243
4.2.1.1 Pruebas de la espina de pescado	246
4.2.1.2 Pruebas de la puerta motorizada de discapacitados	248
4.2.1.3 Pruebas del molinete	249
4.2.1.4 Pruebas de barreras vehiculares asociadas a lectoras vehiculares y boosters	249
4.2.1.5 Pruebas de la puerta de bunker	250
4.2.1.6 Pruebas de los equipos biométricos	251
4.2.2 RESULTADOS.....	254
CAPÍTULO 5	255
CONCLUSIONES Y RECOMENDACIONES	255
5.1 CONCLUSIONES	255
5.2 RECOMENDACIONES	256
REFERENCIAS BIBLIOGRÁFICAS	258
ANEXOS	260

RESUMEN

En la Empresa Pública De Hidrocarburos Del Ecuador (PETROECUADOR) específicamente en Refinería Esmeraldas, el problema de seguridad y control de personal es un factor alarmante ya que sus inmediaciones son extensas y la seguridad implementada actualmente es deficiente ya que se controlan los ingresos con un número escaso de personal y con métodos de control y registro poco adecuados. Razón por la que no se tiene un correcto manejo del personal y de los vehículos que ingresan y salen de las inmediaciones; y a esto se suma que el perímetro está limitado por una malla metálica de 3.5 metros la que con el tiempo se ha deteriorado y en muchos puntos esta se encuentra dañada y facilita el ingreso no autorizado de personas ajenas a la refinería.

Mediante el diseño y la implementación de los subsistemas de control de accesos, CCTV, y seguridad perimetral por cable sensor lo que se busca es eliminar los problemas indicados de una manera eficiente y viable. Los subsistemas de CCTV y control de accesos después de haber sido diseñados y aprobados por la fiscalización, se han implementado y probado a una escala menor en las inmediaciones de SIAPROCI CIA. LTDA. para que así la fiscalización tenga constancia física de los alcances de cada uno de ellos y su eficiencia al momento de eliminar los problemas que se han mencionado.

Como resultado de las pruebas efectuadas con los subsistemas implementados a escala menor, se determinó que el subsistema de CCTV posee las capacidades de monitoreo en tiempo real deseadas, y su fácil manejo permite revisar eventos grabados en caso de ser necesario analizar un evento específico, de manera que se elimina la falta control y monitoreo en los puntos críticos mencionados. En el caso del subsistema de control de accesos se logró probar su eficiencia en el control de personal y de vehículos, los eventos de ingreso y salida son registrados constantemente y en caso de violaciones de seguridad el sistema indica al operador en donde y a qué hora se dio dicho evento, de forma que en conjunto con CCTV, el control de eventos y personal es completo y de fácil manejo para el personal encargado de las labores de seguridad de la refinería.

PRESENTACIÓN

La importancia del presente proyecto de Titulación DISEÑO, IMPLEMENTACIÓN Y PRUEBAS DE LABORATORIO DEL SISTEMA DE SEGURIDAD FÍSICA INTEGRAL DE REFINERIA ESMERALDAS, radica en que busca resolver la inseguridad existente actualmente en refinería Esmeraldas, así como la necesidad de tener la facilidad de monitorear y controlar de forma centralizada los sistemas instalados en las inmediaciones de refinería. Para describir adecuadamente el trabajo realizado, este proyecto se lo ha dividido de la forma siguiente:

En el Capítulo I se tiene la descripción conceptual acerca de los tres subsistemas existentes, como son el subsistema de CCTV, subsistema de control de accesos y subsistema de seguridad perimetral. Se realiza una explicación de los equipos como de protocolos de comunicación a utilizar en la implementación y diseño.

En el Capítulo II se realiza el diseño de las redes de los subsistemas a implementar teniendo en cuenta la arquitectura con la que se cuenta y las necesidades requeridas para así especificar dimensiones y características técnicas de los equipos tanto electrónicos, mecánicos y de infraestructura a utilizar.

En el Capítulo III se detalla el diseño constructivo y configuración de cada uno de los sistemas a implementar de manera que se enfoca en el armado de los módulos a implementar usando los equipos propios del proyecto, y sus configuraciones necesarias para que funcionen como se tiene proyectado en la realidad.

En el Capítulo IV se detalla los resultados obtenidos de las pruebas de funcionamiento realizadas con los módulos armados del subsistema de CCTV y control de accesos, al haber sido integrados mediante software.

En el Capítulo V se tienen las conclusiones y recomendaciones resultantes a las que se ha llegado después de haberse realizado las pruebas de laboratorio del subsistema de CCTV y control de accesos.

CAPÍTULO 1

DESCRIPCIÓN Y DISEÑO CONCEPTUAL DE LOS SUBSISTEMAS QUE INTEGRAN LA SEGURIDAD FÍSICA

El objetivo de este proyecto es diseñar un sistema de seguridad física integral para la refinería Esmeraldas y armar los módulos de simulación para mostrar el funcionamiento de los subsistemas de CCTV y control de accesos.

En este capítulo se describen los alcances que se espera de los tres subsistemas, incluyendo la descripción general de los elementos, es decir equipos y protocolos de comunicación, que conforman dichos subsistemas, y que criterios de diseño se siguieron para conseguir las metas esperadas.

1.1 SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

Circuito cerrado de televisión o CCTV (siglas en inglés de closed circuit television) es una tecnología de video vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión de televisión convencional, todos sus componentes no emiten su señal fuera de un circuito. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

Entre las aplicaciones más usuales se destaca:

- Vigilancia periférica y perimetral de todo tipo de instalaciones.
- Supervisión de espacios de control de accesos y seguimientos interiores.
- Control del estado de áreas restringidas y otras dependencias internas.
- Supervisión y control a distancia de instalaciones.
- Grabación, transmisión y almacenamiento de imágenes y sonido.

En la arquitectura moderna de control de las instalaciones actuales, la incorporación del circuito cerrado de televisión (CCTV) es indispensable.

Los proyectos incluyen cámaras de funcionamiento nocturno y diurno, internas, externas y de iluminación y captación infrarroja para zonas de seguridad crítica, en color y en blanco y negro.

Entre las distintas cámaras y la imagen a presentar al operador se proponen una variedad de posibilidades dependiendo de la arquitectura de la instalación, de la zonificación del mismo y de las posibilidades de control. Entre los distintos equipamientos se tiene: mecanismos de control de posición de cámara (pan-tilt), controles de aproximación (zoom), controladores de señal (switches), grabadores de señal, particionadores de imagen, etc. Todos estos procesos se pueden hoy controlar mediante software especializado, e incluso utilizar las redes instaladas más comunes como las Ethernet, fibras ópticas e incluso la red telefónica del edificio para transmitir las señales de vídeo.

Los sistemas de CCTV están conformados básicamente por una serie de cámaras fijas o con movimiento, ocultas o discretas y sus respectivos monitores.

Para la mejor gestión o manejo de las cámaras hacia los monitores se utilizan las Matrices de Vídeo, que son sistemas capaces de direccionar a través de microprocesadores las entradas (Cámaras) hacia las salidas (Monitores), con las matrices de vídeo se pueden programar las secuencias de cámaras en un monitor,

Las cámaras pueden ser mostradas en otro monitor en caso de alarma, y se puede programar en el caso de las cámaras con movimiento una secuencia o ruta de movimiento y enfoque de una cámara en caso de Alarma. También Los sistemas modernos de CCTV permiten digitalizar las imágenes y comprimirlas para así poder mostrar en un solo monitor toda la información requerida, con los sistemas de videograbación se pueden grabar en tiempo real todas las señales comprimidas de las cámaras, y así tener una mejor secuencia de los hechos.

Ya que las cámaras de video vigilancia usualmente están ubicadas en distintos sectores de las instalaciones y estas deben ser monitoreadas desde un mismo sitio se requiere de un sistema de comunicación adecuado que centralice su

monitoreo así como de otros sistemas que pudieran existir como el control de accesos u otros.

1.1.1 CONCEPTOS BÁSICOS DE UN CCTV

La forma más sencilla de apreciar un sistema de CCTV es como un conjunto cámara- Medio de transmisión – Monitor.



Figura 1.1 Sistema básico de CCTV

1.1.1.1 Tecnologías de sensores de imagen

El sensor de imágenes de la cámara de vídeo transforma la luz en señales eléctricas. Estas cámaras pueden estar dotadas de sensores de imágenes que utilizan dos tipos de tecnología diferentes:

- CCD (Dispositivo de carga acoplada)
- CMOS (Semiconductor complementario de óxido metálico)

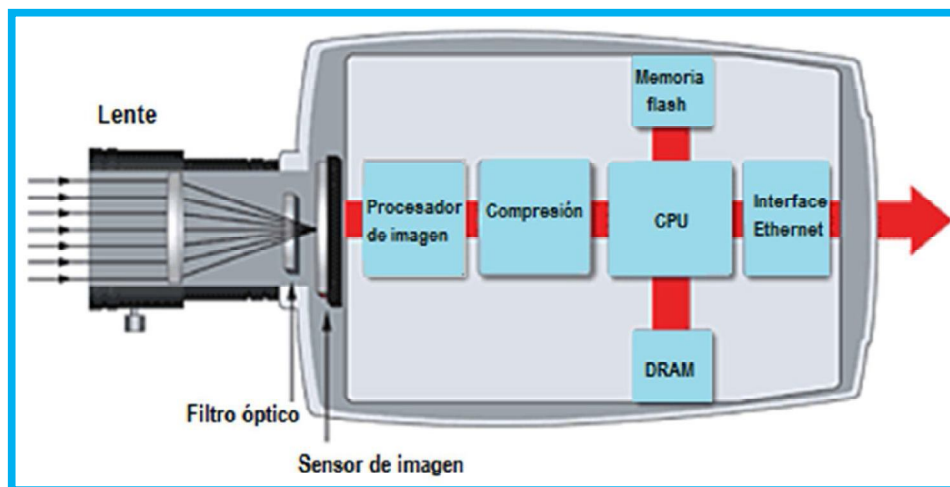


Figura 1.2 Sensor de imagen en cámara de video

Se debe considerar la posición del sensor de imágenes en la cámara de vídeo.

Los sensores CCD utilizan una tecnología desarrollada específicamente para las cámaras de vídeo, mientras que los sensores CMOS usan la tecnología estándar que se suele emplear en los chips de memoria, como los que se instalan en los PC.

1.1.1.1.1 Tecnología CMOS

Los sensores CMOS pueden ofrecer imágenes de alta calidad equivalentes a las de los sensores CCD, pero de todas formas inadecuadas para las cámaras que deben generar imágenes de una calidad elevada. Este tipo de sensores está también disponible en formatos más grandes, que aportan una resolución en megapíxeles a numerosas cámaras de vídeo en red. Una de las limitaciones más significativas de los sensores CMOS deriva de la menor sensibilidad a la luz que tienen, lo que no representa un problema en condiciones de iluminación normal, pero que sí puede serlo si la luz es insuficiente. Las imágenes que estos sensores generan en condiciones de poca iluminación pueden ser muy oscuras o borrosas.

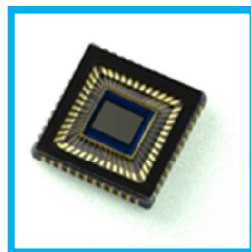


Figura 1.3 Sensor CMOS

1.1.1.1.2 Tecnología CCD

Los sensores CCD, ofrecen muchas ventajas en términos de calidad, como una mayor sensibilidad a la luz con respecto a los sensores CMOS. Esta mayor sensibilidad conlleva que las imágenes que se captan tengan más calidad, incluso en condiciones de poca iluminación. Sin embargo, los sensores CCD tienen un coste más elevado, ya que su incorporación en las cámaras requiere operaciones complicadas. Asimismo, si la escena contiene un objeto muy, el sensor CCD no puede captar correctamente las imágenes, lo que conlleva que en dichas

imágenes a menudo aparezcan líneas verticales encima y debajo del objeto. El núcleo de las cámaras de CCTV modernas es el sensor CCD.



Figura 1.4 Sensor CCD

Los CCD más grandes captan más luz, y por lo tanto tienden a ser más sensibles que los CCD en formato más pequeño. Los precios de las cámaras se incrementan con el tamaño del sensor. Por tanto, la selección del tamaño del sensor debe adecuarse tanto a su presupuesto como a la aplicación.

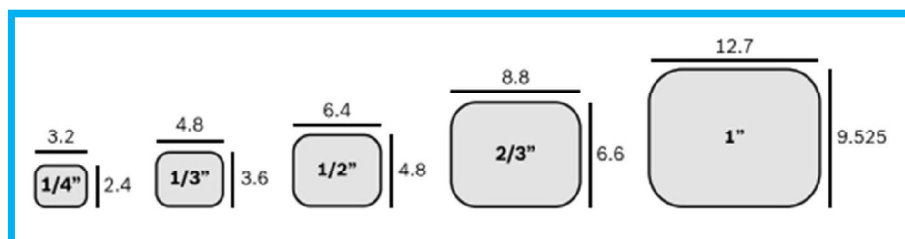


Figura 1.5 Tamaño de la imagen en milímetros

Note que el tamaño del sensor mostrado en la Figura 1.5 debe ser considerado en relación a la lente seleccionada dado que las lentes son también diseñadas para tamaños de sensores específicos.

1.1.1.2 Tecnología POE

PoE (Power over Ethernet) es una tecnología que le permite a las cámaras IP¹ conectarse a la corriente eléctrica utilizando el mismo cable de red. Esta característica no es única para las cámaras IP, existen teléfonos IP, equipos inalámbricos (APs -puntos de acceso WiFi) y controles de acceso IP con ésta característica.

¹Protocolo usado para la comunicación de datos a través de una red.

La ventaja inmediata al utilizar el mismo cable de red tanto para datos de video como para la alimentación eléctrica de la cámara es que se elimina la necesidad de conectarla en un tomacorriente cercano o la necesidad de tener que lidiar con paneles eléctricos.

Otro punto a favor es que el utilizar un sólo cable permite ahorro y minimizar costos al no requerir cableado eléctrico en las instalaciones de los sistemas de video vigilancia.

1.1.1.3 Tecnología megapíxel

Un megapíxel (Mpx) equivale a 1 millón de píxeles, a diferencia de otras medidas usadas en la computación en donde se suele utilizar la base de 1024, en lugar de 1000, para los prefijos debido a su conveniencia con el uso del sistema binario.

Usualmente se utiliza esta unidad para expresar la resolución de imagen de cámaras digitales, por ejemplo, una cámara que puede tomar fotografías o video con una resolución de 2048x1536píxeles se dice que tiene 3,1 megapíxeles ($2048 \times 1536 = 3.145.728$). El mismo principio se aplica a las cámaras de seguridad.

Resolución	Megapíxel
1280x1024	1.3 MP
1600x1200	2 MP
2048x1536	3.1 MP
2592x1944	5 MP
6400x1200	8 MP

Figura 1.6 Resolución de cámaras digitales

La cantidad de megapíxeles que tenga una cámara digital define el tamaño de ésta, pero hay que tener en cuenta que cada megapíxel está siendo distribuido en un área y, por tanto, no hay una diferencia significativa entre una cámara de siete u ocho megapíxeles, ya que no es una medida exponencial.

1.1.1.4 Técnicas de barrido de imágenes

El barrido entrelazado y el barrido progresivo son las dos técnicas disponibles hoy en día para leer y mostrar la información producida por los sensores de imagen. El barrido entrelazado se utiliza principalmente en los sensores CCD. El barrido progresivo se utiliza tanto en los sensores CCD como CMOS. Las cámaras de red o IP pueden utilizar cualquiera de las dos técnicas de barrido. Sin embargo, las cámaras análogas solamente pueden utilizar la técnica de barrido entrelazado para transferir imágenes a través de cable coaxial y para mostrarlas en monitores análogos.

1.1.1.4.1 Barrido entrelazado

Cuando se produce una imagen entrelazada a partir de un sensor CCD, se generan dos campos de líneas: un campo que muestra las líneas impares y un segundo campo que muestra las pares. Sin embargo, para crear el campo impar, se combina la información de ambas líneas de un sensor CCD. Lo mismo se aplica al campo impar, en el que la información de ambas líneas se combina para formar una imagen cada dos líneas.

Cuando se transmite una imagen entrelazada, solamente se envía la mitad del número de líneas alternado entre líneas pares e impares cada vez, lo que reduce el uso del ancho de banda a la mitad. En primer lugar se muestran las líneas impares y después las pares de una imagen y, a continuación, se actualizan de manera alternada a 25 imágenes (PAL²) o 30 imágenes (NTSC³) por segundo, de manera que el sistema visual humano las interpreta como imágenes completas.

Todos los formatos de vídeo análogos son entrelazados, aunque se crea distorsiones como resultado de datos que faltan, no se aprecian realmente en un monitor entrelazado. Sin embargo, cuando se muestra un vídeo entrelazado en monitores de barrido progresivo como son los monitores de computador, los defectos resultan apreciables. Los defectos se aprecian especialmente cuando se detiene el vídeo y se analiza una imagen congelada del mismo.

² Línea de fase alternada, sistema de codificación utilizado en la transmisión de señales de televisión analógica en color en la mayor parte del mundo.

³ Comisión Nacional de Sistema de Televisión, es un sistema de codificación y transmisión de televisión analógica en color en EE.UU.

1.1.1.4.2 Barrido progresivo

Con un sensor de imagen de barrido progresivo, los valores se obtienen para cada píxel del sensor y cada línea de datos de la imagen se barre de manera secuencial, lo que produce una imagen completa. En otras palabras, las imágenes captadas no se dividen en campos separados como ocurre en el barrido entrelazado.

En el barrido progresivo, se envía una imagen completa a través de una red y cuando se muestra en un monitor de computador de barrido progresivo, cada línea de una imagen se coloca en la pantalla en perfecto orden una tras otra. Los objetos en movimiento se muestran mejor en las pantallas de computador mediante la técnica de barrido progresivo. En las aplicaciones de video vigilancia, esto resulta vital para visualizar detalles en movimiento, por ejemplo, una persona que huyendo. La mayoría de las cámaras IP utilizan la técnica de barrido progresivo.

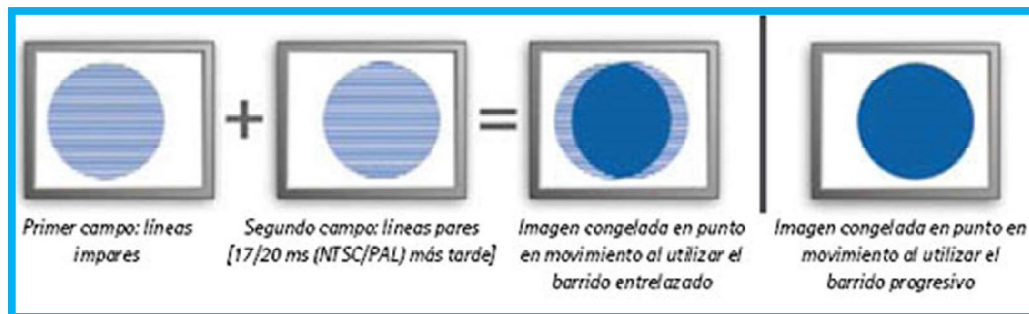


Figura 1.7 Barrido entrelazado y progresivo



Figura 1.8 Comparación entre barridos

A la izquierda, una imagen procedente de una cámara analógica que utiliza el barrido entrelazado. A la derecha, una imagen procedente de una cámara de red o IP que utiliza la tecnología de barrido progresivo. Ambas cámaras utilizaron el mismo tipo de objetivo y la velocidad del vehículo fue la misma de 20 km/h. El fondo es claro en ambas imágenes. Sin embargo, el conductor sólo se aprecia con claridad en la imagen que utiliza la tecnología de barrido progresivo.

1.1.1.5 Lentes

Las lentes son los “ojos” de un sistema de CCTV. Son esenciales para la creación de funciones de video. Las lentes ejecutan dos funciones principales. Primero, determinan la escena que podrá visualizarse en el monitor, esta es una función de la distancia focal. Segundo, controlan la cantidad de luz que alcanza el sensor, esta es una función del iris. La distancia focal puede ser fija o variable (ejemplo una lente con zoom). El iris puede ajustarse manualmente o la cámara puede hacerlo en forma automática.

- *Distancia focal*

La distancia focal es la distancia entre el centro de la lente y el sensor de imagen. Los rayos de objetos distantes son condensados internamente en la lente en un punto común del eje óptico. El punto en el que se posiciona el sensor de imagen de la cámara CCTV es llamado punto focal. Por diseño, las lentes poseen dos puntos principales: un punto principal primario y uno secundario. La distancia entre el punto principal secundario y el punto focal (sensor de imagen) determina la distancia focal de la lente.

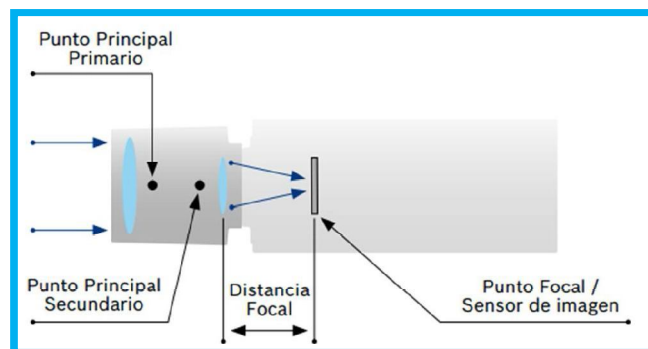


Figura 1.9 Determinación de Distancia focal

La medida de la distancia focal se expresa en milímetros. Las lentes son definidas como normales, gran angular o telefoto de acuerdo a su distancia focal. Por ejemplo, en un formato de cámara de 1/3", una lente de 8 mm es normal ya que es capaz de capturar un amplio campo de visión.

Mientras que, una lente de 125 mm en la misma cámara, en el mismo lugar observa un campo de visión más angosto aunque los objetos se amplíen significativamente (lente de largo alcance).





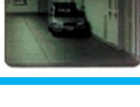
		1/3"	1/4"
	99°	2,8mm	2,1mm
	64°	4mm	2,8mm
	47°	6mm	4mm
	35°	8mm	6mm
	27°	12mm	8mm

Figura 1.10 Distancia focal de lente

- *Iris*

El iris controla la cantidad de luz que bloquea la cara del sensor de imagen. Para un óptimo desempeño, es crítico que no haya ni demasiada ni muy poca luz en el sensor de la cámara. Si mucha luz golpea el sensor de imagen, la imagen se "decolora". Cerrando el iris se corrige esto. En el otro extremo, muy poca luz golpeando la imagen del sensor genera una imagen negra o sólo los objetos más brillantes se tornan visibles. Abrir el iris corrige esta situación. Los iris pueden ser fijos, operar manualmente u operar automáticamente.

1.1.1.5.1 Tipos de lentes

Considerando la distancia a la que se quiere ver y la iluminación disponible en la escena a observar:

- *De iris fijo*

Una lente de iris fijo no ofrece ajustes para las diferentes condiciones de iluminación por lo que es limitada y no conveniente para aplicaciones donde se requieran detalles muy puntuales en forma constante. Se utilizan cuando la iluminación es constante, como por ejemplo los interiores iluminados artificialmente.

- *De iris variable manual*

Las lentes de iris manual son más convenientes para aplicaciones interiores, donde el nivel de iluminación es controlable y consistente. Cuando la iluminación interior puede tener variaciones por alternancias de luz artificial o natural, conviene utilizar estas lentes para lograr un ajuste de mayor precisión.

- *De auto iris*

Es la lente adecuada cuando la cámara está instalada en el exterior, ya que controla en forma automática la cantidad de luz que penetra en la misma manteniendo una señal de video constante, con una efectividad superior al iris electrónico y logrando además una mayor profundidad de campo.

Para observar una escena a una distancia determinada, en tanto, se debe seleccionar la lente en función de la distancia focal adecuada:

- *Lentes de distancia focal fija*

Cuando se ha definido irrefutablemente la lente necesaria. Las lentes fijas son el tipo de lente más simple, y por lo tanto son las menos costosas. Su distancia focal predeterminada requiere un preciso cálculo para la selección de la lente que mejor se adecue a la ubicación. Esta decisión debe estar basada en el tamaño deseado del área de visualización y su distancia desde la cámara.

- *Lentes varifocales*

En las instalaciones donde el campo de visión es inseguro o el usuario debe definirlo una vez instalado el sistema, se hace muy útil el uso de lentes varifocales que permiten ajustar en forma manual la distancia focal. Esto le ofrece al instalador variar el campo visual en presencia del usuario y fijarlo en una posición, de común acuerdo con el mismo.

También, simplifican el proceso de selección de lentes, ya que en un campo de visión flexible significa que se puede seleccionar una única lente para todas las cámaras en una misma instalación, sin interesar la ubicación de cada una de dichas cámaras.

- *Lentes con corrección por IR*

Esta lente compensa el cambio de foco que resulta de las diferentes longitudes de onda de la luz Visible e Infrarroja, permiten enfocar la luz en el mismo plano. La luz IR (infrarroja) afecta negativamente la exactitud de la reproducción del color, por esta razón, todas las cámaras a color emplean un filtro de bloqueo IR para minimizar o eliminar la luz que alcanza al sensor de imagen. El resultado es un mejor enfoque tanto de día como de noche, mejora del contraste, mayor nitidez y una mejor calidad de imagen en general.

Las cámaras Día/Noche y las monocromáticas pueden beneficiarse de las lentes con corrección por IR. El dispositivo CCD dentro de la cámara de seguridad puede detectar la luz IR y utilizarla para ayudar a iluminar el área observada.

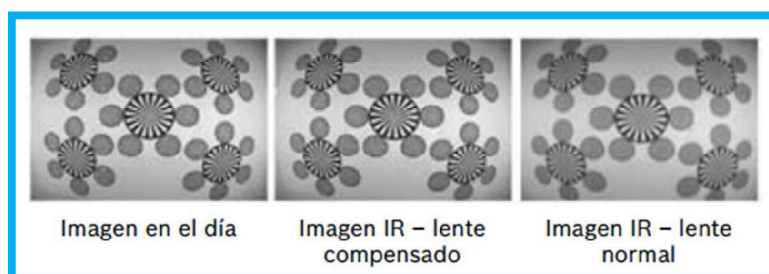


Figura 1.11 Corrección por IR

- *Lentes con zoom motorizado*

Las lentes con zoom son las más complejas pero ofrecen una gran funcionalidad. Éstas pueden ser ajustadas remotamente para permitir la variación de la distancia

focal y mantener el foco mientras se realiza el seguimiento. Esto significa que una lente puede ser utilizada para cubrir un área más amplia, hasta que se detecte un intruso. En ese momento, se puede realizar un acercamiento para captar los detalles de la cara.

Generalmente estas lentes incorporan un zoom motorizado, funciones de foco y auto-iris para permitir su máxima utilización.

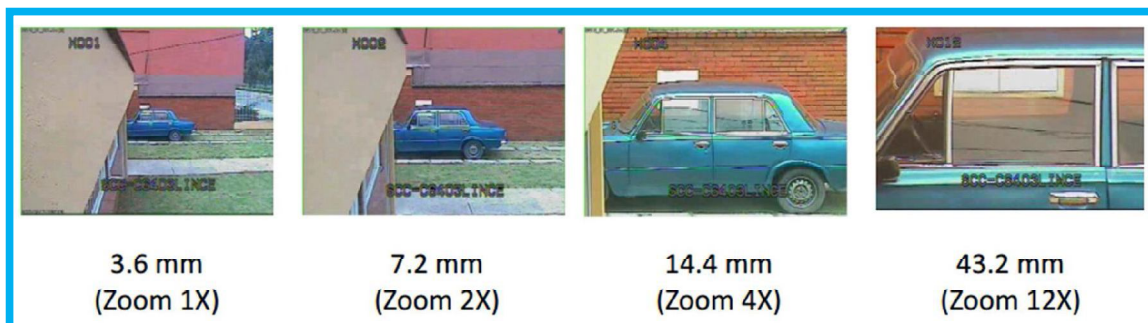


Figura 1.12 Relación de zoom con distancia focal

Comúnmente se expresa el “alcance” de un lente en la cantidad de veces que amplifica la imagen (X), se conoce como aumento o zoom óptico.

1.1.1.5.2 Criterio de selección del lente

Existen distintas herramientas para establecer el lente, siendo las más populares los programas y páginas web que permiten hacer el estimativo de la escena a obtener.

Son 4 los parámetros que se relacionan entre sí: Tamaño del sensor (ancho= a' , alto= h'), distancia de la cámara al objetivo (D), tamaño del objetivo (ancho= a , alto= h), y distancia focal del lente (f).

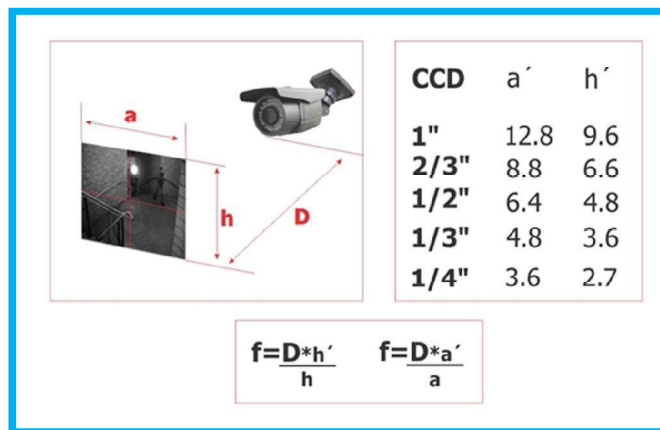


Figura 1.13 Parámetros para establecer el lente

1.1.1.5.3 Montaje de lente

Las lentes de CCTV utilizan montajes "C" o "CS" que especifican el tipo de anillo adaptador de lente y sus dimensiones. La diferencia está en la distancia a la que el lente debe quedar del sensor de imagen (CCD).

Con las lentes CS, la distancia es más corta, permitiendo el uso de vidrios en menores cantidades y en menor tamaño, generando un diseño más compacto de lentes.

La mayoría de las cámaras actuales utilizan montaje de lente tipo CS. Una lente CS puede ser utilizada únicamente en una cámara con un formato de montaje CS. Una lente de montaje debe situarse aproximadamente a 17,526 mm, pero también puede ser utilizada en una cámara de montaje CS sumando un anillo adaptador de 5 mm.

El sistema de montaje C se usa principalmente en cámaras con elementos de captación de imagen relativamente grandes (de 1/2 ó 2/3 pulgadas) mientras que los sistemas con montaje CS se utilizan para cámaras con elementos de captación de imagen más pequeños, del tipo 1/3" ó 1/4". La distancia del lente al sensor de los sistemas de montaje C y CS están estandarizadas en 17,526 mm y 12,5 mm respectivamente.

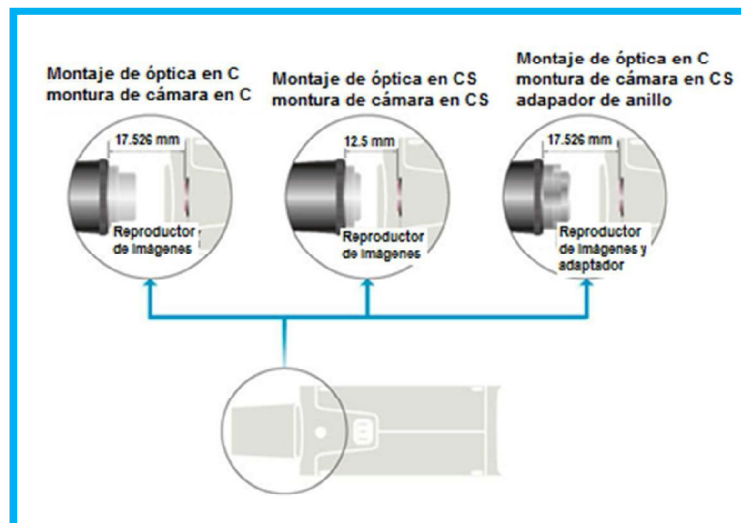


Figura 1.14 Montaje de lente tipo C y CS

1.1.1.6 Sistema de CCTV analógico vs digital

Las cámaras IP y las análogas, pueden parecer más similares de lo que realmente son; ambas emplean sensores CCD o CMOS. Mientras que prácticamente todas las cámaras análogas usan lectores CCD, la mayoría de las cámaras IP actuales utilizan sensores CCD o CMOS indiferentemente. La señal analógica del sensor se convertirá a digital por medio de un convertor analógico - digital y luego al procesador de imagen a bordo de la cámara. En la cámara IP, la imagen será codificada internamente y transmitida por medio de protocolo IP en redes Ethernet hacia los grabadores digitales (NVR); en la cámara analógica, el video se reconvierte nuevamente a analógico mediante un convertidor digital - analógico de forma que la imagen pueda ser transmitida hacia los grabadores analógicos (DVR) donde la señal es codificada y almacenada.

La diferencia entre estos tipos de cámaras es donde se comprime o codifica el video y que componentes utiliza. Hay diferencias significativas de calidad entre los sensores CCD y CMOS con una demostrable superioridad de los sensores CCD.



Figura 1.15 Comparación entre CCD Y CMOS

1.1.1.6.1 Cámara análoga

Una cámara de vigilancia análoga recibe la información en forma de luz mediante un sensor CCD el cual digitaliza la imagen y previo al envío de la información se usa una conversión digital análoga para que pueda ser recibido por un equipo análogo como un monitor o grabador. Diferente a las cámaras IP, las cámaras análogas no tienen ningún tipo de codificadores interno que les permita relacionarse con elementos digitales y su mantenimiento técnico es relativamente escaso.

Cuando se mide la resolución análoga, una línea TV no cuenta con un número definido de pixeles en específico. En su lugar, el término “Líneas TV” hace referencia al número de líneas horizontales o verticales en la pantalla (TVL por sus siglas en inglés). Las cámaras de seguridad análogas se miden en líneas de TV, y la mayoría tiene entre 420 y 580 TVL. Entre más alto sea el número de líneas de TV se logra capturar más información, y por lo tanto se obtiene una mejor imagen.

Las cámaras análogas no requieren de ningún tipo de administración, no existen direcciones IP, no hay programación de por medio y no involucra software.

Para poder ver una cámara analógica a través de la red o del internet esta debe ser conectada directamente a un DVR o a su vez a un NVR mediante un servidor web de video o encoder que codifica la imagen análoga a digital y puede ser recibida vía IP, para así administrar todo el video proveniente de las cámaras análogas.

Generalmente se realiza la conexión de cámaras análogas usando cable coaxial.

1.1.1.6.2 Cámara IP

Lo que comúnmente se conoce como cámara IP, es una cámara que digitaliza y procesa imágenes análogas, que después codifica internamente para ser enviadas por medio de conexiones Ethernet hacia computadoras o equipos similares. Las cámaras IP pueden tener sensores CCD o CMOS, algunas incluyen movimiento vertical, movimiento lateral y acercamiento (Pan / Tilt / Zoom), en forma de domos, tipo bala, con iluminación infrarroja, anti vandalismo y en ocasiones con conexión Wifi⁴.

Típicamente están equipadas con un servidor web de video integrado, y se puede acceder y controlar este tipo de cámaras por medio de cualquier red IP como MAN, WAN, LAN; ya que se utilizan navegadores web estándar o clientes de software, los usuarios pueden ver sus imágenes desde cualquier ubicación local o remota. Las cámaras IP combinan las capacidades de una cámara con las de una computadora; no requieren una conexión directa o dedicada a una computadora y pueden ser colocadas en cualquier lugar dentro de la red, justo como se haría con cualquier computadora. Una cámara IP es un dispositivo de red, tiene su propia dirección IP, se conectan por cable o wifi a la red y requieren un mantenimiento más constante que en el caso de las analógicas.

Entre sus posibles características se tiene:

- Resolución Megapíxel.- Permite visualizar detalles imposibles de ver con cámaras analógicas y/o VGA⁵ tradicionales.
- Zoom óptico.- Acercamiento de imagen mediante el objetivo y sin pérdida de calidad de imagen.
- Zoom digital.- Ampliación o acercamiento de una imagen mediante algoritmos matemáticos con una consiguiente disminución de la resolución de la imagen; este se conoce como falso acercamiento.
- 3GPP video streaming.- Permite visualizar remotamente vídeo online de una cámara IP en un teléfono 3G o smartphone.

⁴ Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica

⁵ Resolución de la matriz de gráficos de video, de 640 píxeles de ancho por 480 píxeles de alto.

- Conector I/O.- Diseñados para conectar dispositivos externos a la cámara tales como sirenas, alarmas, detector de movimientos, sensores de temperatura, iluminador externo, etc.
- Barrido progresivo.- Consigue una mayor nitidez y claridad en la grabación y visualización de imágenes en movimiento.

Una cámara IP con resolución megapíxel amplía el espectro de posibilidades en el mundo del CCTV ya que la mayoría de las instalaciones de CCTV cuentan con cámaras que ofrecen una pobre definición. Puede verse un hecho pero no identificar claramente a su autor.

La tecnología de megapíxeles permite a las cámaras de red ofrecer una resolución en las imágenes de video superior a la de las cámaras análogas. Es decir, tienen la capacidad de ver detalles e identificar personas y objetos, una característica clave al momento de diseñar un sistema de video vigilancia. Con una cámara de red tipo megapíxel la resolución es al menos tres veces mejor que con una cámara análoga.



Figura 1.16 Resolución megapíxel

1.1.2 CRITERIO DE DISEÑO DE UN SISTEMA DE CCTV

En un sistema de CCTV se debe poder realizar identificaciones durante el suceso que está visualizando o después en las grabaciones del sistema. Por eso es muy importante definir qué función van a cumplir y donde serán colocadas las cámaras, estas deben permitir realizar las siguientes identificaciones:

- Personal: esta se refiere a la capacidad del espectador de identificar personalmente alguien o algo. (caras, objetos etc.)
- De acción: esta interactúa mucho con la anterior y debe permitir verificar que realmente sucedió un hecho. (movimientos)
- De escena: se debe poder identificar y diferenciar un lugar de otro similar por la ubicación.

Para un correcto diseño se deben tomar en cuenta los siguientes pasos:

- Determinar el propósito del sistema de CCTV.
- Definir las áreas que cada cámara visualizará.
- Elegir el lente apropiado para cada cámara.
- Determinar donde se localizará el monitor o monitores para visualizar el sistema.
- Determinar el mejor método para transmitir la señal de vídeo de la cámara al monitor.
- Diseñar el área de control.
- Elegir el equipo con base a lo anterior.

1.1.2.1 Selección de cámaras

Las cámaras deben seleccionarse de acuerdo a los siguientes criterios:

- Sensibilidad: se refiere a la cantidad real de luz visible o infrarroja necesaria para producir una imagen de calidad.
- Resolución: define la calidad de imagen a partir de un detalle o perspectiva de reproducción.
- Características: son ajustes extras que le dan ventaja sobre otras cámaras.

1.1.3 ELEMENTOS QUE CONFORMAN EL SUBSISTEMA

Teniendo en cuenta el procedimiento de diseño de un sistema de CCTV se ha escogido los siguientes elementos:

1.1.3.1 Cámaras

- *Cámara domo⁶PTZ presurizada (análoga)*

Para el monitoreo del tránsito de vehículos al ingreso de refinería y de los posibles sucesos de intrusión por el perímetro se ha considerado el uso de cámaras PTZ presurizadas, ya que no se necesita de un mayor detalle de lo visualizado, las cuales estarán situadas en postes ubicados específicamente con el objetivo de cubrir visualmente todo el perímetro de refinería y parte de sus interiores, ya que gracias a sus características previamente mencionadas estas cámaras se pueden mover en varias direcciones y ser enfocadas manualmente.

Las cámaras PTZ, o de paneo, inclinación y ampliación (Pan, Tilt and Zoom) pueden hacer un barrido de 360 grados del ambiente, cambiar ángulos para mirar objetos por encima y por debajo de la cámara, y ampliar para darle más detalles a un objeto.

De esta manera un operador u operadores desde ubicaciones remotas tendrán la capacidad de rastrear eventos sospechosos en los límites de la refinería.

Las cámaras PTZ se controlarán a través de un sistema remoto compuesto por hardware y software de computadora. Se programa la cámara para que se mueva en un patrón establecido, o se controla manualmente con una interfaz que puede ser manipulada por un teclado. Un usuario introduce comandos, grados de ángulo y de rotación y la cámara se mueve según esto. Las cámaras PTZ también pueden ser controladas con palancas de mando u otros controles personalizados.

La característica de presurizada se refiere a que usando una carcasa, fabricada en acero inoxidable, capaz de mantener la impenetrabilidad, crea un ambiente aislado o hermético, este ambiente es rellenado de manera que se usa presión positiva y se inyecta gas no reactivo (nitrógeno seco) para crear una atmósfera que no reacciona con los recubrimientos de las lentes ni con los componentes de las cámaras y que impide la entrada de contaminantes externos.

Debido a que estas cámaras se encontrarán distribuidas en todo el perímetro colindante a la selva que rodea a la refinería se ha escogido cámaras de tipo

⁶ Carcasa en forma de cúpula

analógico, ya que como se ha mencionado estas no requieren un mantenimiento tan frecuente como las de tipo digital.



Figura 1.17 Cámara PTZ

- *Cámara domo fija megapíxel (IP)*

Se ha escogido este tipo de cámaras para monitorear locaciones puntuales, con el objetivo de controlar las áreas de circulación peatonal, y poder visualizar con mayor detalle a personas y objetos.

Se tendrá este tipo de cámaras sobre pared en los ingresos peatonales, pues en estos sitios hay un punto de enfoque fijo hacia los controles de acceso y registro de horario. Estas cámaras contarán con tecnología PoE ya que esto evitará el uso de un cable extra para alimentación, pues al ser POE con un mismo cable se obtiene comunicación y alimentación.

Su ventaja radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Además, la carcasa curva de la cámara la protege de forma eficaz contra el redireccionamiento deliberado y el desenfoco. Gracias a su característica IP se conecta directamente a la red mediante el grabador de video (NVR).



Figura 1.18 Cámara domo fija

1.1.3.2 Grabador de video en red (NVR)

En este sistema se ha seleccionado un NVR por su capacidad de grabación y por su característica de enlazarse a la red.

Tanto para las cámaras fijas IP como para las cámaras PTZ análogas se utiliza el grabador de red (NVR). Para las cámaras análogas al no ser IP se necesita el uso adicional de un servidor web de video o encoder para poder conectarse al grabador de video en red.

Un NVR (Network Video Recorder) es un hardware "grabador de video en red" que funciona en forma independiente de un computador y se presenta como un hardware con funcionalidades de gestión de vídeo preinstaladas. Un NVR está diseñado específicamente para gestión y administración de vídeo digital codificado, por lo que está dedicado a sus tareas específicas de grabación, análisis y reproducción de vídeo en red. El NVR se incorpora con un gran volumen de disco duro para permitirle una gran capacidad de almacenamiento de eventos.

Un NVR se diseña dependiendo del número particular de cámaras de red en el sistema. Esto permite que la unidad resulte más adecuada para sistemas más pequeños donde el número de cámaras se encuentra dentro de los límites de la capacidad del NVR.



Figura 1.19 Grabador NVR con cámaras IP

1.1.3.3 Servidor web de video o encoder

Como se mencionó anteriormente las cámaras análogas requieren de un servidor web de video el cual codifica las imágenes a digitales para de esta forma poderse incorporar al grabador de video en red.

Se usará un servidor web de video de 4 canales análogos; cada cámara PTZ ubicada en el perímetro ocupará uno de los 4 canales, debido a la distancia entre dichas cámaras.

Los usuarios del sistema se beneficiarán de las ventajas del vídeo en red sin tener que usar necesariamente cámaras de tipo digital que cuestan más y que su mantenimiento también es más costoso en comparación de las analógicas con cableado coaxial.

El codificador de vídeo se conectará a la cámara análoga a través de un cable coaxial y convierte las señales de vídeo análogas en secuencias de vídeo digitales que luego se envían a través de una red basada en IP. Para la visualización o grabación el vídeo digital se suelen usar computadores, pero en este caso se usará un NVR por el volumen de información codificada que se manejará.

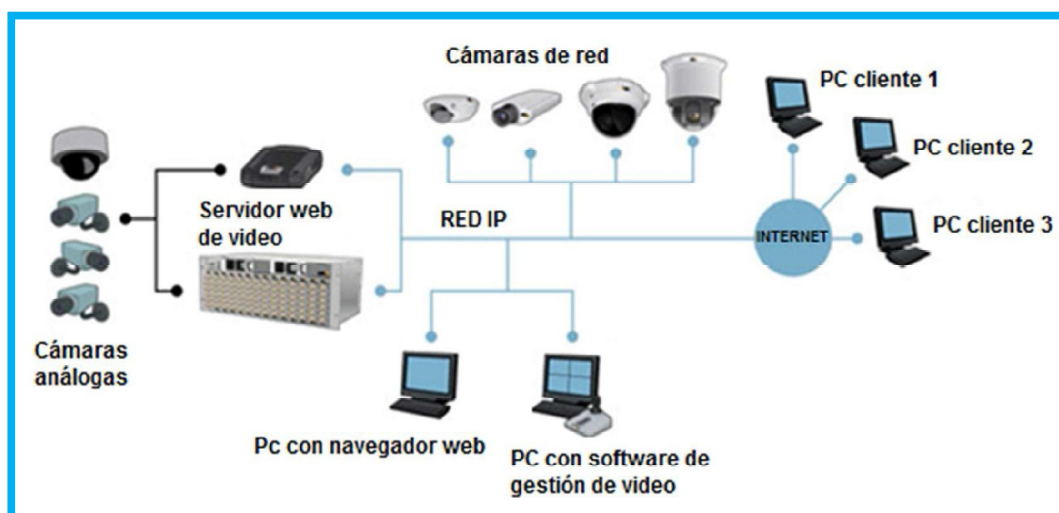


Figura 1.20 Conversión de video análogo a digital

1.1.3.4 Servidor de almacenamiento de video

A más del NVR se utilizará adicionalmente el denominado Servidor de Reserva de Grabaciones (SRG) para un almacenamiento masivo en red, que es un equipamiento secundario de respaldo al subsistema de administración y grabación local. La unidad de almacenamiento se administrará por un software específico para hacer la reserva, exportación, seguimiento etcétera de las grabaciones realizadas.

El SRG se basa en una plataforma que incluye un servidor dedicado con los arreglos de discos duros necesarios para llegar a ofrecer la capacidad de almacenamiento requerida. Dicho servidor es un sistema manual de almacenamiento masivo donde se salvaguardarán secuencias de vídeo.

Básicamente el SRG centralizará sobre un mismo y único repositorio las secuencias de vídeo que se han considerado que deben permanecer por encima del tiempo de grabación definido en los sistemas de grabación locales.

En la Figura 1.21 se ejemplifica el diagrama básico de funcionamiento para la correcta administración de los videos captados por diferentes cámaras de red asociadas al monitoreo en diferentes ubicaciones.

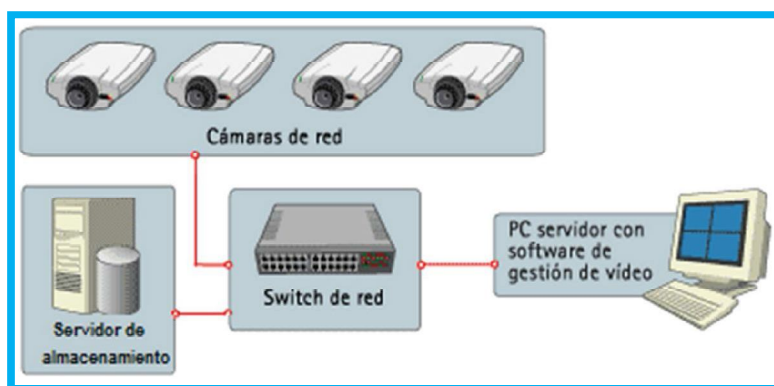


Figura 1.21 Servidor de almacenamiento de video

1.1.3.5 Fuente de alimentación UPS

Ya que es indispensable que el sistema se mantenga en línea y funcionando de forma constante a pesar de posibles fallos de la alimentación principal de la red eléctrica existente, se contará con UPS.

Estos equipos se ubicarán en postes distribuidos en los perímetros de refinería y su fin será tener un respaldo de alimentación para las cámaras PTZ más cercanas ya que estas a diferencia de las cámaras fijas IP, no cuentan con tecnología POE por lo que requieren alimentación independiente de la comunicación. De la misma forma estos equipos alimentan al sistema de transmisión de datos.

El UPS provee de 24 VAC para alimentar las cámaras PTZ, este voltaje ingresará a un transformador que lo incrementará a 110 VAC con lo que podrá alimentar el resto de equipos correspondientes al sistema de transmisión de datos.

El UPS también conocido por las iniciales SAI (Sistema de Alimentación Ininterrumpida), es un conjunto de dispositivos (eléctricos y electrónicos) que aseguran el suministro sin interrupción de energía eléctrica de calidad.

Las UPS además de suministrar energía eléctrica ininterrumpida durante un cierto periodo de tiempo, protegerán los equipos si se presentan variaciones de tensión o perturbaciones, suministrando una energía limpia y estable. Éste dispositivo se colocará entre la salida del servicio eléctrico de corriente alterna y los equipos que requieren ser protegidos de apagones, reducción de tensiones de línea y otros.

El UPS toma corriente alterna de entrada, luego un interruptor detecta el nivel de energía de entrada y una batería simultáneamente se está cargando para ser utilizada en caso de falla de la fuente de energía.

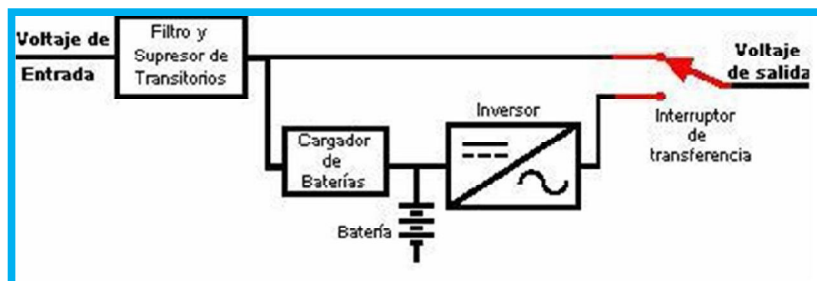


Figura 1.22 Esquema de funcionamiento del UPS

El UPS convierte la energía de la Corriente Alterna que ingresa, a Corriente Directa y luego la reconvierte en Corriente Alterna purificada.

1.2 SUBSISTEMA DE CONTROL DE ACCESOS

Los sistemas de control de acceso son la tecnología con más demanda en el mercado actual, se ha migrado de sistemas mecánicos y con personal especializado, a tener procesos de control de entrada y salida completamente automatizados con diferentes tipos de tecnologías y dispositivos. La función principal de un Sistema de Control de acceso es administrar el acceso de personal o vehículos a áreas consideradas como restringidas, y evitar así que personas no autorizadas o indeseables tengan acceso. Además de esta función principal, un Sistema de Control de Accesos se puede usar para controlar la asistencia del personal y tener un control histórico de entradas de personas a todas las áreas.

Realizar un estudio adecuado es importante, segmentando las zonas, los grupos de acceso, los horarios permitidos, el nivel de acceso de cada usuario, medir la cantidad de personas o vehículos que transitan por cada zona y establecer claramente los objetivos de cada control de acceso.

Es importante el estudio y diseño previo a cualquier instalación y puesta en marcha de un proyecto de seguridad y control de acceso. Una adecuada integración de los dispositivos electrónicos con los dispositivos electromecánicos permitirá incluso reducir drásticamente los costos de personal y totales del proyecto.

1.2.1 CONCEPTOS BÁSICOS DE CONTROL DE ACCESOS

Un control de acceso consta básicamente de tres etapas:

- Reconocer al usuario que desea ingresar a un área determinada, así como un control o registro de asistencia. El reconocimiento puede ser realizado por lectores biométricos (huella dactilar, geometría de la mano), tarjetas de proximidad en el caso de accesos peatonales o control de asistencia de personal, tags o etiquetas de proximidad para parabrisas, transmisores de

radio frecuencia y reconocimiento de número de matrícula, en el caso de accesos vehiculares.

- Procesar la información del usuario en el panel de control de acceso, el cual de acuerdo a las credenciales asociadas otorga o niega el ingreso; el que puede ser regulado con base en la fecha y hora, así como al sitio al cual el usuario desea acceder. Adicionalmente, los paneles de control pueden estar enlazados con computadoras de monitoreo de eventos ubicadas en el cuarto de control, lo que favorece la labor del personal.
- Otorgar el acceso, lo que permite el paso del usuario por medio de la apertura de puertas automáticas, cerraduras magnéticas, torniquetes, molinetes, portones eléctricos, barreras vehiculares, entre otros.

1.2.1.1 Tecnologías de reconocimiento

Los nuevos sistemas de control de acceso se basan en tecnologías de reconocimiento que van desde el uso de una clave numérica o un chip, hasta el aplicación de la biometría.

1.2.1.1.1 Sistemas de uso de tarjetas de proximidad

También conocidos como RFID⁷, este es un sistema de almacenamiento y recuperación de datos de manera remota que usa dispositivos denominados etiquetas, tarjetas o tags RFID. El principal objetivo que cumplen es el de transmitir la identidad de una persona a través de ondas de radio. Esta tecnología también se le denomina de identificación automática.

Este sistema contiene sensores que permiten enviar y recibir ondas de radio sin que se requiera necesariamente una visión directa entre el emisor y el receptor. Cuando capta una señal de una etiqueta la cual contiene la información de identificación de la persona, extrae la información y se la pasa al subsistema de procesamiento de datos.

⁷Identificador de radiofrecuencia

1.2.1.1.2 Sistemas biométricos

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El uso de este tipo de sistemas es el más eficaz en caso de necesitarse una seguridad de alto nivel para el ingreso a ciertas áreas.

Este sistema le permite el acceso a través del escaneo de la huella dactilar, lectoras de geometría de mano u otras características físicas individuales. Esto reduciría los posibles problemas de seguridad y agilizaría el proceso de acceso.

En un sistema de biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta son obtenidas, procesada por un algoritmo numérico, e introducida en una base de datos.

Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente desde valores bajos como el 60%, hasta altos como el 99,9%.

1.2.1.2 Protocolo Wiegand

El protocolo Wiegand es ampliamente utilizado por la mayor parte de los fabricantes de lectores porque permite la transmisión de información a través de un par de cobre acompañado por la alimentación para el dispositivo de lectura sin afectar por ello a los datos.

Como todo protocolo de comunicaciones, Wiegand consta de dos partes fundamentales: una parte describe el modo en que físicamente se transmite la información digital y la otra parte, la forma de interpretar numéricamente dicha información.

La transmisión de datos Wiegand usa tres hilos. La línea para enviar los unos lógicos o DATA1, la línea para hacer lo propio con los ceros lógicos o DATA0 y la línea de masa de referencia de ambos o GND.

Los niveles que se usan son Bajo, a nivel de GND, o Alto a +5V o VCC. En estado de reposo, o sea sin transmitir, la línea de GND siempre está en nivel bajo y las líneas DATA1 y DATA0 están en nivel alto, a nivel de +5V ó VCC.

Para transmitir un Bit 1 se envía un pulso a bajo, normalmente de 50 μ seg (microsegundos) de duración, por la línea DATA1, mientras DATA0 permanece en alto. Para transmitir un Bit 0 se envía un pulso a Bajo, también de la misma duración 50 μ seg (microsegundos).

El código Wiegand enviado a un computador destino consta de 24 bits, pero al momento de la finalización de la adquisición del código se poseen tres variables de 8 bits cada una.

La razón de esto es por la necesidad de optimizar la adquisición de los datos, ya que de esta forma el código ejecutado por cada interrupción es menor. Por lo tanto se debe formular una variable de 24 bits a partir de tres de 8 bits, esta tarea es desarrollada en la aplicación principal.

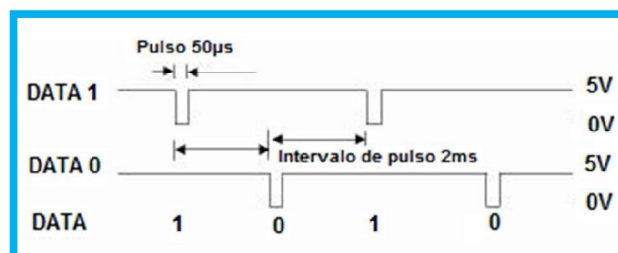


Figura 1.23 Transmisión de datos wiegand

1.2.1.3 Tipos de accesos controlables.



Figura 1.24 Elementos de acceso

Las soluciones en accesos de seguridad le permiten monitorear y controlar tanto el flujo de peatones como de vehículos, según corresponda, que entran y circulan por sus instalaciones. Son compatibles con cualquier sistema de control de accesos, también se atienden distintas necesidades, como los accesos para discapacitados.

Se destacan por la versatilidad y principalmente, por la facilidad de integración con otros componentes de seguridad, tales como lectores biométricos, de geometría de mano y lectoras de proximidad.

1.2.1.4 Seguridad en puertas



Figura 1. 25 Elementos para seguridad en puertas

Para la seguridad en puertas se dispone de dispositivos como cerraduras electromagnéticas, contactos magnéticos y brazo cierra puertas.

La cerradura electromagnética es un dispositivo imantado que fuerza el cierre de la puerta al cortar la corriente, son el complemento ideal para un sistema de control de accesos. Estas cerraduras poseen dos características que son fundamentales: en primer lugar son totalmente silenciosas y en segundo lugar da la oportunidad de permitir la apertura en casos extremos o de emergencia.

El contacto magnético se utiliza para monitorear el estado de puertas y ventanas, con bisagra o corredizas, portones, cortinas metálicas, claraboyas, y en general todo tipo de apertura.

El brazo cierra puertas se trata de un mecanismo que brinda amortiguamiento, cierre automático a todo tipo de puertas y regulación de velocidad de cierre, la mayoría tienen funcionamiento hidráulico pero también hay a resorte.

1.2.1.5 Paneles de control de accesos

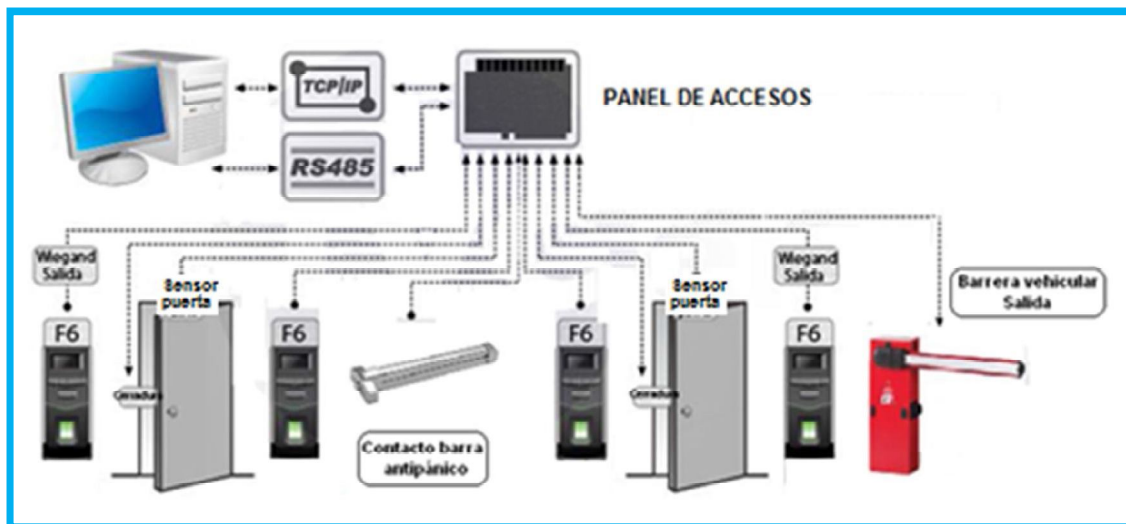


Figura 1.26 Panel de control de accesos

Los paneles con software más básicos sirven para una aplicación de suficiente seguridad, ya que permiten controlar las entradas de todos los lectores, contactos magnéticos de puertas, contacto de barra anti pánico, así como relés de salida para cerraduras magnéticas, torniquetes, molinetes, y barreras vehiculares del sistema para llevar un registro de cuándo y por quién una determinada puerta, torniquete, molinete, barra anti pánico ó barrera vehicular se accionó.

Pueden incluir también la hora en el momento de entrada y salida de los empleados, los horarios de fines de semana o días libres. Pueden también ser compatibles con otras medidas de seguridad ya existente, tales como alarmas o Circuito Cerrado de Televisión.

Los paneles de control pueden funcionar dentro de un mismo sistema o en puntos remotos y reportar los eventos registrados en el mismo a un computador usando un puerto Ethernet o un puerto RS-485.

1.2.2 ELEMENTOS QUE CONFORMAN EL SISTEMA

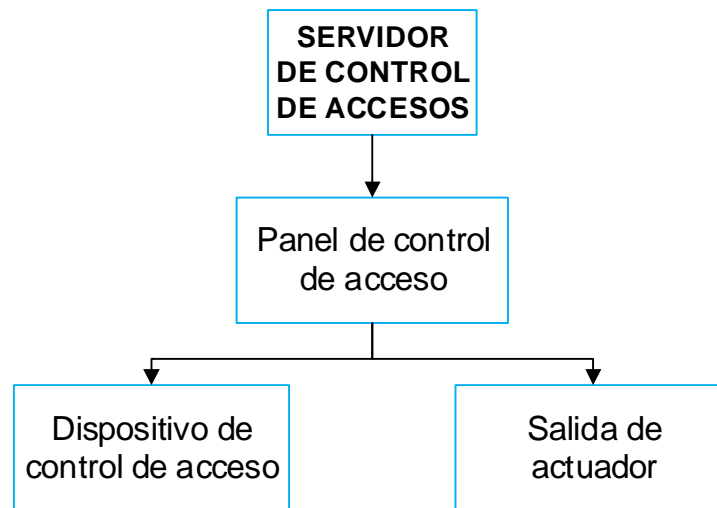


Figura 1.27 Elementos del sistema

1.2.2.1 Lectores

- *Lector Biométrico De Geometría De Mano (Handkey)*

Se ha optado por estos equipos debido a que su tecnología garantiza una forma eficaz de control de ingreso de personal sin que esta pueda ser burlada de alguna forma, ya que las características geométricas de las manos de una persona no se repiten de persona a persona. Estos dispositivos se usarán en los ingresos peatonales, para que luego de haberse permitido el acceso por las entradas de seguridad, se efectúe el control de asistencia, se tendrá un registro de entrada y salida de personal y contratistas de refinería.

El lector de geometría de mano (handkey), verifica las características de la geometría tridimensional peculiar de cada mano de las personas que serán registradas, permitiendo o negando el acceso en función de la evaluación realizada en cada caso.

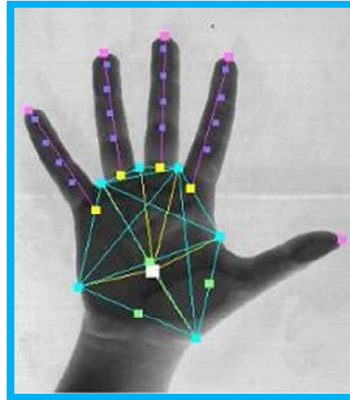


Figura 1.28 Lectura de geometría de mano

El usuario colocará su mano en la parte interna del dispositivo, posicionando sus dedos acorde al juego de pines señalizadores marcados en el dispositivo por aproximadamente 1.2 segundos. Una cámara digital captura la forma de la mano y envía los datos a un microprocesador para su análisis. Este procesador mide las características más resultantes de la geometría de la mano como longitud y ancho de los dedos, área total, etc.



Figura 1.29 Colocación de mano sobre pines

Los datos son comprimidos hasta tener aproximadamente 9 bytes de información fundamental que caracteriza la mano de cada persona y esta información se comparará con todos los perfiles almacenados previamente en la base de datos. La información de los nuevos usuarios se podrá capturar fácilmente ya que este solo tendrá que colocar la mano en el dispositivo tres veces para obtener los datos en forma inicial.

- *Lector Biométrico*

De similar manera que el handkey se ubicará un lector biométrico en el área vehicular, ya que al igual que la geometría de la mano las huellas dactilares son propias y únicas de cada individuo.

El uso de este equipo será para control de asistencia y registro de horario de entrada-salida de contratistas.

El lector de huella dactilar es un periférico para la seguridad del computador y seguridad informática en general. Está equipado con un módulo de lectura de huella dactilar basado en la tecnología de biometría. Este lector reemplaza el acceso por contraseña, lo que hace al sistema menos vulnerable al fraude.

La huella dactilar presenta unas particularidades como son las convergencias, desviaciones, uniones, interrupciones, fragmentos, etc. que forman las crestas que la componen.

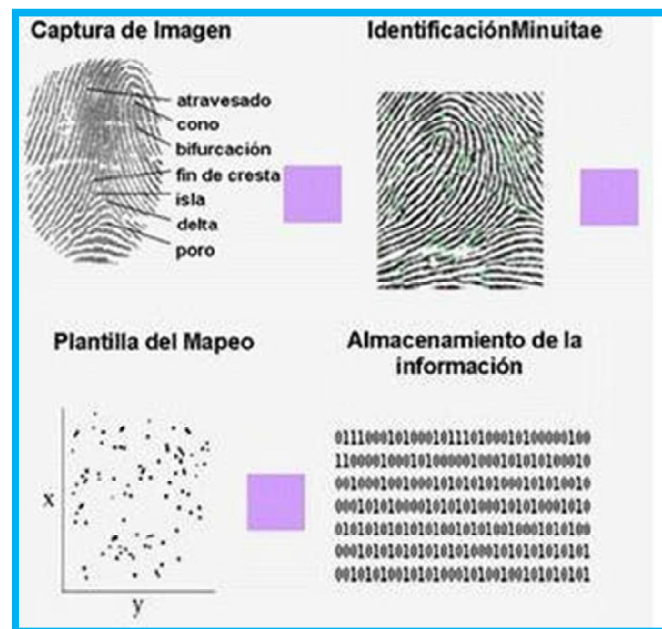


Figura 1.30 Funcionamiento de lector biométrico

En una huella se tiene una serie de crestas y valles que crean el dibujo en el cual se puede reconocer ciertos puntos de interés, comúnmente llamados “minutiae” o minucia. De todos estos puntos, lo que realmente interesa para la identificación son principalmente las terminaciones o bifurcaciones de las crestas. Existen

también otros puntos de interés como: el núcleo (centro del patrón de la huella), las islas, los deltas y las discontinuidades.

El motivo por el cual interesan estos puntos es que, entre ambos, suman casi el 80% de los puntos de la huella dactilar. A una minucia se le atribuyen dos características: la posición y la orientación.

Es absolutamente necesario el uso de un procesado electrónico de la huella dactilar. Para realizar dicho procesado, el algoritmo encargado de comparar la huella debe recibir como parámetros las características de las minucias presentes en la muestra.

Este procedimiento recibe el nombre de filtrado, pues se encarga de eliminar la información no necesaria para quedarse sólo con lo interesante: las minucias y su par posición y dirección.

- *Lectora de Proximidad*

Gracias a su versatilidad de usos y combinaciones en el campo de control de accesos, se usarán lectoras de proximidad en los ingresos peatonales para control de acceso por torniquetes, molinete y puerta cortafuegos.

La lectora de tarjetas es solo el periférico de entrada y accionamiento del sistema ya que el sistema completo actúa como un oficial de seguridad que revisa credenciales, es decir, una tarjeta con los datos del personal y permite a las personas autorizadas ingresar cuantas veces lo deseen.

El funcionamiento básico será:

- Las tarjetas o etiquetas electrónicas llevarán un microchip incorporado que almacenará el código único.
- El lector envía una serie de ondas de radiofrecuencia al tag, que éste capta a través de una antena.
- Las ondas activan el microchip, transmitiendo al lector cual es el código único de la tarjeta.

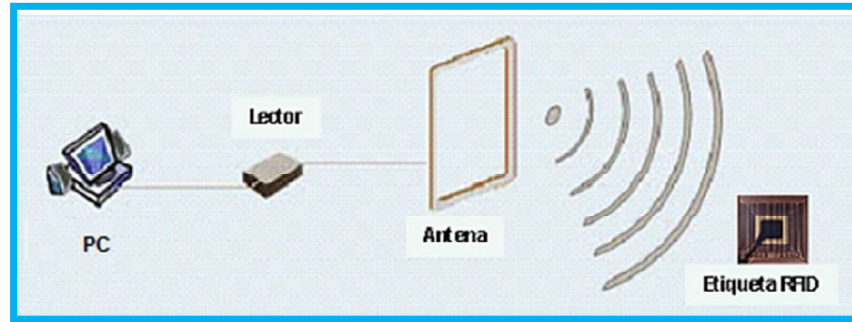


Figura 1.31 Funcionamiento de lectora de proximidad

Luego de recibir los datos, el controlador procesa el código. El primer paso es el análisis del tamaño de la cadena de números y también del formato del código recibido. Si el código se ajusta a las especificaciones determinadas para la puerta, el controlador lo compara con el código establecido para el acceso. Debe tenerse en cuenta que el código puede servir sólo para cierta cantidad de accesos y entre fechas específicas.

Si algún parámetro de la secuencia no concuerda, el controlador denegará la apertura de la puerta. La aplicación de software a la cual se accede desde el computador permite a una persona autorizada actualizar la información del dueño, habilitar o deshabilitar la activación de la tarjeta, configurar el hardware de acceso a la puerta y proveer los informes necesarios sobre el uso del sistema.

- *Lector de largo alcance tag/etiqueta vehicular*

El control de tránsito de vehículos de personal y contratistas de refinería se realiza mediante lectoras de largo alcance que trabajan conjuntamente con un tag o booster ubicado en el interior de cada vehículo.

Esta lectora vehicular trabaja conjuntamente con una etiqueta o tag de identificación, donde se encuentra registrada la información tanto del conductor como del vehículo la cual es verificada por la lectora para así accionar o no las barreras que permiten el acceso.

El lector o antena es un dispositivo emisor de RF (Radio frecuencia), donde una señal no modulada es transmitida por la antena en dirección al tag.

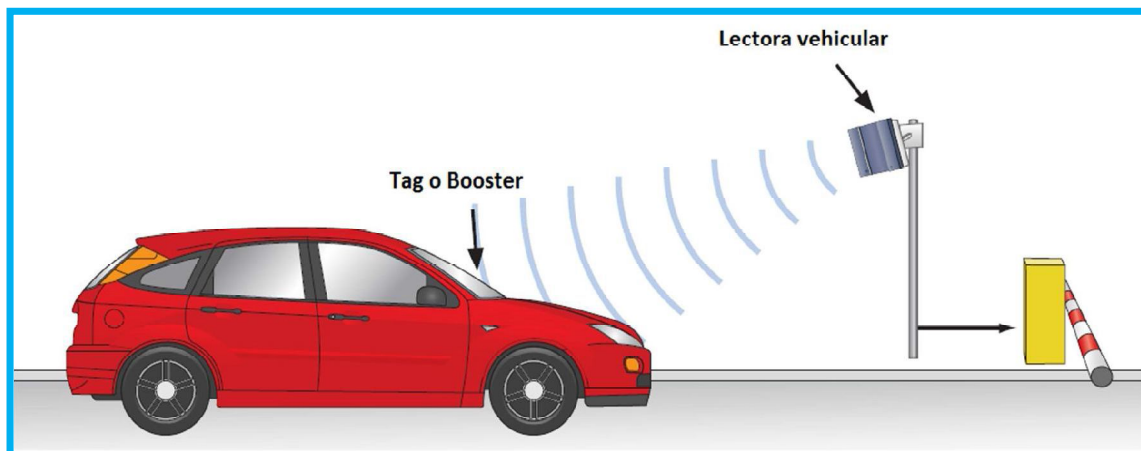


Figura 1.32 Sistema automático de control de acceso vehicular

El tag que se instala en el vehículo modula la señal y la refleja nuevamente al emisor. Luego se decodifica la información contenida en dicho tag, enviándola por un puerto serie a un controlador para su respectiva evaluación.

El lector es un módulo basado en microprocesador, el cual al recibir la señal proveniente de RF la decodifica añadiéndole datos como la hora y el día en que se efectuó la lectura del tag. Una vez realizada dicha operación la unidad lógica del lector almacena la información elaborada en un buffer⁸ interno y la transmite a través de su puerto serie o wiegand, para poder ser procesada por el sistema.

El sistema lector integrado brinda también la posibilidad de manejar contactos de entradas y salidas. Las entradas se utilizan básicamente para recibir la señal de detección de sensores de masa metálica o lazos inductivos, que se activan cuando se detecta la presencia de un vehículo.

- *Booster (Tag o etiqueta vehicular)*

Son etiquetas electrónicas de identificación que estarán ubicadas en los vehículos del personal de refinería que permitirán simultáneamente la identificación de la tarjeta o credencial personal del conductor insertada y la identificación del vehículo integrado, que resulta en un rápido monitoreo de los mismos.

⁸ Dispositivo que acopla impedancias en un circuito.



Figura 1.33 Transmisión de tag vehicular

Es un tag amplificador RFID que envía la identificación de una tarjeta de proximidad al lector vehicular, permitiendo así que la identificación se produzca. Funciona combinando las identificaciones del booster, vinculada al vehículo y de la tarjeta de proximidad, vinculada al conductor.

El conductor inserta su tarjeta personal en el booster, este transmite los códigos de la tarjeta y el booster al lector vehicular y este a su vez envía los códigos al sistema de seguridad, permitiendo el acceso del vehículo y del usuario, una vez estacionado el vehículo retira su tarjeta del Booster para usarla como llave de acceso a las instalaciones: control de accesos o registro de horarios.



Figura 1.34 Tarjeta insertada en booster

El lector emite una señal ondulante continua la cual hace que los tags no tengan que estar sincronizados con el mismo, pudiendo ser leídos desde vehículos que van a distintas velocidades. Cuando el tag recibe la señal de RF no modulada

proveniente de la antena, este la refleja modulada y con el IDC (código de identificación).

1.2.2.2 Entradas de seguridad

- *Barrera Vehicular*

Estarán ubicadas en el área de tránsito en dos vías, tanto al ingreso como salida vehicular de refinería, al validarse la lectura del booster o tag del vehículo se tiene la abertura de la barrera.

Las barreras se utilizan en integración con el control de acceso vehicular, es decir lectoras vehiculares, para un correcto manejo del flujo vehicular. Su principal función se basa en permitir o impedir el paso a los vehículos, realizando la tarea de forma automática, eficiente, rápida y segura.

Es una barrera electromecánica adecuada para delimitar, estacionamientos y accesos de uso exclusivamente vehicular. Los finales de carrera electromecánicos regulables garantizan la posición correcta de parada de la barrera. El desbloqueo de emergencia para la maniobra manual se acciona desde una cerradura con llave personalizada.

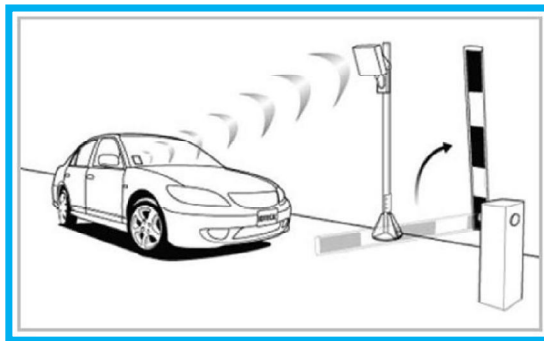


Figura 1.35 Funcionamiento de barrera vehicular

- *Torniquete*

Se contará con torniquetes de simple y doble acceso bidireccionales, en el área de acceso peatonal, tienen como objetivo el comprobar que solo pase una persona a la vez.

Los torniquetes, conocidos también como de altura completa, están diseñados para zonas de alta seguridad donde el énfasis es en un acceso seguro, controlado

y sin supervisión. Su construcción robusta asegura una operación fiable y durable, ofreciendo un excelente control de seguridad para aplicaciones interiores o exteriores.



Figura 1.36 Torniquete

- *Molinete*

En el acceso peatonal de personal y contratistas de refinería en el área de tránsito vehicular, para los ocupantes que acompañan al conductor del vehículo se dispondrá de un molinete.

Se denomina molinete a una especie de barrera física que tras verificar su autorización mediante el circuito electrónico incorporado niega o permite el paso de solo una persona cada vez, para acceder a un lugar determinado. El equipo tiene una conexión con un computador que posee el software del sistema de accesos para la comprobación de la identidad de la persona.

Interactúa fácilmente con un lector de tarjetas u otros dispositivos de control. Puede ser eléctrico, de un único sentido con la salida libre o bloqueada, o de dos sentidos con control eléctrico independiente para la entrada y la salida. Puede suministrarse con bloqueo en caso de fallos, con no bloqueo en caso de fallos o con cualquier combinación.

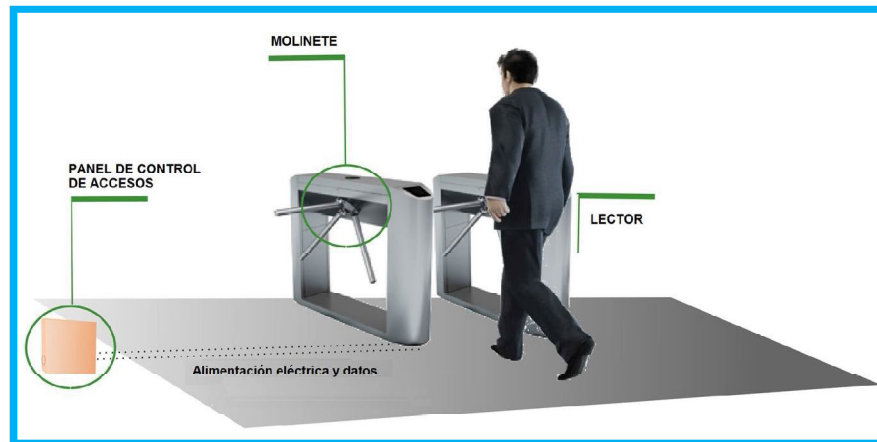


Figura 1.37 Funcionamiento de molinete

- *Puerta Motorizada para personas con capacidades especiales*

Sirve para el acceso de personas con capacidades especiales en el ingreso peatonal, se contará con una puerta motorizada que facilita el acceso para dichas personas.

Está diseñada para brindar acceso a personas con discapacidades físicas a instalaciones que usan torniquetes de altura completa y control de acceso, ya que no pueden utilizar el torniquete tradicional.

Cuenta con panel de puerta interior con un marco fabricado con tubos cuadrados con partes redondeadas horizontales. Debido a la proximidad general de los torniquetes de altura completa, los materiales de construcción usualmente están acordes con los torniquetes.

Fabricados con acero galvanizado, pintado en polvo, aluminio anodizado⁹ con brazos de acero inoxidable o completamente fabricado en acero inoxidable. Cumple con los requerimientos mínimos de la norma ADA¹⁰.

La puerta gira 90 grados con el panel de la puerta adosado al cuerpo a través de una bisagra continua de acero inoxidable. Para aplicaciones industriales, la altura y el ancho final pueden ser hechos a medida.

⁹El aluminio anodizado es aquel que, luego de cierto tratamiento electrolítico, es recubierto con una capa que le brinda una mayor protección ante las amenazas del medio ambiente.

¹⁰ Prohíbe la discriminación por razón de discapacidad en el empleo, los servicios públicos, el transporte, los edificios públicos, las instalaciones empresariales y las telecomunicaciones.

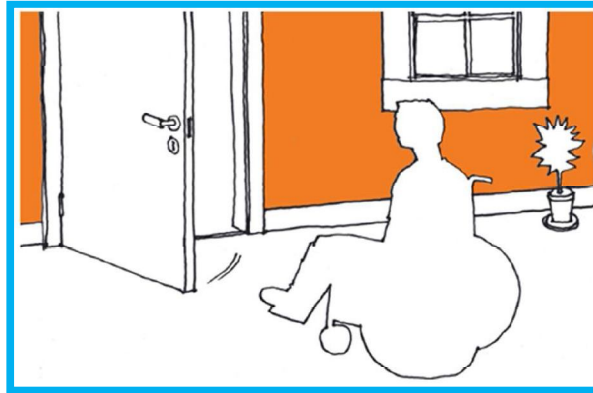


Figura 1.38 Ingreso por puerta motorizada

1.2.2.3 Dispositivos para seguridad en puertas

- *Cerradura Electromagnética*

Se tendrá una cerradura instalada en la puerta cortafuego, para controlar su abertura. La cerradura es un conjunto que dispone de un mecanismo de activación manual, una llave, un pulsador o a distancia, en este proyecto se usará un control por medio de lectoras. Una cerradura electromagnética consta de dos piezas fundamentales:

- Un potente electroimán que se fija en el marco de la puerta.
- Una placa metálica montada sobre la hoja de la puerta objeto de control.

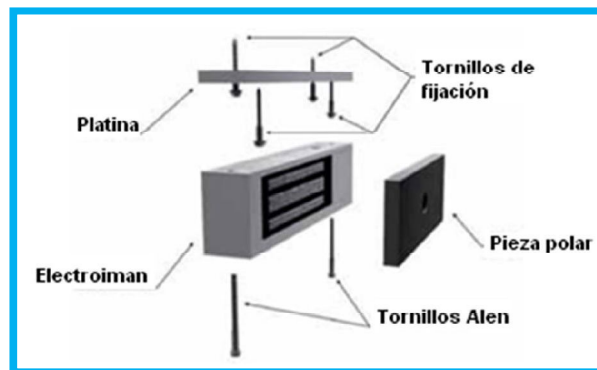


Figura 1.39 Despiece de cerradura electromagnética

El electroimán es el elemento que crea un campo magnético al proporcionarle corriente eléctrica y consta de un núcleo o barra de hierro al que se enrolla un cable barnizado de cobre, creando una bobina.

Este efecto se ha aplicado a la seguridad para crear dispositivos electromagnéticos idóneos para controlar el estado y funcionamiento de puertas.

En estado normal permanecerán bloqueadas y únicamente se desbloquearán cuando una solicitud de acceso sea válida, por comando remoto desde el cuarto de monitoreo o por conato de incendio.

- *Brazo Cierrapuertas*

Este brazo controlará el cierre de la puerta cortafuego de la Sala de control, es regulable, es decir de velocidad variable, el cual garantiza que la puerta se cerrará luego de haber sido abierta por una validación de acceso permitiendo de esta manera que la seguridad se restablezca en la puerta luego de haber sido abierta.

Utiliza un simple mecanismo hidráulico para cerrar y asegurar automáticamente la puerta después de cada uso.



Figura 1.40 Partes de un brazo cierrapuertas

- *Contacto Magnético*

Este dispositivo permitirá conocer el estado de la puerta de la Sala de control con el fin de que el software de gestión y administración pueda considerar el disparo de alarmas. El contacto magnético permitirá a los operadores conocer el estado de la puerta, si está abierta, si está cerrada, si se abrió por un acceso válido, si luego de haberse abierto por un acceso válido permaneció abierta más tiempo del configurado, si el funcionario validó su acceso pero no ingresó al área requerida o

si la puerta fue abierta violentamente. Es un interruptor momentáneo, tal como un pulsador y se presenta con contacto normalmente abierto (NA), normalmente cerrado (NC) o inversor (NA y NC).

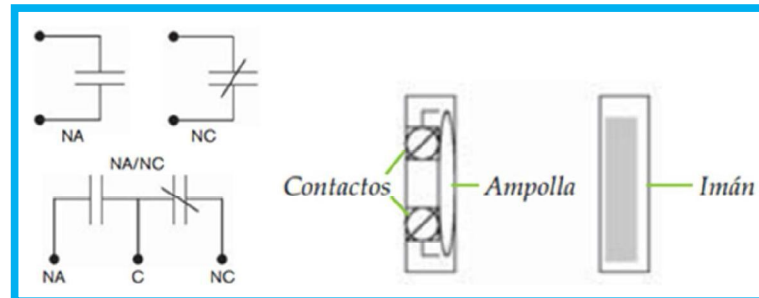


Figura 1. 41 Funcionamiento de contacto magnético

Su funcionamiento es sencillo: los contactos de la ampolla están imantados, y en presencia del campo magnético del imán cambian de posición abriendo o cerrando un circuito. No es necesario que ambas piezas se toquen; bastará que la ampolla esté dentro del campo magnético del imán.

1.2.2.4 Dispositivos de carnetización

- *Capturador de firmas*

Para enrolamiento de personal se utilizará el capturador de firmas, esta firma constará en la tarjeta de proximidad del personal de refinería.

Los dispositivos de captura de firma registran firmas que son capturadas a medida que se van trazando. Es un dispositivo de captura de firmas portátil y ergonómico dedicado a producir firmas digitales legalmente vinculantes. Con los dispositivos de captura de firma electrónica podrá capturar firmas totalmente válidas en formato digital.

Mientras se escribe en la pantalla, el sensor captura la información biométrica de la firma, como la velocidad y la presión de los trazos.

El procesador que lleva integrado es capaz de detectar y reproducir puntos según niveles de presión diferentes. El perfil exclusivo de presión, ritmo y velocidad de escritura permite capturar el perfil individual de la firma. Las firmas capturadas por este dispositivo pueden considerarse como únicas para la persona firmante.



Figura 1. 42 Firma electrónica

- *Tarjetas de Proximidad*

Todo el personal de refinería portará una de estas tarjetas, mientras que a contratistas y visitantes durante su estancia se les proveerá también de una de estas tarjetas.

Una tarjeta de proximidad es una pieza del tamaño de una licencia de conducir o una tarjeta de crédito. La tarjeta contiene información necesaria para activar y abrir puertas a fin de permitir el acceso de quien la porta. Las tarjetas de proximidad se diferencian de las tarjetas comunes que suelen tener una banda magnética en el dorso en el hecho de que no es necesario hacerlas entrar en contacto con el sensor para obtener el acceso, sólo basta con acercarlas al lector de proximidad para que el sistema se active.

La tarjeta lleva impregnado un código binario con una secuencia específica que convierte a la tarjeta en una unidad irreplicable. El lector de tarjetas reconoce el formato del código y luego lo transfiere al panel de control, donde se lo analiza para verificar si el dueño de la tarjeta tiene autorización para entrar en esa área.

Se puede decir que la secuencia de la lectura de la información del chip de una tarjeta de proximidad es la siguiente:

- La lectora genera un campo electromagnético que le entrega energía.

- La tarjeta es colocada a la distancia adecuada para que reciba, por lo menos, la cantidad mínima necesaria de carga.
- Una vez alcanzado este umbral de energía comienza a transmitir la información que tiene programada en su chip.
- El lector decodifica el mensaje recibido de la tarjeta y de acuerdo a su configuración transmite el código recibido de la tarjeta al panel de control de accesos.

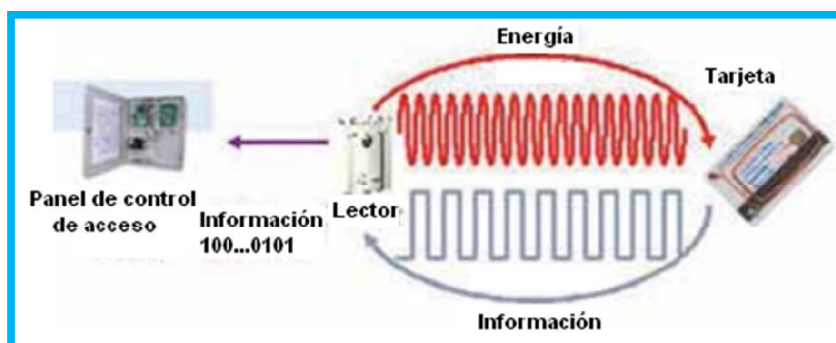


Figura 1.43 Funcionamiento de lectora y tarjeta

1.2.2.5 Tarjetas controladoras

Son las tarjetas que estarán colocadas dentro de los paneles de control de acceso, serán las encargadas de poner en funcionamiento todos los elementos del sistema, mediante el software de control OnGuard.

1.2.2.5.1 LNL-2220 (Controlador inteligente de lectora dual)

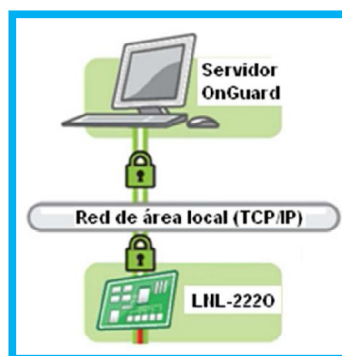


Figura 1.44 Esquema de conexión del controlador LNL-2220

Es la controladora principal que se comunicará con el cuarto de control o monitoreo, en esta se conectarán las demás tarjetas que controlan el resto de

elementos del sistema de accesos, también es la que recibirá directamente los patrones de software de la plataforma “OnGuard”.

Utilizando comunicación Ethernet y un procesador de 32 bits la LNL-2220 permite una conexión Ethernet directamente desde una localidad de accesos a un servidor de OnGuard a través de su puerto o hasta 115.2 kbps. El controlador LNL-2220 tiene la capacidad de almacenar hasta 250000 tarjeta habientes en una memoria flash no volátil y soportar descargas selectivas para bases de datos de tarjeta habientes mayores. Un puerto de dos cables RS-485 puede ser usado para conectar hasta 32 dispositivos (64 puertas máximo).

La interfaz de lectora dual incluye ocho entradas soportando circuitos normalmente abiertos, normalmente cerrados, supervisados y no supervisados. Adicionalmente seis relés de salidas.

1.2.2.5.2 LNL-1320 (Módulo de interfaz de lectora dual)

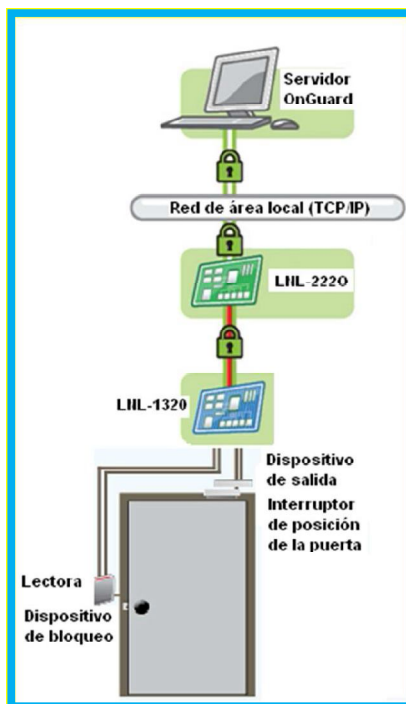


Figura 1.45 Esquema de conexión del módulo LNL-1320

Es un Módulo de interfaz de lectora dual que proporcionará un vínculo entre la controladora principal del sistema LNL-2220 y equipos que den una señal de entrada como lectoras, contactos magnéticos o cerraduras magnéticas. La

mayoría de lectoras de control de acceso que utilizan comunicaciones Wiegand Data1/Data0 o Clock/Data son soportadas por esta interfaz.

Hasta 32 módulos de interfaz de lectora duales pueden ser conectados en un enlace multipunto con RS-485 de dos o cuatro cables hasta 1.219 metros de distancia del controlador LNL-2220 por puerto. Cada módulo de interfaz de lectora dual tiene una dirección individual para ser controlada desde el software de control de accesos OnGuard. La interfaz de lectora dual incluye ocho entradas soportando circuitos normalmente abiertos, normalmente cerrados, supervisados y no supervisados, con los que se podrá controlar salidas como cerraduras, torniquetes, molinetes, indicador de acceso, barrera vehicular. Adicionalmente seis relés de salidas.

1.2.2.5.3 LNL-500B (Interfaz puerta de enlace de lector biométrico)

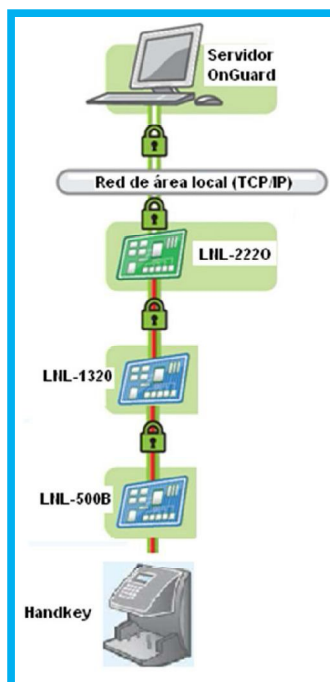


Figura 1.46 Esquema de conexión de la puerta de enlace LNL-500B

El portal de interfaz de lector biométrico es un enlace vital y versátil entre los controladores de lectores biométricos. Utilizando OnGuard, el portal de interfaz será configurado exclusivamente para dar soporte a lectores de geometría de mano.

La interfaz de lector comunica la configuración multipunto al controlador a 38,4 kbps vía RS-485. El portal de interfaz tiene dos puertos de dos cables RS-485, cada uno da soporte a hasta cuatro lectores de dirección única. Cada puerto da soporte a lectores localizados hasta 1,219 m de distancia del portal de interfaz del lector.

1.2.2.5.4 LNL-1100 (Módulo de control de entradas)

El módulo de control de entradas LNL-1100 provee al sistema de control de accesos una capacidad de reconocimiento de alta velocidad de alarmas críticas en las zonas monitoreadas. Esta tarjeta controladora se usa para integrar el sistema de cableado perimetral con el software de monitoreo OnGuard. Se comunica directamente con el controlador vía RS-485 con comunicación de 2 ó 4 cables. El controlador LNL-1100 tiene 16 contactos de entrada configurables y dos controladores de relé de salida. Soporta circuitos normalmente abiertos, normalmente cerrados, supervisados y no supervisados.

Los circuitos de entrada se escanean por medio de un convertidor análogo a digital. El software monitorea y controla la señal digitalizada del estado de entrada para que cada punto de entrada sea programado como punto de alarma supervisado o no supervisado.

1.2.2.6 Software OnGuard

Es el software de administración e integración del sistema de control de accesos, sistema de CCTV y sistema de seguridad perimetral. La plataforma OnGuard proporcionará una centralización integrada, monitoreo y administración de una amplia variedad de aplicaciones, bases de datos y dispositivos unidos a través de una sola interfaz de usuario y optimiza las redes corporativas existentes.

El portafolio de aplicaciones de OnGuard, incluye control de acceso, emisión y administración de credenciales ID, monitoreo de alarmas, administración de video digital, análisis de contenido de video digital, biometría, detección de intrusión, administración de visitantes, tarjetas inteligentes y la capacidad de integrarse con multitud de sistemas de terceros. OnGuard es el encargado de:

- Administra los sistemas de Control de Accesos, Intrusión y CCTV IP.

- Servidor de Licencias.
- Monitorización de Alarmas.
- Diseño de Mapas.
- Interfaz con CCTV.
- Dependiendo de las licencias puede soportar desde 32 Lectoras de Tarjetas a cantidad ilimitada.
- Licencias adicionales para Intrusión de terceros, Video inteligente, Análisis de video, etc.

Todas las aplicaciones OnGuard se podrán configurar y administrar desde una sola estación de trabajo, es decir el computador cliente, y la actividad de eventos puede monitorearse desde una sola estación de trabajo de monitoreo de alarmas, que se encontrará en el cuarto de control o monitoreo de refinería.

1.3 SUBSISTEMA DE SEGURIDAD PERIMETRAL POR CABLE SENSOR DE VIBRACIÓN

Es un sistema de detección electrónica diseñado para proteger perímetros internos y externos. Los sensores de vibración detectan las señales provenientes del perímetro causadas por tentativas de intrusión, generadas por intentos de corte, escalamiento, golpes o pisadas. Reconocidos por su confiabilidad y adaptabilidad en las condiciones topográficas y climáticas más exigentes. Atienden un gran número de casos en que otros sistemas no ofrecen soluciones: lluvia, vegetación, neblina, viento, terrenos accidentados.

Todas estas acciones que generan vibraciones mecánicas o tensión en la malla de la cerca son diferentes de las vibraciones asociadas con la actividad ambiental normal o natural que ocurre a menudo, y típicamente tienen frecuencias más altas y amplitudes más grandes. Los sensores de vibración descubren estas vibraciones usando transductores electromecánicos o piezoeléctricos. Las señales de los transductores son enviadas al procesador de señal para ser analizados.

La instalación apropiada y el espaciado de sensores son críticos para una correcta detección. Las cercas con la malla suelta o floja pueden crear falsas

alarmas. Igualmente, las condiciones meteorológicas adversas pueden causar desajustes de sensibilidad. Las esquinas de la cerca plantean desafíos particulares para descubrir fácilmente vibraciones de intrusión, debido a los refuerzos de los postes de la cerca.

Los Arbustos y las ramas de los árboles así como animales y tiempo severo que entran en contacto con la cerca pueden hacer que la cerca vibre, provocando que los sensores reaccionen. En áreas con viento fuerte o numerosas interacciones de animales con la cerca, los sensores de vibración no deberían ser usados. Los sensores de vibración sólo deberían ser usados en áreas donde las vibraciones ambientales naturales o artificiales son mínimas o inexistentes. Los sensores de vibración no son satisfactorios y tampoco son confiables en áreas, como en la proximidad a obras de construcción, vías de ferrocarril o actividad de carretera y vehicular.

1.3.1 CONCEPTOS BÁSICOS DE SEGURIDAD PERIMETRAL

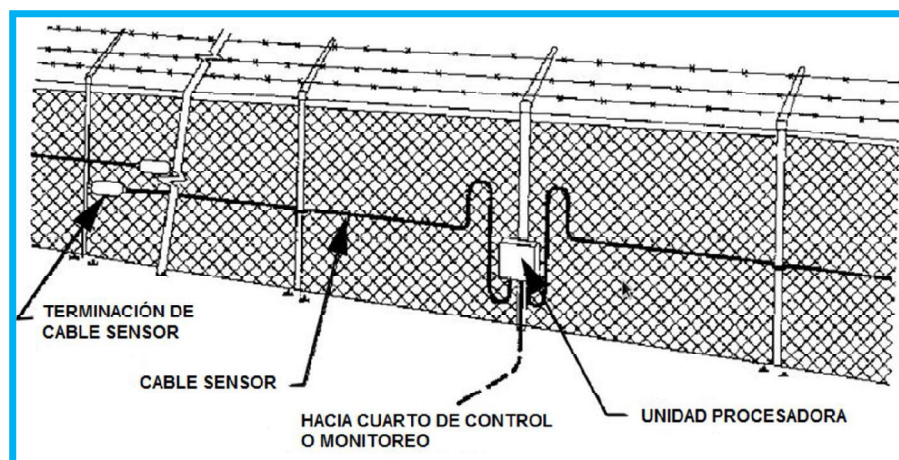


Figura 1.47 Seguridad perimetral

1.3.1.1 Etapas del sistema de seguridad perimetral

- El sensor de intrusión detecta las señales generadas por el cruce de un intruso por la zona del perímetro protegido.
- Las señales son analizadas por el procesador asociado, para identificar si se trata de una alerta legítima o una falsa alerta de intrusión.

- Una vez que se determine que las señales corresponden a una intrusión en curso, una alarma se genera y el cuarto de control o monitoreo es alertado mediante visualización en el software de monitoreo.
- Después que el cuarto de control o monitoreo es alertado, se tomarán las medidas correspondientes.

1.3.1.2 Tipos y configuraciones del sensor

Hay dos tipos básicos de sensores de vibración de mallas, los sensores electromecánicos cuyo procesador de señal tiene un recorrido de acumulación de pulso que reconoce aperturas de contacto momentáneas de interruptores electromecánicos; y sensor piezoeléctrico, cuyo procesador de señal responde a la amplitud, duración, y frecuencia de la señal transmitida.

1.3.1.2.1 Sensores electromecánicos

Los sensores electromecánicos usan interruptores mecánicos de inercia o interruptores de mercurio para descubrir la vibración de la malla. Los interruptores de inercia mecánica consisten en una masa sensible a la vibración, la que descansa en dos o tres contactos eléctricos creando así un circuito cerrado.

La masa es movable y reacciona a mínimos cambios de las vibraciones (frecuencias) generadas en la malla durante una tentativa de intrusión. La vibración perturba la masa y es movida o separada de uno o varios de los puntos de contacto momentáneamente ocasionando la apertura del circuito y creando una alarma. En algunos sensores la masa es intencionadamente restringida por algunas guías internas para asegurar que sólo una vibración significativa causará el movimiento, rompa el recorrido y activará la alarma.

Los interruptores de mercurio constan de un frasco de cristal que contiene una pequeña cantidad de mercurio con contactos eléctricos normalmente abiertos localizados cerca, en contacto o sumergido en el mercurio. Un impacto o la perturbación de la malla hacen que el mercurio sea desplazado de su posición de descanso normal, haciendo contacto momentáneo con uno de los contactos eléctricos y creando una alarma.

1.3.1.2 Sensores piezoeléctricos

Los sensores piezoeléctricos convierten las fuerzas de impacto mecánicas generadas durante una tentativa de intrusión en señales eléctricas. A diferencia de la señal abierta o cerrada generada por sensores electromecánicos, los sensores piezoeléctricos generan una señal análoga que varía proporcionalmente en amplitud y frecuencia a la actividad de vibración en la malla.

Estas señales son enviadas al procesador de señal para su evaluación, donde primero pasan por un filtro para autentificar la alerta de intrusión. El procesador de señal entonces interpreta las señales para determinar si hay actividad suficiente para que haya ocurrido lo necesario para la autorización de una alarma.

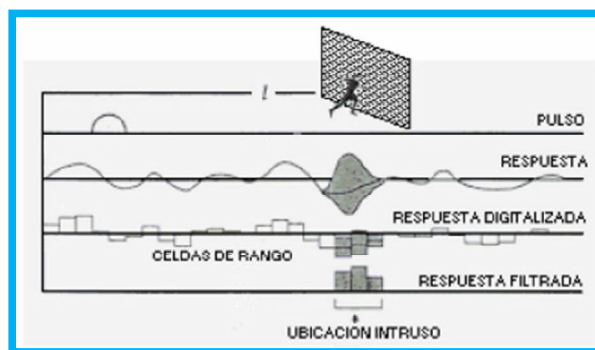


Figura 1.48 Funcionamiento del sensor de vibración

1.3.1.3 Monitoreo local de alarma

Hay una variedad de sistemas de monitoreo de alarmas disponibles, aunque cada sistema sea único en el número y variedad de opciones disponibles, todos los sistemas realizan la función básica de anunciar alarmas y mostrar el área donde se han producido las mismas. La pantalla de monitoreo de la mayor parte de estos sistemas está configurado sobre la utilización de computadoras Windows XP, como sistema operativo. Muchos de estos sistemas funcionan con el software patentado, y desarrollado por el fabricante del sistema de seguridad.

1.3.1.4 Consideraciones ambientales

La mayor parte de zonas de seguridad tienen un conjunto de factores ambientales los que deberán ser tenidos en cuenta al diseñar el sistema, seleccionando los

sensores, y llevando a cabo la instalación. Un error al considerar todos los factores puede ser causa de excesivas falsas alarmas en el sistema.

Cada zona de intrusión, ya sea una malla de perímetro, una entrada exterior, una ventana, un interior, la puerta o un cuarto asegurado, tendrá factores ambientales especiales a ser considerados. Las zonas externas probablemente serán afectadas por el clima predominante, debido a condiciones meteorológicas, o por acción de animales así como factores artificiales como, campos eléctricos o radio transmisiones, vehículos, camiones, ferrocarril o movimiento aéreo.

Hay una amplia variedad de otras consideraciones que deben ser tomadas en cuenta al colocar sensores para supervisar el perímetro de un área. La malla debería estar colocada cuidadosamente, bien construida y firmemente anclada, ya que las mallas pueden moverse con el viento y causar falsas alarmas.

1.3.2 ELEMENTOS QUE CONFORMA EL SISTEMA

El sistema de seguridad perimetral se basará en el sistema INTRUDALERT, este es un sistema electrónico de gran alcance diseñado para la protección total del perímetro de instalaciones críticas. Este sistema se basa en el diseño de un sistema integral de seguridad, capaz de detectar el intento de violación del sector asegurado, ya sea cortando, golpeando o forzando las puertas o mallas aseguradas.

INTRUDALERT proporcionará alerta temprana de los intentos de intrusión, puede ser fácilmente integrado con sistemas de circuito cerrado de televisión que se instalan en puntos clave para proporcionar capacidad de evaluación en tiempo real.

Se denomina VIDALERT al software de control del sistema, el cual se encargará del monitoreo de alarmas, las cuales se mostrarán en un mapa del lugar en el computador cliente.

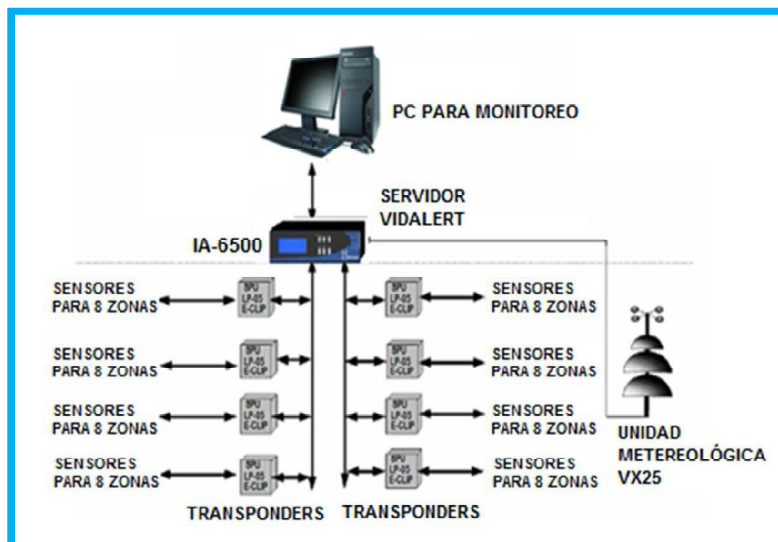


Figura 1.49 Esquema general del sistema INTRUDALERT

1.3.2.1 Sensor de vibración MDS-2

Este sensor de vibración multidireccionales pre-instalado en el cable a lo largo de toda su longitud en intervalos estándar de 3 m, estos se designarán uno en la mitad de cada porción de malla; estos sensores de vibración contienen internamente 10 puntos de contacto electro platinados en oro con capacidad de auto ajuste y auto limpieza, estos puntos de contacto vibran ante el movimiento del cable sensor colgado sobre la malla, y producen las alarmas que se analizarán en la tarjeta SPU-2004.

1.3.2.2 Cable multisensor de choque con sensores de vibración RB-SL3

Es el cable sensor de seguridad que se instalará en el perímetro de refinería sobre la malla, posee sensores MDS – 2 que ya vienen preinstalados e incorporados en el mismo cable y distribuidos a una distancia estándar de 3 m.

El cable contiene 6 alambres aislados en PVC¹¹ dentro de un relleno para conformar una construcción concéntrica y protegida en un 100% con una película fina de poliéster-papel de aluminio. La funda externa es resistente a rayos

¹¹Plástico impermeable y flexible, adecuado para encerrar cables eléctricos.

Ultravioleta (UV), interferencias de Radio Frecuencia (RFI) y a interferencia electromagnética (EMI), diseñado para uso en exteriores.

El cable sensor se conectará a las unidades controladoras analizadoras de campo SPU-2004 para transmitir señales de alarma al Data center donde se encontrará el servidor IA-6500, que serán recibidas por la unidad de interface de control (IA-6500) y reconocidas por el software de monitoreo VIDALERT quien mostrará la gráfica del perímetro cubierto con las alarmas activas.



Figura 1.50 Cable sensor de vibración SL3

1.3.2.3 Cable de comunicación y alimentación RB-4C

Es el cable conductor de datos y suministro de energía para instalación en exteriores sobre la malla. Tiene internamente 4 alambres de cobre encauchetados en PVC. Utiliza dos alambres internos para transmisión de datos y los otros dos para suministrar la energía. Tiene doble funda exterior, resistente a rayos Ultravioleta (UV), resistente a interferencias de Radio Frecuencia (RFI) y resistente a interferencia electromagnética (EMI), diseñado para uso en exteriores.

El cable está diseñado para transmitir señales digitales que serán recibidas de las unidades controladoras analizadoras de campo SPU-2004 (que reciben las alarmas del cable multi - sensor de choque con sensores de vibración), hacia la unidad interfaz de control (IA-6500) mediante el protocolo RS – 485, pero debido a que la distancia desde la SPU más lejana hasta el Data Center supera los 1200 metros de distancia permitidos por este protocolo, se ha requerido el uso de módulos extensores de RS – 485, los cuales nos permiten aumentar el rango de alcance de la comunicación. Además en este proyecto se usa un cable independiente para la alimentación de las SPU.

1.3.2.4 Unidades de procesamiento inteligente de campo SPU-2004

Estas unidades son el conjunto de tarjetas electrónicas y de protecciones eléctricas diseñadas para el procesamiento de señales eléctricas y para la emisión de alarmas hacia el sistema de interfaz de control.

La tarjeta llamada Transponder Card es la tarjeta principal que contiene el micro – controlador principal para el análisis de señales, la tarjeta llamada Lightning Protection Card (LP-05¹²) es una tarjeta de interfaz entre la tarjeta transponder y las unidades de campo y posee en su configuración protecciones eléctricas, así como los módulos (E-CLIP¹³ 6 y E-CLIP 10), que también son protecciones eléctricas de la tarjeta principal, los cuales vienen en pares y están provistos de 6 y 10 entradas respectivamente, el de 6 entradas protege exclusivamente un grupo de 4 zonas, mientras que el de 10 entradas protege las restantes 4 zonas.

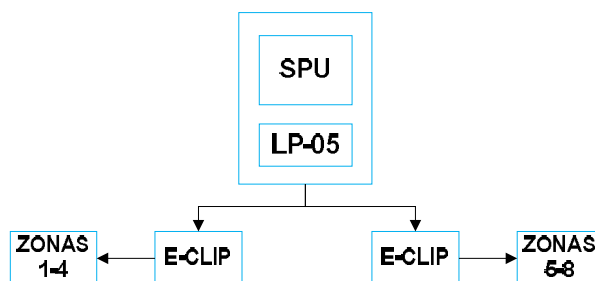


Figura 1.51 Esquema general de conexión de zonas

Su función es recibir las señales de alarma de los sensores (MDS-02) que están instalados en el cable sensor sobre la malla y en base a la intensidad de la vibración que estos perciben el microprocesador de la tarjeta transponder decide si la alarma es verdadera o falsa, y si los cambios requieren la activación de la alarma; también recibe las señales de las unidades meteorológicas por medio del cable de datos y energía RB-4C que está instalado a la par del cable sensor y procesa estas señales para posteriormente enviarlas al Data center por medio del protocolo RS-485. Estas unidades se comunican entre sí por medio del cable RB - 4C.

¹²Tarjeta de protección contra descargas eléctricas para 8 zonas

¹³Unidad supresora de descargas eléctricas

Cada transponder cubre y procesa las señales de hasta 8 zonas de alarma. Cada zona de alarma está normalmente asignada a intervalos de 100 metros, de modo que sólo se requiere un transponder por cada 800 metros de segmento de perímetro.

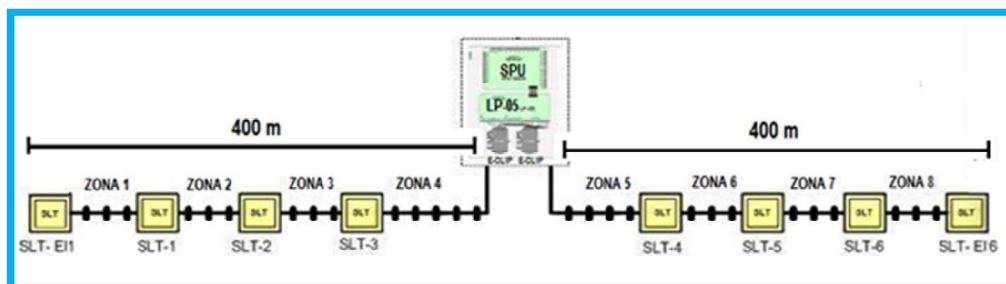


Figura 1.52 Perímetro que cubre un transponder

El microprocesador en la tarjeta de transponder puede ser re-programada durante el funcionamiento del sistema, es decir, la reprogramación se puede requerir como consecuencia de los cambios que se produjeron en estos parámetros durante el mal tiempo debido a condiciones ambientales, etc.

Debido a que el perímetro de refinería es muy largo, se producen diversas condiciones de viento en diferentes puntos de todo el perímetro, por lo que se usarán unidades de compensación meteorológica (VX-25), equipadas con una adaptación de entrada electrónica especial para la tarjeta de SPU-2004.

1.3.2.5 Terminación de zona RB-SLT

Es una tarjeta estándar de 6 x 6 cm que contiene 2 regletas de 8 terminales, 6 puentes de tipo pin y una resistencia para permitir al sensor lineal una simple y rápida instalación, mantenimiento y solución de problemas.

El SLT estará instalado dentro de una caja para intemperie y sellada contra la humedad, mientras que todos los contactos internos se deben proteger contra la corrosión al sellar la caja.

Su uso es fundamental ya que internamente está provista de varias borneras para la interconexión y delimitación física de las denominadas zonas de cobertura de cada SPU-2004, es decir mediante esta unidad se logrará la conexión entre zonas.

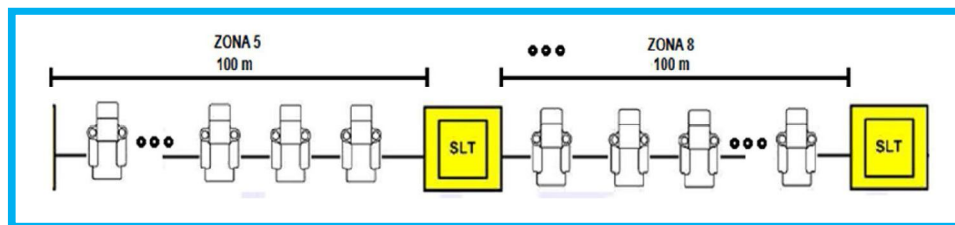


Figura 1.53 Ubicación de fines de zona (SLT)

1.3.2.6 Unidad Meteorológica RB-VX25

La unidad de compensación meteorológica VX-25 está compuesta por un anemómetro¹⁴ de tres cucharas para la medición de la velocidad del viento circundante en la zona y un conjunto de tres discos sensores de impacto para la detección de lluvia o granizo.

En el sistema de alarma perimetral el movimiento de la malla puede ser resultado de fuertes vientos, lluvia y granizo lo que provocaría el movimiento del sensor y la activación no deseada de las falsas alarmas. La velocidad del viento se convierte en vibraciones. Fuerzas de lluvia y el granizo se convierten en impulsos digitales. Esta información es recogida por la SPU y llegará hacia el Data center, ahí se realiza un análisis para determinar si es necesario la calibración de la unidad meteorológica para evitar falsas alarmas.

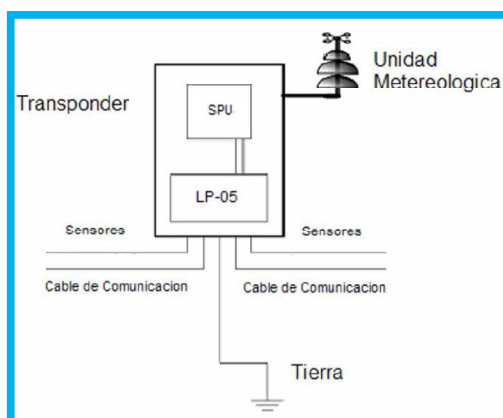


Figura 1.54 Unidad meteorológica RB-VX25

¹⁴Es un aparato meteorológico que se usa para la predicción del clima y, específicamente, para medir la velocidad del viento.

1.3.2.7 Unidad Interfaz de control (IA-6500)

Este equipo se encargará de recibir las señales provenientes de las SPU en campo y las retransmitirá al computador principal que también actuará como computador cliente del sistema, puede ser usado como un respaldo en caso de presentarse alguna falla en la computadora principal, ya que muestra las alarmas en una pantalla LCD que posee. En su interior posee la tarjeta de control central, una tarjeta de control de respaldo, una tarjeta de protección contra rayos LP - 05, sirve de suministro de potencia para las SPU. Además, incluye dos unidades de control interno, un programa de software de respaldo, una batería recargable y una pequeña pantalla LCD para facilitar su configuración.

El seguimiento y control del sistema de INTRUDALERT se llevará a cabo en el cuarto de control por medio del servidor que posee el software de supervisión VIDALERT. La interfaz de control avanzado IA6500 realiza las siguientes funciones:

- Monitorear los sensores perimetrales y "zonas".
- Integrar los sensores de campo con la pantalla gráfica del mapa base en la PC.
- Proporcionar indicación de intrusión a través de mallas o puertas.
- Proporcionar una respuesta automática al activar los dispositivos auxiliares: luces de aviso, sirenas etc.
- Proporcionar interfaz e integración con otros sistemas como de CCTV.
- Control de hasta 16 procesadores de campo SPU.
- Proporcionar información de base de los acontecimientos.
- Administrar la configuración de la zona y los parámetros
- Proporcionar un control completo de respaldo continuo en caso de fallo de alimentación.

1.3.2.8 Software VIDALERT

El Software del sistema llamado VIDALERT se encargará del control y manejo de todo el sistema de detección de intrusión. El software mostrará por medio de un monitor el estado de todo el perímetro protegido, mostrando claramente en un

mapa las zonas del perímetro en diferentes colores, rojo parpadeante si algún sector está en alarma no reconocida o rojo estático si ya se reconoció la alarma y gris si todo está normal, además de una pantalla auxiliar en la cual se muestra por medio de las cámaras existentes, una imagen de la zona.

Además cuenta con una serie de controles, para el manejo de la cámara por medio del mouse, como por ejemplo la posibilidad de aumentar o disminuir la imagen, así como subirla o bajarla y moverla hacia la derecha o a la izquierda.

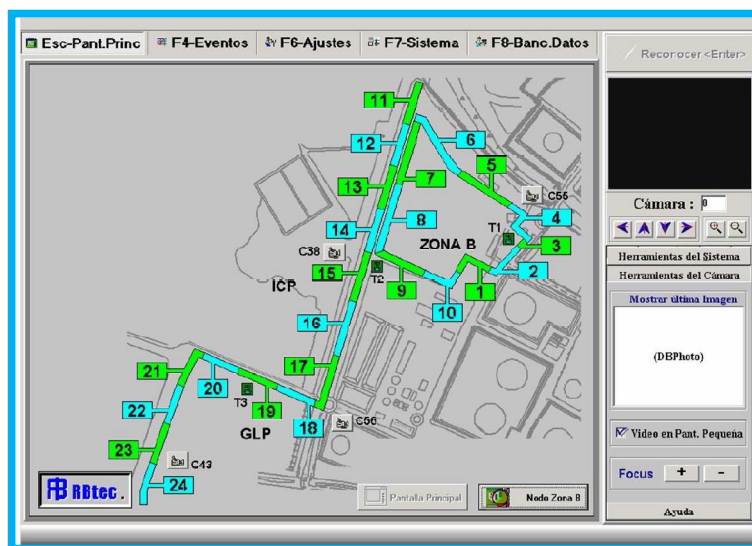


Figura 1.55 Ventana principal de VIDALERT

1.4 SISTEMA DE TRANSMISIÓN DE DATOS

Generalmente, cuando se desea transmitir datos no se tiene ningún problema cuando los portadores de la información están situados relativamente cerca del cuarto de control o monitoreo. Sin embargo, a menudo no es éste el caso, en muchas ocasiones, los portadores de la información tienen que afrontar difíciles obstáculos como, por ejemplo, climas extremos, largas distancias y terrenos montañosos.

Teniendo en cuenta los beneficios de un servicio económico y resistente a las interferencias en lugares de difícil acceso de refinería y debido a la amplia distancia que se tiene hacia el cuarto de control, se revisa el sistema de comunicación CANOPY de Motorola, que no solo ayudará a la transmisión de

datos de las distintas cámaras sino también del subsistema de control de accesos cuando sea necesario, en las áreas alejadas del cuarto de control.

1.4.1 Sistema CANOPY

Canopy es un sistema de red para distribución de datos que ofrece servicios de banda ancha inalámbrica de alto desempeño, el Sistema CANOPY PMP¹⁵ utiliza redes Punto a Punto y Punto a Multipunto que pueden cubrir distancias que van de 3.2 a 16 km (2 a 10 millas) en una configuración multipunto, y hasta 56 km (35 millas) en una configuración punto a punto.

Los bloques de construcción básicos de un Sistema Canopy son:

- El Punto de Acceso (AP) establece fácilmente una interfaz con su Red de Área Local (LAN) existente.
- La Módulo Backhaul (BH) brinda "alimentación" a Internet desde una ubicación remota.
- El Módulo de Suscriptor (SM), receptor de acceso a Internet, a este viene la señal análoga de las cámaras después de haber sido codificadas en el video web server.

Debido a que cada AP tiene un cubrimiento limitado, para lograr el cubrimiento deseado se hace un arreglo de antenas llamado Cluster, por ejemplo, si se quiere tener un cubrimiento de 360° se deben colocar 6 AP.

Es necesario para que esta configuración funcione, añadir un CMM (Cluster Management Module), este equipo se encarga de sincronizar todos los AP del sistema mediante una señal de GPS para así evitar interferencias entre los AP. Este equipo se debe utilizar cuando se utilizan más de 2 AP.

El Punto de Acceso y los Módulos de Suscriptores están diseñados para instalarse al aire libre, por lo que no hay necesidad de tender cables por aire o por tierra, o microondas.

¹⁵Punto-a-Multipunto de Banda Ancha Inalámbrica

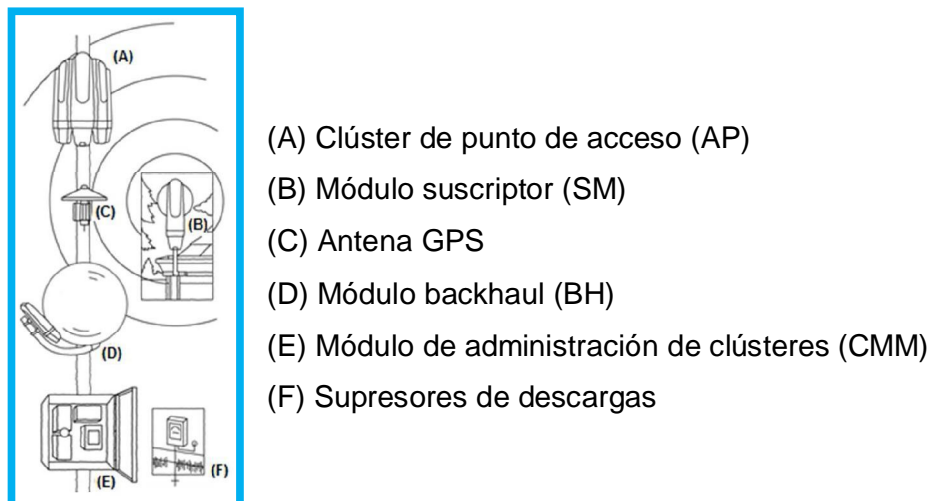


Figura 1.56 Constitución del sistema Canopy

1.4.1.1 Configuración Punto a multipunto (PMP)

El sistema Canopy usualmente es implementado en su configuración PMP. Su rango de operación y rendimiento depende de muchos factores incluyendo: el área, follaje, energía de RF y otras condiciones. Por esta razón, los equipos Canopy que se utilizan en la configuración PMP han sido diseñados para trabajar aún en las más duras condiciones.

La configuración PMP es empleada para conectar múltiples localidades e instalaciones. Se caracteriza por su buen desempeño en zonas altamente pobladas y sobre todo ruidosas.

Los APs y los SMs comprenden la configuración PMP. Cada AP es el centro de la distribución (origen) y cada uno puede servir hasta a 200 SMs.

En este tipo de configuración los SMs deben solicitar permiso para transmitir los datos, de ahí que el AP cumple una función importante que es la de coordinar la recepción y envío de los datos.

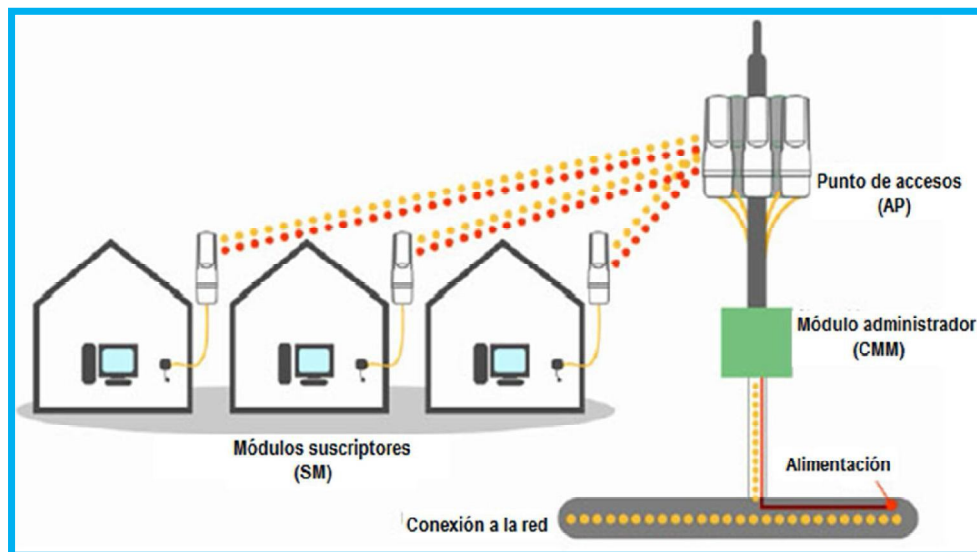


Figura 1.57 Configuración PMP

1.4.1.2 Elementos del sistema de comunicación CANOPY

- *Módulo suscriptor (SM)*

Estos equipos se situarán en los postes donde estarán las cámaras PTZ para de esta forma lograr la comunicación de estas cámaras instaladas en los perímetros de refinería, en el área de acceso vehicular y en la Sala de control, hacia el Data center donde también se contará con un SM, ya que en este lugar se ubicará el grabador NVR y el servidor de CCTV.

El Módulo suscriptor (SM) es la unidad suscriptora terminal. Esta consiste de un simple transceptor¹⁶ que opera con una antena integrada de 60 grados. La sincronización SM y control está dirigida por la señal del Access Point (AP). Una vez que el SM está en funcionamiento, este escanea los canales de RF y automáticamente registra y autentifica al apropiado AP. Cada SM requiere alimentación vía PoE.

¹⁶ Dispositivo que cuenta con un transmisor y un receptor que comparten parte de la circuitería o se encuentran dentro de la misma caja.

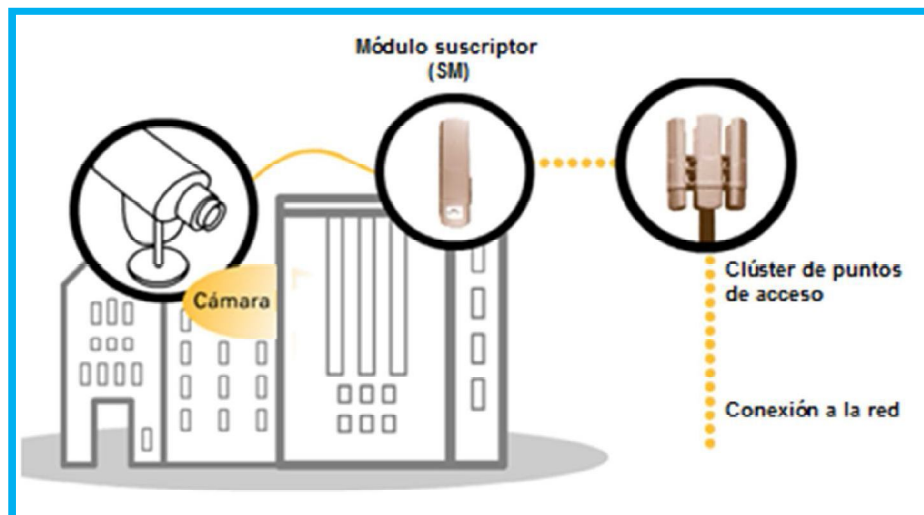


Figura 1.58 Funcionamiento del Módulo suscriptor (SM)

- *Access Point con AES¹⁷ (AP)*

El AP es el módulo encargado de recibir y transmitir datos desde y hacia los SM. Los AP se ubicarán en tres torres de 45m cada una, para de esta manera cubrir el alcance requerido para la comunicación de las cámaras PTZ más cercanas a cada torre. Al llegar los datos hasta el AP, este se encargará de llevar dichos datos hacia el Data Center.

El AP es considerado como la estación base, ya que distribuye servicios de red mediante una antena direccional, logrando una proyección de 60° vertical por 60° horizontal, y sirviendo a una cantidad máxima de 200 usuarios SM por cada AP.

Además actúa como punto de interconexión entre la red Canopy y una red cableada, para ampliar el alcance físico de un servicio al que tiene acceso un usuario inalámbrico. El AP usualmente es empleado en una configuración PMP y puede ser instalado al aire libre.

¹⁷Encriptación Estándar Avanzada, algoritmo de cifrado capaz de proteger información sensible.

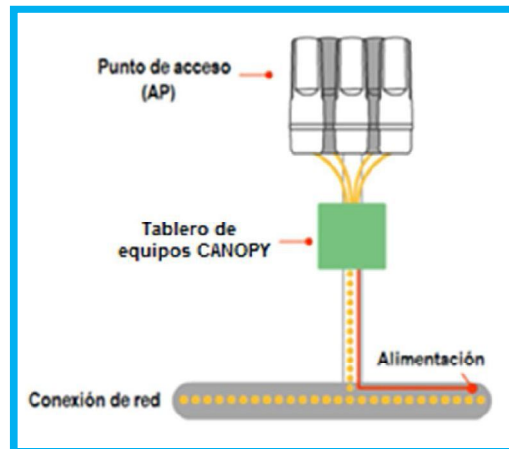


Figura 1.59 Punto de acceso (AP)

- *Módulo Backhaul (BH)*

De la misma manera que el AP, este módulo se instalará en las tres torres de 45m, será el encargado de establecer la conexión de Internet con su Clúster de AP desde una localidad remota, permite un alcance de 32 kilómetros (20 millas) o más a la señal alimentadora del proveedor de servicios de Internet.

Es un equipo capaz de proporcionar conectividad punto a punto mediante la conexión con otro BH. Esta conexión de BHs en parejas maestro esclavo es utilizada para trasportar tráfico desde y hacia el clúster de APs. El BH provee voz, video y datos desde una ubicación remota.

La interface primaria entre el sistema Canopy y la red de internet se realiza mediante el BH del sistema Canopy.

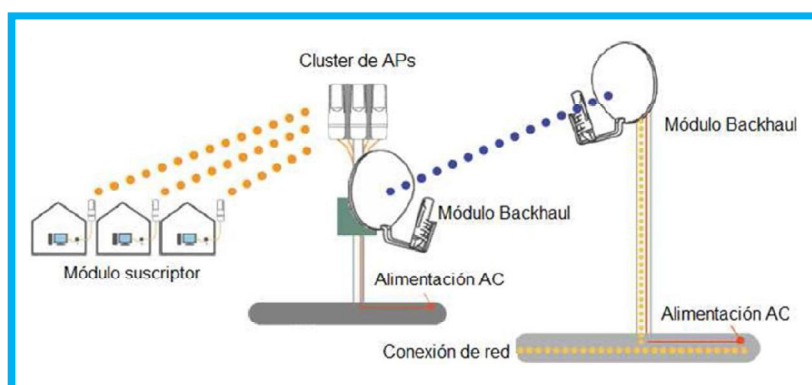


Figura 1.60 Funcionamiento de Módulo Backhaul (BH)

- *Módulo de administración de clúster (CMM)*

Es otro de los equipos situados en las tres torres de 45m, pues para resolver el problema de la interferencia originada por la transmisión no simultánea de los APs se cuenta con el Módulo de administración de Clúster que controla y sincroniza el funcionamiento de cada AP realizando lo que se denomina, duplexación por división d tiempo (TDD). El CMM es requerido cuando se tienen más de 2 APs conectados. El CMM además proporciona alimentación y conexiones de red al clúster.

Se trata de una unidad de control robusta diseñada para la intemperie, que además de suministrar alimentación sobre Ethernet a cada AP e incorporar un switch, sincroniza mediante su antena GPS los ciclos de transmisión de cada elemento de la red (directamente cada AP, y a través de estos cada SM).

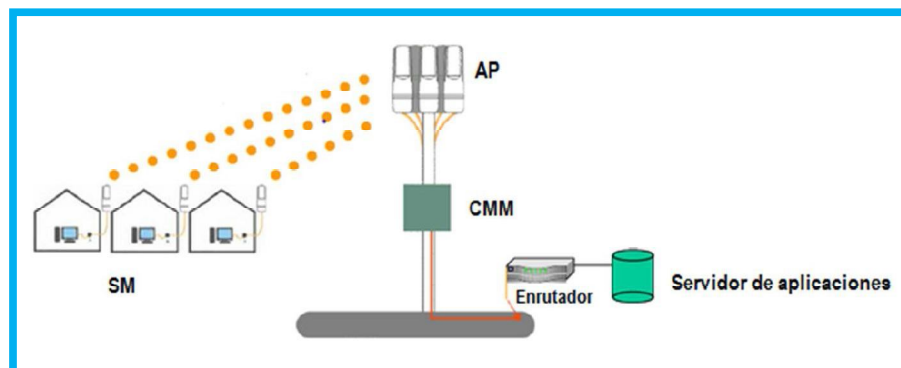


Figura 1.61 Módulo de administración

En este capítulo se ha mostrado las mejores tecnologías que se dispone en el mercado para poder cubrir con la demanda del cliente y las diferentes exigencias que posee el proyecto. Los tres subsistemas propuestos se han diseñado conceptualmente en base a los levantamientos previos realizados en campo, de manera que se ha logrado recopilar información primaria de primera mano para el desarrollo y propuesta de dichos sistemas y equipos.

CAPÍTULO 2

DISEÑO DE LAS REDES DE LOS SUBSISTEMAS QUE INTEGRAN LA SEGURIDAD FÍSICA

En este capítulo se describe el diseño de las redes de cada subsistema aprobado, incluyendo la distribución de equipos en cada área, según sus características técnicas y la función que cumplirán dichos equipos, todo esto tomando en cuenta los requerimientos solicitados por el cliente (Refinería Esmeraldas); además de la afluencia tanto de personal como de vehículos, las características de las distintas áreas como son: las condiciones ambientales del lugar, geografía del terreno, arquitectura nueva y existente en las instalaciones.

Se inicia este capítulo con una descripción de las locaciones de Refinería Esmeraldas en las que se instalarán los diferentes subsistemas.

La Garita Peatonal es el área por donde ingresa el personal de planta, personal administrativo y visitantes. Aquí se realiza el escaneo de maletas, detección de metales en personas, se controla el acceso y la hora de entrada - salida por las entradas de seguridad.

La Garita Vehicular es el área de ingreso de vehículos de personal y contratistas; además, como norma de seguridad el o los acompañantes del conductor deben descender del automóvil y registrar su ingreso por un acceso peatonal designado para este objetivo.

La sala de control de procesos de planta o Bunker es una edificación ubicada estratégicamente en el área central de las inmediaciones de refinería desde la cual se monitorea el estado de los procesos de refinación. Allí, desde varios computadores, grupos del personal técnico de planta que trabajan por turnos las 24 horas del día, monitorean digitalmente la refinación del crudo.

El cuarto de control es una nueva área que se construirá y desde donde se realizará el monitoreo en tiempo real de las alertas de alarmas de cada subsistema, y se visualizará lo captado por las cámaras del nuevo sistema de circuito cerrado de televisión.

El Data Center existente actualmente es en donde funciona el cuarto de telecomunicaciones de refinería, por lo que se lo usará como el sitio adecuado para ubicar armarios de equipos (racks) con algunos de los equipos de los distintos sistemas instalados, entre ellos los servidores de accesos, CCTV y cableado perimetral.

2.1 DISEÑO DE LAS REDES DEL SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN

Siguiendo las revisiones previas por parte de la fiscalización y los levantamientos en campo se ha determinado el diseño del subsistema de CCTV a implementar.

Para el conveniente monitoreo de las distintas áreas donde es requerido, se realiza la siguiente distribución de cámaras:

Tabla 2. 1 Distribución de cámaras en el proyecto

Equipo	Área			
	Garita Peatonal	Garita Vehicular	Sala de Control	Perímetro
Cámara domo fija (POE)	3	2	1	0
Cámara domo análoga PTZ presurizada	0	1	0	41

Se seleccionaron las cámaras fijas de tipo megapíxel debido a que se desea monitorear constantemente y a detalle el ingreso y la salida de personal, razón por la que se ha usado cámaras fijas de 3 MP que permitirán enfocar directamente áreas de ingreso y registro de personal con una nitidez muy elevada.

Se seleccionaron las cámaras PTZ debido a que su fácil re direccionamiento y control de acercamiento y alejamiento hacen de estas los elementos ideales para monitorear remotamente todo el perímetro de la refinería, su calidad de imagen es menor a las cámaras fijas ubicadas en los accesos, pero no es necesario tener una resolución elevada en este caso de monitoreo, ya que el objetivo es detectar cualquier tipo de intrusión o evento no autorizado mas no identificar específicamente un rostro u objeto.

La cantidad de cámaras como fijas megapíxel (POE) establecida se basa en la necesidad de visualización de los sectores de acceso peatonal tanto a la entrada como salida, así como el registro de asistencia de personal y contratistas.

En el caso de las cámaras PTZ la cantidad seleccionada es la requerida para cubrir el monitoreo del perímetro interno de refinería, así como el tránsito de entrada y salida de vehículos en la Garita vehicular.

Se utilizan dos grabadores de video digital NVR, ya que se recomienda usar a cada uno de ellos hasta con 32 cámaras para evitar el excesivo consumo de ancho de banda en la red. Para las conexiones electrónicas a la intemperie o subterráneas, se utiliza cable FTP CAT 6¹⁸.

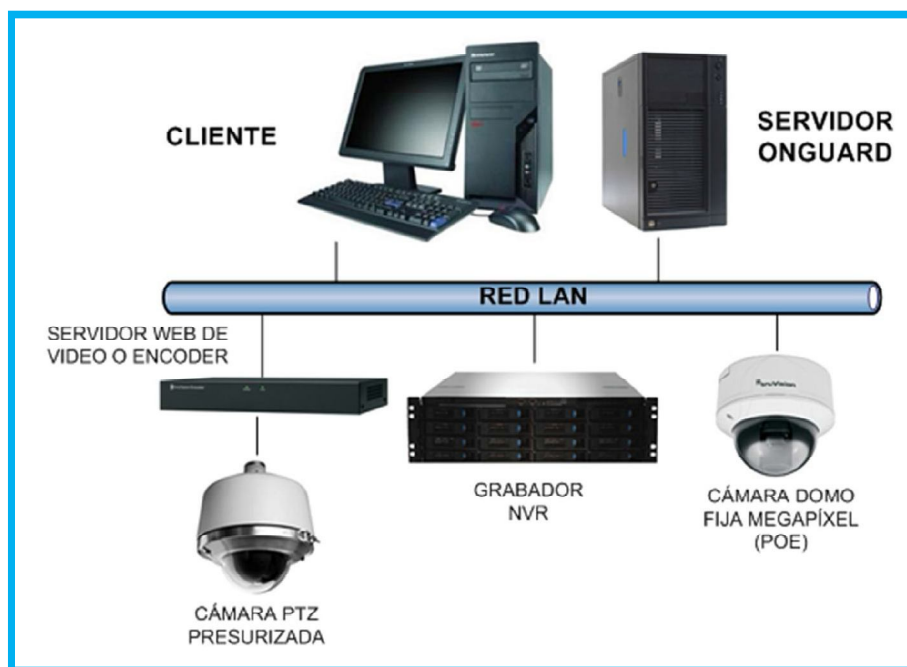


Figura 2. 1 Diagrama general de CCTV

2.1.1 SELECCIÓN DE LENTE DE CÁMARA

Es de gran importancia establecer el tamaño del lente de la cámara según el ángulo de vista que se requiera, mientras mayor es el tamaño del lente menor es el ángulo de visión. En la figura 2.3 se puede observar un ejemplo.

¹⁸Cable diseñado para uso en exteriores o para instalarlo bajo suelo, tiene un blindaje adicional a más de su chaqueta que lo hace más resistente a la intemperie, además tiene un separador en cruz para cada dos pares de cable.



Figura 2. 2 Variación de medida de lente

Para esto se cuenta con herramientas en línea que ayudan a tener un valor de referencia para elegir el lente correcto ingresando ciertos datos como se muestra a continuación:

Para cámara domo PTZ presurizada:

Tamaño del CCD		
1/4" CCD	1/3" CCD	1/2" CCD
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distancia Real		
Distancia Horizontal desde la cámara al objeto		Altura de la cámara desde el suelo
<input type="text" value="5"/> Metros		<input type="text" value="15"/> Metros
Seleccione el tamaño de la lente		
Ancho de objeto	Distancia Real	Tamaño del lente requerido
<input type="text" value="3"/> Metros	<input type="text" value="15.81138"/> Metros	<input type="text" value="19"/> mm

Figura 2. 3 Cálculo del lente de cámara PTZ

Para cámara domo megapíxel fija (POE):

Tamaño del CCD		
1/4" CCD	1/3" CCD	1/2" CCD
<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Distancia Real	
Distancia Horizontal desde la cámara al objeto	Altura de la cámara desde el suelo
<input type="text" value="4"/> Metros	<input type="text" value="2.5"/> Metros

Seleccione el tamaño de la lente

Ancho de objeto	Distancia Real	Tamaño del lente requerido
<input type="text" value="3"/> Metros	<input type="text" value="4.716990"/> Metros	<input type="text" value="7.5"/> mm

Figura 2. 4 Cálculo del lente cámara megapíxel fija

Se puede observar que en ambos casos se tiene un cálculo estimado que cumple con los requerimientos para las áreas visualizadas en refinería.

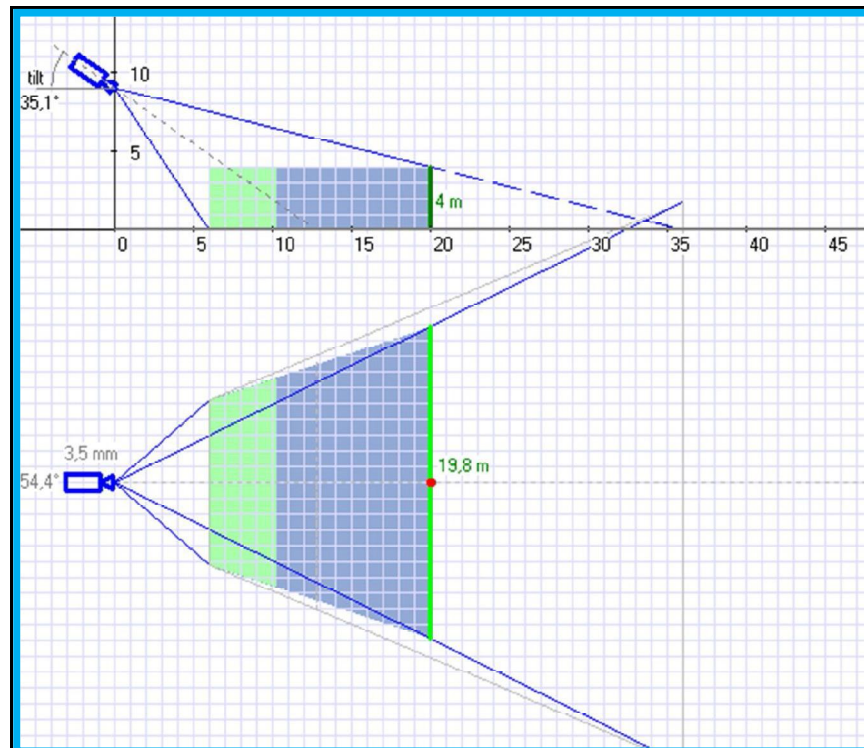


Figura 2. 5 Proyección del rango visual de la cámara elevada a 9 metros desde el piso

ID Cámara	Tamaño CCD	Altura Cam.	Distancia	Ancho CDV	Alto CDV	Inclinación	Distancia Focal
1	1/4 "	9	20	19,8	4	35,1	3,5

Resolución	Zona visible	Descripción	Zona muerta	Anchura Zona muerta
352x240 (CIF NTSC)	<input checked="" type="checkbox"/>		6,02	10,39

Cámara

Altura de instalación (m)
9

Formato CCD/CMOS
1/4 " 4:3

Distancia Focal (mm)
3,5

Inclinación de la Cámara *
35,1

Resolución
352x240 (CIF NTSC)

Ángulos de Visión *

Horizontal
54,4

Vertical
42,2

Resolución	Compresión	Tamaño Frame*, KB	FPS	Días
352x240 (CIF NTSC)	H.264-30 (Calidad Media)	0,7	15	30

Cámaras	Ancho de banda, Mbit/s	Espacio del disco, GB	Bitrate, kbit/s
41	3,53	1142,6	86

Figura 2. 6 Parámetros configurables para el diseño de la cámara PTZ en función de la altura de instalación (9m)

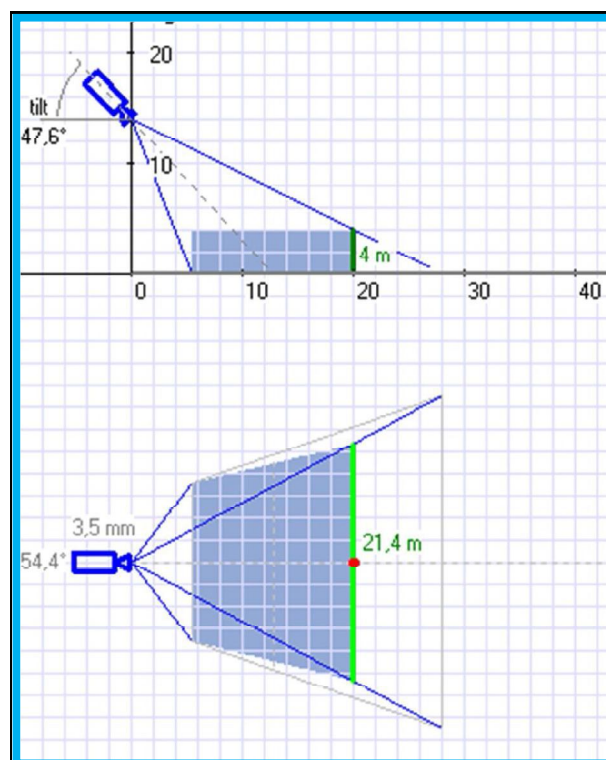


Figura 2. 7 Proyección del rango visual de la cámara elevada a 14 metros desde el piso

ID Cámara	Tamaño CCD	Altura Cam.	Distancia	Ancho CDV	Alto CDV	Inclinación	Distancia Focal
1	1/4 "	14	20	19,2	4	12,5	3,5

Resolución	Zona visible	Descripción	Zona muerta	Anchura Zona muerta
352x240 (CIF NTSC)	<input checked="" type="checkbox"/>		5,44	14,42

Cámara

Altura de instalación (m)
14

Formato CCD/CMOS
1/4 " 4:3

Distancia Focal (mm)
3,5

Inclinación de la Cámara *
47,6

Resolución
352x240 (CIF NTSC)

Angulos de Visión *

Horizontal
54,4

Vertical
42,2

Figura 2. 8 Parámetros configurables para el diseño de la cámara PTZ en función de la altura de instalación (14m)

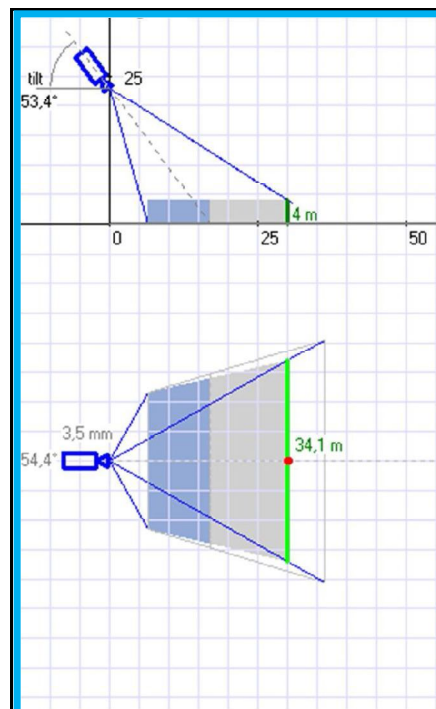


Figura 2. 9 Proyección del rango visual de la cámara elevada a 23 metros desde el piso

Cámara				
Altura de instalación (m)				
23				
Formato CCD/CMOS				
1/4"	4:3			
Distancia Focal (mm)				
3,5				
Inclinación de la Cámara *				
53.4				
Resolución				
352x240 (CIF NTSC)				
Angulos de Visión *				
Horizontal				
54,4				
Vertical				
42.2				

Resolución	Zona visible	Descripción	Zona muerta	Anchura Zona muerta
352x240 (CIF NTSC)	<input checked="" type="checkbox"/>		6,36	22,9

Altura Cam.	Distancia	Ancho CDV	Alto CDV	Inclinación	Distancia Focal
23	30	34,1	4	53.4	3,5

Figura 2. 10 Parámetros configurables para el diseño de la cámara PTZ en función de la altura de instalación (23m).

2.1.2 CARACTERÍSTICAS TÉCNICAS DE EQUIPOS SELECCIONADOS

Tabla 2. 2 Características básicas de la cámara PTZ


<i>CÁMARA DOMO PTZ PRESURIZADA (ANÁLOGA)</i>	
Marca	Pelco
Modelo	SD435-PRE0
Tecnología	Análoga
Alimentación	24V AC ó 24V DC
Resolución	540 líneas
Sensor de imagen	CCD 1/4"
Lente	3.4 a119 mm
Zoom	35X
Ángulo de visión	55.8° a 3.4 mm y 1.7° a 119mm
Domo inferior	LD53PR-0

Tabla 2. 3 Características básicas de la cámara domo fija

<i>CÁMARA DOMO MEGAPIXEL FIJA</i>	
Marca	UTC Fire & Security
Modelo	TVD-M3210V-2-N
Tecnología	IP
Alimentación	12V DC POE
Resolución	3 megapíxeles
Sensor de imagen	CMOS 1/2.5"
Lente	2.7 a 9 mm
Detección de movimiento	Sí
Domo inferior	Anti vandálico

Tabla 2. 4 Características básicas del inyector PoE


<i>INYECTOR POE</i>	
Marca	UTC Fire & Security
Modelo	MS-POE
Dimensiones	Ancho: 73mm Alto: 24 mm Profundidad: 55 mm
Voltaje de entrada	110V AC
Voltaje de funcionamiento	48V DC

Tabla 2. 5 Características básicas del switch de 8 puertos

<i>SWITCH DE 8 PUERTOS</i>	
Marca	Cisco
Modelo	IE-3000-8TC
Dimensiones	Ancho: 152.4mm Alto: 147.32 mm Profundidad: 111.76 mm
Voltaje de entrada	110V AC
Ranuras para SFP (Fibra óptica)	2
Puertos de RED	8

Tabla 2. 6 Características básicas del switch de 24 puertos


<i>SWITCH DE 24 PUERTOS</i>	
Marca	Cisco
Modelo	WS-C3560G-24PS-E
Dimensiones	Ancho: 444.5mm Alto: 43.942mm Profundidad: 378.46 mm
Voltaje de entrada	110V AC
Ranuras para SFP (Fibra óptica)	4
Puertos de RED	24
Descripción	Switch POE

Tabla 2. 7 Características básicas del video web server



<i>SERVIDOR WEB DE VIDEO O ENCODER</i>	
Marca	Truvision
Modelo	TVE-400
Dimensiones	Ancho: 315mm Alto: 45 mm Profundidad: 201 mm
Alimentación	110V AC
Interface de comunicación	Ethernet RJ45, RS-485
Consumo de corriente	1 A
Canales	4

Tabla 2. 8 Características básicas del grabador NVR

<i>GRABADOR DE VIDEO EN RED (NVR)</i>	
Marca	Lenel
Modelo	DVC-HD-A-A00-08-2T
Voltaje de entrada	110V AC
Compresión	H.264

2.1.3 DESCRIPCIÓN DE LOS EQUIPOS DE CCTV

2.1.3.1 Cámara domo megapíxel fija

La cámara digital seleccionada es un dispositivo de red que se configura y maneja mediante el puerto de red que dispone. Este puerto se caracteriza por soportar el

estándar PoE; gracias a esto la única conexión que se necesita para ponerla en funcionamiento es un punto de red con alimentación; el resto de entradas y salidas que dispone no se usan ya que son para manejar más opciones de monitoreo que no se usan en el caso presente.

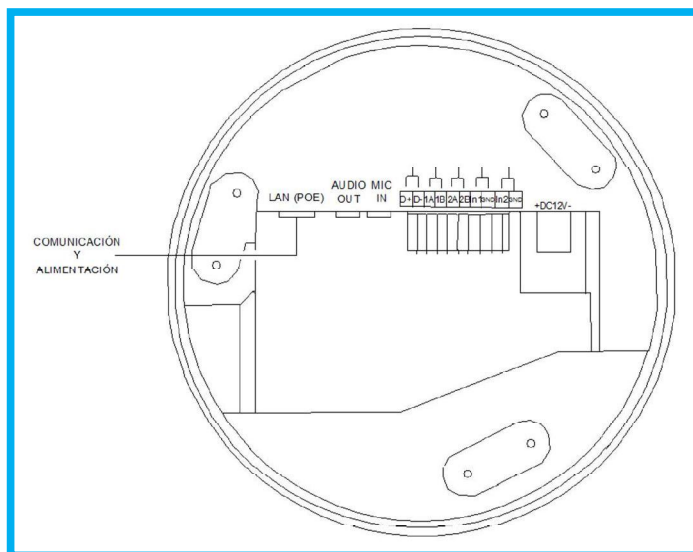


Figura 2. 11 Cámara domo fija megapíxel (PoE)

2.1.3.2 Cámara analógica PTZ

La cámara que se ha seleccionado es de tipo analógica; se necesita de un convertidor de video para que sus grabaciones analógicas sean digitalizadas y se puedan transmitir mediante la red Ethernet disponible.



Figura 2. 12 Cámara analógica PTZ

Esta se constituye de tres piezas fundamentales; la denominada olla o carcasa que es la estructura metálica donde se enrosca la cámara al soporte y por donde se conecta el cableado, el mecanismo de movimiento y funcionamiento del lente denominado robot y por último la carcasa de protección transparente que protege al robot denominado domo. En la Figura 2.13 se puede ver el conjunto de estos elementos formando la cámara.

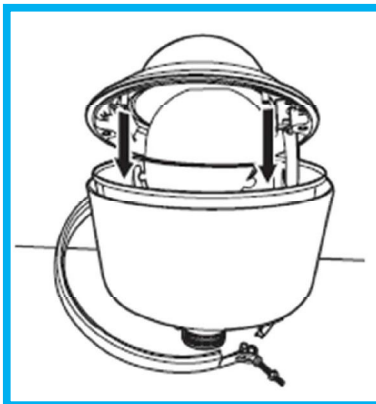


Figura 2. 13 Elementos que conforman la cámara PTZ

Se dispone del denominado cable pulpo el cual es un arreglo de cables de red UTP y FTP, cables de alimentación y cable coaxial fusionados en un solo conector tipo hembra como se puede apreciar en la Figura 2.14, el cual está destinado a ser conectado y asegurado en el zócalo macho de la olla o carcasa de la cámara.

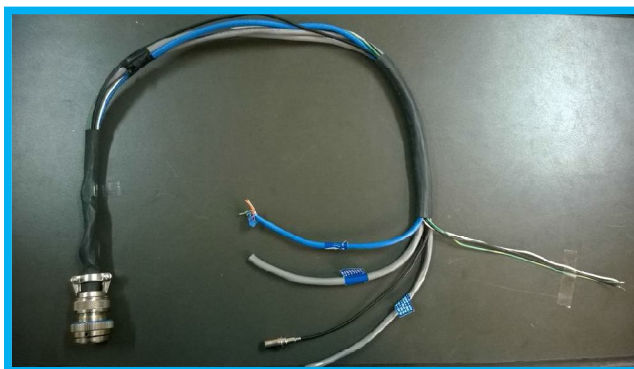


Figura 2. 14 Cable pulpo

En este arreglo de cables se disponen entradas y salidas analógicas, de las cuales para el caso presente se usan la salida de video analógico (cable coaxial), los cables de alimentación (Blanco – Neutro, Negro - fase, Verde – tierra) y del cable FTP el par azul y blanco – azul que son la comunicación RS-485 a dos hilos de recepción de datos para el manejo del movimiento de horizontal y vertical que se tiene en esta cámara; el resto de cables no se los usa ya que estos tienen funciones que no se ocuparán en nuestro caso.

2.1.3.3 Inyector PoE

Este pequeño equipo se utiliza para proveer a las cámaras megapíxel fijas el punto de red + alimentación DC que necesitan. En la Figura 2.15 se puede apreciar su configuración física.

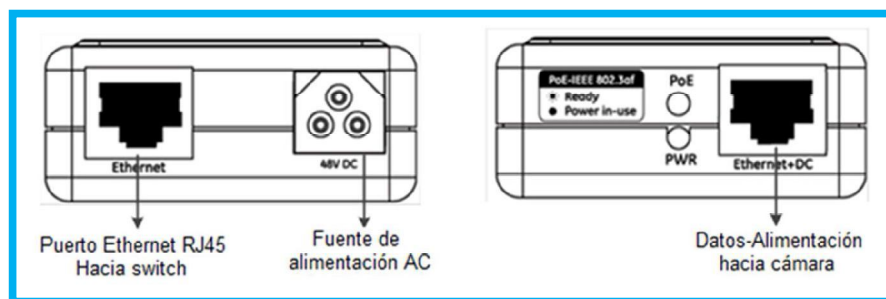


Figura 2. 15 Inyector POE

2.1.3.4 Grabador de video NVR

Se dispone de estos equipos para la administración inicial del video grabado por las cámaras, estos equipos se componen de un chasis con capacidad para 16 discos como máximo y con un arreglo de fábrica de 8 discos de 2 Terabytes cada uno.

2.1.3.5 Servidor web de video

Se dispone de estos equipos para la conversión de video analógico a video digital que se requiere en las cámaras PTZ; este equipo posee cuatro canales de entrada de video analógico de las cuales se ocupa una, el resto se tiene como reserva para un posible incremento de equipos a futuro, y también se usa el puerto de RS-485 para el control del movimiento de la cámara.

En la Figura 2.16 se describen las entradas y salidas de este equipo.

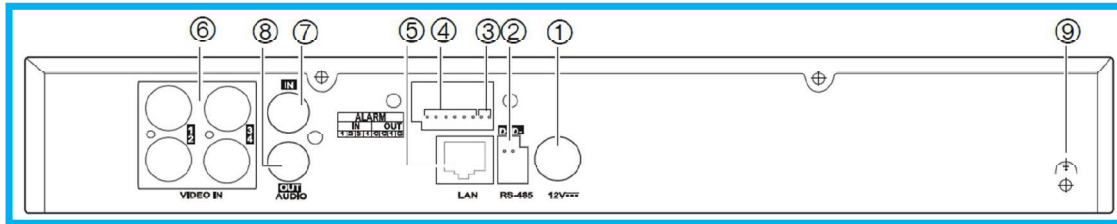


Figura 2. 16 Servidor web de video o encoder

1. Fuente de alimentación 12V DC
2. RS-485 D +, D- (señales de control de movimiento del robot).
3. Salida de alarma
4. Entrada de alarma
5. Puerto Ethernet RJ45
6. Entrada de video
7. Entrada de audio
8. Salida de audio
9. Tierra

2.1.3.6 Switch de 8 puertos no administrable y fuente

Este equipo se caracteriza por su fácil manejo y alto desempeño ya que es de tipo industrial, se dispondrá de estos equipos en racks de 8U y en tableros de equipos en campo para conectar dispositivos de red como cámaras o paneles de control de acceso, se usan los puertos en relación con la necesidad de cada ubicación.

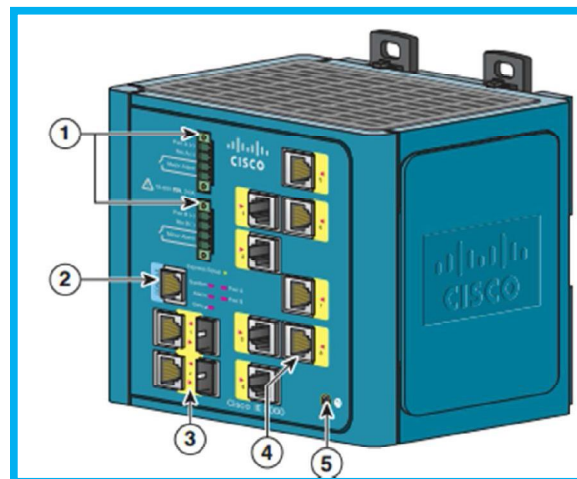


Figura 2. 17 Distribución de puertos del switch de 8 puertos

1. Zócalos de alimentación VAC y VDC.
2. Puerto de consola.
3. Puertos de múltiple propósito.
4. Par de puntos de red (total 4 pares).
5. Tornillo de puesta a tierra.

Como este equipo es de tipo modular se dispone de su fuente de voltaje por separado.



Figura 2. 18 Fuente de alimentación modular

Como se puede apreciar en la Figura 2.18 esta fuente de alimentación posee 3 borneras para el cableado de fuerza a 110VAC (Fase, Neutro, tierra) y la salida de 24VDC que usa el switch para el enlace de la fuente y el switch se usa el puente que viene de fábrica para este propósito.



Figura 2. 19 Puente para alimentación VDC

2.1.3.7 Switch de 24 puertos PoE

Este equipo se caracteriza por proporcionar en cada uno de sus puertos punto de red y alimentación VDC, además este equipo posee 4 puertos para fibra óptica

para el enlace de comunicaciones; su alimentación es de 110VAC desde la red eléctrica.

2.1.4 DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE CCTV EN LAS AREAS A MONITOREAR.

2.1.4.1 Cámara domo fija megapíxel (PoE)

Se tiene como elementos básicos para la conexión de esta cámara el switch del sistema para el punto de red, la alimentación de 110VAC, el inyector PoE, la cámara y los cables de red UTP Cat 6A; en el caso de las ubicaciones con enlace inalámbrico este conecta el switch presente en dichas ubicaciones con la red principal.

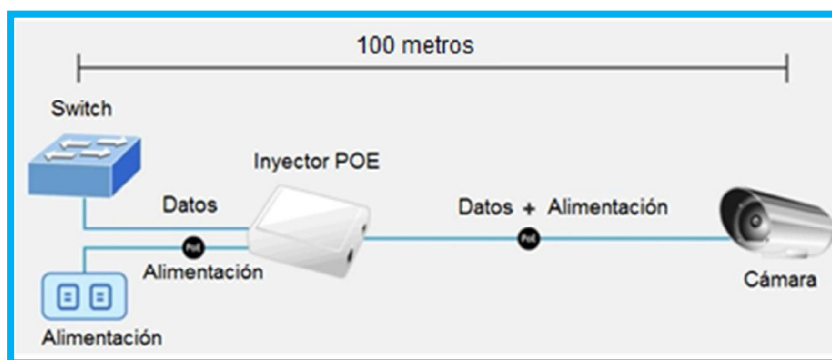


Figura 2. 20 Conexión de cámara fija con inyector POE

- En la garita peatonal:

Se conectan desde sus ubicaciones a través de tubería EMT mediante cables de red directamente al switch PoE de 24 puertos ubicado en el rack, que está dispuesto en el Data center.

En el plano CIV-200 que se presenta la implantación de las cámaras en las diferentes ubicaciones de la nueva arquitectura a construirse.

- En la garita vehicular:

Las cámaras que se encuentran en esta ubicación se alimentan con sus respectivos equipos inyectores de PoE, pero el enlace de red se debe realizar mediante el sistema inalámbrico debido a que esta ubicación se encuentra

demasiado distante del data center excediendo la distancia máxima de 100 metros.

En el plano EE-500 se tiene la implantación de las cámaras en la nueva arquitectura de la garita.

En el plano EE-501 presenta la vista frontal de la implementación de las cámaras en esta ubicación.

En el plano EE-502 presenta la vista lateral de la implementación de las cámaras en esta ubicación.

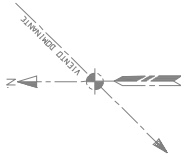
- En la sala de control de procesos (bunker)

En esta locación presenta una sola cámara de este tipo la que se ha dispuesto para monitorear el ingreso.

En el plano CIV-270 presenta la vista isométrica de la implementación de esta cámara para esta ubicación.

IMPLANTACIÓN GARITA VEHICULAR

(1:100)



CALLE DE HORMIGÓN
F_c = 210 kg/cm² EXISTENTE

ÁREA PARQUEO DE
MILLA EXISTENTE

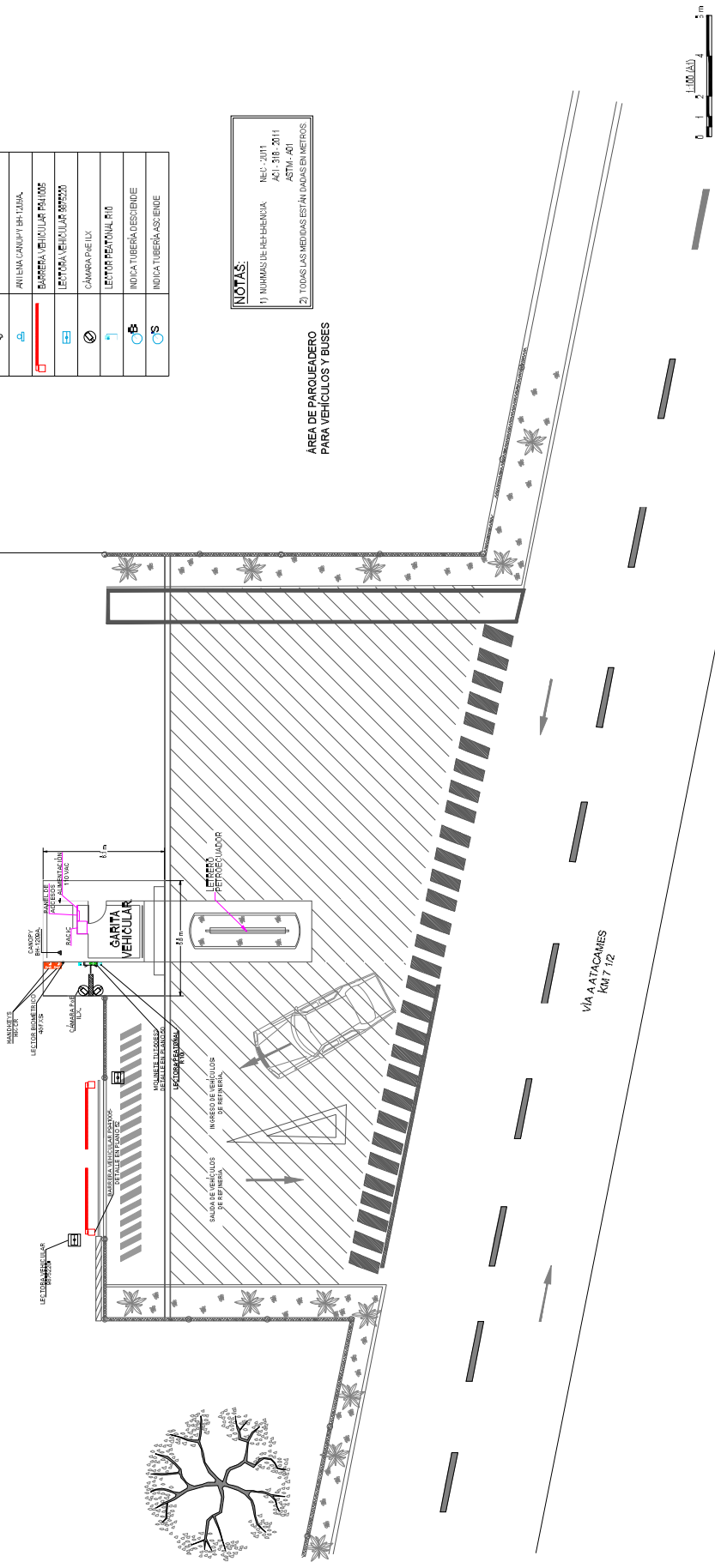
ÁREA DE PARQUEADERO DE VEHÍCULOS
DE REFINERÍA Y VISITANTES

SIMBOLOGÍA

	VOLUMEN DE CONCRETO
	HANDRAIL/REJILLA
	LECTOR BIOMÉTRICO/GPFS
	ANTENA CAROLIN 887.100A
	BARREERA VEHICULAR P/1000
	LECTORA VEHICULAR 800/520
	CÁMARA P/100
	LECTOR PEATONAL R10
	INDICA TUBERÍA DE BIODIESEL
	INDICA TUBERÍA ASFALTADA

NOTAS:
 1) NORMAS DE REFERENCIA: N.E.C. 2011, ACI 308. 2011, ASTM-A01
 2) TODAS LAS MEDIDAS ESTÁN DADAS EN METROS.

ÁREA DE PARQUEADERO PARA VEHÍCULOS Y BUSES



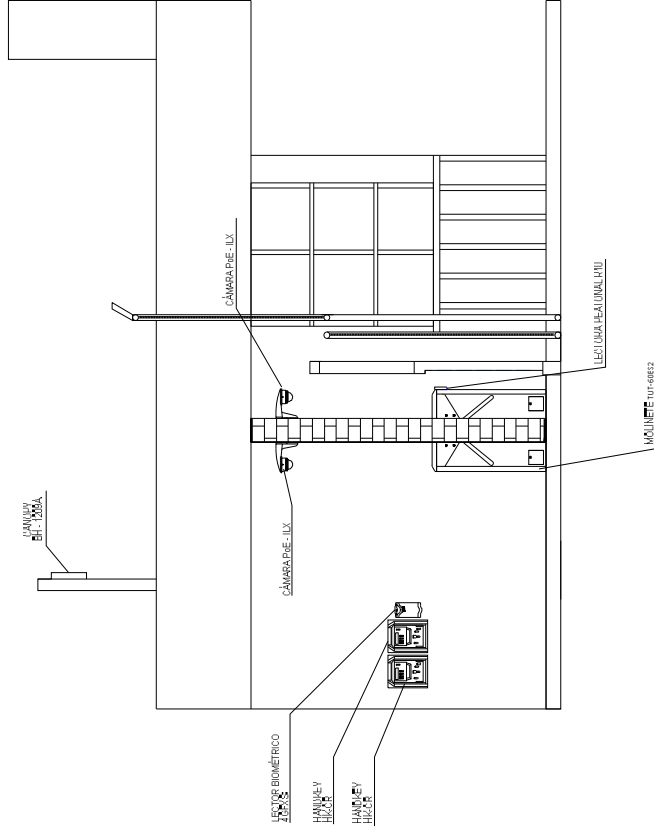
REGISTRO INGENIERÍA / DISEÑO

REV.	FECHA	DISEÑO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Mathis Cajalero Andrés Ceip				

MINISTERIO DE TRANSPORTES E INFRAESTRUCTURA
 SISTEMA DE SEGURIDAD FÍSICA INTEGRAL DE REFINERÍA ESMERALDAS


 Siaproc
 INGENIERÍA Y CONSTRUCCIÓN
 CONTRATO N°: 2012084 ESCALA: 1:100
 GARITA VEHICULAR - PLOT PLAN
 PLANO N°: EE-500 REVISIÓN: 000

DETALLE GARITA VEHICULAR - VISTA LATERAL
(1/20)



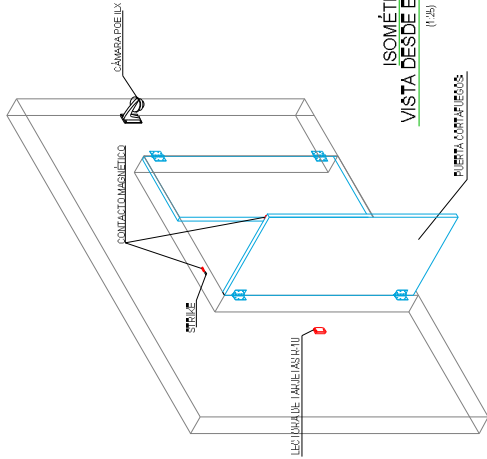
NOTAS:
 1) NOMBRAS DE REFERENCIA: NEC-2011 A01-2011-2011
 2) TODAS LAS MEDIDAS ESTÁN DADAS EN METROS



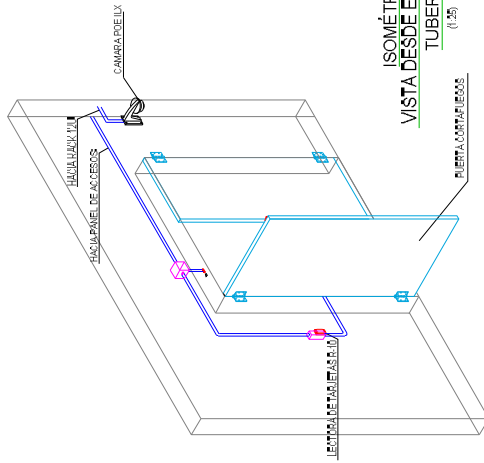

SISTEMA DE SEGURIDAD FÍSICA INTEGRAL DE REFINERÍA ESMERALDAS
 CONTRATO N°: 2012004 ESCALA: 1:20
 GARITA VEHICULAR - VISTA LATERAL
 PLANO N°: EE-502 REVISIÓN: 000

REGISTRO INGENIERÍA / DISEÑO						
REV.	FECHA	DISEÑO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Martha Cajalero Andrés Capó				

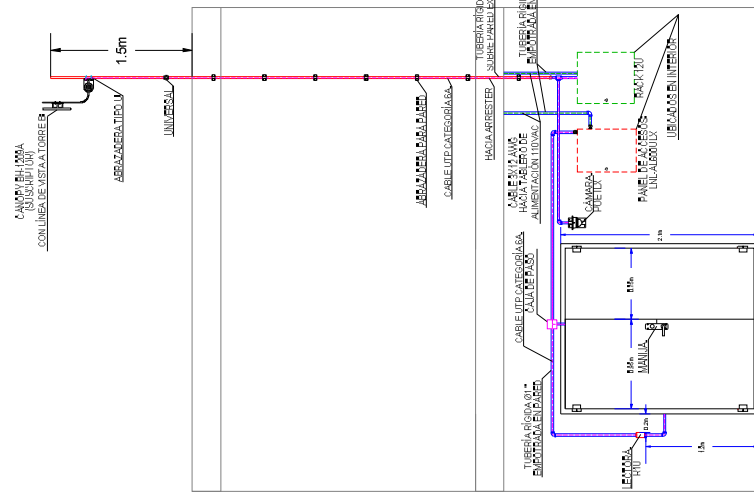
ENTRADA A SALA DE CONTROL - DETALLE DE PUERTA PRINCIPAL



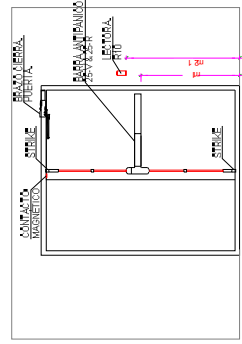
ISOMÉTRICO
VISTA DESDE EL EXTERIOR
(1:25)



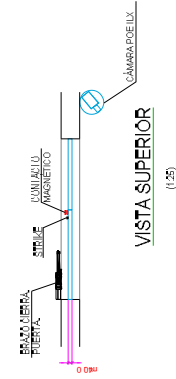
ISOMÉTRICO
VISTA DESDE EL EXTERIOR
TUBERIA
(1:25)



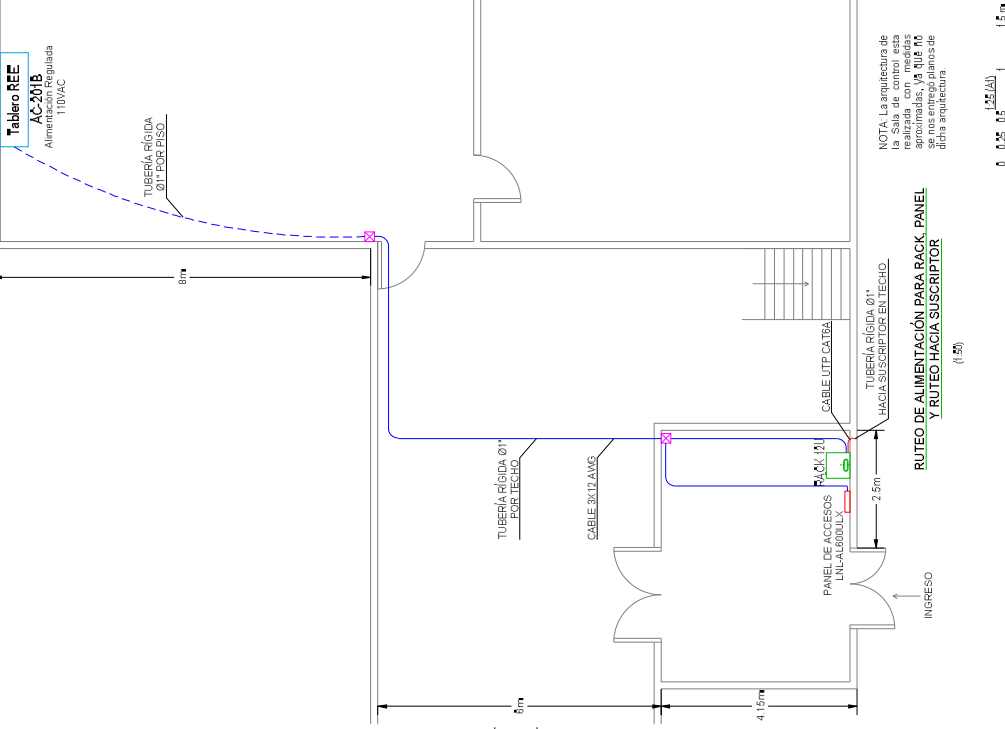
VISTA EXTERIOR
(1:25)



VISTA INTERIOR
(1:25)



VISTA SUPERIOR
(1:25)



RUTEO DE ALIMENTACIÓN PARA RACK, PANEL
Y RUTEO HACIA SUSCRIPCIÓN
(1:25)

NOTA: La ruta de la sala de control esta realizada con medidas aproximadas, ya que no se tiene el plano de la sala de arquitectura.



- NOTAS:
- 1) NORMAS DE REFERENCIA: N.E. 2011, A.S. 204, A.S.T.M. A-61
 - 2) TODAS LAS MEDIDAS ESTÁN DADAS EN METROS.

REGISTRO INGENIERIA / DISEÑO

REV.	FECHA	DISEÑO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Martha Cajalero Andrés Cep				

SISTEMA DE SEGURIDAD FÍSICA INTEGRAL DE REFINERIA ESMERALDAS

 SIA PROCI Ingenieros y Constructores

CONTRATO No.: 2013084 ESCALA: INDICADA

ENTRADA A SALA DE CONTROL
 DETALLE DE PUERTA PRINCIPAL

PLANO No.: CIV-270 REVISIÓN: 000

2.1.4.2 Cámara domo PTZ presurizada (análoga)

Se tienen como elementos básicos para la conexión de este tipo de cámaras el punto de alimentación de 24VAC, el punto de video analógico, el servidor web de video con su respectiva alimentación a 110 VAC, el cableado de RS-485 a dos hilos desde la cámara hacia el servidor web con el que se maneja el movimiento del robot, y el punto de red obtenido mediante el enlace inalámbrico dispuesto para este objetivo.

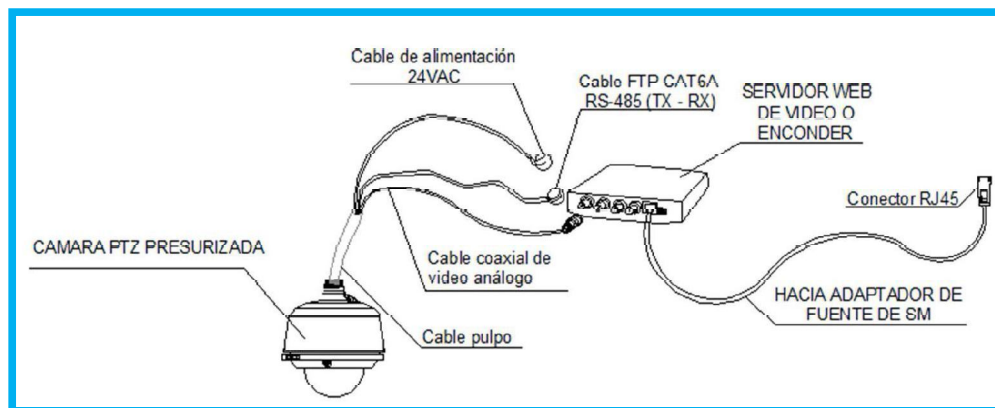


Figura 2. 21 Conexión de cámara PTZ

Las cámaras de este tipo se implementan en el perímetro interno de la refinería de manera que mediante los cálculos previos de alcance y cobertura visual de estas cámaras se ha implementado la distribución de estas como se puede ver en el plano EE – 100 Y 102.

Como la geografía del terreno que alberga a la refinería no es uniforme en nivel se ha implementado instalaciones en postes de 11, 14 y 23 metros, como se puede ver en los planos:

E – 200, 201 Y 202

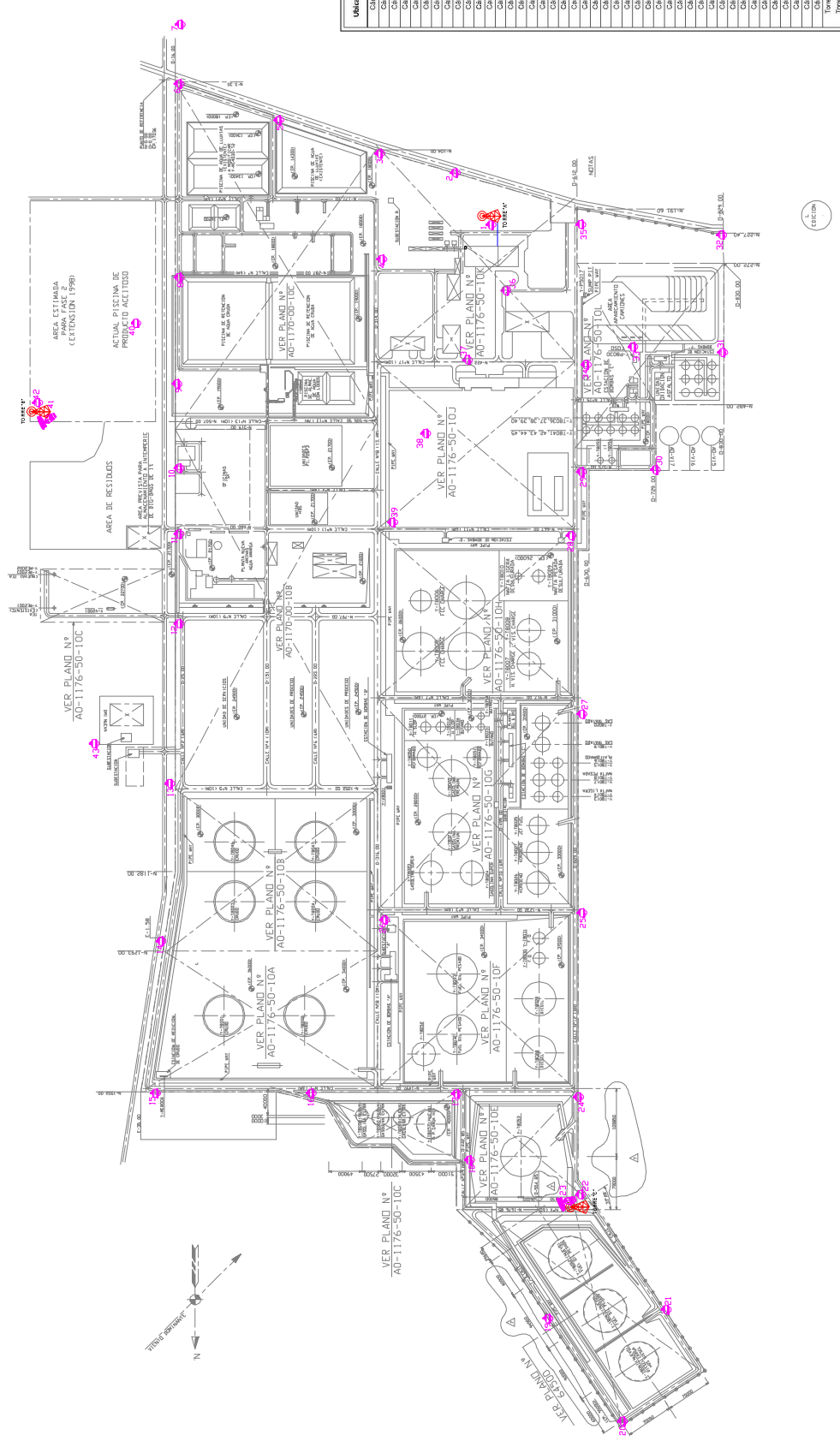
Todo esto con el fin de garantizar una mejor visualización del área designada y de tener línea de vista entre los enlaces inalámbricos emisores y los receptores en las torres de comunicación

Como se observa en los planos anteriores en cada poste se tiene un UPS para garantizar el funcionamiento continuo de cada cámara en caso de una pérdida de alimentación desde la red y se tiene un tablero de equipos, en el cual se tiene

instalados el video web server con las respectivas protecciones eléctricas y el equipo de aterrizaje de energía electroestática para el enlace inalámbrico como se puede apreciar en el plano EE - 604

En el cuarto de monitoreo se tiene el video Wall que permite realizar el monitoreo en tiempo real de todo los sistemas incluyendo el de CCTV.

En el área de data center se ubican la mayoría de equipos de red encargados del almacenamiento – administración de información y de las comunicaciones, se tiene la distribución de estos equipos en un rack de 48 U así como sus conexiones en los planos: EE - 606 y EE – 607.



Ubicación Sitio	Coordenadas UTM
Cámara 01	17 E 646277 N 020550
Cámara 02	17 E 646277 N 020550
Cámara 03	17 E 646277 N 020550
Cámara 04	17 E 646277 N 020550
Cámara 05	17 E 646277 N 020550
Cámara 06	17 E 646277 N 020550
Cámara 07	17 E 646277 N 020550
Cámara 08	17 E 646277 N 020550
Cámara 09	17 E 646277 N 020550
Cámara 10	17 E 646277 N 020550
Cámara 11	17 E 646277 N 020550
Cámara 12	17 E 646277 N 020550
Cámara 13	17 E 646277 N 020550
Cámara 14	17 E 646277 N 020550
Cámara 15	17 E 646277 N 020550
Cámara 16	17 E 646277 N 020550
Cámara 17	17 E 646277 N 020550
Cámara 18	17 E 646277 N 020550
Cámara 19	17 E 646277 N 020550
Cámara 20	17 E 646277 N 020550
Cámara 21	17 E 646277 N 020550
Cámara 22	17 E 646277 N 020550
Cámara 23	17 E 646277 N 020550
Cámara 24	17 E 646277 N 020550
Cámara 25	17 E 646277 N 020550
Cámara 26	17 E 646277 N 020550
Cámara 27	17 E 646277 N 020550
Cámara 28	17 E 646277 N 020550
Cámara 29	17 E 646277 N 020550
Cámara 30	17 E 646277 N 020550
Cámara 31	17 E 646277 N 020550
Cámara 32	17 E 646277 N 020550
Cámara 33	17 E 646277 N 020550
Cámara 34	17 E 646277 N 020550
Cámara 35	17 E 646277 N 020550
Cámara 36	17 E 646277 N 020550
Cámara 37	17 E 646277 N 020550
Cámara 38	17 E 646277 N 020550
Cámara 39	17 E 646277 N 020550
Cámara 40	17 E 646277 N 020550
Cámara 41	17 E 646277 N 020550
Cámara 42	17 E 646277 N 020550
Cámara 43	17 E 646277 N 020550
Cámara 44	17 E 646277 N 020550
Cámara 45	17 E 646277 N 020550
Torre A (45m)	17 E 646277 N 020550
Torre B (45m)	17 E 646277 N 020550
Torre C (45m)	17 E 646277 N 020550

SIMBOLOGÍA	
	Cámara PTZ Térmica
	Cámara PTZ Presunizada
	Torre de Comunicación de 45m
	Fibra óptica

N° de Proyecto: 100-2011-CAP-15
 INSTITUCIÓN: SENASA SAG

EMPRESA: Ship
 CARRERA: INGENIERÍA EN SISTEMAS DE TELECOMUNICACIONES
 ALUMNO: MATHA GUJARRO ANDRÉS CAJO
 TÍTULO: INGENIERO EN SISTEMAS DE TELECOMUNICACIONES
 PLAN: No. EE-100 REVISIÓN: 000

REGISTRO INGENIERIA / DISEÑO			
0	Matha Gujarró Andrés Cajo	DISEÑO	REVISADO
		APROBADO	COORDINADO

2.2 DISEÑO DE LAS REDES DEL SUBSISTEMA DE CONTROL DE ACCESOS

Después de un análisis de los futuros beneficios que el sistema diseñado conceptualmente le puede brindar a la refinería, se ha procedido con el diseño final, se ha realizado nuevos levantamientos en campo para que tomando en cuenta las dimensiones físicas de los accesos y los requerimientos finales se pueda hacer una correcta selección y distribución de equipos, así como también un correcto dimensionamiento de las capacidades de estos.

En la garita peatonal y vehicular se colocan lectores de geometría de mano (handkeys) y un biométrico para el control de asistencia de personal y contratistas.

Para acceder al interior de la refinería se debe ingresar por los torniquetes distribuidos a lo ancho del acceso peatonal, como complemento se tendrá una puerta motorizada para personas con capacidades especiales; en la garita vehicular para el acceso peatonal debido a sus dimensiones lo más acertado es instalar un molinete que cumple una función similar al torniquete pero que ocupa un menor espacio, y en el caso de la sala de control de procesos (Bunker) la puerta de acceso principal se controlará usando lectoras de proximidad y cerraduras electromagnéticas.

Para el control vehicular se disponen las barreras vehiculares cuyo funcionamiento es en conjunto con los booster vehiculares.

La cantidad elegida de torniquetes para acceso peatonal se fundamenta en evitar la congestión peatonal, debido a la afluencia de personal existente en refinería, lo mismo ocurre con el número de handkeys para el control de asistencia, que agilitan el ingreso a la debida hora de trabajadores y contratistas.

En el acceso vehicular con el uso de las barreras vehiculares, se busca evitar que los vehículos sean controlados de manera rustica y así facilitar el tránsito. En la Sala de control se tiene control de acceso ya que este sitio es de acceso exclusivo para personal autorizado, pues aquí se llevan a cabo importantes labores de control de procesos propios de refinería.

Un componente fundamental en la estructura del sistema de control de accesos son los Controladores o Paneles de Control de Acceso. En la memoria interna de los paneles de control de acceso se almacena toda la información de los niveles de acceso asociados a ellos y el control de asistencia del personal y contratistas, por lo que de existir una pérdida de comunicación con el servidor el sistema puede seguir operando sin inconveniente hasta que se restablezca la comunicación y se descarguen los eventos de acceso en la base de datos del servidor.

La cantidad de tarjetas electrónicas esclavas para los paneles de acceso está de acuerdo al número de entradas para lectoras, lo cual se conoce como número de puertas, así también se toma en cuenta si se necesita de salidas de relé adicionales. En el caso de handkeys se usa una tarjeta exclusiva que soporta hasta 8 de estos equipos.

El subsistema de control de accesos se encuentra comandado por el software OnGuard, el cual integra un sistema de monitoreo de alarmas y CCTV, que le brinda la máxima protección, versatilidad y simple operación.

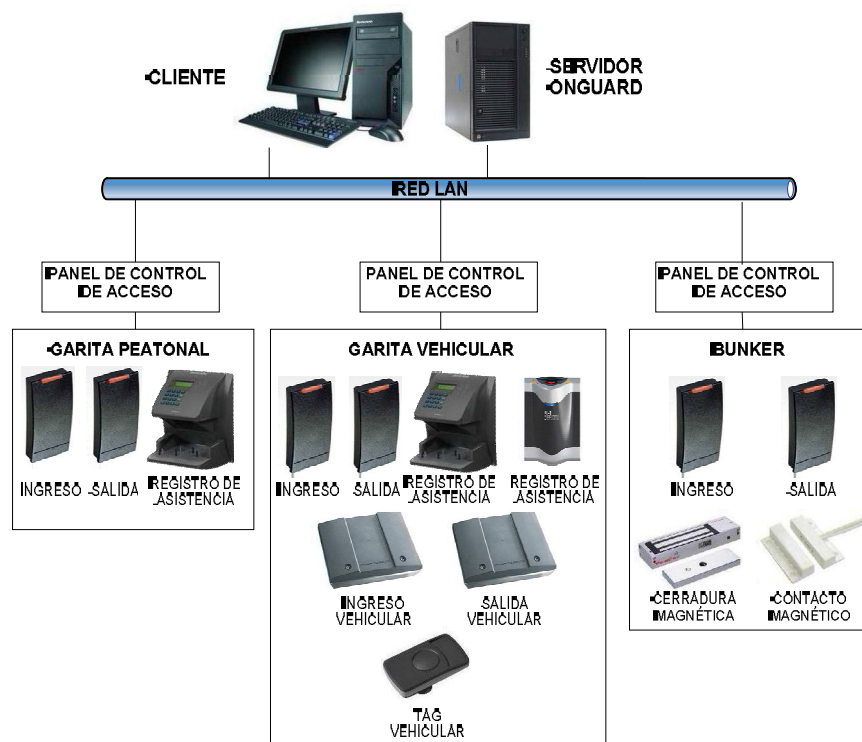


Figura 2. 22 Diagrama general de control de acceso

2.2.1 DISEÑO DEL CONTROL DE ACCESOS DE CADA ÁREA

2.2.1.1 Garita peatonal

Esta área es por donde ingresan a las instalaciones el personal de planta, personales administrativos y visitantes los cuales se movilizan caminando. Para el control de los equipos ubicados en esta garita se cuenta con tres paneles de acceso donde se ubican tarjetas controladoras y fuentes. La comunicación hacia el Data center de los equipos de esta garita es mediante RS-485 a través de la tarjeta controladora LNL-2220 que se conecta al switch PoE de 24 puertos. Se muestra en la tabla 2.9 el consumo de corriente para establecer las fuentes de alimentación necesarias

Tabla 2. 9 Consumo de equipos de control de acceso de garita peatonal

GARITA PEATONAL			
Cantidad	Equipo	Consumo (mA)	Voltaje Dc
1	LNL 2220	500	12 V
1	LNL 500B	250	12 V
9	LNL 1320	4950	12 V
10	Lectoras Proximidad	3000	12 V
6	Handkey	6000	12 V
1	Cerradura 1200 lb	500	12 V
TOTAL	Consumo (A) 12 Vdc	15,2	
TOTAL	Fuentes de 6A a 12 Vdc	3	
6	Luces Indicadoras	240	24 V
1	Puerta motorizada	750	24 V
TOTAL	Consumo (A) 24 Vdc	0,99	
TOTAL	Fuentes de 2,5A a 24 Vdc	2	
1	Espina Simple	Alimentación	110V AC
2	Espina Doble	Alimentación	110V AC

Como dispositivo de identificación en el acceso de personal y contratistas, para control de asistencia y registro de horario de entrada-salida, se dispone de handkeys. Se coloca un protector para estos handkeys que le proporciona un grado de protección contra ambientes polvorientos, sucios o lluviosos.

Sobre cada lector de geometría de mano se asigna un indicador de acceso con el objetivo de dar una señal de aviso visual, cuando se ha realizado correctamente o no el control de asistencia. Cuando se ha ejecutado con éxito la lectura de geometría de mano se enciende la luz verde, caso contrario se mantiene

encendida la luz roja que será indicativo para volver a realizar la lectura de geometría de mano.

Se cuenta con torniquetes de simple y doble acceso bi-direccionales, que tienen como objetivo permitir que solo pase una persona a la vez. Su dispositivo de identificación para control de acceso, tanto para entrada como para salida, son lectoras de proximidad. También se tiene una puerta motorizada adecuada para personas con capacidades especiales, de este modo se accede por la garita peatonal luego de identificarse tanto a la entrada como a la salida en lectoras de proximidad.

2.2.1.2 Garita vehicular

Es el área por donde ingresan los vehículos de personal de trabajo y contratistas. Aquí se realiza un control de acceso mediante barreras vehiculares para entrada y salida, esto mediante lectoras vehiculares que trabajan en conjunto con tags instalados en los vehículos. En esta área se encuentran instalados dos paneles de accesos donde se ubican tarjetas controladoras y fuentes. La comunicación hacia el Data center de los equipos de esta garita es mediante RS-485 a través de la tarjeta controladora LNL-2220 con el switch de 8 puertos usando el sistema de enlace inalámbrico. Para realizar un control completo de acceso en esta locación se cuenta con los siguientes equipos y se muestra en la Tabla 2.10 el consumo de corriente para establecer las fuentes de alimentación necesarias:

Tabla 2. 10 Consumo de equipos de control de acceso garita vehicular

GARITA VEHICULAR			
Cantidad	Equipo	mA	Voltaje Dc
1	LNL 2220	500	12 V
1	LNL 500B	250	12 V
4	LNL 1320	2200	12 V
2	Lectoras Proximidad	600	12 V
2	Handkey	2000	12 V
1	Lector Biométrico	500	12 V
TOTAL	Consumo (A) 12 Vdc	6,05	
TOTAL	Fuentes de 6A a 12 Vdc	2	
2	Lectoras Vehiculares	2000	24 V
TOTAL	Consumo (A) 24 Vdc	2	
TOTAL	Fuentes de 2,5A a 24 Vdc	1	
2	Barreras vehiculares	Alimentación	110V AC
1	Molinete	Alimentación	110V AC

Para control de asistencia y registro de horario de entrada-salida de personal por esta locación, se dispone de handkeys; de la misma forma, para registro de asistencia de contratistas se tienen un biométrico en el cual el funcionario puede validar su huella dactilar.

Se ubica un molinete bi-direccional en la Garita vehicular para registrar el ingreso o salida peatonal de los ocupantes de vehículos, ya que solo se permite que el conductor permanezca dentro del mismo. Para el control de acceso tiene incorporado lectoras de proximidad tanto para la entrada como salida a través de este molinete.

Para entrada y salida de vehículos de personal y contratistas se colocan barreras vehiculares, dos para cada vía. Los vehículos poseen un tag o booster con lo que se obtiene la información tanto del conductor, como del vehículo la cual es verificada por la lectora vehicular y así accionar o no las barreras que permiten el acceso.

2.2.1.3 Sala de control (Bunker)

En esta edificación central se tiene un panel de control de accesos donde se ubican tarjetas controladoras y fuentes. La comunicación hacia el Data center de los equipos en esta ubicación se realiza con la tarjeta LNL-2220 y el switch de 8 puertos a través del sistema de enlace inalámbrico de comunicaciones. Los equipos instalados para el control de acceso a la Sala de control son los siguientes. Se muestra en la Tabla 2.11 el consumo de corriente para establecer las fuentes de alimentación necesarias:

Tabla 2. 11 Consumo de equipos de control de acceso de bunker

SALA DE CONTROL (BUNKER)			
Cantidad	Equipo	mA	Voltaje Dc
1	LNL 2220	500	12 V
1	LNL 1320	550	12 V
2	Lectoras Proximidad	600	12 V
2	Cerradura 1200 lb	1000	12 V
TOTAL	Consumo (A) 12 Vdc	2,65	
TOTAL	Fuentes de 6A a 12 Vdc	1	
1	Puerta cortafuegos		
2	Contactos magnético		

Para el ingreso a la Sala de Control, se instala una nueva puerta de doble batiente, una de ellas fija y otra móvil, que permite tener aislamiento al ruido de áreas próximas, pues debido a la maquinaria circulante que existente en refinería se produce abundante ruido. Se cuenta con lectoras de proximidad tanto a la entrada como a la salida para el control de acceso.

La cerradura electromagnética está ubicada en la parte superior de la batiente móvil. De forma similar se encuentra ubicado el contacto magnético que es el dispositivo que da la señal de abertura de dicha puerta hacia el cuarto de control.

Además se tiene un brazo cierrapuertas también ubicado en la parte superior de la batiente móvil para asegurar su cierre.

2.2.2 CARACTERÍSTICAS TÉCNICAS DE EQUIPOS

Tabla 2. 12 Características básicas del handkey

LECTOR DE GEOMETRÍA DE MANO (HANDKEY)	
Marca	Schlage
Modelo	HK-2
Dimensiones	Ancho: 22,3 cm Alto: 29,6 cm Profundidad: 21,7 cm
Alimentación	12V DC
Consumo de corriente	1000 mA
Capacidad de usuarios	512 usuarios, ampliable a 32.512 usuarios
Interfaz de comunicación	RS-485 (4 y 2 hilos), RS-232 Serial o comunicaciones de red.

Tabla 2. 13 Características básicas de la lectora de proximidad

LECTORA DE PROXIMIDAD	
Marca	HID
Modelo	R10
Dimensiones	Ancho: 48,3 mm Alto: 102,6 mm Profundidad: 20,3 mm
Alimentación	10 a 16 VDC, protegida contra voltaje inverso
Consumo de corriente	300 mA
Alcance Máximo de Lectura	2" -3" (50-76 mm) con la Tarjeta Iclass de HID
Comunicación	Wiegand

Tabla 2. 14 Características básicas de las tarjetas de proximidad

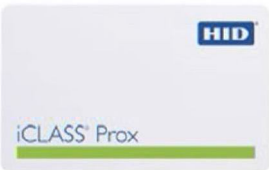
TARJETA DE ACCESO CON MEMORIA (PERSONAL PLANTA)	
Marca	HID
Modelo	2000PGGNN
Dimensiones	Ancho: 85.7mm Alto: 54 mm Profundidad: 0.84 mm
Alcance máximo	De 5 a 7.6 cm
Duración	100.000 lecturas
Retención de datos	10 años

Tabla 2. 15 Características básicas del biométrico

LECTOR BIOMÉTRICO	
Marca	Bioscrypt
Modelo	4GFXS
Dimensiones	Ancho: 96 mm Alto: 159 mm Profundidad: 65 mm
Alimentación	POE o fuente externa
Voltaje de fuente externa	12V DC
Consumo de corriente	500 mA
Interfaz de comunicación	LAN, WAN, RS485, USB, RS232

Tabla 2. 16 Características básicas de la lectora vehicular

LECTORA VEHICULAR DE LAGO ALCANCE	
Marca	Nedap
Modelo	9875220 TRANSIT
Dimensiones	Ancho:310 mm Alto: 250 mm Profundidad:100 mm
Alimentación	24V DC
Consumo de corriente	1000 mA
Distancia de lectura	10 metros
Interfaz de comunicación	RS232, RS422, Profibus DP, TCP/IP
Velocidad del vehículo	Hasta 200km/h
Entrada	1 contacto seco
Salida	Wiegand, código de barras y Omron

Tabla 2. 17 Características básicas del booster

BOOSTER (TAG VEHICULAR)	
Marca	Nedap
Modelo	9895337 TRANSIT
Dimensiones	Ancho:65 mm Alto: 111 mm Profundidad:32 mm
Alimentación	Batería de ión de litio de 5 años, reemplazable
Distancia de lectura	10 metros
Frecuencia	2.400 – 2.482 GHz
Operatividad	Automática o manual

Tabla 2. 18 Características básicas del torniquete simple


TORNIQUETE SIMPLE	
Marca	Boon Edam
Modelo	THT-100ES2
Dimensiones	Ancho de paso libre: 648 mm Altura total: 2261 mm Ancho total:1524mm
Voltaje de entrada	110V AC
Consumo de corriente	1000 mA
Capacidad por minuto	15 personas por minuto
Incluye	Luces de tráfico

Tabla 2. 19 Características básicas del torniquete doble


TORNIQUETE DOBLE	
Marca	Boon Edam
Modelo	THT-100TS2
Dimensiones	Ancho de paso libre: 648 mm Altura total: 2261 mm Ancho total:2438mm
Voltaje de entrada	110V AC
Consumo de corriente	1000 mA
Capacidad por minuto	15 personas por minuto por cada paso libre
Incluye	Luces de tráfico

Tabla 2. 20 Características básicas de la puerta motorizada

PUERTA MOTORIZADA	
Marca	Boon Edam
Modelo	THG-42
Dimensiones	Altura total: 965.2 mm Ancho total:1016 mm
Voltaje de entrada	24V DC
Consumo de corriente	750 mA

Tabla 2. 21 Características básicas del molinete

MOLINETE	
Marca	Boon Edam
Modelo	TUT-60ES2
Dimensiones	Espacio de paso:457.2 mm Alto: 964.9 mm
Voltaje de entrada	110V AC
Requerimiento de corriente	15 A de red de servicio

Tabla 2. 22 Características básicas de la barrera vehicular

BARRERA VEHICULAR	
Marca	BFT
Modelo	MICHELANGELOP941005
Dimensiones	Ancho:460mm Alto: 1200 mm Profundidad:275 mm
Voltaje de entrada	110V AC
Longitud máxima	Hasta 4m
Tiempo de apertura	4 segundos

Tabla 2. 23 Características básicas del indicador de acceso


INDICADOR DE ACCESO PARA HANDKEY	
Marca	Boon Edam
Modelo	400U-L2
Alimentación	24V DC
Consumo de corriente	40 mA

Tabla 2. 24 Características básicas de la cerradura electromagnética


CERRADURA ELECTROMAGNÉTICA	
Marca	ViperTek
Modelo	VIP-1200L
Dimensiones	Ancho:66 mm Largo: 265 mm Profundidad:40 mm
Alimentación	12 V DC
Consumo de corriente	500 mA

Tabla 2. 25 Características básicas del contacto magnético

CONTACTO MAGNÉTICO	
Marca	Tane
Modelo	TAN-FM106
Dimensiones	Ancho:7.62 mm Alto: 13.46 mm Largo:33.78 mm
Voltaje de ruptura mínimo	250V DC
Consumo de corriente	1000 mA
Contacto	Se cierra cuando el imán está cerca

Tabla 2. 26 Características básicas de la tarjeta LNL-1320


TARJETA LNL-1320	
Marca	Lenel
Modelo	LNL-1320
Dimensiones	Ancho:203.2 mm Alto: 152.4 mm
Alimentación	12 V DC
Consumo de corriente	550 mA
Comunicación	RS-485
Capacidad	Hasta dos lectoras

Tabla 2. 27 Características básicas de la tarjeta LNL-2220

TARJETA CONTROLADORA LNL-2220	
Marca	Lenel
Modelo	LNL-2220
Dimensiones	Ancho:203.2mm Alto: 152.4 mm
Alimentación	12 V DC
Consumo de corriente	500 mA
Comunicación	RS-485
Capacidad	Hasta 32 dispositivos
Almacenamiento	Hasta 250000 tarjeta habientes

Tabla 2. 28 Características básicas de la tarjeta LNL-500B



TARJETA INTERFAZ PARA GEOMETRÍA DE MANOLNL-500B			
Marca	Lenel		
Modelo	LNL-500B		
Dimensiones	Ancho: 152.4 mm Alto: 127 mm		
Alimentación	12 V DC		
Consumo de corriente	250 mA		
Comunicación	RS-485		
Capacidad	Hasta 8 handkeys		

Tabla 2. 29 Características básicas de la fuente de 24VDC

FUENTE DE ALIMENTACIÓN 24VDC @ 2.5A			
Marca	Lenel		
Modelo	LNL-OLS75		
Dimensiones	Ancho: 177.8mm Alto: 107.95 mm Profundidad: 44.45 mm		
Voltaje de entrada	110V AC		
Voltaje de salida	24V DC		

Tabla 2. 30 Características básicas de la fuente de 12VDC

<p style="text-align: center;">FUENTE DE ALIMENTACIÓN 12VDC @ 6A</p>	
<p>Marca</p>	<p>Lenel</p>
<p>Modelo</p>	<p>LNL-600ULX-4CB6</p>
<p>Dimensiones</p>	<p>Ancho: 177.8mm Alto: 107.95 mm Profundidad: 44.45 mm</p>
<p>Voltaje de entrada</p>	<p>110V AC</p>
<p>Voltaje de salida</p>	<p>12V DC</p>

2.2.3 DESCRIPCIÓN DE LOS EQUIPOS DE CONTROL DE ACCESOS

2.2.3.1 Lector de geometría de mano (handkey)

Este equipo en su parte frontal superior posee un teclado matricial 4x4 numérico y de funciones; se tiene un lcd 2x16 con backlight de color amarillo donde se verifica el estado de funcionamiento y también se tiene en la parte derecha visto frontalmente un gráfico de ilustración para el correcto posicionamiento de la mano el momento de enrolar o de registrarse. En la parte frontal baja tenemos la distribución de postes guía donde deben tocar correctamente los dedos de forma que se tenga una disposición completamente abierta de la mano, que desde la parte baja del teclado será leída por la cámara interna que posee este equipo.

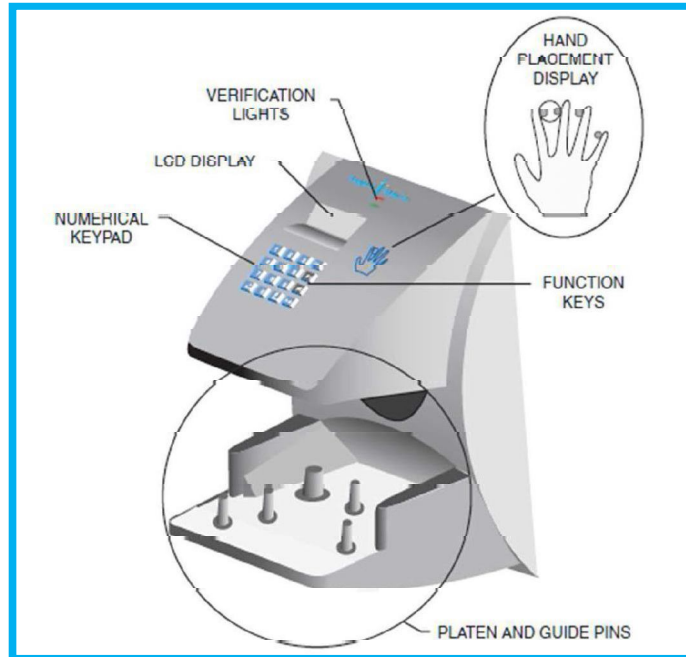


Figura 2. 23 Vista frontal isométrica del lector de geometría de mano

En la parte trasera se dispone de las borneras para conectar el cableado, en nuestro caso este equipo se usara mediante RS – 485 (half dúplex) a dos hilos para la sincronía de los datos de la clave de acceso, wiegand a 3 hilos (DATA, CLK, GND) para realizar la comparación del registro con la lectura realizada y la alimentación de 12VDC. En la Figura 2.24 se detalla esta distribución.

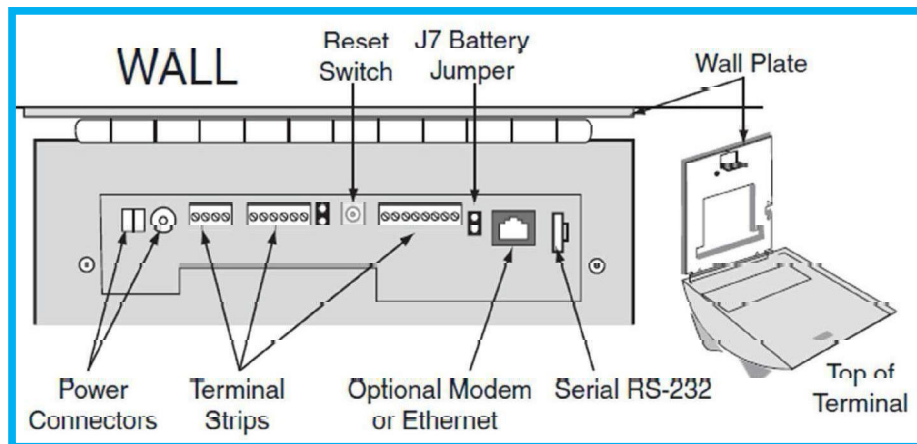


Figura 2. 24 Vista trasera del lector de geometría de mano

2.2.3.2 Lectora de proximidad

Se caracteriza por una carcasa lisa con un led de estado en su parte superior frontal; en la parte trasera dispone del cable (pig tail) que dispone de los diferentes hilos conductores para su manejo.

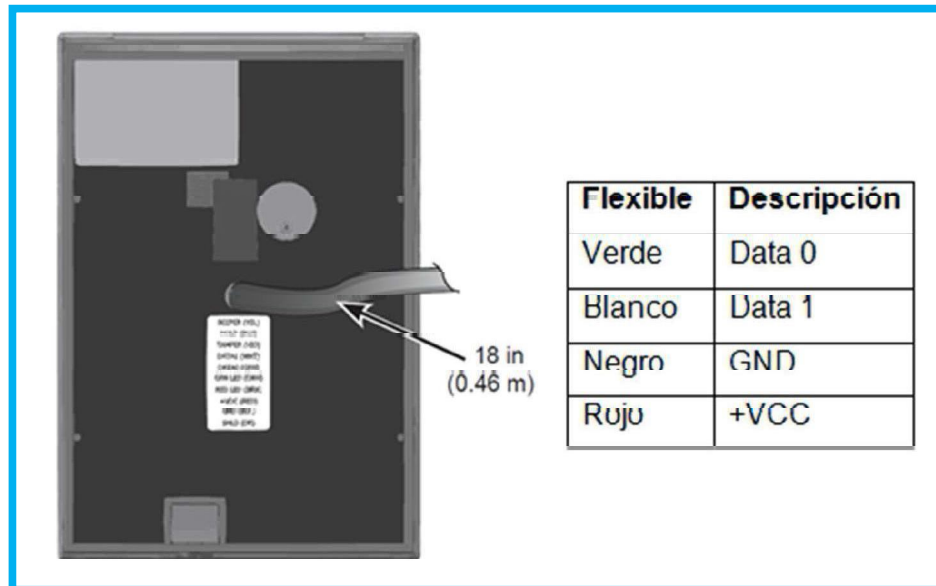


Figura 2. 25 Lectora de proximidad (parte trasera)

2.2.3.3 Tarjetas de proximidad

Las tarjetas de proximidad en conjunto con las lectoras de proximidad permite el manejo del sistema de control de accesos; estas son de PVC de forma rectangular, en su interior poseen una antena que trabaja a 13.56 Mhz y un chip de memoria de 256 byte en el que se graba la información del portador; se puede añadirle características específicas como fotografías, logotipos y códigos de barras mediante una impresora de credenciales adecuada.

Al ser una credencial no aplica ningún procedimiento de instalación, para su uso basta acercarla a menos de 5 cm de una lectora de proximidad.

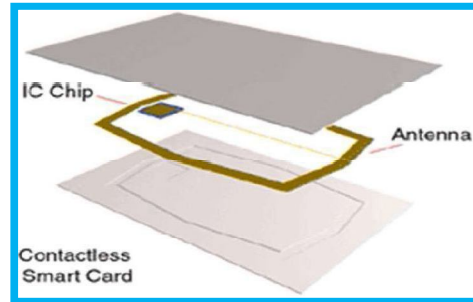


Figura 2. 26 Distribución interna de tarjeta inteligente

2.2.3.4 Lector biométrico

Este equipo dispone en su parte superior un lector de huellas dactilares y 3 leds de estado distribuidos en la parte frontal.



Figura 2. 27 Vista frontal biométrico

En su parte trasera se tiene el acceso a las borneras y pines de conexiones del cableado como se detalla a continuación.

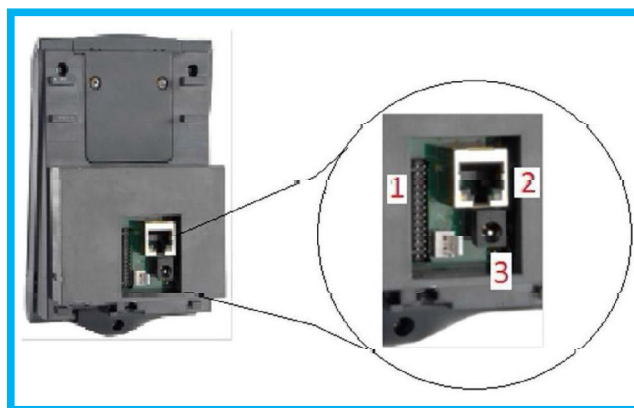


Figura 2. 28 Vista trasera biométrico

- 1) Puerto de 28 pines I/O - RS232/RS485, wiegand.
- 2) Puerto Ethernet con capacidad de PoE.
- 3) Conector hembra para alimentación independiente.

Se tiene el cable pulpo de este equipo, en el cual se distinguen los diferentes hilos conductores asociados a las comunicaciones descritas.



Figura 2. 29 Cable pulpo de biométrico con conector

Del cable se usa el protocolo wiegand a dos hilos (Data 0 – hilo verde y Data 1 – hilo blanco). Se usa el punto de datos para el enrolamiento y para suministrar el voltaje requerido gracias a su capacidad de soportar PoE.

2.2.3.5 Lectora vehicular de largo alcance

Este equipo se dispone en los accesos vehiculares con lo que se realiza un control automático del ingreso y salida de vehículos y conductores usando sus emisores instalados en los parabrisas de los automóviles.

Está formada de dos piezas que se cierran herméticamente, la parte trasera es de acero inoxidable y la frontal es de plástico rígido de alto impacto y no presenta ningún elemento de control.



Figura 2. 30 Vista isométrica de lectora vehicular

En su interior se tienen los circuitos electrónicos dispuestos en placas. En estas se tiene acceso a las diferentes borneras para las conexiones de control, comunicaciones, alimentación VDC y VAC así como elementos de maniobra como potenciómetros para poder regular parámetros de funcionamiento como distancia de alcance y frecuencia de funcionamiento.



Figura 2. 31 Parte interna de lectora vehicular

Mediante cables flex se conecta la parte de los circuitos electrónicos a la placa de lectura de emisores como se puede apreciar en al siguiente imagen.



Figura 2. 32 Placa de detección de emisores

2.2.3.6 Tag vehicular (booster)

Este equipo es el emisor que trabaja en conjunto con las lectoras vehiculares. Internamente se compone básicamente de un lector de chips, de un emisor con

antena y de una batería para su autonomía, en su parte externa presenta una ranura para la inserción de tarjetas de proximidad y un botón central.

Se inserta una tarjeta de proximidad en la ranura y al presionar el botón el emisor transmite el número de identificación del automóvil previamente programado y el número de identificación del conductor programado en la tarjeta de proximidad de manera simultánea, de esta forma la lectora recibe la información y la envía al sistema para su procesamiento y así se da acceso o se deniega en caso de no tener los respectivos permisos.

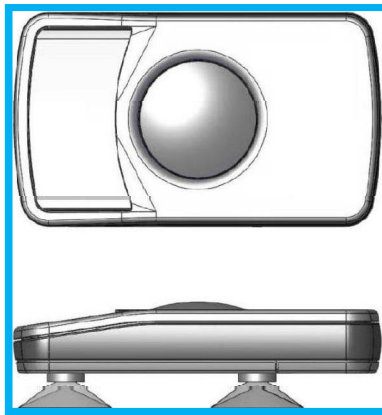


Figura 2. 33 Booster emisor de acceso vehicular

Su instalación es sencilla ya que este pequeño dispositivo dispone de tres ventosas para que pueda ser adherido al parabrisas del automóvil designado.



Figura 2. 34 Modo de empleo del dispositivo

2.2.3.7 Torniquetes simples y dobles

Estos equipos son los elementos físicos que controlan el ingreso por la garita peatonal, se tienen de tipo simple y doble. Se componen básicamente de un eje o

dos con tres espinas metálicas distribuidas en ángulos exactos de 120° . El eje está sujeto en un armazón de acero inoxidable como se muestra en la Figura 2.35.

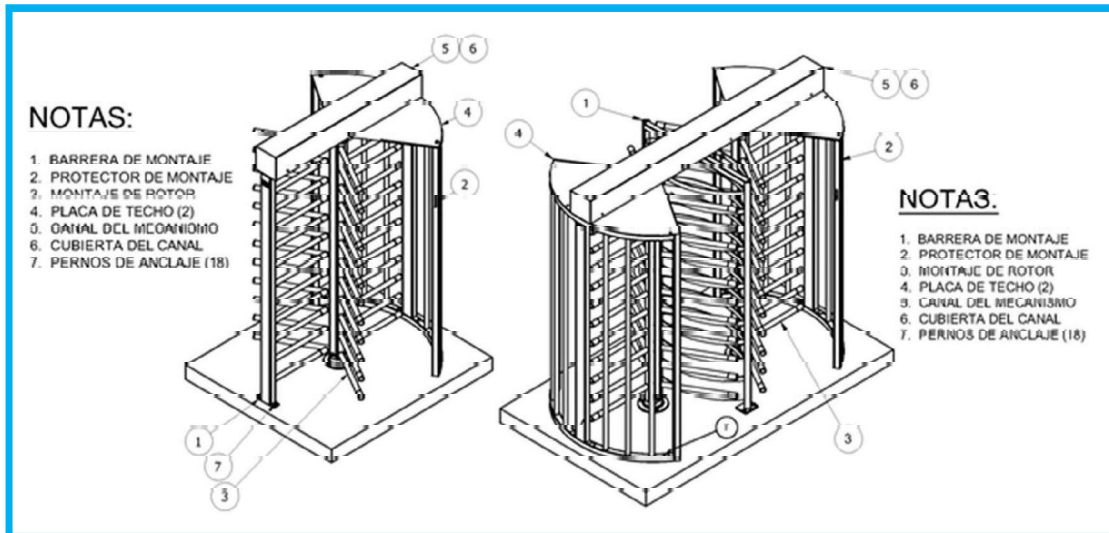


Figura 2. 35 Descripción de las partes de un molinete simple y doble

El armazón es de acero inoxidable y tiene una forma curva con una espina fija extra para garantizar que el paso de personal sea solo cuando el eje este liberado.

En la parte superior se encuentran los elementos electro-mecánicos para el manejo del giro y bloqueo del eje con las espinas.

Los soportes son huecos para poder llevar el cableado necesario de voltaje y control a través de ellos.

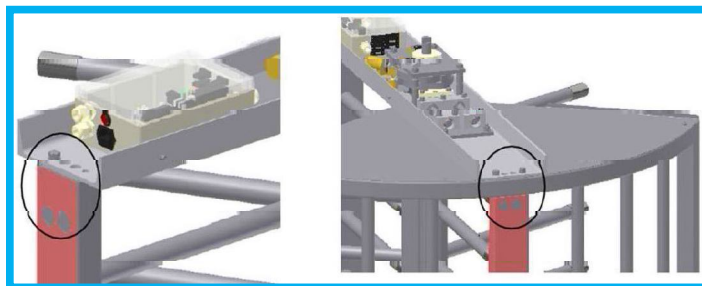


Figura 2. 36 Rutas de cableado a través de armazón metálico

El mecanismo de control básicamente se compone de dos solenoides las que se controlan mediante un circuito de control compuesto por dos MCB.

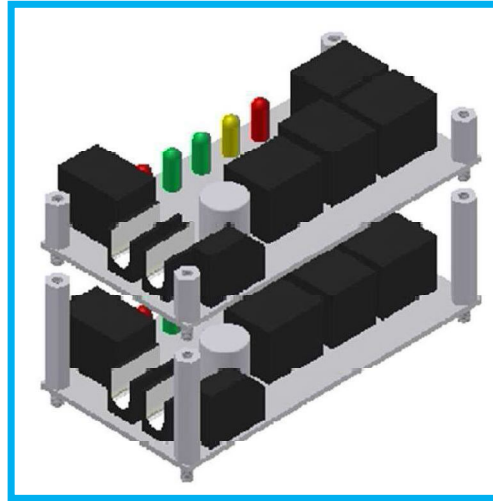


Figura 2. 37 Placas MCB superpuestas

En el interior de una caja estanca donde se encuentran los circuitos de control con las diferentes protecciones eléctricas y el transformador de voltaje que baja el voltaje de 110VAC que alimenta al sistema.

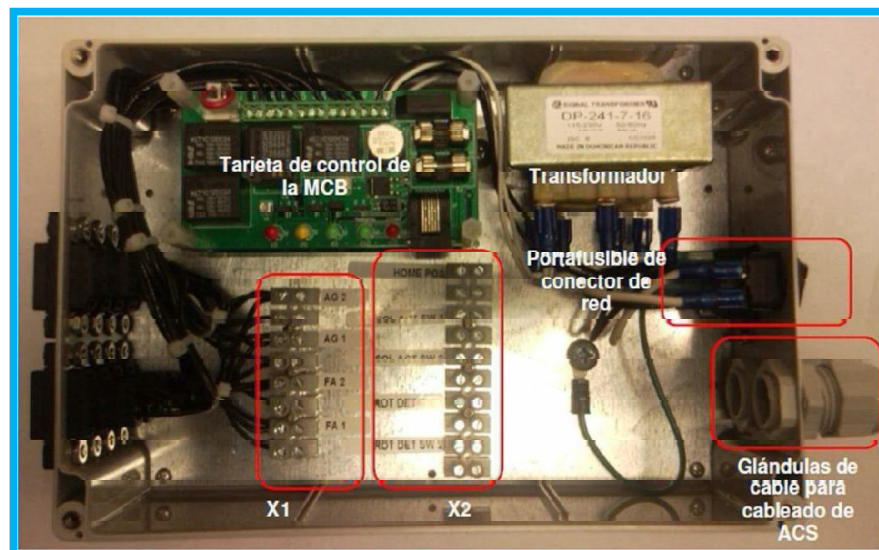


Figura 2. 38 Descripción caja de control

A la salida de la caja de control se tienen los solenoides que se encargan del bloqueo – desbloqueo del eje.

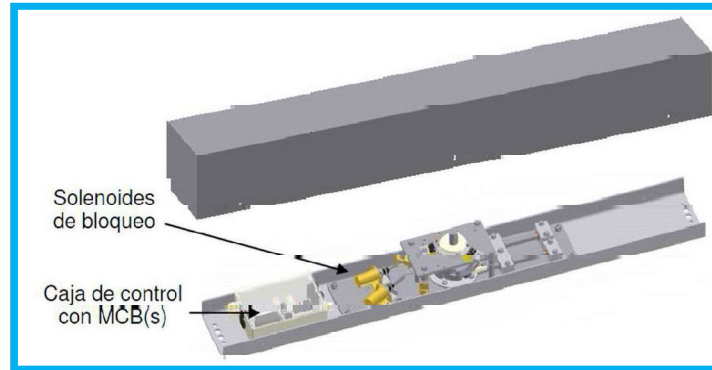


Figura 2. 39 Descripción sistema electro - mecánico

2.2.3.8 Puerta motorizada para personas con capacidades especiales

Este equipo es un elemento de control físico que permite el control del acceso de personal con capacidades especiales perteneciente a la refinería.

Es una puerta que se automatiza de manera que su manejo es automático usando a la par lectoras de proximidad para el ingreso y salida asociadas a ella; en la base de su eje de giro dispone de un motor que realiza la acción de giro para la apertura y un sistema de elementos hidráulicos para el cierre.

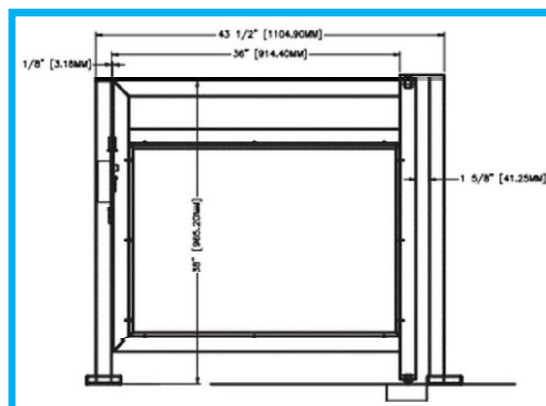


Figura 2. 40 Vista frontal puerta motorizada

2.2.3.9 Molinete

Este equipo es otro tipo de barrera física de control de accesos. Su movimiento es algo singular pero en función realiza el mismo control que un torniquete pero con el uso de menos espacio y una instalación más rápida.

Se forma de un armazón de acero inoxidable con un eje central inclinado hacia abajo aproximadamente 45° y el cual posee 3 agujeros separados 120° el uno del otro alrededor de su circunferencia. Por separado se tienen 3 brazos de acero inoxidable.



Figura 2. 41 Molinete armado

En el interior este posee el sistema electromecánico para el bloqueo y desbloqueo del eje así como la placa electrónica con las respectivas borneras de control y de alimentación.

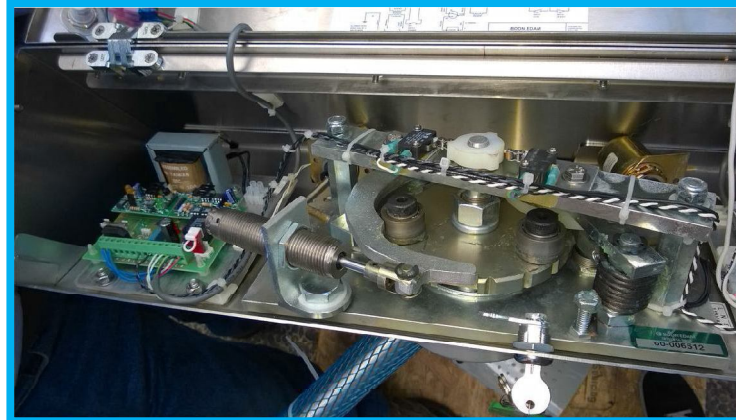


Figura 2. 42 Mecanismo de bloqueo del eje y placa electrónica de control

2.2.3.10 Barrera vehicular

Este equipo es el límite físico que permite controlar el flujo vehicular desde y hacia el interior de la refinería.

Se compone básicamente de dos partes; la carcasa metálica donde se tiene el sistema electro - mecánico para el control de movimiento del brazo, y el brazo.

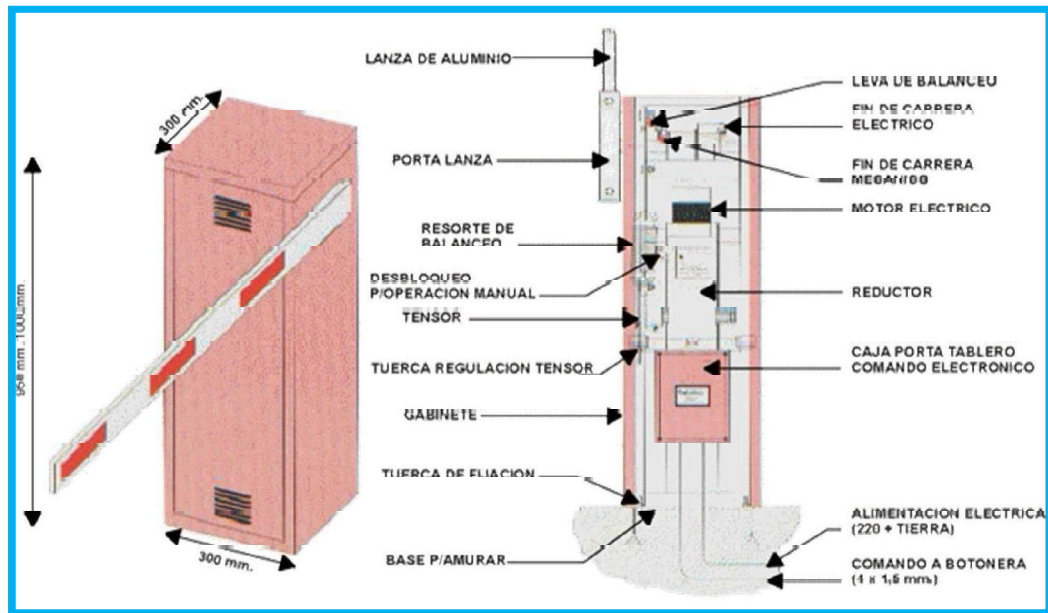


Figura 2. 43 Descripción externa e interna de barrera vehicular

En el interior se tiene el sistema electro – mecánico formado por un motor, su caja reductora para mejorar el torque y el sistema de retorno; en la parte inferior se tiene una caja estanca donde se aloja la placa electrónica que posee las entradas y salidas para realizar el control.



Figura 2. 44 Imagen de parte interna de la barrera vehicular

2.2.3.11 Luces indicadoras de acceso para handkey

Se tiene estos indicadores junto a los “handkeys” ubicados en la garita peatonal, de manera que poseen 2 leds, uno de color verde y el otro de color rojo; el led rojo permanece constantemente encendido y el verde en estado apagado. Si el acceso se concede el led rojo se apaga y se enciende el verde por 2 segundos y regresan a su estado original. Si no se concede el acceso ninguno de los leds cambia de estado original.

En la figura 2.45 se muestra la forma de conexión de estos indicadores a la salida de relé usada en el panel de control de accesos.

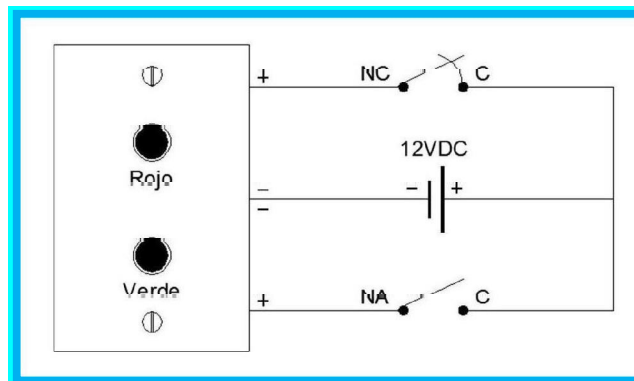


Figura 2. 45 Conexión luces indicadoras

2.2.3.12 Cerradura electromagnética

Este equipo se usa para mantener cerrada la puerta de ingreso en el bunker. Básicamente se compone de dos partes fundamentales: la chapa magnética que genera el campo magnético al energizarla y la placa ferro magnética que es atraída por la chapa que posee un orificio central para su montaje.



Figura 2. 46 Piezas de cerradura electromagnética

2.2.3.13 Contacto magnético

Este pequeño dispositivo se usa como elemento de control del estado de la puerta del bunker, de este modo si se encuentra abierta el contacto está abierto y se detecta el estado de la puerta en el sistema, mientras que si está cerrada el estado del contacto será también cerrado y no dará alarma en el sistema.

Este pequeño dispositivo se compone de 2 partes: la primera es el elemento magnético que básicamente es un imán dentro de una pieza plástica y el otro es un contacto normalmente abierto dentro de otra pieza plástica similar, de la que salen dos hilos conductores de cada extremo del contacto.

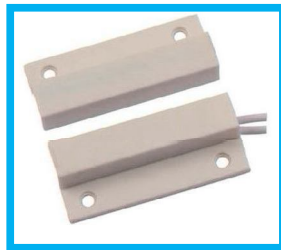


Figura 2. 47 Partes de un contacto magnético

2.2.3.14 Panel de control de accesos

Son los tableros de control de accesos a donde llegan las entradas y salidas de los equipos anteriormente detallados, se arman en función de las necesidades de la ubicación donde se encuentran, y su capacidad tiene un límite máximo de 6 tarjetas electrónicas.



Figura 2. 48 Tablero de control de accesos

Su tamaño es 24" de alto x 18" de ancho y 4.5" de profundidad, está hecho en acero galvanizado y tiene sus acabados con pintura electroestática.

Como estándar de fábrica se tiene montado en el interior una fuente electrónica de 12VDC @ 6A con una placa de extensión de 4 salidas protegidas por fusibles.

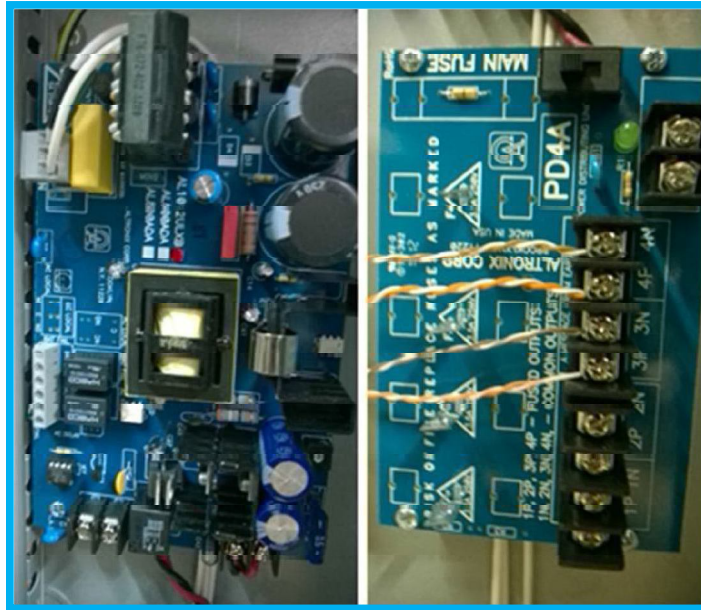


Figura 2. 49 Fuente de 12 VDC y placa expansora de salidas

En la fuente se tiene las borneras de alimentación a 110 VAC y borneras dedicadas a la detección de falla de energía en caso de un corte del suministro eléctrico.

En la placa de expansión se tienen las salidas de voltaje DC y también un switch para apagar dicho suministro.

2.2.3.15 Tarjeta electrónica controladora LNL-2220

Este tipo de tarjeta electrónica se usa en las tres diferentes ubicaciones de la refinería ya que su característica principal es la de enlazarse a la red mediante su puerto Ethernet RJ-45. Posee una memoria de 6 MB con capacidad de almacenamiento de hasta 50000 eventos y manejar hasta 32000 niveles de acceso.

A continuación se detallan sus partes más relevantes.

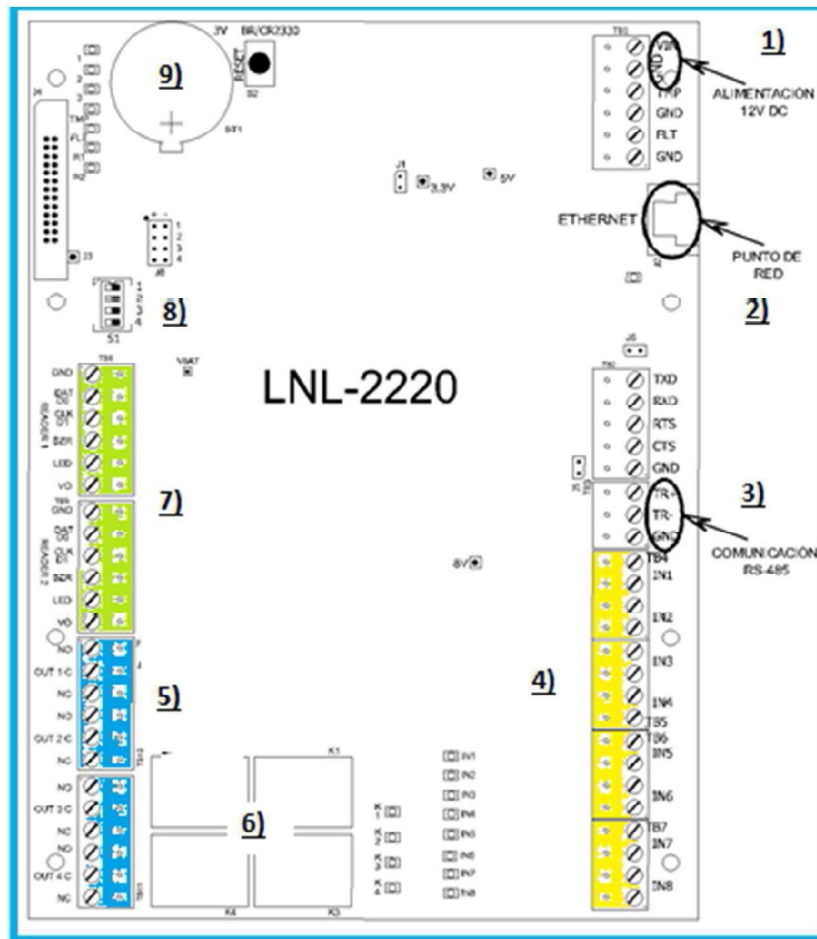


Figura 2. 50 Tarjeta LNL-2220

- 1) Bornera de alimentación a 12 VDC (VIN - GND) y borneras de detección de apertura del gabinete (FLT - GND).
- 2) El puerto de red Ethernet de comunicación.
- 3) Borneras de comunicación RS-485 dedicado para la conexión con tarjetas esclavas.
- 4) Todas las borneras marcadas en amarillo son 8 entradas digitales a dos hilos desde IN1 a IN8.
- 5) Todas las borneras marcadas en azul son las salidas de contactos normalmente cerrados y abiertos así como los respectivos comunes de los 4 relés que se tiene en esta tarjeta; desde OUT1 hasta OUT 4.
- 6) Conjunto de 4 relés de control; 1 y 3 principales, 2 y 4 secundarios auxiliares.
- 7) Todas las borneras marcadas en verde son las dos entradas de lectora que posee esta tarjeta; cada entrada de lectora tiene una bornera para VCC, una

- para GND, una para DATA 0, una para DATA 1, una para LED (opcional) y una para un zumbador (opcional).
- 8) Dip switch de 4 estados para realizar un hard reset en caso de falla de la memoria.
 - 9) Batería tipo botón de 3VDC de respaldo de energía de la memoria de la tarjeta.

2.2.3.16 Tarjeta electrónica esclava LNL-1320

Este tipo de tarjeta electrónica se usa para realizar las acciones de control, ya que a diferencia de la LNL-2220, ésta no posee puerto de red y se administra a través de la controladora maestra.

Al igual que su maestra esta tarjeta permite el manejo de 8 diferentes formatos de tarjetas electrónicas y la detección de la apertura del panel de control de accesos.

A continuación se detallan las partes más relevantes para su uso.

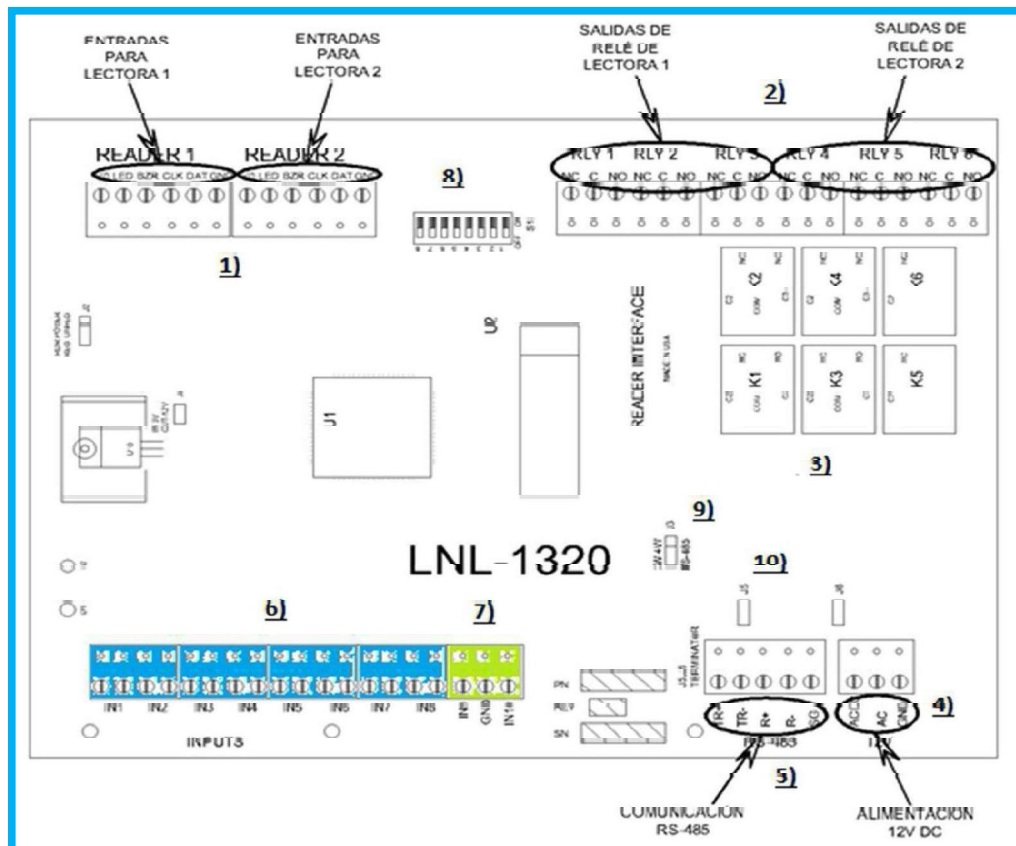


Figura 2. 51 Tarjeta LNL – 1320

- 1) Entradas dedicadas para dos lectoras con distribución individual de pines (Vo, GND, DATA 0, CLK, BZR y LED).
- 2) Salidas de contactos normalmente abiertos, cerradas y los respectivos comunes de los 6 relés presentes en esta tarjeta.
- 3) 6 relés de control montados en la placa; 1 y 4 principales, 2 y 5 auxiliares secundarios, 3 y 6 reservados para usos especiales.
- 4) Bornera de alimentación 12 ó 24 VDC (VIN – GND).
- 5) Borneras de comunicación RS-485 a dos o 4 hilos (TR+, TR-, R+, R- y SG).
- 6) Todas las borneras marcadas en azul son entradas digitales a dos hilos desde IN1 a IN8.
- 7) Borneras dedicadas a la detección de apertura del gabinete (TMP, GND).
- 8) Dip switch de 8 estados para configurar la dirección de la tarjeta.
- 9) J3 (JUMPER 3) puente dedicado a la selección del formato de comunicación RS-485 si se desea a dos o 4 hilos.
- 10) J5 (JUMPER 5) puente dedicado para dar inicio o fin a la cadena de comunicación RS – 485 entre maestra y esclavas.

2.2.3.17 Tarjeta electrónica puente LNL-500B

Esta tarjeta se ubica en los lugares cercanos donde se controla lectores de geometría de mano, ya que esta tarjeta está diseñada y dedicada exclusivamente para realizar la integración de esos equipos con el resto del sistema.

Su alimentación es de 12VDC y cada una de ellas soporta hasta 8 lectores biométricos. Posee 3 puertos de comunicación RS-485 uno está dedicado a la comunicación en la cadena RS-485 formada por las tarjetas LNL-1320 y la maestra LNL-2220, mientras que los otros dos puertos RS-485 están dedicados para las comunicaciones con 4 lectores de geometría de mano cada uno, de manera que se puede usar la saturación de los dos puertos como se requiera sin un orden en específico.

A continuación se detallan sus partes más relevantes.

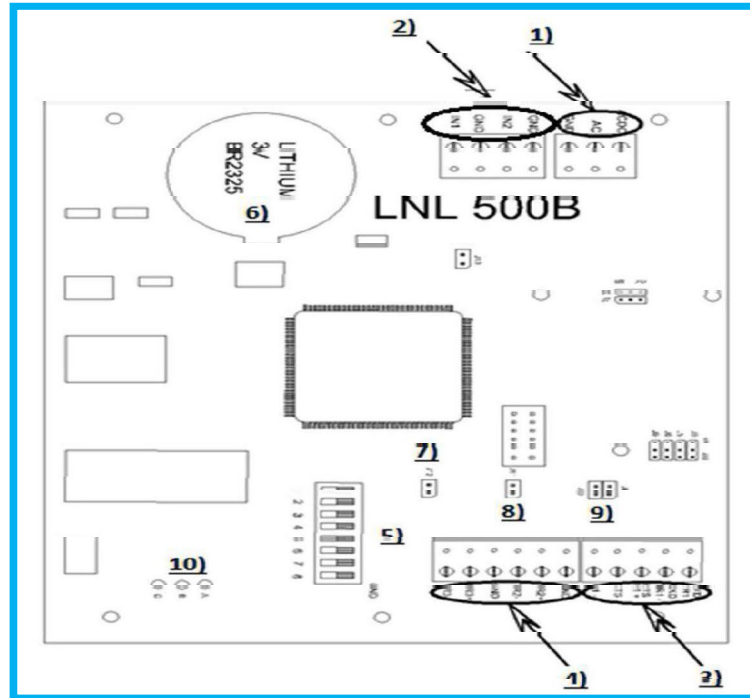


Figura 2. 52 Tarjeta LNL-500B

- 1) Borneras de alimentación a 12VDC.
- 2) Borneras de entradas auxiliares (IN1 – GND, IN2 – GND).
- 3) Borneras de comunicación RS-485 a dos o cuatro hilos a la red de la controladora maestra.
- 4) Borneras de comunicación RS-485 a dos hilos; puerto 2 y puerto 3 con capacidad individual de hasta 4 dispositivos biométricos.
- 5) Dip switch de 8 estados para direccionamiento de la tarjeta.
- 6) Batería tipo botón de 3V para respaldo de alimentación de la memoria montada en la tarjeta.
- 7) J12 (JUMPER 12) puente dedicado para inicializar o finalizar la red de comunicación RS-485 asociada al puerto 3 de biométricos.
- 8) J11 (JUMPER 11) puente dedicado para inicializar o finalizar la red de comunicación RS-485 asociada al puerto 2 de biométricos.
- 9) J9 y J10 (JUMPER 9,10) puentes dedicado para inicializar o finalizar la red de comunicaciones RS-485 proveniente de la controladora maestra a la tarjeta.

2.2.3.18 Fuente electrónica de 24 VDC @ 2.5A

Esta fuente se encuentra en los tableros donde se requiere la presencia de 24VDC como en el caso de la garita vehicular, ya que desde el tablero de esta ubicación se alimentan las lectoras vehiculares cuyos parámetros técnicos requieren de este voltaje o en el caso de la garita peatonal donde las luces indicadoras de los handkeys se alimentan a 24 VDC.

2.2.4 DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE CONTROL DE ACCESOS EN LAS ÁREAS DISEÑADAS

Debido a que en las áreas que se tienen que implementar el sistema de control se tienen casos diferentes de conexiones se indica por cada locación las diferentes conexiones e implementaciones.

2.2.4.1 Diseño de diagramas de conexión del sistema de control de accesos en la garita peatonal

En la garita peatonal como primer elemento de control se instalan el juego de torniquetes, dos dobles y un simple, complementados con la puerta motorizada para personas con capacidades especiales; en cada uno de los ingresos y salidas de los torniquetes y de la puerta motorizada se instalan sus correspondientes lectoras de proximidad de forma que en este límite inicial se tiene 12 lectoras de proximidad.

Después del primer límite físico se distribuyen 6 handkeys con sus respectivas luces indicadoras en los postes destinados para este objetivo, de forma que el personal que pase por los torniquetes registre su ingreso en este punto.

Para el control y alimentación de los diferentes equipos en esta ubicación se necesita 3 tableros electrónicos:

- El primero contiene la tarjeta controladora LNL-2220, 5 tarjetas esclavas LNL – 1320, la fuente de 12VDC @ 6A con su expansora y una fuente de 24VDC.

En cada una de las entradas de lectora de las cinco LNL-1320 presentes se conectan las 10 lectoras correspondientes a los torniquetes, y de la misma forma a las salidas de relé principales (relé 1 y relé 4) de cada una de las tarjetas se

conectan con el cableado disponible proveniente de las borneras de control de los mismos torniquetes.

- El segundo contiene 2 tarjetas esclavas LNL-1320, la fuente de 12VDC @ 6A con su expansora y una fuente adicional de 24 VDC.

En la primera LNL-1320 se conectan el cableado correspondiente a las lectoras de proximidad de entrada y salida de la puerta de discapacitados y también el cableado de control de este equipo.

En la segunda LNL-1320 se conectan dos de los 6 handkeys de esta ubicación con sus correspondientes luces indicadoras conectadas a las salidas de relé principales (relé 1 y relé 4).

- El tercero contiene 2 tarjetas esclavas LNL-1320, una tarjeta puente LNL-500B, la fuente de 12 VDC @ 6A con su expansora y una fuente adicional de 24 VDC.

En la primera y en la segunda LNL-1320 se conectan los 4 handkeys restantes a las entradas de lectora y sus luces indicadoras a las salidas de relé correspondientes.

A la LNL-500B se conecta el cableado de la comunicación RS-485 proveniente de los handkeys procurando que se controlen 3 equipos por cada puerto y también se conecta la comunicación RS-485 que vincula a esta tarjeta con la red de esclavas de la LNL – 2220 presente en el primer tablero.

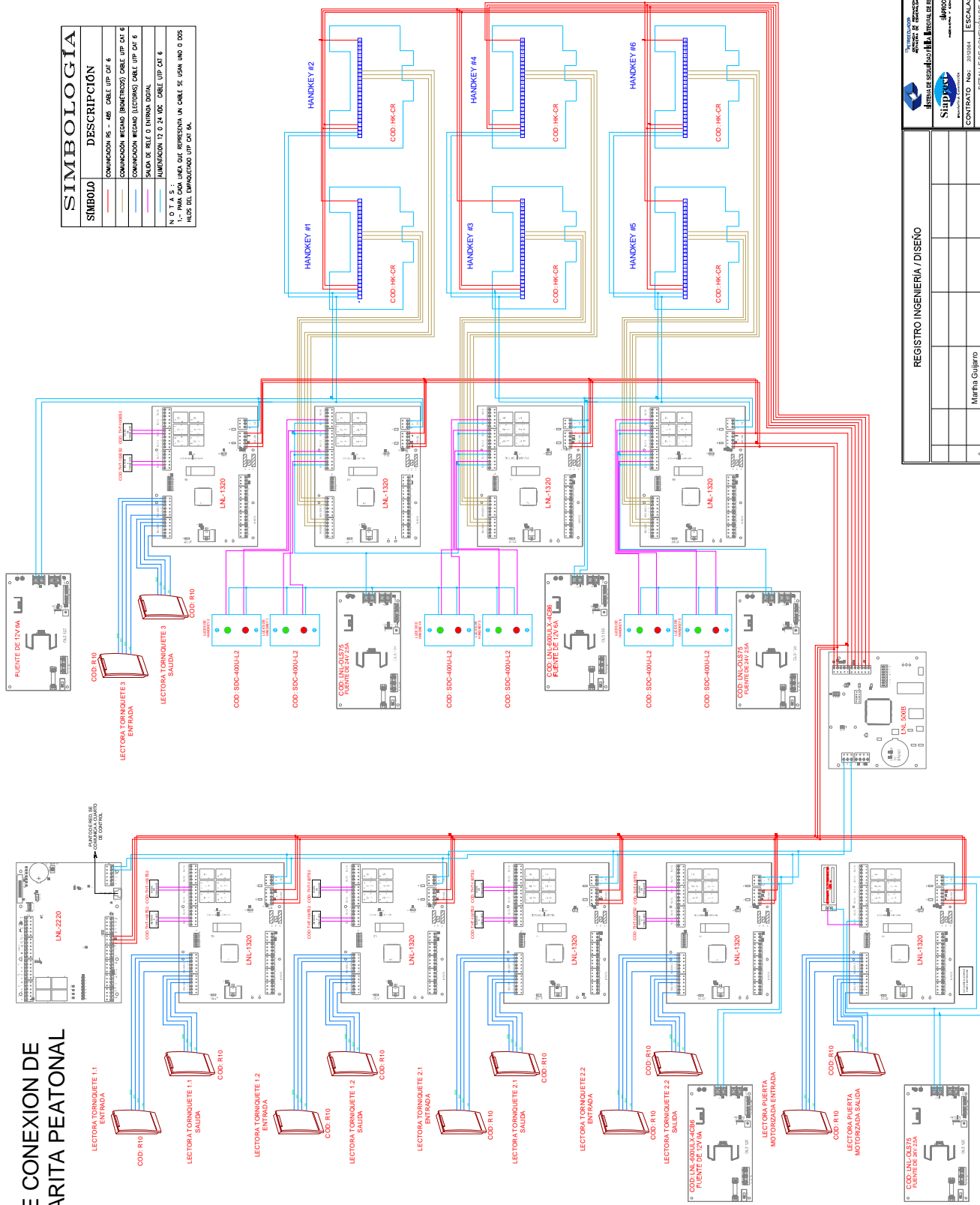
En el plano CIV -200 se presenta la vista superior del área diseñada.

En el plano EE-601 se detallan las conexiones del subsistema en esta ubicación.

DETALLE DE CONEXION DE ACCESOS GARITA PEATONAL

SIMBOLOGIA	
SIMBOLO	DESCRIPCION
	COMUNICACION RS - 485 CABLE UTP CAT 6
	COMUNICACION MEDIO (DIFERENTES) CABLE UTP CAT 6
	COMUNICACION MEDIO (MISMO TIPO) CABLE UTP CAT 6
	ALIMENTACION 12 O 24 VDC CABLE UTP CAT 6
	ALIMENTACION 12 O 24 VDC CABLE UTP CAT 6

N O T A S :
 1. PARA MAS INFORMACION VER CABLE DE USUARIO UNO O DOS.
 2. PARA MAS INFORMACION VER CABLE DE USUARIO UNO O DOS.
 3. PARA MAS INFORMACION VER CABLE DE USUARIO UNO O DOS.



REGISTRO INGENIERIA / DISEÑO						
REV.	FECHA	DISEÑADO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Miriam Quijero Andrés Cajo				

INSTITUCION: INSTITUCION VENEZOLANA DE INVESTIGACIONES CIENTIFICAS Y TECNOLOGICAS AREA: INVESTIGACION Y DESARROLLO DEPARTAMENTO: INVESTIGACION Y DESARROLLO PROYECTO: INVESTIGACION Y DESARROLLO	CONTRATO No.: 202004 ESCALA: 1:1 DETALLE DE CONEXION DE ACCESOS
REVISION: 000 PLANO No.: EE-607	ESCALAS: 1:1 REVISION: 000

2.2.4.2 Diseño de diagramas de conexión del sistema de control de accesos en la garita vehicular

En la garita vehicular se instalan 4 barreras vehiculares con sus respectivos accesorios de manera que en los 4 carriles de flujo vehicular que se tiene en este ingreso estén controlados; asociados a las barreras vehiculares se instalan 4 lectoras vehiculares de largo alcance en postes, estratégicamente ubicadas y direccionadas para la correcta lectura de los booster instalados en los automóviles pre-registrados.

Entre la garita de guardias y las barreras vehiculares se tiene un punto de ingreso peatonal para el ingreso de contratistas y acompañantes de los conductores, de manera que este punto está controlado por el molinete con sus 2 lectoras de ingreso y salida asociadas. El personal de planta que ingrese por el molinete debe registrar su asistencia en cualquiera de los dos biométricos instalados en la pared lateral de la garita, mientras que los contratistas deben registrar su ingreso en el lector biométrico instalado en esta ubicación.

Para el control y alimentación de los equipos de esta ubicación se requieren de 2 tableros electrónicos:

- El primero contiene la tarjeta controladora LNL-2220, dos tarjetas esclavas LNL-1320, la fuente de alimentación de 12VDC @ 6 A con su expansora de salidas y una fuente adicional de 24 VDC.

En las entradas de lectora de la LNL-2220 y de la primera LNL-1320 se conecta el cableado asociado a cada una de las lectoras vehiculares montadas en campo y desde la fuente de 24VDC se implementa la alimentación de dos de estos equipos. Así mismo se conecta el cableado de control de las 4 barreras vehiculares a las salidas de relé principal de las dos tarjetas indicadas (Relé 1 y Relé 4).

En la segunda LNL-1320 se conecta el cableado asociado a las lectoras de entrada y salida del molinete así como su cableado de control a los relés principales 1 y 4.

- El segundo contiene dos tarjetas LNL-1320, una LNL-500B, la fuente de 12VDC @ 6 A con su expansora de salidas y una fuente adicional de 24 VDC.

En las entradas de lectora de la primera LNL-1320 se conecta el cableado asociado a los dos handkeys instalados en campo.

En la segunda LNL-1320 se conecta el cableado proveniente del biométrico. Mientras que en la LNL-500B se conecta el cableado de RS-485 asociado a los dos handkeys en el puerto 2; desde el puerto 1 se realiza la conexión de la red RS-485 de esclavos asociada a la LNL-2220 presente en el primer tablero.

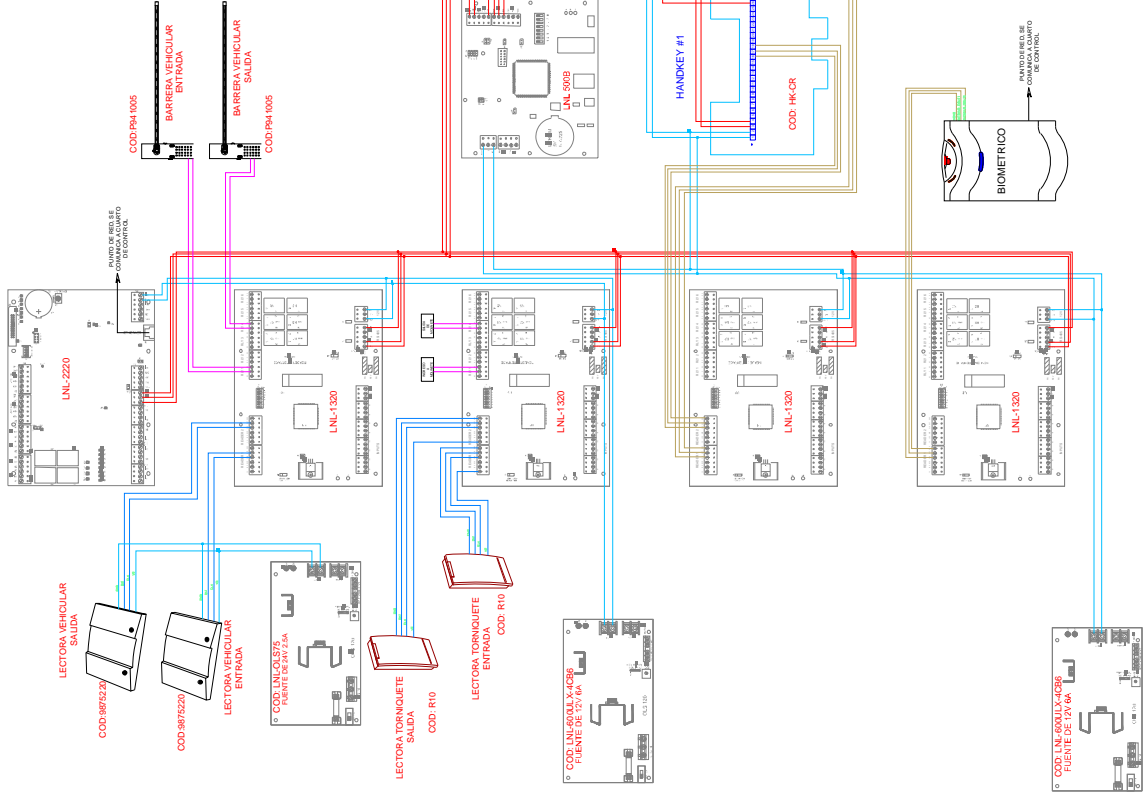
En el plano EE-600 se detalla la implementación de las conexiones de esta ubicación.

En el plano EE-500 se presenta la implementación de los equipos en la arquitectura de esta locación.

En el plano EE-501 se presenta el detalle de la vista frontal de la implementación de los equipos.

En el plano EE-502 se presenta el detalle de la vista lateral de la implementación de los equipos.

DETALLE DE CONEXION DE ACCESOS GARITA VEHICULAR



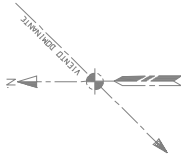
SIMBOLOGIA	
SIMBOLO	DESCRIPCION
	COMUNICACION RS - 485 CABLE UTP CAT 6
	COMUNICACION WEGAND (BIOMETRICO) CABLE UTP CAT 6
	COMUNICACION WEGAND (LECTORAS) CABLE UTP CAT 6
	SALIDA DE RELE O ENTRADA DIGITAL
	ALIMENTACION 12 O 24 VDC. CABLE UTP CAT 6

NOTAS:
 1.- PARA CADA LINEA QUE REPRESENTA UN CABLE SE USAN UNO O DOS HILOS DEL EMPAREJADO UTP CAT 6A.

REGISTRO INGENIERIA / DISEÑO	
MARIO GUJARRERO ASESOR C.A.P.	REVISADO
REV. FECHA	APROBADO
DISEÑADO	FISCALIZADOR
COORDINADOR	PLANO No.: EE-600
REVISION: 000	DETALLE DE CONEXION DE ACCESOS
ESCALA:	No.
CONTRATO No.: 202004	VERSION: 0

IMPLANTACIÓN GARITA VEHICULAR

(1:100)



CALLE DE HORMIGÓN
f_c = 210 kg/cm² EXISTENTE

ÁREA DE PARQUEADERO DE VEHÍCULOS
DE REFINERÍA Y VISITANTES

SIMBOLOGÍA

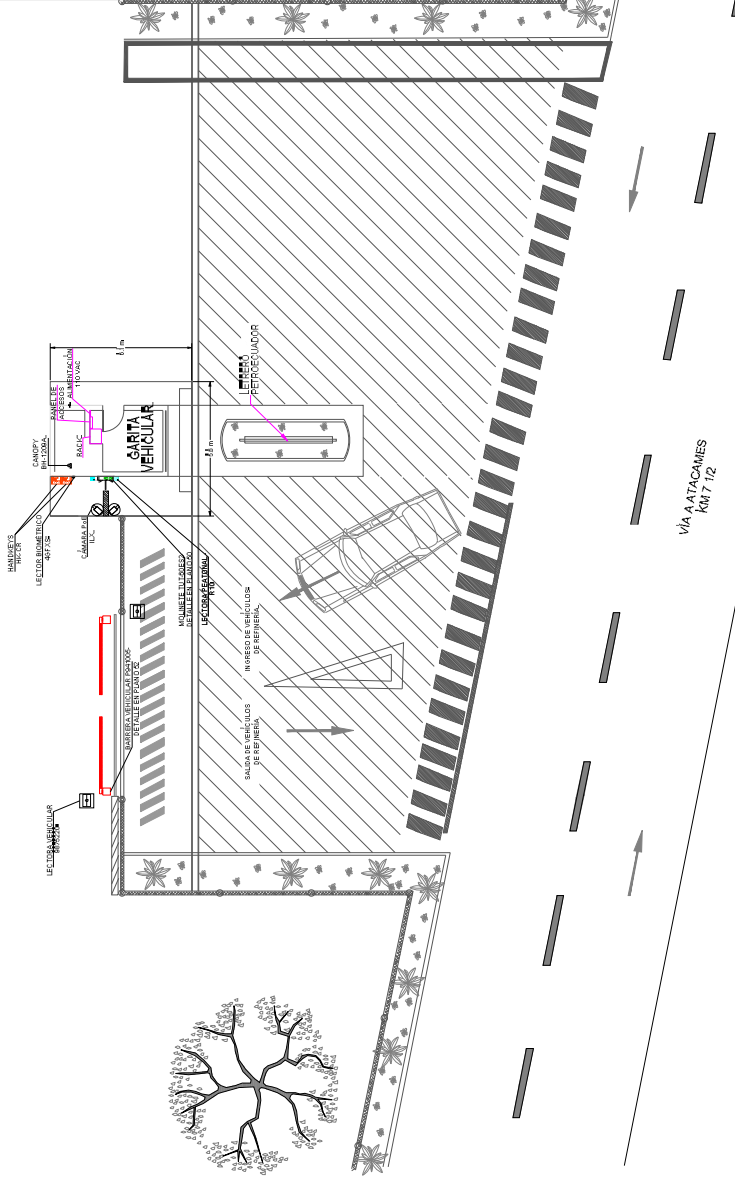
	MOLINETE TUBERÍA
	HANDRAIL/HELICAR
	LECTOR BIOMÉTRICO CASAS
	ANTENA CARPUSY RF/UBAL
	BARRERA VEHICULAR PASADIZO
	LECTURA VEHICULAR 80/520
	CÁMARA PÉLUX
	LECTOR PLANTANAL RÍO
	INDICA TUBERÍA DESBIDE
	INDICA TUBERÍA ASERIE

NOTAS:

1) MEDIDAS DE REFERENCIA
N.E.C. 2011
A.C.I. 318. 2011
A.S.T.M. A01

2) TODAS LAS MEDIDAS ESTÁN DADAS EN METROS.

ÁREA DE PARQUEADERO
PARA VEHÍCULOS Y BUSES

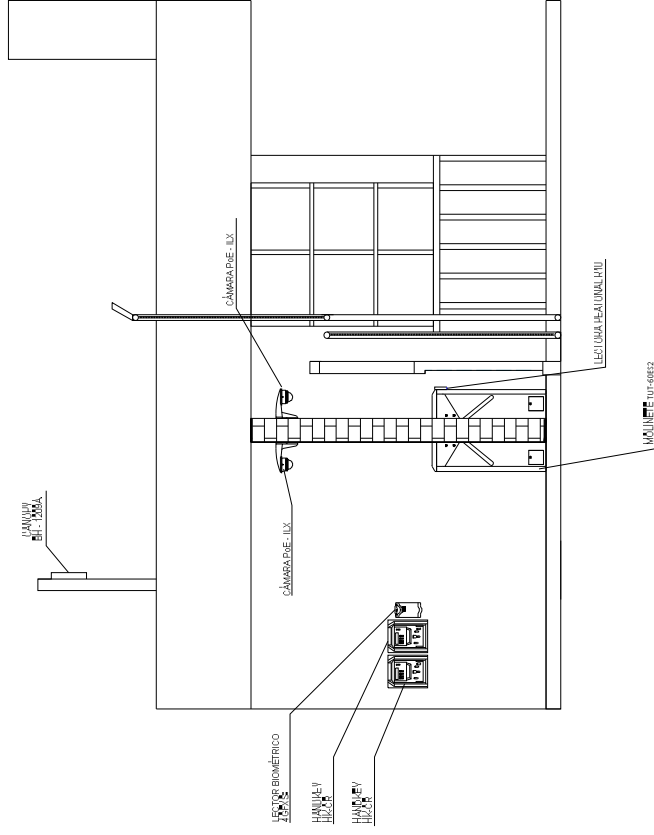


REGISTRO INGENIERÍA / DISEÑO

SISTEMA DE SEGURIDAD FÍSICA INTEGRAL DE REFINERÍA EMERALDAS	
CONTRATO N°:	2012084
ESCALA:	1:100
GARITA VEHICULAR - PLOT PLAN	
PLANO N°:	EE-500
REVISIÓN:	000


REV.	FECHA	DISEÑO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Martha Cujarín Andrés Ceip				

DETALLE GARITA VEHICULAR - VISTA LATERAL
(1/20)



NOTAS:
 1) NÚMERO DE INGENIERÍA: N.E. - 2011
 A.O. - 2011
 2) TODAS LAS MEDIDAS ESTÁN DADAS EN METROS.




SIA PROCI
 Ingenieros y Constructores

EMPRESA DE INGENIERÍA Y CONSTRUCCIÓN
SISTEMA DE SEGURIDAD FÍSICA INTEGRAL DE REFINERÍA ESMERALDAS

CONTRATO No.: 2012004 ESCALA: 1:20
 GARITA VEHICULAR - VISTA LATERAL

PLANO No.: EE-502 REVISIÓN: 000

REGISTRO INGENIERÍA / DISEÑO						
REV.	FECHA	DISEÑADO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Martha Cujigans Andrés Ceja				

2.2.4.3 Diseño de diagramas de conexión del sistema de control de accesos en la sala de control de procesos (Bunker)

En esta ubicación se controlará el acceso por la puerta principal, de este modo se instala en el marco y en la batiente una cerradura electromagnética. Se instalan también dos contactos magnéticos para monitorear la apertura y cierre de la puerta, así como el par de lectoras de proximidad instaladas en la entrada y en la salida.

Para el control y alimentación de los equipos de esta locación se requiere de un solo tablero electrónico.

En el interior de este se monta una tarjeta controladora LNL-2220, una esclava LNL-1320 y la fuente de poder de 12VDC @ 6 A con su expansora de salidas.

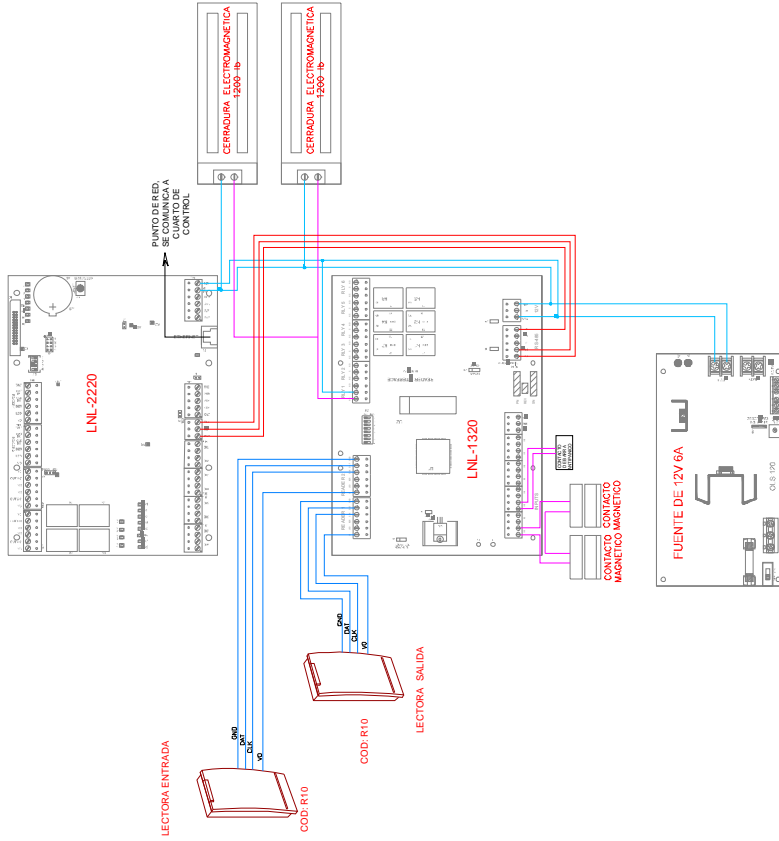
A las entradas dedicadas de lectora de la LNL-1320 se conecta el cableado asociado a las dos lectoras de proximidad.

En las salidas de relé principal (RLY 1 y RLY 4) de la misma tarjeta esclava, se conecta el cableado de control de la cerradura electromagnética asociando esto a la alimentación de 12VDC que requiere este equipo.

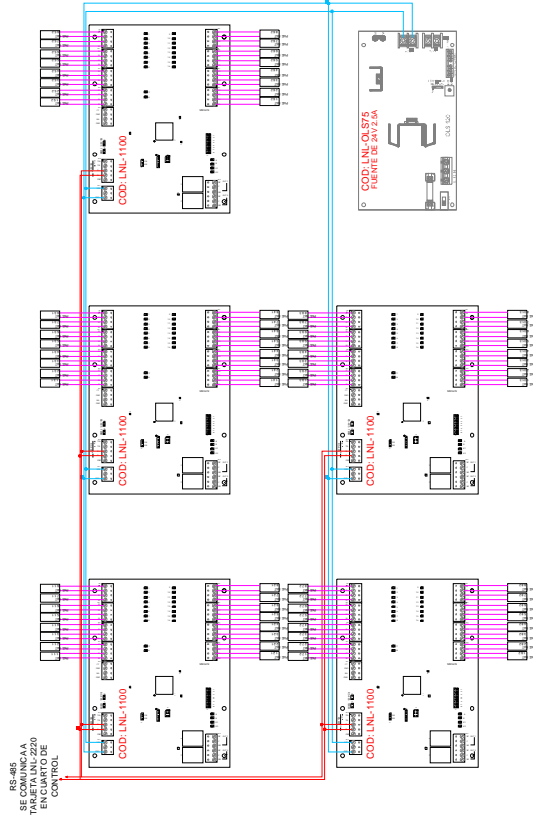
Los contactos magnéticos se conectan entre sí en serie y el par de cables resultante se conecta en la entrada digital IN1 de la LNL-1320.

En el plano EE-602 se detallan las conexiones electrónicas del subsistema en esta ubicación.

DETALLE DE CONEXION DE ACCESOS INGRESO SALA DE CONTROL



DETALLE DE INTEGRACIÓN DE ACCESOS CON SALIDAS DE SEÑAL DEL SIST. PERIMETRAL



SIMBOLOGÍA

SÍMBOLO	DESCRIPCIÓN
(Red line)	COMUNICACION RS - 485 CABLE UTP CAT 6
(Blue line)	COMUNICACION WEGAND (BRONATRICOS) CABLE UTP CAT 6
(Green line)	COMUNICACION WEGAND (LECTORIAS) CABLE UTP CAT 6
(Yellow line)	SEÑAL DE SELE O ENTRADA DIGITAL
(Purple line)	ALIMENTACION 12 O 24 VDC. CABLE UTP CAT 6
(Black line)	N O T.A.S

N O T.A.S
 LA LINEA QUE REPRESENTA UN CABLE SE USAN UNO O DOS
 HUELOS DEL EMPAREJADO UTP CAT 6A.

REGISTRO INGENIERIA / DISEÑO	
REV.	FECHA
DESIGNADO	APROBADO
REVISADO	FISCALIZADOR
COORDINADOR	PLANO No: EE-602
REVISION:	000

INSTITUCION DIVISION DE INGENIERIA DIVISION DE INGENIERIA Y CONSTRUCCION	INSTITUCION DIVISION DE INGENIERIA Y CONSTRUCCION
CONTRATO No: 200804	ESCALA:
DETALLE DE CONEXION DE ACCESOS	No:

2.3 DISEÑO DE LAS REDES DEL SUBSISTEMA DE SEGURIDAD PERIMETRAL

En base al previo diseño conceptual efectuado usando como base la tecnología del cable sensor, la fiscalización realizó su propio análisis y propuso varias alternativas que a su criterio podrían solucionar de una mejor forma el problema de seguridad en el perímetro. Las propuestas fueron las siguientes:

- Detección de intrusos usando lazos de piso.
- Instalación de alambrado eléctrico.
- Detección por cable telefónico.

Las tres alternativas tienen sus ventajas y desventajas en comparación del sistema propuesto; por ejemplo en el caso de los lazos de piso su funcionamiento básicamente se enfoca en detectar vibraciones del suelo cercano a la malla producto de pisadas, pero su instalación representaría un costo elevadísimo ya que la obra civil necesaria es de gran magnitud y dificultad.

En el caso de la instalación de alambrado eléctrico se tiene que el costo de instalación es relativamente bajo en comparación del sistema propuesto pero tiene varias debilidades, las más importantes son que no tiene la capacidad de integrarse al conjunto de subsistemas de seguridad, con lo que no se tiene una verdadera automatización del monitoreo que es lo que busca el cliente y que puede llegar a ser bastante vulnerable e ineficiente impidiendo intrusiones por partes rotas de la malla. El cable telefónico tiene características muy similares al sistema propuesto pero su aplicabilidad en condiciones ambientales como las que se tiene en el caso presente hacen de este un sistema poco preciso y con un costo ligeramente elevado en comparación ya que su alcance es menor y se requiere de más cable para cubrir el recorrido total del perímetro.

Se escoge este tipo de sistema gracias a que el factor costo – beneficio es agradable al cliente, es de fácil instalación y posee la capacidad para integrarse con sistemas de CCTV y control de accesos.

El sistema de detección por sensores de vibración se ubica alrededor de todo el perímetro de refinería para solucionar el problema de posibles intrusiones.

Para el funcionamiento de este sistema se cuenta con las siguientes partes fundamentales que son: la unidad interfaz de control IA-6500, que recibe y retransmite señales del campo hacia el servidor ubicado en el Data center, las unidades controladoras analizadoras de campo SPU-2004, y los sensores de vibración los que ante movimiento o intento de intrusión sobre la malla emiten una señal eléctrica que se traduce en una alarma.

El cable así como sus sensores deben estar fijamente sujetos a la malla para evitar que estos se balanceen por el viento. A pesar de que este sistema está recomendado para usarse en cualquier tipo de terreno, necesita que la malla esté totalmente libre de cualquier objeto extraño, como la maleza o ramas de árboles, ya que el movimiento o presión de estas sobre la malla puede producir falsas alarmas. El número de unidades controladoras SPU, llamada también transponder, se basa en la longitud del perímetro de refinería. Para compensar posibles falsas alarmas en caso de que el ambiente se torne tormentoso o lluvioso se tiene la unidad de compensación meteorológica instalada en campo.

La comunicación de las unidades controladoras SPU hacia el IA-6500, es mediante RS-485, que tiene un alcance máximo de 1200 m, permitiendo así que el sistema cubra todo el perímetro de la refinería.

2.3.1 DISEÑO DEL SUBSISTEMA POR ZONAS DE COBERTURA

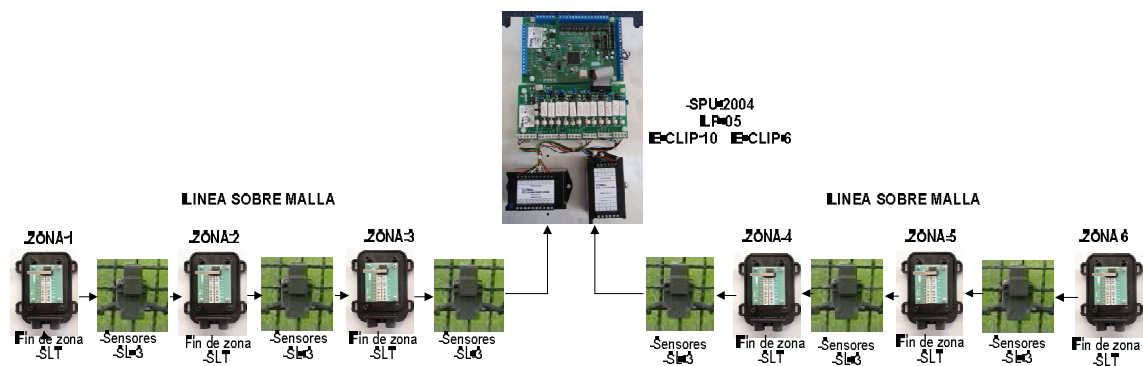


Figura 2. 53 Diagrama general de cableado perimetral

El cableado perimetral que cubre todo el perímetro de refinería sobre las mallas y puertas de doble o simple batiente que la limitan. Se compone de 10 Unidades de procesamiento inteligente cada una con una capacidad usada de 6 zonas (600 metros de cobertura), esto para evitar el uso total de su capacidad máxima de 800 m y así evitar posibles imprecisiones o que el sistema se vuelva lento.

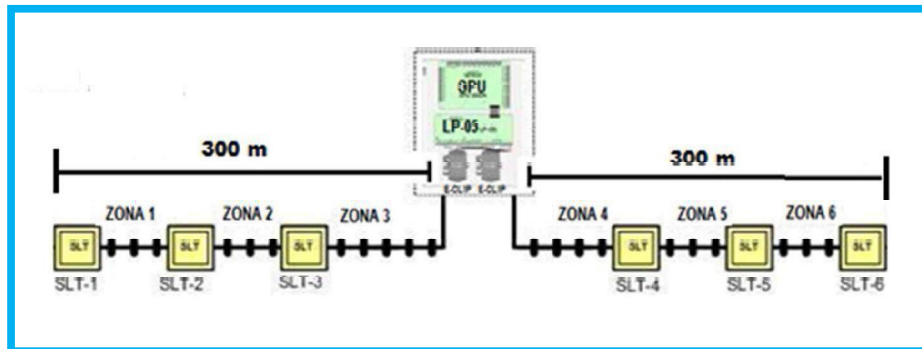


Figura 2. 54 Cobertura usada 600m lineales

El perímetro total a cubrir es de 5640m, aproximado a 6000m, por lo que conociendo las especificaciones de los equipos utilizados se requiere de 10 tarjetas de procesamiento inteligente (SPU-2004) para resguardar el perímetro existente, de acuerdo a lo siguiente:

Perímetro a cubrir = 5640m aproximadamente.

Capacidad utilizada por transponder (SPU-2004)= 600m

Unidades inteligentes a usar= $5640/600=9.4$

De lo anterior se ve que lo adecuado es usar 10 transponders. La alimentación para cada transponder es de 24 VAC que se toma de la UPS del poste más cercano que también alimenta a las cámaras PTZ.

A más de la visualización del mapa del sitio mediante software Vidalert en el computador cliente, el sistema de cableado perimetral se integra también con el software OnGuard, con el que se maneja los anteriores sistemas, mediante las tarjetas expansoras propias del sistema y las tarjetas LNL-1100 que tienen 16 entradas dedicadas a la recepción de señales de tipo digital.

De esta manera se observan las alarmas y eventos del sistema de cableado perimetral en su propio software y en el software OnGuard.

2.3.2 CARACTERÍSTICAS TÉCNICAS DE EQUIPOS

Tabla 2. 31 Características básicas del cale sensor

CABLE 6C Y SENSOR DE VIBRACIÓN	
Marca	RBTEC
Modelo	MDS - 2
Alimentación	15 VDC provisto desde la SPU-2004 respectiva.
Comunicación	NO

Tabla 2. 32 Características básicas del cable de comunicaciones

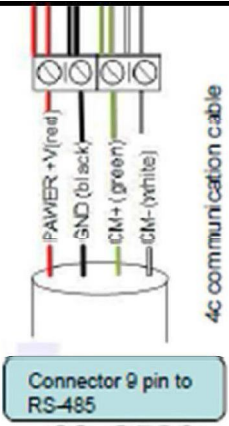
CABLE DE DATOS Y ENERGÍA	
Marca	RBTEC
Modelo	RB - 4C
Alimentación	15VDC
Comunicación	RS - 485

Tabla 2. 33 Características básicas del extensor de RS-485


EXTENSOR DE COMUNICACIÓN RS - 485	
Marca	DETO
Modelo	3345A
Alimentación	12 VDC
Comunicación	RS - 485

Tabla 2. 34 Características básicas de la SPU

UNIDAD DE PROCESAMIENTO INTELIGENTE	
Marca	RBTEC
Modelo	SPU - 2004
Alimentación	24 VAC
Voltaje de salida	15 VDC
Consumo de corriente	35 mA
Capacidad de usuarios	512 usuarios, ampliable a 32.512 usuarios
Comunicación	RS-485, RS-232 Serial o comunicaciones de red.

Tabla 2. 35 Características básicas de la terminación de zona


TERMINACIÓN DE ZONA	
Marca	RBTEC
Modelo	RB – SLT1
Alimentación	NO
Comunicación	NO

Tabla 2. 36 Características básicas de la tarjeta de protección contra descargas eléctricas

TARJETA DE PROTECCIÓN CONTRA DESCARGAS ELÉCTRICAS	
Marca	RBTEC
Modelo	LP-05
Alimentación	Conectado a SPU-2004
Comunicación	RS-485 con módulo SPU - 2004

Tabla 2. 37 Características básicas de la unidad interfaz de control


UNIDAD INTERFAZ DE CONTROL	
Marca	RBTEC
Modelo	IA - 6500
Alimentación	110 VAC
Comunicación	RS-485, RS-232 Serial o comunicaciones de red.

Tabla 2. 38 Características básicas de la unidad supresora de descargas eléctricas

UNIDAD SUPRESORA DE DESCARGAS ELÉCTRICAS	
Marca	RBTEC
Modelo	E-CLIP 6 y E-CLIP 10
Alimentación	Conectado a LP - 05
Voltaje de operación	5V DC
Comunicación	RS-485

Tabla 2. 39 Características básicas de la unidad meteorológica

UNIDAD METEOROLÓGICA	
Marca	RBTEC
Modelo	VX - 25
Alimentación	Conectado a LP - 05
Voltaje de operación	15V DC desde el módulo SPU - 2004
Comunicación	RS-485

2.3.3 DESCRIPCIÓN DE LOS EQUIPOS DE CABLEADO PERIMETRAL.

2.3.3.1 Cable sensor de vibración – 6C

Este cable se compone internamente de 8 conductores de cobre, 6 de estos se usan para la zonificación (rojo, café, verde, azul y negro – GND), el blanco es de reserva y el desnudo es el cable de aterrizaje hacia el chasis.

Pre instalados de fábrica se tienen los sensores de vibración de manera que cada uno de sus contactos electro platinados están asociados a las zonas que representan cada hilo conductor.

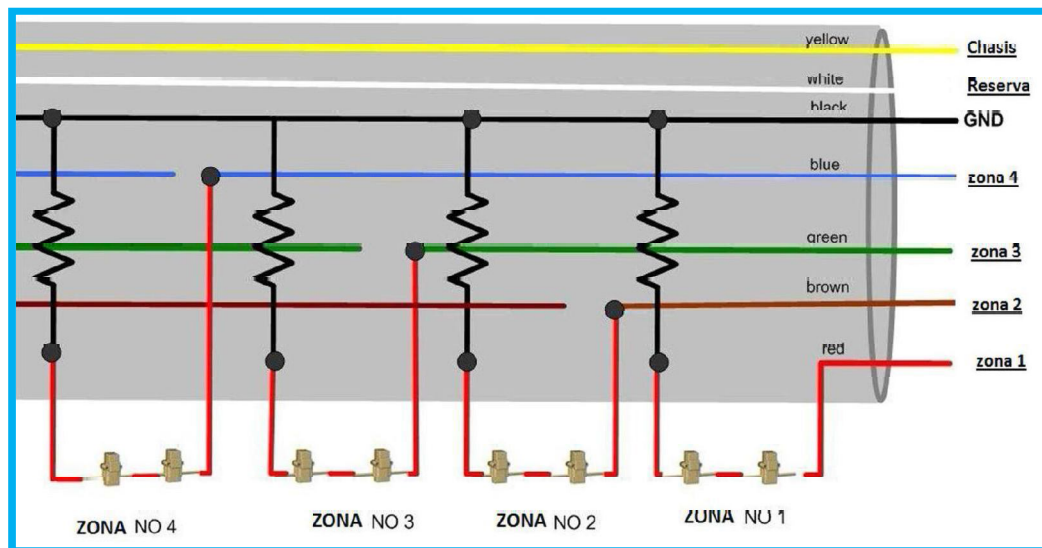


Figura 2. 55 Distribución interna de cable sensor

2.3.3.2 Cable de datos y energía RB – 4C

Es el cable que se usa para comunicar las unidades de campo SPU entre sí y hacia la unidad de respaldo en el Data center. Internamente se compone de 5 conductores, 3 de ellos están designados para la comunicación RS-485 a dos hilos (TR+, TR- y GND), mientras que los 2 restantes son para el voltaje DC, pero en este caso este par no se usa debido a que por la gran distancia del perímetro a cubrir las caídas de tensión sobrepasan el 20% y se puede tener fallas en los equipos.

La alimentación se hace desde el UPS en poste más cercano a la unidad presente en campo.

2.3.3.3 Extensor de comunicación RS-485

Este equipo se usa para extender la capacidad de cobertura en distancia de la comunicación RS-485 proporcionada por la unidad de respaldo, debido a que desde el data center se abren dos brazos de comunicación hacia cada lado del perímetro para rodearlo, pero en cada lado se debe cubrir una distancia de 3000 metros aproximadamente y como el estándar indica la comunicación RS-485 tiene un límite de 1200 metros, el uso de este equipo es totalmente necesario.

Posee una entrada DB – 9 y una salida con realimentación ayudando así a que la señal mantenga sus características y sus niveles de voltaje.

2.3.3.4 Terminación de zona

Este equipo es básicamente una tarjeta de 16 borneras y 5 puentes preinstalada dentro de una pequeña caja plástica diseñada para su uso en intemperie, en ella se hacen las conexiones entre zonas y se colocan las resistencias de fin de zona.

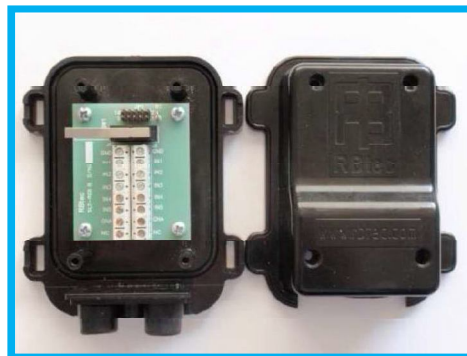


Figura 2. 56 Terminación de zona

2.3.3.5 Unidad inteligente SPU-2004

Es la tarjeta más importante que se encuentra en campo. Su función principal es recibir y convertir la señales emitidas en los sensores para enviarlas vía RS-485 a la unidad de respaldo en el data center. Su alimentación es de 24VAC desde el UPS más cercano montado en poste, el que a su vez alimenta el sistema de transmisión de datos inalámbricos y el funcionamiento de la cámara de perímetro PTZ presente.

A continuación se detallan las partes más importantes para su uso.

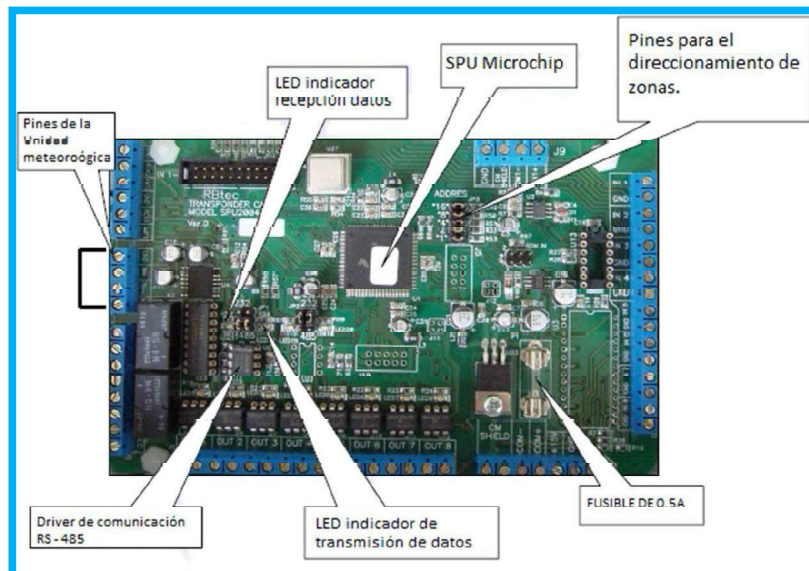


Figura 2. 57 SPU-2004

2.3.3.6 Tarjeta de protección contra descargas eléctricas

Esta tarjeta tiene como objetivo proteger la tarjeta SPU limitando posibles sobre voltajes en las borneras de entrada, en su configuración posee varias resistencias de potencia, varistores y diodos.

A continuación se detalla sus partes más importantes

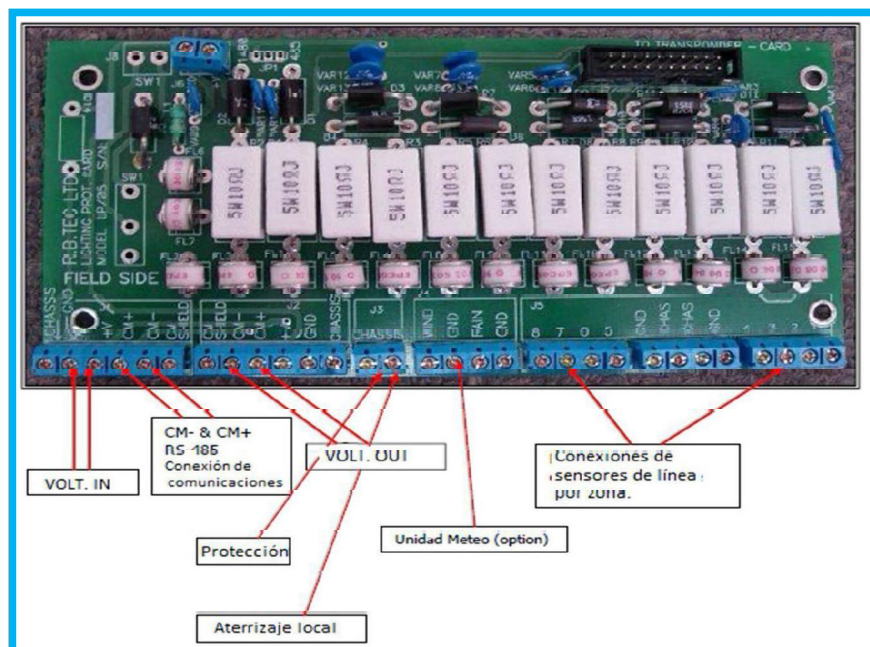


Figura 2. 58 Tarjeta supresora de descargas LP-05

2.3.3.7 Unidad supresora de descargas eléctricas (E-CLIP)

Este equipo es el primer elemento de protección de la SPU antes de la tarjeta LP-05, a este equipo se conectan directamente los diferentes hilos conductores provenientes del cable sensor instalado en campo y se usa como protección adicional con la anterior tarjeta descrita.

En el lado no protegido se conectan las zonas y en el lado protegido se conecta el cableado de enlace con la tarjeta LP-05.



Figura 2. 59 Unidad de protección E-CLIP

2.3.3.8 Unidad meteorológica VX-25

Debido a la sensibilidad de los sensores montados sobre la malla perimetral, se pueden producir falsas alarmas debido a fuertes vientos o lluvia que sacudan la malla, para compensar esos inconvenientes se dispone de este equipo, el que mediante sus diferentes dispositivos permite realizar un monitoreo climático y así determinar si las alarmas provocadas son efectivas o simples efectos de las condiciones ambientales.

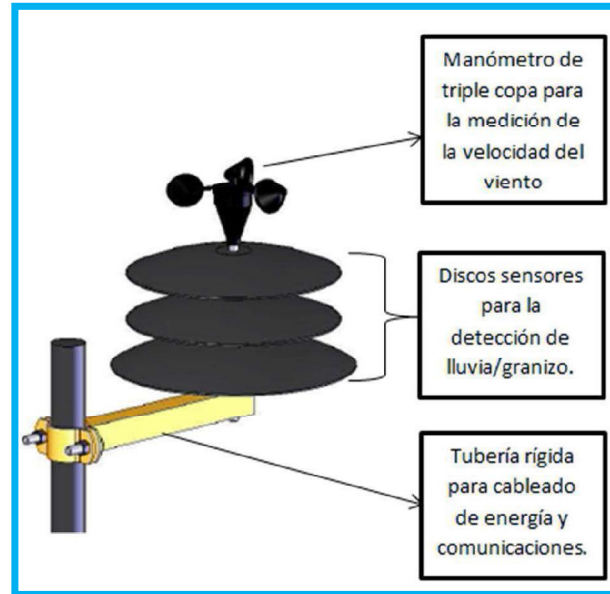


Figura 2. 60 Partes de la unidad meteorológica VX-25

2.3.3.9 Unidad interfaz de respaldo y control IA-6500

A este equipo se conecta el cableado de comunicaciones proveniente del campo. Por su importancia a continuación se detallan las partes más relevantes para su correcto uso.

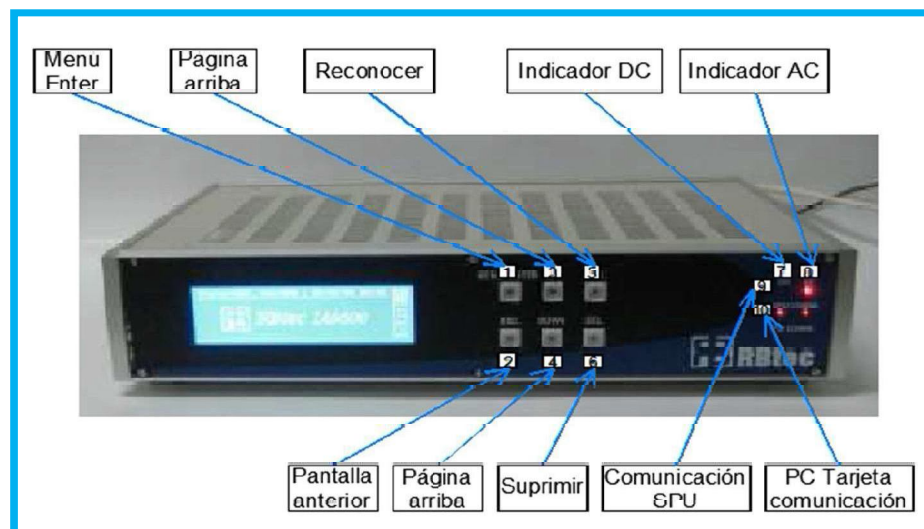


Figura 2. 61 Parte frontal de la unidad interfaz de control

Se puede observar que en la parte frontal se dispone de los indicadores, pantalla y teclado para el manejo y configuración emergente de los parámetros del sistema.

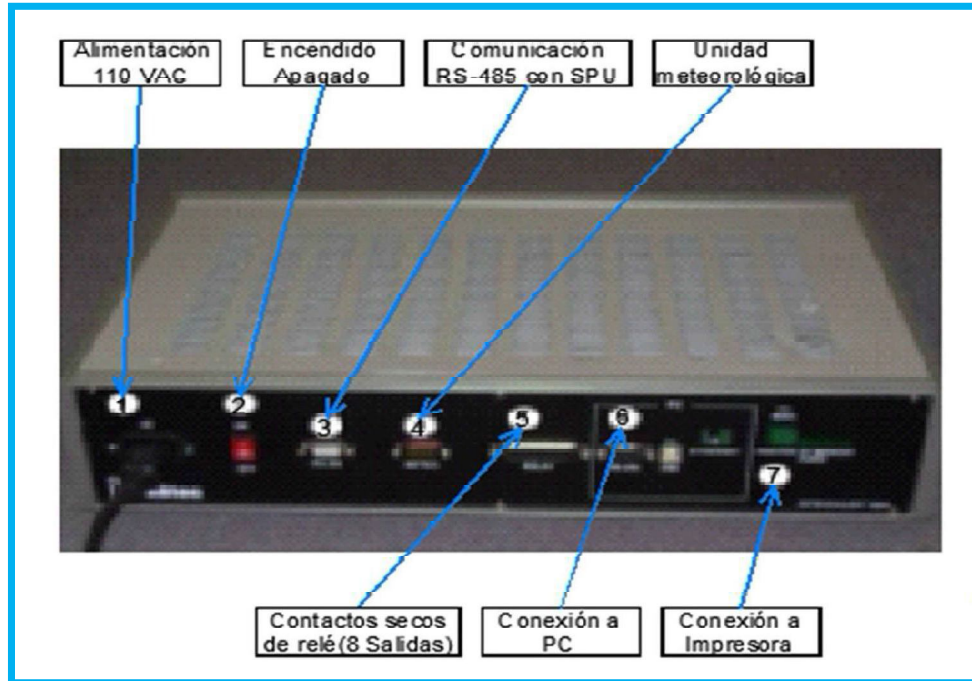


Figura 2. 62 Parte trasera de la unidad interfaz de control

En la parte trasera se identifican las entradas de comunicaciones, el interruptor de encendido del equipo y el punto de alimentación 110VAC.

2.3.4 DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL EN LAS ÁREAS DISEÑADAS

Debido a que la malla perimetral presenta varios puntos de ingreso de vehículos y personas se necesita implementar diferentes configuraciones de conexión del cableado que se presenta a continuación:

En primer lugar se tiene la implantación general del sistema en el plano geográfico de la refinería en el plano EE-101, donde se puede apreciar la ruta del cable sensor, la ruta del cable de comunicaciones y la distribución de SPU (transponders) en el perímetro.

En el plano EE-201 se puede ver el detalle de montaje de la unidad SPU y sus conexiones con los equipos del tablero más cercano montado en poste.

En el plano EE-202 se detalla la implementación del sistema perimetral en una puerta grande de batiente simple.

En el plano EE-203 se detalla la implementación del sistema perimetral en una puerta grande de doble batiente simple.

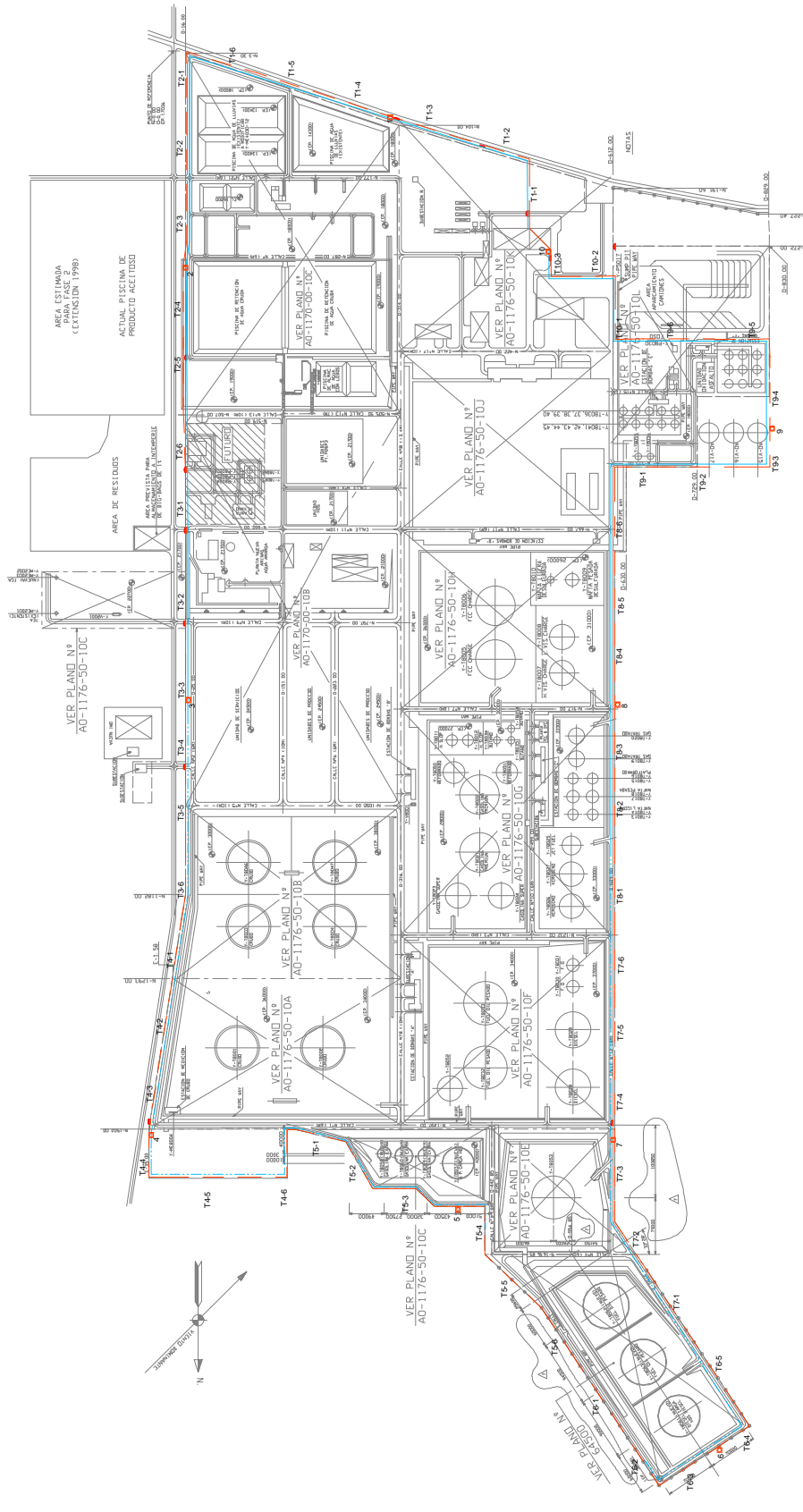
En el plano EE-204 se presenta la implementación del cable perimetral extendido sobre una porción de la malla.

Para las diferentes configuraciones de puertas se implementa diferentes formas de instalación las que se detallan a continuación:

En el plano EE-205 se detalla la implementación del sistema perimetral en una puerta grande de doble batiente con una puerta pequeña embebida en una de las batientes.

En el plano EE-206 se detalla la implementación del sistema perimetral en una puerta grande de tipo deslizante.

En el plano EE-603 se detalla la implementación de las conexiones entre la SPU y la tarjeta de final de zona.



1 EDICIÓN

SIMBOLOGIA	
□	Transponder
■	Puerta
—	Cable RB-SL-3
—	Cable RS-485
—	Cable RS-485 con extensor

Norma: S-9
 I.N.C. 2011 CAPIS

INSTITUCION

INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

SECTOR

SECTOR PÚBLICO

CONTRATO

Nº: 202004

ESCALA:

1:5000

UBICACION DE TRANSPONDERS

PLANO Nº: EE-101

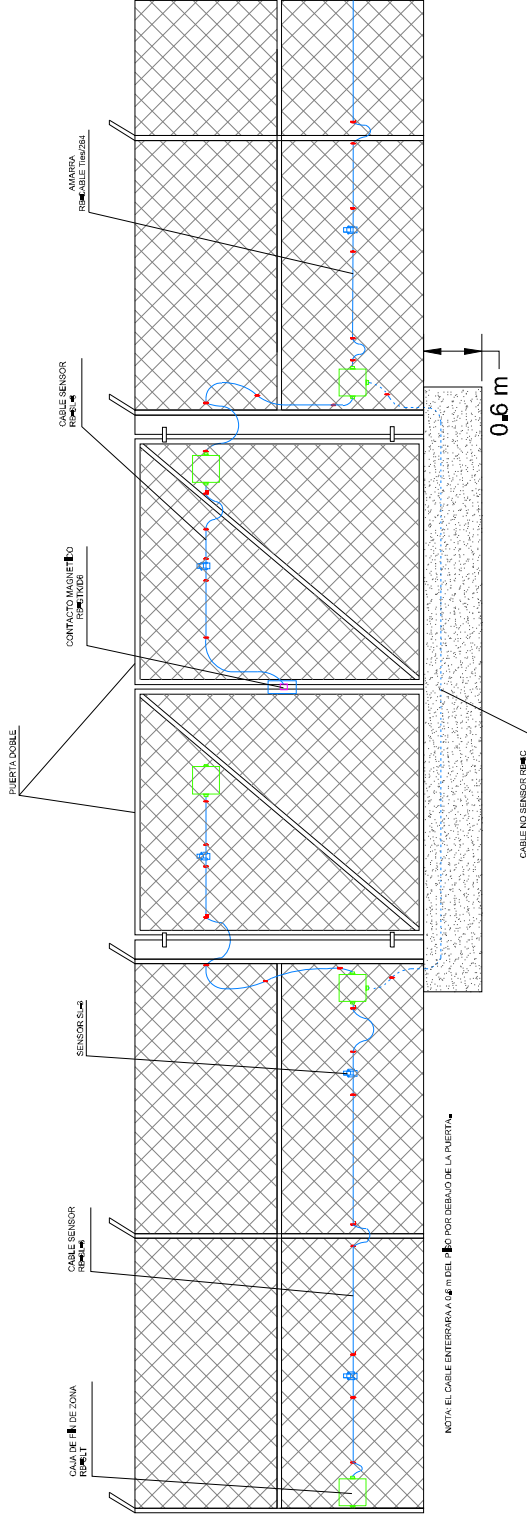
REVISION:

000

REGISTRO INGENIERIA / DISEÑO			
REV.	FECHA	DISEÑADO	APROBADO
0		Martina Culligero Andrés Cajo	
		REVISADO	FISCALIZADOR
		COORDINADOR	

CONEXIÓN SISTEMA PERIMETRAL EN PUERTAS DOBLES

023



NOTA: EL CABLE ENTERRAR A 0.6 m DEL FONDO DE LA PUERTA.

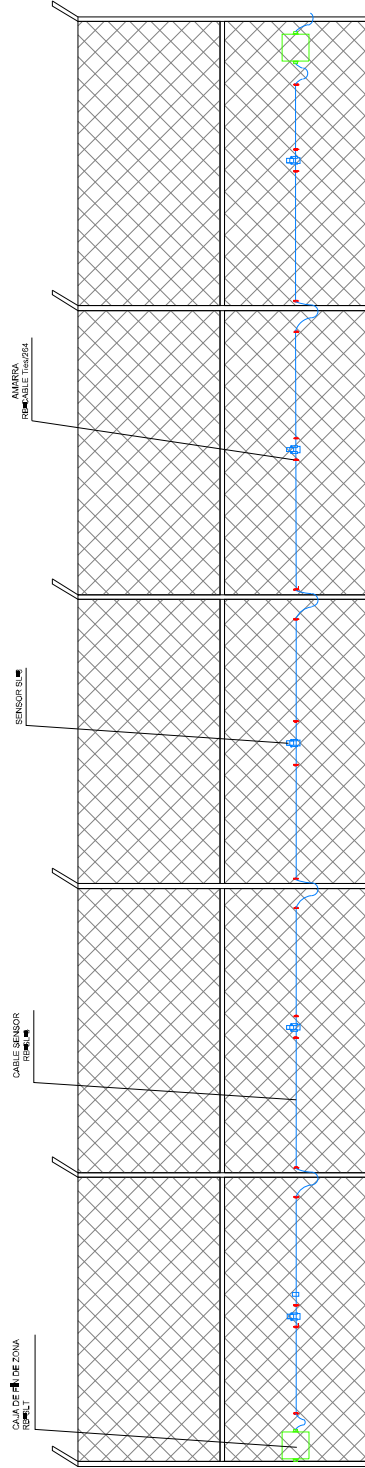
■	BIEN IDENTIFICADA
■	CAJA DE ALIMENTACIÓN DE ZONA
■	CABLE SENSOR
■	AMARRA
■	CONTACTO MAGNÉTICO
■	CABLE NO SENSOR

NOTAS:

- 1) NORMAS DE REFERENCIA: DIN IPR5
ISO-IEC-17025
IEC-60679-1
- 2) LA SIMBOLOGÍA UTILIZADA EN EL PLANO ES SOLO UNA REPRESENTACIÓN DE LOS EQUIPOS A INSTALARSE.

REGISTRO INGENIERIA / DISEÑO	
Mónica Quijero Arteses Cajo	REVISADO
0	APROBADO
REV. FECHA	DISEÑADO
PLANO No: EE-203	COORDINADOR
PUERTAS DOBLES	FISCALIZADOR
REVISIÓN: 000	APROBADO

CONEXIÓN SISTEMA PERIMETRAL EN MALLA (1-28)



■	REGIÓN
□	CAJA DE ZONA R1-1
—	CABLE SENSOR R1-1
■	AMARRA REMOVIBLE R1-1
→	CONEXIÓN CABLE SENSOR R1-1
→	CABLE NO SENSOR R1-1

NOTAS:

- 1) NORMAS DE REFERENCIA: DIN 1915
ISO-IEC-17025
IEC-60894-1
- 2) LA SIMBOLOGÍA UTILIZADA EN EL PLANO ES SOLO UNA REPRESENTACIÓN DE LOS EQUIPOS A INSTALARSE.

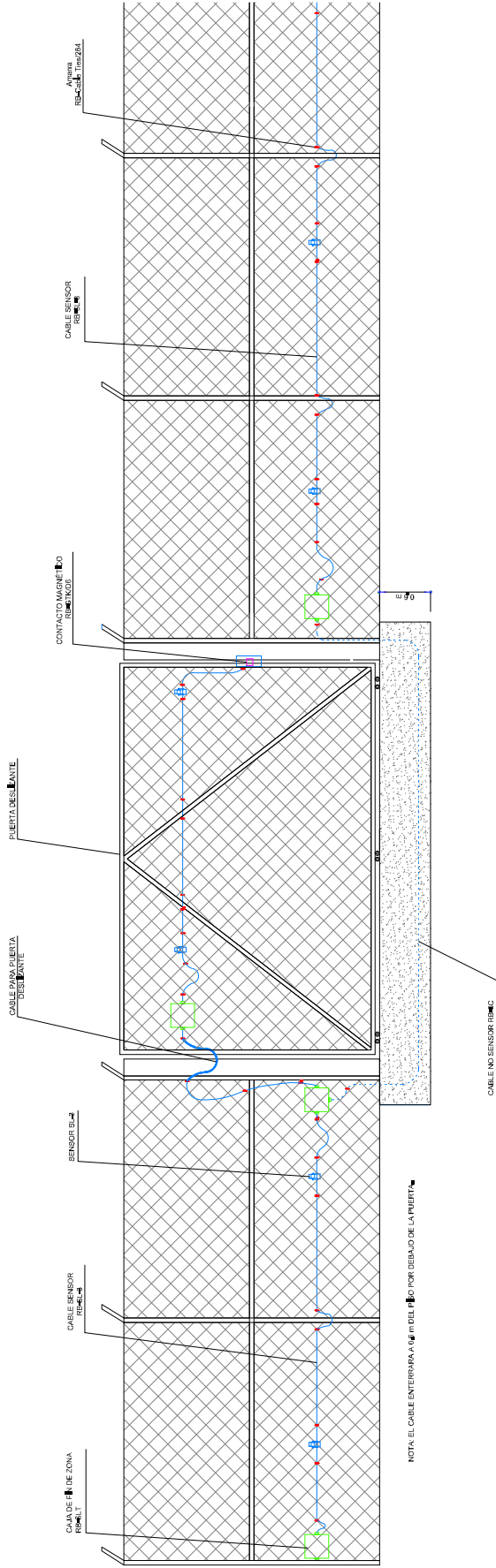


REGISTRO INGENIERIA / DISEÑO						
REV.	FECHA	DISEÑADO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Marta Gujardo Andrés Cajo				

		CONTRATO No.: 202004 ESCALA: 1:28 DETALLE DE CONEXIÓN SISTEMA PERIMETRAL EN MALLA	PLANO No.: EE-204 REVISIÓN: 000
--	--	---	------------------------------------

CONEXIÓN SISTEMA PERIMETRAL EN PUERTA DESLIZANTE

(1-28)



■	REGIÓN
■	CAJA DE ALARMA DE ZONA
■	CABLE SENSOR RBMC
■	ALARMA RBMC
■	CONTACTO MAGNETICO
■	CABLE NO SENSOR RBMC

NOTAS:

- 1) NORMAS DE REFERENCIA: DIN 1915, ISO-IEC-17025, IEC-60670-1
- 2) LA SIMBOLOGÍA UTILIZADA EN EL PLANO ES SOLO UNA REPRESENTACIÓN DE LOS EQUIPOS A INSTALARSE.



REGISTRO INGENIERIA / DISEÑO	
0	María Gujardo Arceño Cabo
0	DISEÑADO
0	REVISADO
0	APROBADO
0	FISCALIZADOR
0	COORDINADOR
0	PLANO No: EE-206
0	REVISIÓN: 000

2.4 DISEÑO DEL SISTEMA DE TRANSMISIÓN DE DATOS

En el diseño conceptual se ha propuesto la idea de implementar el sistema de comunicaciones usando un sistema inalámbrico, esto debido a que hacer la conexión cableada de tan solo una cámara de perímetro hacia el servidor de CCTV implicaría un costo elevadísimo en ingeniería civil y su realización sería muy complicada ya que implica realizar zanjas a través de la refinería destruyendo calles y sorteando tuberías importantes. Dado el ejemplo de tan solo una cámara el proyecto sería inviable tratándose el presente caso que consta de 41 cámaras. La fiscalización ha aceptado la idea de realizar las comunicaciones inalámbricas con la tecnología propuesta ya que son equipos de carácter industrial y su funcionamiento está acorde a este tipo de instalaciones.

Se establece la forma de transmisión de datos de los sistemas de cada área de acuerdo a los requerimientos de cada una de estas, según su ubicación y distancia hacia el Data center donde se concentra la información antes de llegar al cuarto de control para monitorear las alertas de los sistemas integrados.

Los enlaces de comunicación hacia el Data center se realizan tanto de los equipos de CCTV (cámaras), como los de accesos, con excepción de la garita peatonal que se encuentra cercana al Data center y sus comunicaciones son cableadas directamente; cuando las distancias son largas, se usa el sistema de comunicación inalámbrica Canopy ya que cuenta con las características que se requiere para blindar un óptimo funcionamiento de los sistemas integrados.

Para que se lleve a cabo la comunicación inalámbrica se usa tres torres de 45 metros, denominadas torre A, torre B y torre C distribuidas en puntos estratégicos para tener una cobertura correcta. Cada uno de los Access Point ubicados en las torres recibe los datos de tres módulos suscriptores, de manera que se tiene una reserva para futuras ampliaciones de 6 módulos extra.

La comunicación inicia desde la torre A, que es la más cercana al Data center. Esta torre recoge los datos de las otras dos torres, y mediante fibra óptica los lleva hacia el Data center que es donde se encuentran los servidores tanto del

2.4.1 DISEÑO DE LA COMUNICACIÓN DE EQUIPOS DE CADA ÁREA

2.4.1.1 Garita peatonal

Las cámaras fijas POE y la tarjeta LNL-2220 de la garita peatonal al estar cerca al Data center se conectan directamente al switch POE de 24 puertos presente en el rack.

2.4.1.2 Garita vehicular

La comunicación de las cámaras fijas POE como de la LNL-2220 se realiza usando un módulo suscriptor (SM) para llevar la información inalámbricamente de estos equipos hasta el Data Center.

2.4.1.3 Sala de control de procesos (Bunker)

Se usa un módulo suscriptor (SM) para la comunicación de la cámara fija POE y de la tarjeta de control de accesos LNL-2220.

2.4.1.4 Perímetro

Todas las cámaras PTZ distribuidas en el perímetro se comunican inalámbricamente debido a la dificultad física y de costos que implica cablearlas a todas hacia los puntos de red más cercanos. En la Figura 2.64 se presenta un diagrama del diseño descrito.

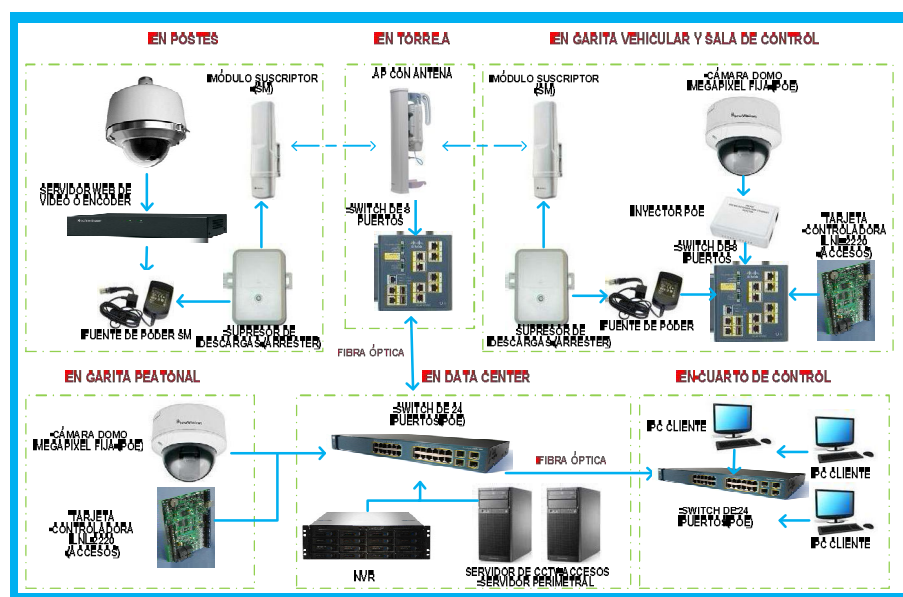


Figura 2. 64 Diagrama general del diseño por áreas

2.4.1.5 Correspondencia de módulos suscriptores

A continuación se presenta la tabla de distribución de módulos suscriptores a las diferentes cámaras PTZ en campo, así como para los equipos de garita vehicular y sala de control. Se indica también a que torre se comunica cada módulo suscriptor, esto se realiza teniendo en cuenta que torre es la más cercana a dichos suscriptores.

Tabla 2. 40 Correspondencia entre cámaras de perímetro y módulos suscriptores

# Módulo suscriptor	Equipos		# Módulo suscriptor	Equipos	
	Cámara	Torre		Cámara	Torre
SU2	Cámara 2	Torre A	SU24	Cámara 24	Torre C
SU3	Cámara 3	Torre A	SU25	Cámara 25	Torre C
SU4	Cámara 4	Torre A	SU26	Cámara 26	Torre B
SU5	Cámara 5	Torre A	SU27	Cámara 27	Torre C
SU6	Cámara 6	Torre A	SU28	Cámara 28	Torre A
SU7	Cámara 7	Torre A	SU29	Cámara 29	Torre A
SU8	Cámara 8	Torre A	SU30	Cámara 30	Torre A
SU9	Cámara 9	Torre B	SU31	Cámara 31	Torre A
SU10	Cámara 10	Torre B	SU32	Cámara 32	Torre A
SU11	Cámara 11	Torre B	SU33	Cámara 33	Torre A
SU12	Cámara 12	Torre B	SU34	Cámara 34	Torre A
SU13	Cámara 13	Torre B	SU35	Cámara 35	Torre A
SU14	Cámara 14	Torre B	SU36	Cámara 36	Torre A
SU15	Cámara 15	Torre B	SU37	Cámara 37	Torre A
SU16	Cámara 16	Torre C	SU38	Cámara 38	Torre A
SU17	Cámara 17	Torre C	SU39	Cámara 39	Torre A
SU18	Cámara 18	Torre C	SU40	Cámara 40	Torre A
SU19	Cámara 19	Torre C	SU43	Cámara 43	Torre B
SU20	Cámara 20	Torre C	SU46	Garita vehicular	Torre A
SU21	Cámara 21	Torre C	SU47	Sala de control	Torre B

2.4.2 CARACTERÍSTICAS TÉCNICAS DE EQUIPOS

Tabla 2. 41 Características básicas del módulo de administración de clúster

<p style="text-align: center;"><i>MÓDULO DE ADMINISTRACIÓN DE CLÚSTER (CMM)</i></p>	
Marca	Motorola
Modelo	1090CKBA
Alimentación de entrada	30V DC Y 56V DC
Puertos de salida de datos	8
Puertos para accionado de APs	8


Tabla 2. 42 Características básicas del Access point

<p style="text-align: center;"><i>ACCESS POINT CON AES (AP) Y ANTENA</i></p>	
Marca	Motorola
Modelo	5481AP
Alimentación	24V DC POE
Interface de comunicación	RJ45, Conexión Ethernet 10/100BASET
Frecuencia	5.4 GHz
Rango típico	18km

Tabla 2. 43 Características básicas del backhaul

<i>BACKHAUL y FUENTE DE PODER</i>	
Marca	Motorola
Modelo	PTP 500
Alimentación	POE
Interface de comunicación	RJ45, Conexión Ethernet 10/100BASET
Frecuencia	5.4 GHz
Rango típico	250km

Tabla 2. 44 Características básicas del módulo suscriptor

<i>MÓDULO SUSCRIPTOR (SM)</i>	
Marca	Motorola
Modelo	54918M20
Alimentación	24V DC POE
Interface	RJ45, Conexión Ethernet 10/100BASET
Frecuencia	5.4 GHz
Rango típico	18km

2.4.3 DESCRIPCIÓN DE LOS EQUIPOS DE COMUNICACIONES

El conjunto de subsistemas que se diseña tiene un sistema de control y seguridad centralizado; este punto de seguridad es el cuarto de control y vigilancia donde el personal de seguridad física de la refinería se encarga de atender eventos y controlar las alarmas de seguridad que arroje el sistema integrado.

2.4.3.1 Módulo de administración de clúster (CMM)

Este equipo se encarga de administrar y sincronizar las comunicaciones de los diferentes access point montados en las torres; básicamente es un switch administrable de 12 puertos de red y 4 de fibra óptica, embebido en una caja metálica para intemperie.



Figura 2. 65 Cluster management module (CMM)

2.4.3.2 Access point con AES y antena

Cada uno de estos equipos se encarga de las comunicaciones de 3 módulos suscriptores de manera que para los 51 módulos distribuidos en campo se requiere de 17 de estos equipos; cuyo nivel de seguridad indicado es (Advanced Encryption System) para tener un nivel de hermeticidad en la red elevado.



Figura 2. 66 AP y antena externa

2.4.3.3 Backhaul y fuente de poder

Es una potente antena que se usa para la transmisión de datos entre las 3 torres de comunicaciones.

2.4.3.4 Módulo suscriptor

Este equipo es una antena de menor tamaño que el backhaul y su función es permitir las comunicaciones multipunto hacia su respectivo Access point.



Figura 2. 67 Módulo suscriptor (SM)

2.4.4 CUARTO DE CONTROL Y DATA CENTER

Los equipos de cada subsistema se enlazan mediante la red, para lo cual se tienen cuatro racks con los equipos necesarios para la integración y monitoreo de los sistemas de refinería.

Básicamente los racks constan de un ODF que es un distribuidor de fibra óptica, en el caso de enlazarse con otro switch a más de 90m entre sí, el patch panel en cambio es el distribuidor de puntos de red mediante conectores RJ45, el switch se conecta al patch panel para mantener ordenada la red. La canaleta ranurada sirve para organizar el cableado que se tiene entre los equipos montados en el rack.

En los racks también se encuentra el multiviewer que divide las pantallas de video wall en varias áreas, es un divisor de pantalla. Se tiene dos bandejas con las tarjetas requeridas para la integración del sistema perimetral con el sistema de CCTV.

Se cuenta también con dos grabadores de video NVR, así como con los equipos de respaldo de grabación. Para alimentación y comunicación de las cámaras fijas POE se encuentran inyectores POE.

El resto de equipos en los racks son los servidores de los distintos sistemas, y el arrester que corresponde al sistema Canopy en los casos en que se utiliza comunicación inalámbrica, a continuación se muestra la distribución de los equipos en los racks.

En el proyecto se realiza un control centralizado es decir todos los sistemas diseñados son controlados mediante un computador cliente por sistema desde un mismo sitio el que conocemos como Cuarto de Control o Monitoreo, que es el lugar donde:

- Se reciben las señales de video y se realiza el control de cámaras.
- Se supervisan las alertas de alarmas.
- Se toman acciones correctivas ante los eventos de alarmas que se presenten.
- Se monitorea el estado de los distintos accesos.
- En este sitio se realiza el enrolamiento de personal para el registro de asistencia.
- Se reciben también las alarmas provenientes del sistema de cableado perimetral.

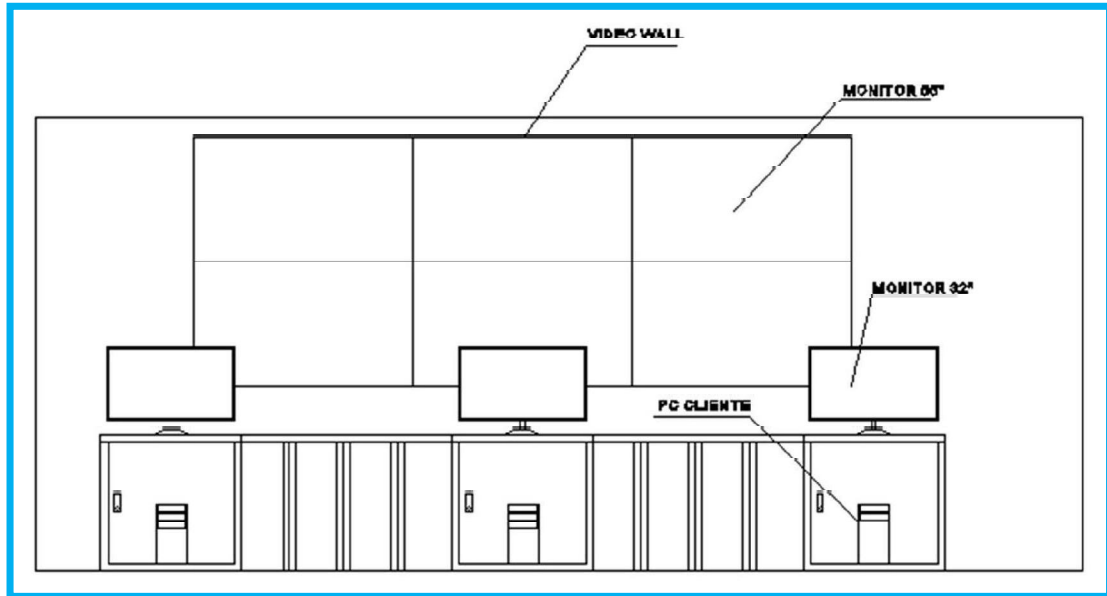


Figura 2. 68 Vista frontal video Wall y monitores

A continuación se tiene el presupuesto del proyecto, solo tomando en cuenta el suministro de los equipos y software necesarios de cada subsistema diseñado para su implementación. La obra civil requerida no se ha estimado en este documento.

Tabla 2. 45 Presupuesto de la ingeniería del detalle

PRESUPUESTO GENERAL					
SISTEMA DE SEGURIDAD FISICA INTEGRAL DE REFINERIA ESMERALDAS					
ITEM	DESCRIPCIÓN	UND.	CANT.	P.UN.	P.TOT.
I	INGENIERÍA				
I-1	Ingeniería Detallada para Sistema de Seguridad Física Integral.	u	1	42050	42050
	SUBTOTAL 1				42050

Tabla 2. 46 Presupuesto de materiales, equipos y software para el subsistema de cableado perimetral

PROCURA – OBRA ELECTRÓNICA					
SISTEMA DE SEGURIDAD FISICA INTEGRAL DE REFINERIA ESMERALDAS					
ITEM	DESCRIPCIÓN	UND.	CANT.	P.UN.	P.TOT.
P	INGENIERÍA				
P-1	SUMINISTRO DE MATERIALES, EQUIPOS, SOFTWARE Y ACCESORIOS PARA SUBSISTEMA DE CABLEADO PERIMETRAL				
P-1-1	Suministro de cable sensor por vibración multidireccional para detección de intrusos.	m	6500	31,98	207870
P-1-2	Suministro de cable de comunicación para conectar las tarjetas analizadoras con el transponder de campo.	m	6000	4,9	29400
P-1-3	Suministro de unidad de compensación meteorológica (incluye módulo de interfase).	u	3	1285,95	3857,85
P-1-4	Suministro de tarjeta transponder para cable sensor (Incluye CPU chip, software de comandos, protector de rayos, 2 Supresor de descargas eléctricas por cada transponder y 1 caja para iterperie).	u	10	5962,15	59621,50
P-1-5	Suministro de Unidad receptora de respaldo con display LCD, 8 relevos de contacto seco (opcional conexión TCP/IP, USB), incluye Tarjeta expansora de 32 relevos para contacto seco.	u	1	9399,17	9399,17
P-1-6	Suministro de Software para el Sistema de Detección de Intrusión (incluye PC).	u	1	14539,15	14539,15
	SUBTOTAL 2				324.687,67

Tabla 2. 47 Presupuesto de materiales, equipos y software para el subsistema de enlaces de comunicación inalámbrica

PROCURA – OBRA ELECTRÓNICA					
SISTEMA DE SEGURIDAD FISICA INTEGRAL DE REFINERIA ESMERALDAS					
ITEM	DESCRIPCIÓN	UND.	CANT.	P.UN.	P.TOT.
P	INGENIERIA				
P-2	SUMINISTRO DE MATERIALES, EQUIPOS Y ACCESORIOS PARA SUBSISTEMA DE ENLACES DE COMUNICACIÓN				
P-2-1	Suministro de accesspoint con AES, incluye 3 módulos subscritor por cada unidad.	u	17	13247,26	225203,42
P-2-2	Suministro de puentes inalámbricos ethernet - PTP (Incluye 625 mts cable UTP intemperie FTP Cat 6 por cada unidad).	u	4	29641,00	118564,00
P-2-3	Suministro de módulo administrador cluster mini (CMM), incluye caja NEMA de 8 puertos con protección de alto voltaje.	u	2	6952,46	13904,92
P-2-4	Suministro de equipos activos para enlaces de comunicación, incluye 4 Switch configurable de 8 puertos – industrial y 1 Switch configurable de 24 puertos + 4SFP-SC.	u	1	24507,42	24507,42
P-2-5	Suministro de torre de comunicación de 45 metros (incluye pararrayos, baliza y tierra).	u	2	50162,24	100324,48
P-2-6	Suministro de torres de 15 metros con sensores (incluye pararrayos, baliza y tierra).	u	1	19832,00	19832,00
	SUBTOTAL 3				502.336,24

Tabla 2. 48 Presupuesto de materiales, equipos y software para el subsistema de enlaces de comunicación inalámbrica y circuito cerrado de televisión

PROCURA – OBRA ELECTRÓNICA					
SISTEMA DE SEGURIDAD FISICA INTEGRAL DE REFINERIA ESMERALDAS					
ITEM	DESCRIPCIÓN	UND.	CANT.	P.UN.	P.TOT.
P	INGENIERÍA				
P-3	SUMINISTRO DE MATERIALES, EQUIPOS, SOFTWARE Y ACCESORIOS PARA SUBSISTEMA DE CONTROL DE ACCESOS				
P-3-1	Suministro de equipos para lectura de tarjetas de acceso.	u	1	34054,32	34054,32
P-3-2	Suministro de espinas de pescado.	u	5	18775,85	93879,25
P-3-3	Suministro de equipos para lectura de geometría de mano.	u	1	32232,62	32232,62
P-3-4	Suministro de equipos para control vehicular.	u	1	27189,56	27189,56
P-3-5	Suministro de Paquete de software de control de asistencia.	u	1	10675,86	10675,86
	SUBTOTAL 4				502.336,24
P-4	SUMINISTRO DE MATERIALES, EQUIPOS Y ACCESORIOS PARA SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN				
P-4-1		u	41	6203,88	254359,08
P-4-2		u	6	2424,49	14546,94
P-4-3		u	41	492,47	20191,27
	SUBTOTAL 5				289097,29

Tabla 2. 49 Presupuesto de materiales, equipos y software del subsistema de servidores, grabadores y cuarto de monitoreo y control

PROCURA – OBRA ELECTRÓNICA					
SISTEMA DE SEGURIDAD FISICA INTEGRAL DE REFINERIA ESMERALDAS					
ITEM	DESCRIPCIÓN	UND.	CANT.	P.UN.	P.TOT.
P	INGENIERÍA				
P-5	SUMINISTRO DE EQUIPOS Y SOFTWARE PARA SUBSISTEMA DE SERVIDORES Y EQUIPOS DE GRABACION				
P-5-1	Suministro de hardware y software para sistema cliente servidor.	u	1	52384,06	52384,06
P-5-2	Suministro de equipos de grabación.	u	1	102174,32	102174,32
P-5-3	Suministro de librería para respaldo en cintas.	u	1	86339,70	86339,70
	SUBTOTAL 6				240898,08
P-6	SUMINISTRO DE EQUIPOS Y SOFTWARE PARA SUBSISTEMA DE CUARTO DE MONITOREO Y CONTROL				
P-6-1	Suministro de hardware y software de cliente de sistema de video y accesos.	u	1	72465,31	72465,31
P-6-2	Suministro de equipos para monitoreo y control del Sistema de Seguridad Física Integral.	u	1	95511,64	95511,64
P-6-3	Suministro de equipos para carnetización.	u	1	15469,05	15469,05
	SUBTOTAL 7				183446,00
	TOTAL				1780546,89

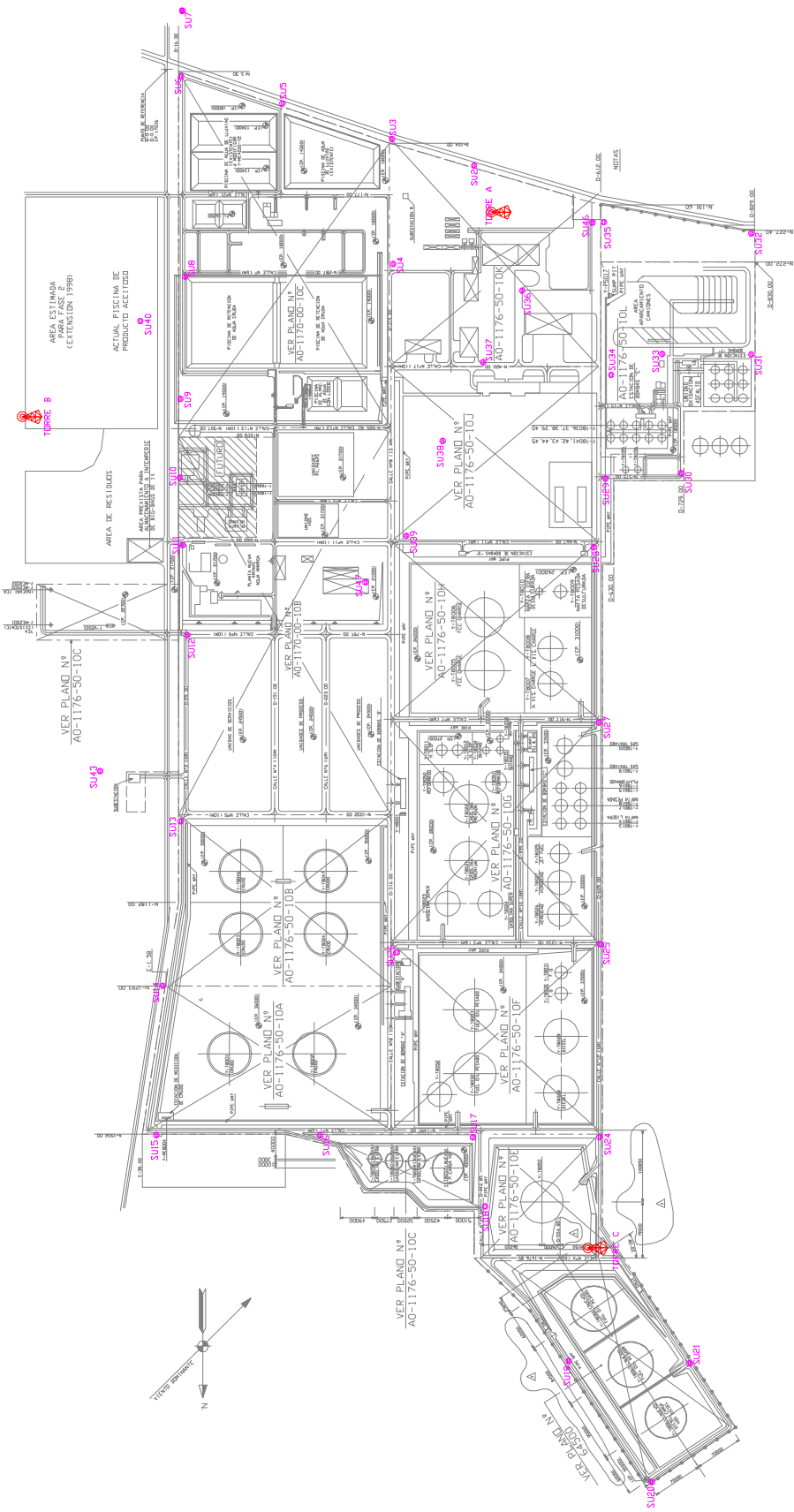
2.4.5 DIAGRAMAS DE CONEXIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL EN LAS ÁREAS DISEÑADAS

En primer lugar se tiene la implantación general del sistema en el plano geográfico de la refinería en el plano EE-103, donde se puede apreciar la distribución de los módulos suscriptores.

En el plano E-600 se puede ver el detalle de montaje de equipos y constitución de las torres de 45 metros.

En el plano CIV-250 se detalla la implementación del cuarto de monitoreo y la distribución de los equipos necesarios para su correcto funcionamiento.

En este capítulo se ha realizado un diseño a fondo de los tres subsistemas a implementarse, tomando en consideración los aspectos económicos, técnicos y de viabilidad del proyecto; la fiscalización después de realizar un análisis exhaustivo de los diseños y equipos propuestos ha aceptado su posterior implementación siguiendo los estándares internos y de la empresa.



Simbolo	Descripción
100	1. FUNDACIONES
101	2. PAREDES EXTERNALES
102	3. PAREDES INTERNALES
103	4. PAREDES DE DIVISION
104	5. PAREDES DE ALBAÑILERIA
105	6. PAREDES DE MORTERO
106	7. PAREDES DE YESO
107	8. PAREDES DE PLASTICO
108	9. PAREDES DE PASTA DE CEMENTO
109	10. PAREDES DE CEMENTO
110	11. PAREDES DE MORTERO
111	12. PAREDES DE YESO
112	13. PAREDES DE PLASTICO
113	14. PAREDES DE PASTA DE CEMENTO
114	15. PAREDES DE CEMENTO
115	16. PAREDES DE MORTERO
116	17. PAREDES DE YESO
117	18. PAREDES DE PLASTICO
118	19. PAREDES DE PASTA DE CEMENTO
119	20. PAREDES DE CEMENTO
120	21. PAREDES DE MORTERO
121	22. PAREDES DE YESO
122	23. PAREDES DE PLASTICO
123	24. PAREDES DE PASTA DE CEMENTO
124	25. PAREDES DE CEMENTO
125	26. PAREDES DE MORTERO
126	27. PAREDES DE YESO
127	28. PAREDES DE PLASTICO
128	29. PAREDES DE PASTA DE CEMENTO
129	30. PAREDES DE CEMENTO
130	31. PAREDES DE MORTERO
131	32. PAREDES DE YESO
132	33. PAREDES DE PLASTICO
133	34. PAREDES DE PASTA DE CEMENTO
134	35. PAREDES DE CEMENTO
135	36. PAREDES DE MORTERO
136	37. PAREDES DE YESO
137	38. PAREDES DE PLASTICO
138	39. PAREDES DE PASTA DE CEMENTO
139	40. PAREDES DE CEMENTO
140	41. PAREDES DE MORTERO
141	42. PAREDES DE YESO
142	43. PAREDES DE PLASTICO
143	44. PAREDES DE PASTA DE CEMENTO
144	45. PAREDES DE CEMENTO
145	46. PAREDES DE MORTERO
146	47. PAREDES DE YESO
147	48. PAREDES DE PLASTICO
148	49. PAREDES DE PASTA DE CEMENTO
149	50. PAREDES DE CEMENTO
150	51. PAREDES DE MORTERO
151	52. PAREDES DE YESO
152	53. PAREDES DE PLASTICO
153	54. PAREDES DE PASTA DE CEMENTO
154	55. PAREDES DE CEMENTO
155	56. PAREDES DE MORTERO
156	57. PAREDES DE YESO
157	58. PAREDES DE PLASTICO
158	59. PAREDES DE PASTA DE CEMENTO
159	60. PAREDES DE CEMENTO
160	61. PAREDES DE MORTERO
161	62. PAREDES DE YESO
162	63. PAREDES DE PLASTICO
163	64. PAREDES DE PASTA DE CEMENTO
164	65. PAREDES DE CEMENTO
165	66. PAREDES DE MORTERO
166	67. PAREDES DE YESO
167	68. PAREDES DE PLASTICO
168	69. PAREDES DE PASTA DE CEMENTO
169	70. PAREDES DE CEMENTO
170	71. PAREDES DE MORTERO
171	72. PAREDES DE YESO
172	73. PAREDES DE PLASTICO
173	74. PAREDES DE PASTA DE CEMENTO
174	75. PAREDES DE CEMENTO
175	76. PAREDES DE MORTERO
176	77. PAREDES DE YESO
177	78. PAREDES DE PLASTICO
178	79. PAREDES DE PASTA DE CEMENTO
179	80. PAREDES DE CEMENTO
180	81. PAREDES DE MORTERO
181	82. PAREDES DE YESO
182	83. PAREDES DE PLASTICO
183	84. PAREDES DE PASTA DE CEMENTO
184	85. PAREDES DE CEMENTO
185	86. PAREDES DE MORTERO
186	87. PAREDES DE YESO
187	88. PAREDES DE PLASTICO
188	89. PAREDES DE PASTA DE CEMENTO
189	90. PAREDES DE CEMENTO
190	91. PAREDES DE MORTERO
191	92. PAREDES DE YESO
192	93. PAREDES DE PLASTICO
193	94. PAREDES DE PASTA DE CEMENTO
194	95. PAREDES DE CEMENTO
195	96. PAREDES DE MORTERO
196	97. PAREDES DE YESO
197	98. PAREDES DE PLASTICO
198	99. PAREDES DE PASTA DE CEMENTO
199	100. PAREDES DE CEMENTO
200	101. PAREDES DE MORTERO
201	102. PAREDES DE YESO
202	103. PAREDES DE PLASTICO
203	104. PAREDES DE PASTA DE CEMENTO
204	105. PAREDES DE CEMENTO
205	106. PAREDES DE MORTERO
206	107. PAREDES DE YESO
207	108. PAREDES DE PLASTICO
208	109. PAREDES DE PASTA DE CEMENTO
209	110. PAREDES DE CEMENTO
210	111. PAREDES DE MORTERO
211	112. PAREDES DE YESO
212	113. PAREDES DE PLASTICO
213	114. PAREDES DE PASTA DE CEMENTO
214	115. PAREDES DE CEMENTO
215	116. PAREDES DE MORTERO
216	117. PAREDES DE YESO
217	118. PAREDES DE PLASTICO
218	119. PAREDES DE PASTA DE CEMENTO
219	120. PAREDES DE CEMENTO
220	121. PAREDES DE MORTERO
221	122. PAREDES DE YESO
222	123. PAREDES DE PLASTICO
223	124. PAREDES DE PASTA DE CEMENTO
224	125. PAREDES DE CEMENTO
225	126. PAREDES DE MORTERO
226	127. PAREDES DE YESO
227	128. PAREDES DE PLASTICO
228	129. PAREDES DE PASTA DE CEMENTO
229	130. PAREDES DE CEMENTO
230	131. PAREDES DE MORTERO
231	132. PAREDES DE YESO
232	133. PAREDES DE PLASTICO
233	134. PAREDES DE PASTA DE CEMENTO
234	135. PAREDES DE CEMENTO
235	136. PAREDES DE MORTERO
236	137. PAREDES DE YESO
237	138. PAREDES DE PLASTICO
238	139. PAREDES DE PASTA DE CEMENTO
239	140. PAREDES DE CEMENTO
240	141. PAREDES DE MORTERO
241	142. PAREDES DE YESO
242	143. PAREDES DE PLASTICO
243	144. PAREDES DE PASTA DE CEMENTO
244	145. PAREDES DE CEMENTO
245	146. PAREDES DE MORTERO
246	147. PAREDES DE YESO
247	148. PAREDES DE PLASTICO
248	149. PAREDES DE PASTA DE CEMENTO
249	150. PAREDES DE CEMENTO
250	151. PAREDES DE MORTERO
251	152. PAREDES DE YESO
252	153. PAREDES DE PLASTICO
253	154. PAREDES DE PASTA DE CEMENTO
254	155. PAREDES DE CEMENTO
255	156. PAREDES DE MORTERO
256	157. PAREDES DE YESO
257	158. PAREDES DE PLASTICO
258	159. PAREDES DE PASTA DE CEMENTO
259	160. PAREDES DE CEMENTO
260	161. PAREDES DE MORTERO
261	162. PAREDES DE YESO
262	163. PAREDES DE PLASTICO
263	164. PAREDES DE PASTA DE CEMENTO
264	165. PAREDES DE CEMENTO
265	166. PAREDES DE MORTERO
266	167. PAREDES DE YESO
267	168. PAREDES DE PLASTICO
268	169. PAREDES DE PASTA DE CEMENTO
269	170. PAREDES DE CEMENTO
270	171. PAREDES DE MORTERO
271	172. PAREDES DE YESO
272	173. PAREDES DE PLASTICO
273	174. PAREDES DE PASTA DE CEMENTO
274	175. PAREDES DE CEMENTO
275	176. PAREDES DE MORTERO
276	177. PAREDES DE YESO
277	178. PAREDES DE PLASTICO
278	179. PAREDES DE PASTA DE CEMENTO
279	180. PAREDES DE CEMENTO
280	181. PAREDES DE MORTERO
281	182. PAREDES DE YESO
282	183. PAREDES DE PLASTICO
283	184. PAREDES DE PASTA DE CEMENTO
284	185. PAREDES DE CEMENTO
285	186. PAREDES DE MORTERO
286	187. PAREDES DE YESO
287	188. PAREDES DE PLASTICO
288	189. PAREDES DE PASTA DE CEMENTO
289	190. PAREDES DE CEMENTO
290	191. PAREDES DE MORTERO
291	192. PAREDES DE YESO
292	193. PAREDES DE PLASTICO
293	194. PAREDES DE PASTA DE CEMENTO
294	195. PAREDES DE CEMENTO
295	196. PAREDES DE MORTERO
296	197. PAREDES DE YESO
297	198. PAREDES DE PLASTICO
298	199. PAREDES DE PASTA DE CEMENTO
299	200. PAREDES DE CEMENTO
300	201. PAREDES DE MORTERO
301	202. PAREDES DE YESO
302	203. PAREDES DE PLASTICO
303	204. PAREDES DE PASTA DE CEMENTO
304	205. PAREDES DE CEMENTO
305	206. PAREDES DE MORTERO
306	207. PAREDES DE YESO
307	208. PAREDES DE PLASTICO
308	209. PAREDES DE PASTA DE CEMENTO
309	210. PAREDES DE CEMENTO
310	211. PAREDES DE MORTERO
311	212. PAREDES DE YESO
312	213. PAREDES DE PLASTICO
313	214. PAREDES DE PASTA DE CEMENTO
314	215. PAREDES DE CEMENTO
315	216. PAREDES DE MORTERO
316	217. PAREDES DE YESO
317	218. PAREDES DE PLASTICO
318	219. PAREDES DE PASTA DE CEMENTO
319	220. PAREDES DE CEMENTO
320	221. PAREDES DE MORTERO
321	222. PAREDES DE YESO
322	223. PAREDES DE PLASTICO
323	224. PAREDES DE PASTA DE CEMENTO
324	225. PAREDES DE CEMENTO
325	226. PAREDES DE MORTERO
326	227. PAREDES DE YESO
327	228. PAREDES DE PLASTICO
328	229. PAREDES DE PASTA DE CEMENTO
329	230. PAREDES DE CEMENTO
330	231. PAREDES DE MORTERO
331	232. PAREDES DE YESO
332	233. PAREDES DE PLASTICO
333	234. PAREDES DE PASTA DE CEMENTO
334	235. PAREDES DE CEMENTO
335	236. PAREDES DE MORTERO
336	237. PAREDES DE YESO
337	238. PAREDES DE PLASTICO
338	239. PAREDES DE PASTA DE CEMENTO
339	240. PAREDES DE CEMENTO
340	241. PAREDES DE MORTERO
341	242. PAREDES DE YESO
342	243. PAREDES DE PLASTICO
343	244. PAREDES DE PASTA DE CEMENTO
344	245. PAREDES DE CEMENTO
345	246. PAREDES DE MORTERO
346	247. PAREDES DE YESO
347	248. PAREDES DE PLASTICO
348	249. PAREDES DE PASTA DE CEMENTO
349	250. PAREDES DE CEMENTO
350	251. PAREDES DE MORTERO
351	252. PAREDES DE YESO
352	253. PAREDES DE PLASTICO
353	254. PAREDES DE PASTA DE CEMENTO
354	255. PAREDES DE CEMENTO
355	256. PAREDES DE MORTERO
356	257. PAREDES DE YESO
357	258. PAREDES DE PLASTICO
358	259. PAREDES DE PASTA DE CEMENTO
359	260. PAREDES DE CEMENTO
360	261. PAREDES DE MORTERO
361	262. PAREDES DE YESO
362	263. PAREDES DE PLASTICO
363	264. PAREDES DE PASTA DE CEMENTO
364	265. PAREDES DE CEMENTO
365	266. PAREDES DE MORTERO
366	267. PAREDES DE YESO
367	268. PAREDES DE PLASTICO
368	269. PAREDES DE PASTA DE CEMENTO
369	270. PAREDES DE CEMENTO
370	271. PAREDES DE MORTERO
371	272. PAREDES DE YESO
372	273. PAREDES DE PLASTICO
373	274. PAREDES DE PASTA DE CEMENTO
374	275. PAREDES DE CEMENTO
375	276. PAREDES DE MORTERO
376	277. PAREDES DE YESO
377	278. PAREDES DE PLASTICO
378	279. PAREDES DE PASTA DE CEMENTO
379	280. PAREDES DE CEMENTO
380	281. PAREDES DE MORTERO
381	282. PAREDES DE YESO
382	283. PAREDES DE PLASTICO
383	284. PAREDES DE PASTA DE CEMENTO
384	285. PAREDES DE CEMENTO
385	286. PAREDES DE MORTERO
386	287. PAREDES DE YESO
387	288. PAREDES DE PLASTICO
388	289. PAREDES DE PASTA DE CEMENTO
389	290. PAREDES DE CEMENTO
390	291. PAREDES DE MORTERO
391	292. PAREDES DE YESO
392	293. PAREDES DE PLASTICO
393	294. PAREDES DE PASTA DE CEMENTO
394	295. PAREDES DE CEMENTO
395	296. PAREDES DE MORTERO
396	297. PAREDES DE YESO
397	298. PAREDES DE PLASTICO
398	299. PAREDES DE PASTA DE CEMENTO
399	300. PAREDES DE CEMENTO
400	301. PAREDES DE MORTERO
401	302. PAREDES DE YESO
402	303. PAREDES DE PLASTICO
403	304. PAREDES DE PASTA DE CEMENTO
404	305. PAREDES DE CEMENTO
405	306. PAREDES DE MORTERO
406	307. PAREDES DE YESO
407	308. PAREDES DE PLASTICO
408	309. PAREDES DE PASTA DE CEMENTO
409	310. PAREDES DE CEMENTO
410	311. PAREDES DE MORTERO
411	312. PAREDES DE YESO
412	313. PAREDES DE PLASTICO
413	314. PAREDES DE PASTA DE CEMENTO
414	315. PAREDES DE CEMENTO
415	316. PAREDES DE MORTERO
416	317. PAREDES DE YESO
417	318. PAREDES DE PLASTICO
418	319. PAREDES DE PASTA DE CEMENTO
419	320. PAREDES DE CEMENTO
420	321. PAREDES DE MORTERO
421	322. PAREDES DE YESO
422	323. PAREDES DE PLASTICO
423	324. PAREDES DE PASTA DE CEMENTO
424	325. PAREDES DE CEMENTO
425	326. PAREDES DE MORTERO
426	327. PAREDES DE YESO
427	328. PAREDES DE PLASTICO
428	329. PAREDES DE PASTA DE CEMENTO
429	330. PAREDES DE CEMENTO
430	331. PAREDES DE MORTERO
431	332. PAREDES DE YESO
432	333. PAREDES DE PLASTICO
433	334. PAREDES DE PASTA DE CEMENTO
434	335. PAREDES DE CEMENTO
435	336. PAREDES DE MORTERO
436	337. PAREDES DE YESO
437	338. PAREDES DE PLASTICO
438	339. PAREDES DE PASTA DE CEMENTO
439	340. PAREDES DE CEMENTO
440	341. PAREDES DE MORTERO
441	342. PAREDES DE YESO
442	343. PAREDES DE PLASTICO
443	344. PAREDES DE PASTA DE CEMENTO
444	345. PAREDES DE CEMENTO
445	346. PAREDES DE MORTERO
446	347. PAREDES DE YESO
447	348. PAREDES DE PLASTICO
448	349. PAREDES DE PASTA DE CEMENTO
449	350. PAREDES DE CEMENTO
450	351. PAREDES DE MORTERO
451	352. PAREDES DE YESO
452	353. PAREDES DE PLASTICO
453	354. PAREDES DE PASTA DE CEMENTO
454	355. PAREDES DE CEMENTO
455	356. PAREDES DE MORTERO
456	357. PAREDES DE YESO
457	358. PAREDES DE PLASTICO
458	359. PAREDES DE PASTA DE CEMENTO
459	360. PAREDES DE CEMENTO
460	361. PAREDES DE MORTERO
461	362. PAREDES DE YESO
462	363. PAREDES DE PLASTICO
463	364. PAREDES DE PASTA DE CEMENTO
464	365. PAREDES DE CEMENTO
465	366. PAREDES DE MORTERO
466	367. PAREDES DE YESO
467	368. PAREDES DE PLASTICO
468	369. PAREDES DE PASTA DE CEMENTO
469	370. PAREDES DE CEMENTO
470	371. PAREDES DE MORTERO
471	372. PAREDES DE YESO
472	373. PAREDES DE PLASTICO
473	374. PAREDES DE PASTA DE CEMENTO
474	375. PAREDES DE CEMENTO
475	376. PAREDES DE MORTERO
476	377. PAREDES DE YESO
477	378. PAREDES DE PLASTICO
478	379. PAREDES DE PASTA DE CEMENTO
479	380. PAREDES DE CEMENTO
480	381. PAREDES DE MORTERO
481	382. PAREDES DE YESO
482	383. PAREDES DE PLASTICO
483	384. PAREDES DE PASTA DE CEMENTO
484	385. PAREDES DE CEMENTO
485	386. PAREDES DE MORTERO
486	387. PAREDES DE YESO
487	388. PAREDES DE PLASTICO
488	389. PAREDES DE PASTA DE CEMENTO
489	390. PAREDES DE CEMENTO
490	391. PAREDES DE MORTERO
491	392. PAREDES DE YESO
492	393. PAREDES DE PLASTICO
493	394. PAREDES DE PASTA DE CEMENTO
494	395. PAREDES DE CEMENTO
495	396. PAREDES DE MORTERO
496	397. PAREDES DE YESO
497	398. PAREDES DE PLASTICO
498	399. PAREDES DE PASTA DE CEMENTO
499	400. PAREDES DE CEMENTO

UNIDAD SUSCRIPTRORA DE RADIO

Torre de Comunicación

NOTA: Este proyecto se utilizó en el sitio 06 de los planos de San José.

INSTRUMENTACIÓN: **INSTRUMENTACIÓN DE PRECISIÓN**

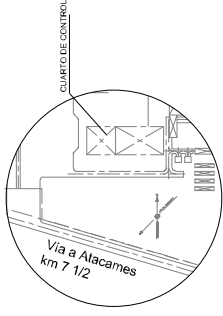
CONTRATO No.: 202004 ESCALA: 1:5000

UBICACIÓN DE SUSCRIPTORES NA AMERICOS Y TORRES DE COMUNICACIÓN

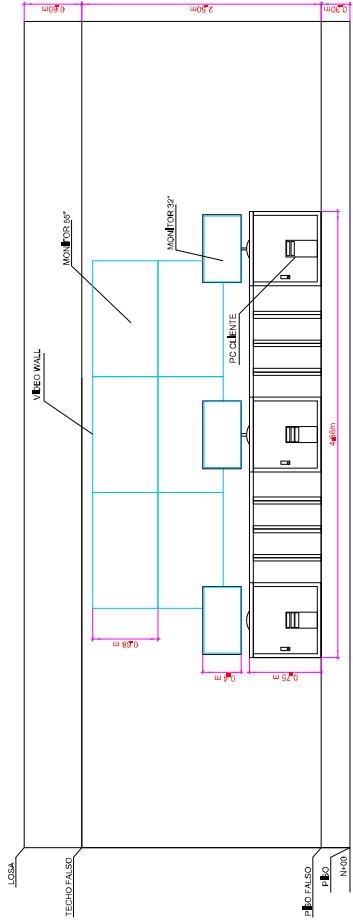
PLANO No.: EE-103 REVISIÓN: 004

REGISTRO INGENIERIA / DISEÑO

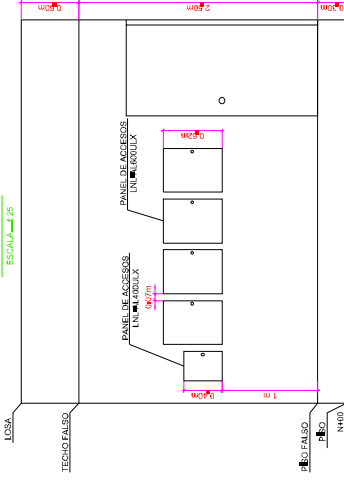
REV.	FECHA	DISEÑADO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Marta Quiroz Arquíeta C. Oro				



UBICACIÓN



VISTA FRONTAL CUARTO DE CONTROL
ESCALA 1:25



VISTA FRONTAL DE TABLEROS
ESCALA 1:25

NOTAS:
EL MOBILIARIO DEL CUARTO DE CONTROL NO SERÁ PROVEDO POR SIEMPRE EN SU ENTERA.

REGISTRO INGENIERÍA / DISEÑO

REV.	FECHA	DISEÑADO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR
0		Martha Guigero Andrés Cajar				

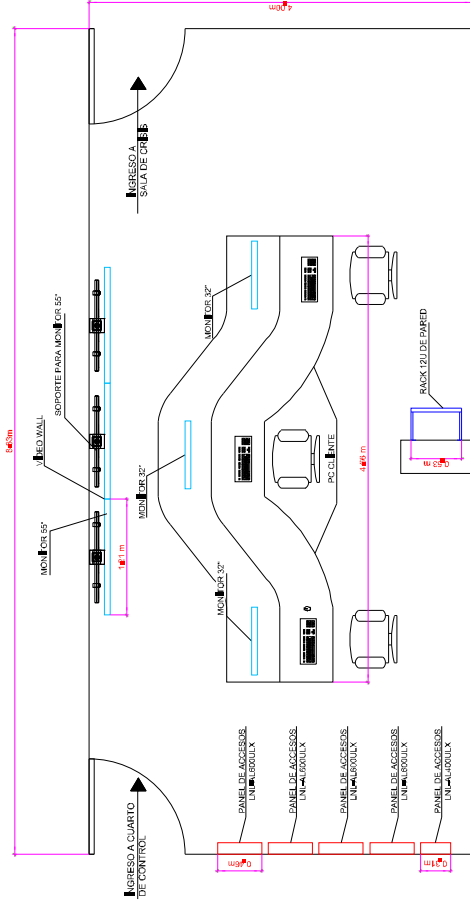
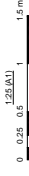
INSTITUCIÓN
AGENCIA DE EFECTUACIÓN
OPERAÇÃO DE ESTACIONES

SIAPROEC
INGENIERÍA Y CONSTRUCCIÓN

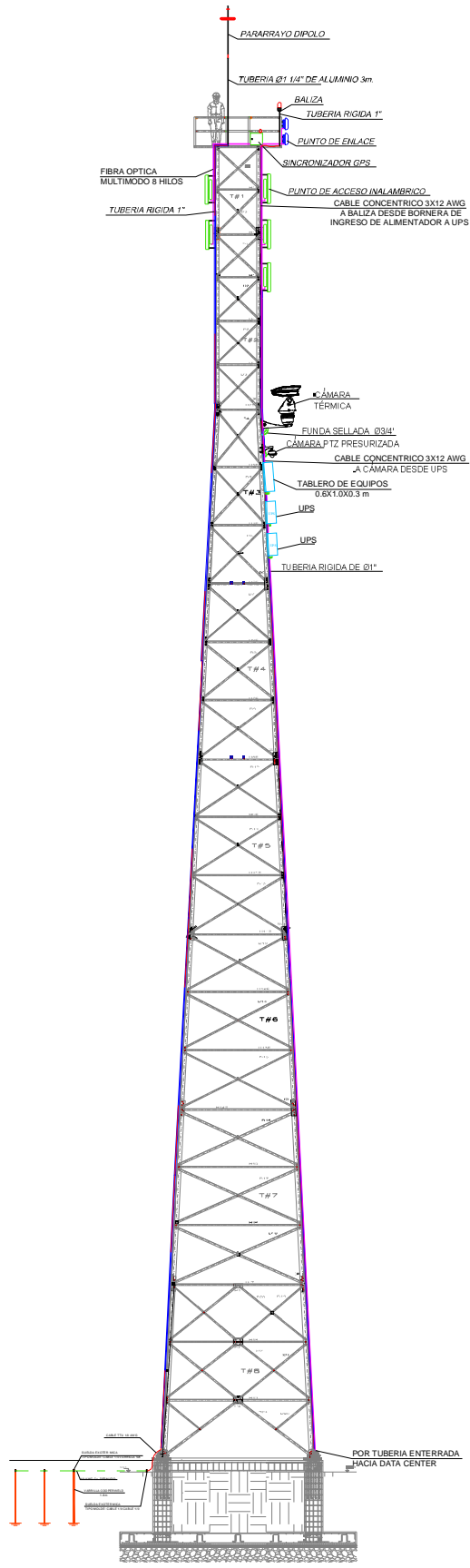
CONTRATO No: 2012064 ESCALA: 1:25

DETALLE - CUARTO DE CONTROL

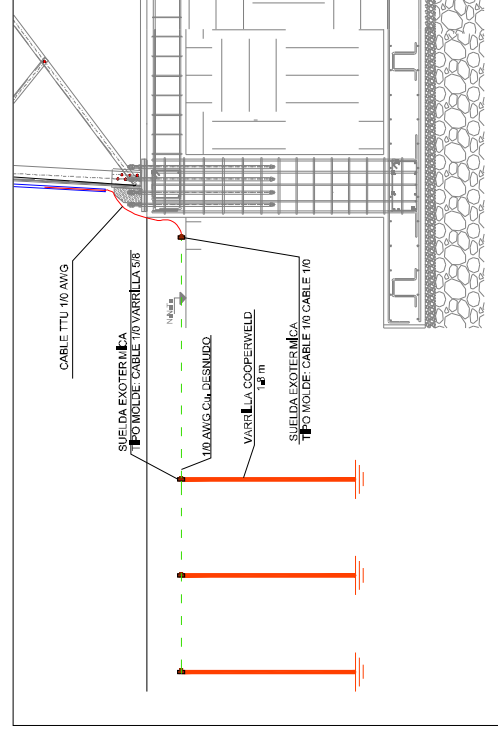
PLANO No: CIV-250 REVISIÓN: 000



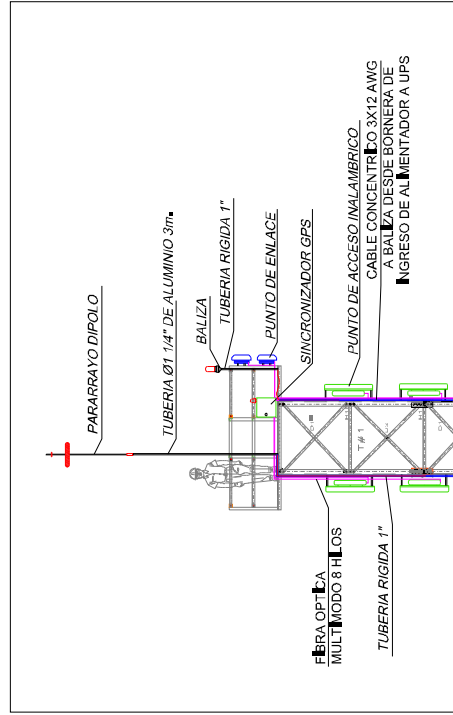
VISTA SUPERIOR CUARTO DE CONTROL
ESCALA 1:25



DETALLE DE ESTRUCTURAL DE TORRE DE COMUNICACION
ESCALA 1:75



VISTA LATERAL DE LA MALLA DE TIERRA DE LA TORRE DE COMUNICACIÓN
ESCALA 1:25



DETALLE DE PARRARAYOS Y BALIZA DE LA TORRE DE COMUNICACIÓN
ESCALA 1:50

NOTA:
- LOS UPS SE UBICARÁN A UNA ALTURA DE 3m EN LA TORRE DE COMUNICACIÓN EN EL PUNTO DE ENLACE A UN NIVEL POR ENCIMA DE LOS UPS. - LAS CÁMARA PIZ Pertenecerán a la TORRE DE COMUNICACIÓN.


Simulpoint
 Ingeniería y Diseño
 Calle 100 No. 100-100, Bogotá, Colombia
 Teléfono: +57 (0)21 2800000
 Email: info@simulpoint.com

REGISTRO INGENIERÍA / DISEÑO			
REV.	FECHA	DISEÑADO	APROBADO
0		Marta Quiroga Arquitecta	

DEFALTE DE CONEXIÓN EN TORRE DE COMUNICACIÓN CON ALIMENTACIÓN ELÉCTRICA			
REV.	FECHA	DISEÑADO	APROBADO

CAPÍTULO 3

DISEÑO CONSTRUCTIVO E IMPLEMENTACIÓN DE LOS MÓDULOS DE SIMULACIÓN DE FUNCIONAMIENTO DE LOS SUBSISTEMAS QUE INTEGRAN LA SEGURIDAD FÍSICA

En este capítulo se describe el criterio de diseño empleado para la construcción, distribución y el software empleados para la implementación de los módulos de simulación de los subsistemas de CCTV y control de accesos que se usan en las pruebas de laboratorio.

Para la implementación de estos módulos se ideó una superficie de montaje de los equipos de manera que estos se puedan distribuir, cablear y conectar entre sí de una manera fácil, ordenada y segura.

3.1 DISEÑO CONSTRUCTIVO E IMPLEMENTACION DE LOS MÓDULOS DE PRUEBAS DEL SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

Para la elaboración de las pruebas de laboratorio de este subsistema se usan los dos tipos de cámaras seleccionadas para el proyecto, de manera que se puedan ejecutar pruebas de monitoreo simultáneo en el software y así comprobar el correcto funcionamiento y manejo de este subsistema.

Se usa dos cámaras fijas para simular el funcionamiento en condiciones reales de la garita vehicular y de la garita peatonal, de este modo se puede comprobar el correcto monitoreo y administración del video grabado en dos ubicaciones fijas diferentes.

Se usa una cámara PTZ para simular el funcionamiento en condiciones reales como las que se tiene en el perímetro de la refinería.

En la figura 3.1 se muestra el esquemático de la red que se armó para hacer las pruebas de laboratorio.

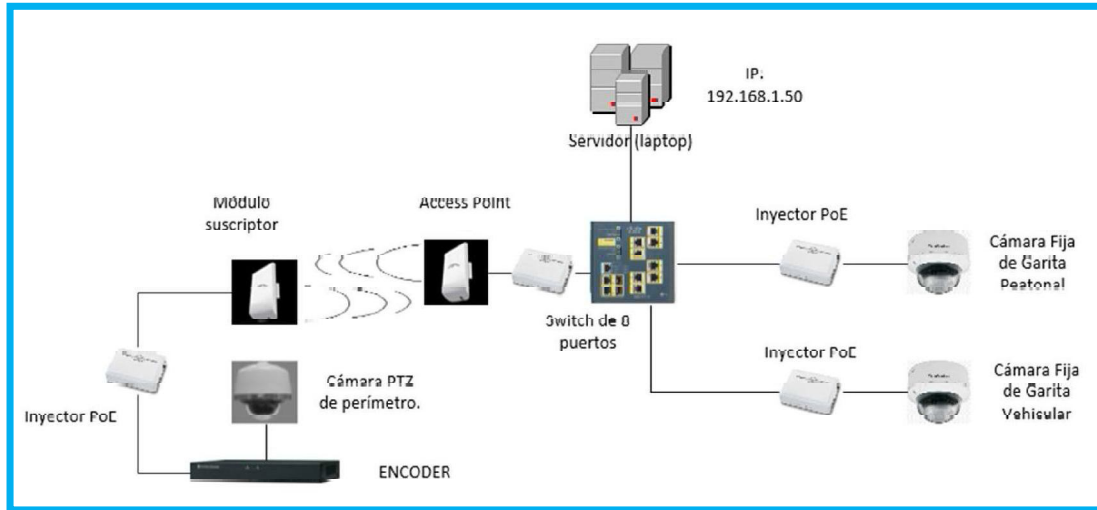


Figura 3. 1 Diagrama de red del subsistema a simular

3.1.1 INSTALACIÓN DE LAS CÁMARAS Y ELEMENTOS COMPLEMENTARIOS PARA LAS PRUEBAS DE LABORATORIO

3.1.1.1 Instalación de la cámara PTZ

Esta cámara se instaló en una ubicación elevada dentro de las inmediaciones de la empresa con el propósito de simular el monitoreo en el perímetro de la refinería.

El funcionamiento de esta cámara se simuló empleando uno de los tableros de poste previamente diseñados y armados. Este tablero contiene en su interior los equipos de video y digitalización necesarios y se lo detalla más adelante, además se usaron dos módulos suscriptores para crear un enlace digital que simula el funcionamiento inalámbrico real de este tipo de cámara.

Se usa un poste para simular el correcto montaje de esta cámara, de manera que, en conjunto con el tablero, se colocan en el sitio elevado previamente seleccionado para probar de manera real su funcionamiento. El conjunto está alimentado desde un tomacorriente de 110 VAC y mediante una fuente interna en el tablero la cámara se abastece de los 24 VAC que requiere para su activación.

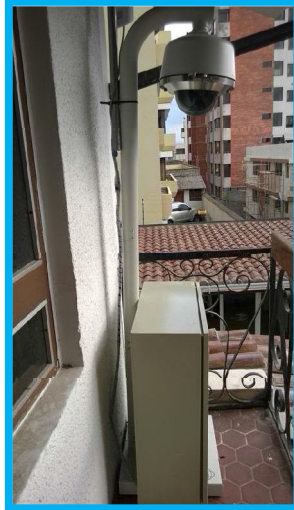


Figura 3. 2 Conjunto de cámara PTZ y tablero electrónico

Siguiendo el esquema de la Figura 3.1 se instalaron los equipos de enlace inalámbrico como se aprecia en las Figura 3.3.



Figura 3. 3 Módulo suscriptor y cámara PTZ montados en conjunto

3.1.1.2 Instalación de las cámaras fijas

Se han usado dos cámaras fijas para simular el monitoreo en tiempo real de dos diferentes ubicaciones mediante el software de monitoreo. En este caso se simula el monitoreo en tiempo real de la garita vehicular y de la garita peatonal.

Usando los elementos de montaje se colocan las dos cámaras sobre la superficie de montaje seleccionada (tablero MDF) de forma que estas puedan ser enfocadas

y ajustadas fácilmente para realizar las pruebas de funcionamiento. Los elementos que se usan para su activación son los inyectores de PoE conectados a un punto de fuerza de 110 VAC de manera que se lleven los datos más alimentación hacia las cámaras como se puede ver en la Figura 3.4.



Figura 3. 4 Cámaras fijas conectadas al equipo PoE

3.1.1.3 Instalación del grabador de video

Para simular el funcionamiento del grabador de video se crea un grabador de video virtual en la maquina física que se usa como punto de monitoreo, de manera que se puede realizar las mismas acciones de visualización de video pregrabado en una partición del disco. Al no ser un elemento físico su configuración se detalla más adelante en este capítulo.

3.1.2 CONFIGURACIÓN DEL SUBSISTEMA DE CCTV

Mediante la correcta configuración de los elementos descritos anteriormente se puede realizar grabaciones y pruebas de monitoreo, exactamente como se realizará en la refinería de Esmeraldas.

El software que se usa para realizar la administración de este subsistema y del subsistema de control de accesos es el ONGUARD que corre sobre el sistema operativo WINDOWS 7 Pro o su versión ULTIMATE. Este se instaló en el servidor (laptop) y se activó la licencia que requiere para manejar los dispositivos que se usan en las pruebas.

Como requisitos básicos para su instalación se tienen que instalar previamente algunos componentes extra y además el equipo servidor debe cumplir con ciertas características que se indican a continuación:

Componentes:

- SQL SERVER 2008 (SOLO SERVIDOR).
- ADOBE READER 10 o una versión superior.
- Crystal .NET components.
- Microsoft DirectX 9.0C o superior.
- Microsoft .NET framework 3.5 SP1 o superior.
- Microsoft XML PARSER 4.0 SP2 o superior.
- Microsoft XML PARSER 6.0

Los anteriores componentes se los tiene en el disco de instalación de ONGUARD por lo que no necesitan ser descargados externamente.

Requisitos básicos del equipo:

- Sistema operativo Windows 7 PRO o superior.
- Memoria RAM DE 4 GB como mínimo.
- Espacio en el disco duro de 15 GB como mínimo.
- Puerto Ethernet 10/100/1000.

El instante en que se finaliza la instalación del software se muestra una pantalla inicial para ingresar la clave y el usuario que por defecto son “sa”, de forma que lo primero que se realiza es el cambio de la clave por parte del administrador para que nadie sin autorización ingrese a las configuraciones del sistema.



Figura 3. 5 Cambio de clave inicial del sistema

3.1.2.1 Configuración del grabador de video (LNVR)

Este equipo físicamente es el encargado de almacenar los diferentes archivos de video generados por las diferentes cámaras que componen el subsistema de CCTV, de manera que tiene una capacidad de almacenamiento elevada, además de tener un respaldo de 16 Terabytes con el uso del grabador de respaldos.

Para realizar las pruebas se usa una laptop (servidor) con una capacidad de almacenamiento destinado de hasta 400 Gigabytes, 12 Gigabytes de RAM y sistema operativo Widows 7 Ultimate de forma que el grabador estará embebido en el propio servidor.

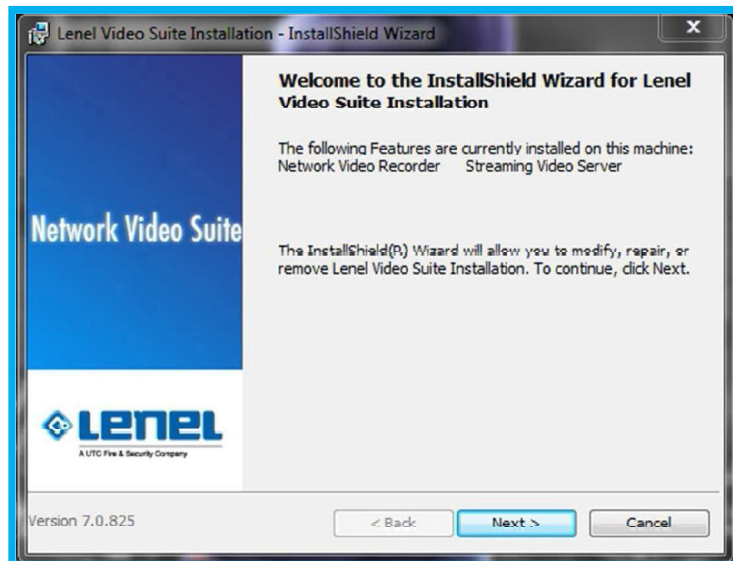


Figura 3. 6 Pantalla de instalación del grabador virtual

Una vez que se ha instalado correctamente el grabador virtual se tiene que configurarlo como un elemento del sistema en el software de integración ONGUARD.

Se ingresa a “System administration” y se digita el usuario y clave de administrador respectivos para ingresar al entorno de configuración.

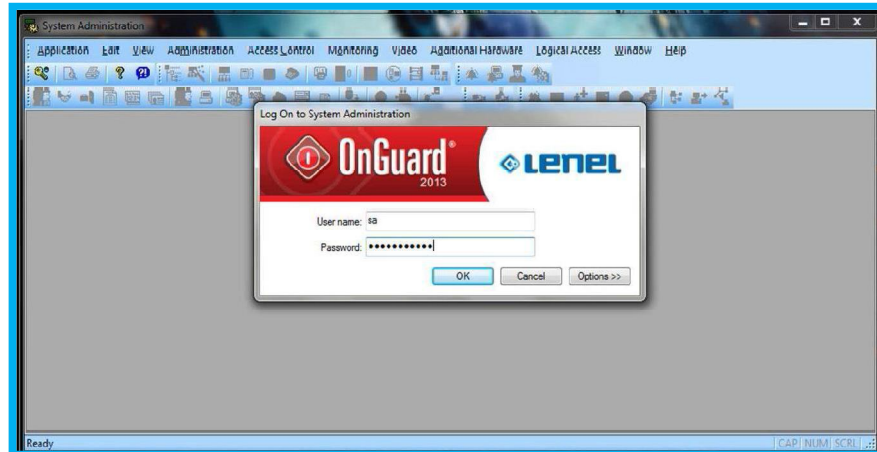


Figura 3. 7 Pantalla de ingreso al administrador del sistema

Una vez ingresado en el entorno de configuraciones, se da clic en el icono denominado Digital Video con lo que se despliega una nueva ventana como se indica en la Figura 3.8.

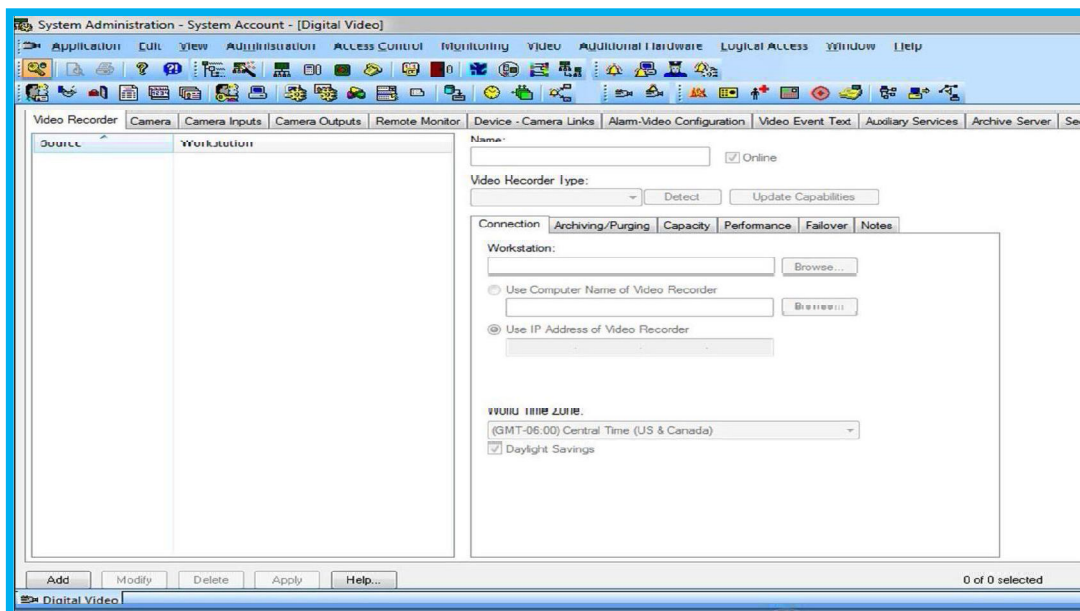


Figura 3. 8 Ventana de configuración de video digital

Se da clic en “ADD (Añadir)” e inmediatamente se despliega un nuevo entorno donde se configura el LNVR previamente instalado. En el caso presente se le da el nombre de Grabador Refinería, se selecciona el tipo de grabador de video, en este caso LNVR.

Al ser un equipo virtual embebido en la laptop no requiere de direccionamiento IP y para que el grabador virtual reconozca como elemento grabador la laptop se le direcciona indicándole el nombre del equipo, en este caso ANDRES.

Para tener una concordancia con las fechas de grabación también se debe seleccionar la misma zona horaria del equipo anfitrión, en este caso la zona horaria de Bogotá, Lima, Quito. En la Figura 3.9 se puede apreciar los parámetros configurados como se ha descrito.

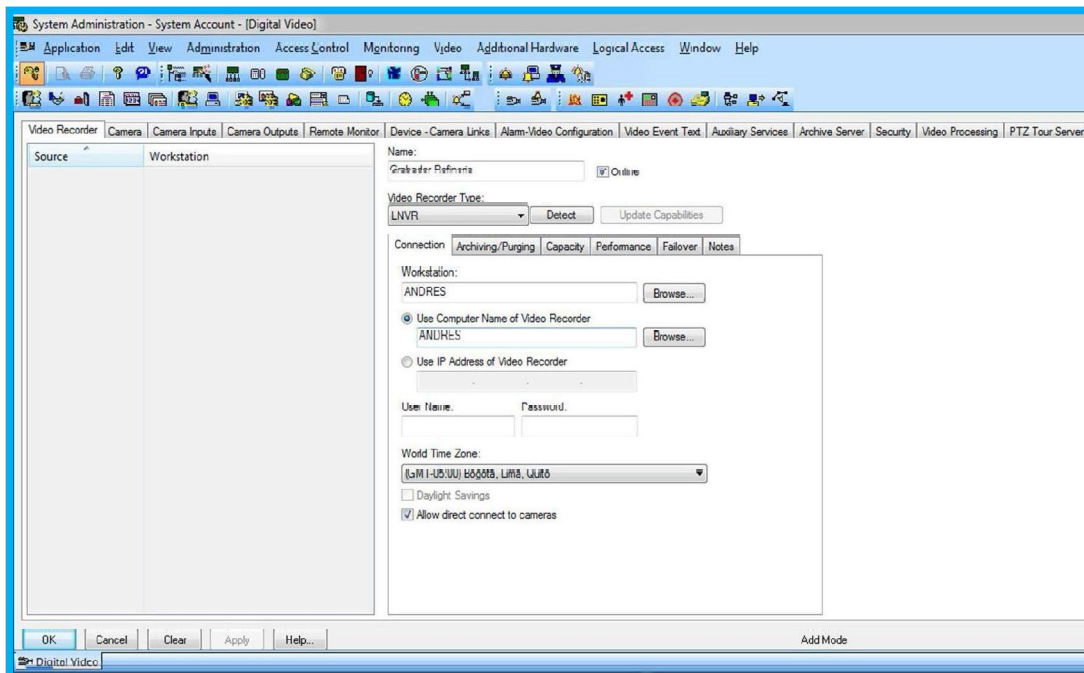


Figura 3. 9 Ventana de configuración de video digital

Una vez se ha establecido todas las características del grabador digital de video se da clic en “OK” en la parte inferior izquierda para finalizar la creación del grabador.

3.1.2.2 Configuración de cámaras fijas

Las dos cámaras seleccionadas son de tipo fijas de manera que necesitan ser ajustadas manualmente y configuradas mediante la red, esto con el objetivo de lograr correctamente su enlace a la red y funcionamiento en condiciones reales.

Se ha establecido que el servidor (laptop) tenga la dirección fija 192.168.1.150 y en esta red privada se configuren el resto de elementos de red a usar.

Las cámaras vienen de fábrica con una dirección IP fija 192.168.0.20 y con sus parámetros de resolución y calidad de video en posiciones iniciales, razón por la cual se debe ingresar a su configuración y cambiar los parámetros necesarios para que se pueda integrar con el programa administrador ONGUARD y que cumplan con la calidad y formato de video requeridos.

Una vez la cámara esté conectada a la red y encendida se ingresa a su configuración usando cualquier navegador de red (Google Chrome, Internet Explorer, etc) y en la barra de direcciones se ingresa la IP de fábrica indicada. Inmediatamente se ingresa al entorno del fabricante de la cámara empleando: “usuario (admin)” y “clave (1234)” para poder ingresar al entorno de configuraciones.

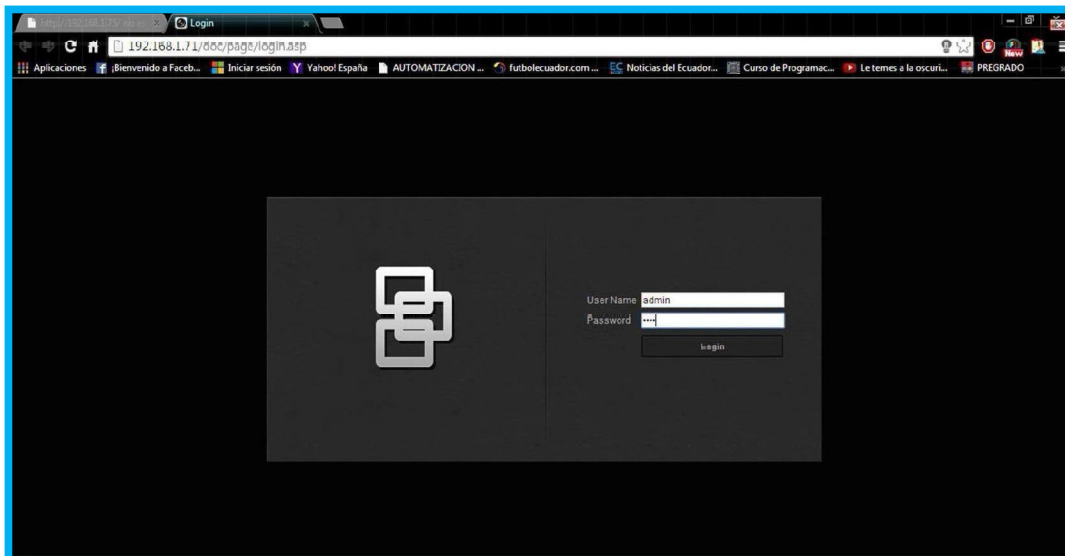


Figura 3. 10 Entorno del fabricante de cámara fija

Al dar clic en login se puede visualizar lo que la cámara está enfocando ese instante en tiempo real como se muestra en la siguiente imagen, pero la cámara aún no está configurada por ello se da clic en la pestaña de Configuration.

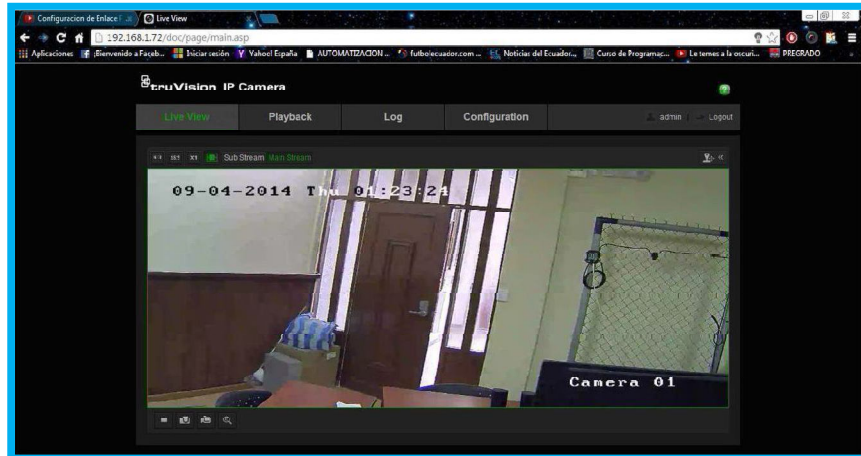


Figura 3. 11 Primera visualización de una cámara antes de configurarse

En la pestaña de Configuration se da clic en “Network” en donde se despliegan los campos necesarios de configuración de red.

En la pestaña de TCP/IP lo primero que se realiza es quitarle la dirección IP de fábrica y darle una nueva, en este caso, para la cámara de la Garita vehicular, se le da la IP 192.168.1.72 y para la cámara de Garita Peatonal se le da la IP 192.168.1.71, para que formen parte de la misma red. Se deshabilita el modo DHCP para que la cámara use la dirección fija asignada y la máscara de subred se mantiene en 255.255.255.0.

Finalmente se hace clic al botón “SAVE” en la parte inferior derecha de la pantalla y se espera a que la cámara se reinicie y adopte los cambios realizados.

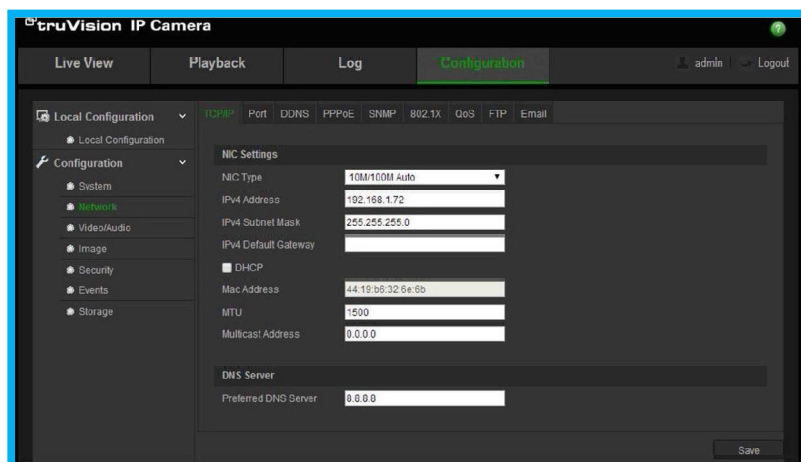


Figura 3. 12 Configuración de parámetros de red

Finalizado los cambios en los parámetros de red se debe configurar los parámetros de video. Para ello se da clic en Video/Audio y en esta pestaña se selecciona el tipo de visualización, en este caso “Main stream (normal)” que permite que el flujo de datos (secuencia de imágenes) sea visualizado prácticamente en tiempo real. Se escoge el tipo de resolución, en este caso como las cámaras son de 3MPX se selecciona la cifra 2048x1536P (aprox. 3000000 P). Otro parámetro es el Bitrate el cual se refiere al flujo de información visualizada e influye directamente en la calidad del video, en este caso se selecciona una calidad media y un bitrate constante, en el caso del frame rate se usa 15 imágenes por segundo (15fsp) esto debido a que con esa cantidad de imágenes se tiene una secuencia de video muy aceptable y el peso del video es mucho menor que usando 30fps que es lo que se tiene en la televisión convencional.

Para el método de compresión del video se usa la norma H.264 que es uno de los métodos más eficientes en cuestión de compresión sin sacrificar la calidad del video almacenado.

En la Figura 3.13 se puede apreciar los campos configurados como se indican previamente.

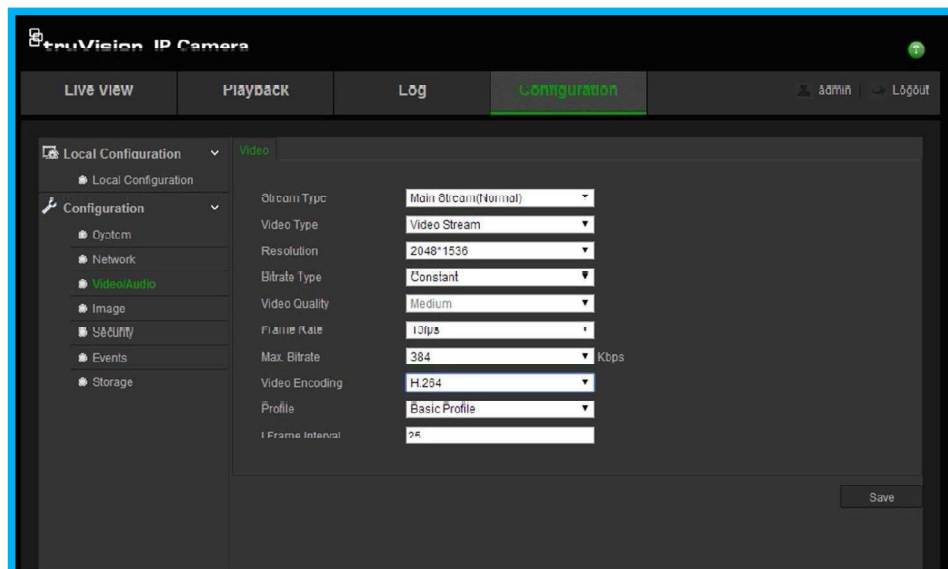


Figura 3. 13 Configuración de parámetros de video

Una vez que se han realizado las configuraciones anteriores en cada una de las dos cámaras fijas, estas se deben integrar en el sistema administrado con el software ONGUARD. Para ello se ingresa a “System administration” y se da clic al icono de “Video digital”. Una vez en el entorno se da clic en la pestaña de Camera y de inmediato se despliega una nueva interfaz en donde se puede integrar las cámaras previamente configuradas.

Primero se debe dar un nombre único a la cámara a integrar como por ejemplo “Cámara Garita Peatonal”; en la pestaña de “Connection” se identifica el modelo de la cámara “(Camera type)” que se está integrando, en este caso, para la garita peatonal, la cámara tiene el modelo Interlogix TVD-M3210V-2-N o en el caso de la garita vehicular el modelo es Interlogix TVD-M32245E-2M-N. Luego se debe indicar la dirección IP de la cámara previamente configurada desde la interfaz del fabricante, para que de este modo el sistema identifique cada cámara y pueda acceder a los datos que esta envía. En el campo de Codec se selecciona nuevamente H.264 para tener concordancia con las configuraciones previas. En el campo de Standard se selecciona NTSC que es el estándar con el que se maneja la región en cuestión de visualización y manejo de las imágenes o cuadros por segundo proyectados para dar la sensación de movimiento.

En los campos de “user name” y de “password” se escriben los mismos datos usados para ingresar a las cámara mediante el navegador de red, esto con la finalidad de que si se necesita realizar algún ajuste se dispone de un botón denominado “Camera web page” el cual nos redirige inmediatamente a la interfaz del fabricante desde el navegador de red disponible para realizar de una manera más ágil dichos cambios.

En el campo denominado “Recorder” se pide el nombre del grabador encargado de almacenar el video adquirido por las cámaras, para la simulación se nombra como “Grabador Refinería” que es el nombre con el que se integra en el sistema.

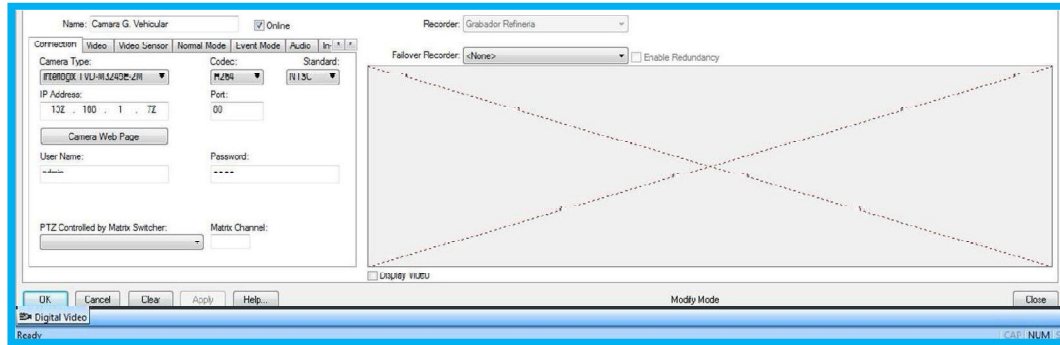


Figura 3. 14 Configuración de parámetros de conectividad para la integración

Ahora se debe ir a la pestaña “Video” en donde se tienen los campos necesarios para poder configurar los aspectos más importantes en cuestión de video; se tiene el campo de resolución que, al igual que en la configuración previa, se selecciona la cifra 2048x1536P. En el campo de rotación la cifra se deja en 0 ya que son cámaras fijas y estas solo enfocan un área específica sin capacidad de redirigirse remotamente.

En el campo de bitrate se mantiene el valor de 384 con el que se realizó la configuración previa y el resto de parámetros y campos se dejan sin cambios. En la Figura 3.15 se puede apreciar estos cambios.

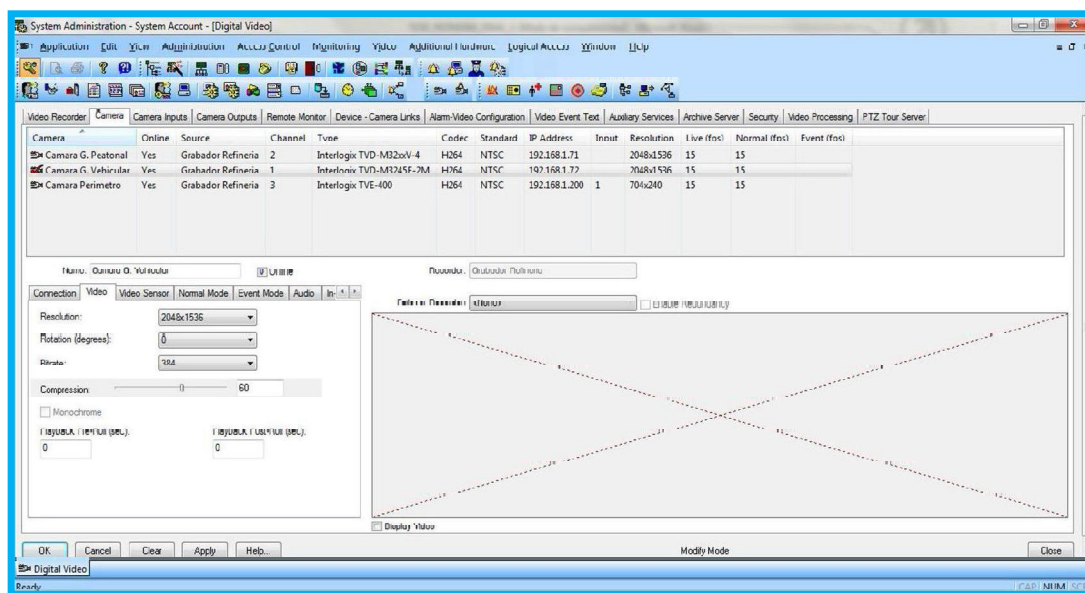


Figura 3. 15 Configuración de parámetros de conectividad para la integración

Una vez realizados los cambios indicados se da clic en OK en la parte inferior izquierda y así se finaliza el proceso de configuración e integración de las cámaras fijas.

Estas cámaras, al no ser equipos de manipulación remota, requieren ser calibradas manualmente para de esta manera ser dirigidas al objetivo a visualizar y sean enfocadas, aprovechando así de mejor forma las capacidades de sus sensores y de sus lentes.

Luego se debe ingresar al visualizador de video primario que se dispone si se ingresa a los parámetros de la cámara desde el navegador, en este se puede ver lo que ve la cámara en tiempo real y así modificar la posición de esta y redirigirla a un punto de interés, en este caso para el efecto de calibración y posteriores pruebas la puerta de ingreso es un objetivo y el escritorio donde está el servidor (laptop) es el segundo objetivo.

Una vez dirigidas las cámaras a sus objetivos estas deben ser enfocadas, para este efecto se tienen dos tornillos de ajuste en el interior de la cámara, específicamente ubicados en el cañón, que permiten girar el arreglo de lentes de las cámaras y así tener una mejor imagen de la que viene de fábrica. En las figuras 3.16 y 3.17 se tiene el ejemplo claro del efecto de acomodar manualmente el arreglo de lentes para tener una imagen más nítida usando los elementos de enfoque (tornillos de ajuste).

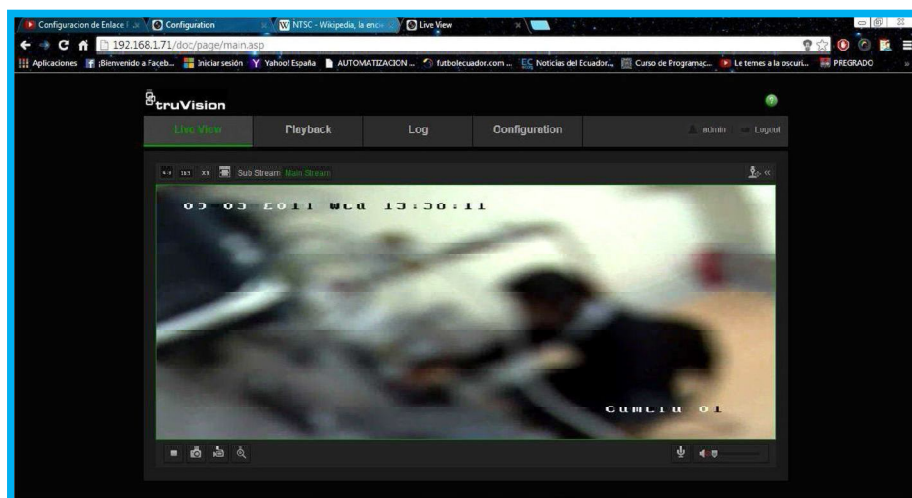


Figura 3. 16 Imagen sin modificar el enfoque de fábrica

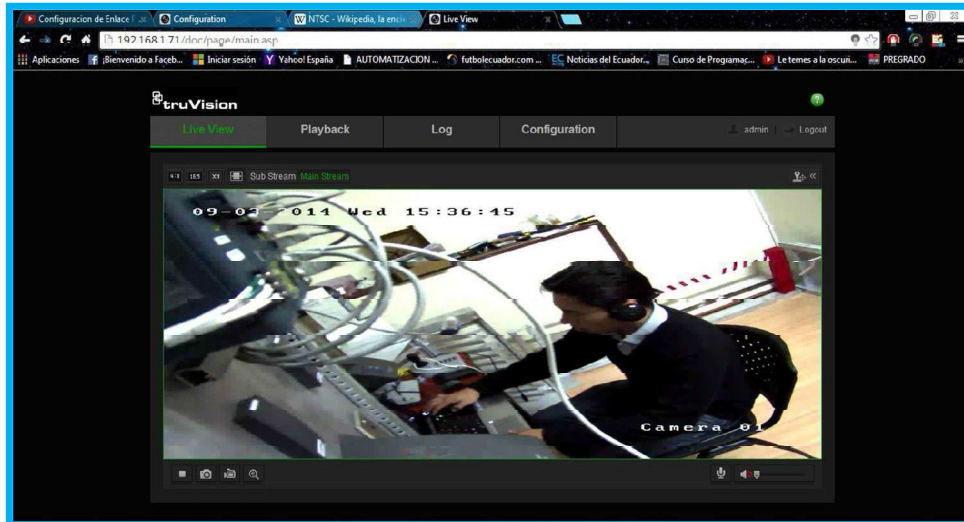


Figura 3. 17 Imagen después de modificar el enfoque

3.1.2.3 Configuración de la cámara PTZ

Debido a que la cámara PTZ es un equipo analógico, por sí sola no puede ser integrado a un sistema informático de red, por esto se emplea un video encoder, que se configura e integra a la red como se puede ver en el esquemático de la Figura 3.1.

Como se ha indicado previamente, para el caso de esta cámara se simula su funcionamiento real mediante el uso de equipos de comunicación inalámbrica, entonces, previo a la configuración de la cámara, se debe configurar el enlace inalámbrico usado para visualizar el video proveniente de esta.

Se debe aclarar que los enlaces inalámbricos usados para la simulación son diferentes a los reales, ya que estos ya se están montado en las inmediaciones de la refinería a pedido de fiscalización.

El funcionamiento es similar, la diferencia es el costo y la calidad un tanto menor.

3.1.2.3.1 Configuración del enlace inalámbrico

El enlace inalámbrico se crea usando dos equipos de transmisión recepción que enlazan un A.P. con su respectivo modulo suscriptor.

En este caso se definirá al equipo 1 como el Access Point y al equipo 2 como el modulo suscriptor encargado de transmitir el video de la cámara PTZ. Tal como

se indicó en la Figura 3.1 el equipo 1 se conecta desde su ubicación en los exteriores hacia el switch de 8 puertos instalado en la maqueta. El equipo 1 y 2 manejan el estándar IEEE 802.3af razón por la que disponen de sus propios inyectores PoE uno de estos conectado a la red eléctrica para así darle la energía que necesita el primer equipo.

El equipo 2 se instala en el poste de la cámara de manera que tenga línea de vista con el primero y también que se conecte al inyector de PoE y este a su vez al puerto de red que dispone el encoder instalado en el tablero en esta ubicación.

Una vez instalados los equipos en sus respectivas posiciones se empezó a realizar las configuraciones empezando por energizar el equipo 1.

Se debe configurar el Access point. Para esto se debe ingresar a su interfaz de usuario, para modificar las direcciones IP provistas de fábrica. En este caso ambos equipos tienen la dirección 192.168.1.20.

Se ingresa a la interfaz de configuraciones usando esa dirección IP y de “usuario” y “password” la secuencia de letras UBNT como se puede apreciar en la Figura 3.18.

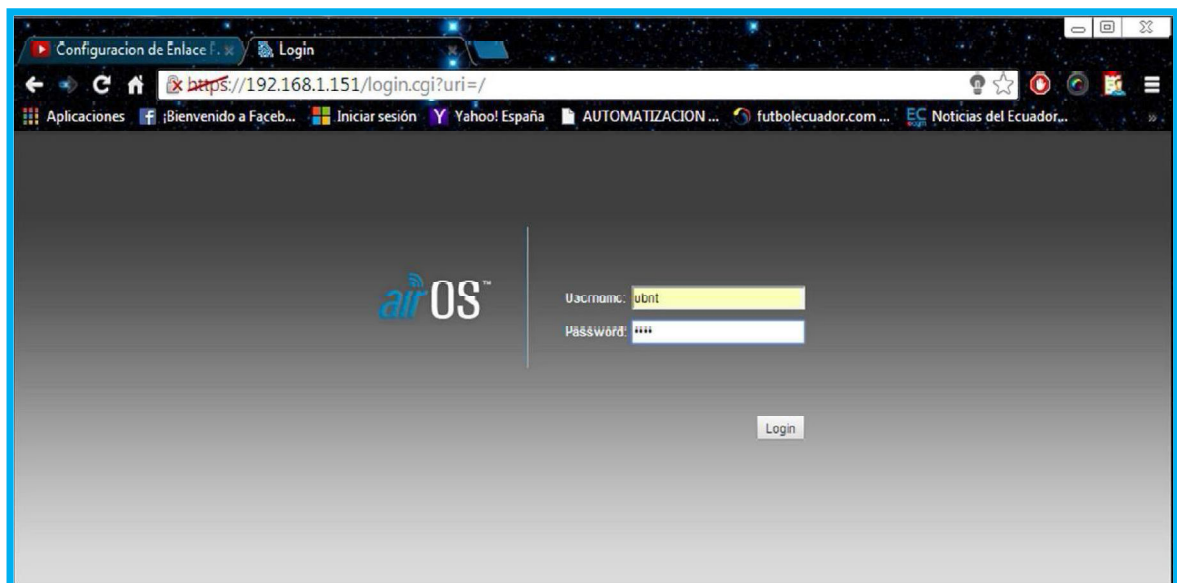
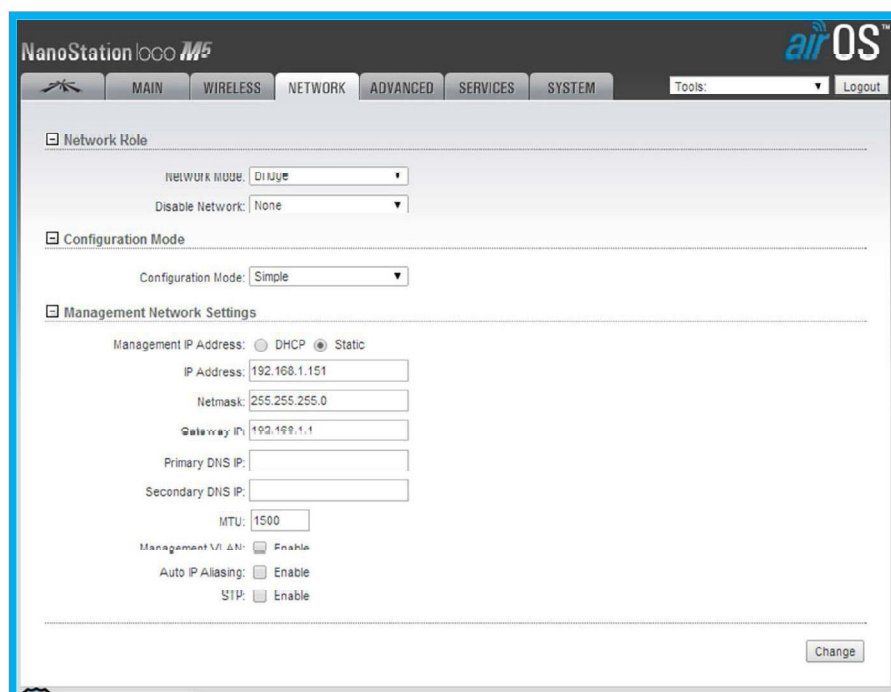


Figura 3. 18 Interfaz de ingreso de los equipos inalámbricos

Al dar clic en “login” se puede ingresar a las diferentes pestañas de parámetros de configuración; en la pestaña “network” se configura la dirección IP estática 192.168.1.151, la máscara de subred se mantiene en 255.255.255.0 y el Gateway se cambia al mismo que posee el servidor (laptop), en este caso 192.168.1.1. El resto de campos se mantienen y para finalizar se da clic en “Change” en la parte inferior derecha y “Apply” en la parte superior derecha, de esta manera se reinicia el dispositivo y se configura la nueva dirección IP asignada.

Antes de seguir con las configuraciones es necesario tomar nota de la dirección MAC del puerto WLAN de este dispositivo ya que para establecer el enlace se necesita registrar este dato en uno de los campos del segundo equipo. El puerto WLAN tiene la dirección MAC 04:18:D6:5A:F1:D9 que se puede ver en la pestaña MAIN.



The screenshot displays the 'Network' configuration page of the NanoStation loco M5 air OS. The interface includes a navigation menu with tabs for MAIN, WIRELESS, NETWORK, ADVANCED, SERVICES, and SYSTEM. The 'NETWORK' tab is active. The configuration is organized into sections: 'Network Role' with 'Network Mode' set to 'Bridge' and 'Disable Network' set to 'None'; 'Configuration Mode' set to 'Simple'; and 'Management Network Settings' where 'Management IP Address' is set to 'Static'. The static IP address is 192.168.1.151, the netmask is 255.255.255.0, and the gateway is 192.168.1.1. Other settings include Primary DNS IP, Secondary DNS IP, MTU (1500), and checkboxes for Management VLAN, Auto IP Aliasing, and STP, all of which are currently disabled. A 'Change' button is located at the bottom right of the configuration area.

Figura 3. 19 Configuraciones de red del equipo Access Point

El instante que se aplican los cambios indicados previamente el equipo se reinicia y es necesario ingresar de nuevo a sus opciones de configuración pero ahora ya con la nueva dirección IP asignada. Una vez dentro se debe ahora configurar los campos de comunicación inalámbrica.

En el campo de modo de “Wireless” se selecciona modo “Access Point”, en el campo de SSID (Service Set Identifier) se cambia el identificador a ubnt_link para diferenciar nuestra red inalámbrica de posibles redes presentes en el ambiente. Se selecciona el país y la frecuencia con la que operará el enlace, en este caso como parámetro recomendado por el fabricante se ocupa la frecuencia de 5300 MHz. En el campo de seguridad de la red se usa el modo WPA2-AES para tener un nivel de encriptación de la información muy elevado. Para darle aún más seguridad al enlace se habilita el campo “Autenticación WPA” y se selecciona “PSK” (claves pre compartidas). De esta manera el equipo permite crear una clave para poder ingresar a la red. Una vez realizados los cambios se da clic en “Change” en la parte inferior derecha y “Apply” en la parte superior derecha y así se tiene el primer equipo configurado.

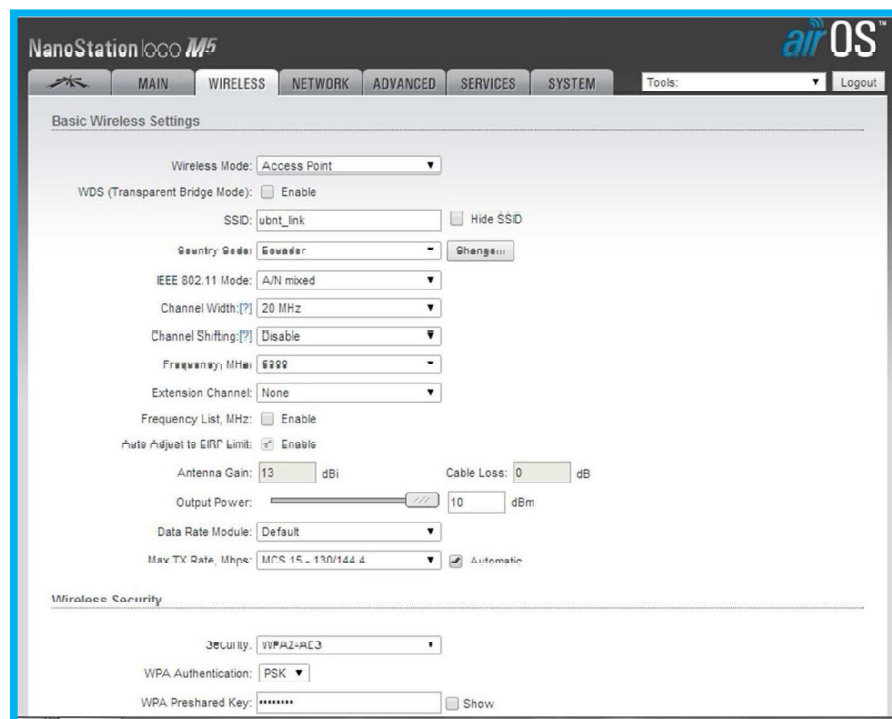


Figura 3. 20 Configuraciones de características inalámbricas del equipo AccessPoint

Al igual que el equipo 1 (Access Point) el equipo 2 está con sus parámetros de fábrica y se deben modificar para poder finalizar el levantamiento del enlace inalámbrico.

Como se hizo en el primer equipo se debe dar una nueva dirección IP, en este caso el equipo 2 (modulo suscriptor) tiene la IP 192.168.1.152 con la misma mascara de sub red 255.255.255.0 y con el mismo Gateway 192.168.1.1. Se aplica los cambios y se ingresa a la pantalla de configuraciones nuevamente pero con la nueva IP designada.

Para finalizar es necesario configurar los parámetros de conexión inalámbrica como se hizo con el primer equipo. Para ello se ingresa a la pestaña Wireless y se cambia el modo de “Wireless” a modo de “Station”. En el campo de SSID se escribe el mismo identificador del primer equipo (ubnt_link). En el siguiente campo denominado Lock to AP MAC se debe escribir la dirección MAC que se tomó nota previamente perteneciente al primer equipo la cual es 04:18:D6:5A:F1:D9. Se selecciona el país y, al igual que en el primer equipo, se debe darle un nivel de seguridad como es WPA2-AES con el parámetro extra de PSK de manera que sea el mismo usuario y clave del primer equipo. Luego se da clic en “Change” en la parte inferior derecha y “Apply” en la parte superior derecha para finalizar con el proceso de configuración.

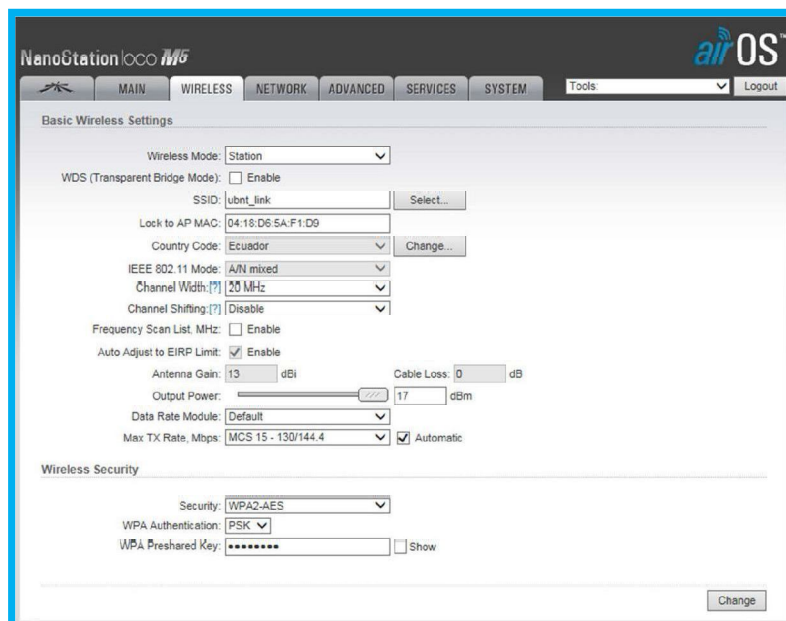


Figura 3. 21 Configuraciones de características inalámbricas del equipo modulo suscriptor

Para tener constancia de que se ha establecido el enlace inalámbrico se selecciona la pestaña “MAIN” de la interfaz del segundo equipo (Modulo Suscriptor) y se verifica que en la parte derecha las barras de fuerza de la señal, “Calidad Airmax” y “Capacidad Airmax” estén activas y su porcentaje este cercano al 100%, de este modo se tiene la certeza de que el enlace inalámbrico se ha establecido correctamente como se puede apreciar en la Figura 3.22.



Figura 3. 22 Graficas y barras del enlace inalámbrico establecido

Al tener listo el enlace inalámbrico se procede a continuación a configurar el encoder con el que se maneja la cámara PTZ. Para ello se ingresa al navegador de red y se ingresa a la dirección IP 192.168.0.70 que es la dirección que el equipo trae de fábrica. Al igual que en las cámaras fijas se tiene la misma clave de ingreso (1234) y el mismo usuario (admin), de forma que dentro de la configuración en la pestaña de “Parámetros Básicos (Basic settings)” de este equipo lo primero que se debe realizar es cambiar la dirección IP en “NIC (NIC settings)”, que para este caso es 192.168.1.200. Se deshabilita el modo DHCP, y el campo de mascara de subred se mantiene en 255.255.255.0 y el resto de campos de esta pestaña se dejan como vinieron de fábrica, se da clic en “Save”

en la parte inferior izquierda y el equipo se reiniciara para ingresar nuevamente pero con la nueva dirección IP asignada.

A continuación se puede ver la Figura 3.23 del procedimiento previamente descrito para el equipo.

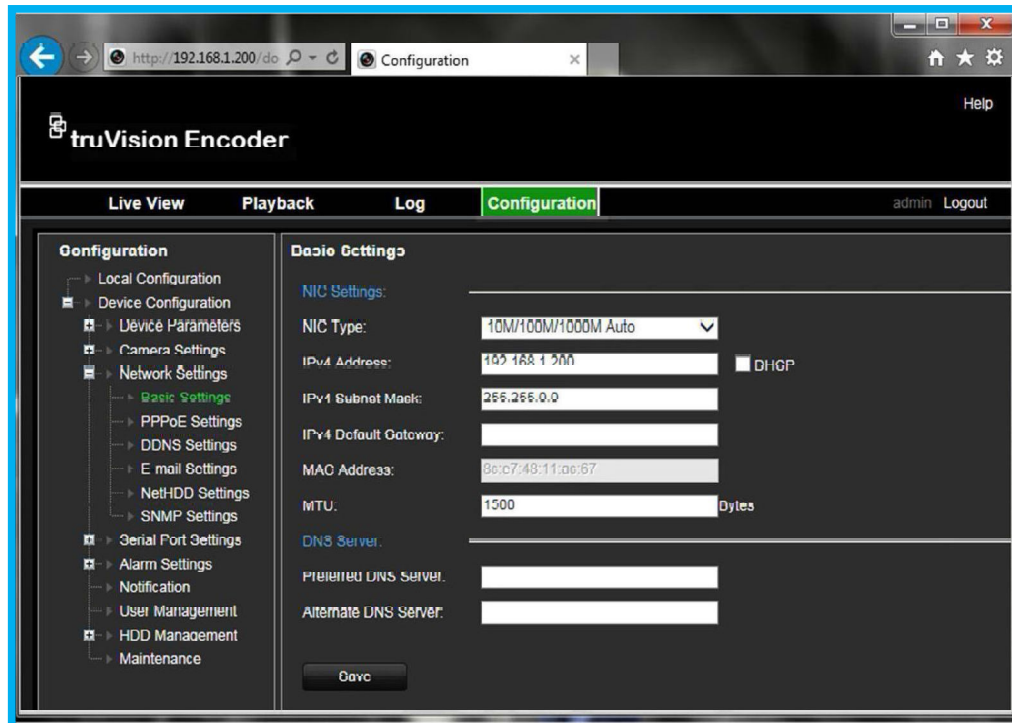


Figura 3. 23 Configuración de los parámetros de red del encoder

Se necesita configurar los parámetros de la cámara PTZ asociada a este equipo para ello se ingresa a “Parámetros de cámara (Camera settings)” y en la sub pestaña de “parámetros de video (video settings)”, donde se identifica el tipo de cámara en este caso “Cámara analógica”. Se selecciona “parámetros de codificación”. En este caso se selecciona “Main stream (normal)”, en el campo de “Stream type” se selecciona “Video únicamente” ya que la cámara no posee características de captura de audio.

La resolución se establece automáticamente al seleccionar un elemento de tipo analógico, el resto de parámetros como el bitrate o el frame rate se establecen con valores similares a los de las cámaras fijas como se puede apreciar en la Figura 3.24.

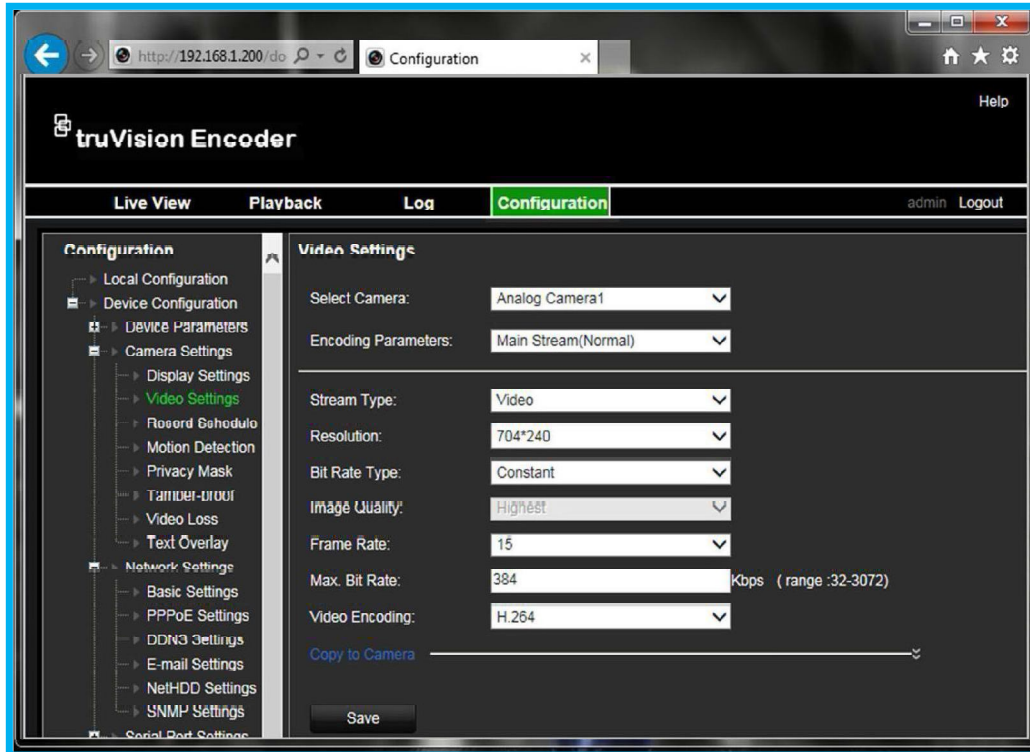


Figura 3. 24 Configuración de los parámetros de video del encoder

Realizados los cambios señalados se da clic en “Save” y el sistema se reinicia para ingresar nuevamente y en la pestaña de “Live View” se puede visualizar en tiempo real lo que la cámara está enfocando.

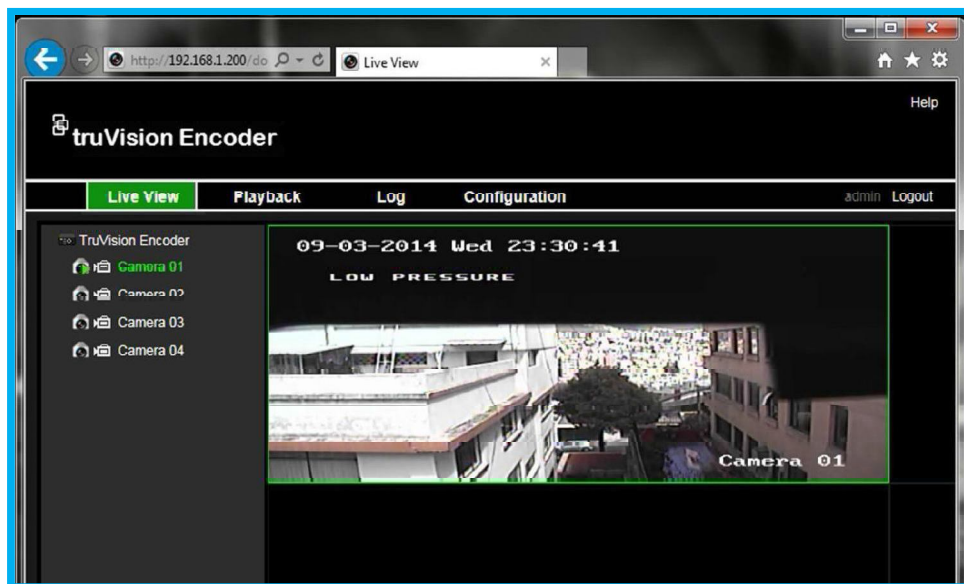


Figura 3. 25 Primera visualización de la cámara PTZ

A diferencia de las cámaras fijas esta se puede reenfozar y redirigir remotamente y no es necesario realizar ajustes manuales a sus arreglos de lentes.

Una vez que se ha verificado el funcionamiento de esta cámara usando el encoder se debe integrarla al sistema administrador ONGUARD.

Se ingresa a “System administration” y se da clic en el icono de “video digital” para acceder a los campos de integración.

De la misma manera que se integraron las cámaras fijas se integra esta cámara con un nombre diferente (Cámara perímetro) y al seleccionar el modelo de cámara lo que se selecciona es el modelo del video web server, en este caso es el Interlogix TVE-400. Se indica la dirección IP del encoder en este caso 192.168.1.200 y en el campo denominado “Input number” se selecciona el número de canal analógico en el que está conectada físicamente la cámara, en este caso el canal es el 1.

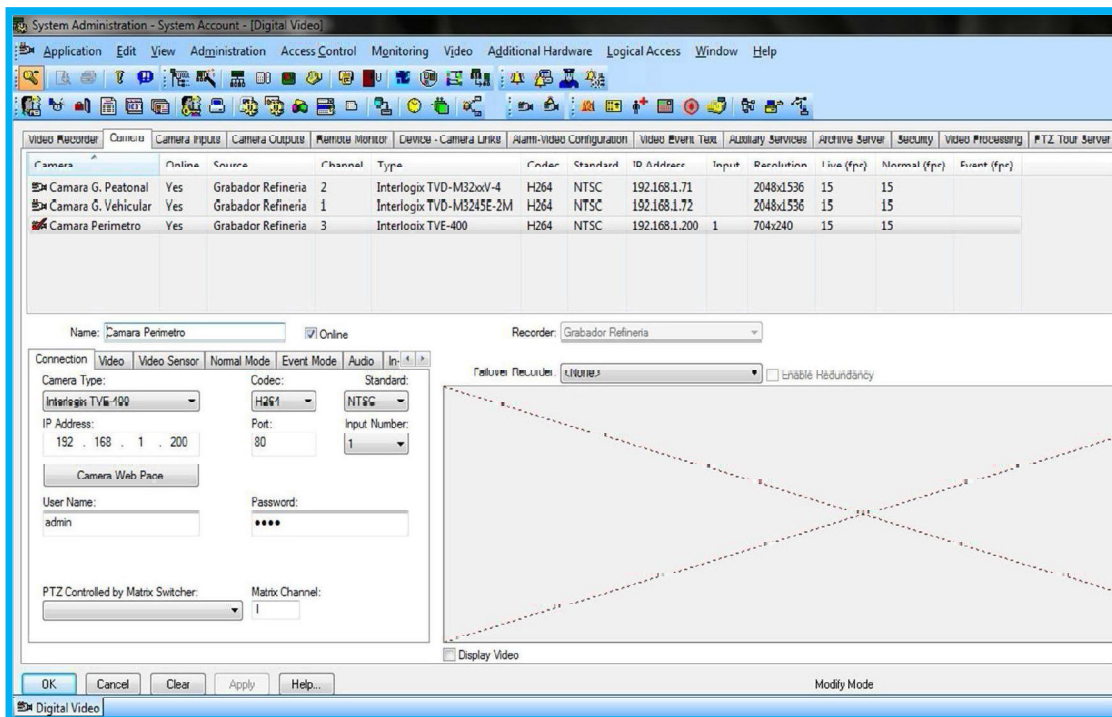


Figura 3. 26 Configuración de conexiones de la cámara PTZ

En la pestaña de video se cambian los campos con valores similares a los que se configuró previamente desde el navegador de red.

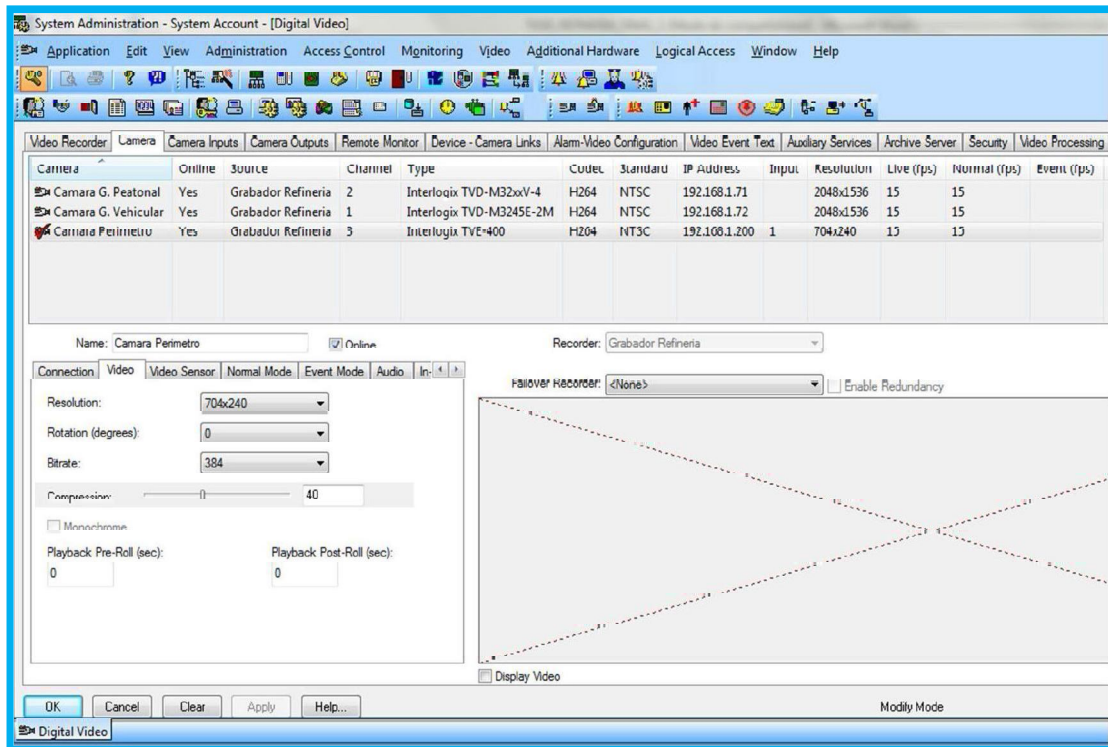


Figura 3. 27 Configuración de video de la cámara PTZ en ONGUARD

Para finalizar el proceso de configuración e integración se da clic en “OK” en la parte inferior izquierda. Una vez terminados los procesos en el sistema administrador se puede ver un listado de las cámaras enroladas como se puede ver en la siguiente figura.

Camera	Online	Source	Channel	Type	Codec	Standard	IP Address	Input	Resolution	Live (fps)	Normal (fps)	Event
Camara G. Peatonal	Yes	Grabador Refineria	2	Interlogix TVD-M32xxV-4	H264	NTSC	192.168.1.71		2048x1536	15	15	
Camara G. Vehicular	Yes	Grabador Refineria	1	Interlogix TVD-M3245E-2M	H264	NTSC	192.168.1.72		2048x1536	15	15	
Camara Perimetro	Yes	Grabador Refineria	3	Interlogix TVE-400	H264	NTSC	192.168.1.200	1	704x240	15	15	

Figura 3. 28 Cámaras integradas en el sistema ONGUARD

3.2 DISEÑO CONSTRUTIVO E IMPLEMENTACION DE LOS MODULOS DE PRUEBAS DEL SUBSISTEMA DE CONTROL DE ACCESOS

Para simular el funcionamiento en condiciones reales de los diferentes equipos que componen este subsistema se ha decidido usar las diferentes tarjetas electrónicas de las tres ubicaciones con el conjunto de elementos que se manejan mediante estas. Ya que estos equipos se tienen disponibles, la empresa junto con la fiscalización acordaron realizar pruebas con los equipos, previo a su implementación en la refinería, esto con el objetivo de que se detecten posibles fallos y que la fiscalización tenga una idea clara del funcionamiento de este subsistema.

En la Figura 3.29 se puede apreciar el diagrama de la red con los elementos del subsistema de “Control de accesos” usados para realizar la simulación.

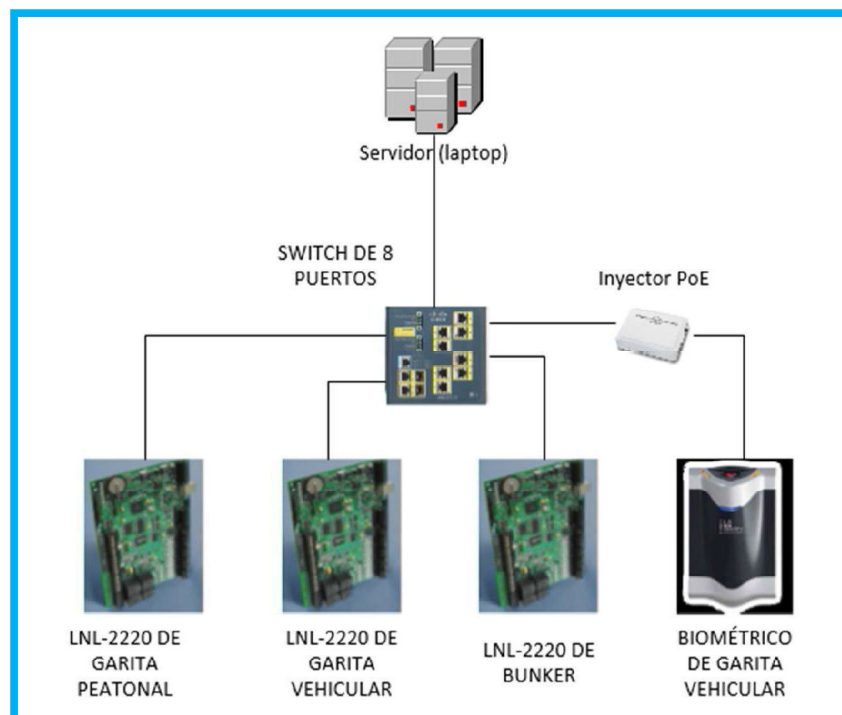


Figura 3. 29 Diagrama de red del subsistema a simular

A continuación se detalla la distribución de los equipos usados para la simulación en cada ubicación a controlarse con el sistema.

3.2.1 INSTALACION DE EQUIPOS DE CONTROL DE ACCESOS Y ELEMENTOS COMPLEMENTARIOS PARA ELABORAR LAS PRUEBAS DE LABORATORIO

Para elaborar el módulo de pruebas y las posteriores pruebas de laboratorio se usan 5 tableros electrónicos distribuidos de la siguiente forma:

Tablero 1 garita peatonal:

- Posee: una controladora LNL-2220, cinco LNL-1320, una fuente de 12 VDC a 6 Amp y una fuente de 24 VDC a 2.5 Amp.
- Controla: 4 lectoras R10 de proximidad y las maquetas de simulación de una espina de pescado (torniquete) y de una puerta de discapacitados motorizada.

Tablero 2 garita peatonal:

- Posee: dos tarjetas electrónicas LNL-1320, una tarjeta de integración de handkeys LNL-500B, una fuente de 12VDC a 6 Amp y una fuente de 24VDC a 2.5 Amp.
- Controla: dos handkeys y dos juegos de luces indicadoras de ingreso.

Tablero 1 garita vehicular:

- Posee: una controladora LNL-2220, dos LNL-1320, una fuente de 12VDC a 6 Amp y una fuente de 24 VDC a 2.5 Amp.
- Controla: dos lectoras vehiculares con sus respectivas maquetas de barreras vehiculares y dos lectoras de proximidad R10 con su respectivo molinete.

Tablero 2 garita vehicular:

- Posee: dos tarjetas electrónicas LNL-1320, una tarjeta de integración de handkeys LNL-500B, una fuente de 12VDC a 6 Amp y una fuente de 24 VDC a 2.5 Amp.
- Controla: un biométrico de huellas dactilares y un lector de geometría de mano (handkey).

Tablero bunker:

- Posee: una controladora LNL-2220, una LNL-1320 y una fuente de 12VDC a 6 Amp.
- Controla: dos lectoras de proximidad R10, una chapa electromagnética de 1200 lbf asociada a una puerta y un contacto magnético.

Se construyeron maquetas que simulan el funcionamiento de una espina de pescado real (torniquete), una maqueta que simula el funcionamiento de una puerta motorizada de discapacitados, una maqueta de dos barreras vehiculares y una maqueta de un molinete. Todas estas maquetas se han creado con características similares a los equipos reales y se escalaron aproximadamente a 0.35 veces el tamaño de los equipos reales.

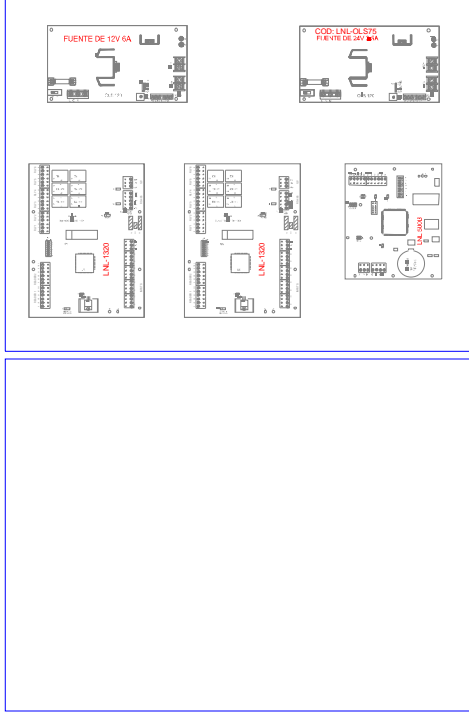
En el plano EE-800 y en el plano EE-801 se puede apreciar la distribución de las tarjetas electrónicas y fuentes de poder en el interior de los gabinetes correspondientes a las diferentes ubicaciones.

GARITA VEHICULAR

PANEL 1

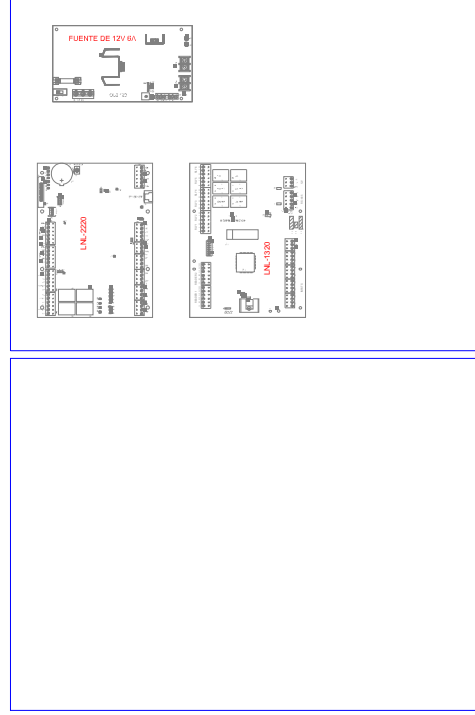


PANEL 2



BUNKER

PANEL 1



REGISTRO INGENIERIA / DISEÑO									
REV.	FECHA	DISEÑADO	REVISADO	APROBADO	FISCALIZADOR	COORDINADOR	PLANO No.	REVISION	000
0		Mariela Quijero Andres Cajo							
DISTRIBUCION DE TARJETAS Y FUENTES EN PANELES DE ACCESOS									
CONTRATO No.: 202004 ESCALAS:									
DISTRIBUCION DE TARJETAS Y FUENTES EN PANELES DE ACCESOS									
PLAN No.: EE-801 REVISION: 000									

3.2.2 CONFIGURACION DEL SUBSISTEMA DE CONTROL DE ACCESOS

Al haber previamente instalado y activado correctamente la licencia del software ONGUARD para la integración del subsistema de CCTV se tiene que iniciar con la integración de las controladoras LNL-2220 que son la base del funcionamiento de este subsistema.

3.2.2.1 Configuración de la controladora LNL – 2220

Una vez que la tarjeta está correctamente alimentada a 12 VDC, se encienda correctamente y está conectada a la red mediante el switch de 8 puertos se debe ingresar a su configuración, para ello se usa el navegador de red y se ingresa a la dirección IP 192.168.0.251 que es la que proveen de fábrica.

Al realizar esto se despliega una pantalla de ingreso en la que se debe ingresar el nombre de “usuario (admin)” y la clave de fábrica que es “password”.

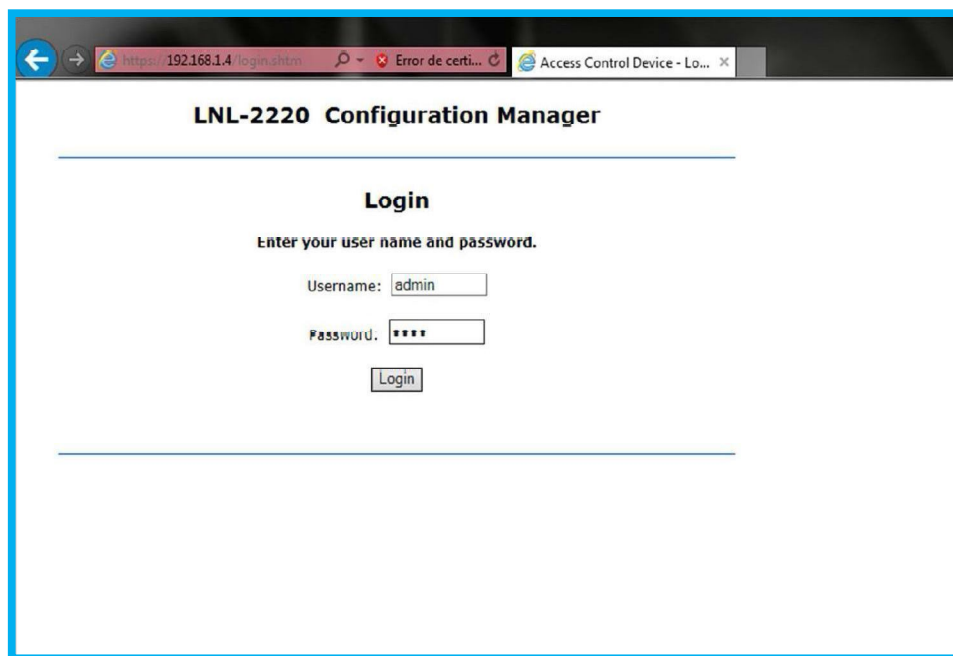


Figura 3. 30 Pantalla de ingreso a la interfaz de configuraciones

Una vez se ha ingresado se tiene varios parámetros que la tarjeta permite configurar. Para las pruebas se necesita modificar los parámetros de red.

Se da clic en “Network” y en esta nueva ventana se modifica los parámetros de red como se puede ver en la Figura 3.31.

LENEL LNL-2220 Intelligent Dual Reader Controller

Network Settings

Use DHCP method to obtain IP address automatically
 Host name of this device:
(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

Use Static IP configuration.

IP Address:
 Subnet Mask:
 Default Gateway:
 DNS Suffix:
(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

Obtain DNS server address automatically
 Use the following DNS server address.

DNS Server:

* Select **APPLY SETTINGS** to save changes.

Figura 3. 31 Configuración de parámetros de red LNL – 2220

Finalizado lo anterior se da clic en Host Com y se configuran los campos como se indica en la siguiente figura.

LENEL LNL-2220 Intelligent Dual Reader Controller

Host Communication

Communication Address: Use IPv6

Primary Host Port

Connection Type: Data Security:

Port Number:

Allow All Authorized IP Address Required

Authorized IP Address:

* Select **APPLY SETTINGS** to save changes.

Figura 3. 32 Configuración de parámetros de huésped de LNL – 2220

Para finalizar la configuración de la tarjeta controladora LNL-2220 se da clic en “Apply Settings” que está ubicado en la parte izquierda de la pantalla que hace que la tarjeta se reinicie con los cambios realizados.

Con los cambios previamente realizados se debe integrar la tarjeta al sistema administrador ONGUARD, para ello se ingresa a “System Administration” y se da clic en el icono denominado “Access Panels” de manera que se despliega una nueva pantalla donde se debe seleccionar la pestaña LNL-2220 que son el modelo de la controladora a usar.

Se da clic en “ADD” y de inmediato se despliega una nueva ventana en donde en la pestaña denominada “Location” se debe establecer los valores de los campos como son la Workstation (Nombre del servidor – laptop), se escoge la zona horaria y se le da un nombre único como se muestra en la Figura 3.33. Para el módulo de pruebas se establece como nombres de las 3 controladoras usadas los siguientes:

Garita peatonal: LNL – 2220 GARITA PEATONAL

Garita vehicular: LNL – 2220 GARITA PEATONAL

Bunker: LNL - 2220 BUNKER

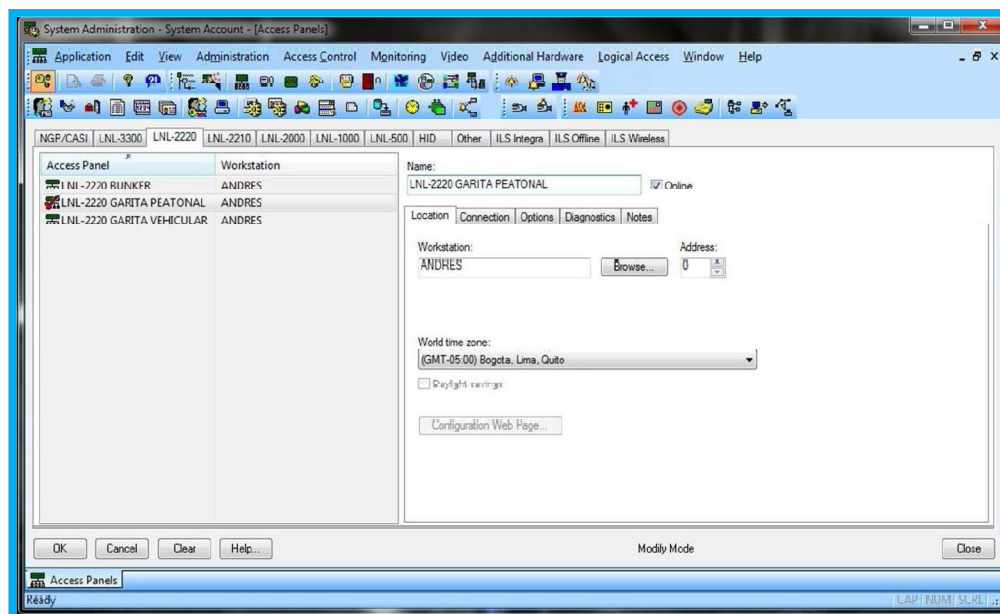


Figura 3. 33 Integración de controladora LNL – 2220

A continuación se da clic en la pestaña “Connection” en donde se debe llenar los campos de direccionamiento IP, de manera que para la garita peatonal se tiene la dirección 192.168.1.2, para la garita vehicular la dirección 192.168.1.3 y para el bunker la dirección 192.168.1.4; el puerto es el mismo que se configuró previamente (3001).

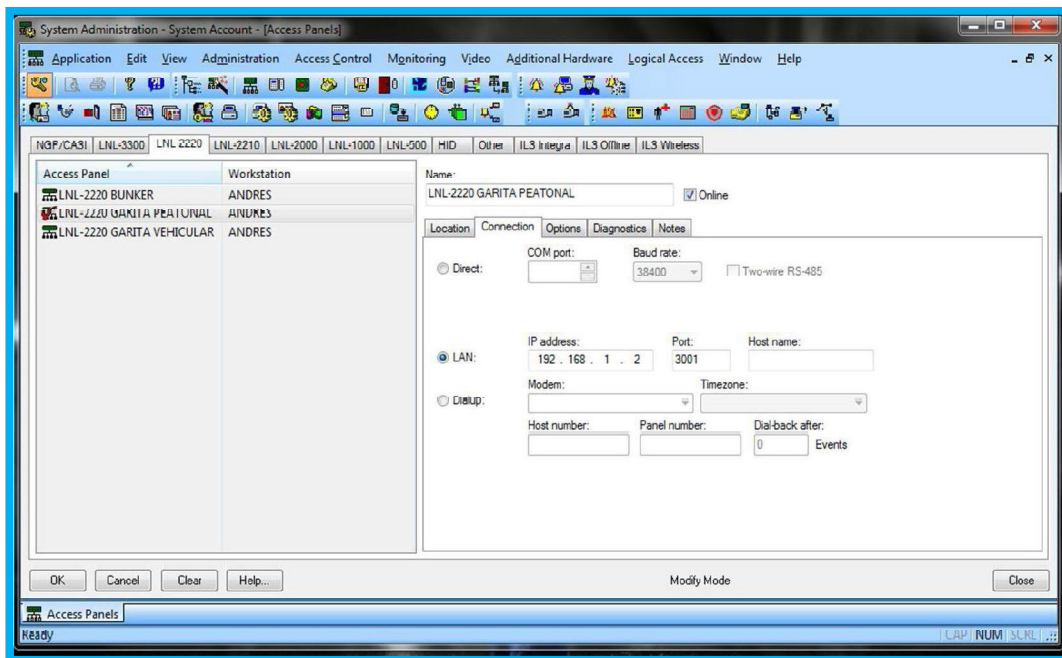


Figura 3. 34 Integración de controladora LNL – 2220

Para finalizar la integración se da clic en la pestaña de “Options” y se modifican los campos de “PIN type” que se refiere a la cantidad de caracteres que tendrán las claves de los usuarios. En este caso se usan claves de hasta 4 dígitos.

Debido a que el tablero 1 y tablero 2 de la garita peatonal o de la garita vehicular se unen vía RS-485 se establece una numeración para tener un orden en la cadena de comunicación y eso se puede apreciar en el plano de distribución de tarjetas en los tableros.

Dicho esto, en la locación de la garita peatonal la controladora LNL-2220 maneja 8 tarjetas esclavas en total, razón por la que en el ejemplo de la Figura 3.35 se tiene que el campo denominado “Alarm panels” está seteado en 8, así mismo en el caso de la LNL-2220 de la garita vehicular el número es 5 o en el caso de la controladora de Bunker es 1. Se finalizan las configuraciones habilitando la opción

de integración de biométricos y handkeys. Se da clic en “OK” en la parte inferior izquierda para terminar el proceso.

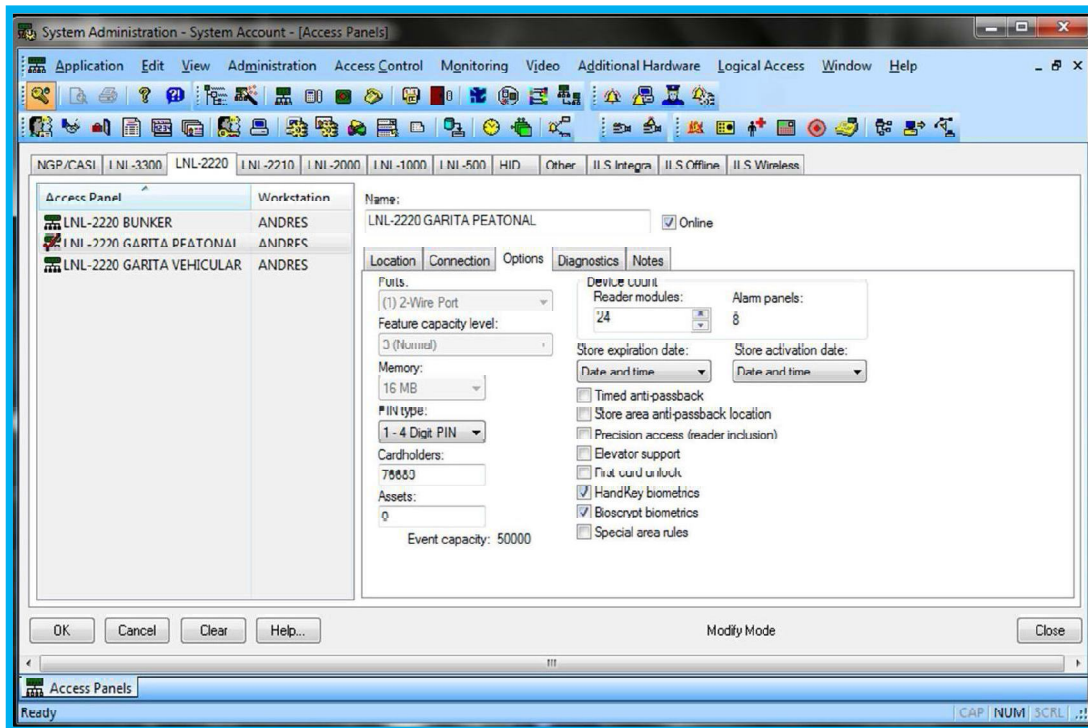


Figura 3. 35 Integración de controladora LNL – 2220

Al finalizar las configuraciones indicadas el sistema lista las tarjetas integradas, como se puede ver a continuación.

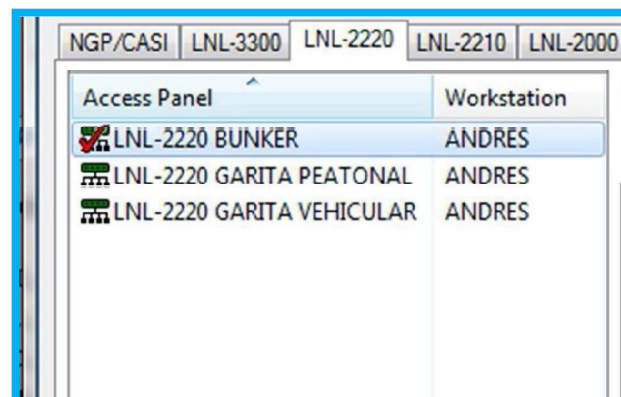


Figura 3. 36 Tarjetas controladoras LNL – 2220 de las 3 áreas integradas en el sistema

3.2.2.2 Configuración de la tarjeta de doble interfaz LNL – 1320

La tarjeta LNL-1320, al no ser un elemento que se puede enlazar a la red directamente, necesita ser configurada de una manera manual.

Lo primero que se requiere es que este equipo este correctamente energizado a 12 VDC y conectado vía RS-485 (a 3 hilos) a la tarjeta controladora LNL-2220 que corresponda, de manera que el cableado de comunicaciones vaya de tarjeta en tarjeta en una secuencia ordenada desde el puerto de RS-485 de la tarjeta maestra hasta el puerto de la última tarjeta LNL-1320. Debido a que estas tarjetas no se direccionan vía IP, las direcciones se asignan manualmente usando el dip switch de 8 estados presente en su configuración, de tal manera que del 1 al 5 son estados para direccionar tarjetas desde el número 1 al 31 en binario.

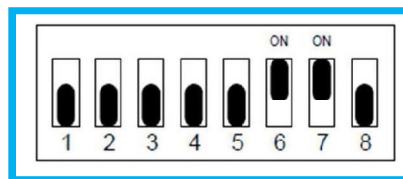


Figura 3. 37 Dip switch de 8 estados

Los estados 6 y 7 son para indicarle a la tarjeta el baud rate (velocidad de comunicación) a la que trabajará. En la figura 3.38 se puede apreciar las diferentes velocidades a las que puede operar una tarjeta de este tipo.

BAUD RATE:	DIP SWITCH	
	6:	7:
38400 bps	ON	ON
19200 bps	off	ON
9600 bps	ON	off
115,200 bps	off	off

Figura 3. 38 Velocidades de comunicación RS-485

Para el caso a implementar en cada una de las LNL-1320 se usó una velocidad “baud rate” de 38400 bps es decir el estado 6 y 7 en ON. El estado 8 del dip switch se refiere a si se va o no a implementar un nivel de encriptación, en este

A continuación se indican las diferentes configuraciones de conexión que requieren las LNL-1320 usadas para la representación de cada área.

En la figura 3.40 se puede apreciar el uso de las respectivas entradas y salidas ejemplificando el caso de la garita vehicular y la garita peatonal con sus posibles periféricos de salida.

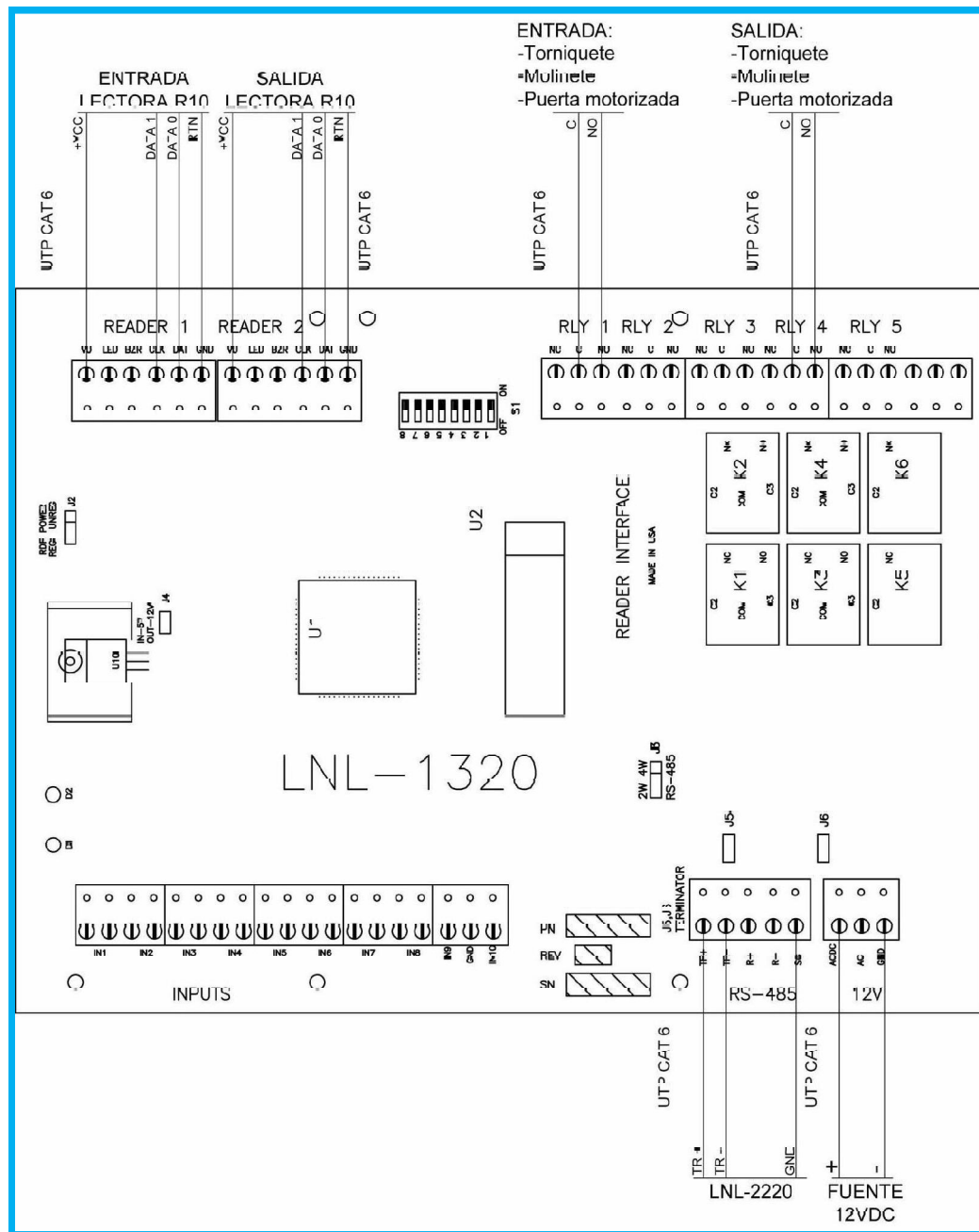


Figura 3. 40 LNL-1320 configurada para uso de lectoras R10 y posibles salidas

En la Figura 3.41 se aprecia la configuración de entrada y salida para el uso de una barrera vehicular.

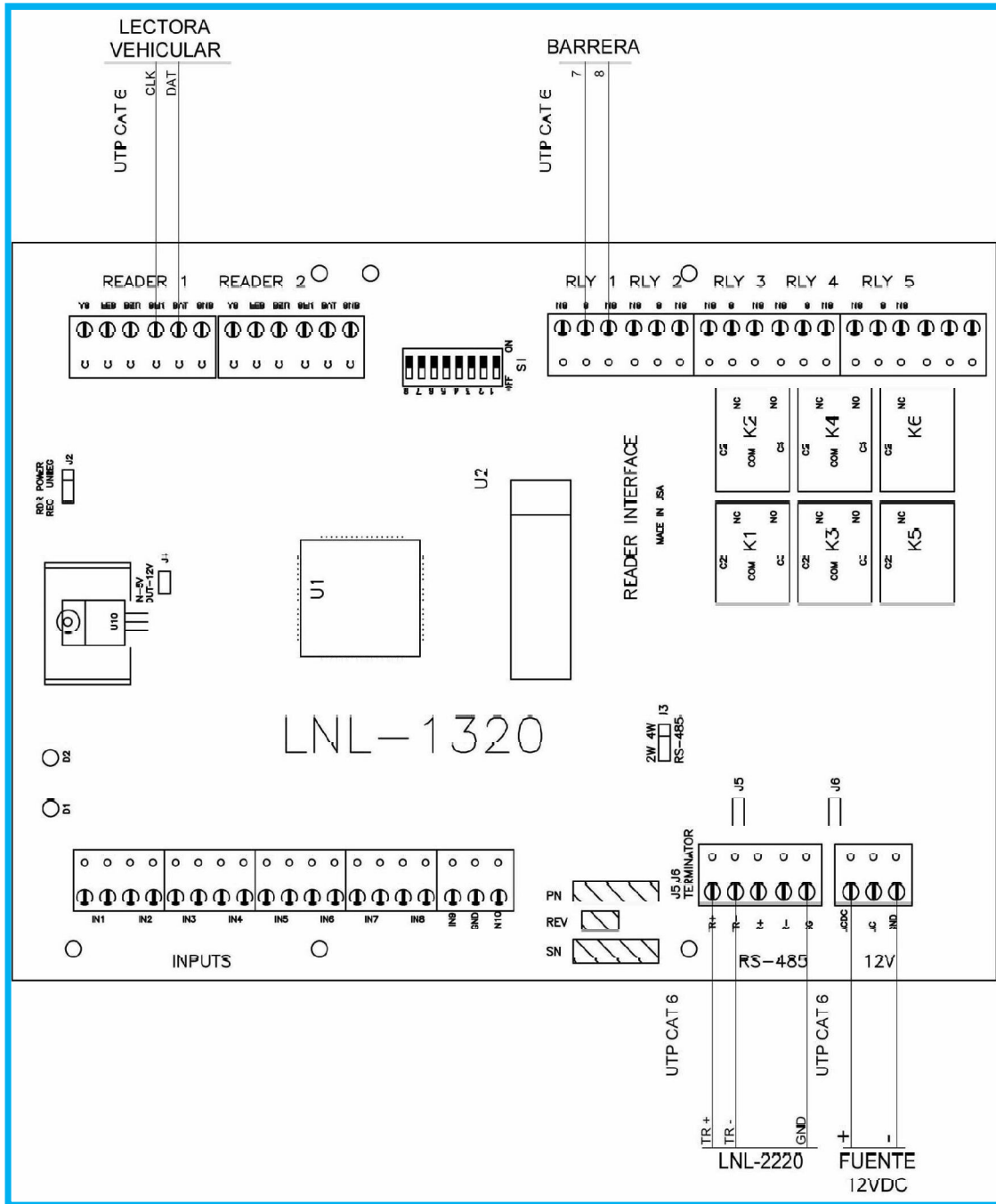


Figura 3. 41 LNL-1320 configurada para uso de lectora y barrera vehicular

En la Figura 3.42 se puede apreciar cómo se configura una tarjeta LNL-1320 para el manejo de un biométrico de huellas digitales.

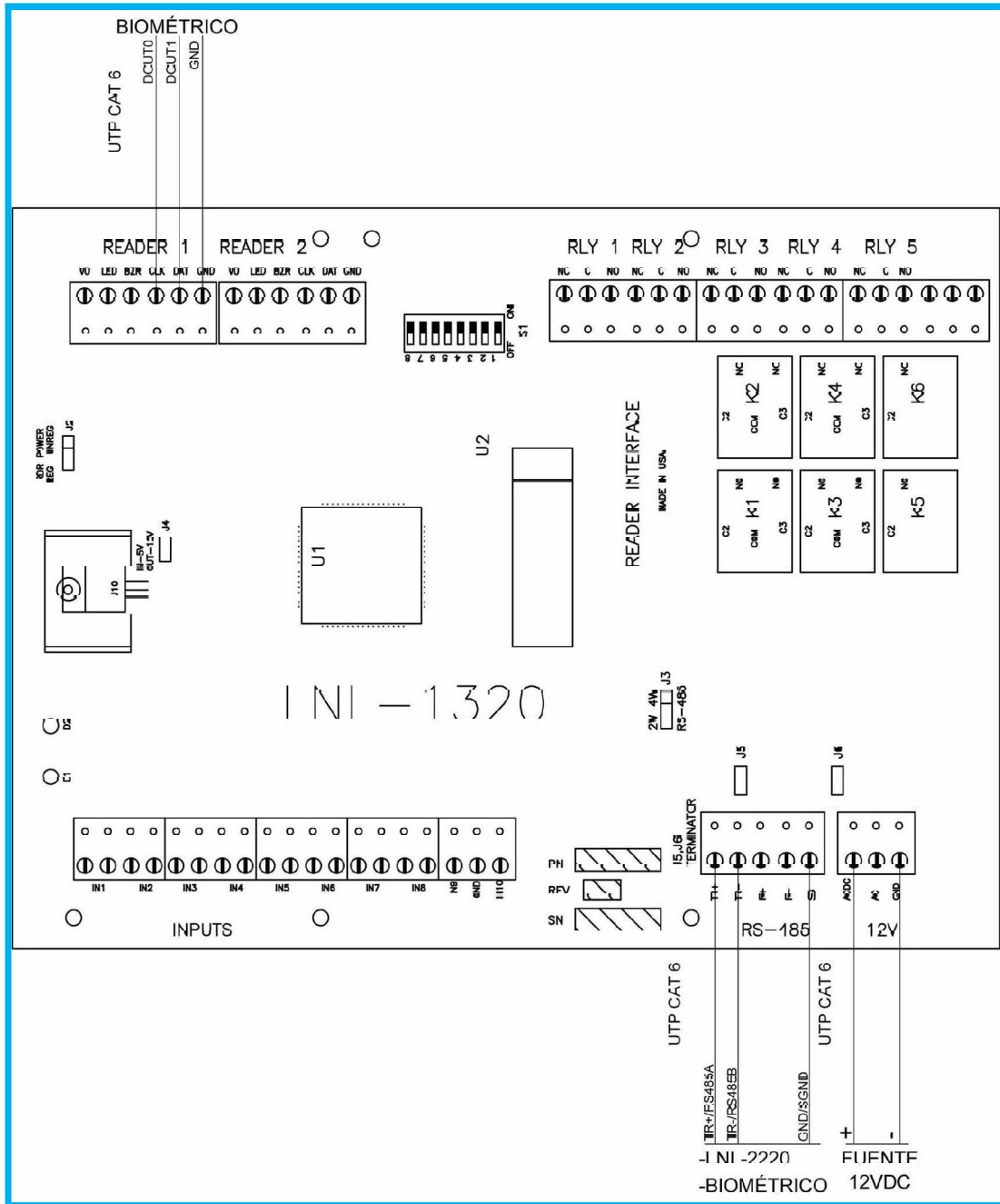


Figura 3. 42 LNL-1320 configurada para uso de un biométrico

A diferencia de las anteriores configuraciones este equipo no maneja ningún equipo de salida y se limita a tomar registros de ingreso de personal más no a realizar algún tipo de acción de control.

En la Figura 3.43 se puede ver la configuración necesaria para el manejo de una chapa electromagnética como la de bunker usando dos lectoras R10 (entrada-salida).

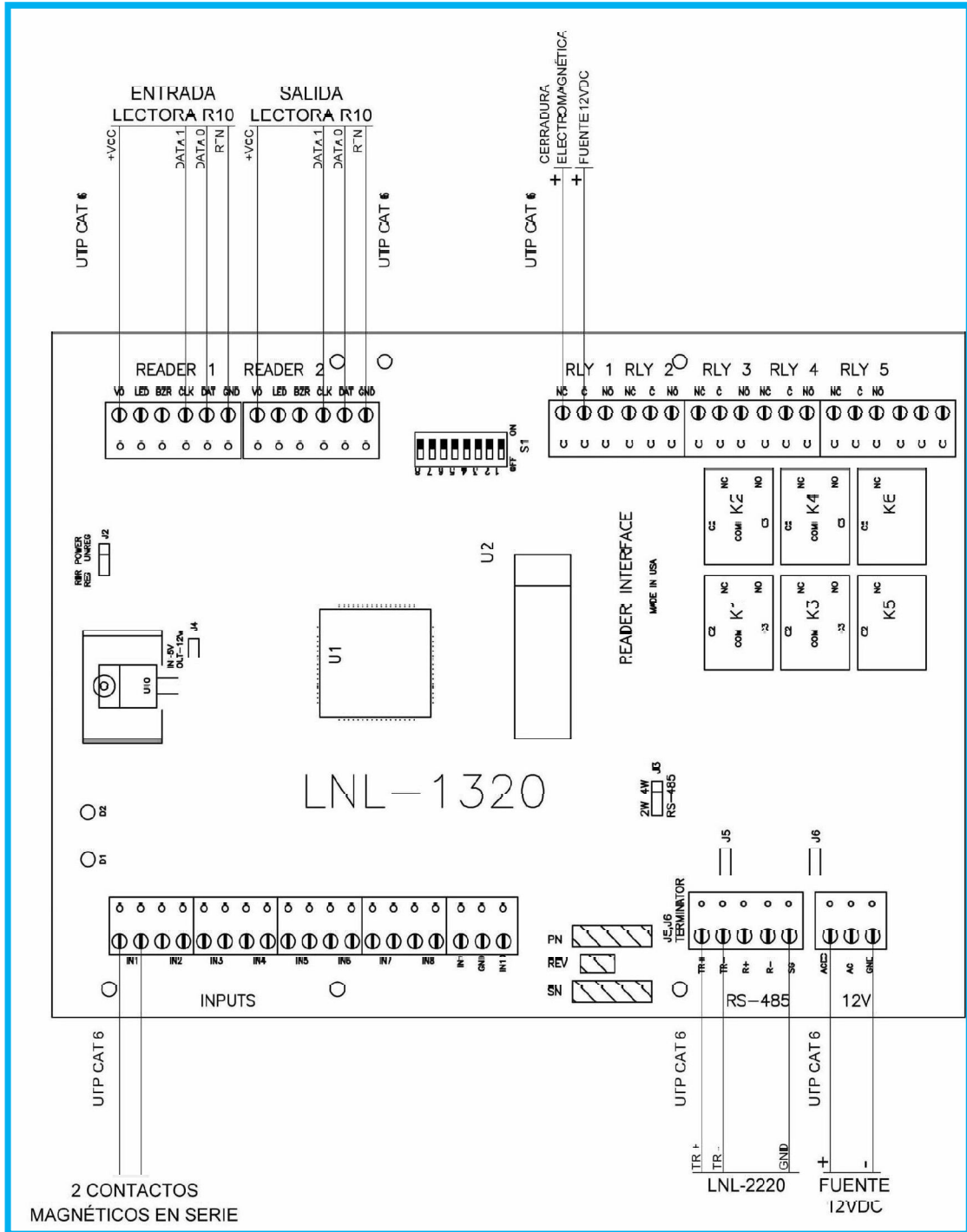


Figura 3. 43 LNL-1320 configurada para el manejo de una chapa electromagnética

3.2.2.3 Configuración de la tarjeta de enlace de handkeys LNL – 500B

De manera similar a la tarjeta LNL-1320 esta tarjeta no puede ser configurada mediante la red, y su configuración se realiza de forma manual.

Como primer paso se debe tener la tarjeta correctamente alimentada a 12VDC y conectada a la red RS-485 presente.

Para su configuración se tiene un dip switch de 8 estados como en el caso de las LNL-1320 y al igual que en ese caso los primeros 5 estados son para direccionamiento, el estado 6 y 7 son para seleccionar la velocidad de la comunicación y el estado 8 es para habilitar o deshabilitar un modo de seguridad avanzado.

Esta tarjeta en su configuración posee 3 puertos de comunicación RS-485, el primero es configurable a 2 o 4 hilos y es de uso único para enlazar la tarjeta a la red presente, el puerto 3 y 4 son puertos dedicados al manejo de handkeys con una capacidad individual de hasta 4 equipos por puerto.

El jumper 8 colocado indica que la tarjeta es final de comunicación y si este se retira significa que permite que continúe la red de comunicación.

En el caso del ejemplo de la garita peatonal y de la garita vehicular donde se manejan handkeys se tiene para el módulo de pruebas dos y un handkey respectivamente y debido a eso se usa solo el puerto 2 de comunicación RS-485 en la LNL-500B correspondiente, es por eso que el Jumper 12 que maneja el puerto 3 se mantiene colocado (posición OFF) y el Jumper 11 que maneja el puerto 2 se mueve (posición ON) para habilitar dicho puerto.

En la Figura 3.44 se puede apreciar la configuración de conexión necesaria de una LNL-500B para que pueda integrar el lector de geometría de mano correctamente.

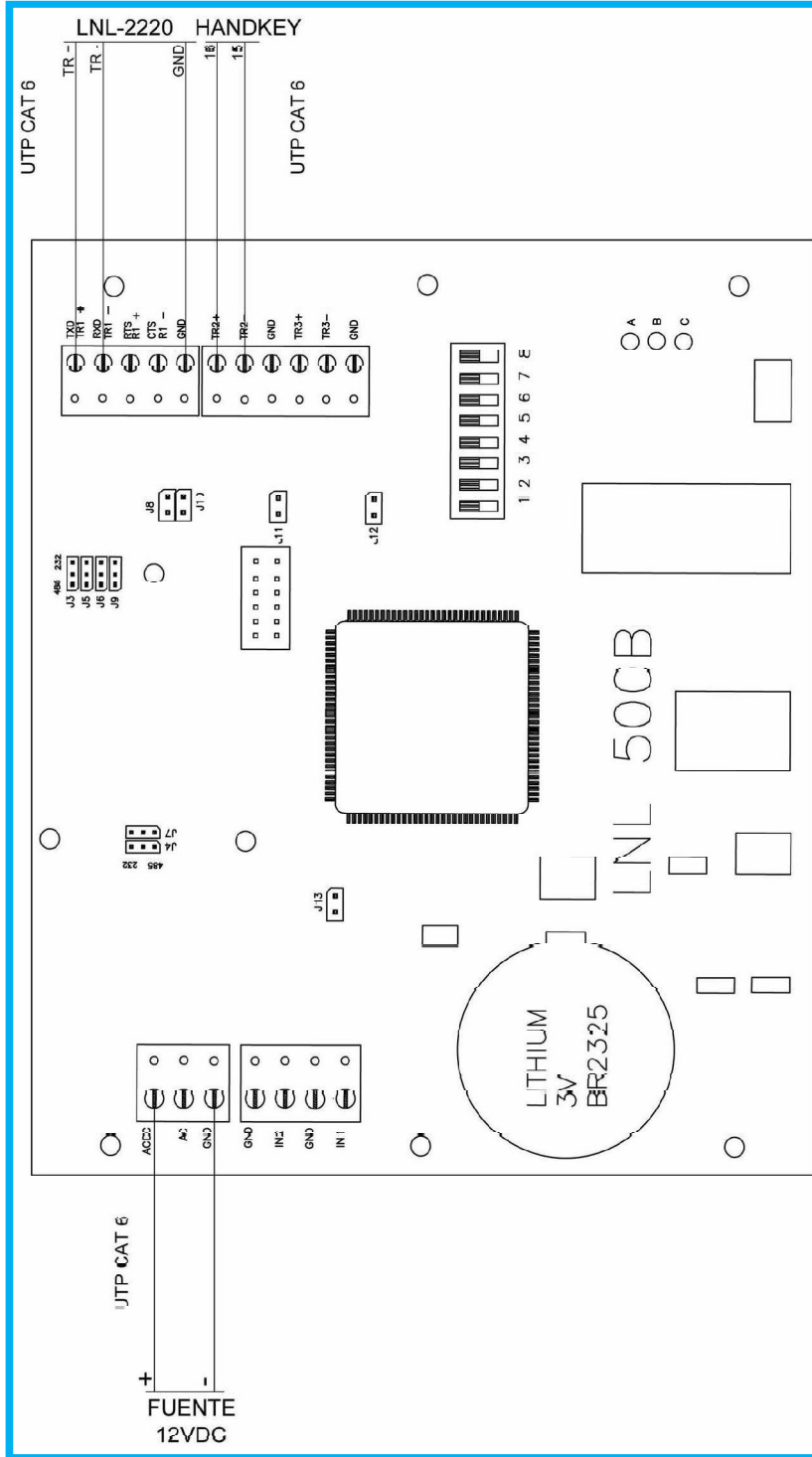



Figura 3. 44 LNL-500B para la integración de handkeys

3.2.2.4 Configuración de lectoras de proximidad R10

Estos equipos se integran al sistema a través de los puertos de lectora que poseen las tarjetas electrónicas LNL-1320 como se puede ver en las figuras de configuración de dicha tarjeta; en general su funcionamiento se realiza en pares ya que están destinadas generalmente al control de acceso de puertas y de esta manera se necesitan dos lectoras para el correcto funcionamiento, una para activar el sistema de seguridad desde un lado de la puerta (dígase entrada) y otra para activar el sistema desde el lado opuesto (dígase salida).

Como primer punto se debe asegurar que la primera lectora está correctamente conectada al puerto READER 1 de lectora de la LNL-1320 y la segunda lectora este correctamente conectada al puerto READER 2 de la misma LNL-1320.

En este caso la comunicación opera a la par de la alimentación debido a eso el momento en que la lectora se conecta al puerto de READER inmediatamente se alimenta y su led de estado se enciende en color rojo.

Para continuar se ingresa a “System Administration” del software ONGUARD y en la segunda barra de opciones se da clic en el icono denominado “Readers and doors” (Lectoras y puertas)  e inmediatamente se despliega la siguiente ventana.

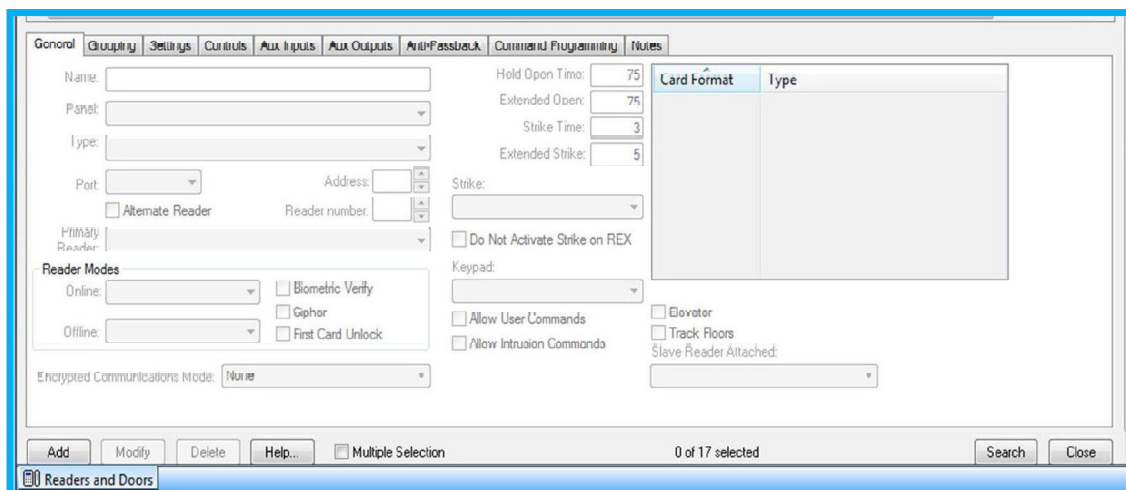


Figura 3. 45 Pantalla de configuración de lectoras

Se inicia como norma de orden integrando la lectora conectada al primer puerto de READER y se le da la jerarquía de “lectora de entrada”; los campos disponibles se deben modificar como se indica en la Figura 3.46 que ejemplifica la integración de la lectora de entrada de la puerta de Bunker.

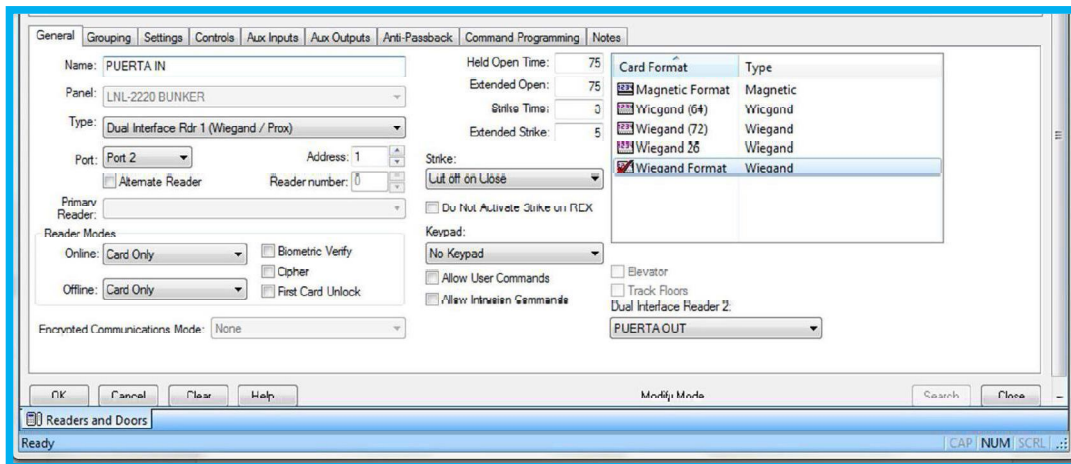


Figura 3. 46 Configuración de lectora de entrada a Bunker

En la anterior figura en la pestaña denominada “General” se puede ver que el nombre asignado es “PUERTA IN”, en el campo de Panel se selecciona la tarjeta LNL-2220 BUNKER correspondiente a esta ubicación, debido a que el formato de uso es en pares en el campo denominado Tipo se selecciona la opción “Dual Interface Rdr 1 (Wiegand/Prox)” que hace referencia a que la primera lectora de proximidad a integrarse esta en el puerto READER 1 que maneja el protocolo Wiegand, en el campo “Reader number” el parámetro se setea automáticamente en 0 esto se da porque para el sistema el puerto READER 1 es en realidad el puerto 0 y el puerto READER 2 es en realidad el puerto 1.

En el campo de dirección (Address) se escribe la dirección que tiene asignada con los dip switch la tarjeta LNL-1320 usada, en este caso la dirección es la 1 que significa que la lectora está conectada en la primera LNL-1320 de la cadena de comunicación RS-485.

En los campos de “modos de lectora (reader modes)” tanto en el campo denominado “online (en línea)” y “offline (fuera de línea)” se selecciona la opción “SOLO TARJETA (CARD ONLY)” que implica que la lectora a integrarse solo

tiene la capacidad de leer tarjetas de proximidad mientras este el sistema en línea o no lo este, en el campo que se denomina “TIEMPO DE DISPARO (STRIKE TIME)” se puede setear el tiempo en segundos que se activará la salida de relé (RELE 1) correspondiente a esa lectora, ese parámetro depende del uso que se le va a dar al acceso y para usos prácticos se da un tiempo de 3 o 4 segundos como tiempo necesario para que una persona después de acercar su tarjeta por la lectora pueda abrir dígase la puerta e ingresar sin que el sistema vuelva a bloquear el acceso, en el campo llamado “STRIKE” se selecciona la opción “(CUT OFF ON CLOSE)” que hace referencia que el instante en que se termina el tiempo de activación indicado, el relé regresa a su posición inicial, en el campo “KEYPAD (TECLADO)” se selecciona la opción “NO KEYPAD” ya que esta lectora no posee ningún periférico extra dígase un teclado añadido.

En el campo de la derecha denominado “FORMATO DE TARJETA (CARD FORMAT)” se da clic en la opción “Wiegand Format” de manera que se marque con un visto color rojo indicando así que ese es el formato de tarjetas que admite el sistema.

Para finalizar se debe dar clic en la pestaña denominada “SETTINGS” en al que se tiene diferentes funciones de control añadidas que permiten jugar dígase así con el funcionamiento de los relés que en este caso le corresponden al puerto de READER 1 el que tiene dominio sobre los 3 primeros relés presentes en la LNL-1320 de manera que el RELÉ 1 es el relé principal, el RELÉ 2 es el auxiliar 1 y el RELÉ 3 es el auxiliar 2, para el caso de bunker se maneja la apertura de una cerradura electromagnética desde el relé principal usando el contacto común y el NC (NORMALMENTE CERRADO) y su accionamiento se controla desde el puerto de READER 1 y puerto de READER 2 razón por la que se habilita en esta sección la opción denominada “(MAESTRO EMPAREJADO) PAIRED MASTER” que hace referencia a que esta primera lectora es el maestro de las dos lectoras y que está asociada directamente con la segunda.

El resto de campos se mantienen y se da clic en “OK” para finalizar la configuración e integración de la lectora 1 al sistema.

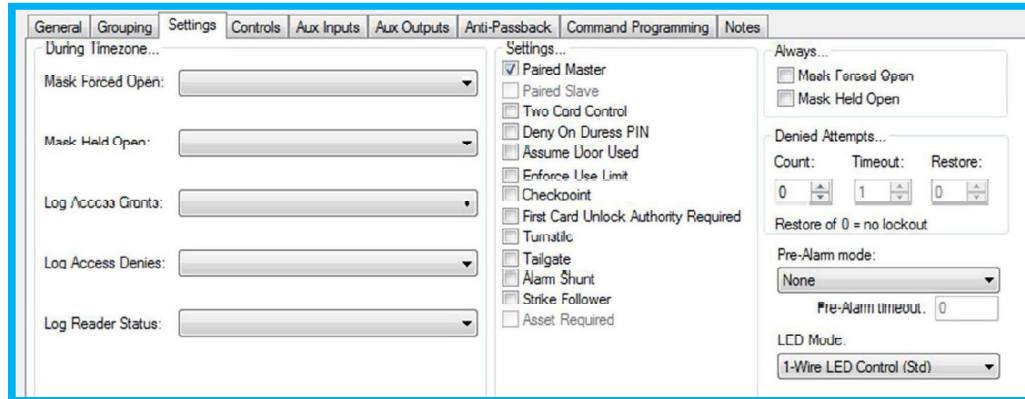


Figura 3. 47 Configuración de acciones de control READER 1

En el caso de la lectora 2 se inicia de manera similar como en la primera pero con algunas diferencias claves que a continuación se pueden ver en la Figura 3.48.

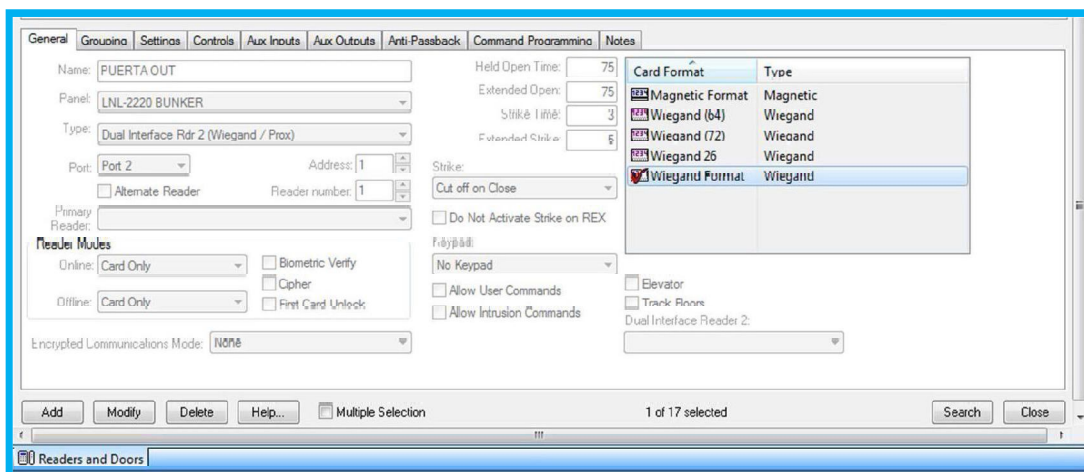


Figura 3. 48 Configuración de lectora de salida de Bunker

Como se puede ver el nombre asignado es ahora “PUERTA OUT”, en el campo “TIPO (TYPE)” se selecciona la opción “DUAL INTERFACE RDR 2 (WIEGAND/PROX)” que hace referencia a que la lectora de proximidad a integrarse está conectada en el puerto READER 2, el campo de dirección “(ADDRESS)” se mantiene en 1 ya que la lectora 2 está conectada en la misma tarjeta LNL-1320 de la primera lectora, de igual manera debido a esto automáticamente se setea el “NUMERO DE LECTORA (READER NUMBER)” en 1 ya que como se indicó previamente, para el sistema el puerto READER 2 es en realidad el puerto 1. En esta sección se configura la pestaña “SETTINGS”, como se indica en la Figura 3.49.

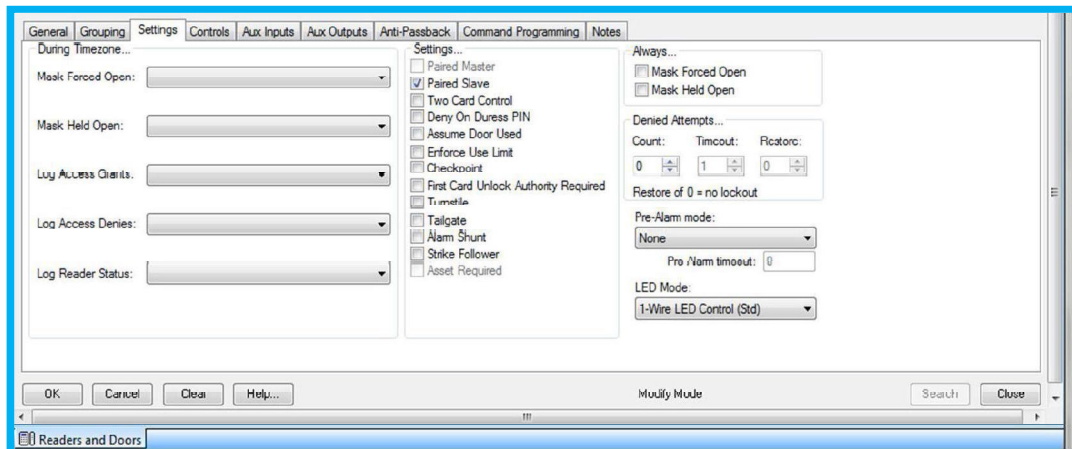


Figura 3. 49 Configuración de acciones de control READER 2

Ahora lo que se necesita es indicarle al sistema que esta lectora trabaja a la par con la primera y que ambas tienen control sobre el relé principal 1, para ello se habilita la opción “(ESCLAVO EMPAREJADO) PAIRED SLAVE”, se da clic en “OK” y para finalizar se regresa a la configuración de la primera lectora y se selecciona la lectora emparejada a esta es decir se le indica que lectora es su esclava en este caso la lectora llamada “PUERTA OUT”.

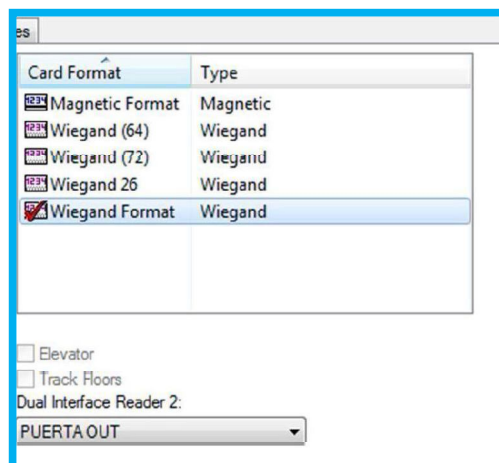


Figura 3. 50 Emparejamiento de lectoras en entrada y salida de BUNKER

Una vez realizados todas las configuraciones y emparejamientos necesarios el sistema registra las lectoras integradas y las muestra listadas, a continuación se indican las diferentes parejas de lectoras usadas en la elaboración del módulo de pruebas.

- Garita Peatonal:
 - LNL – 1320 (#1) integra: ESPINA IN (READER1)
ESPINA OUT (READER2)
 - LNL – 1320 (#2) integra: PUERTA MOTORIZADA IN (READER1)
PUERTA MOTORIZADA OUT (READER2)
- Garita Vehicular:
 - LNL – 1320 (#2) integra: LECTORA ENTRADA MOLINETE (READER1)
LECTORA SALIDA MOLINETE (READER2)
- Bunker:
 - LNL – 1320 (#1) integra: PUERTA IN (READER1) (EJEMPLO)
PUERTA OUT (READER2) (EJEMPLO)

3.2.2.5 Configuración de handkeys (lectores de geometría de mano)

Como primer paso se debe asegurar que las conexiones de comunicaciones WIEGAND y RS-485 estén correctamente cableadas, así como la de alimentación a 12VDC, de manera que el cableado de WIEGAND se conecte de manera similar que el de las lectoras de proximidad al puerto de READER 1 o 2, la comunicación RS-485 debe estar en el puerto 2 de la tarjeta LNL-500B.

Con el equipo encendido se inicia el proceso de configuración e integración; ahora se debe ingresar a “System administration” en ONGUARD y nuevamente dar clic en “READERS AND DOORS”, y de la misma forma que se integraron las lectoras de proximidad se usan muchos de los campos a modificar, con la diferencia que para estos equipos se necesita crear un perfil “REAL” y un perfil “VIRTUAL” debido a que este equipo es controlado e integrado al sistema desde dos diferentes tarjetas electrónicas al mismo tiempo, en la Figura 3.51 se puede ver la creación del perfil “REAL” que se refiere a la integración de este a través de la tarjeta LNL-1320 con la que está conectado.

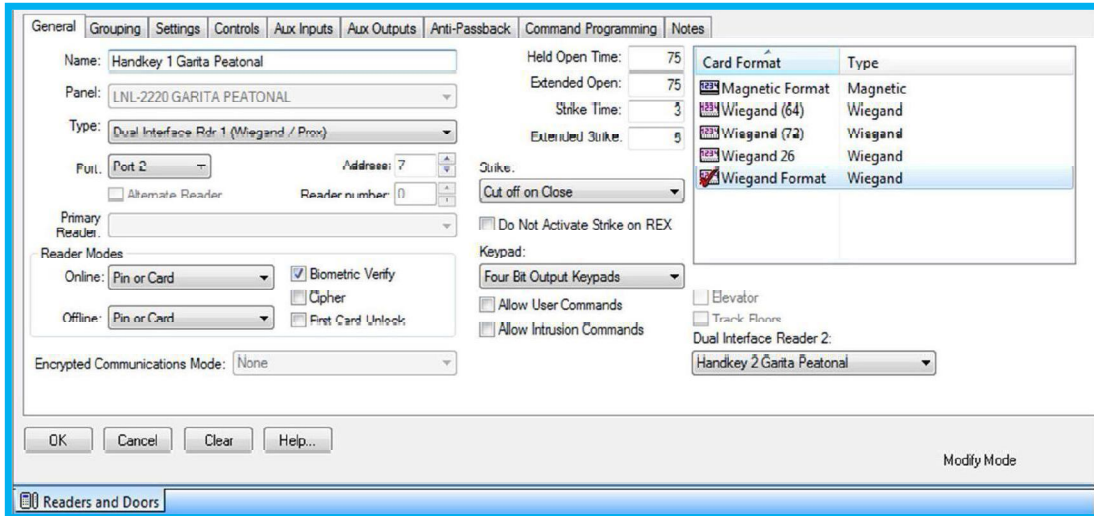


Figura 3. 51 Integración de un HANDKEY (PERFIL REAL)

Se puede ver en la anterior figura que el nombre asignado a este equipo es “HANDKEY 1 GARITA PEATONAL”, se selecciona la controladora presente en esta ubicación LNL – 2220 GARITA PEATONAL, al estar conectado en el puerto READER1 de la LNL-1320 en el campo de “TIPO (TYPE)” se selecciona “Dual Interface Rdr 1 (Wiegand/Prox)” el campo NUMERO DE LECTORA se setea automáticamente en 0 y el direccionamiento es el número 7 debido a que es la LNL-1320 direccionada con ese número en binario a la que está conectado este equipo.

A diferencia de las lectoras de proximidad este equipo no necesita ser emparejado por lo que es independiente del resto de dispositivos de este mismo tipo y no se lo empareja; posee un teclado matricial de 4x4 razón por la que en el campo “KEYPAD” se habilita las claves de 4 dígitos que admite el sistema, además en el campo de “MODOS DE LECTORA” en las opciones de “ONLINE” y “OFFLINE” se habilita el modo “2PIN OR CARD (CLAVE O TARJETA)” que implica que para que el equipo le dé acceso a un usuario este debe digitar una clave y luego pasar una tarjeta o en su defecto en este caso colocar la mano para que esta sea leída, y también se habilita la opción de “BIOMETRIC VERIFY”. El resto de parámetros se configuran de la misma forma que una lectora de proximidad.

Una vez completada la configuración anterior el siguiente paso es crear el perfil “VIRTUAL” que se refiere a la configuración e integración de este equipo a través de la tarjeta electrónica LNL-500B.

Nuevamente en la pantalla de configuración de lectoras se da clic en “ADD” y se realizan los cambios que se pueden ver en la Figura 3.52.

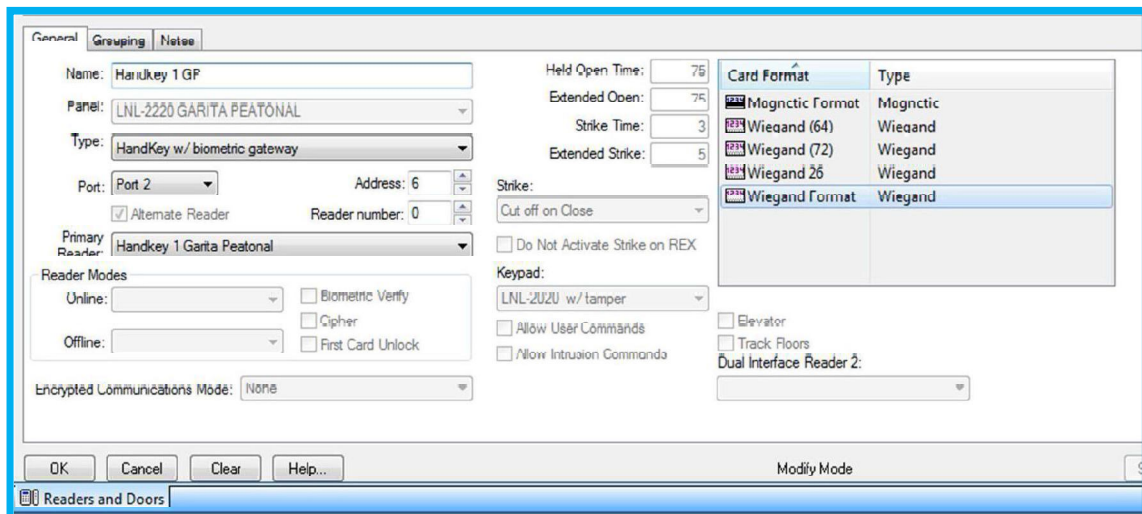


Figura 3. 52 Integración de un HANDKEY (PERFIL VIRTUAL)

Se le da un nombre alternativo pero similar al del perfil “REAL”, en este caso se da el nombre de “HANDKEY 1 GP”, se selecciona la misma controladora LNL-2220 GARITA PEATONAL, en el campo de “TIPO” se selecciona la opción “HANDKEY W/BIOMETRIC GATEWAY” que se refiere a que el handkey conectado a la LNL-500B usa esa tarjeta electrónica como puerta de enlace hacia el sistema, en el campo de dirección se indica la dirección de la LNL-500B en este caso el número 6 con el que esta seteada en binario físicamente con los dip switch, en el campo de “NÚMERO DE LECTORA” se setea el numero 0 debido a que el puerto RS-485 al que está conectado el handkey es el primer puerto dedicado en la LNL-500B, el ultimo campo a modificar es el de “PRIMARY READER (LECTORA PRIMARIA)” y mediante este campo se identifica la relación entre el perfil “REAL” y el perfil “VIRTUAL”, de forma que se selecciona para este caso el nombre de dicho perfil “REAL (HANDKEY 1 GARITA PEATONAL)”.

Se finaliza dando “OK” en la parte inferior izquierda de forma que al finalizar la configuración e integración se listen en el sistema ONGUARD.

Para el diseño constructivo e implementación del módulo de pruebas se seleccionaron los siguientes equipos listados a continuación:

- **GARITA PEATONAL:**

LNL – 1320 (#7) integran: Handkey 1 Garita Peatonal (READER1)

LNL – 500B (#6) Handkey 1 GP

LNL – 1320 (#7) integran: Handkey 2 Garita Peatonal (READER2)

LNL – 500B (#6) Handkey 2 GP

- **GARITA VEHICULAR:**


LNL – 1320 (#3) integran: Handkey 1 Garita Vehicular (READER1)






LNL – 500B (#5) Handkey 1 GP

A diferencia de las lectoras de proximidad los handkeys necesitan ser configurados también desde su interfaz de usuario física es decir desde el teclado y la pantalla lcd 2x16 que poseen como se puede ver en la Figura 3.53



Figura 3. 53 Vista frontal de Handkey

Con el equipo encendido se presiona la tecla “CLEAR” y la tecla “ENTER” simultáneamente de forma que en el LCD se visualice el mensaje “ENTER PASSWORD”; se digita 2 y se da “ENTER” de manera que se despliega la primera opción a ser configurada “(SET LANGUAGE)”, se da clic en  y

con el botón  se puede desplazar en las opciones de idiomas, en nuestro caso ESPAÑOL, una vez seleccionado se da “ENTER” y con el botón  se pasa a la siguiente opción que es el formato de fecha, la siguiente opción es ingresar hora y fecha para lo que se da clic en  y se nos permite ingresar ese dato, la siguiente opción es indicar la dirección de lectora “(SET RDR ADDRESS)” lo que se refiere a indicar en que puerto de READER está conectado el dispositivo, pudiendo ser el valor 0 o 1 y se da entre para confirmar, la siguiente opción es “MODO DE LA CLAVE” el que se refiere a la longitud de las claves que debe aceptar el dispositivo, ya anteriormente se definió ese dato así que se digita 4 para confirmar las claves de 4 dígitos, se sigue el orden de opciones hasta llegar a la opción de “MODO DEL DISPOSITIVO”, en este caso se da clic en  y se selecciona el modo REMOTO, ya que el sistema se considera como el Maestro de estos equipos, el último parámetro a modificar es la velocidad a la que se maneja la comunicación del equipo con la tarjeta LNL-500B de manera que se selecciona 19200 baudios; una vez concluidos los cambios se da clic en  y el LCD regresa a su pantalla de inicio con la frase “LISTO o READY” en la primera fila y en la segunda línea la hora y fecha seteados.

3.2.2.6 Configuración de lectoras vehiculares

Estos equipos deben ser previamente configurados desde su propia interfaz de usuario, debido a esto se necesita hacer una conexión temporal extra entre el puerto SERIAL (RS-232) que poseen y la computadora desde la que se los va a pre-configurar, en este caso se usa un cable de comunicación RS-232 con un terminal Hembra al que se conecta un cable conversor de RS-232 a USB, este cable se reconoce como un dispositivo USB conectado al computador y es necesario identificar el número de puerto que posee para este caso es el COM4.

Previamente es necesario instalar el software para realizar esta configuración, este software se denomina “P81 TEST” y pertenece a la misma marca de estos equipos.

Sus requerimientos son bastante básicos así que corre en Windows 7 o XP sin problemas.

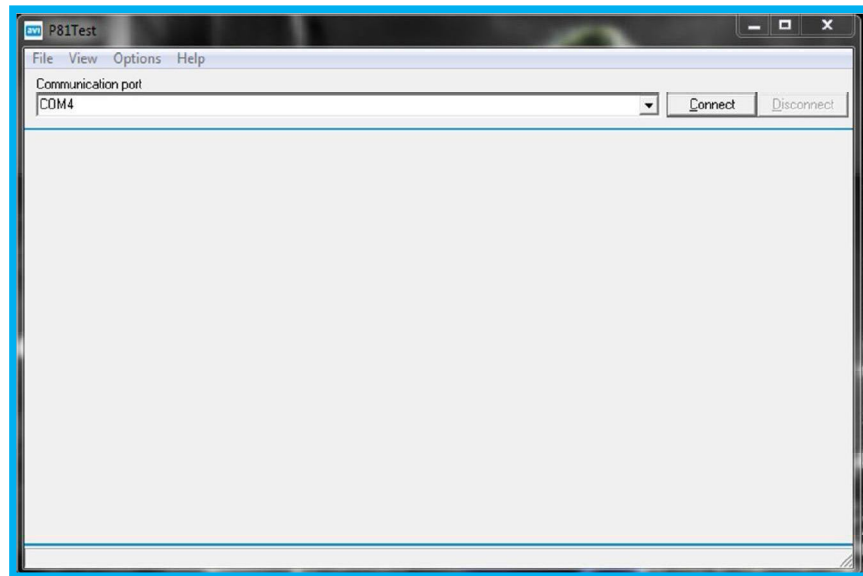


Figura 3. 54 Pantalla de inicio del programa P81 TEST

En la barra de “PUERTO DE COMUNICACIÓN” se digita “COM4” de manera que se indica el puerto por donde se está dando el enlace y se da clic en “CONNECT” para que se despliegue la Figura 3.55.

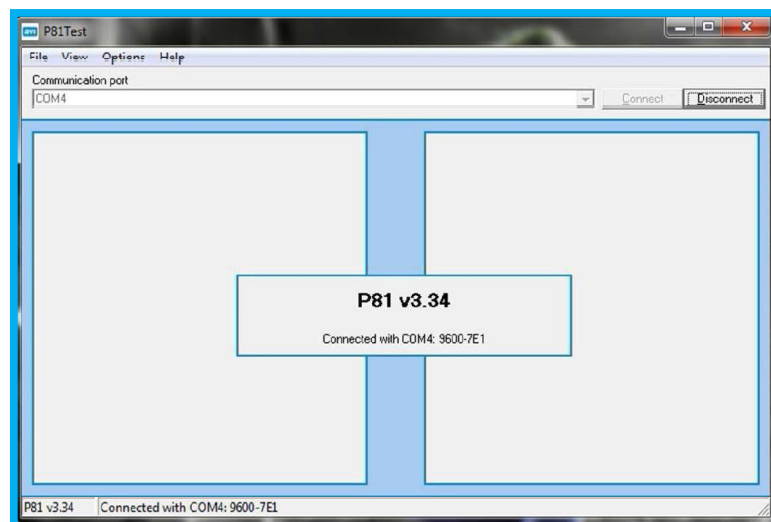


Figura 3. 55 Pantalla de inicio activa del programa P81 TEST

En la ventana de la figura 3.54 se da clic en “OPTIONS” y luego clic en la sub opción denominada “READER CONFIGURATION” de manera que se despliega la ventana de la Figura 3.56.

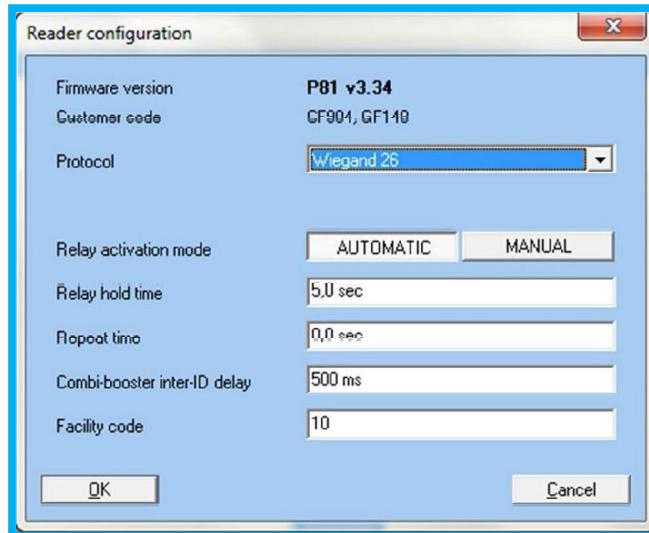


Figura 3. 56 Pantalla de configuración NEDAP READER

Se necesita definir el protocolo con el que va a trabajar por ello se selecciona “WIEGAND 26” en referencia a que el protocolo WIEGAND manejado por todo el sistema usa 26 bits. El resto de parámetros se dejan como están y se da clic en “OK”.

Se regresa a la pantalla de inicio activa, nuevamente se da clic en “OPTIONS” pero ahora se da clic en la sub opción “DUAL-ID CONTROL” donde se despliega la pantalla de la Figura 2.57.

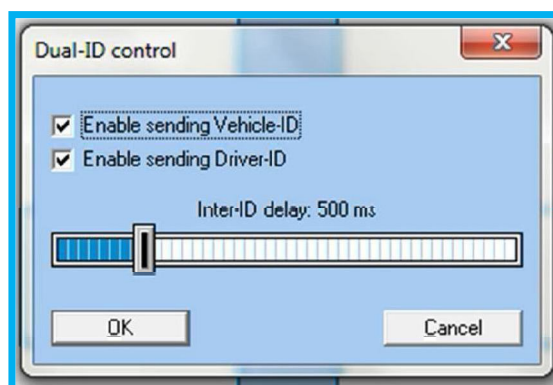


Figura 3. 57 Pantalla de configuración DUAL

Como se puede apreciar en la Figura 3.56 se habilita el envío simultáneo de información del vehículo y del conductor con un tiempo de retardo de 0.5 segundos esto debido a que los booster que son los elementos instalados en el vehículo tienen esa capacidad, para confirmar los cambios se da clic en “OK”.

Para finalizar se vuelve a dar clic en “OPTIONS” y en “SELECT CARD TYPE (DRIVER- ID)” con lo que se abre la siguiente ventana.

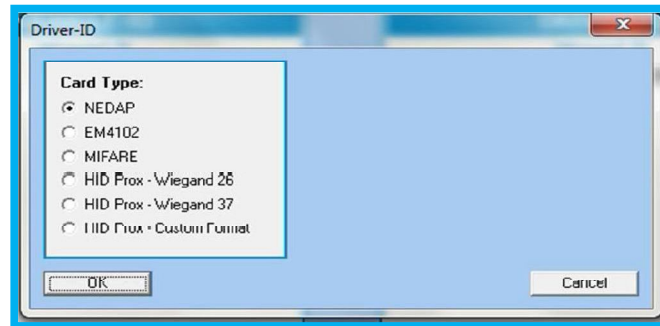


Figura 3. 58 Pantalla de configuración de tipo de tarjeta

En la Figura 3.57 se puede ver la ventana donde se selecciona el modo “NEDAP” que implica una lectura simultánea de información e influye también en el rango de lectura extendiéndose a una distancia de hasta 7 metros. Se finaliza dando “OK” y luego “DISCONNECT”.

Ahora para integrar este equipo en el sistema administrador ONGUARD ingresamos en “READERS AND DOORS” y seteamos los campos como en la Figura 3.59.

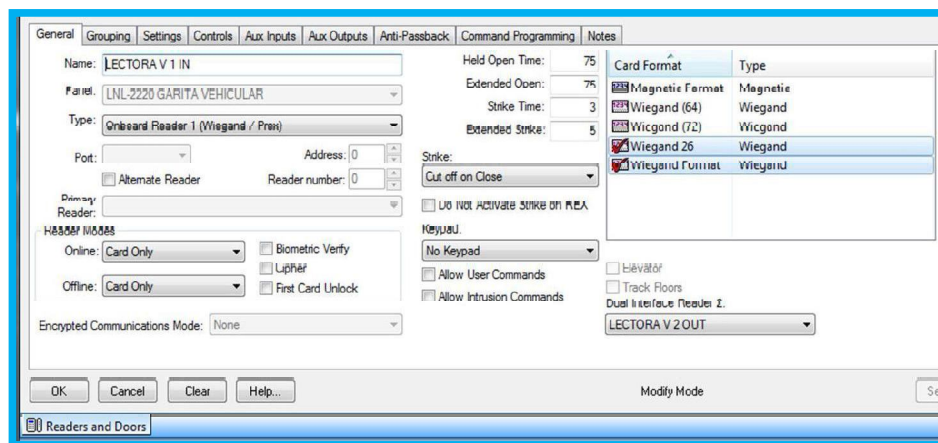


Figura 3. 59 Pantalla de configuración de lectora vehicular

Para el ejemplo se da el nombre de “LECTORA V 1 IN”, se selecciona la controladora correspondiente en este caso LNL-2220 GARITA VEHICULAR, en el campo “TIPO” a diferencia de las lectoras de proximidad se selecciona la opción “ONBOARD READER 1 (WIEGAND/PROX)” esto significa que la lectora está conectada al puerto READER 1 de la propia LNL-2220; otra diferencia es que el equipo requiere que se seleccione a la par dos formatos de Wiegand, en este caso “WIEGAND 26 y WIEGAND FORMAT”,

El resto de parámetros se setean como una lectora normal con la diferencia final que cada una de las dos lectoras funcionan independientemente es decir no se emparejan con la función de control “PAIRED MASTER – PAIRED SLAVE” y así la lectora vehicular 1 maneja los relés 1 principal y 2 auxiliar; mientras que la lectora vehicular 2 maneja los relés 3 principal y 4 auxiliar.

Para el diseño e implementación de estos equipos en el módulo de pruebas se integran dos de estos en la misma controladora como se lista a continuación.

- Garita Vehicular:

LNL – 2220 (MAESTRA) integra: LECTORA V 1 IN (READER1)

LECTORA V 2 OUT (READER2)

3.2.2.7 Configuración del biométrico de huellas digitales

Se necesita configurar previamente los parámetros de red de este equipo para poder usarlo mediante nuestra red privada; para esto es necesario instalar primero el programa propio de este equipo.

El software se denomina “L-1 IDENTITY SOLUTIONS” y es necesario instalar la versión de 64 bits en modo servidor y en modo cliente para que en el sistema se tenga la capacidad de enrolamiento y registro de alarmas.

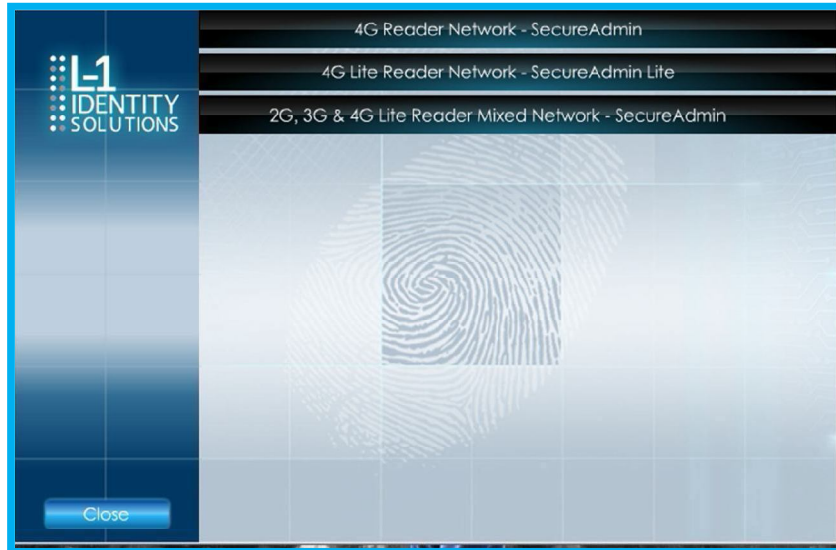


Figura 3. 60 Pantalla de instalación software L-1 IDENTITY SOLUTIONS

En el menú de “NETWORK” se desactiva el modo DHCP y se le da una dirección IP de forma que para este caso es 192.168.1.7 con su máscara de subred 255.255.255.0 y el Gateway 192.168.1.1.

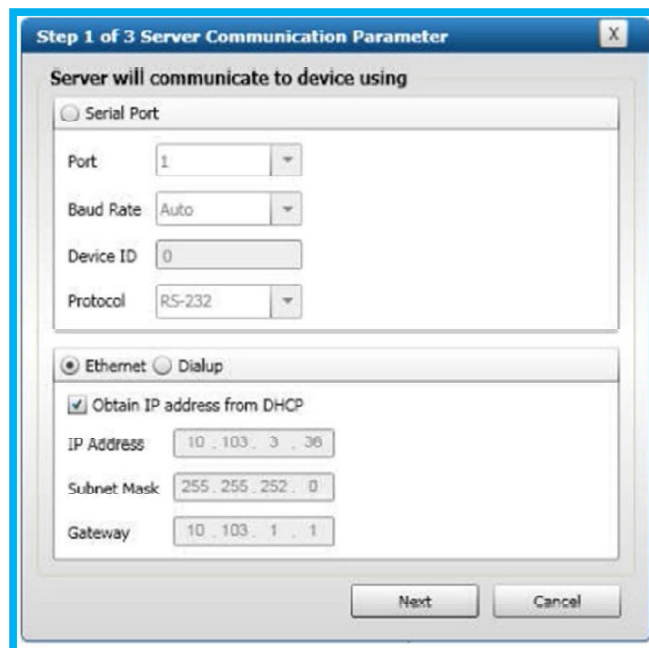


Figura 3. 61 Parámetros de red iniciales

Se continúa ahora con la integración de este equipo en el sistema administrador; se ingresa a “SYSTEM ADMINISTRATION” y se da clic en “READERS AND DOORS” y en la nueva ventana damos clic en “ADD” en la parte inferior izquierda.

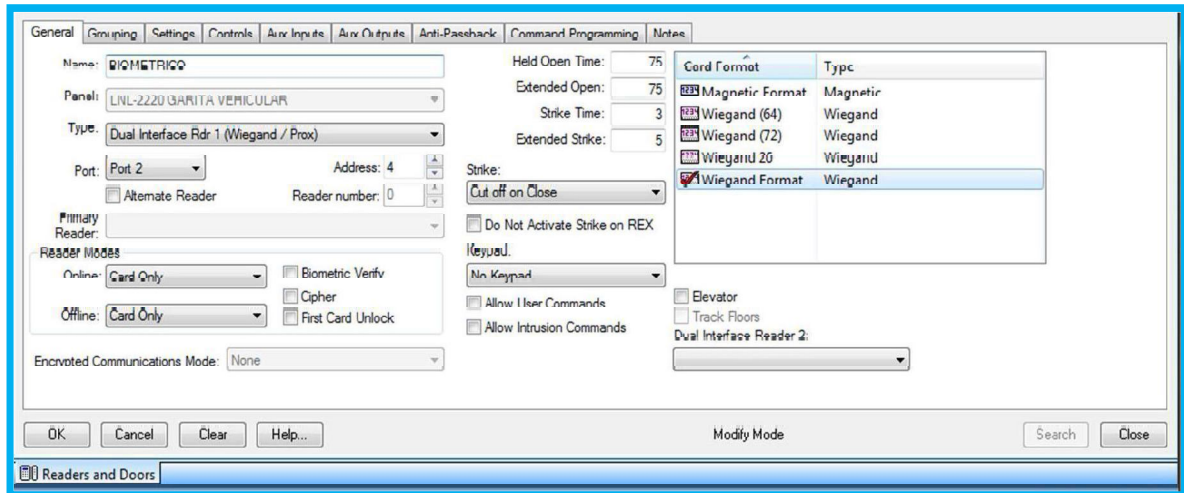


Figura 3. 62 Ventana de configuración e integración del biométrico

En la Figura 3.62 se puede apreciar la configuración de los campos para la integración del biométrico, como se puede ver el procedimiento es similar al de la integración de una lectora de proximidad con la diferencia que este equipo se conecta en el puerto de READER1 de la cuarta LNL-1320 perteneciente a la controladora LNL-2220 GARITA VEHICULAR. Se finaliza dando “OK” para terminar la integración.

Para que el biométrico reconozca el nivel de acceso otorgado en el sistema a cada usuario, se debe registrar el número de “BADGE” también en su propio software.

3.2.2.8 Diseño constructivo e implementación de la espina de pescado

Se ha creado la maqueta de espina de pescado de manera que se pueda simular el funcionamiento del sistema con los periféricos reales.



Figura 3. 63 Vista superior maqueta

Siguiendo la estructura del equipo real se ha armado esta simulación que tiene en su parte superior una placa de madera acoplada directamente al eje de giro, con 3 orificios en su perímetro de manera que cada orificio coincida en posición con una de las 3 espigas móviles, esto con el fin de que usando una solenoide a 24 VDC esta trabe el eje el momento que su parte móvil coincide con cualquiera de los 3 orificios.

El funcionamiento implica que el solenoide esté siempre alimentado y el eje por ende siempre trabado de manera que cuando el usuario intente ingresar o salir debe usar su tarjeta de proximidad con la lectora correspondiente y de esta forma se cambia el estado del RELÉ 1 y así se destraba el eje.



Figura 3. 64 Arreglo de placa de eje y solenoide

El circuito electrónico que se presenta a continuación es el que comanda el funcionamiento indicado anteriormente.

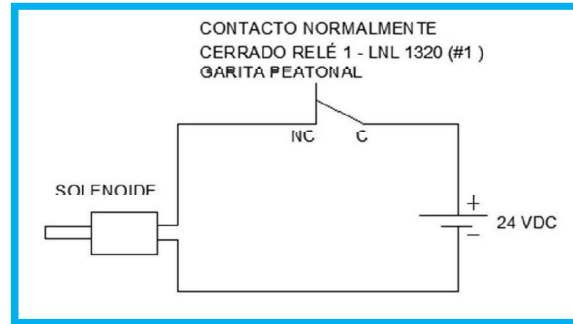


Figura 3. 65 Circuito de control solenoide

3.2.2.9 Diseño constructivo e implementación de la puerta motorizada de discapacitados

Se ha construido esta maqueta para simular el funcionamiento del equipo real como se puede ver en la Figura 3.66.



Figura 3. 66 Vista frontal de la maqueta de la puerta motorizada

Siguiendo la forma del equipo real se ha creado esta simulación de manera que al igual que el equipo real, esta se abra cuando el usuario use su tarjeta con la correspondiente lectora de proximidad y después de un tiempo programado de 4 segundos esta se cierre automáticamente; para este efecto se tiene en la parte baja acoplado al eje una caja reductora con un motor DC a 12VDC que hace que el motor gane torque para girar la batiente y pierda rapidez de giro dándole un efecto de apertura suave y constante.

Para detener la marcha del motor tanto en la apertura y en el cierre se ha usado fines de carrera, en la siguiente figura se detalla el circuito de control implementado en esta maqueta.

Debido a que el motor hace que la batiente se habrá muy rápido se ha añadido una resistencia de potencia en paralelo, con el objetivo de disminuir la potencia absorbida por el motor y este gire más lentamente.

El trabajo de la resistencia en si es disipar una parte de la potencia y ralentizar el giro del motor, se probó con diferentes valores, pero el más acertado fue el seleccionado usando dos resistencias de 1 ohm en paralelo de forma que se obtiene una resistencia comparable a la del motor y la corriente tiende a dividirse en valores similares.

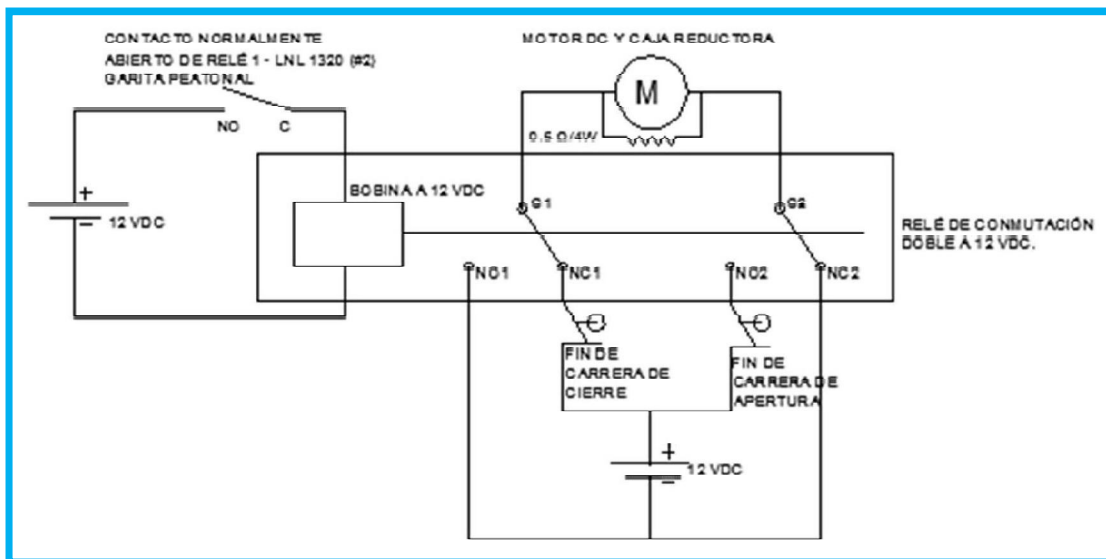


Figura 3. 67 Circuito de control de cierre – apertura de la puerta motorizada

Como se puede ver, el circuito implementado hace que el motor trate constantemente de cerrar la puerta pero el fin de carrera asociado a esta acción detiene la marcha y la batiente se mantiene quieta en la posición de cerrado. El momento en que el relé 1 principal cambia de estado por efecto de que el usuario acerco su tarjeta a la lectora correspondiente se activa el relé de conmutación doble y se invierte la polaridad en las borneras del motor, se abre la batiente 90° hasta que el segundo fin de carrera detiene su marcha, luego que el tiempo

seteado para el disparo del relé 1 se ha terminado, este regresa a su posición normal haciendo que el relé de conmutación doble invierta nuevamente la polaridad del motor y regresando a la batiente a su posición de cerrado.

3.2.2.10 Diseño constructivo e implementación de las barreras vehiculares

Se ha construido esta maqueta para simular el accionamiento del sistema desde las lectoras vehiculares asociadas a los booster.

El funcionamiento de cada barrera es idéntico pero se ha creado una maqueta doble debido a que cada lectora vehicular funciona de manera independiente.



Figura 3. 68 Vista frontal de la maqueta de las barreras vehiculares

Para simular el accionamiento y funcionamiento de los equipos reales se ha implementado esta maqueta que es accionada mediante el siguiente circuito electrónico implementado; al ser maquetas idénticas el circuito se aplica por duplicado.

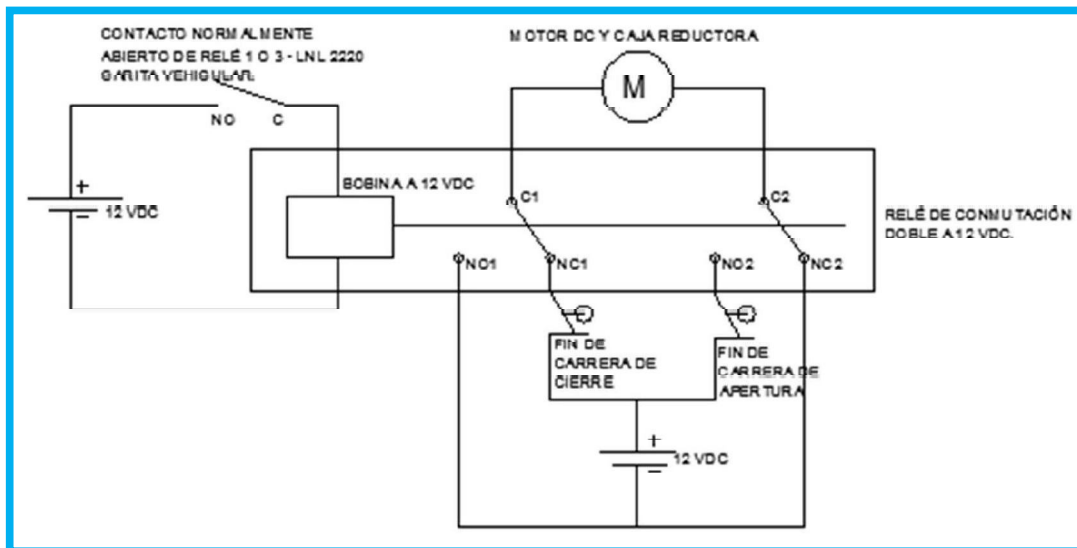


Figura 3. 69 Circuito electrónico de control de barreras vehiculares

El circuito indicado en el anterior figura es idéntico al implementado anteriormente con la puerta motorizada con la diferencia de que no se tiene las dos resistencias de 1Ω a 2W colocadas en paralelo al motor, ya que como el brazo de las barreras necesita ser elevado en contra de la fuerza de gravedad el motor con el arreglo de caja reductora requiere toda la potencia para realizar esa acción y debido a esto no se limita la corriente como en el caso citado de la puerta motorizada.

3.2.2.11 Diseño constructivo e implementación del molinete

Se ha elaborado una maqueta para simular el funcionamiento del sistema con este tipo de equipo y así poder realizar las pruebas necesarias.



Figura 3. 70 Vista frontal maqueta de molinete

Usando el siguiente accionamiento se puede implementar el funcionamiento de la maqueta construida.

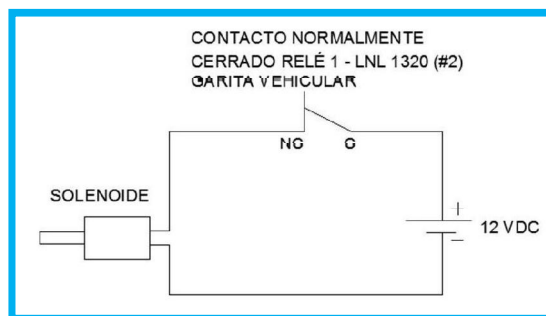


Figura 3. 71 Circuito electrónico de control del molinete

El circuito electrónico anterior permite que a través del relé 1 principal se pueda desactivar el solenoide que constantemente está trabando el mecanismo del molinete que se puede ver en la Figura 3.72.



Figura 3. 72 Vista interior de la maqueta de molinete

3.2.2.12 Diseño constructivo e implementación de la puerta de bunker

En el módulo de pruebas se ha creado una simulación de la puerta de bunker que se controla y se monitorea su estado mediante los paneles presentes en esta ubicación.

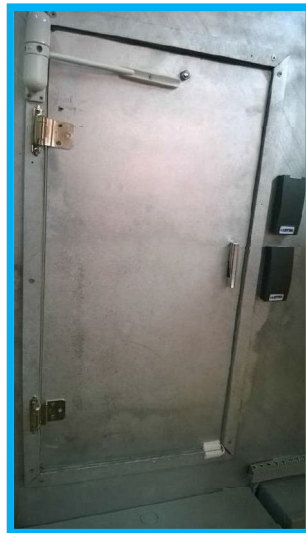


Figura 3. 73 Vista de simulación de puerta de bunker

Se ha instalado en el marco superior la chapa electromagnética de manera que cuando el sistema esté en funcionamiento esta puerta permanezca siempre cerrada, las lectoras previamente asociadas a esta simulación de puerta permiten realizar la acción de control y así desactivar la chapa para realizar la apertura de la puerta.

Se tiene también asociado un contacto magnético en el borde inferior del marco, de manera que este se integra como un periférico de entrada para que el sistema

detecte el estado de la puerta, es decir el sistema identifica si la puerta se encuentra cerrada o abierta.

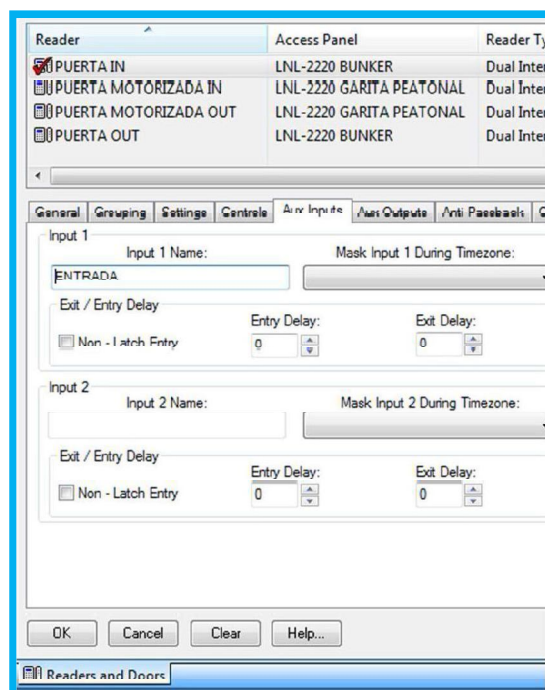


Figura 3. 74 Activación de contacto magnético asociado al estado de la puerta de bunker

3.2.2.13 Creación y configuración de áreas de interés

Se necesita definir las áreas que el sistema divide, es decir el sistema necesita identificar como se llaman las áreas que los equipos de control de accesos separan.

Como ejemplo se da el caso de la puerta de bunker en donde definimos como INTERIOR REFINERIA a lo que está fuera de Bunker y definimos INTERIOR BUNKER lo que está dentro de Bunker, esto con el fin de aplicar la tecnología denominada "ANTI-PASSBACK" en los accesos.

Anti-passback se traduce en que el sistema no deja salir de una ubicación a un usuario que previamente no entro y fue registrado por dicho sistema.

Es decir que si un usuario ingresó de manera fraudulenta en una ubicación en la que su horario no le permitía, si intenta salir usando su tarjeta a pesar de que ya

esté en su horario de trabajo y tenga acceso, el sistema no permitirá que este usuario salga ya que previamente su ingreso no fue registrado y se cumple la lógica de funcionamiento, nada que no haya entrado previamente puede salir.

Para crear áreas de interés se ingresa al “System administration” y se da clic en la opción “Access Control” y luego en “Areas” como se puede ver a continuación.

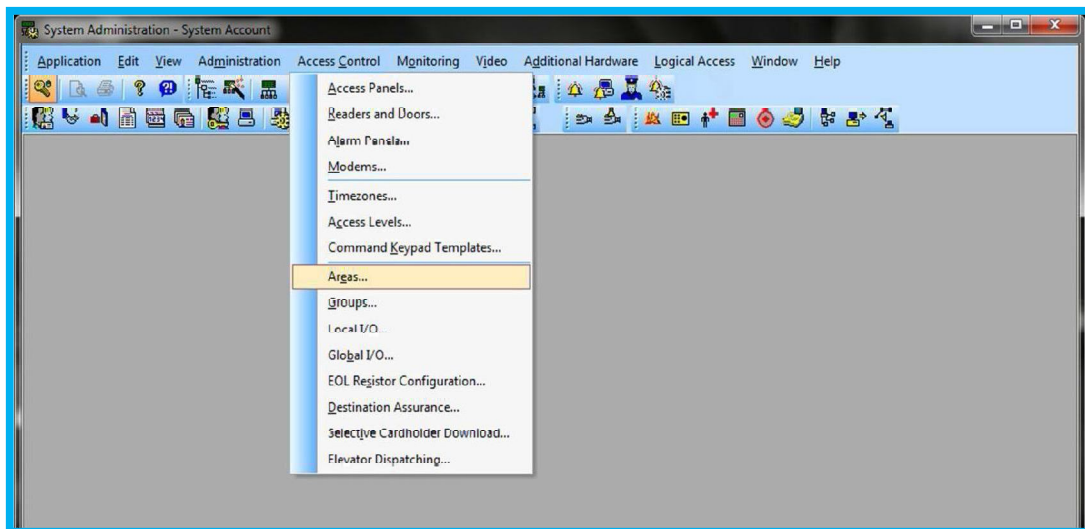


Figura 3. 75 Pantalla de ingreso a creación de áreas

Al ingresar se da clic en ADD y seleccionamos la controladora que comanda la ubicación de las áreas de interés que se van a crear.

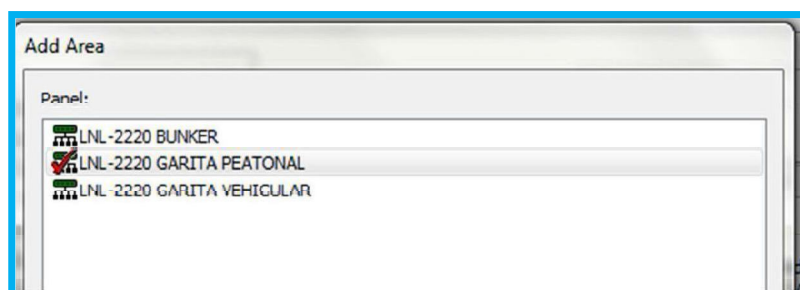


Figura 3. 76 Pantalla de selección de controladora

Una vez se ha seleccionado la controladora correspondiente se da clic en OK y se despliega la ventana de la Figura 3.77.

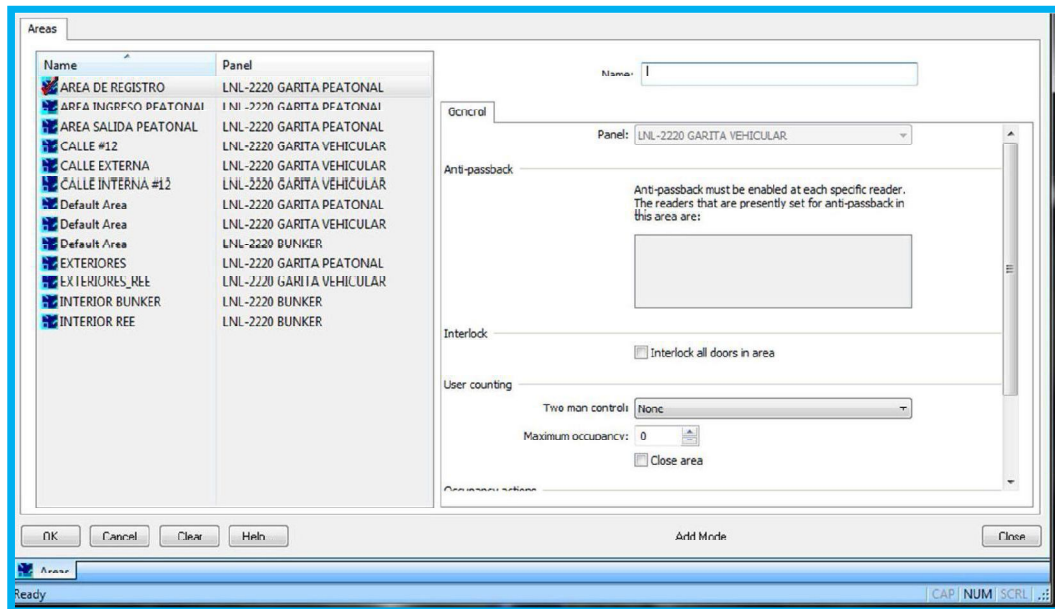


Figura 3. 77 Ventana de creación de área

En la anterior ventana se ingresa el nombre del área a crear y se da clic en OK para confirmar la creación; como también se puede ver se han creado las áreas de interés que a continuación se listan.

- GARITA PEATONAL:
- Área externa desde donde se ingresa: ÁREA INGRESO PEATONAL
- Área interna a la que se está ingresando: ÁREA DE REGISTRO
- GARITA VEHICULAR:
- Área externa desde donde se ingresa: CALLE EXTERNA
- Área interna a la que se está ingresando: CALLE #12 (CALLE INT. REE)
- BUNKER:
- Área externa desde donde se ingresa: INTERIOR REE
- Área interna a la que se está ingresando: INTERIOR BUNKER.

3.2.2.14 Creación y configuración de zonas de tiempo

Se necesita crear horarios de ingreso y salida del personal que usará el ingreso de las 3 diferentes ubicaciones intervenidas, de esta manera se ha creado el siguiente listado de horarios en base de los requerimientos del personal que labora en la refinería.

HORARIOS DE EMPLEADOS DE PLANTA:

Debido a que la refinería Esmeraldas necesita mantenerse funcionando las 24 horas del día, la administración tiene 3 jornadas laborables diarias de 8 horas y de lunes a domingo para cumplir con esta exigencia, dicho esto se ha pensado los siguientes horarios.

Turno #1: inicio 00:00 – finaliza 08:00

Turno #2: inicio 08:00 – finaliza 16:00

Turno #3: inicio 16:00 – finaliza 24:00

Horarios administrativos:

Los usuarios administrativos a diferencia de los empleados de planta tienen un solo horario laboral de 8 horas diarias de lunes a viernes.

Turno administrativo: inicio 07:30 – finaliza 16:30

Horarios de contratistas:

En el interior de la refinería se tienen varias empresas dedicadas a diferentes campos de la ingeniería trabajando, dicho esto estos grupos no son parte de la nómina de la refinería pero necesitan tener acceso para poder trabajar y movilizarse fácilmente. Con el propósito de simular esta situación se ha pensado en un horario de contratistas similar al que se puede tener en la realidad teniendo en cuenta que muchos contratistas no trabajan bajo los horarios de los empleados de planta de la refinería.

Turno contratista: inicio 08:00 – finaliza 16:00 de lunes a sábado

Horarios de visitas:

Se ha pensado en la creación de un horario único de lunes a viernes en el cual se les pueda dar acceso a los visitantes que tiene la refinería, todo en base a las actuales reglas de ingreso que se tiene en la refinería.

Turno Visitas: Inicio 08:00 – Finaliza 13:00

Una vez que se ha definido los horarios estos se crean en el sistema de administración para ello se ingresa en SYSTEM ADMINISTRATION en la opción de ACCESS CONTROL se da clic en TIMEZONES como se indica en la Figura 3.78.

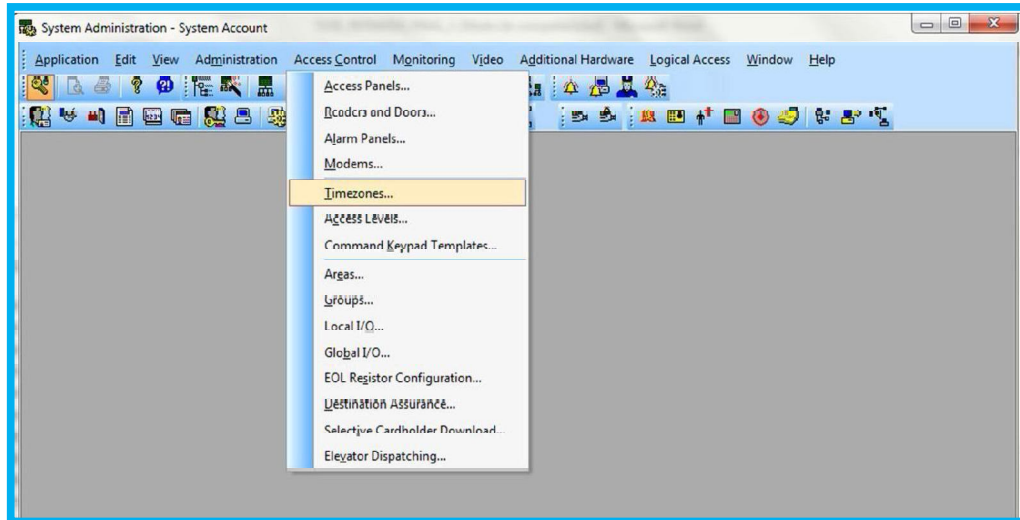


Figura 3. 78 Pantalla de ingreso a creación de horarios

Al ingresar se da clic en la pestaña denominada TIMEZONES y se da clic en ADD, al hacer esto se puede definir el nombre de nuestro horario, los días que está habilitado y su hora de inicio y de fin como se puede ver a continuación.

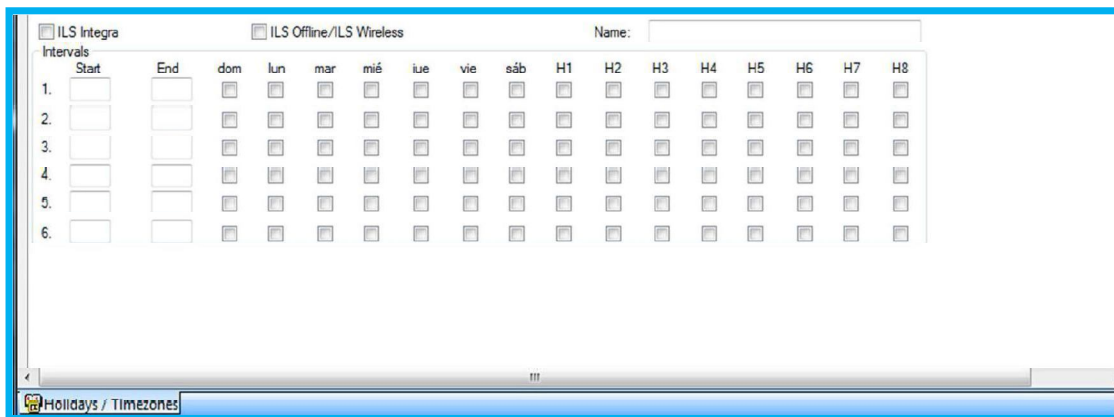


Figura 3. 79 Pantalla de registro de horarios

De esta forma se ingresan al sistema los horarios previamente definidos y quedan listados como se puede ver en la Figura 3.80.

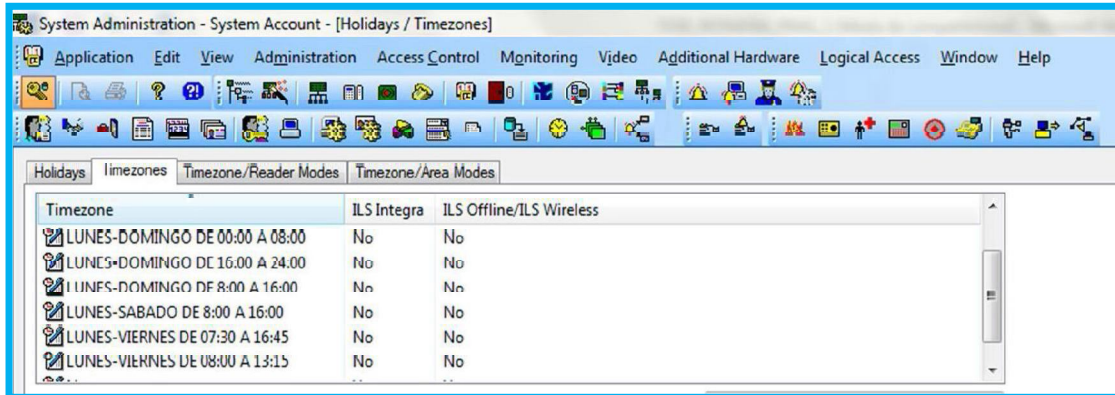


Figura 3. 80 Horarios creados en el sistema

3.2.2.15 Creación y configuración de niveles de acceso

Se necesita crear diferentes niveles de accesos en el sistema, esto se refiere a que un empleado administrativo no puede tener el mismo acceso que un empleado de planta o que un visitante no puede tener el mismo nivel de acceso que un contratista. Dicho esto a continuación se lista los diferentes niveles de acceso que se necesitan para el personal.

Empleados de planta:

- Turno #1 empleados planta
- Turno #2 empleados planta
- Turno #3 empleados planta

Empleados administrativos:

- Turno único personal administrativo

Contratistas:

- Turno normal contratistas

Visitantes:

- Turno único visitas

A diferencia de la creación de los horarios, los niveles de acceso se usan para asociar dichos horarios previamente creados con los equipos de control de

accesos por los que el usuario tendrá o no acceso, por ese motivo se indica a continuación los accesos a los que tienen cada grupo de personas.

Empleados de planta:

- Espinas de pescado (torniquetes) de ingreso - salida por la garita peatonal.
- Puerta motorizada de discapacitados de la garita peatonal.
- Handkeys de registro de personal de la garita peatonal.
- Handkeys de registro de personal de la garita vehicular.
- Molinete de ingreso por la garita vehicular.
- Barreras vehiculares de ingreso – salida de la garita vehicular.
- Puerta de ingreso a bunker.

Empleados administrativos:

- Espinas de pescado (torniquetes) de ingreso - salida por la garita peatonal.
- Puerta motorizada de discapacitados de la garita peatonal.
- Handkeys de registro de personal de garita peatonal.

Contratistas:

- Molinete de ingreso por la garita vehicular.
- Barreras vehiculares de ingreso – salida de la garita vehicular.
- Biométrico de registro de contratistas de la garita vehicular.

Visitantes:

- Espinas de pescado (torniquetes) de ingreso – salida por la garita peatonal.
- Puerta motorizada de discapacitados de la garita peatonal.

El anterior listado se interpreta de manera que no todos los grupos de personas pueden acceder por cualquier acceso.

Para configurar lo anterior en el sistema se ingresa en “System administration” y se da clic en “Access levels” para poder ingresar a la pantalla de configuración.

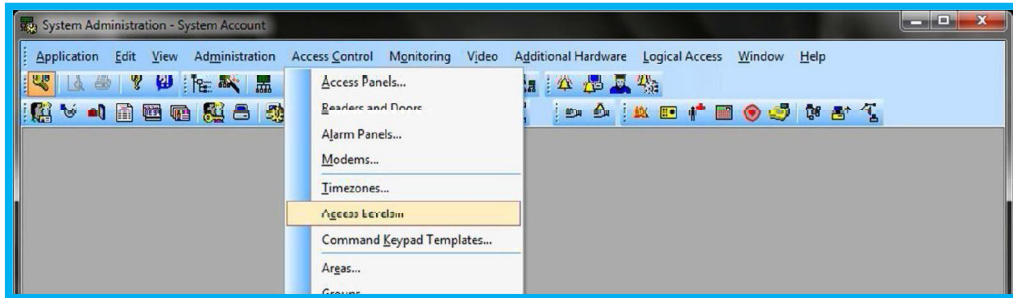


Figura 3. 81 Horarios creados en el sistema

Al ingresar se da clic en “Add” en la parte inferior izquierda e inmediatamente se despliega la siguiente ventana.

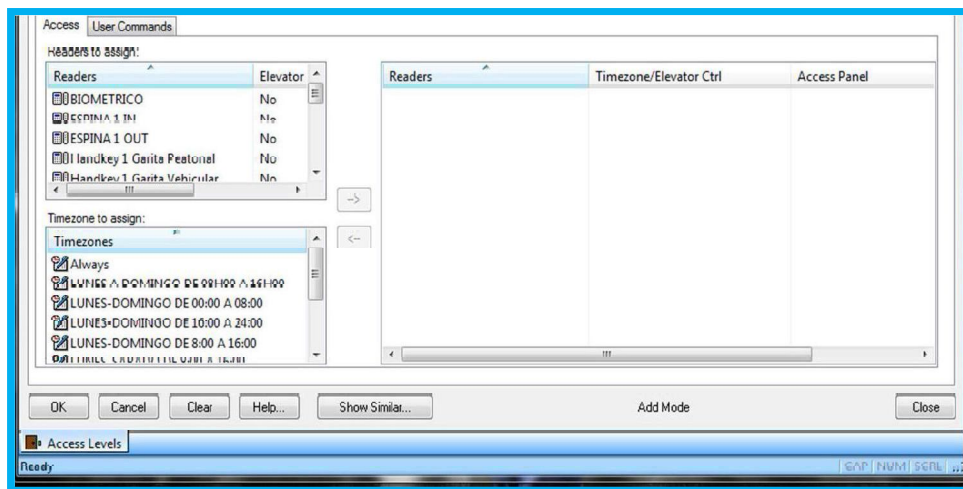


Figura 3. 82 Pantalla de creación de niveles de acceso

En esa ventana se tiene el campo denominado “READERS TO ASSING (LECTORAS A ASIGNAR)” y otro campo denominado “TIMEZONE TO ASSING (HORARIO A ASIGANAR)”; entonces se selecciona un horario y los accesos correspondientes y se los exporta juntos con la flecha que apunta hacia la derecha de manera que en el campo de la derecha se agrupen como se muestra a continuación.

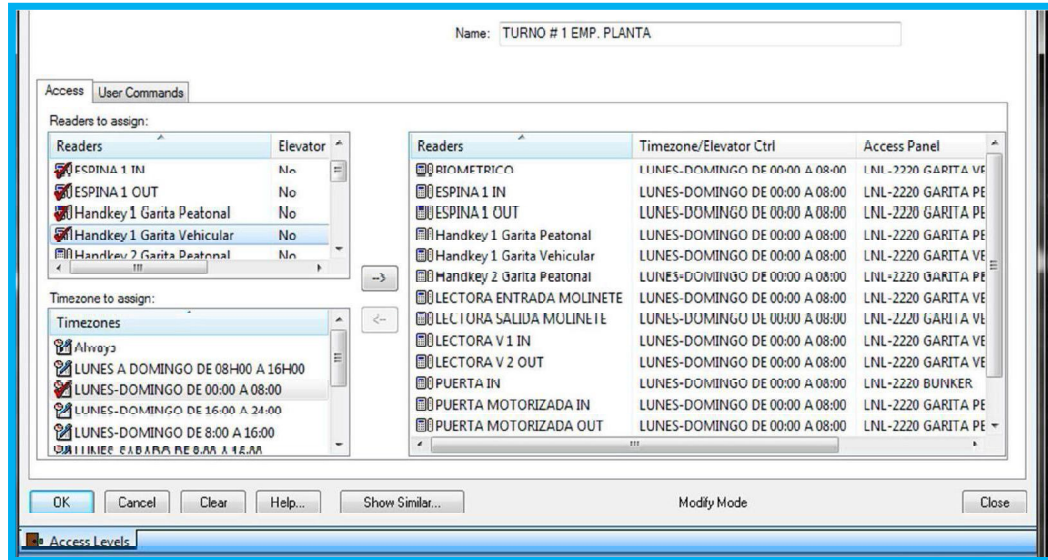


Figura 3. 83 Pantalla de creación de niveles de acceso

Al finalizar el anterior ejercicio los accesos seleccionados se agrupan en un mismo horario, de manera que este se crea como un nivel de acceso dándole un nombre en este caso TURNO #1 EMP. PLANTA. Siguiendo esa misma secuencia se crean el resto de niveles de acceso de manera que al finalizar estos queden listados en el sistema.

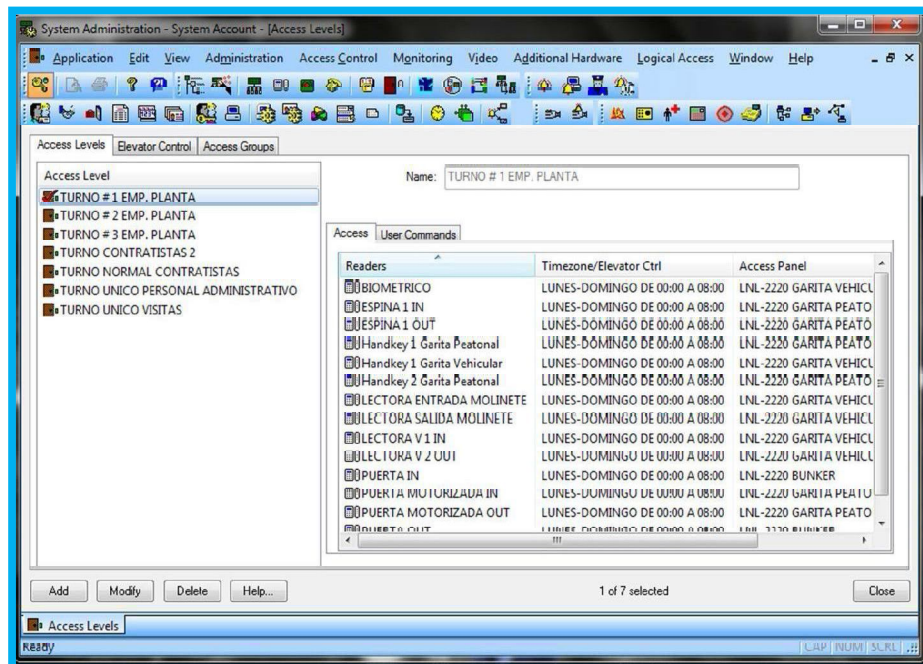


Figura 3. 84 Niveles de acceso creados en el sistema

3.2.2.16 Creación y configuración de usuarios (tarjerahabientes)

Como paso final es necesario crear o enrolar en el sistema a los usuarios que serán portadores de tarjetas de proximidad y de los equipos biométricos.

Para iniciar se ingresa en “System administration” y se da clic en la opción “Administration” y en la sub opción denominada “Cardholders”, al realizar esa secuencia se despliega una nueva ventana en donde se tienen diferentes campos y opciones en los que se ingresa la información de usuario.

Figura 3. 85 Pantalla de creación – enrolamiento del usuario

En los campos que posee la pantalla anterior se debe llenar con los datos básicos y extra del usuario como por ejemplo un nombre y un apellido, el número de cédula o pasaporte, el tipo de cargo, su dirección, ciudad donde reside, email, etc.

Finalizado eso se da clic en la pestaña denominada “Badge”, que se muestra a continuación en la Figura 3.86.

Figura 3. 86 Pantalla de asignación de credencial

En la opción de “Badge” se le indica al sistema que tipo de tarjeta habiente se está creando entre las opciones de EMPLEADO, VISITANTE o EMPLEADO TEMPORAL.

El campo denominado “Badge ID” es donde se le indica al sistema cual es el número de la tarjeta que poseerá el usuario; las tarjetas que se han adquirido están electrónicamente numeradas de fábrica desde el 1 al 2000.

Los campos denominados “Activate” y “Deativate” se refieren a la fecha de inicio y fin del permiso concedido que por estándar es de 5 años a partir de la activación.

El campo llamado “PIN” se refiere a si el usuario a parte de manejar una tarjeta electrónica de proximidad también usará un clave de 4 dígitos, en caso de ser así en este campo se escribe dicha clave.

Una vez se ha finalizado con este proceso se da clic en la siguiente pestaña denominada “Access Levels” que se muestra en la Figura 3.87.

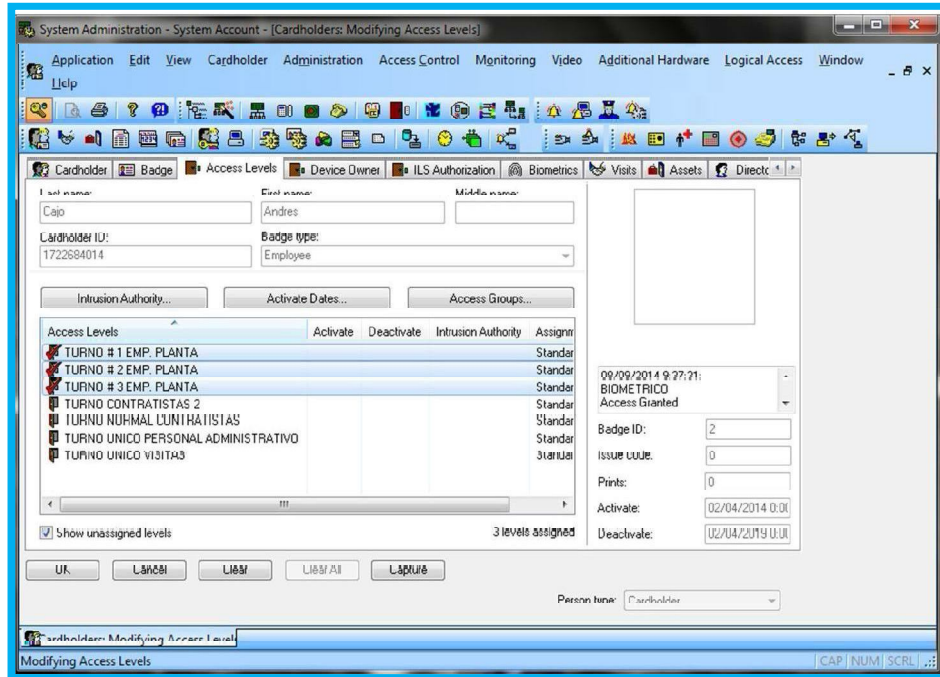


Figura 3. 87 Pantalla de asignación de niveles de acceso

Se ingresa a la ventana de la Figura 3.88 y aquí se le asigna al usuario su nivel de acceso de manera que se puede seleccionar dando clic cualquiera de los niveles creados con anterioridad. A continuación en la pestaña denominada “Device owner” se pueden ver listados los equipos por los que el usuario tiene acceso.

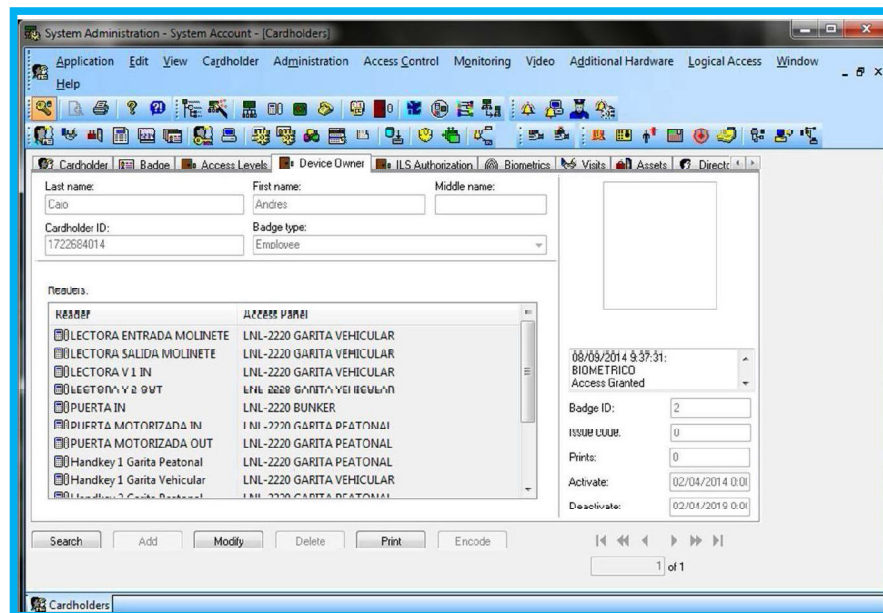


Figura 3. 88 Pantalla de verificación de accesos

Al dar clic en la pestaña llamada “Biometrics” se puede hacer el registro de geometría de mano de los usuarios que deban registrar su ingreso en los handkeys; para esto se da clic en “Capture” y se despliega la siguiente ventana.

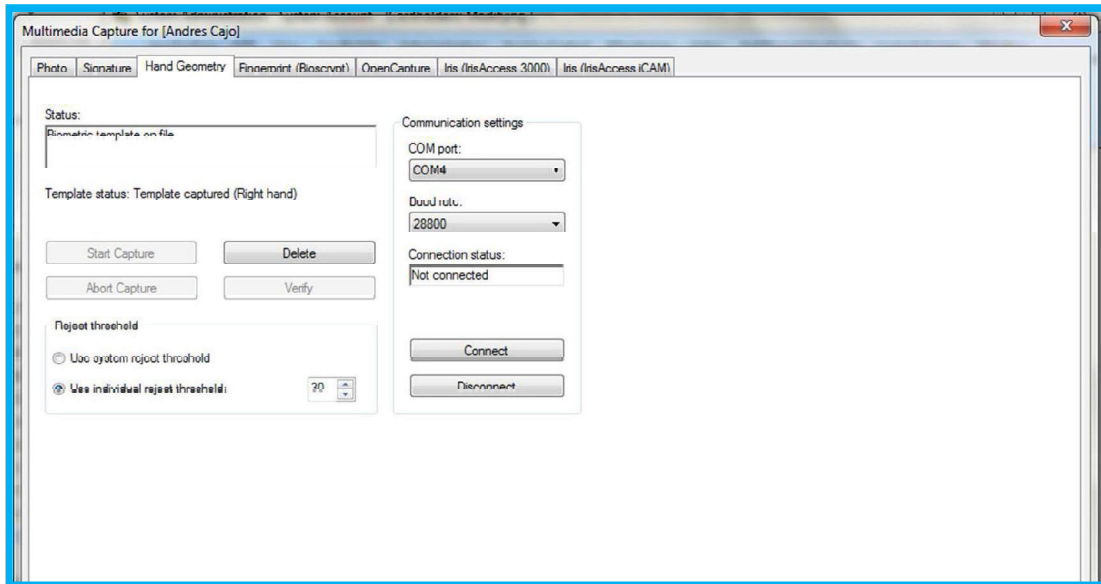


Figura 3. 89 Pantalla de inicio de captura de geometría de mano

Una vez activa la anterior ventana se necesita usar un equipo de lectura de geometría de mano “HANDKEY” aparte de los que se usan en el resto del proyecto; este equipo esta designado exclusivamente para hacer los enrolamientos del personal de la refinera, de manera que se lo energiza a 12 VDC y se lo conecta al servidor donde está instalado ONGUARD usando el cable provisto por el fabricante vía RS-232 y se lo configura de manera que trabaje a una velocidad de 28800 baudios en modo remoto como se recomienda en el manual de usuario o en su defecto 19200 baudios dependiendo esto netamente del puerto del servidor usado para este efecto.

Una vez se ha conectado el equipo y el sistema lo ha reconocido se necesita que el usuario coloque su mano 3 veces para que el equipo tenga un registro claro de la forma de la mano y verifique con claridad las lecturas, finalizado esto se da clic en “OK” y el sistema admite la creación de una característica biométrica como se puede ver en la Figura 3.90.

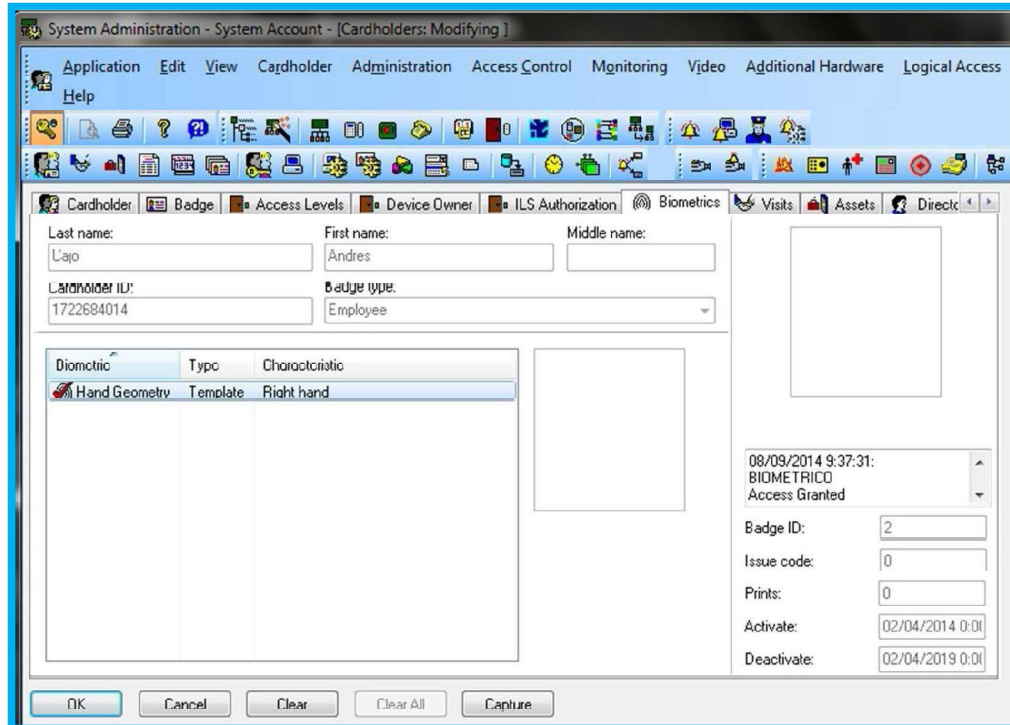


Figura 3. 90 Ventana de registro de la mano derecha del usuario

El anterior grupo de procesos de asignación e identificación se realizan con todos los usuarios tanto empleados de planta como administrativos, contratistas y los visitantes de forma que el sistema tenga un registro total del personal y visitantes que ingresan y salen constantemente de las inmediaciones.

En este capítulo se ha descrito la creación de los módulos de simulación necesarios para realizar las pruebas de funcionamiento de los subsistemas de control de accesos y CCTV con los diferentes equipos adquiridos.

Todas las configuraciones se realizaron en base de un previo análisis del funcionamiento que se tendrá en la realidad, tomando como referencia conversaciones previas con el cliente y para realizarlas fue necesario adquirir varios conocimientos acerca del manejo del software ONGUARD y de los diferentes equipos que se han ocupado.

Las maquetas que se han creado son la representación más tangible posible de los equipos reales que se encuentran en poder de la refinería Esmeraldas.

CAPÍTULO 4

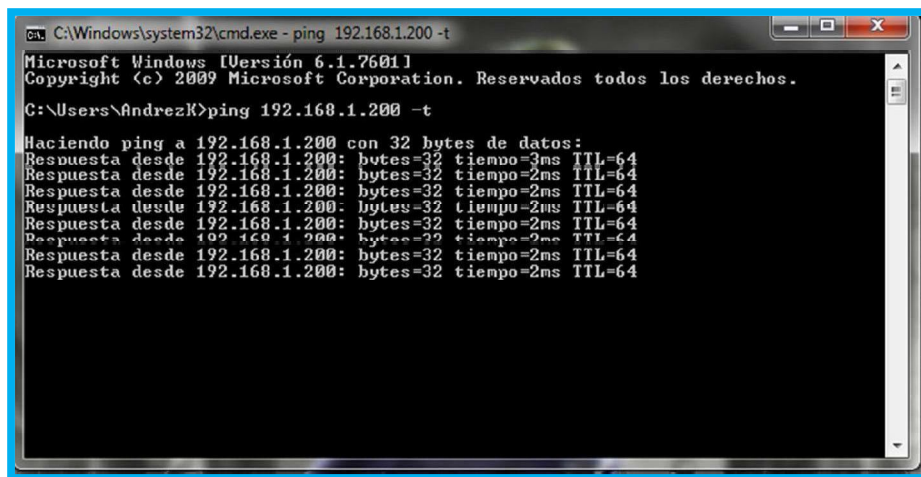
PRUEBAS Y RESULTADOS DEL FUNCIONAMIENTO DE LOS MÓDULOS ARMADOS

4.1 PRUEBAS Y RESULTADOS DEL SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

4.1.1 PRUEBAS DE FUNCIONAMIENTO

Se realizó primero pruebas de conectividad del subsistema a la red privada que se creó para el módulo de pruebas; esto con el objetivo de tener la certeza de que los equipos efectivamente estén correctamente enlazados a esta.

Para esta prueba se ingresó al símbolo del sistema (CMD) y se ingresó el comando PING 192.168.1.XX -t con la dirección IP fija de cada cámara. El sistema devolvió el resultado de conectividad como se puede ver en la Figura 4.1 usando como ejemplo el video web server de la cámara PTZ con IP 192.168.1.200.



```
C:\Windows\system32\cmd.exe - ping 192.168.1.200 -t
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\AndrezK>ping 192.168.1.200 -t
Haciendo ping a 192.168.1.200 con 32 bytes de datos:
Respuesta desde 192.168.1.200: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.200: bytes=32 tiempo=2ms TTL=64
```

Figura 4. 1 Respuesta de conectividad usando el comando PING

Una vez que se comprobó la conectividad se ingresó a “SYSTEM ADMINISTRATION” y se verificó que el sistema efectivamente está recibiendo la información. Para esto se seleccionó “DIGITAL VIDEO” y de la cámara

correspondiente se habilitó la opción que se denomina “DISPLAY VIDEO” que se aprecia en la Figura 4.2.

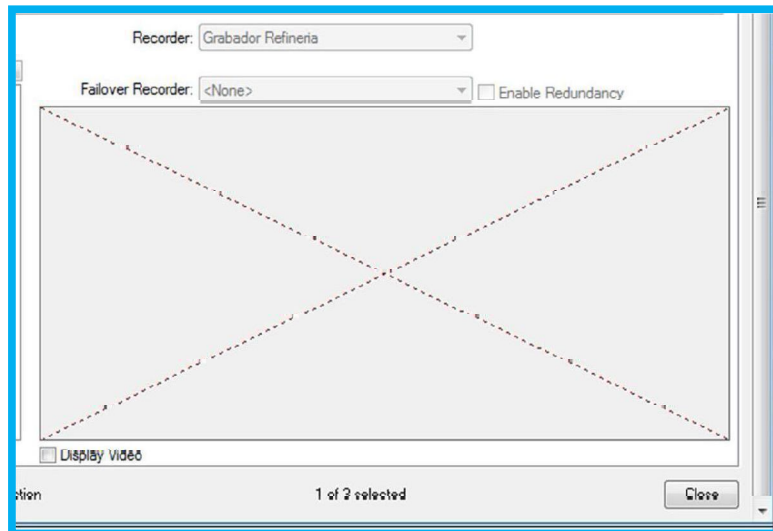


Figura 4. 2 Campo de habilitación y visualización previa de imagen de las cámaras integradas

Para el caso de la cámara fija que corresponde a la GARITA PEATONAL se tuvo la siguiente respuesta de imagen en el sistema.

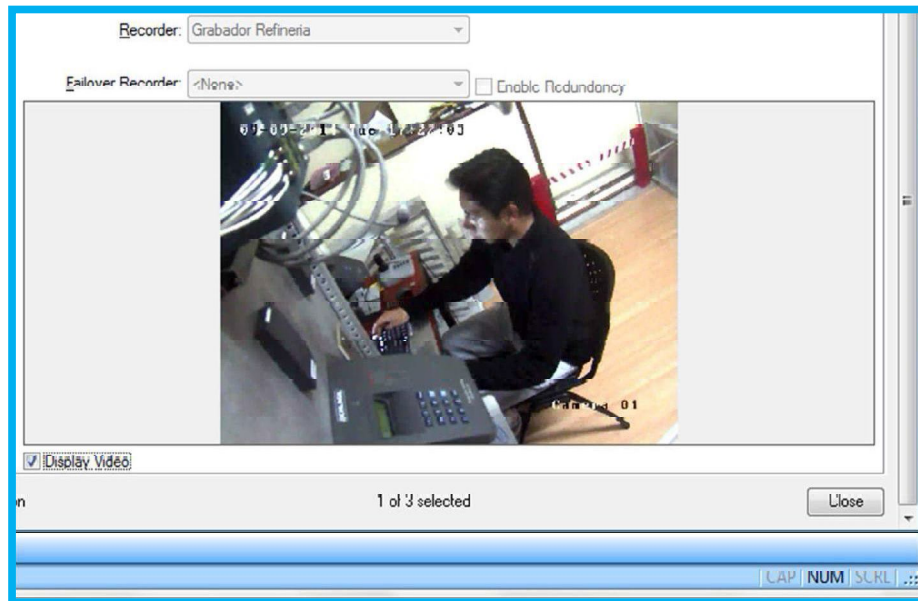


Figura 4. 3 Imagen de visualización inicial de la cámara de la garita peatonal

En el caso de la cámara que corresponde a la garita vehicular se obtuvo la siguiente respuesta del sistema.

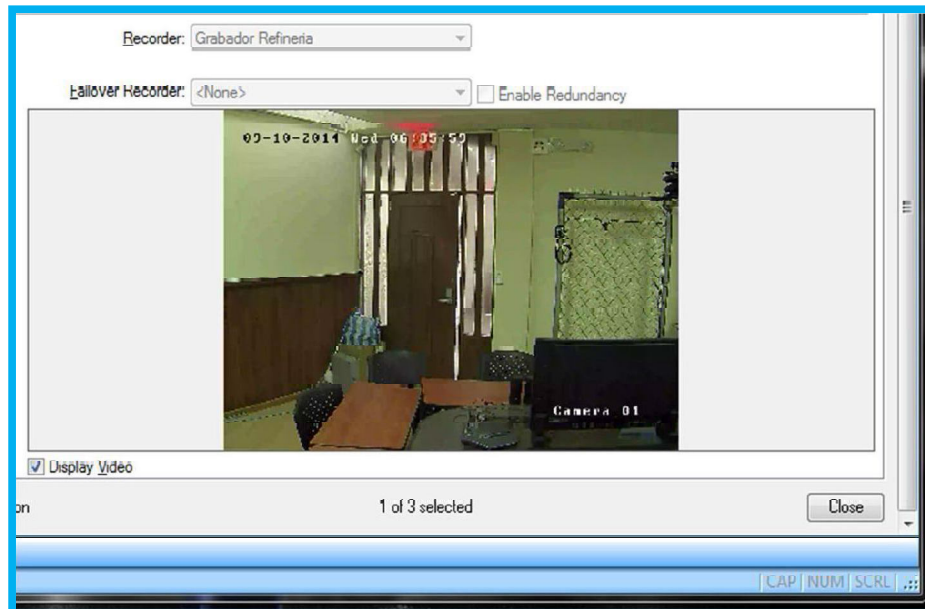


Figura 4. 4 Imagen de visualización inicial de la cámara de la garita vehicular

Finalmente, para el caso de la cámara PTZ se obtuvo la siguiente respuesta del sistema.

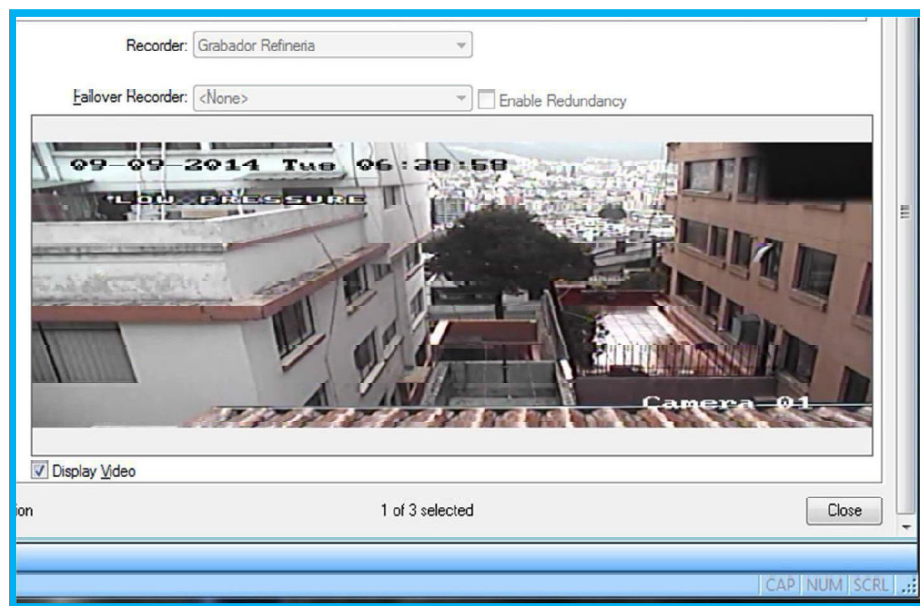


Figura 4. 5 Imagen de visualización inicial de la cámara PTZ de perímetro

Luego que se comprobó exitosamente que el sistema está recibiendo la información captada por las cámaras, se realizó a continuación diferentes pruebas desde la interfaz de usuario que se denomina “VIDEO VIEWER” que es la interfaz de usuario dedicado para el monitoreo que presenta el software ONGUARD.

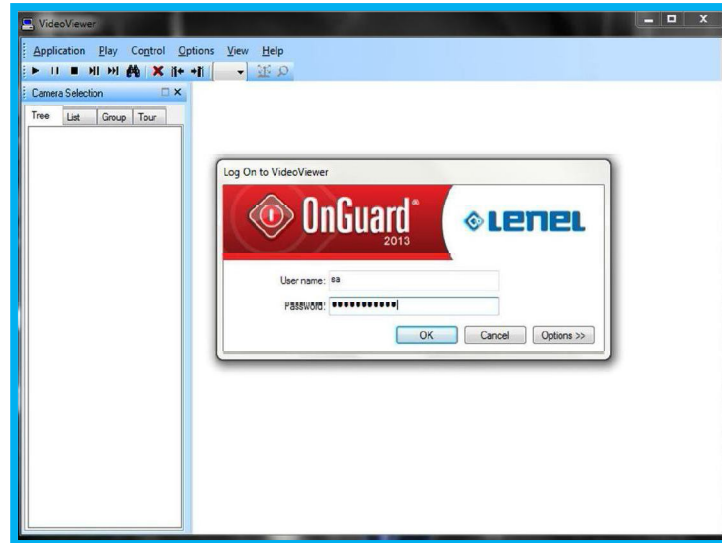


Figura 4. 6 Pantalla de ingreso a la interfaz de VIDEO VIEWER

Al ingresar se pudo comprobar que debido a que se obtuvo previamente resultados exitosos de conexión, en esta interfaz se pudo apreciar, como se indica a continuación, que el grabador y las 3 cámaras usadas se han conectado correctamente.

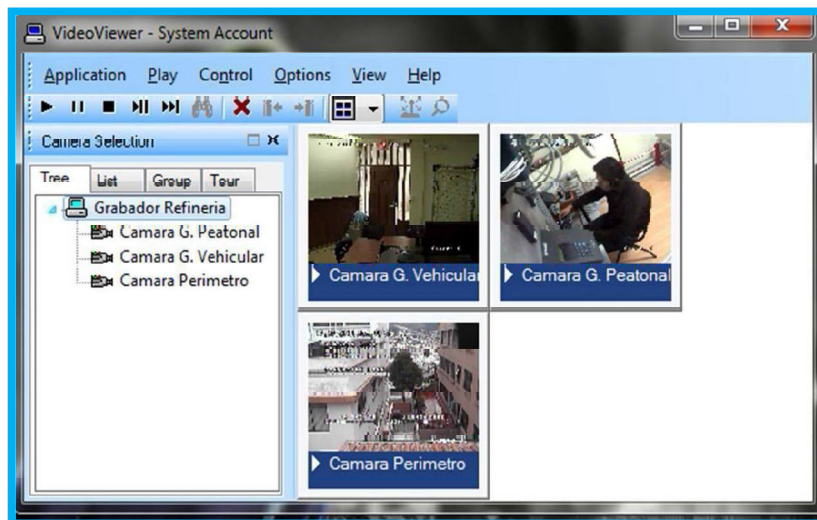


Figura 4. 7 Cámaras conectadas correctamente en el sistema ONGUARD

Se pudo apreciar que el sistema inmediatamente visualiza las diferentes cámaras conectadas e integradas. Cuando se cortó la comunicación simulando una falla el sistema perdió las imágenes y lo que se pudo visualizar es la siguiente imagen.

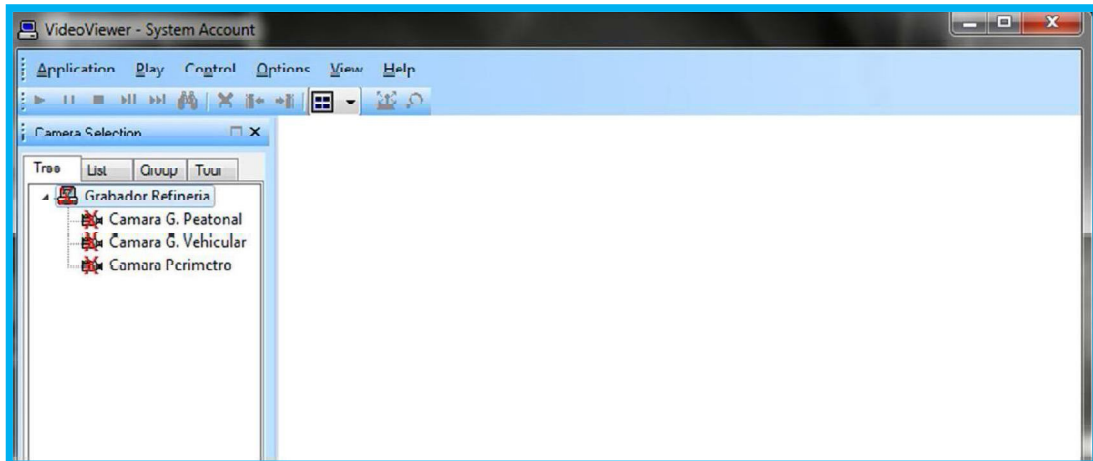


Figura 4. 8 Ventana del sistema cuando la conexión de comunicaciones falla

Para poder realizar la prueba de administración de video se necesitó realizar grabaciones con las diferentes cámaras. Para esto, es necesario que previamente se active el grabador virtual; esto se logra dando clic en "START LNVR SERVICES" que es un servicio manual que se instaló como complemento de funcionamiento del grabador virtual.

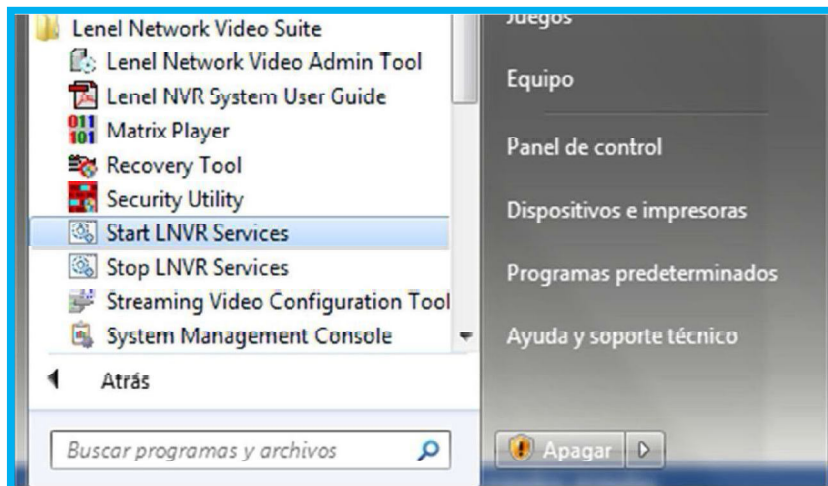


Figura 4. 9 Arranque del grabador virtual LNVR

Luego se debe ingresar nuevamente en la interfaz de “VIDEO VIEWER”, seleccionar las diferentes cámaras que se han de visualizar y de este modo se tienen las 3 cámaras que se integró previamente.

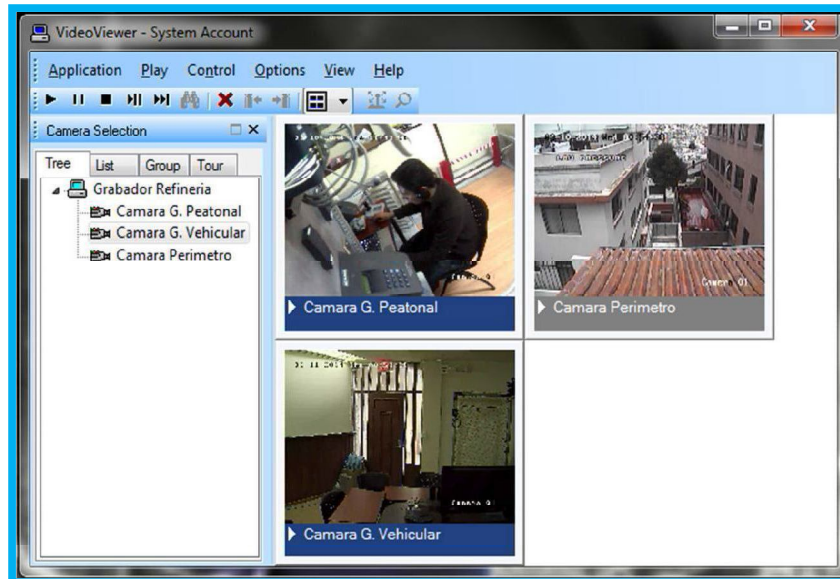


Figura 4. 10 Monitoreo simultáneo desde VIDEO VIEWER

Desde que se arrancó el grabador virtual este está recopilando en tiempo real el video que proviene de las 3 cámaras de manera simultánea. Se pueden ubicar las ventanas de visualización de muchas formas para comodidad del usuario y eso se realizó con el uso del icono denominado “SELECT TEMPLATE MODE”.

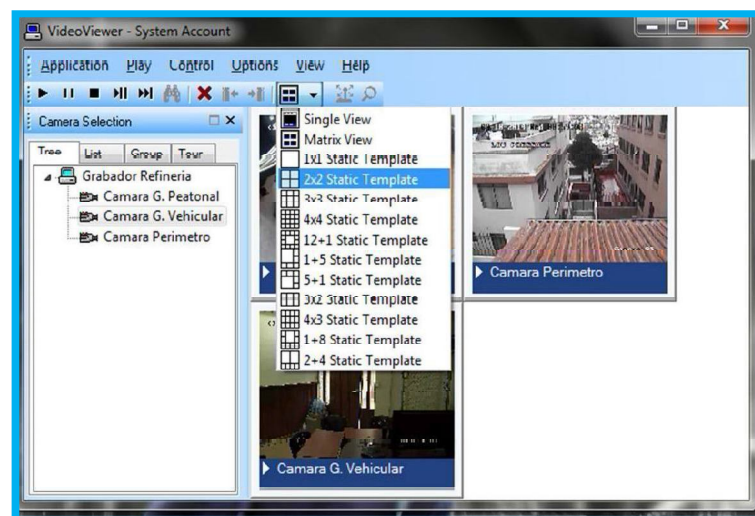


Figura 4. 11 Cambio de vistas en el sistema de monitoreo

Cada una de las ventanas de visualización son interactivas de forma que se realizó pruebas de grabación y monitoreo como se presenta a continuación. Para este efecto se debe dar doble clic sobre la cámara seleccionada de manera que se despliega una ventana individual como en la siguiente figura.

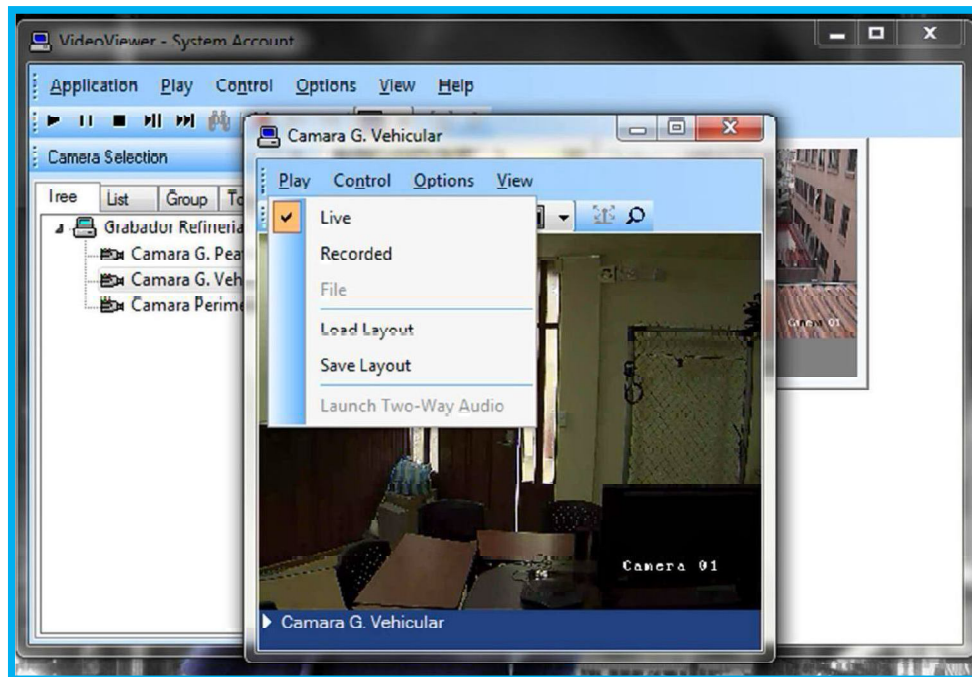


Figura 4. 12 Ventana individual de monitoreo de la cámara de Garita Vehicular

En esta nueva ventana se tiene el control exclusivo de la cámara seleccionada de forma que se puede realizar el monitoreo en tiempo real o se puede navegar por el video que se grabó previamente.

Para ejemplificar la navegación en la grabación de esta cámara se debe fijar un objeto de interés, en este caso se creó el ejemplo de un celular olvidado sobre la mesa. La cámara bajo prueba se puede ver en la Figura 4.13.

La hora de grabación desde que el celular está abandonado es 12 horas 24 minutos y 21 segundos y se marca en la ventana de visualización.

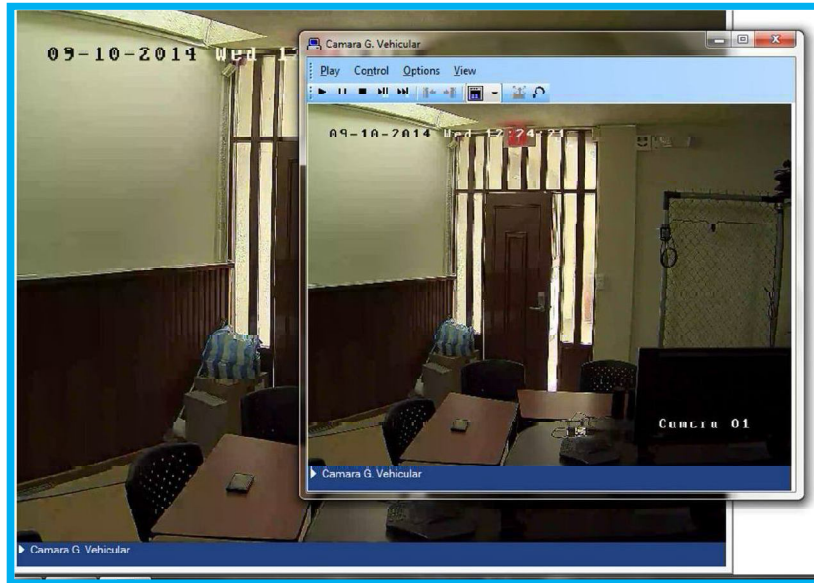


Figura 4. 13 Ventana individual de monitoreo de la cámara de Garita Vehicular

Ha pasado ya unos minutos desde que el teléfono ha sido olvidado y su dueño regresa a recuperarlo pero este ya no se encuentra. Gracias a que se han grabado los eventos y se continúan grabando, se pudo identificar quien se sustrajo el celular y a qué hora ocurrió exactamente dicho evento como se puede visualizar en la Figura 4.14.

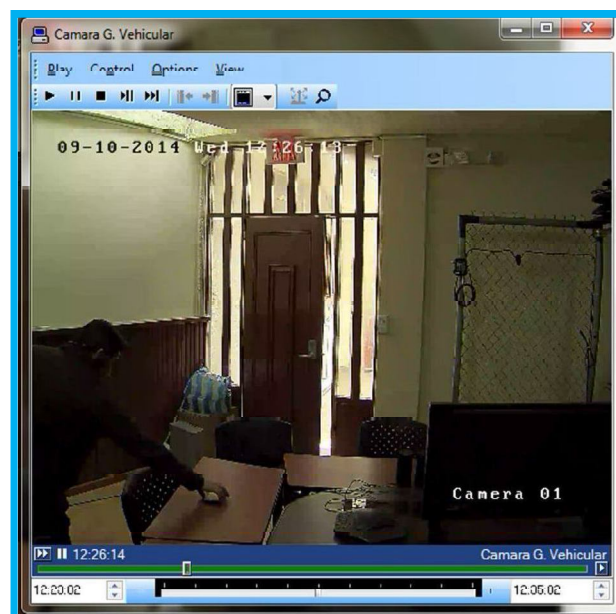


Figura 4. 14 Ventana individual de monitoreo de la cámara de Garita Vehicular

Al igual que el caso anterior se hizo pruebas de monitoreo con la cámara de Garita Peatonal y el funcionamiento es correcto con una imagen definida y tiempos de lag (retardo) menores a 1 segundo.

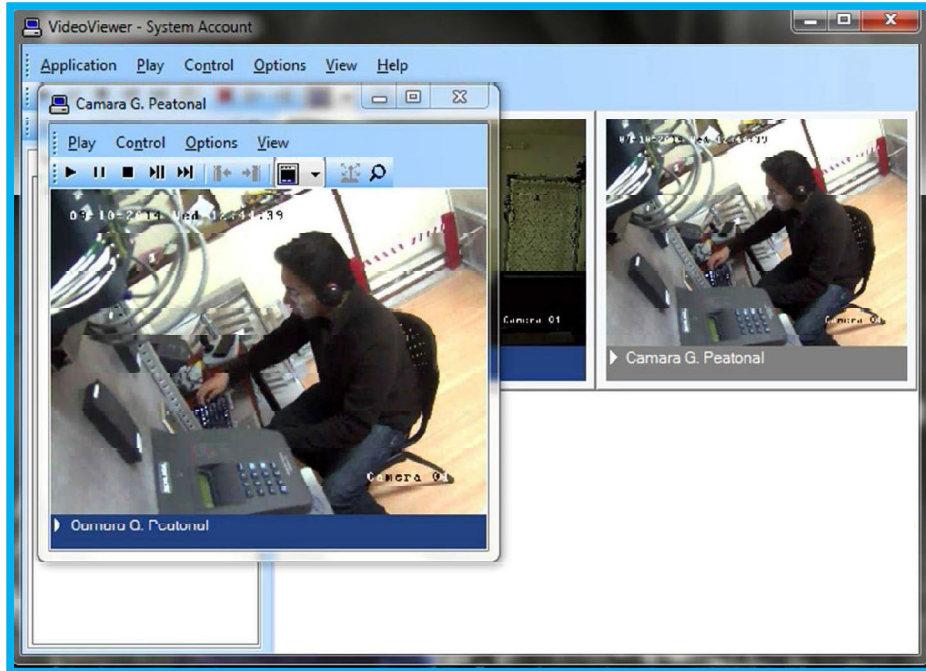



Figura 4. 15 Ventana individual de monitoreo de la cámara de Garita Peatonal

A diferencia de las cámaras anteriores, la cámara PTZ tiene mayores capacidades en cuestiones de monitoreo gracias a que esta puede rotar 360° y realizar zoom óptico remotamente, para probar estos puntos de una manera cómoda y rápida se usó un joystick como el que se puede ver a continuación.



Figura 4. 16 Joystick asociado al monitoreo con la cámara PTZ de perímetro

Este equipo no necesita configurarse manualmente ya que es de tecnología plug and play y se conecta mediante el puerto USB. Las funciones que se asocian directamente en este equipo fueron el zoom de la cámara y el giro que son los aspectos más importantes.

Al ingresar a la ventana individual se activó automáticamente este ícono  que implica que existe un periférico de entrada (joystick) para el manejo adecuado de las capacidades de la cámara PTZ. Caso contrario este ícono permanece inactivo y la cámara se puede manejar desde el mouse disponible.

Como punto de partida usando el joystick se ubicó la cámara en una visualización frontal hacia el paisaje del norte de Quito y con el mínimo de zoom, como se puede apreciar en la Figura 4.17.

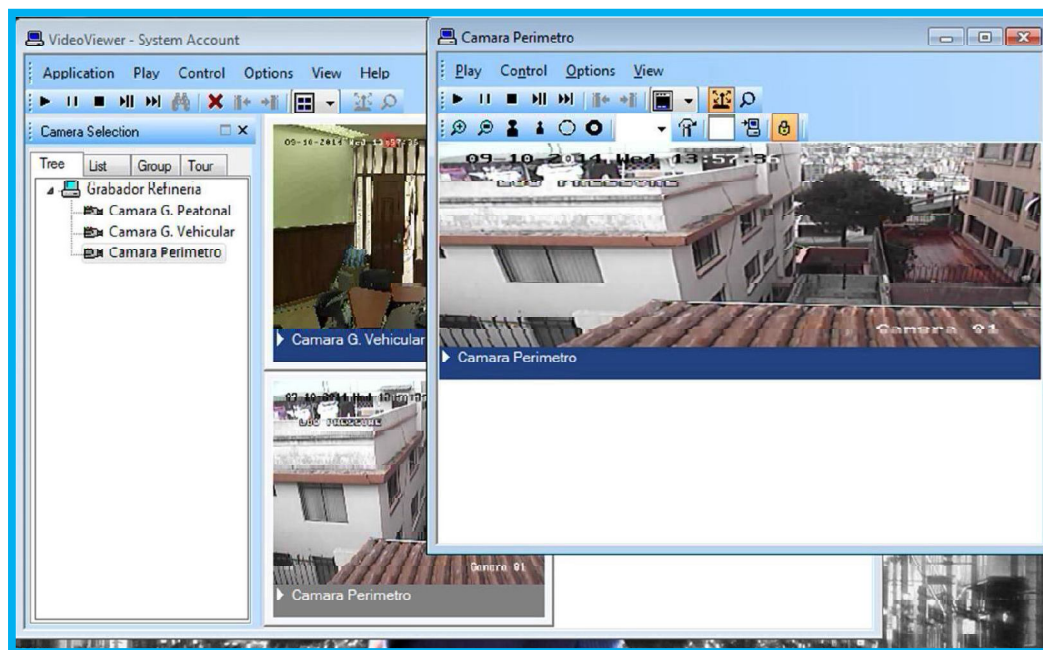


Figura 4. 17 Ventana individual de monitoreo de la cámara PTZ de perímetro

Girando la perilla que dispone el joystick en sentido horario se manipula el zoom de forma que se tiene en la siguiente imagen la vista a aproximadamente la mitad del zoom.

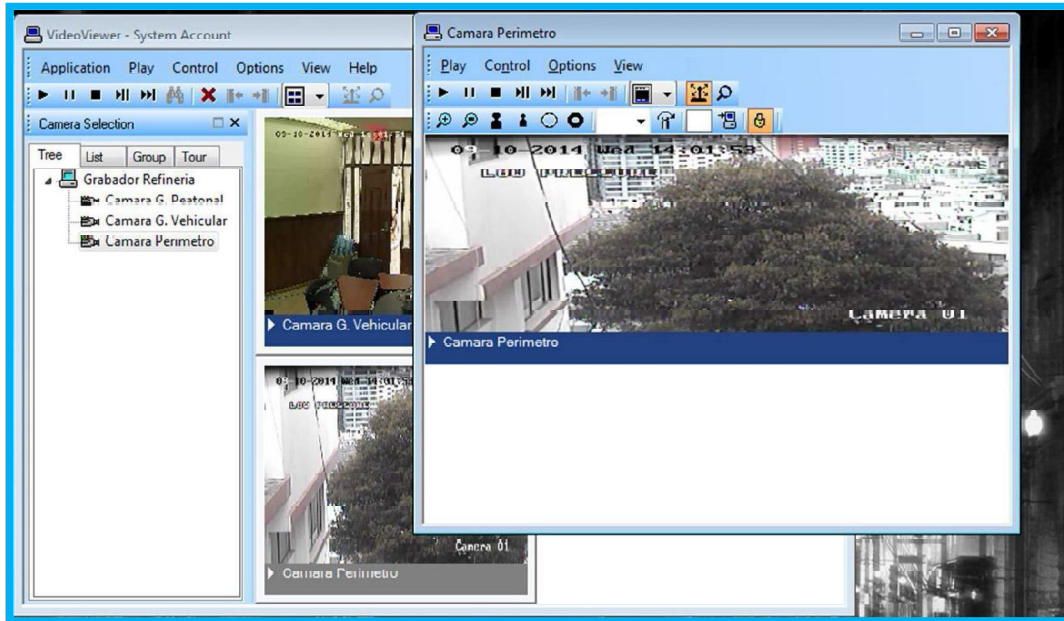


Figura 4. 18 Vista de la cámara PTZ a la mitad del zoom

Se usó nuevamente la perilla para llevar el zoom al máximo y este fue el resultado final.

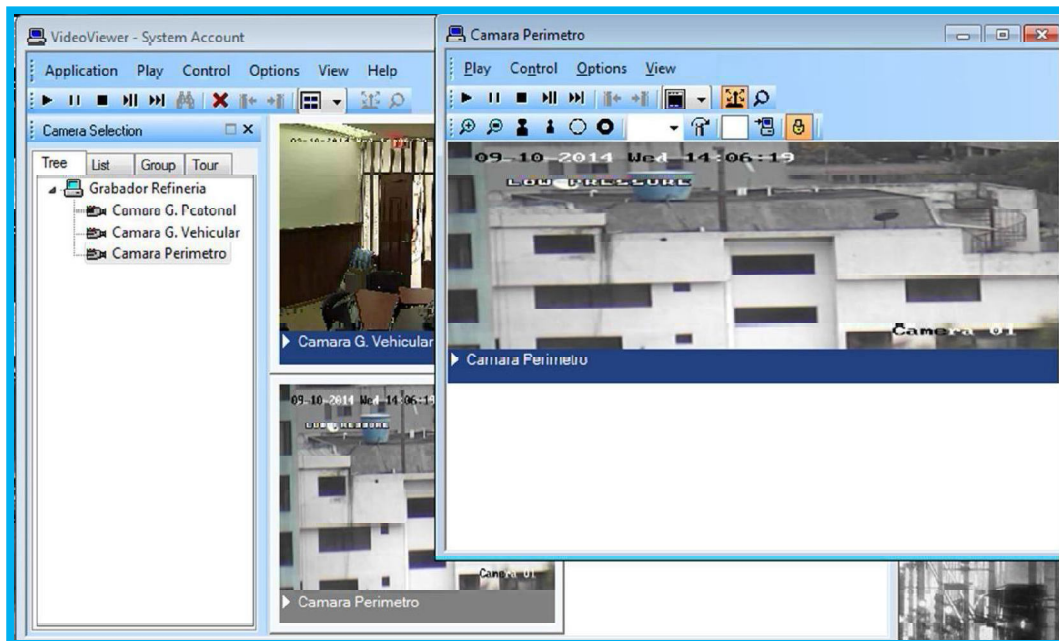


Figura 4. 19 Vista de la cámara PTZ con el zoom al máximo

Con esta prueba se ha demostrado el correcto funcionamiento de la cámara PTZ que está enlazada inalámbricamente y manejada mediante el periférico Joystick.

El siguiente paso fue realizar cambios de posición de la cámara esto usando el Joystick. El resultado fue exitoso con un tiempo de respuesta de aproximadamente 1 segundo.

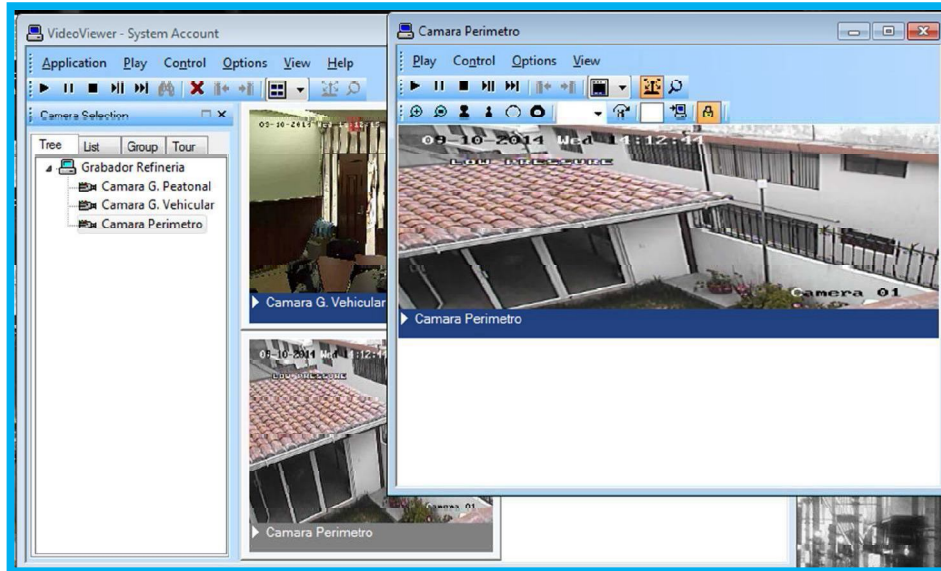


Figura 4. 20 Vista de la cámara PTZ girada hacia la izquierda

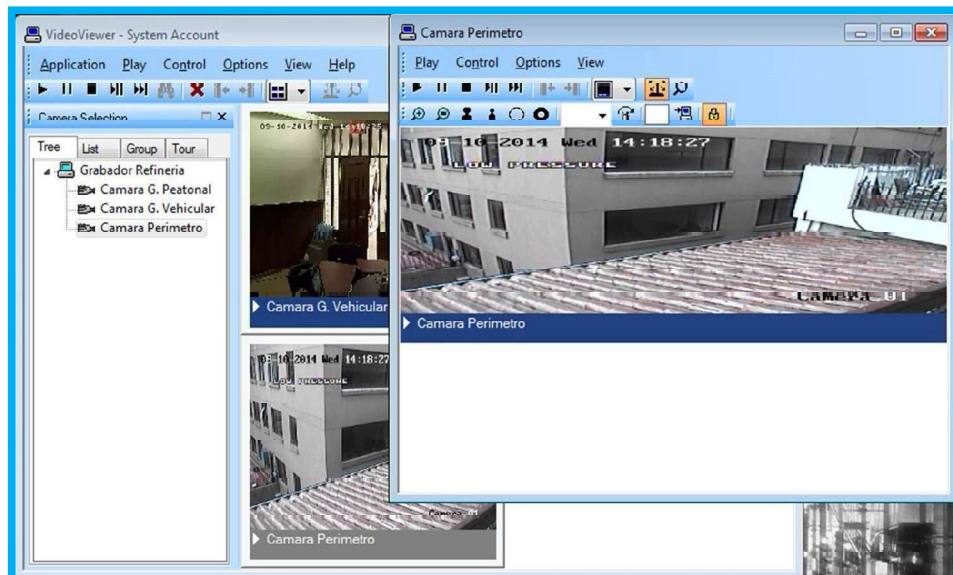


Figura 4. 21 Vista de la cámara PTZ girada hacia la derecha

4.1.2 RESULTADOS

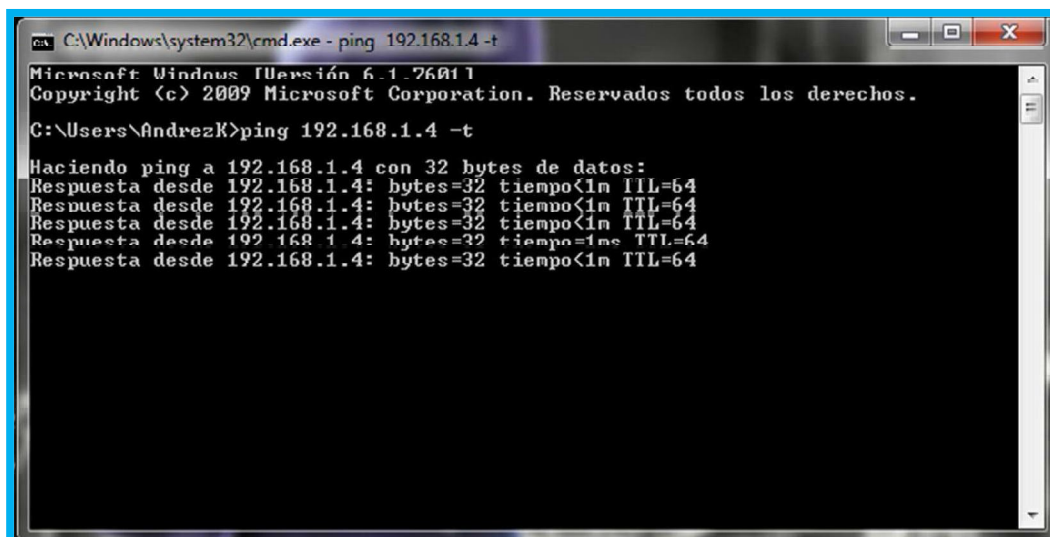
Finalizadas las pruebas de monitoreo y administración de grabaciones se obtuvieron los siguientes resultados notables.

- Cámara de perímetro, garita vehicular y garita peatonal con monitoreo continuo desde un mismo punto de control.
- Interfaz de usuario intuitiva, de fácil acceso y manejo.
- Tiempos de respuesta del sistema menores o iguales a 1 segundo.
- Grabaciones de alta calidad y fácil manejo.
- Ágil acceso a las grabaciones individuales de las diferentes cámaras.
- Monitoreo en vivo de eventos, prácticamente en tiempo real.
- Imagen nítida de ubicaciones enfocadas.

4.2 PRUEBAS Y RESULTADOS DEL SUBSISTEMA DE CONTROL DE ACCESOS

4.2.1 PRUEBAS DE FUNCIONAMIENTO

De manera similar a lo realizado en el subsistema de CCTV se realizó pruebas previas de conexión a la red como se puede ver en el siguiente ejemplo.



```
CA C:\Windows\system32\cmd.exe - ping 192.168.1.4 -t
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\AndrezK>ping 192.168.1.4 -t
Haciendo ping a 192.168.1.4 con 32 bytes de datos:
Respuesta desde 192.168.1.4: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.4: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.4: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.4: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.4: bytes=32 tiempo<1m TTL=64
```

Figura 4. 22 Prueba de conexión a la red de la LNL-2220 de bunker

Una vez que se comprobó que todos los equipos estén en red, se ingresó a la interfaz de usuario denominada “Alarm monitoring” que es la interfaz para el control de accesos que se muestra en la Figura 4.23.

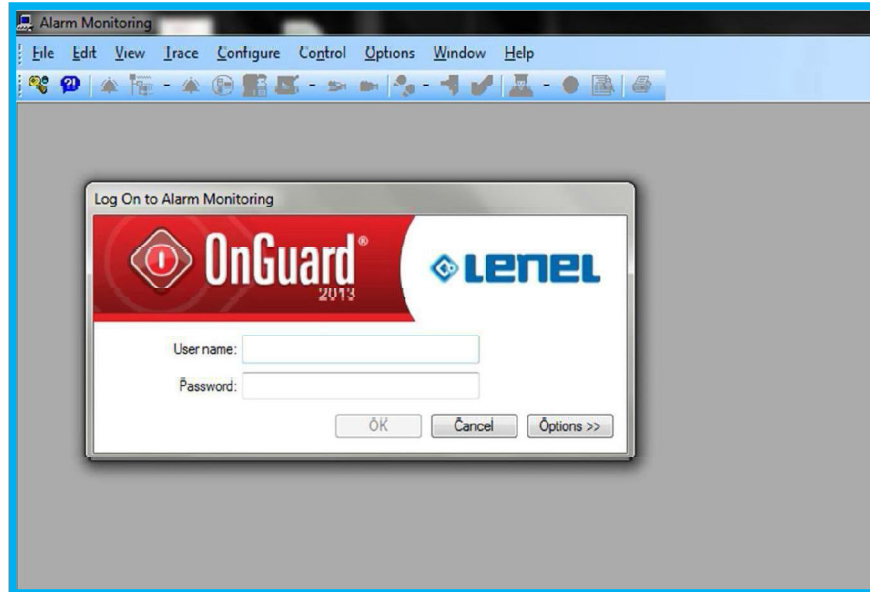


Figura 4. 23 Pantalla de ingreso a ALARM MONITORING

Se ingresó a esta interfaz con el mismo usuario y clave de “System administration”, de manera que dentro se pueden ver en lista los equipos que están enlazados a la red y están enrolados directamente con el servidor, en este caso el grabador virtual y las 3 controladoras que previamente se configuraron.

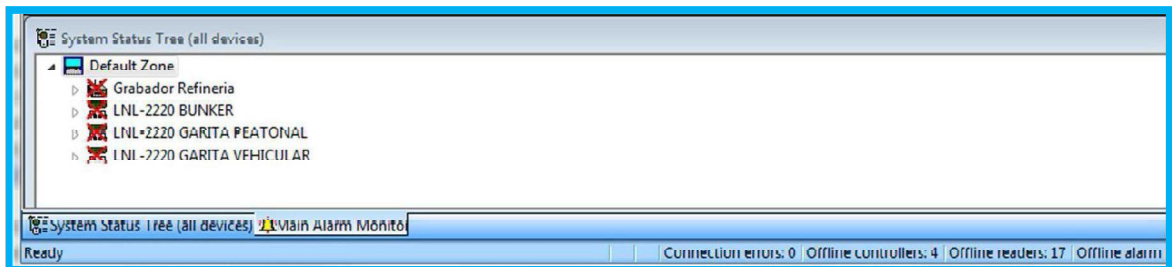


Figura 4. 24 Equipos integrados en el sistema

Se pudo identificar que a pesar de que las pruebas de conectividad realizadas desde el CMD resultaron exitosas, el sistema no reconoce una conexión, por ello todos los equipos listados estaban tachados con una X roja.

El problema radicó en que el software ONGUARD al instante de instalarse añadió su propio servicio de red en el sistema operativo, dicho servicio “(LS Communication)” se necesita iniciar manualmente como se indica en la Figura 4.25.

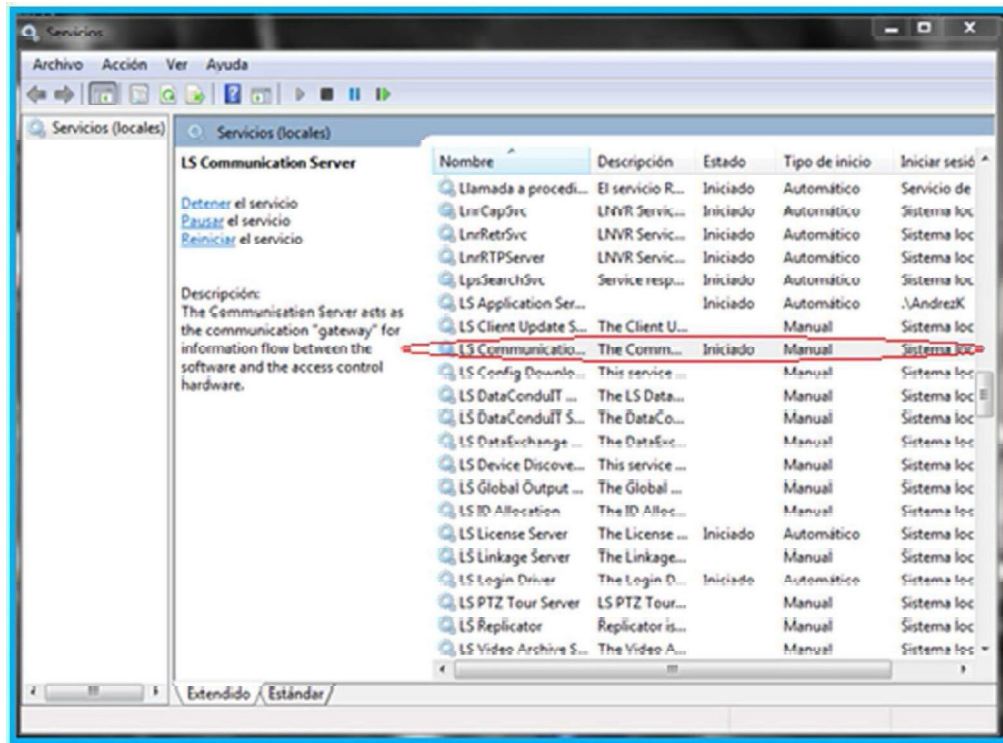


Figura 4. 25 Arranque de servicios de red

Al activar los servicios de red las comunicaciones se establecieron de inmediato de forma que todos los equipos se listaron sin ninguna marca como se ve a continuación.

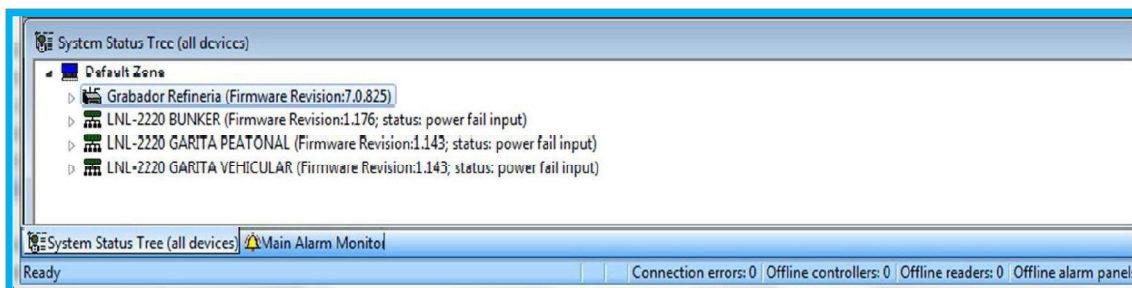


Figura 4. 26 Equipos integrados y conectados al sistema

Al hacer clic en cualquiera de los equipos listados se despliegan sus equipos esclavos como en el siguiente ejemplo de la garita peatonal, en donde se tienen los dos handkeys y las cuatro lectoras de proximidad asociadas a los equipos de salida como la espina de pescado o la puerta motorizada.

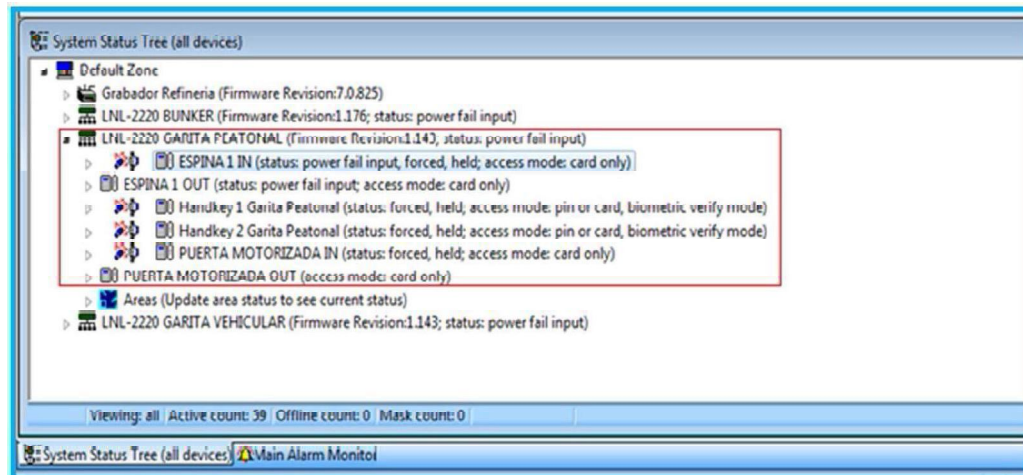


Figura 4. 27 Equipos activos de la controladora LNL-2220 de Garita Peatonal

Como se pudo ver todos los equipos están comunicándose correctamente, caso contrario si alguno de ellos no estuviere con una adecuada función lo que sucede es que el icono que lo representa se vería tachado en rojo.

Teniendo en cuenta las configuraciones de usuarios previas, horarios y niveles de acceso se procedió a realizar las pruebas respectivas de “NIVEL DE ACCESO DENEGADO” cuando un usuario intenta ingresar por un acceso o en un horario no asignado, “INVALID BADGE” cuando el usuario que intenta ingresar posee una tarjeta que no ha sido registrada y “ACCESO CONCEDIDO” cuando el usuario cumplió correctamente con su nivel de acceso y horario.

4.2.1.1 Pruebas de la espina de pescado

Se realizó las pruebas citadas con resultados buenos de funcionamiento como se puede ver en el registro del sistema en la Figura 4.28.

Alarm Description	Time/Date	Controller	Device	Input/Output	Card
Invalid Badge	15:36 10/09/2014	LNL-2220 GARITA PEATONAL	ESPINA 1 OUT	None	Lisa Lake (1)
Invalid Badge	15:36 10/09/2014	LNL-2220 GARITA PEATONAL	ESPINA 1 IN	None	Lisa Lake (1)
Invalid Access Level	15:36 10/09/2014	LNL-2220 GARITA PEATONAL	ESPINA 1 OUT	None	Visitante 1 (5)
Invalid Access Level	15:36 10/09/2014	LNL-2220 GARITA PEATONAL	ESPINA 1 IN	None	Visitante 1 (5)
Granted Access	15:36 10/09/2014	LNL-2220 GARITA PEATONAL	ESPINA 1 OUT	None	Andres Cajo (2)
Granted Access	15:36 10/09/2014	LNL-2220 GARITA PEATONAL	ESPINA 1 IN	None	Andres Cajo (2)

Figura 4. 28 Alarmas del sistema (Prueba Espina De Pescado)

El primer caso se obtuvo al intentar ingresar con una tarjeta no asignada en el sistema, de modo que el sistema mostró la alarma denominada “Invalid Badge” tanto en la lectora de entrada como en la de salida.

En el segundo caso el sistema arrojó la alarma denominada “Invalid Access Level” que corresponde a un usuario que posee una tarjeta con nivel de acceso de visitante y debido a que intentó ingresar fuera del horario de visitas el sistema invalidó el acceso.

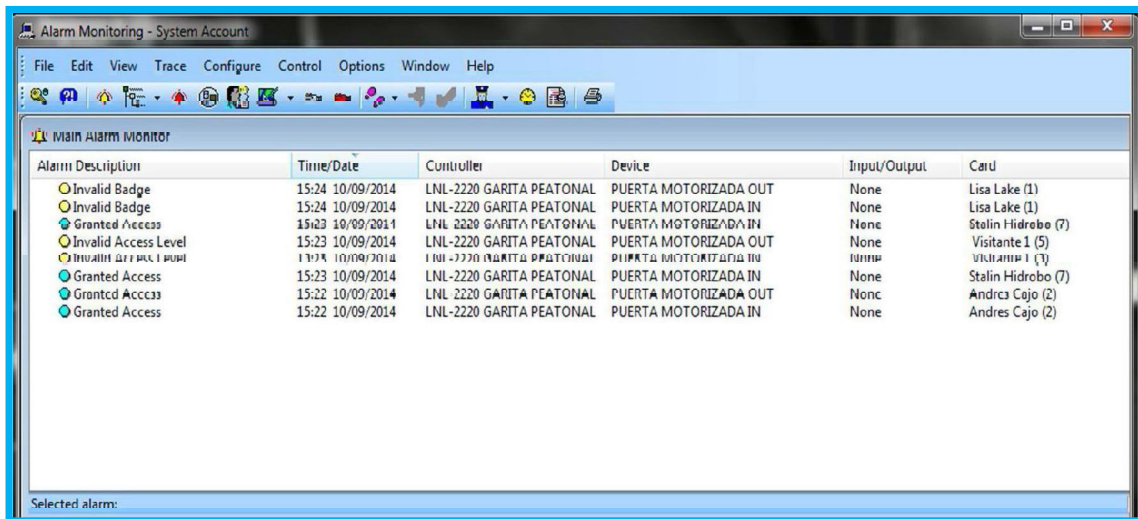
En el tercer caso el sistema arrojó el aviso denominado “Granted Access” en referencia a que el usuario que intentó ingresar obtuvo el acceso ya que cumplió con todos los condicionamientos de nivel de acceso, asignación de tarjeta válido y horario, como efecto se obtuvo que la solenoide de la espina de pescado destrabó el eje y este pudo girar libremente para el paso del usuario.



Figura 4. 29 Eje destrabado luego de que se ha concedido el acceso

4.2.1.2 Pruebas de la puerta motorizada de discapacitados

Se realizaron las 3 pruebas citadas inicialmente con resultados exitosos como se puede ver en la Figura 4.30.



The screenshot shows the 'Alarm Monitoring - System Account' window. The main area is titled 'Main Alarm Monitor' and contains a table with the following columns: Alarm Description, Time/Date, Controller, Device, Input/Output, and Card. The table lists several events, including 'Invalid Badge', 'Granted Access', and 'Invalid Access Level', with corresponding timestamps, controller IDs (LNL-2220 GARITA PEATONAL), device names (PUERTA MOTORIZADA IN/OUT), and card numbers (e.g., Lisa Lake (1), Stalin Hidrobo (7)).

Alarm Description	Time/Date	Controller	Device	Input/Output	Card
Invalid Badge	15:24 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA OUT	None	Lisa Lake (1)
Invalid Badge	15:24 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA IN	None	Lisa Lake (1)
Granted Access	15:23 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA IN	None	Stalin Hidrobo (7)
Invalid Access Level	15:23 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA OUT	None	Visitante 1 (5)
Invalid Access Level	15:23 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA IN	None	Visitante 1 (5)
Granted Access	15:23 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA IN	None	Stalin Hidrobo (7)
Granted Access	15:22 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA OUT	None	Andres Cajo (2)
Granted Access	15:22 10/09/2014	LNL-2220 GARITA PEATONAL	PUERTA MOTORIZADA IN	None	Andres Cajo (2)

Figura 4. 30 Alarmas del sistema (Prueba Puerta De Motorizada)

Se obtuvo los resultados deseados de forma que cuando se dio el acceso concedido por parte del sistema la batiente de la maqueta de puerta de discapacitados se abrió rápidamente sin inconvenientes y después de transcurrido el tiempo previamente programado en el sistema esta se volvió a cerrar automáticamente tanto al ingresar como al salir.

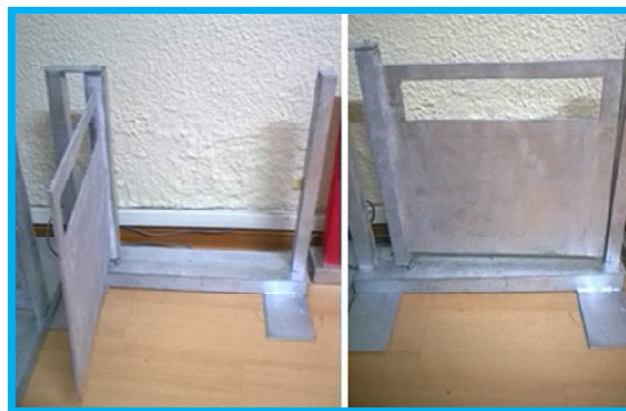
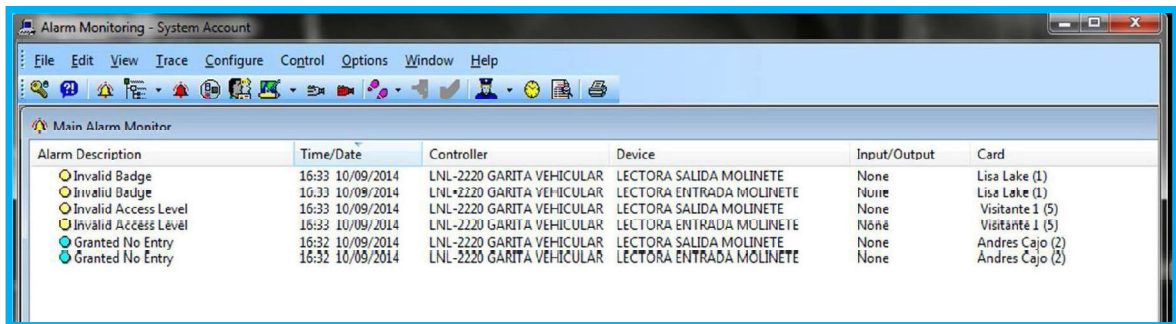


Figura 4. 31 Apertura y cierre de la puerta después de concedido el acceso en el sistema

4.2.1.3 Pruebas del molinete

Se realizaron las pruebas necesarias con las que se obtuvo los siguientes registros de funcionamiento como se puede ver en la Figura 4.32.



Alarm Description	Time/Date	Controller	Device	Input/Output	Card
Invalid Badge	16:33 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA SALIDA MOLINETE	None	Lisa Lake (1)
Invalid Badge	16:33 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA ENTRADA MOLINETE	None	Lisa Lake (1)
Invalid Access Level	16:33 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA SALIDA MOLINETE	None	Visitante 1 (5)
Invalid Access Level	16:33 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA ENTRADA MOLINETE	None	Visitante 1 (5)
Granted No Entry	16:32 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA SALIDA MOLINETE	None	Andres Cajo (2)
Granted No Entry	16:32 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA ENTRADA MOLINETE	None	Andres Cajo (2)

Figura 4. 32 Alarmas del sistema (Prueba Molinete)

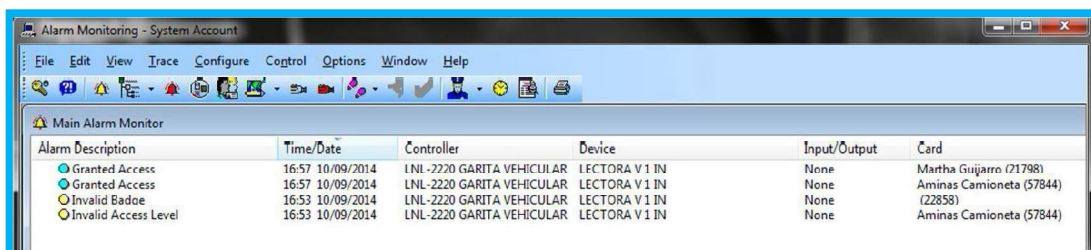
El resultado fue exitoso en los tres diferentes casos de forma que cuando se concedió el acceso la solenoide asociada a esta acción destrabó el eje del molinete para que este pueda ser girado, tanto en sentido de salida o de entrada. Luego de finalizado el tiempo seteado este regresó a su posición normal y se volvió a trabar el eje hasta que un nuevo usuario obtenga el acceso.



Figura 4. 33 Eje destrabado y trabado luego de concedido el acceso

4.2.1.4 Pruebas de barreras vehiculares asociadas a lectoras vehiculares y boosters

Siguiendo la secuencia de pruebas en el caso del funcionamiento de estos equipos se obtuvo el siguiente registro de alarmas en el sistema.



Alarm Description	Time/Date	Controller	Device	Input/Output	Card
Granted Access	16:57 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA V 1 IN	None	Martha Gujjarro (21798)
Granted Access	16:57 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA V 1 IN	None	Aminas Camioneta (57844)
Invalid Badge	16:53 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA V 1 IN	None	(22858)
Invalid Access Level	16:53 10/09/2014	LNL-2220 GARITA VEHICULAR	LECTORA V 1 IN	None	Aminas Camioneta (57844)

Figura 4. 34 Alarmas del sistema (Prueba Barreras Vehiculares)

En el primer caso se registran dos alertas simultaneas a las 16:53 esto se debió al uso en conjunto de la tarjeta Iclass introducida en el booster. La alarma denominada "Invalid Access Level" hace referencia a que el booster correspondiente en este ejemplo a la camioneta que transporta AMINAS, está fuera de horario de acceso, la segunda alarma registrada "Invalid Badge" a la misma hora indica que la tarjeta no ha sido asignada a nadie en el sistema, debido a todos esos incumplimientos de seguridad no se dio el acceso en esta acción.

En el segundo caso se registró de igual forma 2 alarmas simultáneas a las 16:57, la primera es un acceso concedido a la camioneta y la segunda es un acceso concedido a la persona que está manejando, si alguno de los dos requisitos no se cumplen el acceso es denegado.



Figura 4. 35 Barrera vehicular abierta y cerrada luego de concedido el acceso

4.2.1.5 Pruebas de la puerta de bunker

Se realizaron las pruebas que registran los accesos concedidos y no concedidos al tratar de ingresar o salir por la simulación de puerta de bunker.

Alarm Description	Time/Date	Controller	Device	Input/Output	Card
Invalid Badge	17:13 10/09/2014	LNL-2220 BUNKER	PUERTA IN	None	Lisa Lake (1)
Invalid Badge	17:13 10/09/2014	LNL-2220 BUNKER	PUERTA OUT	None	Lisa Lake (1)
Invalid Access Level	17:13 10/09/2014	LNL-2220 BUNKER	PUERTA IN	None	Visitante1 (5)
Invalid Access Level	17:13 10/09/2014	LNL-2220 BUNKER	PUERTA OUT	None	Visitante1 (5)
Granted No Entry	17:13 10/09/2014	LNL-2220 BUNKER	PUERTA IN	None	Andres Cajo (2)
Granted Access	17:13 10/09/2014	LNL-2220 BUNKER	PUERTA OUT	None	Andres Cajo (2)

Figura 4. 36 Alarmas del sistema (Pruebas Puerta Bunker)

Las pruebas fueron exitosas al verificar que si no se cumplen los requisitos de seguridad el sistema no concedió acceso como en los anteriores casos de pruebas. En este caso, el momento que se dio el acceso concedido la cerradura electromagnética se des energizó el tiempo que se programó previamente de forma que la batiente puede ser abierta por el usuario.

Finalizado el tiempo de activación la cerradura electromagnética se energiza automáticamente de forma que la batiente se cierra con la ayuda de un brazo cierra puertas colocado en el marco el que hace que la placa se acerque al imán y nuevamente la puerta quede cerrada fijamente.



Figura 4. 37 Puerta de bunker abierta y cerrada luego de concedido el acceso

4.2.1.6 Pruebas de los equipos biométricos

Se probaron simultáneamente los lectores de geometría de mano de la garita vehicular, peatonal y el biométrico de huellas digitales, de esta forma se obtuvo el siguiente registro de actividad en el sistema.

Alarm Description	Time/Date	Controller	Device	Input/Output	Card
Granted Access	17:49 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Biometric Mismatch	17:49 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Denied, PIN Only Request	17:49 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	(-1)
Granted Access	17:49 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	Andres Cajo (2)
Invalid Facility Code	17:48 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	
Invalid Facility Code	17:48 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	
Invalid Facility Code	17:48 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	
Invalid Facility Code	17:48 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	
Invalid Facility Code	17:48 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	
Invalid Facility Code	17:48 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	
Invalid Facility Code	17:48 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	
Biometric Mismatch	17:48 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Denied, PIN Only Request	17:48 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	(-1)
Granted Access	17:46 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 1 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:46 10/09/2014	LNL-2220 GARITA VEHICULAR	Handkey 1 Garita Vehicular	None	Andres Cajo (2)
Granted Access	17:45 10/09/2014	LNL-2220 GARITA VEHICULAR	Handkey 1 Garita Vehicular	None	Andres Cajo (2)
Granted Access	17:45 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:45 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)

Figura 4. 38 Alertas del sistema (Pruebas De Equipos Biométricos)

En la anterior figura se obtuvo diferentes resultados al realizar pruebas de funcionamiento. La alarma que se denomina “Biometric Mismatch” registrada por el Handkey 2 de la garita peatonal se refiere a que la mano que se colocó para la lectura no está registrada o que simplemente se colocó en una mala posición. El mismo handkey, en otra prueba ejecutada, emitió la alarma denominada “Denied, PIN Only Request”, que se debió a que la clave ingresada previo a la lectura de la geometría de mano es errónea.

Finalmente se tiene el aviso “Granted Access” en el tercer intento cuando se digito correctamente la clave de 4 dígitos y la lectura se realizó correctamente con un usuario enrolado.

Realizada esta última prueba el resultado fue que, a la par de que el sistema concedió el acceso, la acción de control hace que los leds de estado funcionaran como se proyectó, es decir el led rojo se apaga y el verde se enciende como indicador de que el usuario se ha registrado correctamente en el sistema.



Figura 4. 39 Funcionamiento de handkey y leds de estado

El biométrico de la garita vehicular emitió varias alarmas denominadas “Invalid Facility Code”. Esto se debió a que el usuario no colocó bien su dedo registrado o que simplemente era un usuario no autorizado para el registro en este equipo.

Luego se volvió a realizar la prueba usando a un usuario correctamente enrolado con lo que se obtuvo el resultado de “ACCESO CONCEDIDO”. Este, al igual que los anteriores lectores handkey, tiene la función básica de registrar el acceso de los usuarios. Debido a esto no hay equipos periféricos relacionados con estos, con la pequeña diferencia en el caso de los handkey de garita peatonal que hace el cambio de estado de sus leds asociados.

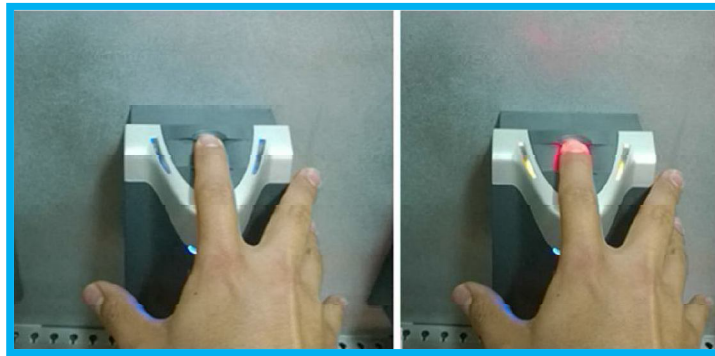


Figura 4. 40 Pruebas de registro de biométrico de huellas digitales

Se realizaron varias pruebas de forma que el sistema registró cada uno de los eventos los cuales al finalizar resultaron exitosos.

Alarm Description	Time/Date	Controller	Device	Input/Output	Card
Granted Access	17:46 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 1 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:46 10/09/2014	LNL-2220 GARITA VEHICULAR	Handkey 1 Garita Vehicular	None	Andres Cajo (2)
Granted Access	17:45 10/09/2014	LNL-2220 GARITA VEHICULAR	Handkey 1 Garita Vehicular	None	Andres Cajo (2)
Granted Access	17:45 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:45 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:44 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:44 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:44 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:44 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:43 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:42 10/09/2014	LNL-2220 GARITA PEATONAL	Handkey 2 Garita Peatonal	None	Andres Cajo (2)
Granted Access	17:42 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	Andres Cajo (2)
Granted Access	17:42 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	Andres Cajo (2)
Granted Access	17:42 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	Andres Cajo (2)
Granted Access	17:42 10/09/2014	LNL-2220 GARITA VEHICULAR	BIOMETRICO	None	Andres Cajo (2)

Figura 4. 41 Pruebas de registro de accesos concedidos de los equipos biométricos

4.2.2 RESULTADOS

Finalizadas las pruebas de control de accesos se obtuvieron los siguientes resultados notables.

- Constante registro de eventos de ingreso y salida de personal.
- Interfaz de usuario intuitiva, de fácil acceso y manejo.
- Respuesta del sistema ante eventos prácticamente inmediata.
- Control sencillo y de fácil reconocimiento.
- Control de asistencia de los diferentes grupos de personal.
- Identificación de la actividad de los usuarios que usan el sistema.
- Control de registro desde un solo punto de monitoreo.
- Control del uso de activos (vehículos asociados a booters).

Se concluye finalmente que al realizar las diferentes pruebas de funcionamiento de los subsistemas a una escala menor, se ha obtenido resultados positivos y satisfactorios en concordancia con los alcances deseados.

El correcto manejo de las diferentes tecnologías involucradas han permitido identificar claramente los alcances que tiene cada uno de los equipos involucrados y el alcance global del proyecto al usarlos en conjunto, sin dejar de tomar en cuenta las peticiones de funcionalidad sugeridas por el cliente.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

Luego de terminado el proyecto, de los resultados de las pruebas realizadas se pueden extraer las siguientes conclusiones:

5.1 CONCLUSIONES

- Los resultados de las pruebas de los dos subsistemas implementados a escala menor fueron exitosas.

Por tal motivo se concluye que la aplicación conjunta y correcta de las tecnologías de seguridad física facilita significativamente el control sobre eventos delictivos que se pudiesen producir.

- Como consecuencia del uso de los subsistemas se ha verificado que se optimiza el control de asistencia.

Por este motivo se concluye que el sistema contribuirá con el cumplimiento de tiempos de trabajo y el incremento de la productividad.

- Usando la tecnología de comunicaciones inalámbricas se tiene facilidad para crear redes de vigilancia a gran escala.

Como consecuencia se concluye que el sistema de CCTV puede crear un ambiente monitoreado remotamente y con gran capacidad de visualización de eventos distantes. De este modo se pueden identificar posibles intrusiones y dar rápidamente aviso al personal de seguridad para controlar dicho evento.

- Al diseñar los diferentes subsistemas se pudo evidenciar que el balance entre el costo y el beneficio que ofrecen al ser implementados es muy bueno

Por lo que se concluye que este nuevo sistema en la refinería mejorará en forma absoluta las condiciones de seguridad actuales en las que la no se tiene un adecuado manejo de activos, personal y eventos de hurto de herramientas y equipos costosos que se usan en las inmediaciones.

- El sistema a implementar como se pudo evidenciar posee herramientas muy poderosas y su manejo desde las diferentes interfaces de monitoreo y registro es relativamente sencillo con lo que el usuario final puede

administrar cómodamente los eventos y tener acceso a los archivos de video sin dejar de tener un monitoreo en vivo.

- Sobre la configuración del software de integración se puede ver que tenemos distintas opciones de funcionamiento de acuerdo a los requerimientos de refinería, así como para tomar acciones inmediatas en el caso de alguna emergencia.

Para esto se dará una capacitación al personal que será el encargado de operar y monitorear los distintos sistemas.

- El historial de acciones que se tiene mediante el software de integración es de gran ayuda.

Gracias a este registro en el caso de presentarse algún problema como de acceso violentado, fuera de horario de acceso permitido, u otro, puede servir para evidenciar hechos ilícitos a más de identificar al personal involucrado, así también facilita cambios en la configuración teniendo en cuenta el estado anterior del respectivo acceso.

5.2 RECOMENDACIONES

- En el subsistema de control de accesos se recomienda un reconocimiento diario de alarmas y registros para tener una correcta administración y la pantalla de registros no se sature de eventos.
- Los equipos de control de accesos deben recibir un mantenimiento periódico de por lo menos 2 veces mensuales de forma que siempre sus superficies se mantengan limpias y así evitar posibles fallos de registro y accesos denegados.
- En el subsistema de CCTV se recomienda una constante administración de forma que por lo menos cada 15 días se respalde la información relevante según el usuario y el resto se descarte, esto con el objetivo de que la administración sea ordenada y se optimice el uso del espacio en el disco de los registros de video.

- Los equipos de enlace inalámbrico necesitan un mantenimiento mínimo pero se recomienda que este debe ser realizado por técnicos especializados.
- Se recomienda como actividad básica realizar un respaldo de la base de datos del sistema por lo menos cada 2 meses, esto con el objetivo de complementar la correcta administración del sistema.
- Se recomienda usar periódicamente la opción de giro y zoom de la cámara PTZ con el objetivo de que el robot no permanezca estático y con el paso del tiempo se trabaje en una sola posición por falta de movimiento.
- En general cuando se desee aplicar sistemas de seguridad física en alguna intermediación, se recomienda el uso conjunto de por lo menos 2 sistemas para tener una redundancia de control en las intermediaciones monitoreadas.
- Para el montaje en campo de los distintos sistemas se recomienda usar los elementos adecuados para el ambiente existente en refinería, ya que las condiciones climáticas pueden causar fallas en el funcionamiento.
- En el sistema de cableado perimetral se debe realizar la calibración de las unidades meteorológicas cuando se requiera, es decir al haber un cambio brusco de clima, así se evitarán falsas alarmas.
- Se recomienda que los equipos de CCTV al estar en contacto directo con el ambiente húmedo y polvoso al notar que la visualización no es la adecuada de inmediato se dé el respectivo mantenimiento para evitar que la imagen se distorsione o se vea opaca por efecto de la suciedad adherida al domo.
- Al realizar las conexiones de tarjetas en los paneles de acceso se recomienda tener un orden al ubicar el cableado en las canaletas para facilitar un adecuado mantenimiento cuando se requiera, de la misma manera de darse el caso, asegurar bien los empalmes del cableado de los equipos que llegan hacia cada panel.
- Se recomienda que se procure que los egresados realicen, en la medida de lo posible, trabajos prácticos y reales tal que les permita adquirir unas experiencias invaluable.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Manual del Handkey, Link:
<http://us.allegion.com/irstdocs/Catalog/106238.pdf>
- [2] Hoja técnica de fuente de poder Lenel, Link:
http://www.lenel.com/assets/library/LNL_TS_AL600ULX-4CB6.pdf
- [3] Hoja técnica de lectora de proximidad, Link:
http://www.keyscan.ca/Languages/Spanish/pdfs/es_iclass_r10.pdf
- [4] Hoja técnica de LNL-2220, Link:
http://cdn.lenel.com/collateral/LNL_TS_2220.pdf
- [5] Hoja técnica de LNL-1320, Link:
http://cdn.lenel.com/collateral/LNL_TS_1320s2.pdf
- [6] Hoja técnica de LNL-500B, Link:
http://www.lenel.com/assets/library/HW_LNL-500B.pdf
- [7] Hoja técnica de lectora vehicular, Link:
<http://www.nedapidentification.com/products/transit-readers/transit-standard.html>
- [8] Hoja técnica del módulo suscriptor Canopy, Link:
http://www.inforede.net/Technical/Layer_1/Wireless_LAN/SM_Manual_E%205200SM.pdf
- [9] Hoja técnica del access point Canopy, Link:
http://www.motorolasolutions.com/web/Business/_Documents/static%20files/Motorola%20Canopy%20Advantage%20Platform%20Access%20Point.pdf?Plibitem=1
- [10] Hoja técnica del torniquete (espina de pescado) doble o simple, Link:
<http://www.fastaccesssecurity.com/proddetail.asp?Prod=BOON-EDAM%2FTOM-THT-100EC>
- [11] Hoja técnica de molinete, Link:
<http://www.boonedam.mx/productos/torniquetes-de-tripode/trilock-60>

- [12] Hoja técnica de puerta motorizada, Link:
<http://www.boonedam.mx/productos/compuertas-de-acceso/thg-42>

- [13] Hoja técnica de sistema de cable perimetral, Link:
<http://www.rbtec.com/Perimeter-intrusion-detection-system>

- [14] Hoja técnica de cámaras fijas, Link:
<http://www.interlogix.com/video/product/truvision-ip-open-standards-dome-cameras/>

- [15] Hoja técnica de cámaras PTZ, Link:
<http://www.pelco.com/sites/global/en/sales-and-support/downloads-and-tools/image-gallery/ptz-cameras.page>

- [16] Hoja técnica de enlaces inalámbricos Ubiquiti, Link:
http://dl.ubnt.com/datasheets/nanostationm/nsm_ds_web.pdf

- [17] Hoja técnica de switch de 8 puertos, Link:
http://www.cisco.com/cdc_content_elements/docs/ie3000datasheet.pdf

- [18] Documentos de entrenamiento en el manejo del software Onguard, Link:
<http://www.lenel.com/onguard.com>

ANEXOS

ANEXO 1

ONGUARD

**MANUAL DE USUARIO
PARA MONITOREO**

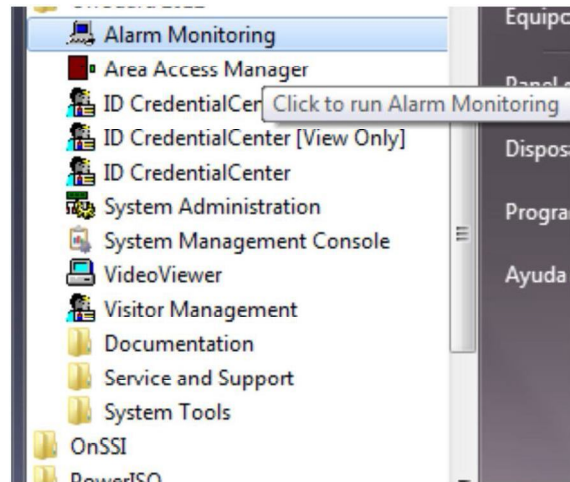
Contenido

APLICACIÓN ALARM MONITORING.....	1
1. INGRESO A LA APLICACIÓN	1
2. ALARMAS	2
Descripción de alarmas.....	2
Reconocimiento de alarmas	3
3. TRACE (RASTREO).....	4
Controler (controlador).....	5
Device (dispositivo)	7
Badge (usuario).....	8
4. ABRIR PUERTAS DESDE EL SISTEMA EN CASO DE EMERGENCIA.....	9
Abrir una puerta determinada	9
Abrir todas las puertas relacionadas con una controladora.....	10
Abrir una o varias puertas permanentemente.....	10
APLICACIÓN VIDEO VIEWER	12
1. INGRESO A LA APLICACIÓN	12
2. MONITOREO EN TIEMPO REAL	13
Descripción de funciones del sistema.....	14
3. NAVEGACION POR EL VIDEO GRABADO.	16
4. CAPTURA DE EVENTOS	17

APLICACIÓN ALARM MONITORING

1. INGRESO A LA APLICACIÓN

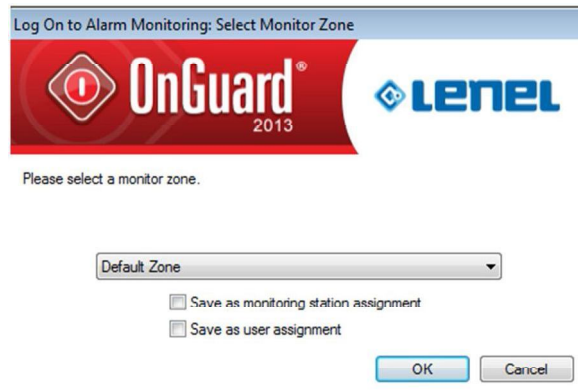
- i. Dar clic en el botón Inicio, luego en la carpeta OnGuard dar clic en *Alarm Monitoring*



- ii. Al ingresar a la aplicación se presenta la ventana para ingresar el nombre de usuario y la clave, una vez se ha digitado los comandos correctamente. Dar clic en "Ok".







- iii. La aplicación indicara una ventana de selección de zona. Se da clic en "OK" en la selección actual y se accede al sistema.



2. ALARMAS

Descripción de alarmas

Las alarmas se diferencian unas a otras de acuerdo a su nivel de importancia, estas cambian de color de acuerdo a si son únicamente informativas del sistema, de la operación normal, o si representan un peligro a la seguridad.

Alarm Priority Level	
	0
	75
	125
	175

ALARMA	DESCRIPCIÓN
Granted-No Entry	Acceso concedido, pero la puerta no fue abierta.
Access Granted	Acceso concedido, ingreso realizado.
Door Forced Open	Puerta Forzada.
Door Held Open	Puerta Mantenido Abierta.
Invalid Badge	Tarjeta Inválida. Esta alarma se da cuando el usuario no tiene acceso a ninguna puerta o cuando no está registrado su número de Badge (número de tarjeta) en el sistema. En el último caso, se deberá enrolar al usuario en el sistema.
Invalid Access Level	Nivel de acceso Inválido. Esta alarma se presenta cuando un usuario no tiene acceso a determinada puerta en ese horario.

Biometric Mismatch	La huella ingresada no corresponde a la huella almacenada.
Alarm Active Alarm Restore (Se presenta cuando la alarma dejó de estar activa)	Indica que se activó una alarma, estas pueden ser de: contactos magnéticos en puertas o barrera perimetral.
Door forced open Cabinet tamper Restored (Se presenta cuando la alarma dejó de estar activa)	Esta alarma se presenta en caso que alguno de los contactos magnéticos de las puertas, hayan sido desconectados físicamente o haya sido cortado el cable.
Open Door Command Issued	Indica que una de las puertas fue abierta desde la aplicación.

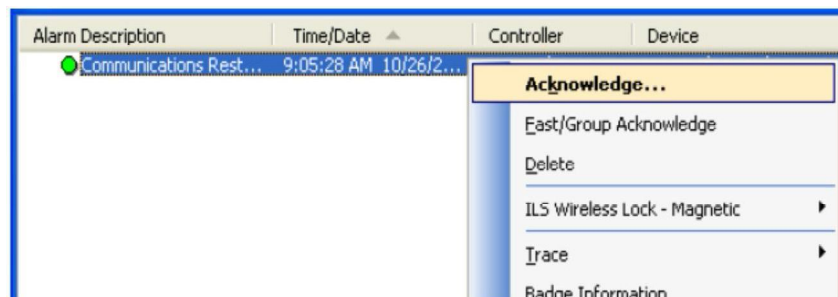
En el sistema se presentarán cualquiera de las alarmas descritas junto con una descripción del dispositivo o cardholder (tarjeta de proximidad) que produjo la alarma, a la hora y fecha en que ocurrió.

Reconocimiento de alarmas

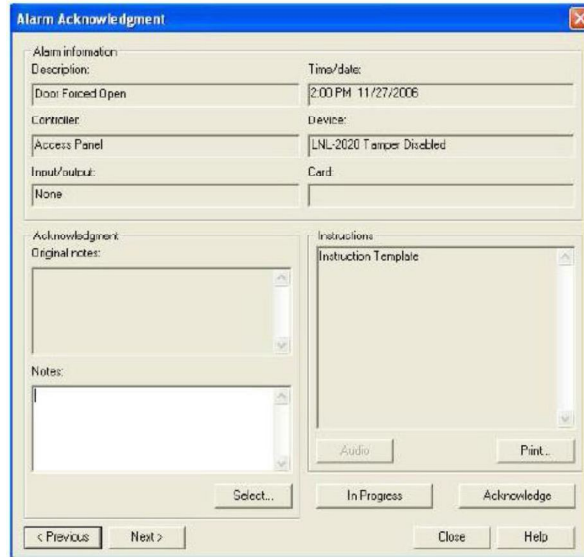
De acuerdo con los permisos otorgados a los operadores, estos tendrán la habilidad para eliminar y reconocer alarmas. Las alarmas que no hayan sido reconocidas no podrán ser eliminadas de la ventana de monitoreo. Se debe reconocer las alarmas para informar al sistema que el operador está al tanto que se presentó la alarma y de ser necesario se tomó acciones para corregir el evento.

Nota: La eliminación de alarmas no implica que estas sean borradas de la base de datos, únicamente dejan de mostrarse en la ventana de monitoreo, pero se puede hacer un rastreo de las mismas en cualquier momento.

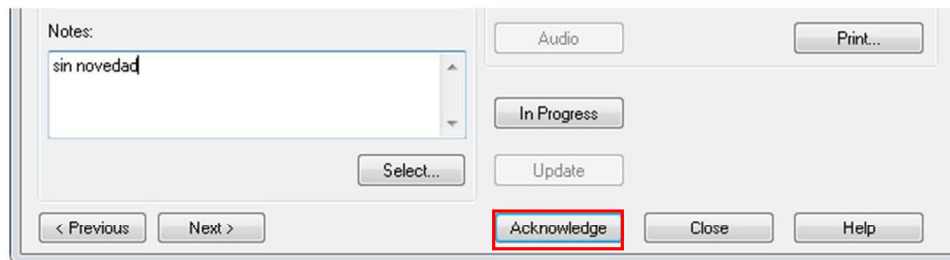
- i. Dar clic derecho sobre la alarma y escoger la opción Acknowledge.



- ii. Se desplegará una ventana en donde en la sección Notes se deben ingresar comentarios especificando el motivo de la alarma y las acciones tomadas para corregir la misma. Si no se ingresa este campo no es posible reconocer la alarma.




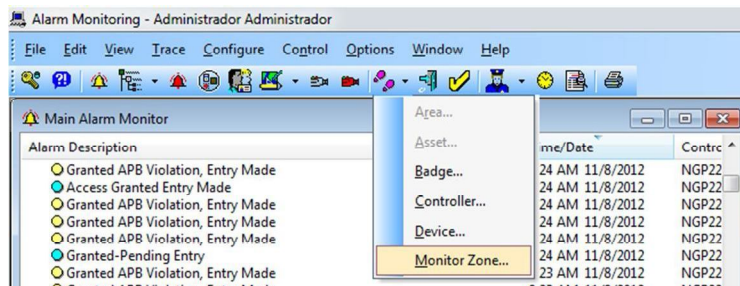
iii. Dar clic en Acknowledge.




Una vez reconocida la alarma esta cambia su color Rojo por Verde

3. TRACE (RASTREO)

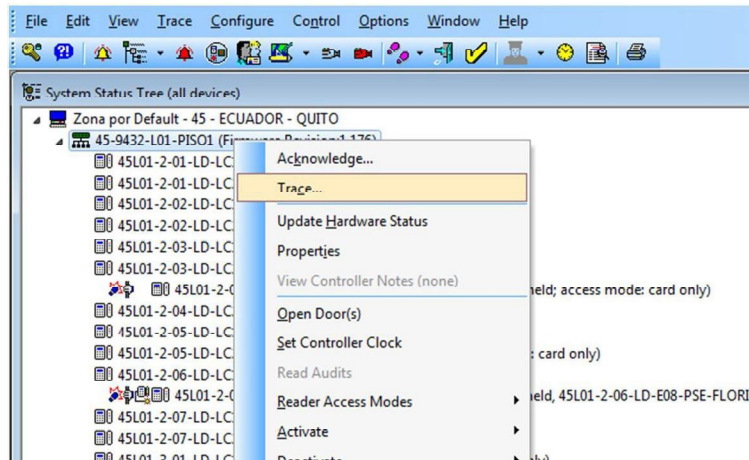
Esta herramienta se utiliza para filtrar la información y ver transacciones pasadas o actuales de un controlador, de un dispositivo o un usuario en específico. Dar clic en  y escoger la opción que se desea rastrear.



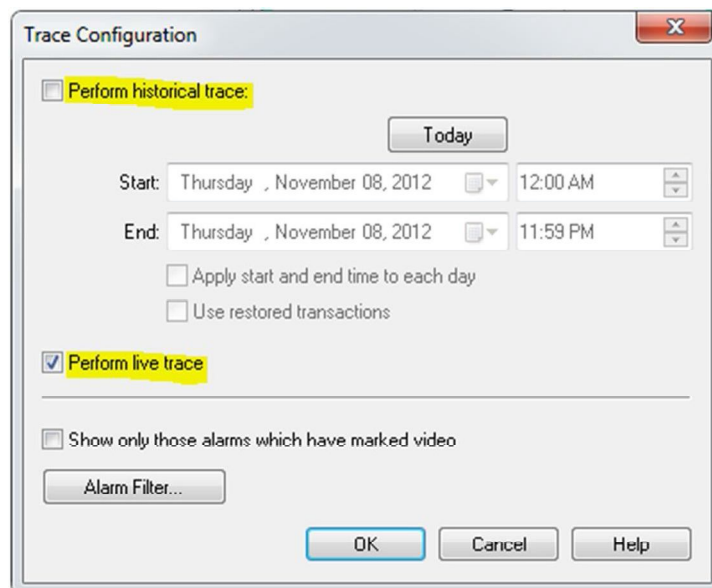
Controler (controlador)

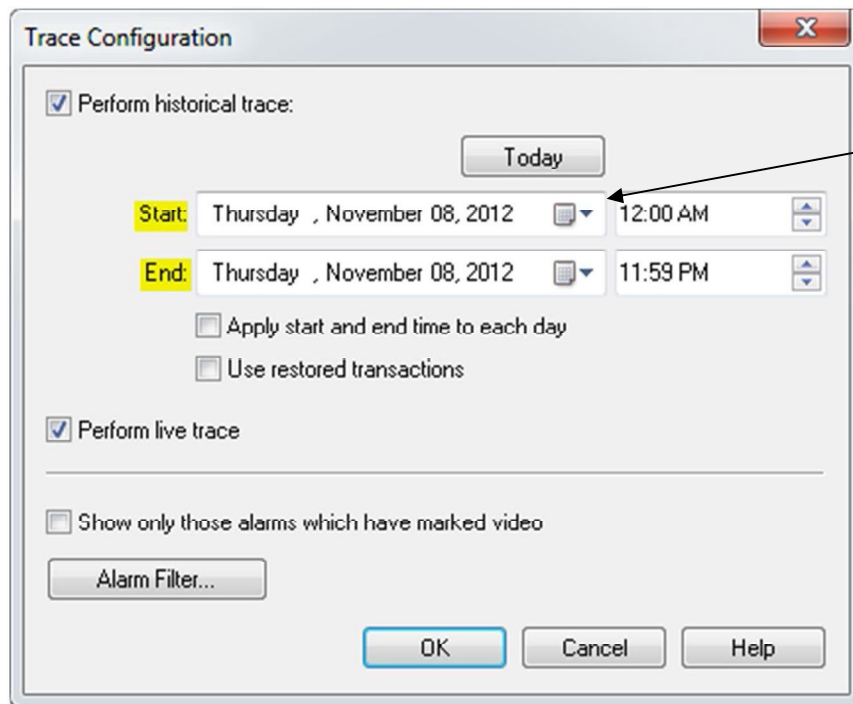
Para monitorear las transacciones únicamente de un controlador determinado. Ir a la ventana System Status . Identificar el controlador.

- i. Dar clic derecho sobre el controlador y escoger la opción "Trace".



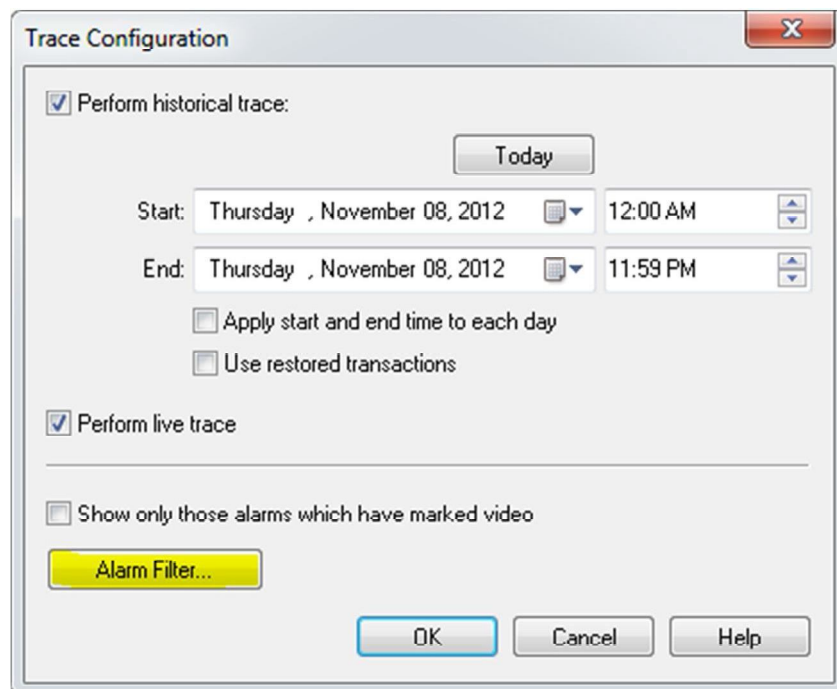
- ii. En la ventana que se despliega seleccionar la opción "Perform historical trace" si se desea visualizar información pasada, para esto se necesita especificar una fecha y hora de inicio y finalización. Si se desea visualizar únicamente transacciones en vivo (realizadas en ese momento), seleccionar la opción "Perform live trace".



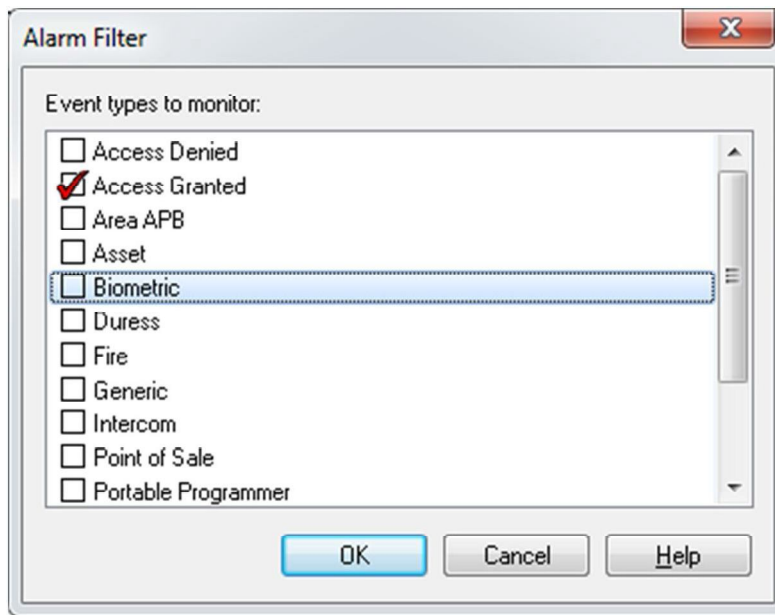


Especificar fechas de inicio y finalización durante la cual se desea ver qué transacciones se han realizado.

- iii. Para especificar qué tipo de alarmas se desean visualizar, dar clic en el botón "Alarm Filter".



- iv. En la ventana que se abre, seleccionar Access Granted si se desea visualizar los accesos concedidos y/o Access Denied si se desea visualizar los accesos denegados.




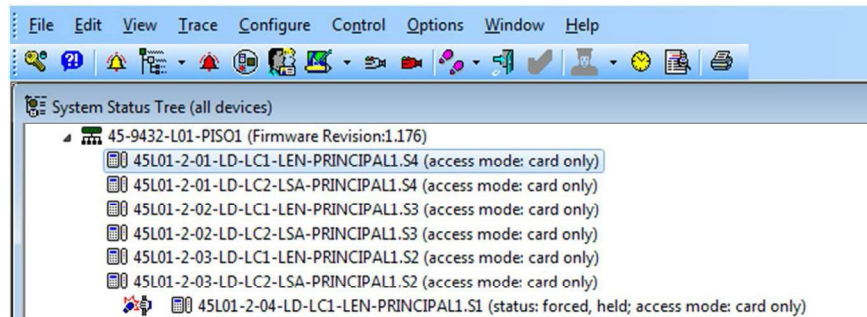
- v. Dar clic en OK. Se abrirá una ventana con la información requerida.

Alarm Description	Time/Date	Controller	Device	Input/Output
Granted Access	15:05 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:53 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:53 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:46 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:44 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:37 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:36 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:24 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:19 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:11 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:09 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	14:01 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	13:54 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	12:54 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	12:31 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None
Granted Access	12:27 07/07/2014	45-9432-L01-PIS...	45L01-2-04-LD-LC1-LEN-PRINCIPAL1...	None

Device (dispositivo)

Permite visualizar únicamente las transacciones que se han realizado y/o se realizan en una lectora de una puerta en específico.


- i. Ir a la ventana System Status . Identificar la lectora a la cual se le quiere hacer un "trace".

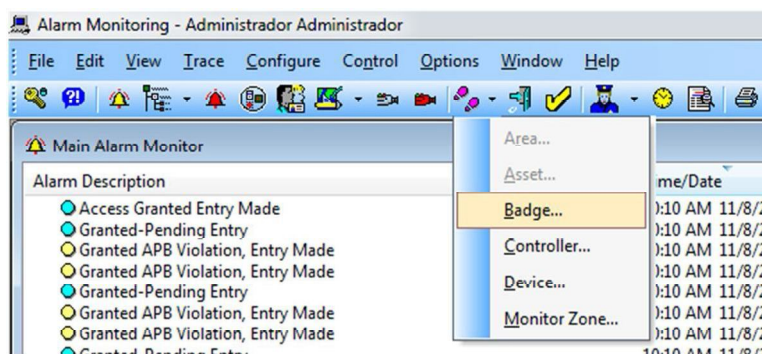


- ii. Dar clic derecho sobre la lectora y escoger la opción "Trace".
- iii. Repetir los pasos del ii al iv del primer item de esta sección para hacer el filtro necesario.
- iv. Al finalizar, se mostrará una ventana en la que se encontrará registrada información pasada si se hizo un "Historical" Trace o si irán registrando las transacciones si se hizo un "Live Trace".

Badge (usuario)

Esta herramienta se utiliza para monitorear únicamente las transacciones de un usuario determinado.

- i. Dar clic en  y seleccionar la opción Badge.




- ii. En la ventana que se despliega, ingresar el número de badge (tarjeta) de la persona sobre la cual se desea obtener información y dar clic en OK.

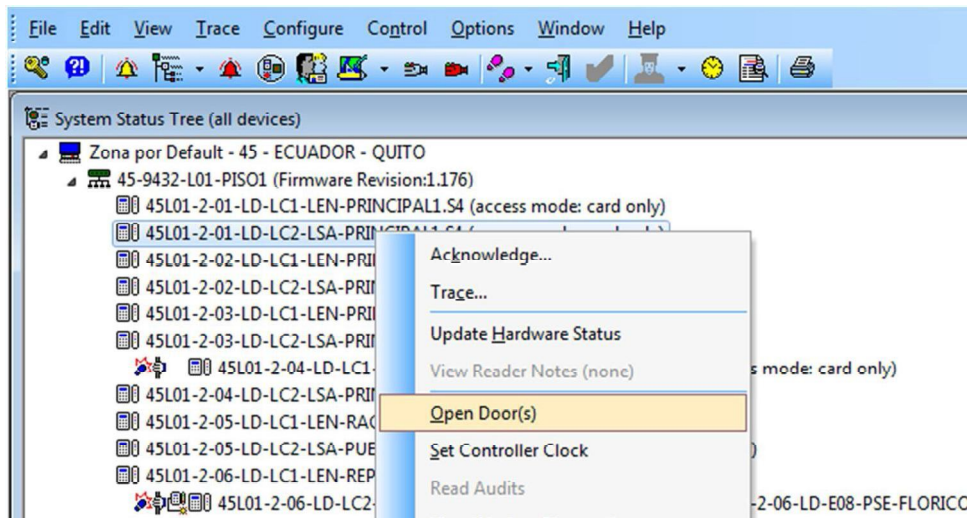


- iii. Repetir los pasos del ii al iv del primer ítem de esta sección para hacer el filtro necesario.
- iv. Se desplegará una ventana con información pasada del usuario especificado si se hizo un "Historical Trace" o se irán registrando sus transacciones si se hizo un "Live Trace."


4. ABRIR PUERTAS DESDE EL SISTEMA EN CASO DE EMERGENCIA

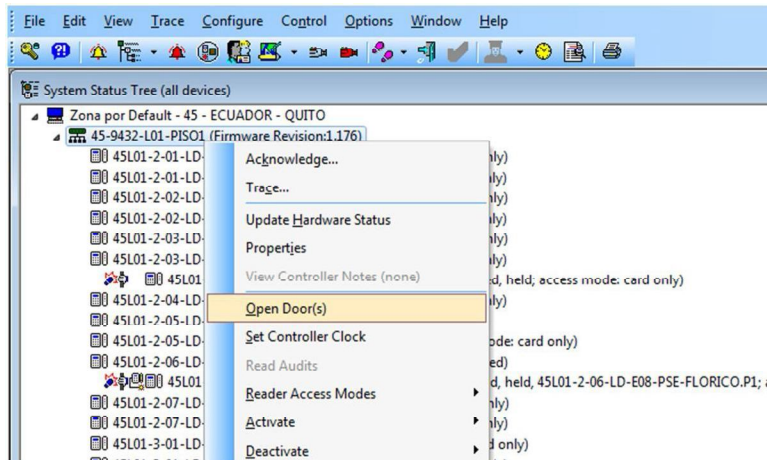
Abrir una puerta determinada

- i. Ir a la ventana System Status . Identificar la lectora de entrada o salida de la puerta que se desea abrir.
- ii. Dar clic derecho y seleccionar la opción "Open Door". La puerta se abrirá y luego de unos segundos se volverá a cerrar.




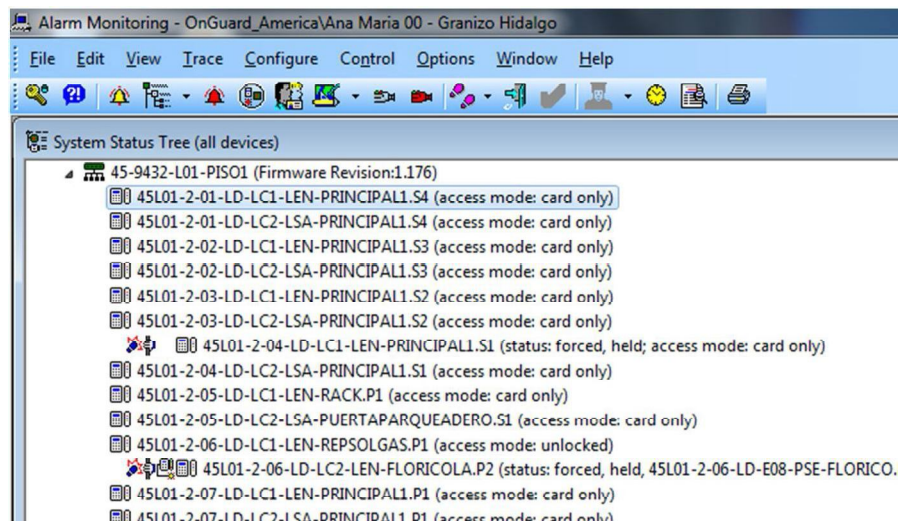
Abrir todas las puertas relacionadas con una controladora

- i. Ir a la ventana System Status . Identificar el controlador al que están conectadas las puertas que se desean abrir.
- ii. Dar clic derecho y seleccionar la opción Open Door. Todas las puertas se abrirán y luego de unos segundos se volverán a cerrar.

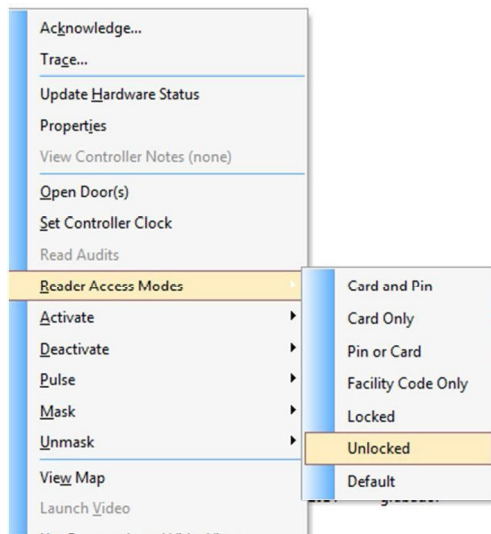


Abrir una o varias puertas permanentemente

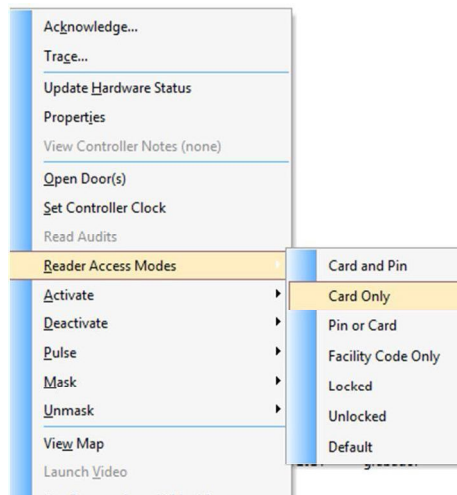
- i. Ir a la ventana System Status . Identificar la lectora de la puerta que se desea abrir permanentemente. En caso que se desee abrir todas las puertas asociadas a un controlador, identificar el controlador al que están conectadas las puertas que se desea abrir permanentemente.



- ii. Dar clic derecho y seleccionar la opción “Reader Access Modes”. Seleccionar la opción “Unlocked”. Todas las puertas permanecerán abiertas.



- iii. Para volver cerrar las puertas y dejarla en el modo normal. Dar clic derecho sobre el mismo controlador, seleccionar la opción “Reader Access Modes” y dar clic en “Card Only”.

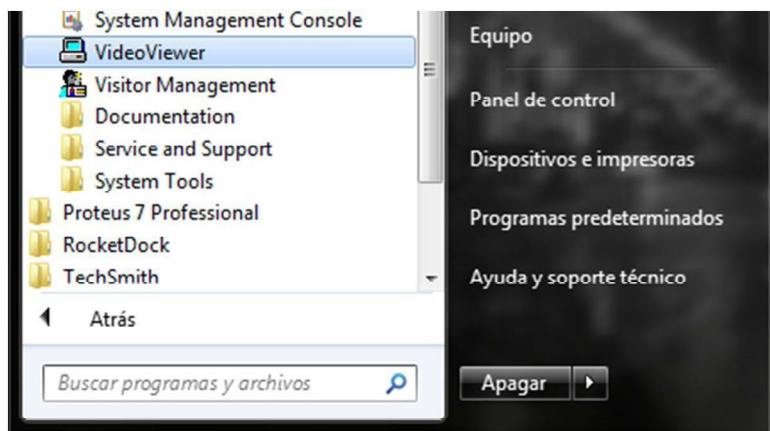


Nota: En caso que se trate de lectores biométricos para volver a su operación normal se debe seleccionar la opción “Pin or Card”.

APLICACIÓN VIDEO VIEWER

1. INGRESO A LA APLICACIÓN

- i. Dar clic en el botón Inicio, luego en la carpeta OnGuard dar clic en *VideoViewer*



- ii. Al ingresar a la aplicación se presenta la ventana para ingresar el nombre de usuario y la clave, una vez se ha digitado los comandos correctamente. Dar click en "Ok".



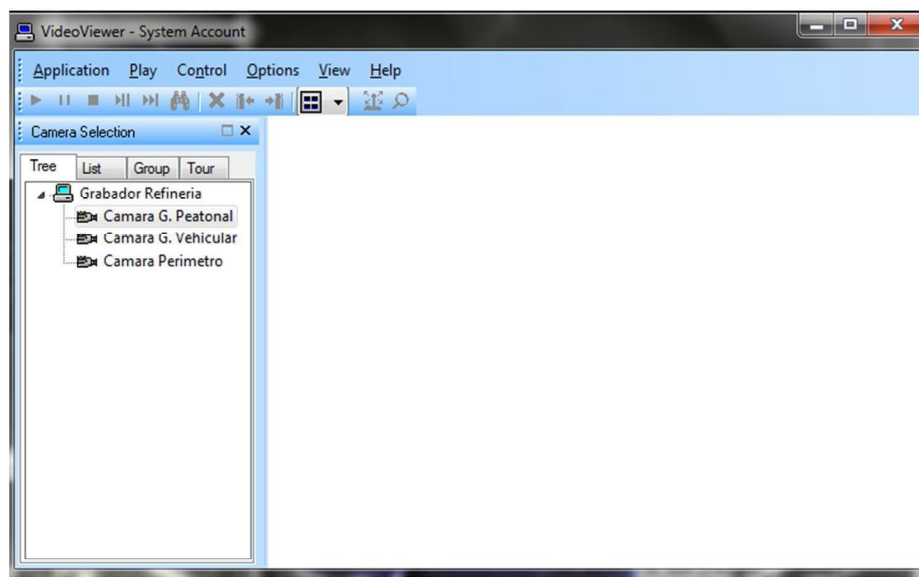
- iii. La aplicación indicará una ventana de selección de zona. Se da clic en "OK" en la selección actual y se accede al sistema.



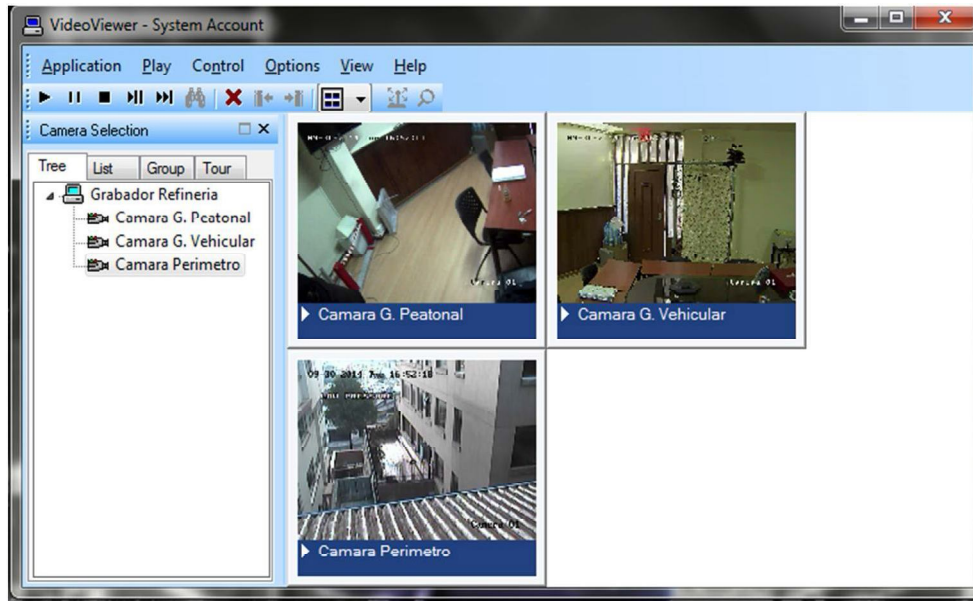
2. MONITOREO EN TIEMPO REAL


Al ingresar se tienen listadas las cámaras disponibles, para acceder a su video se da doble clic sobre la que se desee visualizar, de esta manera se podrán desplegar en el área en blanco los diferentes recuadros con el video digital capturado en vivo, sea de las cámaras fijas como de la PTZ.

La ventana siguiente muestra el ingreso al sistema y las cámaras disponibles.



Al ingresar dando doble clic izquierdo sobre cada una de las cámaras, estas automáticamente se van acomodando en el espacio disponible.



En la anterior ventana usando el icono  “Select template mode” se puede acomodar las ventanas de visualización en la forma matricial que se desee.

Descripción de funciones del sistema

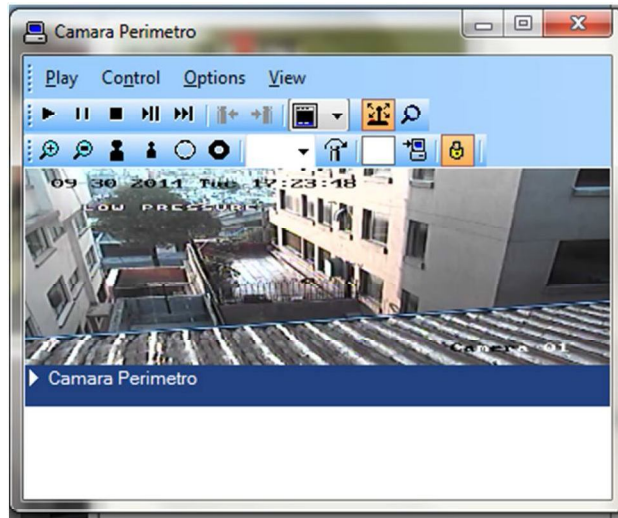
Al dar doble clic sobre la ventana de cualquiera de las cámaras se despliega una nueva ventana. Al realizar esto se adquiere el control exclusivo de la cámara seleccionada.

- i. En el caso de las cámaras fijas la ventana que se despliega es la siguiente.



Al ser cámaras fijas su función de monitoreo es dirigida a un objetivo específico, razón por la que las funciones de movilidad están deshabilitadas.

- ii. En el caso de las cámaras PTZ la ventana que se despliega es la siguiente.



A diferencia de las cámaras fijas, se tienen varios iconos activos para realizar el monitoreo apropiadamente.

Se detallan a continuación los iconos en mención con sus diferentes funciones.

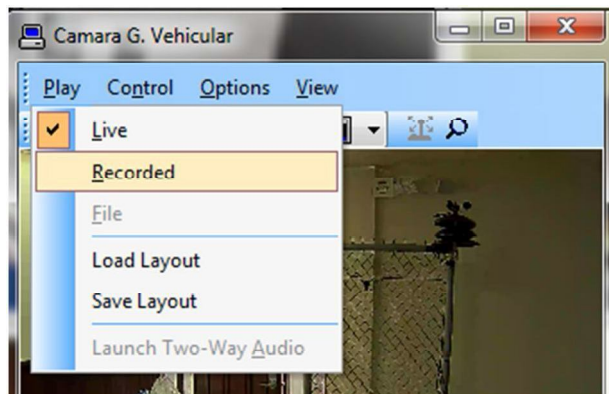
Icono	Descripción
	Activa el control de zoom y movimiento de la PTZ
	Aumenta el zoom de las cámaras PTZ.
	Disminuye el zoom de las cámaras PTZ
	Aumenta el enfoque de las cámaras PTZ
	Disminuye el enfoque de las cámaras PTZ
	Aumenta la apertura del iris de la cámara para captar más luz.
	Disminuye la apertura del iris de la cámara para captar menos luz.

- iii. Se puede usar el mouse disponible para realizar los movimientos de zoom y giro de la cámara. Si se tiene disponible el joystick el giro se realiza moviendo la palanca en la dirección deseada y con la perilla que tiene en la misma palanca se puede

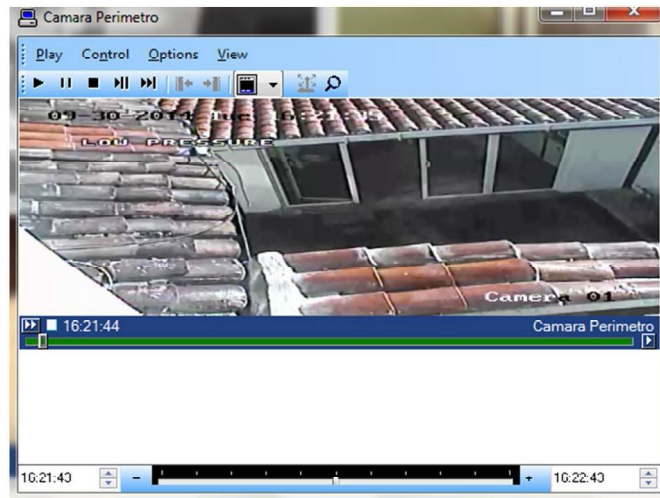
aumentar el zoom girándola hacia la derecha y se disminuye girándola hacia la izquierda.

3. NAVEGACION POR EL VIDEO GRABADO.

En la ventana de la cámara seleccionada, se puede revisar el video grabado por esta, seleccionando la opción “Recorded” al dar clic en la opción “Play”.



- i. Dentro del video grabado se tienen la siguiente ventana.

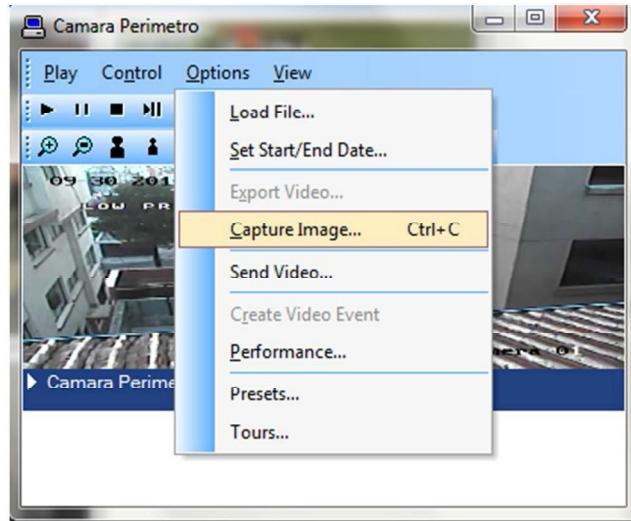


Se tienen dos campos para setear el rango de tiempo que se desea analizar, en la parte superior se tienen los clásicos controles de video para manejar la grabación.

Además se tiene una barra de avance con la que se puede navegar más rápido en la grabación.

4. CAPTURA DE EVENTOS

- i. Si se considera necesario, se puede capturar una imagen como respaldo de algún evento detectado.



Nota: El manual representa los parámetros básicos para una correcta operación de monitoreo.