

**DISEÑO DE UN SISTEMA DE GESTIÓN Y SUPERVISIÓN, DE LOS
LABORATORIOS DEL PROGRAMA DE MECATRÓNICA**

JUAN ALBERTO BERMÚDEZ CADAVID

ANDRÉS FELIPE GALVEZ LEYES

JULIÁN ANTONIO RÍOS GÓMEZ

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

PROGRAMA DE MECATRÓNICA

FACULTAD DE TECNOLOGÍA

PEREIRA

2014

**DISEÑO DE UN SISTEMA DE GESTIÓN Y SUPERVISIÓN, DE LOS
LABORATORIOS DEL PROGRAMA DE MECATRÓNICA**

JUAN ALBERTO BERMÚDEZ CADAVID

ANDRÉS FELIPE GALVEZ LEYES

JULIÁN ANTONIO RÍOS GÓMEZ

Trabajo de grado para optar al título de Tecnólogo en Mecatrónica

Director:

CARLOS ANDRÉS RODRÍGUEZ PÉREZ

Ingeniero en Mecatrónica

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

PROGRAMA DE MECATRÓNICA

FACULTAD DE TECNOLOGÍA

PEREIRA

2014

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

AGRADECIMIENTOS

Le agradecemos en primer lugar a Dios, por habernos acompañado y guiado a lo largo de este proceso de formación, por ser nuestra fortaleza en momentos de debilidad y por brindarnos un camino colmado de éxitos y aprendizajes, que nos ha hecho mejores seres humanos cada día.

A la Universidad Tecnológica de Pereira y al semillero de investigación Mecabot, por brindarnos un lugar de formación en donde siempre hay espacio para las nuevas ideas.

A nuestro director, el ingeniero Carlos Rodríguez Pérez por su acompañamiento a lo largo del desarrollo de este proyecto y sus grandes aportes en pro de la mejora continua.

A nuestra asesora la ingeniera María Elena Leyes, por ser un pilar en nuestras vidas, por su gran apoyo a través de estos años de crecimiento personal e intelectual.

A nuestros padres que día a día han sido nuestro más sincero apoyo en todo momento, por ser ese motor que nos impulsa a seguir a través del buen ejemplo y las buenas costumbres, a ellos mil y mil gracias.

RESUMEN

Durante el desarrollo del sistema de gestión y supervisión de los laboratorios del programa de Mecatrónica, se determinan los diferentes elementos que lo conforman; así mismo, se enuncian los pasos necesarios para acceder y dar un uso eficiente al sistema. El diseño preliminar, se enfoca principalmente en el laboratorio de automatización, ubicado en la sede CDV-San Luis, permitiendo la integración y control centralizado de algunas variables que intervienen en este espacio, dando paso a la expansión, hacia los demás ambientes del programa, dada su flexibilidad. Para el desarrollo del proyecto, se realiza una división en tres niveles:

Nivel de campo: Se controlan dos variables principales, que se encuentran en continuo uso cada día dentro del laboratorio, como lo son: la iluminación y la apertura de puerta. Adicionalmente se plantearon otras variables para el desarrollo del diseño, en pro de la mejora del ambiente de trabajo; estas son: Contactos magnéticos en ventanas y puertas, sensores de movimiento y alarma contra incendios. Así, como los diferentes elementos de hardware necesarios para el funcionamiento de las variables, anteriormente mencionadas.

Nivel de controlador: Se incluyen todos los equipos encargados de la toma de decisiones, a partir de la recolección de datos de los equipos de campo, que para este caso en particular, se seleccionó un PLC marca THINGET de la serie XC3-32r-c, un HMI THINGET 0P 320 A y un ordenador, HP COMPAQ 5700.

Nivel de supervisión y gestión: Se sitúan los sistemas de computación, desde los que se realiza la gestión y almacenamiento de los datos obtenidos en los dos niveles anteriores, así mismo, se hace referencia al uso de una interfaz, que permita al usuario interactuar con el PLC, para cuyo caso, serán comandadas por una HMI, que muestra de forma gráfica el estado de las variables y permite tomar algunas acciones en los actuadores como lo son: la apertura de puerta y activación o desactivación de los sistemas de alarma.

TABLA DE CONTENIDO

INTRODUCCIÓN	12
1. ASPECTOS GENERALES DE LOS PRINCIPALES SISTEMAS DE GESTIÓN Y SUPERVISIÓN.....	14
1.1 PRINCIPALES SISTEMAS QUE PERMITEN IMPLEMENTAR EL DISEÑO PROPUESTO.	14
1.1.1 Sistemas domóticos.	14
1.1.1.1 ¿Qué es domótica?	14
1.1.1.2 Características generales.	14
1.1.1.3 Sistemas domóticos actuales	15
1.1.2 Sistemas Inmóticos.....	17
1.1.2.1 ¿Qué es la inmótica?	17
1.1.2.2 Características generales.....	18
1.1.2.3 Tecnologías Inmóticas actuales	19
1.1.3 Sistemas SCADA.....	21
1.1.3.1 ¿Qué es un sistema SCADA?	21
1.1.3.2 Funciones que un sistema SCADA debe proveer:	21
1.1.3.3 Comunicación y realimentación.....	22
1.1.3.4 Usos Industriales:	22
1.2 CONTROLADORES Y ARQUITECTURAS DE CONTROL.....	22
1.2.1 ¿Qué es un controlador?.....	22
1.2.2 Arquitectura de control.....	22
1.2.2.1 Arquitectura centralizada	23
1.2.2.2 Arquitectura distribuida:	23
1.2.3 Controladores más usados	23
1.2.3.1 PLC.....	23
1.2 SENSORES Y ACTUADORES	24
1.2.3 ¿Qué es un sensor y un actuador?	24
1.3.3.1 Sensor	24
1.2.3.2 Actuador	25
1.2.4 Sensores requeridos para el sistema de gestión y supervisión	

1.3.4.1	Detector de movimiento	25
1.3.4.2	Sensor de luz.....	25
1.3.4.3	Alarma contra incendios	26
1.3.4.4	Contacto magnético.....	26
1.3.4.5	Cámara IP	27
1.3.5	Actuadores requeridos para el sistema de gestión y supervisión	28
1.3.5.1	Cerradura eléctrica	28
1.3.5.2	Sirena	29
2.	CRITERIOS DE SELECCIÓN DE LOS COMPONENTES DEL SISTEMA DE GESTIÓN Y SUPERVISIÓN	30
2.1	SELECCIÓN DEL SISTEMA DE GESTIÓN Y SUPERVISIÓN	30
2.2	CRITERIOS DE SELECCIÓN PARA UN SOFTWARE SCADA	31
2.2.1	InduSoft Web Studio	32
2.2.2	Alcances InduSoft	33
2.2.3	Protocolos de InduSoft	34
2.3	SELECCIÓN DEL SISTEMA DE CONTROL	36
2.3.1	Criterios de selección para el sistema de control	36
2.3.1.1	Criterios de selección del dispositivo que permite la adquisición y control de los datos y/o variables:.....	36
2.3.2	Selección del HMI.....	38
2.3.4	Criterios de selección del computador	38
3.	ÁREAS DE IMPACTO CONTEMPLADAS EN EL SISTEMA DE GESTIÓN Y SUPERVISIÓN	40
3.1	ESTADO ACTUAL	40
3.1.1	Sistema de luces	41
3.1.2	Sistema de acceso	41
3.1.3	Sistema de gestión.....	42
3.2	PROPUESTA DE DISEÑO.....	43
3.2.1	Sistema de luces propuesto	44
3.2.2	Sistema de accesos propuesto	46
3.2.3	Sistema de seguridad propuesto	47
3.3	SENSORES Y ACTUADORES PROPUESTOS	49

3.3.1	Sensor de luminosidad: Idr-720	49
3.3.1.1	Descripción	50
3.3.1.2	Conexiones.....	50
3.3.1.4	Curva característica, sensor de luminosidad	50
3.3.2	Detector de humo autónomo	52
3.3.3	Detector de movimiento por infrarrojos pasivos Blue Line GEN2 53	
3.3.1	Especificaciones técnicas	54
3.3.4	Contacto Magnético fijación adhesivo GL-38B	55
3.3.4.1	Características gl-38b	55
3.3.5	Cámara IP.....	56
3.3.5.1	Características generales	57
3.3.6	Cerradura eléctrica LUBER	57
3.3.6.1	Características generales	58
3.3.7	Sirena multitonal WM 4 tonos 12-24VDC.....	58
3.3.7.1	Características generales	59
3.3.8	Relé PCB G5V-1	59
3.4	PROPUESTA PROGRAMACIÓN DE PLC	60
3.4.1	Programación sistema de luces.....	61
3.4.1.1	Modulo analogico	61
3.4.1.2	Entradas y salidas, sistema de luces	62
3.4.1.3	Descripción de programación para el sistema de luces	63
3.4.2	Descripción de programación para el sistema de acceso.....	64
3.4.2.1	Tabla de entradas y salidas	64
3.4.3	Descripción de programación para el sistema de seguridad..	65
3.4.3.1	Tabla de entradas y salidas	66
3.5	PROPUESTA PROGRAMACIÓN HMI.....	68
3.5.1	Sistema de iluminación desde HMI.....	71
3.5.2	Sistema de accesos desde HMI	73
3.5.3	Panel de alarma desde HMI	75
3.6	PROPUESTA INTERFAZ SCADA	77
3.6.1	Entorno sistema de luces	80

3.6.2 Entorno sistema de acceso	82
3.6.3 Entorno sistema de seguridad	83
3.6.4 Entorno del sistema de gestión	84
3.6.4.1 Generación de usuarios.....	85
3.6.4.2 Prestamos instrumentos del laboratorio.....	86
3.7 MANEJO WEB	88
CONCLUSIONES	95
BIBLIOGRAFIA	97
ANEXOS.....	103
Anexo A [79].....	103
Anexo B [80].....	118
Anexo C [81].....	123
Anexo D	132
Anexo E [82].....	137

LISTA DE FIGURAS

Figura 1: Edificio torre central Pereira, Risaralda	13
Figura 2: Entorno domótico [13].....	14
Figura 3: Principales componentes de un entorno Inmótico	17
Figura 4: Funciones de la tecnología KNX.....	20
Figura 5: Representación gráfica de conexión Wireless, extensión ENOCEAN	20
Figura 6: Ejemplo sistema SCADA	21
Figura 7 : Arquitectura centralizada y distribuida.	23
Figura 8 : PLC Allen Bradley SLC 500.....	24
Figura 9: Detector de movimiento.....	25
Figura 10: Sensor de luminosidad	26
Figura 11: Alarma contra incendios	26
Figura 12: Contactos magnéticos	27
Figura 13: Cámara IP.....	28
Figura 14 : Cerradura eléctrica Luber 2020	28
Figura 15: Sirena	29
Figura 16: Simulación de tanques InduSoft Web Studio.....	32
Figura 17: Representación gráfica de la conexión OPC	35
Figura 18: PLC THINGET	37
Figura 19: HMI THINGET 0P 320-A.....	38
Figura 20: Ordenador HP COMPAQ 5700.....	39
Figura 21: Distribución por módulos, del laboratorio de automatización, situado en el CDV	40
Figura 22: Distribución actual del el sistema de iluminación en el laboratorio de automatización.....	41
Figura 23: Puerta principal laboratorio de automatización CDV.....	42
Figura 24: Sistema de gestión actual.....	43
Figura 25: Propuesta de diseño del laboratorio de automatización, situado en el CDV	44
Figura 26: Propuesta de diseño, control de luces	45
Figura 27: Representación esquema de conexión del sistema de iluminación .	46
Figura 28: Diseño de puerta principal con cerradura eléctrica.....	47
Figura 29: Representación esquema de conexión cerradura eléctrica	47
Figura 30: Distribución propuesta para el sistema de gestión y supervisión.....	48
Figura 31: Representación esquema de conexión del sistema de seguridad propuesto.....	49
Figura 32: Sensor de luminosidad LDR-720	49
Figura 33: Ficha técnica sensor de luminosidad.....	51
Figura 34: Sensor de movimiento BLUE LINE GEN2	53
Figura 35: Contacto magnético GL-38B.....	55

Figura 36: Cama IP Dvr, H.264.....	56
Figura 37: Cerradura eléctrica LUBER	58
Figura 38: Sirena multitonal WM 4 tonos	59
Figura 39: Relé PCB G5V-1.....	60
Figura 40: propuesta conexión sensores y actuadores al PLC.....	61
Figura 41: Modulo analogico THINGUET XC3-32r-c	62
Figura 42: Esquema de programación sistema de iluminación.....	64
Figura 43: Esquema de programación sistema de acceso	65
Figura 44: Esquema de programación sistema de seguridad	68
Figura 45: Pines DB9.....	68
Figura 46: Conexión HMI – Ordenador	69
Figura 47: Venta inicial del HMI, solicitud de contraseña.....	70
Figura 48: Ventana del menú principal del HMI	70
Figura 49: Ventana del panel de alarma en HMI con énfasis en la designación de memorias	71
Figura 50: Menú principal del HMI desde software OP Series Edit Tool con énfasis en la iluminación.	72
Figura 51: Menú de control del sistema de iluminación en OP Series Edit Tool	73
Figura 52: Menú principal del HMI con énfasis en el control de accesos.....	74
Figura 53: Ventana de la puerta principal en el HMI	74
Figura 54: Menú principal del HMI con énfasis en el panel de alarma general.	75
Figura 55: Ventana del panel de alarma general	76
Figura 56: Ventana de estado de contactos magnéticos de puerta y ventana..	76
Figura 57: Ventana de estado la alarma general y señal de la sirena	77
Figura 58: Representación gráfica esquema de conexión InduSoft Web Studio con el PLC	78
Figura 59: Hoja del Driver MODBUS en InduSoft Web Studio.....	78
Figura 60: Vista general de la interfaz diseñada para el sistema de gestión y supervisión.....	80
Figura 61: Botón asignado al TAG M0 desde el software.....	80
Figura 62: Control de luces desde el RUN-TIME de InduSoft Web Studio	81
Figura 63: Pantalla de control y acceso con énfasis en el sistema de acceso..	83
Figura 64: Ventana de control y acceso con énfasis en el sistema de seguridad	84
Figura 65: Ventana de supervisión enlazada a la cámara IP	84
Figura 66: Ventana de generación de usuarios desde la interfaz SCADA.....	86
Figura 67: Ventana del sistema de préstamos en InduSoft Web Studio	87
Figura 68: Base de almacenamiento Access de los datos ingresado en el sistema de prestamos.....	87
Figura 69: Pantalla de selección de implementos a utilizar	88
Figura 70: Representación de la conexión Web de InduSoft Web Studio.....	89

Figura 71: Configuración del servidor de Microsoft IIS	90
Figura 72: Interfaz SCADA diseñada desde Internet Explorer	90

LISTA DE TABLAS

Tabla 1: Principales sistemas comerciales de control domótico.....	16
Tabla 2: Principales tecnologías Inmóticas.....	19
Tabla 3: Principales software SCADA.....	36
Tabla 5: Ficha técnica sensor de movimiento [64].....	54
Tabla 6: Ficha técnica relé G5V-1 [76].....	59
Tabla 7: Entradas y salidas del PLC thinget sistema de luces.....	62
Tabla 8: Entradas y salidas del PLC thinget sistema de acceso.....	64
Tabla 9: Entradas y salidas del PLC thinget sistema de seguridad.....	66
Tabla 10: Tabla de costos en términos de horas trabajadas.....	91
Tabla 11: Tabla de costos de los diferentes elementos de campo requerido.....	92
Tabla 12: Tabla de costos herramientas requeridas.....	93
Tabla 13: Tabla de costos software SCADA y propuesta de diseño.....	93

LISTA DE CUADROS

Cuadro 1: Ficha técnica detector de humo autónomo [64].....	52
--	----

INTRODUCCIÓN

La aparición de los primeros sistemas de administración y supervisión va de la mano con la incursión de un término poco conocido, pero que ha ganado un gran peso en la actualidad, se trata de los sistemas Inmóticos (edificios inteligentes), ya que estos fueron los primeros sistemas que permitían tener el control de diversas variables en una construcción de tipo comercial. Es solo a finales de los años 70, cuando las empresas empiezan a desarrollar algunos productos pensados para las edificaciones, esto debido al progreso de tres grandes sectores de la tecnología como son: las telecomunicaciones, la electrónica y la informática.

La demanda de edificios inteligentes, ha crecido en Colombia, por el auge de la construcción y porque las grandes empresas prefieren contar en sus edificios con servicios y tecnología, tales como: automatización, redes de comunicaciones, seguridad, confort climático etc. En la actualidad el metro cuadrado de un edificio inteligente es más costoso que el de los edificios tradicionales, por lo cual, aumenta el interés de las constructoras por promocionar una inversión de estas características.

Desde hace pocos años relativamente, se empieza a hablar de edificios inteligentes en el país. El primero, fue en 1996 con el edificio Empresas Públicas de Medellín-“EPM”, y poco a poco, los constructores han ido adicionando las diferentes opciones de control y seguridad, pero en forma independiente y separada. El aporte de software centralizado, ha permitido acelerar esa concentración y control, generando la inteligencia de los edificios. Se está entonces, en los inicios de un interés incrementado en la automatización de edificios, pero falta mucho todavía para que en realidad se esté presenciando un “boom”.

Ya existen algunos ejemplos de construcciones inteligentes en Colombia como Santafé, el centro comercial más grande del país y uno de los más grandes en Suramérica, inaugurado el 13 de mayo del 2006, ubicado en la capital del país; el Centro Comercial Plaza Imperial, inaugurado en el segundo semestre del año 2005, el Centro Comercial Palatino, inaugurado el 4 de mayo de 2007 y Edificio Torres Unidas, inaugurado en 2006, entre otras edificaciones [6].

En la región se encuentran algunos ejemplos, como torre central en Pereira (véase figura 1), Risaralda 24 de abril de 2007 [8]. Edificio inteligente, Telefónica de Pereira octubre de 2007 [9].

Figura 1: Edificio torre central Pereira, Risaralda



Fuente: Torre central. [En línea]. [Citado el 6 de abril del 2014]. Disponible en<
<http://www.skyscrapercity.com/showthread.php?t=444138>>

El presente proyecto nace debido a la ausencia de un sistema de gestión y control de acceso a los laboratorios; además, de la necesidad de un sistema de supervisión computarizado, que permita ejercer control y monitoreo de las instalaciones. Cabe resaltar, que la propuesta de diseño, se basa en un sistema Inmótico, sin embargo no comprende a cabalidad todos los elementos que intervienen en un desarrollo de este tipo, pero da la posibilidad de expandir el diseño, en aras de alcanzar los parámetros comprendidos para un entorno de estas características.

Una vez identificado el estado actual de los laboratorios, el paso siguiente es establecer un desarrollo por fases: en primera instancia, se seleccionan todos los componentes de hardware y software necesarios, todos estos basados en los criterios pertinentes y acordes al espacio en donde serán implementados; en segundo lugar se incluyen todos los equipos encargados de la toma de decisiones y recolección de datos; y por último, se sitúan los sistemas de computación, encargados de brindar un entorno de desarrollo.

1. ASPECTOS GENERALES DE LOS PRINCIPALES SISTEMAS DE GESTIÓN Y SUPERVISIÓN

1.1 PRINCIPALES SISTEMAS QUE PERMITEN IMPLEMENTAR EL DISEÑO PROPUESTO.

1.1.1 Sistemas domóticos.

1.1.1.1 ¿Qué es domótica?

El término domótica procede de la combinación de las palabras *domus* (significa casa en el latín) e informática (DRAE). En términos generales se comprende por domótica a la agrupación de sistemas, que permiten y proporcionan las características necesarias para automatizar una vivienda, aportando servicios de: Gestión Energética, Seguridad, Bienestar y Comunicación. Por otra parte, pueden integrarse por medio de redes interiores como de redes exteriores de comunicación, cableadas o inalámbricas, desde el interior como fuera del hogar. En otras palabras se podría definir como la integración de la tecnología en el diseño inteligente de un hogar. En la figura 2 se observa los principales componentes que conforman un ambiente domótico.

Figura 2: Entorno domótico [13]



Fuente: Ventajas de la domótica [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://domoticasape.blogspot.com/2013/10/ventajas-de-la-domotica.html> >

1.1.1.2 Características generales.

Los servicios que brinda la domótica se pueden asociar según cuatro aspectos principales, los cuales son conocidos como los cuatro pilares:

❖ **Ahorro energético:**

- Climatización: programación y zonificación.
- Gestión eléctrica.
- Racionalización de cargas eléctricas: desconexión de equipos de uso no prioritario en función del consumo eléctrico en un momento dado. Reduce la potencia contratada.
- Gestión de tarifas.
- Uso de energías renovables.

❖ **Nivel de confort:**

- Iluminación.
- Apagado general de todas las luces de la vivienda.
- Automatización del apagado/ encendido en cada punto de luz.
- Regulación de la iluminación según el nivel de luminosidad ambiente.
- Automatización de todos los distintos sistemas/ instalaciones / equipos dotándolos de control eficiente y fácil control vía Internet.

❖ **Seguridad y protección patrimonial:**

- Simulación de presencia.
- Detección de conatos de incendio, fugas de gas, escapes de agua.
- Alerta médica. Teleasistencia.
- Cerrado de persianas puntual y seguro.

❖ **Comunicaciones:**

- Ubicuidad en el control tanto externo como interno, control remoto desde Internet, PC, mandos inalámbricos (p.ej. PDA con WiFi), aparellaje eléctrico.
- Transmisión de alarmas.
- Intercomunicaciones.[12]

1.1.1.3 Sistemas domóticos actuales

Existe una gran variedad de sistemas domóticos en el mercado, La mayor parte de ellos destinados a grandes superficies, en sistemas más pequeños para aplicaciones domésticas.

A continuación, en la tabla 1 se muestran los principales sistemas de control domóticos y sus características.

Tabla 1: Principales sistemas comerciales de control domótico

Nombre	Fabricante	Sistema	Protocolo de comunicaciones	Modo de transmisión	Topología
Altolá	Beghelli, S.R.L.	Descentralizado	Protocolo propio	Red eléctrica	Libre
Amigo	Eunea Merlín Gerin	Descentralizado	Batibus	Cableado ded.	Libre
Biodom	EHS	Centralizado	EHS	Red eléctrica / Cableado ded.	Red eléctrica
Cardio	DomoVal Electronic, S.L	Centralizado	X10 / Protocolo propio	Red eléctrica / Cableado ded.	Árbol
Conleac	Logical Design, S.A.	Centralizado	Protocolo propio	Cableado ded.	Estrella
Dialoc	Weidmüller.	Descentralizado	LonWorks	Cableado ded.	Libre
Dialogo	BJC. Fábrica Electrónica Josa, S.A.	Descentralizado	LonWorks	Par trenzado / Cableado ded.	Libre
Domaiké	Aike S.L	Centralizado	X10 / Protocolo propio	Cableado ded. / RF / Red eléctrica	Centralizada
DomoLon	ISDE Ing. S.L.	Descentralizado	LonWorks	Cableado ded.	Libre
DomoScope	Fagor S.L	Centralizado	Bus Fagor	Red eléctrica	Red eléctrica
GIV	Ceilhit - Eurocable, S.A	Centralizado	Protocolo propio	Cableado ded.	Estrella
SimonVis	Simón S.A	Centralizado	Protocolo propio	Cableado ded.	Estrella
SimonVox	Simón S.A	Centralizado	Protocolo propio	Cableado ded.	Estrella
SSI18	SGI Sistemas.	Centralizado	Protocolo propio	Cableado ded.	Estrella
StarboxCPL1	Delta Dore.	Centralizado	X2D	Red eléctrica	Red eléctrica
StarboxDE1	Delta Dore.	Centralizado	Protocolo propio	Cableado ded.	Estrella
Vantage	Vantage S.L	Centralizado	Protocolo propio	Cableado ded.	Bus / Estrella
VivimatC-RF	Dintel.	Centralizado	Protocolo propio	Cableado ded. / RF	Estrella
Vivimat Plus	Dintel.	Centralizado	Protocolo propio	Cableado ded.	Bus / Estrella

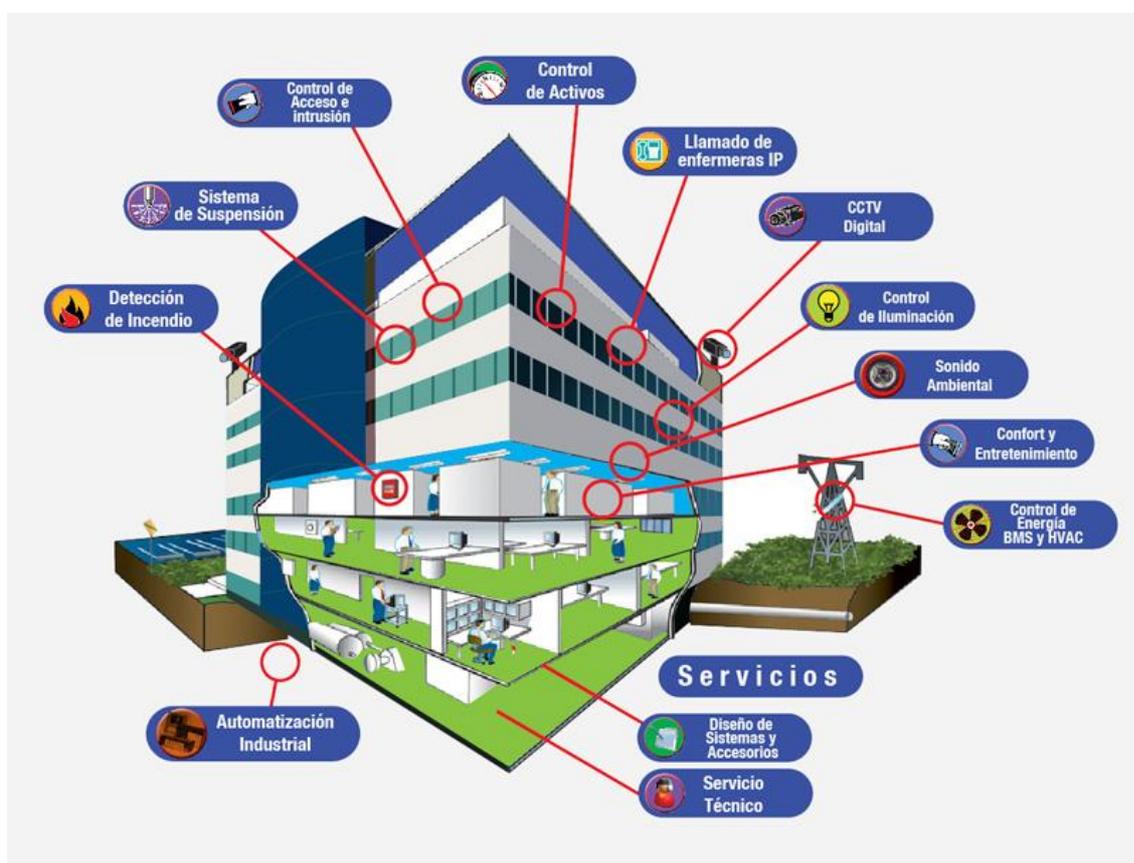
Fuente: Diseño de un sistema domótico de altas prestaciones destinado a viviendas residenciales [En línea]. [Citado el 15 de abril de 2014]. Disponible en <Diseño de un sistema domótico de altas prestaciones destinado a viviendas residenciales>

1.1.2 Sistemas Inmóticos

1.1.2.1 ¿Qué es la inmótica?

La inmótica se entiende como un sistema de gestión remoto, centralizado y automatizado que supone la adición de numerosos subsistemas, Enfocados a instalaciones de edificios terciarios con el fin de optimizar recursos, reducir costos y disminuir el consumo de energía innecesario, al mismo tiempo que aumenta la seguridad y el confort. [15]. En la figura 3 se observa los principales componentes de un sistema Inmótico.

Figura 3: Principales componentes de un entorno Inmótico



Fuente: Inmótica... complemento al edificio inteligente [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://ecoopcion.wordpress.com/2012/04/16/inmotica-complemento-al-edificio-inteligente/>>

La inmótica hace uso de la alta tecnología, para conseguir un ahorro energético considerable, a través del uso responsable y eficiente de la energía. Con la inmótica se puede lograr un control de iluminación por presencia, con una programación horaria o en función de la luz natural que exista en cada una de las diferentes zonas. Además, es posible controlar a través de un sistema inteligente la climatización del edificio, teniendo en cuenta factores como la temperatura del exterior o la incidencia del sol. De esta forma, se puede alcanzar un ahorro energético de hasta un 40%. Esto, combinado con un eficiente aislamiento de los edificios, puede ayudar a reducir bastante los costos.

Con ayuda de la inmótica es posible monitorizar el funcionamiento general del edificio y controlar otros aspectos, como los ascensores, el balance energético, el riego, la sensorización de variables como son la temperatura y humedad, las alertas, el sistema de accesos o de detección de incendios, la supervisión de cuadros eléctricos, entre otros. De esta forma, se logra la creación de edificios “inteligentes” más eficientes, con reducciones en los costos de energía y operación, al igual que el aumento del confort y la seguridad para los usuarios.

Si bien la inmótica está relacionada con la domótica, tiene características propias diferenciadoras. Mientras la domótica se ocupa de la gestión energética de la vivienda de manera individualizada, la inmótica lo hace de forma integral en todo el edificio. Además, esta última está enfocada a complejos y edificios de uso industrial como son: hoteles, hospitales, centros comerciales, comunidades de vecinos, edificios de negocios, gimnasios, colegios, centros de discapacitados, ayuntamientos, instalaciones deportivas, aeropuertos, etc. [15]

1.1.2.2 Características generales

La inmótica, permite controlar y gestionar los diferentes sistemas técnicos del edificio, de una forma óptima e integrada, tanto de forma local como remota. La centralización de los datos de todo el edificio, permite supervisar y controlar desde uno o más sitios de trabajo, las alarmas y los estados de funcionamiento de los sistemas que componen la instalación. Por ejemplo:

- El sistema de climatización.
- El sistema de iluminación.
- El sistema de persianas.
- El sistema de gestión eléctrica (para el control de consumos eléctricos).
- El sistema de control de accesos.
- El sistema de seguridad.
- El sistema de detección de incendios.
- Las telecomunicaciones.
- Sistemas industriales.[17]

1.1.2.3 Tecnologías Inmóticas actuales

Tecnologías que se aplican en el control de automatización de edificios y viviendas.

Tabla 2: Principales tecnologías Inmóticas

KNX	ENOCEAN
	

Fuente: Tecnologías inmóticas [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://www.controlcat.com/index.php/producto/producto-tecnologia>>

❖ **KNX:**

Es un estándar abierto para el control de casas y edificios, permite transferir datos de todos los componentes de gestión de edificios, asegurando que todos los componentes se comuniquen a través de un lenguaje común. En resumen, este estándar está basado en otros con más de 20 años de experiencia en el mercado, A través del medio de transmisión (par trenzado, radio frecuencia, línea de fuerza o IP/Ethernet) de KNX, sobre el que se conectan todos los dispositivos, se intercambia la comunicación. Los dispositivos conectados al bus, tanto sensores como actuadores, son utilizados para el control de equipamiento de gestión de edificios en todas las aplicaciones posibles: iluminación, persianas / contraventanas, sistemas de seguridad, gestión energética, calefacción, sistemas de ventilación y aire acondicionado, sistemas de supervisión y señalización, interfaces a servicios y sistemas de control de edificios, control remoto, medición, audio / video, control de bienes de gama blanca, etc. Todas estas funciones pueden ser controladas, supervisadas y señalizadas utilizando un sistema uniforme sin la necesidad de centros de control adicionales. [19]. En la figura 4 se observa las diferentes funciones que permite implementar la tecnología KNX

Figura 4: Funciones de la tecnología KNX



Fuente: ¿Qué es knx? [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.knx.org/es/knx/que-es-knx/>>

- ❖ **ENOCEAN:** Es la raíz de la tecnología inalámbrica autoalimentada patentada. La empresa, que tiene su sede central en Oberhaching, cerca de Múnich, fabrica y comercializa soluciones de sensores inalámbricos que no requieren mantenimiento para su uso en edificios e instalaciones industriales. Las soluciones de EnOcean se basan en convertidores de energía en miniatura, circuitos electrónicos de bajo consumo energético y sistemas inalámbricos. La combinación de estos elementos permite a EnOcean y a sus socios proveedores ofrecer sistemas de sensores que son fundamentales para edificios con consumo eficiente de energía e industrias innovadoras [20]. En la figura 5 se observa una representación gráfica de conexión Wireless con los elementos de campo.

Figura 5: Representación gráfica de conexión Wireless, extensión ENOCEAN



Fuente: ENOCEAN EXTENSION - SIMPLE, WIRELESS HOME AUTOMATION [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<https://b.loxone.com/Pages/en/produkte/extensions/EnOcean/loxone-rs485.aspx>>

1.1.3 Sistemas SCADA

1.1.3.1 ¿Qué es un sistema SCADA?

Un sistema SCADA (Supervisory Control and Data Acquisition) es una interfaz que permite supervisar procesos en forma remota. Como su nombre indica, el sistema funciona gracias a la adquisición de datos de procesos remotos.

El uso más generalizado de los sistemas SCADA se encuentra en el control de producción, permitiendo controlar todo el proceso desde un ordenador, al establecer una comunicación entre los distintos dispositivos de campo. Permite observar desde la pantalla de un ordenador el estado de las estaciones remotas y tomar, las medidas oportunas en tiempo real en caso de que exista algún problema. En la figura 6, se observa un ejemplo de implementación de un sistema SCADA.

Figura 6: Ejemplo sistema SCADA



Fuente: System Attacks – Turning SCADA into NADA SCADA [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://chenected.aiche.org/process-safety/system-attacks-turning-scada-into-nada/>>

1.1.3.2 Funciones que un sistema SCADA debe proveer:

- Sistema de alarmas que genere un registro de incidencias.
- Posibilidad de realizar cálculos aritméticos complejos.
- Generación de datos históricos sobre el funcionamiento de los sistemas remotos.
- Interfaz HMI (hombre-máquina) amigable para los usuarios.
- Comunicación interna y externa con todos los equipos.
- Un Software SCADA debe estar desarrollado con arquitectura abierta, para que pueda ser ampliado o mejorado en el futuro fácilmente.

- Capacidad de controlar y supervisar todos los sistemas remotos, conocer su desempeño y tener la posibilidad de activarlos o desactivarlos.
- Procesamiento de los datos, comparativa con datos anteriores y generación de reportes.

1.1.3.3 Comunicación y realimentación

Los sistemas SCADA requieren de una comunicación remota entre equipos. Cada fabricante utiliza el protocolo de comunicación que estima oportuno, ya que no existe un estándar generalizado. En muchas ocasiones, la comunicación se realiza con sistemas E/S ubicados en campo mediante RTU, PLC u otros mecanismos.

1.1.3.4 Usos Industriales:

- Gestión de la producción de una fábrica.
- Tratamiento de la información.
- Monitorización de procesos químicos.
- Control de la calidad.
- Administración y mantenimiento. [24]

1.2 CONTROLADORES Y ARQUITECTURAS DE CONTROL

1.2.1 ¿Qué es un controlador?

Se puede definir un controlador como el elemento central de un automatismo. Este recibe la información recogida por los distintos elementos de campo, y envía órdenes a los actuadores conforme a una lógica incorporada al mismo.

La funcionalidad que ofrece un controlador puede variar enormemente, desde la que ofrece, un simple temporizador, o un termostato, hasta sofisticados sistemas basados en escenarios que regulan de una manera coordinada todos los elementos de campo, en base a los valores de múltiples variables: Temperatura, humedad, luminosidad, ruido ambiente, etc. [26]

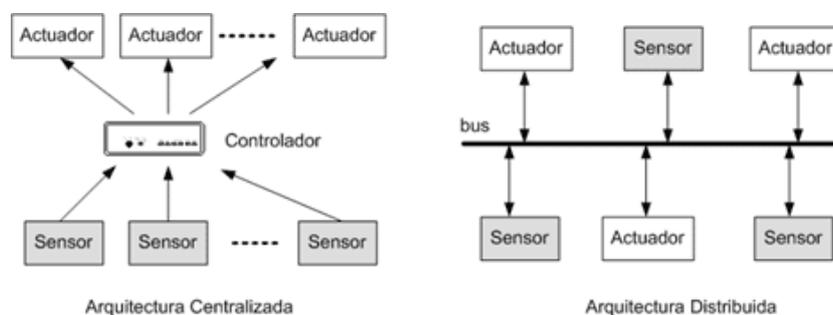
1.2.2 Arquitectura de control

La arquitectura de control, especifica el modo en que los diferentes elementos de control del sistema se van a ubicar. Existen dos arquitecturas básicas, la arquitectura centralizada y la distribuida

1.2.2.1 Arquitectura centralizada

Es aquella en la que los elementos a controlar y supervisar (sensores, luces, válvulas, etc), son cableados hasta el sistema de control de la vivienda (PC o similar). El sistema de control es el corazón de la planta, en cuya falta todo deja de funcionar, y su instalación no es compatible con la instalación eléctrica convencional, por lo tanto en la fase de construcción hay que elegir esta topología de cableado. [28]. En la figura 7, se observa una representación de arquitectura centraliza y distribuida

Figura 7 : Arquitectura centralizada y distribuida.



Fuente: Arquitecturas de un sistema domótico. [En línea]. [Citado el 15 de abril de 2014]. <Disponible en < http://fempa.es/rebt/automatizacion_vigilancia/pto5.htm >

1.2.2.2 Arquitectura distribuida:

Es aquella en la que el elemento de control se sitúa próximo al elemento a controlar. Hay sistemas de arquitectura distribuida en cuanto a su capacidad para ubicar elementos de control físicamente distribuidos, pero no en cuanto a los procesos de control, que son ejecutados en uno o varios procesadores físicamente centralizados. Estos sistemas utilizan como medio de transmisión el cable, existe un concepto a tener en cuenta que es la topología de la red de comunicaciones. [28]

1.2.3 Controladores más usados

1.2.3.1 PLC

- **Principios Básicos**

Con la llegada de los autómatas programables, los llamados PLC (Programmable Logic Controller), la industria obtuvo un impulso importante, lo cual ha facilitado de forma notable, que los procesos de producción o control se hayan flexibilizado. Se encuentran PLC en las industrias, pero también en las casas, en los centros comerciales, hospitales, etc. [30]. En la figura 8 se observa un PLC de uso industrial.

Figura 8 : PLC Allen Bradley SLC 500



Fuente: PLC Allen Bradley SLC 500 [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.automation-drive.com/for-allen-bradley-slc-500>>

1.2 **SENSORES Y ACTUADORES**

1.2.3 **¿Qué es un sensor y un actuador?**

Antes de describir que es un sensor y un actuador, es necesario definir el término transductor.

Un transductor: es un dispositivo que permite convertir un tipo o manifestación de energía en otra, ya sea: Física, química, eléctrica, etc. Para ser procesada o interpretada por un sistema de control, el cual se encarga, de ejecutar una acción previamente programada.

1.3.3.1 **Sensor**

Es un elemento capaz de captar, convertir y transmitir algún tipo de variable, posibilitando la adquisición y procesamiento de la información obtenida. [37]

1.2.3.2 Actuador

Es un dispositivo que recibe una señal del sistema de control y realiza una acción, esta puede ser: mecánica, hidráulica, eléctrica, neumática, etc. Con la finalidad de generar alguna operación dentro de un proceso. Que por lo general es mecánica. [38]

1.2.4 Sensores requeridos para el sistema de gestión y supervisión

1.3.4.1 Detector de movimiento

Son dispositivos de origen electrónico, que permiten la identificación de un movimiento y/o presencia en un recinto, el sistema puede estar conformado por un captador infrarrojo o un generador ultrasónico, permitiendo el mapeo, “en tiempo real” del lugar asignado.

Algunos equipos incorporan un regulador de luminosidad que es pilotado automáticamente, mediante un regulador electrónico, censando los puntos de luz, previamente determinados. [11] (véase figura 9)

Figura 9: Detector de movimiento



Fuente: Climax irp9- detector de movimiento /detección de 12 metros [En línea]. [Citado el 15 de abril de 2014]. Disponible en<
http://convergenciadigital.com/eshop/product_info.php?products_id=831>

1.3.4.2 Sensor de luz

Es un dispositivo que permite la detección de la iluminancia. Posibilitando gobernar automáticamente las escenas de luz, en función de la luz natural. En

los espacios interiores es posible obtener una iluminancia constante, a través de la combinación de la luz natural variable con una instalación de iluminación. [39] (véase figura 10)

Figura 10: Sensor de luminosidad



Fuente: Sensores. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.erco.com/guide/lighting-control/sensors-2611/es/>>

1.3.4.3 Alarma contra incendios

Permite detectar un incendio desde su inicio, generando una alerta en el hogar, edificio, local, oficina, depósito, o cualquier inmueble donde esté instalada. Son dispositivos de detección, que se ubican en diferentes zonas de un inmueble y al estar conectados en forma computarizada, permiten determinar cuál es el área en la que se inició el incendio, evitando su propagación. [40] en la figura 11 se observa una alarma contra incendios de uso comercial.

Figura 11: Alarma contra incendios



Fuente: Alarma contra incendios. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://santafe-ar.all.biz/alarmas-contra-incendios-g5112>>

1.3.4.4 Contacto magnético

Es el nombre genérico de un dispositivo o sensor de apertura, integrado por dos unidades necesariamente hermanadas, en una posición determinada, ver figura 12, al momento de presentarse la separación de estas dos piezas, se produce un cambio mecánico en los contactos de una de ellas, a fin de informar el cambio de “estado”, pasando de un estado cerrado al de “libre acceso” o abierto. [41]

Figura 12: Contactos magnéticos



Fuente: Contactos magnéticos cableados, plástico ABS en color blanco, Salida NC [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.empretel.com.mx/cableado/1570-contactos-magneticos-cableados-plastico-abs-en-color-blanco-salida-nc.html>>

1.3.4.5 Cámara IP

Cámara IP (también conocida como cámara Web o de Red), son videocámaras especialmente diseñadas para enviar señales (video, y en algunos casos audio) a través de internet, por medio de un concentrador (un HUB o un SWITCH) en una Red Local (LAN), ver figura 13.

En las cámaras IP, pueden integrarse a aplicaciones como: Detección de movimiento (incluso el envío de mail si detectan presencia), grabación de imágenes o secuencias en equipos informáticos (tanto en una red local o en una red externa (WAN), de manera que se pueda comprobar, por qué se ha generado una alteración en el entorno y se graben imágenes de lo sucedido. [43]

Figura 13: Cámara IP



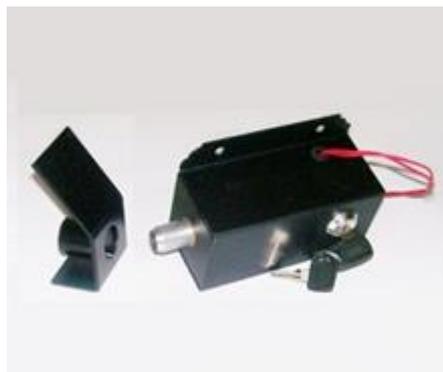
Fuente: Cámara IP [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://totem.com.ec/blog/dato-importante-sobre-las-camaras-ip/>>

1.3.5 Actuadores requeridos para el sistema de gestión y supervisión

1.3.5.1 Cerradura eléctrica

Una cerradura eléctrica es un dispositivo de fijación, que actúa mediante corriente eléctrica, ver figura 14. Las cerraduras eléctricas están conectadas principalmente, con un sistema de control de acceso. [45]

Figura 14 : Cerradura eléctrica Luber 2020



Fuente: Cerradura Eléctrica de Aplicar para Portones Luber 2020 [En línea]. [Citado el 15 de abril de 2014]. Disponible en <http://maxisistemas.com/index.php?route=product/product&product_id=203>

1.3.5.2 Sirena

Es el actuador que permite la emisión de una advertencia sonora, dependiendo de su configuración interna, dichas alarmas posibilitan la configuración de diferentes tonalidades. [47] (véase figura 15)

Figura 15: Sirena



Fuente: Sirena [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://control-ip-alarmas.blogspot.com/2009/06/4.html> >

2. CRITERIOS DE SELECCIÓN DE LOS COMPONENTES DEL SISTEMA DE GESTIÓN Y SUPERVISIÓN

2.1 SELECCIÓN DEL SISTEMA DE GESTIÓN Y SUPERVISIÓN

A la hora de seleccionar el sistema de gestión y supervisión, se optó por una interfaz SCADA, debido a que permite la ampliación y mejora continua del mismo; además, cuenta con un entorno de desarrollo amigable con el usuario y con una programación con un grado medio de complejidad.

Características de selección:

- El número de variables del proceso que se necesita monitorear debe ser alto.
- El proceso debe tener transmisores y actuadores geográficamente distribuidos. Esta condición no es limitativa, ya que puede instalarse un SCADA para la supervisión y control de un proceso concentrado en una localidad.
- La información del proceso se necesita en el momento en que los cambios se producen en el mismo; o en otras palabras, la información se requiere en “tiempo real”.
- Que exista la necesidad de optimizar y facilitar las operaciones de la planta, así como la toma de decisiones, tanto gerenciales como operativas.
- Que los beneficios obtenidos en el proceso a ser controlado puedan reflejarse en aumento de la confiabilidad, disminución de tiempos de operación, aumento de los niveles de seguridad, etc.

Dentro de las funciones básicas realizadas por un sistema SCADA están las siguientes:

- Automatización: Se refiere a recabar, almacenar y mostrar información, en forma continua y confiable, desde los equipos de campo: estados de dispositivos, magnitud de variables. También se refiere a ejecutar en forma automática, disparo de alarmas para que el operador pueda notar un estado anormal en el proceso.
- Supervisión: Por medio de la HMI mostrar y / o alertar al operador de cambios detectados en la planta, tanto aquellos que no se consideren normales (alarmas) como cambios que se produzcan en la operación diaria de la planta (eventos). Basados en los datos enviados, el operador podrá iniciar acciones de control, tales como: abrir o cerrar válvulas,

arrancar o parar bombas, etc., con la aclaración que ya se hizo al respecto.

- Manejo de alarmas: Disparar alarmas en forma automática para que el usuario pueda ejecutar acciones que controlen las situaciones anómalas que las generaron.
- Generación de reportes: Basadas en la información obtenida por el sistema es posible generar: reportes, gráficos de tendencia, historia de variables, cálculos, predicciones, detección de fugas, etc.[48]

2.2 CRITERIOS DE SELECCIÓN PARA UN SOFTWARE SCADA

En la tabla 3 se observan los principales sistemas SCADA, disponibles actualmente.

Tabla 3: Principales software SCADA

Nombre del Producto:	Distribuidor(y fabricante)/Fabricante:
Indusoft:	Indusoft Web Studio HMI SCADA Development
Aimax:	Design Instruments, S.A. (T.A. Engineering)
All-Done Scada:	Freixas i Ros, S.L.
Automainge:	Automainge
Captor:	Sistplant
Checksys Objects:	M2R,S.A.
CIC:	CJM Software,S.A.
Cube:	ORSI España,S.A.
Cx-SuperVisor:	Omron
Digivis:	Elsag bailey Hartmann & Braun,S.A.
Experion PKS	Honeywell,S.A. <i>Evolución de los anteriores TDC3000, TPS y Plantscape.</i>
Factory Suite A2:	Logitek, S.A./Wonderware. <i>Evolución del FactorySuite 2000.</i>
Factorylink ECS y Xfactory:	Tecnomatix (USDATA)
Gefip:	Mondragón Sistemas
Genesis CE(Pocket) y 32:	Aplein Ingenieros, S.A./Iconics
Glassmaster Control System:	Mediterranean Import Trade, S.L./Precise Control Systems
GPAO-SAC:	Sistemas Avanzados de Control,S.A.
I/A:	Foxbor[]
iFIX 3.5:	Intellution(GE Fanuc Automation). <i>Evolución del FIX DMACS 7.0 creado por: CIM(Computer Integrated Manufacturing), Fisher, Rosemount, Omron/Intellution.</i>
IGSS32:	AN Consult España,S.L./7-Technologies A/S (DK)
Intouch:	Logitek,S.A./Wonderware
JUMO SVS-2000:	Jumo Sercon, S.A. (D)
LabVIEW DSC:	National Instruments (1)
NI Lookout 5.1:	National Instruments
Monitor Pro V7.x:	AEA Technology
P6008:	Foxboro Scada (I)
Pack-Centre:	Agecontrol
PCVUE 32:	Rasesa Automatismos, S.L./ARC Informatique
Proasis DAS-Win:	Desin Instruments,S.A.
Processyn:	OBM de Equipos Eléctricos,S.A./Logique Industrie
Pyman:	Pyssa
Quick SPC:	Marposs, S.p.A (I)
RSView32:	Rockwell Automation/Rockwell Software
Scada-Vs:	Foxboro/Foxcada (Australia)
SIMATIC(WinCC):	Siemens (2)
Symcont:	Adasoft, S.A.
SYSMAC-SCS:	Omron
Tactician T3500:	Eurotherm España/Eurotherm Process Automation (UK)
TCS01:	Sistemas Eléctricos Personalizados S.L.
TD-Pro:	Pertegaz,S.L. (I)
Test Point:	Instrumentos de Medida,S.L.
TQWIN:	Vertex Serveis Informàtics, S.L.
WizFactory:	Wizcon Soft España,S.L./PC soft International, Ltd (Israel)

Fuente: sistemas SCADA. [En línea]. [Citado el 16 de abril de 2014]. Disponible en < http://www.sistemamid.com/panel/uploads/biblioteca/2013-08-04_08-34-0840201-3452.pdf>

El software seleccionado para dar respuesta al sistema de gestión y supervisión, bajo sus cuatro parámetros principales: gestión, control, seguridad y la generación de reportes, de acuerdo a los criterios anteriormente mencionados, es la plataforma InduSoft Web Studio®; ya que es una poderosa colección de herramientas de automatización, que proporciona paquetes para desarrollar sistemas HMI's, SCADA y soluciones de instrumentación embebidas. Utiliza la tecnología Web integrada de InduSoft para tomar ventaja de la conectividad a Internet/intranet.

Se determina que este software, cuenta con los requerimientos necesarios para el desarrollo de la propuesta de diseño del sistema de gestión; además, tiene compatibilidad con una gran variedad de autómatas programables. Por otra parte, este sistema cuenta con muchos iconos y librerías, que permiten una interfaz amigable con el usuario. InduSoft es un software de licencia paga y una potente herramienta SCADA, en la figura 16 se observa una vista general del software. [50]

Figura 16: Simulación de tanques InduSoft Web Studio



Fuente: InduSoft Web Studio. [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://www.indusoft.com/Products-Downloads/HMI-Software/Indusoft-en-Espa%C3%B1ol>>

2.2.1 InduSoft Web Studio

InduSoft Web Studio, es un conjunto de materiales de automatización enteramente modular, para el desarrollo de cualquier tipo de automatismo, desde recientes interfaces Hombre-Máquina (HMI), hasta completos sistemas (SCADA), bajo cualquier plataforma Windows. Su entorno de desarrollo le admite trasladar los más complejos comportamientos de sus procesos industriales a aplicaciones con tan solo simples arrastres y clics de ratón.

Las aplicaciones de (InduSoft Web Studio), se elaboran en microcomputadoras, acopladas a máquinas o computadoras mediante controladores programables, dispositivos E/S remotos y otros aparatos de adquisición de datos en "tiempo real". [52]

2.2.2 Alcances InduSoft

Las aplicaciones de InduSoft web Studio consisten en pantallas animadas que sirven de interfaz con el operador, drivers para PLC y otros dispositivos de E/S controlables, una base de datos de etiquetas para aplicaciones, y módulos opcionales tales como monitores para alarmas, gráficas de tendencia, recetas, planificadores de tareas, y un sistema de seguridad. Las aplicaciones de IWS interactúan con sistemas industriales de E/S y con otras aplicaciones de Windows durante la ejecución de la aplicación. Como características generales de InduSoft se encuentran:

- Poderosos Objetos gráficos
- Amplia librería de objetos
- Tendencias en tiempo real e histórico
- Manejador de Alarmas y Eventos en tiempo real e histórico
- Administrador de recetas
- Envío de alarmas y eventos a e-mails y celulares
- Interface a bases de datos
- Generador de Reportes
- Interface con Office vía DDE u ODBC
- Funciones matemáticas avanzadas
- Fácil programación con lenguaje de scripts fácil y flexible
- Además de poderosos scripts de Visual Basic
- Integración transparente con aplicaciones Windows como Microsoft Word and Excel; interfaz con herramientas de terceros como Java, C, C++, y Visual Basic
- Ambiente de Desarrollo/Runtime en Windows NT/2000/XP/Vista
- Ambiente Runtime (ejecución) en WindowsCE
- Gráficos de tiempo real accesibles desde dispositivos inalámbricos y móviles
- 100% "Web based", clientes web accesan en tiempo real

- Provee las herramientas para configurar aplicaciones en cumplimiento con la regulación FDA 21 CFR Parte 11.
- Proporciona multi-niveles de seguridad para aplicaciones, incluyendo acceso a través de Intranets e Internet.
- Cumple con estándares industriales como Microsoft DNA, OPC, DDE, ODBC, XML, y ActiveX
- Proporciona traducción automática de idioma en tiempo real
- Soporta arquitecturas redundantes
- Drivers: contiene más de 240 drivers integrados para la mayoría de PLC's, controladores de temperatura, controladores de movimiento, y lectores de códigos de barra/2D/RFID. Nuevos o actualizados drivers para Eaton ELC, Siemens, Opto 22, CAN, CANopen, y BACnet, también han sido desarrollados. [53]

2.2.3 Protocolos de InduSoft

❖ ODBC (Open Database Connectivity)

Conectividad abierta de bases de datos (ODBC), es la interfaz estratégica de Microsoft, para obtener acceso a datos en un entorno heterogéneo, relacional y no-relacional. Sistemas de administración de bases de datos. Basado en la especificación de una interfaz. En nivel de llamada del grupo de acceso es SQL. ODBC proporciona una forma abierta e independiente del proveedor de acceso, a datos almacenados en una variedad de equipos, minicomputadoras y bases de datos de mainframe.

ODBC alivia la necesidad de proveedores de software independientes y los programadores corporativos, múltiples interfaces de programación de aplicaciones. ODBC proporcionan ahora una interfaz de acceso a datos universal. Con ODBC, los desarrolladores de aplicaciones pueden permitir obtener un acceso y al mismo tiempo, ver y modificar datos procedentes de diversas bases de datos. [59]

❖ DDE (Dynamic Data Exchange)

El intercambio dinámico de datos es una utilidad de Windows que utiliza Visual Basic, y nos permite crear aplicaciones que tomen datos una de otras. Para pasar datos de una aplicación a otra, se necesitan al menos dos aplicaciones. Puede darse el caso que una aplicación esté recibiendo datos de otra aplicación, y a su vez envíe datos a una tercera.

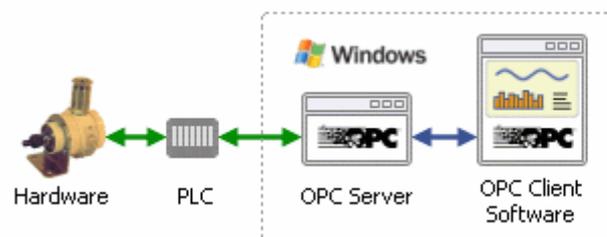
A la aplicación que envía la información se le llama aplicación servidor, y a la que la recibe, aplicación cliente. La aplicación servidor debe estar funcionando antes de que la aplicación cliente le pida la información. Si no es así, se generará un error. Los datos a traspasar de una aplicación a otra pueden ser:

- Textos, de un Label o un TextBox.
- Imágenes, de un PictureBox. [61]

❖ OPC (Open Connectivity)

OPC: Ole for Process Control, es un interfaz de software estándar, que le permite a los programas de Windows, comunicarse con los dispositivos de hardware industrial (véase figura 17).

Figura 17: Representación gráfica de la conexión OPC



Fuente: What is OPC? [En línea]. [Citado el 22 de abril de 2014]. Disponible en <<http://www.opcdatahub.com/WhatIsOPC.html>>

OPC, se implementa en pares de servidor / cliente. El servidor OPC es un programa de software que convierte el protocolo de comunicación de hardware utilizado por un PLC, en el protocolo OPC. El software de cliente OPC es cualquier programa que necesita conectarse al hardware, tales como un HMI. El cliente OPC, utiliza el servidor OPC para obtener datos o enviar comandos al hardware.

El valor de OPC, es un estándar abierto, lo que significa menores costos para los fabricantes y más opciones para los usuarios. Los fabricantes de hardware sólo necesitan dar un solo servidor OPC para permitir que sus dispositivos se comuniquen con cualquier cliente OPC. Los proveedores de software, simplemente incluyen capacidades de cliente OPC en sus productos, y se vuelve al instante compatible con miles de dispositivos de hardware. Los usuarios pueden elegir cualquier software de cliente OPC que necesitan, con la seguridad de que va a comunicarse sin problemas con su hardware OPC -permitido, y vice - versa. [62]

❖ TCP/ IP (Transmission Control Protocol / Internet Protocol) [52]

TCP/IP (Transmission Control Protocol/Internet Protocol), es el lenguaje básico de comunicación o protocolo de Internet. También se puede utilizar como un protocolo de comunicaciones en una red privada (ya sea una intranet o una extranet). Cuando se configura con acceso directo a Internet, su computadora cuenta con una copia del programa de TCP / IP, al igual que cualquier otro equipo que puede enviar mensajes o recibir información, que también tiene una copia de TCP / IP.

TCP / IP es un programa de dos capas. La capa superior, Transmission Control Protocol (Control del Protocolo de Transmisión), gestiona el montaje de un mensaje o archivo en paquetes más pequeños, que se transmiten a través de Internet y se reciben por una capa TCP, que re ensambla los paquetes en el mensaje original. La capa inferior, Protocolo de Internet, se encarga de la parte de dirección de cada paquete, para que llegue a su destino correcto. Cada equipo de puerta de enlace en la red, comprueba esta dirección para ver a donde enviar el mensaje.

TCP / IP utiliza el modelo cliente / servidor de comunicación, en el que un usuario de la computadora (un cliente) solicita y se le proporciona un servicio (como el envío de una página Web), a otro equipo (un servidor) en la red. La comunicación TCP / IP está de punto a punto, principalmente, lo que significa que cada comunicación es de un punto (o computadora host) en la red a otro punto o un ordenador host. TCP / IP y las aplicaciones de nivel superior que lo utilizan colectivamente, se dice que son " sin estado ", ya que cada petición de cliente, se considera una nueva solicitud relacionada con ninguna anterior (a diferencia de las conversaciones telefónicas ordinarias, que requieren una conexión dedicada para la duración de la llamada). [63]

2.3 SELECCIÓN DEL SISTEMA DE CONTROL

2.3.1 Criterios de selección para el sistema de control

2.3.1.1 Criterios de selección del dispositivo que permite la adquisición y control de los datos y/o variables:

- Cantidad de entradas / salidas, y si estas son analógicas ó digitales y sus rangos de operación.
- Cantidad de programas que puede manejar.

- Cantidad de programas que puede ejecutar al mismo tiempo (multitarea).
- Cantidad de contadores, temporizadores, banderas y registros.
- Lenguajes de programación.
- Software especializado para cada modelo de PLC y su facilidad de manejo.
- Software para programación desde la PC y necesidad de tarjeta de interface.
- Capacidad de realizar conexión en red de varios PLC.
- Respaldo de la compañía fabricante del PLC en nuestra localidad.
- Servicio y refacciones
- Capacitación profesional sobre el sistema de control.
- Literatura en nuestro idioma.[54]

Después de considerar aspectos como: el número de entradas y salidas requeridas, facilidad para conectar el dispositivo con un sistema SCADA, una programación sencilla que permita un control óptimo de las variables; se llega a la conclusión de implementar un PLC marca THINGET de la serie XC3-32r-c, el cual, se encuentra actualmente disponible en la universidad. Dicho PLC, cuenta con 16 entradas digitales y 16 salidas digitales y un módulo analógico para la adquisición de datos no booleanos (XC-E3AD4PT2DA), ver figura 18.

Figura 18: PLC THINGET



Fuente: XC series PLC [En línea]. [Citado el: 13 de septiembre de 2013]. Disponible en <<http://www.imenista.com/tingetplc.html> >

2.3.2 Selección del HMI

Teniendo en cuenta la selección realizada del PLC, El HMI seleccionado es el THINGET OP 320-A. Se designa un HMI disponible de la marca THINGET, debido a su compatibilidad, el cual se observa en la figura 19.

Figura 19: HMI THINGET OP 320-A



Fuente: Thinget HMI [En línea]. [Citado el: 13 de septiembre de 2013]. Disponible en <<http://spanish.alibaba.com/product-gs/thinget-hmi-406733528.html>>

2.3.4 Criterios de selección del computador

Con relación al computador, se recomienda usar un HP COMPAQ 5700 (Véase figura 20), teniendo en cuenta los siguientes criterios:

- a. Se encuentra disponible en los laboratorios de Universidad.
- b. El ordenador encargado del sistema de administración debe estar encendido las 24 horas del día, para garantizar un monitoreo constante del proceso.
- c. Se deben proporcionar los recursos mínimos que permitan que el software se ejecute sin ningún inconveniente.

Figura 20: Ordenador HP COMPAQ 5700



Fuente: HP Compaq dc5700 Microtower PC [En línea]. [Citado el 16 de abril de 2014]. Disponible en <http://images.businessweek.com/ss/07/05/0514_greencomputing/source/4.ht>

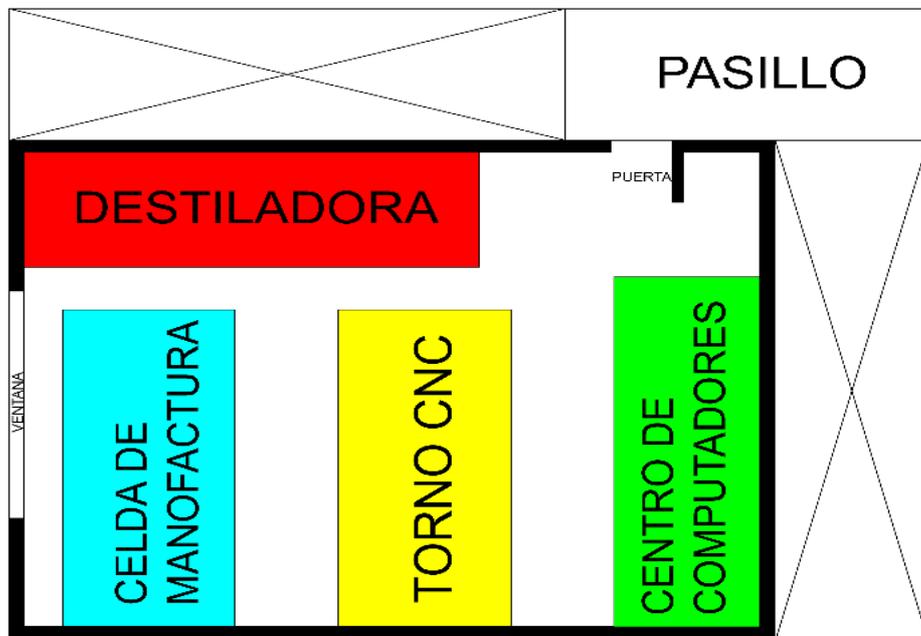
3. ÁREAS DE IMPACTO CONTEMPLADAS EN EL SISTEMA DE GESTIÓN Y SUPERVISIÓN

A continuación se describen las diferentes actividades propuestas para el desarrollo de cada una de las áreas de impacto del sistema de gestión y supervisión, mostrando el estado actual de cada una de ellas y la propuesta de diseño para mejorarlas.

3.1 ESTADO ACTUAL

En la figura 21, se observan los principales componentes encontrados en el laboratorio de automatización y su correspondiente distribución.

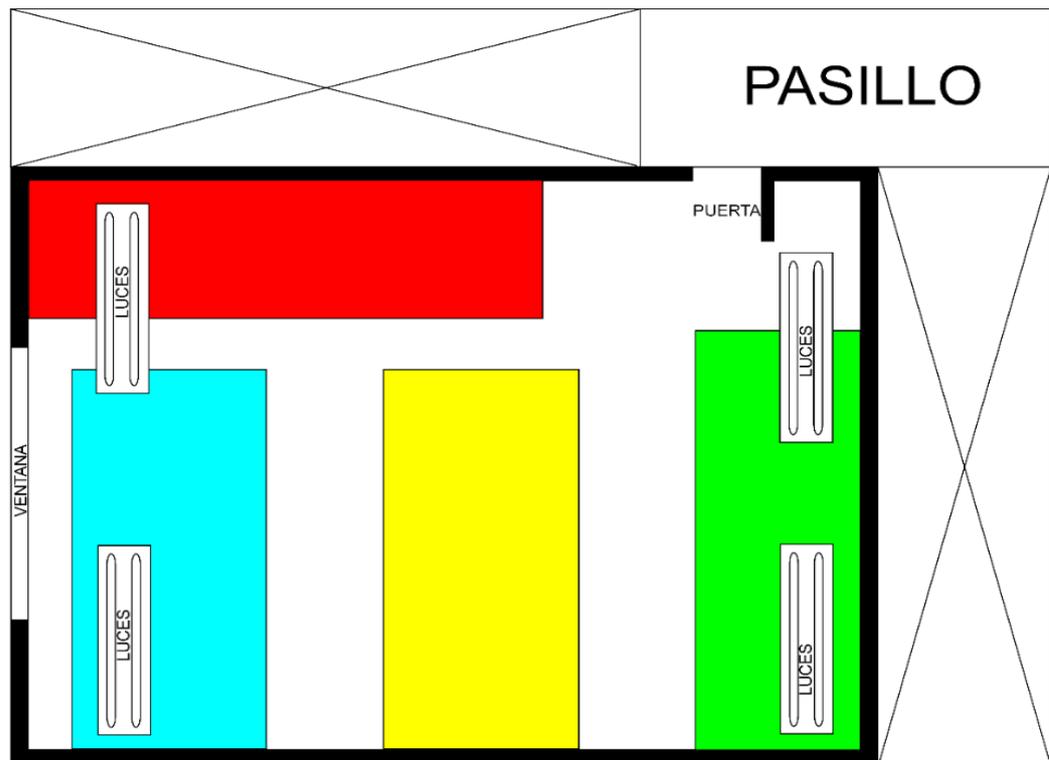
Figura 21: Distribución por módulos, del laboratorio de automatización, situado en el CDV



3.1.1 Sistema de luces

En la figura 22, se observa el estado actual del sistema de iluminación del laboratorio, así como, la distribución de las lámparas dentro de la sala, estas son activadas de forma manual por medio de dos interruptores.

Figura 22: Distribución actual del el sistema de iluminación en el laboratorio de automatización



3.1.2 Sistema de acceso

El acceso al laboratorio de automatización, se da por medio de una puerta principal, que cuenta con una cerradura manual convencional, como se observa en la figura 23.

Figura 23: Puerta principal laboratorio de automatización CDV



3.1.3 Sistema de gestión

En la figura 24, se observa el formato actual con el que cuenta el laboratorio de automatización para realizar la solicitud y préstamo de equipos, este se hace a través de un enlace de “google docs.”, al cual el monitor accede, organiza y asigna las aulas y equipos disponibles. La propuesta de diseño para este sistema se menciona en el numeral 3.5.

Figura 24: Sistema de gestión actual

Formato Solicitud de elementos Laboratorio

***Obligatorio**

Nombre *

Código *
Materia *
Docente *
Fecha y hora de uso de los elementos *
Ejemplo: 03/05/2013 11:30 AM
Elija el espacio Donde va a trabajar *

Laboratorio de Automatización (Primer Piso)

Laboratorio de Electrónica (Segundo Piso)

Laboratorio de Diseño (Segundo Piso)

Elija los elementos a utilizar de Automatización

Equipo de Computo

Plc Thinget XC3-32R-C

Plc Allen Bradley Micrologix 1100

3.2 PROPUESTA DE DISEÑO

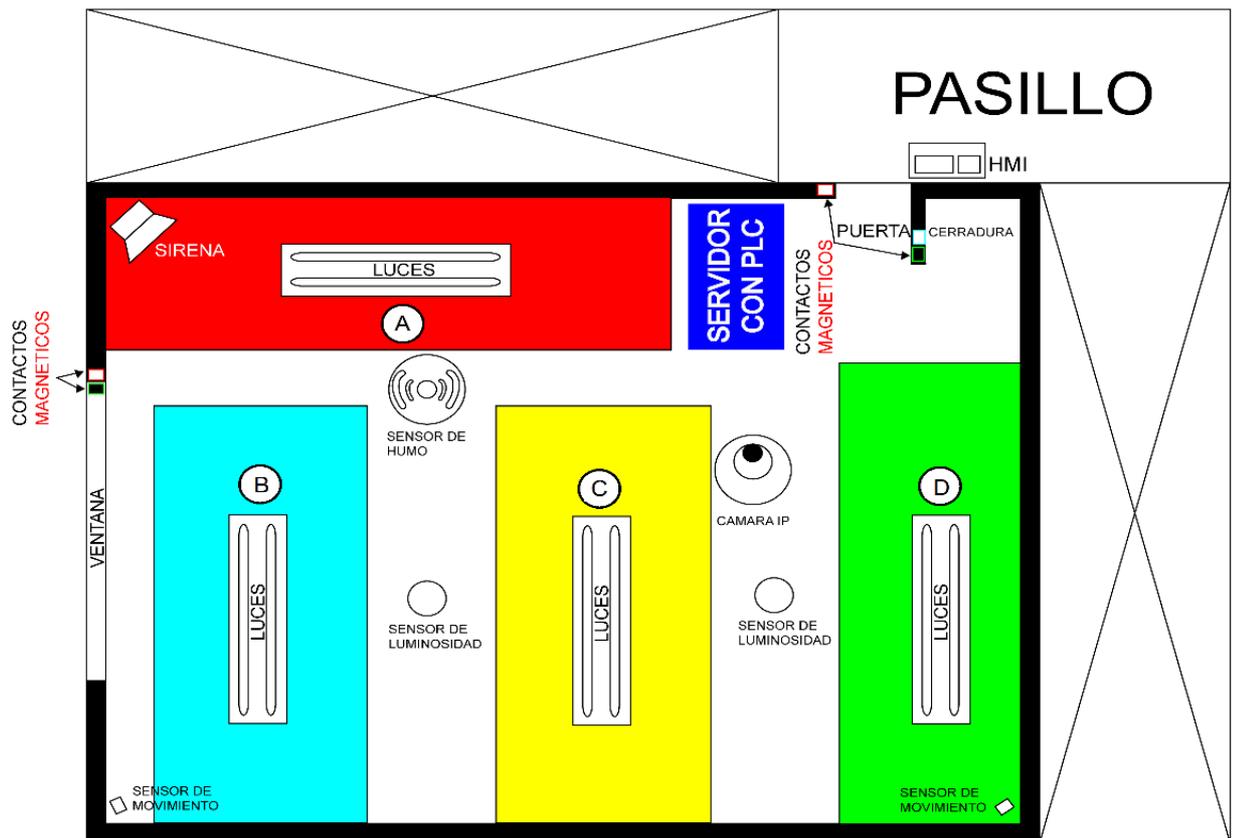
Una vez analizado el estado actual de los diferentes componentes que conforman el laboratorio, se propone un diseño de mejoramiento. En la figura 25, se muestran los diferentes elementos de campo propuestos para el diseño del sistema de gestión y supervisión. Los cuales se clasifican en:

❖ Sensores:

- Sensores de luminosidad (2)
- Sensores de movimiento (2)
- Contactos magnéticos (2)

- Detector de humo (1)
- ❖ Actuadores:
- Sirena (1)
 - Cerradura Eléctrica Luber (1)
 - Relés (4)
- ❖ Control:
- HMI THINGET 0P 320-A (1)
 - Ordenador HP COMPAQ 5700 (1)
 - PLC THINGET XC3-32r-c (1)

Figura 25: Propuesta de diseño del laboratorio de automatización, situado en el CDV



3.2.1 Sistema de luces propuesto

Como se observa en la figura 26, el sistema propuesto para iluminar el laboratorio de automatización del programa de ingeniería Mecatrónica,

consta de 2 sensores de luminosidad que permiten un control automático de 4 pares de tubos fluorescentes, situados estratégicamente para iluminar cada módulo del laboratorio (A, B, C, D), estas lámparas, cuentan con un encendido temporizado para evitar lo picos de voltaje en el sistema. En la figura 27 se observa la forma en la que el sistema de luces es conectado al PLC, la interfaz SCADA y el HMI respectivamente, desde cada uno de estos se puede lograr un encendido general o sectorizado de las lámparas.

Figura 26: Propuesta de diseño, control de luces

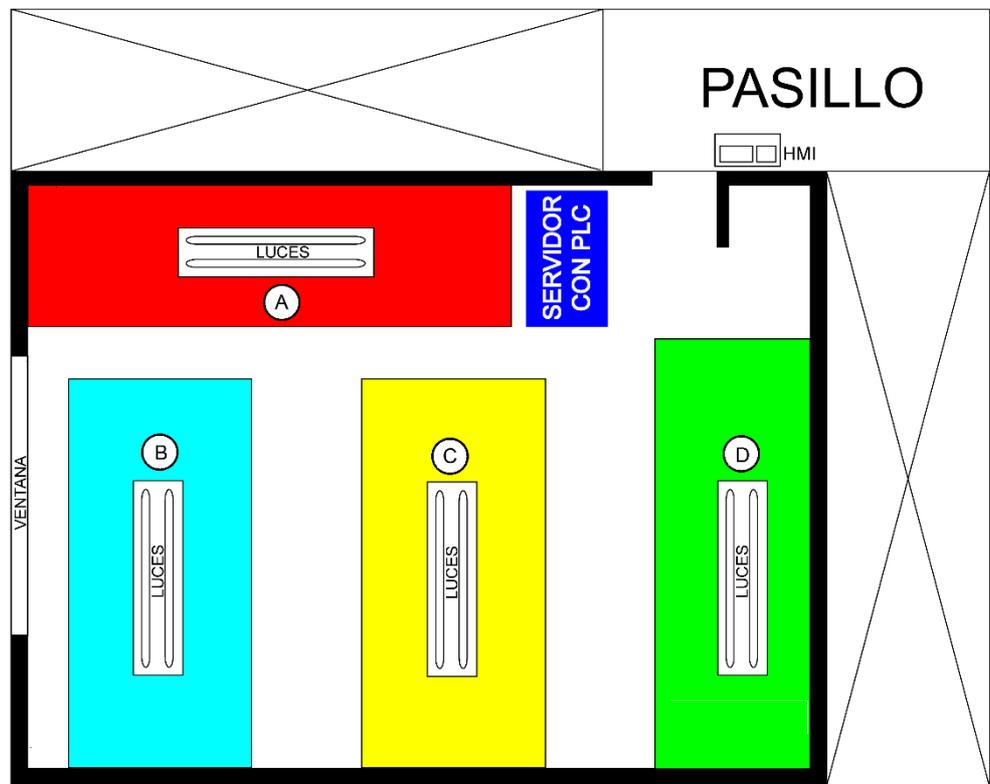
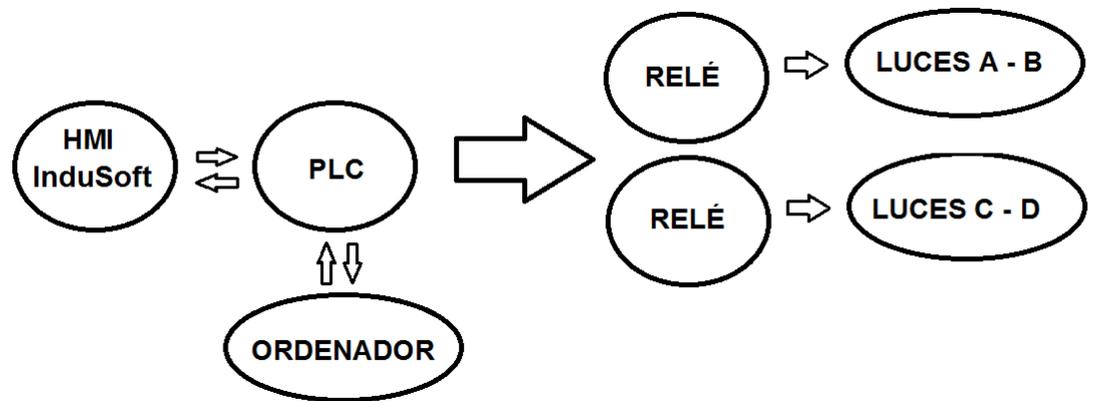


Figura 27: Representación esquema de conexión del sistema de iluminación



3.2.2 Sistema de accesos propuesto

Para dar acceso al laboratorio, se hace uso de una cerradura eléctrica luber, esta se encarga de mover el pestillo de la cerradura, el tiempo suficiente, para que el usuario pueda abrir la puerta. La activación de esta cerradura se hace por medio de la interfaz SCADA y/o HMI. En la figura 28 se observa en color rojo el área de alojamiento para dicha cerradura, en la figura 29 se muestra una representación esquemática de la conexión del actuador, a los diferentes elementos de control.

Figura 28: Diseño de puerta principal con cerradura eléctrica

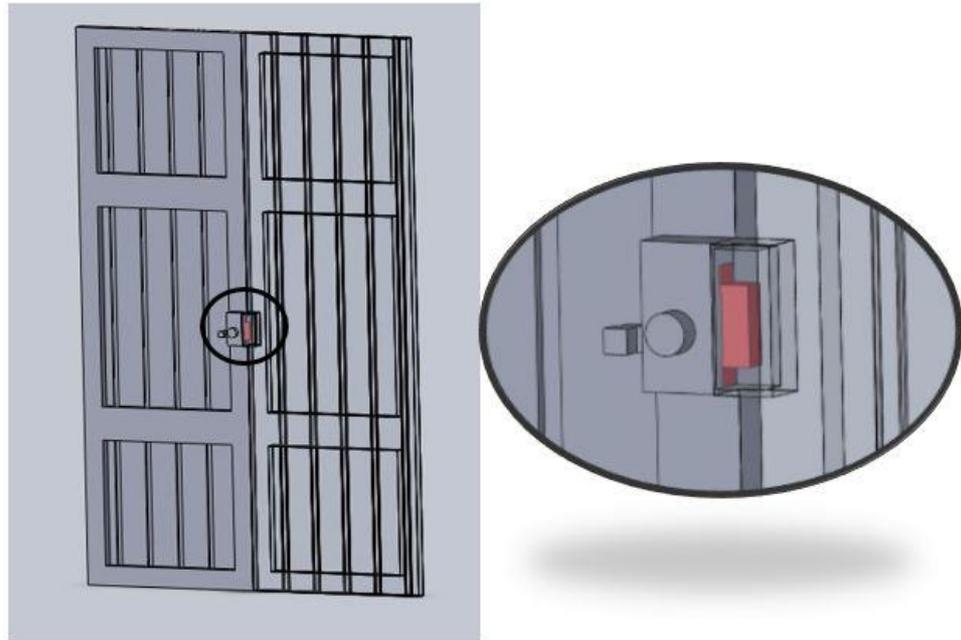
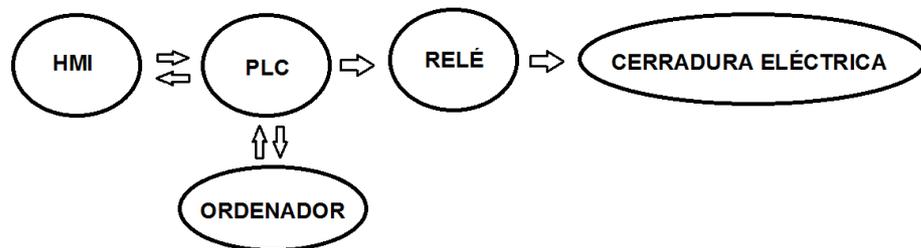


Figura 29: Representación esquema de conexión cerradura eléctrica



3.2.3 Sistema de seguridad propuesto

Como se observa en la figura 30, el sistema de seguridad propuesto consta de una serie de sensores y actuadores que permiten un monitoreo constante de las instalaciones, para ello se cuenta con un alarma general, la cual está compuesta por 2 sensores de movimiento, 2 contactos magnéticos ubicados en puertas y ventanas, un detector de humo, un detector de luminosidad y una cámara IP.

Al momento de ser activada dicha alarma, se hace una lectura de los sensores asignados, y en caso de alguna alteración, proporciona una señal de alerta por

medio de una sirena, cabe resaltar que la alarma de humo es independiente de la activación o desactivación de la alarma, sin embargo la apertura de puerta es dependiente del estado de la alarma, es decir si esta se encuentra apagada es posible abrir la puerta de lo contrario no se genera la señal de activación, dicha entrada solo sería posible con las llaves de la cerradura, pero dicha acción activaría la alarma. Por otra parte, como se observa en la figura 31, el sistema de seguridad se encuentra enlazado al HMI y al sistema SCADA, por lo tanto, es posible modificar su estado a través de estas dos interfaces

Figura 30: Distribución propuesta para el sistema de gestión y supervisión

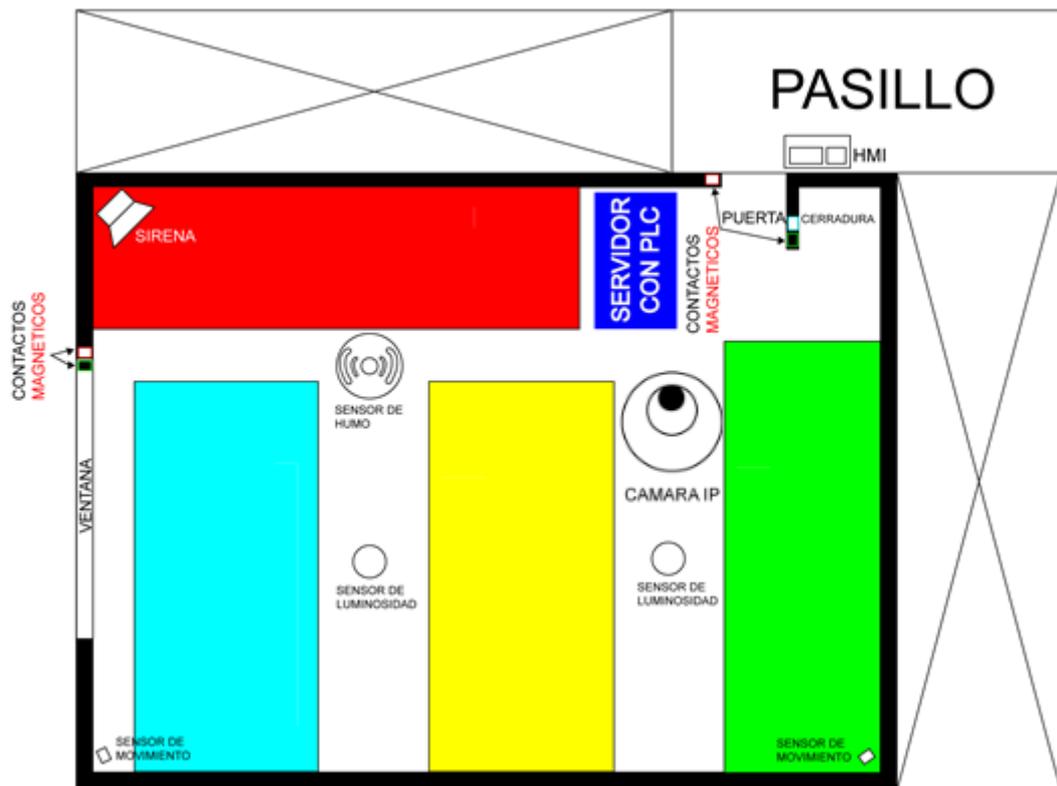
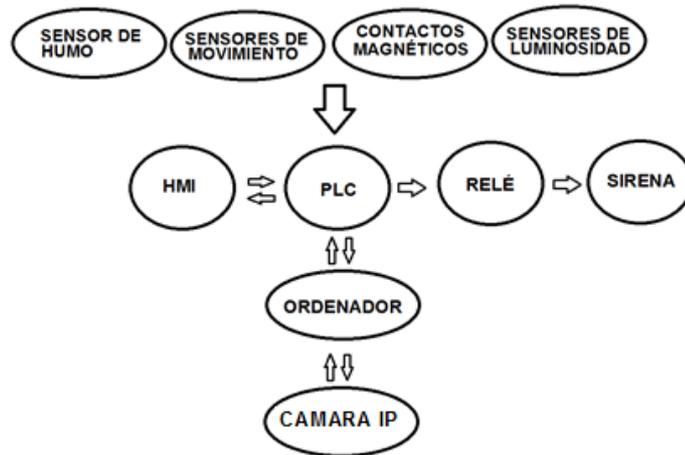


Figura 31: Representación esquema de conexión del sistema de seguridad propuesto



3.3 SENSORES Y ACTUADORES PROPUESTOS

A continuación se describen los sensores y actuadores requeridos para diseñar el sistema de iluminación

3.3.1 Sensor de luminosidad: ldr-720

Figura 32: Sensor de luminosidad LDR-720



Fuente: Copyright © 2002-2004, Reservados todos los derechos. DOMAUT (Domótica y automatización). Av. Virgen de Montserrat 124 - 08210 - Barberà del Vallès (BARCELONA) ESPAÑA Web: www.domaut.com E-mail: domaut@domaut.com

3.3.1.1 Descripción

Este sensor de luz analógico, ha sido fabricado para dar una medida precisa de la luz ambiente existente en una estancia.

Características técnicas

- Sensor de Luminosidad.
- Medidas Reducidas: 48mm x 24mm x 15mm.
- Alimentación: 12 V cc.
- Consumo Máx.: 10mA.
- Medida relativa de luz: 0 – 99.
- Salida Analógica: de 0 a +5 V.
- Temperatura de trabajo -20°C a 40°C.
- Estanco: IP65.
- Color: Blanco.

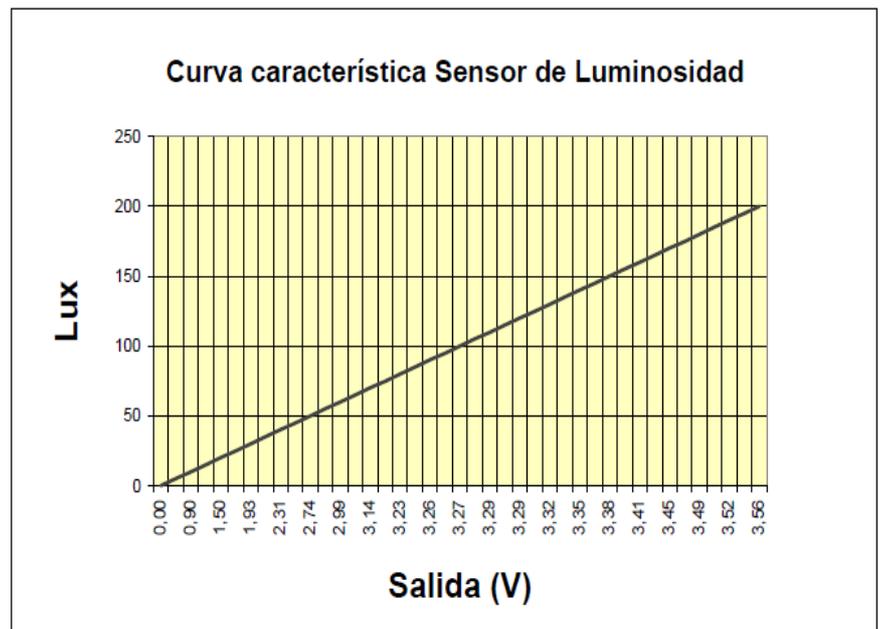
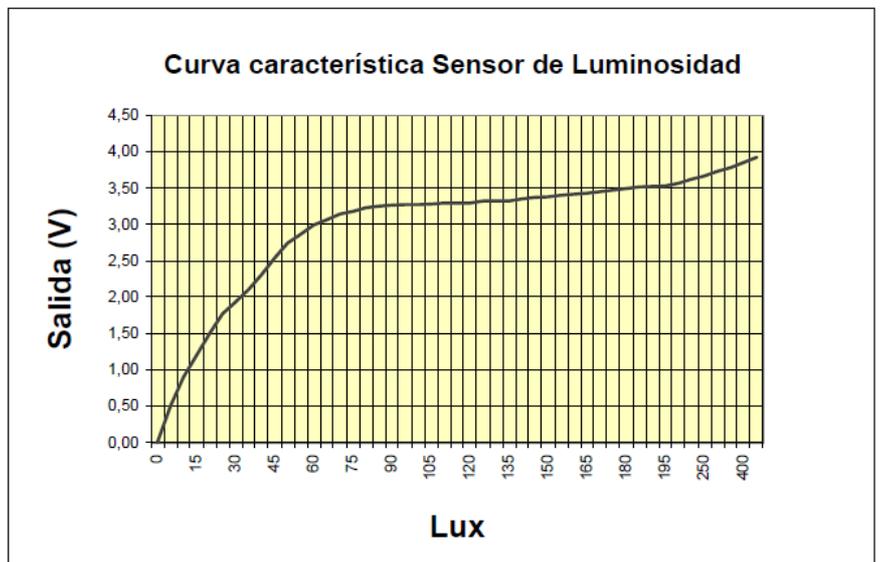
3.3.1.2 Conexiones

- ROJO: + 12V.
- NEGRO: masa.
- VERDE: Salida Analógica 0-5V.

3.3.1.4 Curva característica, sensor de luminosidad

Figura 33: Ficha técnica sensor de luminosidad

Lux	Salida (V)
0	0,00
5	0,50
10	0,90
15	1,20
20	1,50
25	1,77
30	1,93
35	2,10
40	2,31
45	2,54
50	2,74
55	2,86
60	2,99
65	3,06
70	3,14
75	3,18
80	3,23
85	3,25
90	3,26
95	3,27
100	3,27
105	3,28
110	3,29
115	3,29
120	3,29
125	3,32
130	3,32
135	3,32
140	3,35
145	3,37
150	3,38
155	3,40
160	3,41
165	3,43
170	3,45
175	3,47
180	3,49
185	3,51
190	3,52
195	3,53
200	3,56
225	3,62
250	3,66
300	3,73
350	3,78
400	3,85
450	3,92



Fuente: Copyright © 2002-2004, Reservados todos los derechos. DOMAUT (Domótica y automatización). Av. Virgen de Montserrat 124 - 08210 - Barberà del Vallès (BARCELONA) ESPAÑA Web: www.domaut.com E-mail: domaut@domaut.com

3.3.2 Detector de humo autónomo

Este detector, cuenta con tecnología de detección fotoeléctrica (detección de partículas en suspensión en el aire). Estos dispositivos están concebidos para darnos un aviso acústico del menor indicio de fuego. [64]

Cuadro 1: Ficha técnica detector de humo autónomo

DETECTOR ÓPTICO DE HUMO AUTÓNOMO. MONTAJE EN TECHO. ALARMA ACÚSTICA, SALIDA A RELÉ C/N.A/N.C. ALIMENTACIÓN DE 12 A 24VDC	Referencia: GLH-965R-24
<hr/>	
	<p>CARACTERÍSTICAS TÉCNICAS:</p> <ul style="list-style-type: none">✓ Función: Detector autónomo de humo.✓ Tipo de sensor: Óptico fotoeléctrico.✓ Destinado a viviendas, colegios, hoteles, oficinas, etc.✓ Autorearmable.✓ Alarma acústica: 85dB intermitente.✓ Alarma visual: LED rojo intermitente.✓ Instalación: un detector cada 9 metros.✓ Superficie de vigilancia: 50 - 60 m².✓ Alimentación: de 12 a 24VDC.✓ Salida a Relé: contactos C/NA/NC (1A/24VDC).✓ Temperatura de trabajo: -5 y +50°C.✓ Humedad de trabajo máx.: <90% sin condensación.✓ Dimensiones: 120mm de diámetro x 29 de alto.✓ Conexión: regleta de tornillo✓ Certificado CE. <p>CONEXIÓN RELÉ DE SALIDA:</p> <ul style="list-style-type: none">- Borna 1: Alimentación positivo (+ 12 A 24VDC).- Borna 2: Alimentación negativo.- Borna 4: Normalmente abierto. (NA)- Borna 5: Normalmente cerrado. (NC)- Borna 6: Común.

Fuente: Domaut- alarmas técnicas [En línea]. [Citado el 22 de abril de 2014]. Disponible en <http://www.domaut.com/Alarmas_tecnicas.html>

3.3.3 Detector de movimiento por infrarrojos pasivos Blue Line GEN2

Los detectores de movimiento por infrarrojos pasivos (PIR) Blue Line Gen2 (véase figura 34), usan dos lentes Fresnel diseñadas para ofrecer unas imágenes perfectamente enfocadas en todo el campo de visión, proporcionando así una mejor respuesta ante los intrusos. Estas lentes cuentan con un patrón de 7 capas de alta densidad (77 zonas); a su vez, la lente de ángulo cero seleccionable brinda tres zonas de ángulo cero adicionales. La sencilla instalación y las flexibles opciones de montaje proporcionan unas prestaciones de detección muy altas. Los modelos con identificación de mascotas (-WP), generan alarmas por intrusiones de personas sin originar falsas alarmas por mascotas. [70]

Figura 34: Sensor de movimiento BLUE LINE GEN2



Fuente: Detector de movimiento por infrarrojos pasivos Blue Line Gen2 [En línea]. [Citado el 24 de abril de 2014]. Disponible en <http://resource.boschsecurity.com/documents/BlueLine_Gen_2_Data_sheet_esES_2603228171.pdf>

3.3. 1 Especificaciones técnicas

Tabla 5: Ficha técnica sensor de movimiento

Especificaciones eléctricas	
Corriente (en reposo/alarma)	De 10 mA a 12 VCC
Tensión (funcionamiento)	De 9 a 15 VCC
Especificaciones mecánicas	
Color	Blanco
Dimensiones	105 x 61 x 44 mm (4,2 pulg. x 2,4 pulg. x 1,7 pulg.)
Material	Plástico ABS a prueba de fuertes impactos
Inmunidad contra interferencias por Radiofrecuencia (RFI)	En el rango de frecuencias críticas de 150 kHz a 2 GHz con fuerzas de campo inferiores a 30 V/m.
Salidas	
Relé	Contactos de estado sólido supervisados de tipo A, normalmente cerrados (NC) y preparados para ≤ 100 mA, 25 VCC, 2,5 W, < 20 ohmios cerrados
Sabotaje	Contactos normalmente cerrados (NC) (con la cubierta colocada) preparados para ≤ 100 mA, 25 VCC, 2,5 W Conecte el circuito antisabotaje a un circuito de protección de 24 horas.

Fuente: Domaut- alarmas técnicas [En línea]. [Citado el 22 de abril de 2014]. Disponible en <http://www.domaut.com/Alarmas_tecnicas.html>

3.3.4 Contacto Magnético fijación adhesivo GL-38B

Figura 35: Contacto magnético GL-38B



Fuente: Contacto Magnético fijación adhesivo [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.elinstaladorelectricista.es/default/domotica-2/material-domotico/gl38b-contacto-magnetico-fijacion-adhesivo-o-tornillos-puertas-y-ventanas.html>>

Dichos contactos pueden ser instalados en un montaje en superficie, por medio de fijación adhesiva o mediante tornillo en el caso de puertas y ventanas (de madera, PVC, aluminio, etc).

3.3.4.1 Características gl-38b

- Reducido tamaño:
- Dimensiones contacto: 27 mm de ancho x 14 mm fondo x 8 mm alto
- Dimensiones imán: 27 mm de ancho x 14 mm fondo x 8 mm alto
- Carcasa plástica de color blanco
- Contacto normalmente abierto (al acercar el imán el contacto se cierra y al retirarlo el contacto se abre)

- Distancia de actuación $\leq 18\text{mm}$.
- Carga máxima del contacto magnético: 100VDC/0,5A.
- Longitud del cable suministrado 30 Cm, 2 hilos
- Temperatura de trabajo: -40 a +80°C
- Protección: IP45 [71]

3.3.5 Cámara IP

La cámara IP se conecta, a través de una de las tecnologías de comunicación inalámbrica mediante ondas, la cual es una de las más utilizadas hoy en día. (WI-FI), también llamada WLAN (Wireless LAN, red inalámbrica) o estándar IEEE 802.11. [72]

En la figura 36 se observa una cámara robótica (IP DVR H264), la cual se puede conectar de forma inalámbrica. Haciendo uso del router disponible en los laboratorios de Mecatrónica.

Se configura la cámara IP para posibilitar el acceso desde el ordenador seleccionado, una vez hecho esto es posible acceder desde el indusoft a la cámara, a través de un control ActiveX, configurado con la dirección entregada por la cámara.

Figura 36: Cama IP Dvr, H.264



Fuente: Cámara IP DVR [En línea]. [Citado el 24 de abril de 2014]. Disponible en <http://articulo.mercadolibre.com.co/MCO-410291311-camara-ip-robotica-dvr-h264-nocturna-ranura-microsd-wifi-_JM>

3.3.5.1 Características generales

- Visión nocturna: Tecnología de 11 Leds infrarrojos, para no perder detalle de lo que acontezca aun en total oscuridad hasta 10 metros.
- Wi-Fi: Tecnología inalámbrica plug and play. Solo basta configurar la red WIFI a la cámara para tener acceso a través de internet.
- Resolución de video: Res. De 640x480
- Encriptación y acceso seguro: Está protegida con WEP, WAP o WAP2. Además cuenta con 3 niveles de seguridad: Administrador (ingreso y configuración), operador (ingreso y manipulación de movimientos) y visitante (solo ingreso para monitorizar)
- Notificación de movimiento detectado: Alarma vía email y/o disparo de grabación.
- Movimiento rotatorio: Movimientos controlados de 270° x 90°.[73]

3.3.6 Cerradura eléctrica LUBER

En la figura 37, se observa una cerradura eléctrica LUBER, esta permite conmutar el pestillo de la puerta principal.

Figura 37: Cerradura eléctrica LUBER



Fuente: Destradores eléctricos [En línea]. [Citado el 24 de abril de 2014].
Disponibile en < http://www.lubercerraduras.com.ar/cerraduras_electricas.php>

3.3.6.1 Características generales

- De 8 a 12 Volts CA - 1 Amper
- Sistema bobina doble
- Componentes: Doble traba, caja de acero niquelado
- Traba, palanca y gatillo
- Frente: Acero de 2,5 mm.
- Bronce de 2,5 mm pulido o niquelado
- Agujeros de fijación: 2 – 4. [74]

3.3.7 Sirena multitonal WM 4 tonos 12-24VDC

En la figura 38, se observa una sirena multitonal WM, esta cuenta con el número de decibles necesarios, para dar aviso de cualquier anomalía dentro de los laboratorios, además de un voltaje que se ajusta al rango de operación del PLC.

Figura 38: Sirena multitonos WM 4 tonos



Fuente: Sirena multitonos WM 4 tonos 12-24VDC [En línea]. [Citado el 24 de abril de 2014]. Disponible en https://www.werma.com/es/s_c1003i46/Sirena_multitonos_WM_4_tonos_12-24VDC_GY/12605215.html

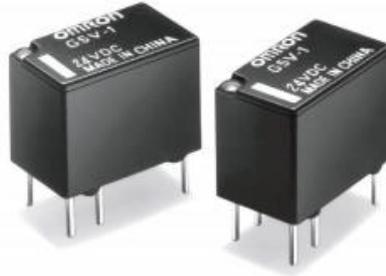
3.3.7.1 Características generales

- Tensión: 12 - 24V CC
- Volumen: 100-105dB
- Tipo de sonido: 4 tonos
- Fijación: Montaje en un tubo
- Diámetro: 70 mm
- Intensidad absorbida: 80 mA
- Rango de temperaturas: -20°C...+50°C
- Tipo de sonido: Tonos
- Frecuencia sonora: ca. 530 - 2700 Hz
- Material de la carcasa: ABS [75]

3.3.8 Relé PCB G5V-1

En la figura 39, se observa un relé G5V-1, el cual es conmutable a 24 VDC y cuenta con los atributos necesarios, para ser acoplado al sistema eléctrico del laboratorio.

Figura 39: Relé PCB G5V-1



Fuente: OMRON PCB Relay [En línea]. [Citado el 24 de abril de 2014]. Disponible en < <http://www.micropik.com/PDF/g5v1.pdf>>

- ❖ En la tabla 6 se observan las características principales de este relé.

Tabla 6: Ficha técnica relé G5V-1

Rated voltaje	24 VDC
Rated current	6.25 mA
Coil resistance	3,840 Ohms
Rated load	0.5 A at 125 VAC; 1 A at 24 VDC
Rated carry current	2 A
Max. switching voltage	125 VAC, 60 VDC
Max. switching current	1 A
Max. switching power	62.5 VA, 30 W

Fuente: OMRON PCB Relay [En línea]. [Citado el 24 de abril de 2014]. Disponible en < <http://www.micropik.com/PDF/g5v1.pdf>>

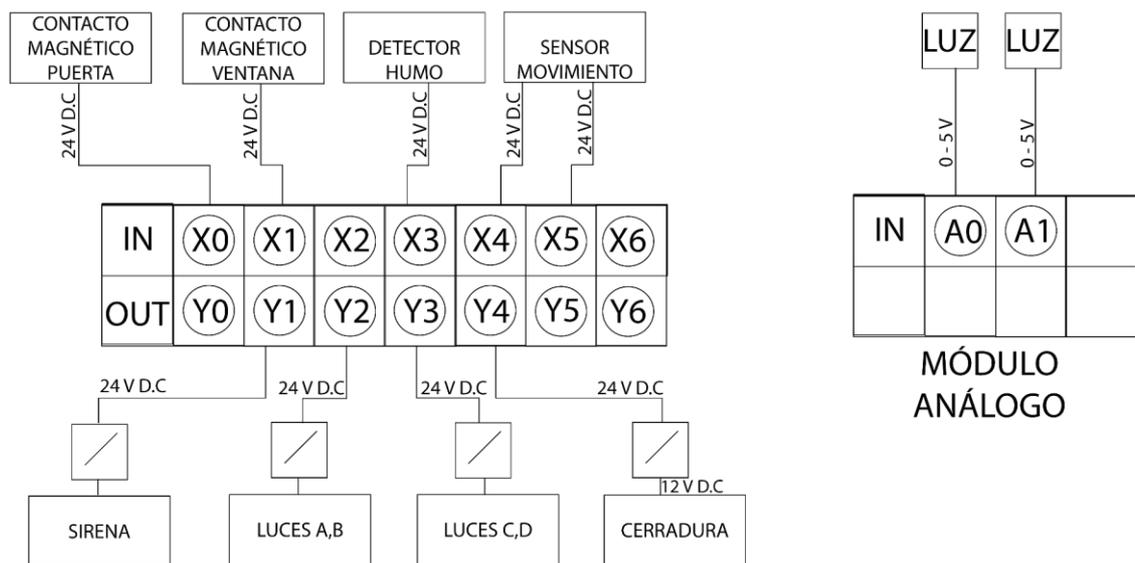
3.4 PROPUESTA PROGRAMACIÓN DE PLC

A continuación, se describen todas las entradas y salidas asignadas a los diferentes sistemas, así como, las respectivas direcciones asignadas al PLC en la figura 40, se observa las entradas y salidas conectadas al PLC, para su posterior implementación en la programación. Además, se describe la forma en la cual se debe establecer la comunicación entre el un autómata programable y el ordenador.

La comunicación del PLC THINGUET XC3-32r-c hacia el ordenador se hace de forma serial, mediante el estándar RS232, usando un conector mini-DIN 8 Core, acoplado a un conector DB9.

Una vez realizada la comunicación del PLC con el ordenador, se posibilita su programación, para esto se hace uso del software XCPPro Series Program Tool. Version 3.3, el cual, permite hacer uso de los lenguajes estandarizados de programación, como: KOP y/o también llamado LADER; este programa también tiene disponible una opción para ser ejecutado “en tiempo real”, brindando una perspectiva, de lo que está sucediendo con el PLC en cada línea de código.

Figura 40: propuesta conexión sensores y actuadores al PLC



3.4.1 Programación sistema de luces

Para dar comienzo a la programación del sistema de iluminación, se debe hacer referencia a las entradas y salidas que intervienen en este, así como, su respectiva adecuación. Dado que los dos sensores de luminosidad que serán usados son de tipo analógico de 0 a 5v, es necesario usar un módulo analógico conectado al PLC.

3.4.1.1 Modulo analogico

Para este modelo, el modulo analogo es una expansion, que se conecta, por medio de un BUS de datos a el PLC, como se observa en la figura 45.

Figura 41: Modulo analogico THINGUET XC3-32r-c



Fuente: Xinje XC Series PLC [En línea]. [Citado el 24 de abril de 2014]. Disponible en http://www.fasttobuy.com/xinje-xc-series-plc-io-expansion-analog-module-xce4ad2da-4channel-14bits-precision-analog-input-2channel-12bit-precision-analog-output-new-free-shipping_p25825.html

3.4.1.2 Entradas y salidas, sistema de luces

A continuacion se describen las entradas y salidas usadas, asi como su direccion dentro de el PLC y el software XcPR0

Tabla 7: Entradas y salidas del PLC thinget sistema de luces

ITEM	ENTRADA/SALIDA	DESCRIPCIÓN
1	ID 100	Sensor análogo de luminosidad 1
2	ID 101	Sensor análogo de luminosidad 1
3	Y2	Salida relé de encendido lámparas A,B
4	Y3	Salida relé de encendido lámparas C,D

5	M16	Memoria interna del PLC encendido total
6	M23-M25	Memoria interna del PLC encendido parcial
7	M19	Apagado sistema de iluminación
8	M24-M26	Apagado parcial de las luces

3.4.1.3 Descripción de programación para el sistema de luces

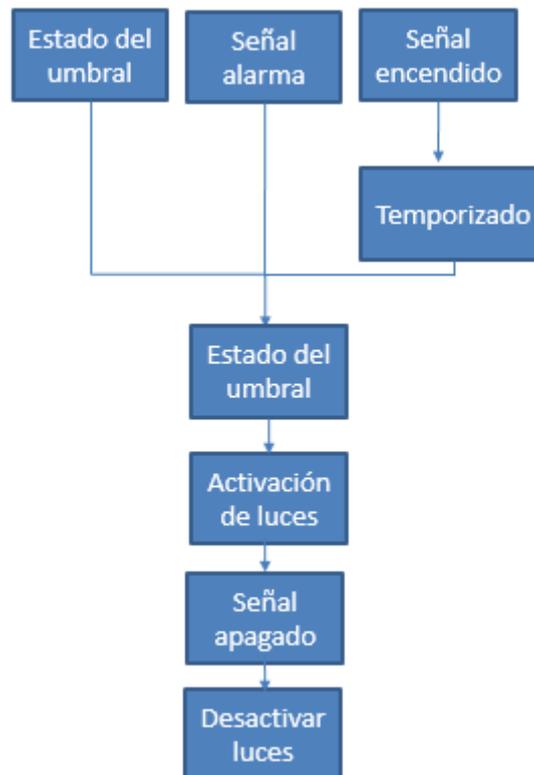
Para dar inicio al ladder, primero, se hace referencia a los dos sensores de luminosidad, correspondientes a la entrada 0 y 1 del modulo analogo, estos se nombran, como una entrada de tipo MOV, seguido de la direccion del puerto analogico y la variable que tendra dicha entrada.

El encendido total del sistema (todas las lámparas), se puede llevar a cabo a través de las memorias del PLC M16 y M19 asignadas al sistema SCADA y el HMI (véase figura 46), sin embargo, cuando la luminosidad en los sensores se encuentra por debajo de un valor de umbral “K” previamente definido, también da inicio al arranque temporizado del sistema de iluminación, en el cual se encienden las lámparas A,B y 5 segundos después C y D, Así mismo, al momento de hacer el apagado del sistema, es posible acceder a la memoria M19, enlazada con las dos interfaces, pero también es posible un apagado automático cuando la luminosidad en el entorno es demasiado alta.

Es posible tambien tener un inicio y/o apagado parcial de el sistema de iluminacion, dividido en dos sectores A,B y C,D , estas opciones se encuentran disponibles tanto en el HMI como en el sistema SCADA, a traves, de las memorias de el PLC M23 y M25.

Una vez las memorias de activacion son asignadas, estas son llevadas a las bobinas de salida identificadas como Y2 y Y3 respectivamente, estas salidas van directamente a lo relés que realizan la labor de intervención, de la red electrica de el laboratorio, (véase ANEXO D), en la figura 42 se observa un diagrama de flujo que muestra una visión general de la estructura de programación.

Figura 42: Esquema de programación sistema de iluminación



3.4.2 Descripción de programación para el sistema de acceso

Para la programación de la apertura de la puerta, no es necesario el uso de ningún sensor físico, sin embargo, se tiene en cuenta a manera de seguridad, el contacto magnético, ubicado en la parte superior de la puerta, en aras de garantizar, que no hallan falsas conmutaciones.

3.4.2.1 Tabla de entradas y salidas

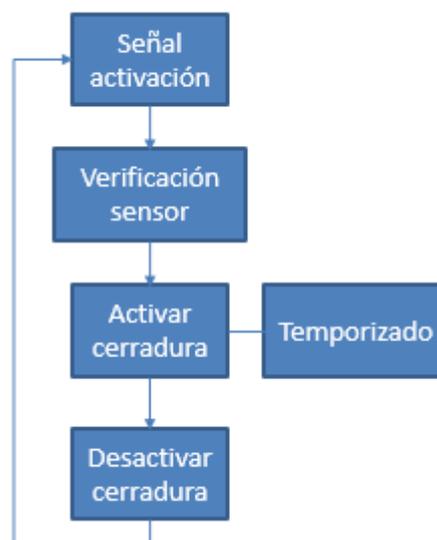
Tabla 8: Entradas y salidas del PLC thinget sistema de acceso

ITEM	ENTRADA/SALIDA	DESCRIPCIÓN
1	X0	Contacto magnético puerta
2	M14	Memoria PLC desde el HMI
3	M27	Memoria PLC desde el SCADA
3	Y4	Salida relé cerradura eléctrica

La entrada digital X0 de el PLC, se encuentra conectada al contacto magnetico ubicado en la puerta principal de el laboratorio,La apertura de la puerta es posible, a través, de las memorias de PLC M14 y M27, correspondientes a señales provenientes del HMI y el SCADA respectivamente, estas activan la cerradura y a su vez un temporizador T2 que desconecta la cerradura 3 segundos después de su activación, para dar tiempo al usuario de abrir la puerta. Cabe resaltar que la puerta solo puede ser abierta si el contacto magnético se encuentra cerrado y la alarma general se encuentra desactivada.

La señal de activación y desactivación, de la apertura de puerta, es dirigida a la bobina Y4, esta se encuentra enlazada directamente con la cerradura LUBER, (véase ANEXO D) , en la figura 43 se observa un diagrama de flujo que muestra una visión general de la estructura de programación.

Figura 43: Esquema de programación sistema de acceso



3.4.3 Descripción de programación para el sistema de seguridad

A continuación, se describe la programación de la alarma general para el laboratorio de automatización, esta hace uso de los contactos magnéticos y los sensores de movimiento, para determinar cualquier posible acceso sin autorización al área de trabajo, la señal de alerta se proporciona a través de una sirena.

3.4.3.1 Tabla de entradas y salidas

Tabla 9: Entradas y salidas del PLC thinget sistema de seguridad

ITEM	ENTRADA/SALIDA	DESCRIPCIÓN
1	X0	Contacto magnético puerta
2	X1	Contacto magnético ventana
3	X3	Detector de Humo
3	X4	Sensor de movimiento 1
4	X5	Sensor de movimiento 2
5	ID 1000	Entrada análoga sensor de luminosidad 1
6	ID 101	Entrada análoga sensor de luminosidad 2

7	M0-M1	Memorias de activación asignadas al SCADA y el HMI
8	M3-M4	Memorias de desactivación asignadas al SCADA y el HMI
9	Y1	Salida a sirena
10	Y2	Salida relé de luces A,B
11	Y3	Salida relé de luces C,D

Para proporcionar un sistema de seguridad “confiable”, se hace uso de los diferentes sensores enlazados a el PLC, conectados a la entradas digitales X0,X1,X3,X4,x5 (vease figuras 53, 54) y para mayor seguridad, se complementa el sistema, con el uso de los sensores analógicos ID100 y ID101.

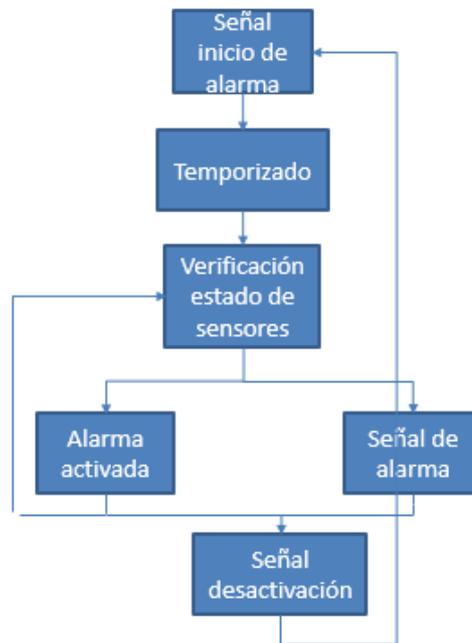
La alarma general del laboratorio, es activada mediante las memorias M0 y M1, estas señales provienen de la interfaz SCADA y HMI respectivamente. Así mismo, las memorias de desactivación de la alarma se designan como M3 y M4

Una vez la señal de activación es proporcionada, se da inicio a un temporizador T2 cuyo objetivo, es proporcionar tiempo al usuario, para salir del recinto sin activar la alarma, el siguiente paso consiste en una verificación de todos los sensores involucrados, para determinar si se encuentran en correcto estado, la condición para esto sería de la siguiente forma: Si el Contacto de puerta y venta se encuentra proporcionando señal y la luminosidad se encuentra por debajo de un rango K (luces apagadas), entonces la alarma es activada, de lo contrario, un indicador proporciona una señal de aviso, a través de la memoria M7

Cuando la verificación del estado inicial de los sensores es correcta, la alarma pasa a activarse, aquí cualquier cambio en uno o varios sensores hacen que la señal de alarma M13 sea activada.

Cuando la memoria de alarma es activada, se excitan las bobinas Y1, Y2, Y3. Cabe resaltar, que la activación de estas 3 salidas se da en paralelo, con la activación del detector de humo, ya que esta señal de aviso debe ser independiente del estado de la alarma, (véase ANEXO D), en la figura 44 se observa un diagrama de flujo que muestra una visión general de la estructura de programación.

Figura 44: Esquema de programación sistema de seguridad



3.5 PROPUESTA PROGRAMACIÓN HMI

El HMI THINGET 0P 320-A, se conecta mediante el estándar RS232, usando un conector DB9, esta conexión debe realizarse, según especificación del manual de la siguiente manera, (ver figura 45 y 46).

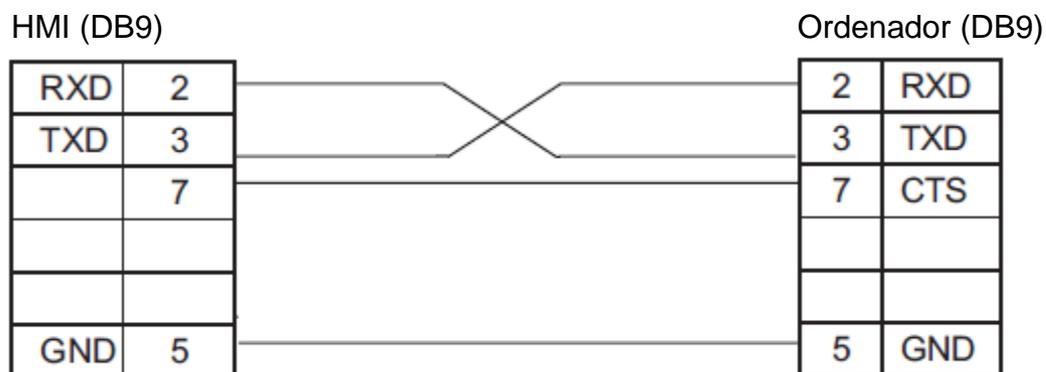
Figura 45: Pines DB9

Pin ID	Definition
1	TD+
2	RXD
3	TXD
4	
5	GND
6	TD-
7	
8	RD-
9	RD+

Fuente: OP series display, xinje Electronic Co. Ltd [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.imenista.com/pdf/OPManual.pdf>>

Figura 46: Conexión HMI – Ordenador

OP-SYS-CAB conexión grafica



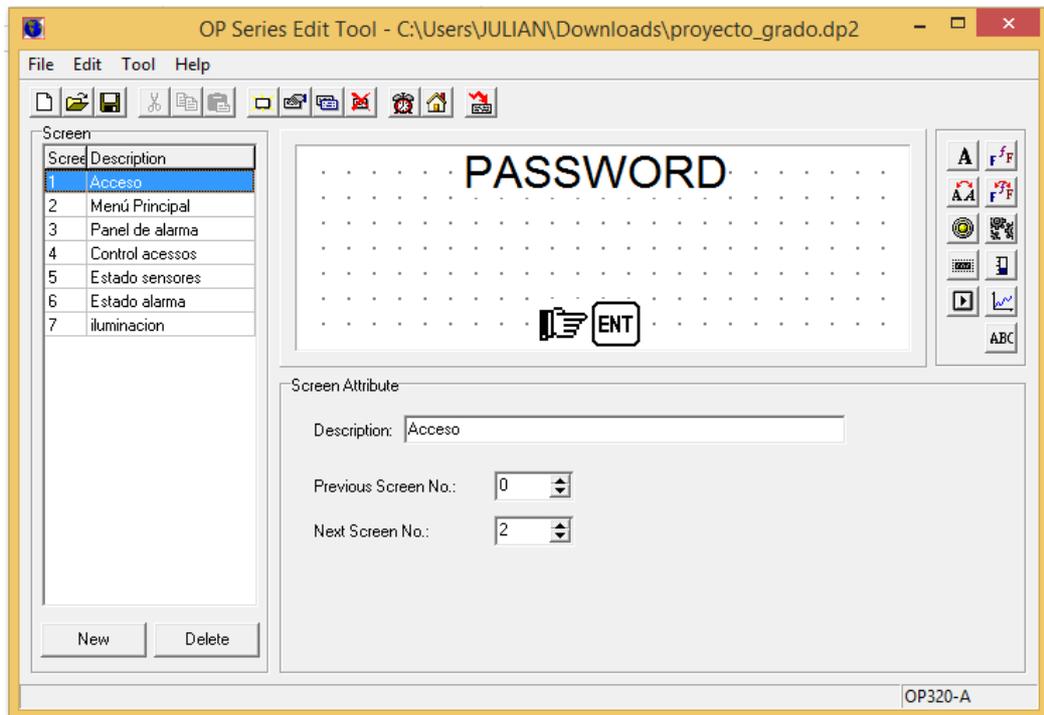
Fuente: OP series display, xinje Electronic Co. Ltd [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.imenista.com/pdf/OPManual.pdf>>

❖ Nivel de acceso

Al realizarse la conexión con el ordenador, se posibilita el vínculo del driver con el dispositivo, dando paso a la programación de la interfaz y posibilitando la asignación de las variables, en aras de mantener un nivel de seguridad alto, antes de acceder al HMI, se activó la opción de contraseña, la cual solo permite

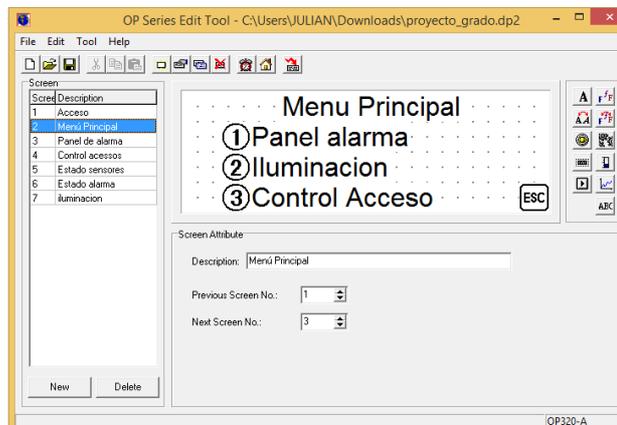
el acceso a las diferentes ventanas del menú. Al haber validado la contraseña, ver figura 47.

Figura 47: Venta inicial del HMI, solicitud de contraseña



Al momento de validar la contraseña, inmediatamente es desplegada la ventana del menú principal, ver figura 48, mostrando las diferentes opciones programadas previamente en el PLC.

Figura 48: Ventana del menú principal del HMI



❖ Asignación de memorias de programa

- Encendido total: Hace referencia a un inicio temporizado de todos los tubos fluorescentes que conforman el laboratorio, encendiendo primero las luces A, B y después de determinado tiempo las luces C, D.
- Encendidos parcial A, B, C, D: Aquí se puede encender el sistema por sectores, en la distribución mencionada anteriormente.
- Apagado total: En esta opción se apaga completamente el sistema de iluminación, incluyendo cada uno de los sectores.

Figura 50: Menú principal del HMI desde software OP Series Edit Tool con énfasis en la iluminación.

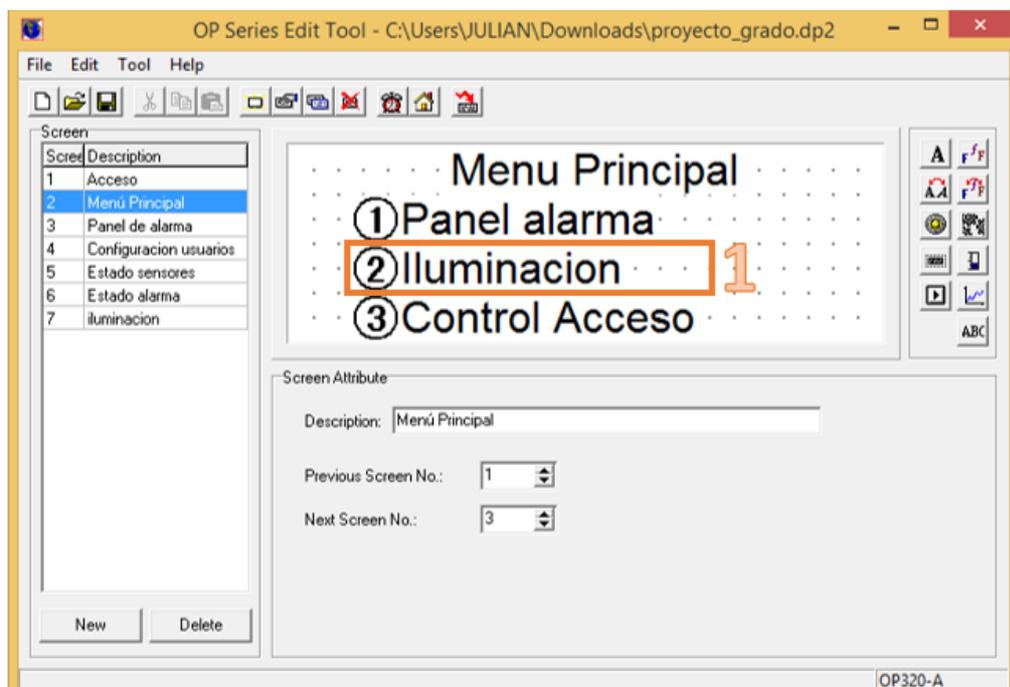
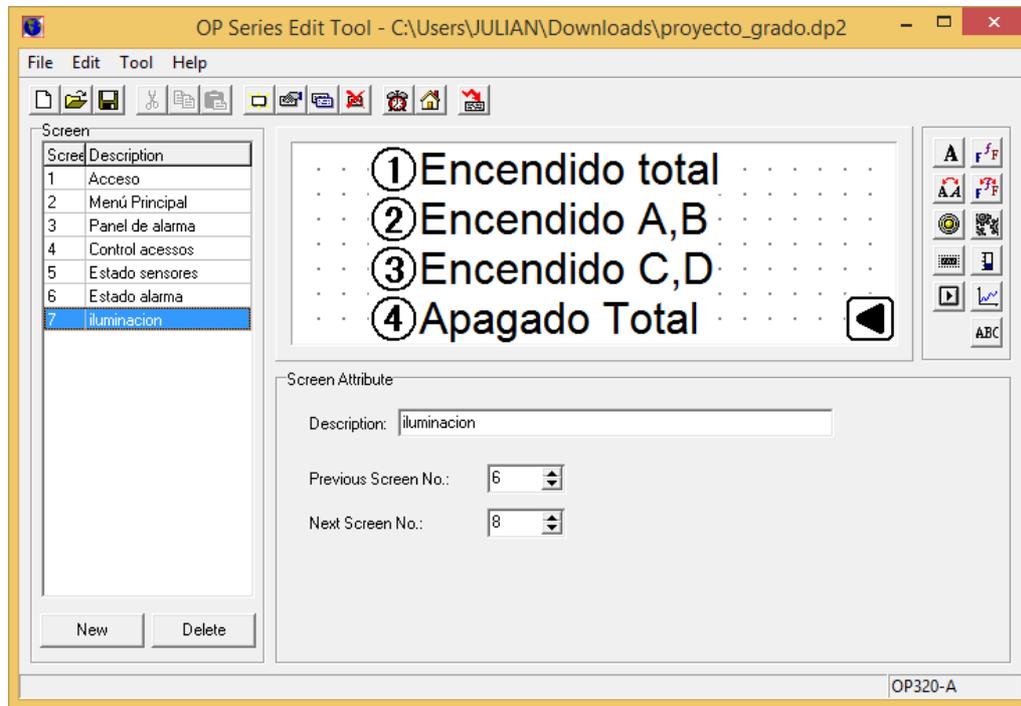


Figura 51: Menú de control del sistema de iluminación en OP Series Edit Tool



3.5.2 Sistema de accesos desde HMI

El control de acceso, se encuentra en la ventana principal del HMI, basta con dirigirse al menú principal (ver figura 52) y seleccionar la opción "3", esta opción direcciona a una ventana, donde se puede acceder a 2 funciones del sistema de acceso, distribuidas de la siguiente forma (véase figura 53).

❖ Puerta principal

- Estado: Esta opción permite a través del cambio de estado de un piloto, conocer la condición en el que se encuentra la cerradura eléctrica (Encendido/apagado).
- Abrir: Esta opción, permite acceder a una posición de memoria a través de la activación de un botón, posibilitando la apertura de la puerta.

Figura 52: Menú principal del HMI con énfasis en el control de accesos

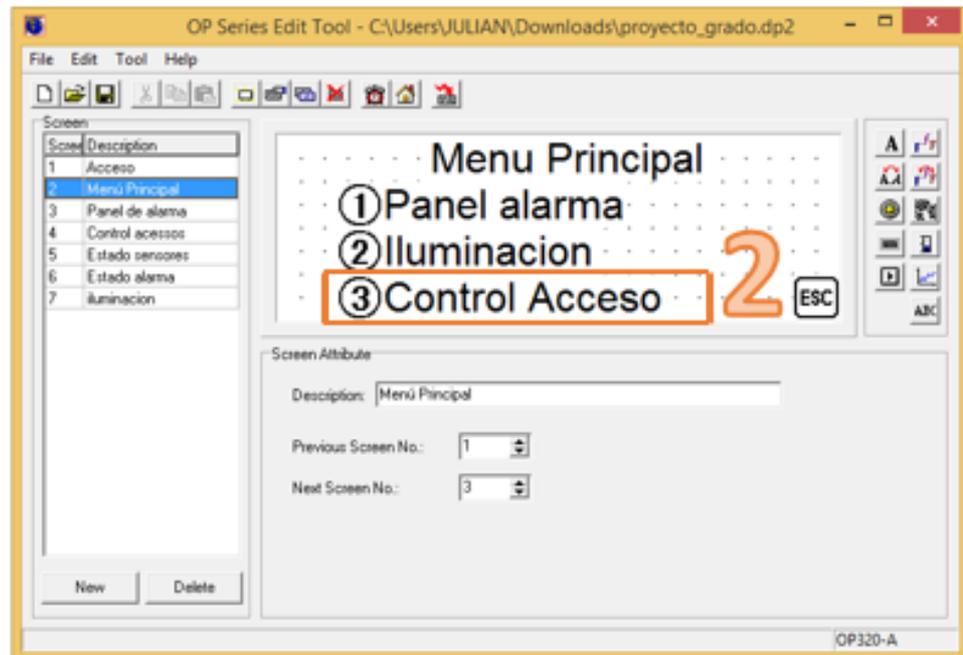
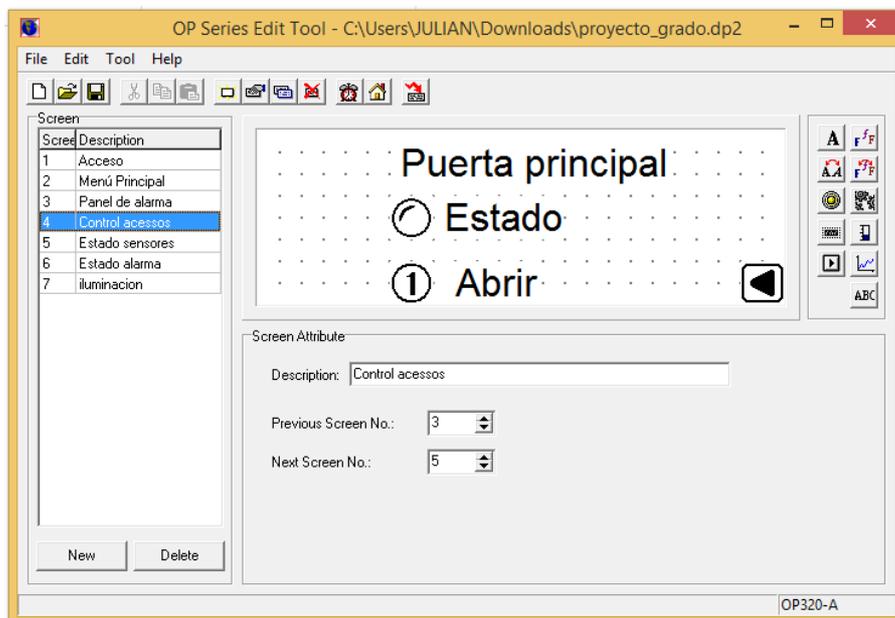


Figura 53: Ventana de la puerta principal en el HMI



3.5.3 Panel de alarma desde HMI

El panel de alarma, se encuentra en la ventana principal del HMI, basta con dirigirse al menú principal y seleccionar la opción "1" (véase figura 54), esta opción direcciona a una ventana, donde se puede acceder a 4 funciones del panel de alarma, distribuidas de la siguiente forma (ver figura 55).

- Activar alarma: El botón 1 activa la memoria encargada de la alarma general
- Desactivar alarma: El botón 2 permite la desactivación del enclavamiento de la memoria de activación, de la alarma general
- Estado de sensores: El botón 4, despliega una ventana que contiene el estado de los sensores, permitiendo el cambio de estado de un piloto, dando a conocer la condición en el que se encuentran los contactos magnéticos correspondientes a puerta y ventana (Abierta/Cerrada) , ver figura 56
- Estado de alarma: El botón 4, despliega una ventana que contiene el estado de la alarma y la sirena , permitiendo el cambio de estado de un piloto, dando a conocer la condición en el que se encuentra las memorias asignadas (Encendido/apagado), ver figura 57.

Figura 54: Menú principal del HMI con énfasis en el panel de alarma general

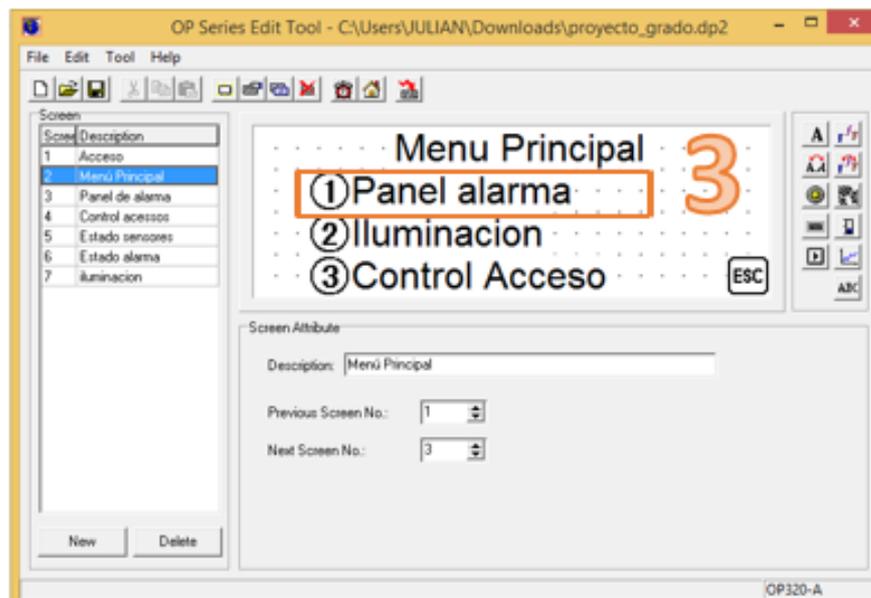


Figura 55: Ventana del panel de alarma general

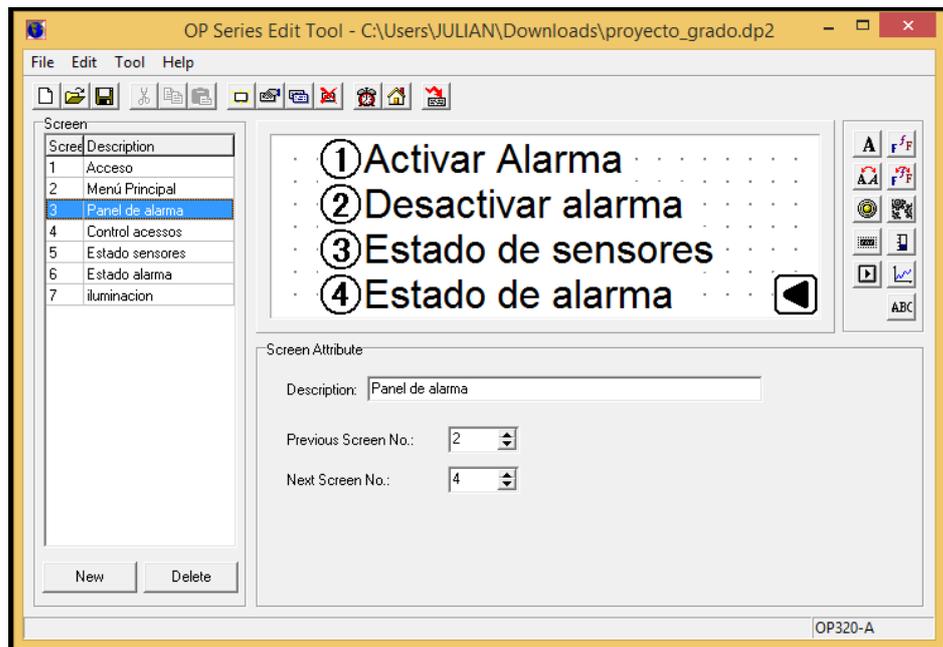


Figura 56: Ventana de estado de contactos magnéticos de puerta y ventana

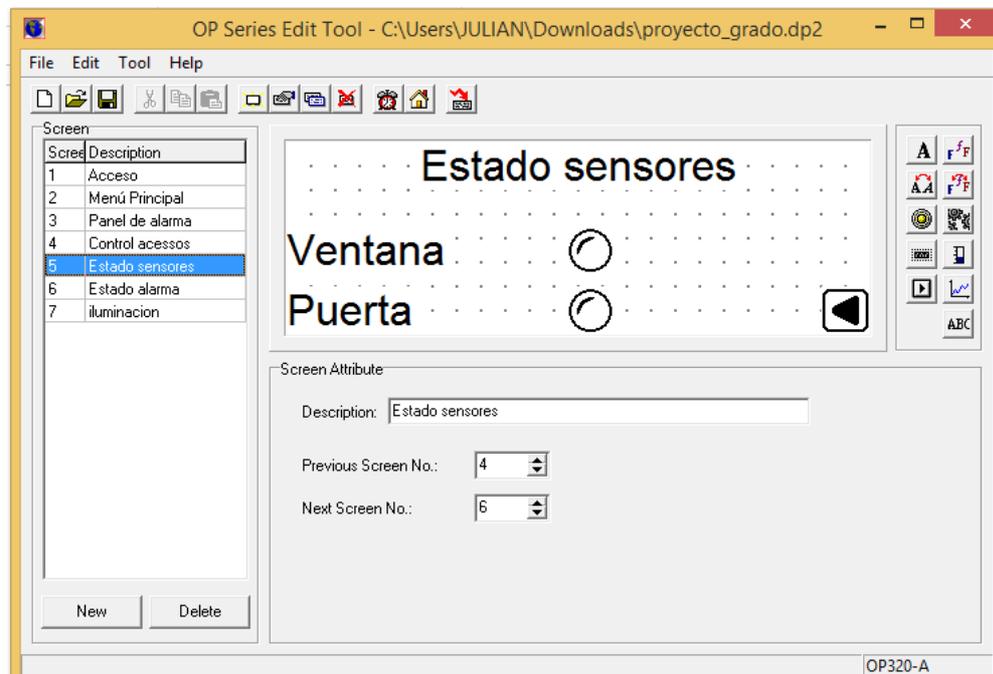
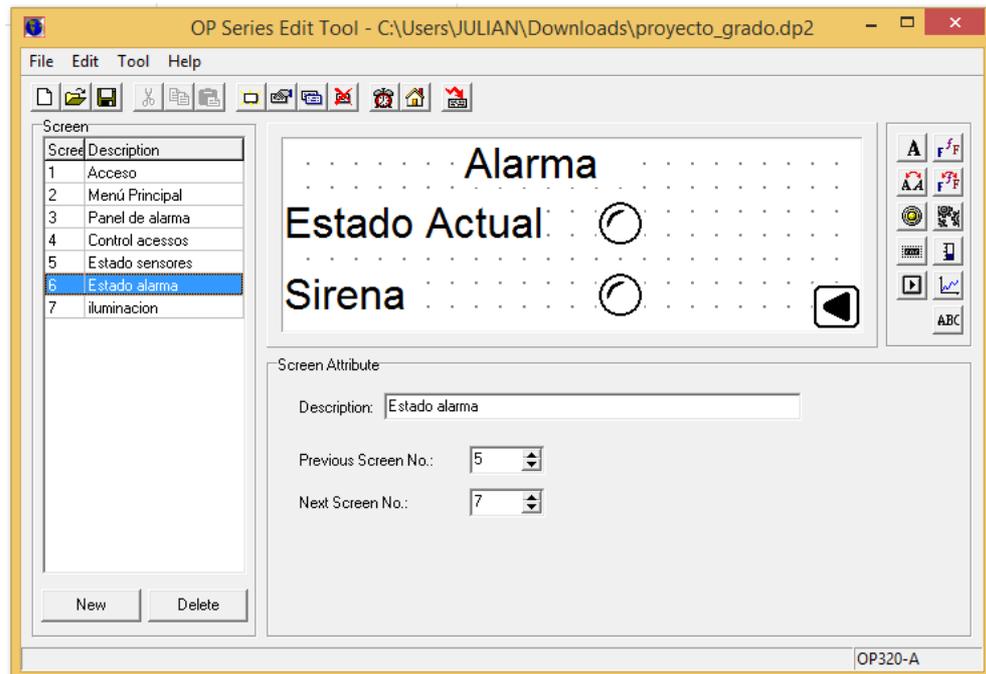


Figura 57: Ventana de estado la alarma general y señal de la sirena



3.6 PROPUESTA INTERFAZ SCADA

La conexión desde InduSoft web Studio, se hace a través del protocolo MODBUS, este especifica el procedimiento que el controlador y el esclavo utilizan para intercambiar datos, el formato de estos datos, y como se tratan los errores. Este protocolo no especifica estrictamente el tipo de red de comunicaciones a utilizar, por lo que se puede implementar sobre redes basadas en Ethernet, RS-485, RS-232 etc. Para este caso específico el PLC se conecta al ordenador a través de RS232.

MODBUS funciona siempre en modo maestro-esclavo (cliente - servidor), siendo el maestro (cliente) quien controla en todo momento las comunicaciones con los esclavos, Los esclavos (servidores) se limitan a retornar los datos solicitados o a ejecutar la acción indicada por el maestro. En la figura 58 se observa una representación gráfica de esta conexión. [69]

Una vez establecido el protocolo, es necesario asignar las entradas y salidas provenientes del PLC a TAG'S del sistema, cuando estos se hayan comprobado correctamente, se puede hacer uso de ellos en todo el proyecto.

Para realizar esta operación, se debe dirigir a la ventana de comunicación en la opción de "insertar Drivers" y allí seleccionar la opción "MODBU", una vez este haya sido agregado, se debe configurar con el respectivo puerto del ordenador

que se está usando, por último, en la hoja principal del driver se mencionan las diferentes memorias del PLC, teniendo en cuenta que: la memoria M0, comienza en la dirección 0X:1, esto quiere decir que la memoria M1, corresponde a 0X:2; y así sucesivamente con el número de memorias que se tengan (véase figura 59).

Figura 58: Representación gráfica esquema de conexión InduSoft Web Studio con el PLC

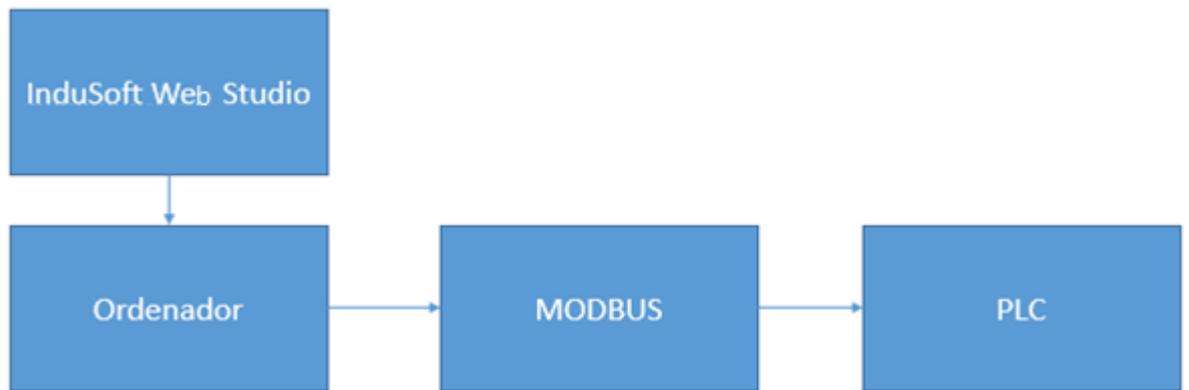
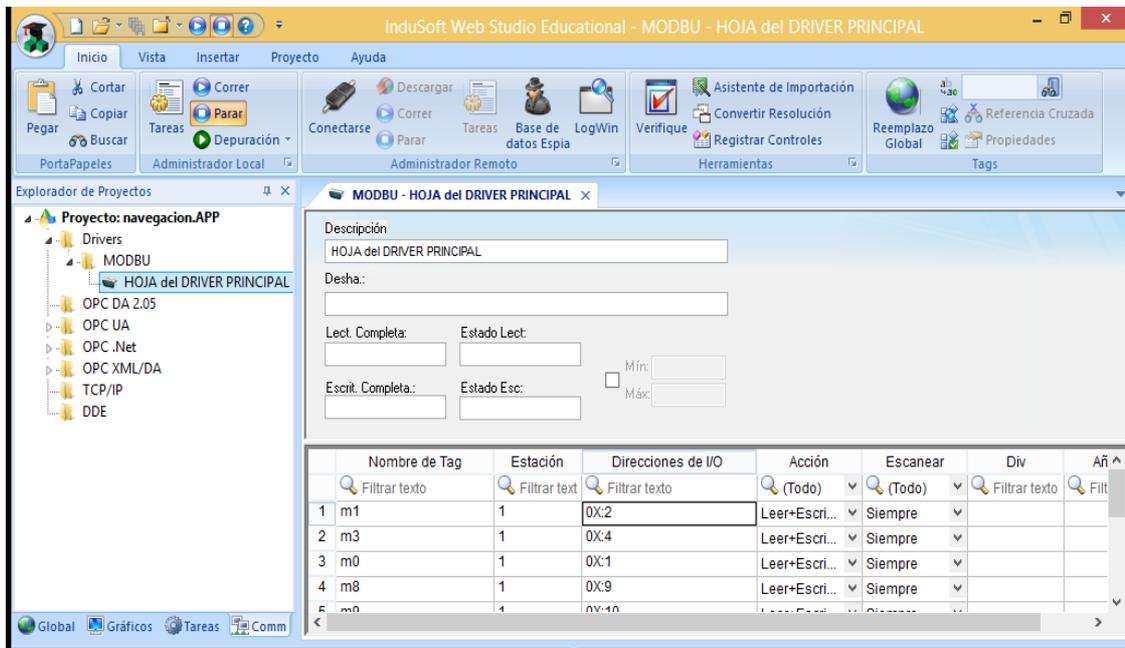


Figura 59: Hoja del Driver MODBUS en InduSoft Web Studio



Como se observa en la figura 60, La interfaz SCADA diseñada cuenta principalmente con una cabecera y un panel de navegación, que permiten recorrer todo el sistema, estas dos se encuentran distribuidas de la siguiente forma:

- (1) En este espacio se encuentra información general, datos como, la fecha, el nombre de usuario con el que se accedió al sistema y su respectivo nivel de seguridad.
- (2) El botón de inicio, se enlaza con una página que contiene toda la información requerida, para usar de forma correcta la interfaz.
- (3) El botón préstamo, proporciona acceso al sistema de gestión, es decir, es la ventana que permite realizar la solicitud de préstamo, de los diferentes componentes que se encuentran en el laboratorio.
- (4) El enlace de supervisión, proporciona un enlace directo con la cámara IP
- (5) En la ventana de control y acceso, se tiene acceso a un plano del laboratorio de Mecatrónica, el cual cuenta, con todos los botones necesarios para interactuar con este.
- (6) Este botón, es un enlace directo con el blog del semillero de investigación Mecabot.
- (7) En este enlace, es posible otorgar y quitar privilegios a un usuario en particular, con el fin de permitir o denegar el acceso a determinadas áreas.
- (8) Aquí, se encuentran los botones cierre de sesión y la salida del modo Runtime

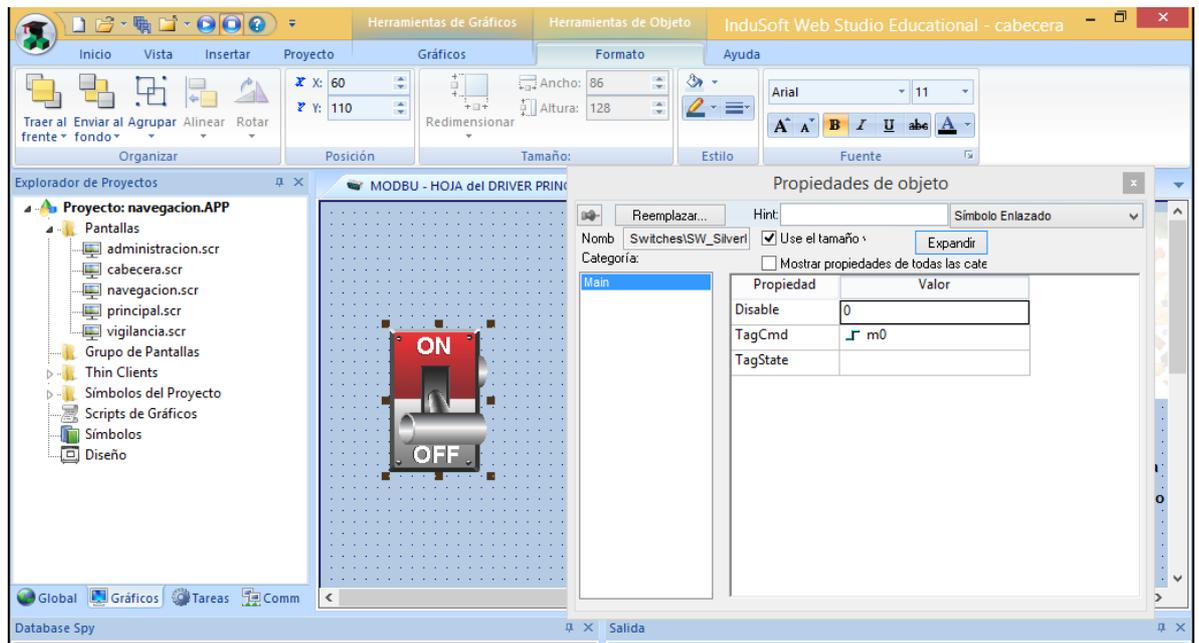
Figura 60: Vista general de la interfaz diseñada para el sistema de gestión y supervisión



3.6.1 Entorno sistema de luces

El software InduSoft cuenta con todos los botones, luces y demás objetos necesarios para realizar un diseño rápido de todas las entradas y salidas que se tienen, basta con hacer doble clic sobre estas para asignar los respectivos TAG's, que se encuentran enlazados a la memoria del PLC (véase figura 61), cabe resaltar que este proceso es válido para los demás subsistemas.

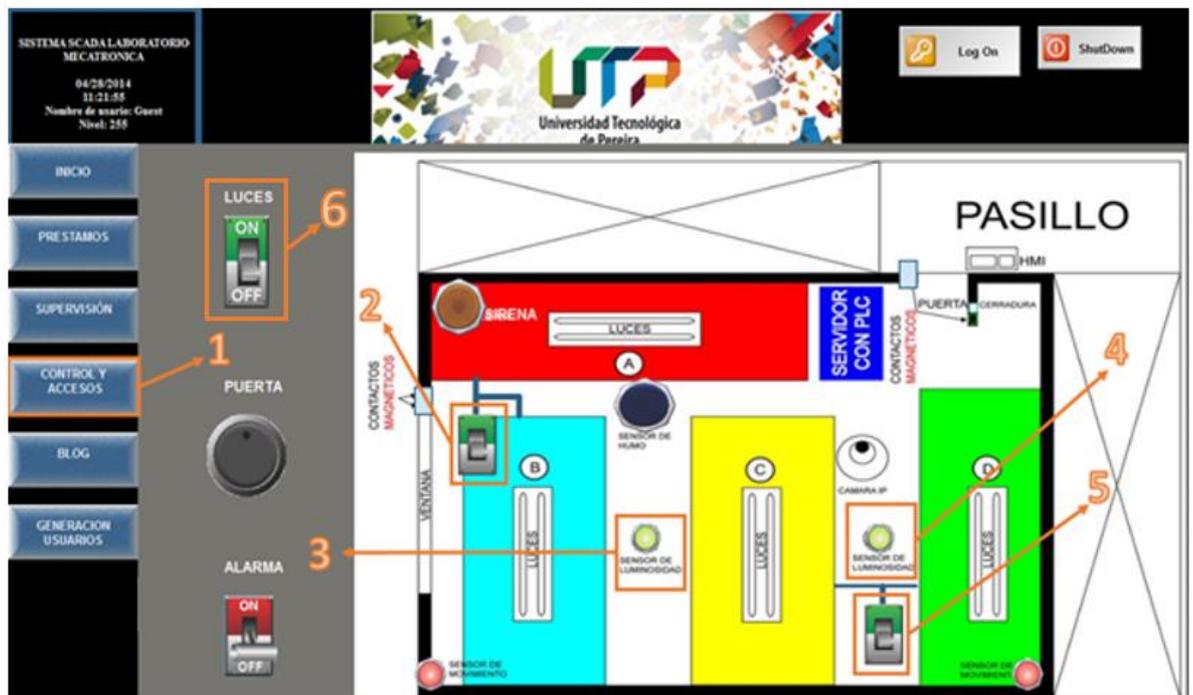
Figura 61: Botón asignado al TAG M0 desde el software



En la figura 62, se observa el sistema de control y acceso del laboratorio, el cual consta de una serie de botones, interruptores y luces piloto previamente asignados a las memorias del PLC, los iconos del sistema de iluminación se encuentran distribuidos de la siguiente forma

- (1) Botón de acceso al entorno de control y acceso en modo "RUN-TIME" desde el InduSoft Web Studio.
- (2) Interruptor, que proporciona la señal correspondiente al encendido parcial de las lámparas A Y B.
- (3) Luz piloto indicadora del estado del sensor de luminosidad 1, correspondiente al sector A, B
- (4) Luz piloto indicadora del estado del sensor de luminosidad 2, correspondiente al sector C, D
- (5) Interruptor que proporciona la señal correspondiente, al encendido parcial de las lámparas A Y B.
- (6) Interruptor encendido total de luces, es el encargado de hacer el inicio temporizado de las lámparas del laboratorio.

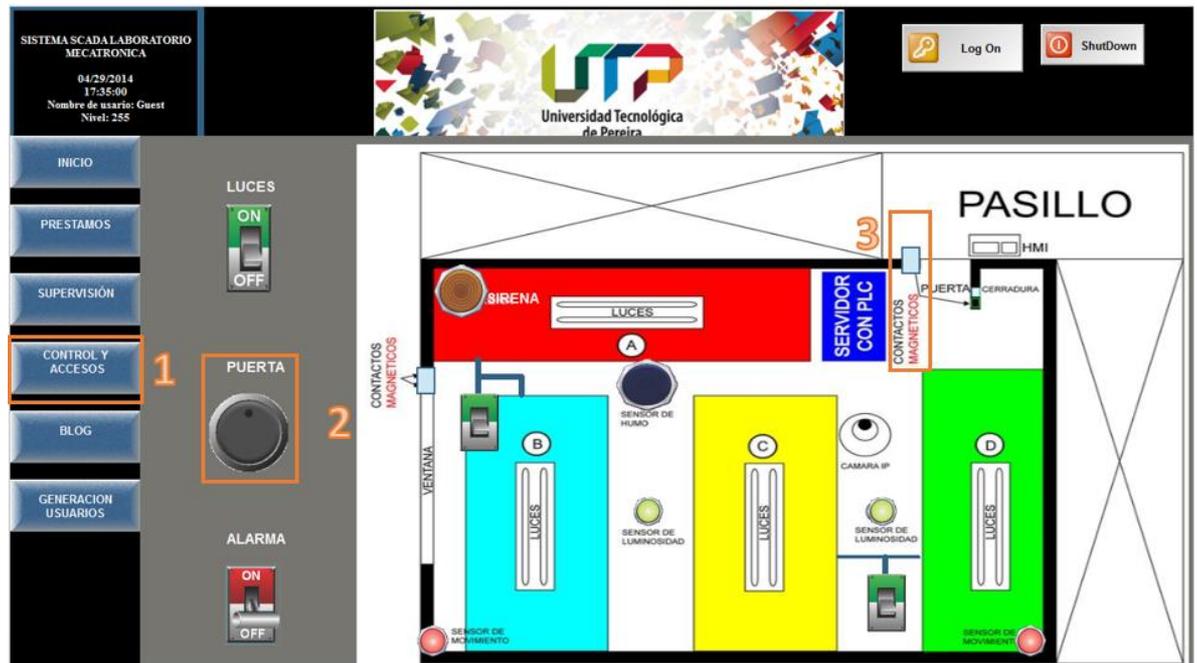
Figura 62: Control de luces desde el RUN-TIME de InduSoft Web Studio



3.6.2 Entorno sistema de acceso

Como se observa en la figura 63, La opción de apertura de puerta también se encuentra disponible en la pantalla de control y accesos (1), en esta pantalla se encuentra un botón normalmente abierto sin enclavamiento (2), que al ser accionado permite la apertura de la puerta y es posible ver el estado de la misma, a través, de la luz piloto correspondiente al contacto magnético ubicado en ella (3).

Figura 63: Pantalla de control y acceso con énfasis en el sistema de acceso



3.6.3 Entorno sistema de seguridad

Como se observa en la figura 64, el sistema de seguridad está comprendido por los siguientes iconos:

- (1) Botón de enlace entorno de control y acceso.
- (2) Luz piloto que permite comprobar el estado de la memoria asignada a la sirena.
- (3) Luz indicadora del estado del contacto magnético ubicado en la ventana.
- (4) Interruptor para activar y/o desactivar la alarma general.
- (5) Luz piloto que muestra el estado en el que se encuentra la memoria del sensor de movimiento 1.
- (6) Luz piloto que muestra el estado de la memoria del detector de humo.
- (7) Luz indicadora del estado del contacto magnético, ubicado en la puerta.
- (8) Este botón proporciona un enlace directo a la venta de supervisión, donde se observa la cámara IP (ver figura 65).
- (9) Luz piloto que muestra el estado en el que se encuentra la memoria del sensor de movimiento 2.

Figura 64: Ventana de control y acceso con énfasis en el sistema de seguridad

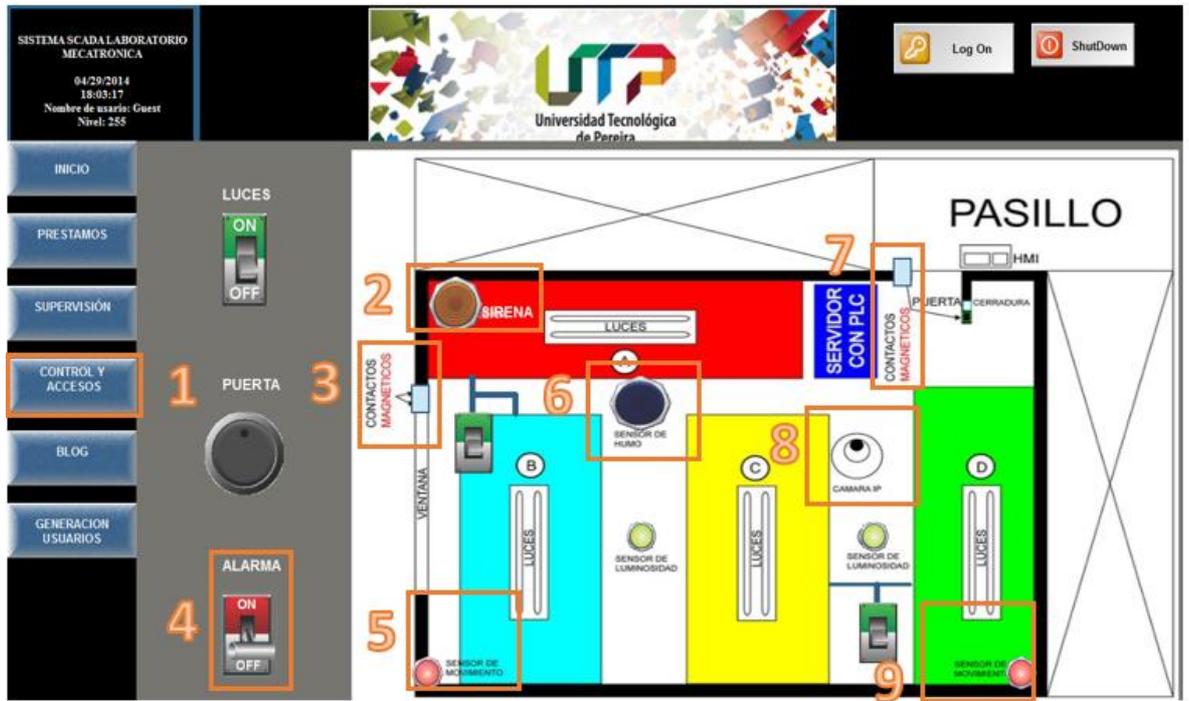
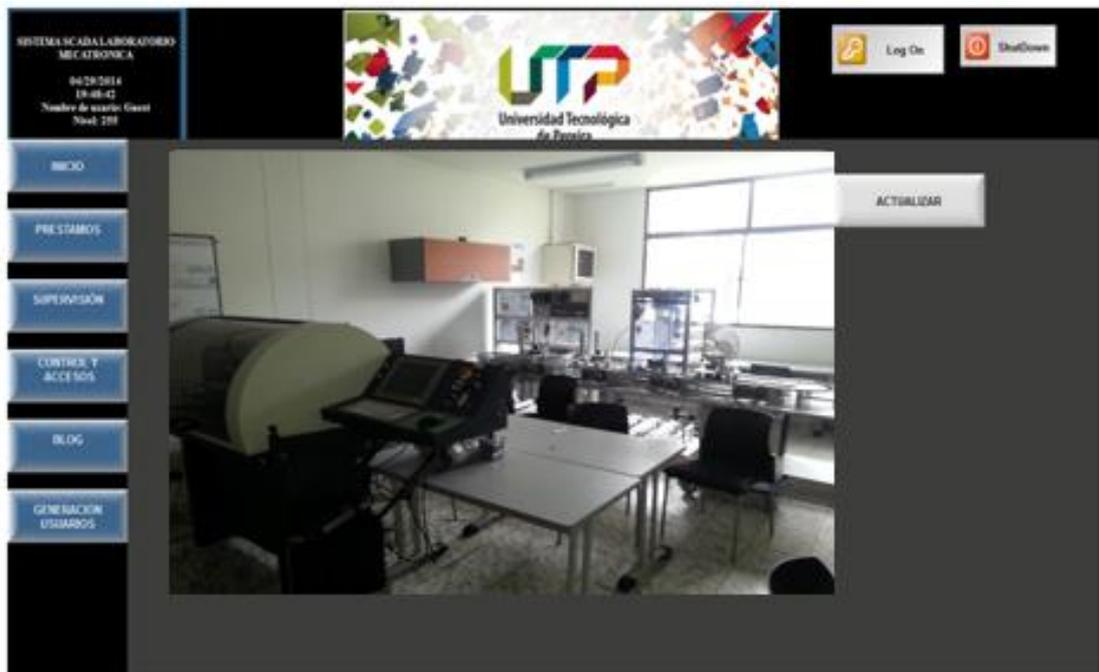


Figura 65: Ventana de supervisión enlazada a la cámara IP



3.6.4 Entorno del sistema de gestión

El sistema de gestión, hace referencia a dos puntos clave, que le dan un valor agregado al diseñado propuesto, estos dos son:

3.6.4.1 Generación de usuarios

Aunque este ítem, podría ser considerado parte del sistema de seguridad y así es, también tiene un componente de gestión ya que estos usuarios pueden ser creados y modificados desde la interfaz de forma online.

Los usuarios que tienes acceso a la interfaz SCADA, se encuentran divididos en tres grupos, cada grupo con un nivel de seguridad que va de 0 a 255 donde cero es ningún permiso y 255 acceso total:

- Súper usuario: A este grupo pertenecen los usuarios que tienen acceso completo a la interfaz, sin ningún tipo de restricción, los integrantes de este grupo poseen un nivel de seguridad 255.
- Monitor: A este grupo pertenecen los usuarios que tienen acceso parcial a la interfaz, pero sin tener acceso a modificaciones relevantes en el sistema. Estos poseen un nivel de seguridad de 180.
- Invitado: En este se encuentran los usuarios que en su mayoría son estudiantes y cuyo propósito principal es acceder al préstamo de equipos. Estos poseen un nivel de seguridad de 80.

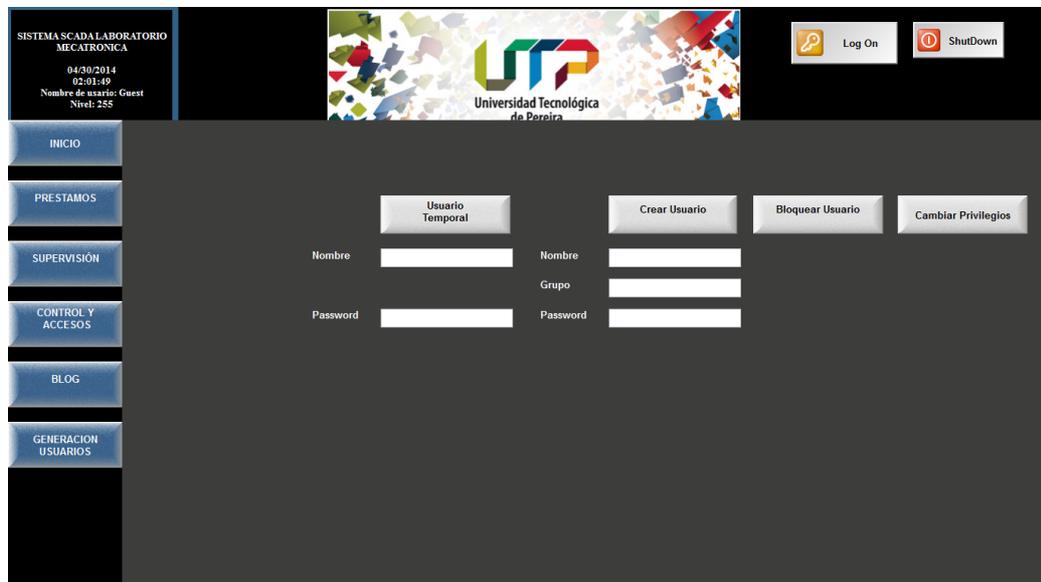
Para que los grupos de usuarios tengan efecto en la interfaz, se asigna un nivel de seguridad a cada botón de navegación, esto permite que solo las personas que tienen un nivel superior al designado al icono, tengan acceso a este. Estos niveles fueron designados de la siguiente forma:

- Botón de inicio: Nivel 0, todos los grupos tienen acceso.
- Botón prestamos: Nivel 50, los 3 grupos de usuarios pueden acceder a este.
- Botón de supervisión: Nivel 100, solo súper usuarios y monitores tienen acceso.
- Botón de control y accesos: Nivel 200, solo súper usuarios pueden acceder.
- Botón Blog: Nivel 0, todos los grupos pueden tener acceso.
- Botón generación usuarios: Nivel 200, solo súper usuarios

En el modo de ejecución de la interfaz, se tiene diferentes opciones con respecto a la generación de usuarios, estas incluyen (véase figura 66):

- Usuario temporal: Con este botón, es posible crear un usuario del grupo de invitado asignando un nombre y una contraseña.
- Crear usuario: Este botón permite crear un usuario completo, asignado un nombre a este, el grupo al cual pertenece y una contraseña.
- Bloquear Usuario: A través de este botón, es posible suspender los permisos de acceso de un usuario, solo basta poner el nombre.
- Cambiar privilegios: Este la posibilidad de modificar el nivel de seguridad y el grupo al cual pertenece un usuario ya registrado.

Figura 66: Ventana de generación de usuarios desde la interfaz SCADA



3.6.4.2 Prestamos instrumentos del laboratorio

La interfaz SCADA, se enlaza con una base de datos Access, que permite llevar un registro de los diferentes instrumentos y espacios solicitados en el laboratorio, en la figura 67, se observa los datos principales que son requeridos para solicitar un préstamo, tales como código, nombre, materia, y espacio a utilizar. Una vez se haya pulsado el botón de guardar, toda esta información es almacena en la base de datos (véase figura 68), a la cual puede acceder el monitor para confirmar la información puesta en la solicitud. Para procesar una nueva solicitud, solo basta con presionar el botón nuevo.

Las funciones de estos botones son programados con comandos sencillo de Visual Basic.

Figura 67: Ventana del sistema de préstamos en InduSfot Web Studio

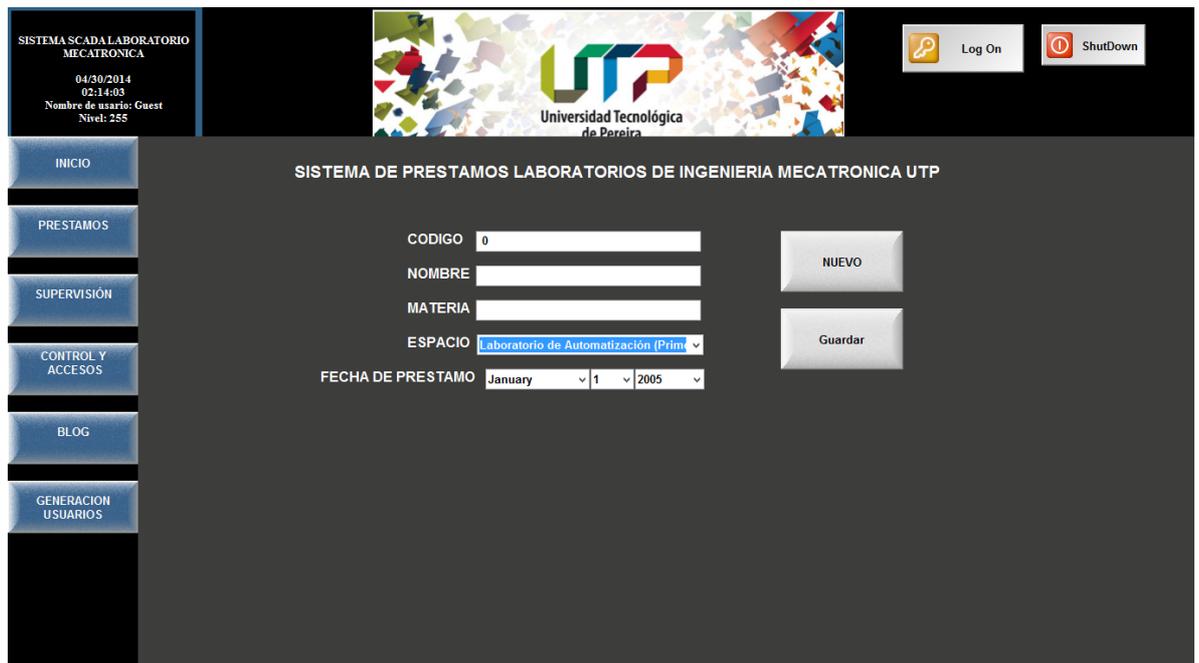


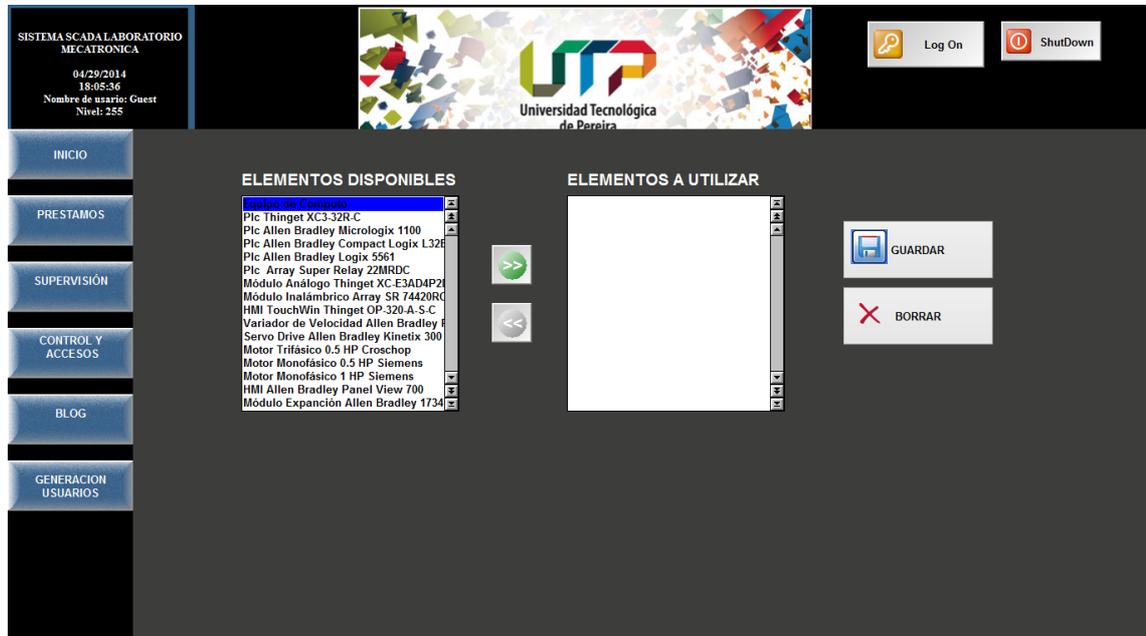
Figura 68: Base de almacenamiento Access de los datos ingresado en el sistema de prestamos

IDPRESTAMO	CODIGO	NOMBRE	MATERIA	FECHA_INGRESO	ESPACIO	FECHA_PRESTAMO
1	94152	Eduard	feqwfwf			
2	555	Juan	Calculo			
3	4444	Juan	Calculo			
4	123	Natalia	Español			
5	1234	Oscar	lallallala			
6	12345	Oscar	CHAACASC	21:46:23		
7	999	JULIAN	Materiales	21:52:16		
8	999	JULI	Materiales	01/31/2014 21:53:40		
9	987	Steve Jobs	Materiales	01/31/2014 21:55:04		
10	123456	juanito	matematica	02/01/2014 12:06:48	Laboratorio de Electrónica (Segundo Piso)	
11	123456	juanito	matematica	02/01/2014 12:07:22	Laboratorio de Automatización (Primer Pi	
12	1088	JULIAN ANTONIO RIOS	CASTELLANO	02/01/2014 12:21:35	Laboratorio de Automatización (Primer Pi	

Por otra parte, el boton guardar, direcciona a una ventana donde en una pantalla 1 se encuentran varios de los impementos con los que cuenta el laboratorio, al seleccionar uno de estos (ver figura 69), se pasa a una pantalla dos, que

representa los elementos escogidos y una vez pulsado el boton guardar nuevamente, estos son almacenados en la base de datos.

Figura 69: Pantalla de selección de implementos a utilizar



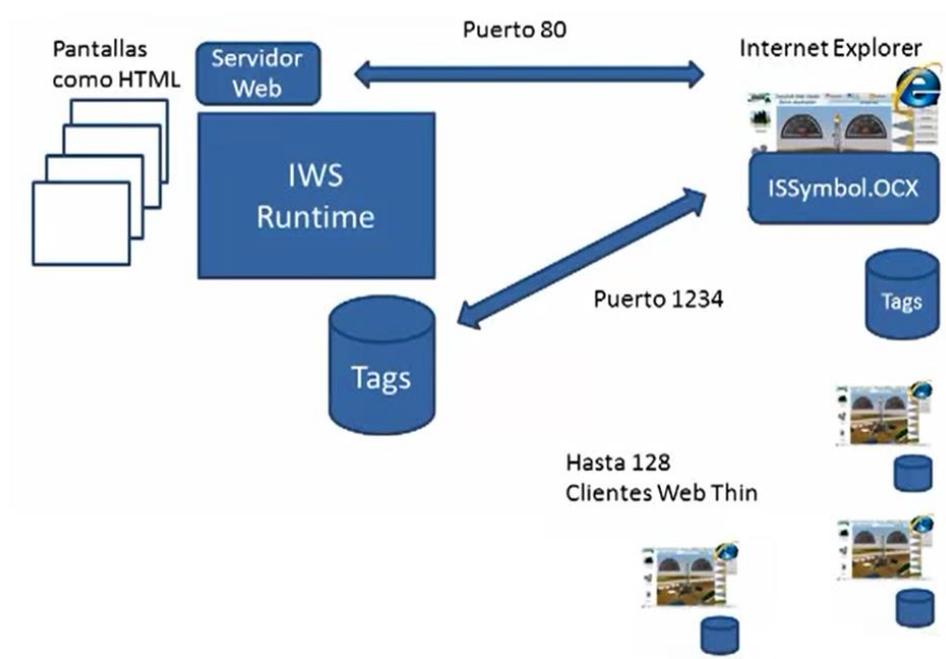
3.7 MANEJO WEB

Una vez toda la interfaz fue diseñada con sus respectivos botones y comandos y la comunicación con el PLC fue establecida, se puede llevar este a la web. Para esto se debe contar con un servidor web, para efectos demostrativos y con el fin de identificar como se realiza este procedimiento se hace uso del servidor web de Microsoft IIS (internet information services) y el ordenador en el cual se encuentra instalado el InduSoft hace la función de servidor (ver figura 70). Para una información detallada de como configurar el IIS, ver anexo C.

Para dar inicio a este proceso primero se debe acceder al proyecto creado en InduSoft Web Studio, allí modificar las configuraciones básicas de comunicación como lo son el puerto con el cual se conectan los TAG's al servidor, las opciones permitidas, etc. (para ampliar esta información se puede hacer uso de la ayuda de InduSoft bajo el parámetro de búsqueda "Web Thin Client". Cuando esto se haya realizado es necesario compilar y/o verificar el proyecto para comprobar el correcto funcionamiento de este. Por último, el proyecto se guarda en formato HTML y a estas pantallas a las que se puede acceder por medio del Internet Explorer.

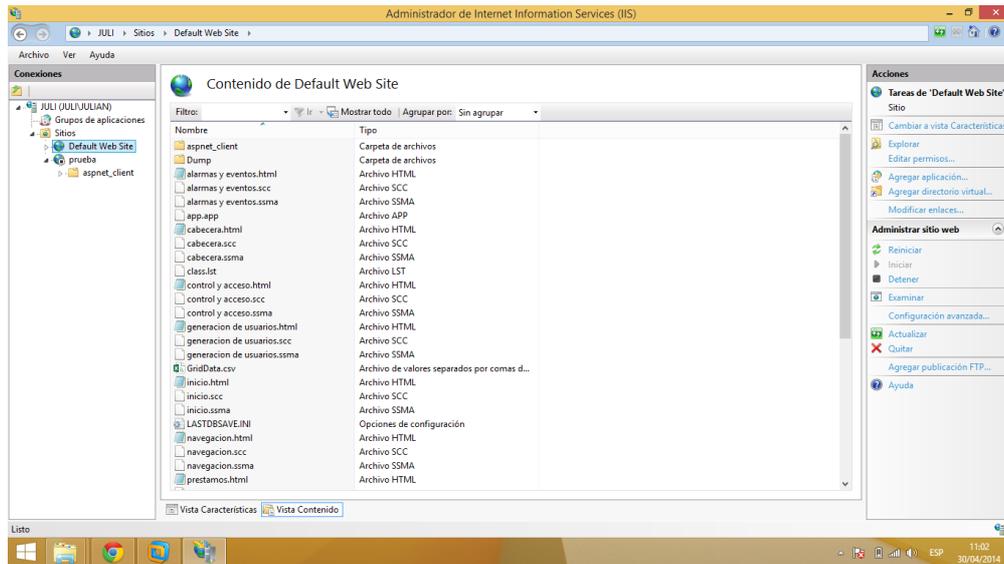
Cuando las configuraciones del software se encuentren completadas el paso por seguir es la configuración del servidor IIS, en este se debe especificar el puerto por el cual se debe conectar, por defecto es el puerto 80, la dirección IP y extensiones requeridos ver anexo C). También, se insertan las pantallas con extensión HTML que fueron creadas por InduSoft (ver figura 71).

Figura 70: Representación de la conexión Web de InduSoft Web Studio



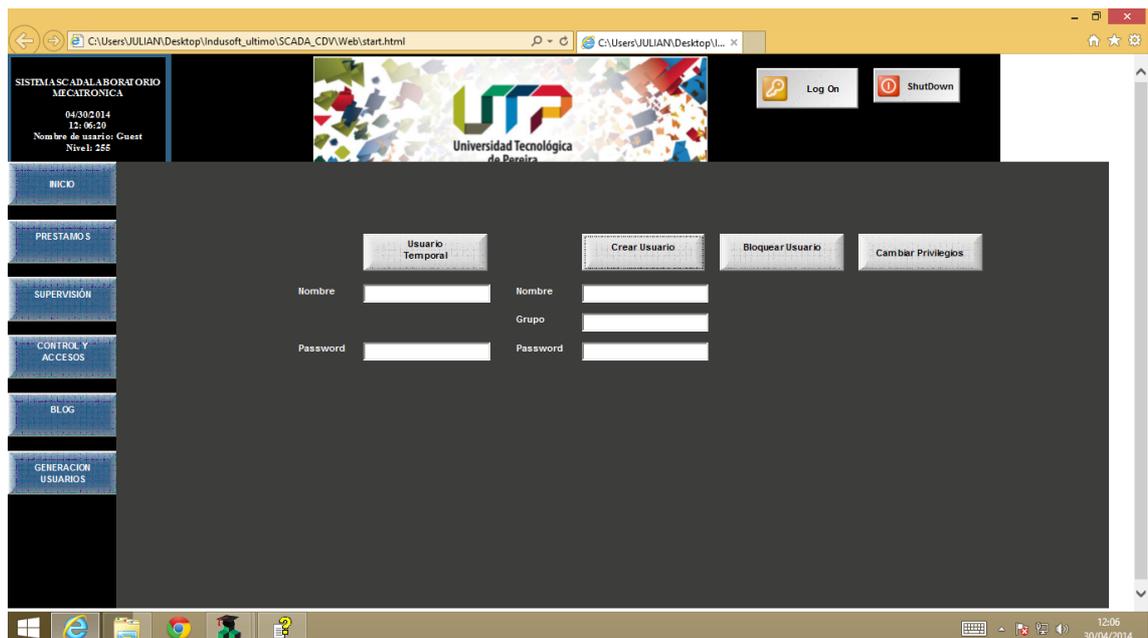
[78] Videos de entrenamiento InduSoft Web Studio [En línea]. [Citado el 25 de abril de 2014]. Disponible en <
<http://www.indusoft.com/Marketing/Article/ArtMID/684/ArticleID/386/Cliente-Web-Thin>

Figura 71: Configuración del servidor de Microsoft IIS



Una vez el servidor Web realizada la configuración, es posible acceder a la interfaz diseñada, a través de internet Explorer, por medio de la IP asignada a el ordenador y el nombre de la pantalla a la que se desea ingresar (ver figura 72), para la correcta visualización de InduSoft web Studio, es necesesario que se encuentre en modo Runtime. La primera vez que el proyecto es ejecutado desde un navegador, requerirá de la instalación de un complemento (ISSYmbol.OCX), necesario para la comunicación con la base de datos de TAG'S.

Figura 72: Interfaz SCADA diseñada desde Internet Explorer



ANÁLISIS DE COSTOS

- ❖ Antes de analizar los costos involucrados en este diseño, es necesario conocer la situación salarial actual del país. S.M.L.V colombiano (616.000). Los salarios promedio entre los profesionales, que han cotizado al sistema de seguridad social en Colombia son:

Formación técnica: Salario promedio de 901.026 mil pesos mensuales

-Formación tecnológica: Ingreso aproximado de 1.030.724 mil pesos al mes

-Formación universitaria: Salario promedio de 1.378.027 mil pesos.

- Especialización: Ingreso aproximado de 2.396.839 mil pesos mensuales.

-Maestría: Salario promedio de 3.007.488 mil pesos al mes.

-Doctorado: Ingreso aproximado de 4.904.102 pesos mensuales.

Estos salarios, son aproximaciones generales de la retribución académica, según el nivel de formación y pueden variar según el campo de acción. [77]

- ❖ Los siguientes cálculos, son basados en los salarios promedios, dependiendo del grado de formación en Colombia.

- Cantidad de semanas trabajadas en un mes

$$\frac{30 \text{ Días}}{1 \text{ Mes}} * \frac{1 \text{ Semana}}{7 \text{ días}} = 4,29 \frac{\text{Semanas}}{\text{Mes}}$$

- Cantidad de horas trabajadas en un mes

$$4,29 \frac{\text{Semanas}}{\text{Mes}} * 48 \frac{\text{Horas}}{\text{Semana}} = 205,7 \frac{\text{Horas}}{\text{Mes}}$$

- Precio promedio hora, técnico profesional

$$901.026 \frac{\text{Pesos}}{\text{Mes}} \div 205.7 \frac{\text{Horas}}{\text{Mes}} = 4380.29 \frac{\text{Pesos}}{\text{Hora}}$$

- Precio promedio hora, tecnólogo

$$1.030.724 \frac{\text{Pesos}}{\text{Mes}} \div 205.7 \frac{\text{Horas}}{\text{Mes}} = 5010.81 \frac{\text{Pesos}}{\text{Hora}}$$

- Precio promedio hora, Ingeniero

$$1.378.027 \frac{\text{Pesos}}{\text{Mes}} \div 205.7 \frac{\text{Horas}}{\text{Mes}} = 6699.20 \frac{\text{Pesos}}{\text{Hora}}$$

- ❖ Costos del recurso humano inherente para la realización de las tareas propuestas, en ámbitos como: La implementación, programación y puesta a punto del diseño.

Tabla 10: Tabla de costos en términos de horas trabajadas

RECURSO HUMANO	TRABAJO A REALIZAR (Mano de obra)	TIEMPO ESTIMADO (horas)	SALARIO/HORA (Monto en pesos)
Técnico Profesional en Mecatrónica	Cableado e instalación total del sistema	36	4380.29
Tecnólogo en Mecatrónica	Programación SCADA, PLC y HMI	36	5010.81
Ingeniero en Mecatrónica	Puesta a punto del sistema de gestión y supervisión	12	6699.20
			\sum 418.470

- ❖ Costos de los diferentes componentes propuestos, entre sensores y actuadores

Tabla 11: Tabla de costos de los diferentes elementos de campo requerido

CANTIDAD	DISPOSITIVO	PRECIO UNITARIO (pesos)	PRECIO TOTAL
Sistema de luces			
1	Sensor de humo GLH-965R-24	98.700	
2	Sensor de movimiento BLUE LINE GEN2	14.5180	290.360
1	Contacto magnético GL-38B	64.860	
1	Cámara IP Dvr, H.264	135.000	
3	Relé PCB G5V-1	5.850	17.550
1	Cerradura eléctrica Luber	42.500	
2	Sensor de luminosidad	100.400	200.800
1	Sirena multitonar WM 4 tonos 12-24VDC	174,600	
1	PLC THINGET XC3- 32r-c	360.000	
1	Ordenador HP COMPAQ 5700	700.000	
1	HMI THINGET OP 320-	203.000	
		Σ	2'244.870

- ❖ Costos de los materiales e implementos básicos, para la instalación en planta.

Tabla 12: Tabla de costos herramientas requeridas

GASTOS GENERALES	COSTO APROXIMADO (en pesos)
Herramental	100.000
cables	120.000
Canaletas	50.000
Conectores	10.000
Equipo de seguridad	25.000
Otros	100.000
	Σ 405.000

- ❖ Costo total del sistema de gestión y supervisión del laboratorio de automatización.

Tabla 13: Tabla de costos software SCADA y propuesta de diseño

COSTO TOTAL DEL SISTEMA. CON LA LICENCIA ESTUDIANTIL, QUE POSEE EL PROGRAMA	3'068.350
COSTO DEL DISEÑO 30%	920.550
	Σ 3'988.900

CONCLUSIONES

- El laboratorio del programa de Mecatrónica cuenta con muchos de los elementos necesarios para la realización del diseño propuesto, sin embargo cabe resaltar que los elementos mencionados en el diseño, que no se encuentran en el inventario, pueden ser reemplazados por referencias similares en aras de reducir costos y/o mejorar las señales que se manejan.
- En la selección del controlador cabe resaltar que los mencionados en el presente documento, pueden cumplir con las tareas asignadas. Para este diseño en específico, se escogió un autómata programable no solo por sus características de diseño, por la compatibilidad con el software seleccionado sino también por su robustez, en el sistema de gestión desarrollado en dicho elemento no han sido aprovechadas todas sus funciones, esto proporciona una base para el desarrollo del control de más variables y hacer enormes mejoras al sistema.
- El software Indusoft Web Studio, proporciona todos los elementos necesarios para diseñar el sistema de gestión y supervisión, pero al ser un software de licencia paga aumenta en gran medida los costos de implementación, sin embargo el soporte técnico que respalda es de alta calidad. Por otra parte, se determinó que es posible diseñar el sistema con una plataforma "open source" como (Easy SCADA), aunque, Indusoft sigue siendo una alternativa muy fiable por lo que se puede ver como una buena inversión.
- En la realización de este diseño, se ven evidenciadas las competencias tecnológicas de la Mecatrónica, debido a que estas actividades involucran problemas eléctricos, electrónicos y mecánicos. En este proyecto, se aprecia los aspectos más relevantes de la pirámide de automatización, necesaria para contemplar los alcances obtenidos y futuros desarrollos, en pro de incluir nuevas tecnologías, que hagan cada vez más cómodas y eficientes las tareas diarias dentro de un recinto.

RECOMENDACIONES

- En aras de mejorar e innovar el diseño propuesto, se sugiere hacer uso de una Tablet con conexión web, para que haga las veces de HMI, proporcionando una interfaz más amigable con el usuario y sin restricciones de programación, debido a que nos permite una comunicación directa con la interfaz SCADA.
- Uno de los aspectos más importantes y relevantes para este diseño, es la seguridad web. Aunque ya se cuenta con una protección previa integrada al software, se hace necesario ahondar más a fondo en la protección del software a nivel de seguridad web (ver anexo E). Debido a las amenazas constantes a la seguridad en el ciberespacio, se recomienda la asesoría de una empresa especializada en protección web.
- Un aporte adicional a este diseño, es en el campo de los sistemas de bases de datos. Es recomendable hacer una búsqueda de una mejora en la construcción y desarrollo de las bases de datos, permitiendo una consignación de los resultados de una forma más eficiente.
- Es de vital importancia tener en cuenta que el Software Indusoft, solo puede ser ejecutado en ordenadores con sistema operativo Windows, ya sea 32 o 64 bits, Por otro lado, cabe resaltar que para tener acceso desde la Web es necesario usar el navegador internet Explorer e instalar un complemento a este, para observar el RUN-TIME del software.
- En pro de la mejora continua, se recomienda a los futuros estudiantes interesados en realizar aportes al proyecto, abarcar tópicos como: sistemas de gestión eléctrica y el sistema de climatización, en aras de realizar un control más eficiente de los recursos disponibles de los laboratorios.
- Las conexiones a bases de datos del Software Indusoft, no poseen una compatibilidad completa con el software de la línea de Microsoft Office versión 2013, por lo que se hace necesario instalar un complemento de compatibilidad para base de datos de Microsoft 2010.

BIBLIOGRAFIA

- [1] SCADA. [En línea]. [Citado el 6 de abril del 2014]. Disponible en<
http://sites.amarillasinternet.com/induelec-servicios-tableros/sistemas_scada.html>
- [2] HMI. [En línea]. [Citado el 6 de abril del 2014]. Disponible en<
<http://www.aie.cl/files/file/comites/ca/abc/hmi.pdf>>
- [3] Inmótica. [En línea]. [Citado el 6 de abril del 2014]. Disponible en<
<http://www.domodesk.com/a-fondo-inmotica>>
- [4] PLC. [En línea]. [Citado el 6 de abril del 2014]. Disponible en<
<http://www.abcinnova.com/articulos-e-informacion/18-ique-es-un-plc-y-que-beneficios-tiene.html>>
- [5] TAG. [En línea]. [Citado el 6 de abril del 2014]. Disponible en<
<http://www.lawebdelprogramador.com/diccionario/mostrar.php?letra=T>>
- [6] Imagen edificio inteligente Pereira. [En línea]. [Citado el 8 de abril del 2014]. Disponible en<
<http://www.skyscrapercity.com/showthread.php?t=444138>>
- [7] Niveles. [En línea]. [Citado el 8 de abril del 2014]. Disponible en<
<http://www.ingenieriatci.es/sistemas-de-supervision-en-la-industria-farmaceutica-evolucion-hacia-la-integracion-total/>>
- [8] Edificio inteligente de Pereira se llamará Torre Central. [En línea]. [Citado el 8 de abril de 2014]. Disponible en <
<http://www.eltiempo.com/archivo/documento/CMS-3519037>>
- [9] En octubre será inaugurado el edificio 'inteligente' de la Telefónica de Pereira. [En línea]. [Citado el 8 de abril de 2014]. Disponible en <
<http://www.eltiempo.com/archivo/documento/CMS-3678844>>
- [10] Climax irp9- detector de movimiento /detección de 12 metros [En línea]. [Citado el 15 de abril de 2014]. Disponible en<
http://convergenciadigital.com/eshop/product_info.php?products_id=831>
- [11] ¿Cómo funciona un detector de movimiento?-Detector de movimientos de ultrasonido [En línea]. [Citado el 15 de abril de 2014]. Disponible en <
<http://intrepido1.overblog.es/categorie-12116752.html>>
- [12] ¿Qué es la domótica? [En línea]. [Citado el 15 de abril de 2014]. Disponible en <
http://domotica.wikia.com/wiki/%C2%BFQu%C3%A9_es_la_dom%C3%B3tica%3F>

[13] Ventajas de la domótica [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://domoticasape.blogspot.com/2013/10/ventajas-de-la-domotica.html> >

[14] Diseño de un sistema domótico de altas prestaciones destinado a viviendas residenciales [En línea]. [Citado el 15 de abril de 2014]. Disponible en <Diseño de un sistema domótico de altas prestaciones destinado a viviendas residenciales>

[15] ¿Qué es la inmótica? [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://twenergy.com/desarrollo-sostenible-curiosidades/que-es-la-inmotica-589>>

[16] Inmótica... complemento al edificio inteligente [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://ecoopcion.wordpress.com/2012/04/16/inmotica-complemento-al-edificio-inteligente/>>

[17] Inmótica [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.controlcat.com/index.php/servicios/inmotica>>

[18] Tecnologías inmóticas [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://www.controlcat.com/index.php/producto/producto-tecnologia> >

[19] ¿Qué es knx? [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.knx.org/es/knx/que-es-knx/>>

[20] ENOCEAN [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://www.futureelectronics.es/es/manufacturers/enoclean/Paginas/index.aspx> >

[21] ENOCEAN EXTENSION - SIMPLE, WIRELESS HOME AUTOMATION [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<https://b.loxone.com/Pages/en/produkte/extensions/EnOcean/loxone-rs485.aspx>>

[22] El protocolo MODBUS [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.tolaemon.com/docs/modbus.htm>>

[23] Convertidores CAN [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.logicbus.com.mx/l-7242d.php>>

[24] Funciones básicas de un sistema SCADA [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://tobas.over-blog.es/article-funciones-basicas-sistema-scada-91082690.html>>

- [25] System Attacks – Turning SCADA into NADA SCADA [En línea]. [Citado el 15 de abril de 2014]. Disponible en < <http://chenected.aiche.org/process-safety/system-attacks-turning-scada-into-nada/>>
- [26] Glosario de términos de Domótica [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.inmomatica.com/glosario-domotica.html>>
- [27] Arquitecturas de un sistema domótico. [En línea]. [Citado el 15 de abril de 2014].
<Disponible en < http://fempa.es/rebt/automatizacion_vigilancia/pto5.htm >
- [28] Arquitectura de sistemas domóticos. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.arqhys.com/arquitectura-de-sistemas-domoticos.html>>
- [29] PLC Allen Bradley SLC 500 [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.automation-drive.com/for-allen-bradley-slc-500>>
- [30] Principios básicos de los PLC [En línea]. [Citado el 15 de abril de 2014]. Disponible en<<http://recursostic.educacion.es/observatorio/web/es/component/content/article/502-monografico-lenguajes-de-programacion?start=2>>
- [31] ¿Qué es un microcontrolador? [En línea]. [Citado el 15 de abril de 2014]. Disponible en< <http://www.electronicaestudio.com/microcontrolador.htm>>
- [32] Ing. Domingo C. Guarnaschelli. ELECTRONICA II –ING. ELECTRICA 7-2 Microcontroladores. UTN REG. SANTA FE . Facultad de Ingeniería eléctrica
- [33] Interfaz Hombre-Máquina pantalla MT506L, Buenos Aires. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://ciudad-buenos-aires.all.biz/interfaz-hombre-maquina-pantalla-mt506l-g15714> >
- [34] Interfaz hombre-máquina. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <http://www.copadata.com/no_cache/es/productos/product-features/interfaz-hombre-maquina-hmi.html >
- [35] Ordenador de mesa. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.centromipc.com/sintomas-de-un-ordenador-infectado-por-virus>>
- [36] ¿Qué es un ordenador? [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.masadelante.com/faqs/ordenador>>
- [37] Definición de sensor. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://definicion.de/sensor/6>>
- [38] Actuadores. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.aie.cl/files/file/comites/ca/abc/actuadores.pdf>>

- [39] Sensores. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.erc.com/guide/lighting-control/sensors-2611/es/>>
- [40] Alarma contra incendios. [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://santafe-ar.all.biz/alarmas-contra-incendios-g5112>>
- [41] Manual de procedimientos de instalaciones. Dispositivos utilizados para alarmas con o sin monitoreo [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://sistemamid.com/panel/uploads/biblioteca//1/619/634/3756.pdf>>
- [42] Contactos magnéticos cableados, plástico ABS en color blanco, Salida NC [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.empretel.com.mx/cableado/1570-contactos-magneticos-cableados-plastico-abs-en-color-blanco-salida-nc.html>>
- [43] ¿Qué es una cámara IP? [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://www.domodesk.com/a-fondo-camaras-ip>>
- [44] Cámara IP [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://totem.com.ec/blog/dato-importante-sobre-las-camaras-ip/>>
- [45] Implementación de una casa domótica residencial utilizando sensores y actuadores [en línea]. [Citado el 15 de abril de 2014]. Disponible en <http://repositorio.ute.edu.ec/bitstream/123456789/16635/1/53661_1.pdf>
- [46] Cerradura Eléctrica de Aplicar para Portones Luber 2020 [En línea]. [Citado el 15 de abril de 2014]. Disponible en <http://maxisistemas.com/index.php?route=product/product&product_id=203>
- [47] Sirena [En línea]. [Citado el 15 de abril de 2014]. Disponible en <<http://control-ip-alarmas.blogspot.com/2009/06/4.html>>
- [48] Luis Corrales, PhD. Interfaces de comunicación industrial. Diciembre 2007. Departamento de automatización y control industrial. [En línea]. Disponible en <<http://bibdigital.epn.edu.ec/bitstream/15000/10020/2/PARTE%202.pdf>>
- [49] proveedores de sistemas SCADAS. [En línea]. [Citado el 12 de septiembre de 2013]. Disponible en <<http://www.scadanews.com>>
- [50] InduSoft Web Studio. [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://www.indusoft.com/Products-Downloads/HMI-Software/Indusoft-en-Espa%C3%B1ol>>
- [51] Proyectos de InduSoft [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://www.side-automatizacion.com/es/product-side/proyectos-indusoft>>

[52] InduSoft Web Studio [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://www.logicbus.com.mx/indusoft.php>>

[53] InduSoft Web Studio [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://www.criticalindustrialsupply.com/Indusoft.html>>

[54] LECCIÓN 17: EL PLC COMO PARTE MEDULAR DE LA AUTOMATIZACIÓN FLEXIBLE [En línea]. [Citado el 16 de abril de 2014]. Disponible en <http://datateca.unad.edu.co/contenidos/2150514/Modulo_exe/leccin_17_el_plc_como_parte_medular_de_la_automatizacin_flexible.html>

[55] XC series PLC [En línea]. [Citado el: 13 de septiembre de 2013]. Disponible en <<http://www.imenista.com/tingetplc.html>>

[56] Thinget HMI [En línea]. [Citado el: 13 de septiembre de 2013]. Disponible en <<http://spanish.alibaba.com/product-gs/thinget-hmi-406733528.html>>

[57] Lenguajes de programación de plc's, programa y lenguaje de programación. [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://esdocs.org/docs/index-50685.html>>

[58] HP Compaq dc5700 Microtower PC [En línea]. [Citado el 16 de abril de 2014]. Disponible en <http://images.businessweek.com/ss/07/05/0514_greencomputing/source/4.htm>

[59] ODBC: Resumen de conectividad abierta de base de datos. [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://support.microsoft.com/kb/110093/es>>

[60] Redes. [En línea]. [Citado el 16 de abril de 2014]. Disponible en <<http://moiseslara565.blogspot.com/2012/08/44-adequacion-de-senales.html>>

[61] Intercambio dinámico de datos. [En línea]. [Citado el 22 de abril de 2014]. Disponible en <<http://ofimaticaeduc.blogspot.com/2012/03/intercambio-dinamico-de-datos-el.html>>

[62] What is OPC? [En línea]. [Citado el 22 de abril de 2014]. Disponible en <<http://www.opcdatahub.com/WhatIsOPC.html>>

[63] TCP/IP [En línea]. [Citado el 22 de abril de 2014]. Disponible en <<http://searchnetworking.techtarget.com/definition/TCP-IP>>

[64] Domaut- alarmas técnicas [En línea]. [Citado el 22 de abril de 2014]. Disponible en <http://www.domaut.com/Alarmas_tecnicas.html>

- [65] XC Series PLC, User Manual [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://oceancontrols.com.au/datasheet/xin/manual-XC.pdf>>
- [66] THINGET [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<file:///C:/Users/Juan/Downloads/opisanie-programmy-XCP-Pro.pdf>>
- [67] Xinje XC Series PLC [En línea]. [Citado el 24 de abril de 2014]. Disponible en http://www.fasttobuy.com/xinje-xc-series-plc-io-expansion-analog-module-xce4ad2da-4channel-14bits-precision-analog-input-2channel-12bit-precision-analog-output-new-free-shipping_p25825.html
- [68] OP series display, xinje Electronic Co. Ltd [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.imenista.com/pdf/OPManual.pdf>>
- [69] El protocolo MODBUS. [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.tolaemon.com/docs/modbus.htm>>
- [70] Detector de movimiento por infrarrojos pasivos Blue Line Gen2 [En línea]. [Citado el 24 de abril de 2014]. Disponible en <http://resource.boschsecurity.com/documents/BlueLine_Gen_2_Data_sheet_esES_2603228171.pdf>
- [71] Contacto Magnético fijación adhesivo [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.elinstaladorelectricista.es/default/domotica-2/material-domotico/gl38b-contacto-magnetico-fijacion-adhesivo-o-tornillos-puertas-y-ventanas.html>>
- [72] WIFI, la comunicación inalámbrica [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.aulaclic.es/articulos/wifi.html>>
- [73] Cámara IP DVR [En línea]. [Citado el 24 de abril de 2014]. Disponible en <http://articulo.mercadolibre.com.co/MCO-410291311-camara-ip-robotica-dvr-h264-nocturna-ranura-microsd-wifi-_JM>
- [74] Destradores eléctricos [En línea]. [Citado el 24 de abril de 2014]. Disponible en <http://www.lubercerraduras.com.ar/cerraduras_electricas.php>
- [75] Sirena multitonal WM 4 tonos 12-24VDC [En línea]. [Citado el 24 de abril de 2014]. Disponible en <https://www.werma.com/es/s_c1003i46/Sirena_multitonal_WM_4_tonos_12-24VDC_GY/12605215.html>
- [76] OMRON PCB Relay [En línea]. [Citado el 24 de abril de 2014]. Disponible en <<http://www.micropik.com/PDF/g5v1.pdf>>

[77] Tendencias Laborales [En línea]. [Citado el 25 de abril de 2014]. Disponible en <http://www.empleo.com/colombia/tendencias_laborales/cuanto-gana-un-colombiano-segun-su-preparacion-academica-----/8540461>

[78] Videos de entrenamiento InduSoft Web Studio [En línea]. [Citado el 25 de abril de 2014]. Disponible en <<http://www.indusoft.com/Marketing/Article/ArtMID/684/ArticleID/386/Cliente-Web-Thin>

[79] Anexo A. XC Series Edit Tool XCP Pro. User Manual. XINJE. Capitulo 2. Basic operation. Xinje. Pages: 10 to 13. Electronic Co., Ltd. Date: 7th of November 2013. Time: 14:37

[80] Anexo B. OP Series Display. User Manual. Catalog. Capitulo 2-2 Edit the user's screen. Pages: 25 to 36. Date: 23rd of November 2013. Time: 17:09.

[81] Anexo C. Building a simple Thin client program: Procedur C: Thin client using IIS, Network IP. Search: IIS. Technical Reference. Indusoft Software. Date: 31st of November 2013. Time: 15:32.

[82] Anexo D. Capítulo 6. Gestión de riesgos de seguridad. Guía para empresas: Seguridad de los sistemas de monitorización y control de los procesos e infraestructuras (SCADA). Observatorio de la Seguridad de la Información. Instituto Nacional de Tecnologías de la Comunicación (INTECO). Páginas: 27 a la 34. Ministerio de Industria, Energía y Turismo. Gobierno de España. Fecha: 9 de Abril de 2014. Hora: 16:54.

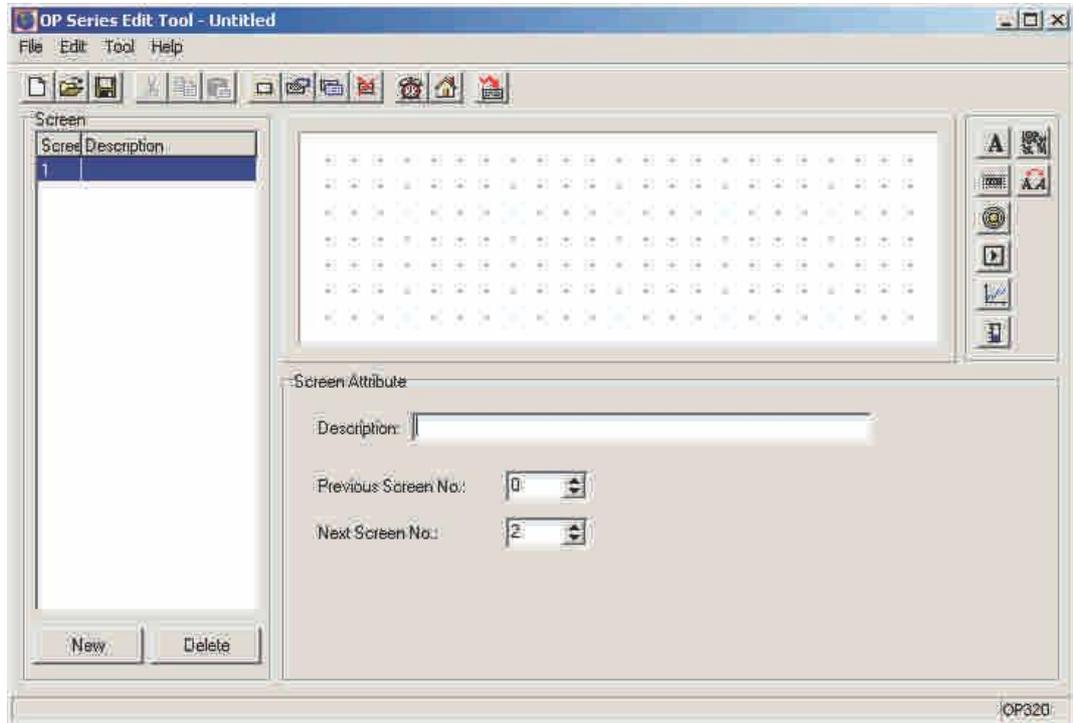
ANEXOS

Anexo A [79]

2-2 Edit the user's screen

2-2-1 Create a project

After running the OP20 Software, There will be a screen editor in the center of the computer's display.



$\frac{3}{4}$
Screen
ns

Display all the screen's serial number in the project.

$\frac{3}{4}$
Descriptio
ns

Simply character description of the screen function

$\frac{3}{4}$ "New"
key

Create a new screen.

$\frac{3}{4}$
"Delete"
" key

Delete the current screen.

In the top of the editor are the menu and tool bars; the content in the left

form is the screen's number and its description. In the bottom of this column there are [new] and [delete] buttons, they are used to create a screen or delete the current screen.

In the center of the editor is the screen edit area. In the display area evenly place light gray lattice, the space of the two dots is 16 pixels. The whole screen is 192x 64 lattice. When the designer place or move any element, refer to the near dot's place in order to snap the element to the grid. When the designer drags the element to move it with the mouse, the move space is integral times of 4 dots.

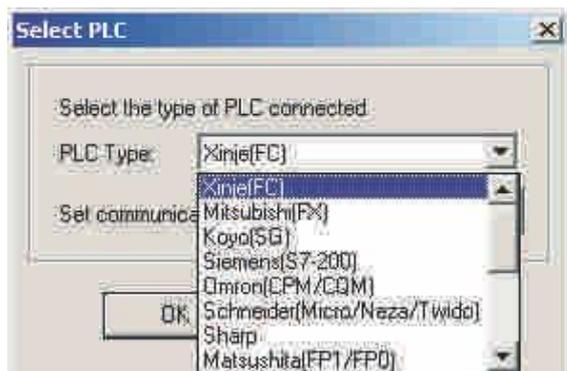
The following is all the keys in the tool bar and their function description.

Key	Description
	Create a new project.
	Open a saved project.
	Save a project that is editing currently
	Cut the characters in the textbox.
	Copy the characters in the textbox.
	Paste the characters in the textbox.
	Create a new screen, its function is the same to the [new] button in the screen indicate window.
	Display the property content of the current screen.
	Copy a screen to be another one
	Delete the current screen.

	Point the system's initial screen, when the display is working, click the [] button to return back to this screen directly. Generally, this screen is main menu or used most often. Set the system's password; Set the alternate
	Log in the alarm list information, each piece of alarm information correspond with a middle relay.
	Via RS232 port of the computer, download the completed project file to OP320 display.

Note: If you want to delete any element in the screen, just choose "DEL" button to realize.

Click on the  button or click [file]Æ[create a new project] command, in the center of the screen there will pop out a dialog box for you to choose PLC's type

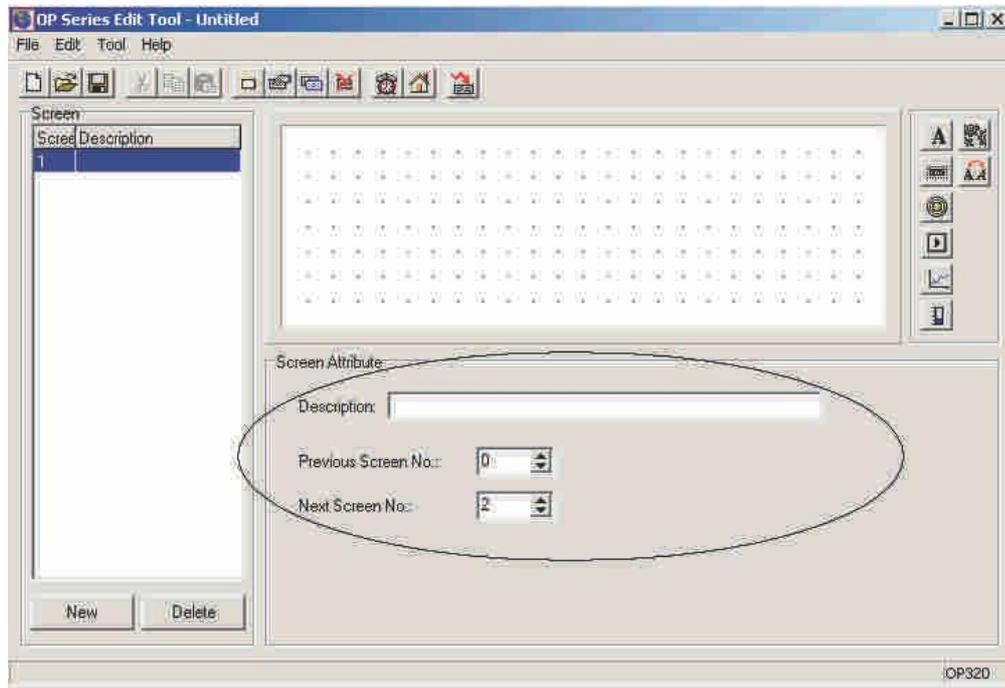


¾ PLC type

Choose PLC's type according to the display's communicate object. When OP20 download the screen, transfer the appoint PLC's communication protocol along with the screen data to the display. When the display is working, it will communicate with PLC according to this protocol.

2-2-2 Make a basic screen

The following we will take Mitsubishi FX series PLC as the example to describe:



First, enter the edit status of the system's initial screen (If default it will be the No.1 screen). In the bottom of the screen is the current screen's (No.1 screen) property, each screen has the property, include three items of the content.

$\frac{3}{4}$ Screen description

Describe the screen's property; enable the designer to manage conveniently. It only has the function of clue, so it also needn't to fill in. Take an example to input "main menu"

$\frac{3}{4}$ Click [^] button to the screen's No.

The value is click [^] button, the display will jump to the screen's No.

$\frac{3}{4}$ Click [v] button to the screen's No.

The value is click [v] button, the display will jump to the screen's No.

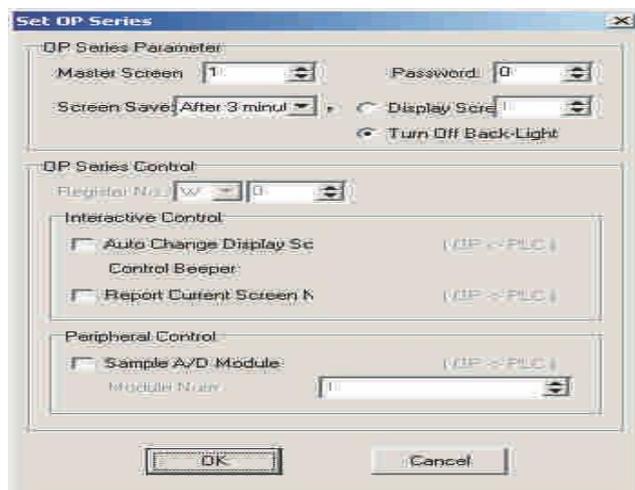
When the display is running, click [] button, [^] button or [v] button is the most brief way to switch the screens. Moreover, you can also realize screen jump by setting the function key.

Not e:

- a. If the [^] button or [v] button in the current screen is set as the function key, then the screen jump parameter in the screen's property is of no use.
- b. If the screen appointed by [^] button or [v] button does not exist, then the actual jump screen's ID spread up or down in turn, stop by 1 when up.
- c. If there are data set elements in the screen, then in the process of data setting, [^] button or [v] button realize the function of data plus or minus. After exit data setting state, [^] button or [v] button can recover the function of screens jump again.

2-2-3 The system parameter of OP20

Click  button, or click "tool"Æ"set OP20" command, there will come out a dialog box of setting OP20's system parameter



- z The main control screen.

After giving it power, the first screen OP320 displays. Generally, set this screen to be the main menu screen or the screen that used most often. During running, click [] button can jump to  his screen directly.

- z Password.

All the screens in a project use a same password, when the encrypt property of "data set window", "function key" is valid, only when the system's password be opened can the elements execute the action. Using

this function you can easily realize screen hide and set data encryption.

z Power conservation protection

The default value of the backlight hold time is 3 minutes. When set it to be 0, the backlight will light from start to end.

z Alternate control

Normally, screen switch is realized by the buttons. Besides, PLC can also realize screen switch by modifying the register's value. If this property is valid, write value n to the register D300 when running. OP20 will auto switch the display to the No,n screen. After this value in D300 will auto set to be 0.

OP320 writes the current screen's ID number to D301, PLC can also know the status of the display in this way.

Note: Designer can define the ID number of alternate control register in this way.

z Sample analog quantity data

OP320 can connect with a 8-route analog quantity sample module or a 8 route temperature sample module via RS485 communication port.

The register's head address which analog quantity auto stores is assigned by this parameter.

2-2-4 Text

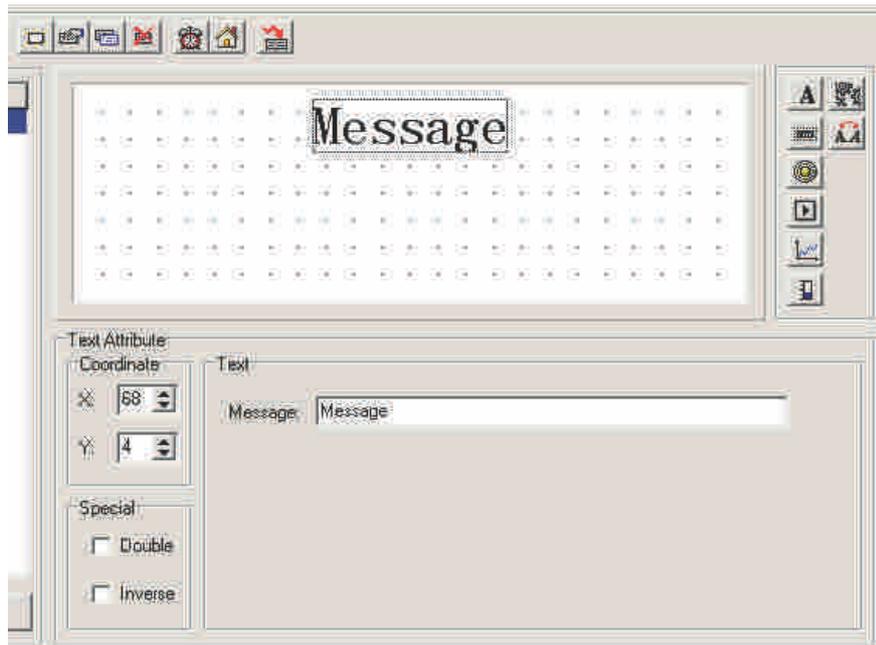
Before editing the screen, describe the 8 elements' function in the right of the screen edit window.

Parts	Function
	Input texts, including Chinese characters and English letters.
	Lay data monitor window or data set window (The object is PLC data register)

	Indicate lamp, display the on-off status of middle relay inside PLC.
	Function key, all the seven keys in the bottom of OP320 can be defined as function keys. The usage of function keys include screen jump and switch control etc.
	In the process of industry control, some parameters changes slowly, the operator want to know the change process of these parameters in a certain time. Fold-line graph is the most ideal
	Bar is used to display analog quantities parameter intuitively, such as flux, pressure, liquid level, etc. Its height, width and direction can be appointed randomly.
	Insert a bitmap file, it can display the machine's graph, make the operator easy to understand. It can also display the mark and badge of the factory, improve the product image.
	Dynamic text, display the current status of the machine with dynamic text. Make the operator easy to operate, improve the produce efficiency. Dynamic text is your ideal choice.

The following, we will take the example of designing the NO.1 screen to be the main menu screen.

First, lay the text "main menu", click the  button, there will be a rectangle dashed frame in the screen, and it moves along with the mouse. The move distance is integrate times of 4. At this time, click the left key of mouse to confirm, and click the right key of mouse to cancel. After confirming, the default content "Message" will display in the window, at the same time there will be the message's attribution displays in the right bottom of the screen.



¾ Coordinate

The X value indicates this text's horizontal position

The Y value indicates this text's vertical position

The coordinate origin point is in the left top of the screen.

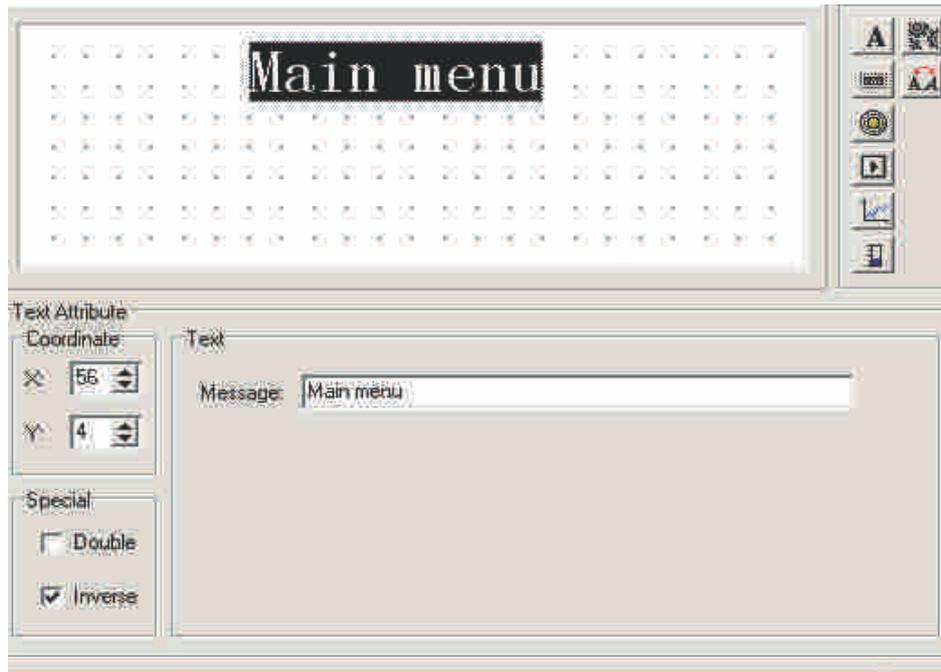
¾ Special

Double: Display the characters multiply in horizontal and vertical. Inverse: The color of the message and the background displays inversely.

¾ Message

The actual display content, we can input Chinese characters or English letters directly with all the Chinese input methods. The content of this column can be cut, copied or pasted.

E.g. Display the text "main menu" in inverse. Input "main menu" in the set column, and choose the "inverse" in the "special" frame.



2-2-5 Function key (screen jump)

The following, set function key in the main menu screen to realizes screen jump function. E.g. when running, click “<” key to enter parameter set screen. Click “<” key to enter mode set screen. The steps of sets function key are the following:

Click  button, there will be a dashed rectangle frame that moves with the mouse. Click the left button of the mouse to confirm the position of the function key. Then there will be a hand graph and the function key (Be “<” when default) to be set in the window. In the right bottom is the attribution of the function key, in which the coordination and its attribution is the same with the texts. It is used to indicate the position, to conform the graph’s size and color.

¾ Key

In the pull down menu of “key”, choose the appropriate key from seven keys.

¾Hand

In order that the operator can operate it correctly and quickly, add a hand graph in front of the button, indicate that press the appointed key can complete an action. In order to save the space, you can also not

choose the hand graph.

$\frac{3}{4}$ Encrypt

This function key is only valid when the system's password be opened.

$\frac{3}{4}$ Set coil

The function key's action is switch quantity setting.

$\frac{3}{4}$ Screen jump

This function key's action is screen jump.

$\frac{3}{4}$ Coil No.:

When the function key's action is switch quantity setting, conform PLC's interior middle relay's define ID number correspond with on-off action.

$\frac{3}{4}$ Force ON

Set the appointed middle relay to be ON.

$\frac{3}{4}$ Force OFF

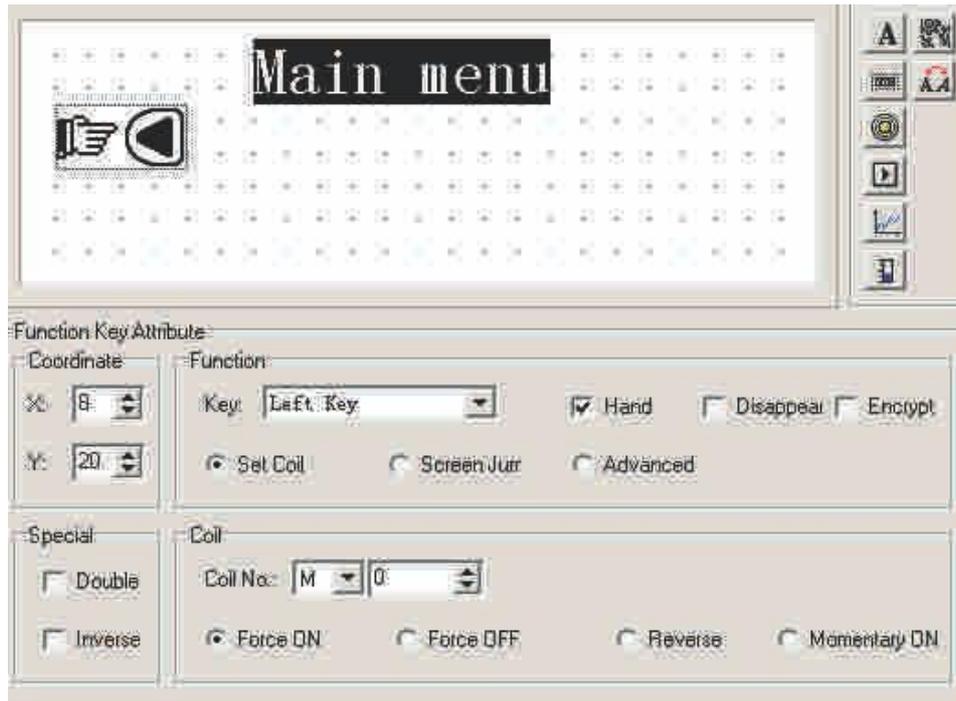
Set the appointed middle relay to be OFF.

$\frac{3}{4}$ Reverse

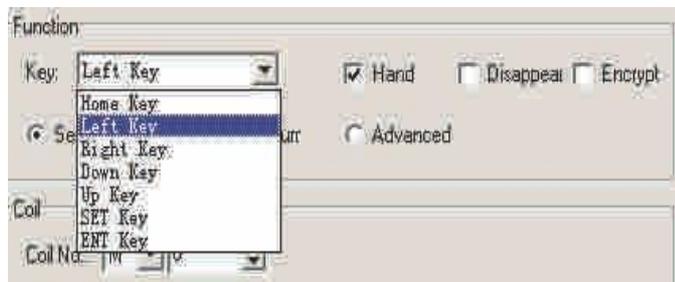
Set the appointed middle relay to be the reverse logic.

$\frac{3}{4}$ Momentary ON

When the key been pressed down, set the appointed middle relay to be ON; when the key pop up, set the appointed middle relay to be OFF.

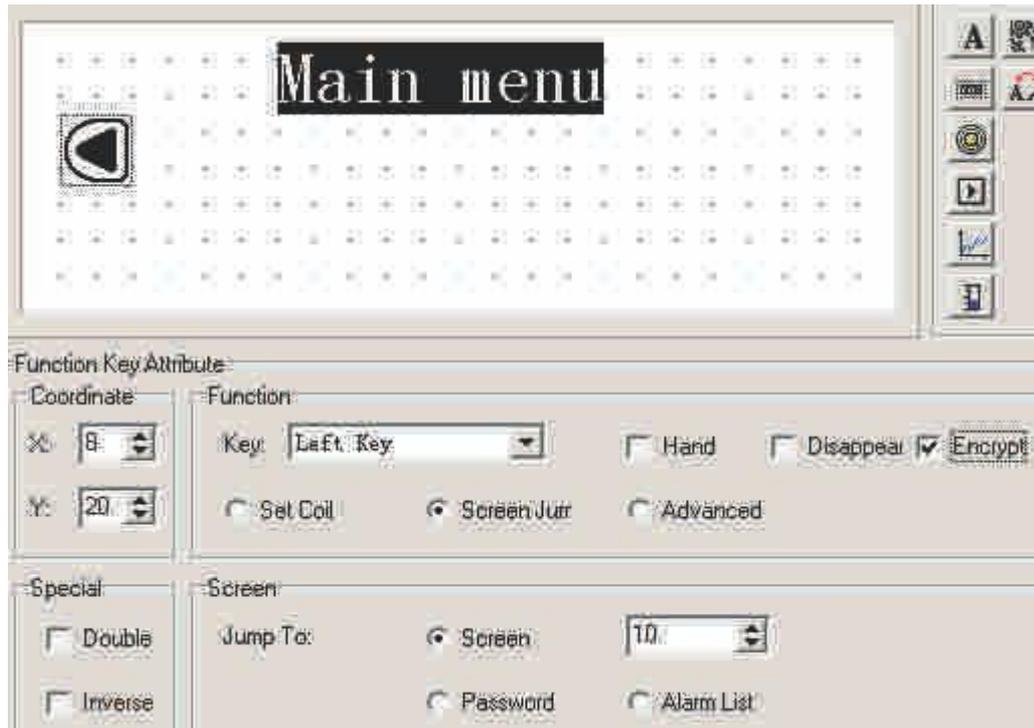


In the pull-down menu of “key”, there are seven keys. Choose the appropriate one among these.



Considering being brief, you can cancel hand display, then in the screen there will be only a button. After this set the function to be screen jump, here underside the screen set the jump screen’s ID number. Set the target screen’s ID number to be 10, i.e. the tenth screen is the parameter set screen.

In order to hide the set screen, set the “Encrypt” property to be valid. Only when the system’s password is opened can it jump to the NO.10 screen.

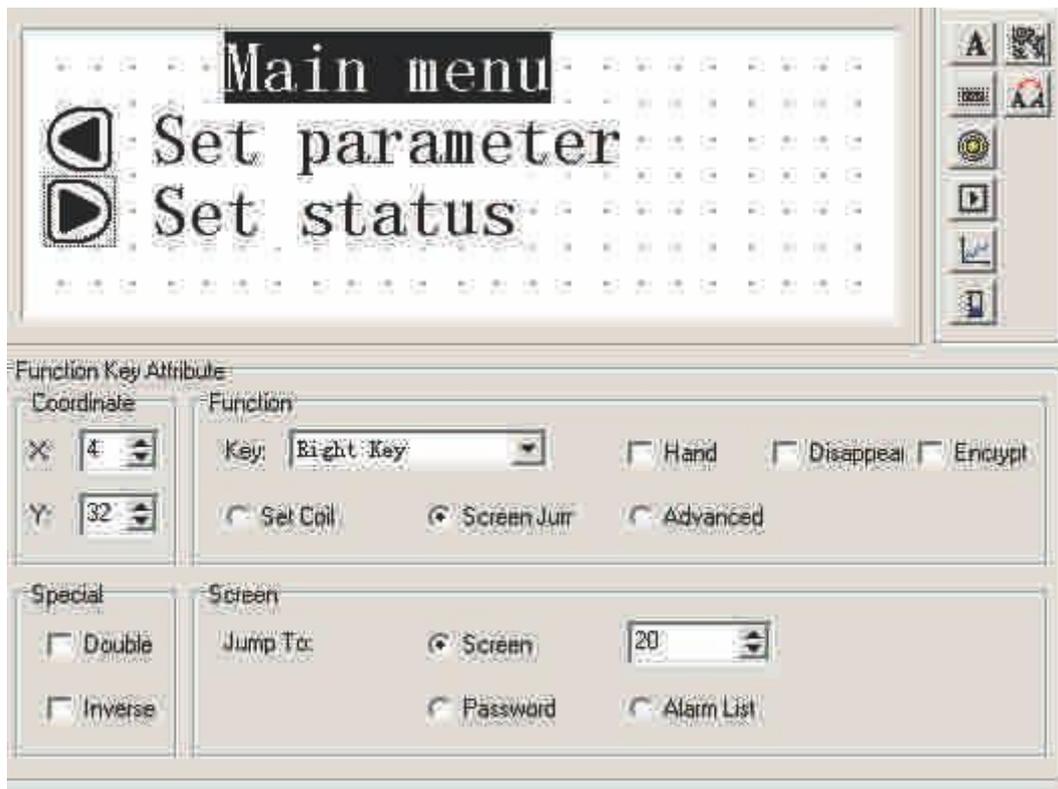
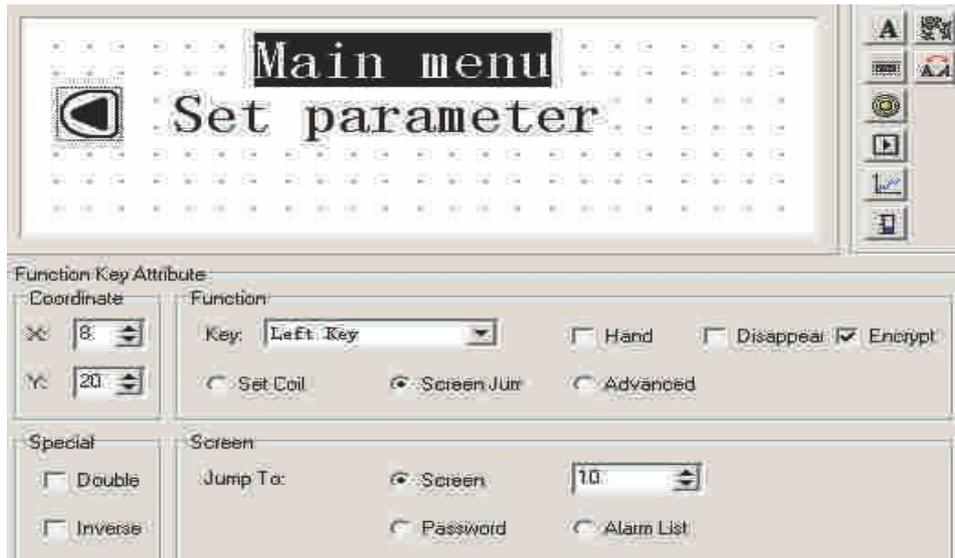


After set the function key, place text “set parameter” to the right of the button graph to prompt the operator. Click “<” key to enter parameter set screen directly.

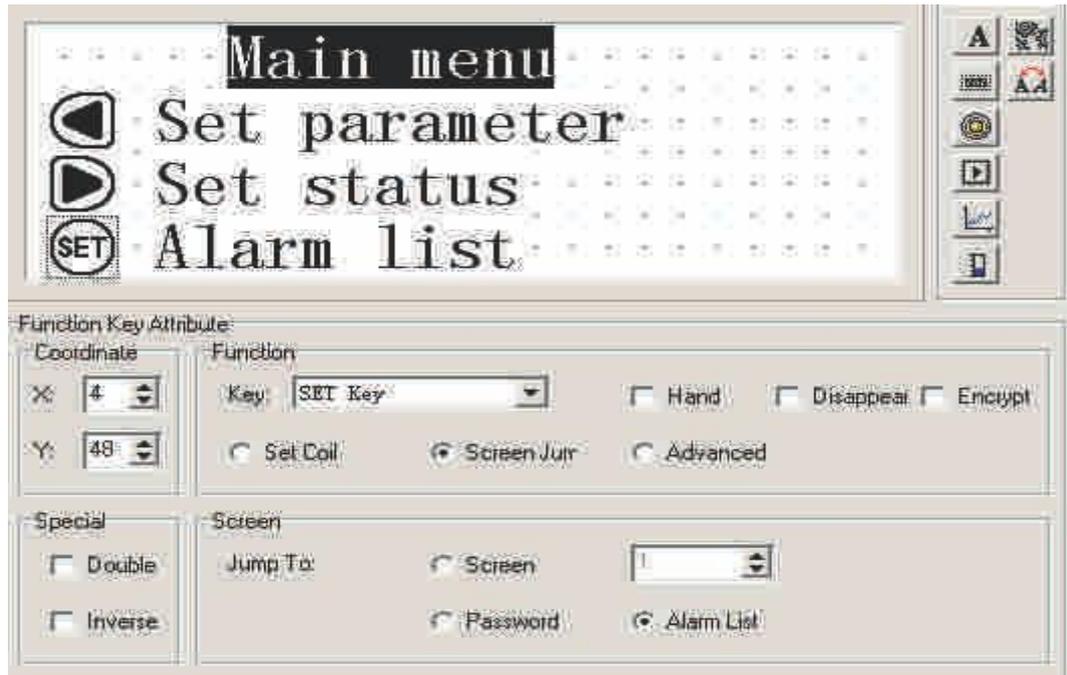
In the same way, place function key “>” and “state setting” in the right of the screen, that means click “>” key to enter state set screen.

You can set the NO.20 screen to be the state set screen.

Note: In order to insert a new screen, you’d better separate the screen’s No. of the different type of screens. E.g. if you want to add a parameter set screen, you can place it to the No.11 screen.



In the main menu screen, add an alarm screen jump key. When click this key, you can jump to the alarm list screen, refer to the alarm information.



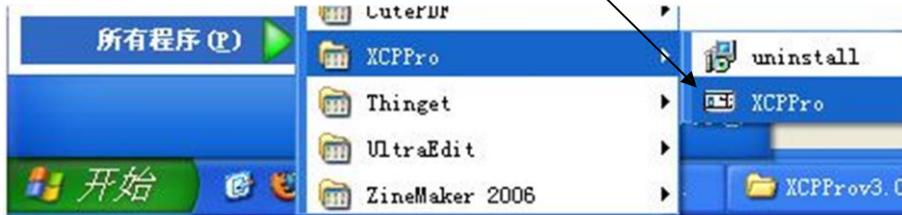
For the methods of log in the alarm information, you can refer to 2-2-14

Anexo B [80]

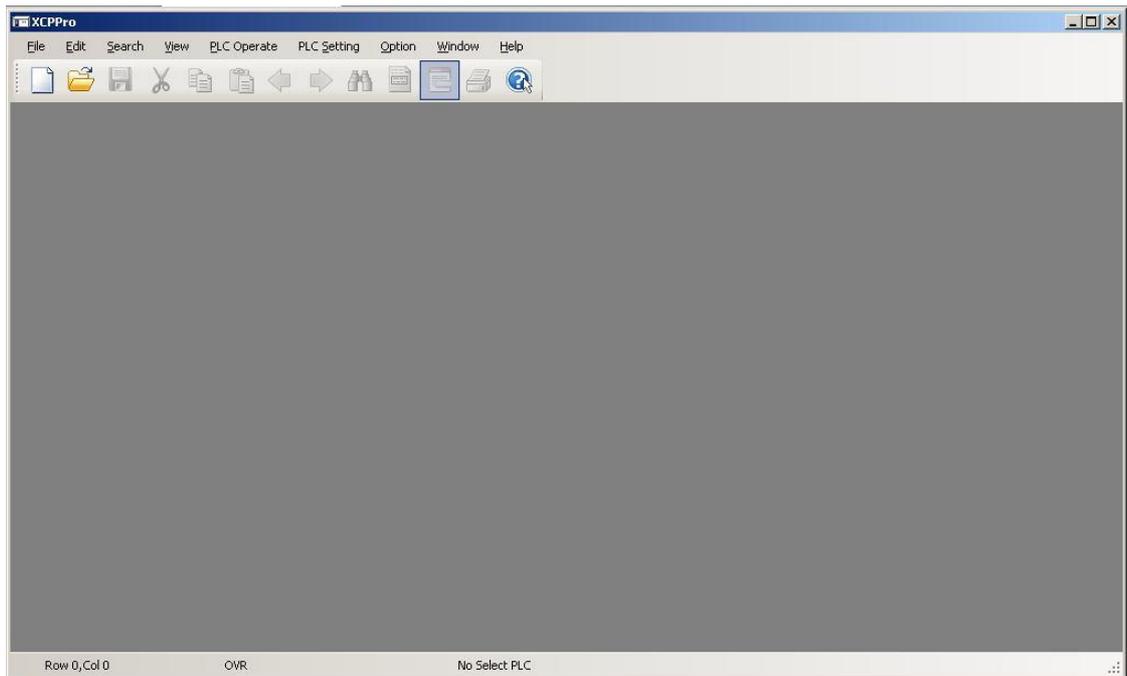
2-1. Open and close the XCP Pro

1、 Open the XCP Pro

(1) Choose "Start "→"All procedures"→"XCP Pro"→"XCPro.exe".



(2) When the XCP Pro has just started, the screen display as shown below:



Note: You can also double-click the shortcut icon "  " on the desktop to open the procedure.

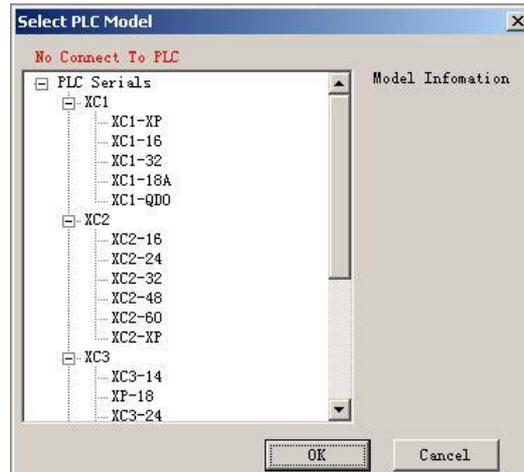
2、 Close the XCP Pro

Choose "File "→"Exit", or directly click the button "  ", the XCP Pro will be closed.

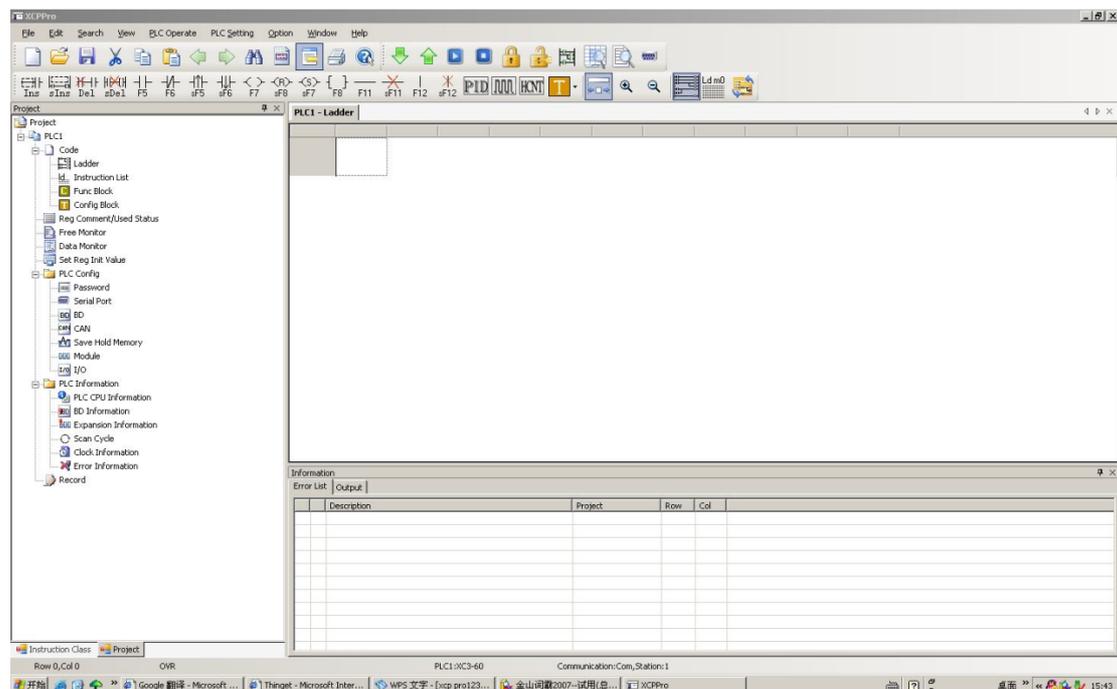
2-2. Create and open the project

1、 Create a new project

(1) Choose "File"→"New project Ctrl+N ", or click icon "", the PLC model selection windows will pop up. If PLC has connected currently, the software will automatically detect the model, as the default, as follows:



(2) Select the PLC model in the "Select PLC Model" windows, then click "OK", the establishment of a new project is completed. As shown below:



2. Open project.

Choose "File"→"Open project", or click icon " ", then select *. xcp type of file in the "Open PLC project file" dialog box, click the "open", it's completed.



Note: Usually, when you open a XCP project, the system backup the original file automatically, file named *. rak for reunification. When the need to use the file, change the suffix to be ". xcp", then open it in XCP Pro.

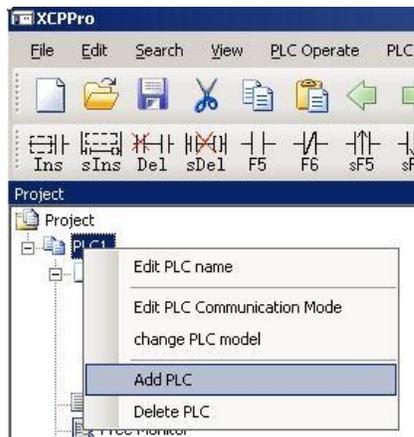
2-3. Add and delete the PLC mode

When project new created, it is defaulted for PLC1. When user needs to edit a number of PLCs, they can add multi-object to a interface.

1. Add PLC

Method 1 : Click "File"→"Add PLC".

Method 2 : In project column which is on the left side, right-click "PLC1"→"Add PLC", as follows:



When PLC is added successfully, it will be named "PLC2" acquiescently, and the project column in the left side will change also, as shown below:



When edit different PLCs, only need to click the plc simply. What's more, users can also modify appropriate name, edit communication mode, change models or delete operation on the corresponding PLC.

2. Delete models

Method 1: Right-click the PLC to delete directly, select "Delete PLC". Method 2: First select the PLC to delete, and then to "File"→"Delete PLC". After the operation, system will hint whether or not to delete, as follows:



To confirm the deletion, click "OK", otherwise, click "Cancel."

Note: The code between different PLC editor objects can copy each other, the code between different projects can also copy and paste.

Anexo C [81]

Procedure C: Thin Client using , Network IP

Once Procedure B has been completed, the next step is to enable to become the Web Server for your Thin Clients instead of NTWebServer. The following are the basic steps to configuring , although depending on your network and Operating System environment, additional settings may need to be configured such as user security.

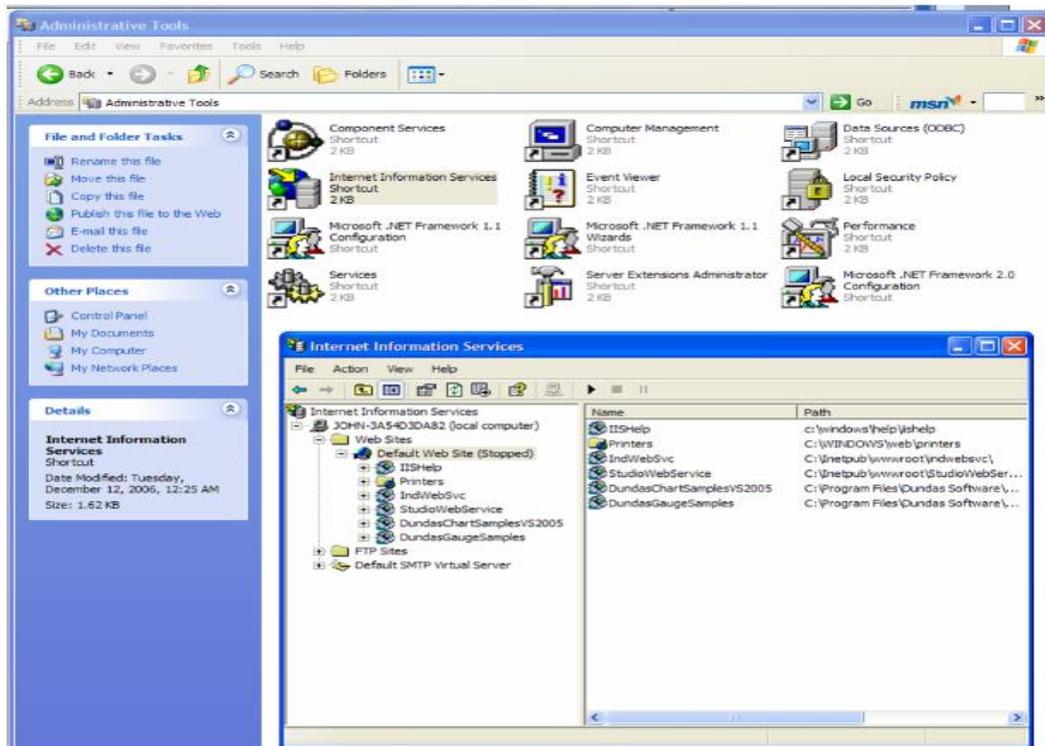
Step 1: Configure IWS Settings

Be sure NTWebServer is terminated.

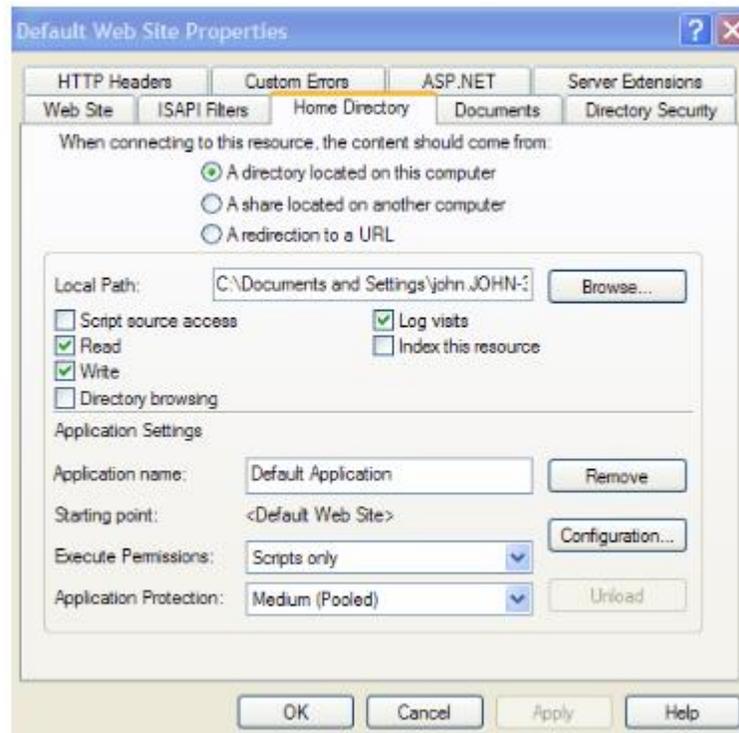
Click the Start button, then Control Panel > Administrative Tools.

Select (click on) Internet Information Services.

Expand the Web Sites tree structure to see the Default Web Site.



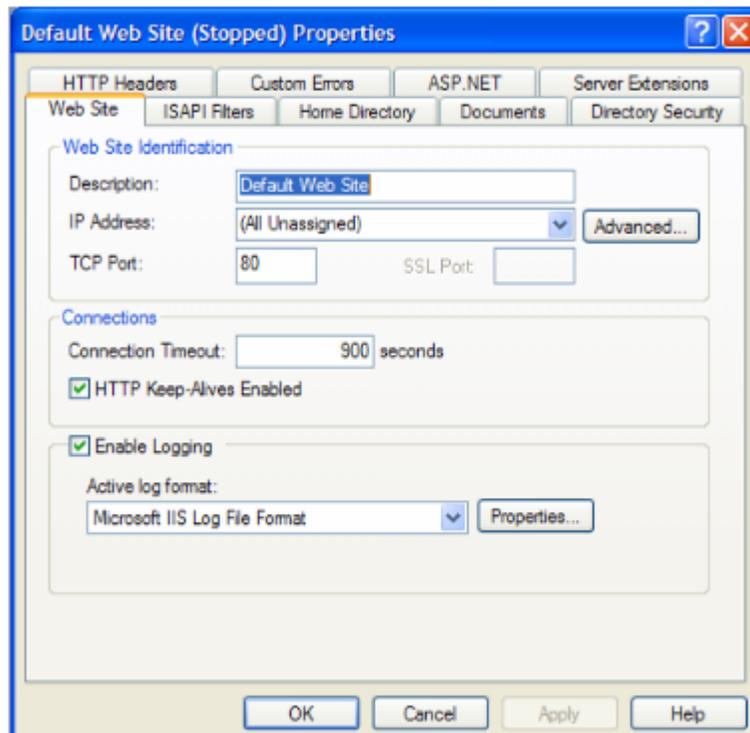
Right click on the Default Web Site and select Properties to get the Default Web Site Properties dialog.



Click on the Home Directory tab. Click on the Local Path Browse button and point to your project's Web subfolder.

Click on the Web Site tab. Make sure the TCP port is set to 80. You can click the Advanced button to enable the Web Server to respond to specific IP addresses and IP Port numbers.

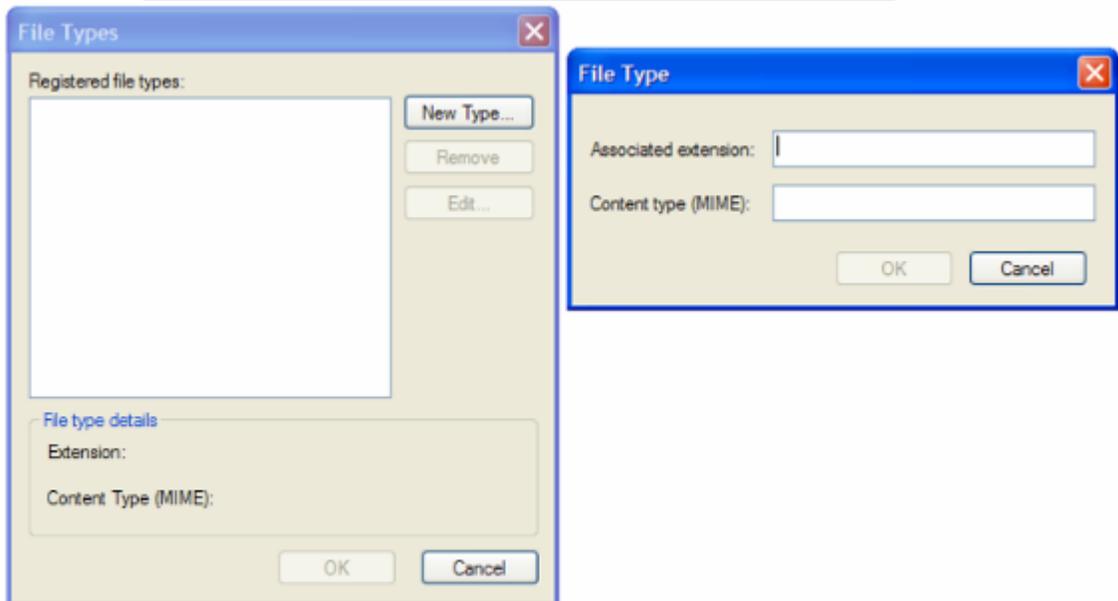
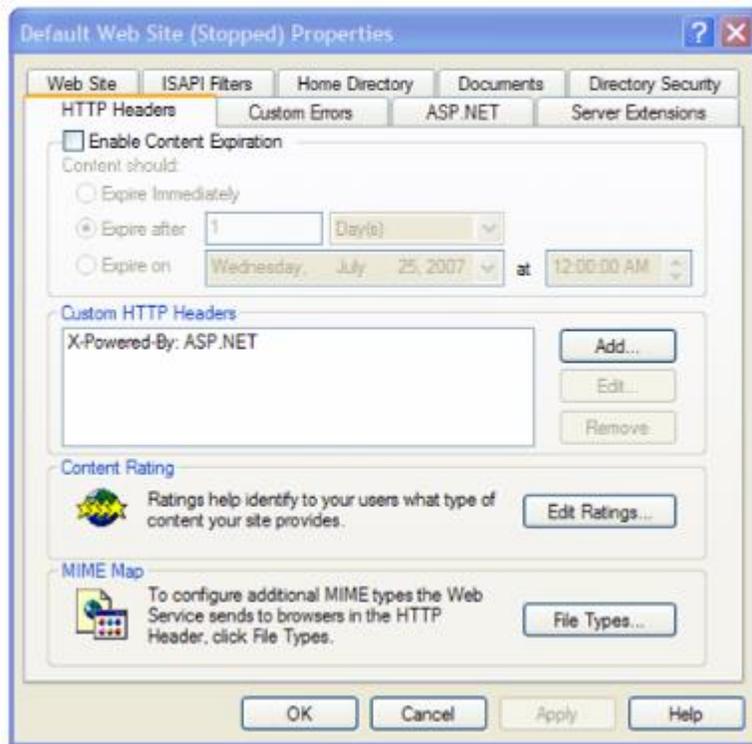
If your Web Server is behind a Proxy, be sure to check the HTTP Keep-Alives Enabled checkbox. It does not hurt anything if this is always checked.



Click on the HTTP Headers tab. Click on the MIME Map File Types button to open the File Types dialog. Next, click on the New Type button to add a new MIME type. Put the file extension in the Associated Extension field. In the Content type (MIME) field, put MIME type followed by a / character, followed by the file extension name (application/studio). E.g.

Associated Extension: .scc

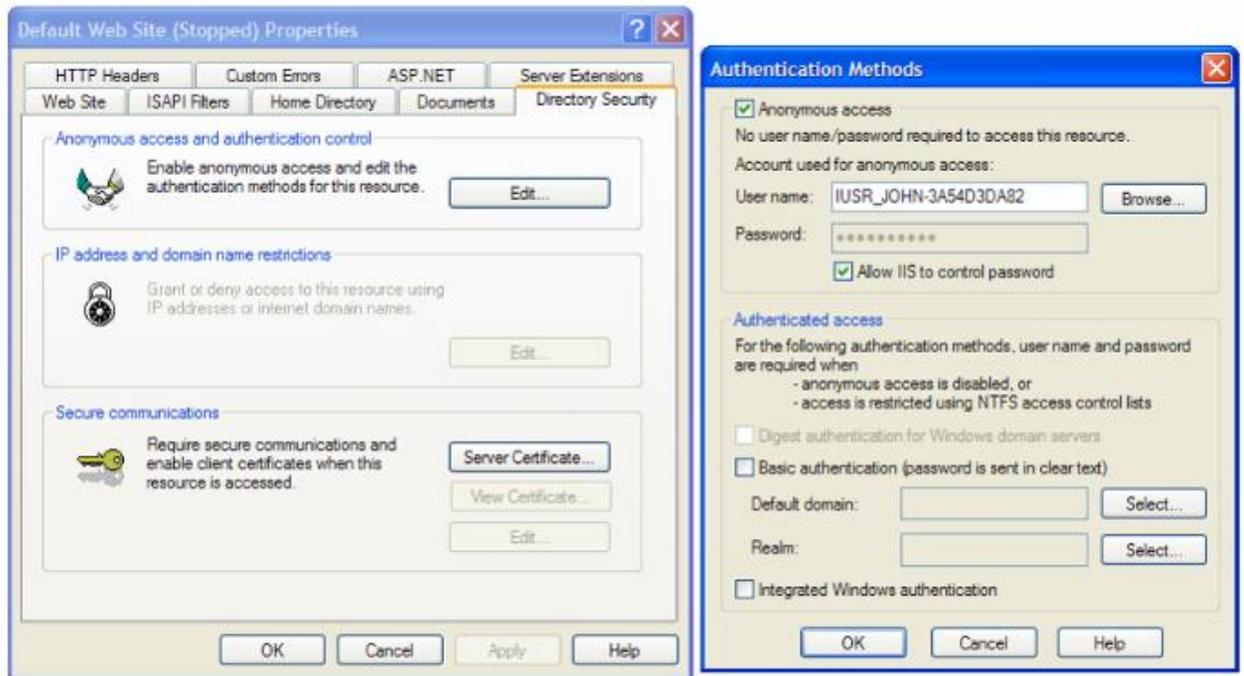
Content Type: application/studio



Click on the Directory Security tab. From this tab, you can change the settings for Anonymous User Access and Authentication Control as well as Secure Communications (i.e., using SSL 3.0).

Click on the Anonymous User Access and Authentication Control Edit button to get the Authentication Methods dialog. Normally, you do not have to do anything in this dialog but depending on the Security system your network administrator has installed, you may need to adjust settings in this dialog.

The Secure Communications Server Certificate button opens a wizard that lets you define a Certificate for support of secure communications using SSL.



About MIMEs

MIME, or Multipurpose Internet Mail Extensions, types instruct a Web browser how to handle files received from a server. For example, when a Web browser requests an item on a server, it also requests the MIME type of the object. Some MIME types, like graphics, can be displayed inside the browser. Others, such as word processing documents, require an external helper program to be displayed.

When a server delivers a Web page to a client Web browser, it also sends the MIME type of the data it is sending. If there is an attached or embedded file in a specific format, the server also tells the client program the MIME type of the embedded or attached file. The client program then knows how to process or display the data being received from

serves only files with known extensions registered in the MIME types list or with the operating system. allows you to configure additional MIME types and change or remove MIME types. Removing a MIME type in does not block access to that MIME type by other programs if it is also registered with the operating system.

is preconfigured to recognize a default set of global MIME types. These MIME types are recognized by all Web sites you create in . MIME types can also be defined at the Web site and directory levels, independent of one another or the types defined globally. When you view MIME types at the Web site or directory level, only the types unique to that level are displayed, not all types inherited from the next level up.

returns a 404.3 error if a client request refers to a file name extension that is not defined in the MIME types

MIME configuration is usually only required for Windows Server 2003, not Windows XP or Vista due to Windows 2003 default settings.

MIME types should include all file extensions found in the Web directory. These include:

.app

.bin

.csv

.gis

.html

.ico

.ini

.lst

.scc

.sg

.stmp

.tra

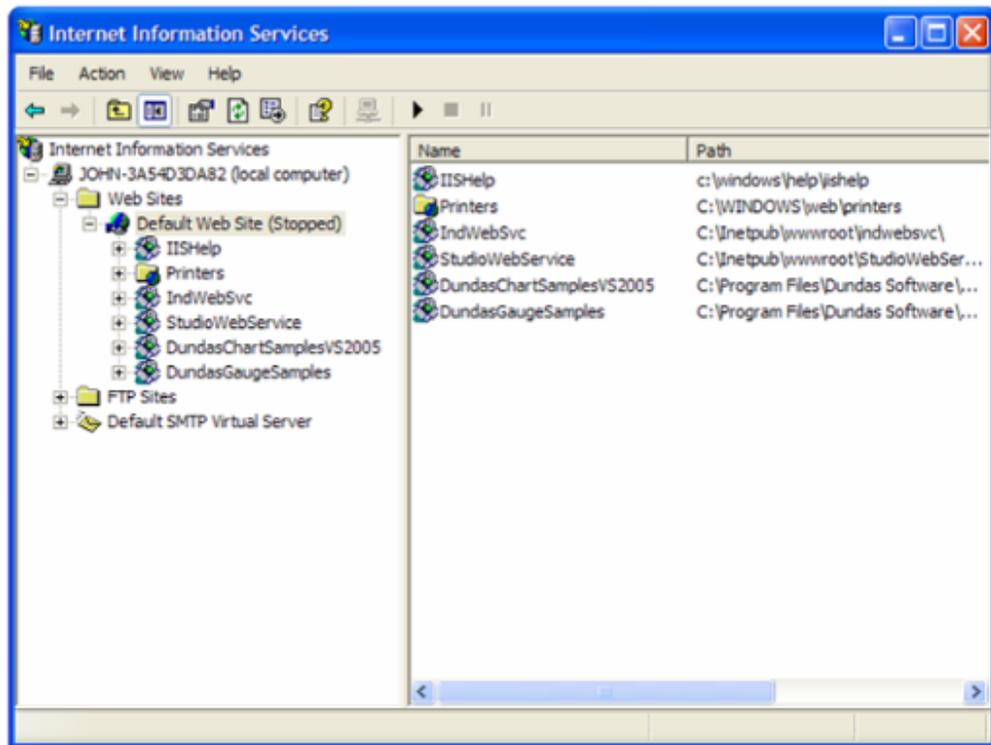
.txt

Step 2: Start and start the IWS Project

Be sure NTWebServer is terminated.

Click on the Start button.

Run the project.



Notes:

If is not installed on your PC, you can add it (to Windows XP Pro/Windows 2000 or Windows Server 2003) by opening the Control Panel, then selecting Add/Remove Programs > Add/Remove Windows Components and checking the Internet Information Services () checkbox in the Windows Components Wizard. You can click on the Details button to select various components of to install. Note that you may need to have your Windows installation disk.

You can get more information on by opening a browser and entering <http://localhost/iishelp> in the browser navigation address bar. Note that must be running.

NTWebServer is a Windows program, while is a Windows service.

It is STRONGLY SUGGESTED that you use instead of NTWebServer in a runtime mode. It is more reliable and higher performance than NTWebServer.

Troubleshooting:

If you get a Cannot find Server error message,

From the browser, ping the server IP address (primary and/or backup). You can ping using the IP address or use the NetBios name to ping the server (e.g., from a command prompt enter

Ping 152.57.100.25 or Ping ServerName.

Be sure is running

Be sure your project is running

Make sure the TCP/IP Server (in the project's Tasks) is running

Be sure is set to the correct Home Page (root directory).

Be sure the Port addresses are correct (HTTP – Port 80, HTTPS (SSL) – Port 443, Data – Port 1234)

Make sure you firewall has these ports open

If you are using a Windows Embedded device, be sure ISSymbol is properly loaded and registered

Be sure your runtime license supports the Web Client configuration

If you get a Page cannot be displayed error message,

From the browser, ping the server IP address

Stop and restart

Be sure the MIME types are properly set

Make sure you updated your web pages (i.e., Save as HTML) and use the Verify Project tool if you change any Web settings.

Verify the Windows security settings are properly set

Be sure that the Screen name (and Web Page name) do not have any spaces in the name

If the web pages are incorrect:

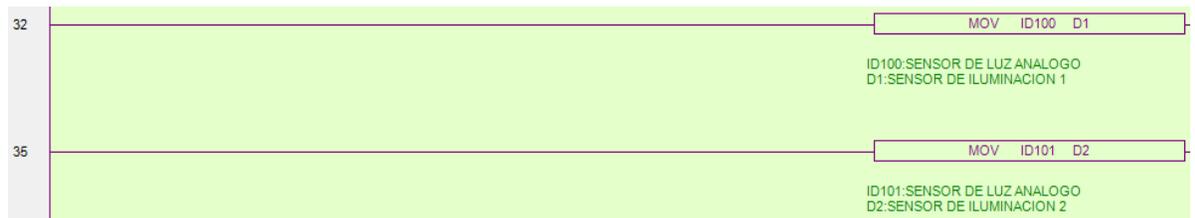
Be sure you are pointing to the correct primary URL

Be sure your backup URL (if you use it) has the correct (updated) web pages

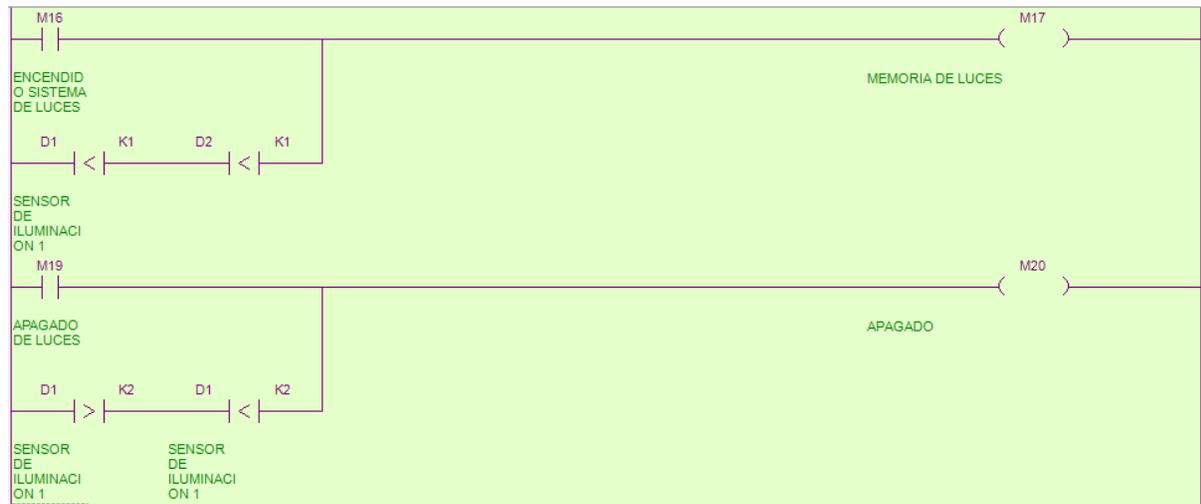
Anexo D

❖ Programacion KOP para el sistema de luces

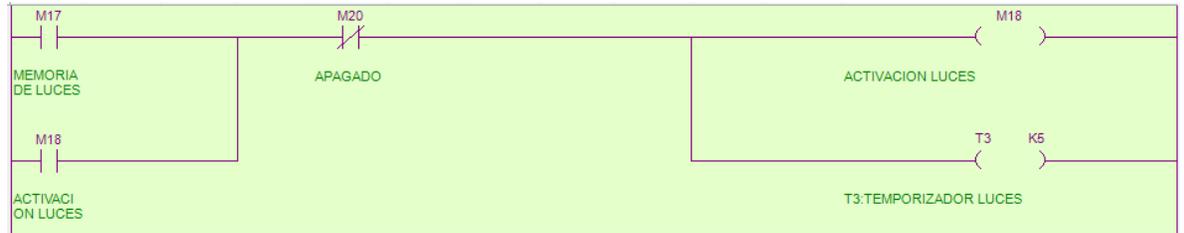
- Entrada análoga PLC THINGET



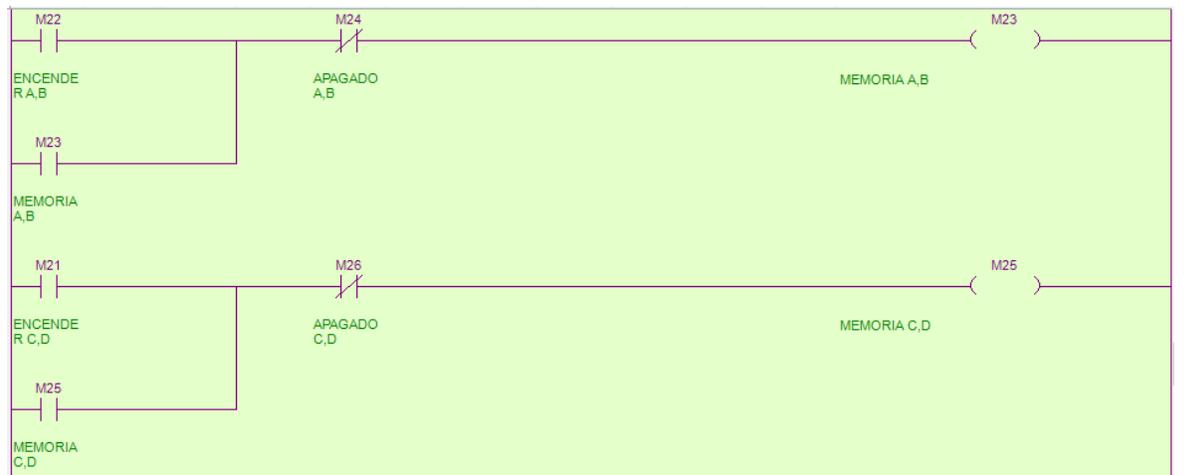
- Encendido temporizado a través de interfaz y/o sensor



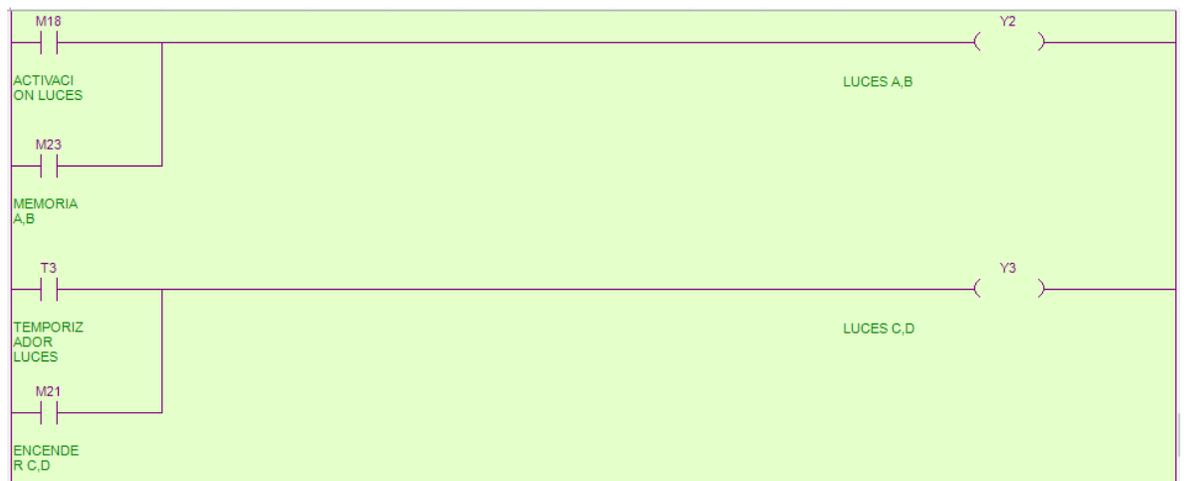
- Uso temporizador



- Inicio parcial sistema de iluminación

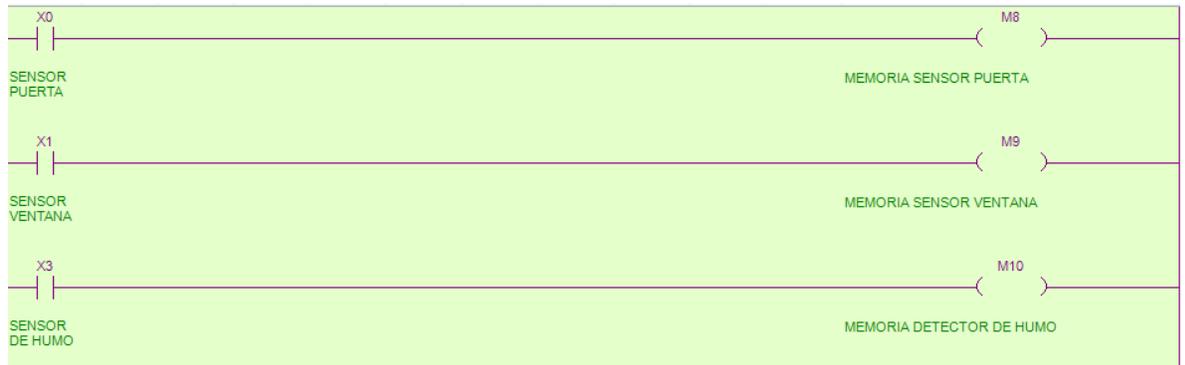


- Salidas a relé del sistema de iluminación

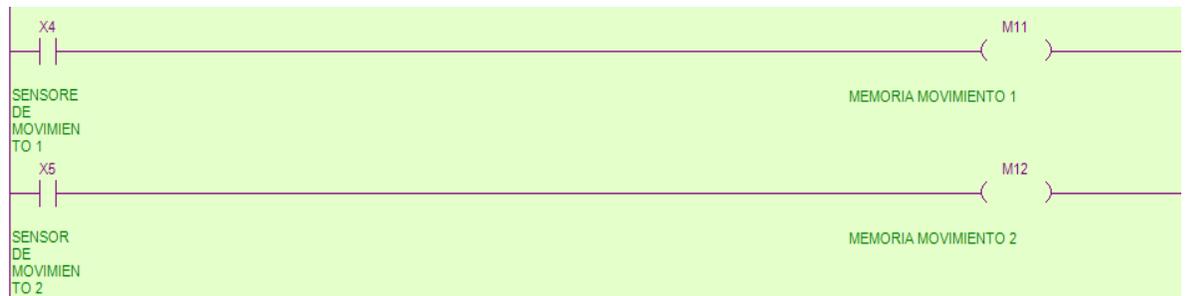


❖ Programacion KOP para el sistema de seguridad

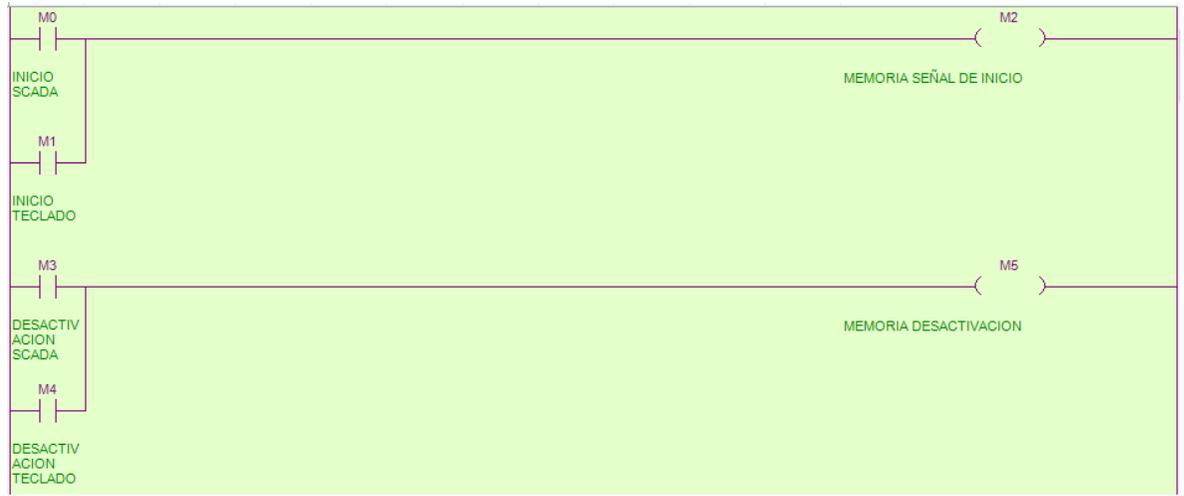
- Entradas digitales X0, X1, X3



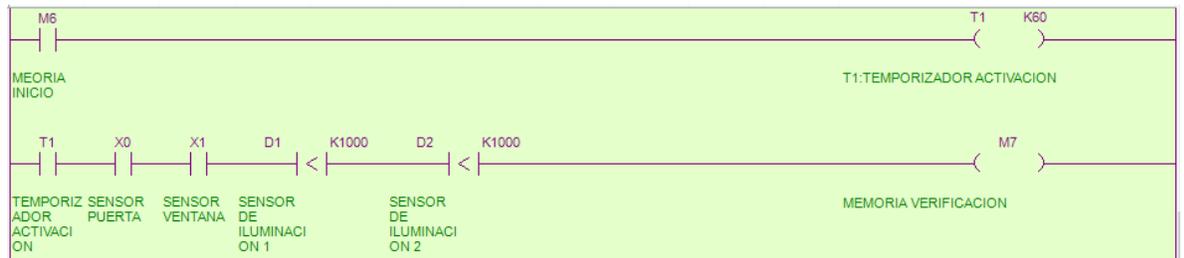
- Entradas digitales X0, X1, X3



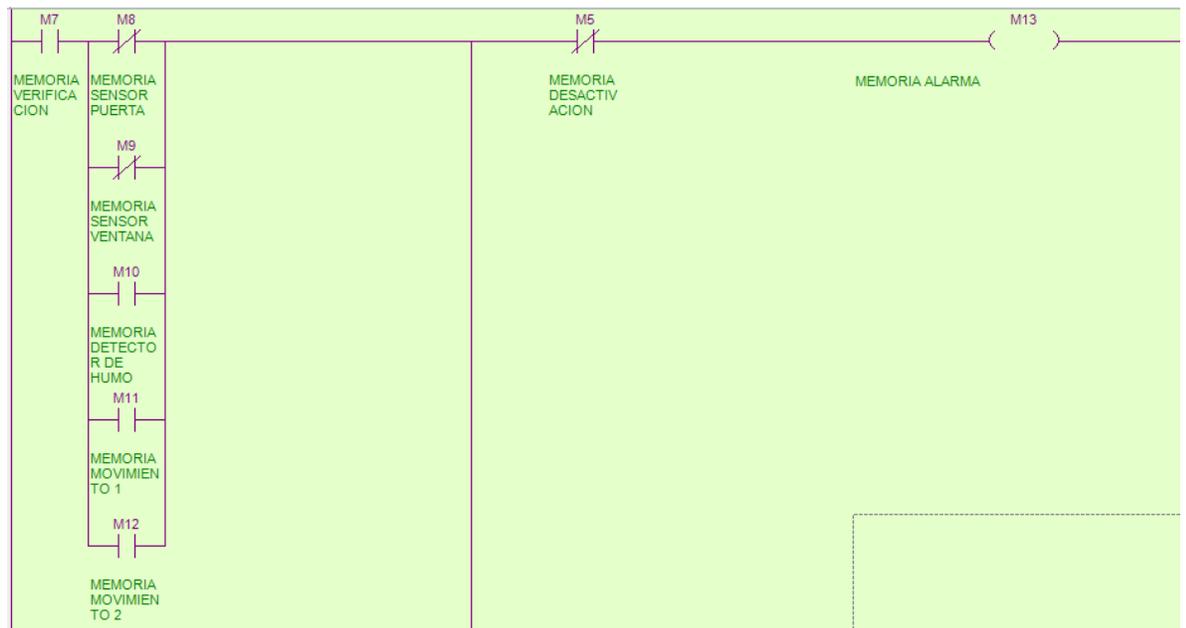
- Activación y desactivación de la alarma general



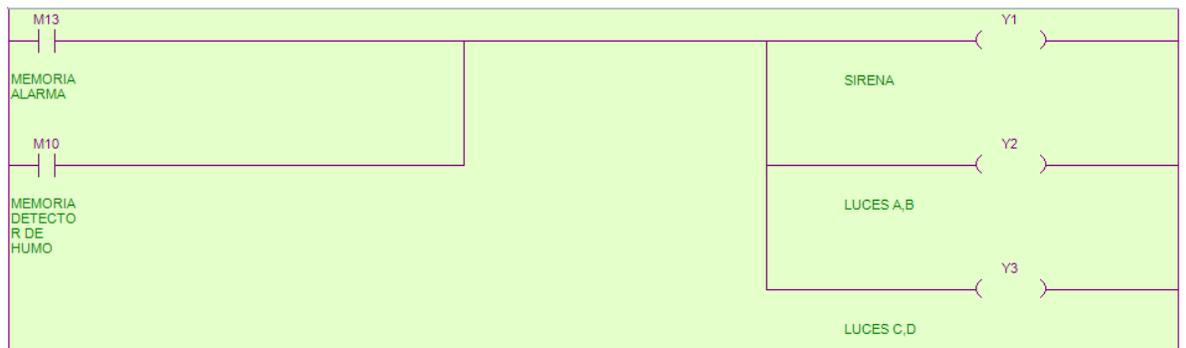
- Conexión en serie de los diferentes sensores



- Conexión en paralelo de la entradas de los sensores llevadas a una memoria de alarma



- Salidas a relé de sirena y luces



Anexo E [82]

6 ■ Gestión de riesgos de seguridad

6.1. INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS SCADA

Antes de tratar en mayor profundidad la seguridad en los sistemas SCADA, es necesario enunciar tres necesidades fundamentales de los sistemas de información. Son las siguientes:

1. **Confidencialidad.** Es la propiedad de la información por la que se garantiza que es accesible únicamente para las personas autorizadas. Por ejemplo, proteger un ordenador con una contraseña es una buena medida para aumentar la confidencialidad de los datos almacenados en él.
2. **Integridad.** Se refiere a la exactitud de los datos, concretamente a la necesidad de asegurar que éstos no han sido manipulados o alterados. Por ejemplo, un error en las comunicaciones puede suponer una pérdida o una distorsión de la información transmitida, por lo que para evitarlo se pueden emplear mecanismos que comprueben la integridad de dicha información.
3. **Disponibilidad.** Es la capacidad de un sistema de estar operativo para realizar las funciones para las que ha sido diseñado. Por ejemplo, cuando una página web no puede ser visitada, se puede decir que ese sistema tiene un problema de disponibilidad.

Mientras que en un sistema informático tradicional la prioridad suele ser la confidencialidad, seguida de la integridad y finalmente de la disponibilidad, en un sistema de monitorización y control en tiempo real lo primordial es garantizar la disponibilidad del servicio y del sistema. Esto es debido principalmente a que su objetivo esencial es mantener en funcionamiento el proceso para el que ha sido creado, además de considerarse como tareas vitales para las empresas e incluso en algunos casos Infraestructuras Críticas para la sociedad.

Este enfoque de prioridades se ha mantenido desde la aparición de estos sistemas hasta la actualidad: los sistemas de monitorización y control en tiempo real son muy robustos funcionalmente, ofreciendo un servicio casi ininterrumpido. Sin embargo, esta desproporcionada priorización de la disponibilidad, unida a otras causas, ha generado una ausencia de seguridad notable en algunos aspectos.



Por ejemplo, se puede tender a no cifrar la información, consiguiendo así mayor rapidez ya que el cifrado y descifrado de la información puede influir negativamente en la disponibilidad. Pero en contrapartida se penalizaría la seguridad, ya que cualquier individuo podría capturar la información en un formato comprensible.

6.2. MOTIVACIÓN Y ORÍGENES DE LOS RIESGOS Y AMENAZAS

Desde sus orígenes, los sistemas de monitorización y control en tiempo real han sido un objetivo de potenciales ataques con distintas motivaciones. Este foco de atención se ha debido principalmente a la propia funcionalidad de estos sistemas, que ofrecen la posibilidad de manipular el entorno físico remotamente, o al menos recabar información de algún proceso en tiempo real. Sin embargo, estos riesgos y amenazas, debido al aislamiento característico de estos sistemas, en sus orígenes se limitaban principalmente a ataques físicos y ataques internos.

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

- **Empleados descontentos.** Estos incidentes cobran especial relevancia debido al conocimiento que tienen dichos empleados sobre el sistema, así como los permisos que tienen asignados para su trabajo diario. Hay que incluir en este caso la posibilidad de acceso por parte de ex-empleados al contar con conocimientos similares.
- **Espionaje industrial.** Aunque este tipo de incidentes son inusuales, una compañía rival podría por ejemplo suministrar al empleado de una empresa algún tipo de software malicioso que produzca acciones no autorizadas sobre el sistema de monitorización y control en tiempo real, ya sea alteración de las comunicaciones, robo de información, o realización de operaciones arbitrarias. Este software podría encontrarse, por ejemplo, en un dispositivo de almacenamiento USB a la espera de ser conectado a un equipo del sistema SCADA para infectarlo.
- **Hackers.** Genéricamente, bajo este término se engloba a cualquier persona con conocimientos técnicos avanzados que realice acciones que vulneren la seguridad de un sistema. Las motivaciones de este tipo de personas pueden ser muy variadas, desde la depuración y resolución de

errores en los sistemas, hasta la intrusión con fines maliciosos, pasando por aspiraciones como comprobar el nivel de conocimientos y las habilidades de intrusión.

- **Activismo ideológico.** Pueden existir grupos u organizaciones que, por motivos ideológicos, se marquen como objetivo los sistemas de monitorización y control en tiempo real de alguna compañía o administración. Entre estas motivaciones ideológicas se pueden encontrar razones políticas, medioambientales, sanitarias, éticas, etc.
- **Terrorismo.** Debido a la criticidad de las instalaciones o servicios controlados por algunos de estos sistemas, se pueden convertir en el objetivo de ataques terroristas.
- **Incidencias accidentales.** Como en todo sistema, muchos de los riesgos podrían tener como causa simples accidentes, desde desastres naturales a incendios de pequeño alcance.

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

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

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

Sin embargo, el desconocimiento general de la tecnología empleada no puede considerarse un mecanismo de seguridad aceptable. Una persona interesada



en atacar un sistema de monitorización y control en tiempo real siempre podría estudiar y analizar una instalación, desarrollando y empleando diversas técnicas de recopilación de información. Por ello, un exceso de confianza en el modelo de seguridad por oscuridad puede generar o agravar ciertas amenazas.

- **Minimización o desestimación de riesgos y amenazas.** Muchos responsables de sistemas de monitorización y control en tiempo real consideran que sus instalaciones carecen de interés para potenciales atacantes, lo que a su juicio reduce la necesidad de seguridad de las mismas. Este hecho no se corresponde con la realidad, ya que un sistema que supervisa y gestiona procesos en tiempo real siempre va a ser un objetivo en potencia para atacantes. Por otro lado, no hay que olvidar que buena parte de los ataques proceden del interior de la propia compañía u organización (empleados descontentos o antiguos trabajadores/colaboradores).
- **Interconexión creciente.** Los sistemas de monitorización y control en tiempo real, desde sus orígenes, fueron diseñados para permanecer aislados del exterior, situación que actualmente se ha modificado en muchas ocasiones. Un claro ejemplo de este hecho es que no fueron pensados para estar interconectados con redes como Internet o las redes corporativas. Esto ha provocado la aparición de nuevos riesgos o amenazas para los que no estaban diseñados al incorporarse este tipo de conexiones.
- **Arquitecturas de red poco seguras.** Muy relacionado con los demás factores. En algunas ocasiones se han incorporado sistemas de comunicación poco seguros que posibilitan la intrusión en el sistema o la interceptación, falsificación y/o bloqueo de las transmisiones entre los dispositivos.
- **Configuraciones por defecto.** No modificar las configuraciones con las que cuentan los equipos y dispositivos desde su fabricación facilita enormemente la intrusión y manipulación de los mismos.
- **Ausencia de concienciación del personal.** Debido al nuevo escenario en el que se encuentran los sistemas de monitorización y control en tiempo real, la labor de concienciación del personal, tanto del operativo como de la alta dirección, se ha hecho más necesaria. Un punto en el que debe ahondar esta

concienciación son los cambios que han sufrido este tipo de sistemas, el detrimento en seguridad que esto puede producir y la importancia del cumplimiento de las medidas que solventen o mitiguen estos inconvenientes.

- **Uso de tecnologías y soluciones de propósito general.** El uso de tecnologías de propósito general ofrece mayor flexibilidad y supone una reducción de costes considerable, aunque por otro lado implica que, debido a que los ataques contra este tipo de tecnología son bastante comunes, los sistemas de monitorización y control pasen a ser un objetivo más fácil.
- **Escasa evolución.** Debido a que el objetivo principal es su disponibilidad, los sistemas de monitorización y control en tiempo real suelen sufrir muy pocas modificaciones a lo largo del tiempo, ya que se consideran peligrosas: cualquier cambio puede introducir algún fallo o problema que afecte negativamente en su rendimiento o incluso paralizar el proceso al que se dedica. Asimismo, estos cambios suelen acarrear un alto coste económico, debido en buena medida a la especialización de los componentes y al amplio ámbito geográfico en el cual suelen estar desplegados.



6.3. IDENTIFICACIÓN Y ANÁLISIS DE LOS PRINCIPALES RIESGOS Y AMENAZAS

Una vez descritas las fuentes de amenaza que pueden encontrarse respecto a los sistemas de monitorización y control en tiempo real, se presentan los principales riesgos, ya sean estos técnicos o de gestión.

Usos inadecuados

La concienciación en cuanto a la seguridad relativa a los sistemas de monitorización y control en tiempo real se ha focalizado tradicionalmente en su vertiente física, no lógica o informática. Esta es una de las principales causas de la inseguridad en estos sistemas. El desconocimiento de los riesgos reales posibilita en muchas ocasiones que los propios empleados, sin ánimo de poner en riesgo el sistema, realicen acciones que podrían comprometer la seguridad. Ejemplos de estas prácticas podrían ser la conexión de dispositivos no asegurados, utilizando los puertos USB, o simples conexiones a través de Internet.



Bloqueo/Intercepción/Falsificación de las comunicaciones

Las comunicaciones entre los dispositivos o de éstos con el puesto de control, en caso de no realizarse mediante un canal modo seguro, podrían ser bloqueadas, interceptadas o falsificadas. En el caso de un bloqueo, la principal consecuencia sería la pérdida de contacto y por tanto de control de algún dispositivo de campo. En cambio, una intercepción de las comunicaciones supondría un riesgo para la privacidad, pudiendo poner al descubierto información sensible respecto al funcionamiento del sistema. Pero sin duda el mayor riesgo sería la falsificación de las comunicaciones, que podría utilizarse para forzar un error inducido.

Los errores inducidos son consecuencia del refinamiento de un ataque, en el cual el objetivo es provocar que se cometan errores al tomar decisiones, automáticamente por el sistema o personalmente por los trabajadores, que provoquen un mal funcionamiento en los procesos controlados.

Este ataque suele realizarse mediante el envío de información errónea, haciendo creer que se ha producido un cambio frente al que hay que actuar, de modo que se trate de solucionar un problema inexistente generando otro. De esta forma, el atacante lograría su objetivo de una forma más sutil, ya que el incidente parecería haber sido producido por un error humano.

Este modelo de ataque también puede utilizarse para encubrir una manipulación, enviando información que indique que no se producen cambios de relevancia cuando sí están ocurriendo. De este modo se trataría de evitar las posibles acciones correctoras que inutilizaran la manipulación.

Virus informáticos o malware

Debido a lo usual de la existencia de software desactualizado y/o configuraciones por defecto, estos sistemas pueden ser vulnerables a los virus informáticos y demás malware que son conocidos desde hace tiempo y para los que ya existen soluciones de prevención. Además del malware de ámbito genérico, hay que señalar la posibilidad de generación de nuevos códigos maliciosos específicos para este tipo de sistemas.

Accesos no autorizados

El desconocimiento de la conectividad del sistema, la utilización de configuraciones por defecto en los mecanismos de acceso y las arquitecturas de red poco seguras, pueden facilitar el acceso no autorizado al sistema de monitorización y control. Este acceso puede comprometer la privacidad de la información acerca del sistema, pero de manera muy especial puede ser un riesgo de importancia en caso de lograr controlar el sistema, pudiendo modificar en el acto el proceso controlado o cambiar las órdenes y protocolos establecidos para su funcionamiento automático, de modo que las consecuencias de estas modificaciones podrían darse tiempo después de la intrusión.

Todo ello da lugar a un riesgo muy importante, ya que cualquier persona con un nivel de conocimiento técnico medio, podría al menos detectar los dispositivos y equipos de este tipo de sistemas. Por ello es necesario diseñar una arquitectura de red segura que permita evitar estas prácticas.

Ataques externos

Mediante este tipo de ataques, usuarios malintencionados pueden hacer uso de distintas herramientas que se encuentran publicadas en Internet para tomar el control, desestabilizar o dañar los sistemas de una organización. No es necesario, por tanto, contar con grandes conocimientos técnicos, ni equipamiento específico, para perpetrar este tipo de ataques.

Debido a que la tendencia actual de las redes SCADA es la de interconectarse a través de redes como Internet o las redes corporativas, es posible realizar ataques desde redes externas a la organización.

Uno de los ataques externos más dañinos para los sistemas SCADA son los conocidos como de Denegación de Servicio (ataques DoS), mediante los cuales un recurso deja de ser accesible para los usuarios legítimos. Normalmente, el objetivo de este tipo de ataques es agotar los recursos disponibles de la red, de tal manera que se provoca una pérdida de la conectividad con los sistemas.



Sabotaje

La mayoría de los ataques notorios son internos. Muchas organizaciones consideran que adoptar unas medidas de seguridad perimetrales robustas es suficiente para mantener un nivel de seguridad adecuado, protegiéndose así de ataques externos pero manteniendo las vulnerabilidades internas.

Igualmente, en muchas ocasiones se considera que los empleados, o bien no tienen los suficientes conocimientos técnicos para perpetrar un ataque, o bien no tienen motivaciones para consumarlos. Esta creencia da lugar a que no se tomen medidas de seguridad que contemplen la posibilidad de ataques por parte de empleados descontentos o motivadas por el espionaje industrial.

Es importante recalcar que este tipo de ataques pueden perpetrarse sobre la infraestructura de soporte de las organizaciones, tales como el soporte energético y la climatización de sistemas, y no únicamente sobre el sistema SCADA de forma directa.

Estos riesgos afectan a los sistemas de monitorización y gestión en tiempo real del mismo modo que al resto de sistemas TIC, pudiendo afectar especialmente al suministro eléctrico o a las comunicaciones. En el caso de estos sistemas, la redundancia de estos servicios es más habitual al ser prioritario su funcionamiento, por lo que suele existir mayor concienciación al respecto.