

Instituto Tecnológico de Costa Rica

Escuela de Ingeniería Electrónica



**DISEÑO Y DESARROLLO DE UN SISTEMA DE DOMÓTICA PARA LA
EMPRESA TECNOLÓGICA DE COSTA RICA S.A**

**Informe de Proyecto de Graduación para optar por el título de Ingeniero en
Electrónica con el grado académico de Licenciatura**

Javier Enrique Brenes Alfaro

Cartago, Abril de 2011

INSTITUTO TECNOLOGICO DE COSTA RICA
ESCUELA DE INGENIERIA ELECTRONICA
PROYECTO DE GRADUACIÓN
TRIBUNAL EVALUADOR

Proyecto de Graduación defendido ante el presente Tribunal Evaluador como requisito para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura, del Instituto Tecnológico de Costa Rica.

Miembros del Tribunal



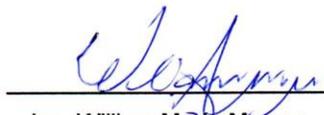
Ing. Néstor Hernández Hostaller

Profesor lector



Ing. Marvin Hernández Cisneros

Profesor lector



Ing. William Mañín Moreno

Profesor asesor

Los miembros de este Tribunal dan fe de que el presente trabajo de graduación ha sido aprobado y cumple con las normas establecidas por la Escuela de Ingeniería Electrónica

Cartago, 2 de Mayo del 2011.

Declaratoria de autenticidad

Declaro que el presente Proyecto de Graduación ha sido realizado enteramente por mi persona, utilizando y aplicando literatura referente al tema e introduciendo conocimientos propios.

En los casos en que he utilizado bibliografía, he procedido a indicar las fuentes mediante las respectivas citas bibliográficas.

En consecuencia, asumo la responsabilidad total por el trabajo de graduación realizado y por el contenido del correspondiente informe final.

San Jose, 27 de Abril del 2011



Javier Enrique Brenes Alfaro

Céd: 1-1131-0442

Resumen

Las empresas de base tecnológica ven en la integración de sistemas una forma de proporcionar soluciones más atractivas a sus clientes, así como un medio muy importante para incrementar esta cartera.

Cada vez más, estas empresas escogen seguir este camino como parte de su estrategia de mercado, un mercado en el cual se hace extremadamente necesario diferenciarse y asumir nuevos riesgos que las hagan crecer en competitividad en diversos ámbitos y que a la postre se traduzcan en nuevas inversiones para sus negocios.

Dentro de este entorno, la empresa Tecnológica de Costa Rica S.A. ha decidido continuar con el proceso de unificación de tecnologías que ha venido implementando, al crear una integración del sistema de seguridad que representa con un sistema de automatización de edificios, el cual le permitirá comenzar a construir su propio sistema centralizado de control, también llamado BMS (*Building Management System*).

El presente proyecto proporciona, como parte principal de esta visión, el paso necesario para lograr comunicar tecnologías y protocolos de dos sistemas que actúan bajo plataformas muy diferentes y que permitirán a la empresa diferenciarse dentro del competitivo mercado tecnológico nacional y regional.

Palabras clave: Integración, BMS, LENEL, WACI NX+, ODBC, Visual Basic.

Abstract

Technology-based companies are in Systems Integration a way to provide attractive solutions to their customers and an important means to increase this portfolio. Increasingly, these companies choose to follow this path as part of its market strategy, a market which is extremely necessary to differentiate and take on new risks that make them grow in competitiveness in various areas and eventually lead to further business investment.

Within this environment, the company Tecnológica de Costa Rica SA has decided to continue the process of technology unification that has been implemented, creating integration between their security system and a building automation system, which allows them to start building their own system of centralized control also called BMS (Building Management System).

This project provides, as major parts of this vision, the necessary step to achieve communicate technologies and protocols of two operating systems on different platforms and allow the company to differentiate themselves in the competitive national and regional technology market.

Keywords: *Integration, BMS, LENEL, WACI NX+, ODBC, Visual Basic.*

Dedicatoria

A mi madre... Por su incondicional apoyo durante toda mi carrera.

A mi padre... Por su apoyo y confianza todos los días de mi vida. Desde el cielo tu estrella continúa cuidándome...

Agradecimiento

A mi novia Maybell Navarro, por ser parte fundamental en la conclusión de mis estudios y por su incondicional apoyo en todos los aspectos de mi vida.

Al Ing. Royden Flores por la oportunidad de realizar este proyecto y por la confianza depositada en mi persona para la realización de muchos otros.

Al Ing. Jorge Tello por su importante aporte de conocimientos para la puesta en marcha de este proyecto.

Al Instituto Tecnológico de Costa Rica, por permitirme no solo la oportunidad de finalizar mis estudios, sino también de crecer de manera integral como persona y representante del movimiento estudiantil en diversos entes.

INDICE GENERAL

Capítulo 1. Introducción	12
1.1. Problema existente e importancia de su solución	13
1.1.1. Interés de las empresas en adquirir sistemas de domótica	14
1.1.2. El papel de Tecnológica de Costa Rica	15
1.2. Solución seleccionada	15
Capítulo 2. Meta y objetivos	17
2.1 Meta	17
2.2 Objetivo general	17
2.3 Objetivos específicos	17
2.3.1. Objetivos de hardware	17
2.3.2. Objetivos de software	17
2.3.3. Objetivos de documentación.....	18
2.3.4. Objetivos de implementación.....	18
Capítulo 3. Marco teórico	19
3.1. Domótica	19
3.2 Evolución de los sistemas de seguridad	20
3.2.1 Sistema de seguridad electrónica	20
3.3 Sistema de Automatización	21
3.4 Edificio inteligente	21
3.4.1 ¿Qué se puede controlar?	22
3.4.2 Métodos para controlar un edificio Inteligente	24
3.4.3 Integración de sistemas para la operación eficiente de recursos en una organización.....	26
3.5 Comunicación mediante bases de datos ODBC	28
3.5.1 Definición estándar ODBC	28
3.5.2 Funcionamiento del software	28
3.6 Conversión de datos a comandos infrarrojos	32
Capítulo 4. Descripción detallada de la solución	35
4.1. Análisis de soluciones y selección final	38
4.1.1. Soluciones planteadas con respecto al hardware	38
4.1.2. Soluciones planteadas con respecto al software.....	39
4.2. Descripción del hardware	42

4.2.1. Módulo de entradas	43
4.2.2. Módulo para interfaz de protocolos.....	47
4.2.3. Módulo de salidas	47
4.3. Descripción del software.....	51
4.3.1. Configuración de la comunicación con bases de datos.....	51
4.3.2. Descripción del software desarrollado para PC.....	56
4.3.3. Descripción del Software del Controlador	63
4.4. Modificaciones posteriores.....	66
4.5. Reevaluación y rediseño	67
Capítulo 5. Análisis de Resultados.....	68
Capítulo 6. Conclusiones y recomendaciones	75
6.1 Conclusiones.....	75
6.2 Recomendaciones.....	76
Bibliografía	77
Apéndices	79
Apéndice A.1 Siglas y acrónimos	79
Apéndice A.2 Manual de usuario	81
Anexos	¡Error! Marcador no definido.
Anexo B.1 Aclaratoria sobre cambios en los objetivos del Proyecto ..	¡Error! Marcador no definido.
Anexo B.2 WACI NX+ (Aurora Multimedia Inc.) [16].....	86
Anexo B.3 Dual Reader Interface Module LNL-1320 Series 2 (LENEL) [4] .	90

INDICE DE FIGURAS

Figura 1.	Ahorro económico debido a la utilización de sistemas de domótica. [2]	14
Figura 2.	Formato de datos para la conversión a IR	33
Figura 3.	Diagrama inicial de conexión de Hardware.	42
Figura 4.	Diagrama final de conexión de Hardware.	43
Figura 5.	Partes del controlador WACI NX+	48
Figura 6.	Arquitectura del Conector/ODBC [14]	52
Figura 7.	Proceso de conexión a origen de datos [15]	54
Figura 8.	Secuencia de funciones ODBC para ejecutar declaraciones SQL [15]	55
Figura 9.	Lógica de operación modo automático	57
Figura 10.	Menú para agregar áreas	61
Figura 11.	Menú para agregar dispositivos	62
Figura 12.	Estructura de código para comandos IR	62
Figura 13.	Aplicación del <i>IR Learning</i> en el WACI NX+	64
Figura 14.	Confirmación de envío correcto de comando de encendido	71
Figura 15.	Confirmación de envío correcto de comando de apagado	72
Figura 16.	Visualización del estado de acción encendido	73
Figura 17.	Visualización del estado de acción apagado	73
Figura A.2.1.	Ventana para agregar edificio	81
Figura A.2.2.	Ventana para agregar áreas de un edificio	82
Figura A.2.3.	Ventana para agregar Dispositivos	82
Figura A.2.4.	Menú de selección de funcionarios	83
Figura A.2.5.	Menú de Visualización y control de dispositivos	84
Figura B.3.1.	Características de lectora LNL-1320	90
Figura B.3.2.	Especificaciones de Lectora LNL-1320	91

INDICE DE TABLAS

Tabla 1.	Descripción de partes del WACI NX+	48
Tabla 2.	Codificación de empleados.....	58
Tabla 3.	Codificación de Eventos	58
Tabla 4.	Codificación de Acciones.....	59
Tabla 5.	Codificación de Estado actual.....	60
Tabla 6.	Tabla de visualización de eventos de LENEL.....	69
Tabla B.2.1.	Especificaciones Generales de Hardware.....	87
Tabla B.2.2.	Rangos de funcionamiento del Hardware	89

Capítulo 1. Introducción

La denominación de empresas de base tecnológica es un término que se refiere al nuevo tipo de empresas que se ha venido desarrollando en el sistema capitalista a nivel mundial. Nuevas empresas que aprovechan la microelectrónica y la informática como factor clave para desarrollar sus mercados. [11]

La empresa Tecnológica de Costa Rica, empresa de base tecnológica, cuenta con un departamento de desarrollo de software, el cual tiene como objetivo el desarrollo de interfaces y/o software a la medida que permita interconectar sus plataformas de integración o cualquiera de las otras aplicaciones de código abierto o propietario con que cuentan, con los sistemas de información que desee el cliente. Esto ha permitido crear interfaces de actualización dinámica entre los diferentes sistemas del cliente y sus aplicaciones. [5]

Dentro de este contexto, y gracias a la expansión de la empresa en los últimos años, la misma requiere de una interfaz de integración para su sistema de seguridad, el cual posee un lenguaje propietario, y un sistema de automatización de edificios (control de iluminación y climatización, sensores de presencia, entre otras) con el fin de cubrir las diferentes necesidades de sus actuales clientes y ofrecer un nuevo servicio a posibles nuevos clientes. Esta integración está enmarcada dentro de la creación de un BMS básico, mediante el cual el usuario pueda tener acceso a la configuración de los elementos conectados en su casa o edificio a través de una interfaz de control vinculada a su vez al sistema de seguridad ya instalado en el sitio. En este informe se analizan las razones por las cuales la empresa desea participar en el desarrollo de esta interfaz así como la solución planteada para atacar el problema expuesto por la empresa.

1.1. Problema existente e importancia de su solución

Actualmente en el mercado es posible encontrar equipos de domótica que cumplen requerimientos de mercados muy específicos: clientes pequeños (casas, residencias pequeñas) y clientes muy grandes (nivel industrial y residencial a gran escala), lo que se ve representado con su respectiva diferencia de precios de acuerdo a sus características.

Así, es posible encontrar equipos sofisticados que permiten la integración de sistemas y se ajustan a los distintos parámetros que se requieran (escalables y modulares) en precios alrededor de varias decenas de miles de dólares para edificios de alrededor de 250 m², (el valor es mayor dependiendo del sistema a instalar y sí el área es mayor). Estos costos están al alcance de unos pocos, empresas lo suficientemente grandes como para invertir estas cantidades de dinero sin ver desfinanciadas sus actividades, sabiendo que la recuperación de su inversión no será necesariamente en el corto plazo.

El caso contrario vendría a ser el de los equipos de tipo “*Stand-alone*” cuyo costo es extremadamente bajo en comparación al anterior. Sin embargo, las características propias de este tipo de sistemas impiden a las empresas lograr la integración de todos sus servicios, pues al ser “sistemas cerrados” carecen de la posibilidad de escalamiento y limitan así su aporte a la empresa. Son equipos utilizados para controlar una variable a la vez y generalmente se utilizan en residencias y no en edificios más grandes.

Este panorama muestra un importante vacío: La inexistencia de un sistema de domótica que se integre con el sistema de seguridad de la empresa (LENEL OnGuard® [9]) y que vaya dirigido a clientes de capital intermedio, los cuales desean equipos y sistemas de domótica lo suficientemente flexibles para lograr la completa integración de sus actividades y servicios y que represente una inversión que se adecúe a sus posibilidades económicas.

1.1.1. Interés de las empresas en adquirir sistemas de domótica

Como se explicó anteriormente, la domótica proporciona a las empresas la posibilidad de controlar las distintas variables en las que está inmersa su actividad y así no sólo lograr identificar falencias en sus operaciones, sino también el de aportar nuevas soluciones para atacar las mismas.

Los sistemas que permiten la integración y escalabilidad de funciones generan a las empresas posibilidades de ahorro de recursos y de personal, incrementando la eficiencia en sus labores.

Dentro de la gama de posibilidades que ofrecen los sistemas domóticos está el manejo del factor energético, el cual es uno de los más requeridos por las empresas clientes de Tecnológica de Costa Rica. Estos sistemas proporcionan a los usuarios un ahorro económico importante dependiendo del tipo de control implementado, tal y como se observa en la Figura 1, donde se puede apreciar, según un estudio realizado a usuarios residenciales españoles durante el año 2008, el ahorro obtenido tras la utilización de la domótica. De este gráfico es claro que el mayor ahorro se obtiene en el control de iluminación y aire acondicionado al comparar sus porcentajes de ahorro.

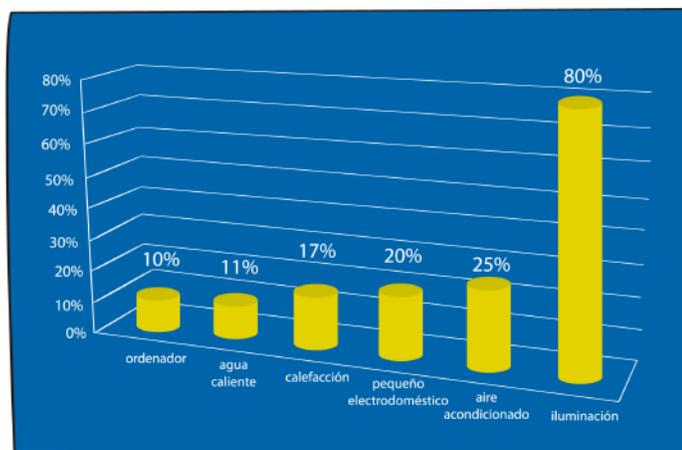


Figura 1. Ahorro económico debido a la utilización de sistemas de domótica. [2]

Por consiguiente, cada día es mayor la cantidad de empresas interesadas en utilizar equipos y sistemas de este tipo, gracias a la gran cantidad de ventajas que estos ofrecen.

1.1.2. El papel de Tecnológica de Costa Rica

Conscientes de la necesidad que existe en torno a este tipo de consumidor, la empresa Tecnológica de Costa Rica desea incursionar en este mercado y desarrollar un sistema que integre los recursos necesarios y requeridos por el cliente, manteniendo siempre la innovación tecnológica que propició su fundación. Debido a su condición de integrador tecnológico y al estar inmerso en la corriente tecnológica del mercado nacional, la empresa ha detectado las ventajas que puede generar para ellos su incursión en el área de la domótica:

1. Ofrecer un nuevo servicio a sus actuales clientes.
2. Generar una nueva herramienta para atraer clientes nuevos.
3. Su inserción en este mercado representaría no sólo un ingreso económico importante sino también la posibilidad de posicionarse aún más en el competitivo mercado tecnológico del país.

1.2. Solución seleccionada

Para atacar este problema es necesario primero que todo identificar cuáles son las variables que se desean controlar con el desarrollo de este proyecto para así formular la mejor forma de implementar su respectiva solución.

Como se mencionó anteriormente, los sistemas actuales de domótica una vez implementados podrían formar parte de un llamado *Building Management System*, capaz de “manejar” los distintos equipos que conforman el sistema de automatización del edificio. Generalmente los BMS se establecen con una serie de parámetros previamente establecidos a requerimiento del cliente y que satisfagan las necesidades particulares de su empresa, o bien proporcionando una interfaz de configuración para el cliente.

Para el caso específico de este proyecto, el cual estaría enmarcado dentro del desarrollo de un BMS propietario, se deberán atender variables específicas, relacionadas al factor energético de las instalaciones.

Dentro de las posibles variables energéticas a controlar se encuentran la iluminación y los aires acondicionados. La justificación de estas variables viene dada a raíz de conversaciones con ingenieros de la empresa quienes, a criterio de experto y respaldados por la información que obtienen de sus actuales clientes, consideran que deben ser las primeras áreas en las que la empresa debe incursionar con un nuevo proyecto. Esto concuerda con datos como los mostrados en la Figura 1, donde se puede concluir el interés de las empresas en estos sistemas de gestión energética.

Como cualquier desarrollo de nuevos equipos, su puesta en marcha estuvo precedida de una investigación, con la cual se pudieron establecer los parámetros técnicos del proyecto y todo lo que involucra el manejo de este tipo de variables. Esta investigación permitió una primera visión de los alcances de hardware y software, necesarios para la completa implementación del sistema.

Dentro de esta misma investigación se determinaron las características de la unidad central de control, la cual llevó a cabo la labor del manejo de señales para el control de los diferentes dispositivos del sistema, como sensores, actuadores y demás elementos de entrada/salida.

Como una de las primeras opciones y siguiendo recomendaciones de la empresa, se valoró la posibilidad de utilizar algún sistema embebido disponible en el mercado para que, con la programación adecuada, se desempeñe como la unidad central de control. En ese sentido la empresa pone a disposición un equipo adquirido hace algún tiempo, el cuál se encuentra actualmente en desuso y que se desea sea utilizado en el desarrollo de este proyecto. Este equipo fue desarrollado por la empresa estadounidense Aurora Multimedia y lleva por nombre WACI NX+[19].

Capítulo 2. Meta y objetivos

2.1 Meta

Generar las herramientas tecnológicas necesarias que le permitan a la empresa ingresar y competir en el área de la domótica.

2.2 Objetivo general

Diseñar e implementar un sistema capaz de integrar una serie de protocolos de comunicación y dispositivos de control que permitan llevar a cabo tareas propias de la automatización de edificios.

2.3 Objetivos específicos

2.3.1. Objetivos de hardware

- Integrar la lectora de control de acceso LNL-1320 (LENEL OnGuard®) al dispositivo controlador WACI NX+ (Aurora Multimedia) para el manejo de las entradas y salidas del sistema de forma que estos se adapten a los requerimientos técnicos y económicos deseados por la empresa.

2.3.2. Objetivos de software

- Configurar y programar el dispositivo central de control WACI NX+ para que este sea capaz de comunicarse y operar bajo el control del sistema de seguridad Lenel OnGuard®, ya implementado en la empresa. El mismo deberá ser capaz de controlar las distintas variables de entrada y salida mediante el procesamiento digital de las mismas.
- Implementar los protocolos necesarios para lograr la comunicación de los dispositivos entrada/salida con la unidad central de control.

- Diseñar el método de interfaz de usuario, el cual le permita hacer uso de los elementos instalados.

2.3.3. Objetivos de documentación

Desarrollar el manual de usuario necesario para la utilización del software de control de la interfaz de usuario.

2.3.4. Objetivos de implementación

Implementar la solución mediante la puesta en marcha en las instalaciones de la empresa Tecnológica de Costa Rica.

Capítulo 3. Marco teórico

A continuación se detallan varios conceptos importantes que se emplean durante este documento los cuales son necesarios para la comprensión de los alcances de este proyecto. Los mismos han sido obtenidos de diversas fuentes, tales como literatura impresa, búsquedas en internet y consultas con expertos.

3.1. Domótica

La domótica, proviene de la unión de dos elementos: Vivienda e Informática. Es el conjunto de sistemas automatizados que permiten controlar manual o automáticamente las variables de una vivienda como: confort, seguridad, comunicación, multimedia y gestión energética, entre otros.

De esta forma, la domótica es la aplicación de las nuevas tecnologías de la informática y otras áreas a las actividades cotidianas, ya sea en el hogar o en el sitio de trabajo, proporcionando una manera más fácil, comfortable y segura de desempeñar las labores diarias.

La domótica se encarga de gestionar principalmente los siguientes cuatro aspectos del hogar:

Energía eléctrica: En este campo, la domótica se encarga de gestionar el consumo de energía, mediante temporizadores, relojes programadores, termostatos, etc.

Confort: Control automático de los servicios de: calefacción, agua caliente, refrigeración, iluminación y la gestión de elementos como accesos, persianas, toldos, ventanas, riego automático, etc.

Seguridad: La seguridad que proporciona un sistema domótico es más amplia que la que nos puede proporcionar cualquier otro sistema, pues integra tres campos de la seguridad que normalmente están controlados por sistemas distintos:

- Seguridad de los bienes.
- Seguridad de las personas.

- Incidentes y averías.

Comunicaciones: La domótica tiene una característica fundamental, que es la integración de sistemas, por eso hay nodos (pasarela residencial) que interconectan la red domótica con diferentes dispositivos, como Internet, la red telefónica, etc.

3.2 Evolución de los sistemas de seguridad

Un sistema de seguridad podría considerarse como un conjunto de dispositivos distribuidos de manera planificada y estratégica en el perímetro de un sitio específico (casas, edificios, terrenos, etc.), con el fin de detectar violaciones en el mismo, como invasión de individuos que no posean un acceso permitido [8]. Estos dispositivos tienen la capacidad de comunicar cuando existe una violación al sistema o bien controlar los niveles de acceso a personal de una organización a diferentes áreas del o los edificios.

A medida que la sociedad ha ido evolucionando, las causas de la inseguridad se tornaron más complejas, lo que ha llevado a que se planifiquen sistemas de seguridad de la misma índole. Por ejemplo, estos sistemas agregaron el monitoreo mediante un microprocesador que incluye un comunicador digital.

3.2.1 Sistema de seguridad electrónica

Los sistemas de seguridad electrónica se compone de tres tipos: control de accesos, vigilancia de seguridad y detección de intrusiones. Los sistemas de control de acceso son dispositivos diseñados para limitar el acceso a un sitio, edificio, habitación, y los contenedores. Pueden ser muy complejos con sistemas biométricos, sistemas de intercambio de placas, y otros dispositivos electrónicos, o pueden ser mediante un simple sistema de tarjetas de acceso. [8]

Se puede decir que la elección de un tipo de sistema u otro dependerá de las necesidades de cada familia, individuo u organización, pues generalmente un sistema de seguridad no es un servicio aislado, sino una combinación de diferentes elementos físicos y electrónicos o una combinación de ambos. [8]

3.3 Sistema de Automatización

Los sistemas de automatización pueden definirse como “El conjunto de equipos, sistemas de información, y procedimientos que van a permitir asegurar un desempeño independiente del proceso, a través de operaciones de control y supervisión” [13]

La automatización tiene como característica principal el hacer funcionar un objeto de forma independiente o bien de forma semi-independiente del control humano (aunque sean los dispositivos los que realicen la mayor parte del trabajo, para su correcto desempeño se necesita una supervisión humana).

3.4 Edificio inteligente

“Un edificio inteligente es aquella edificación equipada con cableado estructurado para permitir a sus ocupantes controlar remotamente o programar una serie de dispositivos automatizados por medio de un solo comando, es decir que un solo botón pueda realizar varias tareas a la vez” [18].

El Instituto de Edificios Inteligentes, tiene su propia definición: “Un edificio inteligente es aquel que es capaz de crear un ambiente que maximice la eficiencia de los ocupantes mientras que permita una administración efectiva de recursos con el menor costo de tiempo”[18].

Algunas entidades especializadas en el tema, enlistaron las 13 características de edificios inteligentes:

1. Un edificio Inteligente debe contar con las facilidades de una red de Fibra óptica
2. Integración de cableados para acceso de Internet
3. Integración de cableados estructurados para redes de alta velocidad
4. Conectividad para servicios LAN y WAN
5. Facilidades para enlaces satelitales
6. Servicios ISDN
7. Fuentes de energía redundantes
8. Canalización propia para los cableado de energía, voz y datos
9. Alta tecnología y sistemas eficientes de HVAC.
10. Sistemas de Iluminación de encendido/apagado con sensores
11. Elevadores inteligentes que agrupen pasajeros por la designación de piso
12. Sensor automáticos instalados en sanitarios y lavamanos
13. Que cuente con un directorio del edificio computarizado e interactivo.

3.4.1 ¿Qué se puede controlar?

Los sistemas básicos de control que debe contar un edificio inteligente son los siguientes:

- Sistema de control autónomo para eficiencia energética.
- Sistema de control de seguridad (CCTV, control de acceso, control de incendio y alarmas).
- Sistemas de telecomunicaciones y tecnología de redes de datos y voz.
- Sistemas de integración.
- Sistemas de automatización de áreas de trabajo.

Sistema de Control Autónomo para eficiencia energética

Estos sistemas son muy sofisticados y sirven en esencia para aprovechar al máximo los recursos de energía y optimizar sus distintos usos en una edificación, tales como la iluminación, los sistemas de refrigeración y ventilación (HVAC), control de humedad, persianas y toldos, entre otros.

Sistema de Seguridad (CCTV, Control de Acceso, Control de Incendio y Alarmas)

Los sistemas de seguridad inteligentes pueden ser controlados y monitoreados de manera independiente y reconocer alarmas para tomar sus respectivas medidas de acción. Estos sistemas pueden controlar los accesos a las diferentes áreas así como modificar sus condiciones de control para resguardar la seguridad e integridad de sus ocupantes y de sus bienes.

Sistema de Telecomunicaciones y Tecnología de Redes de Datos y Voz

Todos los sistemas relacionados a las telecomunicaciones son sistemas sofisticados que proveen el servicio de comunicación interna como comunicación a distancia sea esta comunicación de voz o comunicación de datos. La tecnología de redes para edificios inteligentes esta creada con el fin de compartir los recursos de comunicación para todos y cada uno de los ocupantes del edificio. Los medios básicos mediante los cuales se puede efectuar el control de los sistemas son:

- Sistema centralizado telefónico basado en VoIP (*IP telephony*)
- Sistemas de seguridad de Redes de datos contra ataques del exterior
- Sistema de respaldo y resguardo de información
- Sistemas de video conferencias
- Internet de ancho de banda amplia
- Mensajería electrónica
- Sistema Satelital
- Video y CCTV

Sistema de Integración

Los sistemas de integración sirven para interconectar todos los sistemas inteligentes de un edificio pudiendo controlarlos y monitorearlos, todo a través de una red de datos propia, de Internet o una combinación de ambas.

“La integración consiste en utilizar un protocolo de comunicación que permita a todos los sistemas inteligentes comunicarse con el controlador o el sistema maestro de control y poder hacer que interactúen entre sí y que puedan ser más autónomos y automáticos” [18].

Existen una gran cantidad de protocolos de automatización de edificios en el mercado, donde destacan KNX, BACnet, LonWorks, X10, MODBUS, DALI, etc. Estos estándares de comunicación proporcionan lo necesario para lograr integrar una variedad de sistemas inteligentes de diferentes fabricantes para edificios inteligentes.

Sistema de Automatización de Áreas de Trabajo

Son sistemas que permiten dar un valor agregado y facilidades a los ocupantes del edificio.

“Estos sistemas de automatización, pueden ser en áreas donde exista grupo de máquinas tales como computadoras con aplicaciones específicas, impresoras, escáner, faxes, plotters, cámaras, y otros sistemas de servicios que se puedan prestar con el fin de automatizar y facilitar proceso que deben realizar los ocupantes del edificio inteligente” [18].

3.4.2 Métodos para controlar un edificio Inteligente

Control Remoto Centralizado por Computadora

El control remoto centralizado se genera a partir de un cuarto de control independiente donde se administran todos los servicios y sistemas inteligentes del edificio además de monitorear todos los sistemas y medios de seguridad conectados al edificio.

Control Remoto Individual

“El control remoto individual es aquel que el ocupante o los ocupantes de un edificio inteligente utilizan para poder manipular un dispositivo individual e independiente de los sistemas sofisticados, como el caso de los sistemas de iluminación, y los sistemas de automatización de áreas entre otros”. Los medios de control mayormente utilizados son:

- Sistemas de control infrarrojo: La ventaja es la confortabilidad que da el hecho de no moverse del lugar desde donde está la persona para gestionar el control sobre los dispositivos. La desventaja es que se requiere línea de vista.
- Sistema de control X-10: La ventaja que da es la confortabilidad de poder controlar cualquier dispositivo en cualquier lugar de la casa sin la necesidad de tener línea de vista. La desventaja es que se requiere de filtros y acopladores de fases.
- Sistema de control por radio frecuencia: La ventaja que da es muy similar a la X-10 y además la señal puede pasar las paredes de una casa. La desventaja primordial es la interferencia de señales inalámbricas y el radio de cobertura. También son sistemas más costosos.
- Sistemas de control mediante una red de cableados: Son sistemas muy flexibles, alta velocidad de comunicación entre los controladores y dispositivos a controlar, permite al habitante mantenerse confortable y poder controlar cualquier dispositivo, no existe limitante de distancias. Su desventaja es que es un sistema muy caro para edificios que no fueron diseñados desde el principio para tener la funcionalidad de sistemas inteligentes.

Control Automático

“El control automático agrega más conveniencia al hacer que las cosas sucedan automáticamente con el menor esfuerzo necesario” [18]. Esto quiere decir que se puede tener un control de los niveles de iluminación en

dependencia de presencia, movimiento o por un horario definido, alternar de fuentes de energía cuando se requiera, reconocer alarmas específicas para cambiar políticas de acceso y realizar notificaciones.

3.4.3 Integración de sistemas para la operación eficiente de recursos en una organización

3.4.3.1 Gestión Energética: Uso eficiente de la energía en edificios

Los edificios planificados y operados con eficacia energética ya no son exclusivos.

Ambas tendencias están revolucionando actualmente la, cada vez más ambiciosa, arquitectura y trazando un camino en la lucha mundial contra el cambio climático.

En realidad, la discusión sobre energía en el sector de la construcción se ha convertido en una tendencia y lentamente ha llegado a ser un concepto de uso diario para arquitectos así como para constructores.

“Durante la construcción de un edificio, así como durante su funcionamiento, se emplean grandes cantidades de energía, por esta razón un consumo controlado en esta área es especialmente efectivo” [18].

De esta forma, la operación de calefacción, aire acondicionado, luces y persianas por ejemplo puede estar en concordancia con las condiciones climáticas externas y ser controladas desde una interfaz o bien de forma automática previa configuración del usuario. El consumo energético se mantiene de ese modo dentro de los límites mínimos.

“Dado que todos los equipos e instalaciones manipulados eléctricamente pueden combinarse de manera flexible el uno con el otro y pueden controlarse por paneles táctiles o por redes públicas (teléfono, Internet), esto

abre posibilidades casi ilimitadas en el área de diseño y confort – desde la gestión eficiente del edificio a través de un control de seguridad inteligente hasta el almacenamiento de las diferentes necesidades en materia de iluminación, ruido y calidad de aire las cuales pueden ejecutarse sin gran esfuerzo” [18].

En la etapa de diseño es cuando se hace necesaria la creatividad del diseñador, para de este modo acercarse a la meta de crear arquitectura tanto ecológica como rentable.

3.4.3.2 El papel central de control de edificios inteligentes

Este papel consiste en generar la ingeniería de sistemas inteligentes con el apoyo de salas de red y controladores de edificio (iluminación, protección solar, calefacción, ventilación y aire acondicionado, así como los otros sistemas del edificio de ingeniería) que contribuyan de manera significativa a utilizar la energía de forma conservadora y dependiente de variables específicas de configuración.

Varios conceptos y enfoques son posibles en la optimización de la eficiencia energética en los edificios. En este contexto, el uso de control de edificios inteligentes proporciona una probada e interesante relación costo-beneficio.

Eficiencia del Consumo de Energía

La “inteligencia” con respecto a la energía en un edificio inteligente consiste de la reducción del uso de energía a un mínimo consumo.

Estos sistemas son nombrados de muchas maneras: *Bulding Automation System (BAS)*, *Building Automation Systems (BMS)*, *Energy Management System (EMS)*, *Energy Management and Control System (EMCS)*, *Central Control and Monitoring System (CCMS)* y *Facilities Management System (FMS)*.

Algunas estrategias usadas para reducir el consumo de energía en edificios inteligentes son:

- Encendido/Apagado Programado
- Encendido/Apagado optimizado
- Ciclo de Uso
- De Reajuste
- Limitante de demanda eléctrica
- Control adaptado
- Optimización de chillers
- Optimización de *Boylers*
- Fuentes óptimas de energía y alternas
- Aislamientos Térmicos
- Entre otros

3.5 Comunicación mediante bases de datos ODBC

3.5.1 Definición estándar ODBC

Open Data Base Connectivity (ODBC) es un estándar de acceso a Bases de datos desarrollado por *SQL Access Group*, el cual permite mantener independencia entre distintos lenguajes de programación, bases de datos (sin importar qué Sistema Gestor de Bases de Datos (DBMS)) y sistemas operativos en su uso en distintas aplicaciones. Para lograr la correcta comunicación entre estos sistemas, ODBC inserta una capa intermedia entre la aplicación y el DBMS conocida como: Nivel de Interfaz de Cliente SQL, esto con el propósito de que traduzca las consultas de datos de la aplicación en comandos que el DBMS entienda. Es necesario que tanto la aplicación como el DBMS deban ser compatibles con ODBC, para que esto funcione.[6]

3.5.2 Funcionamiento del software

El funcionamiento del software se da en dos modos:

1. Con un software manejador en el cliente, donde el driver interpreta las conexiones y las llamadas SQL y las traduce desde el API ODBC hacia el DBMS.
2. Una filosofía cliente-servidor, donde para conectarse a la Base de Datos se crea una DSN dentro del ODBC que define los parámetros, ruta y características de la conexión según los datos que solicite el fabricante.

Orígenes de datos ODBC

Se llama origen de datos ODBC a los datos e información necesaria para tener acceso a esos datos desde programas y bases de datos que admitan el protocolo ODBC. Estos pueden ser por ejemplo, una base de datos con su respectivo servidor. Los controladores ODBC utilizan Lenguaje de Consulta Estructurado (SQL por sus siglas en inglés) para obtener datos externos.

Dentro de los ejemplos de orígenes de datos se pueden citar: Microsoft Access, Microsoft SQL Server, Oracle RDBMS, hojas de cálculo y un archivo de texto. En lo que se refiere a la información de conexión, esta podría consistir por ejemplo en: la ubicación del servidor, el nombre de la base de datos, la identificación para el inicio de sesión, la contraseña y diversas opciones de controlador ODBC.

En la arquitectura ODBC, una aplicación específica se conecta al administrador de controladores ODBC. Este a su vez utiliza un controlador ODBC específico (como por ejemplo, el controlador ODBC de Microsoft SQL) para conectarse a un origen de datos (en este caso, una base de datos de Microsoft SQL Server). [14]

Características de ODBC

ODBC es una interfaz de programación de aplicaciones estándar (API) que permite acceder a datos contenidos y manejados por sistemas de gestión de bases de datos (DBMS). Mediante la utilización de ODBC, las aplicaciones

pueden acceder a gran cantidad de datos almacenados en diversos dispositivos tales como ordenadores personales, miniordenadores y grandes ordenadores, aunque cada DBMS utilice un formato diferente para guardar la información.

Entre sus características, destacan [1]:

- ODBC es una interfaz de programación de aplicaciones estándar que utiliza SQL (*Structured Query Language*).
- Oculta al programador la complejidad a la hora de conectarse a un origen de datos: por ejemplo, el acceso a los datos a través de redes de comunicación es transparente.
- Permite a múltiples aplicaciones acceder a múltiples orígenes de datos.
- Proporciona un modelo de programación homogéneo, es decir, bases de datos muy diferentes se manejan, vía ODBC, como si fueran idénticas, siendo ODBC el encargado de realizar las adaptaciones necesarias.
- Se basa en el modelo cliente/servidor.

Arquitectura de ODBC [1]

Se basa en cuatro componentes:

- Aplicaciones: son las responsables de interactuar con el usuario y de llamar a las funciones ODBC para ejecutar sentencias SQL y recoger los resultados.
- El driver manager: se encarga de cargar y llamar a los drivers según lo demanden las aplicaciones.
- Drivers: procesan las llamadas a las funciones ODBC, ejecutan sentencias SQL y devuelven los resultados a las aplicaciones. Son también responsables de interactuar con cualquier capa software necesaria para acceder a las fuentes de datos, como puede ser el software de red.

- Orígenes de datos: consisten en conjuntos de datos, más todo lo que pueda ser necesario para llegar hasta ellos; sistemas operativos, gestores de bases de datos, redes de comunicación, etc.

Handles en ODBC [1]

Un *handle* no es más que una variable de una aplicación, en la cual el sistema operativo es capaz de guardar información sobre la aplicación y sobre alguno de los objetos que maneja dicha aplicación. Todas las funciones ODBC usan un *handle* como primer parámetro.

ODBC usa tres tipos de *handles*:

- De sistema (*environment*): es el *handle* de contexto global. Todo programa que utilice ODBC comienza solicitándolo y acaba liberándolo. Sólo puede haber uno por aplicación.
- De conexión (*connection*): maneja toda la información relativa a una conexión. Identifica el driver que debe ser utilizado al realizar una conexión y en las llamadas posteriores a funciones ODBC. Puesto que se permiten varias conexiones, una aplicación puede solicitar varios.
- De sentencia (*statement*): se utiliza para manejar todo el procesamiento relativo a una sentencia SQL, desde su ejecución hasta la recogida de datos.

Controladores y orígenes de datos

“El controlador (driver) es un dispositivo intermedio entre los datos y el programa de acceso a dichos datos. Los controladores se almacenan en ficheros con extensión DLL (librerías dinámicas de Windows) que generalmente se copian en el directorio SYSTEM de Windows. Tiene que haber un controlador para cada formato de bases de datos que se quiere utilizar” [1].

Los orígenes de datos (*data source*) son los ficheros o directorios específicos donde se encuentran los datos.

En los servidores SQL no sólo es necesario indicar donde se encuentran los datos, sino que además es necesario que se encuentre disponible el programa servidor de datos (SQL Server, Oracle, SQL Base, etc.). El concepto de origen de datos es independiente del controlador y de los datos. Por ejemplo, se podrían crear dos orígenes de datos diferentes para la misma base de datos, uno de ellos configurado para usar la base de datos en modo sólo lectura y el otro con autorizaciones para leer y escribir en la base de datos.

3.6 Conversión de datos a comandos infrarrojos

Aplicación para convertir datos en comandos IR y enviarlos a través del controlador WACI NX+ [19]

Esta aplicación consiste en la conversión de determinada información de datos en formatos establecidos (por ejemplo Hexadecimal), en comandos válidos de infrarrojo para ser enviados a través del puerto de IR del dispositivo controlador WACI NX+.

El procedimiento mediante el cual se realiza esta conversión se muestra a continuación.

Tomando el caso en que se presente una serie de datos en formato hexadecimal, cuyos valores representan el ancho de pulso de las señales a ser generadas de forma infrarroja, se tiene:

0000 005C 0000 0004 001C 09C4 0030 03CC 0030 03CC 0034 00D4

Esta secuencia es formateada como sigue:

Offset	Size (in 16 bit words)	Ident.	Name	Description	Sample
0	1	wFormat	Format.	0100: No carrier 0000: Use carrier	0000
1	1	wFreq	Carrier frequency	The formula below is used to calculate this value.	005C
2	1	wOnce	Once size	The number of on/off pairs in the sequence that is sent only once	0000
3	1	wRepeat	Repeat size	The number of on/off pairs in the repeating sequence	0004
4	2*wOnce	aOnce	Once sequence	The sequence that is sent only once	N/A
4 + 2*wOnce	2*wRepeat	aRepeat	Repeat sequence	The sequence that is repeated	001C 09C4 0030 03CC 0030 03CC 0034 00D4

Figura 2. Formato de datos para la conversión a IR

Calculo de wFreq:

$$wFreq = \frac{4.145146 * 10^6}{Carrier_Freq}$$

O bien

$$Carrier_{Freq} = \frac{4.145146 * 10^6}{wFreq}$$

En el ejemplo mostrado, el valor de wFreq es de 005C (o 92 decimal).

De esta forma, la frecuencia de portadora será:

$$Carrier_{Freq} = \frac{4.145146 * 10^6}{92} = 45kHz$$

Las secuencias de datos consisten en pares de tiempo de encendido/apagado y representan el número de ciclos (o ancho de pulso) en el que el emisor esta encendido y el número de ciclos en el que el emisor está apagado.

En este ejemplo, el primer par es 001C:09C4. Este par enciende el emisor por 28 ciclos (001C) o bien:

$$28 * \left(\frac{1}{45000}\right) s = 0.622ms$$

Y 2500 ciclos (09C4) para el apagado, lo que se traduce en:

$$2500 * \left(\frac{1}{45000}\right) s = 55ms$$

Capítulo 4. Descripción detallada de la solución

Como una primera etapa, se realizaron investigaciones sobre los requerimientos que pretendía la empresa en cuanto a los alcances reales del proyecto. Estas investigaciones consistieron en primera instancia en entrevistas tanto con el presidente de la empresa como con personal del departamento de ingeniería de la compañía. Lo primero fue llegar a comprender los orígenes de la empresa, su estructura, mercado meta y posibles objetivos a corto, mediano y largo plazo. Esto permitió tener la visión global en la cual estaba enmarcado el problema en cuestión y así orientar, de una forma más apegada a la realidad, las posibles soluciones. De esta forma la solución final tomaría en consideración no solo las características técnicas necesarias para resolver el problema, sino también el entorno en el cual debía hacerse, con lo cual se aseguraba una correcta correspondencia entre el problema planteado y la forma de abordarlo, o sea de manera integral.

Como resultado de esta investigación previa, se determinó la necesidad de la empresa de ingresar a un nicho de mercado a la que por años estaba viéndose forzada a entrar: la automatización residencial y terciaria. Al estar la empresa involucrada durante muchos años en el mercado de la seguridad física y lógica principalmente, y al tener como uno de sus fuertes la integración de diversos sistemas en la búsqueda de soluciones integrales de diseño, se hizo imprescindible su incorporación a la integración de sistemas de control automático a su plataforma.

Esta decisión no fue arbitraria pues, cada vez más, sus clientes requieren de estos servicios, por lo que estos se encargaron de generar ese espacio de necesidad para solventar esos vacíos.

Al verse en estas instancias, la empresa toma la decisión de invertir en un equipo que le permita ejecutar ciertas acciones de control en diversos dispositivos usados generalmente en oficinas pequeñas, salas de reunión, etc. Dentro de las pruebas preliminares del equipo, el mismo parece cumplir con las expectativas para las cuales fue adquirido. Sin embargo, una de sus limitantes primordiales en su

momento fue el hecho de que funcionaba como un sistema *Stand-Alone*, donde se podían generar acciones de manera aislada a los diferentes sistemas instalados en la edificación. Esto, aunado al complicado manejo de la configuración de acciones y eventos (al menos para el usuario final, el cual no necesariamente tenía conocimiento técnico) puso en riesgo la posible utilización del dispositivo en futuros proyectos. Estos proyectos consistían en la integración del dispositivo de control (WACI NX+) al sistema de seguridad que la empresa representa (LENEL OnGuard®) con la idea de ofrecerlo como un valor agregado a la instalación del cliente, a un valor mucho menor y con características similares o superiores a los diferentes sistemas de automatización en baja potencia, que se encuentran actualmente en el mercado. El tipo de proyecto a manejar sería la integración al sistema para el manejo de salas de reunión u oficinas pequeñas.

Al haberse invertido una cantidad de dinero en este dispositivo, era preciso sacarle el provecho necesario y encontrar la forma de vincularlo dentro de un solo sistema.

De esta forma, el proyecto se direcciona a la integración del dispositivo de control al sistema de seguridad que representa la empresa, dirigido a clientes que ya cuentan con la plataforma y donde su nivel de inversión para la etapa de automatización no podía ser muy alto.

Así, de las posibles soluciones que se pudieran visualizar, era necesario que el factor de integración fuese prioritario, seguido de una amigable interfaz con el usuario; coincidentemente ambas, características básicas de los sistemas más robustos de automatización que se encuentran en el mercado.

Obtención y análisis de información

Una vez realizada la delimitación de la solución fue necesario realizar diversas investigaciones bibliográficas, principalmente en internet, para determinar las características técnicas de los elementos involucrados, así como las orientaciones del mercado hacia el uso de estos dispositivos y sistemas. Específicamente, esta investigación consistió en:

- Determinar sus ventajas y desventajas a nivel de integración

- Identificar sus limitantes tecnológicas
- Conocer su uso actual en el mercado
- Verificar la disponibilidad de información técnica relevante
- Comprobar su nivel de soporte técnico disponible

Los resultados de esta investigación fueron necesarios para cotejarlos con las limitantes proporcionadas por la empresa para así determinar la viabilidad del proyecto y el camino a seguir en las etapas siguientes.

Evaluación de las alternativas y síntesis de la solución

Una vez conocidos los requerimientos base, con los que se debía llevar a cabo el proyecto y efectuadas las investigaciones bibliográficas respectivas mencionadas en el apartado anterior, se identificaron una serie de posibles métodos de abordar la solución al problema.

El método empleado para evaluar la validez de cada una de ellas fue mediante simulaciones, análisis de diseño para lograr la integración con otros sistemas y pruebas controladas de las aplicaciones. De esta forma, cada una de las posibles soluciones fue probada mediante el uso de su software de aplicación, en los cuales se realizaron pruebas básicas de configuración de Eventos y Acciones, por ejemplo, para determinar su grado de complejidad tanto para la implementación de configuraciones de uso como para su nivel de manejo intuitivo de cara al usuario final, el cual no necesariamente tendría conocimientos técnicos. Otro criterio tomado en cuenta durante estas pruebas, fue la rapidez de implementación de la solución en estudio, ya que es determinante a la hora de realizar cálculos de costos de implementación, donde no solo se toman en cuenta dispositivos y software, sino también las horas-hombre destinadas para completar la tarea.

Como uno de las principales limitantes suministradas por la empresa fue la apertura o permisibilidad de trabajar con otro sistema, por lo que uno de los criterios principales que debieron ser tomados en cuenta en esta etapa fue el nivel de integración que permitía cada propuesta. En este sentido la investigación debió

tornarse más profunda en relación al tipo de comunicación que era soportado por cada solución y que esta fuera compatible con el protocolo utilizado para el manejo de base de datos (el cual debía ser el más sencillo y robusto que se tuviera a la mano) con el que se quería trabajar.

A continuación se detalla el proceso de diseño de la solución implementada con respecto a las diferentes soluciones propuestas durante el planteamiento de la solución hasta llegar a la solución final tanto de hardware como de software.

4.1. Análisis de soluciones y selección final

4.1.1. Soluciones planteadas con respecto al hardware

Utilización de controlador WACI NX+

Por requerimiento de la empresa, es necesario utilizar un equipo adquirido hace algún tiempo por la misma, el cual no se encuentra actualmente en uso. El mismo fue desarrollado por la empresa estadounidense Aurora Multimedia y lleva por nombre WACI NX+ [19]. Al estar enmarcado como un requerimiento básico de la empresa para el desarrollo de la integración, el planteamiento respecto a la solución de hardware se limitó a investigar los diferentes alcances y características de este dispositivo con el fin de propiciar el mejor aprovechamiento de sus propiedades.

Interfaz de usuario

Inicialmente la solución planteada a nivel de interfaz con el usuario, residía en la utilización de pantallas táctiles, las cuales simplificaran el uso del software y proporcionara un valor agregado a la solución.

Sin embargo y luego de verificar algunas condiciones, tales como costos y prestaciones se concluyó por parte de la empresa que esta opción quedara para una futura etapa del proyecto.

De esta forma, se determinó la utilización de una interfaz instalada en una computadora personal (PC) suministrada por la empresa, donde residiría el

software de aplicación y se realizaría la comunicación con la base de datos del sistema de seguridad.

4.1.2. Soluciones planteadas con respecto al software

Dado que la solución debe realizar una integración entre el sistema de seguridad y el controlador de puertos, lo básico que debe aplicarse es que el manejo de las acciones dependa del comportamiento de los dispositivos de control de acceso, por lo que el criterio primordial a cumplir es que se permita la integración con bases de datos provenientes de sistemas externos, en este caso generado por el sistema de seguridad Lenel OnGuard® [9] instalado en la empresa. En este sentido se hace necesaria la utilización de estándares abiertos para lograr esta comunicación.

Inicialmente, se consideraron algunas soluciones de software, las cuales se detallan a continuación:

- Utilización de software de diseño para páginas de control gráfico

Se valoró emplear el software conocido como YIPI (*Your IP Interface*), el cual es una Interfaz Gráfica de Usuario (GUI por sus siglas en inglés) para sistemas basados en la marca Aurora Multimedia, fabricante del WACI.

Dentro de sus ventajas se puede mencionar que sus botones de comando están diseñados para “hablar” directamente con el controlador WACI, lo que facilita la configuración y el manejo de puertos del dispositivo. Además, proporciona una plataforma gráfica configurable que simplificaría el trabajo de diseño de interfaz de usuario.

Sin embargo, se han considerado algunas desventajas que, al ser valoradas en relación a sus ventajas, propician su descarte en la implementación final.

Dentro de estas desventajas se pueden citar que sus botones gráficos no son editables y estos están orientados al manejo de dispositivos multimedia (Audio, Video, DVD, proyectores, etc.) y no al manejo de sistemas de iluminación, aire acondicionado, sensores, etc. A esto se le suma la falta de bases de datos de botones de comandos, lo que limita el funcionamiento óptimo de esta interfaz para el enfoque que se le quiere dar.

Adicionalmente, y quizá su desventaja principal para este proyecto, es que no se permite una integración con bases de datos externas, pues está diseñado para trabajar directamente sobre las acciones que el usuario genere desde esta interfaz y no de señales externas, por ejemplo el control de acceso instalado en el edificio, tal y como se requiere.

La poca información técnica y soporte técnico existente de esta aplicación ayudan a descartar esta opción y a seguir en la verificación de medios alternos para cumplir los requerimientos del proyecto.

- Utilización del servidor web del dispositivo

Se evaluó la posibilidad de emplear el Web Server que provee el dispositivo el cual tiene una interfaz de configuración de las distintas variables, condiciones y acciones que se quieran realizar con el WACI. Dentro de sus ventajas, se puede citar la simplicidad de diseño de una interfaz de usuario final, pues al realizarse sobre una interfaz web esta permite distintas formas de generar interfaces de alto nivel en base a formato .html.

Sin embargo, una de sus principales desventajas es lo complicado que es la manipulación del menú de configuración de eventos o “*Event Manager*” para un usuario final. Se debe tener en cuenta que cualquier cambio de configuración de eventos y acciones debe ser completamente posible de realizar por parte del usuario y tomando en cuenta que la manipulación de esta configuración será bastante periódica, por ejemplo al establecer parámetros de uso de instalaciones por horarios previamente configurados, esta operación hace más complicado el uso del sistema.

- Aplicativo basado en lenguaje de programación Visual Basic

Al crear un aplicativo para manejar no solo la configuración de parámetros sino también la interfaz de alto nivel para el usuario final, se tiene la posibilidad de diseñarlo de forma completamente configurable y “a gusto del cliente”. Esta opción además permite de una manera más sencilla la integración y manejo de base de datos externo mediante el estándar abierto

ODBC [14], sobre una plataforma de basada en un lenguaje de programación soportado por el dispositivo de control, en este caso Visual Basic.

Esta solución flexibiliza el manejo de la información enviada por el sistema de seguridad así como la configuración y manejo de los puertos de salida del controlador, llámense puertos infrarrojos, serie, relés y entradas y salidas analógicas y digitales. Esto representa la mayor ventaja en comparación a las soluciones anteriormente planteadas, por lo que se optó por la implementación de esta solución.

4.2. Descripción del hardware

La primera labor de implementación fue la de pruebas a nivel de hardware. En estas, se establecieron los parámetros necesarios para realizar una comunicación entre el dispositivo de control WACI NX+ y los elementos conectados en el edificio, tales como máquinas de aire acondicionado. De esta forma se pudieron probar los puertos infrarrojos del dispositivo de control, así como el método mediante el mismo es capaz de “aprender” los códigos de los distintos elementos, lo cual se analizará posteriormente en este apartado.

Una vez completada esta etapa, fue necesario investigar la forma en que los comandos del WACI NX+ pueden ser implementados desde distintos programas y no necesariamente desde el propio. Específicamente, fue necesario comprender el formato de envío de comandos por puerto infrarrojo desde una aplicación desarrollada en lenguaje Visual Basic, para así proporcionar un método externo de control capaz de comunicarse con otros sistemas, que para el caso de este proyecto, será el de seguridad.

Inicialmente, la propuesta de diseño de hardware comprendía lo mostrado en la Figura 3. Esta incorpora algunos factores como interfaces Infrarrojos y seriales para poder llevar a cabo el control de iluminación regulable con balastos electrónicos. Sin embargo y tras requerimientos suministrados por la empresa dueña del proyecto, se ha modificado el diseño eliminando el control de iluminación vía infrarrojo de esta etapa del proyecto, por considerarse que este rubro ya estaba siendo atacado mediante otros métodos existentes en la empresa (Ver **¡Error! No se encuentra el origen de la referencia.**)

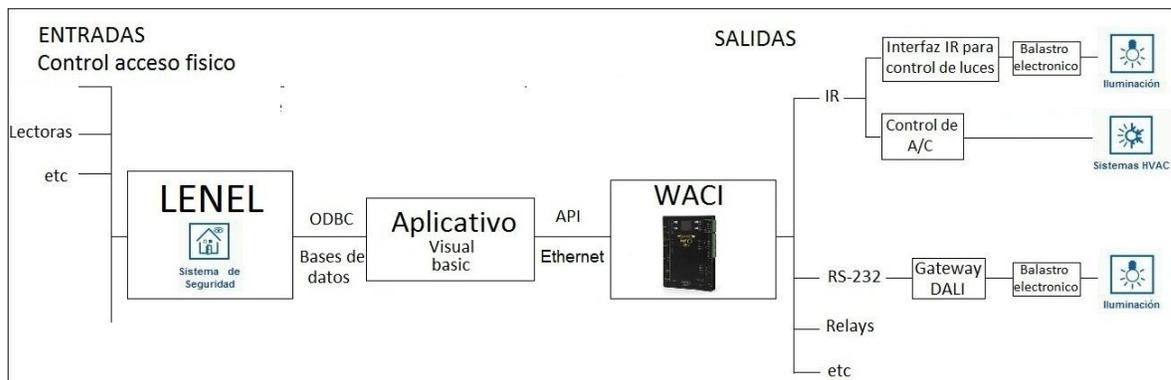


Figura 3. Diagrama inicial de conexión de Hardware.

De esta forma, se replanteó la solución de hardware haciendo los ajustes necesarios requeridos por la empresa. Este nuevo diseño se muestra en la Figura 4.

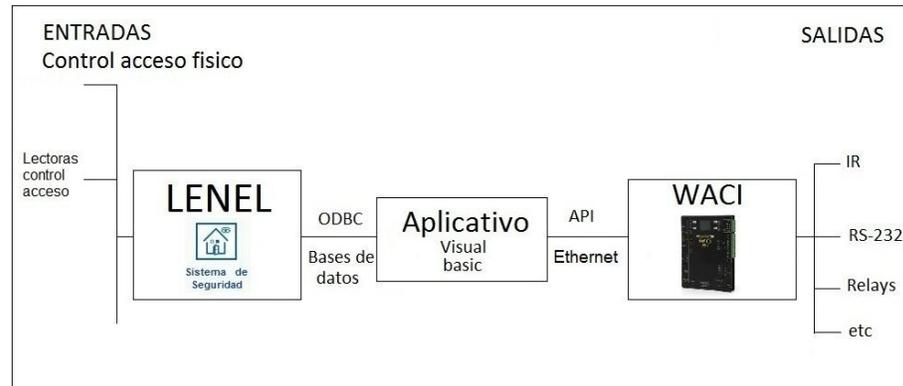


Figura 4. Diagrama final de conexión de Hardware.

De esta figura se pueden definir los siguientes módulos:

4.2.1. Módulo de entradas

Este módulo está compuesto básicamente por las lectoras de control de acceso del sistema de seguridad LENEL OnGuard® instalado en la empresa.

Estas lectoras de control de acceso, las cuales se encuentran distribuidas en las distintas áreas de los edificios de Tecnológica de Costa Rica, proveen las señales de alarmas y eventos necesarios para la lógica de control automatizado de funciones, que se desarrolló en este proyecto. Estos eventos, que se producen cada vez que los usuarios presentan sus credenciales de identificación, son almacenados en la base de datos del sistema de seguridad desde donde los mismos son accedados para realizar las distintas funciones de control que se requieran y dependiendo del área y dispositivos que se desean intervenir.

La acción que se requiere del usuario para generar acciones de automatización es la misma que se requiere del mismo para proporcionarle acceso a determinada sección del edificio, el cual consiste en presentar su tarjeta inteligente de

identificación a una distancia en la cual el lector de tarjetas pueda obtener la información del usuario contenida en la misma.

A continuación una descripción detallada del funcionamiento del hardware de control de acceso de LENEL OnGuard®.

Descripción General del Sistema LENEL OnGuard®

El sistema de integración LENEL OnGuard® [9], proporciona un número de funciones, como la habilidad de regular el acceso a través de puertas y entradas específicas hacia las distintas áreas de la instalación del cliente. Además permite generar credenciales por computadora para empleados y visitantes. Este sistema utiliza una única base de datos de funcionamiento relacional, que se integra perfectamente con todas las funcionalidades.

La integración descrita se proporciona a través de un solo sistema operativo. Además, las aplicaciones basadas en Web utilizan la misma base de datos común que los otros módulos. “El sistema está programado de tal manera que los módulos (control de accesos, monitoreo de alarmas, administración de ID, administración de visitantes, administración de activos, video digital, etc.) son desarrollados y construidos a partir de un código fuente único de 32 bits. No hay fuentes de código por separado para los módulos individuales” [17].

Control de acceso físico del sistema de seguridad Lenel OnGuard®.

El sistema Lenel OnGuard® permite la creación de distintos tipos de perfiles de acuerdo al tipo de usuarios y a las diferentes categorías de acceso deseadas, por ejemplo: empleado de mantenimiento, personal administrativo, servicio técnico, etc. A cada uno de ellos se les podrá restringir el ingreso a ciertas áreas, a las cuales tendrá acceso con horarios limitados, o bien pueden crearse con mayores atributos. Esto les permite a los administradores del sistema, por ejemplo, que el empleado del departamento de servicio técnico no pueda acceder a la puerta de un área

restringida en otro horario que no sea el que se le asignó en el sistema de control de acceso.

Las credenciales utilizadas para este control, con las que los usuarios accederán a las áreas, contienen un microchip inteligente en donde el o los administradores del sistema podrán almacenar la información necesaria para generar los accesos adecuados para cada colaborador en referencia a su cargo, y esto se almacena directamente en la credencial. Adicionalmente, para lograr alcanzar un mayor nivel de seguridad, se pueden implementar sistemas biométricos (huella dactilar, palma de la mano, iris del ojo) dando acceso en forma conjunta con la credencial inteligente (*Smartcard*).

Control de Acceso Físico

“Esta solución permite el control de los puntos estratégicos de una compañía mediante equipos que verifican la identidad de las personas en el momento de ingresar a las instalaciones” [3].

Este tipo de control maneja distintas políticas de acceso, totales o parciales, además de permitir un control del tiempo en que los usuarios de la instalación realizan sus transacciones en las distintas áreas.

El manejo avanzado de credenciales permite controlar, limitar, monitorear y auditar el acceso físico. “Este tipo de sistema es ideal para organizaciones que desean controlar una única área restringida o múltiples puertas de acceso”[3].

Lectoras de control de acceso físico LNL-1320 [4]

Las lectoras de control de acceso instaladas en la empresa son las denominadas LNL-1320. Estas, como todos los sistemas de LENEL proporcionan un módulo para soluciones de control de acceso llamado *Dual Reader Interface* (DRI). Cada DRI permite hasta ocho diferentes formatos de tarjeta así como códigos para formatos de tarjeta magnética y Wiegand.

El DRI constituye un vínculo vital entre Sistema de Control Inteligente o *Intelligent System Controller* (ISC) y el lector de tarjetas conectado a la interfaz. Además, es posible manejar hasta 32 módulos de DRI usando comunicación RS-485 2 hilos o 4 hilos hasta 1200 metros por puerto desde el ISC.

Cada módulo DRI es direccionado individualmente para incrementar sus capacidades de generar reportes con las distintas aplicaciones del software de control de acceso de LENEL OnGuard®. El DRI incluye además 8 entradas que soportan circuitos de tipo normalmente abierto, normalmente cerrado, supervisados y no supervisados. Además, 6 relés de salida que soportan operaciones a prueba de fallos o no seguros.

Especificaciones y Funcionalidades [4]

- Alimentación a 12 o 24 VDC
- Soporta Data1/Data0, *Clock/Data* y Lenel OSDP-compatible con lectores y teclados RS-485
- Firmware descargable
- Seis salidas de relé Form-C de 5 A a 30 VDC
- Hasta 16 diferentes formatos (8 formatos de tarjeta y 8 formatos de activos)
- Soporta formatos de código magnético y Wiegand
- Supervisión de contacto de puerta (abierto/cerrado)
- Monitor de interruptor REX
- Paro por salida de control
- LED bicolor para lectura de estado y LED de 2 hilos
- Control con Beeper
- Manipulación dedicada y circuitos por fallo de alimentación
- Soporta “modo de acceso sin conexión del lector”
- Posee puentes de terminación
- Regulador permite compatibilidad de lectores de 12 VDC con fuente de alimentación de 24 VDC
- Interruptor DIP para seleccionar direcciones

4.2.2. Módulo para interfaz de protocolos

Consiste en una computadora personal (PC) conectada al servidor de la base de datos del sistema de seguridad, donde estará instalado el programa de aplicación encargado de integrar el sistema de entradas provenientes del sistema LENEL descrito anteriormente con el módulo de salidas compuesto por el dispositivo de control WACI NX+ que se detallara posteriormente. Además, este módulo se encargará de gestionar la configuración del sistema mediante el manejo de puertos, áreas del edificio, horarios, presencia, entre otros criterios.

Las características básicas de la PC utilizada, para el uso específico de la aplicación:

- Procesador Pentium® Dual Core, 2.1 GHz
- Memoria RAM de 4 Gb
- Disco duro de 320 Gb
- Diversos adaptadores de red (VPN, WLAN, Virtual WiFi Miniport Adapter, entre otros)
- Teclado PS/2 estándar
- Monitor Genérico PnP

4.2.3. Módulo de salidas

Este módulo recibe la información del aplicativo de comunicación y configuración instalado en la PC. Maneja los puertos de comunicación infrarroja, RS-232, relés y DSP. Además propicia el control de los distintos medios infrarrojos mediante el *IR Learning*, el cual se analizará posteriormente en el apartado de descripción de software. Este permite al dispositivo “aprender” los códigos de los diferentes equipos para ser utilizados por la interfaz de comunicación del sistema de control y así gestionar el manejo de los distintos parámetros que estos proporcionan.

Descripción de partes del WACI NX+ [16].

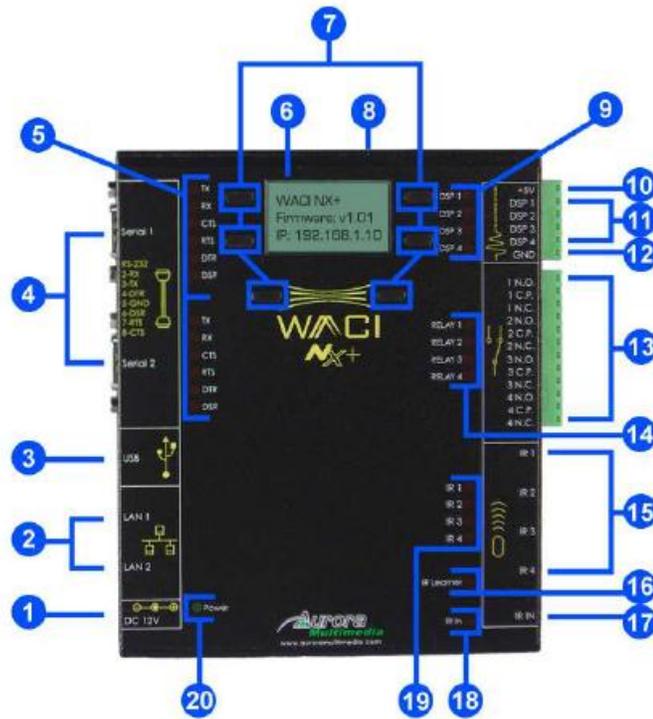


Figura 5. Partes del controlador WACI NX+

Tabla 1. Descripción de partes del WACI NX+

Número	Descripción
1	Puerto de alimentación
2	2 Puertos LAN 10/100 Auto-MDX
3	Puerto USB 1.1 On-The-Go
4	2 Puertos seriales RS-232/422/485
5	LED Indicadores para puertos seriales 1 y 2
6	Display LCD para configuración y diagnósticos
7	6 botones para navegación del menú
8	Puerto de expansión Compact Flash Tipo 2
9	Indicadores LED para DSP 1-4
10	Alimentación de +5V para DSP
11	Puertos DSP 1-4
12	Línea de tierra para DSP

13	Puertos de Relé 1-4 (Normalmente Abierto, Center Pin, Normalmente cerrado)
14	LED indicadores para Relés 1-4
15	Puertos Infrarrojos 1-4
16	Puerto de aprendizaje IR
17	Puerto de entrada infrarrojo
18	LED indicador de entrada infrarrojo
19	LED indicador para puertos IR 1-4
20	LED para estado de la alimentación

Características de los puertos infrarrojos

Los cuatro puertos infrarrojos del WACI NX+ son utilizados para enviar comandos a dispositivos que puedan ser controlados usando un control remoto estándar. Para controlar un dispositivo, es necesario conectar uno de los sensores emisores de IR al sensor IR del dispositivo a ser controlado.

Para programar el WACI NX+ para enviar comandos IR, se puede hacer de dos métodos diferentes. El primero es descargando el archivo .WIR del dispositivo (si existe). El segundo es utilizando el IR Learner, el cual se “aprenderá” el comando desde el control remoto del dispositivo.

Emisores de IR

Los emisores de IR son pequeños cables con un emisor de infrarrojo en un extremo y un pequeño terminal de audio en el otro. Estos emisores son conectados en los puertos IR del WACI NX+. El extremo del emisor IR se acopla al dispositivo a controlar. Cuando el WACI está enviando información a través del emisor, el LED ubicado en la parte posterior del emisor se encenderá.

Indicadores LED para puertos IR

Cuando un comando IR es enviado desde un puerto IR específico, el LED de ese puerto estará encendido.

IR Learner

El *IR Learner* es utilizado para aprender los códigos IR desde el control remoto del dispositivo. Puede leer diferentes tipos de controles remotos.

Puerto de *IR Learner*

Para que el WACI NX+ aprenda el código IR, es necesario apuntar el control remoto hacia la “ventana” del *IR Learner*. Adicionalmente, es necesario usar la página de diagnósticos de IR para poder aprender el comando.

LED para el *IR Learner*

Este LED se encenderá durante el proceso de aprendizaje cuando una señal IR sea detectada en el sensor de IR del WACI NX+. Cuando el proceso recién comienza el LED parpadeará despacio hasta que la señal sea recibida. La distancia correcta para mantener la fuerza de la señal es de aproximadamente de 15 cm y pondrá el LED con la luz fija cuando la distancia adecuada sea alcanzada. Si el control remoto está demasiado cerca el LED parpadeará rápidamente.

4.3. Descripción del software

Durante la investigación inicial se fueron realizando paralelamente otras actividades, como el reconocimiento de formas de manejo de bases de datos. Esta investigación se basó principalmente en consultas realizadas a expertos en la materia, los cuales a pesar de proporcionar diversos métodos, ubicaron la mejor opción en el sistema abierto ODBC (que se explicará más adelante en esta sección). Esta opción no solo permitía una forma más sencilla de comunicación con la base de datos sino que además proporcionaba muchas facilidades para gestionar acciones desde aplicativos como los desarrollados en lenguaje Visual Basic.

A partir de ese momento, se comenzó con la implementación de un aplicativo que fuera capaz de gestionar lo referente a la información proveniente de las bases de datos del sistema y que a su vez manejara los requerimientos del usuario en relación al manejo de puertos del dispositivo WACI NX+, en un ambiente de interfaz de usuario intuitivo.

La propuesta para el diseño de software consistió en la utilización de un aplicativo externo a cualquier otro desarrollado para el controlador. La razón primordial por la que se adoptó esta solución reside en la simplicidad con que se puede abordar tanto la configuración y uso por parte del usuario así como la facilidad para gestionar la comunicación con la base de datos del sistema de seguridad, elementos que no están muy desarrollados en el WACI NX+ y que no implicarían desarrollos más complicados para llevarse a cabo.

4.3.1. Configuración de la comunicación con bases de datos

La comunicación con la base de datos del sistema se realiza mediante la utilización del protocolo abierto ODBC. El proceso mediante el cual se da esta comunicación se muestra en la Figura 6, cual permite obtener los datos necesarios para que el sistema se comporte de acuerdo a lo planteado en la Figura 9.

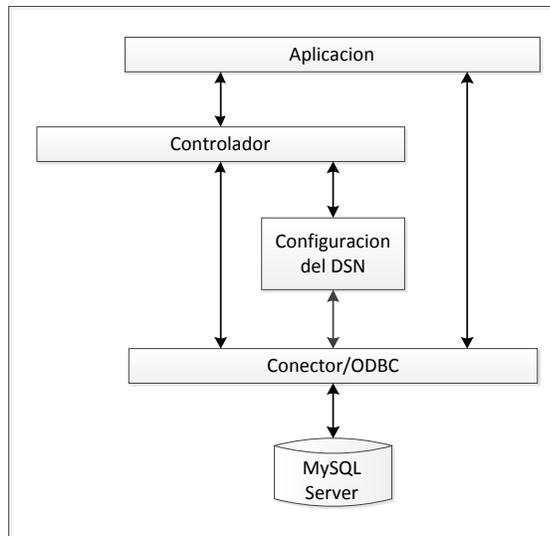


Figura 6. Arquitectura del Conector/ODBC [14]

Para conectarse a los orígenes de datos fue necesario instalar el controlador ODBC apropiado en el equipo que contiene el origen de datos. Como se consignó anteriormente, los orígenes de datos es la información necesaria para tener acceso a los datos, desde programas y bases de datos que admitan el protocolo ODBC.

En este caso particular el origen de datos es Microsoft SQL Server, donde se encuentran alojados los datos del personal de la empresa, y a su vez es administrado por el sistema de seguridad para generar distintas acciones y reportes.

Adicionalmente fue necesario definir un Nombre de Origen de Datos (DSN) utilizando el administrador de orígenes de datos ODBC para así almacenar la información de conexión en: el registro de Microsoft Windows, en un archivo DSN, y en una cadena de conexión en código de Visual Basic para pasar la información de conexión directamente al Administrador de controladores ODBC.

Antes de que una aplicación pueda enviar una instrucción SQL, es necesario asignar un identificador de instrucción (*Statement Handle*) para dicha instrucción. Para realizar esta tarea, se debió realizar en la aplicación lo siguiente:

- Declarar una variable de tipo HSTMT

- Solicitar la instrucción `SQLAllocStmt` (*SQL Allocate Statement*) y pasar la dirección de la variable y el `HDBC` con la que desea asociar la declaración. De esta forma, el controlador asigna memoria para almacenar información acerca de la instrucción, se asocia el identificador de instrucción con la `HDBC`, y devuelve el identificador de instrucción en la variable.

Para interactuar con un origen de datos, la aplicación debe seguir los siguientes procedimientos:

1. Conectarse a un origen de datos especificando el `DSN` y cualquier información adicional necesaria para completar la conexión.
2. Procesos de una o más sentencias `SQL`:
 - a. La aplicación ingresa la cadena (*string*) de caracteres en el buffer. Si la instrucción incluye marcadores de parámetros, establece los valores de parámetro.
 - b. Si la instrucción devuelve un conjunto de resultados, la aplicación asigna un nombre de cursor para la instrucción o bien, permite al driver que lo haga.
 - c. La aplicación ingresa la instrucción para una ejecución preparada o inmediata.
 - d. Si la instrucción genera un conjunto de resultados, la aplicación puede solicitar información sobre los atributos del conjunto de resultados, tales como el número de columnas y el nombre y tipo de una columna específica. Tal como se visualiza en la Figura 8. Se asigna almacenamiento para cada columna en el conjunto de resultados y obtiene los resultados.
 - e. Si la instrucción causa un error, la aplicación recupera información del error desde el driver y toma las acciones necesarias.
3. Termina cada “transacción” confirmándola o repitiéndola.
4. Finaliza la conexión cuando ha terminado de interactuar con el origen de datos.

El diagrama mostrado en la Figura 7 proporciona las “llamadas a funciones” que la aplicación ejecuta para: conectarse al origen de datos designado, procesar instrucciones SQL y desconectarse del origen de datos. Dependiendo de las necesidades y configuraciones, la aplicación puede ser capaz de “llamar” otras funciones ODBC.

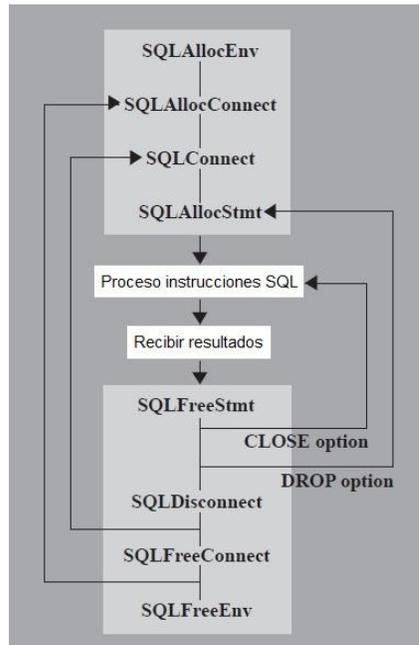


Figura 7. Proceso de conexión a origen de datos [15]

Una aplicación en particular, diseñada bajo determinado lenguaje de programación, puede admitir cualquier instrucción SQL suministrada por un origen de datos. Es importante resaltar que ODBC define una sintaxis estándar para definir las instrucciones de SQL. Esta aplicación deberá admitir instrucciones SQL que usen esta sintaxis, para lograr el máximo de interoperabilidad y para que el controlador pueda traducirlas al tipo de sintaxis que utiliza el origen de datos. En caso de que una aplicación ingrese una instrucción SQL que no use la sintaxis definida por el protocolo ODBC, el controlador la pasará directamente al origen de datos. La ejecución de instrucciones SQL se genera siguiendo la lógica mostrada en la Figura 8.

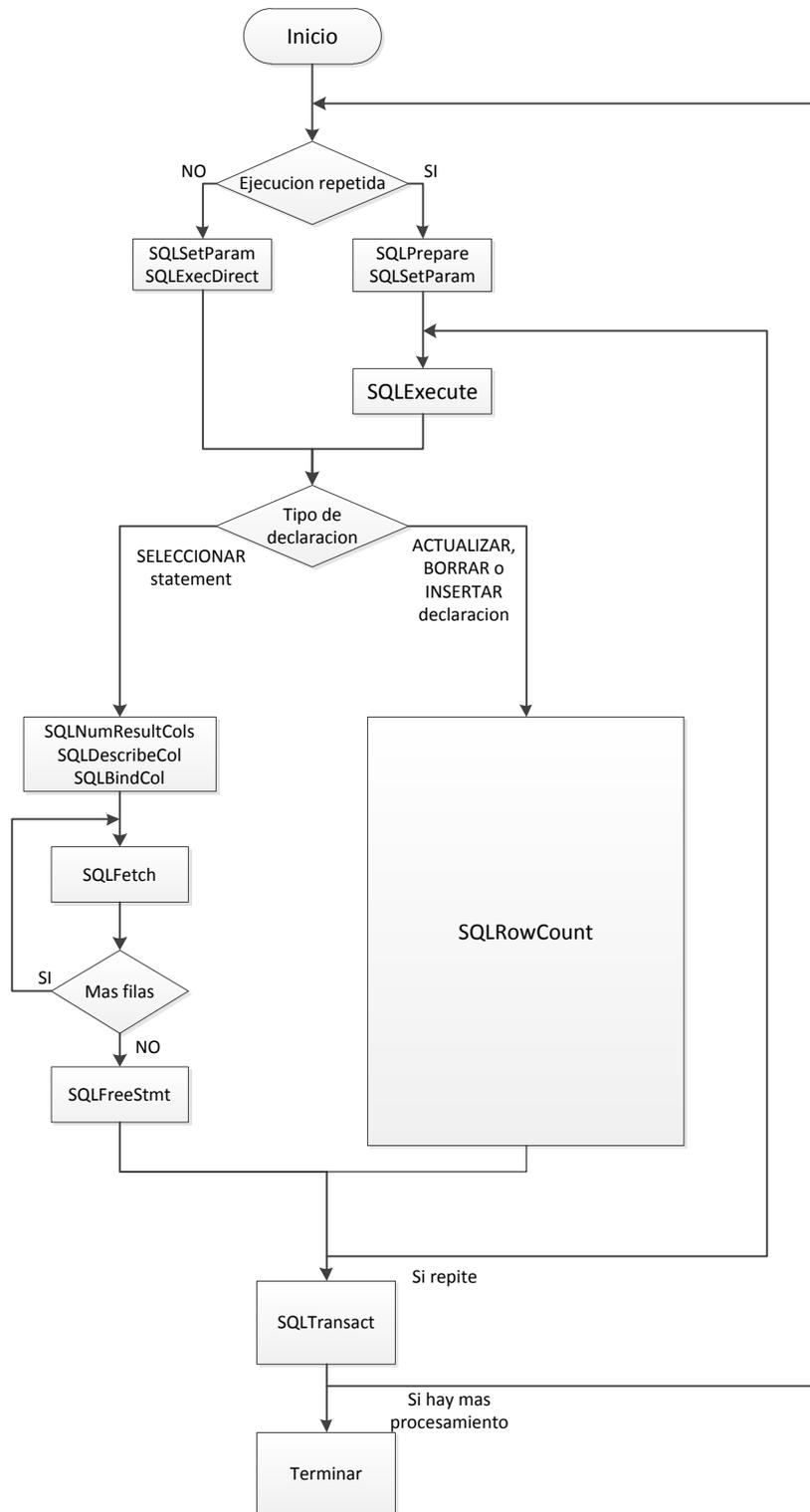


Figura 8. Secuencia de funciones ODBC para ejecutar declaraciones SQL [15]

El desarrollo de la aplicación a nivel de usuario puede dividirse en dos partes, el primero, un aplicativo de usuario para configuración a alto nivel (Eventos y acciones propias del manejo de las actividades y criterios de la empresa), control y visualización. El segundo consiste en la configuración de los parámetros de control a nivel de programación de los equipos a ser controlados, el cual se realiza utilizando la aplicación de *IR Learner* con la que viene preparado el software del controlador WACI NX+.

A continuación se detallan estas dos aplicaciones.

4.3.2. Descripción del software desarrollado para PC

A nivel de usuario final, el aplicativo desarrollado presenta una serie de ventanas en las cuales, de manera muy intuitiva, el usuario puede acceder a los distintos elementos instalados en la edificación de la empresa u organización. El control de dispositivos puede realizarse de dos modos: automático y manual. La escogencia de estos quedará a opción del administrador del sistema.

El modo automático consiste en programar previamente las acciones y los eventos que “disparan” estas acciones, los cuales se basan en las lecturas del control de acceso a los distintos miembros de la organización, ya sea por cumplimiento de permisos de uso, horarios o una combinación de ambas. De igual forma, existen elementos en la programación que gestionan el correcto uso de los recursos, como el apagado general de dispositivos en caso de la no presencia de personas en determinada área, por ejemplo. El funcionamiento de la lógica de operación, para el modo automático así como la codificación de empleados, eventos, acciones y estado se muestra en la Figura 9 y en la Tabla 2, 3, 4 y 5 respectivamente.

El modo manual se basa en la operación de los elementos de forma directa, mediante gestión del administrador del sistema. Las acciones en este modo no requieren programación de actividades de ningún tipo, simplemente la intervención directa del usuario para generar acciones tales como encendido, apagado, subir, bajar, etc., esto mediante la utilización de los

Tabla 2. Codificación de empleados

1. Empleados		
ID	Usuario	Estado (Act/Inact)
11	Javier	Ver cuadro de Estado
12	Jorge	
13	William	

Tabla 3. Codificación de Eventos

2.Eventos		Especificaciones	
ID	Evento	ID	Especificación
21	Ingreso Edificio	211	Puerta principal
		212	Cochera
		213	Edificio 2
22	Ingreso a la Oficina		
23	Salió del Edificio		
24	Salió de la Oficina		
25	Control manual de luces (Viene de sensor)	251	Pasillo principal
		252	Oficina
		253	Sala de reuniones
26	Control manual de A/C (Viene de sensor)	261	Oficina
		262	Sala de reuniones

Tabla 4. Codificación de Acciones

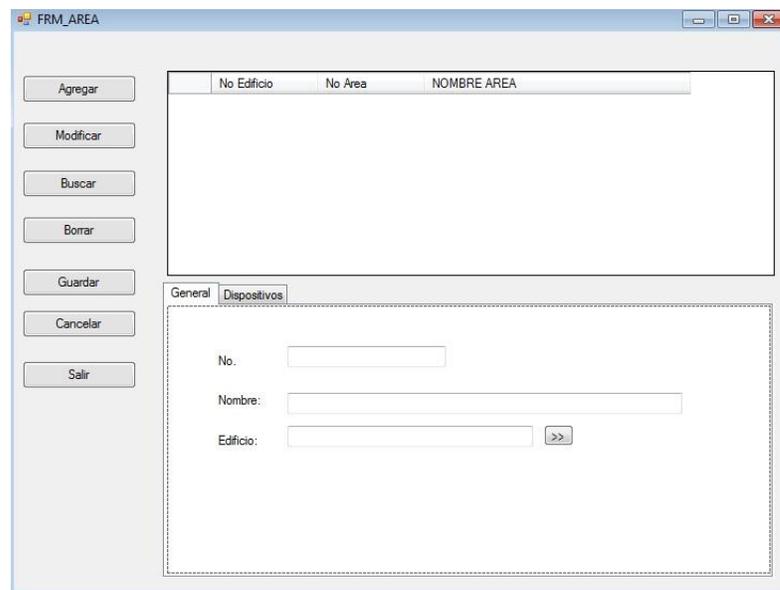
3. Acciones		Especificación		Detalle	
ID	Acción	ID	Especificación	ID	Detalle
31	Encender luces	311	Pasillo principal	3111	100%
				3112	75%*
				3113	50%*
		312	Oficina	3121	100%*
				3122	75%*
				3123	50%*
		313	Sala reuniones	3131	100%
				3132	75%*
				3133	50%*
32	Apagar luces	321	Pasillo principal		
		322	Oficina		
		323	Sala reuniones		
33	Abrir puerta	331	Oficina		
		332	Sala reuniones		
34	Cerrar puerta	341	Oficina		
		342	Sala reuniones		
35	Encender Aire	351	Oficina		
		352	Sala reuniones		
36	Apagar Aire	361	Oficina		
		362	Sala reunión		
37	Actualizar estado	371	Luz	3711	Pasillo Principal
				3712	Oficina
				3713	Sala reuniones
		372	Aire	3721	Oficina
				3722	Sala reuniones

Tabla 5. Codificación de Estado actual

Estado actual		
Especificación	ID	Detalle
Usuario	11A	Activo
	11B	Inactivo
	12A	Activo
	12B	Inactivo
	13A	Activo
	13B	Inactivo
	14A	Activo
	14B	Inactivo
Luz	311A	ON
	311B	OFF
	311C	%
	312A	ON
	312B	OFF
	312C	%
	313A	ON
	313B	OFF
	313C	%
Aire	371A	ON
	371B	OFF
	372A	ON
	372B	OFF

Menús para la interfaz con el usuario

El usuario podrá a través de una serie de menús de la aplicación, incorporar información referente a los edificios y áreas de la empresa así como los dispositivos que se encuentran conectados en cada uno de ellos. Algunos de estos menús se presentan a continuación. La Figura 10, por ejemplo presenta la ventana correspondiente para agregar o seleccionar el área del edificio que se desea controlar.



The screenshot shows a window titled "FRM_AREA" with a standard Windows-style title bar. On the left side, there is a vertical column of buttons: "Agregar", "Modificar", "Buscar", "Borrar", "Guardar", "Cancelar", and "Salir". The main area of the window is divided into two sections. The top section is a table with three columns: "No Edificio", "No Area", and "NOMBRE AREA". The bottom section is a form with two tabs: "General" (selected) and "Dispositivos". The "General" tab contains three input fields: "No.", "Nombre:", and "Edificio:". The "Edificio:" field has a small button with ">>" next to it.

Figura 10. Menú para agregar áreas

La Figura 11 de igual forma, muestra la ventana desde la cual se seleccionan los dispositivos conectados al área respectiva y que serán controlados por el usuario.

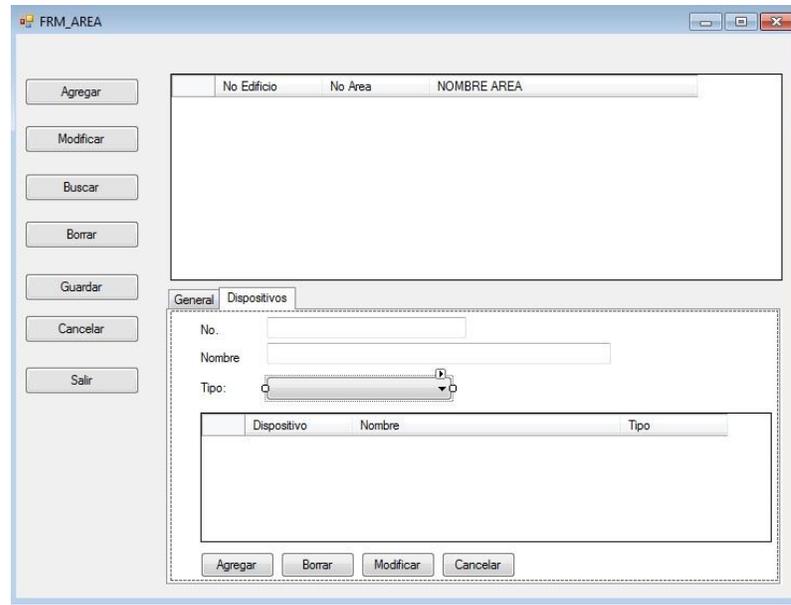


Figura 11. Menú para agregar dispositivos

Estas ventanas son solo parte del software desarrollado para interfaz con el usuario, desde el cual puede configurarse además los criterios de funcionamiento que requiera la empresa.

Software de manejo de puerto infrarrojo

El manejo del puerto infrarrojo vía Visual Basic se realizó implementando una serie de comandos, los cuales requirieron cumplir con la estructura o sintaxis necesaria para que el controlador WACI NX+ los pudiera traducir en el envío de datos infrarrojos. La estructura de este código se detalla en la Figura 12.

```

“Private Sub cmdIR_Click(ByVal sender As System.Object, ByVal e
As System.EventArgs) Handles cmdIR.Click
Waci.IR.SendCommand(1, "AireAcondicionado", "ON")
End Sub”

```

Figura 12. Estructura de código para comandos IR

Básicamente, esta estructura se puede explicar de la siguiente forma:

Para enviar un comando desde un puerto específico:

IR_SendCommand (Puerto, Grupo, Comando)

Sintaxis

```
HRESULT IR_SendCommand(  
[in] long Port,  
[in] BSTR Group,  
[in] BSTR Command,  
[out, retval] VARIANT_BOOL * Success  
);
```

Parámetros

Port [in]: Número de puerto IR (1-4)

Group [in]: Nombre del grupo que contiene el comando (Previamente grabado en el controlador)

Command [in]: Nombre del comando a enviar (Previamente grabado en el controlador)

Success [out, retval] TRUE si el comando fue enviado exitosamente, y FALSE si el WACI falló enviando el comando.

Nota

Comandos son típicamente agrupados por dispositivo.

4.3.3. Descripción del Software del Controlador

IR Learning

Como se mencionó anteriormente, el WACI NX+ tiene la capacidad de “aprender” o copiar los comandos enviados desde el control remoto de cierto dispositivo con el fin de poder controlarlo mediante el uso de parámetros definidos por la empresa o el usuario final.

El método empleado para proceder con este paso, se explica en la Figura 13, la cual muestra el menú de la aplicación del *IR Learning* situado en el web server del WACI NX+.

WACI NX+ by **AUROPA Multimedia**

SETUP DIAGNOSTICS EVENTS FILES

IR LEARNING

[Go to IR Diagnostics](#) - [Go to IR Setup](#)

Step 1 :

Choose or create a device file name:

File Name*: MillerDeluxe
 Device Make: AirConditioning
 Device Model: NCX1-024KNW2
 Remote Model: R11CQ/E
 Comment: Aire acondicionado Ing.

NOTE: Items with an asterisk (*) are required. Any new commands learned will be added to this file.

Step 2 :

Learn Mode: Standard Alternate

NOTE: Use Alternate learn mode only if there is trouble using Standard mode.

Step 3 :

Select the number of commands or template to learn:

Learn 1 commands or Select a template

NOTE: When using a template, skip the learn procedure for unwanted commands. More commands can be added at any time.

Step 4 :

Type in the name of command(s) below:

Select the IR port to test with Port 1

Name:

Figura 13. Aplicación del *IR Learning* en el WACI NX+

El primer paso consiste en escoger o bien crear un nombre para el dispositivo, el cual se guardará como un archivo particular. En esta sección se debe proveer cierta información del hardware, para así tener mayores referencias de cada uno y evitar errores de etiquetado.

El siguiente paso consiste en escoger el “modo de aprendizaje” a utilizar. Generalmente se utiliza el método estándar, mientras que el método alternativo se utiliza en caso de tener problemas con la comunicación durante el proceso de aprendizaje.

Como tercer paso es necesario escoger el número de comandos que se van a copiar o bien escogerlo desde una lista predeterminada.

Una vez realizados estos pasos, se escoge el puerto con el cual se va a probar el envío. En este punto, se ingresa el comando que quiere ser aprendido (*ON*, *OFF*, *DIM*, etc.) y se presiona el botón de “*TEST*”. El LED del *IR Learning* empezará a parpadear. Es en este momento en el que se apunta con el control remoto hacia el WACI NX+ y se presiona el botón que se quiere copiar. Se deberá seguir con este proceso hasta que el LED del *IR Learning* se apague. El botón “*TEST*” permitirá probar si en efecto el comando fue copiado de manera correcta.

4.4. Modificaciones posteriores

Al inicio de la implementación de la solución, se enmarcaron ciertos objetivos específicos los cuales debían cumplirse al finalizar el proyecto. Dentro de estos objetivos se encontraban el manejo de dispositivos vía comunicación infrarroja. Dichos dispositivos serían principalmente máquinas de aire acondicionado tipo *Split* y sistemas de iluminación fluorescente con balastro electrónico. Sin embargo, durante la implementación de este proyecto, la empresa determinó que el manejo de estos elementos fuese llevado a cabo en una etapa posterior y fuera de los alcances de este proyecto, pues consideraba evaluar otros métodos para hacerlo. Sin embargo, por motivos de que para ese momento el desarrollo de la aplicación se encontraba bastante avanzado, estos rubros fueron incorporados dentro de la solución ofrecida (como se mostró anteriormente en los diagramas de flujo, tablas y figuras de la aplicación), lo cual le permite a la empresa implementar esta etapa cuando lo considere pertinente en el momento que se cuente con los dispositivos de hardware necesarios (Interfaces IR para iluminación).

De esta forma se delimita el objetivo del proyecto a lograr la comunicación entre el sistema de seguridad y el del controlador automático. Este cambio se ilustró en la Figura 3 y Figura 4. La autorización para realizar este cambio de objetivos se muestra en el Figura A.2.1.

Al finalizar estas etapas de implementación, el procedimiento analítico empleado para comprobar la validez de la solución implementada se centró en la evaluación de desempeño obtenido contra desempeño esperado. El mismo se realizó mediante pruebas de campo y la utilización de páginas de diagnóstico proporcionadas por el WACI NX+, en donde se visualizara el estado de la comunicación de datos. Esta información se puede corroborar en los resultados presentados en la Figura 14, donde se muestra el resultado de las pruebas de envío de comandos vía infrarroja.

Una vez concluidas estas labores se procedió a informar mediante una exposición al personal del departamento de ingeniería de los resultados obtenidos en las pruebas del sistema.

4.5. Reevaluación y rediseño

La utilización de elementos de control, como el utilizado, proporciona muchas ventajas en cuanto al envío de información en diferentes vías y sobre distintos protocolos, sin embargo, es necesario considerar la necesidad de utilizar dispositivos similares cuando se quieran manejar áreas más grandes que las que están planteadas en este proyecto. Es por esto que se considera primordial definir los ambientes en los cuales se van a implementar soluciones de este tipo.

Además, es necesario valorar distintos medios de comunicación para control de iluminación, adicionales a la comunicación vía infrarrojo, pues aparte de tener algunas desventajas de operación, se queda muy atrás con respecto a soluciones encontradas en el mercado tecnológico actual.

Capítulo 5. Análisis de Resultados

A partir de la solución implementada se obtuvieron resultados con respecto a pruebas de campo realizadas para determinar el correcto funcionamiento del sistema. Principalmente, y como característica primordial de los objetivos del proyecto, se determinó que a partir de un evento enviado por el sistema de seguridad, el cual en este caso es el ingreso de determinado empleado por determinada lectora de control de acceso, se obtuviera una salida desde algún puerto del controlador WACI NX+, la cual en este caso se realizó por el puerto de comunicación Infrarrojo.

A continuación se presentan los resultados obtenidos en las pruebas de campo finales del sistema.

Inicialmente, fue necesario ingresar en el menú de funcionarios de la aplicación, los empleados a los cuales se les va asignar los permisos asociados para el uso del sistema. Esto consiste en importar de la base de datos del sistema LENEL los funcionarios que se requieran e incorporarlos dentro de la aplicación del usuario. Esto permitirá poder asignar tareas al sistema en dependencia del funcionario que ingrese por la lectora de control de acceso respectiva.

Una vez ingresados los funcionarios requeridos, se realizó la verificación de ingreso mediante la tabla de visualización de eventos que puede ser accesada desde la base de datos de LENEL, un segmento de la misma se muestra en la Tabla 6.

.

Tabla 6. Tabla de visualización de eventos de LENEL

ID	Date	Time	Device	Aut	DevFunc
1236761083	3/16/2011	10:14 AM	3	0	0
1236761085	3/16/2011	10:15 AM	7	0	0
1236761084	3/16/2011	10:15 AM	7	0	0
1236761086	3/16/2011	10:17 AM	6	0	0
1236761087	3/16/2011	10:20 AM	7	0	0
1236761088	3/16/2011	10:21 AM	6	0	0
1236761088	3/16/2011	10:22 AM	7	0	0
1236761088	3/16/2011	10:23 AM	6	0	0
1236761088	3/16/2011	10:23 AM	7	0	0
1236761092	3/16/2011	10:24 AM	3	0	0
1236761093	3/16/2011	10:25 AM	7	0	0
1236761088	3/16/2011	10:26 AM	6	0	0
1236761095	3/16/2011	10:27 AM	3	0	0
1236761096	3/16/2011	10:28 AM	6	0	0
1236761097	3/16/2011	10:29 AM	5	0	0
1236761098	3/16/2011	10:30 AM	3	0	0
1236759987	3/16/2011	10:30 AM	0	0	4
1236760076	3/16/2011	10:30 AM	0	0	4
1236761099	3/16/2011	10:32 AM	5	0	0
1236761100	3/16/2011	10:35 AM	6	0	0
1236761088	3/16/2011	10:37 AM	7	0	0
1236761102	3/16/2011	10:37 AM	5	0	0
1236760078	3/16/2011	10:40 AM	0	0	4
1236761103	3/16/2011	10:50 AM	7	0	0
1236761104	3/16/2011	10:52 AM	7	0	0
1236761105	3/16/2011	10:54 AM	6	0	0
1236761106	3/16/2011	10:56 AM	3	0	0
1236759089	3/16/2011	10:59 AM	0	0	4
1236761108	3/16/2011	10:59 AM	0	0	4

En esta tabla, se indica el "ID" o identificación del funcionario, la fecha y la hora en que generó el evento (entrada o salida), y en lectora lo hizo (*Device*). El nombre del funcionario al cual se refiere el número de identificación no se muestra en esta tabla debido a configuraciones de seguridad propias del sistema, por lo que la

corroboración de esta relación se debió realizar mediante otros métodos los que no se mencionan por no creerse conveniente revelar ese tipo de información, la cual es confidencial de la empresa e irrelevante en demostrar los resultados del sistema.

De esta forma se permite verificar que la condición principal del sistema se cumple, o sea, que dado un evento en el sistema de seguridad se desencadenen una serie de acciones en la aplicación.

En esta tabla se describe el ingreso de una cantidad considerable de funcionarios en distintas lectoras por lo que para estas pruebas se tomaron los eventos generados por el funcionario con la ID número 1236761088 en la lectora número 6 y número 7, ubicadas en la oficina del Departamento de Ingeniería de la empresa. Los eventos generados quedan registrados en esta tabla y como se ha explicado anteriormente, dicha información es tomada como base en la ejecución de rutinas dentro del aplicativo para lograr una señal de salida en el controlador.

Básicamente, cuando se tiene registro de que se generó un evento (entrada de funcionario en este caso) por parte del funcionario 1236761088 en la lectora número 7, se procederá a verificar la salida del puerto IR-1 del dispositivo de control WACI NX+.

De igual forma, cuando el funcionario presente su identificación en la lectora número 6 (la cual está dentro de la oficina, permitiendo su salida de la misma), propicia que el sistema genere un evento de “apagado”, por lo que el dispositivo envía esta señal a través del puerto IR-1.

Para la verificación de funcionamiento de esta comunicación se debe realizar la verificación de dos formas:

1. Visual, pues cada vez que se envía algún dato vía puerto infrarrojo, el emisor de IR encenderá el LED ubicado en la parte posterior del mismo (Ver apartado 5.2.3.2).
2. Verificando los estados de puertos y confirmación de envío de información por parte del controlador. Esto se puede realizar corroborando en el

dispositivo el diagnóstico de puertos (Esta opción la proporciona el web server del WACI NX+).

Justamente este diagnóstico de estados de la comunicación es el que se muestra en la Figura 14 y Figura 15, donde es posible verificar que el envío de datos por el puerto infrarrojo, para ambas funciones, se hizo correctamente.

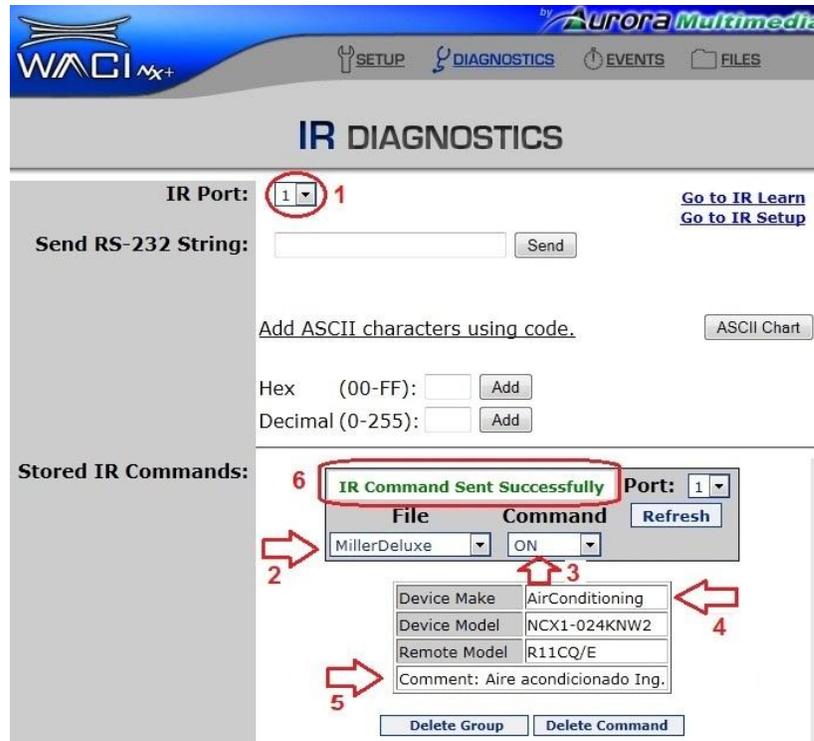


Figura 14. Confirmación de envío correcto de comando de encendido

La información que proporciona esta ventana puede describirse de la siguiente forma, de acuerdo a la numeración mostrada en la Figura 14 (y de similar forma en la Figura 15):

1. Se ingresa el número de puerto por el cual se está enviando la información y en el cual se desea hacer el diagnóstico.
2. Se describe el dispositivo al cual se está enviando el comando, el cual debió ser previamente grabado en el controlador utilizando el procedimiento mostrado en

la Figura 13. En este caso se tomó el dispositivo guardado en archivo como “MillerDeluxe”.

3. Se describe cual comando es el que se envió al dispositivo anteriormente seleccionado. Para el caso en cuestión se envió un comando de “ON” (encendido) y otro de OFF (apagado).
4. Se describe el tipo de dispositivo que se está controlando. En este caso, corresponde a un aire acondicionado.
5. Se describen detalles del dispositivo como por ejemplo su ubicación en el edificio. En esta caso, se muestra el aire acondicionado del Departamento de Ingeniería (Ing.)
6. Se visualiza el estado del comando IR que fue enviado. En este caso se observa que el comando IR ha sido enviado satisfactoriamente (“*IR Command Sent Successfully*”).

De esta forma es posible comprobar el correcto envío de datos a través del sistema, correlacionando lo observado en el emisor de IR con el diagnóstico mostrado en el WACI NX+.

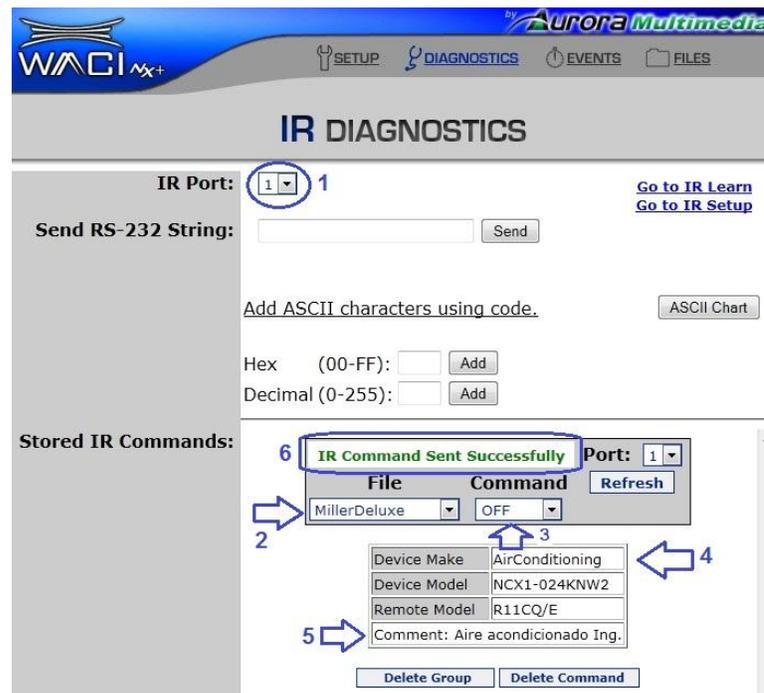


Figura 15. Confirmación de envío correcto de comando de apagado

Adicionalmente a estas pruebas, fue posible visualizar la ventana de la aplicación en la cual se publica la información del estado de las acciones ejecutadas mediante el número de Edificio, Área, Dispositivo, tipo de dispositivo y estado del mismo. Esta información se muestra en la Figura 16, donde el estado del puerto en cuestión es de “encendido”.

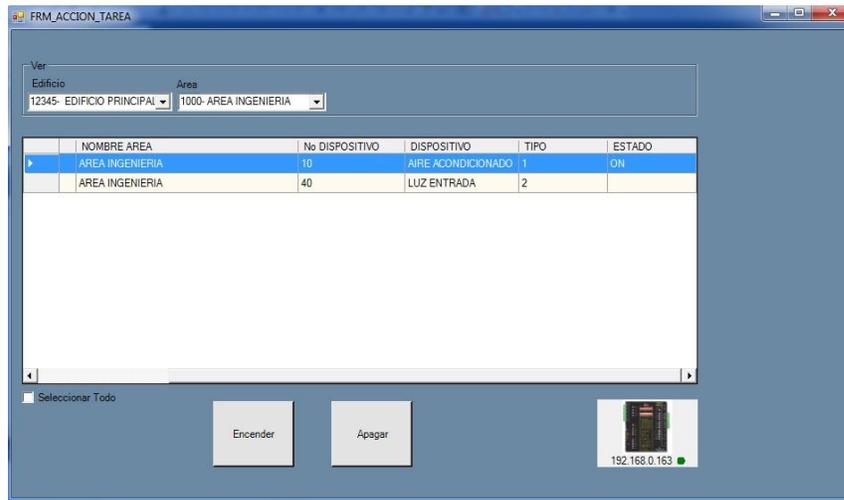


Figura 16. Visualización del estado de acción encendido

De igual forma la Figura 17 proporciona información del otro estado del sistema, en este caso el de “apagado” mostrando el comportamiento de acuerdo a las entradas de eventos provenientes de las dos lectoras que se utilizaron en la prueba, una para cada estado.

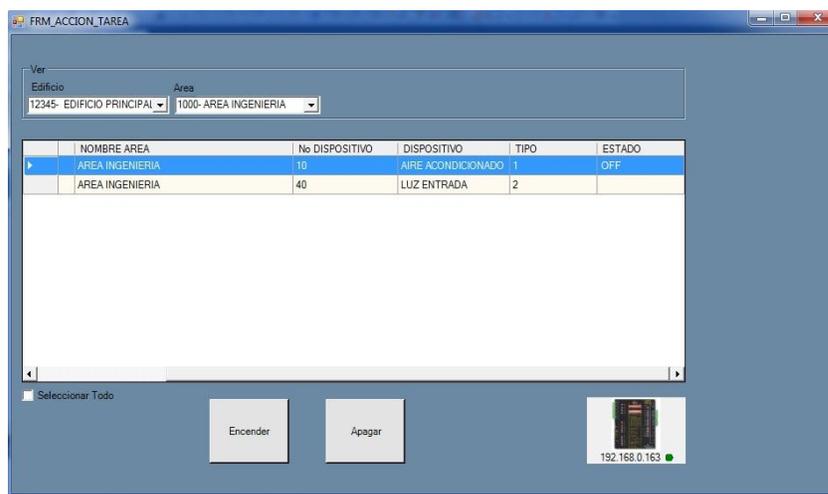


Figura 17. Visualización del estado de acción apagado

La información suministrada en este apartado evidencia el correcto funcionamiento de la integración entre los dos sistemas de interés para la empresa, el de seguridad y el de automatización, en cuanto a la “traducción” de protocolos para lograr la comunicación entre ellos y lograr acciones de uno sobre otro. Esto ha quedado demostrado mediante el desarrollo de las pruebas antes descritas, sin embargo, es necesario para futuras etapas implementar el control de los distintos dispositivos que inicialmente se plantearon dentro de los objetivos de este proyecto y que, como se ha explicado a lo largo de este documento, fueron modificados en el proceso. De esta forma se logrará un mayor entendimiento de los alcances de la aplicación desarrollada así como la comprobación de sus ventajas y limitantes en comparación a sistemas de control existentes como lo son el de la iluminación, la climatización, elementos multimedia y dispositivos motorizables (persianas y toldos).

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones.

1. La integración de diferentes sistemas en una edificación mediante una sola interfaz generan ventajas al usuario final en cuanto a simplicidad de operación desde un solo punto.
2. La integración de sistemas le provee a las empresas integradoras posibilidades para expandir sus operaciones y ganancias con clientes que ya posean una de sus plataformas.
3. El protocolo ODBC permite establecer de manera simple una comunicación entre bases de datos y aplicaciones realizadas en Visual Basic.
4. Mediante el lenguaje de programación Visual Basic es posible lograr el manejo de puertos infrarrojos del dispositivo controlador WACI NX+ de Aurora Multimedia.
5. El Controlador WACI NX+ es capaz de manejar vía remota diferentes puertos a través de aplicaciones externas no necesariamente nativas.
6. El sistema de seguridad LENEL OnGuard® proporciona la suficiente información de eventos y alarmas necesaria para ejecutar funciones de automatización.

6.2 Recomendaciones

1. Implementar esta aplicación en el control de dispositivos como balastos electrónicos de iluminación, aires acondicionados, persianas, etc.
2. Realizar pruebas de consumo energético para visualizar el ahorro que la aplicación de automatización genera en un edificio.
3. Generar información para los clientes de la empresa en donde se resalte la integración del sistema de seguridad que poseen con un sistema de automatización de edificios.
4. De ser posible, implementar el uso de elementos de control como sensores de temperatura, de presencia y de movimiento para darle más funcionalidades al sistema de automatización.
5. Investigar posibles integraciones del sistema implementado con protocolos abiertos de control de edificios tales como KNX, BACNET o LONWORKS y protocolos de automatización industrial tales como MODBUS y OPC.

Bibliografía

- [1] CASAS A., *Sistema Telefónico Multilínea con Reconocimiento de Voz y Acceso a Base de datos Remota*. Departamento de Ingeniería Electrónica, Universidad Politécnica de Madrid, España, 1997.
- [2] CEDOM. *Cómo ahorrar energía instalando domótica en su vivienda. Gane en confort y seguridad* [en línea], 2008. Disponible en WWW: http://www.idae.es/index.php/mod.documentos/mem.descarga?file=/documentos_11187_domotica_en_su_vivienda_c7a81517.pdf. [Consulta: 18 Mayo, 2010]
- [3] *Control de acceso físico* [en línea]. Tecnológica de Costa Rica. 2008. Disponible en WWW: <http://www.grupotec.com/index.php?page=control-de-acceso&hl=esp>. [Consulta: 4 de abril, 2011]
- [4] *Dual Reader Interface Module* [en línea]. LENEL. 2010. Disponible en WWW: http://www.lenel.com/sites/default/files/HW_LNL-1320-Series2.pdf. [Consulta: 20 de setiembre, 2010]
- [5] FLORES, R. *Tecnológica de Costa Rica* [en línea], 2008. Disponible en WWW: <http://www.grupotec.com>. [Consulta: 18 Mayo, 2010]
- [6] *Getting Started Using ODBC with SAS and SPSS* [en línea]. Indiana University. 2003. Disponible en WWW: <http://www.indiana.edu/~statmath/stat/all/odbc/printable.pdf>. [Consulta: 17 de Octubre, 2011]
- [7] HORST F. *Espectro electromagnético* [en línea]. 2009. Disponible en WWW: http://es.wikipedia.org/wiki/Archivo:Electromagnetic_spectrum-es.svg [Consulta: 1 de abril, 2011].
- [8] KIBBEY, R. *Understanding Security Basics: A Tutorial on Security Concepts and Technology*. Science Applications International Corporation, Melbourne, Florida. 2005.
- [9] *LENEL OnGuard* [en línea]. LENEL. 2010. Disponible en WWW: <http://www.lenel.com/onguard>. [Consulta: 23 de Agosto, 2010].
- [10] *Manual de Microsoft Access: ODBC* [en línea]. Disponible en WWW: <http://www.duiops.net/manuales/access/access16.htm>. [Consulta: 06 de marzo, 2011].

- [11] MARTINEZ, L. *Empresas con base Tecnológica* [en línea], 2007. Disponible en WWW:
http://www.gestiopolis.com/recursos/documentos/fulldocs/emp/ebt.htm_
[Consulta: 18 Mayo, 2010]
- [12] MARTINEZ, M.; SENDRA F. *Radiación Infrarroja* [en línea]. Disponible en WWW:
http://www.sld.cu/galerias/pdf/sitios/rehabilitacion-fis/radiacion_infrarroja.pdf.
[Consulta: 1 de abril, 2011]
- [13] MENDIBURU, H. *Automatización Medioambiental*. INDECOPI – PERU. Lima Perú. Mayo, 2003.
- [14] *MySQL Connector/ODBC* [en línea]. Oracle, 1997, 2011. Disponible en WWW: downloads.mysql.com/docs/connector-odbc-en.pdf. [Consulta: 23 de Octubre, 2010]
- [15] *ODBC 2.0: Programmer's Manual* [en línea]. Inprise Corporation. 2000. Disponible en WWW:
http://download.oracle.com/otn_hosted_doc/timesten/706/TimesTen-Documentation/ms.odbc.pdf. [Consulta: 24 Octubre, 2010]
- [16] *Reference Manual & Programming Guide* [en línea]. Aurora multimedia, 2007. Disponible en WWW: <http://waciworld.com/?section=products&id=4>. [Consulta: 19 de Julio, 2010]
- [17] *Software de Integración* [en línea]. Tecnológica de Costa Rica. 2008. Disponible en WWW:
<http://www.grupotec.com/index.php?page=integracion&hl=esp>. [Consulta: 4 de abril, 2011]
- [18] SOLIDES, G. *Edificios Inteligentes* [en línea]. Disponibles en WWW: <http://www.gruposolides.com/dloads/SOLIDES-EdificioInteligente.pdf>. [Consulta: 22 de marzo, 2011]
- [19] *WACI Control Products* [en línea]. Aurora Multimedia, 2011. Disponible en WWW: <http://waciworld.com/?section=products&id=4> [Consulta: 18 de Julio, 2010]

Apéndices

Apéndice A.1 Siglas y acrónimos

API	Application Programming Interface Interfaz de Programación de Aplicaciones
BMS	Building Management System Sistema de Administración de Edificios
CCTV	Circuito Cerrado de Televisión
DBMS	Database Management System Sistema Gestor de Bases de Datos
DRI	Dual Reader Interface Interfaz de Doble Lectura
DSN	Data Source Name Nombre de Origen de datos
DSP	Digital Signal Processor Procesador Digital de Señal
GUI	Graphical User Interface Interfaz Gráfica de Usuario
HDBC	Handle Data Base Connectivity Conectividad Manejo de Base de Datos
HVAC	Heating, Ventilacion, Air Conditioning Calefacción, Ventilación, Aire Acondicionado
IDE	Integrated device Electronics Dispositivos Electrónicos Integrados
IR	Infrarrojo
ISC	Intelligent System Controller Controlador de Sistema Inteligente
LED	Light-Emitting Diode Diodo Emisor de Luz
ODBC	Open Database Connectivity

Conectividad Abierta de Base de Datos

PC	Personal Computer Computadora Personal
SQL	Structured Query Language Lenguaje de Consulta Estructurado
YIPI	Your IP Interface Su Interfaz IP

	<p>Sistema de control de edificios Tecnológica de Costa Rica S.A.</p>	<p>Página 1/4</p>
<p>Manual de Usuario</p>		

La presente es una guía del Sistema de control de edificios creado por la empresa Tecnológica de Costa Rica y tiene como objetivo orientar al usuario en la configuración y utilización del mismo.

Configuración del Edificio y sus componentes

Inicialmente, es necesario configurar el número y nombre de edificios con los que cuenta la empresa o usuario, esto se logra mediante la utilización de la pestaña “Edificio”. Esta configuración se muestra en la siguiente figura:

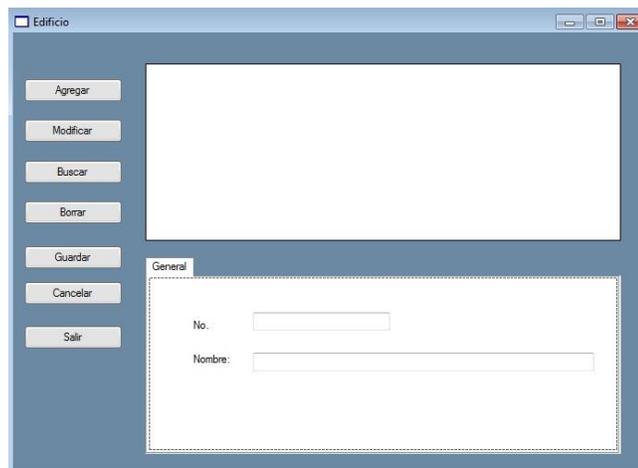
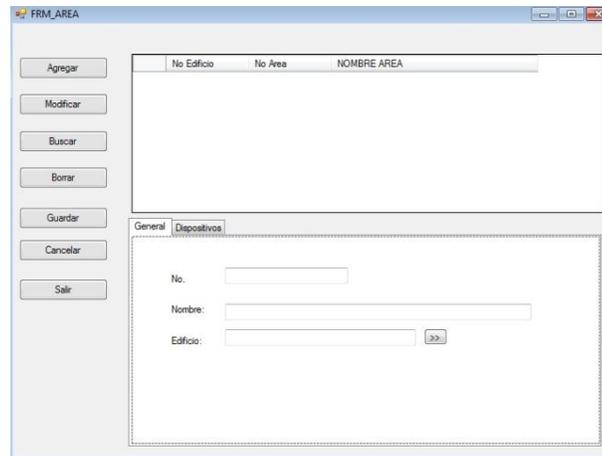


Figura A.2.1. Ventana para agregar edificio

Una vez agregados los edificios correspondientes, se deben ingresar el o las áreas que se desean estén vinculadas a cada edificio. (No es necesario incorporar áreas que no cuenten con dispositivos a ser controlados). Esta acción se lleva a cabo mediante el menú de “Áreas”, donde además de ingresar el número y nombre de la misma se debe indicar en cual edificio (previamente ingresado, ver paso anterior) se encuentra ubicado. Esto se muestra en la figura siguiente:

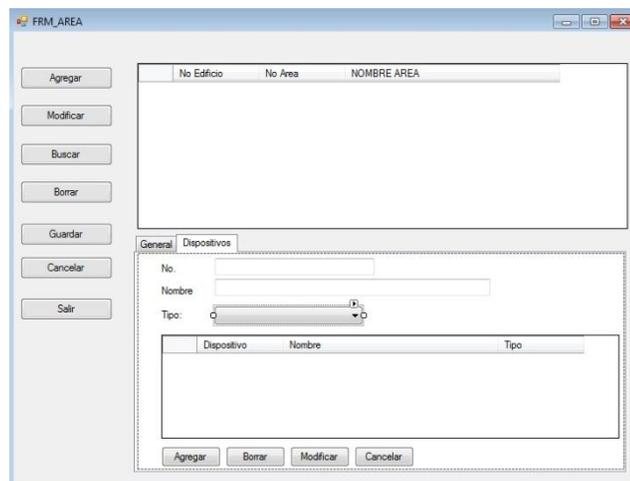
Manual de Usuario



The screenshot shows a software window titled 'FRM_AREA'. On the left side, there is a vertical column of buttons: 'Agregar', 'Modificar', 'Buscar', 'Borrar', 'Guardar', 'Cancelar', and 'Salir'. The main area of the window is divided into two sections. The top section contains a table with three columns: 'No Edificio', 'No Area', and 'NOMBRE AREA'. The bottom section is a form with two tabs: 'General' and 'Dispositivos'. The 'Dispositivos' tab is active, showing three input fields labeled 'No.', 'Nombre:', and 'Edificio:', with a right-pointing arrow button next to the 'Edificio:' field.

Figura A.2.2. Ventana para agregar áreas de un edificio

Una vez realizada esta acción, se deben vincular los dispositivos que se encuentran dentro de cada área, con el fin de identificarlos y así efectuar acciones de control sobre ellos. Mediante la pestaña “Dispositivos” es posible indicar el número, nombre y tipo de dispositivo que se quiere agregar, tal como se muestra a continuación:



The screenshot shows the same 'FRM_AREA' window, but with the 'Dispositivos' tab selected. The 'Dispositivos' tab contains three input fields: 'No.', 'Nombre', and 'Tipo:'. The 'Tipo:' field has a dropdown arrow. Below these fields is a table with three columns: 'Dispositivo', 'Nombre', and 'Tipo'. At the bottom of the 'Dispositivos' tab, there are four buttons: 'Agregar', 'Borrar', 'Modificar', and 'Cancelar'.

Figura A.2.3. Ventana para agregar Dispositivos

Manual de Usuario

Se tienen ahora los distintos edificios con sus respectivas áreas, vinculadas a los diferentes dispositivos que se encuentran en cada uno de ellos.

Configuración de usuarios

Es necesario en este punto ingresar los funcionarios de la empresa, a los cuales se le asignaran condiciones de control vinculados de dispositivos vinculados a ciertas características del control de acceso. La lista de funcionarios de la empresa se importa directamente de la base de datos del sistema de seguridad, por lo que la acción necesaria por parte del usuario será escoger de dicha lista los funcionarios que desea asociar. Este menú se ilustra en la

Figura A.2.4. En caso de que la lista sea demasiado extensa, es posible generar una búsqueda ingresando el nombre y apellido del funcionario que se desea ingresar y pulsar el botón “Buscar”.

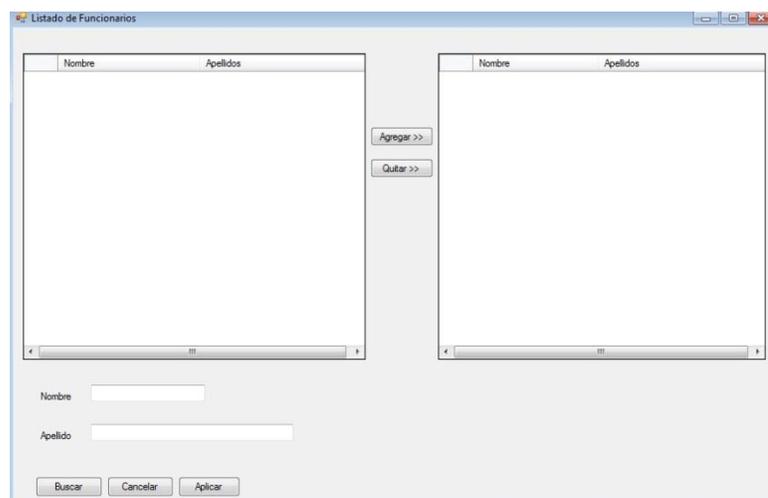


Figura A.2.4. Menú de selección de funcionarios

Manual de Usuario

Con la información ingresada en los puntos anteriores es posible asignar ciertas condiciones de uso de los distintos dispositivos. Sin embargo, al tratarse de información confidencial de los sistemas de control de acceso del sistema de seguridad de la empresa es necesario contar con los permisos y condiciones necesarias para manipular acciones dentro de los distintos edificios. Es por esta razón que la vinculación de las distintas acciones, que se generen de forma automática dada la programación del sistema, sea manejada por un administrador de red o del sistema de seguridad, con el fin de salvaguardar las políticas de seguridad establecidas previamente.

El usuario puede realizar monitoreo sobre el estado del sistema y actuar de forma manual sobre los dispositivos instalados mediante el menú de control de la Figura A.2.5. Desde aquí es posible accionar todos los dispositivos que se hayan ingresado anteriormente, así como visualizar el estado y dirección IP del controlador.

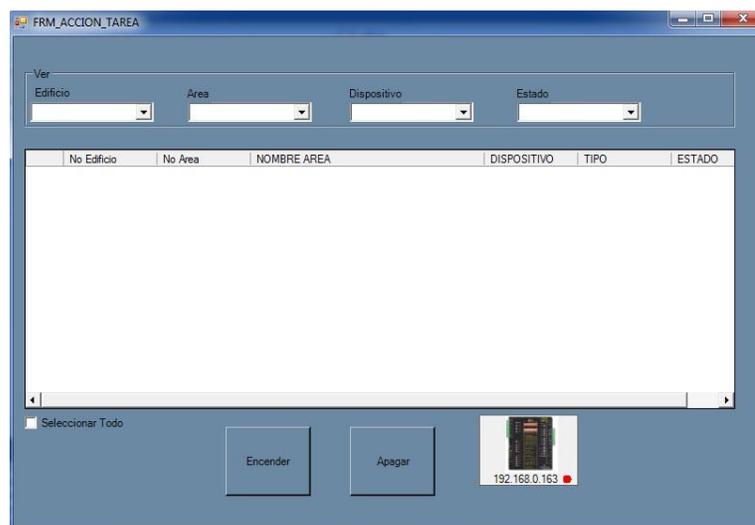


Figura A.2.5. Menú de Visualización y control de dispositivos

Anexos

Anexo B.1 Aclaratoria sobre cambios en los objetivos del Proyecto

A quien interese

Por este medio realizo la aclaratoria respectiva con respecto a los cambios hechos en los objetivos originalmente planteados de este proyecto. Estas variantes se debieron primordialmente a aspectos de tiempo, valoración de nuevas tecnologías y razones económicas.

Durante la realización de este proyecto se lograron determinar ciertas etapas primordiales en relación a los requerimientos inmediatos de la empresa, lo cual dio como resultado la aprobación de una nueva dirección del mismo. Los resultados finales que se dieron de este análisis permitieron concluir la necesidad de limitar el proyecto a la fase de integración de sistemas, la cual se describe a lo largo de este informe.

Se extiende esta nota de aclaración y autorización a solicitud del interesado.

Rohrmoser, Febrero del 2011.



Royden Flores C., Presidente
Tecnológica de Costa Rica S.A.



*Reference Manual &
Programming Guide*



WACI NX+



**WACI NX
Jr.**

Revision 2007.01.09

*Aurora Multimedia
205 Commercial Court
Morganville, NJ 07751
(732) 591-5800
(732) 591-5801 (Fax)
www.auroramultimedia.com*

Tabla B.2.1. Especificaciones Generales de Hardware

V. Hardware Specifications

General Specifications

		WACI NX Jr.	WACI NX+	Notes
Size	5.8" H x 4.9" W x 0.9" D	√	√	
Weight	0.6 lbs.	√	√	
Power Adapter	12V DC	15watt	15watt	
Processor	32-Bit	√	√	750 MIPS Normal Mode 1 BIPS Super Mode
Co-Processing	DSP		√	
	Cipher (Safenet)	√	√	Supports DES, 3DES, AES, ARC-4, SHA-1, MD5 Implements entire IPsec packet processing in hardware – no CPU burden True Random Number Generator (RNG) in hardware Robust security is ideal for most business network environments – meets U.S. government and banking industry requirements
	IR (True Trigger)	√	√	Highly Accurate IR Capture and reproduction
Memory	Total RAM	32M	64M	500DDR 32 bit wide
	Total Flash	16M	32M	
	Available Flash	5M	20M	Available Flash Memory may vary, based on firmware version.

Display	106 x 56 Pixels Backlit	√	√	
Ports	LAN Network Adapter (RJ-45 / Ethernet)	2	2	10/100Mbits Auto MDX POE add-on available
	USB OTG (On-The-Go) v1.1	1	1	11Mbits Host or Client
	RS-232/422/485 (DB-9)	2	2	15KV Protection, 115KB Max
	Infrared Outputs (IR)	2	4	30KHz – 2MHz RS-232 TX as well
	Infrared Input	1	1	IR input device triggers
	DSP (4 modes of Operation) Analog to Digital Input (A/D) Digital to Analog (D/A) Digital Input Digital Output		4	12-Bit Accuracy 16-Bit Accuracy High Impedance 200ma Sink Open Drain
	Relay (SPDT)		4	C-Type (NO, NC, CP)
Monitoring	32-Bit Internal Clock/Calendar	√	√	
	IR Learner	√	√	30KHz – 2MHz
	Internal Temp Sensor	√	√	
Network Access	Web & FTP	√	√	

Specifications subject to change without notice.

Tabla B.2.2. Rangos de funcionamiento del Hardware

Absolute Maximum Ratings for Hardware

Below is a summary of the minimum, maximum, and typical values for the hardware.

These are maximum ratings only. Operation of the device at or above these ratings for extended periods of time may affect reliability.

	Min	Typ	Max	Units	Notes
WACI Input Voltage	+8	+12	+18	V	WACI NX: Min. 15watt supply
Storage Temperature	-20		+55	°C	
Digital I/O Input	-5		5	V	
Digital I/O Output	0		5	V	Can source up to 20mA at 5V
A/D Input	-5		5	V	
Relay	0		2	A	Max 30V DC

Anexo B.3 Dual Reader Interface Module LNL-1320 Series 2 (LENEL) [4]



Access Control

Dual Reader Interface Module

LNL-1320 Series 2

Lenel Systems International offers a Dual Reader Interface (DRI) module for access control solutions. Most access control card readers, keypads, or readers with keypads that use standard Wiegand Data1/Data0 or Clock/Data communication are supported, as are those that support the bidirectional RS-485 Open Supervised Device Protocol (OSDP). Lock, unlock, and facility code offline access modes are supported on all readers connected to the DRI. Each DRI supports up to eight different card formats as well as issue codes for both magnetic and Wiegand card formats.

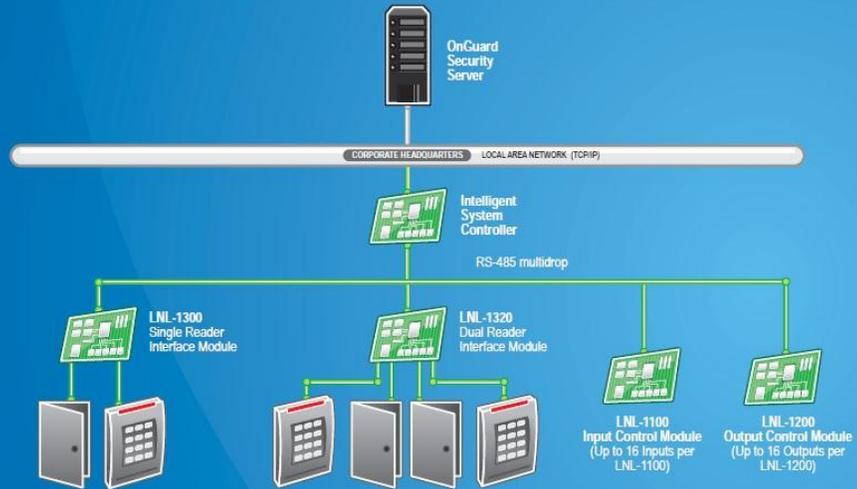
The DRI provides a vital link between the Intelligent System Controller (ISC) and the card reader attached to the interface. As many as 32 DRI modules can be multidropped using RS-485 2-wire or 4-wire communication up to 4,000 feet per port away from the ISC. Each DRI module is individually addressed for increased reporting capabilities with OnGuard access control software applications. The DRI includes eight inputs that support normally open, normally closed, supervised, and non-supervised circuits. In addition, six output relays support fail-safe or fail-secure operation.

Features and Functionality

- 12 or 24 VDC power supply
- Supports Data1/Data0, Clock/Data and Lenel OSDP-compatible RS-485 readers and keypads
- Downloadable firmware
- Six Form-C 5 A at 30 VDC relay outputs
- Up to 16 different formats (8 card formats and 8 asset formats)
- Issue code support for magnetic and Wiegand formats
- Door contact supervision (open/closed)
- REX push-button monitor
- Strike control output
- Bicolor reader status LED support and 2-wire LED support
- Beeper control
- Dedicated tamper and power failure circuits
- Support for offline reader access mode
- On-board jumpers for termination
- On-board regulator allows 12 VDC reader support from 24 VDC power source
- DIP switch-selectable addressing



Figura B.3.1. Características de lectora LNL-1320



Access Control

Power Supplies & Enclosures

LNL-AL400ULX	Lenel UL-listed 4 A, 110 VAC power supply - 12 or 24 VDC 4 A output (switch-selectable), 120 VAC input, continuous supply current with enclosure (12 x 16 x 4.5 in. / 305 x 406 x 114 mm), lock and open frame transformer, tamper switch, UPS-capable (battery optional), UL-listed
LNL-AL600ULX-4CB6	Lenel UL Listed Power Supply - 12 or 24 VDC 6 A output (switch-selectable), 120 VAC (1.6 amps) input, continuous supply current with enclosure (18 x 24 x 4.5 in. / 457 x 610 x 114 mm), lock and open frame transformer, tamper switch, UPS-capable (battery optional), UL-listed
ABT-12	Battery kit - 12 VDC, 12 AH battery (PS-12120)

Specifications

Primary Power (DC)	* The DRI is for use in low voltage, power-limited, class 2 circuits only.
DC input:	12 or 24 VDC ± 15% 450 mA
Reader Power	
DC output:	12 VDC, 125 mA regulated or 12 to 24 VDC 125 mA current limited
Reader Port Compatibility	Wiegand Data 1/Data 0 Magnetic Clock/Data F/2F single-wire protocol Open Supervised Device Protocol (RS-485)
Environmental	
Temperature:	Operating: 0° to +70° C (32° to 158° F) Storage: -55° to +85° C (-67° to 185° F)
Humidity:	0 to 95% RHNC
Mechanical	
Dimension:	6 x 8 x 1 in. (152 x 203 x 25 mm)
Weight:	10 oz. (290 g) nominal
Approvals	UL 294 and 1076-listed, CE-marked, ROHS compliant

Figura B.3.2. Especificaciones de Lectora LNL-1320