



Universidad
Zaragoza

Proyecto Fin de Carrera

Diseño del nuevo SCADA para el laboratorio de Tecnologías Avanzadas Digitales de Producción (ADMT) mediante LabVIEW

Autor

Noel Pueyo Izquierdo

Director:

Ramón Piedrafíta Moreno

Escuela de Ingeniería y Arquitectura

2014



**PROPUESTA y ACEPTACIÓN DEL
PROYECTO FIN DE CARRERA DE INGENIERÍA TÉCNICA**

DATOS PERSONALES

APELLIDOS, Nombre

Pueyo Izquierdo, Noel

Nº DNI 72992579-D Dirección Juan José Lorente; Nº:52; 3lзда

C.P. 50005 Localidad Zaragoza

Provincia Zaragoza Teléfono 650903654 NIA: 604397

Firma:

DATOS DEL PROYECTO FIN DE CARRERA

INGENIERIA TECNICA INDUSTRIAL, Especialidad Electrónica Industrial

TITULO Diseño del nuevo SCADA para el laboratorio de Tecnologías Avanzadas Digitales de Producción de UCLan mediante LabVIEW

DEPÓSITO EN: ZAGUAN (Obligatorio) ☐ y CD-ROM ☐ (si PFC es tipo B aplicación informática)

DIRECTOR Ramón Piedrafita Moreno

VERIFICACIÓN EN SECRETARÍA

El alumno reúne los requisitos académicos (1) para la adjudicación de Proyecto Fin de Carrera

SELLO DEL CENTRO



Escuela de
Ingeniería y Arquitectura
Universidad Zaragoza

EL FUNCIONARIO DE SECRETARIA

Fdo.:

SE ACEPTA LA PROPUESTA DEL PROYECTO (2)

En Zaragoza, a 20 de NOVIEMBRE de 2.0 14

Fdo.: RAMON PIEDRAFITA MORENO

DIRECTOR DEL PFC

SE ACEPTA EL DEPÓSITO DEL PROYECTO

En Zaragoza, a 20 de NOVIEMBRE de 2.0 14

Fdo.: RAMON PIEDRAFITA MORENO

DIRECTOR DEL PFC

(1) Requisitos académicos: tener pendientes un máximo de 24 créditos o dos asignaturas para finalizar la titulación.

(2) Para que la propuesta sea aceptada por el Director, es imprescindible que este impreso esté sellado por la Secretaría de la EINA una vez comprobados los requisitos académicos.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

PROYECTO FINAL DE CARRERA

Diseño del nuevo SCADA para el laboratorio de Tecnologías Avanzadas Digitales de Producción de UCLan mediante LabVIEW



Universidad Zaragoza



Dpto. de Informática e
Ingeniería de Sistemas
Universidad de Zaragoza



Escuela de
Ingeniería y Arquitectura
Universidad Zaragoza

Autor: Noel Pueyo Izquierdo

Director: Ramón Piedrafíta Moreno

Diciembre 2014



Índice

<u>1.- INTRODUCCIÓN.....</u>	<u>2</u>
<u>2.- CONTEXTO.....</u>	<u>4</u>
2.1 CENTRO PARA TECNOLOGÍAS DIGITALES AVANZADAS PARA PRODUCCIÓN (ADMT).....	4
2.2 TIM.....	6
<u>3.- OBJETIVO Y ALCANCE DEL PROYECTO.....</u>	<u>8</u>
3.1 SCADA.....	9
3.2 LABVIEW.....	12
3.3 ARQUITECTURA.....	16
3.4 PROTOCOLO DE COMUNICACIÓN.....	17
3.5 SERVIDOR OPC.....	18
<u>4.- COMUNICACIÓN CON LOS PLC.....</u>	<u>20</u>
4.1 PROTOCOLOS Y LIBRERÍAS.....	20
4.2 ELECCIÓN.....	23
<u>5.- ADQUISICIÓN DE LOS DATOS.....</u>	<u>24</u>
5.1 ENCAPSULADO DE DATOS.....	24
<u>6.- TERMINAL DE EXPLOTACIÓN.....</u>	<u>25</u>
6.1 DIRECTRICES PARA LA NUEVA INTERFAZ GRÁFICA.....	26
6.2 OPCIONES PARA LA NUEVA INTERFAZ.....	28
6.3 TIPO DE INTERFAZ SELECCIONADA.....	29
<u>7.- COMUNICACIÓN CON PROYECTOS NO INTEGRADOS.....</u>	<u>30</u>
7.1 FORMATOS DE COMUNICACIÓN.....	30

7.2 ELECCIÓN.....	32
<u>8.- VIDEO Y VISIÓN POR COMPUTADOR.....</u>	<u>33</u>
8.1 OPCIONES.....	34
8.2 ELECCIÓN.....	37
<u>9.- SEGURIDAD.....</u>	<u>38</u>
9.1 POR QUÉ TENERLA EN CUENTA.....	38
9.2 SOLUCIONES A LA SEGURIDAD.....	41
9.3 ALGORITMO DE CIFRADO.....	43
9.4 CIFRADO CON LABVIEW.....	44
9.5 HERRAMIENTA ELEGIDA.....	48
9.6 GESTIÓN DE USUARIOS.....	49
9.7 VIS PARA LA GESTIÓN DE USUARIO.....	52
9.8 SEGURIDAD EN TIM.....	52
9.9 SHODAN.....	54
<u>10.- OTRAS HERRAMIENTAS.....</u>	<u>55</u>
10.1 VIS UTILIZADOS.....	55
<u>11.- LICENCIA.....</u>	<u>56</u>
11.1 LICENCIAS DE LAS LIBRERÍAS USADAS.....	56
11.2 QUÉ ES SOFTWARE LIBRE.....	57
11.3 LICENCIAS LIBRES.....	57
11.4 LICENCIA ELEGIDA.....	60
<u>12.- PROGRAMACIÓN DEL TERMINAL DE EXPLOTACIÓN.....</u>	<u>61</u>
12.1 ESTRUCTURA DEL PROGRAMA.....	61
12.2 LIBRERÍA ETHERNET/IP.....	63
12.3 LIBRERÍA CON VLC.....	69
12.4 LIBRERÍA DE CONTROL DE ACCESO.....	74

12.5 PROGRAMA PRINCIPAL.....	88
12.6 VÍDEO.....	93
<u>13.- CONCLUSIONES.....</u>	<u>94</u>
13.1 ANÁLISIS DEL RESULTADO.....	94
13.2 TRABAJO FUTURO.....	94
<u>14.- BIBLIOGRAFÍA.....</u>	<u>101</u>
<u>15.- ANEXO A: LICENCIA COMPRADA.....</u>	<u>1</u>
<u>16.- ANEXO B: PROCEDIMIENTO DE TRABAJO.....</u>	<u>2</u>
16.1 UNIVERSIDAD DE CENTRAL LANCASHIRE.....	3
16.2 UNIVERSIDAD DE ZARAGOZA.....	4
<u>17.- ANEXO C: ETIQUETAS.....</u>	<u>1</u>
17.1 LOGIX5000.....	1
17.2 TAGS.....	2
17.3 TIPOS BÁSICOS DE DATOS.....	4
17.4 MATRICES.....	8
17.5 ESTRUCTURAS.....	8
17.6 DIFERENCIAS ENTRE ESTRUCTURA Y MATRIZ.....	9
<u>18.- ANEXO D: SEGURIDAD.....</u>	<u>1</u>
18.1 IMPACTO DE UN ATAQUE.....	3
18.2 RAZONES POR LAS QUE SUFRIR UN ATAQUE.....	4
18.3 DISEÑO DEL SISTEMA.....	5
18.4 SISTEMA EN PRODUCCIÓN.....	7
18.5 SISTEMAS DE CONTROL INDUSTRIAL.....	7
18.6 VULNERABILIDADES DE LA RED.....	9
18.7 TERMINAL DE EXPLOTACIÓN.....	11
18.8 ACTUALIZACIÓN DEL SOFTWARE.....	12

18.9 ACCESO REMOTO.....	13
18.10 OPERARIOS.....	14
18.11 CONTRASEÑAS.....	15
18.12 SEGURIDAD FÍSICA.....	17
 19.- ANEXO E: PRUEBAS DE USUARIO.....	1
19.1 PRUEBA 1: PRUEBA DE FUNCIONALIDADES DE ADMINISTRACIÓN.....	1
19.2 PRUEBA 2: PRUEBA 2ª DE FUNCIONALIDADES DE ADMINISTRACIÓN.....	6
 20.- ANEXO F: MANUAL DE USUARIO.....	1
21.1 INSTALACIÓN.....	7
21.2 CONFIGURACIÓN.....	7
21.3 TIPOS DE CUENTAS.....	8
21.4 SEGURIDAD DE LA CONTRASEÑA.....	8
21.5 LOG IN.....	9
21.6 PANTALLA PRINCIPAL.....	9
21.9 NUEVO USUARIO.....	13
21.8 CIERRE DE SESIÓN.....	12
21.10 ACCESO AL LOG.....	14
21.11 GESTIÓN DE USUARIOS.....	15
21.12 LICENCIAS.....	18

Resumen

En el presente proyecto se pretende dar solución a los problemas existentes en el ADMT (Centre for Advanced Digital Manufacturing Technologies) y en el proyecto TiM (Tele-immersive Digital Manufacturing) resultantes del incremento en complejidad de algunas de sus partes aunándolas en una nueva terminal de explotación, para ello se modificará su arquitectura SCADA y se rediseñará el terminal de explotación usando LabVIEW.

1.- Introducción

Debido al crecimiento de los proyectos en el Centre for Advanced Digital Manufacturing Technologies (ADMT) se requería un nuevo terminal de explotación para su plataforma Tele-inmersiva de fabricación electrónica (Tele-immersive Digital Manufacturing platform).

El SCADA ha de sustituir al actual, integrar y comunicarse con los proyectos existentes y permitir su escalabilidad para integrar proyectos futuros.

EL proyecto fue iniciado originalmente en el laboratorio del ADMT de la University of Central Lancashire situado en Burnley (Inglaterra) pero debido a diversos problemas tuvo que ser reconstruido y terminado en los laboratorios de la universidad de Zaragoza, este documento muestra los resultados finales obtenidos.

Motivación

Este proyecto surgió debido a mi interés por profundizar en mis conocimientos de LabVIEW y a que se me planteara la colaboración para solventar un problema real en el Centro para tecnologías digitales avanzadas para producción.

Agradecimientos

Al departamento ADMT de la universidad de central Lancashire por permitirme realizar mi proyecto con y para ellos, especialmente a Geoff Hall.

A ramón Piedrafita por tutorear mi proyecto.

A los amigos que hice durante mi estancia en UCLan, a mis amigos y compañeros de la carrera.

También quiero hacer mención a mi familia y a todos aquellos que me han ayudado en mayor o menor medida con este proyecto especialmente a Sandra por las horas de ayuda y apoyo y a Carla por su comprensión en los malos ratos que he tenido.

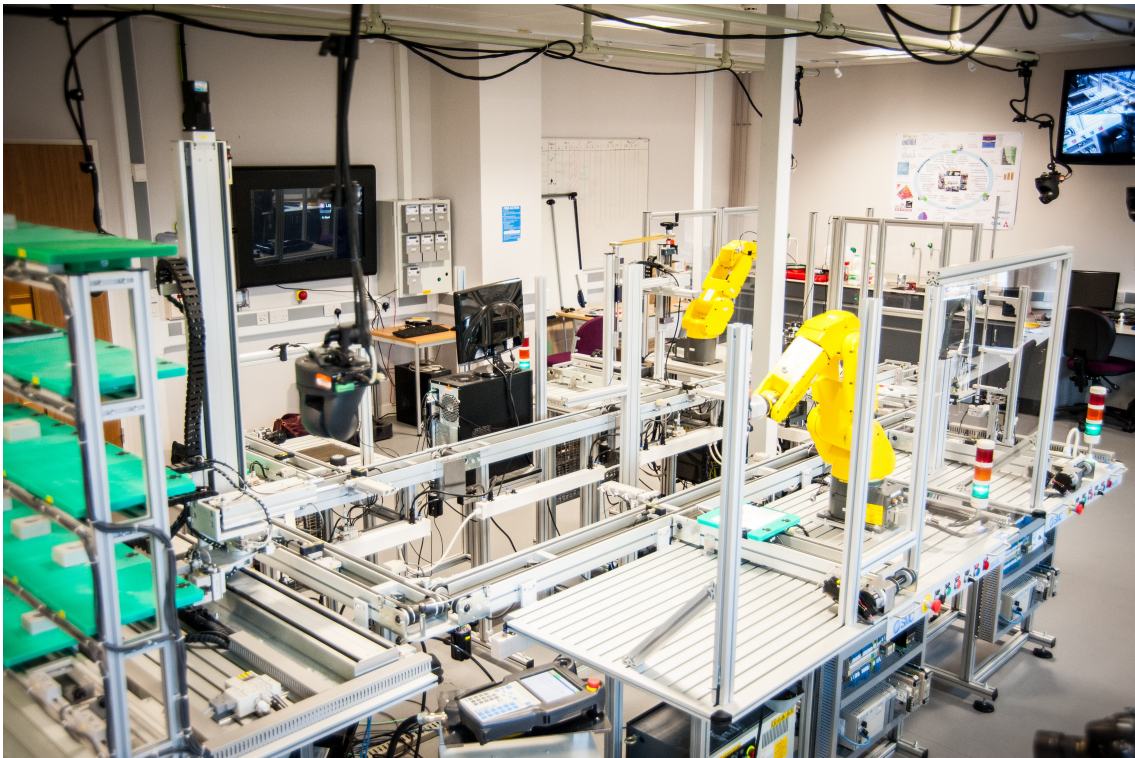
Licencia

Este documento se encuentra bajo licencia Creative Commons BY.



2.- Contexto

2.1 Centro para tecnologías digitales avanzadas para producción (ADMT)



1: Centre for Advanced Digital Manufacturing Technologies.

"ADMT trabaja en estrecha colaboración proveedores de tecnología puntera mundial y las industrias regionales en sistemas de ejecución de manufactura integrados con las TIC, enfocándose en la fabricación sistemas de ejecución de la producción controlados por los datos e integradas digitalmente y explotando su situación geográfica en una la de regiones manufactureras más grandes del mundo, ADMT ha desarrollado la primera plataforma de fabricación Digital Tele-inmersiva del mundo (TiM) y su visión de fabricas autónomas y baratas a través de los lazos con las empresas punteras aeronáutica, automovilística, alimentaria, energía nuclear y sector submarino de la región, habiendo atraído a varios proveedores de tecnología puntera mundial. En cuanto a la infraestructura de comunicación, TiM es el primer y único laboratorio en el sector de la educación que tiene la última versión del sistema de redes de alta disponibilidad con seguridad adaptativa proporcionada por Cisco; en términos de tecnología de la información, TiM se apoya en una amplia gama de tecnologías innovadoras en procesamiento de señales e imágenes, visión por ordenador 3D / 4D, así como visualización interactiva e inmersiva, que han sido desarrollados por ADSIP debido a las sinergias producidas en las investigaciones en los sectores aeroespacial y médico desde finales de 1990."

(ADMT, 2014)¹

¹ "ADMT WORKS CLOSELY WITH WORLD LEADING TECHNOLOGY PROVIDERS AND REGIONAL INDUSTRIES ON FUTURE ICT-ENABLED MANUFACTURING EXECUTION. BY FOCUSING ON DATA-DRIVEN DIGITAL-INTEGRATED MANUFACTURING EXECUTION AND EXPLOITING THE GEOGRAPHICAL POSITION IN ONE OF THE MOST IMPORTANT MANUFACTURING REGIONS IN THE WORLD, ADMT HAS DEVELOPED THE WORLD'S FIRST TELE-IMMERSIVE DIGITAL MANUFACTURING PLATFORM (TiM) AS ITS VISION FOR THE AFFORDABLE AND AUTONOMOUS FACTORY OF THE FUTURE THROUGH ITS CLOSE LINKS WITH THE REGIONAL PRIME MANUFACTURING COMPANIES IN AEROSPACE, AUTOMOTIVE, FOOD, NUCLEAR, AND SUBMARINE SECTORS, AND HAS BROUGHT IN VARIOUS WORLD LEADING TECHNOLOGY PROVIDERS. IN TERMS OF COMMUNICATION INFRASTRUCTURE, TiM IS THE FIRST AND THE ONLY LABORATORY IN THE EDUCATION SECTOR HAVING THE LATEST INDUSTRIAL FAULT-TOLERANT NETWORKING SYSTEM WITH ADAPTIVE SECURITY PROVIDED BY CISCO. IN TERMS OF INFORMATION TECHNOLOGY, TiM IS SUPPORTED BY AN EXTENSIVE RANGE OF INNOVATIVE TECHNOLOGIES IN SIGNAL AND IMAGE PROCESSING, 3D/4D COMPUTER VISION, AS WELL AS INTERACTIVE AND IMMERSIVE VISUALISATION, WHICH HAVE BEEN DEVELOPED BY ADSIP FROM SYNERGISTIC RESEARCH IN THE AEROSPACE AND MEDICAL SECTORS SINCE THE LATE 1990s." (ADMT, 2014)

2.2 TiM

El proyecto de producción tele-inmersiva tiene el objetivo final de disponer de una fábrica autónoma la cual podrá producir productos en función de la demanda del cliente, siendo el propio cliente el que envíe los diseños directamente a producción.

En la práctica el proyecto consta de una maqueta formada por 6 módulos y un almacén; en el almacén se guardan los diferentes palés que servirán de superficie para transportar el producto, cada pale contiene un sensor RFID que almacena los datos de la pieza.

Los palés pasan primero por el módulo de impresión donde la pieza diseñada es impresa mediante una impresora 3-D, después pasan por un robot donde mediante pruebas no destructivas se comprueba su integridad y la calidad de su acabado (el mismo robot cambia su herramienta para poder realizar ambas comprobaciones) finalmente pasa al último módulo donde se realiza una comprobación mediante visión por computador; durante la realización de este proyecto cambió la configuración de TiM y debido a su condición, es de suponer que seguirá cambiando en el futuro.

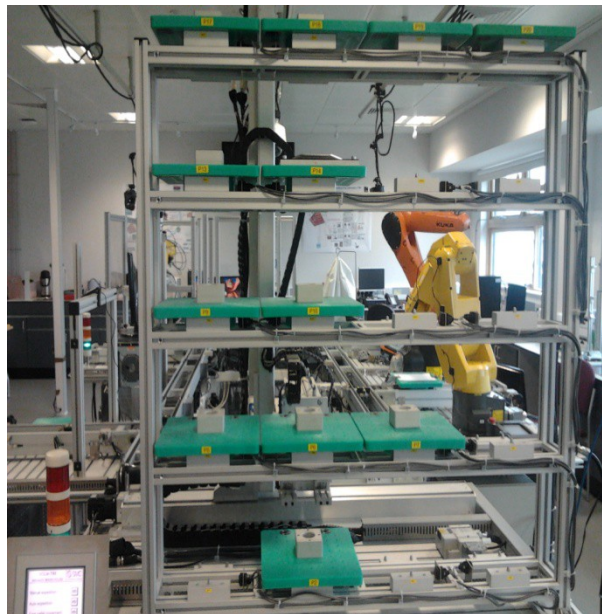
“La plataforma consiste en unas células de trabajo reconfigurables bajo demanda que están listos para funcionar nada más ser conectados, unidos a una cinta transportadora que transporta los componentes en palés de una célula a otra o usando robots industriales equipados con unidades de pick and place. Las células de trabajo incluyen a un almacén para el reparto del material y para el almacenaje de productos, una impresora 3D, láseres y ultrasonidos para la inspección de elementos y 2 robots que colaboran en el pre-ensamblado y ensamblado, Cada célula de trabajo puede ser programada, controlada y monitorizada remotamente en tiempo real a través de internet. Diferentes tecnologías de seguimiento, sensorización y monitorización se

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

integran para proporcionar un conjunto completo de los datos del proceso y la calidad del producto con su consumo de energía asociado.

Basándose en el éxito del desarrollo de TiM la investigación se extiende a la fabricación en la nube haciendo accesibles los centros de producción dispersos en la geografía para su pago por uso a través de internet, por cualquier persona, desde cualquier lugar y en cualquier momento.”

(ADMT, 2014)²



2: Célula de fabricación TiM

² “The platform consists of reconfigurable work cells which can plug and play in manufacturing, in different configurations on demand, by attaching to a conveyer system that transports components in pallets from one work cell to another or using mobile robots equipped with a pick and place unit. The work cells include automatic warehouse for material delivery and product storage, 3D printer for manufacturing, measurement systems based on camera, laser or ultrasound for component inspection, as well as collaborative robots for product pre-assembly and assembly. Each work cell can be programmed, controlled and monitored remotely in real time via internet. Various digital tracking, sensing and monitoring technologies are integrated to provide a comprehensive set of process and product quality data with associated energy consumption. Building on the successful development of TiM, the research is now extended to cloud manufacturing to make geographically dispersed manufacturing facilities accessible via the internet on a pay-per-use basis by anyone, anywhere and anytime.” (ADMT, 2014)

3.- Objetivo y alcance del proyecto

El objetivo de este proyecto es desarrollar un SCADA que sea útil para que un operador controle la información presente en el sistema de fabricación tele-inmersiva, también se pretende ahorrar gastos en licencias, integrar el control de otros proyectos en el terminal de explotación y la comunicación con aquellos que no puedan ser integrados.

Hay que destacar que previamente a la realización de este proyecto se intento rediseñar la arquitectura del SCADA para no tener la necesidad de usar un servidor OPC (es decir, accediendo directamente a los datos en la red Ethernet/IP), pero ese intento no tuvo frutos.

Se seguirán los siguientes pasos:

1. Analizar el sistema SCADA previo para no perder funcionalidades.
2. Desarrollar una nueva arquitectura SCADA.
3. Realizar un Nuevo terminal de explotación que reproduzca el anterior
4. Analizar qué proyectos del ADMT van a ser integrados dentro del terminal de explotación y cómo se comunicará con ellos.
5. Diseño y realización del nuevo terminal de explotación.

En el anexo B se detalla como se realizó este proyecto y alguno de los principales problemas durante el proceso de trabajo.

3.1 SCADA

“SCADA es la tecnología que permite al usuario comunicarse con una o más instalaciones para recoger o enviar información mediante un juego limitado de instrucciones”

(Boyer, 1999)³

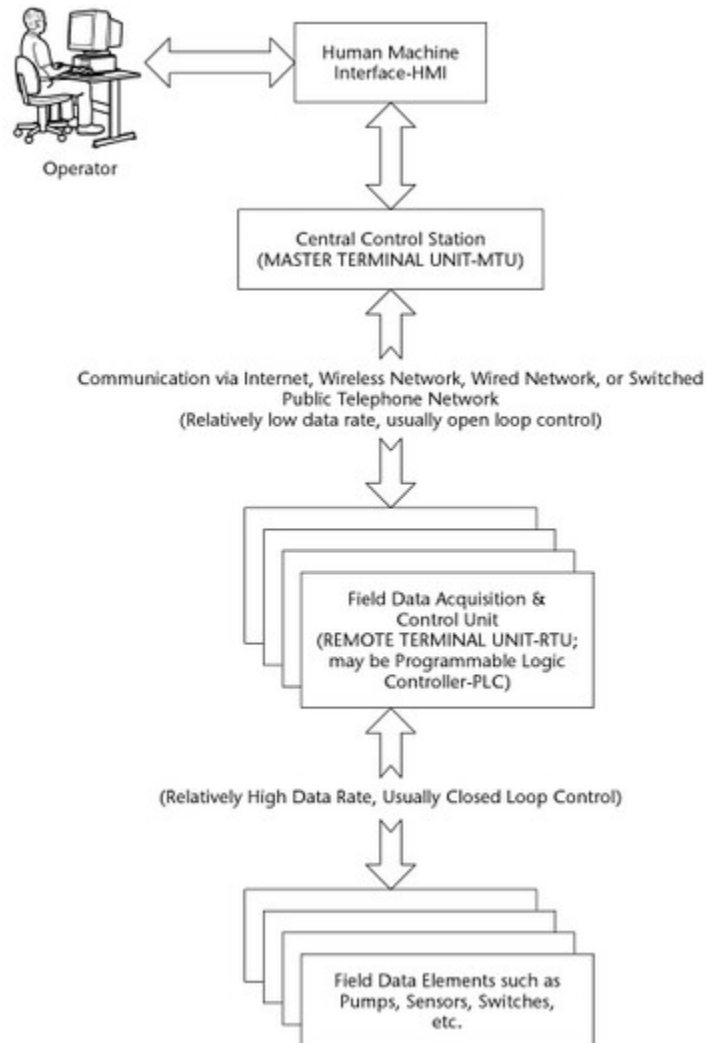
Un SCADA es definido mediante la arquitectura que interconecta al operario, al terminal de explotación (HMI), al maestro (MTU), al esclavo o esclavos (RTU), a los sensores de campo... y al sistema de comunicación usado para que se comuniquen entre ellos (ModBus, Ethernet/IP, AS-i...) .

“Una arquitectura SCADA es el compromiso Entre 2 niveles: el maestro o cliente de centro de control y supervisión y el esclavo o nivel de datos que interactúa con los procesos bajo control”

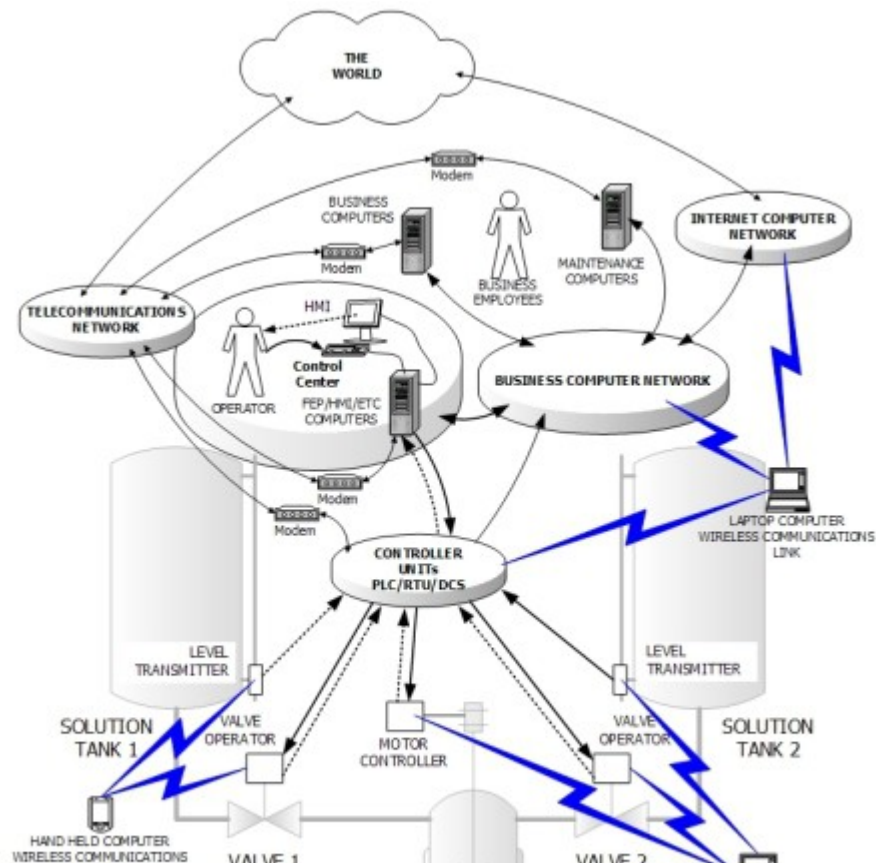
(Krutz, 2005)⁴

³ “SCADA IS THE TECHNOLOGY THAT ENABLES A USER TO COLLECT DATA FROM ONE OR MORE DISTANT FACILITIES AND/OR SEND LIMITED CONTROL INSTRUCTION TO THOSE FACILITIES.” (BOYER, 1999)

⁴ “A SCADA ARCHITECTURE COMPROMISES TWO LEVELS A MASTER OR CLIENT LEVEL AT THE SUPERVISORY CONTROL CENTRE AND A SLAVE OR DATA SERVER LEVEL THAT INTERACTS WITH THE PROCESSES UNDER CONTROL.” (KRUTZ, 2005)



3: Típica arquitectura de un sistema SCADA (Kruz, 2005)



4: Arquitectura SCADA real. Ejemplo del ICS-CERT del gobierno americano (ICS-CERT, s.f.)

3.2 *LabVIEW*

LabVIEW es un lenguaje de programación multiplataforma (Linux, Windows, OSX, Lego Mindstorm...) diseñado por National Instruments enfocado a la programación de instrumentos de medida virtuales.

Sus principales características son:

El lenguaje de programación usado en LabVIEW (también conocido como G) sigue el paradigma de programación por flujo de datos, el orden de ejecución es determinado por la posición de los bloques dentro del flujo de los datos a través de los hilo que los unen, ejecutándose en el momento en el que se reciben los datos, explotando por lo tanto la posibilidad de paralelizar procesos de la que disponen los nuevos microprocesadores pero da una falsa sensación de concurrencia cuando esto no es así, siendo ésta una de las críticas hacia este lenguaje.

El diseño de la interfaz gráfica está incluido dentro del ciclo de programación del programa siendo las variables de entrada de los instrumentos virtuales los controles de la interfaz y las salidas los indicadores, facilitando así el encapsulado del instrumento programado, puesto que los controles e indicadores pueden ser usados para introducir datos desde VIs en un nivel superior; todo ello facilita el uso de LabVIEW a aquellos que no se habían aproximado previamente a la programación e impidiendo en gran medida la realización de malas prácticas (siguiendo el hilo, se comprueba visualmente el origen de los datos, y visualmente también se comprueba el tipo de dato tanto existente como necesario).

Dispone de un muy buen soporte para acceder a hardware comercial y a protocolos de comunicación mediante drivers, ofreciendo una capa de abstracción que permite el realizar programas algo complejos sin necesidad de conocerlo en profundidad o la realización de programas en un menor espacio de tiempo con el consecuente ahorro

en dinero y personal; también ofrece una interfaz para comunicarse con el framework .NET de Microsoft.

El software generado con LabVIEW es compilado y ejecutado por el motor de tiempo de ejecución de LabVIEW, lo que le facilita el ser multiplataforma a cambio de generar ejecutables más pesados y más lentos y por lo tanto necesitando una máquina con mayores prestaciones que la necesaria para hacer funcionar otros sistemas.

También incluye un lenguaje de texto similar a MatLab llamado MathScript pero menos potente.

-Es un lenguaje propietario que no es administrado por un comité de estandarización como ANSI, IEEE o ISO.

-No existe licencia para estudiantes en plataformas Linux (aunque sí licencia profesional).

NI lanza al mercado periódicamente nuevas versiones, actualizaciones, toolkits y librerías, además, la comunidad de usuarios (LAVA.com principalmente o en los foros oficiales de LabVIEW) es muy activa publicando tanto bajo licencias libres (BSD, MIT, LGPL) como sin ellas; existen también compañías dedicadas a realizar librerías y toolkits que extienden las posibilidades de LabVIEW donde NI no llega.

3.2.1 Programación con LabVIEW y otros lenguajes

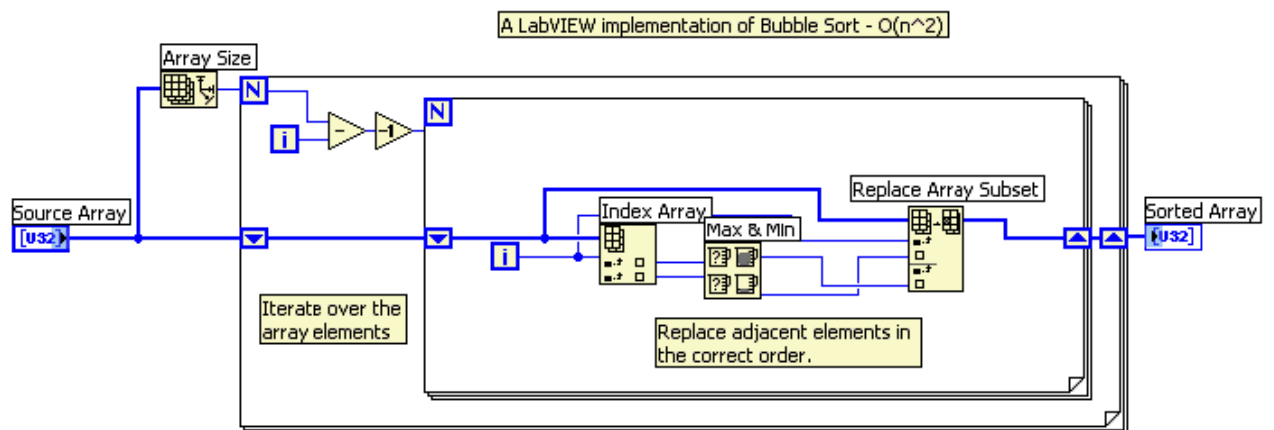
A continuación se presentan varios ejemplos de comparación e interacción de LabVIEW, C, fórmulas matemáticas y librerías dinámicas (NI.com, 2010).

Algoritmo de burbuja para ordenar valores en un vector en C y en LabVIEW, como se puede observar el flujo de los datos puede seguirse más fácilmente en el diagrama de LabVIEW para un inexperto en ambos lenguajes.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

```
void bubbleSort(int *array)
{
    int holder, x, y;
    for(x = 0; x < ARRAYSIZE; x++)
    {
        for(y = 0; y < ARRAYSIZE-1-x; y++)
        {
            if(array[y] > array[y+1])
            {
                holder = array[y+1];
                array[y+1] = array[y];
                array[y] = holder;
            }
        }
    }
}
```

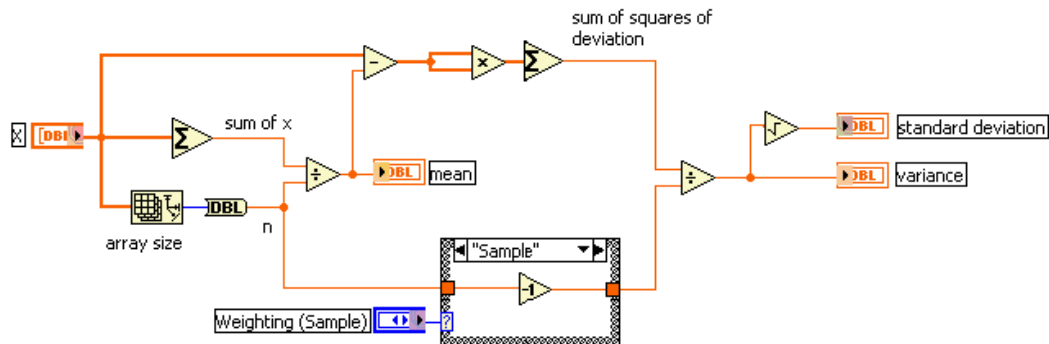
5: Ordenamiento de burbuja en C (NI.com, 2010)



6: Ordenamiento de burbuja en LabVIEW (NI.com, 2010)

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

La transposición de algoritmos matemáticos a LabVIEW es más fácil y entendible.



$$\sigma = \sqrt{\frac{\sum (x_i - \mu)^2}{n}}$$

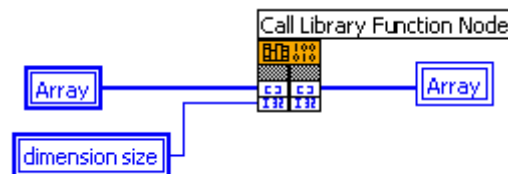
Population standard deviation

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n - 1}}$$

Sample standard deviation

7: Desviación estándar y varianza en LabVIEW y en formato matemático (NI.com, 2010)

De todas formas, se pueden realizar llamadas a funciones dentro de una librería dinámica (DLL) realizadas en otros lenguajes.



8: Código LabVIEW que llama a una función dentro de una DLL (NI.com, 2010)

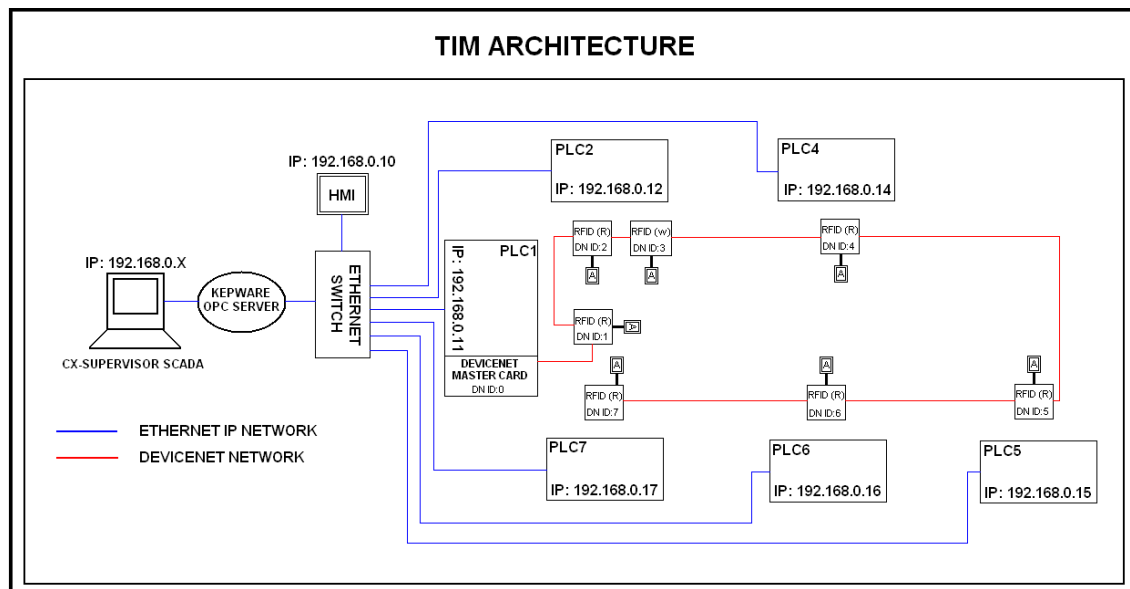
```
void __declspec(dllexport) generateRand(int *iArray, int ARRAYSIZE)
{
    long int i, sTime;
    time(&sTime); // gets time to seed the random number
    srand(sTime*100); // seeds each random from an offset of the time
    for (i=0; i<ARRAYSIZE; i++)
    {
        iArray[i]=rand()*100/RAND_MAX; // inserts the random number into the array
    }
}
```

9: Código C de la función GenerateRand() (NI.com, 2010)

1.- Análisis del SCADA previo y especificaciones

3.3 Arquitectura

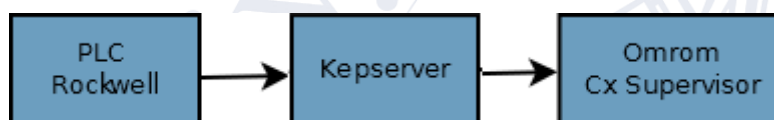
La arquitectura SCADA previa al proyecto era tal y como se muestra en la imagen.



10: Arquitectura de TiM

Había un sistema provisto por Omrom (el Omrom Cx supervisor) que era usado mediante un terminal de explotación en una pantalla LCD para controlar las salidas y la entradas de las estaciones de trabajo de la planta de producción.

Este terminal de explotación no disponía de ningún medio para comunicarse con otros proyectos del laboratorio ni para integrarlos, además de necesitar un servidor OPC en un ordenador del laboratorio.



11: Conexión con los PLC por el SCADA Omrom usando el servidor OPC

El principal problema existente para querer eliminar el servidor OPC de la arquitectura SCADA es su precio excesivo, teniendo en cuenta que uno de los objetivos de TiM es ser de bajo coste.

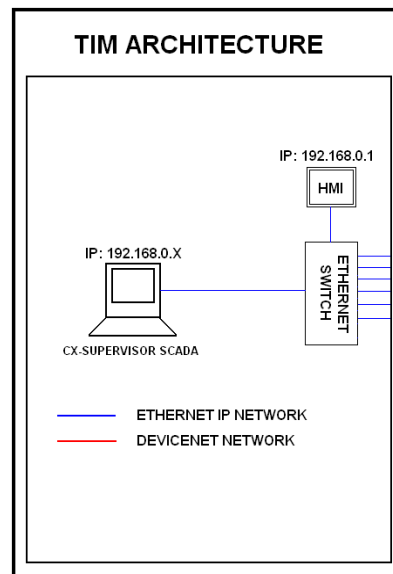
3.4 *Protocolo de comunicación*

Los PLC existentes en el laboratorio eran 2 modelos (L23E y L32E) de la serie CompacLogix de Rockwell, ambos comunicados con el servidor OPC mediante Ethernet/IP.

EtherNet/IP es un protocolo de comunicación creado por Rockwell Automation cuyos derechos están administrados por la Open DeviceNet Vendors Association; fue diseñado para usarse en procesos de control y automatizaciones industriales sobre la capa física del protocolo Ethernet.

3.5 Servidor OPC

El servidor OPC es el que accede a los tags (etiquetas que almacenan una copia de los



12: Cambios realizados a la arquitectura TiM original

datos que el autómata tiene actualmente en memoria) del PLC para que posteriormente el terminal de explotación pueda consultarlos y modificarlos.

Se sugirió una conexión directa entre el terminal de explotación y los PLCs para la nueva arquitectura y así prescindir de los gastos en licencias que un servidor OPC acarrea, para ello será necesario encontrar un medio (toolkit, librería, herramienta...) que nos permita comunicarnos mediante Ethernet/IP.



13: Arquitectura deseable en la conexión entre el PLC y el SCADA

Otra opción que fue valorada es el conseguir un servidor OPC fiable y sin costes de licencias, bien por ser software libre, de código abierto o simplemente gratuito.

Aunque los servidores OPC son caros hay unos pocos servidores OPC de código abierto pero ninguno de los revisados soporta diferentes marcas de autómatas como sí hace el actual (ni la serie de autómatas de la que disponemos), ni los que son software gratuito (descontando los que son de uso limitado), ni los libres o de código abierto; otros, que podrían haber cumplido los criterios, fueron discontinuados, como LightOPC⁵, o están enfocados a su uso por un lenguaje de programación concreto (OpenOPC⁶ para Python); LabVIEW podría comunicarse mediante datasockets (NI.com, 2013) a un servidor OPC (siempre y cuando se haya comprado esa parte del sistema).

Otro problema de los servidores OPC es que no son firewall-friendly, lo que implica que las reglas del cortafuego no pueden ser configuradas en detalle tal y como se dice en “Implementar una arquitectura segura” (CCN-STIC-480C) (Centro Criptológico Nacional, 2010).

⁵ <http://www.ipi.ac.ru/lab43/lopc-en.html>

⁶ <http://openopc.sourceforge.net>

4.- Comunicación con los PLC

Dado que el uso de un servidor OPC ha sido descartado debido a su precio, se ha buscado otros medios de acceder a la red Ethernet/IP o valorar el uso de otros protocolos de comunicación como ModBus.

4.1 *Protocolos y librerías*

4.1.1 MODBUS Library Para LabVIEW (NI.com, 2012)

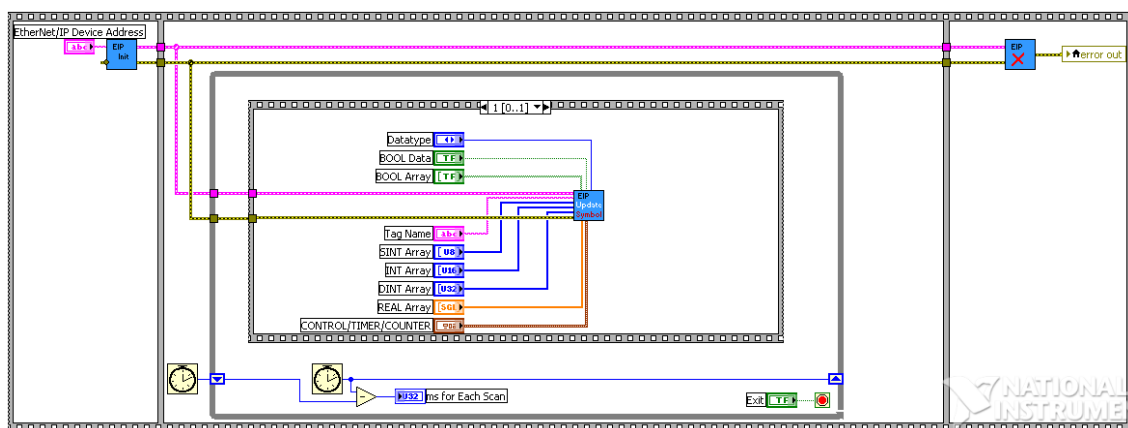
Desarrollada por NI, es una librería ofrecida de manera gratuita por National Instruments, algo compleja de utilizar y no actualizada a las últimas revisiones del protocolo MODBUS

4.1.2 GModBus Over TCP Toolkit (SAPHIR, s.f.)

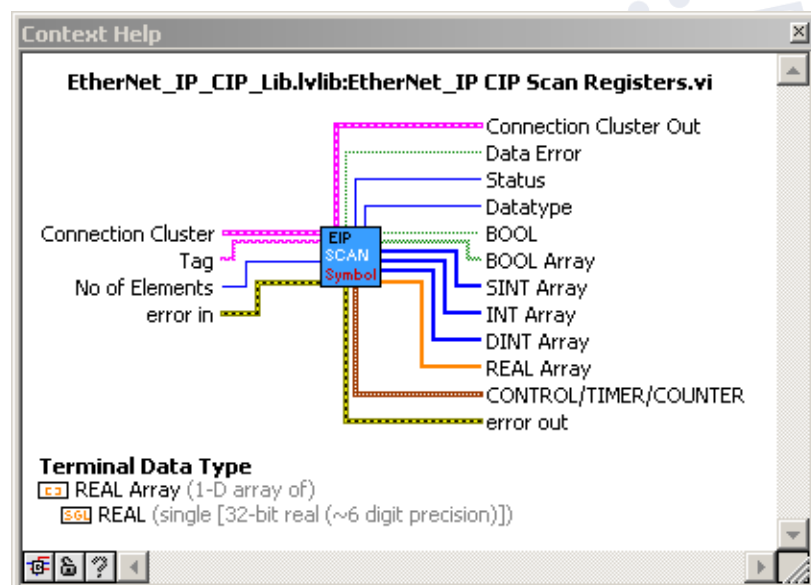
Desarrollada por SAPHIR, es la alternativa que apareció cuando la otra librería se quedó desactualizada, siendo además de pago y no mejorando la usabilidad.

4.1.3 EtherNet_IP_CIP (Siva, 2012)

Desarrollada por Siva (Usuario de los foros LAVA), más fácil de utilizar que las librerías para comunicarse por MODBUS y puede comunicarse con los autómatas existentes sin tener que cambiar de protocolo de red.



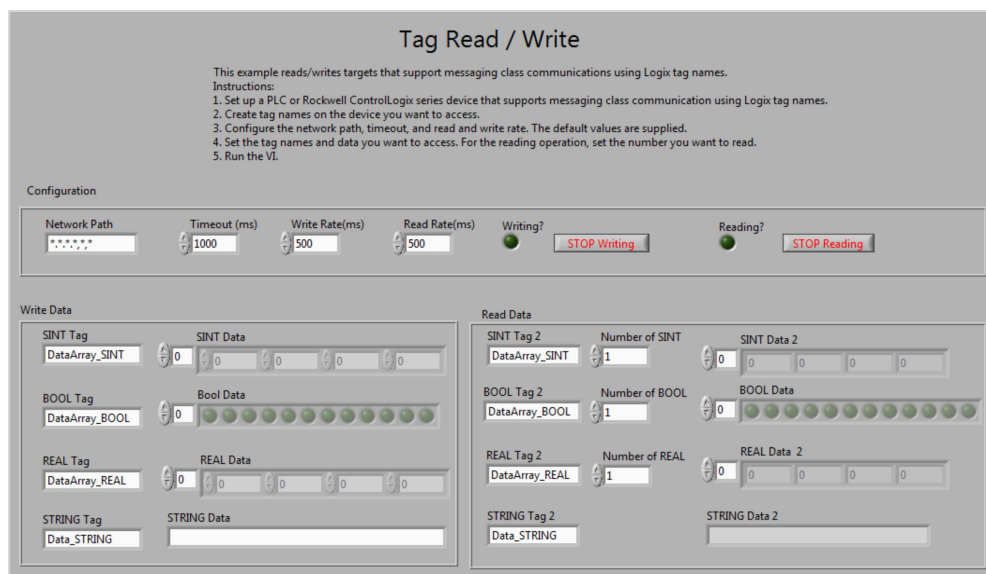
14: Diagrama de bloques de la lectura de datos de una red Ethernet/IP mediante EtherNet_IP_CIP



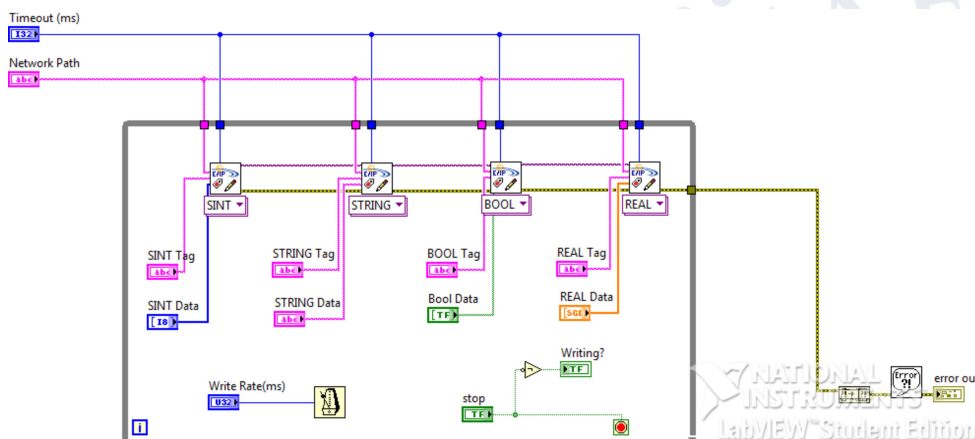
15: VI de lectura de datos mediante EtherNet_IP_CIP

4.1.4 NI-Industrial Communications para EtherNet/IP 1.2.1 (NI.com, 2014)

Similar al EtherNet_IP_CIP pero desarrollada por National Instruments y siendo de pago; es más simple de usar que EtherNet_IP_CIP.



16: Panel frontal de la lectura/escritura de datos en Ethernet/IP



17 : Diagrama de bloques de la lectura/escritura de datos en Ethernet/IP

4.2 Elección

Pese a los problemas de usabilidad existentes se eligió EtherNet IP CIP como librería a usar en el proyecto para la comunicación con los PLC.

5.- Adquisición de los datos

En el apéndice sobre los tags están las conclusiones obtenidas tras ahondar en la programación de los autómatas CompactLogix5000, ya que cuando se fue a afrontar la adquisición de los datos existentes en los tags del sistema emergió la falta de documentación, su mala calidad y que el sistema no funcionaba correctamente, pudiendo acceder sólo a uno de los huecos del almacén -porque en el resto se iniciaba un mal funcionamiento del sistema- y no realizando las lecturas y escrituras a las etiquetas RFID amén de otras faltas.

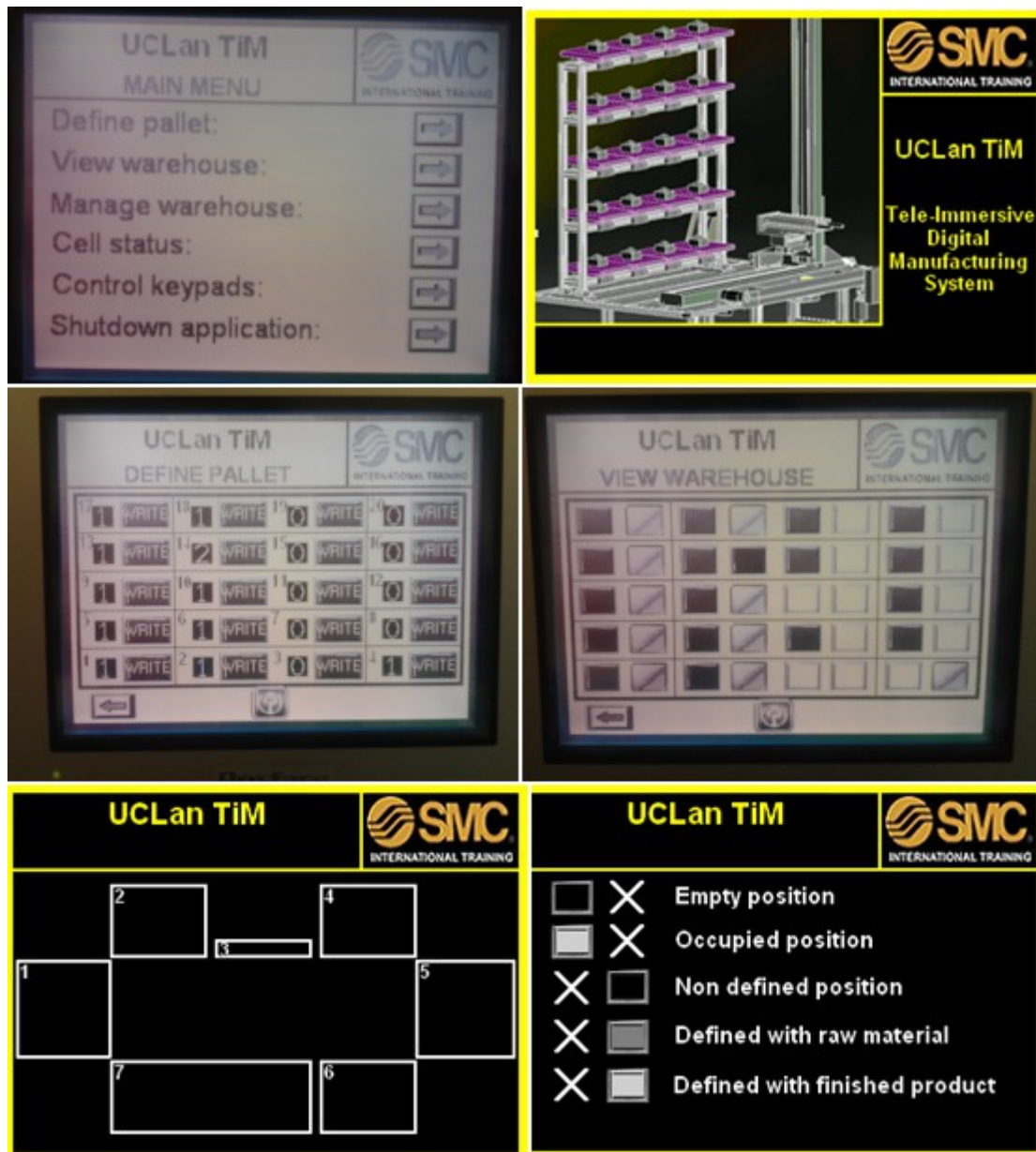
Por ello se decidió simplemente acceder a aquellos datos suficientemente bien documentados, posteriormente, en Zaragoza, se decidió afrontar su escritura, puesto que no se trabajaría con un sistema en producción.

5.1 Encapsulado de datos

El uso de las técnicas de programación recomendadas por Rockwell lleva a que en vez de utilizar una vector/Array de datos booleanos se encapsularon éstos en un dato de tipo doble entero, lo que obliga a su extracción para realizar un tratamiento individual.

6.- Terminal de explotación

Las siguientes imágenes corresponde al terminal de explotación existente, la adecuación de su interfaz gráfica será analizada tras una revisión de las directrices recomendadas a la hora de diseñar interfaces gráficas para la industria.



18: Fotos y pantallas de la interfaz de TiM

6.1 *Directrices para la nueva interfaz gráfica*

La interfaz gráfica (GUI de su acrónimo en inglés, Graphical User interface) es una de las partes más importantes de un proyecto con terminal de explotación debido a que va a ser el medio por el cual el operario va a interactuar con el sistema, es un apartado que suele ser poco cuidado pero en el cual nos hemos querido detener para darle la importancia que creemos que requiere.

Según “The LabVIEW Style Book” (Blume, 2007) las interfaces gráficas para aplicaciones industriales tienen diferencias con respecto a las realizadas para otros entornos; algunas de las recomendaciones realizadas por dicho libro son:

- Uso de botones con estilo 3D para mejorar su visibilidad y accesibilidad -en inglés affordability-, es decir que el usuario sepa que puede interactuar con el objeto.
- Fácilmente visible desde media distancia.
- Información centrada
- Uso de pestañas.
- Limitar el número de controles que son visible al mismo tiempo.
- Minimizar la cantidad de texto en las pantallas.
- La información importante ha de aparecer en tamaño grande y en negrita.
- Para los encabezados texto plano a gran tamaño.
- El resto de textos y los objetos a tamaño grande y sin efectos visuales.
- Colores con alto contraste entre ellos par las cosas importantes (Alarmas, advertencias...).

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

- Usar sólo 3 estilos
 1. Estándar: para la mayor parte de los textos.
 2. Grande o en negrita: para los datos importantes o críticos y los controles.
 3. Estilo de alto contraste para los títulos o encabezados.
- Incluir el logotipo de la compañía.

Al diseñar la GUI también se ha de tener en cuenta a la gente con problemas de visión como los daltónicos (10% de la población), para ello se recomienda el uso de solo 3 colores complementarios, colores apagados y uno de la escala de grises.

6.2 Opciones para la nueva interfaz

A la hora de afrontar el diseño de la nueva interfaz nos encontramos con 3 posibles diseños.

- Recrear la GUI existentes en LabVIEW:

La interfaz previa cumple la mayoría de las directrices, rompiéndola solo debido a sus limitaciones técnicas (pantalla en escala de grises y de reducido tamaño) y a causas menores que son mejorables; esto tendría grandes ventajas para los operarios puesto que el cambio no les supondría mucho aprendizaje pero se perdería el potencial que ofrece una pantalla como la de un ordenador que es más grande y que tiene más que la escala de grises; y encorsetaría el añadido de las nuevas funcionalidades que son requeridas.

- Diseñar una nueva interfaz:

Siguiendo las directrices e incluyendo de forma más amigable las opciones que el resto de proyectos tengan, como contra tiene el hecho de que costará más a los operarios acostumbrarse a ella, por lo tanto requeriría la realización de pruebas de usabilidad con ellos.

- Zoom semántico:

Durante el diseño de los requerimientos del proyecto se me pidió considerar el uso del zoom semántico a la hora de diseñar la nueva interfaz; el zoom semántico (también

llamado ZUI de Zoomable User interface) consiste en que el sistema mostrará la información al usuario en función de lo que haya estado viendo previamente.

Este tipo de interfaces van en contra de los principios antes expuestos puesto que pueden llevar a confusión al operario del sistema al ofrecerle diferente información aun habiendo realizado los mismos pasos que otras veces (Blume, 2007).

6.3 *Tipo de interfaz seleccionada*

Se implementará una interfaz nueva.

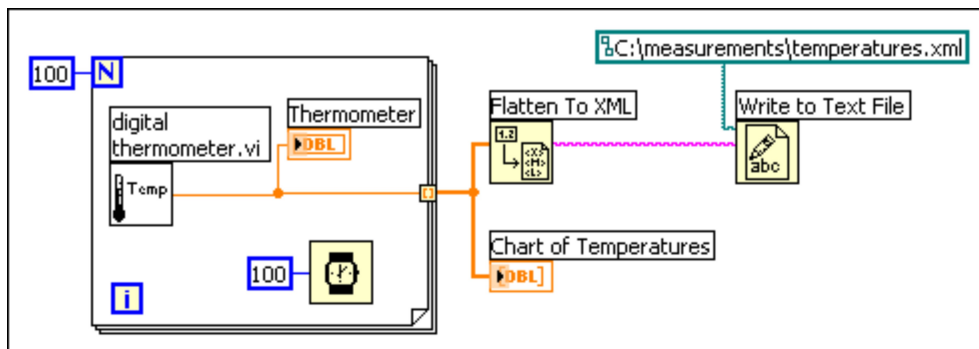
7.- Comunicación con proyectos no integrados

En el laboratorio del ADMT los proyectos se comunican entre ellos haciendo uso de archivos JSON aunque también es posible haciendo uso de archivos XML ya que su conversión a JSON se puede realizar fácilmente.

7.1 Formatos de comunicación

7.1.1 XML

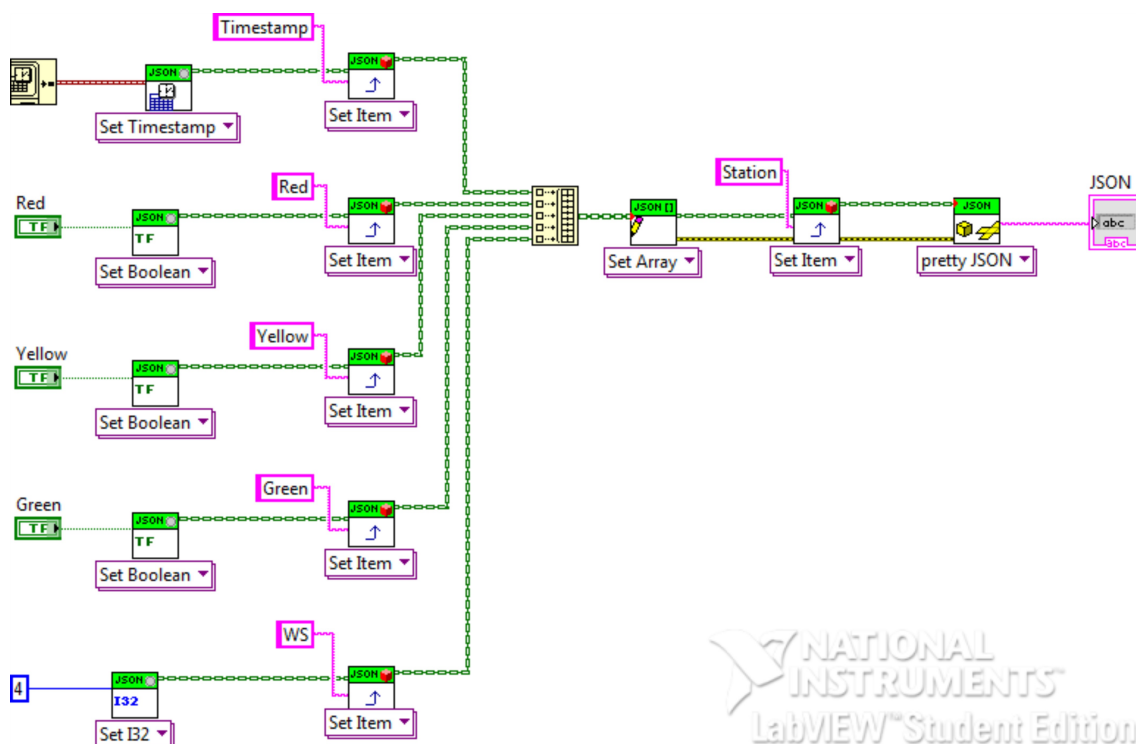
La conversión a XML de los datos adquiridos se realiza de forma nativa por LabVIEW.



19: Función nativa en LabVIEW que guarda una cadena en formato XML (NI.com, 2012)

7.1.2 I3 JSON Toolkit (i3 JSON, 2012)

, Interactive Internet Interface: JSON Toolkit for LabVIEW, Desarrollada por un equipo de usuarios de LabVIEW (Rohama_K, MilanRet AI) bajo el nombre Interactive Internet Interface, está disponible de manera gratuita en la comunidad decibel NI, disponible solo para LabVIEW 2012 o superior y necesita el gestor de paquetes JKI.



20: Escritura de datos en un fichero JSON

7.2 Elección

El ADMT dispone de LabVIEW 2010 y por lo tanto no podría utilizarlo, pero se está planeando actualizar en un futuro cercano la versión disponible, esto unido al hecho de que la comunicación mediante archivos JSON era un requisito recomendado hace que i3 JSON toolkit sea la herramienta seleccionada.

8.- Video y visión por computador

Una de las características deseadas para el TiM es que sea controlado y administrado sin estar presentes en la planta, para ello disponen de webcams Ethernet para controlar el recinto.

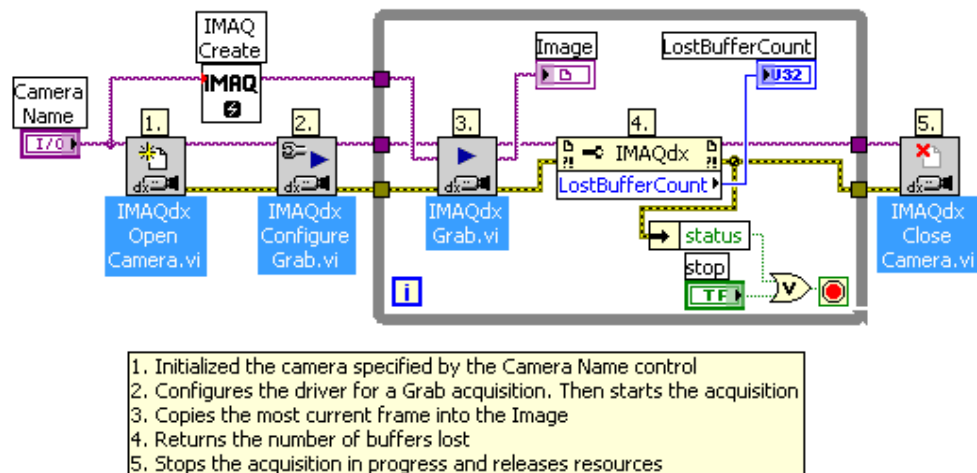
El control de la calidad de la producción se realiza mediante visión por computador, actualmente este control no está integrado en la célula de fabricación pero se desea que lo esté, así como que se pueda realizar un control visual por parte del operario.

Para solventar ambos problemas se desea integrar un módulo para adquirir las imágenes de video y en un futuro el control de las cámaras de vigilancia.

NI y otros proveedores de hardware incluyen drivers para controlar su hardware, pero implica el seguir usándolo en caso de sustitución y actualización, además de que, excepto que sea hardware de NI, el hardware no sea accesible mediante instrumentos Virtuales.

8.1 Opciones

8.1.1 NI-IMAQdx driver (NI.com, s.f.)

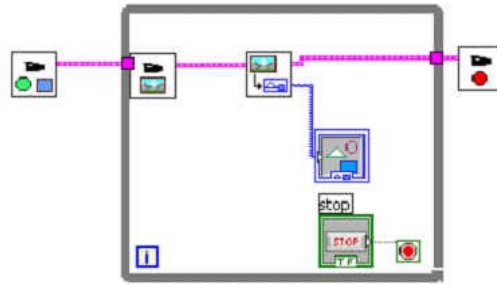


21: Ejemplo con NI-IMAQdx

Incluido en el paquete de adquisición de imágenes de NI llamado NI-IMAQdx es la solución proporcionada por National Instruments para cámaras que cumplan en estándar IEEE 1394, su principal problema es el precio, siendo la mejor opción disponible si no tuviéramos restricciones presupuestarias.

8.1.2 ROBOLAB (CEEQ, 2013)

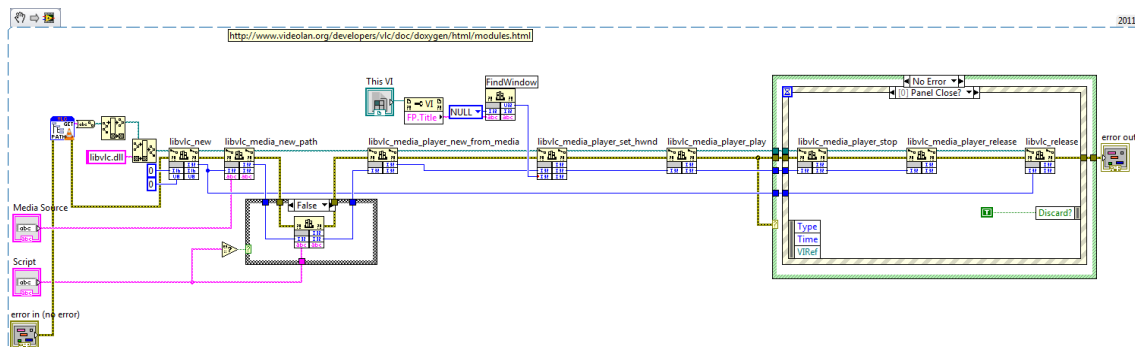
Es la extensión para LabVIEW utilizada en la plataforma LEGO MINDSTORMS aunque disponible también para LabVIEW, es gratuita pero requiere Quick Time Media Player.



22: Ejemplo con Robolab

8.1.3 VideoLAN (VLC, s.f.)

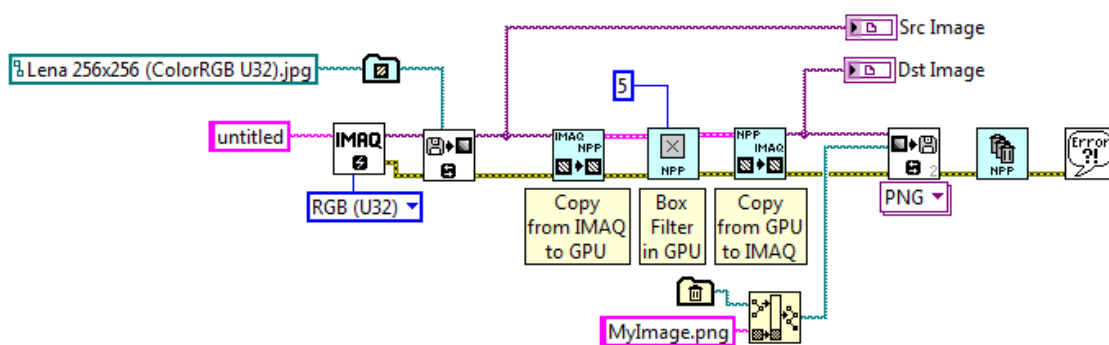
Dado que las cámaras de vigilancia actualmente controlan mediante VLC se sugirió intentar usarlas para adquirir las imágenes; basándonos en ejemplos hospedados en Decibe.ni.com (GriffinRU, 2012) y (ShaneDonn, 2013) se puede programar un driver para gestionar la adquisición de imágenes, esto implicaría un trabajo mayor y a más bajo nivel.



23: Ejemplo con las DLL de VLC (GriffinRU, 2012)

8.1.4 AD Vision Toolkit (Dmitriev, 2010)

ADV es un toolkit desarrollado por Andrey Dmitriev basado en la tecnología de tarjetas gráficas CUDA de N-VIDIA, pese a ser una buena opción exige que el hardware permita utilizarla, cosa no siempre posible y que podría dar problemas en un futuro al poder quedarse obsoleta CUDA.



24: Ejemplo con AD Vision Toolkit

8.1.5 OpenCV

OpenCV⁷ es una biblioteca libre de visión artificial originalmente desarrollada por Intel.

Contiene más de 500 funciones desde reconocimiento de objetos (incluido el reconocimiento facial), calibración de cámaras, visión estereoscópica. Existen wrappers de pago como (Eran Herman Engineering, 2013), (XIMEA Corp., s.f.) o (HYtek Automation, s.f.) o gratuitos (canming, 2014) y (Klemen, 2014) además de múltiples ayudas y ejemplos (Klemen, 2014), (Sabtu, 2010), (daarwin, 2013) o (Fernando, 2011).

⁷ <http://opencv.org>

8.2 Elección

Las 2 principales opciones tenidas en cuenta fueron el acceso mediante las librerías de VLC y el uso de Robolab; se tuvo también en cuenta Open CV debido a que la visión por computador es utilizada en otros proyectos relacionados con TiM pero se dejó para líneas futuras de investigación, primando el tener algo funcional que posteriormente se iría ampliando.

- Programar con Robolab es más fácil que realizar llamadas a las DLLs de VLC, pero esto se puede mejorar realizando una librería de VIS que hagan uso de VLC al igual que
- El uso de las DLLs de VLC implica el aprender cosas nuevas de LabVIEW
- Robolab está listo para ser usado cuando se instala mientras que VLC será una herramienta para programar unos Vis para conectar la cámara a LabVIEW.
- VLC se usa actualmente en otros proyectos del ADMT siendo utilizado para ver las cámaras web.
- VLC está disponible en versión portable, permitiendo el uso de la librería sin tener que tener privilegios de administrador para su instalación.

Bajo estos puntos se decidió usar las DLL de VLC para la comunicación con las cámaras web.

9.- Seguridad

9.1 Por qué tenerla en cuenta

"Los sistemas SCADA (Supervisory Control and Data Acquisition) se utilizan en redes de control de equipamiento en procesos industriales para monitorizar y controlar infraestructuras importantes tales como plantas de generación de energía, redes de transmisión eléctrica, control de aguas, refinerías, oleoductos o gaseoductos, además de sistemas de transporte y comunicaciones. Basta con echar un vistazo a la lista anterior para darnos cuenta de la importancia que pueden tener."

(Morant, 2013), coordinador técnico del CSIRT-CV.

"Los propietarios y gestores de los sistemas de control industrial tienen gran experiencia en el establecimiento y desarrollo de medidas de seguridad física, medio ambiental, de prevención laboral, lo cual, indudablemente ha salvado muchas vidas y protegido a las instalaciones industriales de ataques físicos (que requieren presencia física). Sin embargo, desde un punto de vista lógico, la gran mayoría de los sistemas de control industriales son vulnerables (malware, botnets, DDoS). Esto supone un cambio de tendencia importante ya que debido a la integración de las redes de control con las corporativas, hoy en día, los ataques ya no requieren presencia física en las instalaciones y pueden ser realizados de manera remota a través de redes públicas."

Mapa de Ruta de la Ciberseguridad Industrial en España 2013 – 2013 (Centro de Ciberseguridad Industrial, 2012)

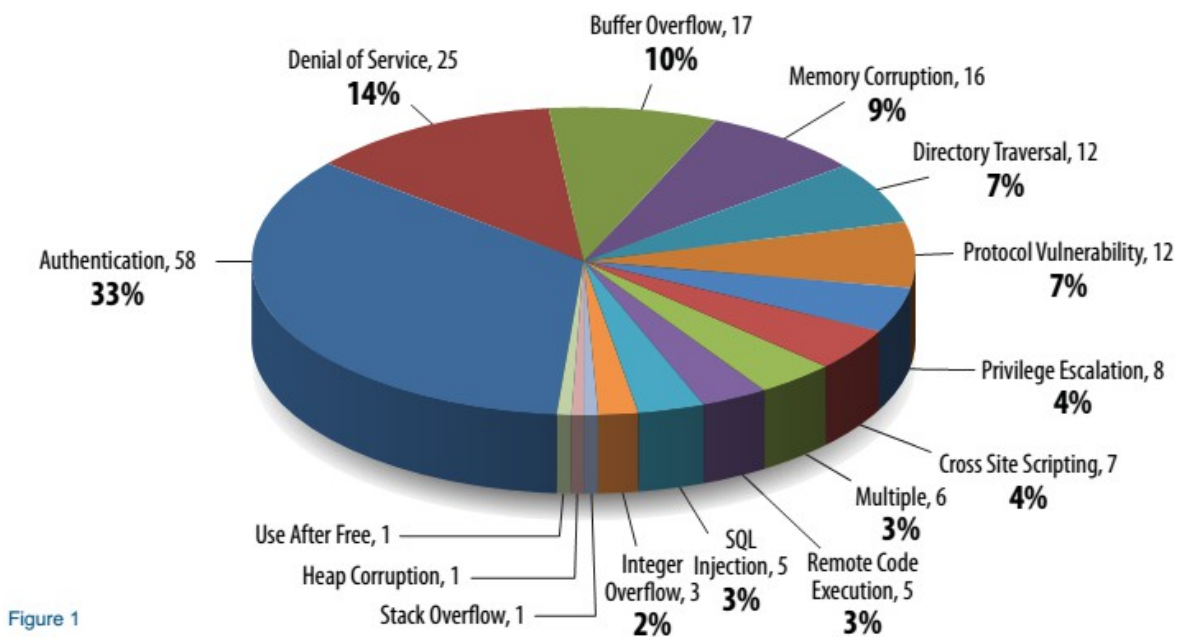
Durante los últimos años diversas incidencias relacionadas con la seguridad en los sistemas industriales han saltado a la prensa generalista; entre los caso más relevante encontramos: el gusano Stuxnet (Paone, 2010) (Symantec, 2010) (que ataca directamente a entornos de producción en plataformas Siemens; los primeros ataques fueron sufridos por plantas iraníes relacionadas con sus investigaciones nucleares, modificaciones posteriores, como Duqu (Kaspersky Lab , 2011) (El País, 2011), han atacado sistemas en otros países), la campaña de ataques denominada Dragonfly (Security ledger, 2014) (Symantec Security Response, 2014) (sistemas de más de 1000 empresas en 80 países mediante un malware llamado Havex (ICS-CERT, 2014) sufriendo España uno de cada cuatro ataques producidos), la Operación Aurora (también conocida como Comele o HydrAq) realizada, entre otros, por el grupo de origen chino llamado Hidden Lynx group tras haber troyanizado unos binarios de la empresa Bit9 (Symantec, 2013) (Symantec, 2010) y el fallo de la bomba de agua en Illinois debido a una intrusión que causó que el sistema SCADA se apagase y que la bomba de agua se quemase (ICS-CERT, 2011); sin olvidar uno de los primeros y más notables, el gusano Slammer (F-Secure, 2003) que provocó el apagado de la central nuclear de Davis-Besse (SecurityFocus, 2003).

“ICS-CERT recibió 181 informes de vulnerabilidad por parte de investigadores y de proveedores de sistemas de control durante todo el año. De ellos, 177 se determinó que eran verdaderas vulnerabilidades que involucraron coordinación, pruebas y análisis por parte de 52 proveedores. La mayoría de ellos, o el 87 por ciento eran explotables de forma remota mientras que el otro 13 por ciento requerían acceso en local necesaria para explotar las vulnerabilidades.”.

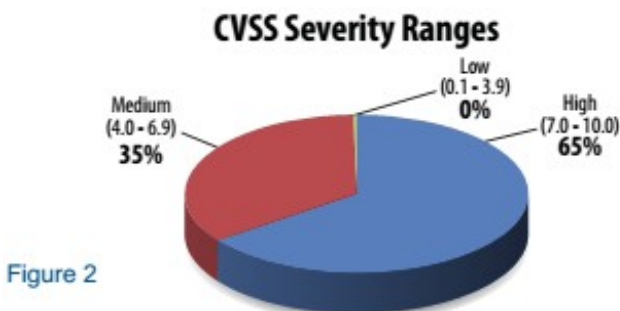
(National Cybersecurity and Communication Integration Center, 2014)⁸

⁸ “ICS-CERT RECEIVED 181 VULNERABILITY REPORTS FROM RESEARCHERS AND ICS VENDORS THROUGHOUT THE YEAR. OF THOSE, 177 WERE DETERMINED TO BE TRUE VULNERABILITIES THAT INVOLVED COORDINATION, TESTING, AND ANALYSIS ACROSS 52 VENDORS. THE MAJORITY OF THESE OR 87 PERCENT WERE EXPLOITABLE REMOTELY WHILE THE OTHER 13 PERCENT REQUIRED LOCAL ACCESS TO EXPLOIT THE VULNERABILITIES.” (NATIONAL CYBERSECURITY AND COMUNICATION INTEGRATION CENTER, 2014)

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan



25: Distribución de las vulnerabilidades reportadas al ICS-CERT en 2013 (National Cybersecurity and Communication Integration Center, 2014)



26: Gravedad de las vulnerabilidades reportadas al ICS-CERT en 2013 (National Cybersecurity and Communication Integration Center, 2014)

Esto nos debería llevar a plantear una estrategia integral de seguridad para el SCADA pero dicha estrategia se sitúa fuera del objetivo (realizar un nuevo terminal de explotación para TiM) y alcance del proyecto (no se puede modificar el protocolo de la red, ni el cortafuegos, ni el sistema operativo) pese a que los posibles clientes de la industria de la región (aeronáutica, automoción, alimentación, energía nuclear y naval) sean foco de los ataques, por ello se recomienda un análisis en profundidad como proyecto independiente a este.

Aún así, se tomarán soluciones a los problemas que estén a nuestro alcance y se dejará planteado para que un futuro proyecto pueda afrontarlo en su totalidad.

9.2 Soluciones a la seguridad

Visto que el tema de la seguridad en los SIC es algo integral y nuestra aportación con este proyecto a TiM solo abarca una pequeña modificación a la arquitectura SCADA y el diseño de la nueva terminal de explotación, se propone para ésta:

1.- Gestión de los usuarios, independiente al S.O.:

Al estar funcionando continuamente la delegación de la gestión de los permisos de usuario en el S.O. se antoja restrictiva, puesto que para pasar de niveles de administrador a usuario se necesitaría perder de vista la información presente en la interfaz gráfica; aún así, una integración sería posible si así se necesitase.

2.- Codificación de las contraseñas:

Mediante un algoritmo de cifrado; idealmente la consulta de la clave debería de ser en un servidor, no en la máquina en local, pero al no disponer de permiso para modificar otros ordenadores la aplicación la puede conservar en local; otra opción viable sería que la clave se encontrase en una memoria USB externa, pero eso implicaría dejar un puerto USB accesible para un posible atacante.

3.- Condiciones mínimas para la contraseña:

Se plantea el requisito de que la contraseña cumpla unos requisitos para ser considerada segura -sin entrar en si estos requisitos son recomendables o no, en ello se ahondará en el anexo de seguridad- como por ejemplo que contenga variedad de caracteres (también se podría optar por que esta fuera un patrón de desbloqueo, algo externo o un control biométrico), que caduque al cabo de unos días o que la pantalla se autobloquee si no hay operario presente (bien sea mediante un sensor externo o si no hay interacciones con la terminal, ambas u otras) límite de introducción de contraseña, o, incluso, verificación en 2 pasos.

4.- También habrá que gestionar el alta y baja de usuarios.

5.- Para probar que todos lo aquí expuesto es lo necesario se planearon unos pruebas de usuario con un administradora de sistemas con cierta experiencia para no dejar sin cubrir ningún flanco.

9.3 Algoritmo de cifrado

El algoritmo elegido es el AES (*Advanced Encryption Standard*), es un algoritmo de clave simétrica (una clave vale para cifrar y descifrar el texto cifrado).

El Instituto Nacional de Normas y Tecnología (NIST, National Institute for Standards in Technology) eligió al algoritmo Rijndael como el ganador en un concurso público para elegir un algoritmo de cifrado para proteger información sensible que denominó AES (NIST, 2001).

AES también es el algoritmo de cifrado aprobado por la NSA (National Security Agency) para proteger información de alto secreto (NSA, 2009).

Se valoró también el uso de hash MD5 que, pese a no ser un algoritmo de cifrado, nos permite almacenar el hash de la contraseña en vez de esta, y compararlo con el hash de la contraseña que el usuario introduzca cuando inicie sesión y, en caso de que los hashes sean iguales las contraseñas también lo serían; se rechazó porque se consideró que el administrador del sistema debería de tener acceso a las contraseñas.

9.4 Cifrado con LabVIEW

En LabVIEW disponemos de diferentes toolkits y librerías relacionadas con la seguridad, además de múltiples ejemplos en decibel.ni.com y lava.org.

9.4.1 The Crypto-G toolkit (VARTOR , s.f.)

Contiene más de 50 Vis de cifrado simétrico, hashing y autenticación de mensajes.

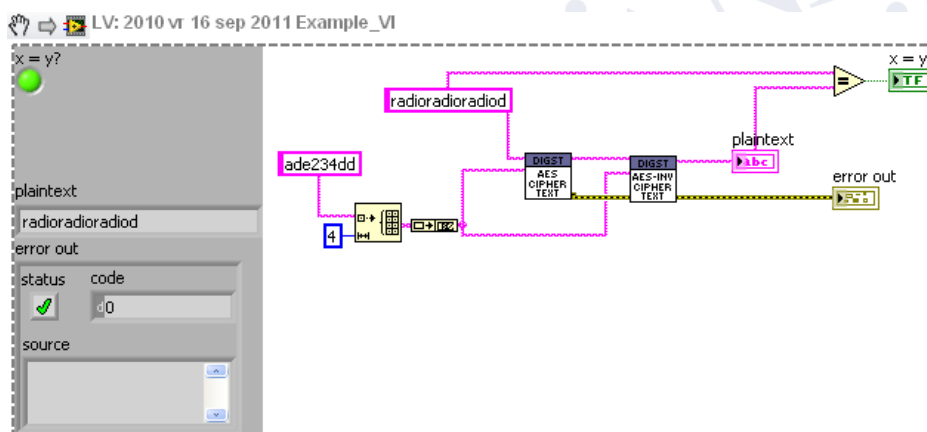
Es de pago, 20 US\$



27: Paleta de Crypto-G toolkit

9.4.2 Encryption V 1.0

(Plomp, 2011)



28: Ejemplo con Encryption V 1.0

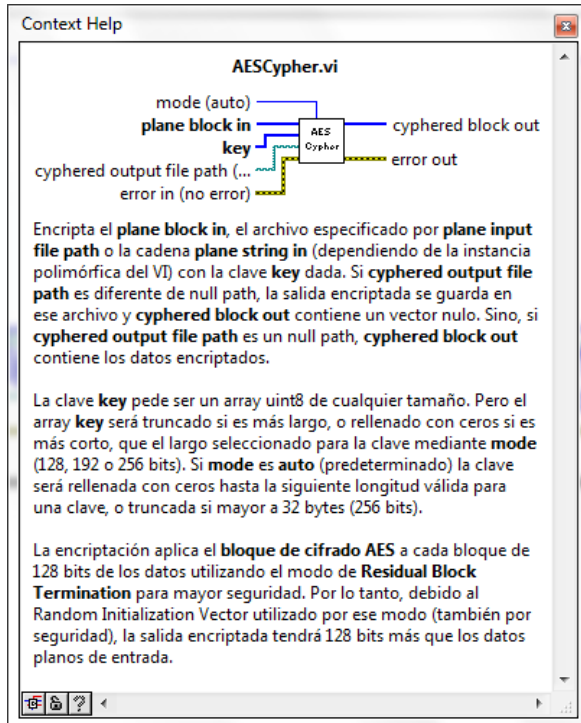
Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Paquete de Vis creado por Ton Plomp que implementan en LabVIEW diferentes algoritmos de cifrado y descifrado como el AES; difícil de usar pero con múltiples ejemplos (JodyK, 2011).

Puede requerir las librerías OpenG para el uso de MD5.

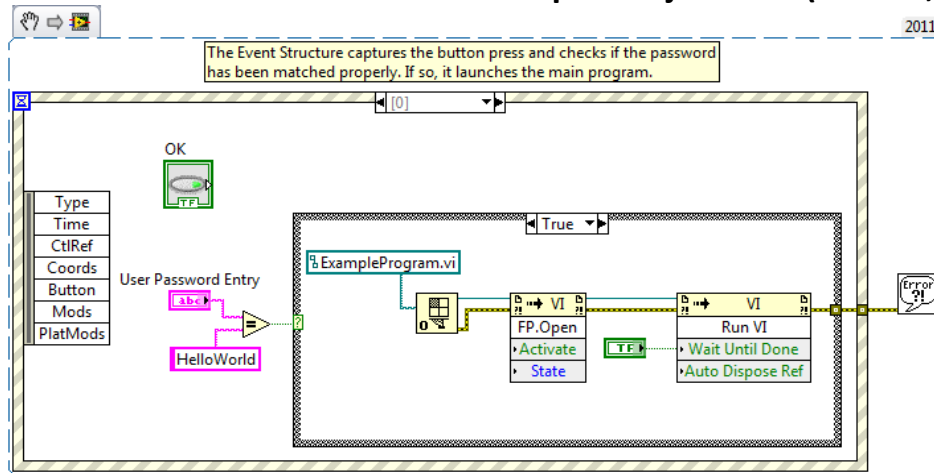
9.4.3 AES Library for LabVIEW (Muñoz, 2011)

Esta es una biblioteca diseñada por Daniel Muñoz para añadirle soporte nativo para encriptación a LabVIEW sin que dependa de .NET u otro recurso externo.



29: Ayuda de AES Library for LabVIEW

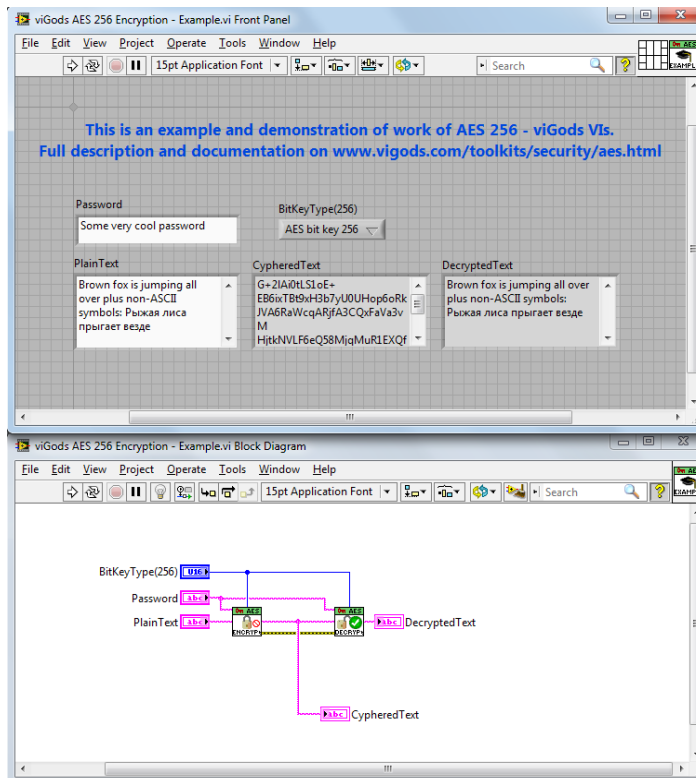
9.4.4 Protección con contraseña en tiempo de ejecución (NI.com, 2009)



30: Protección en tiempo de ejecución

Es la forma más sencilla y sin el uso de librerías de terceros para proteger de manera simple el acceso al VI cuando está funcionando.

9.4.5 AES toolkit (Titov, s.f.)

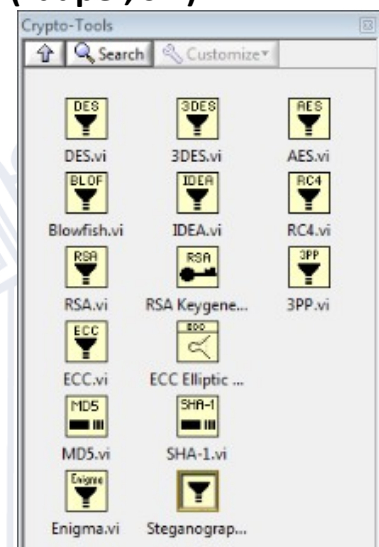


El AES toolkit ha sido desarrollado por Igor Titov y dispone del certificado de compatibilidad con LabVIEW dispensado por National Instruments.

31: Ejemplo con AES Toolkit

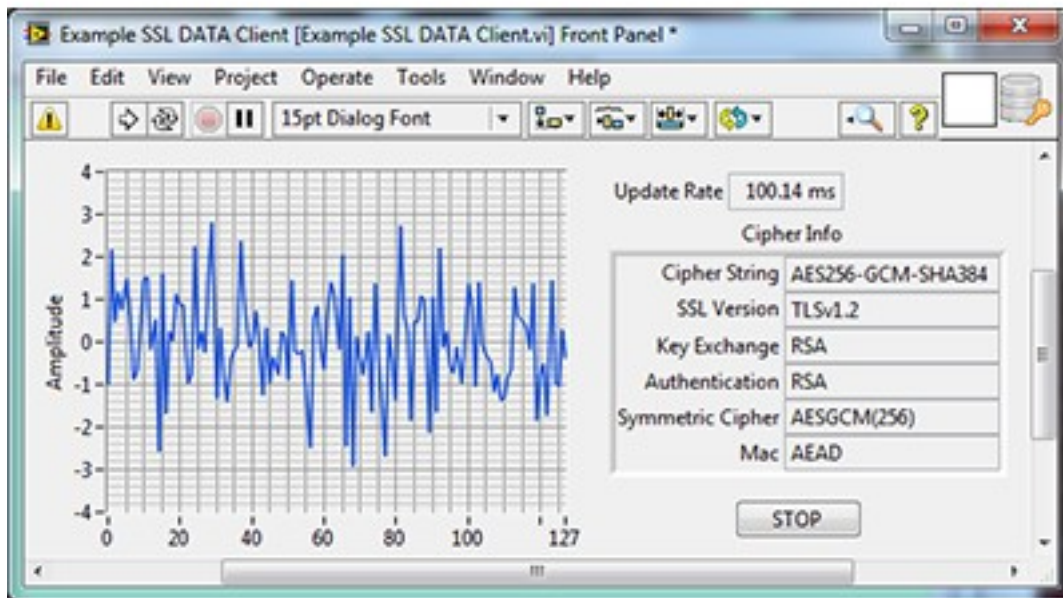
9.4.6 Crypto-Tools for LabVIEW (Lauper, 2012) (Lauper, s.f.)

Crypto-Tools contiene las librerías Crypto.llb y Large Numbers.llb desarrollada por Alfred Lauper y contiene, entre muchos otros algoritmos, DES, 3DES, AES, RSA, MD5, SHA-1 o SHA-2.



32: Paleta de Crypto-tools

9.4.7 Encryption Compendium (LVS-Tools , s.f.)



33: Ejemplo de Encryption Compendium

9.4.8

Es una librería de pago desarrollada por LVS-Tools implementando más funcionalidades que el resto, entre ellas SSL, TLS, generación de certificados o direcciones de Bitcoin.

9.5 Herramienta elegida

Puesto que el algoritmo elegido previamente era el AES y el AES toolkit disponía del certificado de compatibilidad con LabVIEW este toolkit fue el elegido.

9.6 Gestión de usuarios

La gestión de los usuarios es un tema importante, puesto que se ha de permitir diferentes niveles de acceso al terminal de explotación y se ha de gestionar.

Desgraciadamente o nadie se ha preocupado hasta ahora o se ha hecho vagamente o se ha delegado en el SO, pero no se han encontrado herramientas que cumplan nuestras expectativas por ello se desarrollará una librería propia.

En el siguiente apartado se listan las opciones revisadas.

9.6.1 Grupos de usuarios de Windows (lavezza, 2011)

Se podría delegar la gestión de usuarios en el Sistema Operativo, si este fuera Windows haciendo uso de los VI programados por Lavezza del foro LAVA, si fuera otro SO usando unos VI análogos para cada SO, pero esto obligaría a usar el programa siempre sobre el mismo SO.

En un principio se buscó sólo para Windows debido a que la licencia de estudiante de LabVIEW comprada sólo funcionaba en dicho sistema operativo.

9.6.2 Simple LabVIEW User Log-In Demo (RER, 2012)

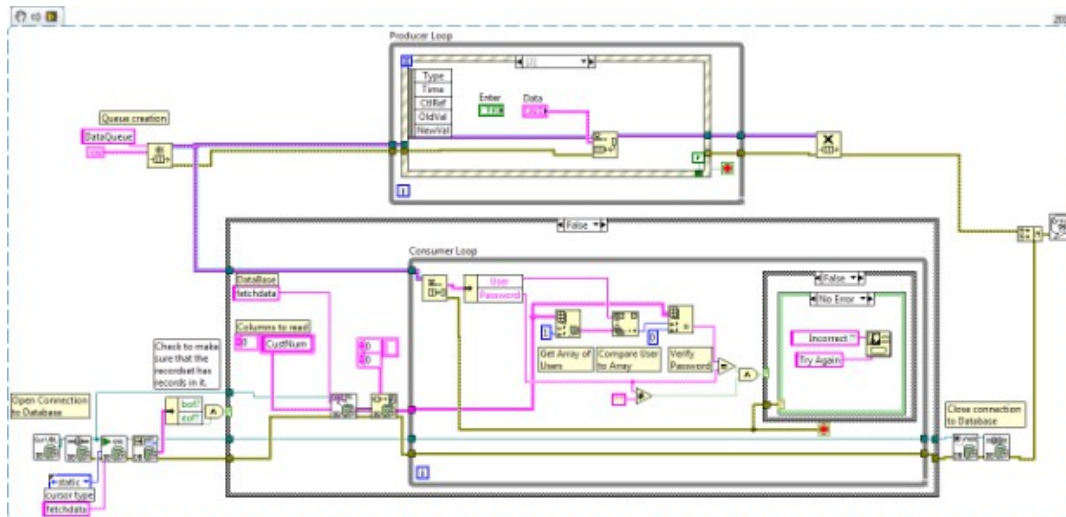


Programa de ejemplo creado por RER de los foros decibel.ni, proporciona diferentes funciones para el control de 2 usuarios cuyas contraseñas están dentro del código.

9.6.3

9.6.4 Inicio de sesión de usuario con clave almacenada en una base de datos (MarisolM, 2013)

Programa de ejemplo creado por MarisolM de los foros decibel.ni y haciendo uso de LabVIEW DataBase Connectivity Toolkit para almacenar las contraseñas.



35: Ejemplo de MarisolM

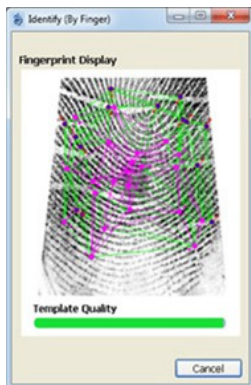
9.6.5 AutoTEC Logon (AutoTEC, 2008)

The screenshot shows a 'Logon Information' dialog box with a title bar and a key icon. It contains two text input fields: 'User name' and 'Password'. Below the fields are two buttons: 'Login' (with 'Ent' as a tooltip) and 'Cancel' (with 'Esc' as a tooltip).

36: Ejemplo de UtoTEC

Ejemplo proporcionado por el usuario AutoTEC (actualmente se llama GITA_A) en el cual proporciona una serie de Vis que leen de un archivo los usuarios existentes y comprueba si el introducido por el usuario existe; también permite la creación de nuevos usuarios.

9.6.6 Biometric Login Toolkit (Blue Ridge Test , s.f.)



Toolkit desarrollado por la empresa Blue Ridge Test⁹ para el uso de su hardware biométrico.

37: Ejemplode Biometric

Login toolkit

9.6.7 Secure Login Framework (IMS, s.f.)

This is the IMS Secure Login Example. This is an example program that uses secure login to limit access to program features and shows you one way of implemented secure login.

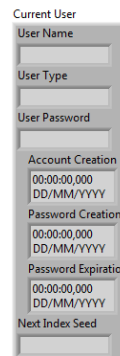
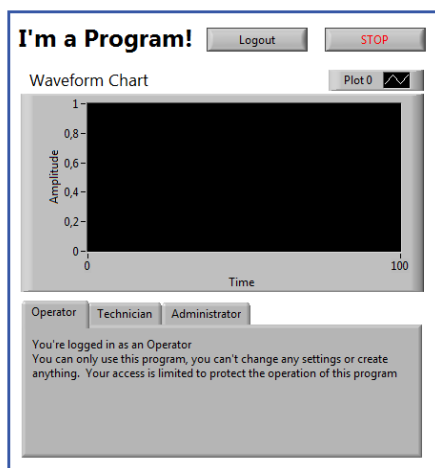
View the configuration options on the block diagram for how to setup Secure Login. Then, select a theme below, and run the program.

Log in with your default user name and password:

User Name: Administrator
Password: password

Enter the administrator user name and password and press "Manage" instead of Login to configure users. Add different user accounts and login as them and see how the program responds. The program will also log you out after 1 minute of inactivity.

Theme
Silver



This is the current user you are logged in as. This is just for example. You don't want to give your program access to plain-text passwords of your user like this



38: Secure Login Framework

Vis de la empresa IMS, Inc. Que proporcionan multitud de funcionalidades tales como creación y borrado de usuarios, almacenaje del hash MD5, encriptación entre muchas otras. Está sólo en versión demostración en la web.

⁹ <http://www.blueridgetest.com>

9.7 *Vis para la gestión de usuario*

La herramienta deseada hubiera sido muy parecida a Secure Login Framework pero al ser de pago se tuvo que desechar pasando a desarrollar una librería propia tomando conceptos de AutoTEC Logon y Simple LabVIEW User Log-In Demo.

9.8 *Seguridad en TiM*

Los elementos que forman el sistema SCADA a los que tenemos acceso en el laboratorio del ADMT y el software necesario para su configuración y programación son:

- PLCs (L23E y L32E) de la serie CompacLogix de Rockwell.
- RSLogix 5000
- FactoryTalk

Lo primero que se debería de hacer es consultar las alertas de seguridad publicadas en los boletines; este tipo de comprobaciones ha de ser continuo en el tiempo para poder aplicar las medidas de seguridad recomendadas por los fabricantes cuando surja la vulnerabilidad.

En este apartado haremos una consulta de los últimos meses de los incidentes relacionados con los elementos previamente listados.

Todas ellas están solucionadas con sus correspondientes parches de seguridad.

9.8.1 Rockwell Automation ControlLogix PLC Vulnerabilities: Advisory (ICSA-13-011-03) (ICS-CERT, 2013)

Vulnerabilidad que afecta a los dispositivos con conectividad EtherNet/IP y CompactLogix L32E and L35E Controllers.

Explotable mediante la transmisión de comandos arbitrarios desde una interfaz de control al PLC o a la tarjeta de red.

La explotación exitosa de esta vulnerabilidad puede resultar en una denegación de servicio (DoS), un fallo del controlador, permitir un ataque Man in The Middle (Mitm) o un ataque de reinyección.

9.8.2 Rockwell Automation FactoryTalk and RSLinx Vulnerabilities (Update A): Advisory (ICSA-13-095-02A) (ICS-CERT, 2013)

Vulnerabilidad que afecta a Factory Talk y RSLinx versiones CPR9, CPR9-SR1, CPR9-SR2, CPR9-SR3, CPR9-SR4, CPR9-SR5, CPR9-SR5.1, y CPR9-SR6.

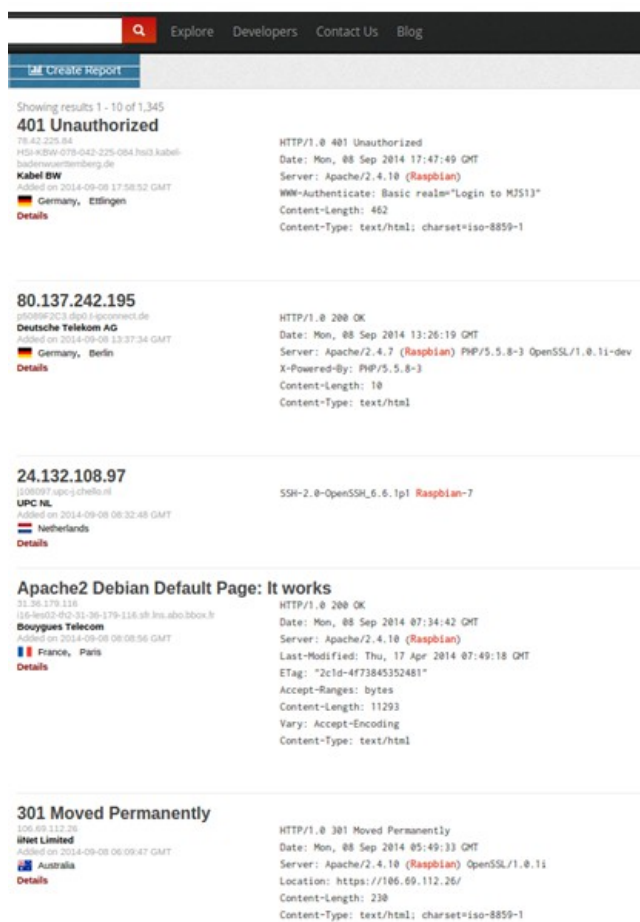
Puede causar una denegación de servicio (Do), el apagado o una inyección de código.

9.8.3 Rockwell RSLogix 5000 Password Vulnerability: Advisory (ICSA-14-021-01) (ICS-CERT, 2014)

Vulnerabilidad que afecta a los programas protegido por el usuario con contraseña programados con RSLogix 5000 V7 hasta V21.0.

Una explotación exitosa puede dar lugar al acceso no autorizado a contenido creado por el usuario pero no interrumpirá directamente el funcionamiento normal del autómatas.

9.9 Shodan



39: Ejemplo de búsqueda en Shodan (Moreno, 2014)

Shodan se utiliza en este proyecto para comprobar la no accesibilidad de las máquinas de la red donde está nuestro sistema.

Pese a que TiM es un sistema que no está en producción sí que está conectado a internet; no es posible encontrarle con Shodan por lo que en este punto cumple los requisitos.

Shodan¹⁰ es una empresa fundada por John Matherly que dispone de un buscador, al igual que Google o Bing, pero en vez de indexar la información presente en los servicios web lo hace con las características de la máquina conectada a internet (Moreno, 2014).

Se puede usar para saber características del hardware de la máquina, del software (programas, versiones...) y de su configuración (puertos abiertos), permitiendo hacer búsquedas sabiendo la IP o el rango en el que se encuentra, localidad u organización siempre y cuando la máquina provea esa información.

¹⁰ <https://www.shodan.io/>

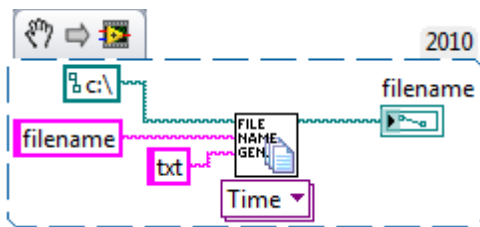
10.- Otras herramientas

Este apartado recoge aquellas herramientas que habiendo sido utilizadas no forman parte de las principales, bien por ser de apoyo o bien por ser la única disponible.

10.1 VIs utilizados

10.1.1 Filename generator (jtagg, 2012)

Librería creada por jtagg para la generación de nombres de ficheros con nombres

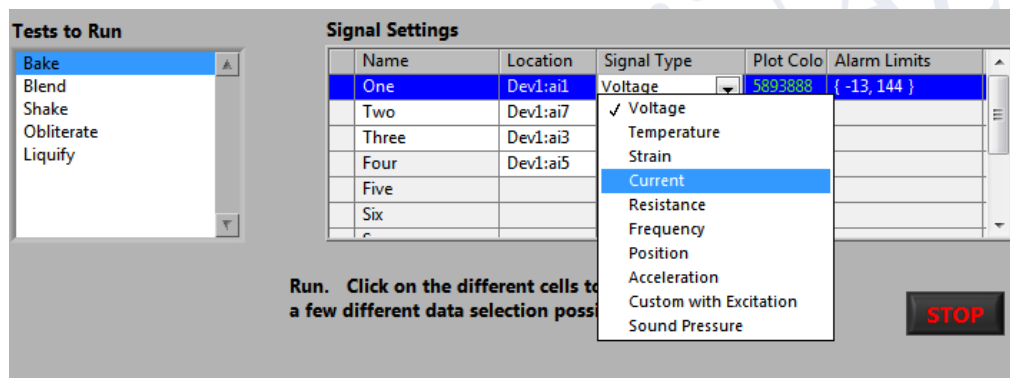


autoincrementando la fecha u hora sin necesidad de que sean modificados internamente.

40: FileName Generator

10.1.2 Type Sensitive Popup (Saunders, 2007)

Vi creados por David Saunders para crear interfaces más intuitivas, permitiendo manipular datos tabulados en tiempo de ejecución de la aplicación.



41: Type Sensitive Popup

11.- Licencia

A la hora de licenciar un proyecto software además de las necesidades e intereses del programador o la empresa en la que este trabaje, se han de tener en cuenta las licencias de las librerías y toolkits que el proyecto utiliza.

En este apartado se intentará determinar que licencia o tipo de licencias son susceptibles de ser aplicadas a este proyecto.

11.1 Licencias de las librerías usadas

Librería	Licencia
VideoLAN	GNU LGPLv2.1+ (GNU, s.f.)
Type Sensitive Popup	BSD (Berkeley, s.f.)
FileName Generator	BSD-3 (Berkeley, 1999)
Ethernet IP CIP	Sin Licencia
I3 JSON	MIT (MIT, s.f.)
AES toolkit	Licencia propia similar a la licencia BSD-3

Las licencias (o ausencia de ellas) de la tabla anterior limitan las opciones disponibles. Las licencias BSD y MIT son las más permisivas, pudiendo relicenciarse tanto para proyectos de software libre como para proyectos privativos.

El software bajo licencia LGPL permite su inclusión en otros proyectos que sean software libre y el que sean enlazadas por terceros.

El Software sin licencia es el más problemático, prohíbe su distribución, modificación e inclusión en otros proyectos, pero viendo el post de LAVA donde el autor lo publicó

podemos leer que está a favor de la modificación y publicación de forma gratuita por terceras partes.

“Estaría agradecido si alguien actualiza el código de acuerdo con las directrices e hiciera que estuviese disponible para todos gratuitamente.”

(Siva, 2007)¹¹

Siendo la GPL la licencia más estricta no tendremos que atener a utilizar una licencia que sea compatible, es decir, una licencia libre.

11.2 Qué es Software libre

Software libre (FSF y GNU, s.f.) es todo aquel que cumple las 4 libertades:

- Libertad 0: Usar el programa, con cualquier propósito.
- Libertad 1: Estudiar cómo funciona el programa y modificarlo para adaptarlo a tus necesidades.
- Libertad 2: Distribuir copias del programa a terceros.
- Libertad 3: Mejorar el programa y hacer públicas esas mejoras, de modo que toda la comunidad se beneficie.

Sólo el acceso al código fuente garantiza que las libertades 1 y 3 se cumplan.


11.3 Licencias Libres


¹¹ “I would appreciate, if somebody updates the code as per guidelines and makes it available free to all.” (Siva, 2007)


Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

La existencia de decenas de licencias libres hace muy difícil conocerlas, saber cómo se relacionan y elegir entre ellas, para ello webs como Choose A License¹² o Copyleft¹³ nos permiten conocerlas, pudiendo acudir también a la Wikipedia donde se recogen y sintetizan (Anon., s.f.) También existen tablas como la que se adjunta que resumen las características de las principales licencias (no se ha encontrado al autor original, parece ser que fue Adriaan de Groot (Miembro de la Free Software Foundation Europa) el autor o el inspirador al autor en base a una serie de artículos en la web de la FSFE (Groot, 2009) (Groot, 2009) (Groot, 2009).

 Garantiza al usuario las cuatro libertades del Software Libre.


 Garantiza el acceso al código fuente.

 Los cambios realizados deben ser publicados.

 El software derivado debe tener la misma licencia.

 Utilizar el *software* a través de la red cuenta como distribución.

 Contiene garantía contra patentes.

 Contiene garantía contra *tivoización*.

 Contiene condiciones poco usuales que deben estudiarse.

42: Leyenda de la tabla comparativa

¹² <http://choosealicense.com/>

¹³ <http://copyleft.org/>

AFL	fs	src						pat	
APL	fs	src						pat	
Artistic	fs	src						pat	
BSD 2-Clause	fs	src						pat	
CDDL	fs	src						pat	
CPL	fs	src						pat	
CPOL	fs	src						pat	
EPL	fs	src						pat	
GPLv2	fs	src						pat	
GPLv3	fs	src						pat	
LGPLv2	fs	src						pat	
LGPLv3	fs	src						pat	
MIT	fs	src						pat	
MPL1.0	fs	src						pat	
MPL1.1	fs	src						pat	
MS-PL	fs	src						pat	
OSL	fs	src						pat	
php	fs	src						pat	
ruby	fs	src						pat	
zlib	fs	src						pat	

43: Tabla comparativa entre licencias libres

11.4 *Licencia elegida*

Dentro de las comunidades de usuarios de LabVIEW las licencias que permiten el uso privativo del software derivado son predominantes, bien por filosofía de los programadores o bien por necesidades de la industria, por lo tanto será la licencia BSD-3 la que adoptará este proyecto.

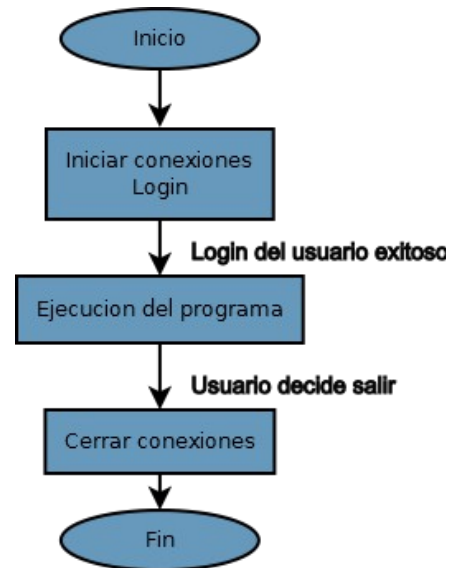
12.- Programación del terminal de explotación

12.1 Estructura del programa

FALTA

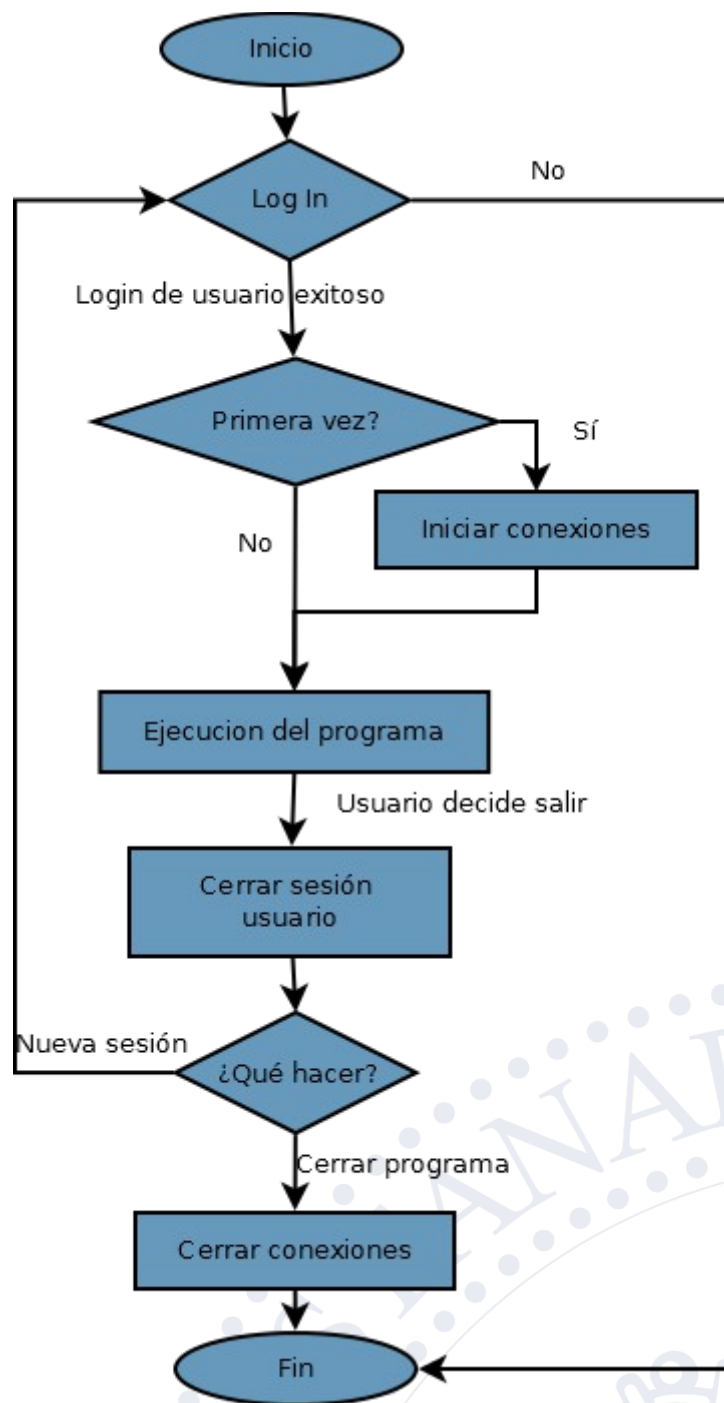
Inicialmente se intentó optar por un desarrollo lineal del programa (abrir comunicaciones, adquirir/escribir datos, cerrar comunicaciones), pero tras las primeras pruebas de usuario se vió que las necesidades iban más allá y se necesitaba una estructura más compleja.

Finalmente se optó por un flujo del programa como se detalla en la imagen siguiente



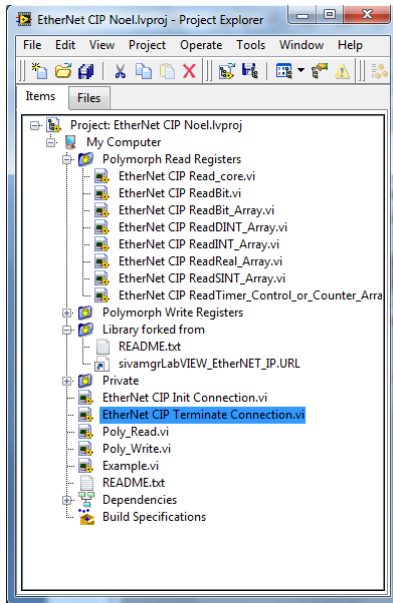
44: Flujograma inicial

Secuencia para la inicialización, programación por eventos para la interfaz.



45: Flujograma del programa

12.2 Librería Ethernet/IP



La librería consta de 4 VI:

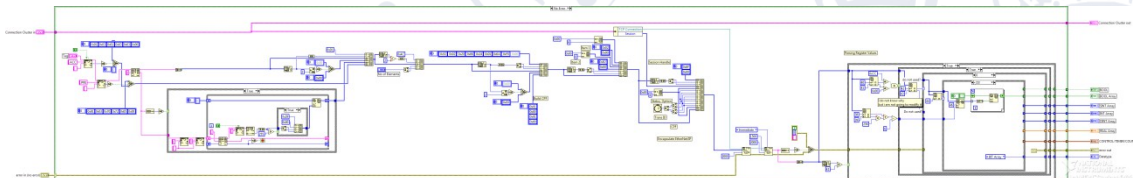
- EtherNet CIP Init Connection.vi
- EtherNet CIP Terminate Connection.vi
- Poly_Read.vi
- Poly_Write.vi

Los 2 primeros abren y cierran la conexión respectivamente y los 2 últimos leen y escriben en los tags del autómatas.

46: Librería Ethernet/IP

Poly_Read y *Poy_Write* están formados internamente de 7 VI diferentes, cada uno lee/escribe un tipo diferente de dato y todos ellos usan internamente *EtherNet CIP Write_Core* (en el caso de los de escritura usan *Read_Core*) que es el VI de la librería *EtherNet_IP_CIP* pero con algunas mejoras a su código (tanto funcionales como estéticas).

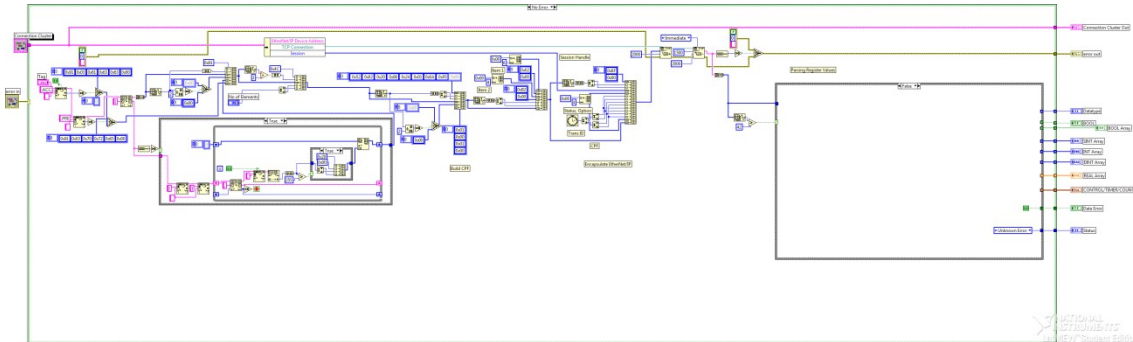
12.2.1 Mejora de la legibilidad



47: Read_Core

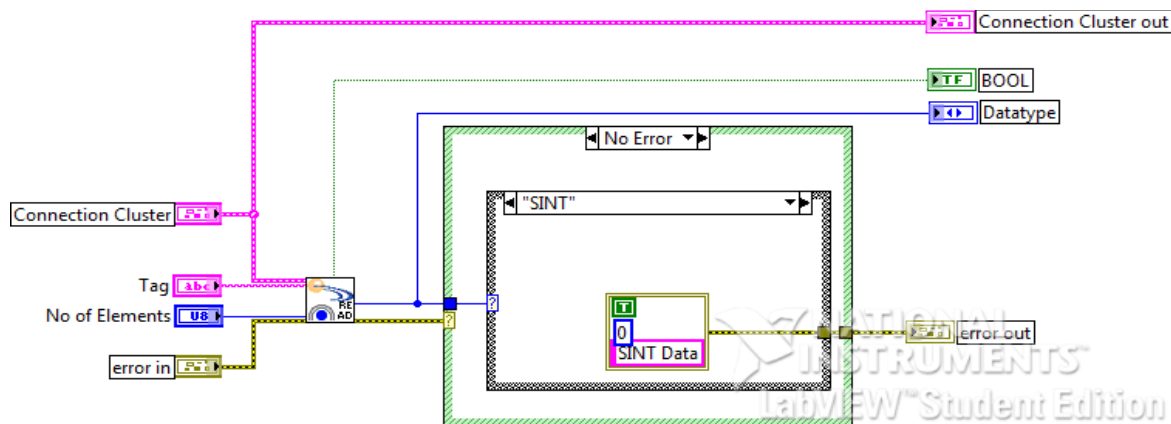
Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Como se puede observar en el código, el VI original no tenía una buena legibilidad, con hilos que volvía hacia atrás en el diagrama y cruces confusos; se decidió reorganizar el diagrama y encapsularlo.



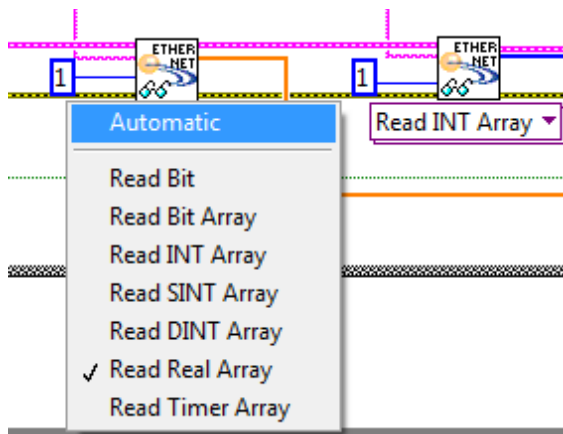
48: Ethernet_CIPScan_Registers

Se creó *Ethernet_CIP_Read_core* y *Ethernet_CIP_Write_core*, que serían los VI originales, que a su vez son llamados por *Ethernet_CIP_Read_bit/bitArray/...* Vis que cada uno se encarga de un tipo de dato.



48 bis: Ethernet_CIPScan_Registers

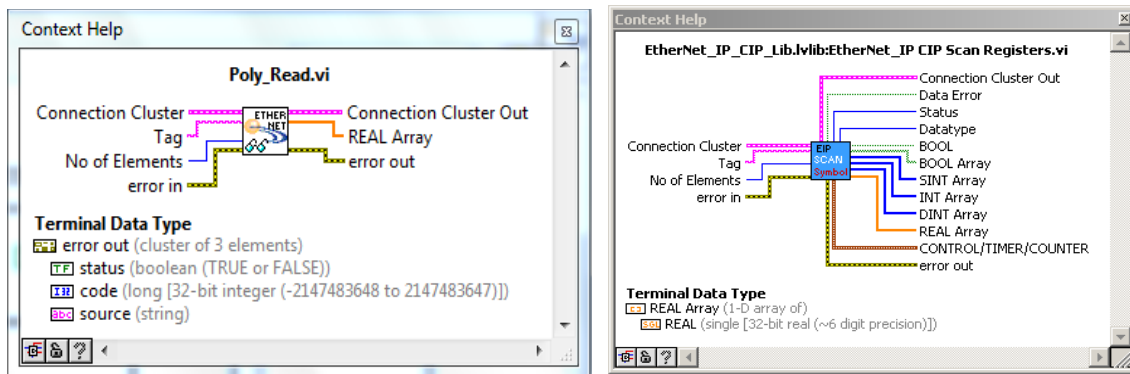
12.2.2 VIs polimorfos



Todos ellos se agruparían en un VI polimorfo que permite el uso de múltiples VI dentro del principal siempre y cuando compartan terminales en pos de mejorar la usabilidad de los VI.

49: ejemplo del polimorfismo

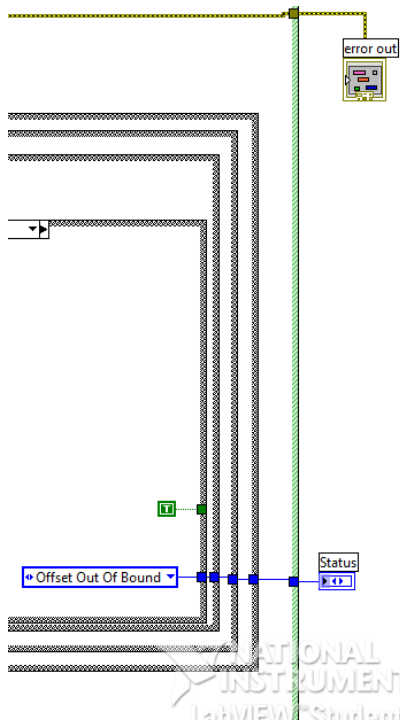
Pasando de VI con más de 10 salidas a unos nuevos sólo 3.



50: Comparación de las ayudas de la librería antes y ahora

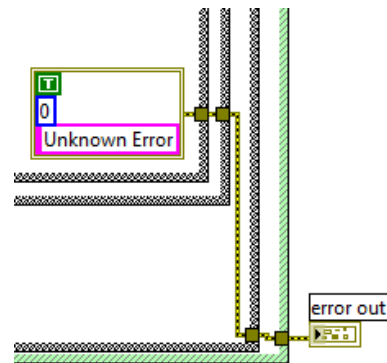
12.2.3 Errores

El manejo de errores (mal implementado en la librería original).



51: error ml implementado

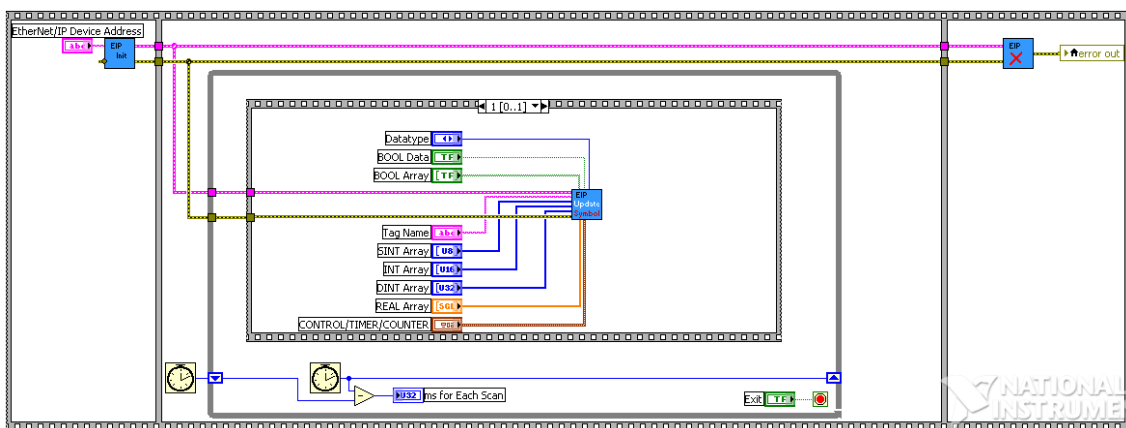
Se pasó de tener errores sin mensaje, con el mensaje de error pasado al exterior del VI mediante un tipo de dato enum, a integrar estos mensajes dentro de errores



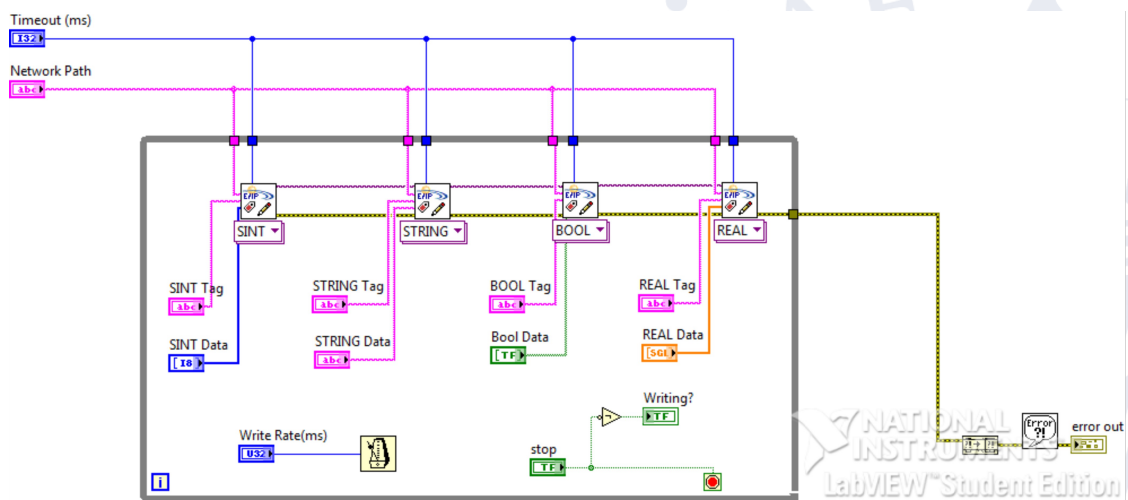
52: nuevo error

12.2.4 Comparación

Para valorar las mejoras, se puede comparar un ejemplo usando esta librería final con el inicial y con NI-Industrial Communications para EtherNet/IP 1.2.1

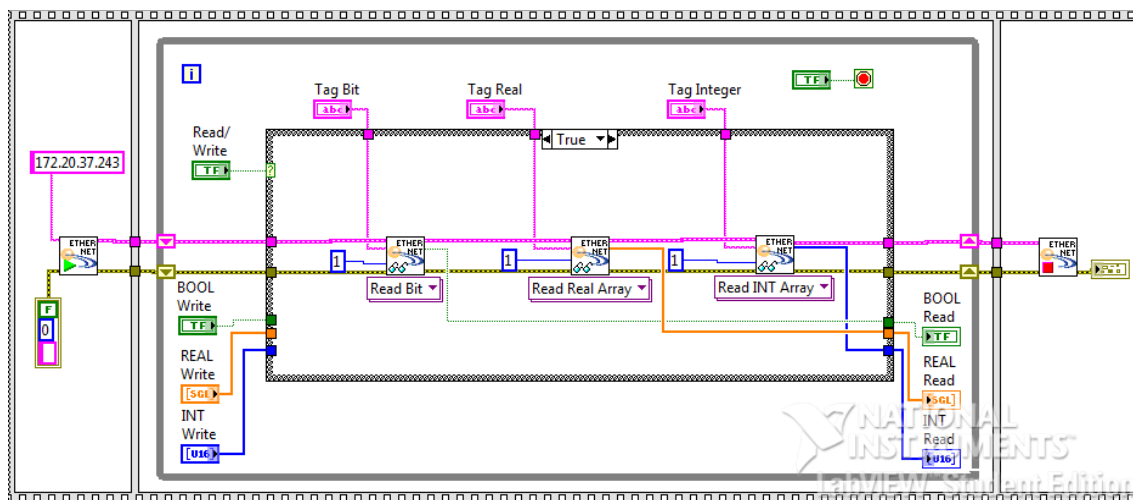


53: Ejemplo con la librería tal y como la encontramos en internet



54: Ejemplo con la librería NI-Industrial Communications para EtherNet/IP 1.2.1

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan



55: Ejemplo con la librería al final de todo el proceso

Se puede observar que la mejora es notable (sólo un dato de salida por cada VI) y su alta similitud en las entradas y salidas con los VI de la librería provista por National Instruments.

12.2.5 Iconos

Otra mejora es la actualización de los iconos para que sean legibles y reflejen más fielmente lo que representan.



56: Comparación de iconos de la librería de Ethernet

Se deja para más adelante a eliminación de trozos de código duplicados que existen entre los actuales *Ethernet_CIP_Read_core* y *Ethernet_CIP_Write_core*.

12.3 Librería con VLC

12.3.1 Wrapper

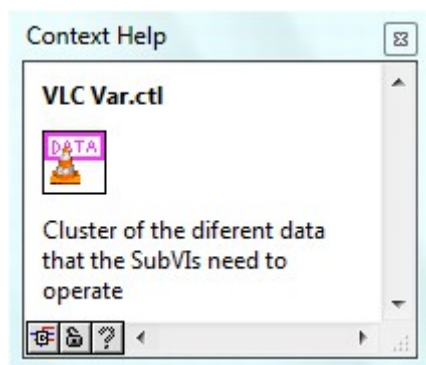
Del inglés to wrap, envolver, es una técnica por la cual se pueden utilizar librerías que de otra forma no se podría, en este caso el uso de una librería escrita en C y C++ dentro de un programa escrito en LabVIEW.

12.3.2 Tipos de datos

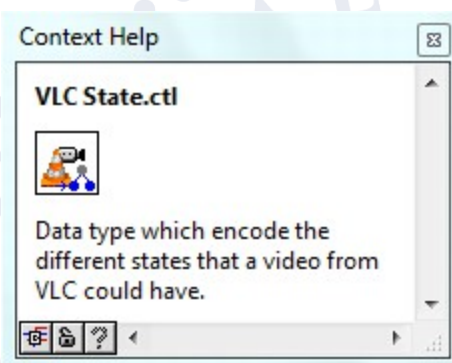
Para el manejo de VLC se tuvo que crear 2 tipos de datos propios, *VLC State* y *VLC Var*, el uno para saber el estado de la transmisión de vídeo y el otro para almacenar la información necesaria para realizar una transmisión.



57: Librería LabVIEW VLC



58: Ayuda de VLC Var

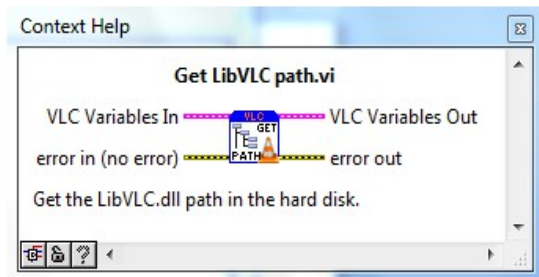


59: Ayuda de VLC State

12.3.3VI básicos

Hay 3 Vis que son básicos para iniciar una transmisión:

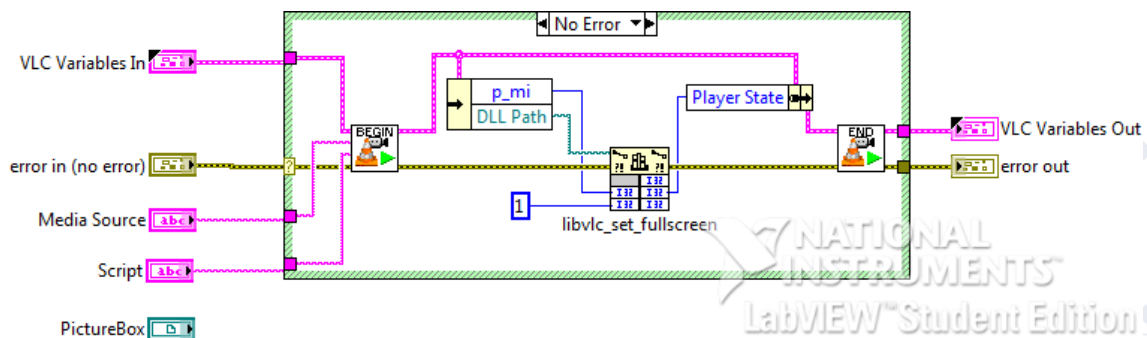
- *Get LibVLC Path.*
- *Start Vídeo.*
- *Stop Video.*



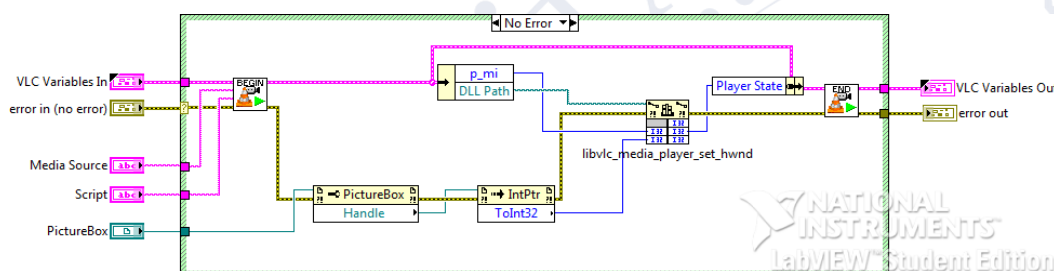
El primero obtiene la dirección de VLC en el disco duro, originariamente fue creado por GriffinRU y se llamaba *VLC - Get Program Location (path).vi* (GriffinRU, 2012)

60: Obtencion de la carpeta donde está

El segundo inicia la transmisión de la cámara web, al ser un VI polimorfo permite la visualización mediante 3 métodos: embebido en el VI, en una nueva ventana o en pantalla completa, esto 3 VI comparten trozos de código que no están accesibles al usuario de la librería y se encuentran en la carpeta subs\private.

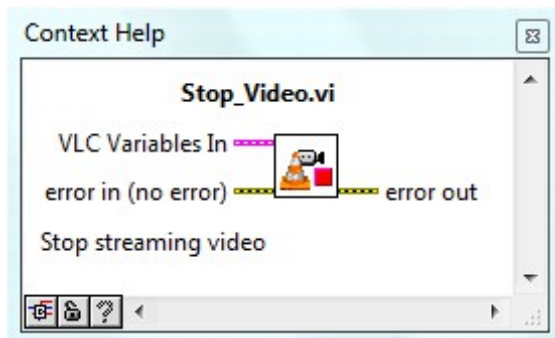


61: Vídeo a pantalla completa



62: Video embebido dentro de LabVIEW

Otro punto importante es que VLC y nuestros VI permiten el uso de scripts programados en LUA.



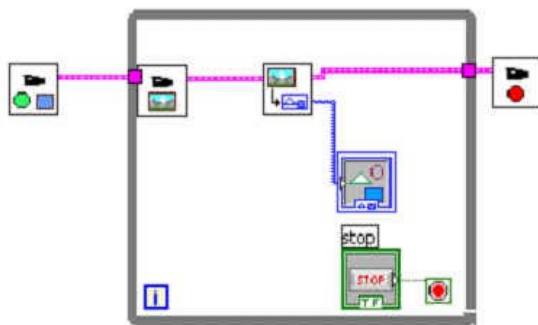
El tercer VI es *Close Video* que sirve para cerrar correctamente la conexión con la webcam.

63: Cierre de la conexión con la webcam

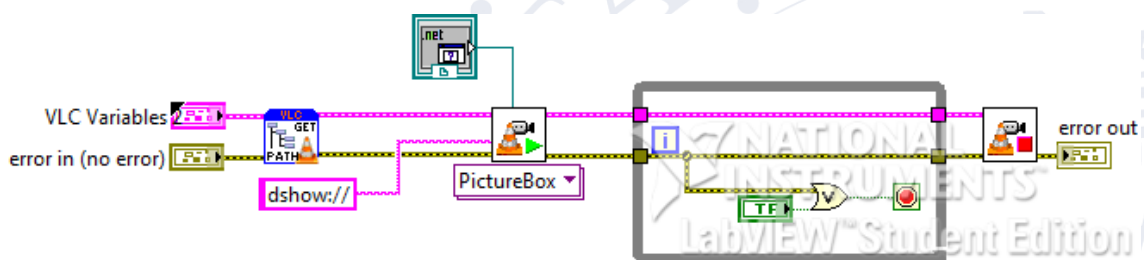
12.3.4 Comparativa

Al igual que con la librería de Ethernet, con la librería de VLC se ha conseguido alcanzar en simplicidad a la librería más sencilla de las valoradas, Robolab.

Aún así, al ser un desarrollo propio en estado embrionario no se alcanza a disponer de las capacidades de algunas de las otras librerías, sobretodo de las comerciales.



64: Ejemplo con Robolab

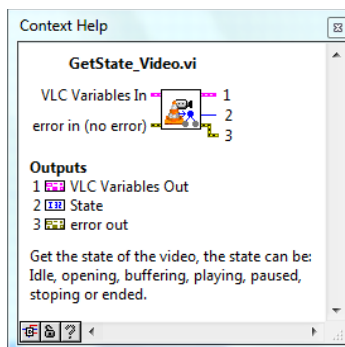


65: Ejemplo con la librería creada

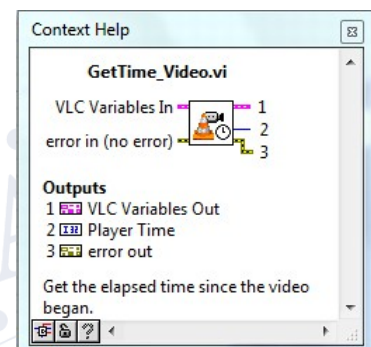
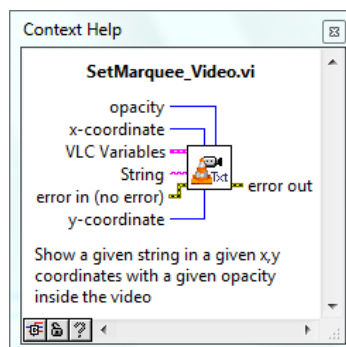
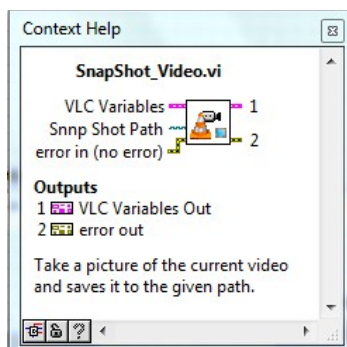
12.3.5 VI complementarios

Otros VI que se han creado, pese a que no se han usado en el proyecto final son:

- *GetState_Video*
- *GetTime_Video*
- *SetMarquee_Video*
- *SnapShot_Video*
- *Coonverting to mp4*



GetState_Video captura el estado del vídeo (*Idle, opening, buffering, playing, paused, stoping* y *ended*), es muy útil cuando se hacen aplicaciones más complejas que requieran más interacción por parte del usuario.



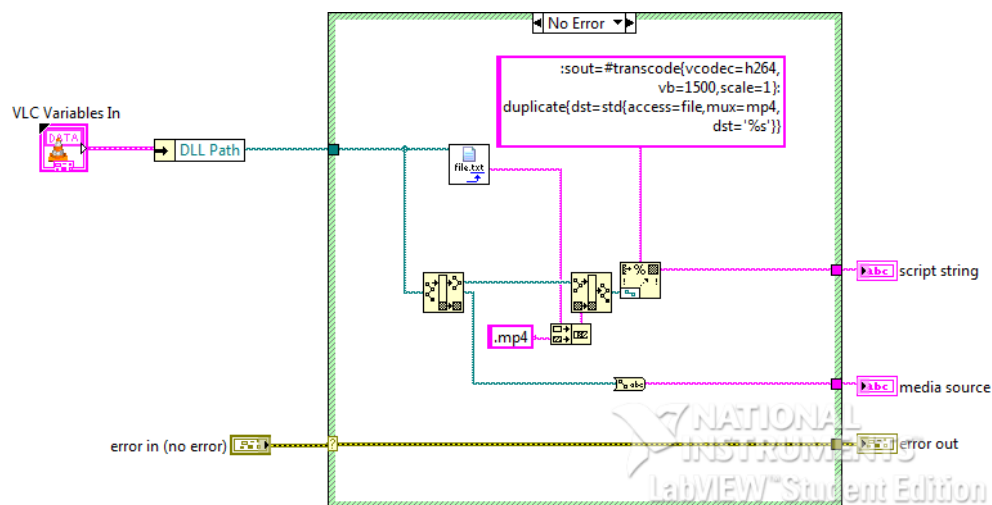
66: Ayuda dentro dle programa de varios de los VIs creados

GetTime obtiene cuanto tiempo lleva corriendo el vídeo.

SetMarquee embebe en el vídeo una cadena de texto

Snapshot captura un frame del video.

También se ha incluido 2 VI de ejemplo, el primero ya visto antes cuando hemos comparado el resultado con lo que nos ofrecía Robolab y el otro contiene un script para convertir un archivo de vídeo que tengamos en nuestro ordenador al formato mp4.



67: Script para la conversión a formato MP4

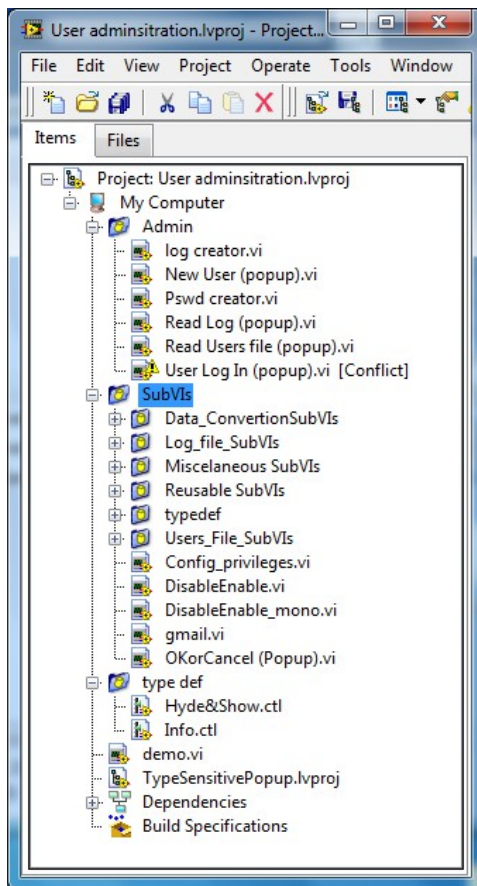
12.3.6 Iconos

Otro aspecto no menos importante es la uniformidad en los iconos que, como se ha visto, comparten plantilla (el logotipo de VLC y una cámara) y se les añaden otro glifo que se le identifica indefectiblemente entre todos los demás.

12.3.7 Ampliación futura

Los VI antes comentados son los que han sido programados y utilizados para este proyecto -pese a que alguno no ha sido utilizado- pero pueden ser fácilmente ampliables siguiendo el mismo procedimiento de wrapping de DLLs.

12.4 Librería de control de acceso



Esta ha sido la librería más compleja de las realizadas, tanto por la cantidad de VI creados como por las interrelaciones entre ellos, por ello y para no saturar este apartado, aquí se explicarán aquellos VI que sean accedidos directamente y esbozándose la estructura interna de la librería.

Aquí es donde se ha hecho uso de la librería Type Sensitive Popup y de AES toolkit.

Este sistema crea y hace uso de 2 archivos en texto plano: log.txt y usuarios.txt.

68: Librería de control de accesos

12.4.1 Log.txt

Guarda las acciones que se crean importantes, el usuario que lo hizo, el tipo de usuario y la fecha y hora.

El tipo de acciones que se almacenan en el log es limitado, pero sirven como ejemplo de cómo se debería de hacer en caso de expandirse para cumplir las necesidades de los usuarios de la librería.

Este era uno de los VI más complicados debido a la cantidad de información que se puede recopilar en un log, así mismo es el que más ha cambiado durante el proyecto

debido a fallos encontrados y sugerencias recibidas durante las pruebas de usuarios, por lo tanto se puede considerar que se ha conseguido un modelo mínimo de lo que se ha considerado necesario pero que permite su expansión en un futuro; si fuese necesario usando diferentes archivos de log para diferentes situaciones (almacenar todas las acciones realizadas, movimientos de ratón...), también se puede almacenar todo en el mismo log pero proveyendo al administrador de herramientas de filtrado del log.

12.4.2 Usuarios.txt

Este fichero almacena los usuarios que tienen permiso para acceder al sistema, se prevé que no sea muchos debido a que un sistema de control industrial no debería de ser un sistema al que puedan acceder muchos usuarios.

Se almacenan nombre, clave, tipo de usuario y fecha de creación del usuario.

12.4.3 Tipos de datos

Hay 2 tipos de datos que se han considerado útiles para los usuarios de esta librería.

Info, que simplemente es un icono basado en un control booleano que se usa para que cuando se posa el ratón encima suyo muestre una ayuda al usuario (esta ayuda se puede configurar en *propiedades->documentation->Tip Strip*).

Hyde&Show es el tipo de dato que junto con los VIs *Config privileges*, *DisableEnable* y *DisableEnable_mono* permite esconder, habilitar, deshabilitar y deshabilitar poniéndolo en gris los controles e indicadores de la aplicación (opciones: *hide*, *enabled*, *disabled* y *disabled and grayed out*).

12.4.4 VIs de administrador

Son los VI más importantes al hacer uso de la librería y son:

- *New User*
- *Read Log*
- *Read Users file*
- *User Log In*

Todos ellos son ventanas emergentes.

12.4.5 New User

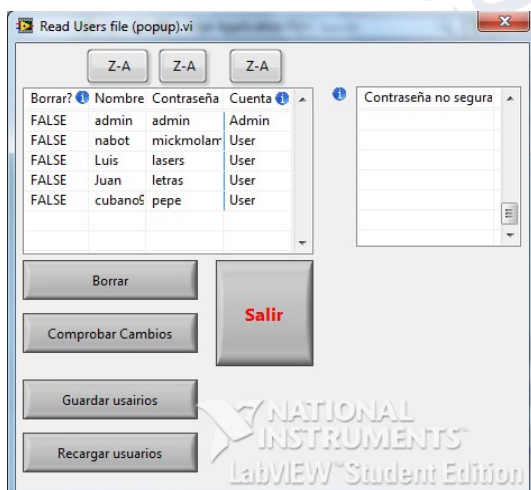
Sirve para la creación de un nuevo usuario; Pide doble comprobación de la contraseña, comprueba que esta cumpla unos criterios mínimos y guarda en el log que usuario ha creado la nueva cuenta ya que para ejecutarlo se necesita haber entrado como administrador.

12.4.6 User Log In

Pide el usuario y la contraseña al operario del programa, pudiéndose realizar hasta 4 intentos y almacenando en el log quien ha entrado intentado entrar y tras cuantos intentos.

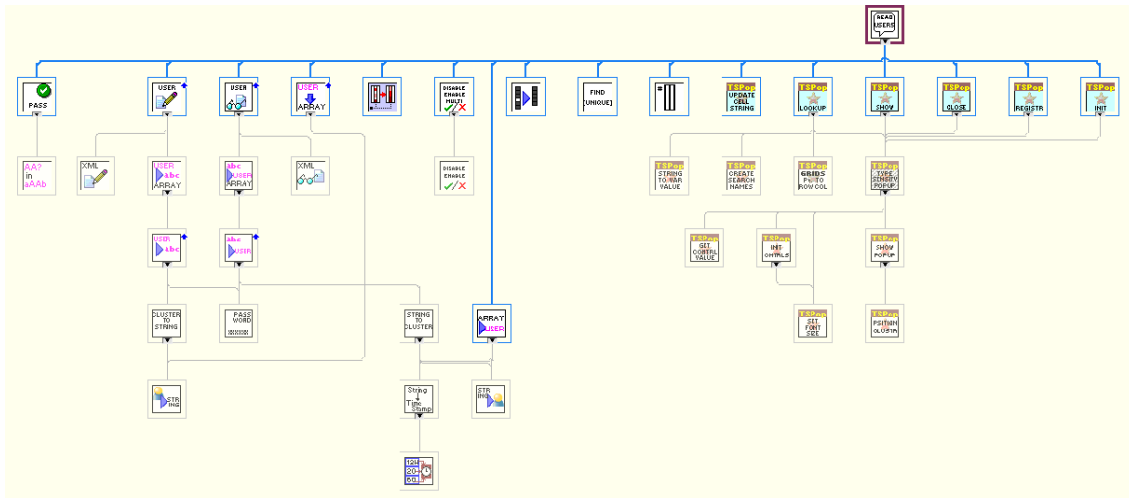
Read Users file y Read Log son los VI que leen los archivos usuario.txt y log.txt.

12.4.7 Read Users file

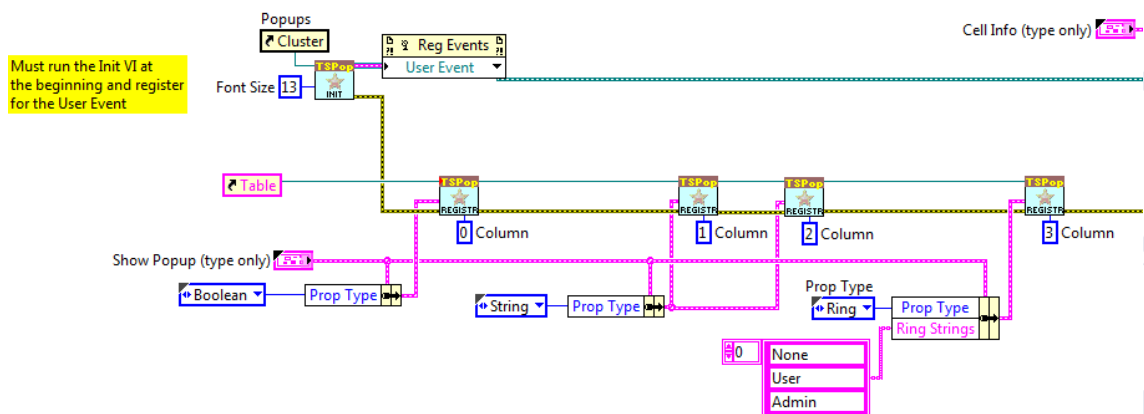


Es uno de los VI más complejos de la librería haciendo uso de la librería *Type Sensitive Popup* (Vis de la derecha en árbol de jerarquía), consta de 2 partes, inicialización y un event structure que realiza diferentes acciones según lo que haga el usuario

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan



70: Arbol de jerarquía de Read Users File



71: Inicialización de Type Sensitive Popup

Inicialización de *Type Sensitive Popup*, indicamos que campos de la tabla pueden ser editados en tiempo de ejecución y mediante que método.

vent structure dentro de un bucle while

finalización de procesos, que es lo que se ha puesto al final del bu-

78

unizar.es



The screenshot shows a LabVIEW front panel with a yellow and black striped border. At the top center is a 'Timeout' control with a dropdown menu set to '[0]'. On the left side, there is a 'Time' indicator. A green 'T' icon is located on the right side of the panel, with a dashed line connecting it to a red circle icon in the bottom right corner. The background features a large, faint watermark that reads 'NATIONAL INSTRUMENTS' and 'LabVIEW Student Edition'.

La librería exige una finalización de procesos, que es lo que se ha puesto al final del bucle while.

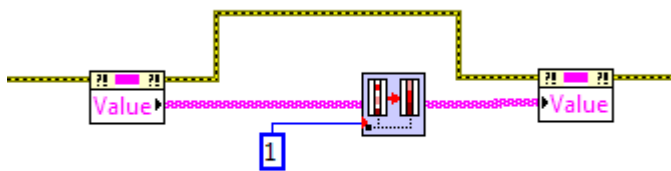
Run at the end of the program to close down the monitoring VI that runs in parallel.



74: Finalizacion de Type Sensitive Popup

Dentro de la estructura gestionada por eventos se han creado 9 diferentes, 2 de ellos necesitados por *Type Sensitive Popup* para su correcto funcionamiento, los otros son eventos que responden a las acciones de operario en los botones de la interfaz.

Los botones Z-A/A-Z, ordenan de manera ascendente o descendente los valores de la tabla



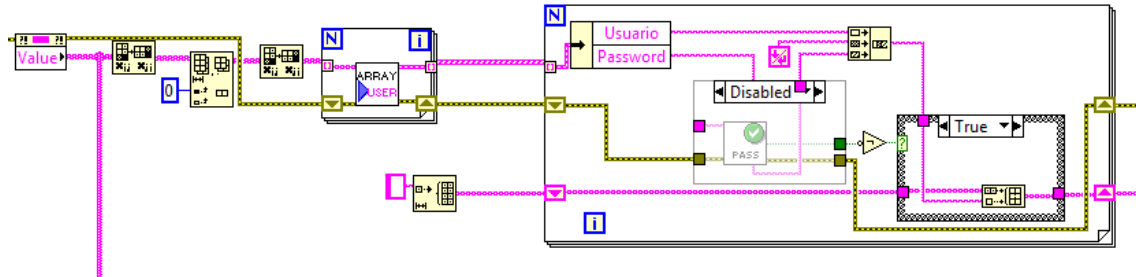
75: Organizador ascendente/descendente

Reload, recarga los datos del archivo y cancel hace que volvamos a la ventana del terminal de explotación y borrar elimina aquellos usuarios que tengan en la primera casilla marcado como true.

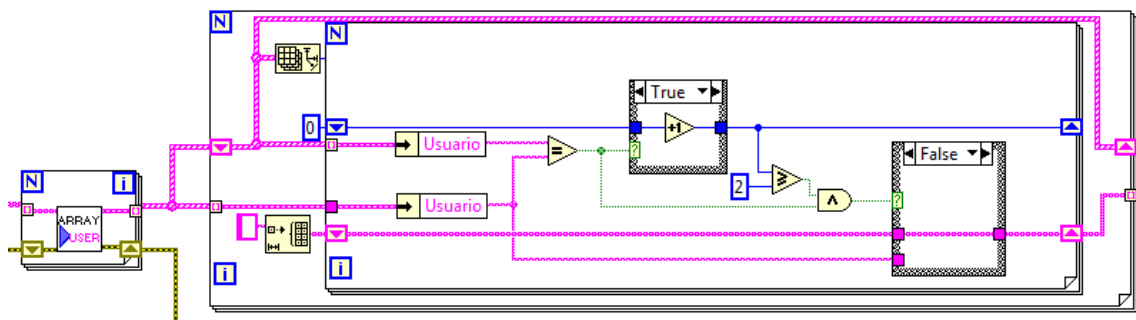
El evento más importante es *check changes and save*, que es el que se encarga de comprobar la integridad de los datos devueltos por el programa, realizando las mismas comprobaciones que se hacen cuando se crea un usuario (que la contraseña sea segura y que no existan duplicados) pero de una forma mucho más compleja debido a que no solo se ha de comprobar el nuevo usuario, sino todos los usuarios; el diagrama

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

contiene la completitud del código pese a que no debería, esto se subsanará en futuras versiones.

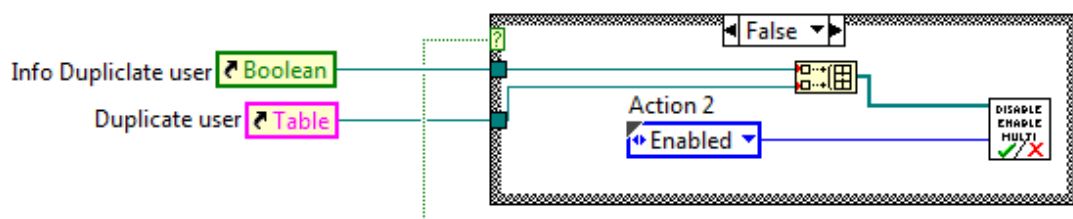


76: Comprobación de que no hay usuarios con contraseñas débiles



77: Comprobación de que no hay nombres de usuario duplicados

Otra característica de este VI es que las tablas de la derecha en el panel frontal se muestran o esconden dependiendo de si existen errores o no.



78: DisableEnable_mono en Read User

12.4.8 Log creator y Pswd creator

Son 2 VI que se hicieron para la asistencia mientras se programaba la librería, pero como fueron suficientemente útiles se mantienen para el futuro, sirven ambos para crear un archivo con una primera incidencia primero y un primer usuario el segundo.

Pswd creator es imprescindible para el funcionamiento de la librería ya que la creación del primer usuario, cuando el terminal de explotación está en funcionamiento, es imposible (puesto que se necesita un usuario con credenciales de administrador para poder crear el primer usuario); esto obedece a la posible necesidad por parte de futuros usuarios de la librería que cierren su código para que no se pueda usar si no se les entrega el fichero con el primer usuario creado, esto se podría haber solventado pidiendo la creación del usuario en el momento en el que no hubiera ninguno previamente en el fichero log.txt o incluyendo un usuario por defecto.

12.4.9 Otros SubVIs

Existen varios Vis sueltos en la carpeta raíz que pueden ser útiles a la hora de usar esta librería *Config privileges*, *DisableEnable*, *DisableEnable_mono* y *Gmail*, los 3 primeros hacen uso del tipo de dato *Hyde&Show*, siendo el primero configurable para hasta 3 tipos de usuario diferente pudiendo decidir que ve y que no ve cada uno, el segundo y el tercero son iguales, pero uno acepta un Array de referencias (VI server reference) y el otro sólo una, el último no ha sido utilizado pero se encontró mientras se hacía una búsqueda por los foros de National Instruments y se consideró que podía ser útil para usuarios de esta librería, dentro del archivo se encuentra el enlace al comentario del autor del VI.

12.4.10 Miscelánea y reusable

Son 2 carpetas que contienen SubVIs, la primera contiene VIs que son usados en el proyecto pero que, por sus funciones, no pueden ser agrupados juntos con otros y la segunda carpeta contiene aquellos VIs que son usados en este proyecto y que son susceptibles de ser usados independientemente de esta librería, son en su mayoría VIs relacionados con la búsqueda, selección o eliminación de filas o columnas dentro de matrices, también hay otra carpeta con los SubVI relacionados con el manejo del tiempo.

12.4.11 Tipos de datos internos

12.4.12

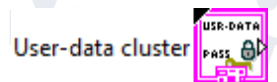


Account: tipo de dato que tiene como valores los 3 tipos de usuario creado (*None*, *User* y *Admin*).

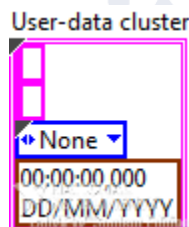
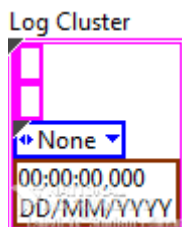
79: *Account*

(icono)

Log Cluster y *User data Cluster* son los tipos de datos que la librería utiliza para almacenar los usuarios y los log dentro del programa, la estructura de ambos datos es idéntica y consta de 2 datos de tipo string (nombre y clave en *User Data Cluster* y Nombre y acción en *log Cluster*), el rol del usuario y la fecha (en el log se almacena la fecha en la que se ha creado la entrada y en *User Data* la fecha de la creación del usuario).



80: *User-Data Cluster* y *Log Cluster* (iconos)



81: Comparación entre *Log cluster* y *User-Data Cluster*

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

A la hora de guardar los datos en el fichero de texto los datos tipo time_stamp y account han de ser convertidos a cadena de caracteres, para ellos se crearon 3 Vis (la conversión de time_stamp a cadena de caracteres tiene un VI por defecto en la instalación de LabVIEW).



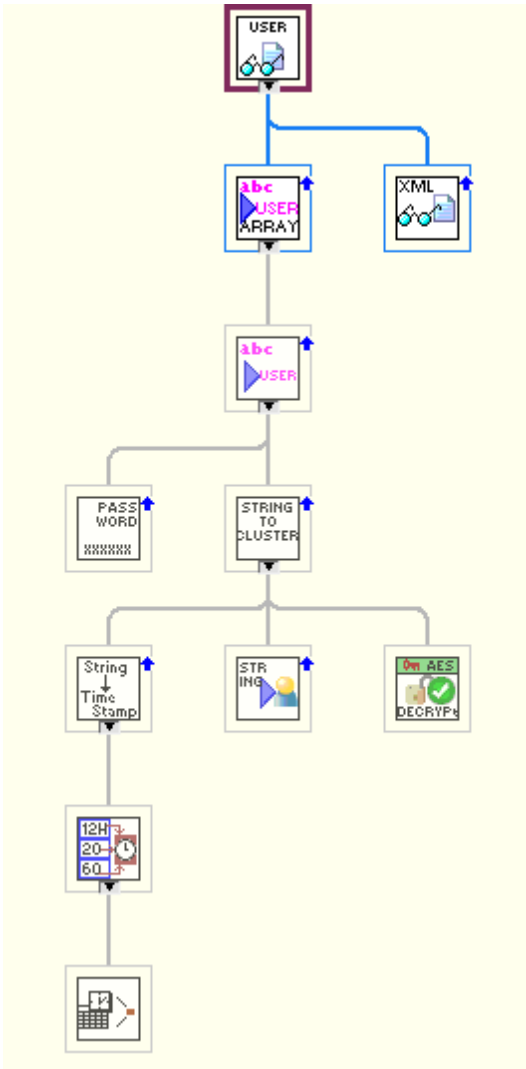
82: Vis de conversión de datos

12.4.13

Estructura de la librería

La estructura de los VI que se usan para almacenar los usuarios y el log son iguales, compartiendo VI a nivel interno, mientras que en el tipo *User-data Cluster* lo que se cifra son todos los datos (nombre, clave, rol, fecha), en Log Cluster se cifra, además, la segunda cadena de caracteres se llama data.

Las razones para hacer esto es que data puede ser solo unas pocas de cadenas de texto (numero de intentos entre 0 y 4, [Nombre Usuario] se ha añadido, etc) y porque los usuarios se repiten (un usuario puede realizar diferentes acciones todas ellas susceptibles de almacenarse) por lo que un simple intercambio de ficheros y un ataque de fuerza bruta podrían ser suficientes para entrar, además, la separación da pie a que en un futuro cada parte se desarrolle independientemente.



:83 Arbol de jerarquía de Read Users File

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

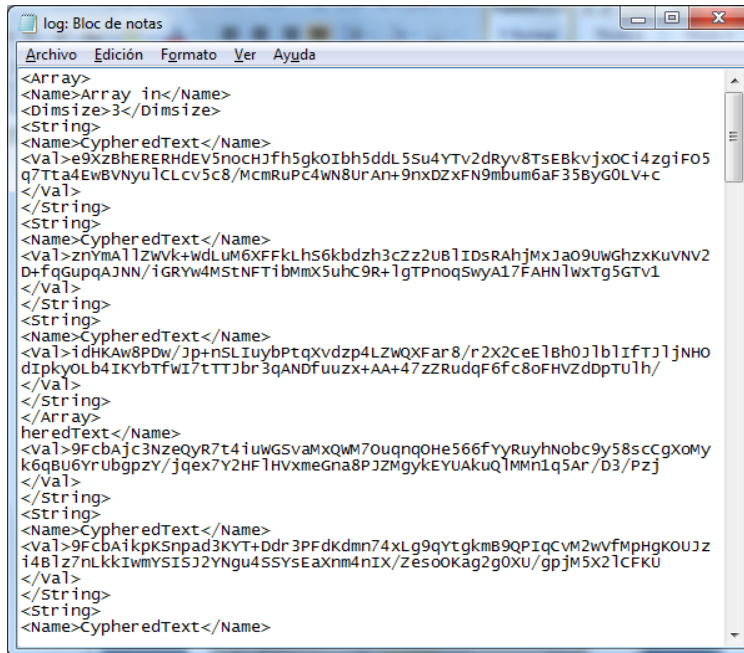


84: Iconos de los VIs de gestión de usuarios

Esto son los iconos de los 6 VI utilizados para gestionar los datos de usuario, y, exceptuando get UDcluster, que sirve para adquirir datos introducidos por el operario en el panel frontal, el resto tienen su equivalente para la gestión de log Cluster.

- ABC: formato listo para escribir (es decir, una sola cadena de caracteres)
- User: Cluster de dato usuario
- Array User: vector formado por Users.
- Array ABC: vector con los 4 parámetros del Cluster pasados a cadena de caracteres

12.4.14 Log.txt y Usuarios.txt



Los usuarios se guardan en una estructura XML (se usó XML en vez de JSON debido a que JSON es solo requerimiento para la comunicación otros proyectos y Log.txt y Usuario.txt son de uso interno, pero se podría cambiar de uno a otro fácilmente).

85: fichero de log

```
<Array>
<Name>Array in</Name>
<Dimsize>3</Dimsize>
<String>
<Name>CypheredText</Name>
<Val>e9XzBhERERHdEV5nocHJfh5gk0Ibh5ddL5Su4YTv2dRyv8TsEBkvjxOCi4zgiFO5
q7Tta4EwBVNyulCLcv5c8/McmRuPc4WN8UrAn+9nxDZxFN9mbum6aF35ByG0LV+c
</Val>
</String>
```

Array: indica que el fichero es un Array.

Name: Nombre del Array.

Dimsize: numero de datos en el Array (dimensión del Array).

String: tipo de dato.

Name: nombre del string.

Val: valor del string.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Tanto para la escritura del log como de los usuarios se hace uso de unos Vis que son equivalentes, otros elementos comunes a ambos grupos de Vis son log file name y y cipher log (y sus análogos user file name y cipher log), el primero almacena la URI a donde está el archivo y el segundo almacena la clave con la que cada tipo de datos se cifra.

Log tambien dispone de add to log, que añade un dato al final del fichero y 2 VI obtenidos de internet que obtienen las posiciones del raton en la pantalla y cuando hace clic, serán usados en un futuro para obtener en que botones ha pulsado el usuario (o que acciones ha realizado).



86:log file +1

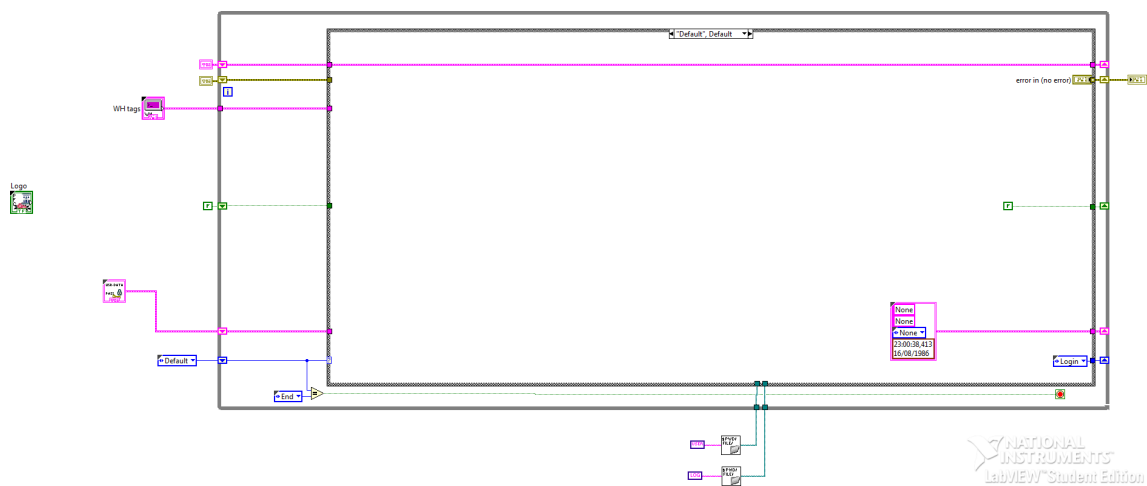
Por otra parte Users dispone de 2 VI, uno llamado Hard pass para comprobar que la clave (creada o modificada) y otro llamado User Exists, que compara un Array de Users con una cadena de caracteres que ha de contener el posible usuario, devolviendo un valor booleano (verdadero si existe, falso si no).



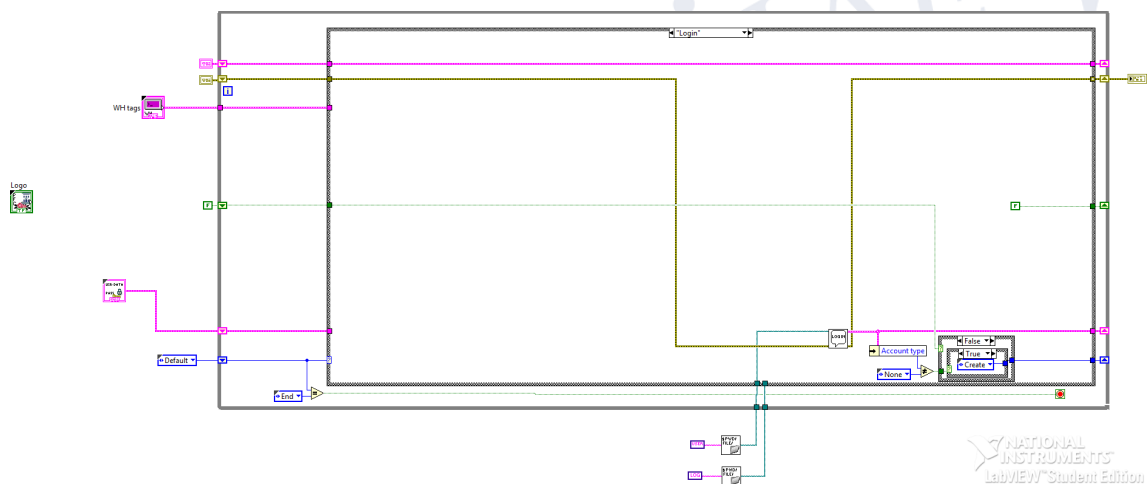
87: hardpass y User exists

12.5 Programa Principal

Primero se van a mostrar imágenes de los diferentes estados por los que pasa el flujo del programa, con el flujograma anterior y los nombres identificativos dentro de cada evento es fácil de seguir.



88: Default

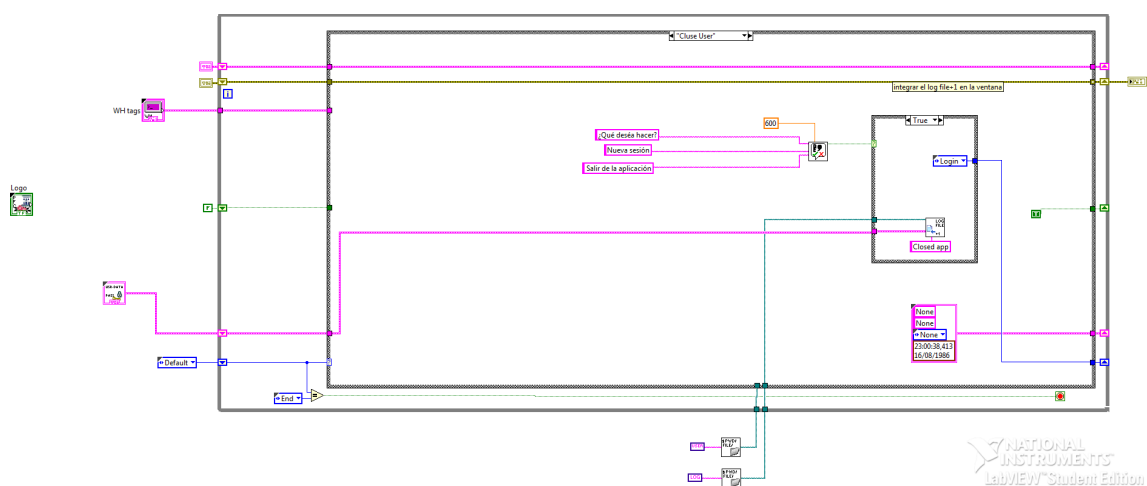


89: Login

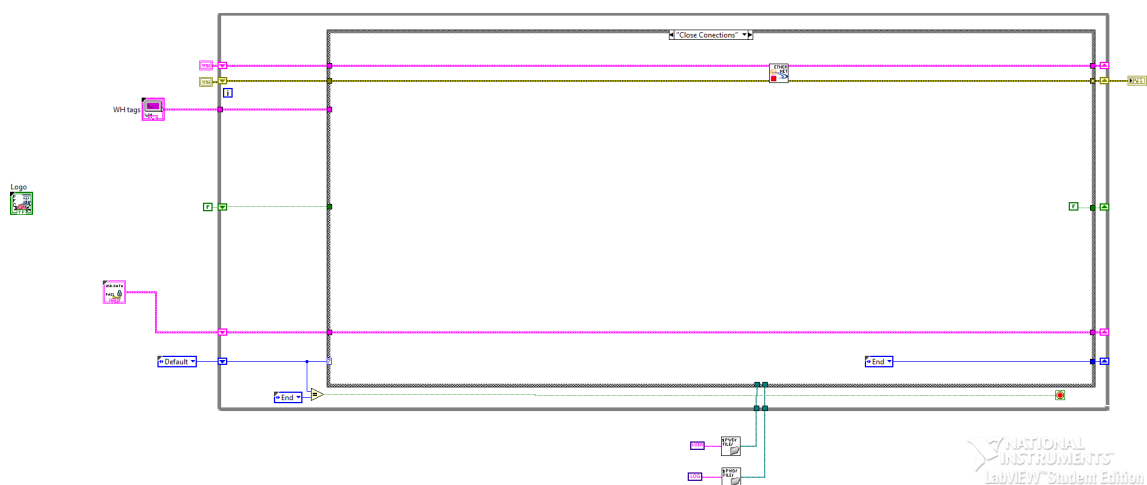
The diagram illustrates a LabVIEW program for a user login system. It features a 'User' dropdown menu, an 'Account type' dropdown menu, and a 'Disabled and Grayed Out' indicator. The 'Admin Options' section includes a 'None' button and a 'Running' button. A 'configured para 30 minutos' label is present. The program uses a 'Wait' block to pause execution for 30 minutes. A 'NATIONAL INSTRUMENTS LabVIEW Student Edition' watermark is visible in the background.



Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

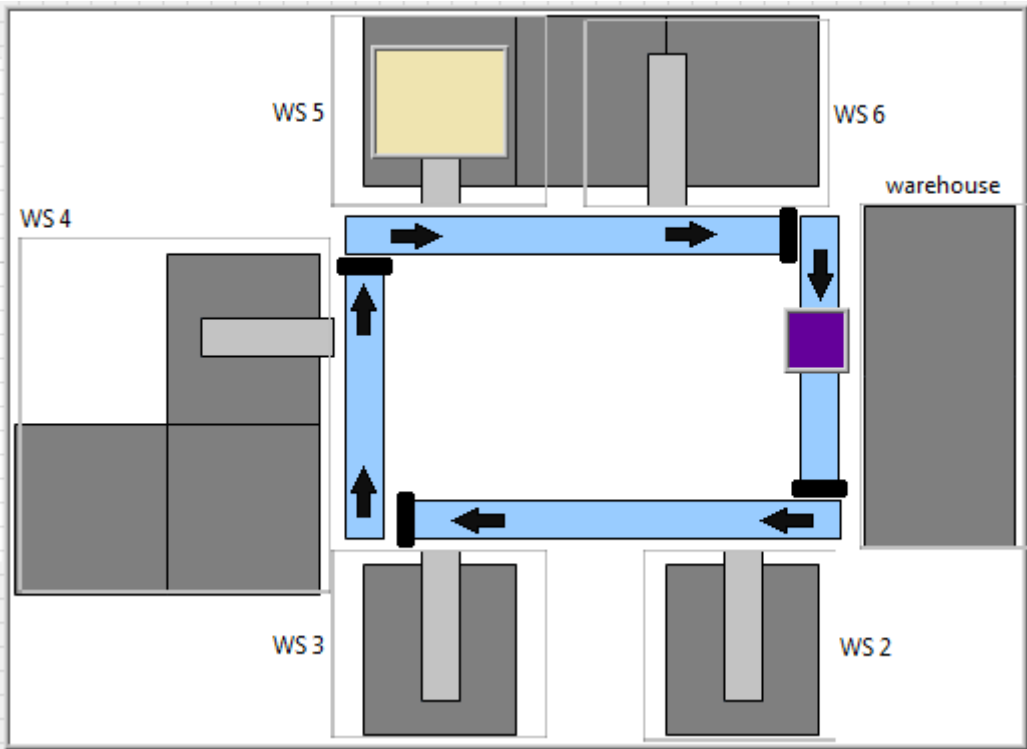


92: Close Cluster

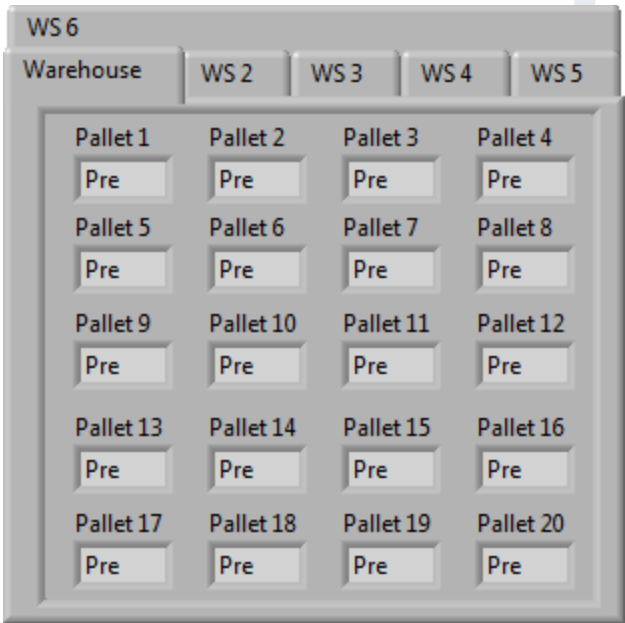


93: Close connections

12.5.1Estaciones de trabajo



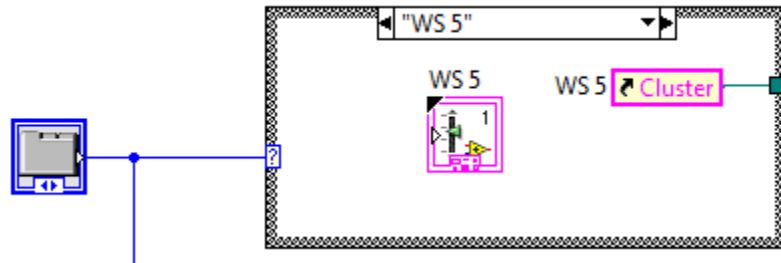
94: Vista de planta de TiM en el Terminal de explotación



Con la estación de trabajo se puede interactuar tanto clicando en las pestañas como haciendo click encima de la estación que se quiere ver.

95: pestañas para seleccionar las diferentes estaciones de trabajo

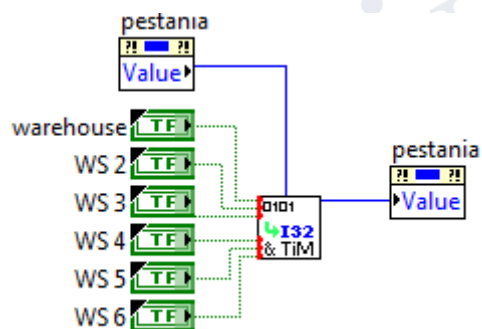
Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan



:96 como están conectadas las pestañas a un case structure

Para poder seleccionar seleccionando en cada estación de trabajo se creó un VI que convertía de digital a analógico, siendo cada botón una potencia de 2, así para activar la WS3 el valor que devolverá será 2^3 que internamente selecciona dicha pestaña a través del *property node*.

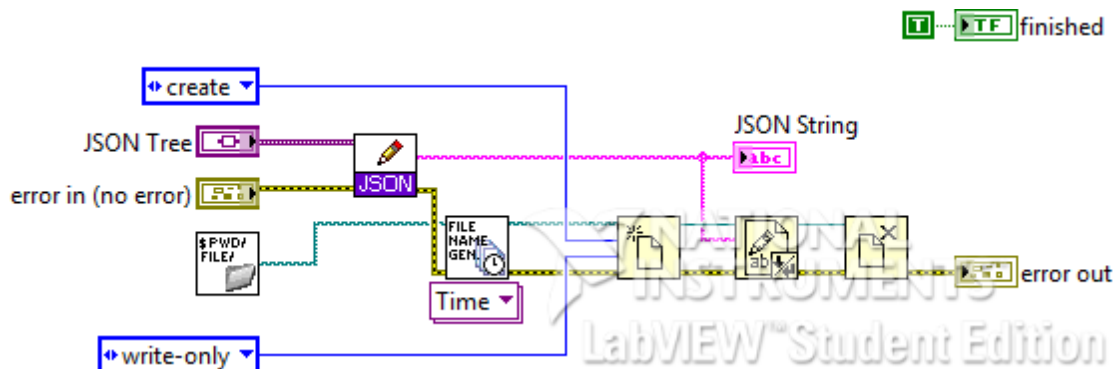
En caso de que por un mal funcionamiento se diese un número que no fuera potencia de 2, la salida nos daría el valor actual.



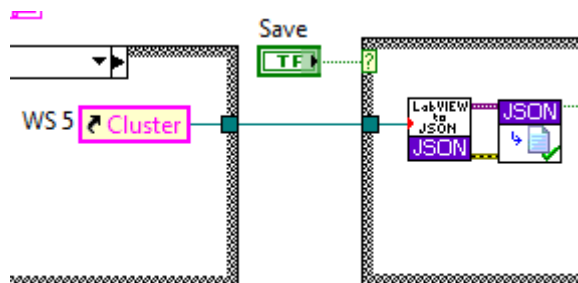
97: VI de adquisición de dibujo pulsado.

12.5.2 Exportación de datos

Para exportar los datos se ha creado un VI que tiene la estructura de la siguiente imagen.



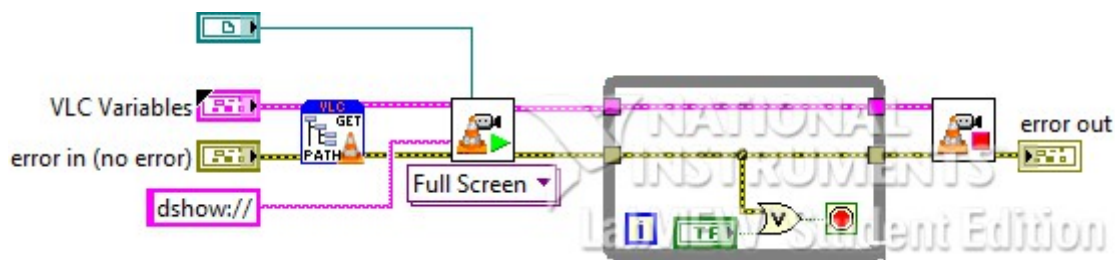
98: Para pasar los datos al VI se hace uso de un VI server Deference para que así el VI sea genérico



12.6 Vídeo

La llamada al VI del video se hace mediante un case structure.





13.- Conclusiones

13.1 Análisis del resultado

El resultado ha sobrepasado mis expectativas, consiguiendo realizar un terminal de explotación usable e iniciando 2 bibliotecas de VI que pueden ser utilizadas libremente y que pueden servir de referencia de cómo me desenvuelvo programando en el entorno LabVIEW.

Ha quedado pendiente el terminar unos VI para el mejor manejo de los datos adquirido, se pretende terminar antes de la defensa del proyecto.

13.2 Trabajo futuro

A día de hoy, más de año y medio después de mi vuelta de la Universidad de Central Lancashire desconozco a ciencia cierta como está el proyecto de TiM.

Lo recomendable sería integrar dentro de la interfaz los proyectos del laboratorio en vez de realizar una comunicación mediante ficheros JSON, la realización de Wrapping con OpenCV sería un buen primer paso.

Con respecto a lo que he desarrollado en este proyecto se intentará completar las librerías LabVIEW VLC y la librería de control de accesos que considero muy interesante tanto por el hecho de que no haya librerías libres del mismo tipo como por que al estar en github pueden ser accedidas y modificadas por otros programadores.

Índice de ilustraciones

1: Centre for Advanced Digital Manufacturing Technologies.....	4
2: Célula de fabricación TiM.....	7
3: Típica arquitectura de un sistema SCADA (Kruz, 2005).....	10
4: Arquitectura SCADA real. Ejemplo del ICS-CERT del gobierno americano (ICS-CERT, s.f.).....	11
6: Ordenamiento de burbuja en LabVIEW (NI.com, 2010).....	14
10: Arquitectura de TiM.....	16
12: Cambios realizados a la arquitectura TiM original.....	18
14: Diagrama de bloques de la lectura de datos de una red Ethernet/IP mediante EtherNet_IP_CIP.....	21
15: VI de lectura de datos mediante EtherNet_IP_CIP.....	21
17 : Diagrama de bloques de la lectura/escritura de datos en Ethernet/IP.....	22
18: Fotos y pantallas de la interfaz de TiM.....	25
19: Función nativa en LabVIEW que guarda una cadena en formato XML (NI.com, 2012).....	30
20: Escritura de datos en un fichero JSON.....	31
22: Ejemplo con Robolab.....	35
23:Ejemplo con las DLL de VLC (GriffinRU, 2012).....	35
24: Ejemplo con AD Vision Toolkit.....	36
25: Distribución de las vulnerabilidades reportadas al ICS-CERT en 2013 (National Cybersecurity and Communication Integration Center, 2014).....	40

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

26: Gravedad de las vulnerabilidades reportadas al ICS-CERT en 2013 (National Cybersecurity and Communication Integration Center, 2014).....	40
27: Paleta de Crypto-G toolkit.....	44
28: Ejemplo con Encryption V 1.0.....	44
29: Ayuda de AES Library for LabVIEW.....	45
31: Ejemplo con AES Toolkit.....	47
32: Paleta de Crypto-tools.....	47
33: Ejemplo de Encrytion Compendium.....	48
34: Simple LabVIEW User Log-In.....	49
35: Ejemplo de MarisolM.....	50
36: Ejemplo de UtoTEC.....	50
37: Ejemplode Biometric Login toolkit.....	51
38: Secure Login Framework.....	51
39: Ejemplo de búsqueda en Shodan (Moreno, 2014).....	54
40: FileName Generator.....	55
41: Type Sensitive Popup.....	55
42: Leyenda de la tabla comparativa.....	58
43: Tabla comparativa entre licencias libres.....	59
44: Flujograma inicial.....	61
45: Flujograma del programa.....	62
46: Librería Ethernet/IP.....	63
47: Read_Core.....	63

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

48: Ethernet_CIPScan_Registers.....	64
49: ejemplo del polimorfismo.....	65
50: Comapración de las ayudas de la librería antes y ahora.....	65
51: error ml implementado.....	66
52: nuevo error.....	66
53: Ejemplo con la librería tal y como la encontramos en internet.....	67
54: Ejemplo con la librería NI-Industrial Communications para EtherNet/IP 1.2.1.....	67
55: Ejemplo con la librería al final de todo el porceso.....	68
56: Comparación de iconos de la librería de Ethernet.....	68
57: Librería LabVIEW VLC.....	69
59: Ayuda de VLC State.....	69
58: Ayuda de VLC Var.....	69
60: Obtencion de la carpeta donde está.....	70
61: Vídeo a pantalla completa.....	70
63: Cierre de la conexión con la webcam.....	71
64: Ejemplo con Robolab.....	71
65: Ejemplo con la librería creada.....	71
66: Ayuda dentro dle programa de varios de los VIs creados.....	72
67: Script para la conversión a formato MP4.....	73
68: Librería de control de accesos.....	74
69: Panel frontar de Read Users File.....	76

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

70: Arbol de jerarquía de Read Users File.....	77
71: Inicialización de Type Sensitive Popup.....	77
72: Lectura del fichero de usuarios.....	78
73: Ejemplo de un envent structure dentro de un bucle while.....	78
74: Finalizacion de Type Sensitive Popup.....	79
75: Organizador ascendente/descendente.....	79
76: Comprobación de que no hay usuarios con contraseñas débiles.....	80
77: Comprobación de que no hay nombres de usuario duplicados.....	80
78: DisableEnable_mono en Read User.....	80
79: Account (icono).....	82
80: User-Data Cluster y Log Cluster (iconos).....	82
81: Comaración entre Log cluster y User-Data Clusted.....	82
82: VIs de conversión de datos.....	83
:83 Arbol de jerarquía de Read Users File.....	84
84: Iconos de los VIs de gestión de usuarios.....	85
85: fichero de log.....	86
86:log file +1.....	87
87: hardpass y User exists.....	87
88: Default.....	88
89: Login.....	88
90: Create.....	89

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

91: Running.....	89
92: Close Cluster.....	90
93: Close conections.....	90
94: Vista de planta de TiM en el Terminal de explotación.....	91
95: pestañas para seleccionar las diferentes estaciones de trabajo.....	91
:96 como están conectadas las pestañas a un case structure.....	92
98: Definición de Tag.....	2
99: Estructura de acceso de datos.....	3
100: Tags al alcance del controlador.....	4
101: Tipos de Datos.....	4
102: Tamaño en Bits de cada tipo de dato.....	5
103: Tipos de datos entero booleano, doble entero, entero largo en RSLogix5000.....	6
104: Tipo de dato Alarma en RSLogix5000.....	7
106: Matriz en RSLogix5000.....	8
107: diferencia entre estructuras y matrices.....	9
108: Organización de datos en memoria para mejorar su uso.....	11
109: Frecuencia de los diferentes ataques en las empresas del estudio (Ponemon, 3013).....	1
110: Media anual del coste para cada sector (Ponemon, 3013).....	1
112: Informe de riesgos mundiales de 2014 (World Economic Forum, 2014).....	2
113: Informe de riesgos mundiales de 2014 (II) (World Economic Forum, 2014).....	3
114: Curva típica de coste de cambio en un proyecto software. (Ambler, s.f.).....	6

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

115: Distribución de los SO en los ordenadores industriales (IMS Research, 2013).....	8
116: Arquitectura típica con 2 cortafuegos (ICS-CERT, s.f.).....	10
117: (Munroe, s.f.).....	15
118: Diferentes formas de implementar las contraseñas. (Dinei Florencio, 2014).....	16
119: Login.....	1
120: New user.....	2
121: Read Users.....	3
122: Interfaz principal.....	4
123: Flujograma final.....	5
124: flugrama inicial.....	5
125: Read log.....	7
126: Read users.....	7

14.- Bibliografía

ADMT, 2014. *Advanced Digital Manufacturing Technology Research Centre (ADMT)*. [En línea]

Available at: http://www.uclan.ac.uk/research/explore/groups/centre_advanced_digital_manufacturing_technologies.php

Ambler, S. W., s.f. *Agile Modeling*. [En línea]

Available at: <http://www.agilemodeling.com/essays/costOfChange.htm>

Anon., s.f. *Comparison of free and open-source software licenses*. [En línea]

Available at: http://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses

AutoTEC, 2008. *How to create login and password for my application*. [En línea]

Available at: <http://forums.ni.com/t5/LabVIEW/how-to-create-login-and-password-for-my-application/m-p/787259/highlight/true#M359694>

Berkeley, s.f. *BSD 4-clause "Original" or "Old" License*. [En línea]

Available at: <https://spdx.org/licenses/BSD-4-Clause>

Berkeley, U., 1999. *New BSD*. [En línea]

Available at: <http://choosealicense.com/licenses/bsd-3-clause/>

Blue Ridge Test , s.f. *Biometric Login Toolkit - Blue Ridge Test*. [En línea]

Available at: <http://sine.ni.com/nips/cds/view/p/lang/es/nid/209106>

Blume, P. A., 2007. *The LabVIEW style book*. s.l.:Prentice Hall.

BOE, 2011. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección. *Boletín Oficial del Estado*, 28 Abril, pp. 43370-43380.

BOE, 2011. Reglamento de protección de las infraestructuras críticas. *Boletín Oficial del Estado*, 21 Mayo, pp. 50808-50826.

Boyer, S., 1999. *Scada: Supervisory Control and Data Acquisition*. s.l.:Isa.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

canming, 2014. *Emgu CV*. [En línea]

Available at: <http://sourceforge.net/projects/emgucv/>

CEEO, 2013. *ROBOLAB for LabVIEW*. [En línea]

Available at: <http://www.legoengineering.com/robolab-for-labview/>

Centro de Ciberseguridad Industrial, 2012. *Mapa de Ruta Para la Ciberseguridad en España*, s.l.: s.n.

daarwin, 2013. *ocv2lv*. [En línea]

Available at: https://github.com/daarwin/ocv2lv/tree/master/ocv2lv_dll

Dmitriev, A., 2010. *LabVIEW InsightsAD Vision Toolkit*. [En línea]

Available at: <http://vi-lib.com/>

Eran Herman Engineering , 2013. *OpenCV 2.4.6 Wrapper*. [En línea]

Available at: https://www.ehe-lab.com/OpenCV_Wrapper.html

FSF y GNU, s.f. *What is free software? The Free Software Definition*. [En línea]

Available at: <http://www.gnu.org/philosophy/free-sw.en.html>

GNU, s.f. *GNU LGPL v2.1*. [En línea]

Available at: <http://choosealicense.com/licenses/lgpl-2.1/>

GriffinRU, 2012. *VLC scripting in LabVIEW*. [En línea]

Available at: <https://decibel.ni.com/content/docs/DOC-24114/>

HYtek Automation, s.f. *IVision LabVIEW Toolkit 2.2*. [En línea]

Available at: <http://www.hytekautomation.com/Products/IVision.html>

i3 JSON, 2012. *Interactive Internet Interface: JSON Toolkit for LabVIEW*. [En línea]

Available at: <https://decibel.ni.com/content/groups/interactive-internet-interface-json-toolkit-for-labview>

ICS-CERT, 2011. *ICSB-11-327-01 - ILLINOIS WATER PUMP FAILURE REPORT*. [En línea]

Available at: <https://ics-cert.us-cert.gov/tips/ICSB-11-327-01>

ICS-CERT, 2013. *Rockwell Automation ControlLogix PLC Vulnerabilities*. [En línea]
Available at: <https://ics-cert.us-cert.gov/advisories/ICSA-13-011-03>

ICS-CERT, 2013. *Rockwell Automation FactoryTalk and RSLinx Vulnerabilities (Update A)*. [En línea]
Available at: <https://ics-cert.us-cert.gov/advisories/ICSA-13-095-02A>

ICS-CERT, 2014. *Rockwell RSLogix 5000 Password Vulnerability*. [En línea]
Available at: <https://ics-cert.us-cert.gov/advisories/ICSA-14-021-01>

IMS, I., s.f. *Secure Login Framework - IMS, Inc.*. [En línea]
Available at: <http://sine.ni.com/nips/cds/view/p/lang/es/nid/211427>

JodyK, T. P. y., 2011. [CR] *Encryption*. [En línea]
Available at: <http://lavag.org/topic/14889-cr-encryption/>

jtagg, 2012. *Filename generator for LabVIEW*. [En línea]
Available at: <https://decibel.ni.com/content/docs/DOC-14791>

Klemen, 2014. *Create a Visual Studio project from source files using Cmake (OpenCV and PCL)*. [En línea]
Available at: <https://decibel.ni.com/content/blogs/kl3m3n/2014/04/22/create-a-visual-studio-project-from-source-files-using-cmake-opencv-and-pcl>

Klemen, 2014. *Point cloud library (PCL) and Open Computer Vision (OpenCV) toolkit for labview*. [En línea]
Available at: <https://decibel.ni.com/content/blogs/kl3m3n/2014/09/05/point-cloud-library-pcl-and-open-computer-vision-opencv-toolkit-for-labview>

Krutz, R., 2005. *Securing SCADA Systems*. s.l.:Wiley.

Lauper, A., 2012. *Cryptography*. [En línea]
Available at: <https://decibel.ni.com/content/docs/DOC-22585>

Lauper, A., s.f. *Kryptographie*. [En línea]
Available at: <http://www.wingover.ch/Kryptographie/>

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

lavezza, 2011. *LabVIEW and windows authentication*. [En línea]
Available at: <http://lavag.org/topic/15260-labview-and-windows-authentication/?p=92010>

LVS-Tools , s.f. *Encryption Compendium for LabVIEW by LVS-Tools*. [En línea]
Available at: <http://sine.ni.com/nips/cds/view/p/lang/es/nid/212735>

MarisolM, 2013. *User log-in with password from Database*. [En línea]
Available at: <https://decibel.ni.com/content/docs/DOC-30425>

MIT, s.f. *MIT License*. [En línea]
Available at: <http://choosealicense.com/licenses/mit/>

Morant, X., 2013. *Security ar(t) work*. [En línea]
Available at: <http://www.securityartwork.es/2013/09/23/scada-e-internet-una-pareja-mal-avenida-i>

Moreno, M., 2014. *Shodan Reports*. [En línea]
Available at: <http://www.securityartwork.es/2014/09/12/shodan-reports/>

Muñoz, D., 2011. *Biblioteca AES (Advanced Encryption Standard) para LabVIEW*. [En línea]
Available at: <http://www.soslabview.com.ar/es/biblioteca-aes-labview>

National Cybersecurity and Communication Integration Center, 2014. *ICS-CERT Monitor Jan-April*, s.l.: U.S. Department of Homeland Security.

NI.com, 2009. *Password Protect LabVIEW Applications at Run-Time*. [En línea]
Available at: <http://digital.ni.com/public.nsf/allkb/A3A3312AAEF4CC5286257558007E8B22>

NI.com, 2010. *Can LabVIEW C?*. [En línea]
Available at: <http://www.ni.com/white-paper/2718/en/>

NI.com, 2012. *Flatten To XML Function*. [En línea]
Available at: <http://zone.ni.com/reference/en-XX/help/371361J->

01/glang/flatten_to_xml/

[Último acceso: 2014].

NI.com, 2012. *MODBUS Library for LabVIEW*. [En línea]

Available at: <http://www.ni.com/example/29756/en/>

NI.com, 2014. *NI-Industrial Communications for EtherNet/IP 14.0*. [En línea]

Available at: <http://www.ni.com/pdf/manuals/374775a.html>

NI.com, s.f. *Software NI Vision Acquisition*. [En línea]

Available at: sine.ni.com/nips/cds/view/p/lang/es/nid/12892

NIST, 2001. *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*. [En línea]

Available at: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

NSA, 2009. *Suite B Cryptography*. [En línea]

Available at: https://www.nsa.gov/IA/Programs/suiteb_cryptography/

Plomp, T., 2011. *Download Encryption V 1.0*. [En línea]

Available at: <http://lavag.org/files/file/198-encryption/>

Ponem, 2013. *2013 Cost of Cyber Crime Study*, s.l.: s.n.

RER, 2012. *Simple LabVIEW User Log-In Demo (Admin and Operator User Accounts)*.

[En línea]

Available at: <https://decibel.ni.com/content/docs/DOC-21163>

Rockwell Automation, s.f. *Datos de tags y E/S en los controladores Logix5000*. [En línea]

Available at:

http://literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm004_-es-p.pdf

Sabtu, 2010. *Combining Intel OpenCV and NI Labview*. [En línea]

Available at: <http://machine-vision-adhiguna.blogspot.com.es/2010/10/combining-intel-opencv-and-ni-labview.html>

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

SAPHIR, s.f. *Sine.ni.com.* [En línea]

Available at: <http://sine.ni.com/nips/cds/view/p/lang/es/nid/209754>

Saunders, D., 2007. *Type Sensitive Popup.* [En línea]

Available at: <http://lavag.org/files/file/31-type-sensitive-popup/>

SecurityFocus, 2003. *Slammer worm crashed Ohio nuke plant network.* [En línea]

Available at: <http://www.securityfocus.com/news/6767>

ShaneDonn, 2013. *LabVIEW and VLC - My Go.* [En línea]

Available at: <https://decibel.ni.com/content/docs/DOC-26397>

Siva, 2007. *Industrial EtherNet (EtherNet/IP).* [En línea]

Available at: <http://lavag.org/topic/6104-industrial-ethernet-ethernetip/?p=35402>

Siva, 2012. *LabVIEW_EtherNET_IP.* [En línea]

Available at: https://github.com/sivamgr/LabVIEW_EtherNET_IP

Symantec, 2010. *Hydraq - An Attack of Mythical Proportions.* [En línea]

Available at: <http://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions>

Symantec, 2013. *Hidden Lynx – Professional Hackers for Hire.* [En línea]

Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/white_papers/hidden_lynx.pdf

Titov, I., s.f. *Advanced Encryption Standard (AES) in LabVIEW.* [En línea]

Available at: <http://vigods.com/toolkits/security/aes.html>

US-CERT, 2010. *USB USAGE.* [En línea]

Available at: <https://ics-cert.us-cert.gov/tips/csar-10-114-02>

US-CERT, s.f. *Overview of Cyber Vulnerabilities.* [En línea]

Available at: <https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities>

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

VARTOR, s.f. *Crypto-G*. [En línea]

Available at: <http://www.vartortech.com/cryptog.html>

VLC, s.f. *VLC Documentation*. [En línea]

Available at: <http://www.videolan.org/developers/vlc/doc/doxygen/html/>

World Economic Forum, 2014. *Global Risks 2014 Ninth Edition*, s.l.: World Economic Forum.

XIMEA Corp., s.f. *XIMEA API Software Package*. [En línea]

Available at: http://www.ximea.com/support/wiki/apis/XIMEA_API_Software_Package

Diseño del nuevo SCADA para el laboratorio de Tecnologías Avanzadas Digitales de Producción de UCLan mediante LabVIEW



Universidad Zaragoza



Dpto. de Informática e
Ingeniería de Sistemas
Universidad de Zaragoza



Escuela de
Ingeniería y Arquitectura
Universidad Zaragoza

Anexos

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

15.- Anexo A: Licencia comprada

Como se comenta a lo largo de la memoria compré una licencia de LabVIEW para estudiante para mi propio uso, aquí adjunto la factura recibida.

Gmail - Studica Order # 291902 <https://mail.google.com/mail/u/0/?ui=2&ik=8b064ae5bf&view=pt&q=...>

 Noel PI <[redacted]@gmail.com>

Studica Order # 291902
1 message

orders_uk@studica.com <orders_uk@studica.com> 19 October 2012 19:20
To: [redacted]@gmail.com


Studica Ltd.
Unit 15, Brentford Business Centre
Commerce Road
Brentford, TW8 8LG
Tel. 0800 195 1157
Fax. 020 8758 9238
VAT # 912 87 16 20

Invoice
Order Number : **291902**
Order Date : **Oct/19/2012**

Bill To:
Noel Pueyo
Flat: 8A; 51 Marsh Lane
Preston, Lancashire United Kingdom
pr1 8rq
Email: residuohumano@gmail.com
Phone: 07767198609

Ship To:
Noel Pueyo
Flat: 8A; 51 Marsh Lane
Preston, Lancashire United Kingdom
pr1 8rq
Email: [redacted]@gmail.com
Phone: [redacted]

Customer ID	Shipping Method	Payment
310415	FS	Credit Card - Visa, MasterCard, Solo, Switch, Maestro

Qty	Description	Part Number	Unit Price	Extension
1	NI LabVIEW Student Edition - (windows/Mac Download - available to Students & Faculty for lab preparation)	779252-02	£19.00	£19.00

Sub Total: £ 19.00
Shipping: £ 0.00
VAT £ 3.80
Total: £ 22.80
*all prices are in £
GBP*

Important Order Information

Your Order #: 291902
Your Order Date: Oct/19/2012
Your Customer Login: [redacted]@gmail.com

Thank you for your order! We appreciate your business.
Get the newest info on releases, special promotions, sales and resources! [Sign up](#) for our eNewsletter.

Education / NonProfit Verification

To complete your order, you are required to send acceptable verification. This can be done by scanning or taking a digital photograph of one of the following items,

- Dated Current Student Photo ID Card
- Dated Current Faculty Photo ID Card
- Dated Current class schedule
- Dated Letter from your school on your school letterhead
- **NonProfit Organizations should send a copy of their Federal 501(c)3 form**

1 de 2 10/11/2014 6:06

<https://mail.google.com/mail/u/0/?ui=2&ik=8b064ae5bf&view=pt&q=>

16.- Anexo B: Procedimiento de trabajo

En este anexo se explicará cómo se ha procedido a la realización del proyecto.

El presente proyecto se realizó en 2 fases, la primera en la universidad de Central Lancashire y la segunda en la Universidad de Zaragoza.

16.1 Universidad de Central Lancashire

El trabajo se realizó con un portátil Lenovo E530 al que se le instaló LabVIEW Student Edition y con los ordenadores disponibles en el laboratorio del ADMT.

En el portátil se desarrollaba el software que se probaba posteriormente en el laboratorio, hay que añadir que las versiones de LabVIEW no coincidían y esto llevó a tener diferentes problemas como que algunas de las herramientas seleccionadas no podían funcionar en el laboratorio o que al tener que guardarlo con la opción de compatibilidad se des configuraba la organización del proyecto.

Se mantuvieron 2 copias del software, una en local y otra en la nube mediante Google Drive, así como las copias que se guardaba en el ordenador del laboratorio.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

16.2 Universidad de Zaragoza

El proyecto se continuó en la universidad de Zaragoza una vez terminado el convenio Erasmus y se decidió, que ya que se disponía de más tiempo y del mismo modelo de autómatas, el ampliarlo y completarlo, cubriendo aquellos apartados que debido a diferentes problemas no se pudieron tener en cuenta previamente.

16.2.1 Máquina virtual



97: Máquina Virtual utilizada

Las herramientas de programación de los autómatas del laboratorio L0.06 del edificio Ada Byron se encuentran en una máquina virtual por lo tanto se procedió a trabajar con ella.

16.2.2 Tamaño insuficiente

Durante el proceso de instalación de los programas emergió el primer problema, el espacio del disco duro era inferior al necesario, para ello se necesitó ampliarlo (Hoffman, 2012).

Primero se ha de apagar la máquina virtual.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Después abrimos la consola de línea de comandos y cambiamos al directorio donde tenemos instalado Virtual Box (en este caso C:\Program Files\Oracle\ pero puede variar):

```
cd "C:\Program Files\Oracle\VirtualBox"
```

Y a continuación usamos el comando modifyhd [..\Maquina virtual a redimensionar.vdi] --resize [tamaño en bytes].

```
VBoxManage modifyhd "C:\Users\Noel\VirtualBox VMs\Windows XP\Windows.vdi" --resize 81920
```

Otra opción sería:

```
C:\Program Files\Oracle\VirtualBox\VBoxManage modifyhd  
"C:\Users\Noel\VirtualBox VMs\Windows XP\Windows.vdi"  
--resize 81920
```

Una vez ampliado el disco hay que ampliar la partición, para ellos haremos uso de GParted Live CD, una distribución de Linux que dispone de herramientas para redimensionar particiones sin tener que instalarla en el ordenador.

Se carga la ISO en la máquina virtual e inmediatamente tras el inicio arranca GParted pudiendo redimensionar la partición acorde a nuestra necesidad.

Apagamos GParted, quitamos GParted del lector virtual de DC/DVD y arrancamos Windows con la partición con su nuevo tamaño

16.2.3 Webcam no disponible

La webcam que se utilizó para hacer las pruebas es una webcam Logitech 210 USB 2.0 que, pese a que en el sistema anfitrión funcionaba bien, en el huésped no aparecía como dispositivo útil; tras muchos problemas y pruebas se encontró solución en el manual de Virtual Box (Oracle, s.f.), agregar un nuevo filtro USB copiando los datos que del “*administrador de dispositivos*” del sistema anfitrión o haciendo uso del comando “VBoxManage list usbhost”.

Otro problema que se tuvo y que no se consideró muy grave en su momento, pese a que se intentó solventar, fue que la máquina virtual no disponía de MS Paint herramienta simple pero suficientemente completa para la edición de los iconos de los VI creados.

16.2.4 Copias de seguridad

Se mantuvieron 3 copias de seguridad, una en el anfitrión, otra en el huésped y otra en Dropbox.

Las copias entre anfitrión y huésped se realizaban mediante una carpeta compartida y entre ambos y Dropbox mediante el cliente nativo de Windows.

16.2.5 Programas instalados

- LabVIEW: Plataforma de programación visual.
- JKI¹⁵: Gestor de paquetes de instrumentos virtuales (VI)
- VLC¹⁶: Para la creación de la librería que adquiere las imágenes de la webcam.

¹⁵ <http://jki.net>

¹⁶ <http://www.videolan.org>

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

- Quicktime¹⁷: Para realizar pruebas con Robolab para LabVIEW.
- Dropbox: Copia de seguridad de archivos.

16.2.6 Rendimiento de la webcam

Pese a que en un principio se trabajó en la máquina virtual, debido a que la comunicación con la cámara web se hacía a través del huésped resultó bastante lenta, no ofreciendo el mismo rendimiento que si se conectase directamente al sistema operativo, por ello se decidió pasar a trabajar en el anfitrión cuando se programasen VI relacionados con la cámara web en vez de en el huésped.

16.2.7 Otros programas de los que se ha hecho uso

- Dia¹⁸: para la edición de los diagramas.
- MS Word 2007: para escribir este documento.
- MS Paint: Para editar los iconos de los VI y para editar las imágenes de este documento.
- GIMP¹⁹: Para editar todo aquello que MS Paint no podía.

¹⁷ <http://www.apple.com/quicktime/download>

¹⁸ <http://dia-installer.de>

¹⁹ <http://www.gimp.org>

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

17.- Anexo C: Etiquetas

El presente anexo se realizó para suplir la falta de documentación del programa de la célula automatizada y está basado íntegramente en los siguientes documentos ofrecidos por Rockwell Automatiozo.:

- “Datos de tags y E/S en los controladores Logix5000” (Rockwell Automation, s.f.)
- “Produced and consumed tags” (Autimation, Rockwell, s.f.)
- “Logix5000 Controllers Sequential Function Charts” (Rockwell Automation, s.f.)
- “Introduction to Logix Controllers” (Rockwell Automation, s.f.)

También se consultaron, pero no se utilizaron para este documento algunos libros de la serie Hands-On Lab Workbook de Rockwell, concretamente: “Introduction to Logix” (Rockwell Automation, s.f.), “Logix For Programmers I” (Automation, s.f.), “Introduction to EtherNet/IP” (Rockwell Automation, s.f.).

17.1 Logix5000

Los autómatas utilizados para realizar el proyecto pertenecen a la serie CompactLogix que está basada en el sistema operativo Logix5000, por lo tanto todo lo aquí expuesto es válido para el resto de series basadas en el mismo sistema operativo (Controladores CompactLogix, ControlLogix, DriveLogix, FlexLogix o SoftLogix5800).

Los controladores con sistema operativo Logix5000 son programados mediante RSLogix 5000, provisto por Rockwell.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

17.2 Tags

En los controladores Logix5000 los valores de entradas y salidas de los módulos de autómatas se actualizan de forma asíncrona a la ejecución de la lógica, transmitiéndose, entre otros métodos, mediante etiquetas o tags.

Término	Definición
Tag	<p>Un tag es un nombre basado en texto para un área de la memoria del controlador donde se almacenan datos.</p> <ul style="list-style-type: none">• Los tags son el mecanismo básico para asignar memoria, hacer referencia a datos de la lógica y monitorear los datos.• La asignación mínima de memoria para un tag es de cuatro bytes.• Cuando se crea un tag con datos que requieren menos de 4 bytes, el controlador asigna 4 bytes pero los datos solo ocupan la parte que necesitan.

98: Definición de Tag

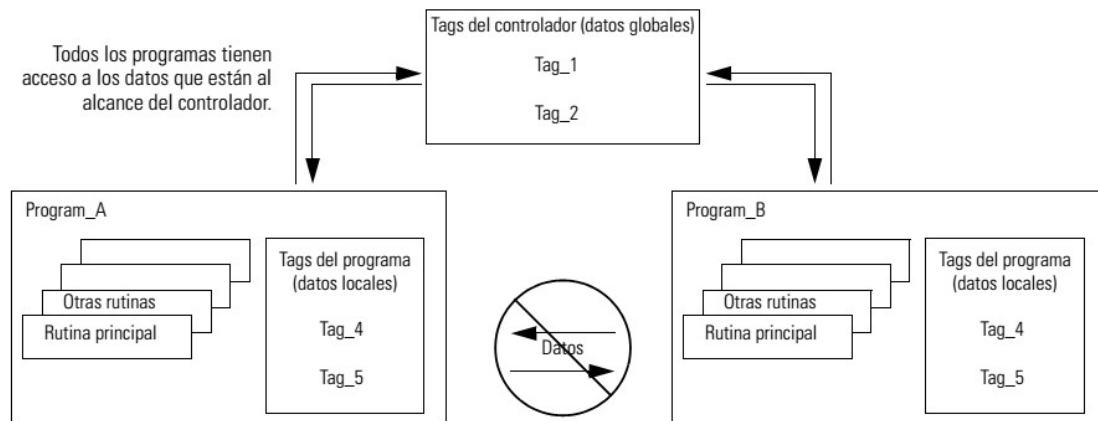
Los programas de una tarea acceden a los datos de entrada y salida a través de los tags almacenados en la memoria del controlador; encaso contrario los datos podrían cambiar durante la ejecución de una tarea haciendo que no funcionase correctamente.

Los tags pueden ser de 4 tipos dependiendo de su función:

- Base: sirven para el almacenamiento interno de los datos dentro del programa.
- Alias: referencia a otro tag existente.
- Producido: Es aquel tag que nuestro controlador utiliza para almacenar valores que va a transmitir a otro controlador.
- Consumido: Es el tag que almacena valores que otro controlador ha generado para este controlador.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Los tags también pueden ser clasificados según su ámbito de utilización, pudiéndose definir como tag del controlador (datos globales) o como tag del programa para un programa específico (datos locales).



99: Estructura de acceso de datos

Esto permite partir la aplicación en diferentes programas, cada uno con sus propios datos, pudiendo duplicar nombres si el ámbito de cada uno está separado; así mismo es recomendable no usar el mismo nombre para un tag de controlador y otro de programa ya que no se puede hacer referencia a un tag de controlador si hay otro con el mismo nombre dentro del programa

Algunos tags, según su función, han de estar obligatoriamente al alcance del controlador tal y como se ve en la tabla adjunta.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Tags al alcance del controlador

Si desea utilizar el tag	Entonces asigne este alcance
En más de un programa del proyecto	Alcance de controlador (tags de controlador)
En una instrucción Message (MSG)	
Para producir o consumir datos	
En cualquiera de los siete tipos de datos AXIS	
Para comunicarse con un terminal PanelView	
En ningún caso de los anteriores	Alcance del programa (tags de programa)

100: Tags al alcance del controlador

17.3 Tipos básicos de datos

Los tipos básicos de datos disponibles en los controladores CompactLogix5000 son: booleano, entero, entero con signo, doble entero y real, tal y como se puede ver en la tabla adjunta.

Tipos de datos

Término	Definición
Tipo de datos	El tipo de datos que el tag almacena, como bit, número entero, valor con punto flotante, cadena, etc.
Estructura	<p>Un tipo de datos que es una combinación de otros tipos de datos.</p> <ul style="list-style-type: none">• Una estructura se formatea para crear un tipo de datos único que coincida con una necesidad específica.• Dentro de una estructura, cada tipo de datos individual se conoce como miembro.• Al igual que los tags, los miembros tienen un nombre y un tipo de datos.• Todos los controladores Logix contienen estructuras predefinidas (tipos de datos) que deben utilizarse con instrucciones específicas como temporizadores, contadores, bloques de funciones, etc.• Puede crear sus propias estructuras, denominadas tipos de datos definidos por el usuario.

101: Tipos de Datos

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Tipo de datos	Bits						
	31	16	15	8	7	1	0
BOOL	no se usa						0 o 1
SINT	no se usa				-128...+127		
INT	no se usa		-32,768...+32,767				
DINT	-2,147,483,648...+2,147,483,647						
REAL	-3.40282347E ³⁸ ... -1.17549435E ⁻³⁸ (valores negativos)						
	0						
	1.17549435E ⁻³⁸ ... 3.40282347E ³⁸ (valores positivos)						

102: Tamaño en Bits de cada tipo de dato

En las siguientes imágenes se puede ver como son mostrados los diferentes tipos de datos dentro de RSLogix5000.






Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Nombre	Valor	Máscara de fuerza	Estilo	Data Type
Boolean	0		Decimal	BOOL
Entero	0		Decimal	INT
Entero.0	0		Decimal	BOOL
Entero.1	0		Decimal	BOOL
Entero.2	0		Decimal	BOOL
Entero.3	0		Decimal	BOOL
Entero.4	0		Decimal	BOOL
Entero.5	0		Decimal	BOOL
Entero.6	0		Decimal	BOOL
Entero.7	0		Decimal	BOOL
Entero.8	0		Decimal	BOOL
Entero.9	0		Decimal	BOOL
Entero.10	0		Decimal	BOOL
Entero.11	0		Decimal	BOOL
Entero.12	0		Decimal	BOOL
Entero.13	0		Decimal	BOOL
Entero.14	0		Decimal	BOOL
Entero.15	0		Decimal	BOOL
DobleEntero	0		Decimal	DINT
DobleEntero.0	0		Decimal	BOOL
DobleEntero.1	0		Decimal	BOOL
DobleEntero.2	0		Decimal	BOOL
DobleEntero.3	0		Decimal	BOOL
DobleEntero.4	0		Decimal	BOOL
DobleEntero.5	0		Decimal	BOOL
DobleEntero.6	0		Decimal	BOOL
DobleEntero.7	0		Decimal	BOOL
DobleEntero.8	0		Decimal	BOOL
DobleEntero.9	0		Decimal	BOOL
DobleEntero.10	0		Decimal	BOOL
DobleEntero.11	0		Decimal	BOOL
DobleEntero.12	0		Decimal	BOOL
DobleEntero.13	0		Decimal	BOOL
DobleEntero.14	0		Decimal	BOOL
DobleEntero.15	0		Decimal	BOOL
DobleEntero.16	0		Decimal	BOOL
DobleEntero.17	0		Decimal	BOOL
DobleEntero.18	0		Decimal	BOOL
DobleEntero.19	0		Decimal	BOOL
DobleEntero.20	0		Decimal	BOOL
DobleEntero.21	0		Decimal	BOOL
DobleEntero.22	0		Decimal	BOOL
DobleEntero.23	0		Decimal	BOOL
DobleEntero.24	0		Decimal	BOOL
DobleEntero.25	0		Decimal	BOOL
DobleEntero.26	0		Decimal	BOOL
DobleEntero.27	0		Decimal	BOOL
DobleEntero.28	0		Decimal	BOOL
DobleEntero.29	0		Decimal	BOOL
DobleEntero.30	0		Decimal	BOOL
DobleEntero.31	0		Decimal	BOOL
EnteroCorto	0		Decimal	SINT
EnteroCorto.0	0		Decimal	BOOL
EnteroCorto.1	0		Decimal	BOOL
EnteroCorto.2	0		Decimal	BOOL
EnteroCorto.3	0		Decimal	BOOL
EnteroCorto.4	0		Decimal	BOOL
EnteroCorto.5	0		Decimal	BOOL
EnteroCorto.6	0		Decimal	BOOL
EnteroCorto.7	0		Decimal	BOOL

103: Tipos de datos entero booleano, doble entero, entero largo en RSLogix5000

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

También existen de manera nativa (es decir, sin que el programador tenga que crearlos) tipos de datos como contador, temporizador, alarma o cadena que son datos de tipo estructura (están formados por los tipos básicos).

	Nombre 	Valor 	Máscara de fuerza 	Estilo	Data Type
	 Alarma	{ ... }	{ ... }		ALARM
	Alarma.EnableIn	1		Decimal	BOOL
	Alarma.In	0.0		Float	REAL
	Alarma.HHLimit	3...		Float	REAL
	Alarma.HLLimit	3...		Float	REAL
	Alarma.LLimit	-...		Float	REAL
	Alarma.LLLimit	-...		Float	REAL
	Alarma.Deadband	0.0		Float	REAL
	Alarma.ROCPosLimit	0.0		Float	REAL
	Alarma.ROCNegLimit	0.0		Float	REAL
	Alarma.ROCPeriod	0.0		Float	REAL
	Alarma.EnableOut	0		Decimal	BOOL
	Alarma.HHAlarm	0		Decimal	BOOL
	Alarma.HAlarm	0		Decimal	BOOL
	Alarma.LAlarm	0		Decimal	BOOL
	Alarma.LLAlarm	0		Decimal	BOOL
	Alarma.ROCPosAlarm	0		Decimal	BOOL
	Alarma.ROCNegAlarm	0		Decimal	BOOL
	Alarma.ROC	0.0		Float	REAL
	 Alarma.Status	1...		Hex	DINT
	Alarma.InstructFault	0		Decimal	BOOL
	Alarma.DeadbandInv	0		Decimal	BOOL
	Alarma.ROCPosLimitInv	0		Decimal	BOOL
	Alarma.ROCNegLimitInv	0		Decimal	BOOL
	Alarma.ROCPeriodInv	0		Decimal	BOOL

104: Tipo de dato Alarma en RSLogix5000

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

	Nombre	Valor	Máscara de fuerza	Estilo	Data Type	Descripción
	[-] Cadena.LEN	0		Decimal	DINT	
	[-] Cadena.DATA	{ ... }	{ ... }	ASCII	SINT[82]	
	[-] Cadena.DATA[0]	' ... '		ASCII	SINT	
	[-] Cadena.DATA[0].0	0		Decimal	BOOL	
	[-] Cadena.DATA[0].1	0		Decimal	BOOL	
	[-] Cadena.DATA[0].2	0		Decimal	BOOL	
	[-] Cadena.DATA[0].3	0		Decimal	BOOL	
	[-] Cadena.DATA[0].4	0		Decimal	BOOL	
	[-] Cadena.DATA[0].5	0		Decimal	BOOL	
	[-] Cadena.DATA[0].6	0		Decimal	BOOL	
	[-] Cadena.DATA[0].7	0		Decimal	BOOL	
	[+] Cadena.DATA[1]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[2]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[3]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[4]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[5]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[6]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[7]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[8]	' ... '		ASCII	SINT	
	[+] Cadena.DATA[9]	' ... '		ASCII	SINT	

105: Tipo de dato cadena en RSLogix5000

17.4 Matrices

Una matriz es un tag que contiene un bloque de múltiples datos del mismo tipo (denominados elementos), se pueden organizar en un bloque de hasta 3 dimensiones.

Uno o más subíndices identifican cada elemento individual dentro de la matriz. Un subíndice empieza en 0 y se prolonga hasta el número de elementos menos 1 (con base cero).

	[-] MatrizEnteros			INT[4]	Decimal
	[+] MatrizEnteros[0]			INT	Decimal
	[+] MatrizEnteros[1]			INT	Decimal
	[+] MatrizEnteros[2]			INT	Decimal
	[+] MatrizEnteros[3]			INT	Decimal

106: Matriz en RSLogix5000

17.5 Estructuras

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

El programador también puede crear sus propios tipos de datos mediante estructuras; una estructura, como se vio previamente, es un dato que agrupa datos de diferente tipo (al contrario que las matrices en las que todos los datos tienen que ser del mismo tipo).

17.6 Diferencias entre estructura y matriz

Este tag utiliza la estructura del temporizador (tipo de datos).

Nombre del tag	Tipo de datos
Timer_1	TIMER
Timer_1.PRE	DINT
Timer_1.ACC	DINT
Timer_1.EN	BOOL
Timer_1.TT	BOOL
Timer_1.DN	BOOL

Este tag utiliza una matriz del tipo de datos del temporizador.

Nombre del tag	Tipo de datos
Timers	TIMER[3]
Timer[0]	TIMER
Timer[1]	TIMER
Timer[2]	TIMER

107: diferencia entre estructuras y matrices

A la hora de crear tags para ser usados en un proyecto se han de seguir unas pautas dadas por Rockwell (siendo algunas de ellas parte de las técnicas clásicas de buena programación), a continuación se listan algunas: las más importantes y aquellas que han sido utilizadas en el proyecto.

- Usar estructuras para mantener juntos todos los datos relacionados con un aspecto específico del sistema.
- Servirse de que cada miembro de una estructura tiene un nombre para que este sea descriptivo y ayude a la documentación.
- Creación de estructuras reutilizables para cuando existan múltiples partes de un sistema iguales. Reducir el uso de matrices con datos de tipo bool, muchas instrucciones de matriz no funcionan en matrices de tipo bool dificultando s

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

inicialización y su borrado., para ello mejor usar los bits individuales de un tag DINT o una matriz de DINT.

- No usar el mismo nombre para tags de controlador y tags de programa.
- Usar matrices para que los datos se ajusten a aquello que representan.
- Si incluye una matriz, que sea de una sola dimensión.
- Minimizar el uso de datos de tipo entero o entero con signo para aumentar la eficacia de la lógica, usar mejor datos de doble entero
- Los controladores Logix5000 generalmente comparan y manipulan los datos como valores de 32 bits (DINT o REAL) convirtiendo los datos de tipo SINT o INT a datos de tipo REAL o DINT, si el destino es un dato del tipo original el valor es nuevamente convertido de manera automática sin intervención del programador, pero obviamente consume tiempo de ejecución y memoria.
- Asignar valor constante a un tag para evitar que los valores respaldados por la tabla se cambien programáticamente para así reducir el riesgo de cambiar los valores de los tags por accidente Utilizar el acceso externo (tags de controlador) de manera restrictiva para evitar la capacidad del usuario de cambiar los valores.
- Con respecto a los nombres de los tags:

Limitar los nombres de los tags a 40 caracteres, utilizar solo caracteres alfabéticos (A-Z o a-z), numéricos (0-9) o de subrayado (_), no empezar por carácter numérico, sin tener 2 subrayados consecutivos, el compilador no distingue mayúsculas de minúsculas.
- Coloque todos los datos de tipo DINT, SINT, INT y BOOL de forma consecutiva para realizar un mejor uso de la memoria.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Más eficaz

BOOL
BOOL
BOOL
DINT
DINT

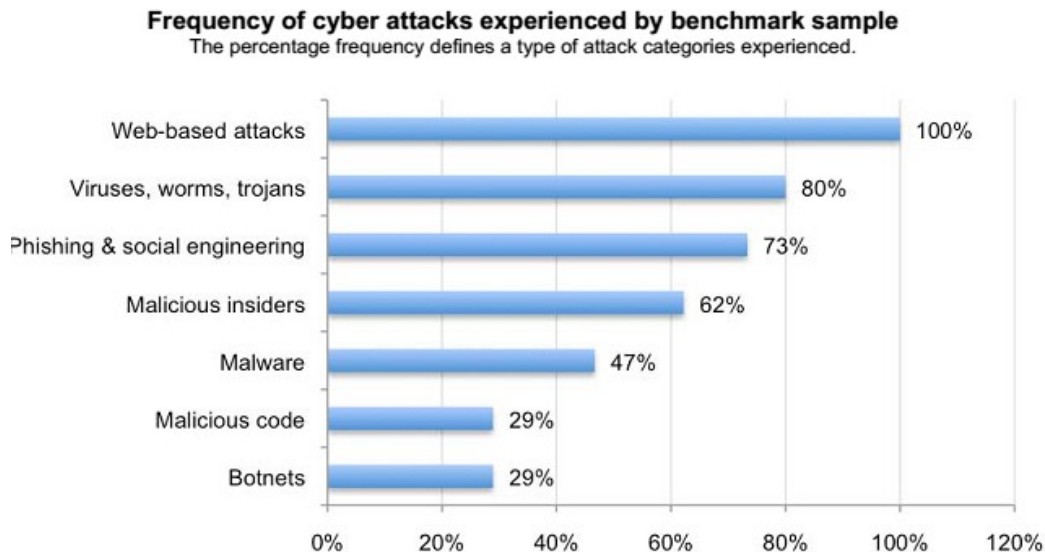
Menos eficaz

BOOL
DINT
BOOL
DINT
BOOL

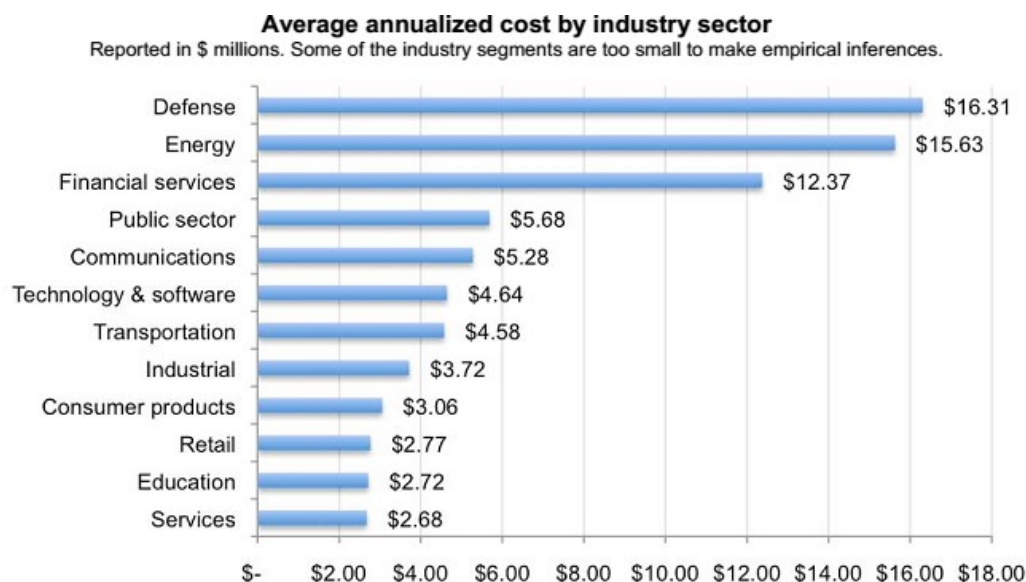
108: Organización de datos en memoria para mejorar su uso

18.- Anexo D: Seguridad

El Ponemon Institute en su Cuarto estudio anual del coste del cibercrimen (Ponemon, 3013) concluye que el coste medio anual para las empresas analizadas es de 3.8 millones de dólares por año siendo los ataques vía web, con código malicioso o por atacantes internos más del 90% de todos ellos



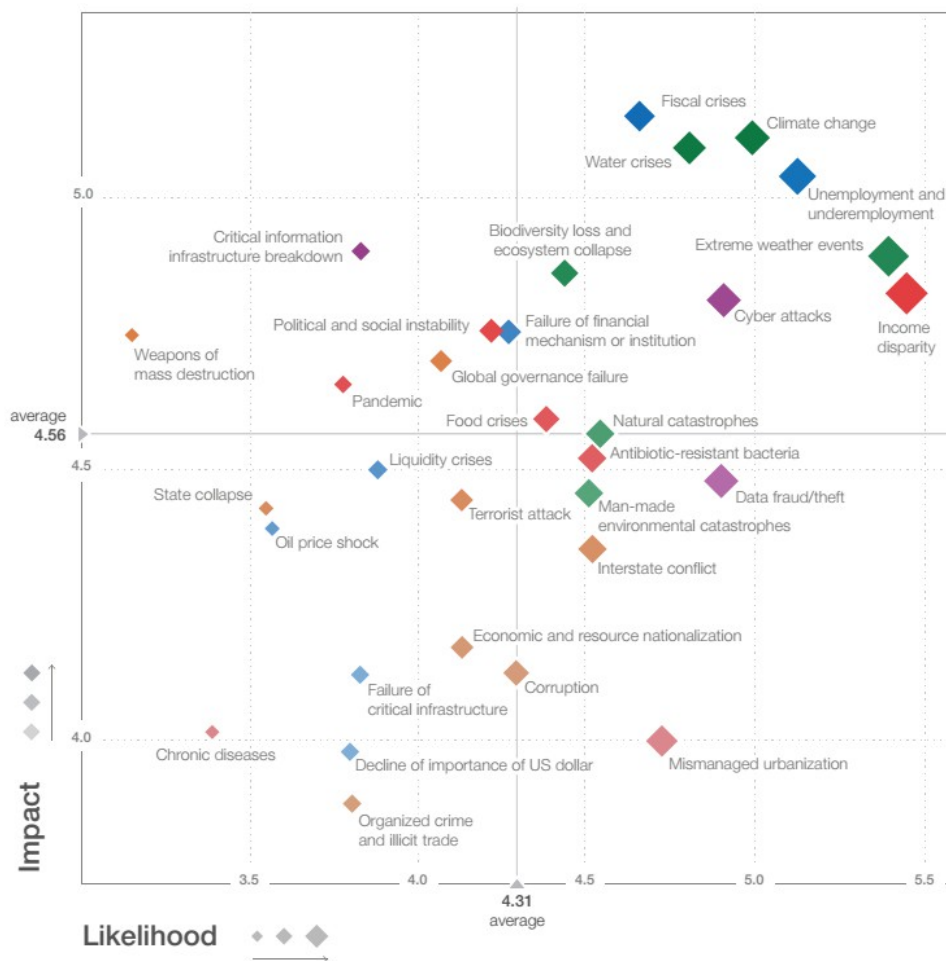
109: Frecuencia de los diferentes ataques en las empresas del estudio (Ponemon, 3013)



110: Media anual del coste para cada sector (Ponemon, 3013)

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Y según el Foro económico Mundial (World Economic Forum, 2014) los ciberataques están entre los principales riesgos de los próximos 10 años.



112: Informe de riesgos mundiales de 2014 (World Economic Forum, 2014)

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Top 5 Global Risks in Terms of Impact



113: Informe de riesgos mundiales de 2014 (II) (World Economic Forum, 2014)

18.1 Impacto de un ataque

Una de las cosas a tener en cuenta es el posible impacto de un problema en la seguridad de nuestro SCADA y por lo tanto han de estar cubiertas previamente con su diseño.

Según la Ley 8/2011, de 28 de abril (BOE, 2011), por la que se establecen medidas para la protección de las infraestructuras críticas (Morant, 2013) se podría hablar de 4 tipos:

- Impacto físico: daños a personas y bienes muebles e inmuebles.
- Impacto económico: Principalmente derivado del impacto físico, aunque también relacionado con la reputación de la empresa que ha sufrido el ataque que podría derivar en pérdidas futuras de contratos o de clientes insatisfechos.
- Impacto financiero: tras la supuesta pérdida de ingresos debido a clientes insatisfechos, desconfiados, se debería de aumentar el gasto en marketing para promover una mejoría de la imagen de la empresa.
- Impacto social: Desconfianza por parte de los usuarios finales a los que la empresa que ha sufrido el ataque presta servicios.

18.2 Razones por las que sufrir un ataque

La posibilidad de sufrir un ataque es independiente de la importancia del sistema atacado si el ataque se realiza porque el atacante quiere demostrar su capacidad y conocimientos; para evitarlo habría que ser simplemente menos vulnerable que el resto de nuestro entorno para que el foco de los posibles atacantes se centrara en ellos; también pueden existir posibilidad de sufrir un ataque por causas que se nos escapan a nuestra capacidad de previsión, lo importante son las razones que el atacante pueda tener, por lo tanto el ser un sistema pequeño o no importante (bajo nuestra opinión) no nos hace menos vulnerable (sino más, puesto que el tamaño puede indicar la poca capacidad de sobreponernos ante un ataque)

El CCN-STIC-480 “Seguridad en sistemas SCADA” (Centro Criptológico Nacional, 2010) identifica (pero sin limitar) a los atacantes potenciales (conscientes o inconscientes) incluyendo:

- Hackers y delincuentes
- Malware de propagación automática (gusanos, bots, etc.).
- Personal interno (descontentos o tras realizar acciones no autorizadas).
- Atacantes externos (Inteligencia corporativa, Contratistas, Servicios de inteligencia extranjeros).
- Crimen organizado.
- Terroristas.
- Manifestantes y activistas.

18.3 Diseño del sistema

Tradicionalmente los diseños para soluciones industriales han priorizado la disponibilidad, robustez y fiabilidad del sistema frente a otros factores pero, como se indica en el Mapa de Ruta de la Ciberseguridad Industrial en España 2013 – 2018:

“Esta decisión, estaba justificada por la simplicidad y el ahorro que suponía el sacrificio de estas características que no eran consideradas necesarias en los entornos tremendamente controlados en los que residían estos sistemas. Sin embargo, hoy en día la situación ha cambiado, y los sistemas de control comparten su ubicación en la red con dispositivos de diferentes tipos, con variadas funcionalidades y que pueden introducir en la red tráfico perniciosos para su correcto funcionamiento. Además, en muchas ocasiones están conectados a redes públicas y abiertas como Internet, lo cual les hace mucho más accesibles y evidentemente vulnerables”

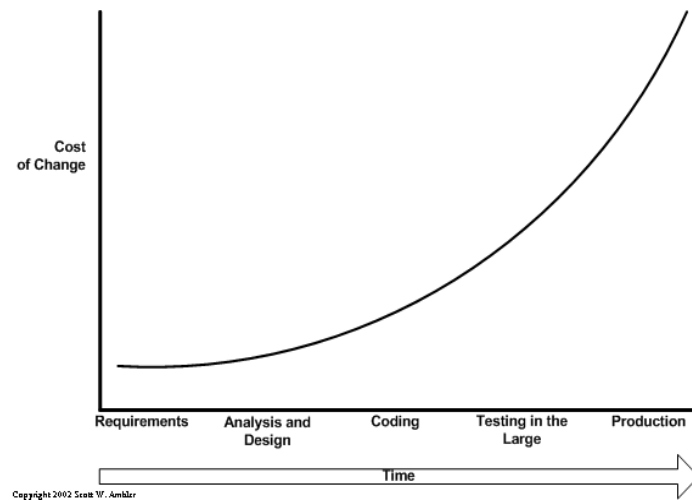
Mapa de Ruta de la Ciberseguridad Industrial en España 2013 – 2018 (Centro de Ciberseguridad Industrial, 2012)

Todo ello nos lleva a deber tener en cuenta la seguridad desde el inicio del diseño, Para ello lo ideal es conocer y comprender el proceso a automatizar, no solo como un ente aislado sino dentro de un sistema mayor (¿Qué es/hace? ¿Cómo es/hace? ¿Dónde? ¿De dónde? ¿A dónde? ¿Por qué? ¿Para qué?) Teniendo en cuenta, además, la legislación vigente, por lo tanto y en consecuencia evitaremos problemas por la falta u olvido de comunicar de información por parte del cliente, disminuyendo la posibilidad de fallo del sistema, algo vital en los sistemas de control industrial.

Otros factores a tener presentes (vistos los apartados anteriores y debidos a la vida útil de hasta 20 años) son las actualizaciones de firmwares y software futuras, ya que requerirán periodos de estudio y planes de contingencia para implantarlos los cuales harán incrementar su coste y complejidad cuanto peor haya sido el diseño inicial.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

La interfaz de un SCADA es la parte accesible de este y por ello es por donde los posibles atacantes pueden entrar, para evitarlo es indispensable minimizar el número de conexiones a los sistemas de control, separar los SCADA entre si y entre de las demás redes presentes en la empresa, controlar todas las conexiones al sistema y realizar el análisis de riesgo de aquello que tenga que estar expuesto.



114: Curva típica de coste de cambio en un proyecto software. (Ambler, s.f.)

Para ello se podría recurrir a las guías existentes de buenas prácticas que recogen las vulnerabilidades más habituales y las medidas para su evitar su aparición; algunas de ellas pueden ser los proyectos OWASP (OWASP, s.f.), las guías 480 del centro Criptológico Nacional, especialmente: CCN-STIC-480 “Seguridad en sistemas SCADA” (Centro Criptológico Nacional, 2010), CCN-STIC-480A “Seguridad en el control de procesos y SCADA” (Centro Criptológico Nacional, 2010) y CCN-STIC-480C “Guía 2 Implementar una arquitectura segura” (Centro Criptológico Nacional, 2010) o los recursos ofrecidos por el Observatorio del Instituto Nacional de Tecnologías de las Telecomunicaciones como la guía “Software Exploitation” (Febrero, s.f.).

Cuando se realiza el análisis de riesgos para las partes de la interfaz que estén expuestas aparecen tres tipos de acciones disponibles: reducir su importancia

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

mejorando la seguridad en ese apartado, no solventarlo pero tener en cuenta que es un posible vector de ataque o tratarlo como riesgo residual y simplemente anotar su existencia por si en un futuro su nivel de riesgo cambia.

A la hora de aplicar las medidas ante cada riesgo, los factores como el coste, la eficacia de la medida propuesta o su dificultad son los que determinaran finalmente si se llevarán a cabo y cómo.

Otro apartado importante son las contramedidas a aplicar en el caso de que la penetración sea exitosa, tales como la preparación un equipo de seguridad SCADA, estar atentos a las alertas de seguridad (mediante los boletines del ICS-CERT, CCN u otros organismos) así como disponer de planes de mantenimiento y seguridad y procedimientos para monitorizar y evaluar los incidentes

18.4 Sistema en producción

Durante la explotación del sistema se podría tener la necesidad de crear y actualizar documentos y protocolos relacionados con las políticas de seguridad (ISO/IEC 27001 (AEN/CTN 71, 2007) e ISO/IEC 27002 (AEN/CTN 71, 2009)) en coordinación con las fuerzas y cuerpos de seguridad del estado y el Centro Criptológico Nacional (RD 704/2011, de 20 de mayo, (BOE, 2011)) si fuese necesario.

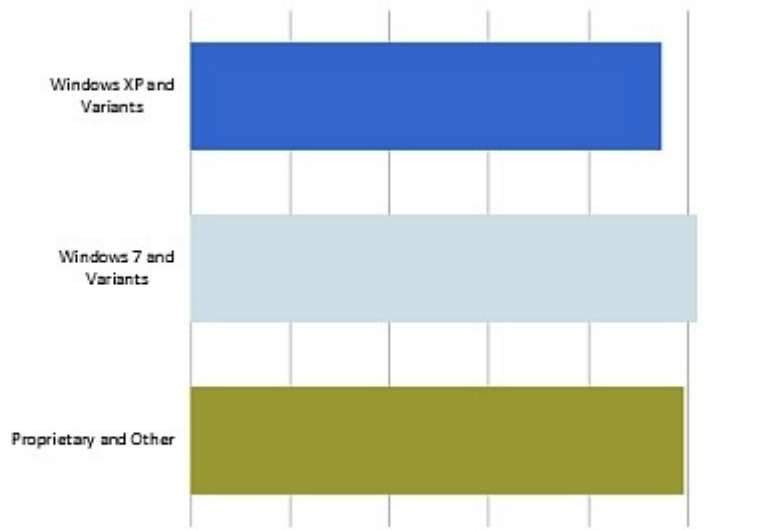
18.5 Sistemas de Control Industrial

Los sistemas de control industrial eran, en su origen, desarrollos propietarios, heterogéneos, cerrados, no estándares y aislados de su entorno, pero con el paso del tiempo se tiende a converger al uso de protocolos estandarizados (como Ethernet/IP) así como en Sistemas Operativos de propósito general (Windows y Linux principalmente); esto proporciona una ganancia en productividad, prestaciones, funcionalidad e interoperabilidad muy importante, pero a su vez es un riesgo que hay

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

que tener en cuenta, por lo tanto también tenemos que converger con las herramientas y metodologías existentes en el campo de la informática.

The World Market for Industrial PCs by Operating System
Comparative Market Size - 2014



[Aggregate of all product types: Panel IPC, Box IPC, Rackmount IPC, Embedded Panel IPC, Embedded Box IPC, DIN Rail IPC and Thin Client IPC]

Source: IMS Research

Feb-13

115: Distribución de los SO en los ordenadores industriales (IMS Research, 2013)

“En general, cualquier medida técnica de seguridad que se pueda aplicar en TI puede ser utilizada en SCADA y viceversa, siempre que se cumplan una serie de requisitos formales en SCADA que garanticen una coherencia y un endurecimiento de dichas medidas.”

CCN-STIC-480 “Seguridad en sistemas SCADA” (Centro Criptológico Nacional, 2010)

18.6 Vulnerabilidades de la red

Se suele considerar que una red es de bajo riesgo cuando ésta no tiene acceso a internet o al estar formada por elementos propietarios con un número limitado de expertos, pero hay que aceptar que el aislamiento no nos protege de los ataques que puedan provenir de dentro de la organización, teniendo que hacer hincapié en la administración de los permisos de usuario, la gestión de las contraseñas y el cifrado de los datos y las comunicaciones.

“La consideración habitual de que no existe comunicación o interconexión entre las redes corporativas y las redes industriales (el mito del air gap) se ha demostrado que es incorrecta. La interconexión existe pero puede no ser obvia o en otros casos se crea temporalmente una conexión que no está documentada ni procedimentada, por ejemplo acceso remoto o local desde un ordenador portátil o conexión de un dispositivo de almacenamiento (discos externo, memorias flash). [...] puede tomar diversas formas como conexiones directas, enrutamiento o mediante máquinas puente en ambas redes [...] Posiblemente el caso más típico sea la instalación de accesos remotos en distintos puntos de las redes de las instalaciones para permitir la gestión y mantenimiento remoto de ciertos equipos. Esto plantea diversos problemas desde el punto de vista de la ciberseguridad, ya que cada acceso remoto aumenta la superficie expuesta de los sistemas de la planta en redes públicas.”

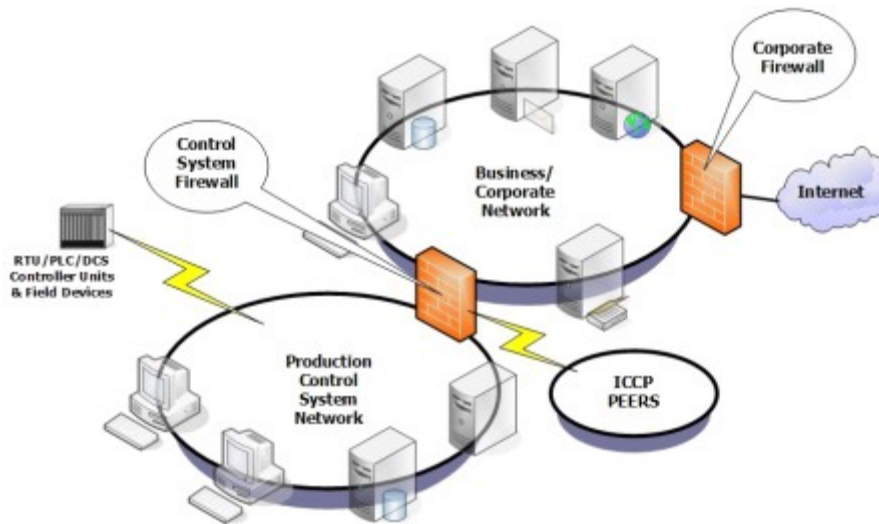
Mapa de Ruta de la Ciberseguridad Industrial en España 2013 – 2018 (Centro de Ciberseguridad Industrial, 2012)

En informes como el de protección de las infraestructuras críticas hecho por el S2 Grupo se han encontrado varios cientos de infraestructuras críticas accesibles desde internet, Informe PIC Colombia 2013 (Marín, 2013) e Informe PIC España 2012 (Pablo Marín, s.f.), utilizando herramientas como SHODAN y realizando búsquedas asociadas a las firmas de los componentes SCADA obtenidas del US ICS-CERT.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Antonio Villalón y Pablo Marín

Las medidas básicas es la instalación de un cortafuegos debidamente configurado con solo aquellos puertos necesarios para el sistema “CCN-STIC-408 Seguridad perimetral - cortafuegos” (Centro Criptológico Nacional, s.f.) que aísle la red del SCADA de la corporativa.



116: Arquitectura típica con 2 cortafuegos (ICS-CERT, s.f.)

También es recomendable una monitorización de las conexiones y los logs de las partes del sistema de seguridad (cortafuegos, antivirus...) así como de disponer de un sistema de detección de intrusiones (IDS) y de realizar todas las comunicaciones mediante conexiones cifradas.

18.7 Terminal de explotación

La configuración del Sistema Operativo presente en el terminal de explotación es vital para su seguridad, para ello, por lo menos, se han de seguir unas pautas mínimas como: eliminar servicios y software no necesario, restringir puertos en local (USB, RS232...) y el autoarranque del CD/DVD, antivirus actualizado (realizando comprobaciones periódicas de infecciones), gestión adecuada de los usuarios, monitorización de los accesos remotos, realización de copias de seguridad y conexión en remoto mediante VNC cuando sea necesario un acceso remoto.

Otro punto importante es la comprobación, siempre que se pueda, de que los binarios que se van a instalar en la máquina sean los mismos que el fabricante ha compilado y éstos no han sido troyanizados e instalemos un programa con una puerta trasera, para ello se puede recurrir a la comprobación del hash MD5 si el proveedor del ejecutable lo proveyera.

En el caso de que el uso de memorias USB sea necesario para el funcionamiento del sistema el ICS-CERT recomienda (ICS-CERT, 2010), deshabilitar el autoarranque, establecer políticas estrictas del uso de los USB y una formación de los trabajadores ante la posibilidad de sufrir ataques usando el USB como vector.

18.8 Actualización del software

Los PC de control y supervisión suelen tener el sistema operativo de uso corriente en el momento en que se implantó el sistema/instalación. Y suele permanecer así para siempre, pudiéndose no instalar las actualizaciones pertinentes si se asume que el equipo va a estar conectado a ninguna red.

Todo esto puede venir causado por, entre otras razones, a) desconocimiento o incapacidad del o de los responsables, b) la no comunicación entre los departamentos que lleva a que cada uno opere independientemente, c) tener que subcontratar la modificación y si el sistema es muy antiguo el servicio puede ser muy caro o no existir, d) aversión al posible riesgo que puede existir al modificar algo que “funciona” o e) pensar que, como “funciona”, la actualización no nos reportará ningún beneficio, f) peligros consecuentes a la interdependencia del software (tener que actualizar el S.O. puede requerir una nueva versión del SCADA que puede generar problemas) (Navarro, 2013).

Siendo muchos sistemas SCADA de disponibilidad permanente la preparación de actualización y parcheo del software ha de estar muy bien procedimentada, existiendo procedimientos de regresión si falla durante una ventana de prueba.

En el caso de que no sea parcheable, reemplazable o actualizable también se han de disponer de medidas para solventarlo, entre ellas pueden estar: aislarlo físicamente de su entorno, aumentar la seguridad mediante protecciones adicionales o protegerlos con sistemas de prevención de intrusos.

Para estar al día con las vulnerabilidades y los bugs de los elementos del sistema se puede suscribir a boletines de vulnerabilidades como los del CCN-CERT²⁰, OWASP²¹, ICS-CERT²² o Naked Security²³.

²⁰ <https://www.ccn-cert.cni.es>

²¹ <https://www.owasp.org>

²² <https://ics-cert.us-cert.gov>

²³ <http://nakedsecurity.sophos.com>

18.9 Acceso remoto

Los accesos remotos tanto desde la propia organización como desde sistemas ajenos a ella, aunque poco deseables, pueden ser necesarios cuando el sistema ha sido diseñado por terceras partes para su mantenimiento o soporte, o cuando existe una centralización fuera del entorno donde está el sistema instalado.

Para que no se convierta en un agujero de seguridad es recomendable mantener un inventario de todas aquellas empresas (y empleados) y de las múltiples conexiones que pueden existir; también es recomendable comprobar que existe una necesidad de negocio válida para dichas conexiones y un método válido de autenticación para identificar indefectiblemente al usuario en todo momento (autenticación fuerte) y que dichas conexiones sean solamente a las máquinas que sea necesario y no a todo el sistema.

Para ello es recomendable siempre que sea posible, que sean realizadas mediante VPN pudiendo seguir la guía “Seguridad en VPN” (Centro Criptológico Nacional, 2007), aunque posiblemente sea también necesaria la conexión mediante puerto serie o vía modem, siempre y cuando se dispongan de mecanismos de autenticación.

Estas medidas han de ser complementadas con una certificación equipo a equipo para que todo equipo que se conecte a nuestra red esté debidamente protegido (antivirus y cortafuegos personal).

“Cuando se necesite acceso remoto se recomienda realizarlo mediante Redes Privadas Virtuales (VPN de las siglas en inglés Virtual Private Network) teniendo en cuenta que la VPN podría tener vulnerabilidades y ha de estar actualizada a la última versión disponible. También hay que tener en cuenta que una VPN es tan segura como los dispositivos conectados a ella.”

(ICS-CERT, 2014)²⁴

18.10 Operarios

Como se ha visto anteriormente, los ataques internos son una de las fuentes principales de la rotura de la seguridad, por ello los trabajadores que vayan a disponer de acceso operativo o administrativo son una parte a vigilar y a controlar, por lo tanto: hay que disponer y hacer cumplir una política de contraseñas para todos los sistemas de control que obligue a utilizar contraseñas fuertes con tiempos de caducidad (nunca la contraseña por defecto, si es posible), revisar periódicamente los derechos y permisos de los usuarios, evitar el uso indiscriminado de contraseñas dejando el acceso libre (pej. Modo solo visualización).

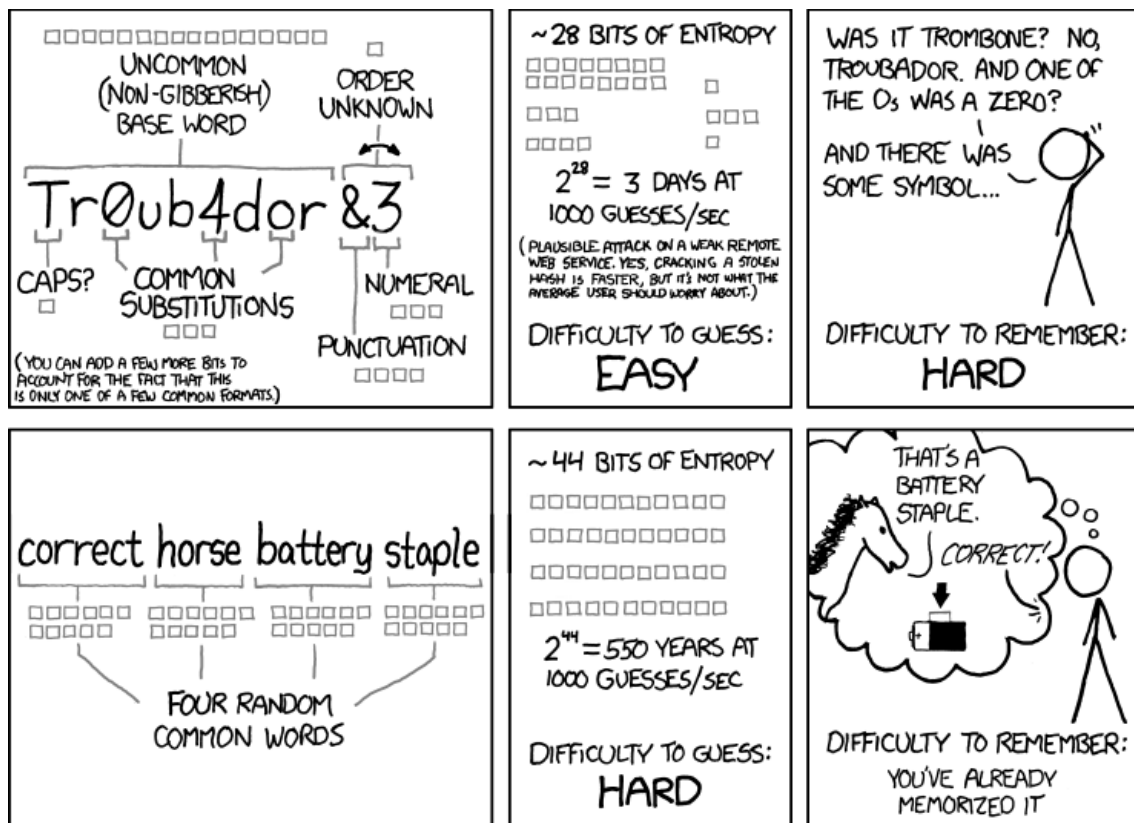
Una vez finalizado el contrato por el trabajador se ha de eliminar o bloquear sus usuarios y revocar sus permisos, cambiando las contraseñas de administrador a las que tuviese acceso.

²⁴ “When remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.” (ICS-CERT, 2014)

18.11 Contraseñas

“Los usuarios responden a las políticas de composición [de contraseñas] con opciones compatibles con los mínimos exigidos como Pa\$\$w0rd y Snoopy2. Las contraseñas que sacan mejores resultados usando esta métrica no está garantizado que resulten más seguras ante ataques en los que se intente adivinar la contraseña.”

(Dinei Florencio, 2014)²⁵



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

117: (Munroe, s.f.)

²⁵ "Users respond to composition policies with minimally compliant choices such as Pa\$\$w0rd and Snoopy2. Passwords scoring better by this metric are not guaranteed to fare better under guessing attacks" (Dinei Florencio, 2014)

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

IMPLEMENTATION ASPECT	ATTACKS STOPPED OR SLOWED	USER IMPACT	REMARKS
Password stored non-plaintext	Full compromise on server breakin alone	None	Recommended
Salting (global and per-account)	Pre-computation attacks (table lookup)	None	Recommended
Iterated hashing	Slows offline guessing proportionally	None	Recommended
MAC of iterated, salted hash	Precludes offline guessing (requires key)	None	Best option (key management)
Rate-limiting & lockout policies	Hugely reduces online guessing	Possible user lockout	Recommended
Blacklisting (proactive checking)	Eliminates most-probable passwords	Minor for small lists	Recommended
Length rules	Slows down naive brute force attacks	Cognitive burden	Recommended: length ≥ 8
Password meters	Nudges users to "less guessable" passwords	Depends on user choice	Marginal gain
Password aging (expiration)	Limits ongoing attacker access;	Significant;	Possibly more harm than good
	indirectly ameliorates password re-use	annoying	
Character-set rules	May slow down naive brute-force attacks	Cognitive burden. Slows entry on mobile devices	Often bad return on user effort

118: Diferentes formas de implementar las contraseñas. (Dinei Florencio, 2014)

Otra razón para no recomendar este tipo de técnicas para la creación de contraseñas es debido a que programas de crackeo como JohntheRipper²⁶ o Hashcat²⁷ también las incorporan (Marechal, 2012), además, este tipo de políticas hacen que el usuario sea más previsible y a que confíe en que las políticas impuestas son suficientes (Dinei Florencio, 2014).

Ilustración 1 who and link

Tampoco se recomienda el uso de políticas de caducidad de contraseñas (Yinqian Zhang, 2010).

“Confirmamos las conjeturas previas de que la eficacia de la caducidad en el cumplimiento de su objetivo previsto es débil.”

(Yinqian Zhang, 2010)²⁸

Ni seguir políticas “agresivas” para con los usuarios

“Cuando las voces que abogan por la usabilidad están ausentes, las medidas de seguridad se vuelven innecesariamente restrictivas”.

²⁶ <http://www.openwall.com/john>

²⁷ hashcat.net

²⁸ “Using this framework, we confirm previous conjectures that the effectiveness of expiration in meeting its intended goal is weak” (Yinqian Zhang, 2010)

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Cormac Herley, Microsoft Research (Merino, 2014)

Por lo tanto se recomienda seguir directrices similares a las dadas por el especialista en seguridad Bruce Schneier (Schneier, 2007), dar una formación adecuada y concienciar a los usuarios (Benet, 2014).

“Hacer recaer la carga de la seguridad en el usuario final y centrarse en aumentar la complejidad sencillamente no funciona”

Donna Dodson, asesora jefe de ciberseguridad en NIST (Merino, 2014)

18.12 Seguridad física

Otro aspecto relacionado con la seguridad es la seguridad física de la instalación y del sistema de control, pues no vale de nada la seguridad informática si el sistema es accedido físicamente.

El acceso al sistema ha de estar restringido, solo disponible para aquellas personas autorizadas, ha de existir una vigilancia y monitorización en las dependencias más sensibles mediante grabaciones de vídeo y registro de acceso.

También se ha de proteger físicamente otras dependencias como: las instalaciones de suministro eléctrico del sistema SCADA así como de las del sistema auxiliar si este existiese y aquellas instancias donde se almacene información digital o no del sistema (logs, informes, guías, auditorías...).

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

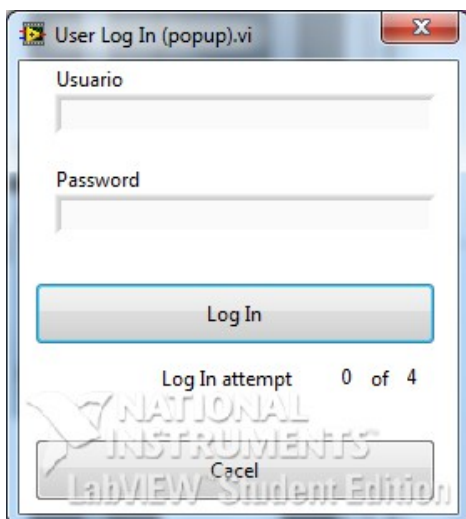
19.- Anexo E: Pruebas de Usuario

19.1 Prueba 1: Prueba de funcionalidades de administración.

Durante el proceso de programación de la gestión de las funcionalidades de administración se realizó una prueba con una administradora de sistemas para comprobar la adecuación de las funcionalidades proyectadas y la adecuación de su implementación.

Para ello se le acompañó en el uso de la interfaz de administración anotando sus comentarios e impresiones que se recogen a continuación.

19.1.1 Interfaz del login de usuario

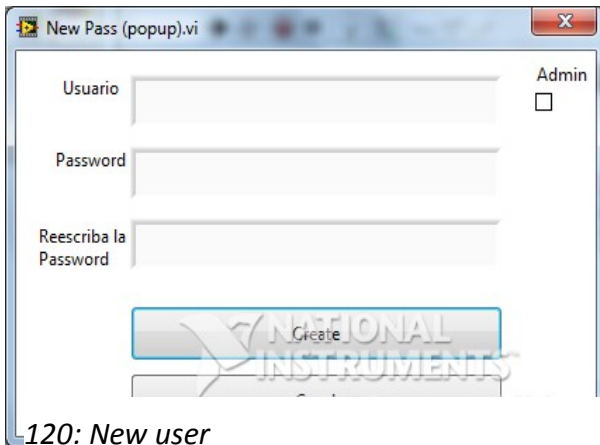


No hubo comentarios.

119: Login

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

19.1.2 Interfaz para la creación de nuevos usuarios

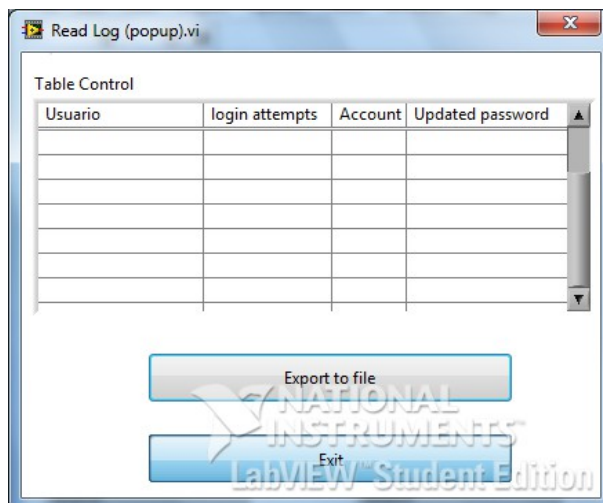


120: New user

No se puede navegar mediante la tecla tabulador.

- Se había detectado este problema pero se había pospuesto su solución.

19.1.3 Interfaz para ver el log de accesos al sistema



Detectar si el archivo donde se guarda el log existe y sino crearlo.

- Sencilla, se implemento posteriormente.

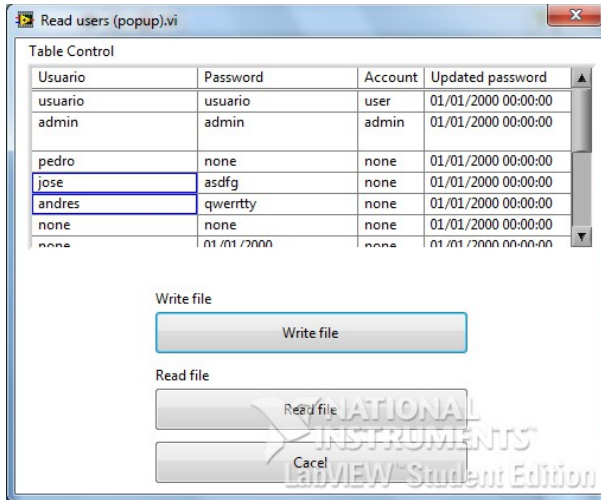
Guardar en el log la fecha de creación de usuarios.

- Modificación nada complicada que se realizó in situ, se

cambió también el nombre de la columna y la cadena de caracteres que se guardaba.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

19.1.4 Interfaz para la lectura y modificación de usuarios en el sistema



121: Read Users

No se pueden borrar usuarios.

Se sugirió la limitación de usuarios directamente desde la tabla o desde un campo a su pié.

- Difícil de realizar lo primero, se implementará la segunda forma y si hay tiempo se verá si se puede hacer de la otra.



La fecha de actualización del usuario no es útil y se confunde con la de creación.

- Se eliminó.

“Read”, no es descriptivo de la función, mejor usar “Reload”.

- Cambiado en el momento

Indicar como escribir en los diferentes usuarios en la tabla mediante un menú de ayuda (i) y los roles.

- *Admin/administrador*: instala y configura la aplicación para que los usuarios la usen, solo se recurre a él en caso de tener problemas
- *User/Usuario*: usa la aplicación.

None/ninguno: usuario nulo, creado para que su configuración se aplique cuando exista algún problema inesperado o no haya ningún usuario conectado.

Detectar si el archivo donde se almacenan los usuarios ha desaparecido y avisar ya que sin un usuario administrador no se pueden crear nuevos usuarios.

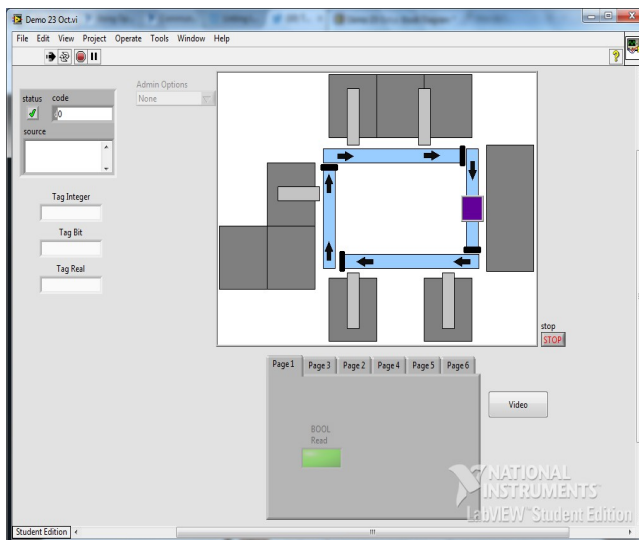
Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

- Para ello se creó el Pswd creator, un instrumento virtual que ha de poseer el programador al que se le ha comprado la aplicación (otra opción es incluir en el código un usuario maestro).

Ordenación de los usuarios en base a diferentes parámetros (rol, fecha de creación...).

- Se implementará si da tiempo, en principio no sería imprescindible ya que no se espera un gran número de usuarios (2 por turno de trabajo y 2 administradores).

19.1.5 Interfaz principal



El indicador no se sabe si es de pieza o de en que estación de trabajo se está leyendo los datos.

- Se ha decido añadir un segundo indicador.

Aparecen datos desconocidos para el usuario

122: Interfaz principal

- Son necesarios para las pruebas que está realizando el programador, se eliminaran posteriormente.

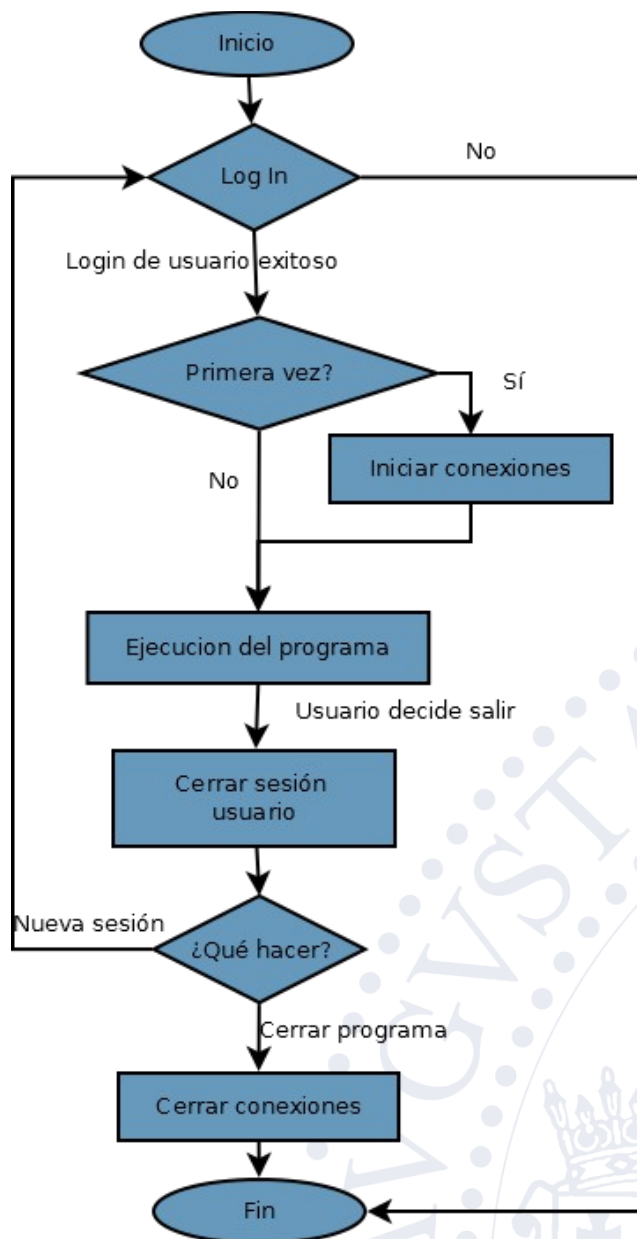
Permitir el cambio de usuario/cierre de sesión.

- Estaba previsto aunque no se había implementado en la fecha en la que se realizó la prueba.

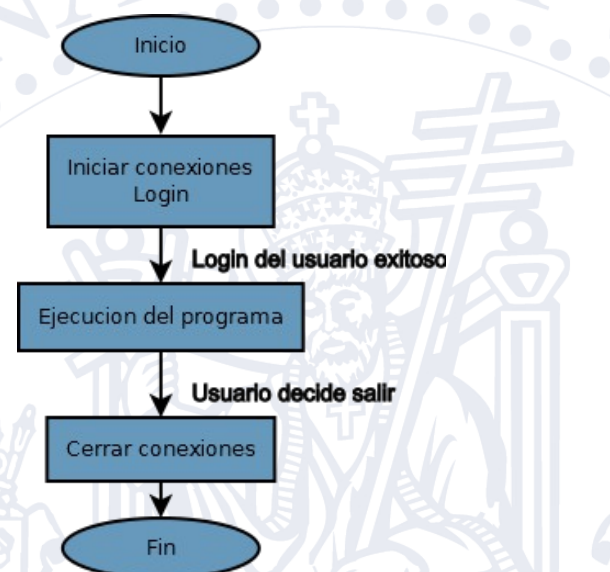
Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan
Gestión de de la desconexión del autómatas al cerrar sesión y al final de la jornada laboral en vez de disponer de un botón con el incierto nombre de “Cancel” (nombre por defecto en este tipo de botones)

Desconexión del usuario tras un tiempo de inactividad.

Para solucionar estos problemas se planteó cambiar la opción de cambiar la lógica del flujo del programa del diagrama que hay a la izquierda en el que se hacía uso de una estructura *flat sequence* a una como la del diagrama de la derecha (mediante una *Stacked sequence*).



123: Flujograma final



124: flugrama inicial

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

19.2 Prueba 2: Prueba 2ª de funcionalidades de administración.

Tras la primera prueba se realizaron las modificaciones pertinentes (incluidas algunas de las rechazadas en un principio).

Ni la Interfaz del login, ni la Interfaz para la creación de nuevos usuarios, ni la principal fueron modificadas en su apariencia y por ello no se incluyen imágenes en este apartado.

19.2.1 Interfaz del login de usuario

Poner asteriscos cuando se introduce la contraseña.

- No estaba realizado en el momento para agilizar las pruebas.

Presionando la tecla enter no se valida el usuario y la contraseña

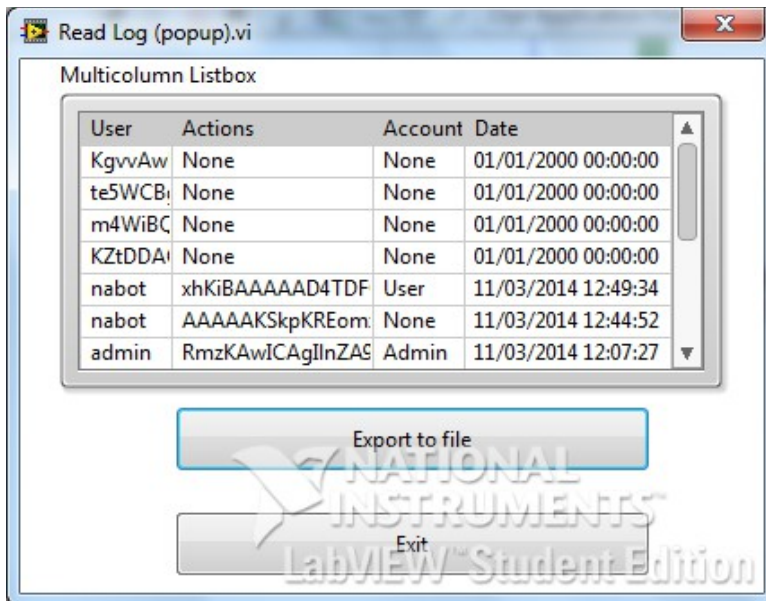
- Debido a como es LabVIEW introducía un salto de línea, se solventó sin muchos problemas.

19.2.2 Interfaz para la creación de nuevos usuarios

Cuando se crea un usuario nuevo se guarda en el log None en la columna account en vez del tipo de cuenta.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

19.2.3 Interfaz para ver el log de accesos al sistema

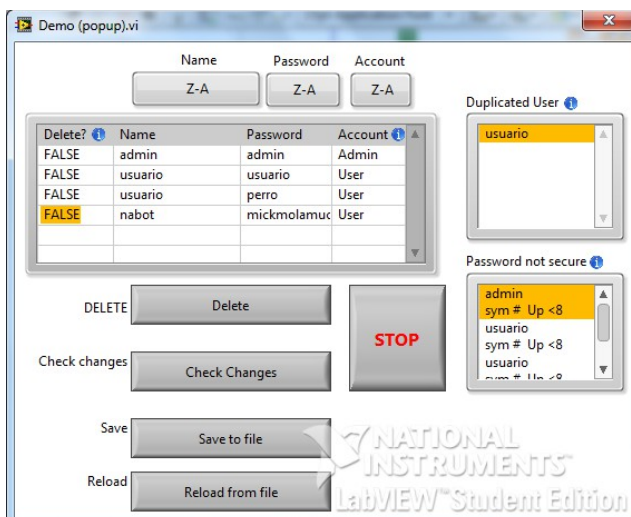


Descifrar las acciones realizadas almacenadas en el log.

- Fácil solución.

125: Read log

19.2.4 Interfaz para la lectura y modificación de usuarios en el sistema



Información en español y en inglés para la publicación de las librerías en internet.

- Se añadirá la traducción de los "Tip Strip" al inglés para que programadores que quieran usar esta librería y tengan este programa de ejemplo puedan entender su funcionamiento.

126: Read users

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Algunos de iconos de información tienen errores.

Quitar el resaltado amarillo de algunos controles de la interfaz.

- Dificil modificación al ser inherente al controla que indica que línea se está siendo editada, pero dadas las modificaciones realizadas se perdía la funcionalidad (las opciones implementadas para poder seleccionar diferentes opciones).

Permitir la escritura

- Debido a un bug en la presentación no se podía escribir.

19.2.5 Interfaz principal

Desconectar de los autómatas si se lleva mucho tiempo sin acciones (para evitar que alguien no indicado acceda, planeado pero no implementado por olvido).

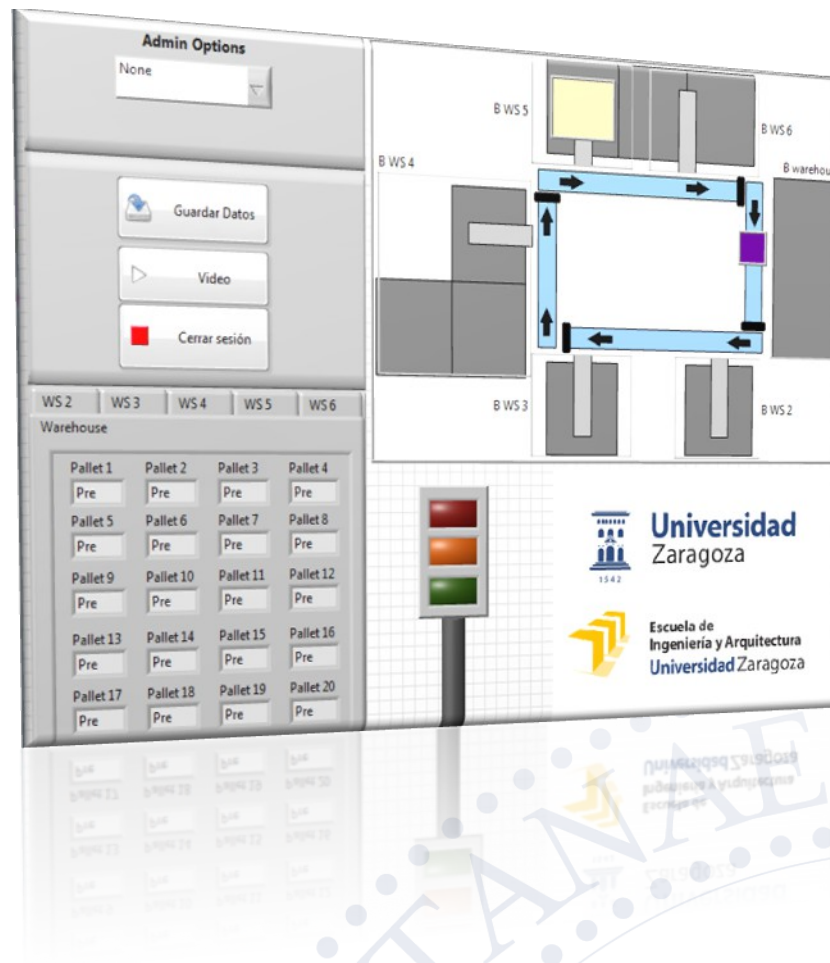
20.- Anexo F: Manual de usuario



21.-

Manual de Usuario

Terminal de explotación



Terminal de explotación para TiM -001

MANUAL DE USUARIO

Este manual es parte inseparable del software por lo que debe estar a disposición de los usuarios del equipo. Se recomienda leer atentamente el presente manual y seguir rigurosamente los procedimientos de uso para obtener las máximas prestaciones.

Índice

1	INSTALACIÓN	- 7 -
2	CONFIGURACIÓN	- 7 -
3	TIPOS DE CUENTAS	- 8 -
4	SEGURIDAD DE LA CONTRASEÑA	- 8 -
5	LOG IN	- 9 -
6	PANTALLA PRINCIPAL	- 9 -
7	ESTACIONES DE TRABAJO	- 10 -
8	CIERRE DE SESIÓN	- 12 -
9	NUEVO USUARIO	- 13 -
10	ACCESO AL LOG	- 14 -
11	GESTIÓN DE USUARIOS	- 15 -
12	LICENCIAS	- 18 -
12.1	VIDEOLAN	- 18 -
12.2	I3JSON	- 26 -
12.3	AES TOOLKIT	- 28 -
12.4	TYPE SENSITIVE POPUP	- 30 -
12.5	FILENAME GENERATOR FOR LABVIEW	- 31 -

Introducción

Gracias por elegir este producto.

Antes de utilizar el terminal de explotación, lea atentamente este manual y consérvelo para consultarlo en el futuro.


Por favor, tenga en cuenta que el uso de cifrado fuerte podría estar bajo fuertes restricciones en su país, compruebe la regulación vigente antes de hacer uso de este software.

Tenga especialmente presente lo siguiente:

- Antes de comenzar a utilizar el instrumento, es conveniente familiarizarse con su interfaz y el sistema que controla, así como con las funciones de sus controles.
- El terminal de explotación debe ser utilizado por personal cualificado, que conozca el equipo y su manejo mediante el manual de uso.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

- Este manual es parte inseparable del terminal de explotación, por lo que debe estar disponible para todos los usuarios del equipo.
- La manipulación del sistema por personal no autorizado provocará la pérdida total de la garantía.
- El fabricante se reserva los derechos a posibles modificaciones y mejoras sobre este manual y equipo.

El icono  indica que existe información extra sobre un elemento de la interfaz, no dude en posar el ratón encima del icono para obtenerla.



Si este manual de instrucciones no le facilita respuesta a su pregunta, puede llamar al Servicio de Atención al Consumidor de su país o a la central de Servicio. Búsquelos en la garantía que le hemos entregado.

Por favor, tenga a mano antes de llamar a la Línea de ayuda, la versión del software que está utilizando, la encontrará en el menú ayuda de la ventana principal.

Para cualquier otro asunto relacionado con servicio o garantía por favor diríjase a la dirección indicada en los documentos de servicio o garantía adjuntados con el producto.

Palabras, imágenes y logotipos como Rockwell, LabVIEW, National Instruments o Ethernet/IP tiene copyright (c) y pertenecen a sus respectivos dueños siendo marca registrada (TM) de los mismos en todo el mundo y están incluidos aquí sin mala intención y meramente con fines informativos.

Características

Este software está diseñado para trabajar con TiM (Tele-immersive Manufacturing), no intente hacerlo funcionar con otra instalación diferente y compruebe que esta no ha cambiado desde que se diseñó este terminal de explotación.



Por favor, lea el documento *“Starting up The System”* para saber cómo poner en marcha la instalación.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Las imágenes de este manual pueden diferir de las que se encuentre haciendo uso del programa, correspondiendo a versiones previas.

El software al que hace referencia el presente manual le permitirá:

- Controlar el estado de TiM.
- Controlar el perímetro de la instalación.
- Exportar datos para ser utilizados por programas externos.

Las ayudas dentro del programa están en español.



Licencia

El presente programa está bajo licencia BSD-3, también llamada BSD revisada.

Cada librería externa de la que se hace uso está bajo su propia licencia que se puede encontrar al final de este manual.

Texto traducido por el usuario Tximitx de Wikipedia²⁹

Texto original en la Open Source Initiative en inglés.³⁰

Copyright (c) 2014, Noel Pueyo
Todos los derechos reservados.

La redistribución y el uso en las formas de código fuente y binario, con o sin modificaciones, están permitidos siempre que se cumplan las siguientes condiciones:

1. Las redistribuciones del código fuente deben conservar el aviso de copyright anterior, esta lista de condiciones y el siguiente descargo de responsabilidad.
2. Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente renuncia en la documentación y/u otros materiales suministrados con la distribución.
3. Ni el nombre de los titulares de derechos de autor ni los nombres de sus colaboradores pueden usarse para apoyar o promocionar productos derivados de este software sin permiso previo y por escrito.

ESTE SOFTWARE SE SUMINISTRA POR NOEL PUEYO "COMO ESTÁ" Y CUALQUIER GARANTÍA EXPRESA O IMPLÍCITAS, INCLUYENDO, PERO NO LIMITADO A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN Y APTITUD PARA UN PROPÓSITO DETERMINADO SON RECHAZADAS. EN NINGÚN CASO NOEL PUEYO SERÁ RESPONSABLE POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENTE (INCLUYENDO, PERO NO LIMITADO A, LA ADQUISICIÓN DE BIENES O SERVICIOS; LA PÉRDIDA DE USO, DEDATOS O DE BENEFICIOS; O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) O POR CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA POR CONTRATO, RESPONSABILIDAD Estricta O AGRAVIO (INCLUYENDO NEGLIGENCIA O CUALQUIER OTRA CAUSA) QUE SURJA DE CUALQUIER MANERA DEL USO DE ESTE SOFTWARE, INCLUSO SI SE HA ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS.

²⁹ http://es.wikipedia.org/wiki/Licencia_BSD#Nueva_Licencia_BSD_o_BSD_modificada_.28de_3_cl.C3.A1usulas.29

³⁰ <http://opensource.org/licenses/BSD-3-Clause>

Requerimientos

Para el uso del terminal de explotación de TiM necesitará:

- Acceso a la instalación de producción teleinmersiva (TiM en sus siglas en inglés)
- Un (1) ordenador con un sistema operativo Linux, OSX o Windows instalado y con acceso a la red donde se encuentra TiM.
- Licencias de Run Time Environment (RTE) de LabVIEW y Manual de instalación³¹
- Un monitor con una resolución de pantalla de al menos 1024x768.

Archivos esenciales.

Por favor compruebe que en la copia que ha recibido se encuentre todo lo necesario para hacer uso del terminal de explotación.

- Un (1) Manual del terminal de explotación en .pdf.
- Un (1) ejecutable con el nombre de TerminaldeExp.exe.
- Una (1) carpeta con el Código fuente del terminal de explotación y de las librerías usadas.
- Un (1) archivo de texto con el nombre usuarios.txt con el nombre de usuario y contraseña que se le adjunta en la garantía del programa.

21.1 Instalación

1. Copie la carpeta comprimida a su ordenador.
2. Compruebe que la instalación este funcionando y el equipo donde está instalado tenga acceso a la red.
3. Descomprima la carpeta donde quiera tenerla instalada
4. Haga doble clic en el TerminaldeExp.exe.

21.2 Configuración

Copie el archivo usuarios.txt a la carpeta file dentro de la carpeta raíz donde ha instalado el terminal de explotación.

Generalidades

³¹ <http://www.ni.com/white-paper/11024/en/>

21.3 Tipos de cuentas

Existen 3 tipos de usuarios:

- Admin: instala y configura la aplicación para que los usuarios.
- Usuario: usa la aplicación.
- None: usuario nulo, creado para que su configuración se aplique cuando exista algún problema inesperado o no haya ningún usuario conectado; también puede ser usado por parte de administrador para dejar sin credenciales a un usuario determinado sin tener que borrarlo.

Medidas de seguridad

El terminal de explotación para TiM dispone de diversas medidas de seguridad para evitar el acceso de terceros a información confidencial

- Los archivos tanto de usuarios como del log están cifrados mediante AES y con claves independientes.
- La contraseña de cada usuario tiene unos requisitos mínimos
- El terminal de explotación se desconectará tras un tiempo predeterminado de inactividad del usuario.
- El terminal de explotación se desconectará de los PLCs tras pasar un tiempo sin que un nuevo usuario acceda al programa.

Todas estas medidas solo han de usarse en caso de despiste o de urgencia, la seguridad de un sistema ha de depender principalmente del usuario por lo tanto:

- No deje el quipo desatendido.
- Cierre su sesión cuando se tenga que ausentar.

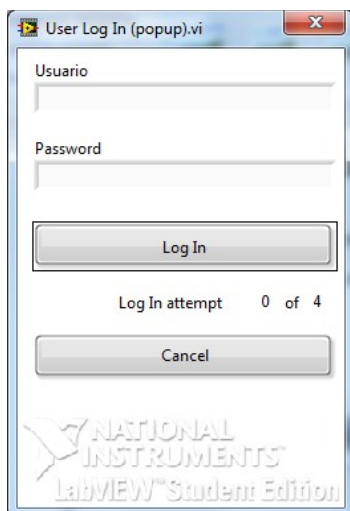
21.4 Seguridad de la contraseña

Aquí se listan los requisitos mínimos que ha de tener una contraseña para que sea válida en el terminal de explotación.

- Más de 8 caracteres.
- Al menos un carácter numérico.
- Al menos una mayúscula.
- Al menos una minúscula.
- Al menos un símbolo.

Ejecutando el Terminal de explotación

21.5 Log In



Tras iniciar el programa nos aparecerá una ventana emergente pidiendo el usuario y la clave, se dispone sólo de 4 intentos para iniciar el terminal de explotación.

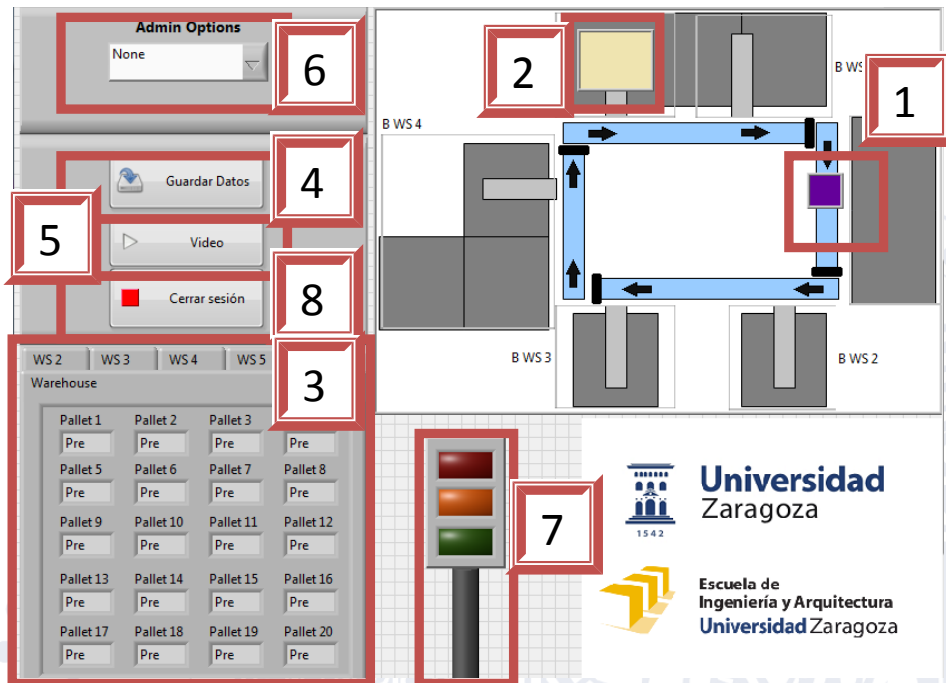
Si no dispone de un usuario contacte con el administrador del terminal de explotación para que nos asigne uno.

Si iniciamos por accidente el terminal de explotación podemos salir del programa presionando a cancelar.

21.6 Pantalla principal

En la pantalla principal podemos interactuar con TiM.

1. Indica en qué posición esta el palé sobre el que se está produciendo.
2. Indica que estación de trabajo estamos viendo.
3. Cada pestaña permite el acceso a los controles e indicadores de la estación de trabajo correspondiente.
(ver sección siguiente)



4. JSON, permite la exportar los datos actuales a un archivo JSON para ser usados en otro proyecto.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

5. Video, permite visualizar el estado de la instalación en directo.
6. Admin Option da acceso a las opciones de administrador del sistema, solo están accesibles si el usuario del sistema tiene cuenta de administrador. (será en profundidad más adelante).
7. Indica las alarmas de todas las estaciones de trabajo.
8. Cerrar sesión, permite salir de la sesión para que posteriormente acceda otro usuario o desconectar el terminal de explotación.



Si se está 10 minutos sin interactuar con el sistema este se desconectará para prevenir el acceso a terceras personas que no deban de poder hacerlo.



Si hace click sobre las estaciones de trabajo de la imagen también puede acceder a la información

21.7 Estaciones de trabajo



El almacén dispone de 20 palés que pueden tomar 3 estados

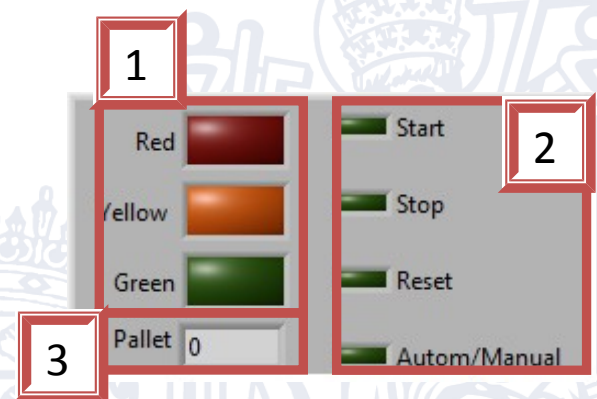
- Pre: Elemento Preprocesado en el almacén
- No: Sin ningún elemento.
- Post: Elemento postprocesado en el almacén

Cada estación de trabajo dispone de 7 indicadores booleanos y uno numérico.

Los 3 primeros [1] indican el estado de la estación:

- Verde: correcto.
- Amarillo: alarma.
- Rojo emergencia.

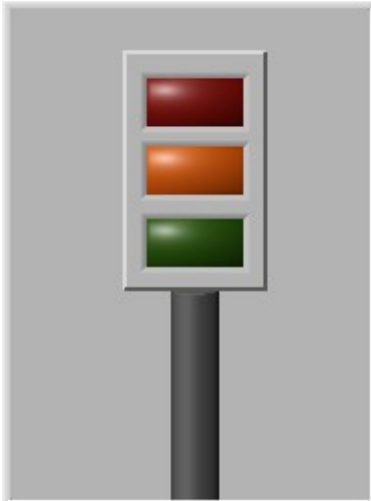
Los 4 [2] siguientes como funciona la estación de trabajo:



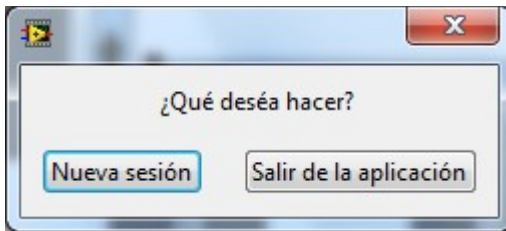
Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

- Start: iniciando.
- Stop: parada.
- Reset: reiniciando.
- Auto/manual: Automático o manual

El indicador numérico **[3]** induca el número del último palé que ha pasado.



21.8 Cierre de sesión



Tras cerrar sesión aparecerá una ventana preguntando si quiere iniciar una nueva sesión o si desea salir del terminal de explotación de TiM.

Si su turno de trabajo es el último, salga de la aplicación, en caso contrario deje la ventana abierta.



Tenga en cuenta que aún no ha desconectado el terminal de explotación de los PLCs, sólo se desconectará saliendo de la aplicación.

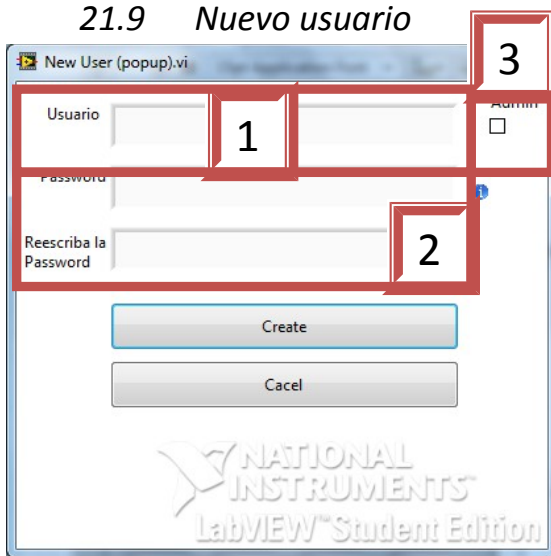


El programa se desconecta de los autómatas por si mismo si el nuevo usuario tarda más del tiempo estipulado en iniciar sesión.

Opciones de administrador

El administrador o administradores del terminal de explotación tiene acceso a un menú que le servirá para configurar y administrar el sistema y los usuarios.

21.9 Nuevo usuario



Desde esta opción puede crear nuevos usuarios para del sistema.

Para ello escriba el nombre del usuario [1] y la contraseña [2] que desea que tenga.

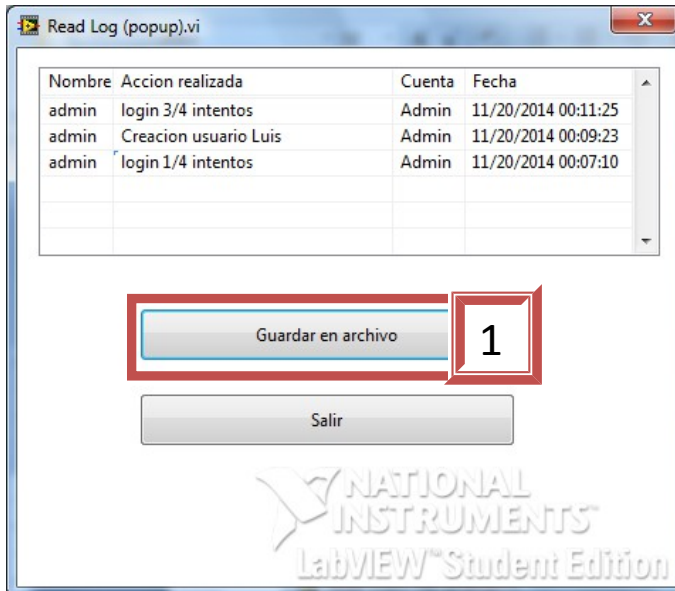
Se le pide que introduzca 2 veces la contraseña para evitar errores de coincidencia al teclearla mal.

Marque la casilla Admin [3] si desea que el nuevo usuario tenga credenciales de administrador.



Recuerde que la contraseña ha de cumplir los requisitos que puede encontrar en: generalidades>> Seguridad de las contraseñas.

21.10 Acceso al log



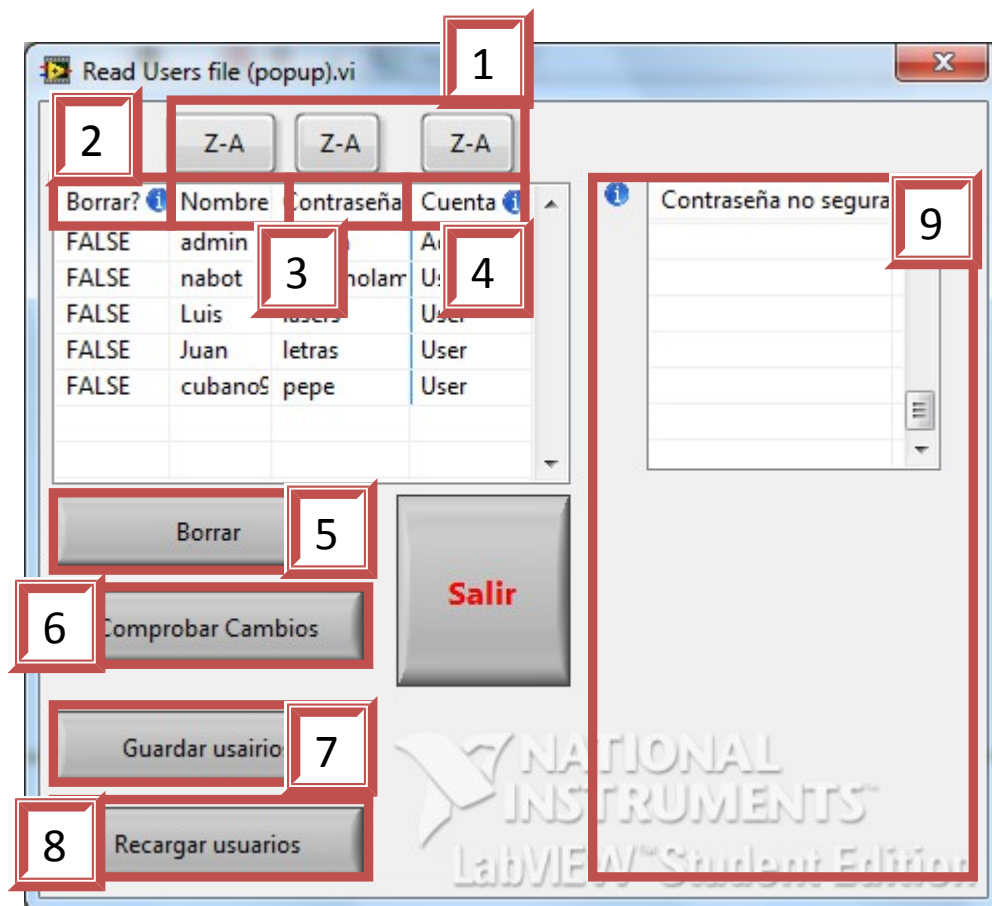
El log del terminal de explotación se mantiene cifrado en la capeta file, pudiéndose acceder a él sólo mediante este menú.

Aquí el administrador dispone de una relación de que usuarios han accedido al sistema a qué hora y las acciones realizadas en él.

También se permite exportar el log a un archivo XML **[1]** para su posterior manejo.

21.11 Gestión de usuarios

En esta pantalla el administrador dispone de múltiples opciones para la gestión de usuarios.



- [1] Teclas Z-A/A-Z permiten organizar usuarios en orden alfabético ascendente (A-Z) o descendente (Z-A) de los nombres, contraseñas y tipos de cuenta.



Si desea deshabilitar un usuario pero no quiere borrar su cuenta puede poner None como tipo de cuenta.

- [2] Tabla- borrar? Seleccionando true el valor se borrarán los datos del usuario de esa fila cuando se presiones borrar [5].
- [3] Nombre y Contraseña: permiten modificar libremente ambos campos.
- [4] Tipo de cuenta: nos ofrecerá un menú desplegable con las 3 opciones de cuenta.



Los acrónimos en el indicador de contraseña

#: Carácter numérico.

Up: mayúscula.

Low: minúscula.

Sym: símbolo.

<8: No hay caracteres.

[6] Comprobar cambios: comprueba que los cambios realizados en la tabla no tienen ningún problema, en caso contrario aparecerán 2 avisos en el lateral [9] Usuario duplicado y contraseña no segura que indicaran los errores existentes.

[7] Salvar: guarda las modificaciones en el archivo sólo.

[8] Volver a cargar: vuelve a cargar los últimos datos guardados.

Resolución de problemas

Averías conocidas solucionables por parte del usuario	
Síntoma	Posible Causa
Ausencia de imagen (la pantalla aparece oscura).	<ul style="list-style-type: none">➤ Revise la conexión entre el monitor y el ordenador.➤ Compruebe que el cable de alimentación esté conectado a la red eléctrica.➤ Compruebe que el ordenador está encendido.
Aparecen pequeños puntos negros.	<ul style="list-style-type: none">➤ La pantalla está compuesta de píxeles. Los pequeños puntos negros y/o brillantes (píxeles) no son síntoma de un funcionamiento defectuoso.
No aparece ninguna imagen o está en blanco y negro.	<ul style="list-style-type: none">➤ Ajuste los valores de color.➤ Compruebe los valores de contraste y brillo de la imagen.
Hay interferencias en la imagen.	<ul style="list-style-type: none">➤ Trate de identificar el aparato eléctrico que las genera y aléjelo de él.➤ Enchufe el televisor en una toma eléctrica distinta.
No se ve la imagen de TiM o de alguno de los indicadores.	<ul style="list-style-type: none">➤ Compruebe que existen los archivos background.png, box.png y WS.png
No recuerdo la contraseña.	<ul style="list-style-type: none">➤ Si es usted usuario contacte con su administrador.➤ Si es usted administrador: contacte con su proveedor del software.
No encuentro el archivo JSON.	<ul style="list-style-type: none">➤ Si no se encuentra en la carpeta file consulte con el servicio técnico.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

Por qué no veo el log.

- Puede que el archivo haya sido borrado, se creará uno nuevo cuando se inicie sesión.

Si existen otras incidencias no documentadas, consulte al servicio técnico.

Apagando y cerrando el terminal de explotación el equipo se pueden solucionar algunos de los problemas, inténtelo antes de llamarnos.



21.12 *Licencias*

21.12.1 **VideoLAN**

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in objects code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies,

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

21.12.2 i3JSON

Interactive Internet Interface: JSON Toolkit for LabVIEW (i3 JSON)

Copyright (c) 2013 Milan Raj

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

i3 JSON was based on the C# JSON Parser written by Patrick van Bergen available at the following URL: [http://techblog.procurios.nl/k/news/view/14605/14863/how-do-i-write-my-own-parser-\(for-json\).html](http://techblog.procurios.nl/k/news/view/14605/14863/how-do-i-write-my-own-parser-(for-json).html) and released under the following license:

Copyright (c) 2008 Patrick van Bergen

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

21.12.3 AES toolkit

This archive contains AES library in pure LabVIEW (it contains only native LabVIEW code).

It was written by me (c) Igor Titov (igor.ev.titov@gmail.com) in 2011 and uploaded to the web-site www.vigods.com in 2012.

This software went through NI evaluation and was granted "Compatible with LabVIEW" status.

I have taken care in the preparation of this software, but make no expressed or implied warranty of any kind and assume no responsibility for errors. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the software contained herein.

Please note that use of strong encryption may be under regulations in your country. Please check your own country's regulations on the use of strong cryptography before using or redistributing this file.

Visit www.vigods.com to know more about this product, its author and other LabVIEW-related information.

Please visit <http://www.vigods.com> to learn more about this and other LabVIEW libraries.

Copyright (C) 2012 Igor Titov igor.ev.titov@gmail.com (Certified LabVIEW Developer)

All rights reserved.

Redistribution and use without modification are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions of source code and in binary form may be freely used in all sorts of projects (including commercial ones).

It is not obligatory to place copyright notice, this list of conditions and the following disclaimer in your product but you must mention the source (www.vigods.com, Igor Titov) on the web-site of the product.

Diseño del nuevo SCADA con LabVIEW para el ADMT de UCLan

* Neither the name of "viGods", "vigods.com", "Igor Titov", nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission (except in situations mentioned in the terms and conditions of use of the "viGods").

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

21.12.4 Type Sensitive Popup

Copyright (c) 2009, David Saunders "JDave"

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

21.12.5 Filename generator for LabVIEW

Copyright (c) 2012, Jtagg

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.