

**UNIVERSIDAD POLITÉCNICA SALESIANA**

**SEDE CUENCA**

**CARRERA DE INGENIERÍA ELÉCTRICA**

*Trabajo de titulación previo  
a la obtención del título de  
Ingeniero Eléctrico*

**PROYECTO TÉCNICO CON ENFOQUE INVESTIGATIVO:**

**“IMPLEMENTACIÓN DEL SISTEMA DE COMUNICACIÓN IEC 61850  
PARA MONITOREO Y CONTROL DEL MÓDULO DE PRUEBAS PARA EL  
LABORATORIO DE PROTECCIONES DE LA UNIVERSIDAD  
POLITÉCNICA SALESIANA SEDE CUENCA”**

**AUTORES:**

RODRIGO NIKOLAS TORRES LUNA

OSCAR JAMIL FAREZ JUMBO

**TUTOR:**

ING. FLAVIO ALFREDO QUIZHPI PALOMEQUE

CUENCA - ECUADOR

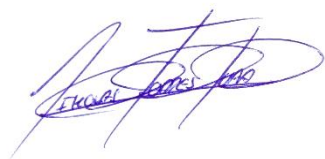
2021

## CESIÓN DE DERECHOS DE AUTOR

Nosotros, Rodrigo Nikolas Torres Luna con documento de identificación N° 0106889801 y Oscar Jamil Farez Jumbo con documento de identificación N° 0705786994, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación: **“IMPLEMENTACIÓN DEL SISTEMA DE COMUNICACIÓN IEC 61850 PARA MONITOREO Y CONTROL DEL MÓDULO DE PRUEBAS PARA EL LABORATORIO DE PROTECCIONES DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE CUENCA”**, mismo que ha sido desarrollado para optar por el título de: *Ingeniero Eléctrico*, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores, nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, diciembre de 2021.



Rodrigo Nikolas Torres Luna

C.I. 0106889801



Oscar Jamil Farez Jumbo

C.I. 0705786994

## CERTIFICACIÓN

Yo, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **“IMPLEMENTACIÓN DEL SISTEMA DE COMUNICACIÓN IEC 61850 PARA MONITOREO Y CONTROL DEL MÓDULO DE PRUEBAS PARA EL LABORATORIO DE PROTECCIONES DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE CUENCA”**, realizado por Rodrigo Nikolas Torres Luna y Oscar Jamil Farez Jumbo, obteniendo el *Proyecto Técnico con enfoque investigativo*, que cumple con los requisitos estipulados por la Universidad Politécnica Salesiana.

Cuenca, diciembre de 2021.

A handwritten signature in blue ink, consisting of a large, stylized initial 'F' followed by several cursive letters, likely representing the name of the certifier.

Ing. Flavio Alfredo Quizhpi Palomeque

C.I. 0102257482

## DECLARATORIA DE RESPONSABILIDAD

Nosotros, Rodrigo Nikolas Torres Luna con documento de identificación N° 0106889801 y Oscar Jamil Farez Jumbo con documento de identificación N° 0705786994, autores del trabajo de titulación: **“IMPLEMENTACIÓN DEL SISTEMA DE COMUNICACIÓN IEC 61850 PARA MONITOREO Y CONTROL DEL MÓDULO DE PRUEBAS PARA EL LABORATORIO DE PROTECCIONES DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE CUENCA”**, certificamos que el total contenido del *Proyecto Técnico con enfoque investigativo*, es de nuestra exclusiva responsabilidad y autoría.

Cuenca, diciembre de 2021.



Rodrigo Nikolas Torres Luna

C.I. 0106889801



Oscar Jamil Farez Jumbo

C.I. 0705786994

## **DEDICATORIAS**

A mis padres, Joselo y Eva por ser un ejemplo y un pilar fundamental en el transcurso de esta carrera, les agradezco por haber estado pendientes cada día del proceso de titulación y con el fin de apoyarme y poder culminar el presente trabajo.

A mi Abuelo y hermanos y familiares que me brindaron su apoyo y cariño incondicional.

Dedico este trabajo a todas las personas que me han apoyado para la realización del mismo, a mis padres Manuel y Gladys, quienes siempre creyeron en mí, con sus consejos y aliento me han impulsado a cumplir mis metas y a crecer cada día más como persona y profesional y a todos mis amigos y demás familiares.

## **AGRADECIMIENTOS**

Un agradecimiento al tutor Ing. Flavio Quizhpi, al Dr. Arturo Peralta y al Ing. Carlos Vallejo por compartir su conocimiento con nosotros, y su apoyo para la culminación del proyecto de titulación.

A mi compañero Oscar Farez por su interés y esfuerzo por sacar el proyecto adelante.

Agradecer de manera muy especial a tutor Ing. Flavio Quizhpi y al Ing. Carlos Vallejo y cada uno de los docentes que siempre nos brindaron su apoyo y conocimiento para el desarrollo de este proyecto.

A mi compañero Nikolas Torres por aquella dedicación y entusiasmo que se puso desde un principio para la culminación de este proyecto.

## RESUMEN

El presente proyecto técnico práctico tiene como finalidad la implementación del sistema de comunicación basado en la norma IEC 61850, el cual se desarrolló en dos partes, la primera con el proyecto en general y la segunda parte con una guía de ocho pruebas.

El proyecto general consta de la creación de la Red LAN, la cual se encargó de que todos los equipos como IED, RTU, PC y CMC, estén comunicados entre ellos, para luego implementar el estándar IEC 61850, junto a sus mensajerías como GOOSE, SV y MMS. Asimismo, el desarrollo de Data Sets, reportes e informes y alarmas dentro del software NCD de Novatech<sup>®</sup>, con la finalidad de crear una interfaz gráfica amigable con el usuario en el software Inkscape<sup>™</sup>, para posteriormente con la ayuda de la maleta de pruebas CMC356, inyectar voltajes y corrientes, los cuales van a ser monitorizados en el entorno WEB Server de la RTU.

La guía de pruebas se basa en la documentación de ensayos, enfocado en el estudiante, el cual le permitirá la creación de un proyecto desde cero hasta la monitorización de datos en el HMI.

Los bancos de pruebas constan de tres partes: dos bancos contienen IED's de la marca SIEMENS<sup>®</sup> y el otro banco contiene IED's de la marca SCHNEIDER ELECTRIC<sup>®</sup>, la RTU y el Switch, con la finalidad de que estos bancos sean amigables e intuitivos para el estudiante y ellos puedan familiarizarse con varios equipos de diferentes marcas que se encuentran dentro de una subestación eléctrica.

Palabras Claves: IED, RTU, PC, CMC, GOOSE, MMS, SV.

## **ABSTRACT**

The purpose of this technical practical project is the implementation of the communication system based on the IEC 61850 standard, which was developed in two parts, the first one with the project in general and the second part with a guide of six tests.

The general project consists of the creation of the LAN Network, which ensured that all equipment such as IED, RTU, PC and CMC, are communicated with each other, and then implement the IEC 61850 standard, along with its messaging such as GOOSE, SV and MMS. Also, the development of Data Sets, reports and reports and alarms within the Novatech<sup>®</sup> NCD software, in order to create a user-friendly graphical interface in the Inkscape<sup>™</sup> software, and then with the help of the CMC356 test bag, inject voltages and currents, which will be monitored in the WEB Server environment of the RTU.

The test guide is based on test documentation, focused on the student, which will allow the creation of a project from scratch to the monitoring of data in the HMI.

The test benches consist of three parts, two benches contain IED's of the SIEMENS<sup>®</sup> brand and the other bench contains IED's of the SCHNEIDER ELECTRIC<sup>®</sup> brand, the RTU and the Switch, with the purpose that these benches are friendly and intuitive for students and they can become familiar with various equipment of different brands that are found within an electrical substation.

Keywords: IED, RTU, PC, CMC, GOOSE, MMS, SV.



# ÍNDICE DE CONTENIDOS

<b>CESIÓN DE DERECHOS DE AUTOR</b> .....	i
<b>CERTIFICACIÓN</b> .....	ii
<b>DECLARATORIA DE RESPONSABILIDAD</b> .....	iii
<b>DEDICATORIAS</b> .....	iv
<b>AGRADECIMIENTOS</b> .....	v
<b>RESUMEN</b> .....	vi
<b>ABSTRACT</b> .....	vii
<b>ÍNDICE DE CONTENIDOS</b> .....	viii
<b>ÍNDICE DE FIGURAS</b> .....	xiii
<b>LISTA DE TABLAS</b> .....	xxi
<b>ABREVIATURAS</b> .....	xxii
<b>CAPÍTULO I</b> .....	23
<b>1. EL PROBLEMA</b> .....	23
<b>1.1. Descripción del problema</b> .....	23
<b>1.2. Antecedentes</b> .....	23
<b>1.3. Importancia y Alcances</b> .....	24
<b>1.4. Delimitación</b> .....	24
<b>1.5. Objetivos</b> .....	24
<b>1.5.1. Objetivo General</b> .....	24
<b>1.5.2. Objetivos Específicos</b> .....	25
<b>1.6. Marco Metodológico</b> .....	26
<b>1.6.1. Estado del arte</b> .....	26
<b>1.6.2. Análisis</b> .....	26
<b>1.6.3. Diseño</b> .....	26
<b>1.6.4. Implementación</b> .....	27
<b>1.6.5. Resultados</b> .....	27
<b>CAPÍTULO 2</b> .....	28
<b>2. MARCO TEÓRICO</b> .....	28
<b>2.1. Automatización de subestaciones</b> .....	28
<b>2.1.1. Nivel de Proceso</b> .....	28
<b>2.1.2. Nivel de Bahía</b> .....	28
<b>2.1.3. Nivel de Estación</b> .....	29

<b>2.2.</b>	<b>Protocolos de comunicación .....</b>	<b>29</b>
2.2.1.	MODBUS.....	29
2.2.2.	DNP 3.0 .....	30
2.2.3.	IEC 60870 .....	30
2.2.3.1.	IEC 60870-5-101.....	30
2.2.3.2.	IEC 60870-5-103.....	31
2.2.3.3.	IEC 60870-5-104.....	31
2.2.4.	IEC 61850 .....	31
2.2.4.1.	IEC 61850-1 .....	32
2.2.4.2.	IEC 61850-2.....	32
2.2.4.3.	IEC 61850-3.....	33
2.2.4.4.	IEC 61850-4.....	33
2.2.4.5.	IEC 61850-5.....	33
2.2.4.6.	IEC 61850-6.....	33
2.2.4.7.	IEC 61850-7.....	34
2.2.4.8.	IEC 61850-8.....	35
2.2.4.9.	IEC 61850-9.....	35
<b>2.3.</b>	<b>Unidades de proceso disponible .....</b>	<b>36</b>
2.3.1.	RTU NOVATECH® ORION LXM .....	36
2.3.2.	Switch industrial administrable HIRSCHMANN® tipo GREYHOUND..	37
2.3.3.	Analizador de redes ION7400 .....	39
2.3.4.	CMC 356 equipo de pruebas de protección universal y herramienta de puesta en servicio.....	40
2.3.5.	Relés SIEMENS® de la familia SIPROTEC 5 .....	41
2.3.5.1.	Relé de protección a distancia compacto (SIPROTEC 7SA86) .....	42
2.3.5.2.	Relé de sobrecorriente y protección del alimentador (SIPROTEC 7SJ85) 44	
2.3.6.	Relés SCHNEIDER ELECTRIC® EASERGY P3 .....	45
2.3.6.1.	Relé de protección del alimentador (P3F30).....	46
2.3.6.2.	Relé de protección de línea, diferencial y distancia (P3L30).....	47
2.3.7.	Relés SCHNEIDER ELECTRIC® EASERGY P5 .....	47
2.3.7.1.	Relé de protección diferencial y de transformador (P5F30) .....	48
2.3.7.2.	Relé de protección del motor (P5M30).....	49
<b>CAPÍTULO 3.....</b>		<b>51</b>
<b>3.</b>	<b>ESTANDAR IEC 61850.....</b>	<b>51</b>

3.1.	Modelo de datos .....	52
3.1.1.	Nodos Lógicos.....	52
3.2.	Tipos de mensajes y su estructura .....	54
3.2.1.	Mensajería MMS .....	54
3.2.2.	Mensajería GOOSE.....	55
3.2.3.	Mensajería SV .....	56
3.3.	Lenguaje de configuración de subestación SCL .....	57
CAPÍTULO 4.....		60
4.	MANUAL DE IMPLEMENTACIÓN .....	60
4.1.	Herramientas de software.....	61
4.1.1.	NCD.....	62
4.1.2.	OMICRON® Test Universe.....	63
4.1.3.	DIGSI® 5 .....	64
4.1.4.	INKSCAPE™ .....	66
4.2.	Implementación de la red LAN.....	67
4.2.1.	Implementación.....	68
4.2.2.	Ajuste de parámetros de red del switch industrial.....	69
4.2.3.	Ajuste de parámetros de red de la RTU.....	69
4.2.4.	Ajuste de parámetros de red del PC.....	71
4.2.5.	Ajuste de parámetros de red en CMC 356.....	72
4.2.6.	Ajuste de parámetros de red en IED's SIEMENS® .....	74
4.2.7.	Verificación de red.....	78
4.3.	Implementación del estándar IEC 61850 .....	80
4.3.1.	Ajuste de IED's SIEMENS® en DIGSI® 5 .....	80
4.3.2.	Creación estación IEC 61850 .....	84
4.3.3.	Creación de un proyecto en NCD .....	90
4.3.4.	Exportación de proyecto a la RTU .....	95
4.3.5.	Creación de HMI en Inkscape™ .....	98
4.3.6.	Exportación de archivos SVG a la RTU .....	102
4.3.7.	Análisis de funcionamiento (Prueba de comunicación).....	104
4.3.8.	Creación de alarmas y archivos.....	109
4.4.	Guía de pruebas.....	116
4.4.1.	Prueba #1 – Creación de red LAN IEC 61850.....	116
4.4.1.1.	Objetivos.....	116

4.4.1.2.	Recursos.....	116
4.4.1.3.	Descripción y funcionamiento.....	116
4.4.1.4.	Desarrollo .....	117
4.4.1.5.	Conclusiones.....	123
4.4.1.6.	Recomendaciones.....	123
4.4.2.	<b>Prueba #2 - Cargar archivo SCL a la RTU Orion LXM.....</b>	124
4.4.2.1.	Objetivos.....	124
4.4.2.2.	Recursos.....	124
4.4.2.3.	Descripción y funcionamiento.....	124
4.4.2.4.	Desarrollo .....	124
4.4.2.5.	Conclusiones.....	136
4.4.2.6.	Recomendaciones.....	137
4.4.3.	<b>Prueba #3 - Desarrollo de HMI en Inkscape™.....</b>	138
4.4.3.1.	Objetivos.....	138
4.4.3.2.	Recursos.....	138
4.4.3.3.	Descripción y funcionamiento.....	138
4.4.3.4.	Desarrollo .....	138
4.4.3.5.	Conclusiones.....	143
4.4.3.6.	Recomendaciones.....	143
4.4.4.	<b>Prueba #4 - Prueba de comunicación entre HMI e IED's.....</b>	145
4.4.4.1.	Objetivos.....	145
4.4.4.2.	Recursos.....	145
4.4.4.3.	Descripción y funcionamiento.....	145
4.4.4.4.	Desarrollo .....	145
4.4.4.5.	Conclusiones.....	150
4.4.4.6.	Recomendaciones.....	151
4.4.5.	<b>Prueba #5 - Manejo de mensajería y alarmas.....</b>	152
4.4.5.1.	Objetivos.....	152
4.4.5.2.	Recursos.....	152
4.4.5.3.	Descripción y funcionamiento.....	152
4.4.5.4.	Desarrollo .....	152
4.4.5.5.	Conclusiones.....	157
4.4.5.6.	Recomendaciones.....	157
4.4.6.	<b>Prueba #6 – Usuarios y Permisos.....</b>	158

4.4.6.1.	Objetivos .....	158
4.4.6.2.	Recursos .....	158
4.4.6.3.	Descripción y funcionamiento.....	158
4.4.6.4.	Desarrollo .....	160
4.4.6.5.	Conclusiones .....	164
4.4.6.6.	Recomendaciones .....	164
4.4.7.	<b>Prueba #7 – Comparativa entre la señal de disparo por cable y señal de disparo por GOOSE.....</b>	<b>165</b>
4.4.7.1.	Objetivos .....	165
4.4.7.2.	Recursos .....	165
4.4.7.3.	Descripción y funcionamiento.....	165
4.4.7.4.	Desarrollo .....	166
4.4.7.5.	Conclusiones .....	168
4.4.7.6.	Recomendaciones .....	168
4.4.8.	<b>Prueba #8 - Envío remoto con el protocolo IEC 60870-5-101/104.....</b>	<b>169</b>
4.4.8.1.	Objetivos .....	169
4.4.8.2.	Recursos .....	169
4.4.8.3.	Descripción y funcionamiento.....	169
4.4.8.4.	Desarrollo .....	169
4.4.8.5.	Conclusiones .....	174
4.4.8.6.	Recomendaciones .....	174
<b>CAPITULO 5.....</b>		<b>175</b>
<b>5. CONCLUSIONES Y RECOMENDACIONES .....</b>		<b>175</b>
<b>5.1. CONCLUSIONES.....</b>		<b>175</b>
<b>5.2. RECOMENDACIONES.....</b>		<b>176</b>
<b>BIBLIOGRAFÍA.....</b>		<b>177</b>
<b>ANEXO 1.....</b>		<b>180</b>
<b>ANEXO 2.....</b>		<b>183</b>

## ÍNDICE DE FIGURAS

Figura 1: Flujograma de proceso metodológico a aplicar. Fuente: Autores. ....	25
Figura 2: Arquitectura básica de la automatización de SE. Fuente: [1].....	28
Figura 3: Vista del panel frontal del Orion LXM. Fuente: [5].....	37
Figura 4: Switch Industrial GREYHOUND. Fuente: [6].....	38
Figura 5: Analizador de redes ION 7400. Fuente: [7]. ....	39
Figura 6: Unidad de pruebas CMC 356. Fuente: [8].....	40
Figura 7: Dispositivos y campo de aplicación de la familia SIPROTEC 5. Fuente: [10]. ....	42
Figura 8: Vista frontal y posterior de dispositivos SIPROTEC 5. Fuente: [11]. ....	44
Figura 9: Rango de operación de los dispositivos P3. Fuente: [12].....	46
Figura 10: Panel frontal de dispositivos P3F30/P3L30. Fuente: [13].....	47
Figura 11: Rango de operación de los dispositivos P5. Fuente: [15].....	48
Figura 12: Panel frontal de Easergy P5x30. Fuente: [15].....	49
Figura 13. Modelo de datos según el estándar. Fuente: Autores. ....	53
Figura 14. Estructura del nodo lógico. Fuente: Autores. ....	54
Figura 15. Prioridad en transmisión de mensajes GOOSE. Fuente: Autores. ....	56
Figura 16. Mensajería SV. Fuente: Autores.....	57
Figura 17. Lenguaje SCL. Fuente: Autores. ....	59
Figura 18. Proceso metodológico del manual de implementación. Fuente: Autores. ....	61
Figura 19: Software NCD. Fuente: Autores.....	62
Figura 20. Software OMICRON <sup>®</sup> Test Universe - Version 4.00. Fuente: Autores... ..	63
Figura 21: Pasos para asociar equipo OMICRON <sup>®</sup> con PC. Fuente: Autores.....	64
Figura 22: Software DIGSI <sup>®</sup> 5 - Versión 7.91. Fuente: Autores. ....	65
Figura 23: Visualización del administrador de controladores de dispositivos. Fuente: Autores. ....	66
Figura 24: Software INKSCAPE <sup>™</sup> - Versión 0.92. Fuente: Autores. ....	67
Figura 25: Topología estrella simple a implementar. Fuente: Autores.....	68
Figura 26: Pasos para configurar los parámetros de red del switch industrial. Fuente: Autores. ....	69
Figura 27: Creación de conexión serial en la RTU. Fuente: Autores. ....	70

Figura 28: Pasos para configurar los parámetros de red de la RTU. Fuente: Autores. .....	71
Figura 29: Pasos para configurar la red del PC. Fuente: Autores. ....	71
Figura 30: Propiedades de Ethernet. Fuente: Autores.....	72
Figura 31: Parámetros a configurar en la PC. Fuente: Autores.....	72
Figura 32: Ventana del módulo OMICRON Device Link. Fuente: Autores. ....	73
Figura 33: Configuración de la red local. Fuente: Autores.....	73
Figura 34: Ajustes de red establecidos en equipo OMICRON <sup>®</sup> . Fuente: Autores.....	74
Figura 35: Vista del panel frontal del equipo SIPROTEC 5. Fuente: Autores. ....	75
Figura 36: Panel frontal del IED SIEMENS <sup>®</sup> . Fuente: Autores. ....	76
Figura 37: Menú de Hardware y protocolos en DIGSI <sup>®</sup> 5. Fuente: Autores. ....	77
Figura 38: Propiedades del puerto de comunicación en DIGSI <sup>®</sup> 5. Fuente: Autores.	77
Figura 39: Ventana para cargar la configuración en el equipo. Fuente: Autores.....	78
Figura 40: Ventana de solicitud de código de confirmación en DIGSI <sup>®</sup> 5. Fuente: Autores. ....	78
Figura 41: Ventana Ejecutar de Windows. Fuente: Autores.....	79
Figura 42: Ventana Símbolo del Sistema para el comando PING. Fuente: Autores.	79
Figura 43. Ajuste de nombre IEC 61850 del IED. Fuente: Autores. ....	80
Figura 44. Ajuste de interface IP del IED. Fuente: Autores. ....	81
Figura 45. Ajuste de protocolos de comunicación del IED. Fuente: Autores.....	81
Figura 46. Vista de la interface Homepage del puerto E del IED. Fuente: Autores. .	82
Figura 47: Ajustes del equipo referente a la comunicación IEC 61850. Fuente: Autores. ....	83
Figura 48. Ajuste de seguridad para el acceso a la red. Fuente: Autores.....	83
Figura 49. Ajuste del modelo de datos del IED. Fuente: Autores.....	84
Figura 50. Pasos para la creación de la estación IEC 61850. Fuente: Autores.....	85
Figura 51. Ventana del configurador del sistema IEC 61850. Fuente: Autores. ....	85
Figura 52. Vista del módulo Subestación en el configurador del sistema. Fuente: Autores. ....	86
Figura 53. Vista del módulo GOOSE en el configurador del sistema. Fuente: Autores. ....	87
Figura 54. Pasos para configurar la mensajería GOOSE. Fuente: Autores. ....	87
Figura 55. Pasos para configurar el módulo de Informes y registros. Fuente: Autores. .....	88

Figura 56. Vista del panel de Control de informe y log bloqueados. Fuente: Autores. .....	89
Figura 57. Pasos para importar cambios al DIGSI® 5. Fuente: Autores.....	89
Figura 58. Pasos para crear un proyecto en NCD. Fuente: Autores. ....	90
Figura 59. Pasos para configurar el protocolo cliente/servidor en el NCD. Fuente: Autores. ....	91
Figura 60. Pasos para importar el archivo SCL de los IED's en el NCD. Fuente: Autores. ....	92
Figura 61. Selección de archivo SCD correspondiente al IED. Fuente: Autores. ....	92
Figura 62. Selección de datos para los puntos de entrada del IED. Fuente: Autores.	93
Figura 63. Selección de datos para los puntos de salida del IED. Fuente: Autores. ..	93
Figura 64. Pasos para configurar el protocolo XML en el NCD. Fuente: Autores....	94
Figura 65. Selección de datos para los puntos de entrada en el puerto XML. Fuente: Autores. ....	95
Figura 66. Selección de datos para los puntos de salida en el puerto XML. Fuente: Autores. ....	95
Figura 67. Ajustes para crear conexión online vía red. Fuente: Autores. ....	96
Figura 68. Pasos para realizar la comunicación SSH entre la PC y la ORION. Fuente: Autores. ....	97
Figura 69. Pasos para transferir datos y reiniciar la ORION. Fuente: Autores.....	98
Figura 70. Ventana de trabajo del software Inkscape™. Fuente: Autores.....	99
Figura 71. Vista del archivo HMI en el Inkscape™. Fuente: Autores.....	99
Figura 72. Ajustes realizados a los objetos “botones” en la extensión HMI. Fuente: Autores. ....	100
Figura 73. Ajustes realizados a los objetos “luminicos” en la extensión HMI. Fuente: Autores. ....	101
Figura 74. Vista del archivo Arquitectura en el Inkscape™. Fuente: Autores. ....	101
Figura 75. Ajuste realizado a la etiqueta de comunicación. Fuente: Autores. ....	102
Figura 76. Ventana inicial del WEBserver. Fuente: Autores. ....	102
Figura 77. Pasos para exportar archivos SVG a la ORION. Fuente: Autores. ....	103
Figura 78. Pasos para configurar archivos como acceso directo en el WEBserver. Fuente: Autores. ....	103
Figura 79. Ventana Device del WEBserver. Fuente: Autores. ....	104
Figura 80. Ventana Datavalues del WEBserver. Fuente: Autores. ....	105



Figura 81. Variables del HMI vistas del WEBserver. Fuente: Autores. ....	105
Figura 82. Vista del archivo HMI en el WEBserver. Fuente: Autores. ....	106
Figura 83. Inyección de tensiones y corrientes desde la CMC 356. Fuente: Autores. .....	106
Figura 84. Vista del archivo Arquitectura en el WEBserver. Fuente: Autores.....	107
Figura 85. Ventana Wireshark. Fuente: Autores.....	107
Figura 86. Trafico de paquete de datos GOOSE entre IED's. Fuente: Autores.....	108
Figura 87. Trafico de la mensajería GOOSE ante una falla. Fuente: Autores. ....	108
Figura 88. Trafico de la mensajería frente a la desconexión del IED de la red. Fuente: Autores. ....	109
Figura 89. Pasos para configurar el complemento AAR. Fuente: Autores.....	110
Figura 90. Pasos para seleccionar las variables necesarias en el módulo AAR. Fuente: Autores. ....	111
Figura 91. Pasos para añadir páginas de alarmas en el Annunciator. Fuente: Autores. .....	111
Figura 92. Ajustes realizados para las notificaciones de las Alarmas. Fuente: Autores. .....	112
Figura 93. Ventana Annunciator del WEBserver. Fuente: Autores.....	113
Figura 94. Notificación de la alarma por falta de comunicación con el IED1. Fuente: Autores. ....	113
Figura 95. Registro de la alarma por falta de comunicación con el IED1. Fuente: Autores. ....	114
Figura 96. Vista de las notificaciones de alarmas en el Annunciator. Fuente: Autores. .....	115
Figura 97. Topología de red para Prueba #1. Fuente: Autores. ....	116
Figura 98. Ajustes de direccionamiento IP del switch en Prueba #1. Fuente: Autores. .....	118
Figura 99. Creación de conexión serial en la RTU para Prueba #1. Fuente: Autores. .....	119
Figura 100. Ajustes de direccionamiento IP de la RTU para Prueba #1. Fuente: Autores. ....	119
Figura 101. Ajustes de direccionamiento IP del IED en Prueba #1. Fuente: Autores. .....	120

Figura 102. Ajustes de direccionamiento IP del PC en Prueba #1. Fuente: Autores. .....	121
Figura 103. Ajustes de direccionamiento IP de la CMC en Prueba #1. Fuente: Autores.....	122
Figura 104. Pasos para verificar red en Prueba #1. Fuente: Autores.....	122
Figura 105. Pasos para añadir IED's para Prueba #2. Fuente: Autores.....	125
Figura 106. Ajuste de nombre IEC 61850 del IED para Prueba #2. Fuente: Autores. .....	125
Figura 107. Ajuste del direccionamiento IP del IED en Prueba #2. Fuente: Autores. .....	126
Figura 108. Ajuste de protocolo de comunicación del IED para Prueba #2. Fuente: Autores.....	126
Figura 109. Ajuste de la comunicación IEC 61850 para Prueba #2. Fuente: Autores. .....	127
Figura 110. Ajuste de seguridad de acceso a la red para Prueba #2. Fuente: Autores. .....	127
Figura 111. Ajuste del modelo de datos para Prueba #2. Fuente: Autores.....	128
Figura 112. Pasos para la creación de la estación IEC 61850 en Prueba #2. Fuente: Autores.....	129
Figura 113. Pasos para crear dataSets en Prueba #2. Fuente: Autores.....	130
Figura 114. Pasos para crear los reportes para Prueba #2. Fuente: Autores.....	130
Figura 115. Pasos para importar cambios al DIGSI® 5 para Prueba #2. Fuente: Autores.....	131
Figura 116. Pasos para configurar protocolo cliente/servidor en Prueba #2. Fuente: Autores.....	131
Figura 117. Pasos para importar archivo SCL al NCD para Prueba #2. Fuente: Autores.....	132
Figura 118. Selección de datos para las Inputs en Prueba #2. Fuente: Autores.....	133
Figura 119. Pasos para configurar protocolo XML en Prueba #2. Fuente: Autores.	133
Figura 120. Selección de datos para las Inputs del XML en Prueba #2. Fuente: Autores.....	134
Figura 121. Pasos para la comunicación SSH entre PC y ORION para Prueba #2. Fuente: Autores.....	134

Figura 122. Pasos para cargar la configuración a la ORION para Prueba #2. Fuente: Autores. ....	135
Figura 123. Ventana Device del WEBserver para Prueba #2. Fuente: Autores. ....	136
Figura 124. Variables HMI vistas desde el WEBserver para Prueba #2. Fuente: Autores. ....	136
Figura 125. Ajustes para crear proyecto en Inkscape™ para Prueba #3. Fuente: Autores. ....	139
Figura 126. Ajuste para ventana HMI en Prueba #3. Fuente: Autores. ....	140
Figura 127. Creación de diagrama unifilar para Prueba #3. Fuente: Autores. ....	140
Figura 128. Vista del menú “Extension” en el Inkscape™ para Prueba #3. Fuente: Autores. ....	141
Figura 129. Ajustes en extensión HMI para Prueba #3. Fuente: Autores. ....	142
Figura 130. Ajustes de los objetos botones en el HMI para Prueba #3. Fuente: Autores. ....	143
Figura 131. Vista del archivo HMI para Prueba #3. Fuente: Autores. ....	143
Figura 132. Nodos lógicos Mapeados para Prueba #4. Fuente: Autores. ....	146
Figura 133. Nodos lógicos del archivo XML para Prueba #4. Fuente: Autores. ....	146
Figura 134. Puertos de comunicación creados en el NCD para Prueba #4. Fuente: Autores. ....	147
Figura 135. Pasos para cargar el archivo “NCD” a la RTU para Prueba #4. Fuente: Autores. ....	147
Figura 136. Página web principal del ORION para Prueba #4. Fuente: Autores. ...	148
Figura 137. Enviar Diagrama Unifilar a la ORION para Prueba #4. Fuente: Autores. .....	148
Figura 138. Pasos para habilitar la página Web para Prueba #4. Fuente: Autores. .	149
Figura 139. Verificación de la Comunicación en la ORION para Prueba #4. ....	150
Figura 140. Diagrama unifilar con el monitoreo de datos para Prueba #4. Fuente: Autores. ....	150
Figura 141. Pasos para configurar el complemento AAR para Prueba #5. Fuente: Autores. ....	153
Figura 142. Configuración de alarmas en módulo AAR para Prueba #5. Fuente: Autores. ....	154
Figura 143. Pasos para crear la matriz de eventos para Prueba #5. Fuente: Autores. .....	154

Figura 144. Páginas de alarmas para comunicación y protección para Prueba #5. Fuente: Autores. ....	155
Figura 145. Configuración de las notificaciones de eventos para Prueba #5. Fuente: Autores. ....	156
Figura 146. Visualización de alarmas en estado normal para Prueba #5. Fuente: Autores. ....	156
Figura 147. Visualización de alarmas en estado activo para Prueba #5. Fuente: Autores. ....	156
Figura 148. Generación de Archivos para Prueba #5. Fuente: Autores. ....	157
Figura 149. Ajustes realizadas a la barra de enlaces para Prueba #6. Fuente: Autores. .....	160
Figura 150. Opciones de visualización y seguridad de acceso para Prueba #6. Fuente: Autores. ....	161
Figura 151. Reglas de autenticación para Prueba #6. Fuente: Autores. ....	161
Figura 152. Pasos para añadir privilegios a los usuarios creados para Prueba #6. Fuente: Autores. ....	162
Figura 153. Ajustes realizados a los usuarios creados para la Prueba #6. Fuente: Autores. ....	162
Figura 154. Ventana inicial del WEBserver para Prueba #6. Fuente: Autores. ....	163
Figura 155. Ventanas orientadas al privilegio de usuarios para Prueba #6. Fuente: Autores. ....	164
Figura 156. Esquema de conexionado para Prueba #7. Fuente: Autores. ....	165
Figura 157. Configuración de parámetros eléctricos en Modulo “Control Center”, para Prueba #7. Fuente: Autores. ....	166
Figura 158. Ensayo de sobrecorriente trifásica, para Prueba #7. Fuente: Autores. .	167
Figura 159. Diagrama ampliado que muestra la diferencia de tiempo entre la señal GOOSE y la señal WIRE, para Prueba #7. Fuente: Autores. ....	167
Figura 160. Pasos para configurar el puerto de protocolo IEC 60870-5-104. Fuente: Autores. ....	170
Figura 161. Pasos para la creación del puerto para la RTU. Fuente: Autores. ....	171
Figura 162. Pasos para cargar el archivo “NCD” a la RTU. Fuente: Autores. ....	172
Figura 163. Página Web de la RTU. Fuente: Autores. ....	172
Figura 164. Verificación de la Comunicación. Fuente: Autores. ....	173
Figura 165. Página Web de la RTU. Fuente: Autores. ....	173

Figura 166. Banco de pruebas con IED's SIEMENS® y maleta CMC 356. Fuente: Autores. ....	181
Figura 167. Banco de prueba #2 con IED's SIEMENS® y PC. Fuente: Autores. ...	181
Figura 168. Rack de comunicación ELSYTEC. Fuente: Autores. ....	182
Figura 169. Laboratorio de Protecciones UPS. Fuente: Autores. ....	182

## LISTA DE TABLAS

Tabla 1: Estructura de la norma IEC 61850.....	51
Tabla 2: Nodos Lógicos. ....	54
Tabla 3: Direcciones IP asignadas. ....	68
Tabla 4: Nombres y direccionamiento de IED's. ....	80
Tabla 5: Elementos del menú subestación. ....	86
Tabla 6: Pestañas de datos.....	94
Tabla 7: Direccionamiento IP de los equipos para Prueba 1. ....	117
Tabla 8. Aspectos para la regla de bloqueo de usuarios. ....	158
Tabla 9. Aspectos para la regla de contraseñas.....	159
Tabla 10. Permisos de Usuarios. ....	159

## ABREVIATURAS

AAR	Alarm/Archive/Retentive Module
ASCI	Abstract Communication Service Interface
CDC	Common Data Classes
CID	Configured IED Description
DNP3	Distributed Network Protocol - version 3
DO	Data object - Objeto de Datos
GOOSE	Generic Object Oriented Substation Event
HMI	Human Machine Interface - Interfaz Hombre Máquina
ICD	IED Capability Description
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
LAN	Local Area Network
LD	Dispositivo Lógico
LN	Nodo Lógico
MMS	Manufacturing Message Specification
NCD	NovaTech Communications Director
RTU	Remote Terminal Unit - Unidad de Transmisión Remota
SAS	Sistemas de Automatización de Subestaciones
SCADA	Supervisory Control and Data Acquisition
SCD	Substation Configuration Description
SCL	Substation Configuration description Language
SSD	System Specification Description
SSH	Secure Shell
SV	Sampled Values - Valores Muestreados
SVG	Scalable Vector Graphics
TCP/IP	Protocolo de Control de Transmisión/Protocolo de Internet
XML	Extensible Markup Language

## **CAPÍTULO I**

### **1. EL PROBLEMA**

#### **1.1. Descripción del problema**

Hoy en día existe una gran inclinación a la automatización de las subestaciones eléctricas, esta inclinación a llevado a buscar un sistema de comunicación que garantice una interoperabilidad entre los diferentes IED's que intervienen en su control, monitoreo y protección.

El estándar internacional IEC 61850 que soporta varios protocolos de comunicación, nace como consecuencia de la evolución de los diferentes estándares de comunicación que han sido desarrollados a lo largo de la historia para la automatización de subestaciones, y ha sido adoptado para la solución de problemas de integración e interoperabilidad en subestaciones y extendiéndose a centrales de generación. Desgraciadamente los nuevos profesionales y estudiantes de ingeniería presentan inexperiencia acerca del estándar IEC 61850 y no desarrollan capacidades en la rama de configuración de protecciones eléctricas y redes de comunicación.

Es por esta razón que se hace necesario implementar una red LAN de comunicación para realizar prácticas correspondientes a las materias de protecciones y comunicaciones. El problema principal radica en que la Universidad Politécnica Salesiana Sede Cuenca carece de un sistema o módulo de comunicación para ejecutar pruebas y simulaciones que faciliten el aprendizaje y capacitación en sistemas de automatización de subestaciones, para enlazar los IED's que cubran áreas de monitorización y acción.

#### **1.2. Antecedentes**

La Universidad Politécnica Salesiana Sede Cuenca dentro de la Carrera de Ingeniería Eléctrica, dispone de un Laboratorio de Protecciones, el cual permite realizar ensayos de funcionamiento y simulación de fallas con los diversos equipos entre ellos IED's.

Sin embargo, tiene la limitación de no poder comprobar el comportamiento general de los equipos, además, no dispone de un sistema de comunicación el cual permita supervisar controlar y adquirir datos de los diferentes ensayos de una manera rápida y



eficiente. Tales ensayos deben estar regidos a normas internacionales que sean utilizados por las empresas del sector energético del país.

### **1.3. Importancia y Alcances**

La Universidad Politécnica Salesiana sede Cuenca se encuentra en fase de construcción e implementación de un banco de ensayos para IED's en el Laboratorio de Protecciones enfocados a la protección de sistemas eléctricos de potencia, contando en su laboratorio con equipos como: la unidad de prueba de relés (CMC 356, marca OMICRON<sup>®</sup>), los relés de protección a distancia compacto (7SA86, marca SIEMENS<sup>®</sup>), y los relés de sobrecorriente y protección del alimentador (7SJ85, marca SIEMENS<sup>®</sup>).

La necesidad que los estudiantes conozcan sobre el estándar IEC 61850, hace necesario implementar un sistema de comunicación para realizar las prácticas correspondientes en dichos dispositivos. Además, es elemental que estas prácticas sean documentadas, es decir poder contar con una guía de pruebas, la cual contenga todos los pasos para la ejecución de las mismas. Con el fin, de gestionar mejor los recursos se dispone de un tablero concentrador de datos basado en Orion LXM (RTU, marca Novatech<sup>®</sup>), el cual también albergará al switch industrial administrable Hirschmann<sup>®</sup> tipo GREYHOUND, el analizador de redes ION7400, y relés de protección (marca SCHNEIDER ELECTRIC<sup>®</sup>).

### **1.4. Delimitación**

El presente proyecto, se realizará con fines educativos y tiene como meta la implementación de mensajería GOOSE bajo el estándar IEC 61850, para monitoreo y control en el módulo de pruebas localizado en el Laboratorio de Protecciones de la Universidad Politécnica Salesiana Sede Cuenca.

Este proyecto no está enfocado en los siguientes puntos:

- Estudio de cortocircuitos.
- Estudio de coordinación de protecciones eléctricas de un SEP.

### **1.5. Objetivos**

#### **1.5.1. Objetivo General**

Realizar la implementación de un sistema de comunicación IEC 61850 para monitoreo y control del módulo de pruebas para el laboratorio de protecciones de la Universidad Politécnica Salesiana sede Cuenca.

### 1.5.2. Objetivos Específicos

- Analizar los beneficios técnicos que se pueden lograr al implementar el estándar IEC 61850.
- Realizar pruebas de comparación entre la metodología de protección con mensajería GOOSE y la metodología de protección convencional.
- Elaborar una guía de pruebas, la cual contenga cada uno de los pasos a seguir para poder implementar la comunicación entre IED's aplicando la mensajería GOOSE.

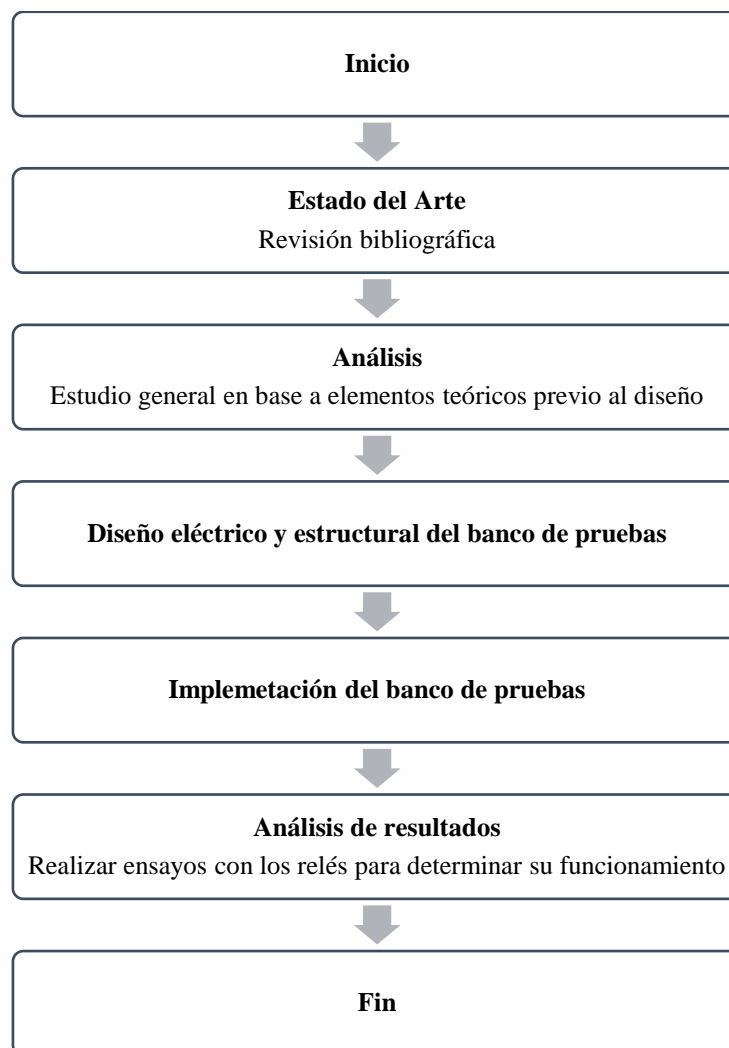


Figura 1: Flujograma de proceso metodológico a aplicar. Fuente: Autores.

## **1.6. Marco Metodológico**

Este proyecto se desarrollará en cinco etapas, las cuales se centran en la comunicación de los IED's mediante la mensajería GOOSE (Estándar IEC 61850), y otros protocolos soportados en la RTU. En la Figura 1 se muestra esquematizado el proceso a seguir.

### **1.6.1. Estado del arte**

En esta etapa, se revisará los elementos teóricos necesarios para el correcto desarrollo del proyecto. Se realizará investigaciones de manejo, configuración y conexión de los equipos de protección en subestaciones como dispositivos de protección de sobrecorriente, protección de alimentadores con diferencial de línea y protección de distancia, protección de transformador y protección de motor. Se revisará el funcionamiento del módulo de pruebas y calibración de equipos de medida (OMICRON<sup>®</sup> CMC 356), del RTU, del switch industrial, del analizador de redes (ION7400), también se investigará la configuración del software NCD que maneja la interfaz gráfica de los IED's.

### **1.6.2. Análisis**

Se realizará un análisis general de los elementos necesarios para el correcto funcionamiento, y posterior implementación de la comunicación IEC 61850.

### **1.6.3. Diseño**

En esta etapa se plasmará toda la información obtenida para realizar el diseño eléctrico de conexionado de los dos tipos de IED's conjuntamente con el módulo de pruebas CMC 356. La realización del diagrama unifilar será primordial, fácil entendimiento en la etapa de implementación. Se tomará en cuenta también los dispositivos de protecciones del banco de pruebas y la señalización.

El diseño estructural se realizará con las normativas de construcción de tableros de ensayo (NTE INEN 2568:2010) con elementos de prueba y borneras para un correcto entendimiento al momento de realizar las respectivas pruebas de los IED's. La normativa para el grado de protección para el gabinete (ANSI/IEC 60529-2004). También, normativas de diseño eléctrico (IEC 61439), de seguridad (ISO 45001), y de sistemas de cableado para telecomunicación (ISO/IEC 11801).

El diseño también considera la incorporación de un módulo de comunicaciones (conmutador industrial y una PC) para prácticas de comunicaciones con los IED's, además, dispondrá de un punto de acceso para red inalámbrica que permite el monitoreo de varios usuarios vía Web Broser. Es decir, el tablero constará con dos módulos generales, uno para simulación de fallas y otro para comunicaciones, separados modularmente en el mismo tablero.

#### **1.6.4. Implementación**

En la parte de implementación se realizará la comunicación con mensajería GOOSE bajo normativa IEC 61850. Luego se realizará la implementación eléctrica y de todos los elementos necesarios para la comunicación, como son: IED's, switch industrial, RTU, software NCD, access point inalámbrico, equipos de protección, marquillado en cables.

#### **1.6.5. Resultados**

En esta fase, los resultados deben satisfacer los objetivos propuestos anteriormente. Además, una vez terminado la comunicación se realizará diferentes ensayos con los diversos equipos para determinar su funcionamiento y tiempo de repuesta; lo que conlleva a elaborar un manual de técnicas y procedimientos para realizar pruebas de comunicación bajo la mensajería GOOSE, para el uso didáctico del sistema de comunicación entre los módulos existentes.

## CAPÍTULO 2

### 2. MARCO TEÓRICO

#### 2.1. Automatización de subestaciones

Los enfoques de las subestaciones tienen como fin una correcta funcionalidad y operación de todos los equipos que la conforman, las nuevas subestaciones eléctricas integran todos sus equipos a un sistema SCADA HMI (Human Machine Interface), con diferentes protocolos de comunicación.

La automatización de subestaciones eléctricas se enfoca en 3 niveles de operación, los cuales definen la conexión y funcionamiento de los equipos, en la Figura 2 se muestra la jerarquía de los niveles de operación [1].

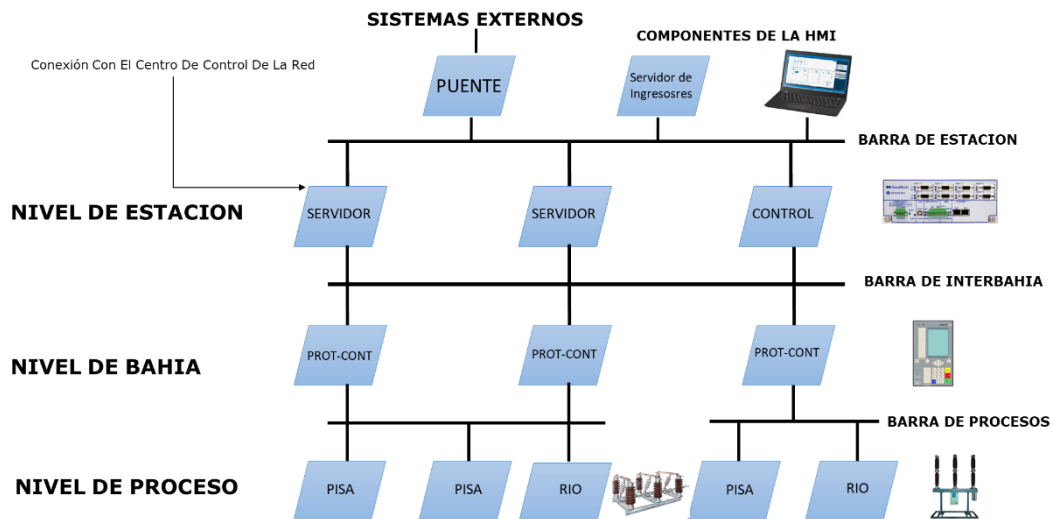


Figura 2: Arquitectura básica de la automatización de SE. Fuente: [1].

#### 2.1.1. Nivel de Proceso

El nivel de proceso se conforma por los equipos primarios (interruptores, seccionadores y transformadores de corriente y tensión).

La barra de procesos o de comunicación de este nivel se encuentra equipos conectados como sensores, actuadores, unidades remotas analógicas/digitales, los procesamientos de estos datos son en tiempo real y son transmitidos en el menor tiempo posible.

#### 2.1.2. Nivel de Bahía

El nivel de bahía o nivel de control de posición, está compuesto por los armarios de control y protección, selectores, pulsadores, relés, y las protecciones de todos los elementos de control, supervisión, regulación y protección.

La barra de comunicación está conectada con el nivel de estación y nivel de proceso permitiendo la interacción y la comunicación de los equipos.

### **2.1.3. Nivel de Estación**

El nivel de estación es el encargado de la supervisión, maniobras y control de la subestación ya sea en alta y media tensión.

La comunicación en este nivel es utilizada para la conexión de HMI a los terminales.

## **2.2. Protocolos de comunicación**

Los dispositivos usados en la automatización de subestaciones deben estar intercomunicados y deben seguir protocolos de comunicación.

El objetivo de un protocolo internacional es permitir la interoperabilidad entre los diferentes dispositivos garantizando así la integridad del sistema.

### **2.2.1. MODBUS**

El protocolo de transmisión Modbus fue introducido en 1979 por la compañía Modicon (ahora Schneider Electric<sup>®</sup>) para los sistemas de control de procesos. Se trata de un protocolo de mensajería de capa de aplicación, es decir, posicionado en el nivel 7 del modelo OSI, que se utiliza para la comunicación cliente/servidor entre dispositivos conectados a la misma red. Hay dos formas de implementar este protocolo: en serie o a través del TCP/IP. La implementación en serie se realiza a través de cable RS-232, 422, o 485, fibra, o inalámbrico, mientras que la opción TCP/IP se construye sobre cable Ethernet, fibra, o inalámbrico.

Por lo general, los mensajes Modbus son de tipo consulta/respuesta, y la comunicación es iniciada por el cliente, con una sola solicitud a un dispositivo en específico, que responde. También se dispone de mensajes del tipo difusión/no respuesta, y en la versión TCP/IP, el servidor puede iniciar una transmisión mediante el envío de un mensaje de excepción [2].

Por lo general, la comunicación entre los equipos de alto nivel (controladores e interfaces hombre-máquina) se establece a través de TCP/IP, mientras que el intercambio de información entre los equipos de alto y bajo nivel, como los controladores, se realiza a través de la opción de serie. Mediante el uso de pasarelas, estos tipos de implementación pueden existir en una red de comunicación al mismo tiempo [2].

### **2.2.2. DNP 3.0**

El DNP3 es un estándar de dominio abierto del IEEE para las comunicaciones de los sistemas de energía eléctrica y fue desarrollado por la General Electric Company (GE) basado en las primeras partes de la IEC 60870-5. Lo hicieron público en 1993, y la propiedad se le dio al recién formado Grupo de Usuarios de DNP. Diseñado inicialmente para funcionar en la red eléctrica convencional, A diferencia de Modbus, los mensajes DNP3 pueden proporcionar la marca de tiempo y la calidad de los datos, y no están restringidos a la transferencia de un punto de datos, ya que se pueden encapsular múltiples tipos de datos (por ejemplo, el punto booleano floating) en un solo mensaje para reducir el tráfico de datos. Además, el DNP3 ofrece características robustas para permitir flexibilidad y seguridad [2].

### **2.2.3. IEC 60870**

La "IEC 60870 - Equipo y sistema de telecontrol" es una norma publicada inicialmente en 1988 por la IEC y se utiliza principalmente en los países europeos. Su aplicación principal es para el control de supervisión y la adquisición de datos en plantas eléctricas y sistemas de transmisión. Es un estándar abierto compuesto de seis partes principales, donde la parte cinco, IEC 60870-5, es para los protocolos de comunicación. Los acompañantes IEC 60870-5-101/104 proporcionan funciones y objetos a los sistemas SCADA, mientras que los IEC 60870-5-102/103 proporcionan apoyo a los sistemas de protección eléctrica [2].

#### **2.2.3.1. IEC 60870-5-101**

“Norma de acompañamiento para tareas básicas de telecontrol” se basa en la comunicación en serie [2].

Tiene el fin de buscar la interoperabilidad entre distintos fabricantes. El ámbito de aplicación es en la comunicación entre los sistemas de telecontrol SCADA y los equipos remotos RTU, medidores y controladores programables, de sistemas eléctricos.

#### **2.2.3.2. IEC 60870-5-103**

Esta sección, permite la interoperabilidad entre equipos de protección y dispositivos de un sistema de control dentro de la subestación.

#### **2.2.3.3. IEC 60870-5-104**

“Acceso a la red utilizando perfiles de transporte estándar” es una combinación de la capa de aplicación del IEC 60870-5-101 y las funciones de transporte del TCP/IP. Es una evolución del procedimiento de transporte físico y de datos, en la que los niveles inferiores del protocolo se sustituyen completamente por los protocolos de transporte y de red TCP e IP [2].

Este protocolo permite la comunicación entre la MTU y los distintos PLCs o RTUs. Para ello se utiliza conexiones a través de TCP/IP. El protocolo TCP garantiza una transmisión de datos fiable. Además, por norma, este protocolo tiene establecido que el puerto estándar sea el 2404 de TCP.

#### **2.2.4. IEC 61850**

La norma internacional IEC 61850 tiene la finalidad de estandarizar el intercambio de información mediante redes de comunicaciones y lograr la interoperabilidad entre IED's en subestaciones eléctricas. La misma es el resultado del trabajo conjunto de los principales organismos mundiales de estandarización del sector eléctrico.

La primera versión de la norma IEC-61850 fue publicada entre 2001 y 2004. Desde entonces, cada una de sus partes ha sido revisada y extendida hacia una versión 2 para mejorar su contenido y responder a las necesidades de otros aspectos del sector eléctrico [3].

Dicha edición 2 incluye mejoras, tales como [3]:

- Mejora la interoperabilidad con respecto a la edición 1 (restringe varios aspectos opcionales).



- Añade más información en los ficheros de configuración SCL para mejorar la ingeniería.
- Incluye opciones de redundancia de red.
- Mejora la definición de los modos de prueba de los equipos para perfeccionar tareas de mantenimiento.
- Crea un modelo de información más preciso corrigiendo errores e incluyendo funciones (nodos lógicos) y plantillas de datos de otros campos fuera de la subestación eléctrica.

El estándar consta de 10 capítulos. Estos 10 capítulos son los siguientes:

- IEC 61850-1: Introducción y generalidades.
- IEC 61850-2: Glosario.
- IEC 61850-3: Requerimientos generales.
- IEC 61850-4: Sistema y gestión de proyectos.
- IEC 61850-5: Requerimientos de comunicación para funciones y modelado de dispositivos.
- IEC 61850-6: Descripción de la configuración del lenguaje para la comunicación en subestaciones eléctricas relacionadas con IED's.
- IEC 61850-7: Estructura básica de comunicación para la subestación y equipos alimentadores.
- IEC 61850-8: Servicios de comunicación específicos de mapeo (SCSM)-MMS.
- IEC 61850-9: Servicios de comunicación específicos de mapeo (SCSM)-SV.
- IEC 61850-10: Pruebas de conformidad.

El alcance principal de cada capítulo, se describe brevemente en lo que sigue:

#### **2.2.4.1. IEC 61850-1**

Este reporte técnico es aplicable a Sistemas de Automatización de Subestaciones. Define la comunicación entre IED's en la subestación y los requerimientos relacionados del sistema. Esta parte brinda una introducción y una visión general de la serie IEC61850 [4].

#### **2.2.4.2. IEC 61850-2**

Este documento contiene el glosario de la terminología específica y definiciones utilizadas en el contexto de SAS en las diferentes partes del estándar [4].

#### **2.2.4.3. IEC 61850-3**

Las especificaciones de esta parte pertenecen a los requerimientos generales de la red de comunicaciones con énfasis en los requerimientos de calidad. Trata además las pautas para condiciones ambientales y servicios auxiliares, con recomendaciones basados en la relevancia de requerimientos específicos de otros estándares y especificaciones [4].

#### **2.2.4.4. IEC 61850-4**

Las especificaciones de esta parte se refieren a la gestión del sistema y del proyecto con respecto al proceso de ingeniería y sus herramientas de soporte; al ciclo de vida del sistema global y sus IED's; al aseguramiento de la calidad comenzando con la etapa de desarrollo y finalizando con la discontinuación y fuera de servicio del equipamiento del SAS y sus IED's. Se describen los requerimientos del sistema y el proceso de gestión del proyecto y herramientas especiales de soporte para ingeniería y ensayo [4].

#### **2.2.4.5. IEC 61850-5**

Las especificaciones de esta parte se refieren a los requerimientos de comunicaciones de las funciones realizadas en el SAS y en los modelos de dispositivos. Se identifican todas las funciones conocidas y sus requerimientos de comunicaciones. La descripción de las funciones no se utiliza para estandarizar las funciones, sino para identificar los requerimientos de comunicaciones entre servicios técnicos y la subestación y requerimientos de comunicaciones entre IED's en la subestación. El objetivo básico es la interoperabilidad para todas las interacciones [4].

#### **2.2.4.6. IEC 61850-6**

Esta parte de la serie IEC61850 especifica un formato de archivo para describir configuraciones vinculadas con comunicaciones con IED's y parámetros de IED's, configuraciones de sistemas de comunicaciones, estructuras de playas o patios, y las relaciones entre ellas. El principal propósito de este formato es intercambiar descripciones de capacidad de IED's, y descripciones de SAS entre herramientas de

ingeniería de IED y herramientas de ingeniería de sistemas de diferentes fabricantes en forma compatible. El lenguaje definido se denomina Lenguaje de descripción de Configuración de Subestación (SCL). El IED y el modelo del sistema de comunicaciones en SCL están de acuerdo con IEC 61850-5 e IEC 61850-7-x. Las extensiones específicas SCSM o reglas de utilización pueden ser requeridas en partes apropiadas. El lenguaje de configuración se basa en el Extensible Markup Language (XML) versión 1.0 [4].

#### **2.2.4.7. IEC 61850-7**

##### **2.2.4.7.1. IEC 61850-7-1 - Estructura básica de comunicación para subestación y equipo de alimentación – Principios y modelos**

Este documento de la serie IEC61850 introduce los métodos de modelado, los principios de comunicaciones, y los modelos de información que son utilizados en las partes de IEC 61850-7-x. El propósito de este documento es proveer, desde un punto de vista conceptual, asistencia para entender los conceptos básicos de modelado y métodos de descripción para modelos específicos de información de subestación para sistemas de automatización de subestación, funciones de dispositivos utilizadas para propósitos de automatización de subestaciones, y sistemas de comunicaciones para proveer interoperabilidad [4].

##### **2.2.4.7.2. IEC 61850-7-2 - Estructura básica de la información y comunicación – Interfaz de servicio de comunicación abstracta (ASCI).**

Define el ASCI en términos de un modelo de clase jerárquico de toda la información que puede ser accedida a través de una red de comunicaciones y los servicios que operan sobre estas clases de parámetros asociados con cada servicio [4].

##### **2.2.4.7.3. Estructura básica de comunicación para subestaciones y equipo**

Esta parte de la norma IEC61850 especifica tipos de atributos comunes y clases de datos comunes relacionadas con aplicaciones en subestaciones [4].

##### **2.2.4.7.4. Estructura básica de comunicación para subestaciones y equipos alimentadores – Clases de datos comunes**

Esta parte de la IEC61850 especifica la información del modelo de dispositivo y funciones relacionadas a las aplicaciones de una subestación. En particular, especifica

los nombres de nodos lógicos compatibles y los nombres de los datos para la comunicación entre IED's. Esto incluye la relación entre nodos lógicos y datos. Para alcanzar interoperabilidad, todos los modelos de datos necesitan una buena definición en cuanto a semántica y sintaxis. La semántica de los datos es provista por nombres asignados a nodos lógicos y a los datos que ellos contienen, como fueron definidos en esta parte del documento. Las definiciones de nombres de datos y nombres de nodos lógicos compatibles encontrados en esta parte y la semántica asociada son fijos. La sintaxis de todas las clases de datos son definiciones abstractas provistas por IEC 61850-7-2 e IEC 61850-7-3 [4].

#### **2.2.4.8. IEC 61850-8**

##### **2.2.4.8.1. Servicios de comunicación específicos de mapeo (SCSM) – Mapeo para MMS (ISO 9506-1 e ISO 9506-2) y para ISO/ IEC 8802-3**

El mapeo permite el intercambio de datos sobre Redes Locales ISO/IEC 8802-3, entre los diversos tipos de equipamiento de una subestación. Algunos de los protocolos utilizados en este documento son de ruteo, por lo que las comunicaciones no están restringidas a la red de área local. El intercambio de datos permite el monitoreo en tiempo real de datos de control, incluyendo valores medidos, etc. También especifica un método para el intercambio de datos críticos y no críticos en tiempo, a través, de la red de área local relacionando, las tramas ACSI a MMS e ISO/IEC 8802-3. Los servicios y protocolos MMS son especificados para operar sobre los modelos de comunicaciones OSI y TCP completos. También provee soporte para arquitecturas centralizadas y distribuidas [4].

#### **2.2.4.9. IEC 61850-9**

##### **2.2.4.9.1. Servicios de comunicación específicos de mapeo (SCSM) – Valores muestreados sobre enlace serial unidireccional multipunto punto a punto**

Esta parte se aplica a transformadores de medida de tensión y corriente (ECT y EVT) con salida digital vía una unidad concentradora (merging unit), para su utilización con instrumentos electrónicos de medida y de protecciones. Para salidas digitales el estándar considera conexiones punto a punto desde la unidad concentradora a los instrumentos electrónicos de medida. Esto permite interoperabilidad entre dispositivos de distintos fabricantes [4].

##### **2.2.4.9.2. Servicios de comunicación específicos de mapeo (SCSM) – Valores muestreados sobre ISO/IEC 8802-3**

Define el SCSM para valores muestreados sobre ISO/IEC 8802-3. La intención de esta definición es reforzar la IEC61850 -9-1 para incluir el mapeo completo del modelo de valores muestreados. Se aplica a transformadores de corriente y tensión electrónicos (ECT y EVT con salida digital), unidad concentradora, y dispositivos electrónicos inteligentes como por ejemplo: unidades de protección, controladores de bahía y medidores [4].

### **2.3. Unidades de proceso disponible**

Las unidades de proceso que se disponen son los dispositivos que nos permiten realizar monitoreo y operaciones de manera remota, poseen entradas y salidas estándar además de módulos de comunicación para interactuar entre ellos. Estas unidades de proceso forman parte de un sistema integrado que reúne procesos de control, protección, monitoreo y adquisición de datos de los sistemas eléctricos.

#### **2.3.1. RTU NOVATECH® ORION LXM**

La RTU de NOVATECH® (Figura 3), es una plataforma de automatización multipuerto. Está diseñado para operar todos los puertos independientemente uno del otro.

La plataforma Orion es usada por cientos de empresas eléctricas de generación, transmisión y distribución para realizar una amplia gama de aplicaciones smart grid y de ciberseguridad, no solo a nivel subestación sino también de redes de distribución y centros de control. La Orion LXM es ideal para subestaciones de distribución. Ejecutando todas las opciones y protocolos de la Orion LX. Ideal para aplicaciones de poste a lo largo de la red de distribución, bóvedas así como subestaciones rurales, la Orion LXM cuenta con gran poder y flexibilidad inigualable [5].



Figura 3: Vista del panel frontal del Orion LXM. Fuente: [5].

Cada puerto puede admitir un protocolo de comunicaciones único:

- Modo maestro: conectado a IED's u otros dispositivos esclavos.
- Modo esclavo: conectado a Control de supervisión y maestros de adquisición de datos (SCADA) o HMIs.

La unidad base Orion LXM viene con las siguientes características:

- Diagnóstico / configuración del puerto USB tipo B (puerto A)
- Una entrada digital
- Una salida digital (alarma)
- IRIG-B
- Dos puertos Ethernet de cobre (ETH0, ETH1)
- Se pueden agregar hasta dos tarjetas de comunicación o tarjetas de E / S en cualquier combinación

### 2.3.2. Switch industrial administrable HIRSCHMANN® tipo GREYHOUND

El switch industrial permite conectar y servir de puente entre varias redes, tiene la particularidad de ser gestionable y soportar temperaturas de funcionamiento extremas, lo cual le da una característica de soportar entornos industriales adversos.

Los dispositivos GREYHOUND (Figura 4) están diseñados para los requisitos especiales de la automatización industrial. Cumplen con los estándares relevantes del

sector industrial, brindan una confiabilidad operativa muy alta, incluso en condiciones extremas, y también confiabilidad y flexibilidad a largo plazo. Los dispositivos le permiten configurar redes Ethernet industriales conmutadas que cumplan con el estándar IEEE 802.3.



Figura 4: Switch Industrial GREYHOUND. Fuente: [6].

El switch presenta una alta variedad de funciones de software a través del sistema operativo HiOS de Hirschmann<sup>®</sup>, y es flexible a medida que la red evoluciona a través de sus módulos de puerto intercambiables en campo, con opciones de puertos de cobre, fibra de Gigabit disponibles [6].

El dispositivo presenta características generales, tales como [6]:

- Flexible: diseñado con el futuro en mente, a través, de módulos de medios personalizables e intercambiables para mantener el ritmo de las necesidades cambiantes de la red.
- Diseñado para entornos industriales: construido para soportar altas temperaturas, altas vibraciones y descargas electrostáticas que a menudo se encuentran en la automatización industrial y la configuración de la red eléctrica.
- Disponibilidad de red confiable: las nuevas funciones de administración, incluidos los protocolos de redundancia, las funciones de diagnóstico y los mecanismos de seguridad integrales, ayudan a las redes a lograr un alto tiempo de actividad.

Los robustos interruptores GREYHOUND han sido especialmente diseñados para manejar aplicaciones exigentes de generación y distribución de energía eléctrica, incluidas nuevas instalaciones y modernizaciones de subestaciones existentes, donde

la temperatura ambiente puede ser extremadamente alta. Los dispositivos también funcionan bien en aplicaciones de transporte y automatización industrial. Por ejemplo, con redes ópticas ferroviarias, sistemas de pasajeros e información en estaciones de tren, sistemas de transporte, así como vigilancia del tráfico en carreteras, puentes y túneles [6].

### 2.3.3. Analizador de redes ION7400

El medidor ION 7400 de Schneider Electric<sup>®</sup> (Figura 5), es un medidor de Energía de alta precisión clase 0.2, extremadamente confiable, con flexibilidad y facilidad de uso sin igual.

El analizador combina mediciones precisas de energía y potencia trifásicas con almacenamiento de datos, análisis de calidad de energía, alarmas y capacidades de Entrada/Salida que comúnmente no están disponibles en otro medidor tan pequeño. Proporciona gran visibilidad de los datos y activos, facilitando un tiempo de respuesta rápido y la toma de mejores decisiones. La integración de software proporciona acceso remoto de fácil manejo de los datos de energía, variaciones en la calidad de la energía, previsión y más desde páginas web personalizables. El analizador de redes ION 7400 se adecua fácilmente a los sistemas de facturación o SCADA existentes, y es amigable con diferentes protocolos [7].



Figura 5: Analizador de redes ION 7400. Fuente: [7].

ION constituye el protocolo y la arquitectura, fundamentales de la central de medida. Esta puede integrarse en diferentes redes estandarizadas. Los datos que emplea la central de medida pueden ponerse a disposición de otros dispositivos a través de Modbus, DNP 3.0, SNMP y el sistema de traducción MV-90. Es posible configurar la central de medida de manera que importe datos procedentes de otros dispositivos



ubicados en dichas redes. Este medidor es compatible con el protocolo IEC 61850 y el formato de datos de COMTRADE. Además, admite los protocolos IPv6, DPWS, RSTP y Ethernet [7].

### 2.3.4. CMC 356 equipo de pruebas de protección universal y herramienta de puesta en servicio

La maleta de pruebas o también conocido como valija de inyección, se compone de elementos electrónicos que se operan a través de un software licenciado con una gran variedad de herramientas que adecuándolas de manera correcta sirven para simular cualquier tipo de falla en un sistema de protección eléctrico.

La unidad CMC 356 (Figura 6) es la solución universal para realizar pruebas a todas las generaciones y tipos de relés de protección. Sus seis potentes fuentes de corriente (modo trifásico: hasta 64A / 860VA por canal) con un gran rango dinámico, permiten probar hasta los relés electromecánicos de alta carga con una demanda de potencia muy alta [8].

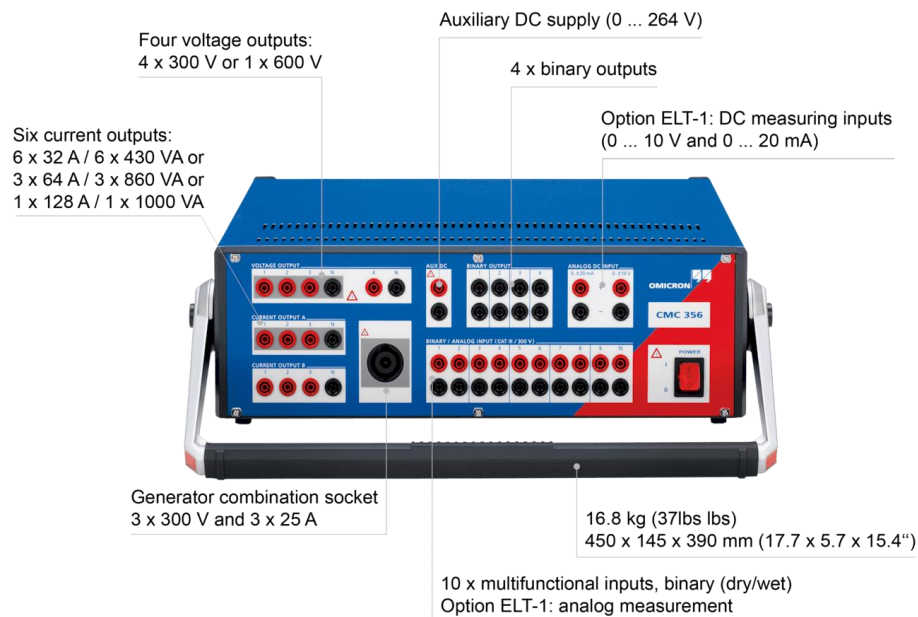


Figura 6: Unidad de pruebas CMC 356. Fuente: [8].

La unidad CMC 356 es la opción ideal para aplicaciones que requieren la más alta versatilidad, amplitud y potencia. Los ingenieros y técnicos de puesta en servicio aprecian especialmente su capacidad de realizar comprobaciones de cableado y

plausibilidad de los transformadores de corriente, mediante la inyección primaria de altas corrientes desde el equipo de prueba [8].

Sus funciones claves son, [8]:

- Potentes fuentes de corriente para pruebas, incluso de relés electromecánicos de alta carga.
- Altas amplitudes de corriente para prueba de relés de 5A.
- Alta exactitud y versatilidad para pruebas de relés estáticos y numéricos de todo tipo.
- Red integrada para prueba de dispositivos IED de tipo IEC 61850.
- Funciones de medición analógica de 10 canales y registro de transitorios.

### **2.3.5. Relés SIEMENS® de la familia SIPROTEC 5**

La generación de dispositivos SIPROTEC 5 (Figura 7) proporcionan una plataforma moderna de hardware y software, proporcionando una excelente solución a los desafíos asociados con la evolución de las redes estructurales y los flujos de trabajo. Preserva la calidad, la fiabilidad y las funciones comprobadas de gamas anteriores, tales como, la modularidad y flexibilidad de sus componentes. Agregando enfoques innovadores que incluyen flujo de trabajo holístico, seguridad y vigilancia de la estabilidad de la red (funcionalidad PMU). Esta familia de SIPROTEC es perfecta para aplicaciones de protección, control, monitoreo y medición en sistemas de energía eléctrica.

Beneficios generales de estos dispositivos, [9]:

- Seguridad debido a las potentes funciones de protección.
- Seguridad de datos y transparencia durante todo el ciclo de vida de la planta.
- Mayor fiabilidad y calidad del proceso de ingeniería.
- Cyber Security según NERC CIP y requerimientos BDEW Whitepaper.
- Máxima disponibilidad incluso en condiciones ambientales extremas mediante en serie de los módulos.
- Compatibilidad total entre IEC 61850 Ediciones 1 y 2.

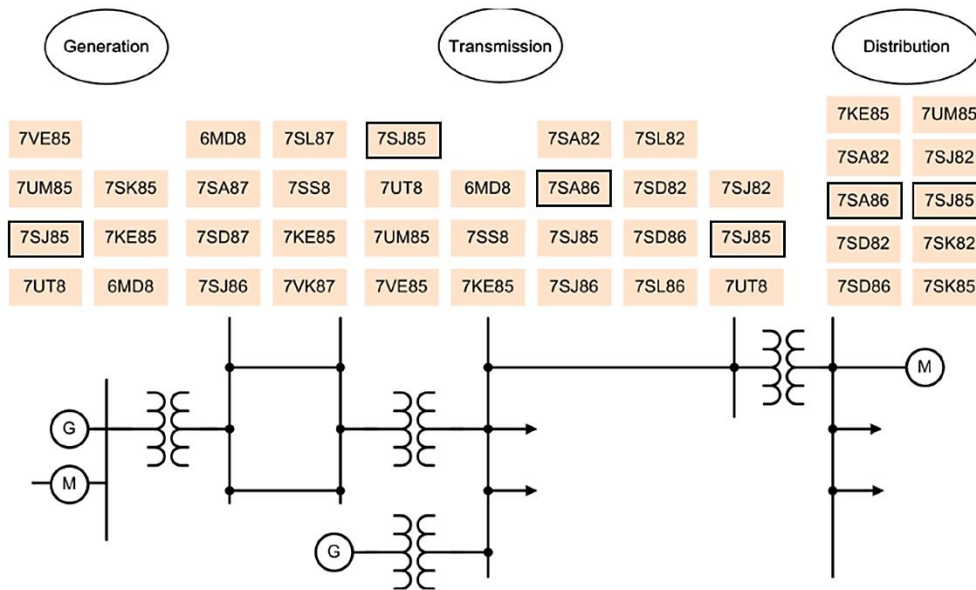


Figura 7: Dispositivos y campo de aplicación de la familia SIPROTEC 5. Fuente: [10].

### 2.3.5.1. Relé de protección a distancia compacto (SIPROTEC 7SA86)

El IED 7SA86 (Figura 8), es utilizado para la protección a distancia de líneas eléctricas de potencia. Su función principal es de la protección a distancia para sistemas de media tensión y alta tensión, tiene una estructura modular y flexible.

Entre las principales características del dispositivo destacan las siguientes, [11]:

- Disparo tripolar, tiempo de disparo mínimo 9 ms.
- Entradas y salidas: 12 variantes estándar predefinidas con 4/4 ó 8/8 transformadores de intensidad/transformadores de tensión, 5 hasta 31 entradas binarias, 8 hasta 46 salidas binarias.
- Estructura cuantitativa de hardware: la estructura cuantitativa de E/S, es ajustable de forma flexible dentro del alcance del sistema modular SIPROTEC 5.

Aplicaciones principales, [11]:

- Detección de cortocircuitos y disparo tripolar selectivo en los componentes eléctricos de redes radiales, líneas alimentadas unilateral o bilateralmente, líneas paralelas y redes anulares en funcionamiento abierto o cerrado en todos los niveles de tensión.

- Detección de fallas a tierra en redes aisladas y compensadas en configuración radial anular o mallada.
- Protección de respaldo para dispositivos de protección diferencial de todo tipo: para líneas, transformadores, generadores, motores y barras colectoras.
- Comunicación de protección en serie con dispositivos SIPROTEC 5 y SIPROTEC 4 para diferentes distancias y diferentes medios físicos, como fibra óptica, conexiones de dos hilos y redes de comunicación.
- Unidad de Medición de Fasor, PMU.

Comunicación, [11]:

- Cifrado de comunicaciones: Normal.
- Puerto J, Ethernet integrado: para DIGSI® 5
- Modulo Plug-in en la posición E: ETH-BA-2EL: 2x electric Ethernet 100 Mbit/s, RJ45 Protocolos de comunicación: aplica para DIGSI® 5, IEC 61850-8-1 MMS y GOOSE, IEC 60870-5-104, DNP3 TCP, Modbus TCP, Synchrophasor (IEEE C37.118 - IP), Profinet IO, SUP, DHCP, SNTP, SNMP, etc. Protocolos redundantes: Line Mode, RSTP, HSR, PRP.
- Modulo Plug-in en la posición F: USART-AC-2EL: 2 x electric serial RS485, RJ45, aplica para protocolos seriales, etc. IEC60870-5-103, DNP3.0 etc.

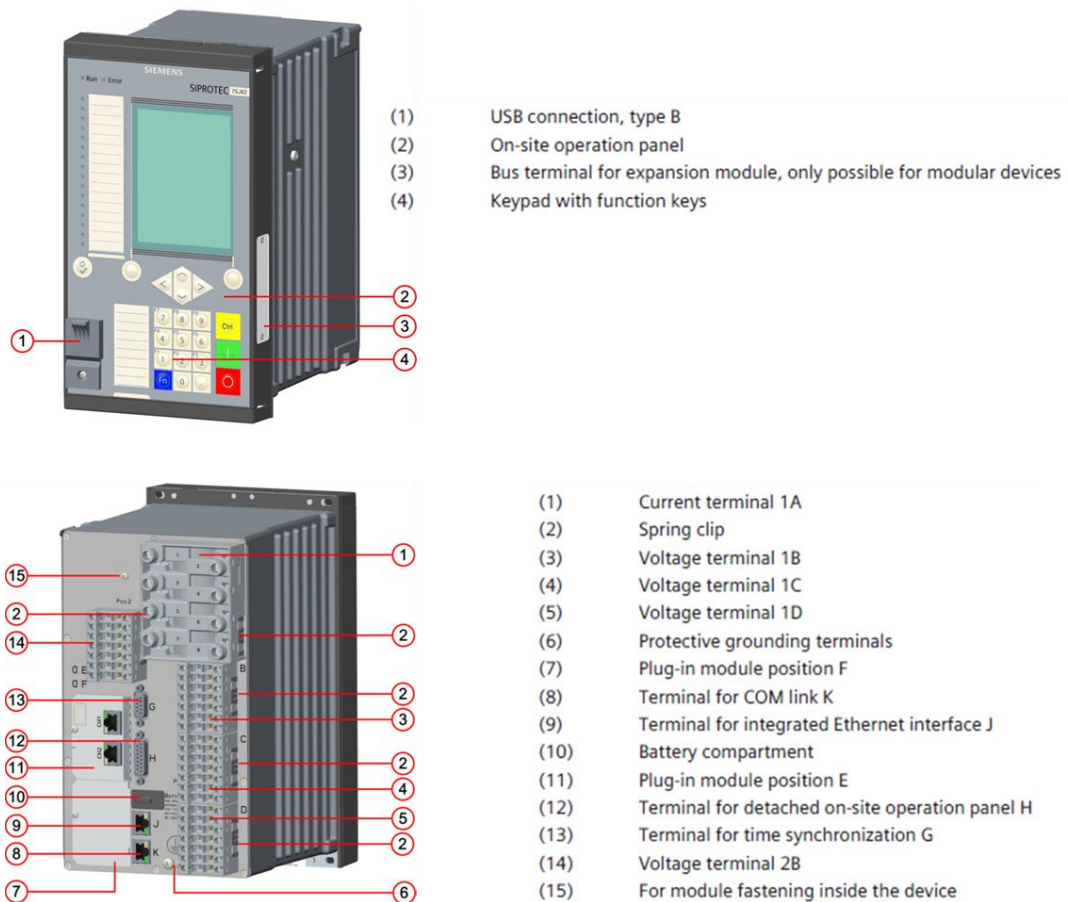


Figura 8: Vista frontal y posterior de dispositivos SIPROTEC 5. Fuente: [11].

### 2.3.5.2. Relé de sobrecorriente y protección del alimentador (SIPROTEC 7SJ85)

El IED 7SJ85 (Figura 8), es utilizado para la protección contra sobrecorriente de alimentadores, líneas y banco de condensadores. Cuenta con una estructura modular y flexible, y opera en todos los niveles de tensión.

Entre las principales características del dispositivo destacan las siguientes, [11]:

- Entradas y salidas: 5 variantes estándar predefinidas con 4 transformadores de intensidad, 4 transformadores de tensión, 11 hasta 59 entradas binarias, 9 hasta 33 salidas binarias.
- Flexibilidad de hardware: Estructura cuantitativa flexible de entradas/salidas, adaptable y ampliable en el marco de la estructura modular SIPROTEC 5; se pueden añadir módulos de extensión 1/6 adicionales con pantalla grande, pequeña o sin pantalla.

Aplicaciones principales, [11]:

- Detección de cortocircuitos y disparo tripolar selectivo en los componentes eléctricos de redes radiales, líneas alimentadas unilateral o bilateralmente, líneas paralelas y redes anulares en funcionamiento abierto o cerrado en todos los niveles de tensión.
- Protección de respaldo para dispositivos de protección diferencial de todo tipo para líneas, transformadores, generadores, motores y barras colectoras.
- Protección y monitoreo de bancos de condensadores.
- Unidad de Medición de Fasor, PMU.
- Protección de potencia inversa.
- Aplicaciones de deslastre de carga.
- Automatismo de conmutación.
- Regulación o control de transformadores de potencia (transformadores de dos devanados, transformadores de tres devanados, transformadores de acoplamiento de red).

Comunicación, [11]:

- Cifrado de comunicaciones: Normal.
- Puerto J, Ethernet integrado: para DIGSI® 5
- Modulo Plug-in en la posición E: ETH-BA-2EL: 2x electric Ethernet 100 Mbit/s, RJ45 Protocolos de comunicación: aplica para DIGSI® 5, IEC 61850-8-1 MMS y GOOSE, IEC 60870-5-104, DNP3 TCP, Modbus TCP, Synchrophasor (IEEE C37.118 - IP), Profinet IO, SUP, DHCP, SNTP, SNMP, etc. Protocolos redundantes: Line Mode, RSTP, HSR, PRP.
- Modulo Plug-in en la posición F: USART-AC-2EL: 2 x electric serial RS485, RJ45, aplica para protocolos seriales, etc. IEC60870-5-103, DNP3.0 etc.

### **2.3.6. Relés SCHNEIDER ELECTRIC® EASERGY P3**

La gama Easergy P3 (Figura 9) está diseñado para aplicaciones de uso estándar de media tensión, adecuadas para edificios, industrias y aplicaciones de servicios eléctricos por igual. Funciones de protección como: protección de alimentador, motor,

transformador y generador, y protección de arco opcional y funciones avanzadas como diferencial de línea y distancia [12].

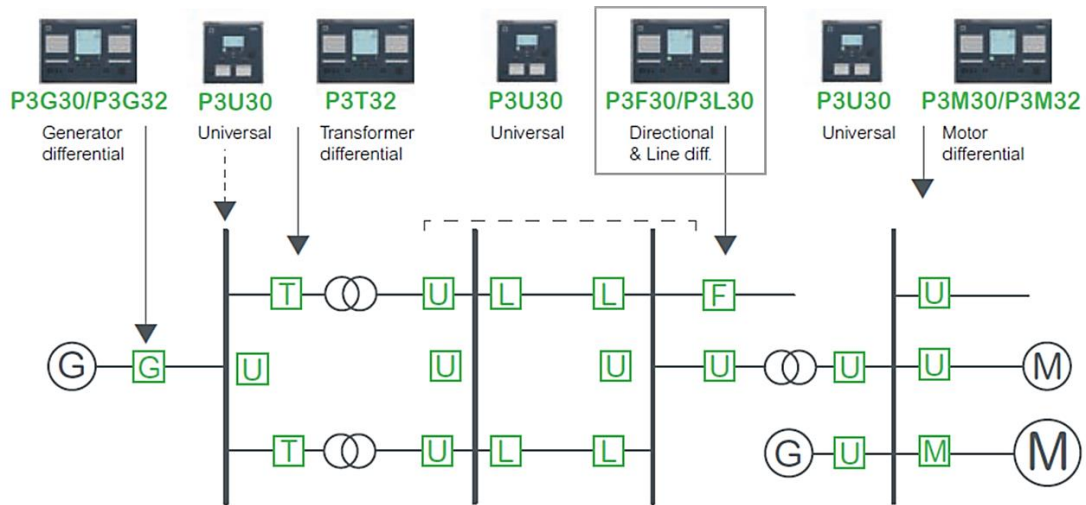


Figura 9: Rango de operación de los dispositivos P3. Fuente: [12].

### 2.3.6.1. Relé de protección del alimentador (P3F30)

El IED P3F30 (Figura 10) es utilizado para la protección del alimentador, entre las principales características del dispositivo destacan las siguientes, [13]:

- Entradas para medición: 1/0.2 A CT corriente residual (x1), 1/5 A CT corriente de fase (x3), 100 V/110 V VT voltaje (x4), 5/1 A CT corriente residual (x1).
- Entradas y salidas: de 6 a 36 entradas digitales, de 9 a 21 salidas digitales.
- Protocolos de comunicación, dependiendo del modelo: DNP3, DNP3 a través de Ethernet, DeviceNet, Ethernet/IP, IEC 60870-5-101, IEC 60870-5-103, IEC 61850 ed. 1, IEC 61850 ed. 2, Modbus RTU, Modbus TCP, Profibus DP, SPAbus.
- Fuente de alimentación nominal: 24...48 V DC o 110...240 V AC/DC.
- Temperatura de ambiente, en servicio: -40...60°C (-40...140°F)

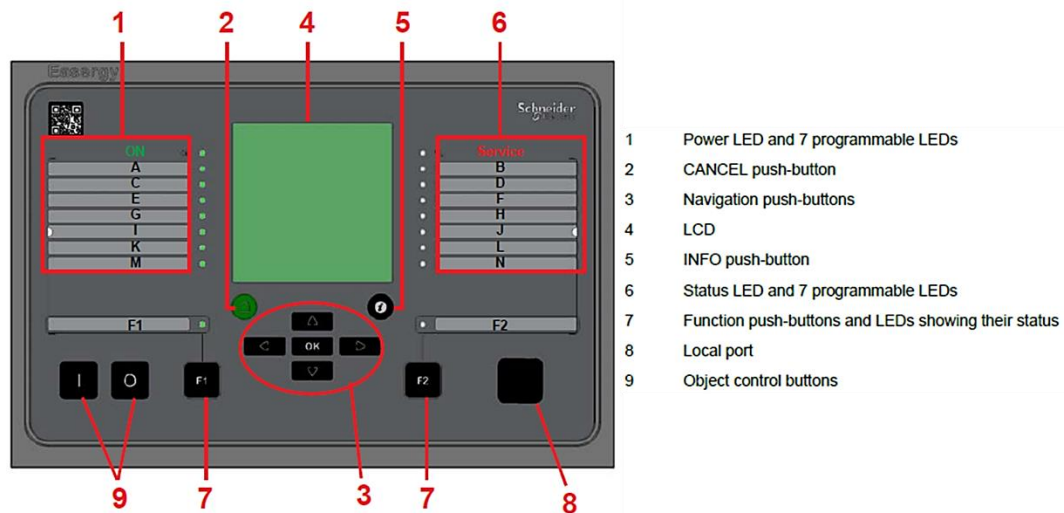


Figura 10: Panel frontal de dispositivos P3F30/P3L30. Fuente: [13].

### 2.3.6.2. Relé de protección de línea, diferencial y distancia (P3L30)

El IED P3L30 (Figura 10) es utilizado para la protección del alimentador con diferencial de línea y protección de distancia, entre las principales características del dispositivo destacan las siguientes, [14]:

- Entradas para medición: 1/0.2 A CT corriente residual (x1), 1/5 A CT corriente de fase (x3), 100 V/110 V VT voltaje (x4), 5/1 A CT corriente residual (x1).
- Entradas y salidas: de 6 a 36 entradas digitales, de 9 a 21 salidas digitales, de 0 a 4 (usando un módulo externo RTD) E/S analógicas.
- Protocolos de comunicación, dependiendo del modelo: DNP3, DNP3 a través de Ethernet, DeviceNet, Ethernet/IP, IEC 60870-5-101, IEC 60870-5-103, IEC 61850 ed. 1, IEC 61850 ed. 2, Modbus RTU, Modbus TCP, Profibus DP, SPAbus.
- Fuente de alimentación nominal: 24...48 V DC o 110...240 V AC/DC.
- Temperatura de ambiente, en servicio: -40...60°C (-40...140°F).
- Entradas del sensor de arco eléctrico: Sensor de 0 a 4 puntos.

### 2.3.7. Relés SCHNEIDER ELECTRIC® EASERGY P5

La familia de dispositivos Easergy P5 (Figura 11) está diseñada para usos severos de medio voltaje, en: empresas de electricidad, aeropuertos, hospitales, edificios e



industrias, minería, petróleo y gas. Son dispositivos más potentes, seguros y mejor conectados mediante herramientas digitales.

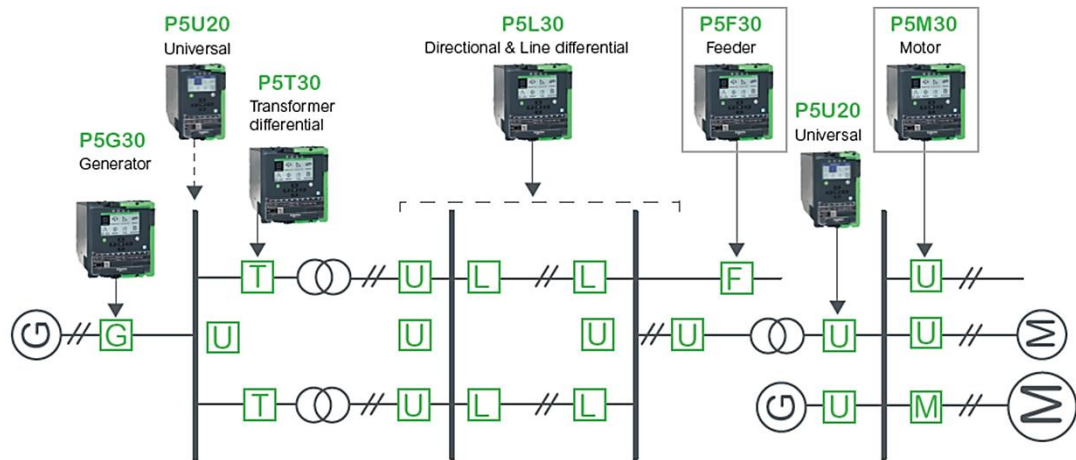
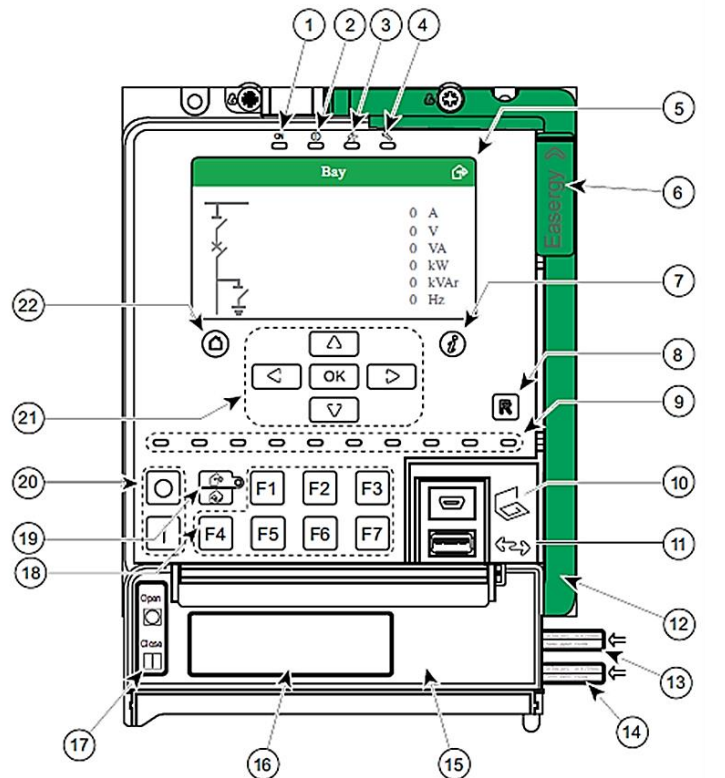


Figura 11: Rango de operación de los dispositivos P5. Fuente: [15].

### 2.3.7.1. Relé de protección diferencial y de transformador (P5F30)

El IED P3F30 (Figura 12) es utilizado para la protección del alimentador, entre las principales características del dispositivo destacan las siguientes, [15]:

- Entradas para medición, dependiendo del modelo: 1 A CT corriente residual (x1), 1/5 A CT corriente de fase (x3), 1/5 A CT corriente residual (x1), VT voltaje (x4); ó, CSH corriente residual (x1), LPCT corriente de fase (x3), LPVT voltaje (x4).
- Entradas y salidas: de 4 a 22 entradas digitales, de 3 a 15 salidas digitales.
- Protocolos de comunicación, dependiendo del modelo: IEC 61850 Ed.1 & Ed.2, IEC 60870-5-103 & 101, DNP3 Ethernet, DNP3 serial, Modbus Ethernet, Modbus serial, EtherNet IP.
- Fuente de alimentación nominal: 48-250 V DC; 100-230 V AC.
- Temperatura de ambiente, en servicio: -40 to 70°C (-40 to 158°F).
- Entradas del sensor de arco eléctrico: Sensor de 0 a 6 puntos.
- Protocolos redundantes: RSTP, PRP / HSR.



- |  |   |
|--|---|
| 1 Power ON/OFF LED   | 12 Handle   |
| 2 Alarm LED  | 13 Label for protection relay name (inserted in the shutter)              |
| 3 Trip LED   | 14 LED identification label (inserted in the shutter)                     |
| 4 Maintenance/Test LED   | 15 Shutter  |
| 5 Graphic 480 x 272 color LCD screen                                 | 16 Label for programmable function key (stuck on the back of the shutter) |
| 6 Handle lock (movable up and down)                                  | 17 Label for CB open and CB close keys (stuck on the back of the shutter) |
| 7 Information key  | 18 F1 - F7 function keys  |
| 8 Reset key  | 19 Remote Control/Local Control key                                       |
| 9 10 LEDs, user programmable   | 20 CB Open (upper) and CB Close (lower) keys                              |
| 10 Mini-USB connector for connecting laptop (behind a plastic cover) | 21 Navigation keypad and confirmation key                                 |
| 11 USB connector for data transfer (behind a plastic cover)          | 22 Home key   |

Figura 12: Panel frontal de Easergy P5x30. Fuente: [15].

### 2.3.7.2. Relé de protección del motor (P5M30)

El IED P3M30 (Figura 12) es utilizado para la protección del motor, entre las principales características del dispositivo destacan las siguientes, [15]:

- Entradas para medición, dependiendo del modelo: 1 A CT corriente residual (x1), 1/5 A CT corriente de fase (x3), 1/5 A CT corriente residual (x1), VT voltaje (x4); ó, CSH corriente residual (x1), LPCT corriente de fase (x3), LPVT voltaje (x4).

- Entradas y salidas: de 4 a 22 entradas digitales, de 3 a 15 salidas digitales.
- Protocolos de comunicación, dependiendo del modelo: IEC 61850 Ed.1 & Ed.2, DNP3 Ethernet, Modbus TCP, EtherNet IP.
- Fuente de alimentación nominal: 48-250 V DC; 100-230 V AC.
- Temperatura de ambiente, en servicio: -40 to 70°C (-40 to 158°F).
- Entradas del sensor de arco eléctrico: Sensor de 0 a 6 puntos.
- Protocolos redundantes: RSTP, PRP / HSR.

## CAPÍTULO 3

### 3. ESTANDAR IEC 61850

El estándar IEC 61850 permite la automatización de equipos de Subestaciones Eléctricas, su principal objetivo es la comunicación y operación de los equipos de control y medición permitiendo la interoperabilidad entre diversos fabricantes [16].

De esta forma el estándar IEC 61850, maneja un modelo de datos llamado nodo lógico, el cual permite conocer de manera estandarizada y sencilla todos los componentes de la subestación, este estándar da un gran beneficio en la parte económica con la sustitución de cobre por una red LAN, y la transmisión de datos entre IED's es mediante los protocolos que maneja esta norma.

El estándar está conformado por 10 partes, las cuales se visualizan en la Tabla 1.

Tabla 1: Estructura de la norma IEC 61850.

<b>IEC 61850</b>	<b>NOMBRE</b>	<b>DESCRIPCIÓN</b>
IEC 61850-1	INTRODUCCIÓN Y RESUMEN	Descripción de alcances de la norma
IEC 61850-2	GLOSARIO	Describe los términos definiciones empleadas en la redacción de la norma y en el contexto de los sistemas automatizados de subestaciones
IEC 61850-3	REQUERIMIENTOS GENERALES	Define los requisitos de desempeño que deben tener los componentes asociados a la norma.
IEC 61850-4	SISTEMA Y ADMINISTRACIÓN DEL PROYECTO	Defina conceptos de administración para proyectos de sistemas automatizados de subestaciones.
IEC 61850-5	REQUERIMIENTOS DE COMUNICACIÓN	Define los requisitos de comunicación para los modelos planteados para los equipos y funciones.
IEC 61850-6	LENGUAJE DE DESCRIPCIÓN DE LA CONFIGURACIÓN PARA LA COMUNICACIÓN	Define el lenguaje que describe la comunicación en la subestación SCL.
IEC 61850-7-1	MODELOS Y PRINCIPIOS	Describe los métodos de modelado y los principios de comunicación utilizados para el desarrollo del estándar.

IEC 61850-7-2	SERVICIOS DE COMUNICACIÓN ABSTRACTOS (ASCI)	Descripción del interfaz ACSI, especificación de los servicios de comunicación abstractos
IEC 61850-7-3	CLASES DE DATOS COMUNES	Describe las clases de datos comunes (CDC) y sus atributos.
IEC 61850-7-4	CLASES DE NODOS LÓGICOS COMPATIBLES Y CLASES DE DATOS	Describe los nodos lógicos determinados en la norma, especificados en el modelado de funciones y equipos.
IEC 61850-8	SERVICIOS DE COMUNICACIÓN ESPECÍFICOS DE MAPEO MMS	Describe los métodos en los cuales implementar los servicios de comunicaciones descritas en el estándar.
IEC 61850-9	SERVICIOS DE COMUNICACIÓN ESPECÍFICOS DE MAPEO SV	Describe la implementación de comunicación entre los equipos de patio y los IED.
IEC 61850-10	PRUEBAS DE CONFORMIDAD	Describe las pruebas de conformidad para validar los dispositivos que se comunicarán utilizando estos protocolos.

### 3.1. Modelo de datos

#### 3.1.1. Nodos Lógicos

En la comunicación vertical, el IEC 61850 utiliza el concepto de cliente-servidor, ya que el IED es el servidor en el nivel de proceso o de bahía, así proporcionando todos los datos al cliente en la estación o en cualquier otro nivel. Todos los datos se proporcionan a petición del servidor mediante un informe del servidor emitido si se cumplen ciertas condiciones [17].

Principalmente el cliente debe ser un ordenador que representa un puesto de trabajo del operador, una de las acciones que realiza el cliente es enviar comandos al servidor para cambiar los datos en servidor para:

- Emitir comandos para el funcionamiento de interruptores
- Modificar el comportamiento del servidor mediante el cambio de datos internos (por ejemplo, cambio de conjuntos de parámetros, puntos de ajuste analógicos, habilitación o desactivar funciones)

En una comunicación cliente-servidor, el cliente controla el intercambio de datos. Por lo tanto, la comunicación cliente-servidor es muy flexible en cuanto a los datos a

transmitir. En comparación con un sistema maestro-esclavo, el concepto cliente-servidor permite la implementación de múltiples clientes en el mismo sistema. La comunicación cliente-servidor se basa en la pila completa de siete capas utilizando una capa de transmisión confirmada y, en consecuencia, es muy fiable, pero consume relativamente tiempo. Por lo tanto, la comunicación cliente-servidor no es adecuada para la transmisión de datos en tiempo crítico, pero sí para la comunicación con un operador que tiene un tiempo de respuesta del orden de 1seg. [17].

La norma IEC 61850 no sólo especifica el método de la transferencia de datos, véase la Figura 13. También define los datos de proceso de los servidores. Para ello, IEC 61850 utiliza un enfoque orientado a objetos con LN como objetos centrales [17].

LN consiste en la agrupación de datos que representan una función más pequeña, que puede implementarse de forma independiente en dispositivos, se tiene como ejemplos los datos de interruptor disyuntor que contiene datos de su nodo lógico XCBR o todos los datos del nodo lógico de una protección de sobre intensidad temporizada que se va a reflejar como PTOC [17].

IEC 61850 puede extraer las definiciones de los objetos del dispositivo a través de la red. El resultado es un gran ahorro en el coste y el esfuerzo para configurar un dispositivo IEC 61850.

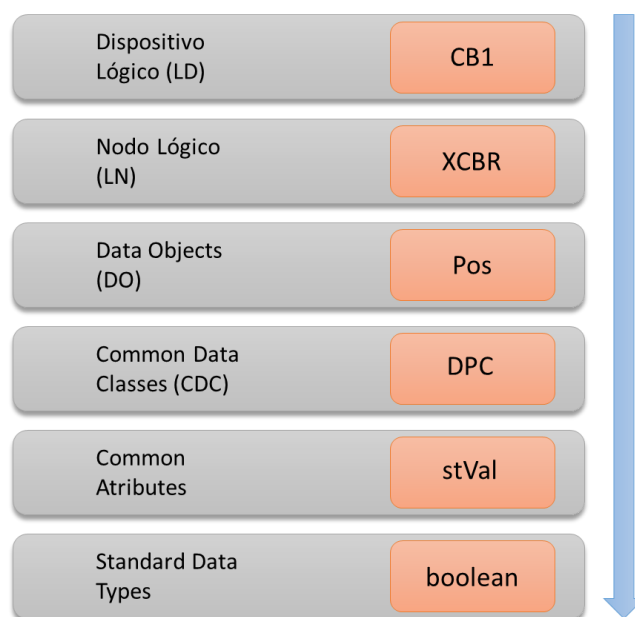


Figura 13. Modelo de datos según el estándar. Fuente: Autores.

Existen nodos lógicos para el control automático cuyos nombres comienzan con la letra "A". Hay NL para la medición, cuyos nombres comienzan con la letra "M". Cada nodo lógico tiene un LN-Instance-ID como sufijo al nombre del nodo lógico como se indica en la Tabla 2.

Tabla 2: Nodos Lógicos.

LETRA	DESCRIPCION
A	CONTROL AUTOMATICO
M	MEDIDAS Y MEDICION
C	CONTROL Y SUPERVICION
G	FUNCION GENERICA
I	INTERFACES Y ARCHIVOS
L	NODOS LOGICOS DEL SISTEMA
P	PROTECCION
R	PROTECCIONES RELATIVAS
S	SENSORES Y MONITOREO
T	INTRUMENTOS DE TRANSFORMACION
X	INTERRUPTORES (DISYUNTORES)
Y	TRANSFORMADORES DE POTENCIA
Z	OTROS EQUIPOS DEL SISTEMA DE POTENCIA

La estructura del nodo lógico está conformada por las siguientes partes y cada elemento determina la funcionalidad y operación a la que está asignada el IED, véase la Figura 14, se describe con la notación siguiente:

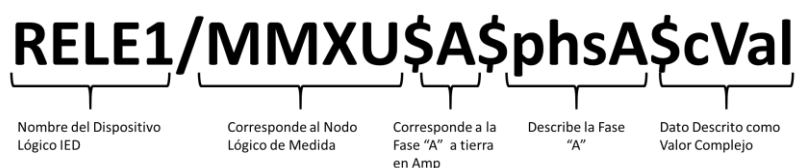


Figura 14. Estructura del nodo lógico. Fuente: Autores.

## 3.2. Tipos de mensajes y su estructura

### 3.2.1. Mensajería MMS

La mensajería MMS es ISO/IEC9506, es más conocido como un estándar internacional de paquetes, estos realizan la interacción y supervisión de los datos en tiempo real entre los dispositivos. Los servicios proporcionados por mensajería MMS que se aplica

en áreas industriales de automatización por esa razón la norma IEC 61850 adopta a las normas ISO/IEC9506-1 e ISO/IEC9506-2, y hace un mapeo de ACSI a MMS [18].

La mensajería MMS se caracteriza por, [18]:

- Define la forma de interacción de los paquetes y la expresión de datos estructurados y representa cualquier estructura de datos compleja.
- Define el servicio del objeto de datos.
- Proporciona a los usuarios un entorno de comunicación general independiente de las funciones alcanzadas.

### **3.2.2. Mensajería GOOSE**

La mensajería de clase GOOSE, es utilizada para la distribución de datos en entrada y salida entre los IED que se encuentran en el nivel de bahía, los mensajes GOOSE son de alta prioridad en una acción de disparo de una protección y el accionamiento de un interruptor [19].

Los mensajes GOOSE son unidireccionales, teniendo así una gran ventaja de comunicación, ya que cuando existe una falla o novedad en los datos, su transmisión de datos tiene una prioridad de adelantarse ante cualquier otro dato enviado [19].

El modelo de servicio GOOSE de la norma IEC 61850-7-2 ofrece la posibilidad de una distribución rápida y fiable de los valores de los datos de entrada y salida en todo el sistema [19].

En la siguiente Figura 15 podemos observar cómo se da el salto de prioridad de los mensajes GOOSE.



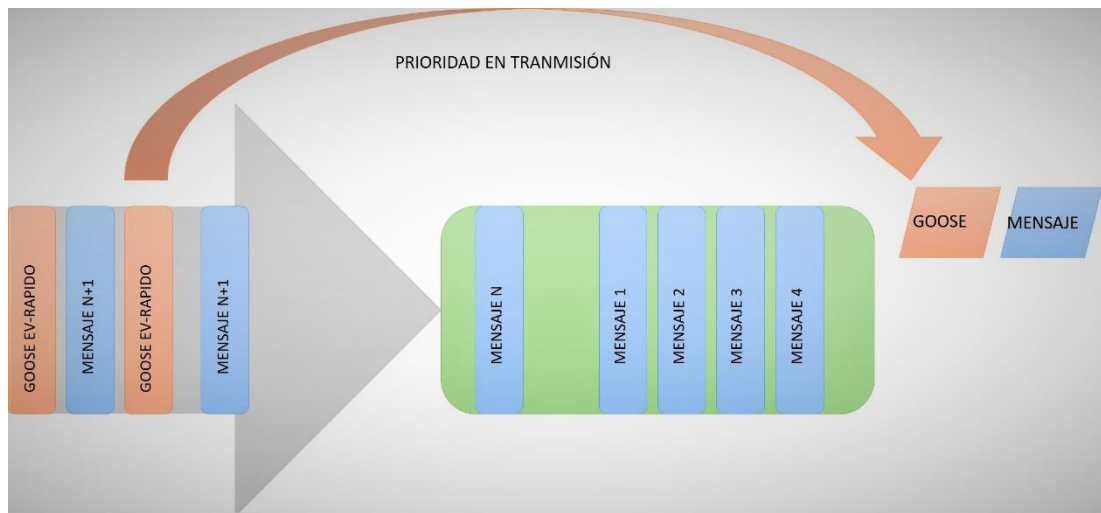


Figura 15. Prioridad en transmisión de mensajes GOOSE. Fuente: Autores.

### 3.2.3. Mensajería SV

La mensajería SV, de tipo comunicación editor/suscriptor, es utilizado para el intercambio de información entre las Merging Units y los IED en una subestación eléctrica a través de Ethernet [19]. Véase la Figura 16.

Una de las guías más comunes para referenciar la implementación del protocolo SV, se puede encontrar en el capítulo IEC 61850-9-2LE.

En definición la mensajería SV, el editor envía periódicamente mensajes con intervalos de tiempo definidos, para determinar el intervalo de tiempo se da por dos factores, [20]:

- La frecuencia de la señal medida, valores por norma (50 o 60 hz).
- Las muestras por periodo (SPP), valores por norma SPP: 80 y 256.
- Como el protocolo SV se basa en el editor/suscriptor, la comunicación sólo es posible dentro de la LAN.

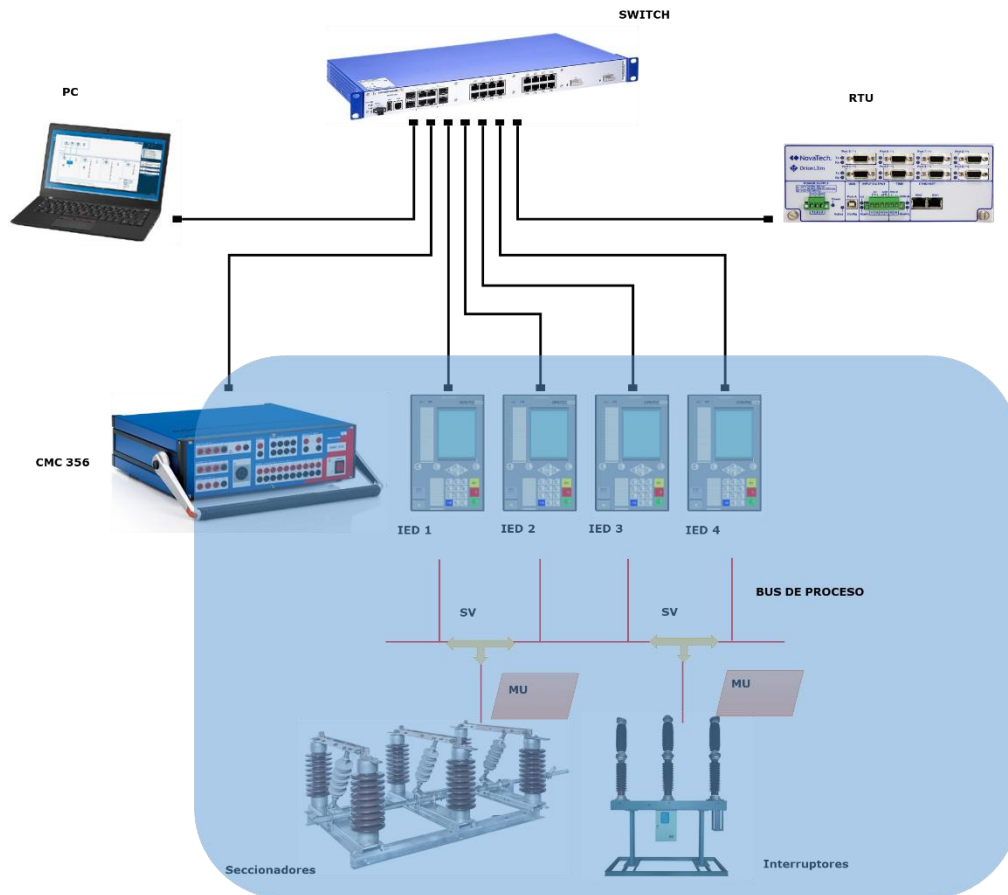


Figura 16. Mensajería SV. Fuente: Autores.

### 3.3. Lenguaje de configuración de subestación SCL

El lenguaje de comunicación SCL, se basa en XML, pero no es necesario tener conocimiento detallado en XML, los archivos que maneja XML SCL (ied.ICD o station.SCD), estos archivos contienen cinco partes que se especifican en la norma IEC 61850-6 en la cláusula 9 y son, [20]:

- La cabecera
- La sección de la subestación describe la estructura funcional y su relación con los dispositivos primarios.
- La sección de comunicación describe la conexión entre los puntos de acceso del IED a la respectiva subred. e incluye también las propiedades (direcciones) de los puntos de acceso.
- La sección IED contiene una descripción de los servicios de comunicación soportados, los puntos de acceso y los dispositivos lógicos del IED, los nodos lógicos y sus atributos.

- La sección de la plantilla de tipos de datos contiene una declaración de todos los tipos utilizados en el archivo SCL el tipo de nodos lógicos, los tipos de DO, los atributos y los enums.

La sección de subestación y la sección de comunicación son tareas para organizar los IED's dentro de la subestación y para establecer la comunicación.

La sección de plantillas de tipos de datos proporciona el contenido correcto de cada tipo de nodo lógico a todas las herramientas y usuarios (clientes) de la información. Cada IED y proveedor puede tener sus propias definiciones de tipos de nodos lógicos incluidas en la sección de plantillas de tipos de datos junto con todos los demás tipos de nodos lógicos basados en la norma [20].

El lenguaje SCL (Véase la Figura 17) establece cuatro archivos:

**El archivo SSD;** (System Specification Description), contiene la especificación completa de un sistema de automatización de subestaciones, incluido el diagrama unifilar de la subestación y sus funcionalidades (nodos lógicos).

**El archivo ICD;** (IED Capability Description), define la capacidad completa del IED.

**El archivo SCD;** (Substation Configuration Description), describe los detalles completos de la subestación. Contiene secciones de subestación, comunicación, IED y plantilla de tipos de datos.

**El archivo CID;** (Configured IED Description), describe las configuraciones completas de los IED.

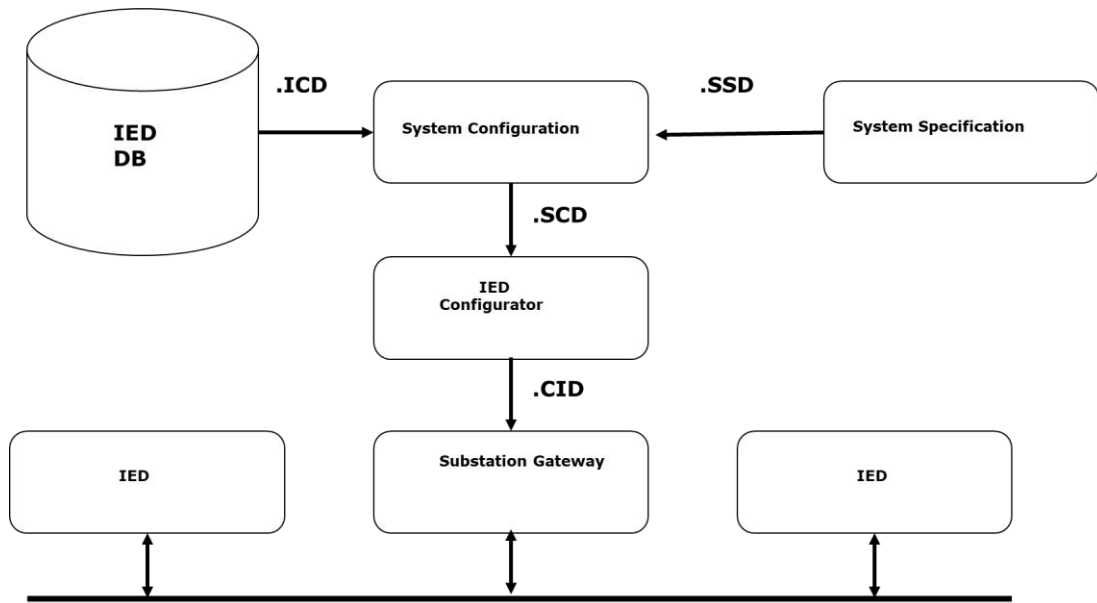


Figura 17. Lenguaje SCL. Fuente: Autores.

## **CAPÍTULO 4**

### **4. MANUAL DE IMPLEMENTACIÓN**

Una vez estudiado el fundamento teórico necesario para la elaboración de este proyecto, se procedió a redactar el manual de implementación, el cual se estableció como uno de los objetivos específicos. Este manual fue elaborado como una guía base con la que se podrá implementar el estándar IEC 61850 en los diferentes IED's, desde la instalación de software requeridos hasta el mapeo de datos. Para esto se trazó una metodología de trabajo (véase la Figura 18) como sigue:

- Herramientas de software: Conoceremos el software necesario para el desarrollo del proyecto, cuáles son sus requerimientos mínimos para la instalación, y alguna configuración en particular.
- Implementación de la red LAN: Se realiza la comunicación de los puertos de los IED's, PC, switch, RTU y maleta de pruebas.
- Implementación del estándar IEC 61850: En esta sección se incorpora el protocolo GOOSE en los IED's, se detallará cómo crear y configurar los archivos SCL, hasta como cargar dichas configuraciones a los dispositivos.
- Guía de pruebas: Se realizará 8 guías de pruebas utilizando el estándar IEC 61850, se detallará la configuración de los dispositivos.

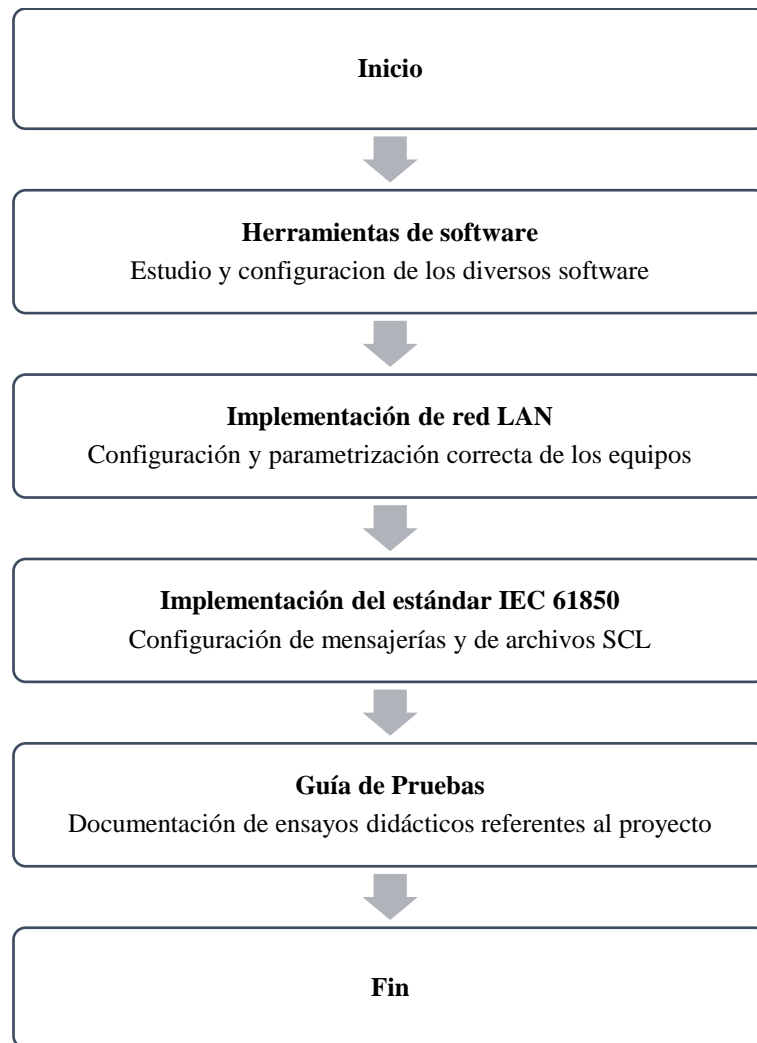


Figura 18. Proceso metodológico del manual de implementación. Fuente: Autores.

#### 4.1. Herramientas de software

Para poder realizar este proyecto se requiere el software de los diferentes dispositivos, los cuales son proporcionados por los respectivos fabricantes.

- NCD
- OMICRON<sup>®</sup> Test Universe
- DIGSI<sup>®</sup> 5
- INKSCAPE<sup>™</sup>

Cada una de estas herramientas se encuentra disponibles desde su sitio web oficial, cabe mencionar, para poder descargar cualquier software es necesario registrarse y crear una cuenta.

#### 4.1.1. NCD

Este es un software de configuración que no requiere ninguna programación o secuencia de comandos para establecer comunicaciones entre el Orion y un maestro de protocolo, la HMI, el Controlador Lógico Programable (PLC), o un IED como un relé o un medidor. Las comunicaciones se establecen en pocos minutos entre productos Orion y los IED's, y entre Orion y los maestros SCADA.

Además de las opciones de configuración, NCD proporciona una ventana terminal incorporada para ver los valores de los datos, las comunicaciones de los puertos, las estadísticas de los dispositivos, los eventos del sistema y la información del sistema/versión. En la Figura 19 se puede apreciar la pantalla inicial de este software.

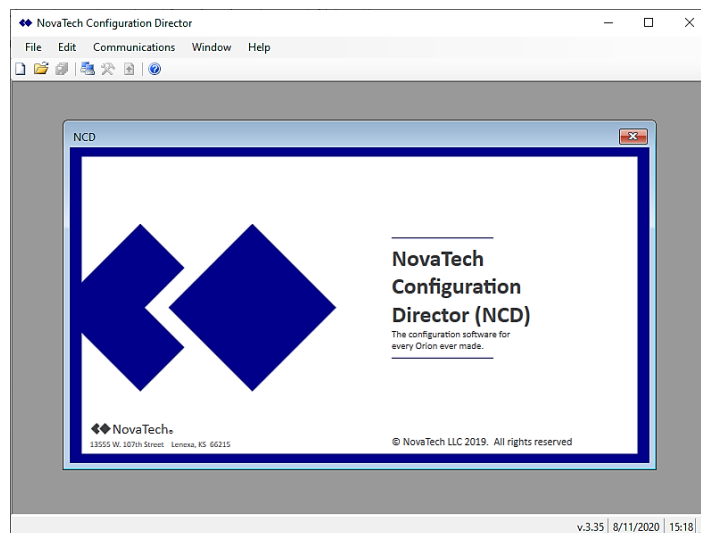


Figura 19: Software NCD. Fuente: Autores.

#### Requisitos mínimos del sistema

- >100 MB de espacio en disco duro
- Windows<sup>®</sup> 7, Windows<sup>®</sup> 8, Windows<sup>®</sup> 10
- .NET 4.0
- Ratón
- Resolución de gráficos 1024 × 768 o mejor
- Unidad de CD / DVD
- Puerto USB o Puerto Serial
- Puerto Ethernet

### 4.1.2. OMICRON® Test Universe

El Test Universe (Figura 20) es la herramienta de software más potente y práctica para las pruebas relacionadas con parámetros básicos de dispositivos de protección y medición en sistemas eléctricos. Incluye varios métodos de pruebas, desde pruebas manuales hasta pruebas totalmente automatizadas y normalizadas, que se ejecutan en un PC [21].

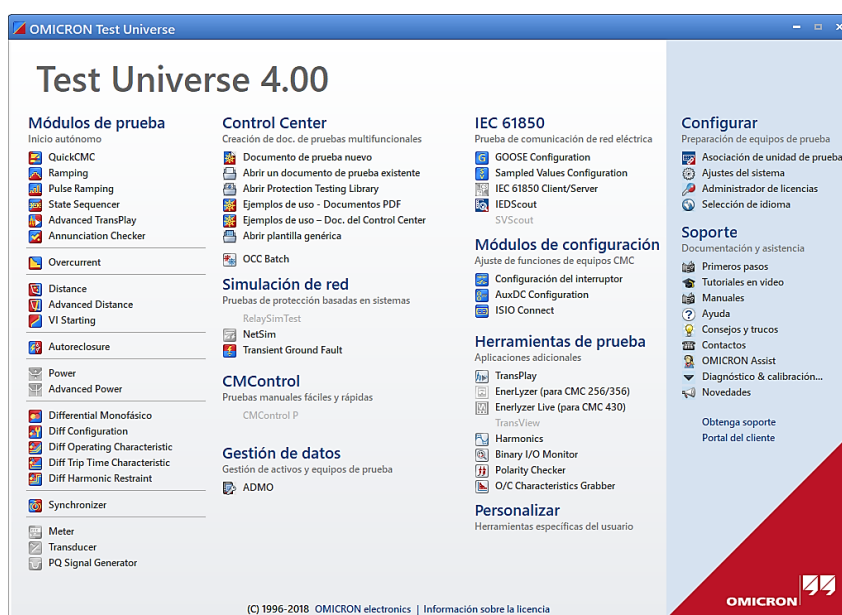


Figura 20. Software OMICRON® Test Universe - Version 4.00. Fuente: Autores.

#### Requisitos mínimos del sistema

- Windows® 7, Windows 8®, Windows® 10
- Puerto USB o Puerto Serial
- Puerto Ethernet
- Teclado y ratón

#### Configuración adicional: Asociar PC con equipo OMICRON®

Teniendo el software Test Universe instalado en la PC, se requiere asociar con el equipo OMICRON® para desarrollar las pruebas, esto se debe realizar cada vez que se haya operado con diferente PC.



La asociación de un equipo de prueba CMC de la forma descrita a continuación, se aplica solamente a la conexión ETH y Wi-Fi. Un equipo de prueba conectado mediante USB no requiere una asociación.

- a. En primer lugar, energizar la OMICRON<sup>®</sup> CMC y junto a la PC conectar a red. Luego, abrir el programa “Test Universe” y en él seleccionar la aplicación “Asociación de unidad de prueba”, esto permitirá abrir el módulo “OMICRON Device Link”.
- b. Después, seleccione el equipo de prueba a asociar.
- c. En el equipo de prueba presione su botón “Asociar” que se encuentra en la parte posterior del equipo por un tiempo menor a 30 segundos.
- d. Finalmente, en el módulo “OMICRON Device Link” se mostrará la palabra “Listo” lo cual significa una correcta asociación.

Al presionar el botón Asociar/ASC se asocian la computadora y el equipo de prueba. Los módulos de Test Universe pueden ahora funcionar con el equipo de prueba. En la Figura 21 se puede apreciar los pasos para asociar el equipo OMICRON<sup>®</sup> con la PC.

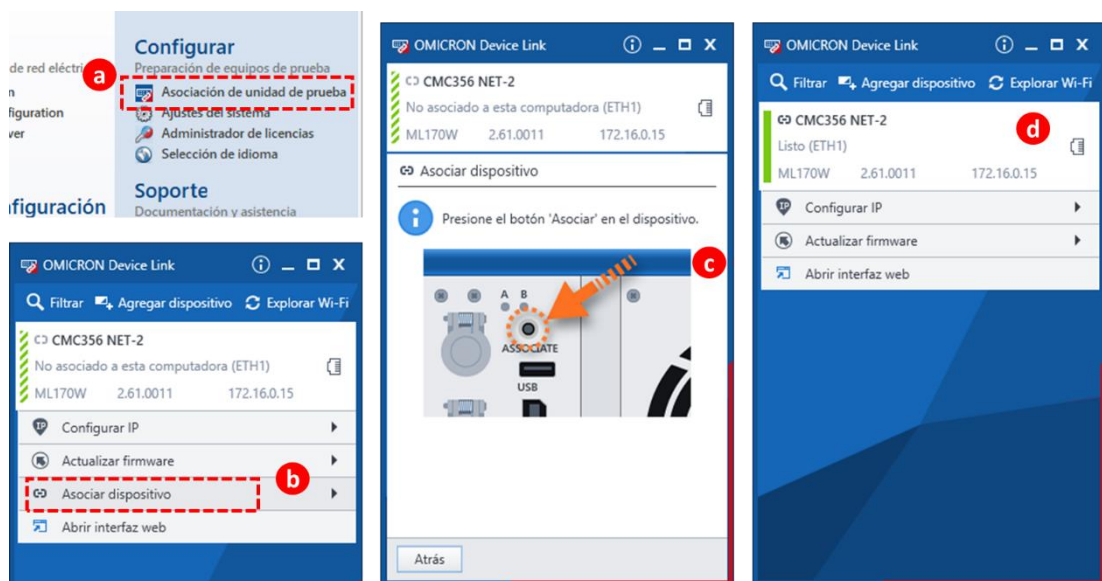


Figura 21: Pasos para asociar equipo OMICRON<sup>®</sup> con PC. Fuente: Autores.

#### 4.1.3. DIGSI<sup>®</sup> 5

DIGSI<sup>®</sup> 5 es la herramienta de ingeniería versátil para la parametrización, puesta en marcha y operación de todos los dispositivos SIPROTEC 5. Su innovadora interfaz de usuario incluye instrucciones de usuario sensibles al contexto. La simple conexión al dispositivo a través de USB le permite trabajar con un dispositivo de manera fácil y

eficiente. Las capacidades completas de DIGSI® 5 se revelan cuando se conecta a una red de dispositivos de protección: entonces puede trabajar con todos los dispositivos en una subestación en un solo proyecto [22]. En la Figura 22 se puede apreciar la pantalla inicial de este software.

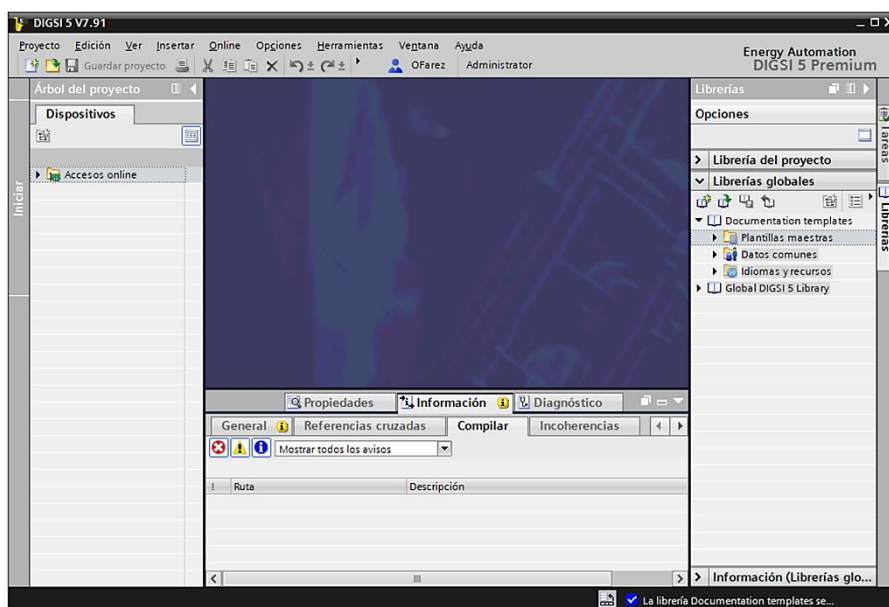


Figura 22: Software DIGSI® 5 - Versión 7.91. Fuente: Autores.

### Requisitos mínimos del sistema

- Intel® Celeron® de doble núcleo 2,2 GHz (Ivy / Sandy Bridge)
- 5 GB de espacio libre en el disco duro (se recomienda un SSD)
- 2 GB de RAM (se recomiendan 8 GB)
- Pantalla gráfica HD ready 1280 x 1024 o 1376 x 768 píxeles
- Unidad de DVD-ROM
- Teclado y ratón
- Puerto USB
- Microsoft Windows® 7 Professional y Enterprise / Ultimate de 32 y 64 bits
- Microsoft Windows® 8.1 de 64 bits
- Soporte VMWare para máquinas virtuales

### Configuración adicional: Instalar controladores de dispositivos

El software DIGSI® 5 requiere importar drivers o controladores de dispositivos (archivos con extensión “.ddd”, Digsig 5 Device Driver) necesarios para la operación

de cada dispositivo específico (protección de sobrecorriente, protección de línea, protocolos de comunicación, etc.). La versión de los controladores de dispositivo debe ser adecuada para la versión del firmware del relé o a la versión del archivo de configuración. En la Figura 23 se puede apreciar los controladores requeridos para este proyecto.

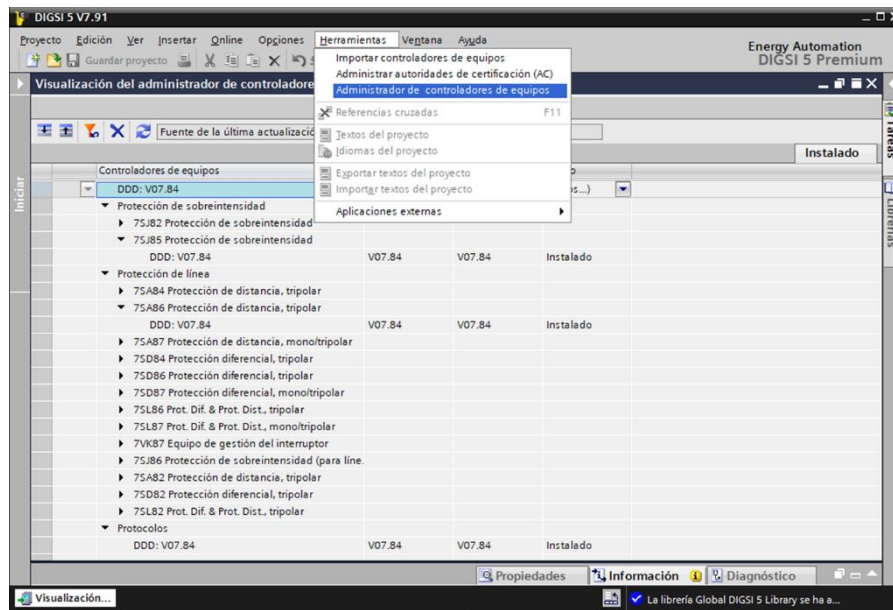


Figura 23: Visualización del administrador de controladores de dispositivos. Fuente: Autores.

#### 4.1.4. INKSCAPE™

INKSCAPE™ es un software de dibujo vectorial, además usa el formato SVG (Scalable Vector Graphics), el cual es un formato de archivo estandarizado, abierto y gratuito para gráficos vectoriales. Es mantenido y desarrollado por el W3C (World Wide Web Consortium), como su formato nativo. Los dibujos SVG se pueden ver directamente en los principales navegadores web, incluidos Firefox, Opera, Safari, Chrome y Edge. Mediante HTML5, SVG se integra fácilmente en las páginas web. Inkscape™ está disponible de forma gratuita para los sistemas operativos Windows®, Macintosh® y Linux™. En la Figura 24 se puede apreciar la interfaz del software.

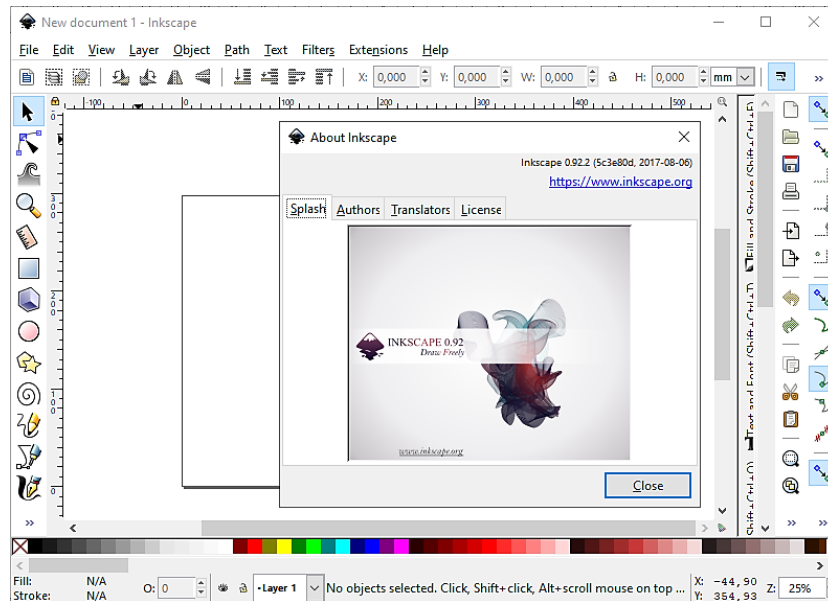


Figura 24: Software INKSCAPE™ - Versión 0.92. Fuente: Autores.

### Requisitos mínimos del sistema

- Multiplataforma: Windows<sup>®</sup>, Linux<sup>™</sup>, MacOS<sup>®</sup>
- Software libre
- Teclado y ratón

### 4.2. Implementación de la red LAN

La elección de una topología de red depende principalmente por ciertos factores como: coste, flexibilidad y fiabilidad. Será de escoger una topología que mejor se adapte a nuestro ambiente de trabajo.

A pesar que el estándar IEC 61850 no define una topología en particular, en el presente proyecto se implementará la topología estrella simple, como se muestra en la Figura 25, en la cual todos los dispositivos van conectados directamente al switch (conmutador); esta topología se caracteriza por no poseer redundancia a nivel de comunicación y su uso general es en aplicaciones de automatización básicos en los cuales existen pocas bahías con sus respectivos IED's.

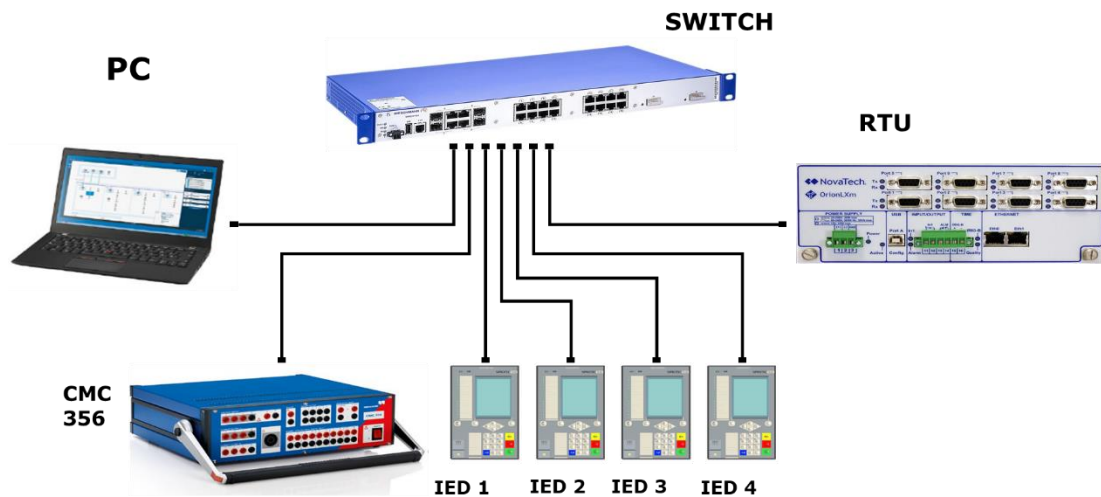


Figura 25: Topología estrella simple a implementar. Fuente: Autores.

#### 4.2.1. Implementación

Para establecer nuestra red LAN se utiliza direcciones IP de clase “C”, la cual tiene aplicaciones en redes pequeñas. Las direcciones IP de clase C tienen un rango desde 192.0.0.0 a 223.255.255.255, y su máscara de subred es 255.255.255.0. Asimismo, el switch industrial administrable permite realizar un subneteo de la red LAN, esto proporciona mayor orden y seguridad al segmento de red física

La finalidad de configurar las IP de los dispositivos y que dichos dispositivos se encuentren dentro del mismo segmento de red, es para poder establecer el control, monitoreo y comunicación entre ellos.

Las direcciones IP asignada a los dispositivos son atribuidas de acuerdo a la Tabla 3.

La configuración de la red LAN en los dispositivos, se realizó mediante el software propietario de cada uno respectivamente. A continuación, se describe la configuración realizada en cada uno de ellos.

Tabla 3: Direcciones IP asignadas.

Dispositivo	Dirección IP	Mascara de Subred	
SWITCH	192.168.1.1	255.255.255.0	
RTU	192.168.1.3		
PC	192.168.1.10		
CMC 356	192.168.1.112		
IED 1: 7SA86	Puerto J		172.16.0.31
	Puerto E		192.168.1.31

IED 2: 7SJ85	Puerto J	172.16.0.32
	Puerto E	192.168.1.32
IED 3: 7SA86	Puerto J	172.16.0.33
	Puerto E	192.168.1.33
IED 4: 7SJ85	Puerto J	172.16.0.34
	Puerto E	192.168.1.34

#### 4.2.2. Ajuste de parámetros de red del switch industrial

Para realizar la configuración de la red en el switch, se deben seguir los pasos que a continuación se detallan:

- En primer lugar, energizar el switch y conectar a la PC mediante el cable USB. Después, abrir el software “HiDiscovery”.
- Seleccionar la tarjeta de red correcta.
- Volver a escanear la red “Rescan”, esto permitirá encontrar los dispositivos Hirschmann® conectados al PC.
- Dar doble clic en el dispositivo encontrado, y ajustar los parámetros de red según sean nuestros requerimientos, véase la Figura 26.

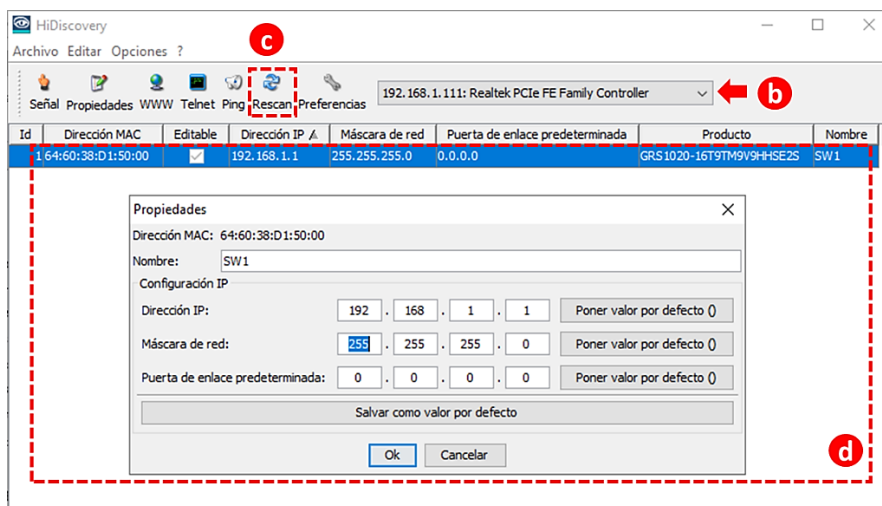


Figura 26: Pasos para configurar los parámetros de red del switch industrial. Fuente: Autores.

#### 4.2.3. Ajuste de parámetros de red de la RTU

En la RTU, la manera de ajustar los parámetros de red es mediante el software NCD. Para ello se deben han adoptado los siguientes pasos:

- a. En primer lugar, energizar la RTU y conectar a la PC mediante el cable USB. Entonces, abrir el software NCD.
- b. Crear una nueva conexión “Orion LXM 01” de tipo serial, la cual permitirá abrir una consola serial, cabe mencionar que se debe escoger el puerto COM correcto, véase la Figura 27.

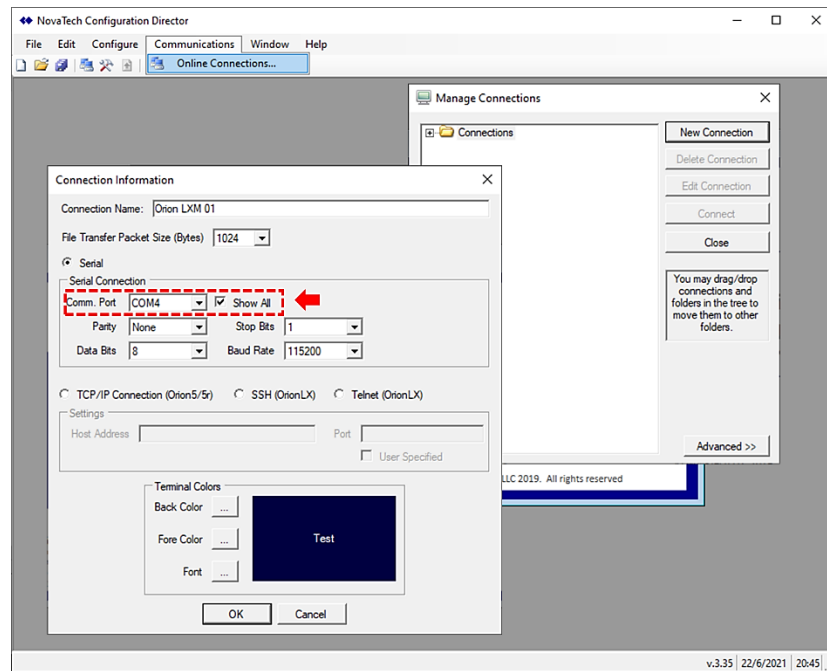


Figura 27: Creación de conexión serial en la RTU. Fuente: Autores.

- c. Abrir la conexión “Orion LXM 01”. Para iniciar sesión, se coloca tanto para usuario como para contraseña la palabra “novatech”.
- d. En el menú principal seleccionar la opción “8. Network Menu”. Después, escoger el puerto deseado, en este caso la opción “1. Edit Eth0 (eth0)”. Posteriormente se procede a configurar los parámetros de Dirección IP, máscara de red y puerta de enlace en el caso de ser necesario. Finalmente, preferir la opción “4. Save Settings” para guardar los cambios, véase la Figura 28.

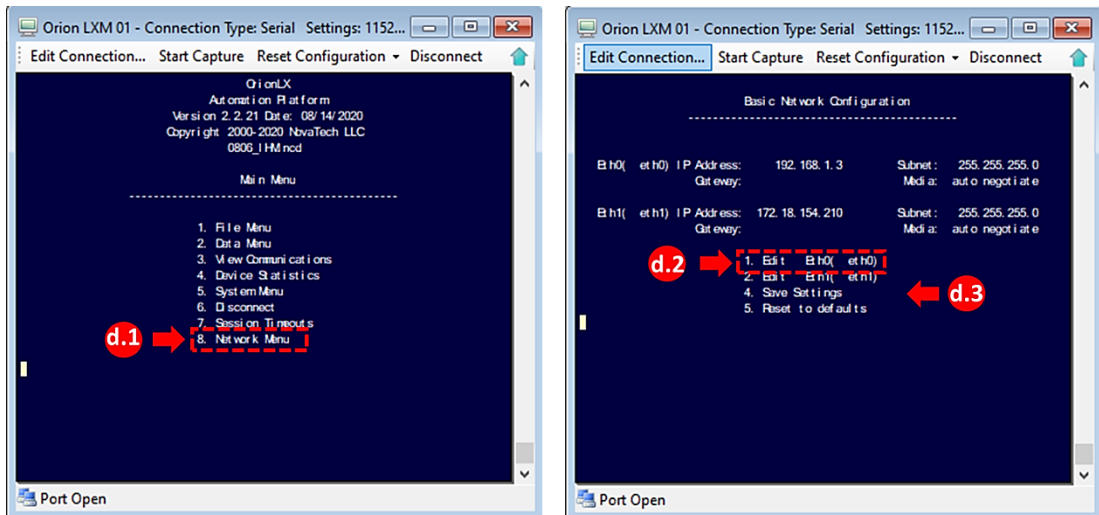


Figura 28: Pasos para configurar los parámetros de red de la RTU. Fuente: Autores.

#### 4.2.4. Ajuste de parámetros de red del PC

En la PC se realiza los siguientes pasos para configurar una red, los cuales se describen a continuación:

- Ingresar al “Panel de Control” y dar clic en “Ver el estado y las tareas de red”.
- Luego, clic en la opción “Cambiar configuración del adaptador”.
- Clic derecho en la opción “Ethernet” y seleccionar “Propiedades”, véase la Figura 29.

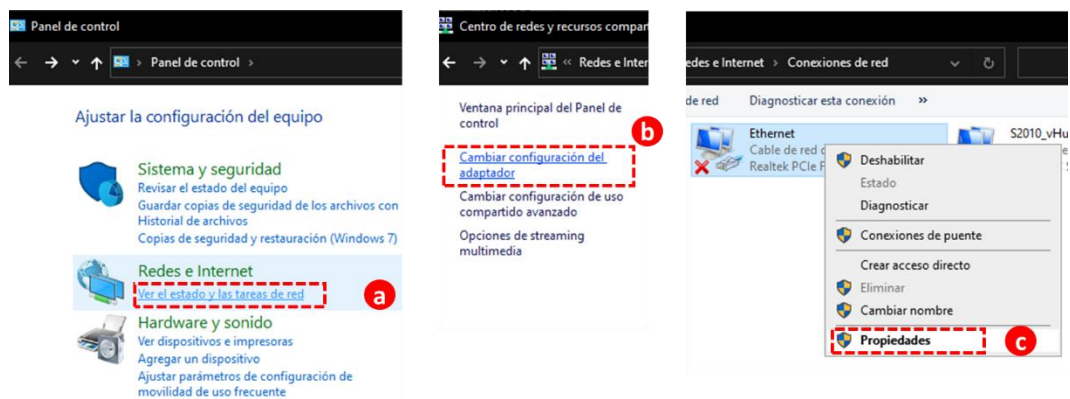


Figura 29: Pasos para configurar la red del PC. Fuente: Autores.

- Después, seleccionar “Habilitar el protocolo de Internet versión 4 (TCP/IPv4)”, y clic en “Propiedades”, tal como muestra la Figura 30.



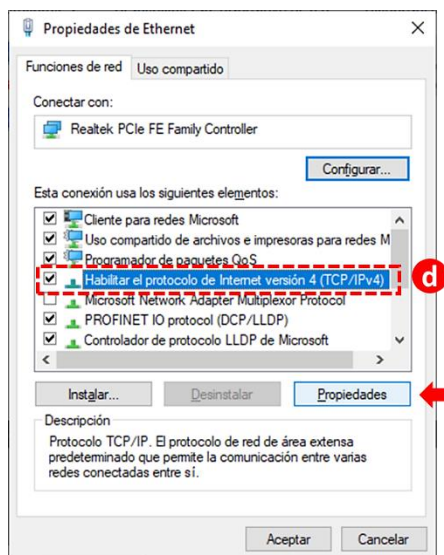


Figura 30: Propiedades de Ethernet. Fuente: Autores.

- e. Finalmente, seleccionar “Usar la siguiente dirección IP” y rellenar los campos de: “Dirección IP”, “Puerta de enlace predeterminado” y “Mascara de subred”, de acuerdo a la Tabla 3; y clic en “Aceptar” para guardar la configuración. Véase la Figura 31.

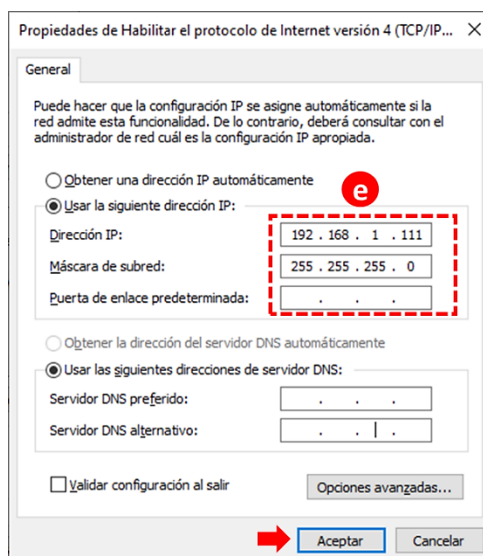


Figura 31: Parámetros a configurar en la PC. Fuente: Autores.

#### 4.2.5. Ajuste de parámetros de red en CMC 356

Para realizar la configuración de la red en el equipo OMICRON®, se deben seguir los pasos descritos a continuación:

- a. En primer lugar, energizar la OMICRON<sup>®</sup> CMC y conectar a la PC mediante el cable USB. Después, abrir el módulo “OMICRON Device Link”. Mediante este tipo de conexión no se requiere una asociación previa.
- b. Seleccionar la opción “Abrir interfaz web” tal como se muestra en la Figura 32, esto permite abrir una ventana con las propiedades del equipo CMC 356 en su navegador web predeterminado.

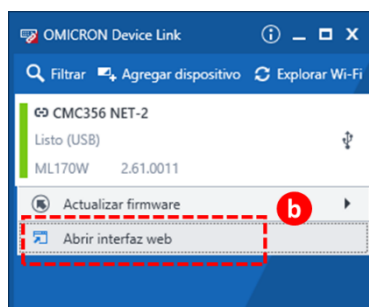


Figura 32: Ventana del módulo OMICRON Device Link. Fuente: Autores.

- c. Seleccionar en el menú principal, la opción “Network”.
- d. Luego, seleccionar “Port ETH1” o “Port ETH2” según criterio de conexión o de topología elegida, para nuestro caso se selecciona “Port ETH1”.
- e. A continuación, seleccionar “Static” para la asignación de red.
- f. Finalmente, rellenar los campos: “Dirección IP”, “Puerta de enlace predeterminado” y “Mascara de subred” de acuerdo a la Tabla 3; y clic en “Apply” para guardar la configuración. Véase la Figura 33.

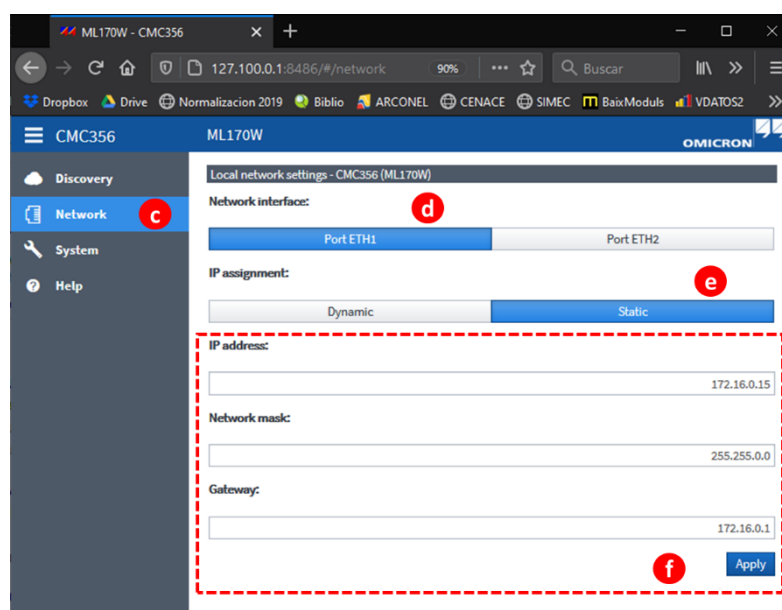


Figura 33: Configuración de la red local. Fuente: Autores.

En el menú principal, opción “System”, se puede visualizar las direcciones IP asignadas o que tienen por defecto los puertos “Port ETH1” y “Port ETH2”, véase la Figura 34.

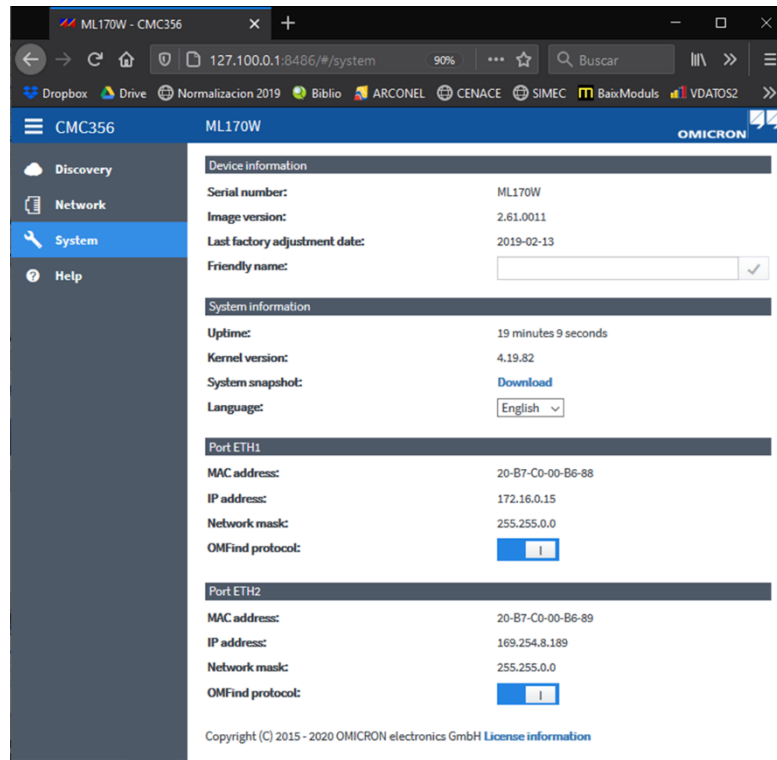


Figura 34: Ajustes de red establecidos en equipo OMICRON®. Fuente: Autores.

#### 4.2.6. Ajuste de parámetros de red en IED's SIEMENS®

En los IED's SIEMENS®, existen dos maneras de ajustar la dirección IP: la primera es manualmente desde el panel frontal del equipo físico y la segunda es mediante el software DIGSI® 5.

El acceso a la información del IED desde el panel frontal se realiza a través de los botones de navegación, Login/Esc y Menú/Enter; además, para la edición de parámetros cuenta con un teclado numérico y demás funciones especiales que son el resultado de la combinación con la tecla Ctrl. En la Figura 35 se puede visualizar el panel frontal de relé SIEMENS®.

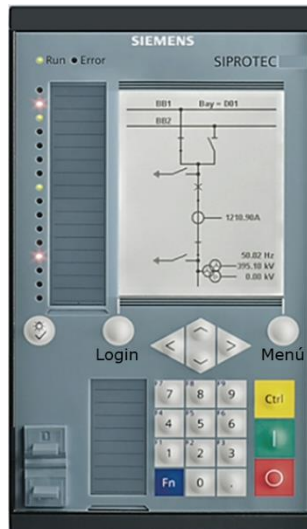


Figura 35: Vista del panel frontal del equipo SIPROTEC 5. Fuente: Autores.

Pasos para identificar o configurar el direccionamiento IP desde el panel frontal del IED; para este caso, se explica la configuración del Puerto E, de igual manera, es para el Puerto J y Puerto F.

1. Seleccionar “Menu”.
2. Seleccionar “Communication”. Esto permite ver los módulos de comunicación disponibles en el equipo.
3. Seleccionar “Menue\_Settings\_ComModule2”, referente al puerto E.
4. Seleccionar “Channel 1”.
5. Seleccionar “IP setting”. Este permite visualizar los parámetros de red.
6. Ingresar la “ID de confirmación” (222222) para modificar cualquier parámetro de red.
7. Finalmente, ajustado todos los parámetros de red, se debe presionar la tecla “Esc” tantas veces sea necesario hasta que solicite reiniciar el equipo, esto permitirá guardar y aplicar la configuración de red establecida.

Los pasos descritos anteriormente se muestran en la Figura 36. Fuente: Autores.

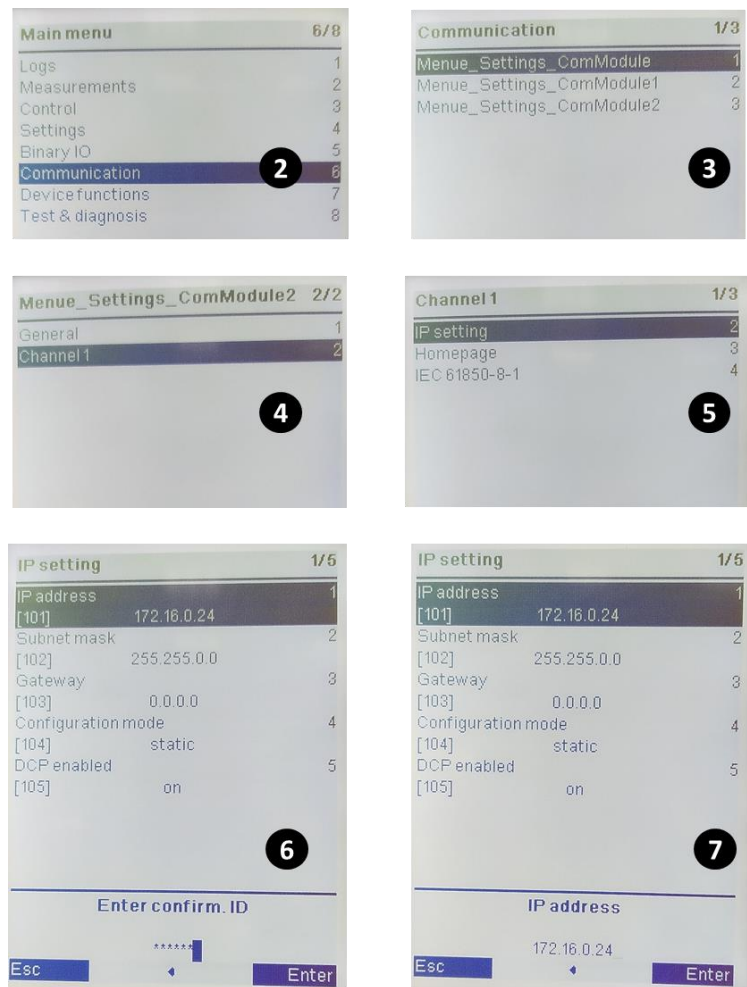


Figura 36: Panel frontal del IED SIEMENS®. Fuente: Autores.

Pasos para configurar el direccionamiento IP desde el software DIGSI® 5:

- a. En primer lugar, encender el IED y conectar a la PC mediante el cable USB. Inmediatamente, abrir el software DIGSI® 5.
- b. Después, añadir un nuevo equipo, ya sea en un proyecto nuevo o en uno existente. Luego, abrir el equipo y seleccionar “Hardware y protocolos”, tal como se muestra en la Figura 37.

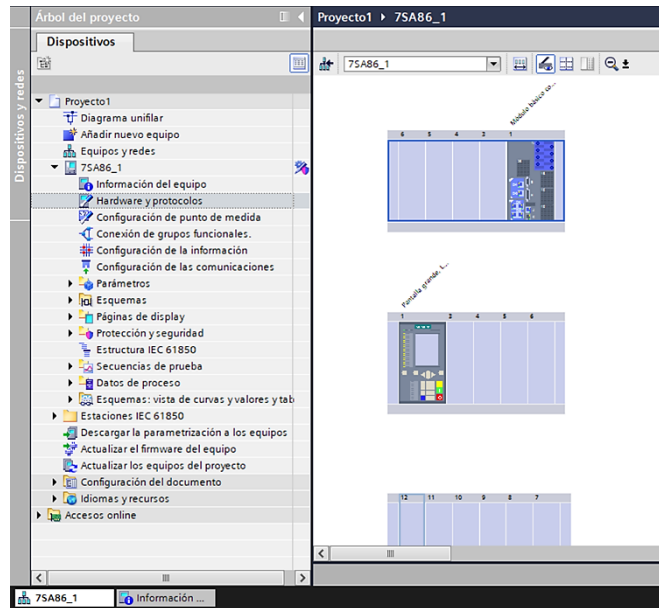


Figura 37: Menú de Hardware y protocolos en DIGSI® 5. Fuente: Autores.

- c. Posteriormente, dar doble clic izquierdo sobre el puerto de comunicación a configurar, ya sea el puerto E, F o J; lo cual permitirá abrir una ventana de propiedades, dentro de la cual se puede configurar el direccionamiento de red, tal como se muestra en la Figura 38.

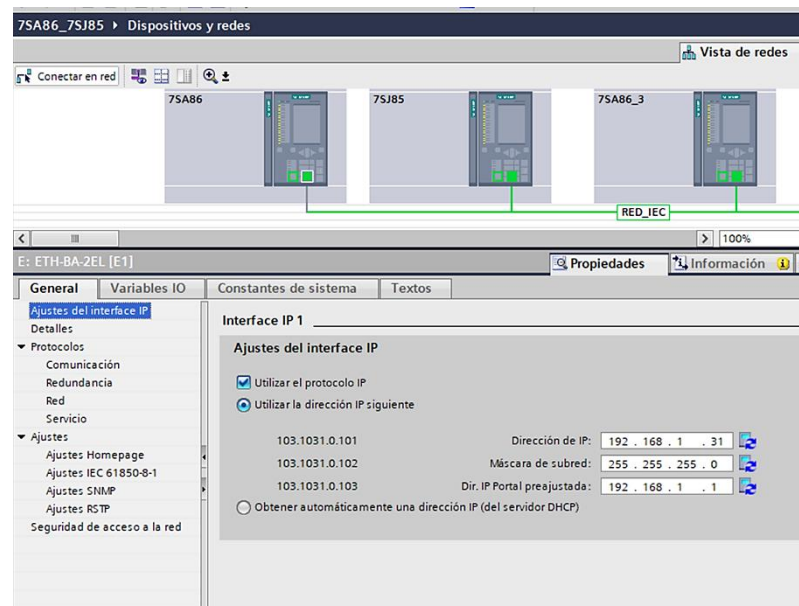


Figura 38: Propiedades del puerto de comunicación en DIGSI® 5. Fuente: Autores.

- d. Una vez configurado el o los puertos de comunicación, clic derecho sobre el equipo, y seleccionar “Cargar la configuración al equipo”, tal como se muestra en la Figura 39.

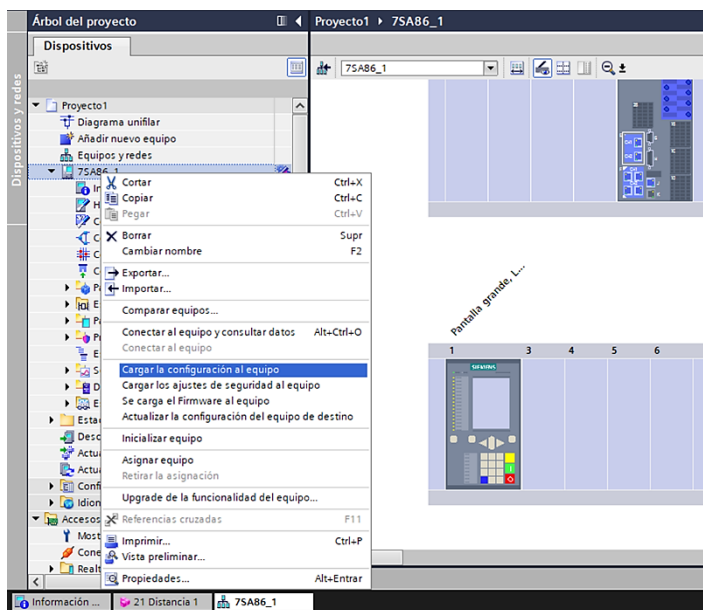


Figura 39: Ventana para cargar la configuración en el equipo. Fuente: Autores.

- e. Finalmente, introducir el código de confirmación (222222) para cargar la configuración al equipo; tal como se muestra en la Figura 40.

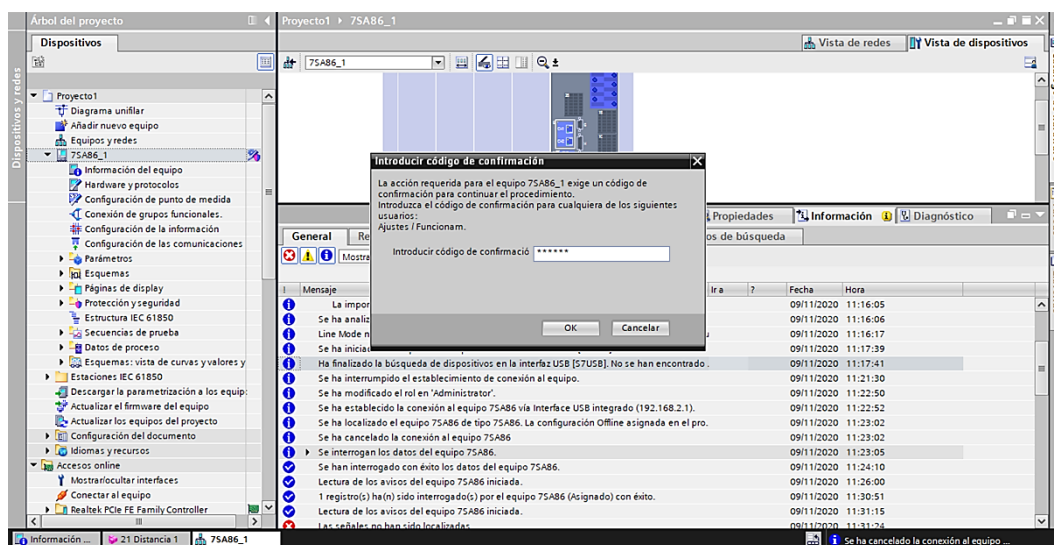


Figura 40: Ventana de solicitud de código de confirmación en DIGSI® 5. Fuente: Autores.

#### 4.2.7. Verificación de red

Para verificar que el estado de la red LAN sea la correcta, se requiere ejecutar el comando Ping desde una PC. Este comando permite diagnosticar el estado de la red, es decir, determina si una IP específica es accesible desde ella o no. El comando PING

funciona a través del envío de un grupo de paquete de datos a una dirección IP, y mediante el tiempo de espera de la respuesta a ese envío de datos se determina el retraso o no de esa respuesta.

Para ejecutar el comando PING se debe seguir los pasos descritos a continuación:

- a. Acceder a la herramienta de “Símbolo del sistema”, ejecutando el atajo tecla Windows + R.
- b. Escribir “CMD” y clic en aceptar, tal como se muestra en la Figura 41.

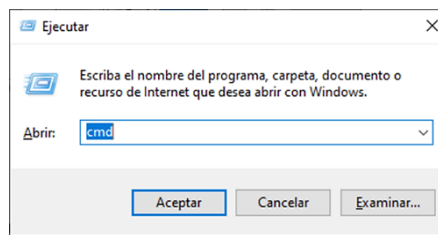


Figura 41: Ventana Ejecutar de Windows. Fuente: Autores.

- c. Luego, se abrirá una ventana del programa, tal como se muestra en la Figura 42; a continuación, digitar el comando “PING” más una dirección IP del equipo con el cual se desee establecer conexión, según la Tabla 3, y presionar la tecla Enter.

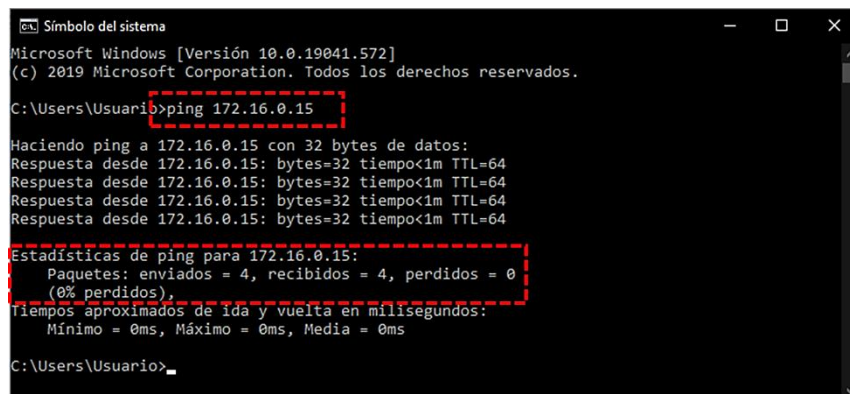


Figura 42: Ventana Símbolo del Sistema para el comando PING. Fuente: Autores.

En función de la respuesta obtenida del PING se puede determinar el estado de la red; si hay 0% de paquetes perdidos indica que la conexión es correcta, por el contrario, si aparece un mensaje como “Red de destino inaccesible” indica que no existe esa dirección IP, o “Tiempo de espera agotado para esta solicitud” indica que hay errores en la conexión.



### 4.3. Implementación del estándar IEC 61850

#### 4.3.1. Ajuste de IED's SIEMENS® en DIGSI® 5

Previamente creado un proyecto en DIGSI® 5, en el cual se ajustó las funciones de protección en los IED's, tales como la protección de sobrecorriente y de distancia. Ahora, se procede a ajustar parámetros relacionados con el estándar IEC 61850, entre las cuales se tiene la asignación de un Nombre y dirección IP del equipo, con el afán de facilitar su identificación dentro de la estación IEC, ya sea para la comunicación horizontal (GOOSE) entre los IED's o para la fácil identificación al mapear datos en la comunicación vertical (MMS).

Tabla 4: Nombres y direccionamiento de IED's.

Dispositivo	Nombre	Nombre IEC 61850	Dirección IP – Port E	Edición
IED 1: 7SA86	7SA86	IED1_86	192.168.1.31	Edición 2
IED 2: 7SJ85	7SJ85	IED2_85	192.168.1.32	
IED 3: 7SA86	7SA86_3	IED3_86	192.168.1.33	
IED 3: 7SJ85	7SJ85_4	IED4_85	192.168.1.34	

Para realizar los ajustes se dirige al “Árbol del proyecto”, sea el caso de editar el “Nombre IEC 61850” seleccionar el menú “Información del equipo” el cual está dentro de cada relé creado (véase la Figura 43); y en el caso del direccionamiento IP seleccionar el menú “Equipos y redes” y cambiar la vista a “Vista de redes”, finalmente seleccionar el puerto “E” del relé a editar (véase la Figura 44). En la Tabla 4 se encuentran los nombres y las direcciones IP establecidas.

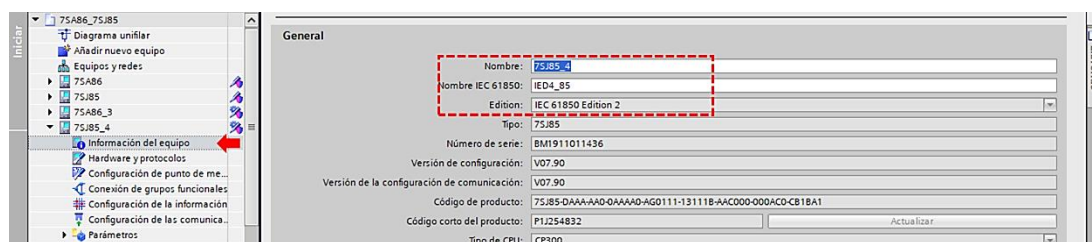


Figura 43. Ajuste de nombre IEC 61850 del IED. Fuente: Autores.

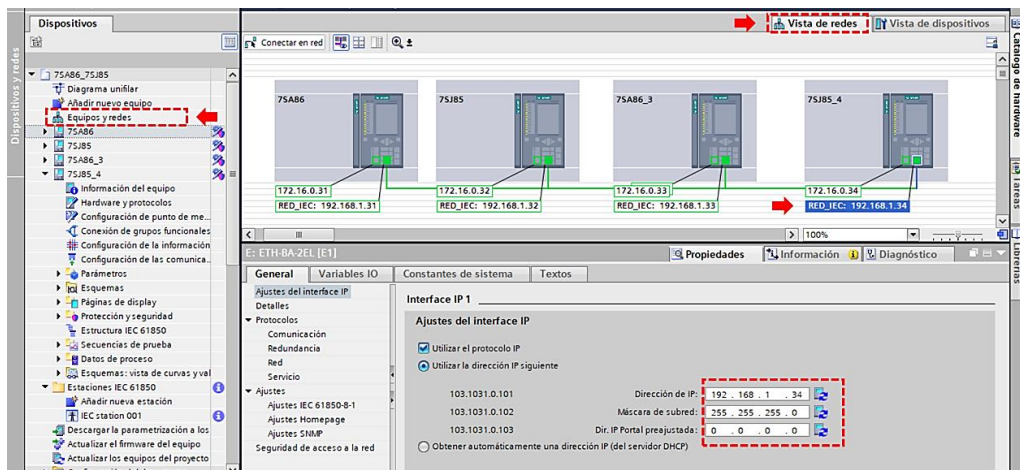


Figura 44. Ajuste de interface IP del IED. Fuente: Autores.

Además, con el puerto “E” seleccionado; dirigirse al menú “Protocolos” (véase la Figura 45) y habilitar el protocolo de comunicación mediante el estándar “IEC 61850”, en el caso de redundancia habilitar el “modo Línea”, en el caso de protocolo de red se debe habilitar “DCP” (Protocolo de Descubrimiento y Configuración Básica, se utiliza para el reconocimiento automático de dispositivos sin una dirección IP configurada) y “SNMP” (Protocolo simple de administración de red, se utiliza para la supervisión de la red), en el caso de servicio habilitar el protocolo “Homepage” (se utiliza con fines de diagnóstico y proporciona los detalles de configuración de los puertos, Port J: http://IP:8080 y Port E: http://IP:8081, véase la Figura 46) y en ajustes seleccionar “ON”.

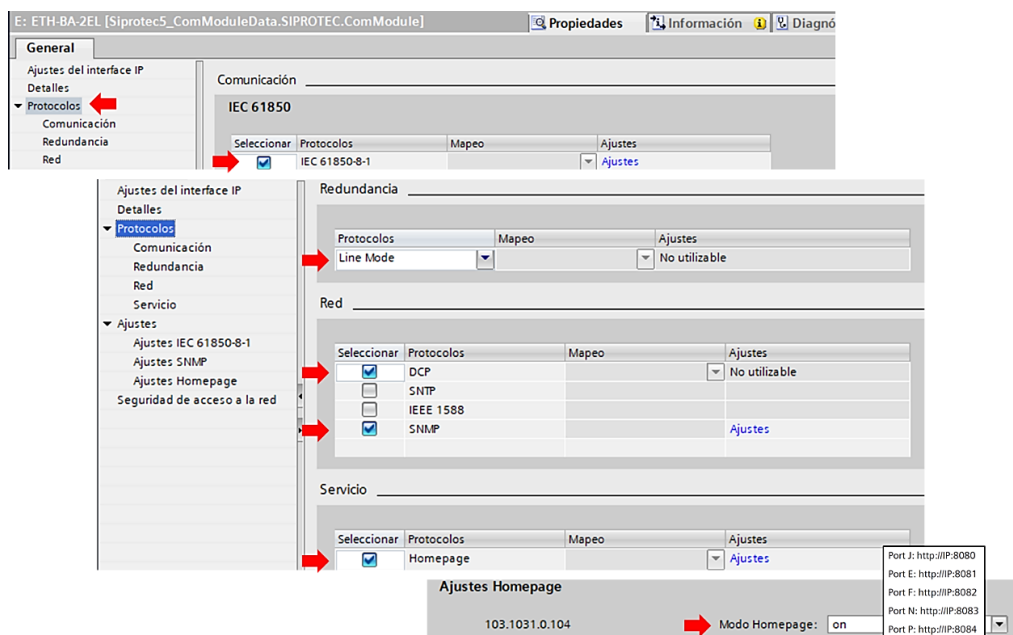


Figura 45. Ajuste de protocolos de comunicación del IED. Fuente: Autores.

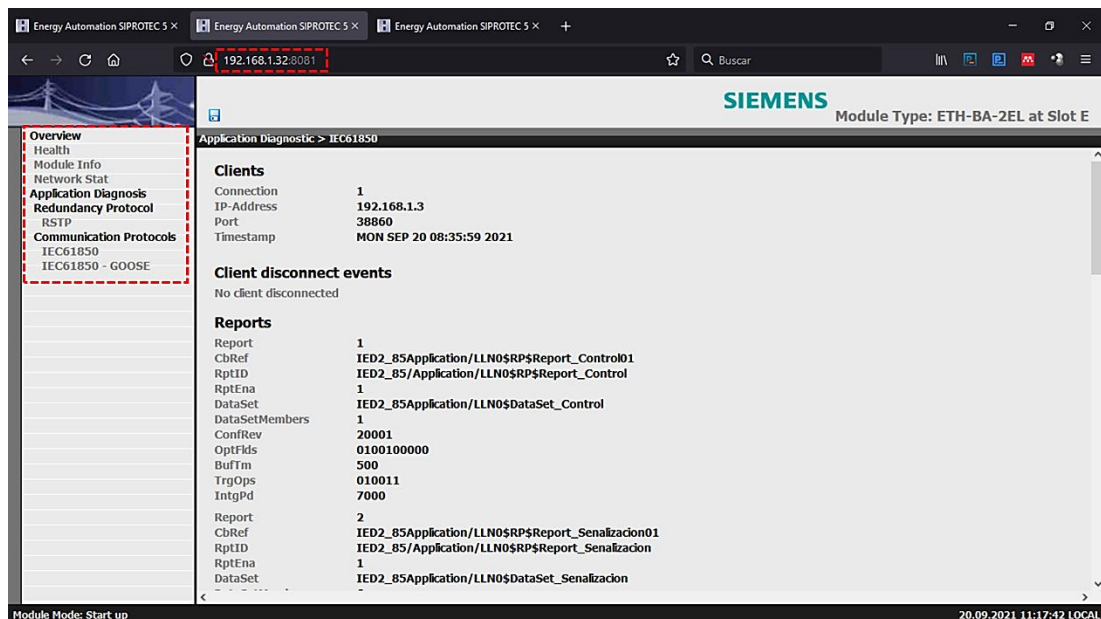


Figura 46. Vista de la interface Homepage del puerto E del IED. Fuente: Autores.  
A continuación, dirigirse al “Árbol del proyecto” y seleccionar el menú “Parámetros” y clic en “Ajustes del equipo” (véase la Figura 47) en él se debe habilitar:

- El “Puerto E” para hacer uso del DIGSI® 5.
- En “Señalización de los ajustes en la estructura IEC 61850” seleccionar “Mostrar todos los ajustes” para que en el modelo de datos se amplíe con todos los ajustes existentes.
- En “Señalización de las extensiones en la estructura IEC 61850” seleccionar “Mostrar todas las extensiones” para que en el modelo de datos se amplíe con todas las señales que no están definidas en el estándar IEC 61850-7-4.
- Además, marcar la casilla “Activar supervisión GOOSE”, para habilitar la funcionalidad de supervisión de conexión mediante ese protocolo.

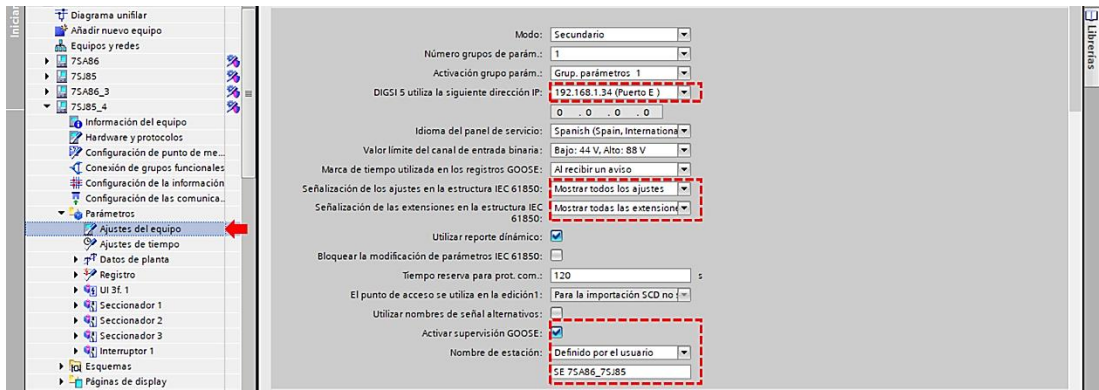


Figura 47: Ajustes del equipo referente a la comunicación IEC 61850. Fuente: Autores.

A continuación, se debe dirigir al “Árbol del proyecto” y seleccionar el menú “Protección y seguridad” y clic en “Seguridad de acceso a la red” (véase la Figura 48), en él chequear que los accesos para el DIGSI®, MMS y Web esté seleccionada la casilla de “Acceso lectura/escritura”.

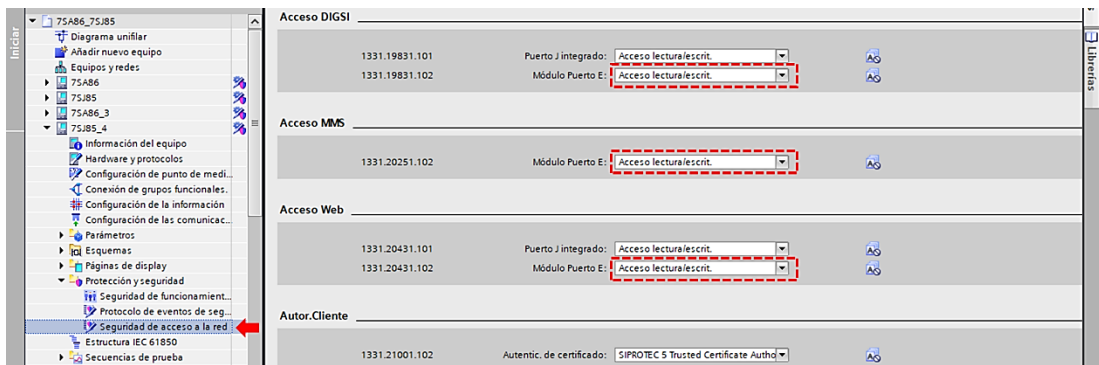


Figura 48. Ajuste de seguridad para el acceso a la red. Fuente: Autores.

Finalmente, ajustar el modelo de datos del dispositivo a una configuración de interfaz deseada, como cambiar el nombre de los LD existentes, modificar los LN, modificar o crear o eliminar DO, activar o desactivar la transmisión de datos, entre otros ajustes. Para ello debe dirigirse al “Árbol del proyecto” y seleccionar el menú “Estructura IEC 61850” (véase la Figura 49) y en el realizar los ajustes necesarios.

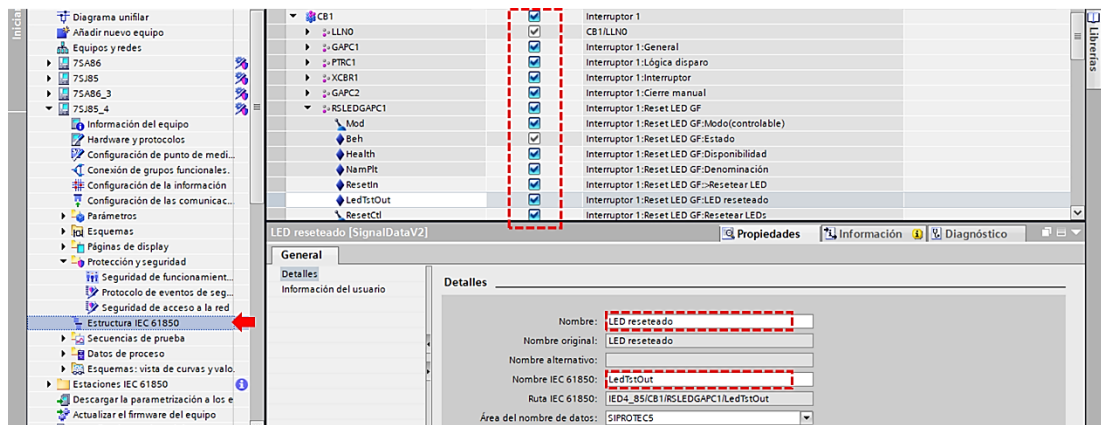


Figura 49. Ajuste del modelo de datos del IED. Fuente: Autores.

### 4.3.2. Creación estación IEC 61850

Una vez creado y ajustados los IED's dentro del proyecto DIGSI® 5 se procederá a crear la “Estación IEC61850” en donde se podrá ajustar los parámetros definidos dentro de la norma, es decir que en dicha estación se podrán realizar los ajustes de comunicación GOOSE, SV o MMS, incluyendo tanto IED's SIEMENS® como de otros fabricantes, véase la Figura 50, a continuación, se listan los pasos a seguir para su creación:

1. Dirigirse al “Árbol del proyecto” y seleccionar el menú “Estaciones IEC 61850” y dar doble clic en “Añadir nueva estación”, se creará una nueva estación, posteriormente, clic sobre ella.
2. Modificar el nombre de la estación IEC y elegir la “Edición 2” ya que actualmente es la más común en los diversos dispositivos.
3. Crear nuevo fichero SCD (Descriptor de configuración de subestación IEC 61850) el cual forma parte del archivo SCL. Luego elegir la ruta en la cual guardar el fichero.
4. Cargar el/los dispositivos necesarios a la estación.
5. Exportar los cambios del dispositivo al configurador del sistema IEC 61850.
6. Proceso de transferencia de archivos.

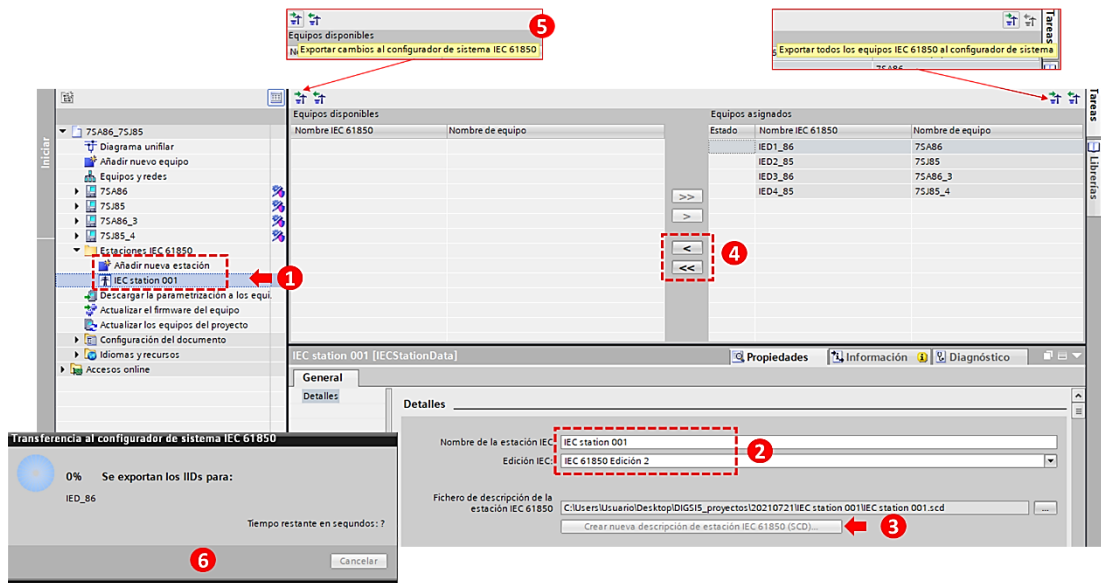


Figura 50. Pasos para la creación de la estación IEC 61850. Fuente: Autores.

Una vez realizada la transferencia al configurador del sistema, inmediatamente se abrirá el software “IEC 61850 System Configurator” tal como se muestra en la Figura 51.

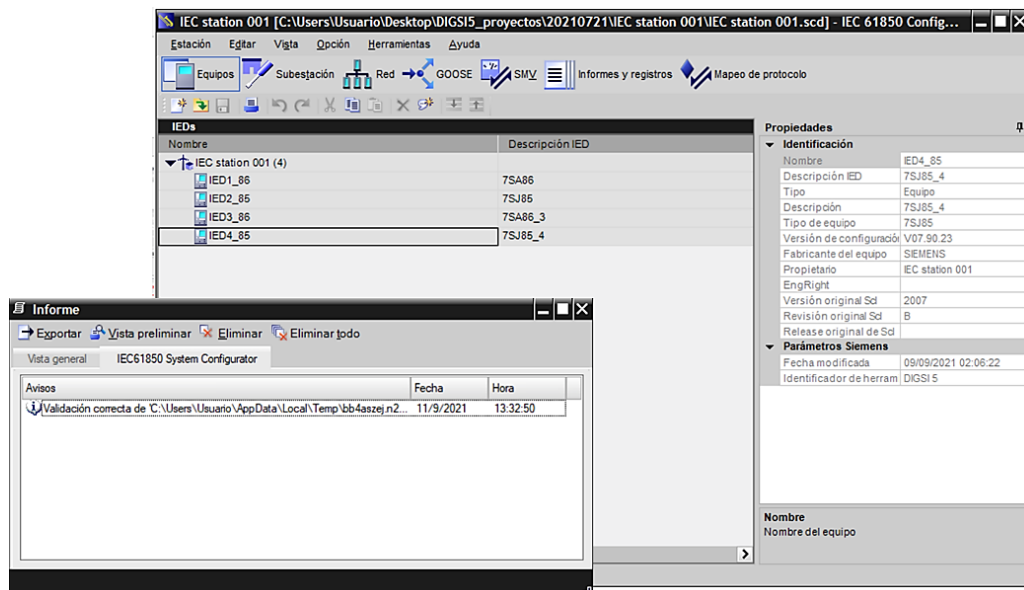


Figura 51. Ventana del configurador del sistema IEC 61850. Fuente: Autores.

En la barra de navegación, seleccionar “Subestación” la cual permite configurar la topología, e incorporar elementos tales como se muestra en la Tabla 5. Tal como se puede visualizar en la Figura 52.

Tabla 5: Elementos del menú subestación.

Nivel	Opción elementos
Estación	Subestación
Subestación	Nivel de Voltaje, Transformador de Potencia
Nivel de voltaje	Bahía, Transformador de potencia
Bahía	Nodo de Conectividad, Equipo conductor

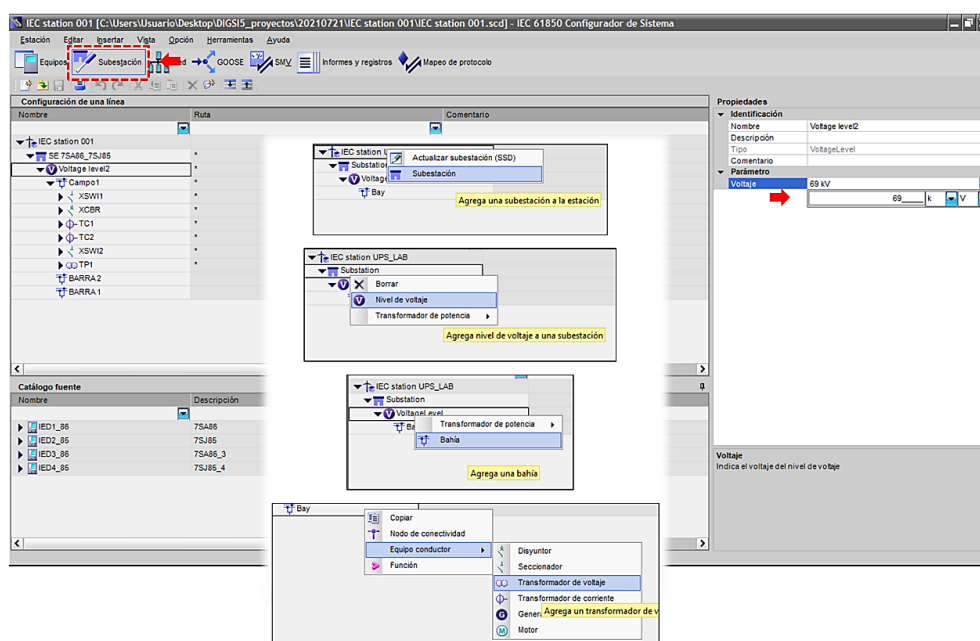


Figura 52. Vista del módulo Subestación en el configurador del sistema. Fuente: Autores.

## Mensajería GOOSE

Para crear mensajes GOOSE se debe insertar la “Aplicación GOOSE” (véase la Figura 53), la cual permite crear conjuntos de datos y dataSets en los diferentes equipos garantizando la comunicación horizontal y transmitiendo mensajes con prioridad alta, a continuación, se listan los pasos a seguir para su creación:

1. Dirigirse a la barra de navegación y seleccionar el menú “GOOSE”.
2. Dar doble clic en “Añadir nueva estación”, se creará una nueva estación, en ella se ajusta la mensajería arrastrando el objeto de datos desde el “Catálogo fuente” y “Catálogo de destino”.

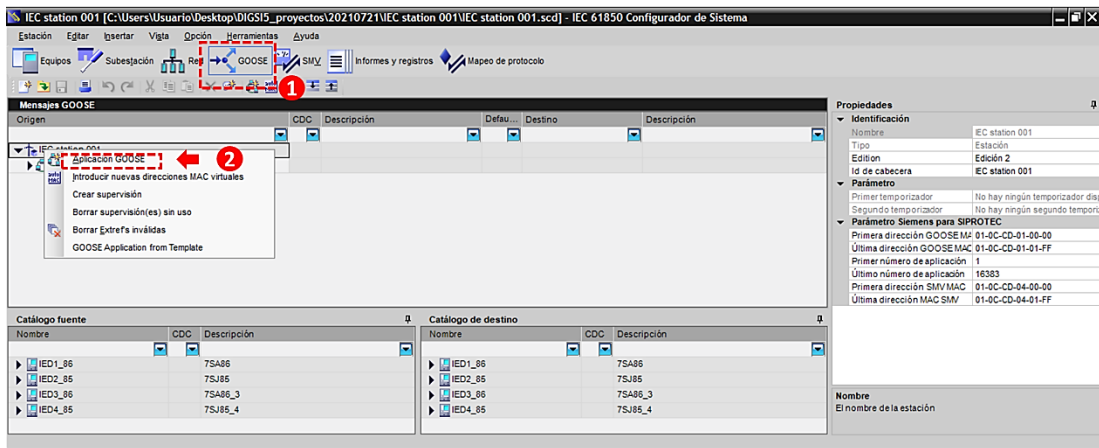


Figura 53. Vista del módulo GOOSE en el configurador del sistema. Fuente: Autores.

- Se crean los dataSets según se arrastre los objetos de datos desde el equipo desglosado, empezando del “Catálogo fuente” y posteriormente del “Catálogo de destino”. También, el objeto de origen puede recibir más de un objeto de destino, véase la Figura 54.

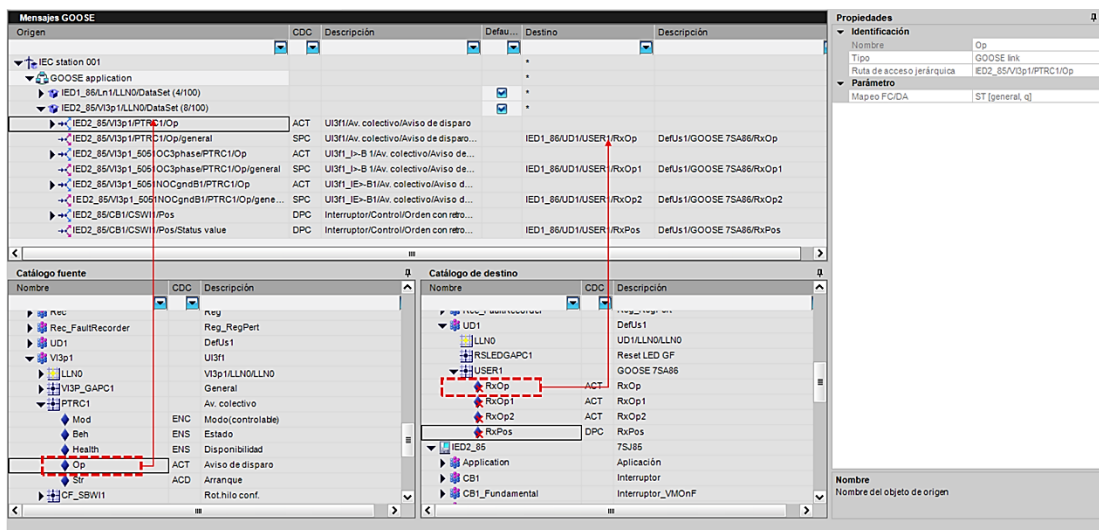


Figura 54. Pasos para configurar la mensajería GOOSE. Fuente: Autores.

Para el caso del ejemplo se ajustó la mensajería de manera que cuando la función de protección principal falle entonces entre a actuar la función de protección de respaldo, es decir, si el rele 7SA86 (IED1\_86) falla o por alguna razón no detecta la falla quien lo respaldaría sería el rele 7SJ85 (IED2\_85).

## Informes y Registros



Dentro del configurador del sistema se procede a crear Informes y registros, en primer lugar, se crea el dataset y a su vez los objetos de datos. Para ello, se han seguido los pasos que a continuación se detallan:

1. Dirigirse a la barra de navegación y seleccionar el menú “Informes y registros”, véase la Figura 55.
2. Insertar los dataSets necesarios en cada equipo, para ello clic derecho sobre el IED y seleccionar “Insert dataset”.
3. Seleccionado el dataset creado se procede a renombrarlo en la ventana de “Propiedades”.
4. Asignar objetos de datos en el dataset, para ello identificar el objeto de dato en el “Catálogo fuente” y arrastrarlo a la ventana (Contenido del dataset).
5. Para la creación de reportes de datos se dirige a la ventana “Control de informes y logs bloqueados”, clic derecho y seleccionar “Insert report”.

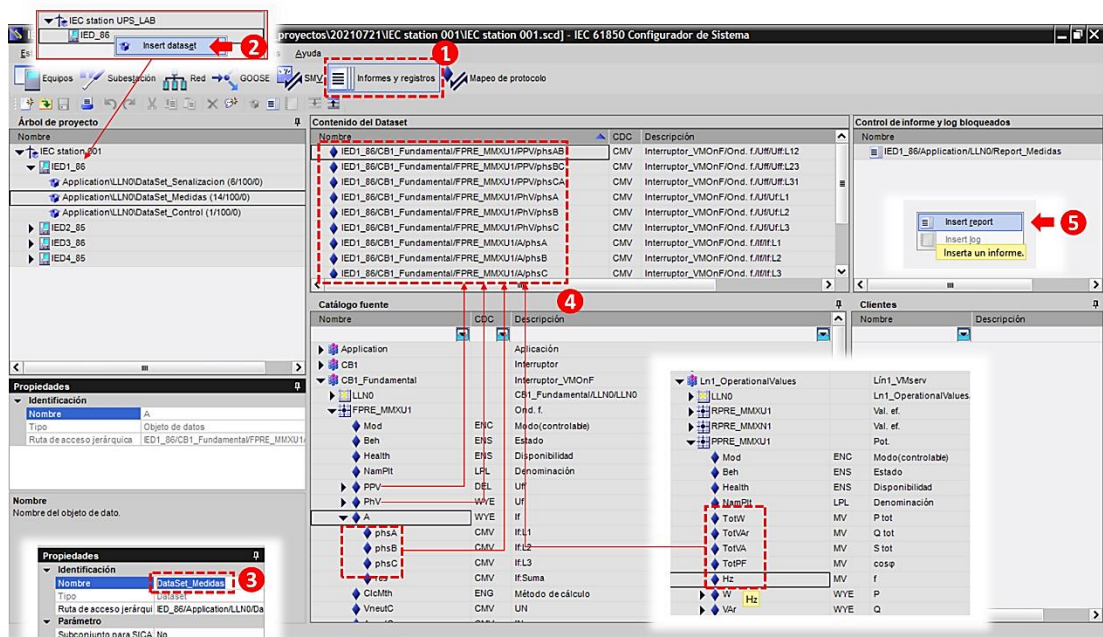


Figura 55. Pasos para configurar el módulo de Informes y registros. Fuente: Autores.

6. Teniendo seleccionado el informe creado se procede a renombrarlo en la ventana de “Propiedades”.
7. Renombrar el informe para una fácil identificación, véase la Figura 56. En el campo de “Parámetro” se puede ajustar la memorización del reporte con el fin de almacenar eventos sucedidos en el caso que la comunicación falle.

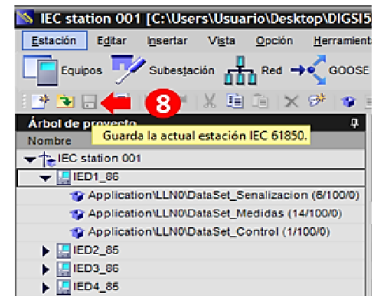
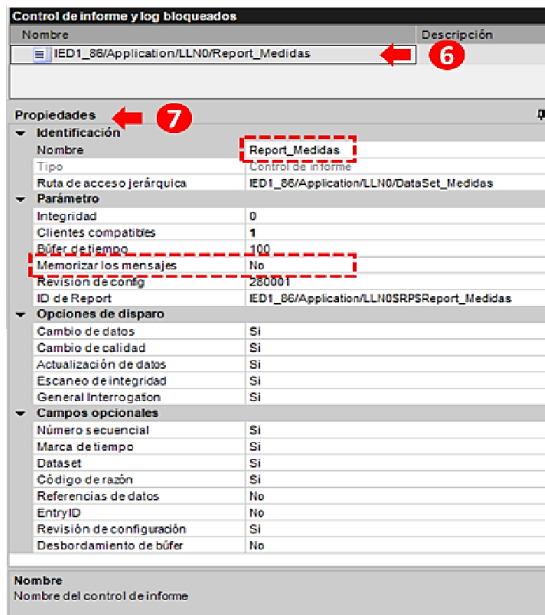


Figura 56. Vista del panel de Control de informe y log bloqueados. Fuente: Autores.

8. Finalmente, guardar el proyecto creado para continuar con la importación de cambios al DIGSI® 5.

### Importar cambios al DIGSI® 5

En el DIGSI® 5, dirigirse al “Árbol de proyecto”, y clic derecho sobre la estación IEC creada, inmediatamente seleccionar “Importar cambios del configurador del sistema IEC 61850”, tal como se muestra en la Figura 57.



Figura 57. Pasos para importar cambios al DIGSI® 5. Fuente: Autores.

Finalmente, cargar los cambios generados en todo el proyecto, a cada uno de los IED's correspondientes.

### 4.3.3. Creación de un proyecto en NCD

El cliente IEC 61850 se configura en un puerto Ethernet del Orion de la siguiente manera, tener en cuenta que solo se puede configurar un puerto de cliente.

1. Abrir el software NCD y crear un nuevo archivo, para ello ir al menú “File” y seleccionar “New”.
2. Enseguida, se abrirá una ventana en la cual se podrá seleccionar el hardware con el que se desea trabajar, en este caso escoger la RTU “Orion LXM” y clic en “OK”, véase la Figura 58.
3. Guardar el documento.

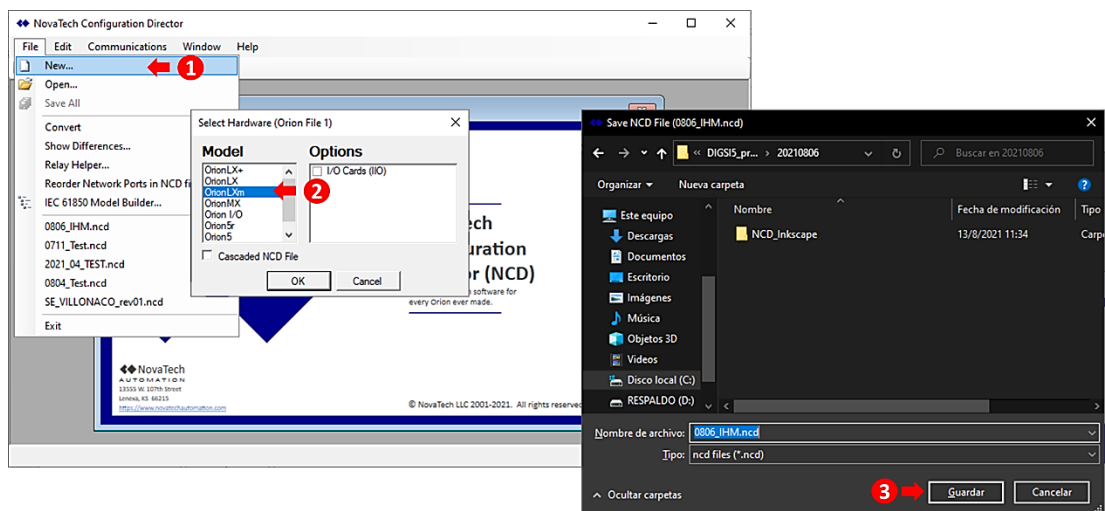


Figura 58. Pasos para crear un proyecto en NCD. Fuente: Autores.

4. Seleccionar el menú “Configure” y clic en el archivo guardado recientemente.
5. Clic sobre la opción “Network”.
6. Se abrirá una ventana en la cual se podrá seleccionar el protocolo de comunicación, seleccionar la opción “IEC 61850 - Client/Server”, y clic en “OK”, véase la Figura 59.

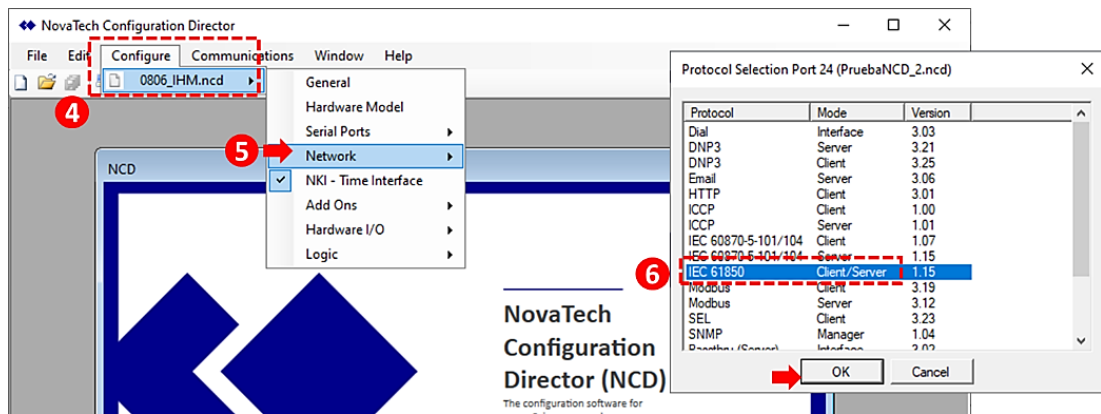


Figura 59. Pasos para configurar el protocolo cliente/servidor en el NCD. Fuente: Autores.

Después de crear el puerto de configuración IEC 61850, se añaden los dispositivos clientes, los cuales se deben configurar con el archivo SCL del dispositivo servidor IEC 61850, archivo del cual el cliente obtendrá los datos. Por lo tanto, se debe configurar de la siguiente manera:

1. Para agregar un dispositivo dirigirse al menú del puerto (panel izquierdo) y haga clic en “Add new device”.
2. Se agrega un nuevo dispositivo etiquetado como Device 1 con subtítulos de Entradas y Salidas. Para importar el archivo configurador SCL, ICD, CID, SCD, o IID, dirigirse al menú del dispositivo y seleccionar “Device 1” y clic en “Import”. Tal como se muestra en la Figura 60.
3. Escoger la carpeta donde se guardó el archivo importado desde la Estación IEC 61850 el cual tiene una extensión “SCD”, seleccionar archivo para importar y clic en “Abrir”.

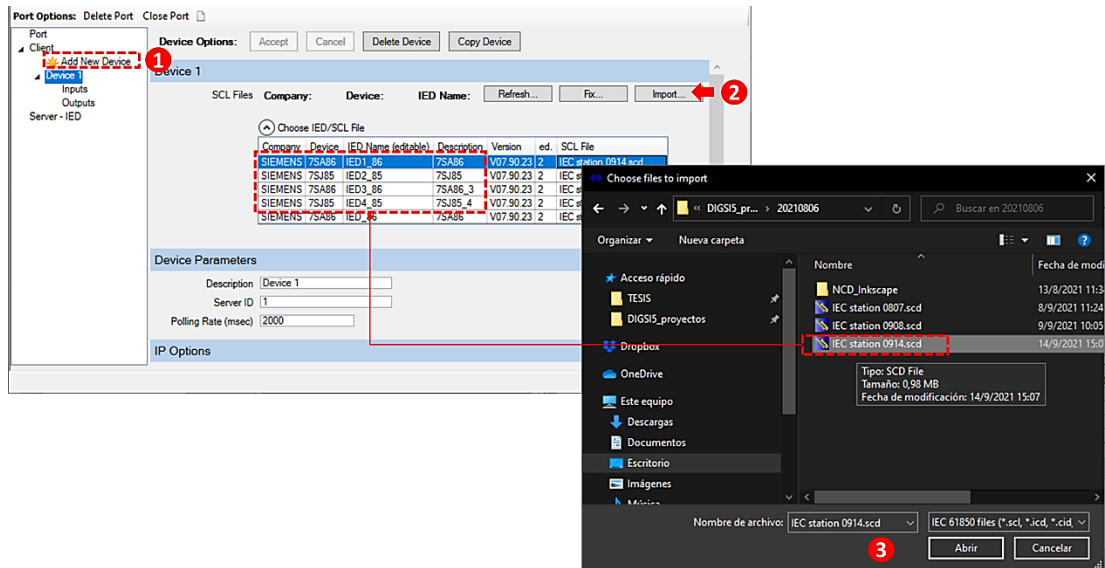


Figura 60. Pasos para importar el archivo SCL de los IED's en el NCD. Fuente: Autores.

4. Seleccionar el archivo SCL que admite el Servidor/IED para cada dispositivo correspondiente, en este caso es el archivo SCD (véase la Figura 61).
5. Renombrar la descripción del dispositivo
6. Clic en “Accept”, y el dispositivo queda configurado.

En el caso de añadir más dispositivos se debe omitir el paso 2 y 3.

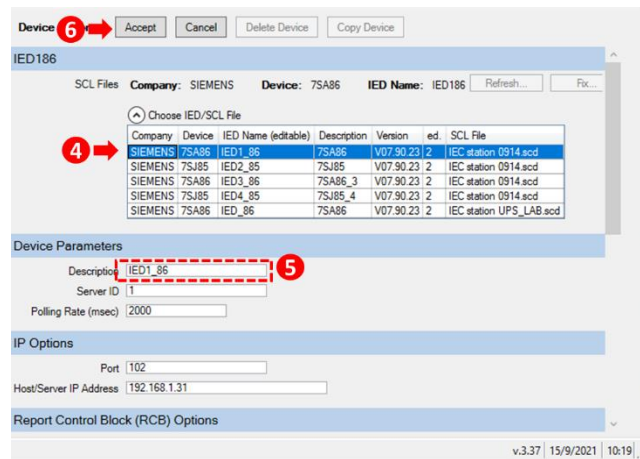


Figura 61. Selección de archivo SCD correspondiente al IED. Fuente: Autores.

A continuación, se selecciona los datos para los puntos de entrada “Inputs” y puntos de salida “Ouputs” de cada uno de los dispositivos (véase la Figura 62), tener en cuenta que los puntos de entrada son aquellas variables que solo pueden ser monitorizadas, en cambio los puntos de salida son aquellas variables que se pueden forzar su valor.

1. Con el dispositivo seleccionado, clic en “Inputs”.
2. En el panel de entradas se muestra una estructura de árbol el cual representa la estructura lógica de un dispositivo y sus nodos, objetos y atributos. Seleccionar o deseleccionar las variables necesarias mediante la activación o desactivación de su correspondiente casilla.
3. Agregar los puntos de entrada seleccionados haciendo clic en “>>”, de lo contrario, hacer clic en “<<”.

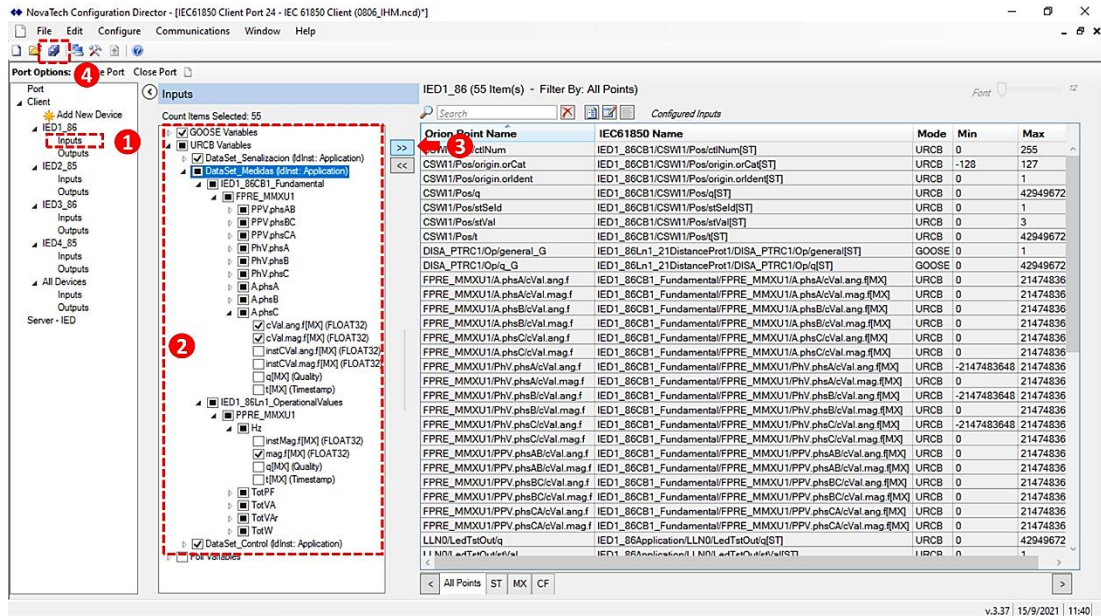


Figura 62. Selección de datos para los puntos de entrada del IED. Fuente: Autores.

Para cambiar el nombre de los puntos de entrada en el campo “Orion Point Name” ingrese el nuevo nombre, luego presione <Enter> para realizar el cambio.

De igual manera se agrega los puntos de salida, en la opción “Outputs” se selecciona las variables y finalmente se transmiten, véase la Figura 63.

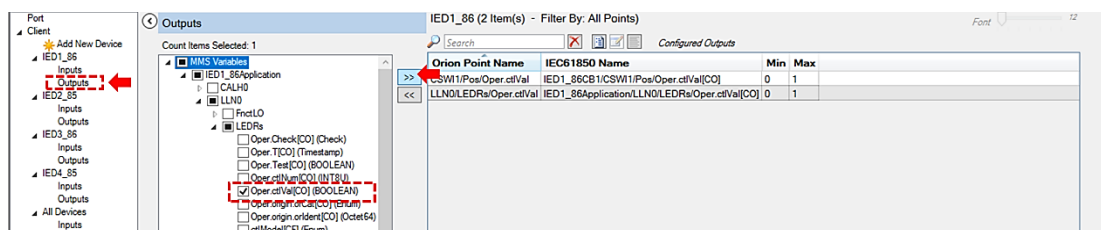


Figura 63. Selección de datos para los puntos de salida del IED. Fuente: Autores.

Las pestañas de filtro para todos los puntos permiten clasificar los puntos de entrada mapeados desde el dispositivo y están ubicados en la parte inferior del panel derecho, y son: ST (información de estado), MX (medidas) y CF (configuración), ver Tabla 6.

Tabla 6: Pestañas de datos.

Pestañas	Descripción Inputs	Descripción Outputs
All points	Muestra todos los puntos de entrada configurados en el panel “Orion Point Name”.	
ST	Muestra solo los puntos de información de estado cuyo valor se puede leer, sustituir, informar y registrar.	Mostrar puntos de control cuyo valor se puede operar (modelo de control).
MX	Muestra solo puntos de información de medición cuyo valor se puede leer, sustituir, informar y registrar.	Muestra los puntos de consigna cuyo valor se puede controlar (modelo de control).
CF	Muestra solo los puntos de información de configuración cuyo valor se puede escribir y leer.	Muestra los puntos de configuración cuyo valor se puede escribir.

A continuación, se procede a configurar el protocolo del servidor XML, en el cual se selecciona las variables a utilizar en el HMI, véase la Figura 64. Se listan los pasos a seguir para su creación:

1. Ir al menú “Configure” y clic en el archivo creado desde el principio.
2. Seleccionar “Network” y clic en “Configure New Port”.
3. Se abrirá una ventana en la cual se podrá seleccionar el protocolo de comunicación, seleccionar la opción “XML - Server”, y clic en “OK”.
4. Para agregar un archivo dirigirse al menú del puerto (panel izquierdo) y haga clic en “Add new File”.

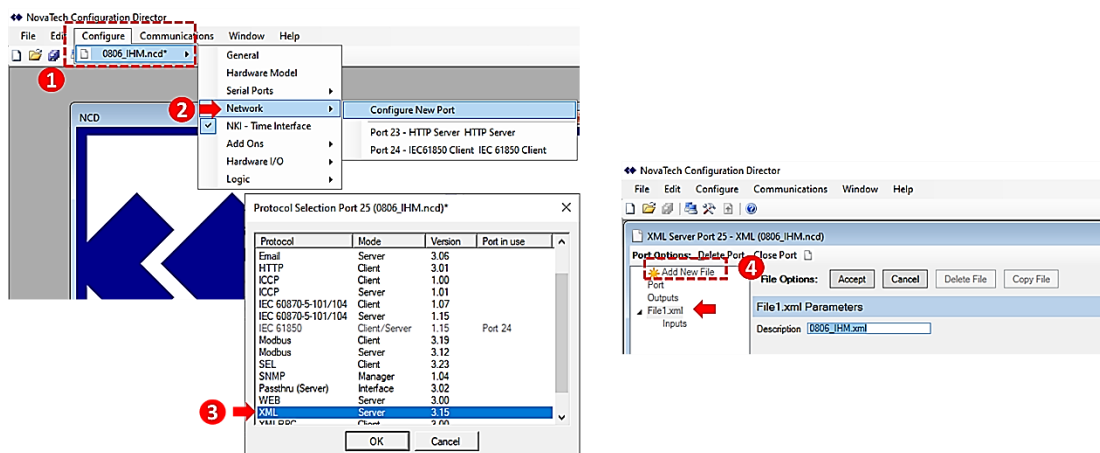


Figura 64. Pasos para configurar el protocolo XML en el NCD. Fuente: Autores.

5. Dirigirse al menú del puerto (panel izquierdo) y clic en “Inputs”.
6. En el panel de entradas seleccionar las variables necesarias para ser visualizadas en el HMI.
7. Agregar los puntos de entrada seleccionados haciendo clic en “>>”, de lo contrario, hacer clic en “<<”, tal como se muestra en la Figura 65.

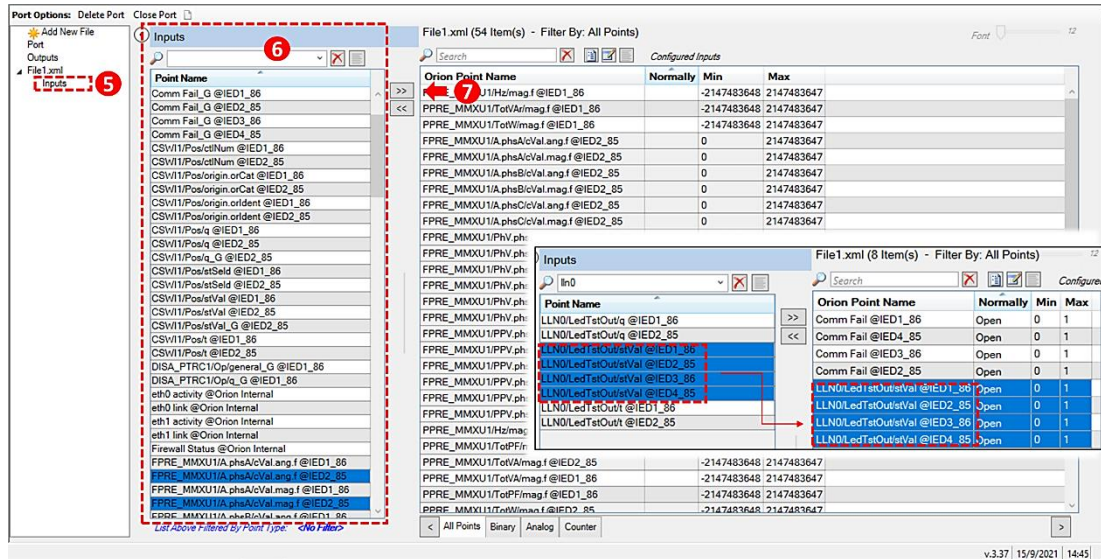


Figura 65. Selección de datos para los puntos de entrada en el puerto XML. Fuente: Autores.

De igual manera se agrega los puntos de salida, en la opción “Outputs” se selecciona las variables y finalmente se transmiten, véase la Figura 66.

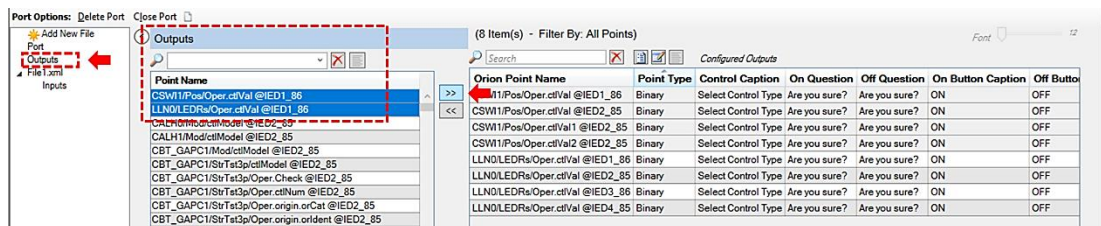


Figura 66. Selección de datos para los puntos de salida en el puerto XML. Fuente: Autores.

#### 4.3.4. Exportación de proyecto a la RTU

Para proceder con la exportación hacia la RTU, primero se debe crear una nueva conexión, la cual este en red con todos los dispositivos, para ello se han adoptado los siguientes pasos:



1. Seleccionar el menú “Communications” y clic en “Online Connections”.
2. Se abrirá una ventana “Manage Connection”, clic en “New Connection”.
3. Renombrar la conexión “VIA RED”.
4. Escribir la dirección IP de la RTU, en este caso es “192.168.1.3”, y clic en “OK”, véase la Figura 67.

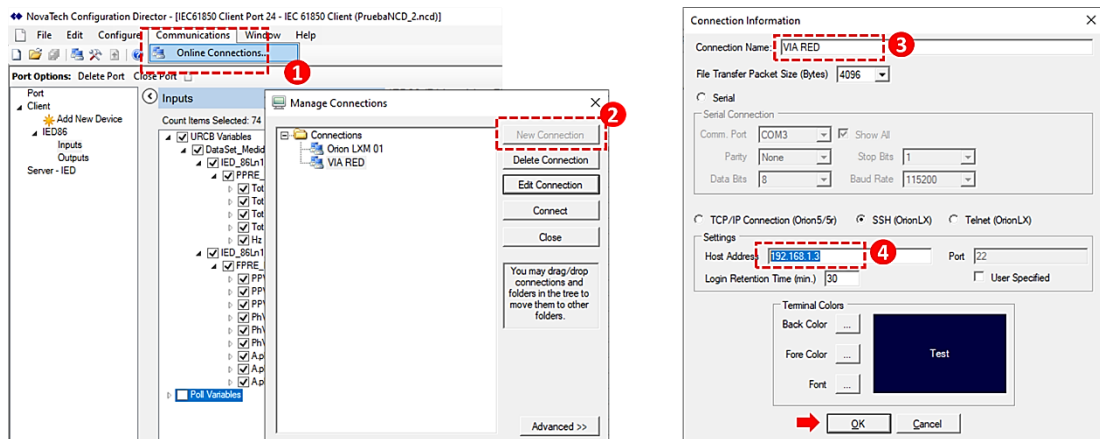


Figura 67. Ajustes para crear conexión online vía red. Fuente: Autores.

La opción de transferencia se realiza mediante la conexión SSH (Secure Shell) entre la PC y la ORION, la cual es muy habitual en un modelo cliente servidor. Los archivos necesarios tienen extensión “NCD” el cual contiene los archivos de configuración de la Orion LXM y “NCZ” contiene los archivos comprimidos de IEC 61850. A continuación, se listan los pasos para cargar los archivos a la RTU:

1. Seleccionar la conexión creada y clic en “Connect”.
2. Se abrirá la ventana de conexión online y solicitará acceso a la conexión, para iniciar sesión, digitar tanto para usuario como para contraseña la palabra “novatech”. Y clic en “OK”.
3. Inmediatamente se visualiza el menú principal en la ventana de comandos, para seleccionar alguna opción basta con digitar el número que la precede, en este caso digitar “1” para seleccionar el menú de archivos, véase la Figura 68.

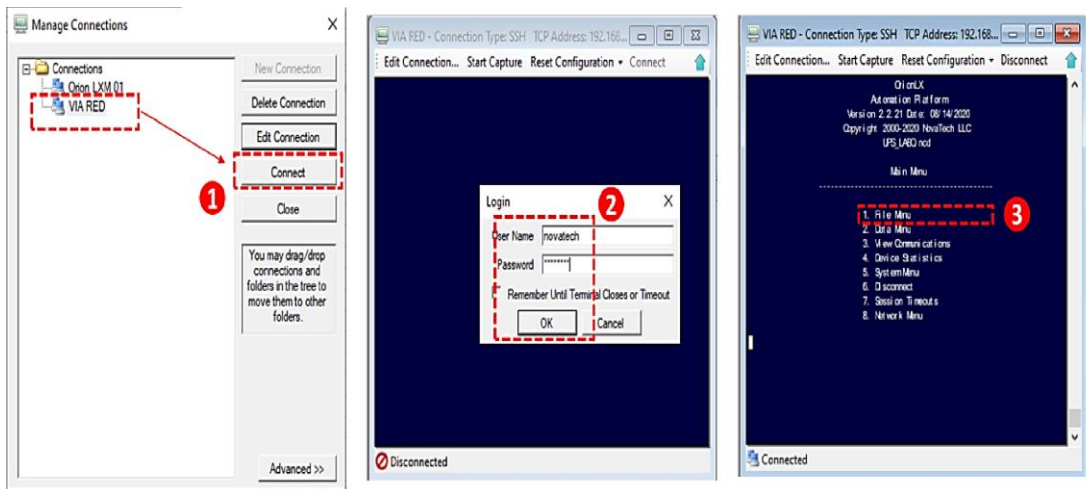


Figura 68. Pasos para realizar la comunicación SSH entre la PC y la ORION. Fuente: Autores.

4. Digitar “1” para transferir los archivos desde la PC hacia la ORION.
5. Se abrirá una ventana en la cual se debe escoger los 2 archivos generados en el proyecto, con extensión “NCD” y “NCZ”, los cuales serán transferidos a la RTU, véase la Figura 69.
6. Digitar “3” para activar el archivo de configuración correspondiente a la RTU.
7. Digitar la opción correspondiente al archivo cargado recientemente, en este caso opción “3”.
8. Digitar opción “1”, es un reinicio completo y sirve para restablecer todo el hardware y reiniciar todo el software y controladores, incluido el sistema operativo.

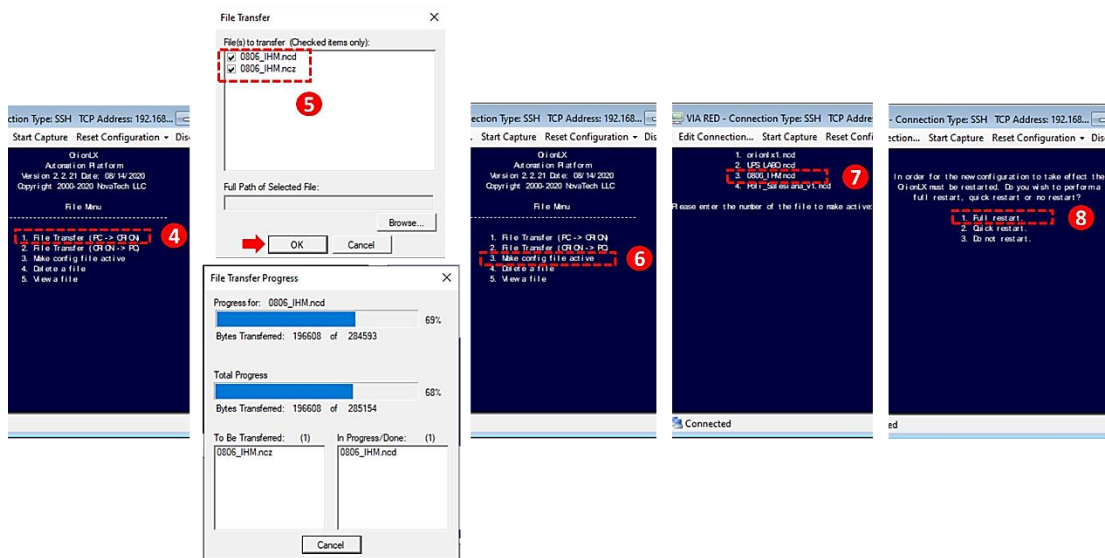


Figura 69. Pasos para transferir datos y reiniciar la ORION. Fuente: Autores.

Finalmente, una vez reiniciado el equipo, éste se encontrará listo para ser usado desde el navegador.

#### 4.3.5. Creación de HMI en Inkscape™

Esta extensión vincula NCD e Inkscape™ para facilitar la creación de archivos SVG, el cual permite configurar el archivo XML de origen para crear una interfaz amigable con el usuario. Para crear el HMI, seguir los pasos que a continuación se detallan:

1. Una vez abierto el Inkscape™ se debe empezar configurando las propiedades generales del documento, para ello dar clic en “Document Properties”, véase la Figura 70.
2. Se abrirá una ventana, en la cual se debe personalizar el tamaño del documento y las unidades de la ventana, para ello seleccionar las unidades de “px” que son los píxeles.
3. Seleccionar “Landscape” la cual permite orientar el documento de forma horizontal.
4. Seleccionar color para fondo del documento.
5. Seleccionar color para identificar los límites de la pantalla.
6. Crear la interfaz gráfica mediante la caja de herramientas.

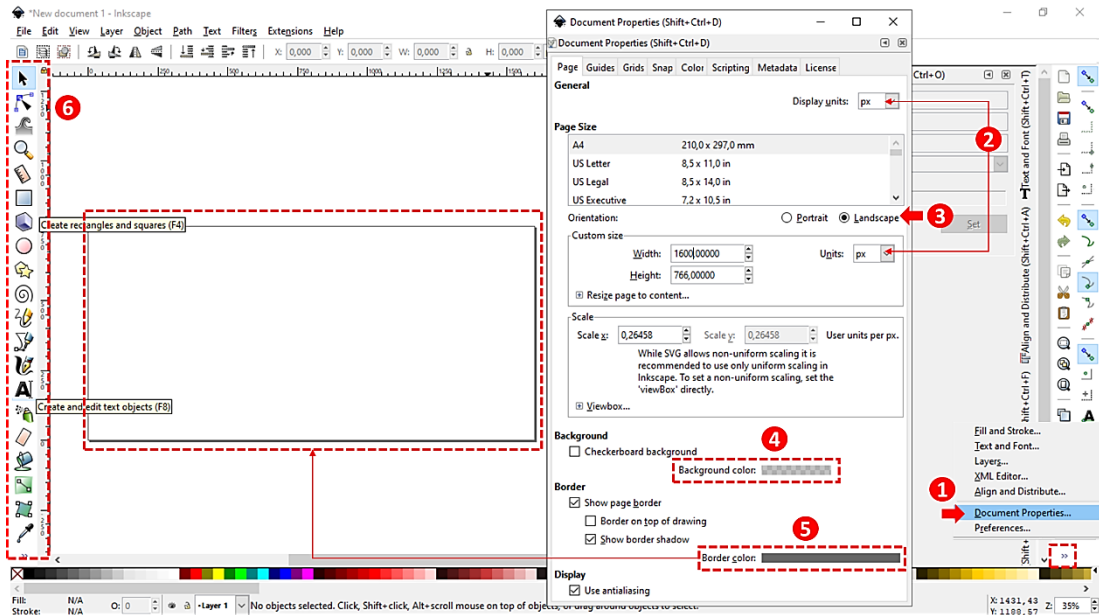


Figura 70. Ventana de trabajo del software Inkscape™. Fuente: Autores.

En la Figura 71 se observa los objetos e imágenes insertadas en el HMI, lo cual genera la interfaz gráfica intuitiva.

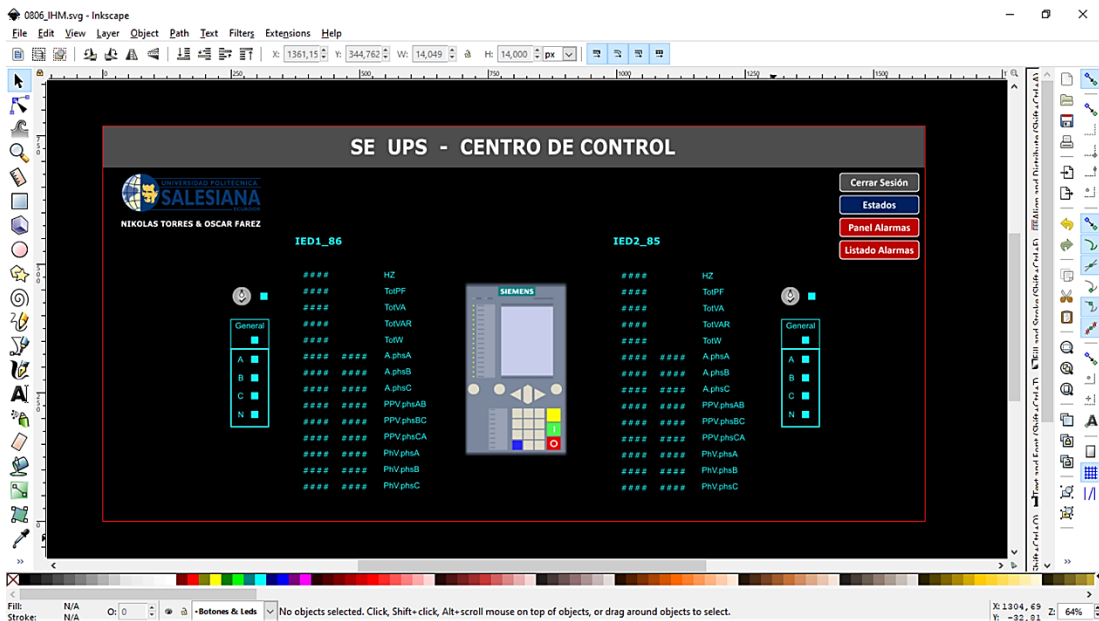


Figura 71. Vista del archivo HMI en el Inkscape™. Fuente: Autores.

Para configurar los objetos y acceder a la extensión HMI, se debe seguir los pasos que a continuación se detallan:

1. Teniendo seleccionado el objeto, en este caso el botón para resetear los leds del IED, clic en el menú “Extensions” y seleccionar “HMI”.

2. Inmediatamente se abre una ventana de configuración, en él seleccionar correctamente los archivos “NCD” y “XML”, véase la Figura 72.
3. Seleccionar el tipo de control deseado para el botón, en este caso, seleccionar “Control No Confirm”.
4. Seleccionar la variable a controlar. Y finalmente clic en “Aceptar”.

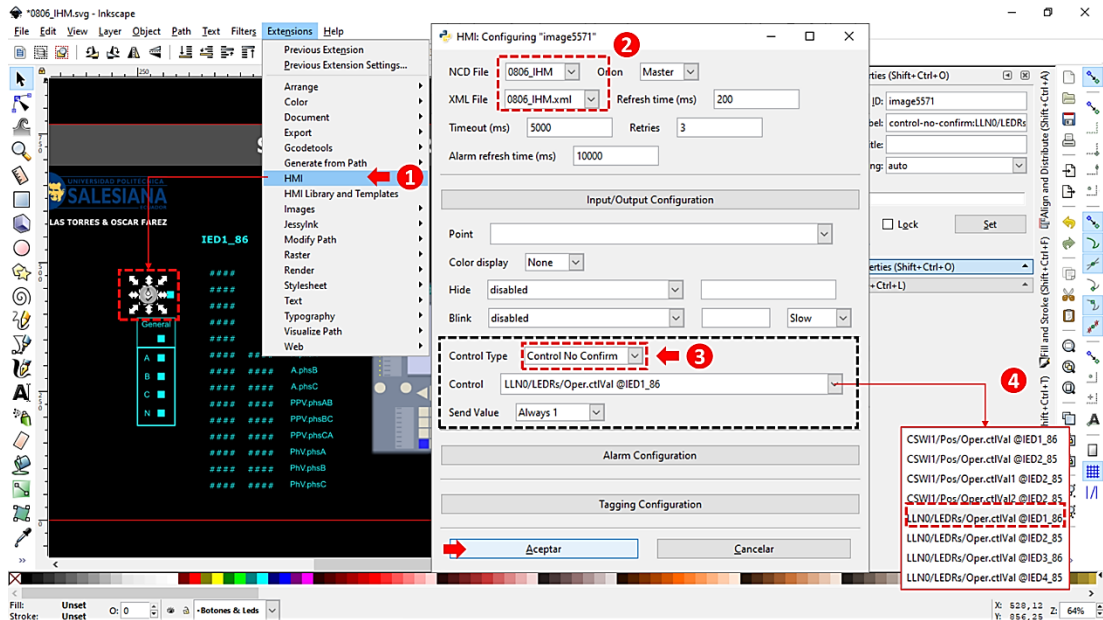


Figura 72. Ajustes realizados a los objetos “botones” en la extensión HMI. Fuente: Autores.

De igual manera se configura los objetos lumínicos, se abre la extensión HMI y se selecciona la variable correspondiente, en este caso como es un indicador lumínico se selecciona el tipo de dato para dar el color a los diferentes estados del indicador, el cual es un dato binario, clic en “Binary”, tal como se muestra en la Figura 73.

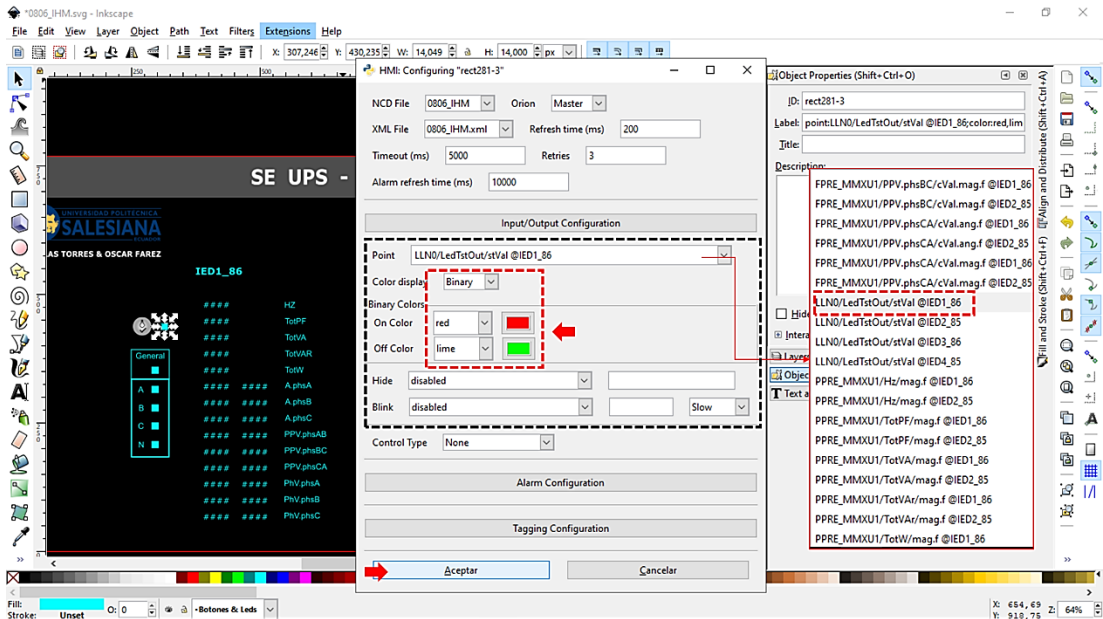


Figura 73. Ajustes realizados a los objetos “luminicos” en la extensión HMI. Fuente: Autores.

También se da el caso de crear un grupo de atributos (véase la Figura 74), es decir crear dos objetos por separado y luego agruparlos, su actuación es dependiendo el estado en que se encuentre la variable correspondiente, en este caso cuando la variable “Common Fail @IED1\_86” tenga un valor “1” se activará la etiqueta “Online” y cuando sea “0” se activara la etiqueta “Offline”, véase la Figura 75.

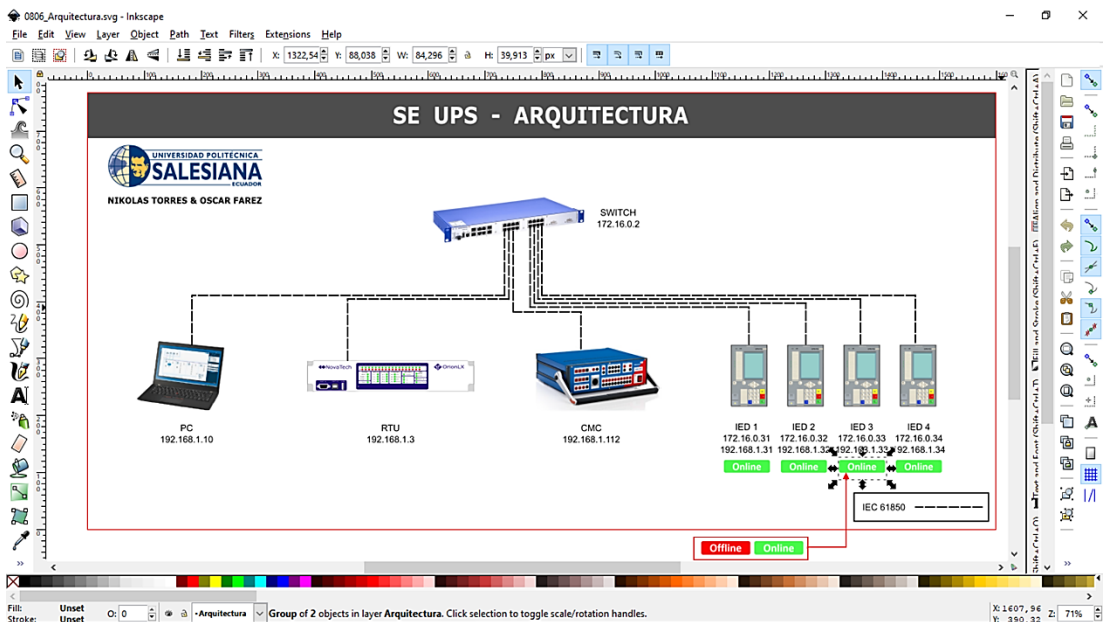


Figura 74. Vista del archivo Arquitectura en el Inkscape™. Fuente: Autores.

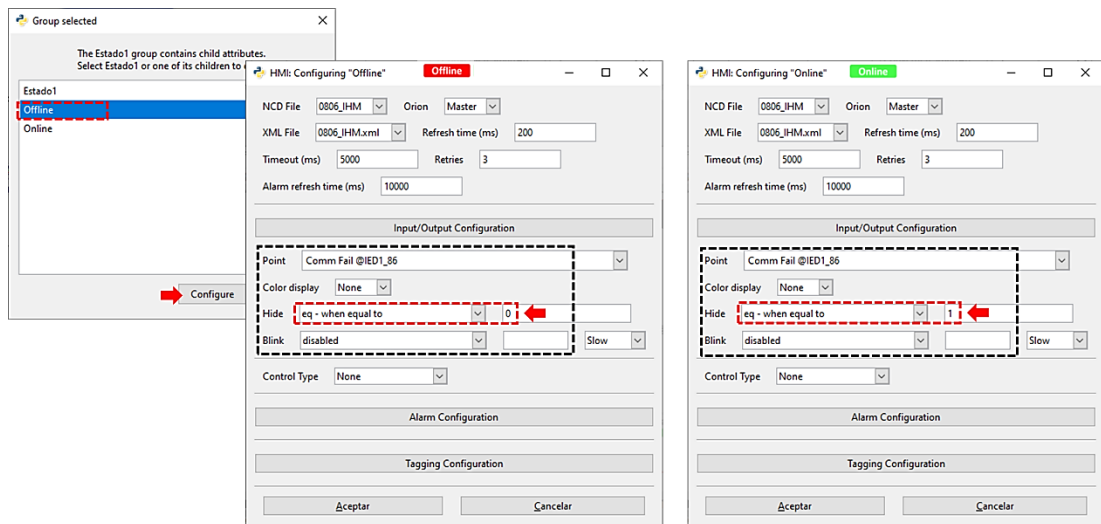


Figura 75. Ajuste realizado a la etiqueta de comunicación. Fuente: Autores.

### 4.3.6. Exportación de archivos SVG a la RTU

A continuación, se listan los pasos para transferir los archivos SVG recién creados a la RTU:

1. Acceder a la página web mediante la dirección IP “https://192.168.1.3” a través de un navegador web, véase la Figura 76.

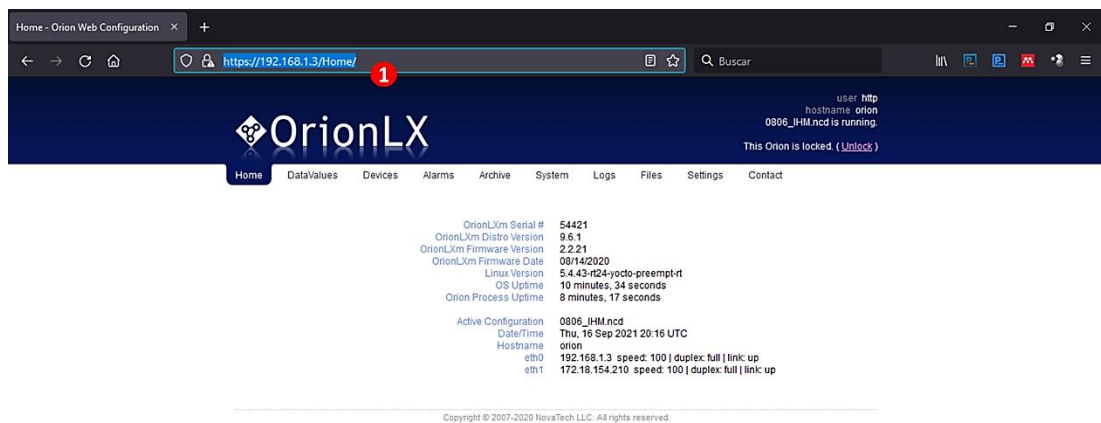


Figura 76. Ventana inicial del WEBserver. Fuente: Autores.

2. En la página de inicio de Orion, haga clic en la pestaña “Files”.
3. Arrastre todos los archivos “SVG” necesarios al navegador, véase la Figura 77.
4. Clic en “Send”.

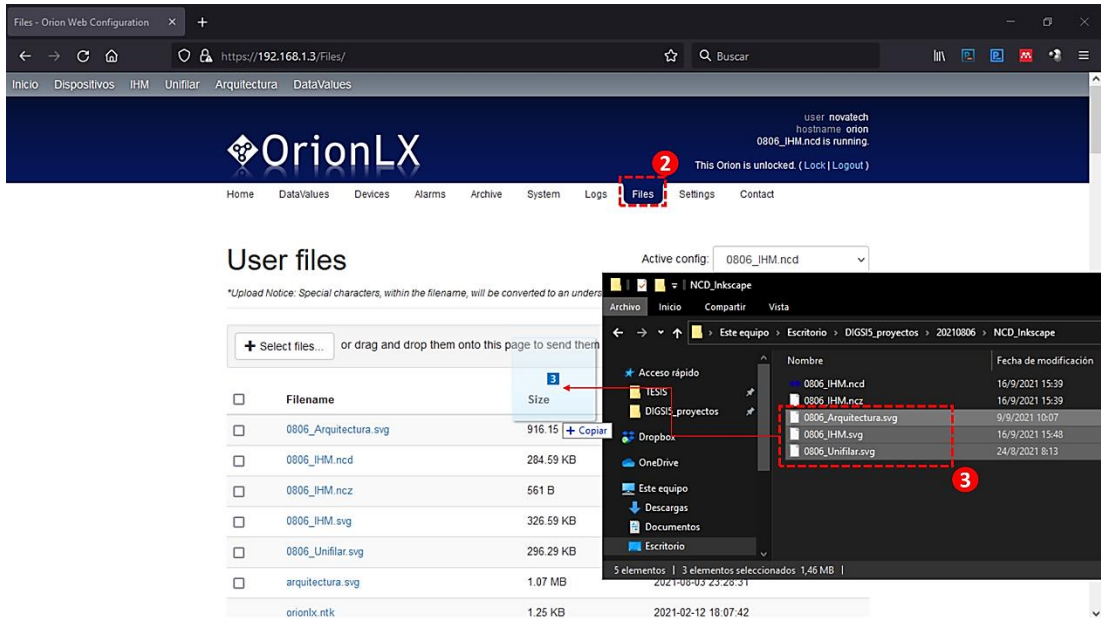


Figura 77. Pasos para exportar archivos SVG a la ORION. Fuente: Autores.

- Luego, hacer clic en la pestaña “Settings” y en la lista de opciones del “Web Page” seleccionar “WebUI”.
- Seleccione el/los archivos “NCD” para configurar el acceso directo desde la página principal, es decir, que estos archivos serán accesibles directamente desde la página de inicio de Orion, véase la Figura 78.

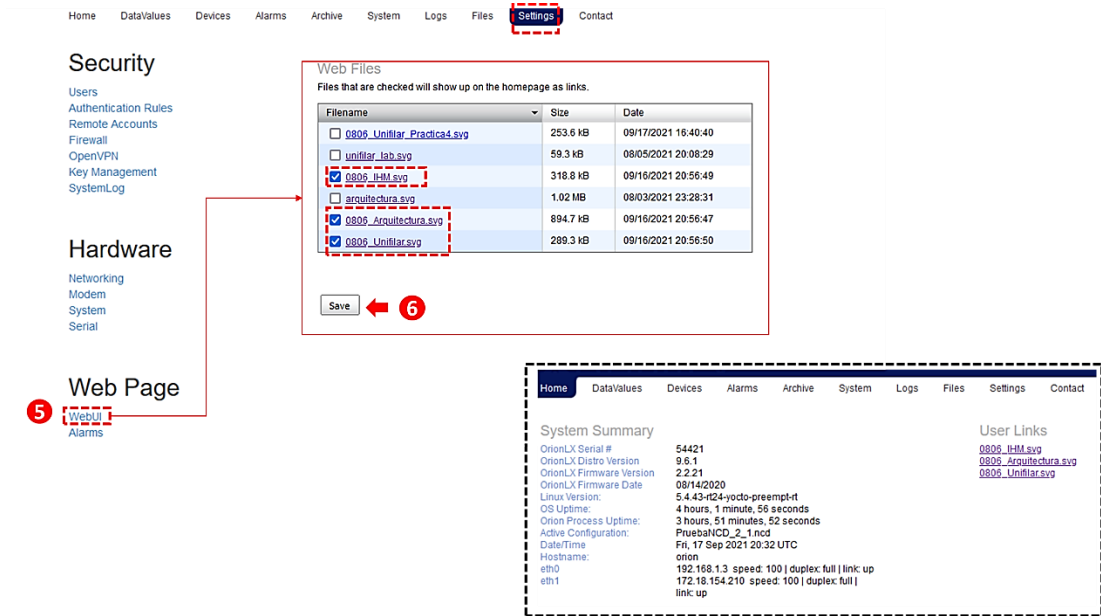


Figura 78. Pasos para configurar archivos como acceso directo en el WEBserver. Fuente: Autores.



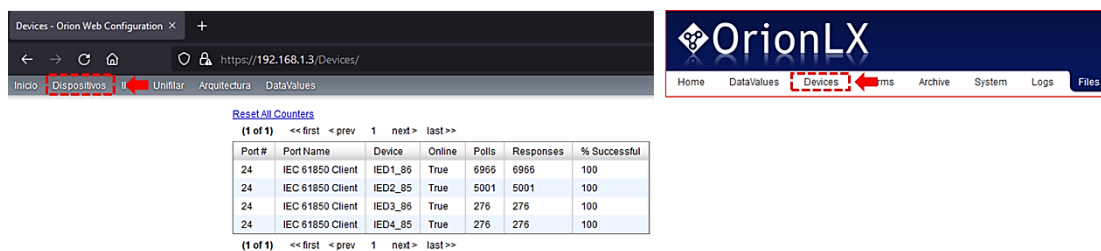
#### 4.3.7. Análisis de funcionamiento (Prueba de comunicación)

El análisis de funcionamiento permite verificar la comunicación correcta y la existencia de tráfico de paquetes de datos bajo el estándar IEC 61850. Tal análisis se realizará de dos formas: la primera es mediante la aplicación de WEBserver que permite alojar datos en tiempo real en páginas web de cualquier navegador; y la otra forma es mediante el software “Wireshark que permite capturar paquetes de datos y analizarlos.

#### Aplicación WEBserver

Se inicia accediendo al menú “Devices” (véase la Figura 79), el cual se encuentra en la cabecera de la página web principal de la ORION, en ella se muestra una tabla estadística de cada dispositivo servidor conectado a la red, esto permite verificar la conectividad y la calidad de la comunicación de cada uno de ellos.

En la columna “Online” se visualiza el estado de la comunicación, si el estado es “True” indica que el equipo si está conectado a la red, caso contrario el estado será “False”. En las columnas “Polls” y “Responses” se visualiza la cantidad de paquetes de datos tanto enviados como recibidos los cuales deben ser iguales en ambas columnas para una correcta comunicación y tal factor porcentual de éxito se visualiza en la columna “Successful”.



The screenshot shows the OrionLX web interface. The top navigation bar includes 'Home', 'DataValues', 'Devices', 'ms', 'Archive', 'System', 'Logs', and 'Files'. The 'Devices' menu is highlighted. Below the navigation bar, there is a table with the following data:

Port#	PortName	Device	Online	Polls	Responses	% Successful
24	IEC 61850 Client	IED1_85	True	6966	6966	100
24	IEC 61850 Client	IED2_85	True	5001	5001	100
24	IEC 61850 Client	IED3_85	True	276	276	100
24	IEC 61850 Client	IED4_85	True	276	276	100

Figura 79. Ventana Device del WEBserver. Fuente: Autores.

También, se accede al menú “Datavalues” (véase la Figura 80) el cual se encuentra en la cabecera de la página web principal de la ORION. La página Datavalues permite ver y forzar en tiempo real el valor de cada punto de entrada/salida y la información de los puntos en cada puerto.

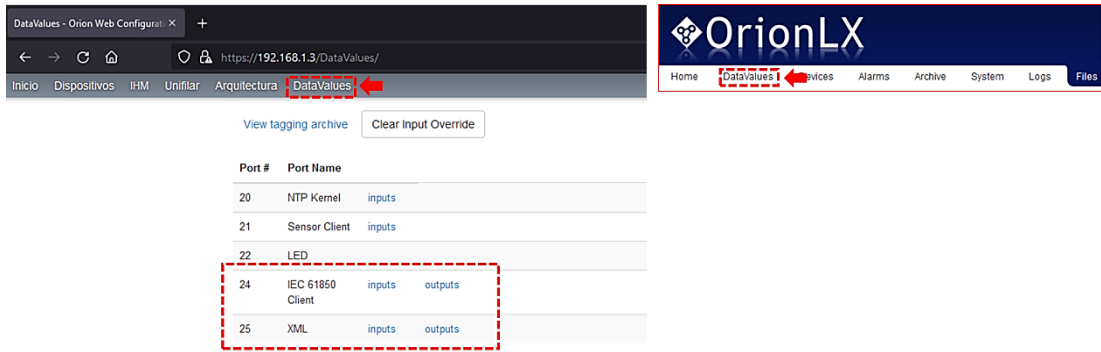


Figura 80. Ventana Datavalues del WEBserver. Fuente: Autores.

Previamente configurados los puertos “24 – IEC 61850 Client” y “25 – XML”, acceder al puerto 25 en el apartado “Inputs” y observar las variables o nodos lógicos configurados para el HMI (véase la Figura 81), si alguna fila se resalta en rojo indica que el punto está fuera de línea, e indica la existencia de algún error.

Point Name	Device	Type	Point Number	Value	Percent FS	Status	Forced
Comm Fail @IED1_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
Comm Fail @IED4_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
Comm Fail @IED3_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
Comm Fail @IED2_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
LLN0/LedTstOut/stVal @IED1_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
LLN0/LedTstOut/stVal @IED2_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
LLN0/LedTstOut/stVal @IED3_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
LLN0/LedTstOut/stVal @IED4_86	File1.xml	N/A	N/A	0.000000	0.000000	Online	No
FPRE_MMXU1/A.phsA/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	-0.289322	-0.000000	Online	No
FPRE_MMXU1/A.phsA/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	16.028709	0.000001	Online	No
FPRE_MMXU1/A.phsB/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	-120.092163	-0.000006	Online	No
FPRE_MMXU1/A.phsB/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	15.917196	0.000001	Online	No
FPRE_MMXU1/A.phsC/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	120.073303	0.000006	Online	No
FPRE_MMXU1/A.phsC/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	15.993863	0.000001	Online	No
FPRE_MMXU1/PhV.phsA/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	0.000000	50.000000	Online	No
FPRE_MMXU1/PhV.phsA/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	5.996160	0.000000	Online	No
FPRE_MMXU1/PhV.phsB/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	-119.998779	49.999997	Online	No
FPRE_MMXU1/PhV.phsB/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	5.995988	0.000000	Online	No
FPRE_MMXU1/PhV.phsC/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	120.035553	50.000003	Online	No
FPRE_MMXU1/PhV.phsC/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	5.997133	0.000000	Online	No
FPRE_MMXU1/PPV.phsAB/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	29.998474	0.000001	Online	No
FPRE_MMXU1/PPV.phsAB/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	10.385527	0.000000	Online	No
FPRE_MMXU1/PPV.phsBC/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	-89.980507	-0.000004	Online	No
FPRE_MMXU1/PPV.phsBC/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	10.384251	0.000000	Online	No
FPRE_MMXU1/PPV.phsCA/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	150.015076	0.000007	Online	No
FPRE_MMXU1/PPV.phsCA/cVal.mag.f @IED1_86	File1.xml	N/A	N/A	10.388160	0.000000	Online	No

Figura 81. Variables del HMI vistas del WEBserver. Fuente: Autores.

A continuación, se visualiza la página web del archivo “SVG” correspondiente al “HMI” el cual fue creado previamente en el Inkscape™. En el HMI (véase la Figura 82) se observa la toma de magnitudes eléctricas en tiempo real, tales valores son inyectados desde la maleta de prueba “CMC 356” tal como se muestra en la Figura 83.



Figura 82. Vista del archivo HMI en el WEBserver. Fuente: Autores.

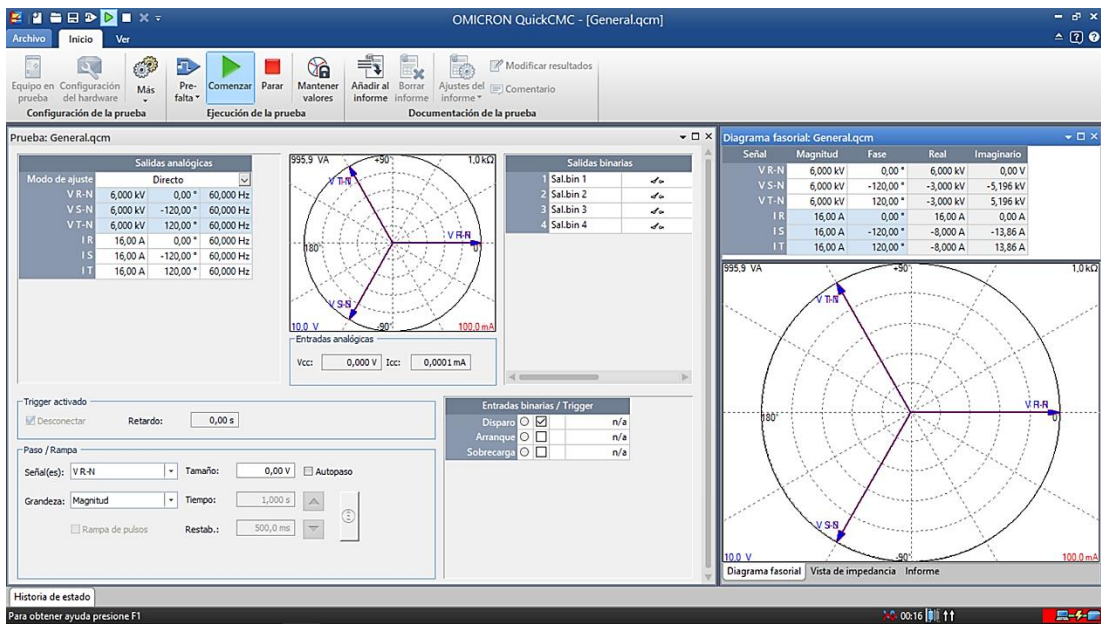


Figura 83. Inyección de tensiones y corrientes desde la CMC 356. Fuente: Autores.

En la página web llamada “Arquitectura” (véase la Figura 84) se visualiza el resultado proveniente de la prueba de desconectar y conectar el cable de red del dispositivo “IED 2”, lo que resulta el cambio de etiqueta de un estado “Online – color verde” a un estado “Offline – color rojo” y viceversa.

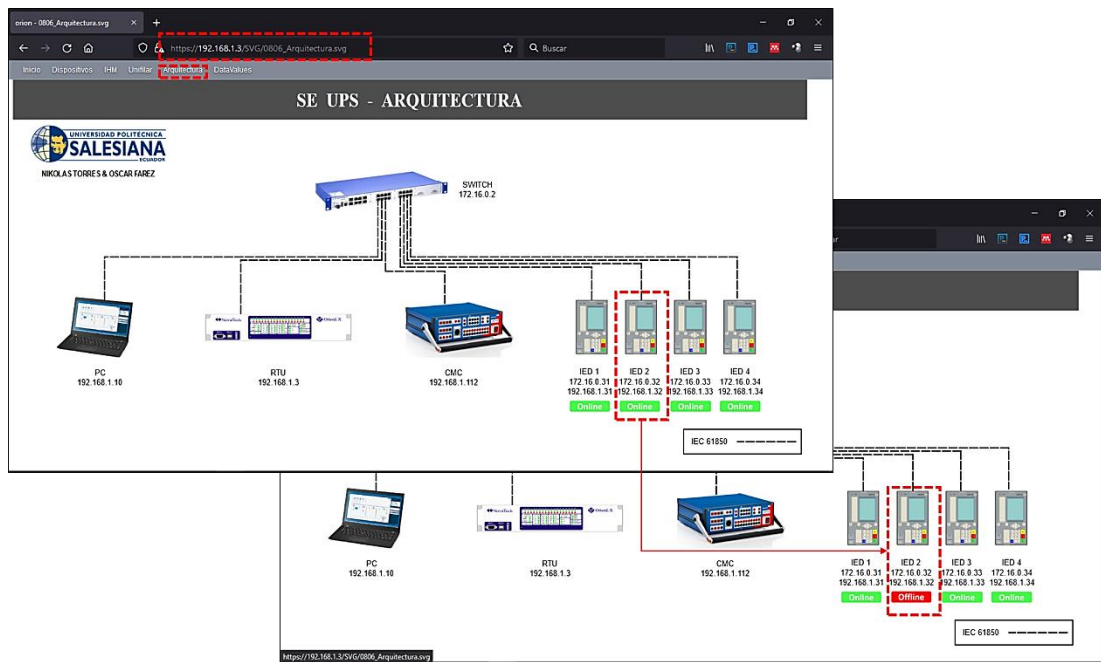


Figura 84. Vista del archivo Arquitectura en el WEBserver. Fuente: Autores.

## Software “Wireshark”

En su página principal se observa los adaptadores de red con el tráfico real (véase la Figura 85), se procede a seleccionar el adaptador de Ethernet al cual está conectado físicamente la red.

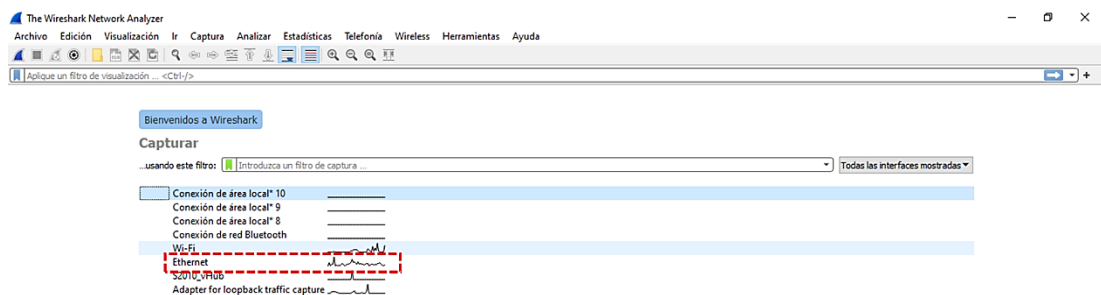


Figura 85. Ventana Wireshark. Fuente: Autores.

Posteriormente se inicia la captura del tráfico de red, para este caso se filtra los paquetes de datos en función de la mensajería “GOOSE” (véase la Figura 86), y se observa que los paquetes proviene de dos direcciones MAC, lo cual se puede corroborar en la ventana de detalles, específicamente en el ítem correspondiente a la

capa de “Enlace de datos”, y las direcciones fuente son de los IED1\_86 y IED2\_85 los cuales tienen ajustada la mensajería GOOSE.

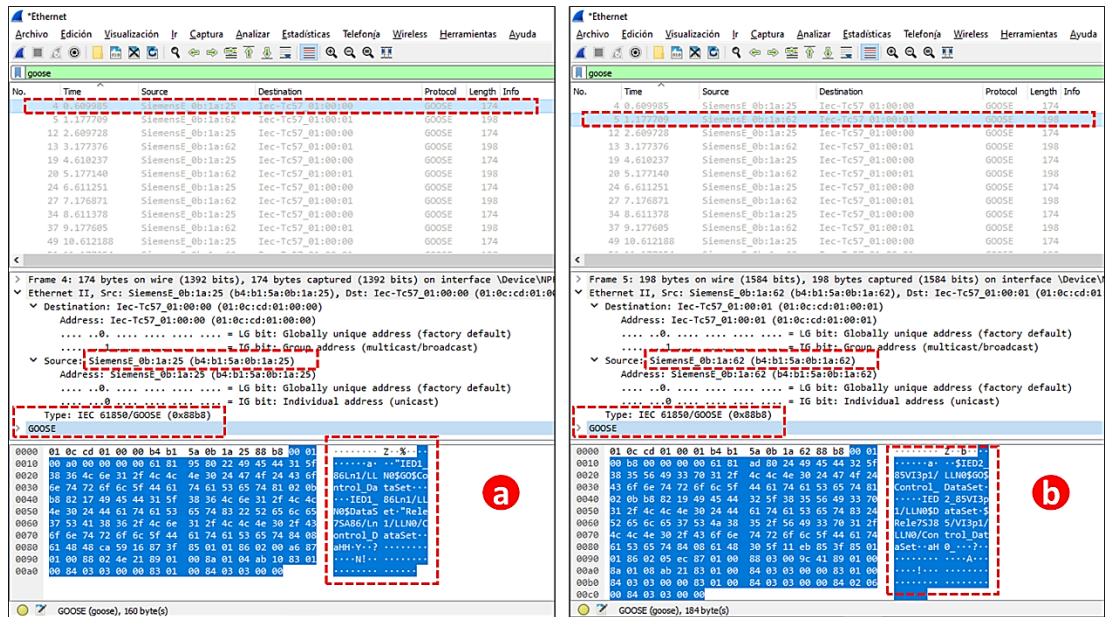


Figura 86. Trafico de paquete de datos GOOSE entre IED’s. Fuente: Autores.

Posteriormente se realizó la actuación de la protección del IED1\_86, la cual se puede observar de como los paquetes pasaron de transmitirse cada 2seg a transmitirse muchos en un segundo en el momento de la falla y provenientes solo del dispositivo actuado, véase la Figura 87.

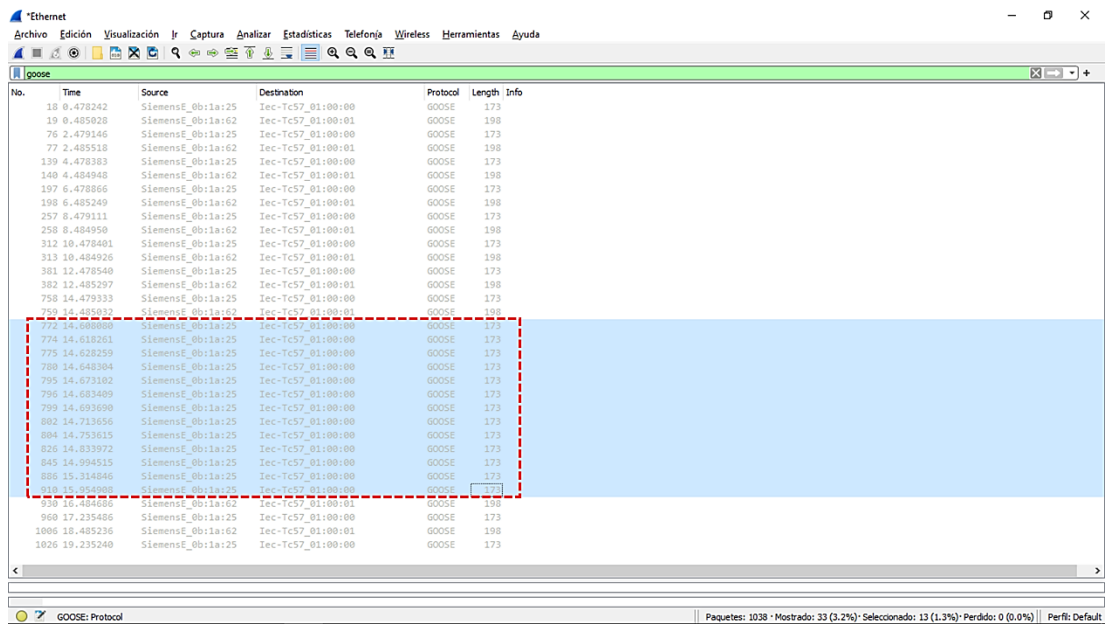


Figura 87. Trafico de la mensajería GOOSE ante una falla. Fuente: Autores.

A continuación, se visualiza el resultado proveniente de la prueba de desconectar y conectar el cable de red de los dispositivos “IED4\_85 y IED3\_86” respectivamente (véase la Figura 88), mediante un filtrado en función de sus direcciones IP (192.168.1.34 y 192.168.1.33), por lo que la dirección fuente del mensaje corresponde a la RTU la cual está tratando de localizar a los dispositivos desconectados.

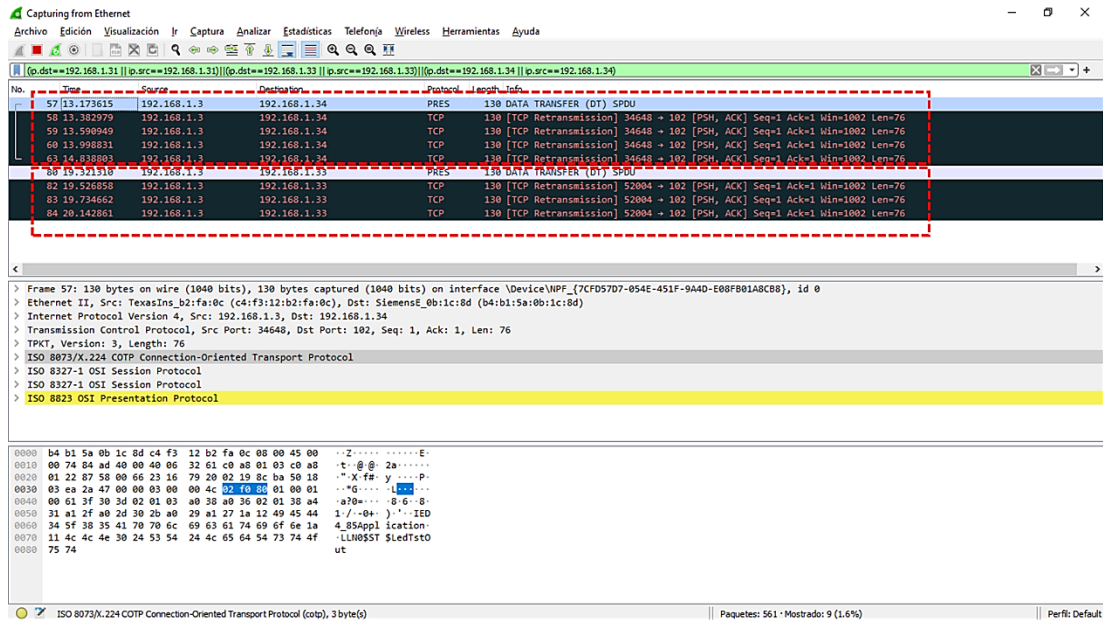


Figura 88. Trafico de la mensajería frente a la desconexión del IED de la red. Fuente: Autores.

### 4.3.8. Creación de alarmas y archivos

El módulo de Alarma /Archivo/Retención (AAR - Alarm/Archive/Retentive Module) se puede solicitar para que Orion maneje alarmas, archive y retenga valores de puntos. Una vez configurado este complemento, en la página web “Datavalues” se creará un nuevo puerto “Port # 26” con el módulo AAR, el cual permite la visualización de los datos históricos para un análisis de secuencia de eventos, además del reconocimiento e historial de las alarmas.

#### Configuración del módulo AAR

Para incorporar este complemento se debe dirigir al menú “Configure” y seleccionar el proyecto actual, en el submenú seleccionar “Add Ons” y clic en “Alarm/Archive/Retentive”, inmediatamente se abrirá la ventana correspondiente al módulo AAR, tal como se muestra en la Figura 89.

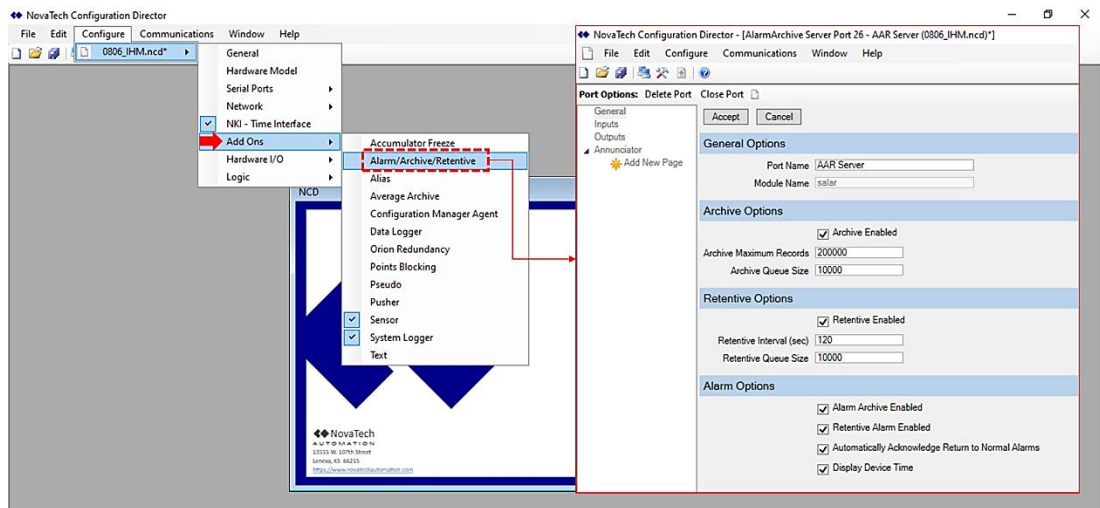


Figura 89. Pasos para configurar el complemento AAR. Fuente: Autores.

A continuación, se selecciona las variables o nodos lógicos para la configuración de las alarmas y archivos (véase la Figura 90), para ello se listan los pasos a seguir:

1. Clic en “Inputs”.
2. Seleccionar las variables necesarias para el módulo AAR.
3. Agregar las variables seleccionadas haciendo clic en “>>”, de lo contrario, hacer clic en “<<”.
4. Marque las casillas de verificación de cada variable en función de su necesidad. En la columna “Initial Value” corresponde al valor inicial para determinar el estado normal del parámetro, en este caso será en función de algún evento. La columna “Alarm Enable” habilita la alarma para ese parámetro. La columna “Binary Alarm” es marcada para determinar que es una alarma binaria, caso contrario será tomada como una alarma analógica. La columna “Retentive Enable” permite activar el historial de eventos frente a una ausencia de energía.

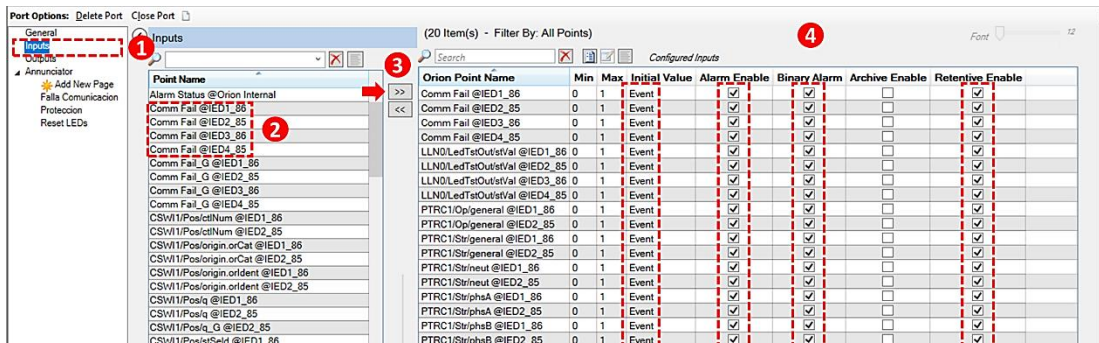


Figura 90. Pasos para seleccionar las variables necesarias en el módulo AAR.  
Fuente: Autores.

5. En el árbol de menú (panel izquierdo) seleccionar “Annunciator” y clic en “Add New Page” para añadir una nueva página de alarmas, la cual puede ser renombrada en la descripción.
6. Seleccionar los nodos lógicos correspondientes a esa página de alarmas y transferirlos haciendo clic en “>>” al mosaico de alarmas.
7. Se puede ordenar las alarmas mediante arrastrar/soltar las casillas, además de modificar el tamaño de la tabla o mosaico y opción a renombrar las alarmas. Véase la Figura 91.

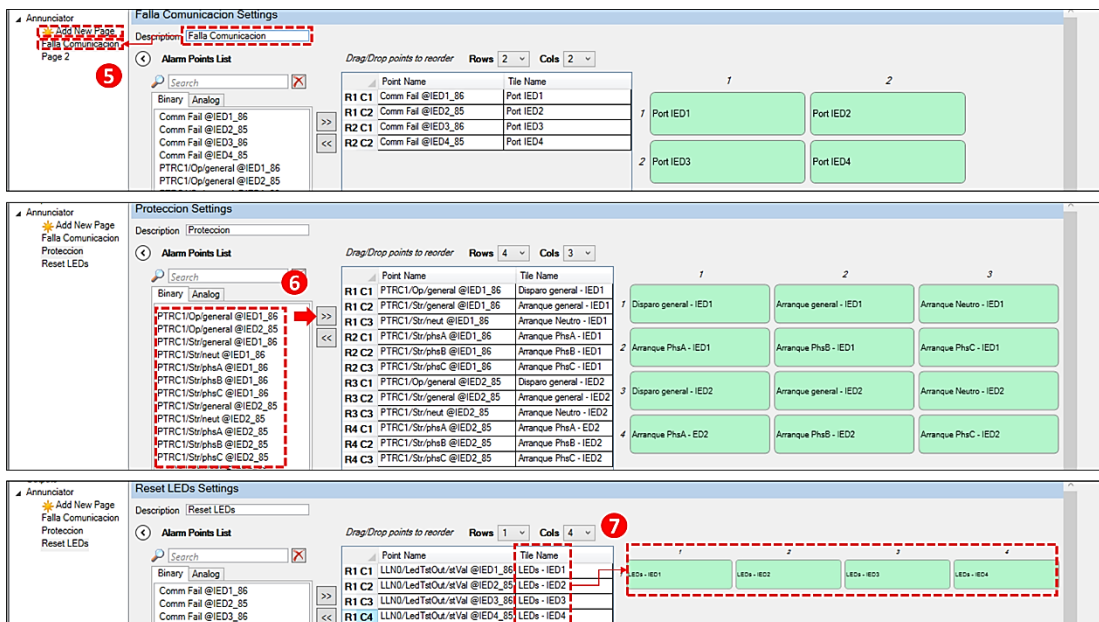


Figura 91. Pasos para añadir páginas de alarmas en el Annunciator. Fuente: Autores.



Posteriormente guardar los cambios en el archivo “NCD”, y transferir a la RTU. Este procedimiento actualizará la página web del ORION con los ajustes realizados.

### Interfaz del módulo AAR en la WEBserver

En la página web “https://192.168.1.3/AlarmSettings/” (véase la Figura 92) se configura las notificaciones ante la existencia de alarmas, entre ellas se tiene: el casillero para mostrar el banner de advertencia, el casillero para mostrar la alarma más reciente en el banner, y el casillero para activar el sonido ante la presencia de alarmas. Luego guardar los cambios.

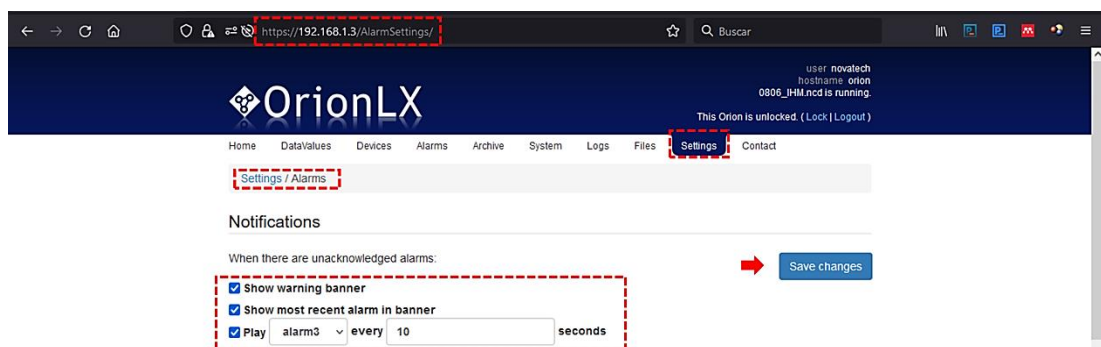


Figura 92. Ajustes realizados para las notificaciones de las Alarmas. Fuente: Autores.

A continuación, se visualiza la página de alarmas, las cuales fueron configuradas en el módulo AAR, para ello se dirige a la página web https://192.168.1.3/Annunciator/, tal como se muestra en la Figura 93.

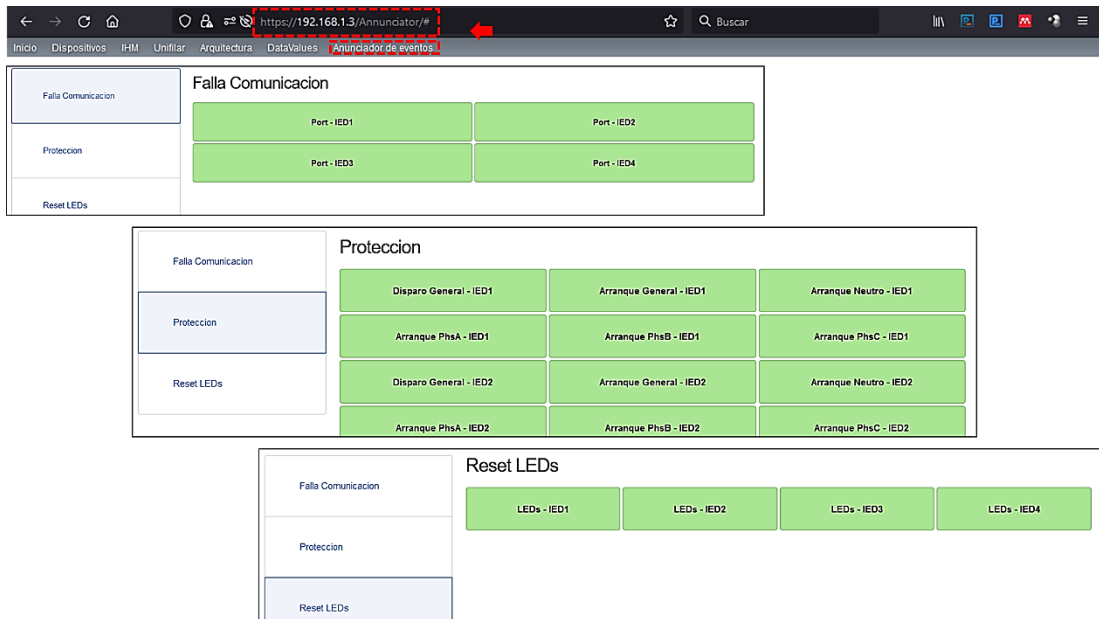


Figura 93. Ventana Anunciador del WEBserver. Fuente: Autores.

Adicionalmente en la Figura 94 se visualiza el resultado proveniente de la prueba de desconectar y conectar el cable de red del dispositivo “IED 1”, lo que resulta la activación de la alarma correspondiente a la falla de comunicación del “Port – IED1”. Se puede observar como las etiquetas cambian a un color rojo y se activa el banner de advertencia notificando la presencia de una alarma.

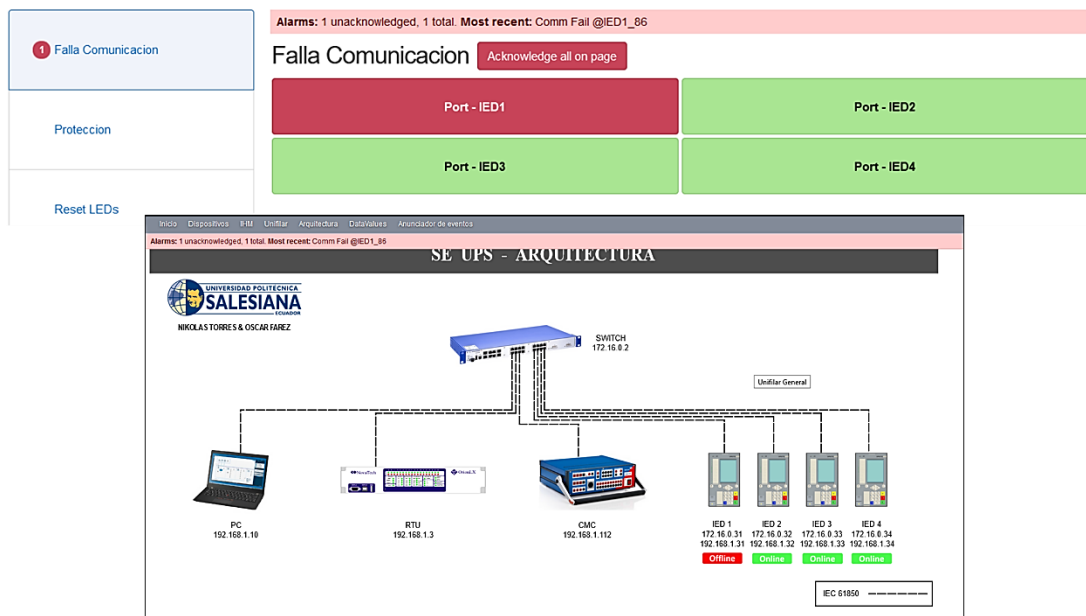


Figura 94. Notificación de la alarma por falta de comunicación con el IED1. Fuente: Autores.

También en la página <https://192.168.1.3/Alarms/>, se visualiza los reportes de alarmas generadas y el historial de eventos, véase la Figura 95.

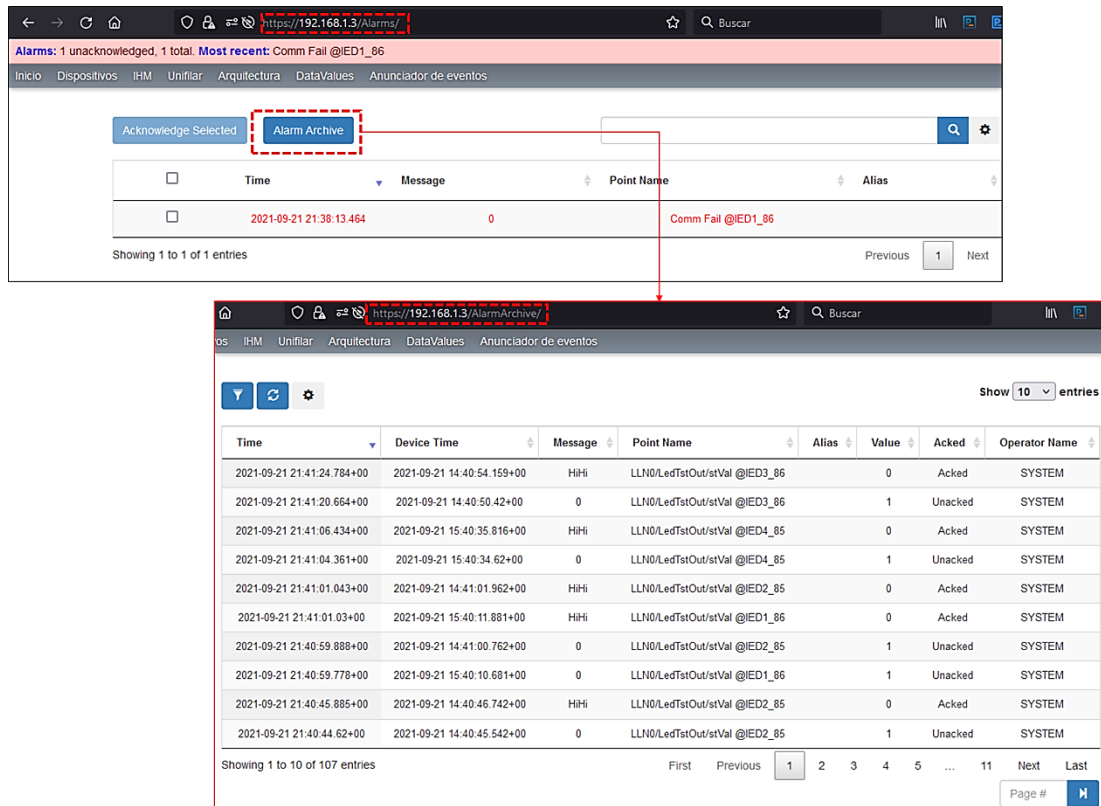


Figura 95. Registro de la alarma por falta de comunicación con el IED1. Fuente: Autores.

Asimismo se realizaron pruebas para corroborar la funcionalidad de las alarmas, tales pruebas corresponde a: generar una alerta al momento de resetear los leds físicamente del panel principal del IED2, y generar alertas ante la presencia del disparo y arranque de las protecciones. Véase la Figura 96.

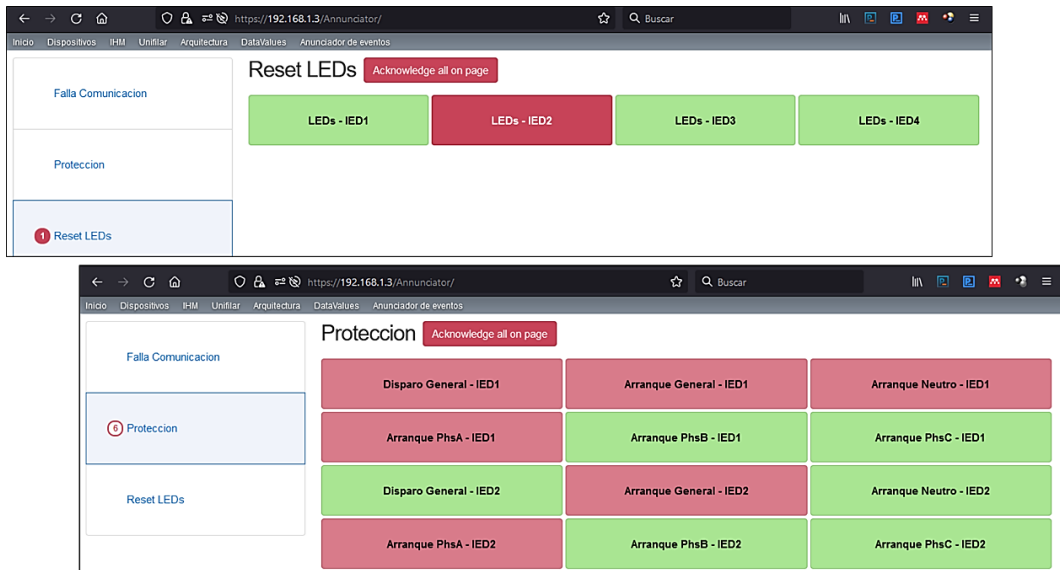


Figura 96. Vista de las notificaciones de alarmas en el Annunciator. Fuente: Autores.

#### 4.4. Guía de pruebas

##### 4.4.1. Prueba #1 – Creación de red LAN IEC 61850

###### 4.4.1.1. Objetivos

- Implementar la red LAN entre los diversos equipos.
- Identificar los cables y puertos para usar en la red.
- Verificar el estado de la conexión entre el PC y los demás equipos, mediante la utilidad del PING.

###### 4.4.1.2. Recursos

- Switch industrial GREYHOUND
- RTU Orion LXM
- IED
- Maleta de pruebas CMC 356
- PC
- Cables de red

###### 4.4.1.3. Descripción y funcionamiento

Para poder crear una red LAN, donde se encuentren comunicados todos los equipos, es importante primero definir el tipo de topología de red, en este caso se utiliza la topología de red tipo estrella simple, tal como se muestra en la Figura 97.

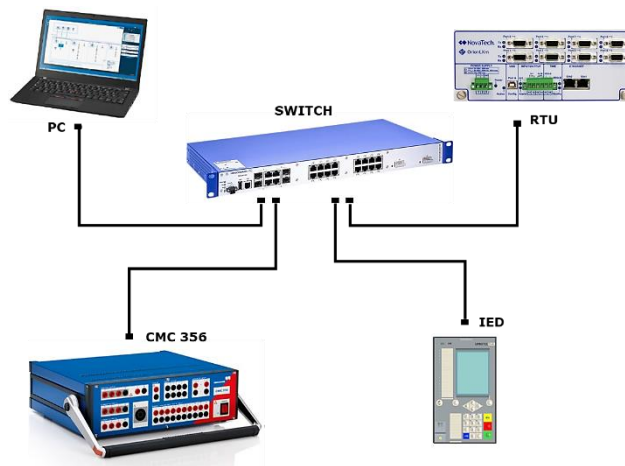


Figura 97. Topología de red para Prueba #1. Fuente: Autores.

Además, es necesario definir el tipo de clase de direccionamiento IP a utilizar, en este caso se utiliza la CLASE C, la cual tiene un rango inicial 192.0.0.0 a un rango final 223.255.255.255 y una máscara de subred 255.255.255.0. Asimismo, el switch

industrial administrable permite realizar un subneteo de la red LAN, esto proporciona mayor orden y seguridad al segmento de red física

A continuación, se mostrará el direccionamiento para la configuración de red de cada uno de los equipos a utilizar, ver Tabla 7.

Tabla 7: Direccionamiento IP de los equipos para Prueba 1.

Dispositivo		Dirección IP	Mascara de Subred
SWITCH		192.168.1.1	255.255.255.0
RTU		192.168.1.3	
PC		192.168.1.10	
CMC 356		192.168.1.112	
IED 1: 7SA86	Puerto E	192.168.1.31	

#### 4.4.1.4. Desarrollo

##### Configurar parámetro de comunicación en SWITCH

Para ello, se listan los pasos a seguir:

- a. En primer lugar, energizar el switch y conectar a la PC mediante el cable USB. Después, abrir el software “HiDiscovery”.
- b. Luego, seleccionar la tarjeta de red correcta.
- c. Volver a escanear la red “Rescan”, esto permitirá encontrar los dispositivos Hirschmann<sup>®</sup> conectados al PC, véase la Figura 98.
- d. Dar doble clic en el dispositivo encontrado, y ajustar los parámetros de red según sean nuestros requerimientos.

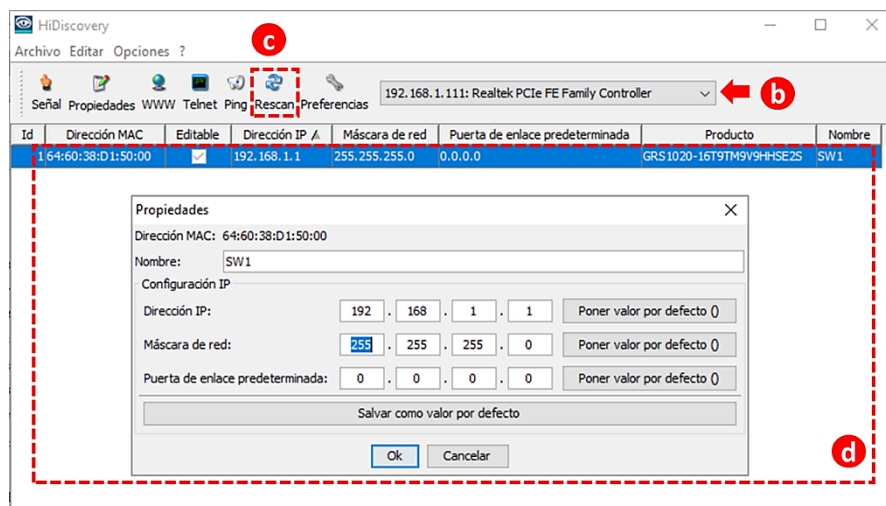


Figura 98. Ajustes de direccionamiento IP del switch en Prueba #1. Fuente: Autores.

### Configurar parámetro de comunicación en RTU

Para ello se deben seguir los pasos que a continuación se detallan:

- a. En primer lugar, energizar la RTU y conectar a la PC mediante el cable USB, después, abrir el software NCD.
- b. Crear una nueva conexión “Orion LXM 01” de tipo serial, la cual permitirá abrir una consola serial, cabe mencionar que se debe escoger el puerto COM correcto, véase la Figura 99.
- c. Abrir la conexión “Orion LXM 01”. Para iniciar sesión, digitar la palabra “novatech”, tanto para usuario como para contraseña.
- d. En el menú principal seleccionar la opción “8. Network Menu”, luego seleccionar el puerto deseado, en este caso la opción “1. Edit Eth0 (eth0)”. Posteriormente, se configura los parámetros de dirección IP, máscara de red y puerta de enlace en el caso de ser necesario. Finalmente seleccionar la opción “4. Save Settings” para guardar los cambios, véase la Figura 100.

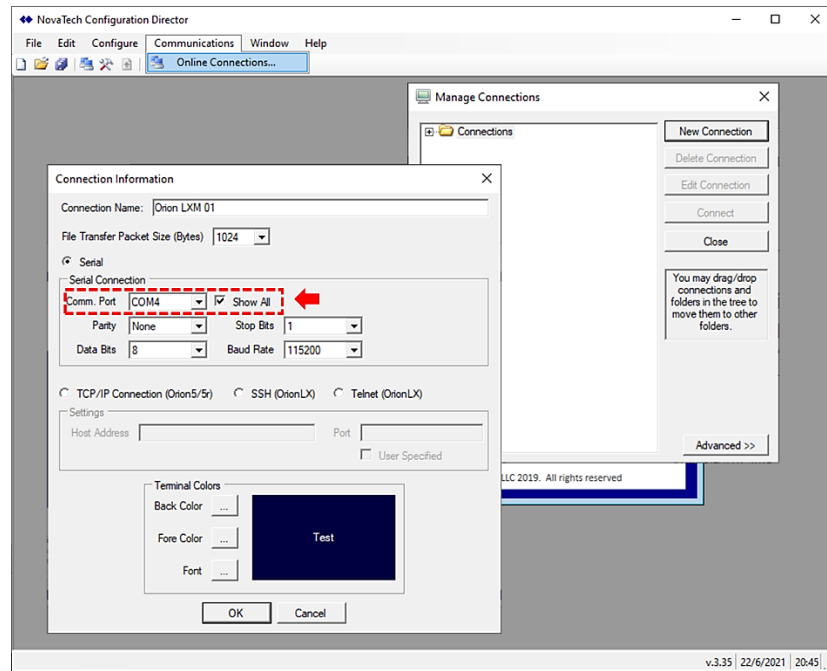


Figura 99. Creación de conexión serial en la RTU para Prueba #1. Fuente: Autores.

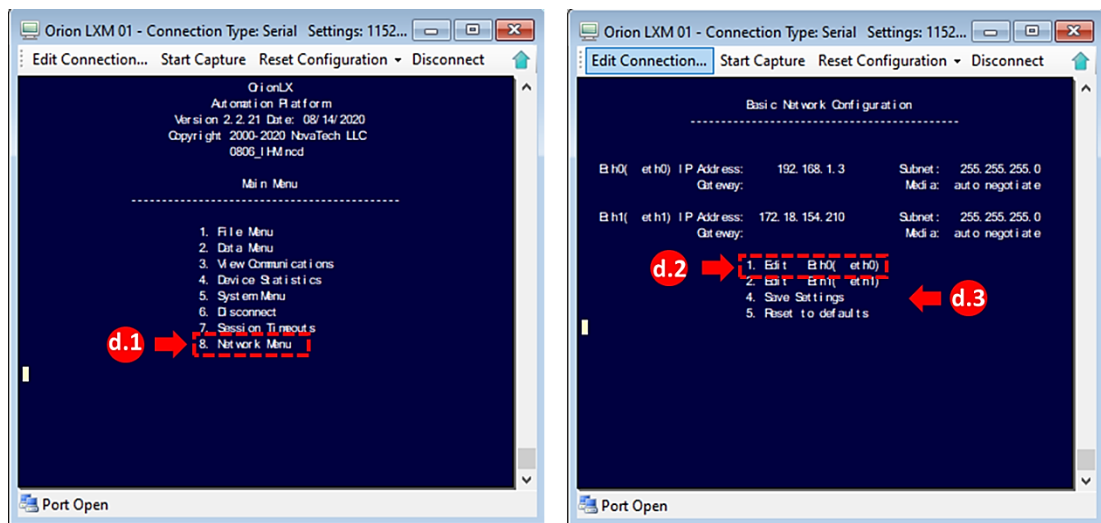


Figura 100. Ajustes de direccionamiento IP de la RTU para Prueba #1. Fuente: Autores.

### Configurar parámetro de comunicación en IED

Pasos para configurar el direccionamiento IP desde el software DIGSI® 5, véase la Figura 101.

- a. En primer lugar, encender el IED y conectar a la PC mediante el cable USB, luego, abrir el software “DIGSI® 5”.



- b. Después, añadir un nuevo equipo, ya sea en un proyecto nuevo o en uno existente. Inmediatamente, abrir el equipo y seleccionar “Hardware y protocolos”.
- c. Luego, dar doble clic izquierdo sobre el puerto de comunicación “F”; lo cual permitirá abrir una ventana de propiedades, dentro de la cual se puede configurar el direccionamiento de red.
- d. Una vez configurado el puerto de comunicación, clic derecho sobre el equipo, y seleccionar “Cargar la configuración al equipo”.
- e. Finalmente, introducir el código de confirmación (222222) para cargar la configuración al equipo.

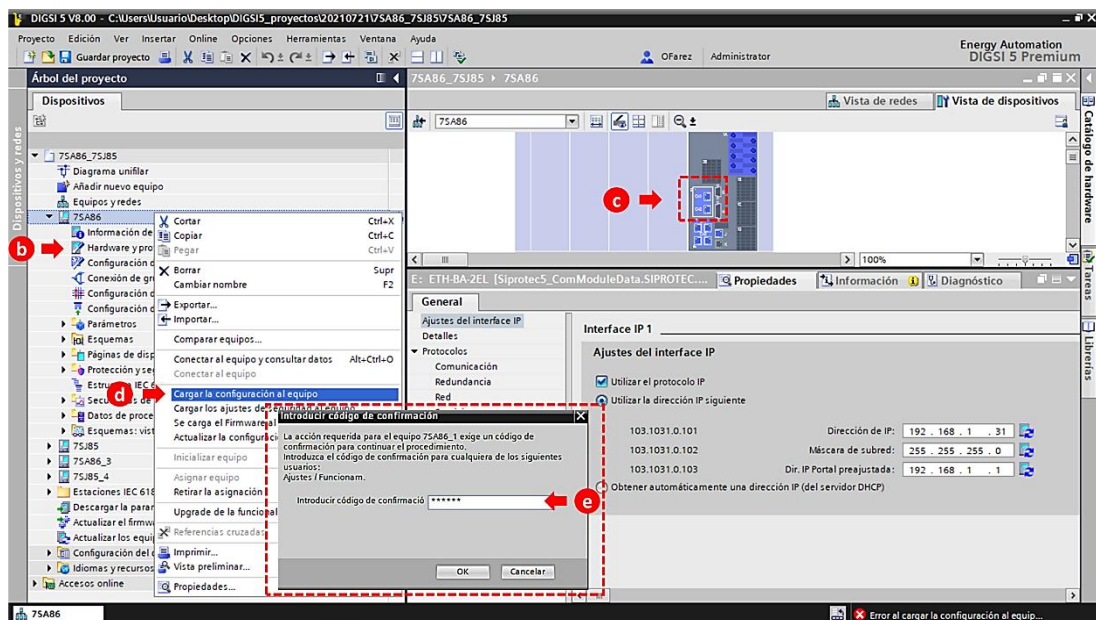


Figura 101. Ajustes de direccionamiento IP del IED en Prueba #1. Fuente: Autores.

## Configurar parámetro de comunicación en PC

Para ello se han adoptado los siguientes pasos:

- a. Ingresar al “Panel de Control” y dar clic en “Ver el estado y las tareas de red”.
- b. Luego clic en la opción “Cambiar configuración del adaptador”.
- c. Clic derecho en la opción “Ethernet” y seleccionar “Propiedades”.
- d. Después, seleccionar “Habilitar el protocolo de Internet versión 4 (TCP/IPv4)”, y clic en “Propiedades”.

- e. Finalmente, seleccionar “Usar la siguiente dirección IP” y rellenar los campos de “Dirección IP” y “Mascara de subred”; y clic en “Aceptar” para guardar la configuración. Véase la Figura 102

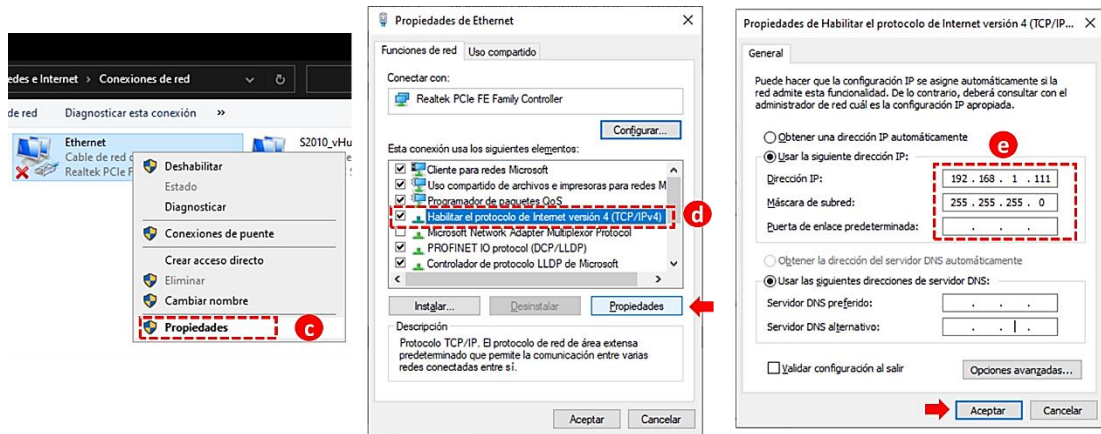


Figura 102. Ajustes de direccionamiento IP del PC en Prueba #1. Fuente: Autores.

### Configurar parámetro de comunicación en CMC 356

Para ello se deben seguir los pasos que a continuación se detallan:

- Conectar mediante cable USB la OMICRON<sup>®</sup> CMC con la PC, abrir el módulo “OMICRON Device Link”.
- Seleccionar la opción “Abrir interfaz web”.
- Seleccionar en el menú principal, la opción “Network”.
- Luego, seleccionar “Port ETH1”.
- A continuación, seleccionar “Static” para la asignación de red.
- Finalmente, rellenar los campos: “Dirección IP” y “Mascara de subred”, y clic en “Apply” para guardar la configuración, véase la Figura 103.

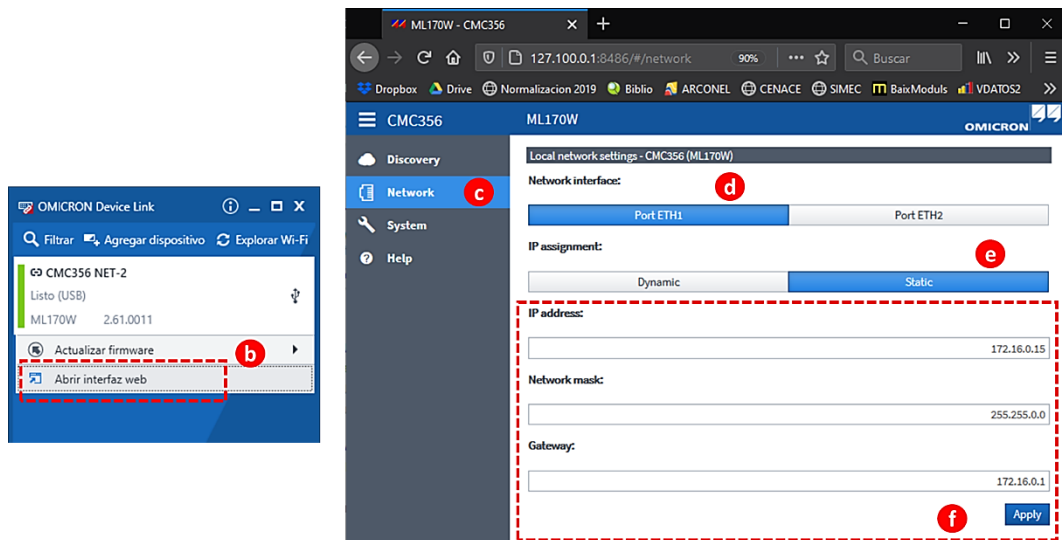


Figura 103. Ajustes de direccionamiento IP de la CMC en Prueba #1. Fuente: Autores.

## Verificación de red

Para verificar que el estado de la red LAN sea la correcta, se requiere ejecutar el comando PING desde la PC. Para ejecutar el comando PING se debe seguir los pasos descritos a continuación:

- Acceder a la herramienta de “Símbolo del sistema”, ejecutando el atajo tecla Windows + R.
- Escribir “CMD” y clic en aceptar.
- Luego, se abrirá una ventana del programa, a continuación, digitar el comando “PING” más una dirección IP del equipo con el cual se desea verificar la conexión, y presionar la tecla Enter.

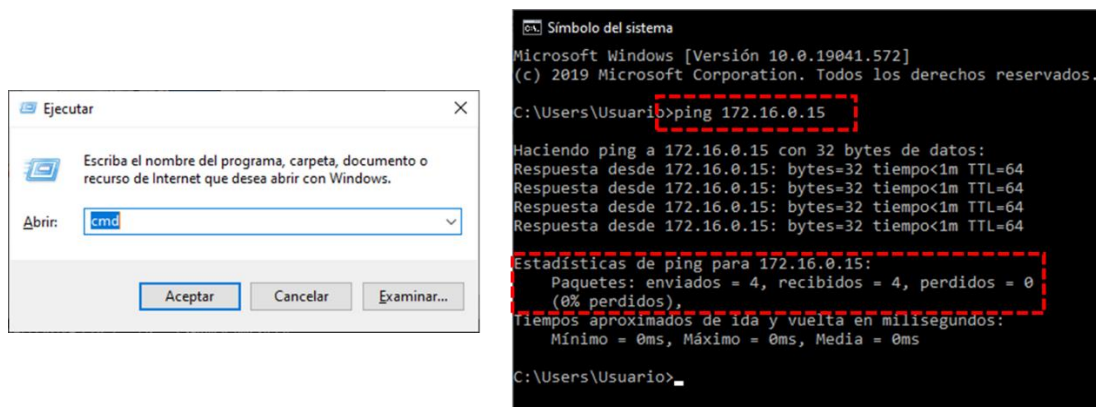


Figura 104. Pasos para verificar red en Prueba #1. Fuente: Autores.

Si la cantidad de paquetes enviados es igual a la cantidad de paquetes recibidos, se puede asegurar que la comunicación es la correcta, véase la Figura 104.

#### **4.4.1.5. Conclusiones**

Se puede verificar mediante el comando PING, digitado en la aplicación Símbolo del sistema; que todos los equipos configurados están conectados a una misma red LAN, en la cual pueden enviar y recibir cierta cantidad de datos sin existir pérdida alguna.

#### **4.4.1.6. Recomendaciones**

Verificar las direcciones IP y la máscara de subred de los diversos equipos, estén digitados correctamente, para que no exista errores al momento de comprobar la red.

## **4.4.2. Prueba #2 - Cargar archivo SCL a la RTU Orion LXM**

### **4.4.2.1. Objetivos**

- Creación de archivo “SCD”.
- Crear Informes y reportes en base al protocolo MMS.
- Monitorizar variables eléctricas desde el navegador.

### **4.4.2.2. Recursos**

- Switch industrial GREYHOUND
- RTU Orion LXM
- IED
- PC
- Cables de red

### **4.4.2.3. Descripción y funcionamiento**

La obtención de archivos SCL, implica en primer lugar crear un proyecto en el “DIGSI® 5” y configurar las variables eléctricas en los IED’s. Luego crear la estación IEC 61850 en el “IEC 61850 System Configurator” el cual permite ajustar los parámetros definidos en el estándar, es decir, que en dicha estación se podrá realizar los ajustes de comunicación GOOSE, SV o MMS. Posteriormente, se debe crear un proyecto en el NCD y configurar el puerto de red con el estándar IEC 61850 en la modalidad cliente/servidor. Finalmente cargar el archivo SCD.

### **4.4.2.4. Desarrollo**

#### **Crear proyecto en DIGSI® 5**

Inicialmente crear un proyecto y añadir el equipo con el cual se desea trabajar, en este caso ingresar el código largo “7SA86-DAAA-AA0-0AAAA0-AK0111-13111B-AAC000-000AC0-CH1BA1” o el código corto “P1A150332” del producto y comprobar, véase la Figura 105. Luego, seleccionar la plantilla “Básico” con la versión más actual; puesto que, sea acorde a la versión de los controladores instalados en el equipo.

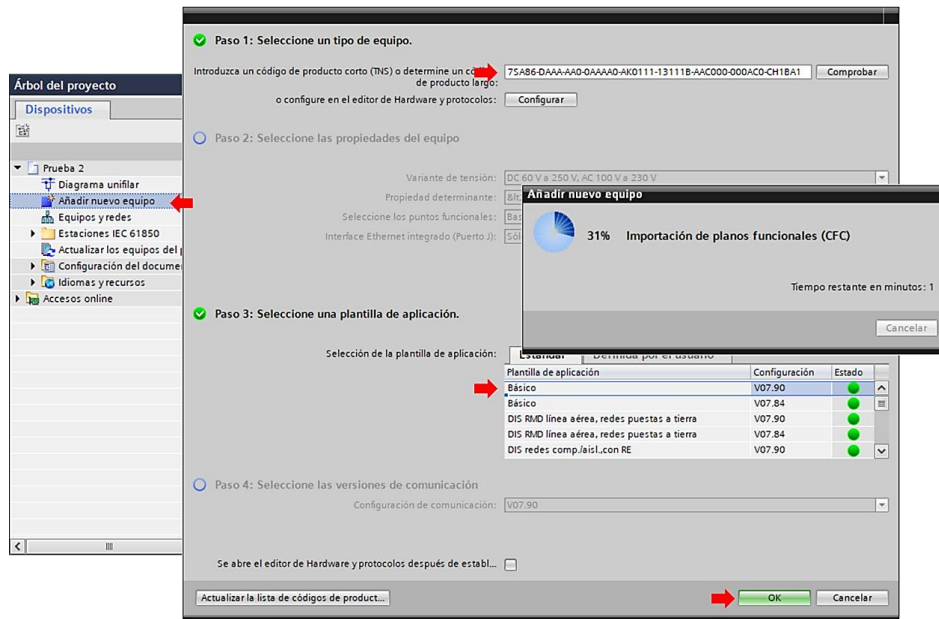


Figura 105. Pasos para añadir IED's para Prueba #2. Fuente: Autores.

Una vez añadido el equipo, en este caso se añadió el IED de distancia 7SA86, se procede a configurarlo, para ello se dirige al “Árbol del proyecto”, clic en el dispositivo creado “7SA86” y seleccionar el menú “Información del equipo”, en él se realiza: el renombre del dispositivo con el cual se identificará en el software DIGSI® 5; y en “Nombre IEC 61850” se ingresa el nombre con el cual se identifica al dispositivo en el mapeo de datos dentro de la estación IEC. Finalmente seleccionar la “Edición 2” la cual es correspondiente a la versión actual del estándar. Véase la Figura 106.



Figura 106. Ajuste de nombre IEC 61850 del IED para Prueba #2. Fuente: Autores.

De igual forma, se configura los ajustes que están dentro del menú “Hardware y protocolos”, posteriormente se realiza los ajustes en el puerto E: cambiar la Dirección IP y la Máscara de subred. Véase la Figura 107.

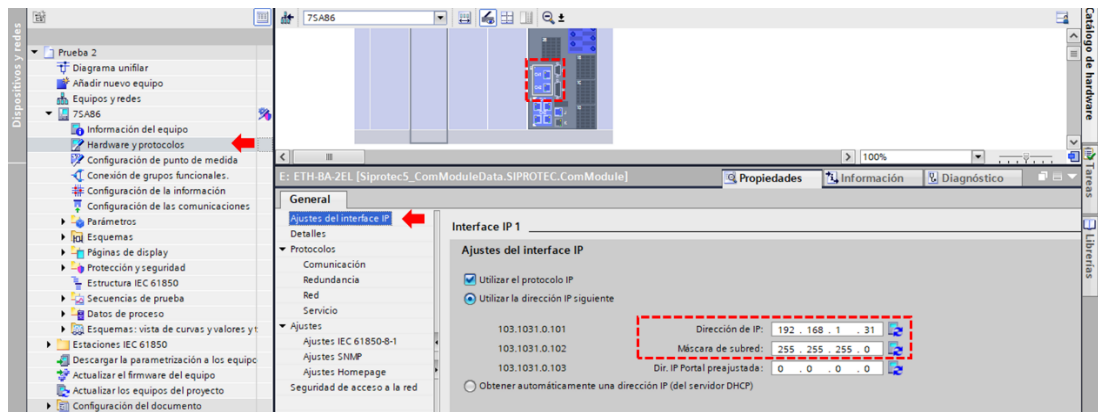


Figura 107. Ajuste del direccionamiento IP del IED en Prueba #2. Fuente: Autores.

- En el campo “Protocolos”, habilitar el estándar “IEC 61850”, en el caso de redundancia habilitar el “modo Línea”, en el caso de protocolo de red habilitar “DCP” y “SNMP”, en el caso de servicio habilitar el protocolo “Homepage” y en ajustes seleccionar “ON”. Tal como se muestra en la Figura 108.

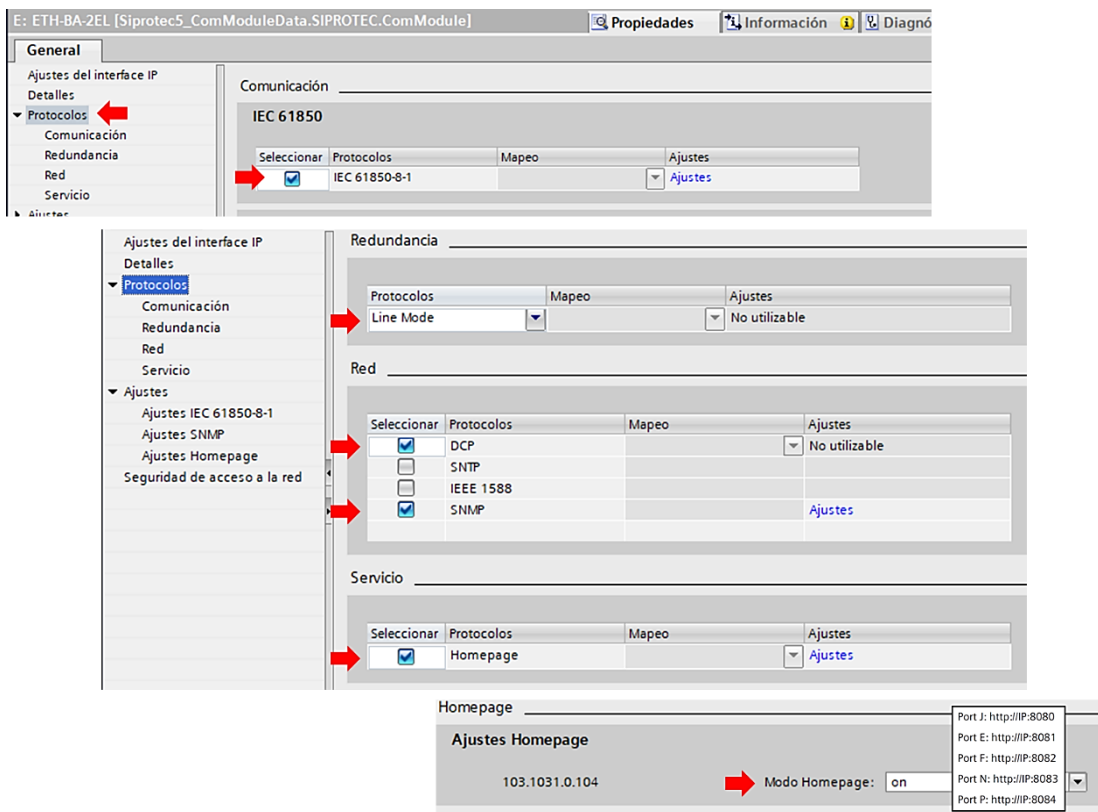


Figura 108. Ajuste de protocolo de comunicación del IED para Prueba #2. Fuente: Autores.

Luego, ajustar los parámetros en el menú “Ajustes del equipo” (véase la Figura 109), en él se debe habilitar:

- El “Puerto E” para hacer uso del DIGSI® 5.
- En “Señalización de los ajustes en la estructura IEC 61850” seleccionar “Mostrar todos los ajustes”.
- En “Señalización de las extensiones en la estructura IEC 61850” seleccionar “Mostrar todas las extensiones”.
- Además, marcar la casilla de “Activar supervisión GOOSE”, para habilitar la funcionalidad de supervisión de conexión mediante ese protocolo.

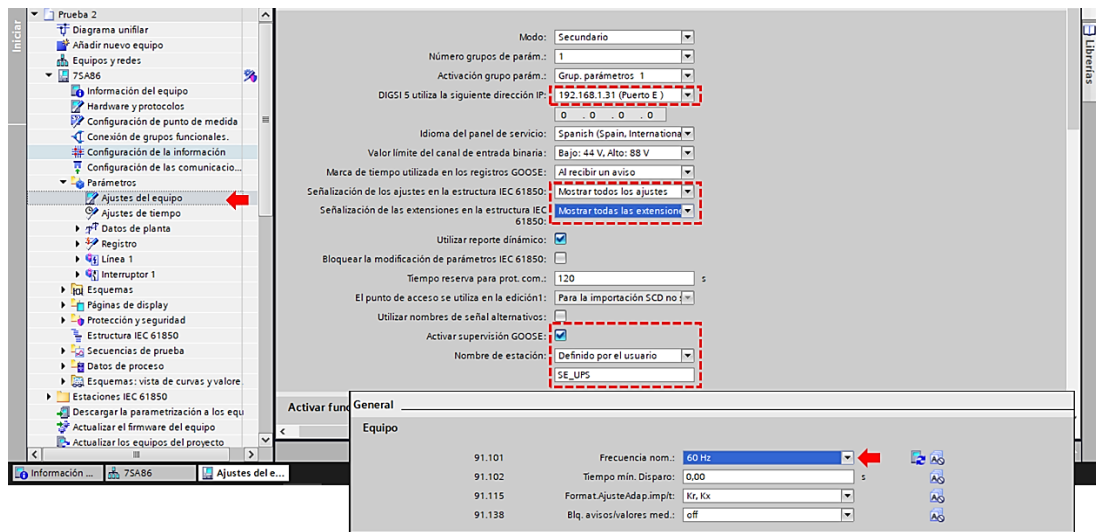


Figura 109. Ajuste de la comunicación IEC 61850 para Prueba #2. Fuente: Autores.

A continuación, revisar que dentro del menú “Seguridad de acceso a la red”, los accesos para el DIGSI®, MMS y Web estén seleccionados “Acceso lectura/escritura”. Véase la Figura 110.



Figura 110. Ajuste de seguridad de acceso a la red para Prueba #2. Fuente: Autores.

Finalmente, ajustar el modelo de datos del dispositivo a una configuración de interfaz deseada, como cambiar el nombre de los LD existentes, modificar los LN, modificar o crear o eliminar DO, entre otros ajustes. Para ello debe dirigirse al “Árbol del



proyecto” y seleccionar el menú “Estructura IEC 61850” y en el realizar los ajustes necesarios. Véase la Figura 111.

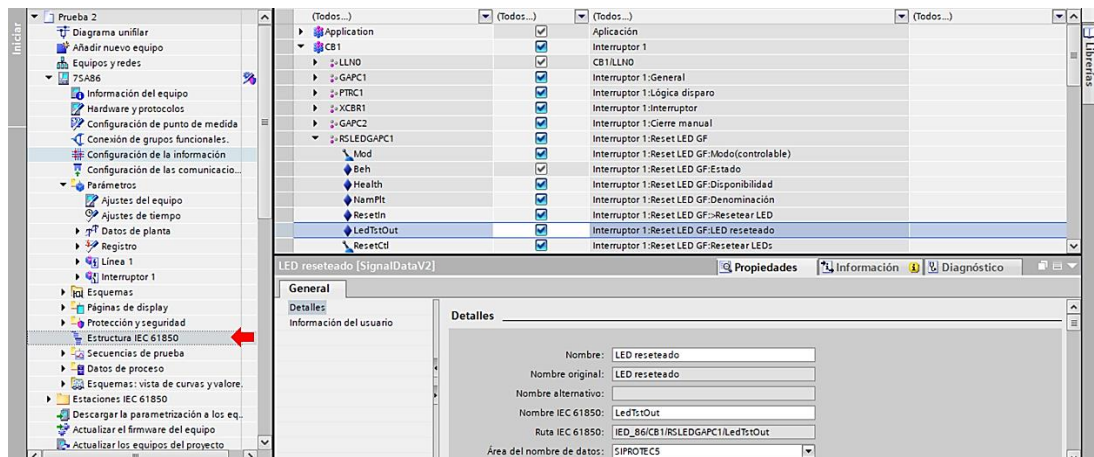


Figura 111. Ajuste del modelo de datos para Prueba #2. Fuente: Autores.

## Crear estación IEC 61850

Una vez creado y ajustados los IED’s dentro del proyecto DIGSI® 5 se procederá a crear la “Estación IEC61850” (véase la Figura 112) en donde se podrá realizar los ajustes de comunicación GOOSE, SV o MMS, a continuación, se listan los pasos a seguir para su creación:

1. Dirigirse al “Árbol del proyecto” y seleccionar el menú “Estaciones IEC 61850” y dar doble clic en “Añadir nueva estación”, se creará una nueva estación y dar clic sobre ella.
2. Modificar el nombre de la estación IEC y elegir la “Edición 2” ya que actualmente es la más común en los diversos dispositivos.
3. Elegir la ruta en la cual guardar el fichero “SCD”.
4. Exportar los cambios del dispositivo al configurador del sistema IEC 61850.

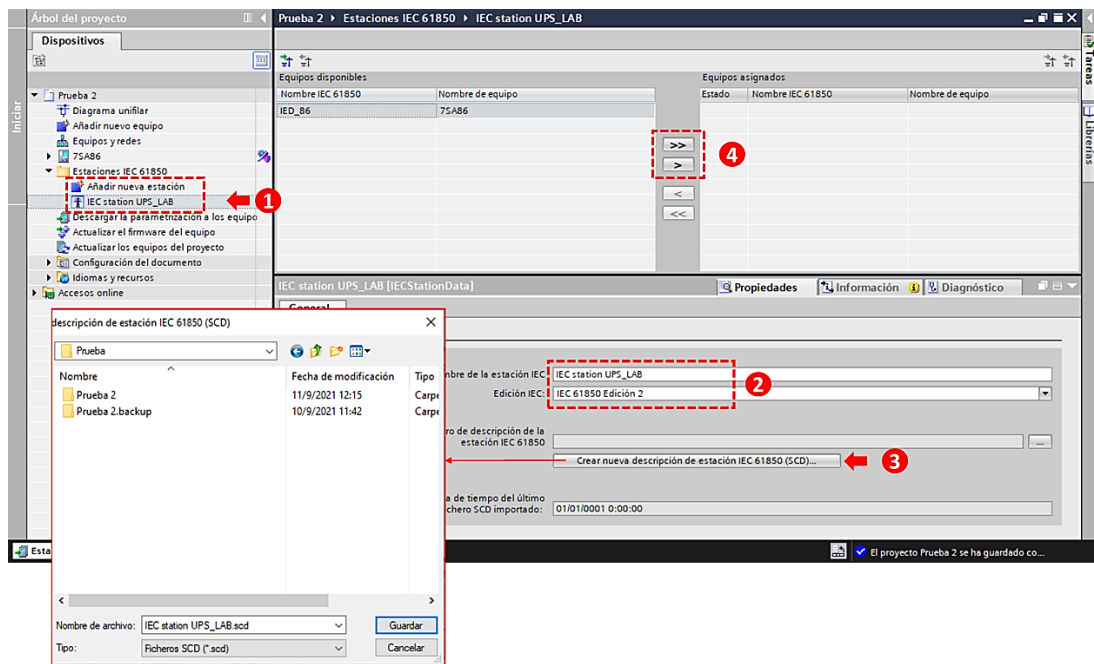


Figura 112. Pasos para la creación de la estación IEC 61850 en Prueba #2. Fuente: Autores.

Una vez realizada la transferencia al configurador del sistema, inmediatamente se abrirá el software “IEC 61850 System Configurator”.

Dentro del configurador del sistema proceder a crear Informes y registros (véase la Figura 113), para ello primero crear el dataset y a su vez los objetos de datos, a continuación, se enumeran los pasos a seguir:

1. Seleccionar el menú “Informes y registros” y en el “Árbol de proyecto” clic en el dispositivo IED.
2. Clic derecho y seleccionar “Insert dataset”.
3. En la ventana de propiedades, renombrar el dataset creado para una fácil localización.

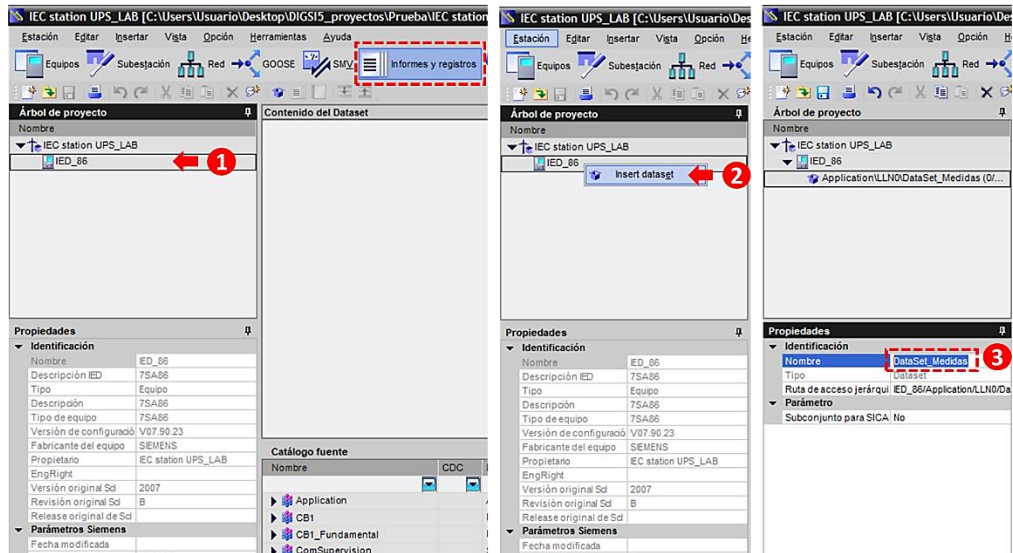


Figura 113. Pasos para crear dataSets en Prueba #2. Fuente: Autores.

4. Arrastrar los objetos de datos desde el catálogo fuente a la ventana “Contenido del Dataset”, tal como se muestra en la Figura 114.
5. En la ventana “Control de informe y log bloqueados” clic derecho y seleccionar “Insert report”.
6. En la ventana de propiedades, renombrar el reporte creado para una fácil localización.
7. Guardar la estación creada.

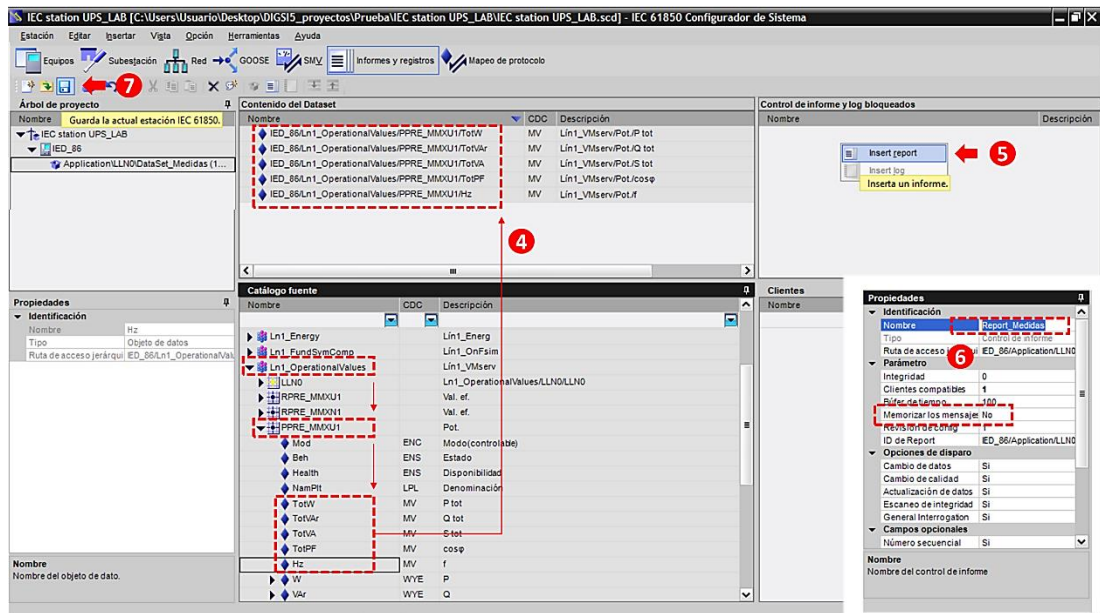


Figura 114. Pasos para crear los reportes para Prueba #2. Fuente: Autores.

Finalmente, importar los cambios del configurador de sistema IEC 61850 al DIGSI® 5 (véase la Figura 115), además, cargar los cambios generados en todo el proyecto, a cada uno de los IED's correspondientes.

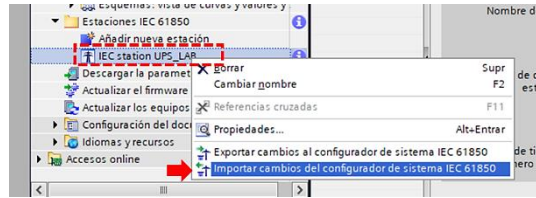


Figura 115. Pasos para importar cambios al DIGSI® 5 para Prueba #2. Fuente: Autores.

### Crear proyecto en NCD

1. Abrir el software NCD y crear un nuevo archivo, en el escoger el modelo de RTU “Orion LXM” y clic en “OK”.
2. Seleccionar el menú “Configure”, clic en el archivo guardado recientemente, luego seleccionar la opción “Network”, y clic en “Configure new port”.
3. Se abrirá una ventana en la cual se podrá seleccionar el protocolo de comunicación, seleccionar la opción “IEC 61850 - Client/Server”, y clic en “OK”. Véase la Figura 116.

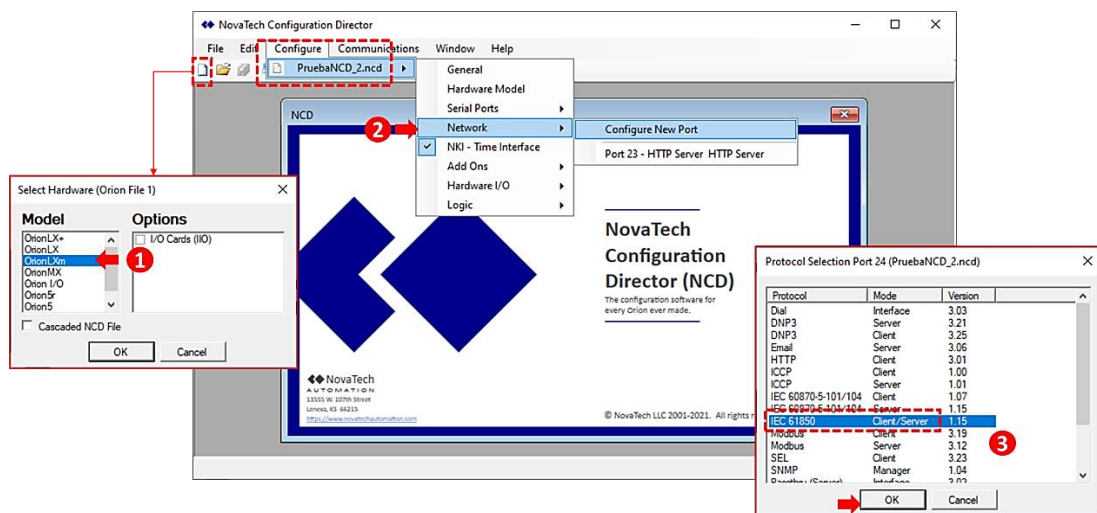


Figura 116. Pasos para configurar protocolo cliente/servidor en Prueba #2. Fuente: Autores.

4. Para agregar un dispositivo dirigirse al menú del puerto (panel izquierdo) y haga clic en “Add new device”. Véase la Figura 117.

5. Se agrega un nuevo dispositivo etiquetado como Device 1 con subtítulos de Entradas y Salidas. Para importar el archivo configurador SCL, ICD, CID, SCD o IID, dirigirse al menú del dispositivo y seleccionar “Device 1” y clic en “Import”.
6. Escoger la carpeta donde se guardó el archivo importado desde la Estación IEC 61850 el cual tiene una extensión “SCD”, seleccionar archivo para importar y clic en “Abrir”.
7. Escoger el archivo SCL correspondiente al dispositivo y clic en “Accept”.

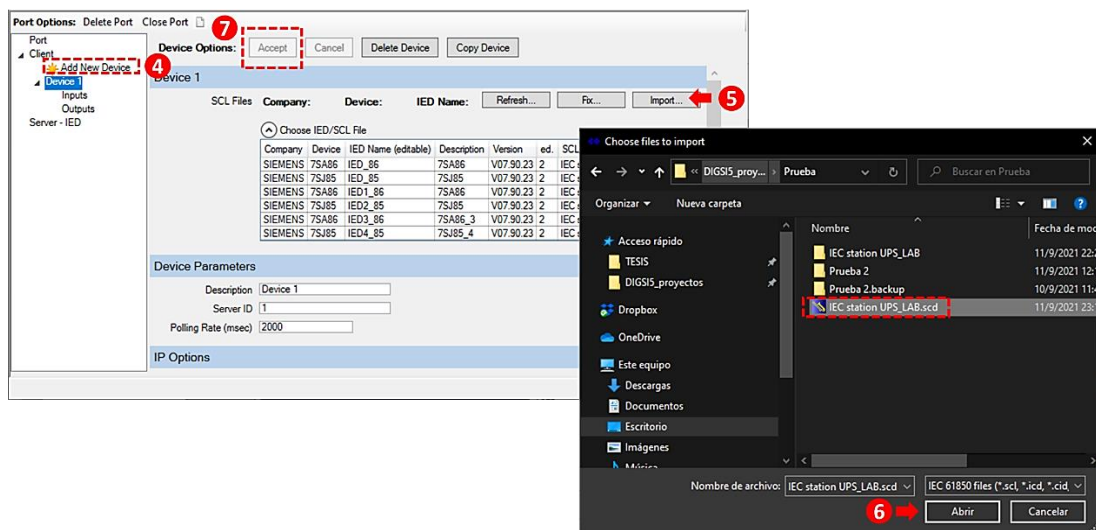


Figura 117. Pasos para importar archivo SCL al NCD para Prueba #2. Fuente: Autores.

8. Seleccionar los datos para los puntos de entrada “Inputs” y puntos de salida “Outputs” del dispositivo, mediante la activación o desactivación de su correspondiente casilla, en este caso se selecciona de forma general el dataset creado en la estación IEC, tal como se muestra en la Figura 118.
9. Agregar los puntos de entrada seleccionados haciendo clic en “>>”.
10. Guardar el archivo.

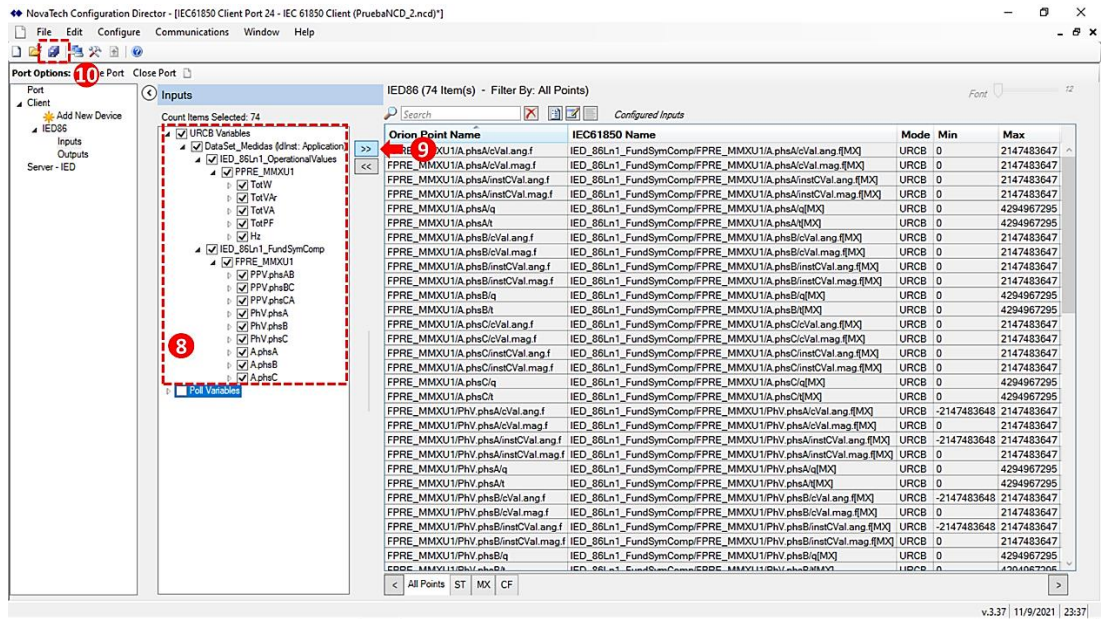


Figura 118. Selección de datos para las Inputs en Prueba #2. Fuente: Autores.

Luego se procede a configurar el protocolo del servidor XML (véase la Figura 119), en el cual se selecciona las variables a utilizar en el HMI. A continuación, se listan los pasos a seguir para su creación:

1. Ir al menú “Configure” y clic en el archivo creado en un principio, después, seleccionar “Network” y clic en “Configure New Port”.
2. Se abrirá una ventana, seleccionar la opción “XML - Server”, y clic en “OK”.
3. Para agregar un archivo dirigirse al menú del puerto (panel izquierdo) y haga clic en “Add new File”.

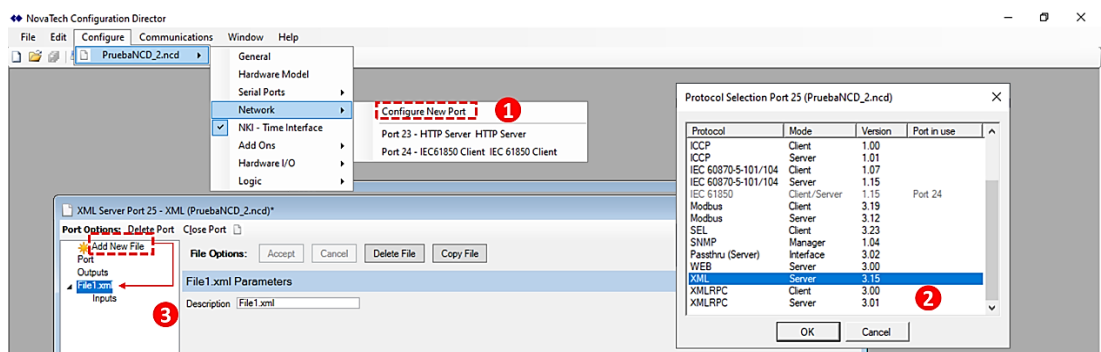


Figura 119. Pasos para configurar protocolo XML en Prueba #2. Fuente: Autores.

4. Seleccionar los datos para los puntos de entrada “Inputs” y puntos de salida “Outputs”.
5. Agregar las variables seleccionadas haciendo clic en “>>”, véase la Figura 120.

## 6. Guardar el archivo.

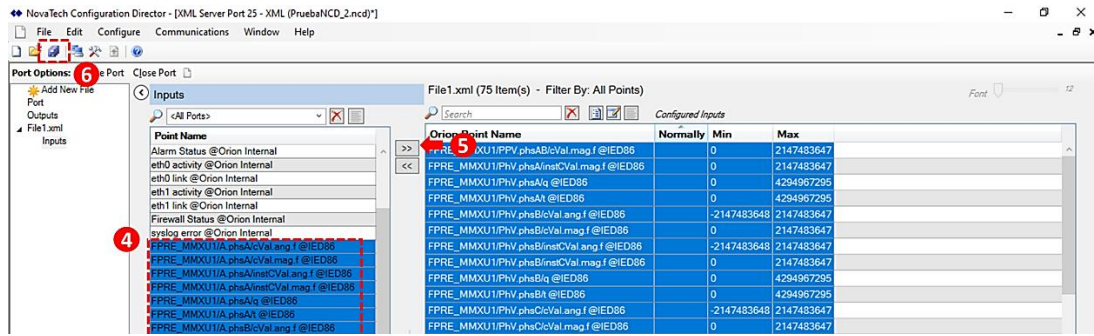


Figura 120. Selección de datos para las Inputs del XML en Prueba #2. Fuente: Autores.

## Exportación de un proyecto a la RTU

Teniendo ya creada la conexión de red se procede a transferir los archivos desde la PC a la ORION. A continuación, se listan los pasos para cargar los archivos a la RTU:

1. Abrir “Manage Connections” y conectar a la red.
2. Se abrirá la ventana de conexión online y solicitará acceso, para iniciar sesión, digitar la palabra “novatech”, tanto para usuario como para contraseña. Véase la Figura 121.
3. Inmediatamente se visualiza el menú principal en la ventana de comandos, para seleccionar alguna opción basta con digitar el número que precede a la opción, en este caso digitar “1” para seleccionar el menú de archivos.

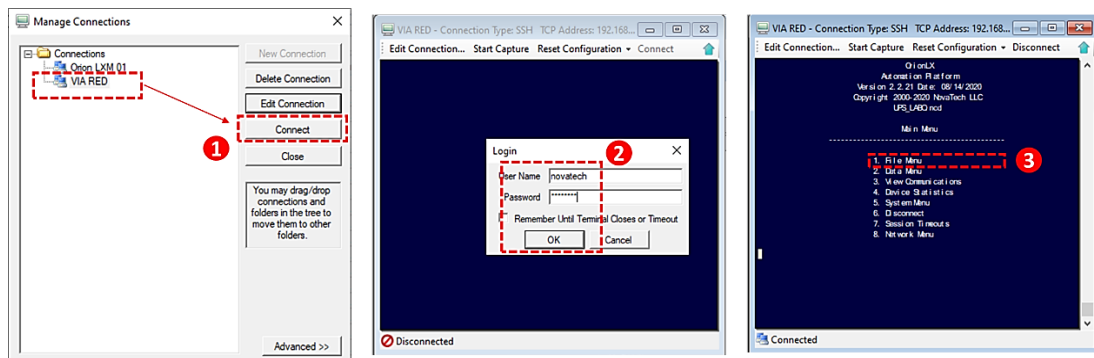


Figura 121. Pasos para la comunicación SSH entre PC y ORION para Prueba #2. Fuente: Autores.

4. Digitar “1” para transferir los archivos desde la PC hacia la ORION.

5. Se abrirá una ventana en la cual se debe escoger los 2 archivos generados en el proyecto, con extensión “NCD” y “NCZ”, los cuales serán transferidos a la RTU. Véase la Figura 122.
6. Digitar “3” para activar el archivo de configuración correspondiente a la RTU.
7. Digitar la opción correspondiente al archivo cargado recientemente, en este caso opción “2”.
8. Digitar opción “1”, para realizar un reinicio completo.

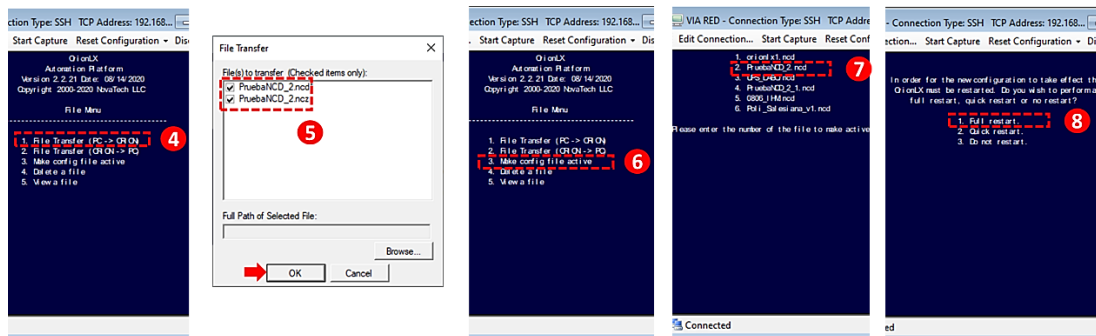


Figura 122. Pasos para cargar la configuración a la ORION para Prueba #2. Fuente: Autores.

Finalmente, una vez reiniciado el equipo, éste se encontrará listo para ser usado desde el navegador.

### Aplicación WEBserver

En la página “Devices” con dirección ip “https://192.168.1.3/Devices/” (véase la Figura 123), la cual se encuentra en la cabecera de la página web principal, muestra una tabla estadística del dispositivo servidor conectado a la red, esto permite verificar la conectividad y la calidad de la comunicación del dispositivo.

La columna “Online” indica la existencia de comunicación entre el dispositivo servidor y el dispositivo cliente. En cambio, en las columnas “Polls” y “Responses” se visualiza que la cantidad de paquetes de datos enviados es igual a la cantidad de paquetes recibidos; y la columna “Successfull” representa que la comunicación es 100% exitosa.





Figura 123. Ventana Device del WEBserver para Prueba #2. Fuente: Autores.

En la página “DataValues” (véase la Figura 124) con dirección ip “https://192.168.1.3/DataValues /”, muestra los puertos de comunicación configurados, entre ellos se encuentra el puerto “25 – XML”. A continuación, se accede al apartado de “Inputs” y se visualiza todas las variables o nodos lógicos importados hacia el HMI, en la columna de “Status” se observa que todas las variables están en modo “Online”, es decir, que la transmisión de paquetes de datos es la correcta.

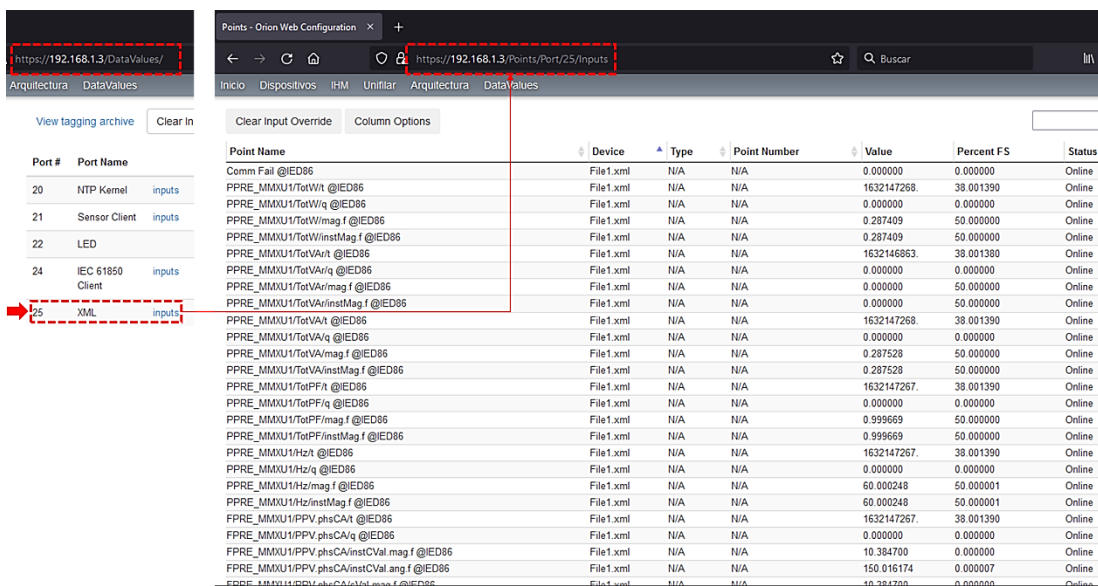


Figura 124. Variables HMI vistas desde el WEBserver para Prueba #2. Fuente: Autores.

#### 4.4.2.5. Conclusiones

Se logró realizar el monitoreo de variables eléctricas (corriente, tensión, frecuencia, y potencias), haciendo uso del protocolo MMS para la transmisión de datos bajo el estándar IEC 61850.

#### **4.4.2.6. Recomendaciones**

Una vez creada la Estación IEC 61850, si se requiere hacer cambios en el proyecto en DIGSI® 5, el menú contextual de la Estación IEC mostrará el símbolo “(i)”, lo cual indica la existencia de cambios que requieren ser exportados al configurador del sistema, es decir, que siempre que haya modificaciones se debe exportar e importar del DIGSI® a la Estación IEC 61850 y viceversa.

### **4.4.3. Prueba #3 - Desarrollo de HMI en Inkscape™**

#### **4.4.3.1. Objetivos**

- Crear la interface Web del proyecto en el cual se puede supervisar y monitorizar los parámetros eléctricos del proyecto.
- Diseñar el HMI con el software Inkscape™.
- Creación de botones, librerías y diagramas unifilares.

#### **4.4.3.2. Recursos**

- Software Inkscape™
- PC

#### **4.4.3.3. Descripción y funcionamiento**

El Software Inkscape™ permite realizar el HMI y visualizarlo en el navegador Web, ya que este es un editor gráfico vectorial libre y de código abierto, en el cual se realizará los diagramas unifilares, cuadro de mediciones y esquema de comunicación. Para los accionamientos y visualizaciones de monitoreo se utiliza la mensajería XML, esta permite mapear los datos que se desea mostrar, para luego ser enlazados a la interfaz gráfica.

#### **4.4.3.4. Desarrollo**

##### **Crear proyecto en Inkscape™**

- Para crear el proyecto primero se debe dirigir al menú “File”, luego clic en “New From Template”, y seleccionar “Page”, y se escoge el formato deseado, en este caso se utilizó A4. Véase la Figura 125.
- Posteriormente, se abre el cuadro de diálogo, en él ingrese el nombre del proyecto y la ruta donde va a ser guardado.
- Finalmente, clic en “Create from template”.

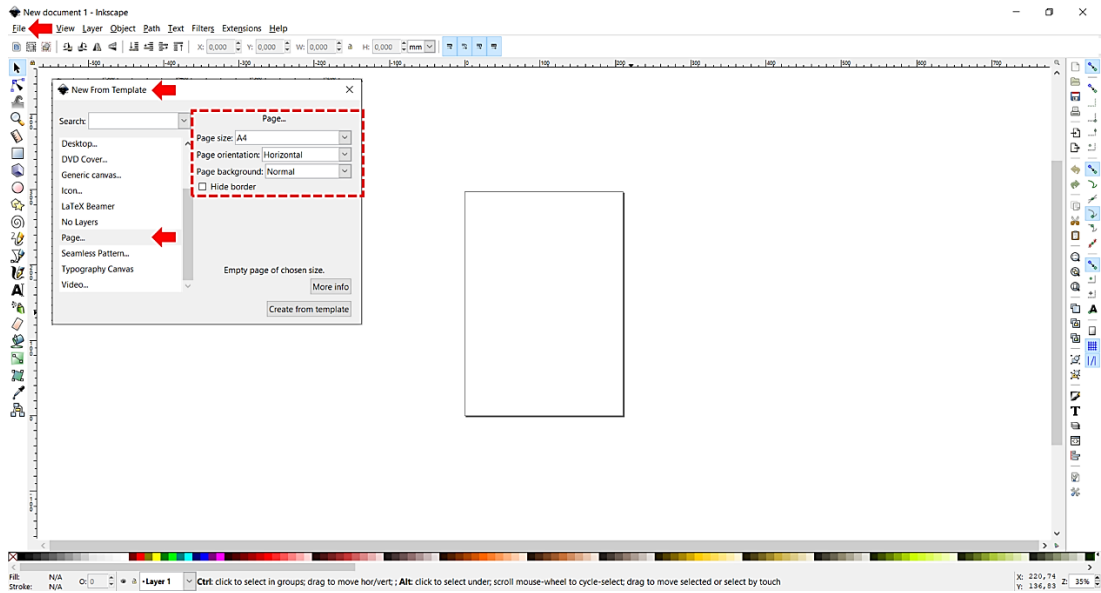


Figura 125. Ajustes para crear proyecto en Inkscape™ para Prueba #3. Fuente: Autores.

- Se procede a modificar el fondo de pantalla para una mejor visualización en el navegador Web, para ello dar click en “Edit Properties”.
- Ajustar colores de fondo y de formato a convenir.
- En las opciones “General” y “Page Size”, seleccionar las unidades de “px” pixeles, para un mejor ajuste de interfaz con el navegador, con el fin de tener una vitalización en dispositivos como PC, Tablet y Móviles. Véase la Figura 126.

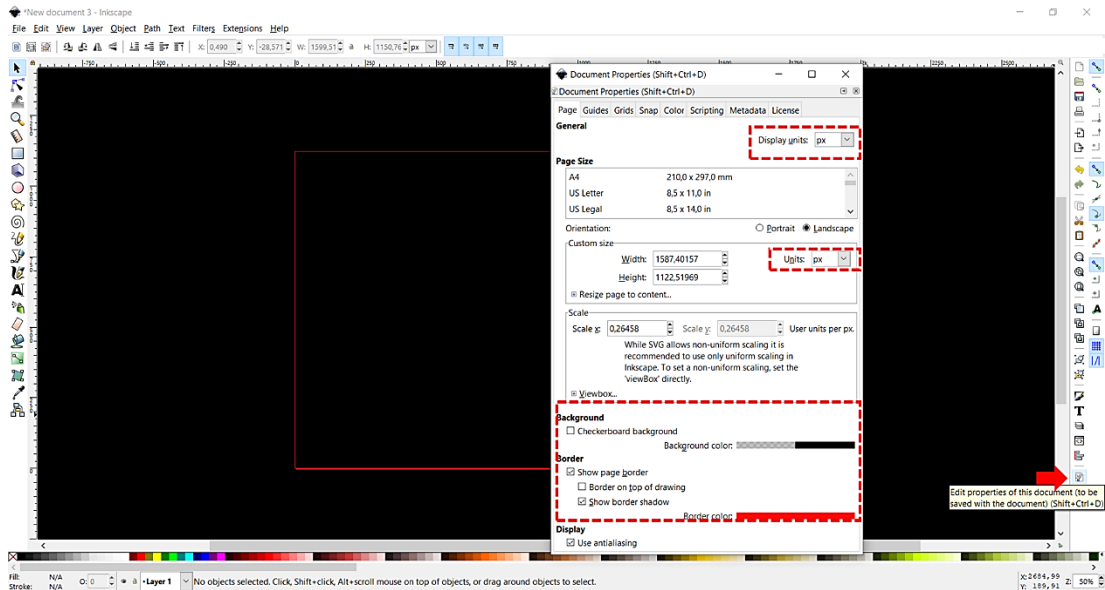


Figura 126. Ajuste para ventana HMI en Prueba #3. Fuente: Autores.

### Creación del Diagrama Unifilar

Para la creación del diagrama unifilar, se dibuja cada elemento con las diferentes herramientas que tiene el Inkscape™, para realizar una barra y las conexiones entre elementos y los IED's se utiliza "Create Rectangles", y para dibujar los TC y TP con la herramienta "Create Circles". En cambio, para la creación de textos se utiliza la herramienta "Create and edit Text". Véase la Figura 127.

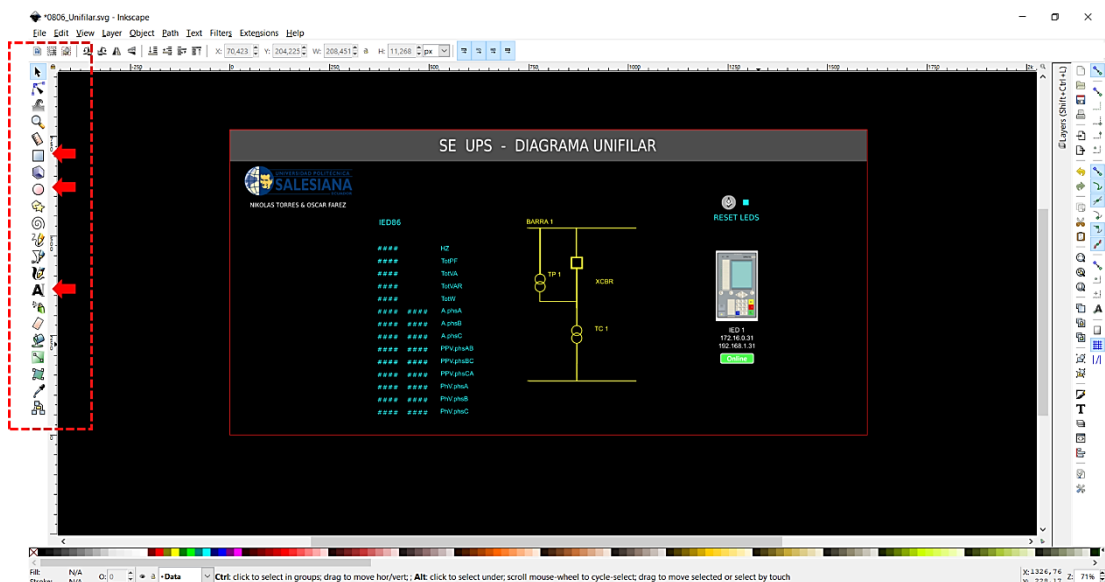


Figura 127. Creación de diagrama unifilar para Prueba #3. Fuente: Autores.

### Creación de enlace de datos XML

Para la creación del enlace de datos XML se selecciona el menú “Extensions”, luego la opción “HMI”, esta extensión enlaza el archivo NCD con el Inkscape™ para facilitar la creación de archivos SVG.

Para acceder a la Extensión HMI, tanto NCD como Inkscape™ deben estar ejecutándose al mismo tiempo debe estar seleccionado un objeto. Desde la pestaña de Extensiones, se puede seleccionar la opción HMI (Véase la Figura 128).

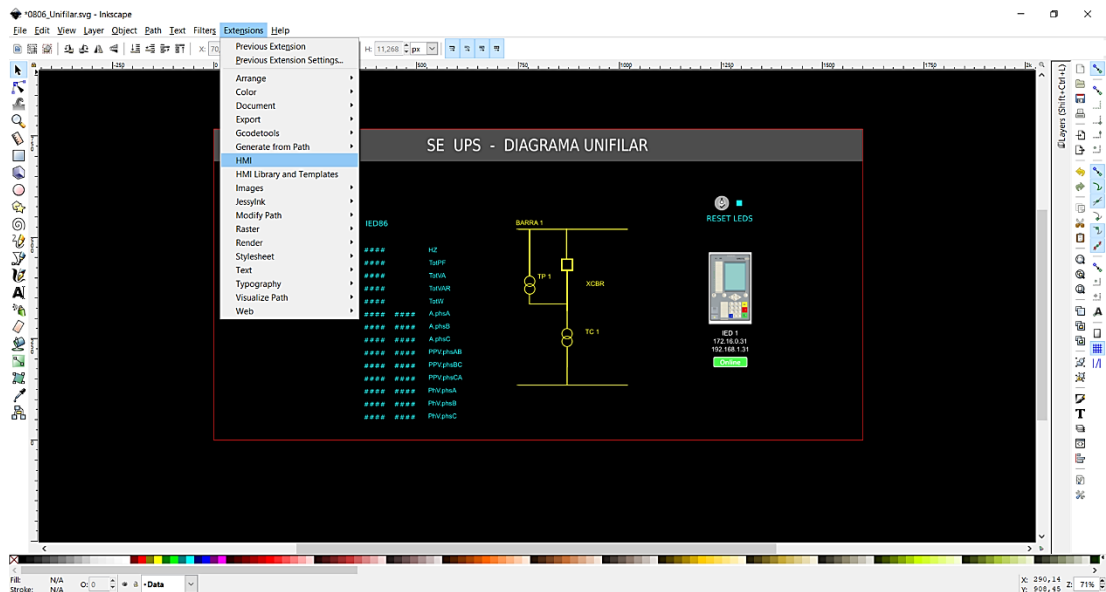


Figura 128. Vista del menú “Extension” en el Inkscape™ para Prueba #3. Fuente: Autores.

Una vez seleccionada la opción HMI, aparecerá una ventana la cual está dividida en cuatro secciones (véase la Figura 129). A continuación, se explican los parámetros de cada sección. Los parámetros de la parte superior de la ventana se aplican a toda la página, mientras que los parámetros de las secciones Configuración de entradas/salidas, Configuración de alarmas y Configuración de etiquetas sólo se aplican al objeto seleccionado.

Para crear la extensión, se realiza los siguientes pasos:

1. En la opción “XML File”, se selecciona el archivo XML que se crea en el NCD.
2. En la opción “Point”, se selecciona el tipo de nodo lógico que se quiere enlazar con el elemento seleccionado en el Inkscape.
3. En la opción “Test Display”, se selecciona el tipo de dato.

4. Se selecciona en “Aceptar”.

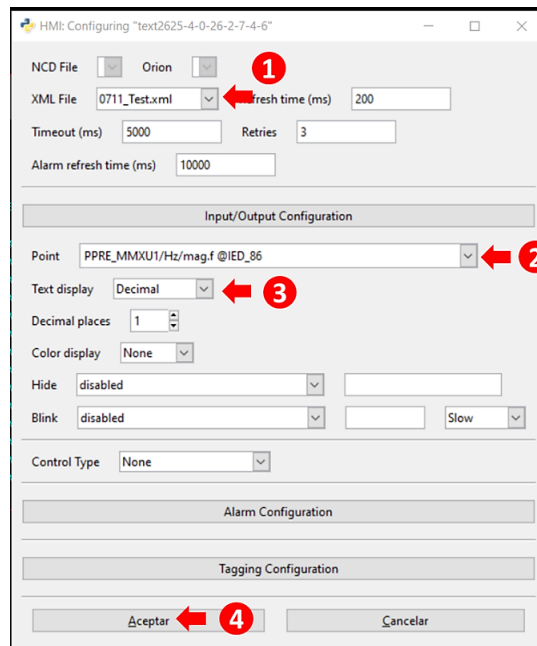


Figura 129. Ajustes en extensión HMI para Prueba #3. Fuente: Autores.

Para crear los botones, se realiza los siguientes pasos:

1. En la opción “Control Type”, se selecciona el tipo de funcionamiento del botón, en este caso se selecciona “Control No Confirm”. Véase la Figura 130.
2. En la opción “Control”, se selecciona el tipo de nodo lógico que se quiere enlazar con el elemento seleccionado en el Botón.
3. Se selecciona en “Aceptar”.

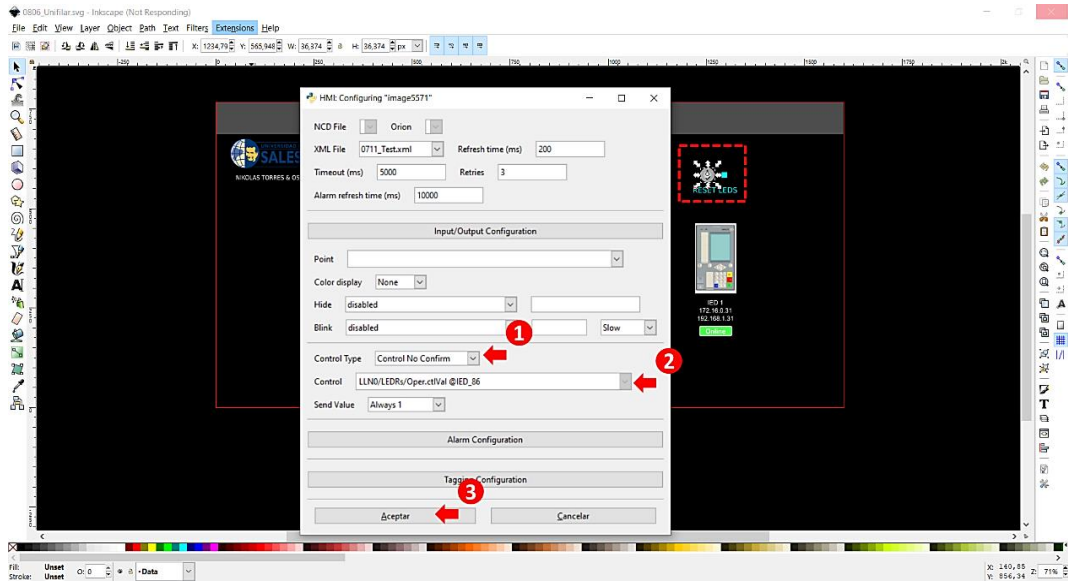


Figura 130. Ajustes de los objetos botones en el HMI para Prueba #3. Fuente: Autores.

En la siguiente Figura 131 se muestra la visualización que tendrá en la página Web.

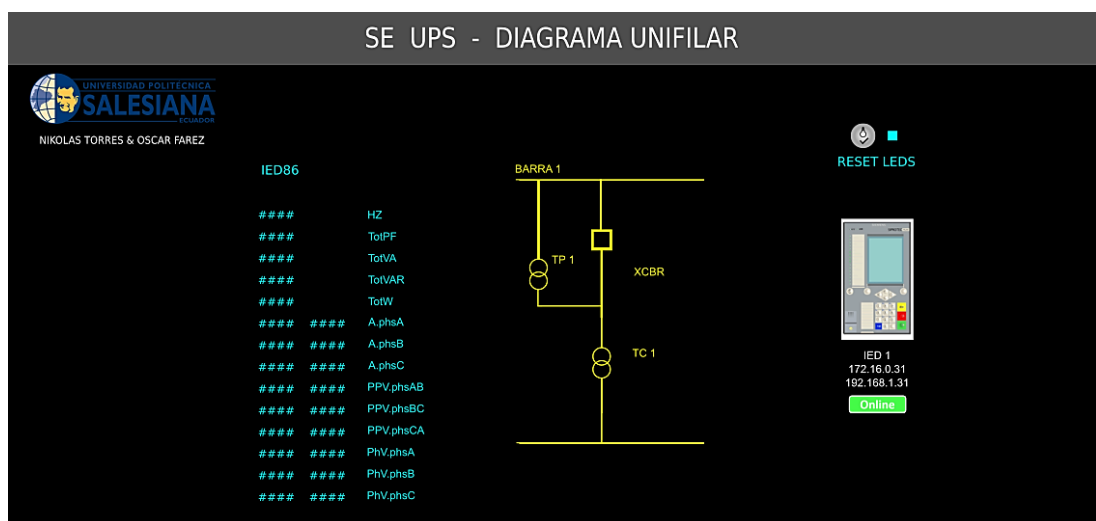


Figura 131. Vista del archivo HMI para Prueba #3. Fuente: Autores.

#### 4.4.3.5. Conclusiones

Con la ayuda de este software se puede realizar varias interfaces según las necesidades del usuario ya que es una herramienta de fácil manejo.

#### 4.4.3.6. Recomendaciones



Al momento de mapear los datos, estos deben ser identificados de manera correcta para tener una fácil incorporación de los nodos lógicos que se encuentran en el archivo XML.

#### **4.4.4. Prueba #4 - Prueba de comunicación entre HMI e IED's**

##### **4.4.4.1. Objetivos**

- Verificar la comunicación de los datos de los IED's, que van a ser monitorizados por el HMI.
- Monitorear parámetros eléctricos inyectados desde la maleta de pruebas CMC.
- Configurar el mapeo de protocolos para la lectura de parámetros mediante la red LAN IEC 61850.

##### **4.4.4.2. Recursos**

- Switch industrial GREYHOUND
- RTU Orion LXM
- IED
- PC
- Cables de red
- Software NCD
- Software Inkscape™
- OMICRON® CMC 356

##### **4.4.4.3. Descripción y funcionamiento**

La comunicación entre el HMI y los IED's, permite monitorizar en la página web todo lo que se realizó en la práctica anterior, mediante el software NCD el cual permite cargar el archivo "SVG" del Inkscape™ al entorno web de la RTU.

El entorno Web de la RTU contiene varias configuraciones dentro de la misma, en este caso solo se debe de cargar los archivos de los mapeos de datos y el archivo "SVG" el cual contiene la interfaz del diagrama unifilar.

Para verificar la comunicación de los equipos en el entorno Web se entra en la pestaña "Dispositivos" en el cual se visualiza el porcentaje de datos transmitidos.

##### **4.4.4.4. Desarrollo**

###### **Cargar los archivos al entorno Web de la RTU.**

Ya con los nodos lógicos bien mapeados y el archivo XML listo, se procede a cargar los archivos al entorno Web de la RTU, para ello se han adoptado los siguientes pasos (véase la Figura 132).

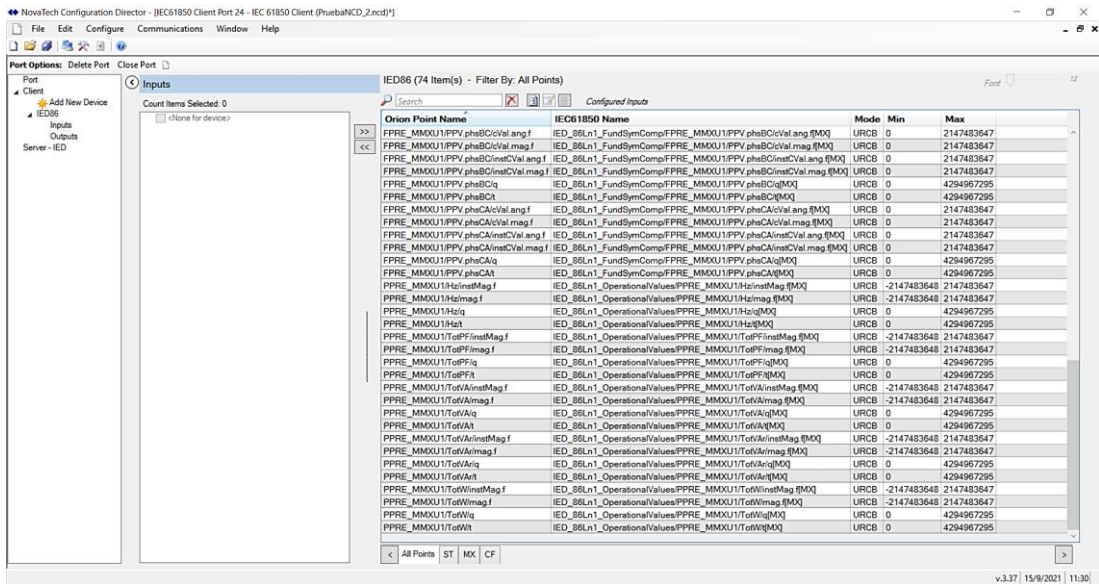


Figura 132. Nodos lógicos Mapeados para Prueba #4. Fuente: Autores.

Se mapean los nodos lógicos que se van a utilizar para enlazar con el HMI (véase la Figura 133), en este caso se utilizan los nodos lógicos que contienen las características de medición, estado de la comunicación como es el reseteo de Leds.

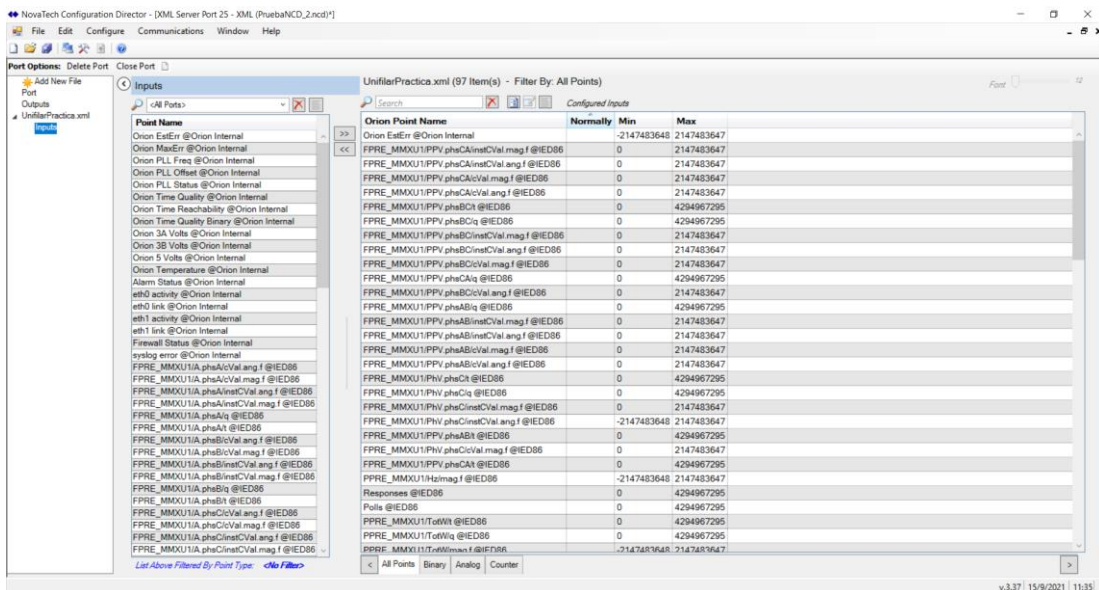


Figura 133. Nodos lógicos del archivo XML para Prueba #4. Fuente: Autores.

Cuando ya se tiene creado los puertos de comunicación como muestra en la siguiente Figura 134, se requiere cargar el archivo “NCD” a la RTU.



Figura 134. Puertos de comunicación creados en el NCD para Prueba #4. Fuente: Autores.

Para cargar los archivos “NCD” a la RTU, se realizan los siguientes pasos (véase la Figura 135):

1. “File Transfer (PC a ORION)”, en el menú se escoge la opción 1.
2. Se carga los archivos que se van a subir y se da en “OK”.
3. Es necesario la activación del archivo para ello se selecciona el archivo que se va a subir.
4. Es necesario resetear la RTU, para que todos los cambios se realicen, se va a la opción “Full restar”

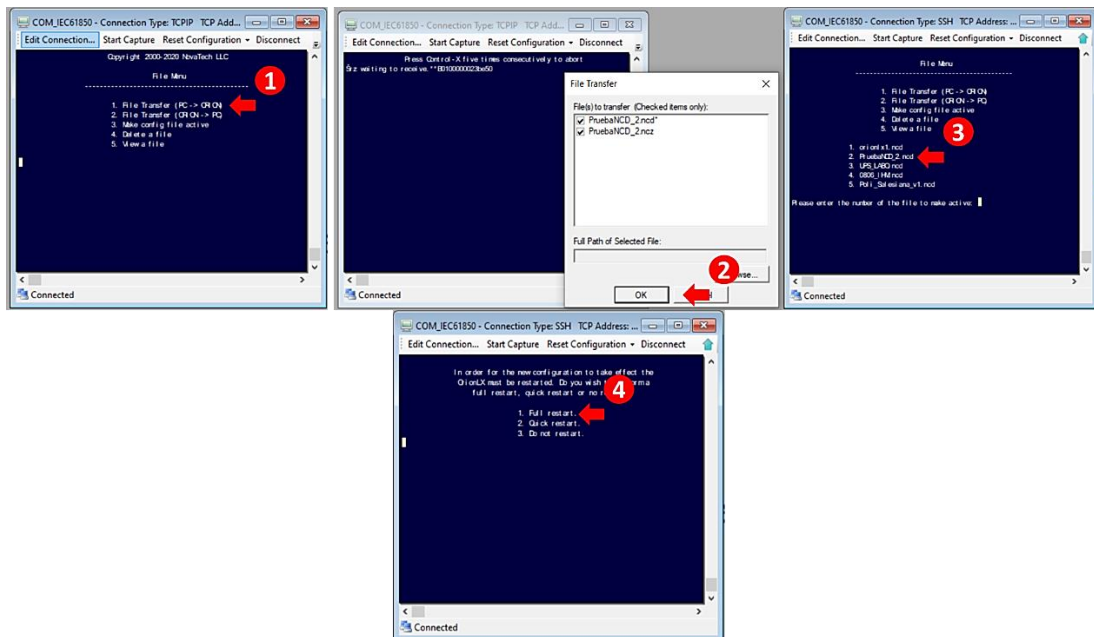


Figura 135. Pasos para cargar el archivo “NCD” a la RTU para Prueba #4. Fuente: Autores.

En la siguiente Figura 136 se muestra el entorno web de la RTU, para entrar se va al navegador web y en la barra de búsqueda colocar la dirección IP, de la RTU en este caso “192.168.1.3” y se accede.

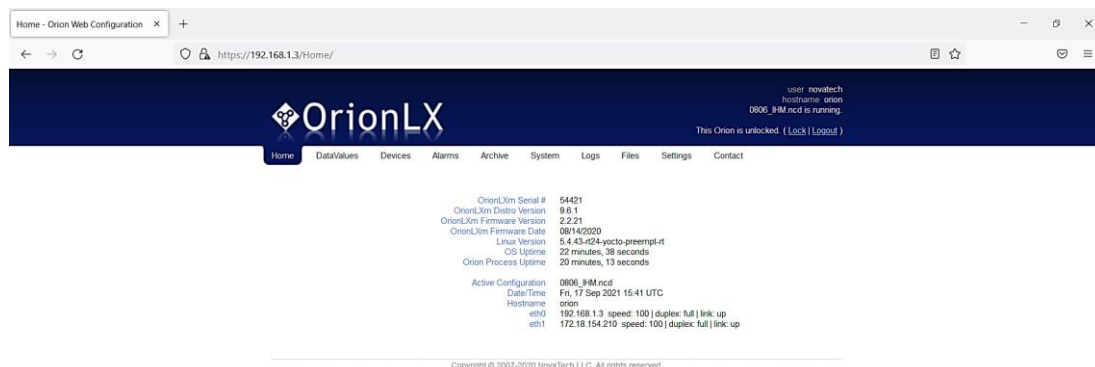


Figura 136. Página web principal del ORION para Prueba #4. Fuente: Autores.

En la barra de herramientas dirigirse a la opción “Files”, luego la opción “Select Files”, y cargar el archivo que contiene el diagrama unifilar tal como se muestra en la Figura 137.

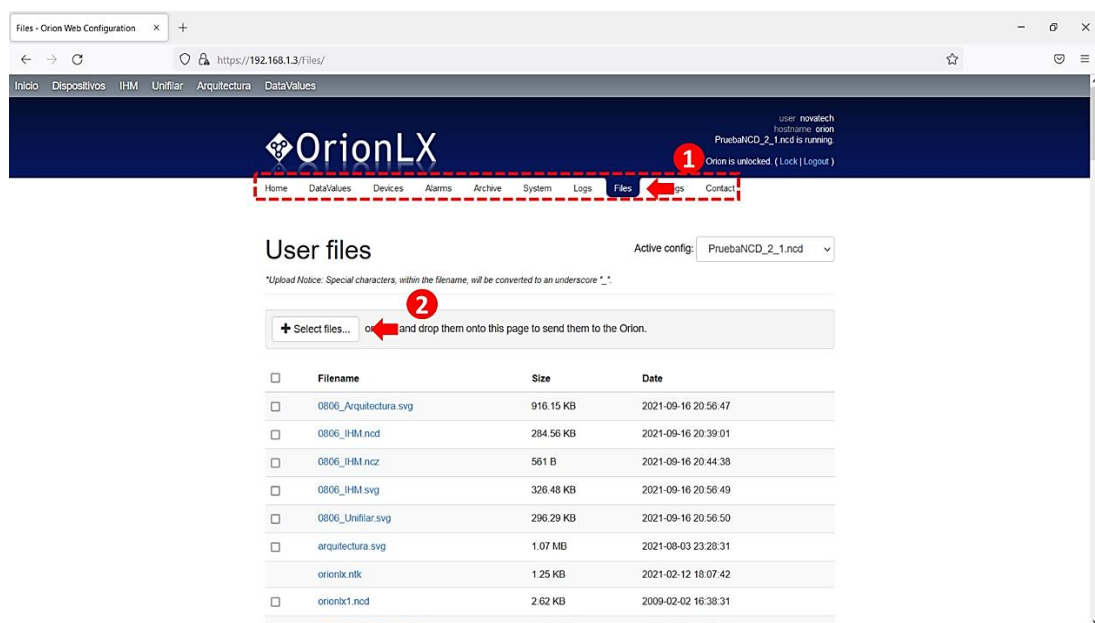


Figura 137. Enviar Diagrama Unifilar a la ORION para Prueba #4. Fuente: Autores.

Ya con los archivos cargados, se tiene que habilitar la página web (véase la Figura 138), se requiere realizar los siguientes pasos:

1. En la barra de menú en la opción “Settings”.
2. En la parte de Web Page, se escoge la opción “WebUI”, inmediatamente, se abre la siguiente pestaña la cual permite habilitar la página web del Diagrama Unifilar.
3. Habilitar el archivo del Diagrama Unifilar, en este caso “0806\_Unifilar\_Practica”, y luego clic en “Save”.

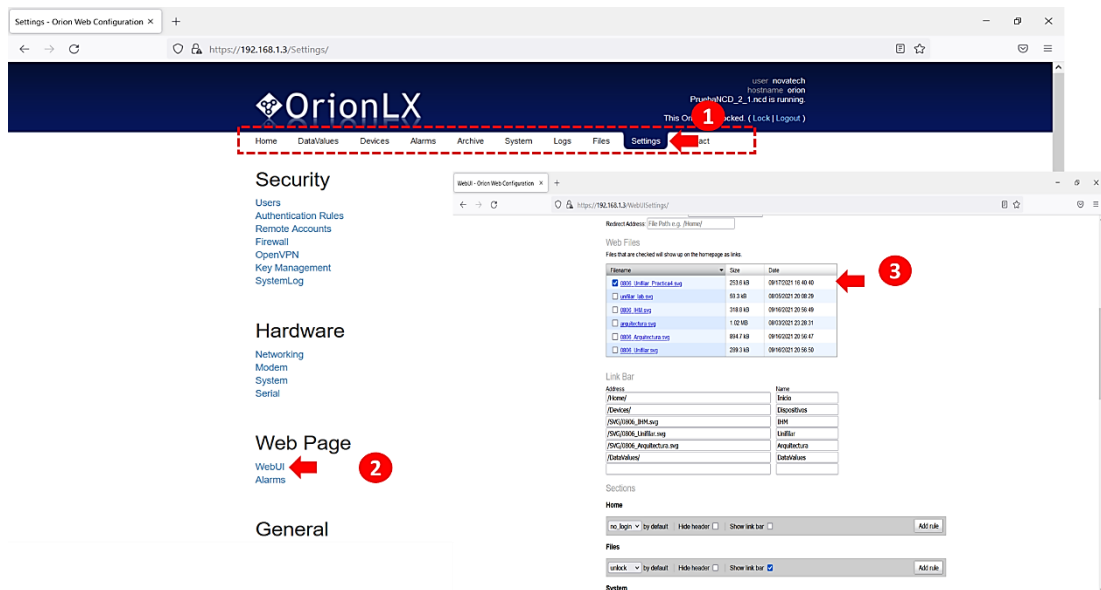


Figura 138. Pasos para habilitar la página Web para Prueba #4. Fuente: Autores.

En el menú en la opción de “Devices”, se observa de manera porcentual la comunicación del IED con la RTU, como se observa en la Figura 139, el 100% de datos son transmitidos con éxito.

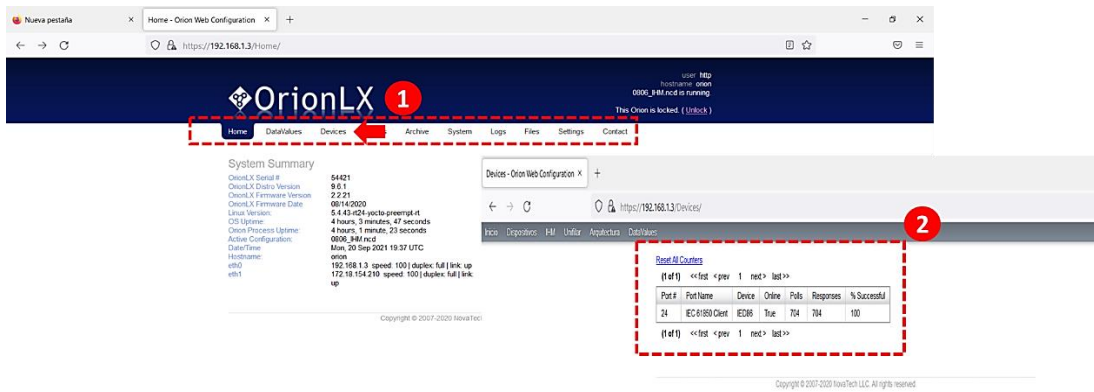


Figura 139. Verificación de la Comunicación en la ORION para Prueba #4.

Verificada la comunicación se abre la página web donde se encuentra el Diagrama Unifilar, en la siguiente Figura 140, se puede observar los valores de medición y estado del IED, de esta manera se da por culminada esta práctica.

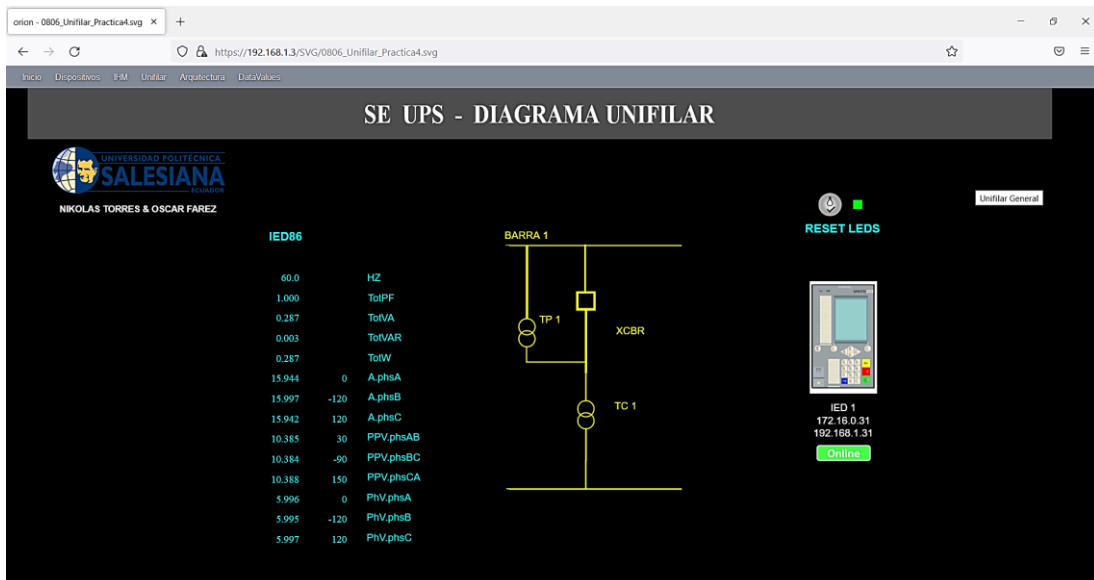


Figura 140. Diagrama unifilar con el monitoreo de datos para Prueba #4. Fuente: Autores.

#### 4.4.4.5. Conclusiones

La creación del HMI ayuda a una mejor interacción del usuario con el sistema, por tal razón, es necesario crear una interfaz amigable, sencilla e interactiva.

El manejo del HMI facilita la operación y monitorización de los equipos que se encuentran en campo. Además, se puede visualizar desde el entorno web de la RTU mediante cualquier dispositivo inteligente.

#### **4.4.4.6. Recomendaciones**

Al crear un HMI tener en cuenta la visualización de datos y gráficos ya que la interfaz es muy importante el manejo de colores y tamaños, para ofrecer una mayor visibilidad de sus operaciones y eventos con el fin de obtener un mayor rendimiento.



#### **4.4.5. Prueba #5 - Manejo de mensajería y alarmas**

##### **4.4.5.1. Objetivos**

- Habilitar las alarmas y los archivos, ya que estos son importantes en el funcionamiento de todo el sistema.
- Obtener un registro de las alarmas accionadas por eventos predispuestos.

##### **4.4.5.2. Recursos**

- Switch industrial GREYHOUND
- RTU Orion LXM
- IED
- PC
- Cables de red
- Software NCD
- Software Inkscape™
- OMICRON® CMC 356

##### **4.4.5.3. Descripción y funcionamiento**

El uso de alarmas y archivos es muy importante en el funcionamiento del sistema por lo que de igual manera se tiene que mapear los nodos lógicos que van a ser designados para cuando ocurra un evento.

Al momento de generarse una alerta, las alarmas tienen prioridad y se ven reflejadas con una etiqueta y un sonido predeterminado, y al mismo tiempo se genera un reporte de archivo el cual contiene información del evento.

##### **4.4.5.4. Desarrollo**

###### **Configuración del módulo AAR**

Para incorporar el complemento AAR (véase la Figura 141), se debe seguir los pasos que a continuación se detallan:

1. Clic en “Configure”.
2. Clic en “Add Ons”.
3. Clic en “Alarm/Archive/Retentive”.
4. Se abre la ventana donde se va a generar la configuración de las alarmas y archivos.

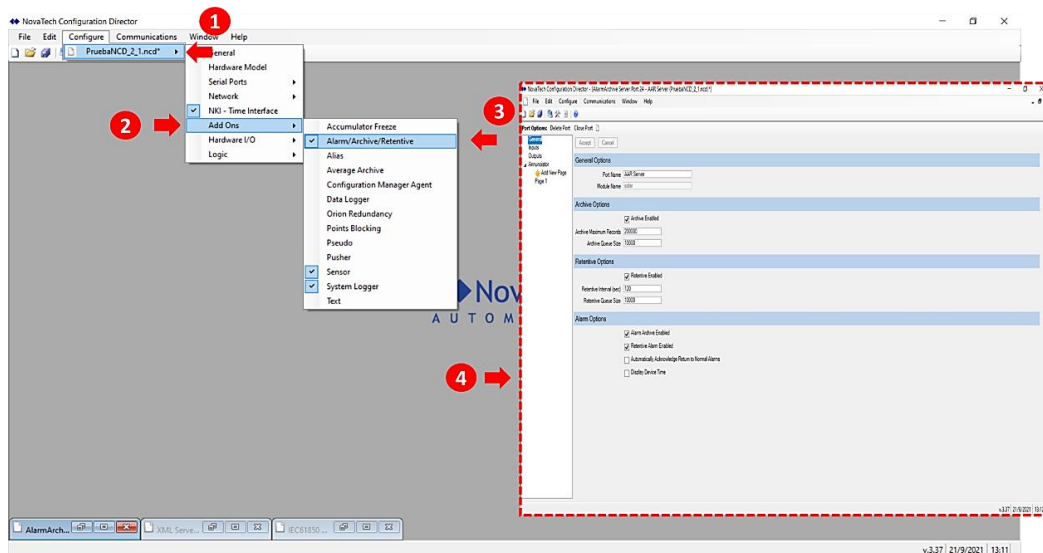


Figura 141. Pasos para configurar el complemento AAR para Prueba #5. Fuente: Autores.

Los LN que se van a mapear son de aviso disparo y de comunicación, ya que cuando se produce una falla en seguida se accionan las alarmas, y por la parte de comunicación cuando el dispositivo se desconecte o pierda comunicación lanza una alerta y así se generan los archivos de los eventos para así tener un control del sistema.

A continuación, se listan los pasos a seguir (véase la Figura 142):

1. Seleccionar los LN que se deben asociar a una alarma.
2. Los nodos seleccionados pasarlos a la parte derecha.
3. Clic en “Alarm Enable”.
4. Guardar.

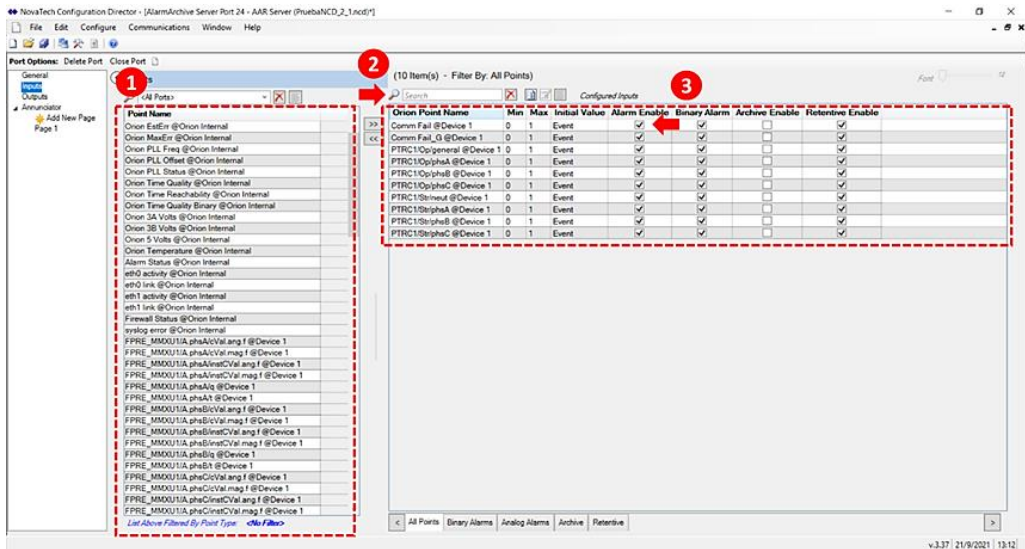


Figura 142. Configuración de alarmas en módulo AAR para Prueba #5. Fuente: Autores.

En la parte izquierda en la opción de “Annunciator”, crear una nueva página para tipo de alarmas que se requiera en el sistema, para esta práctica se genera dos páginas la una de protecciones y la otra de comunicación.

Para generar las páginas, se han adoptado los siguientes pasos:

1. Seleccionar Page1 y se cambia el nombre al que desean.
2. Los LN mapeados anteriormente se pasan a la matriz del lado derecho, véase la Figura 143.
3. La matriz generada es la forma como se va a visualizar las alarmas en el entorno Web de la RTU.
4. Guardar.

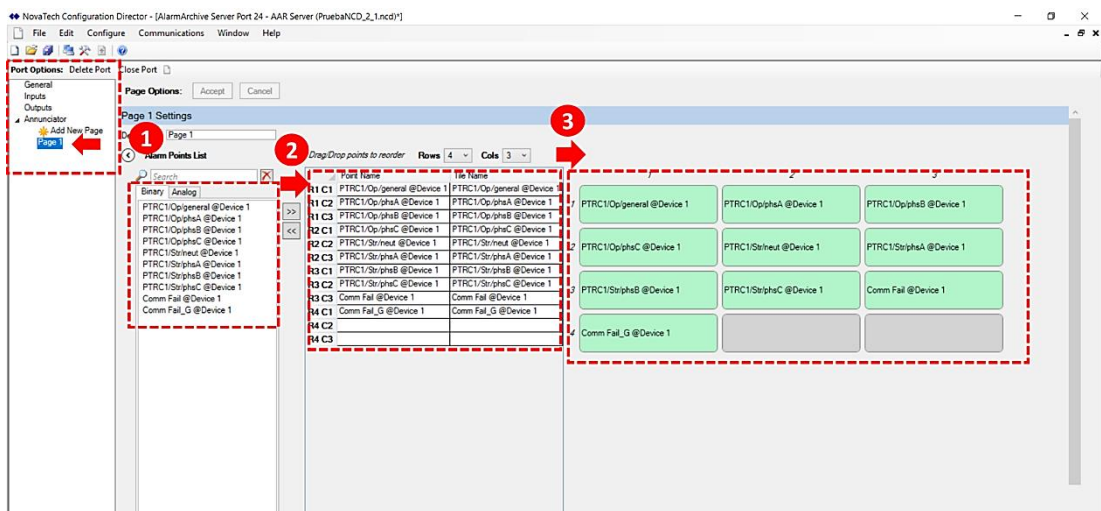


Figura 143. Pasos para crear la matriz de eventos para Prueba #5. Fuente: Autores.

Como se puede observar en la Figura 144, están creadas las matrices de las alarmas de Protección y Comunicación.

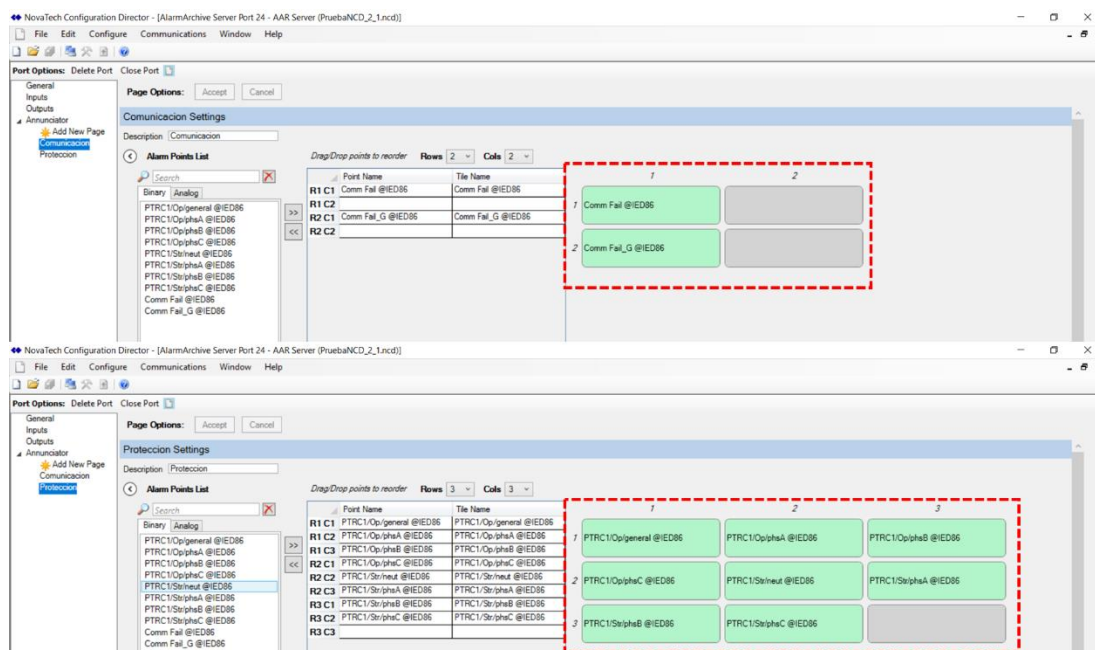


Figura 144. Páginas de alarmas para comunicación y protección para Prueba #5.  
Fuente: Autores.

### Interfaz del módulo AAR en la WEBserver

En la página web “<https://192.168.1.3/AlarmSettings/>” (véase la Figura 145) se activan las alarmas, para la configuración de las alarmas se designa un color a cada estado de la alarma y un sonido de alerta.

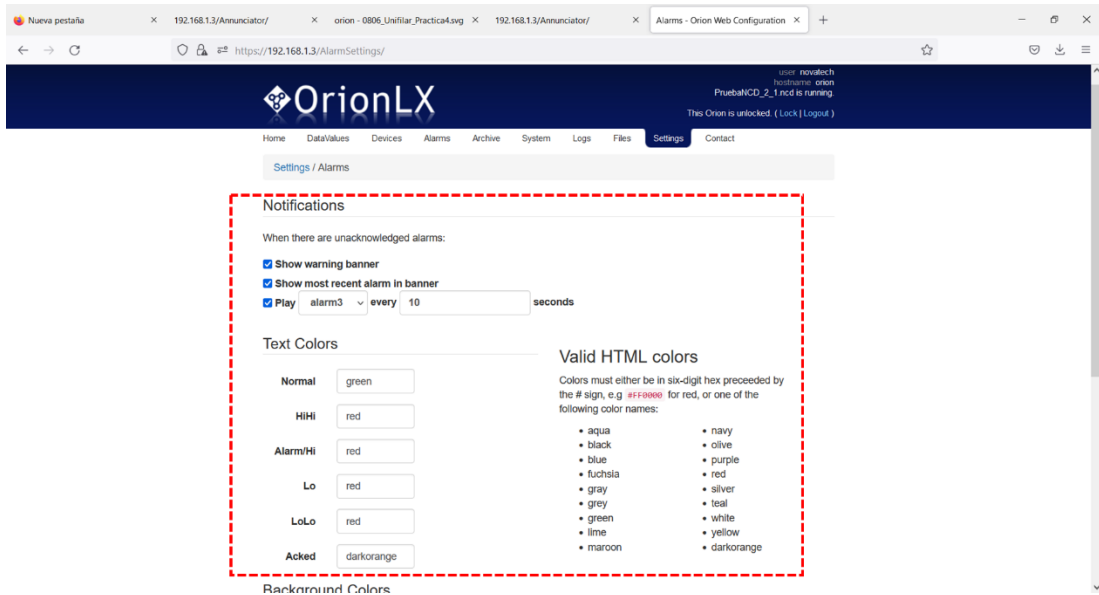


Figura 145. Configuración de las notificaciones de eventos para Prueba #5. Fuente: Autores.

## Funcionamiento de las Alarmas y Archivos

Se puede observar en la Figura 146, las alarmas se encuentran en verde esto quiere decir, que no tienen ningún problema de comunicación.

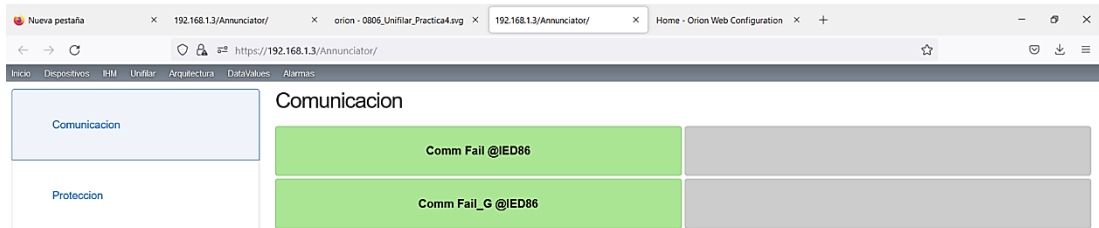


Figura 146. Visualización de alarmas en estado normal para Prueba #5. Fuente: Autores.

Se procede a desconectar el cable de comunicación, y en la Figura 147 se observa el comportamiento de la alarma.

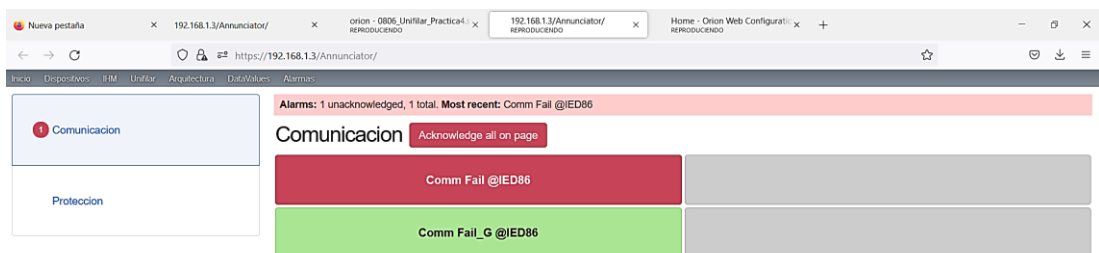


Figura 147. Visualización de alarmas en estado activo para Prueba #5. Fuente: Autores.

Cuando se genera la alarma, inmediatamente, se crea un archivo con la información del evento generado, tal como se observa en la Figura 148.

ID	Time	Device Time	Point Name	Alias	Value	Online	DTime
43	2021-09-21 20:43:59.591+00	2021-09-21 20:43:59.591+00	LLN0LEDs/Oper ctVal @IED06		1	offline	no
42	2021-09-21 20:35:56.389+00	2021-09-21 20:35:56.344+00	LLN0LEDs/Oper ctVal @Device 1		1	offline	no
41	2021-09-21 20:29:21.929+00	2021-09-21 20:29:21.91+00	LLN0LEDs/Oper ctVal @Device 1		0	offline	no
40	2021-09-21 20:28:48.79+00	2021-09-21 20:28:48.769+00	LLN0LEDs/Oper ctVal @Device 1		1	offline	no
39	2021-09-21 19:59:52.098+00	2021-09-21 19:59:52.077+00	LLN0LEDs/Oper ctVal @Device 1		1	offline	no
38	2021-08-05 20:28:18.913+00	2011-01-01 01:08:59.111+00	Siemens31 Disparo General @Siemens31		0	online	no
37	2021-08-05 20:28:18.398+00	2011-01-01 01:08:59.043+00	Siemens31 Disparo General @Siemens31		1	online	no
36	2021-08-05 20:20:51.621+00	2011-01-01 01:01:31.781+00	Siemens31 Disparo General @Siemens31		0	online	no
35	2021-08-05 20:20:51.099+00	2011-01-01 01:01:31.712+00	Siemens31 Disparo General @Siemens31		1	online	no
34	2021-08-05 20:18:19.512+00	2011-01-01 00:58:59.666+00	Siemens31 Disparo General @Siemens31		0	online	no

Figura 148. Generación de Archivos para Prueba #5. Fuente: Autores.

#### 4.4.5.5. Conclusiones

El uso de alarmas es importante en el funcionamiento de un sistema, ya que permite estar al corriente de cualquier alerta que se genera en ese instante, y poder dar una solución en el menor tiempo posible.

#### 4.4.5.6. Recomendaciones

Mapear bien los nodos lógicos que se quieren asociar a las alarmas, por eso es importante desde el comienzo del proyecto tener en cuenta el alcance que se quiere obtener, para que todos los nodos lógicos mapeados sean los necesarios.

#### 4.4.6. Prueba #6 – Usuarios y Permisos

##### 4.4.6.1. Objetivos

- Crear usuarios con cierto nivel de acceso al HMI.
- Configurar un conjunto de privilegios según el nivel de acceso del usuario.
- Familiarizarse con el entorno de configuración de la ORION WEBserver.

##### 4.4.6.2. Recursos

- Switch industrial GREYHOUND
- RTU Orion LXM
- PC
- Cables de red

##### 4.4.6.3. Descripción y funcionamiento

La administración de privilegios en perfiles y grupos de usuarios es una excelente herramienta para mejorar la seguridad del sistema evitando el acceso de usuarios no deseados en áreas comprometedoras. Estas buenas prácticas resultan de gran utilidad en todo sistema, garantizando la estabilidad y confiabilidad del mismo.

Las normas de autenticación establecen criterios para los inicios de sesión fallidos y las contraseñas inválidas, tales criterios se denotan a continuación:

- Las reglas de bloqueo de usuario (Véase la Tabla 8) definen el número de intentos de contraseña fallidos consecutivos antes de que se bloquee o deshabilite una cuenta de usuario. Esta es una configuración importante para evitar que usuarios no autorizados accedan al Orion LXM.

Tabla 8. Aspectos para la regla de bloqueo de usuarios.

<b>Función</b>	<b>Descripción</b>
Reglas de bloqueo de usuarios	Habilitar / deshabilitar las reglas de bloqueo. Cuando esta configuración está activada, Orion LXM utilizará las siguientes configuraciones para decidir cuándo deshabilitar a un usuario debido a intentos fallidos de inicio de sesión. Predeterminado: Activado
Max. Intentos de acceso	Define el número de intentos de contraseña fallidos consecutivos antes de que se bloquee o deshabilite la cuenta de usuario. Predeterminado: 5
Bloquear permanentemente	Indica al Orion LXM que desactive permanentemente una cuenta de usuario después de varios intentos fallidos. Predeterminado: desactivado
Tiempo hasta desbloquear (seg)	Define la cantidad de segundos que Orion LXM permanecerá bloqueado. Predeterminado: 172800 segundos (2 días)
Tiempo de bloqueo temporal (seg)	La cantidad de tiempo entre intentos fallidos para que la Orion LXM bloquee. Predeterminado: 3 segundos

- Las reglas para la contraseña configuran la cantidad de dígitos y tipos de caracteres se requieren en una contraseña (véase la Tabla 9). Una contraseña larga con una combinación de mayúsculas, minúsculas, números y caracteres especiales es la más segura. Esta verificación de conformidad de contraseña se ejecuta cuando se agrega un nuevo usuario o cuando un usuario cambia la contraseña.

Tabla 9. Aspectos para la regla de contraseñas.

<b>Función</b>	<b>Descripción</b>
Reglas de contraseña	Activar/desactivar las reglas de contraseña. Cuando esta configuración está activada, Orion LXM verificará las contraseñas de los usuarios para asegurarse de que sigan las reglas definidas a continuación. Predeterminado: Seleccionado (Activado)
Longitud min.	Define el número mínimo de caracteres que debe tener una contraseña para ser aceptada. Predeterminado: 8
Min. Dígitos	Define el número mínimo de dígitos numéricos (0-9) que se deben utilizar en una contraseña. Predeterminado: 1
Min. Mayúsculas	Define el número mínimo de letras mayúsculas (A-Z) que se deben utilizar en una contraseña. Predeterminado: 1
Min. Minúsculas	Define el número mínimo de letras minúsculas (a-z) que se deben utilizar en una contraseña. Predeterminado: 1
Min. Caracteres especiales	Define el número mínimo de dígitos de caracteres especiales que se deben utilizar en una contraseña. Los caracteres especiales incluyen: ! @ # \$ % ^ & * () +, -, . / : ; <=> ? “ [ ] _ ` {   } ~ Predeterminado: 1
Max. Repetidos	Define el número máximo de veces que se puede repetir un carácter.
difok	Establece el número mínimo de caracteres que deben ser diferentes al cambiar una contraseña. Predeterminado: 5
Historial de contraseñas	Define el número de cambios de contraseña antes de que se pueda reutilizar una contraseña utilizada anteriormente. Predeterminado: 3

Se establecen permisos de usuarios según se observa en la Tabla 10. Considerando la previa existencia de 2 súper usuarios tales como “root” y “novatech”, los cuales están establecidos de fábrica y recordando que el banco de pruebas es de uso didáctico.

Tabla 10. Permisos de Usuarios.

<b>Función</b>	<b>Supervisor</b>	<b>Operador</b>	<b>Observador</b>
Reconocimiento de alarmas	x	x	
Programación	x		
Forzar entradas y salidas de la Orion LXM	x	x	
Casillas de control	x	x	
Visualización de HMI	x	x	x
Visualización de alarmas y base de datos	x	x	x
Modificar y guardar parámetros de red	x		
Crear y eliminar usuarios	x		
Más funciones	x		



#### 4.4.6.4. Desarrollo

Para definir los usuarios, primero se debe realizar ajustes generales de la interfaz web, ello implica dirigirse como súper usuario “novatech” al menú “Settings”, a continuación se listan los pasos a seguir:

1. En la sección “Web Page” seleccionar “WebUI”.
2. Seleccionar los archivos SVG para convertirlos en acceso directo desde la página principal.
3. Seleccionar las páginas para mostrar en la barra de enlaces, véase la Figura 150.

The screenshot shows the OrionLX Settings page. The 'Web Page' section is active, and the 'WebUI' option is selected. The 'Web Files' table lists the following files:

Filename	Size	Date
<input type="checkbox"/> 0806_Unifilar_Practica4.svg	253.6 kB	09/21/2021 20:43:10
<input type="checkbox"/> unifilar_lab.svg	59.3 kB	08/05/2021 20:08:29
<input checked="" type="checkbox"/> 0806_HMI.svg	318.8 kB	09/16/2021 20:56:49
<input type="checkbox"/> arquitectura.svg	1.02 MB	08/03/2021 23:28:31
<input checked="" type="checkbox"/> 0806_Arquitectura.svg	894.7 kB	09/16/2021 20:56:47
<input checked="" type="checkbox"/> 0806_Unifilar.svg	288.3 kB	09/16/2021 20:56:50

The 'Link Bar' table lists the following links:

Address	Name
<input type="text" value="/Home/"/>	<input type="text" value="Inicio"/>
<input type="text" value="/Devices/"/>	<input type="text" value="Dispositivos"/>
<input type="text" value="/DataValues/"/>	<input type="text" value="DataValues"/>
<input type="text" value="/Anunciador/"/>	<input type="text" value="Anunciador de eventos"/>
<input type="text" value="/SVG/0806_HMI.svg"/>	<input type="text" value="HMI"/>

Figura 149. Ajustes realizadas a la barra de enlaces para Prueba #6. Fuente: Autores.

4. Cada sección tiene tres parámetros que se pueden personalizar: el cuadro desplegable para la configuración de acceso, Ocultar encabezado y Mostrar barra de vínculos. Seleccionar según convenga, véase la Figura 150.

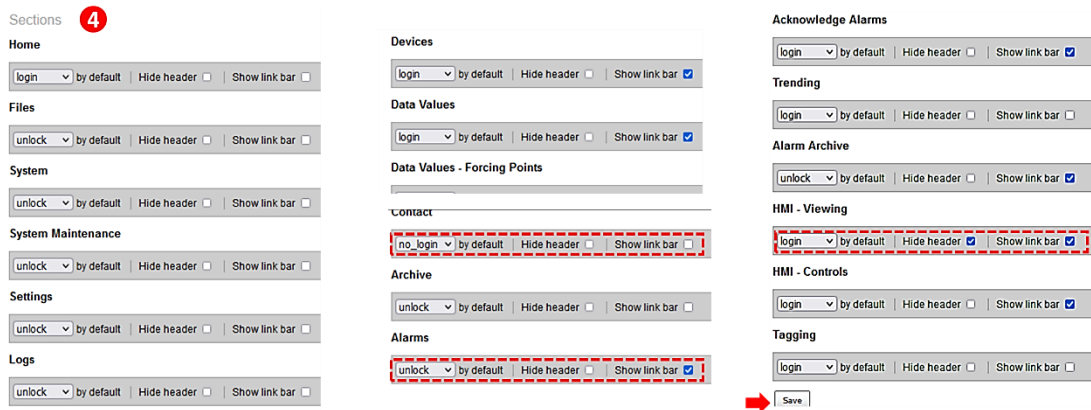


Figura 150. Opciones de visualización y seguridad de acceso para Prueba #6. Fuente: Autores.

Luego, se debe establecer criterios para los inicios de sesión fallidos y las contraseñas inválidas; para ello se debe dirigir a la sección “Security” y seleccionar “Authentication Rules”, y en base a la Tabla 8 ajustar la sección de bloqueo de usuario “User Lockout”, en cambio con la Tabla 9 ajustar las reglas de contraseña “Password Rules”. Finalmente, guardar los cambios, tal como se muestra en la Figura 151.

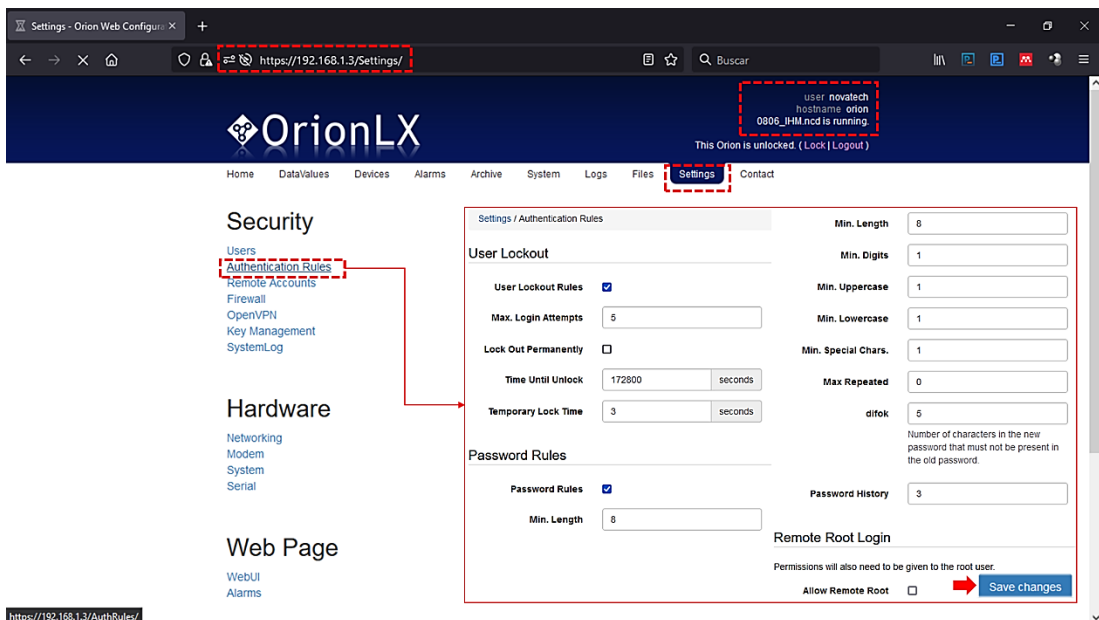


Figura 151. Reglas de autenticación para Prueba #6. Fuente: Autores.

A continuación, se listan los pasos para crear los usuarios y asignarles privilegios:

1. Dirigirse a la sección “Security” y seleccionar “Users”.
2. Ajustar el nombre de usuario y contraseña, además se puede establecer una cantidad de días de validez, véase la Figura 152.
3. Seleccionar los permisos marcando las casillas, en función del privilegio de usuario, en base a la Tabla 10.

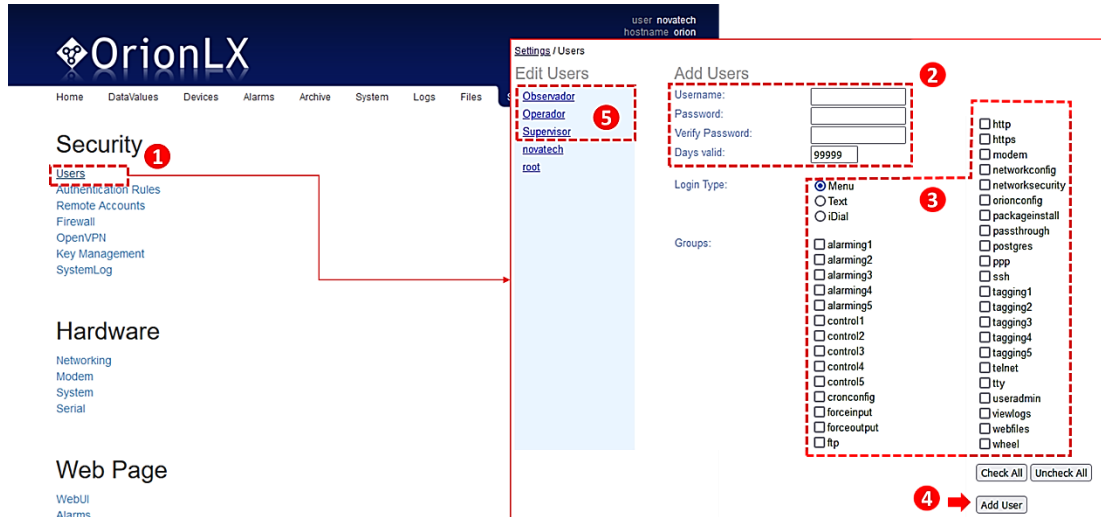


Figura 152. Pasos para añadir privilegios a los usuarios creados para Prueba #6.  
Fuente: Autores.

En la Figura 153 se puede visualizar los privilegios asignados a los usuarios Supervisor, Operador y Observador respectivamente.

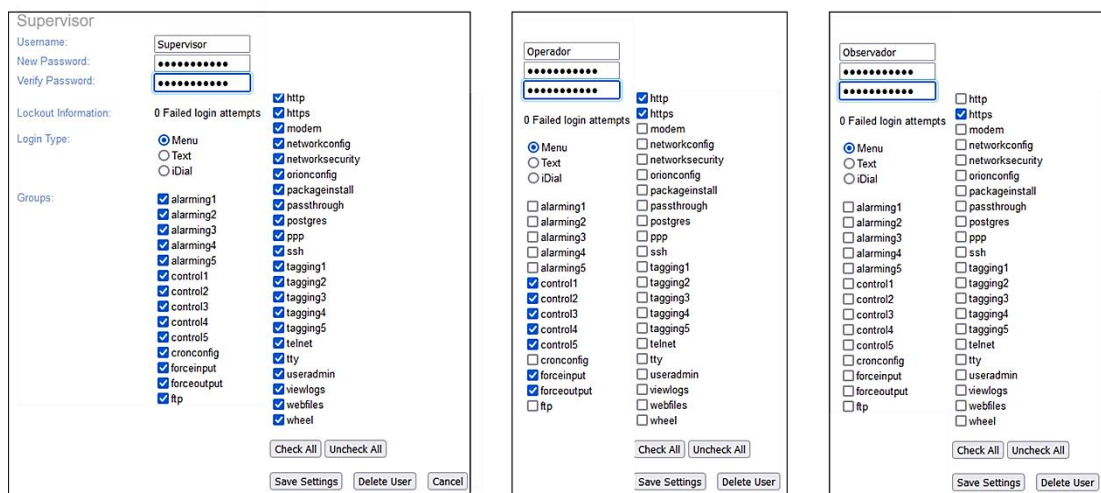


Figura 153. Ajustes realizados a los usuarios creados para la Prueba #6. Fuente: Autores.

Luego de haber configurado los privilegios de usuario y demás, se tiene la nueva interfaz de la página inicial del WEBserver, y se visualiza en la Figura 154, la cual solicita un “Usuario” y “Clave de acceso” para el ingreso al sistema, además de mostrar un texto personalizado de bienvenida.

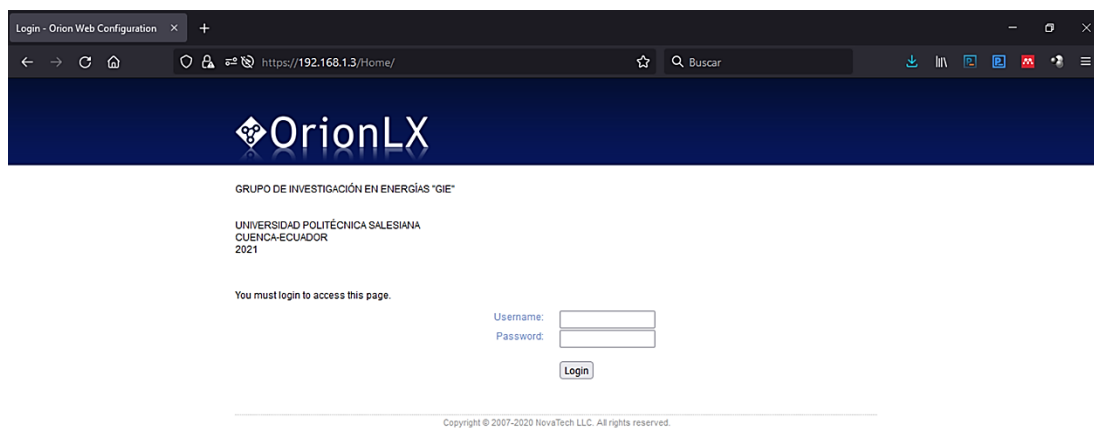


Figura 154. Ventana inicial del WEBserver para Prueba #6. Fuente: Autores.

Finalmente se visualiza el comportamiento del WEBserver ante la configuración de los privilegios de usuarios, véase la Figura 155, en este caso se accedió con el usuario “Observador”, a continuación, se exponen ciertos aspectos generados por los privilegios:

- a. Al momento de iniciar sesión, se tiene acceso a ciertas páginas en función de los privilegios asignados, sin embargo, la Orion continúa bloqueada, para desbloquear totalmente se debe dar clic en “Unlock” y volver a iniciar sesión. Cabe mencionar que para cerrar sesión se debe dar clic en “Logout”.
- b. Algunos menús y características están bloqueados debido a los permisos asignados a cada usuario, por lo que presenta un aviso mencionando que el usuario no tiene el correcto grupo de privilegios asignados para tal acción, o en su efecto solicita el inicio de sesión de otro usuario.
- c. Si el usuario que ha iniciado sesión no tiene permiso para administrar usuarios, la página “Cambiar contraseña” se muestra cuando se accede al menú “Settings” opción “Users”. Esta es la única opción disponible para usuarios sin autorización de gestión de usuarios.

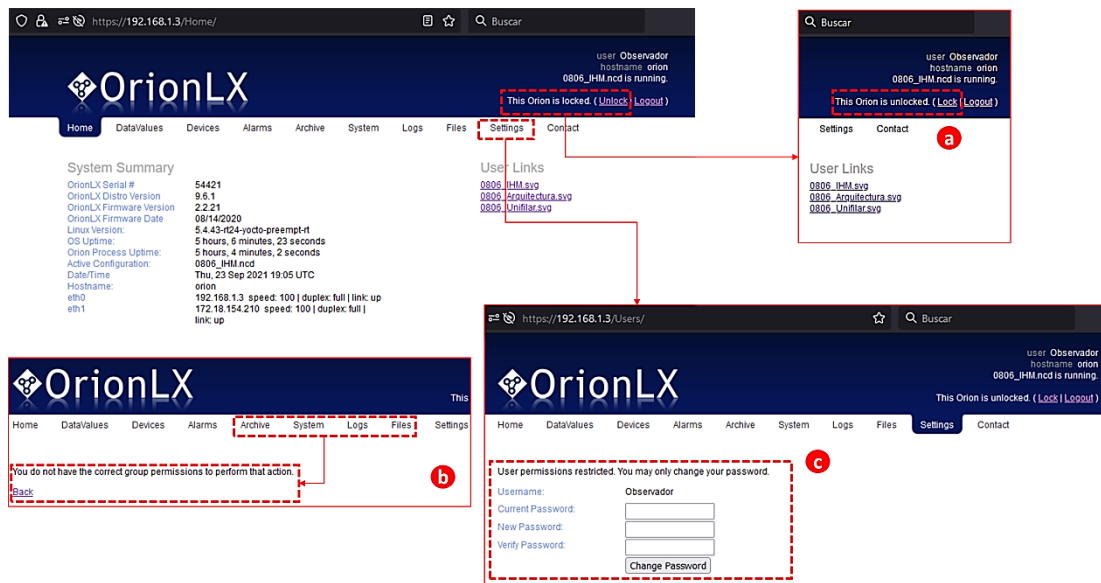


Figura 155. Ventanas orientadas al privilegio de usuarios para Prueba #6. Fuente: Autores.

#### 4.4.6.5. Conclusiones

La creación de usuarios permite mejorar la seguridad del sistema, garantizando su estabilidad y confiabilidad. Además, se debe verificar que los usuarios tengan el correcto grupo de privilegios o permisos asignados.

#### 4.4.6.6. Recomendaciones

Revisar los diversos privilegios que puede asignar el supervisor, y demás usuarios; asegurando así la integridad de la información del sistema.

#### 4.4.7. Prueba #7 – Comparativa entre la señal de disparo por cable y señal de disparo por GOOSE

##### 4.4.7.1. Objetivos

- Analizar el rendimiento temporal de la mensajería GOOSE frente a un sistema convencional cableado
- Configurar el simulador de pruebas CMC para simular fallos estándar de la industria.

##### 4.4.7.2. Recursos

- Switch industrial GREYHOUND
- IED's
- PC
- Cables de red
- OMICRON® Test Universe
- OMICRON® CMC 356

##### 4.4.7.3. Descripción y funcionamiento

La comparación del rendimiento temporal entre un GOOSE y las señales analógicas cableadas, conlleva el uso de la unidad de prueba OMICRON® CMC 356, para la inyección de corrientes en los IED's. Además, esto permitirá comprender los beneficios que brinda el estándar.

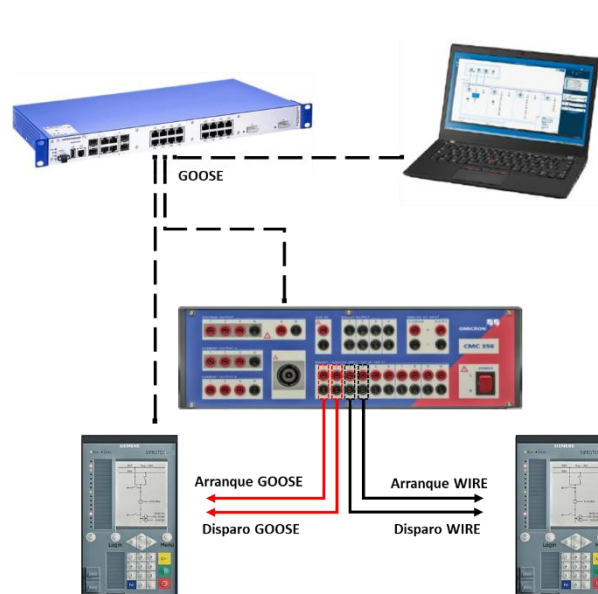


Figura 156. Esquema de conexionado para Prueba #7. Fuente: Autores.

La Figura 156 muestra el conexionado de los dispositivos utilizados, tanto para la mensajería GOOSE, como la conexión cableada para la detección del arranque y disparo ante el fallo.

#### 4.4.7.4. Desarrollo

El proceso de configuración empezaría con la programación de las funciones de protección y control de cada IED. Posteriormente, uno de los IED's debe configurarse la mensajería GOOSE para la comunicación con otros dispositivos. Cabe mencionar que estos pasos se encuentran en pruebas anteriores.

Después, configurar el simulador de pruebas de sobrecorriente de OMICRON®, y ajustar los parámetros eléctricos acorde a lo establecido en los IED's, tal como se observa en la Figura 157.

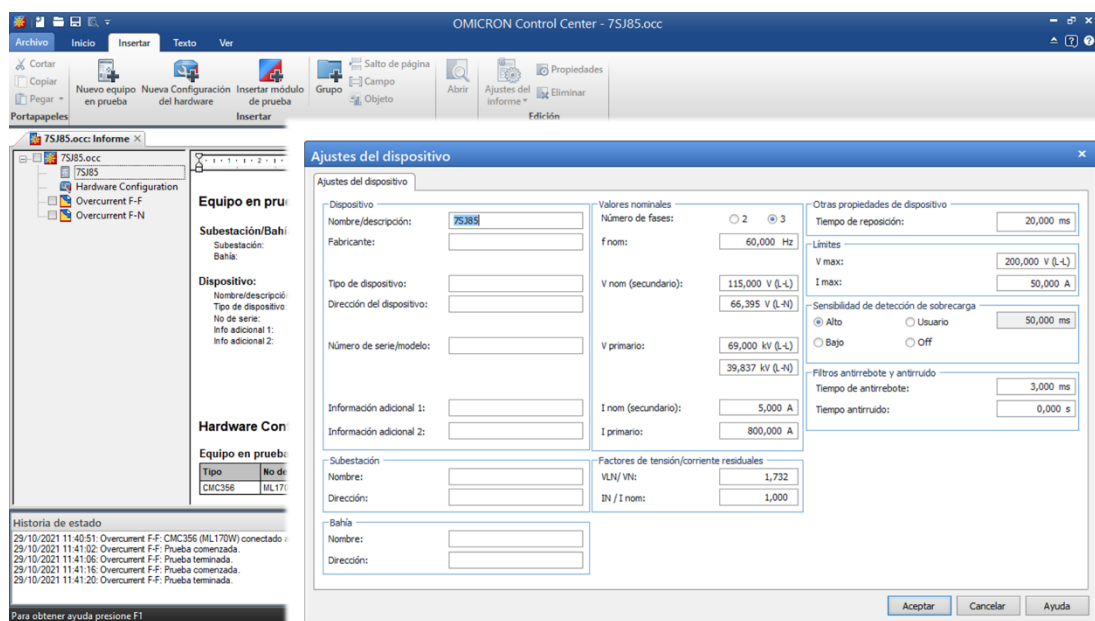


Figura 157. Configuración de parámetros eléctricos en Modulo “Control Center”, para Prueba #7. Fuente: Autores.

Después de esto, se procede a ejecutar el fallo, ya sea falla trifásica o entre fase y tierra. A la vez, se analiza la oscilografía generada; mediante el movimiento de los cursores se puede determinar el lapso de tiempo, entre un disparo mediante GOOSE y el disparo mediante cable. Véase la Figura 158.

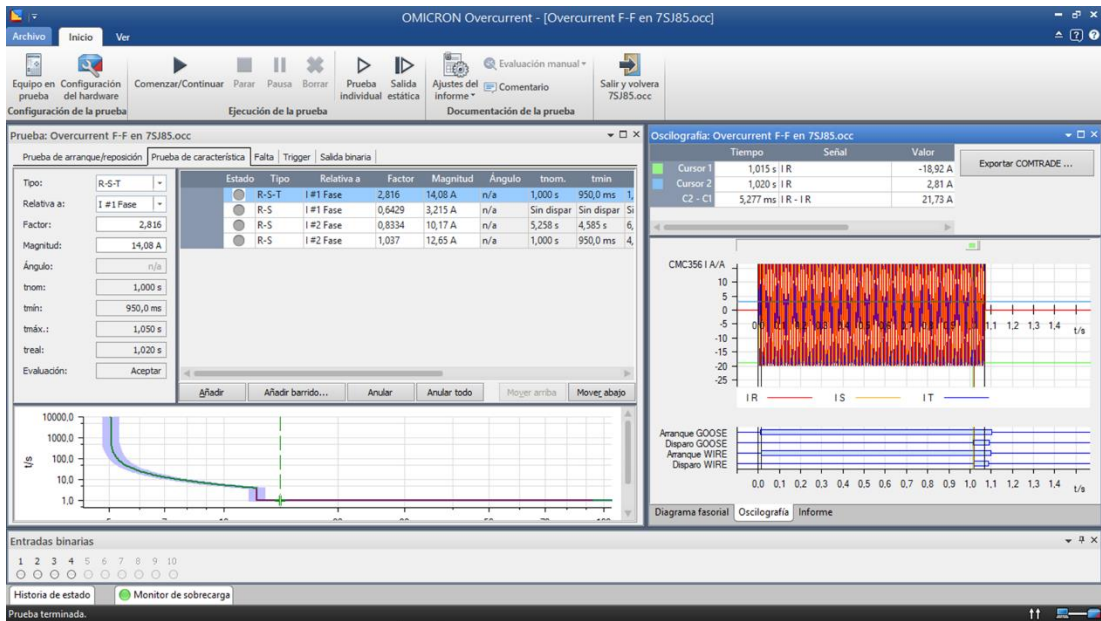


Figura 158. Ensayo de sobrecorriente trifásica, para Prueba #7. Fuente: Autores.

En la Figura 159 se amplía los resultados y se muestra claramente que la señal GOOSE de disparo es 5,277 ms mas rápida que la señal que viaja por el cable.

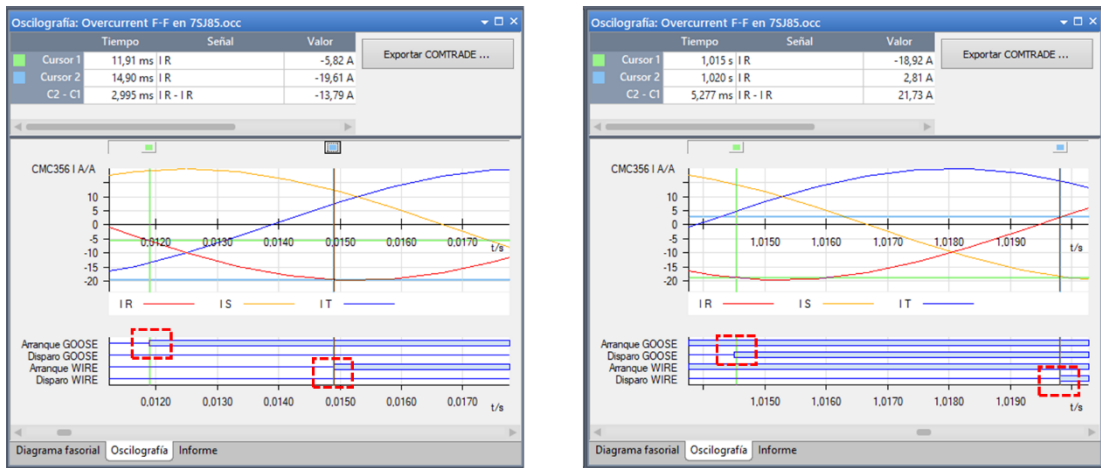


Figura 159. Diagrama ampliado que muestra la diferencia de tiempo entre la señal GOOSE y la señal WIRE, para Prueba #7. Fuente: Autores.



#### **4.4.7.5. Conclusiones**

Esta práctica ilustra que la tecnología GOOSE es superior a los métodos convencionales de comunicación, más aun, cuando las señales o los comandos de control se encuentran a largas distancias en la red.

#### **4.4.7.6. Recomendaciones**

Revisar y estudiar los distintos módulos que tiene la CMC 356, para el desarrollo de diversos ensayos en el campo de la IEC 61850.

#### **4.4.8. Prueba #8 - Envío remoto con el protocolo IEC 60870-5-101/104.**

##### **4.4.8.1. Objetivos**

- Utilizar el protocolo de servidor IEC 60870-5-10, quien se va a comunicar mediante un puerto TCP/IP.
- Con la herramienta de Wireshark se comprueba la transferencia de datos.

##### **4.4.8.2. Recursos**

- Switch industrial GREYHOUND
- IED's
- PC
- Cables de red
- OMICRON® Test Universe
- OMICRON® CMC 356

##### **4.4.8.3. Descripción y funcionamiento.**

El protocolo de servidor IEC 60870-5-101 se comunica a través de un puerto serie, y el protocolo de servidor IEC 60870-5-104 se comunica a través de un puerto TCP/IP. Este módulo de software permite que Orion funcione como una RTU, utilizando una conexión serie (RS-232, RS-485, fibra) o TCP entre la estación cliente y la RTU. Dependiendo de la configuración de Orion, se puede configurar para emular una sola RTU o múltiples RTU. Dado que cada RTU emulada tiene su propia dirección de RTU única, también es posible operar otras RTU en el mismo enlace de comunicaciones en serie.

Los datos devueltos al cliente en respuesta a sus sondeos se obtienen de cualquier número de dispositivos de campo, como PLCs, relés, contadores, HMIs, etc. Del mismo modo, cualquier comando enviado desde el cliente se envía al dispositivo final respectivo según lo configurado en el software de Orion. El protocolo(s) utilizado para comunicarse con los dispositivos finales de campo es independiente de 101/104. Esto permite una integración transparente de múltiples y diferentes dispositivos de campo como una única RTU o múltiples RTU, dependiendo de los requisitos de la aplicación.

##### **4.4.8.4. Desarrollo**

#### **Configuración del nuevo puerto para el protocolo IEC 60870-5-104**

Para incorporar este complemento se debe seguir los siguientes pasos (Véase la Figura 160):

1. Clic en “Configure”.
2. Clic en “Network”.
3. Clic en “Configure New Port”.
4. Se abre la ventana donde se va a generar la configuración del nuevo canal.

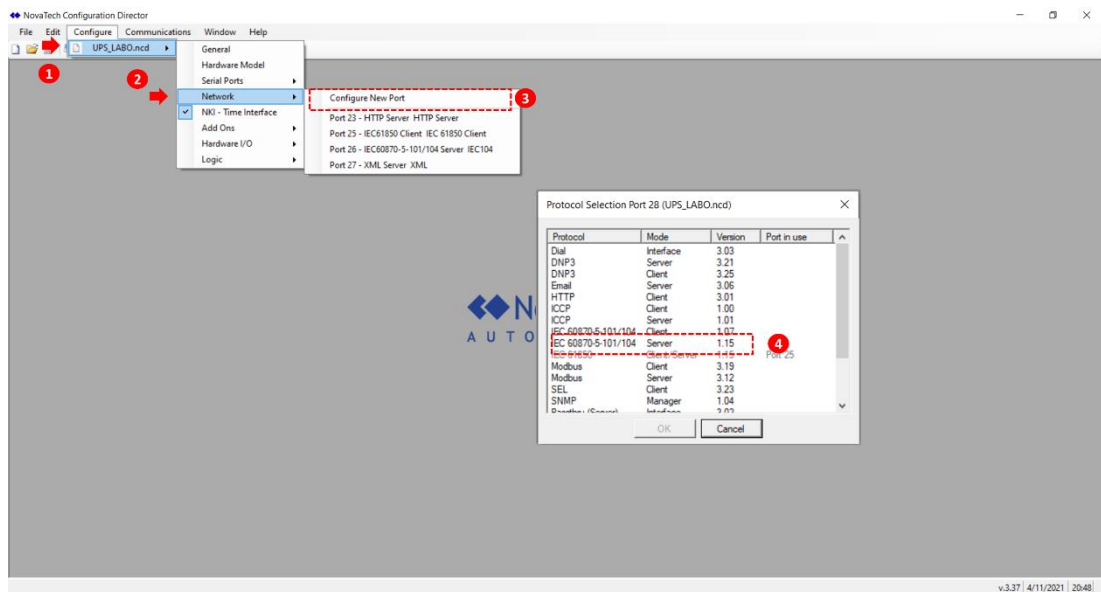


Figura 160. Pasos para configurar el puerto de protocolo IEC 60870-5-104. Fuente: Autores.

Se crea el nuevo puerto para la RTU, se da clic en “Add New RTU”, y se abre las siguientes opciones de “Inputs” y “Outputs”, se seleccionan todos los nodos que van a ser mapeados por el Canal TCP. Véase la Figura 161.

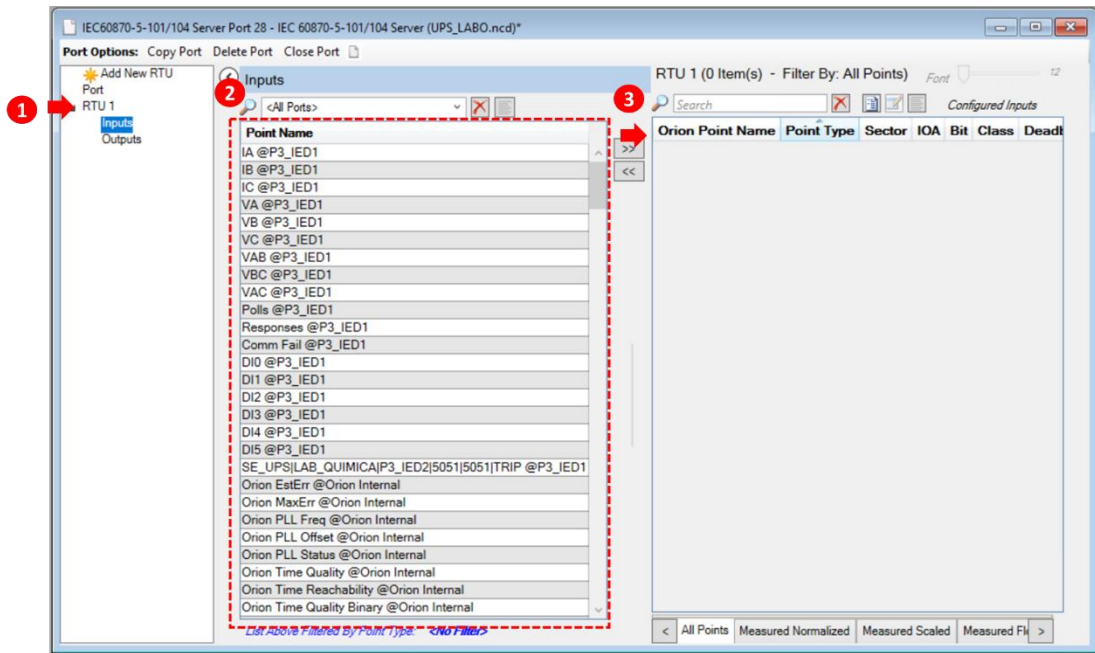


Figura 161. Pasos para la creación del puerto para la RTU. Fuente: Autores.

Para cargar los archivos “NCD” a la RTU, se realizan los siguientes pasos (Véase la Figura 162):

1. “File Transfer (PC a ORION)”, en el menú se escoge la opción 1.
2. Se carga los archivos que se van a subir y se da en “OK”.
3. Es necesario la activación del archivo para ello se selecciona el archivo que se va a subir.
4. Es necesario resetear la RTU, para que todos los cambios se realicen, se va a la opción “Full restar”

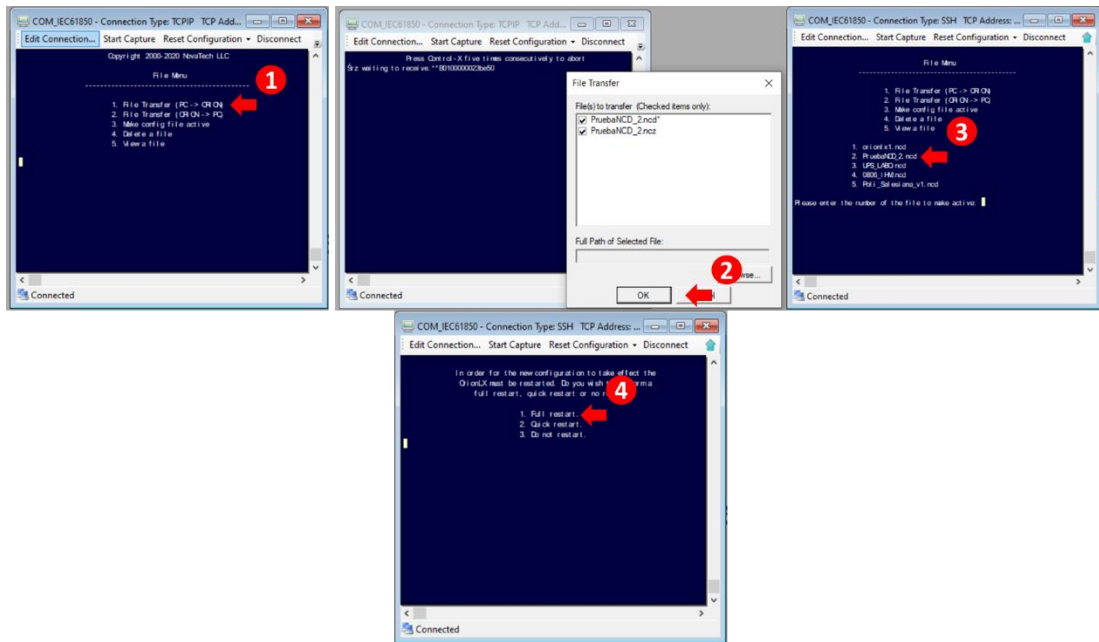


Figura 162. Pasos para cargar el archivo “NCD” a la RTU. Fuente: Autores.

En la siguiente Figura 163, se muestra el entorno web de la RTU, para entrar se va al navegador web y en la barra de búsqueda colocar la dirección IP, de la RTU en este caso “192.168.1.3” y se accede.

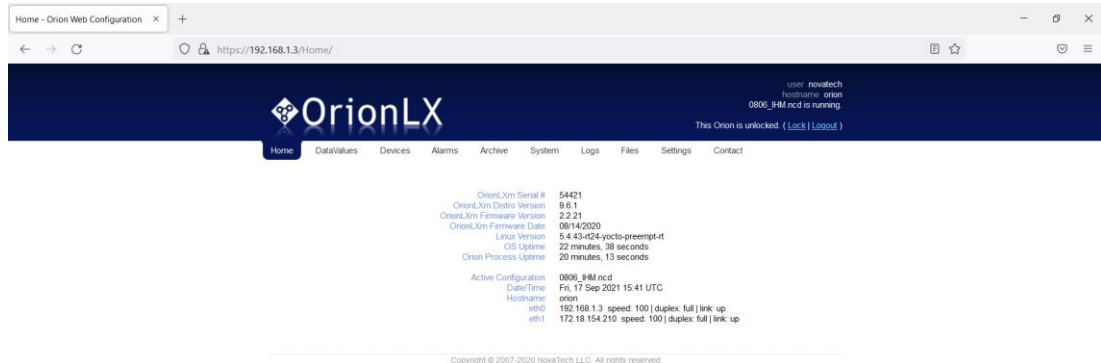


Figura 163. Página Web de la RTU. Fuente: Autores.

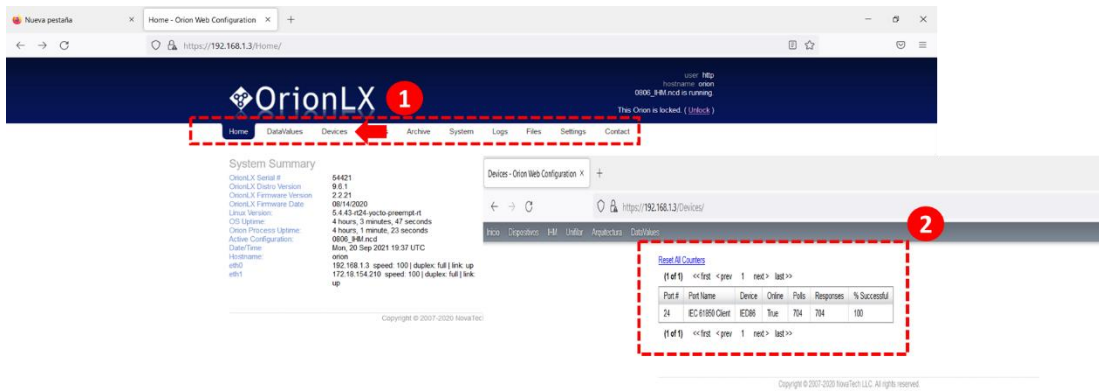


Figura 164. Verificación de la Comunicación. Fuente: Autores.

Verificada la comunicación se abre la página web donde se encuentra el “Devices”, en la siguiente Figura 164, se puede observar que se tiene un 100% de comunicación.

### Verificación del envío de datos con la Herramienta Wireshark

Como podemos observar en la Figura 165, en el puerto 26 con nombre IEC 608070-5-101/104 Server, se verifica la creación del puerto como tal con sus entradas y salidas de Datos.

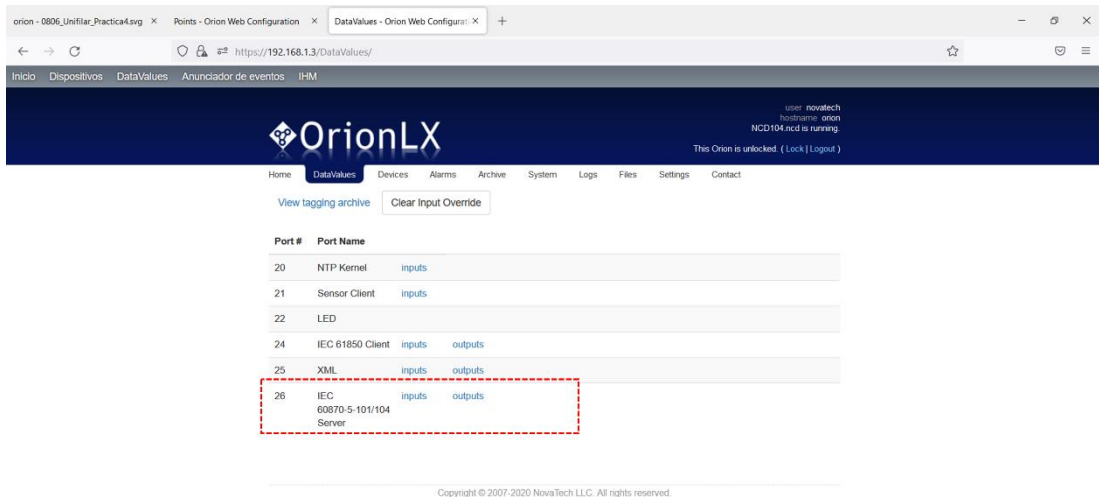


Figura 165. Página Web de la RTU. Fuente: Autores.

Con la ayuda del software Wireshark, se verifica el intercambio de datos mediante el protocolo establecido. Tal como se observa en la Figura 166.

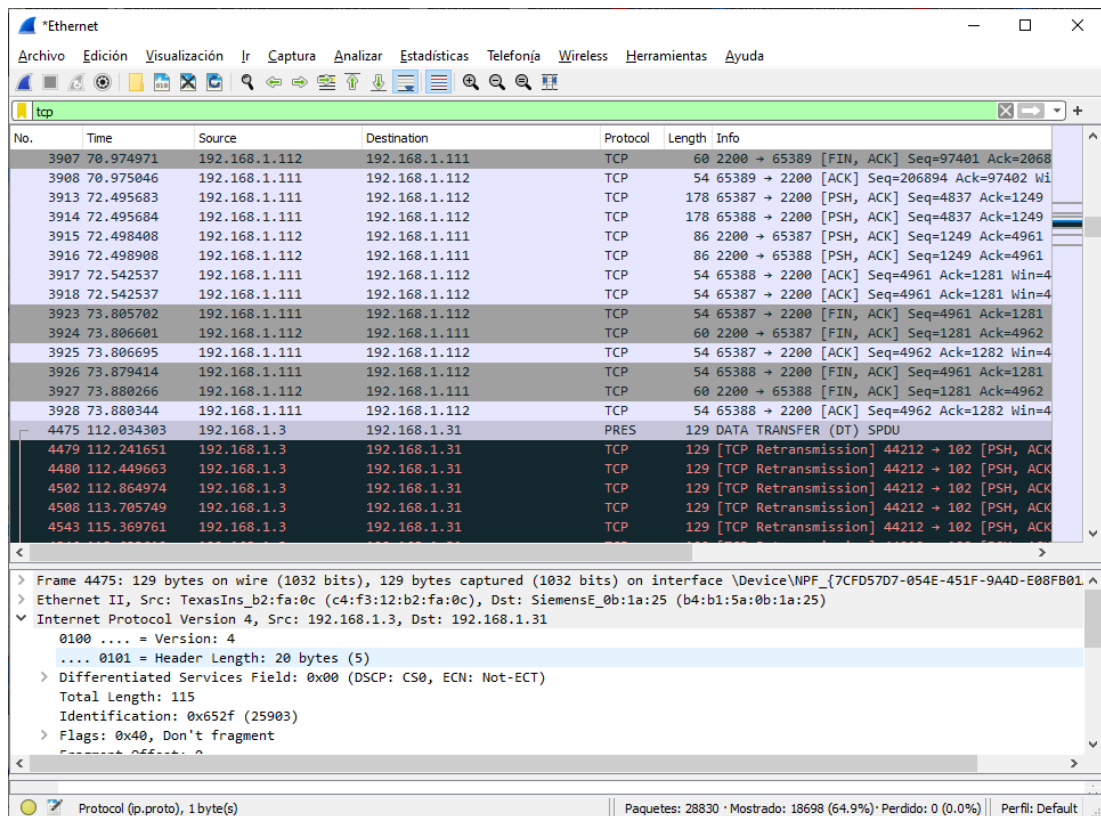


Figura 166. Mapeo de datos con Wireshark. Fuente: Autores.

#### 4.4.8.5 Conclusiones

Este protocolo nos permite la comunicación a través de TCP/IP, lo cual nos permite la transmisión de datos de una manera segura.

La creación de su puerto de acceso es con una configuración sencilla.

#### 4.4.8.6 Recomendaciones

Se debe tener en cuenta la limitación de datos que se transmiten con este protocolo al igual que la configuración de parámetros ya que no son las mismas del IEC 608070-5-101, con esto se trata de explicar que no todas las funciones compatibles con IEC 608070-5-101 y IEC 608070-5-104.

## **CAPITULO 5**

### **5. CONCLUSIONES Y RECOMENDACIONES**

#### **5.1. CONCLUSIONES**

- El estándar IEC 61850 propone un enfoque de estandarización orientado a la integración de dispositivos de diferentes fabricantes, los cuales manejan un lenguaje estandarizado basado en archivos XML, asimismo, los nombres de objetos están estandarizados y definidos en el contexto de la subestación, permitiendo reducir los costos de migración y ampliación al optar por dispositivos con esta tecnología.
- El software de ingeniería NCD en conjunto con la RTU Orion LXM permitió llevar a cabo la implementación del sistema de comunicación IEC 61850. De igual manera consintió el desarrollo de las guías de pruebas evidenciando el funcionamiento de los dataSets, los informes y registros, la mensajería GOOSE, y la actuación de las protecciones eléctricas. Siendo una herramienta muy útil para la ejecución de este proyecto.
- Debe señalarse que para operar idóneamente los diversos dispositivos del laboratorio de Protecciones se hizo uso de sus respectivos manuales, además, es importante resaltar que estos manuales sirvieron de guía para la presente descripción técnica.
- Mediante el SCADA se logró adquirir paquetes de datos en tiempo real, datos como las variables eléctricas (corrientes, voltajes, potencias, frecuencia y factor de potencia), asimismo, la gestión de la red de comunicación y el manejo de eventos, entre otras funciones.
- Es importante mencionar que el estándar IEC 61850 es muy extenso y puede traer consigo complicaciones al momento de implementarlo por lo que se precisa la ayuda de un especialista en el área de comunicación y protecciones, de la misma manera la intervención del proveedor del equipo.



## 5.2. RECOMENDACIONES

- Incorporar el receptor GPS para proporcionar una referencia de tiempo de precisión a los diversos equipos que conforman el laboratorio de Protecciones y garantizar una mejor coordinación entre ellos al momento de realizar los ensayos.
- Implementar un sistema más completo junto a los relés Schneider Electric<sup>®</sup>, de tal manera que se pueda aprovechar todas las prestaciones de la Orion LXM y de los IED's mismos.
- Continuar con el proceso de implementación del sistema de comunicación IEC 61850 entre las distintas sedes que conforman la Universidad, con el fin de conformar una red más amplia y tener así un sistema SCADA gratificante.
- Adquirir los módulos de Merging Unit para poder digitalizar todos los datos primarios cercanos al proceso, y así aprovechar el protocolo Sampled Values en el sistema de comunicación de los IED's SIEMENS<sup>®</sup>.
- Implementar nuevas guías de pruebas en donde se pueda realizar la coordinación de protecciones mediante el uso de la mensajería GOOSE.

## BIBLIOGRAFÍA

- [1] J. L. Yepes and K. A. Granda, “Implementación de mensajería Goose bajo la norma IEC61850 en relés Sel para esquemas de protección de barra,” 2017.
- [2] H. T. Mouftah, M. Erol-Kantarci, M. Husain Rehmani, L. D. Oliveira, T. Abrao, and E. Hossain, “LTE-D2D Communication for Power Distribution Grid: Resource Allocation for Time-Critical Applications,” in *Transportation and Power Grid in Smart Cities*, 1st ed., Wiley Telecom, 2018, pp. 21–67.
- [3] I. D. Claros, “¿Conoce las diferencias entre la edición 1 y edición 2 del estándar IEC 61850? | Axon Group,” Nov. 08, 2016. <https://www.axongroup.com.co/conoce-las-diferencias-entre-la-edicion-1-y-edicion-2-del-estandar-iec-61850/> (accessed Aug. 12, 2020).
- [4] “IEC-61850 | Axon Group.” <https://www.axongroup.co/iec-61850/> (accessed Aug. 12, 2020).
- [5] NovaTech, “OrionLXm - User Manual.” Lenexa, 2015.
- [6] H. Automation and C. Gmbh, “Installation GREYHOUND Switch - User Manual.” Belden Inc, Neckartenzlingen, 2017.
- [7] Schneider Electric, “PowerLogic ION7400 | Schneider Electric.” <https://www.se.com/co/es/product-range-presentation/63502-powerlogic-ion7400/> (accessed Aug. 12, 2020).
- [8] OMICRON, “User Manual CMC 356.” pp. 1–142, 2018, doi: 10.1086/675853.
- [9] SIEMENS, *SIPROTEC 5: Protection, Automation, Monitoring*, 5th ed. Nuremberg, 2018.
- [10] SIEMENS, *SIPROTEC 5: Protection, Automation, Monitoring*, 6th ed. Nuremberg, 2020.
- [11] SIEMENS, “SIPROTEC 5: Hardware Description.” Nuremberg, 2019.
- [12] S. Electric, *Powerlogic Easergy P3 - Catalog 2019 - Network Protection Relays*. Rueil Malmaison, 2019.

- [13] S. Electric, “Easergy P3F30 - Feeder Protection Relay - User Manual.” Rueil Malmaison, 2017.
- [14] S. Electric, “Easergy P3L30 - Feeder protection relay with line differential and distance protection - User Manual.” Rueil Malmaison, 2020.
- [15] S. Electric, “Powerlogic Easergy P5 - Catalog 2019 - Network protection relays.” Rueil Malmaison, 2019.
- [16] R. A. Ayala Ramírez and J. E. Tenesaca Chacaguasay, “Implementación de un sistema de comunicación IEC 61850 para monitoreo y control de los módulos de protección de líneas de transmisión, sistemas de generación y redes de distribución.” 2018.
- [17] O. M. Prada Ríos, “GUÍA PRÁCTICA PARA LA COMUNICACIÓN BAJO LA NORMA IEC61850 PARA RELÉS ABB Y SIEMENS,” 2019.
- [18] R. L. O’fallon, D. A. Klas, T. Tibbals, and S. Shah, “IEC 61850 MMS SCADA Network Optimization for IEDs,” *IEC 61850 MMS SCADA Network Optimization for IEDs Ryan L. O’Fallon, Dean A. Klas, Timothy Tibbals, and Saurabh Shah Schweitzer Engineering Laboratories, Inc. Presented at Rockwell Automation on the Move Spokane*, Washington, Jun. 2016.
- [19] K. Brand, C. Brunner, and I. De Mesmaeker, “How to use IEC 61850 in protection and automation,” no. 222, pp. 11–21, 2005, [Online]. Available: <https://library.e.abb.com/public/fed26a71538479c3c12570d50034fbe4/Rapport.pdf>.
- [20] M. El Hariri, T. Youssef, E. Harmon, H. Habib, and O. Mohammed, “The IEC 61850 Sampled Measured Values Protocol: Analysis, Threat Identification, and Feasibility of Using NN Forecasters to Detect of Spoofed Packets,” *2019 IEEE Int. Conf. Environ. Electr. Eng. 2019 IEEE Ind. Commer. Power Syst. Eur. IEEEIC/I CPS Eur. 2019*, Jun. 2019, doi: 10.1109/IEEEIC.2019.8783253.
- [21] OMICRON, “Test Universe - Potente software de PC para pruebas avanzadas en secundario - OMICRON.” <https://www.omicronenergy.com/es/productos/test-universe/> (accessed Nov. 08, 2020).

- [22] SIEMENS, “Engineering software for SIPROTEC 5 - DIGSI 5 | Engineering tools for protection | Siemens Global.”  
<https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/protection-relays-and-control/engineering-tools-for-protection/engineering-software-digsi-5.html> (accessed Nov. 08, 2020).

# **ANEXO 1**

## **FOTOGRAFÍAS DE BANCO DE TRABAJO DEL LABORATORIO DE PROTECCIONES**



Figura 166. Banco de pruebas con IED's SIEMENS® y maleta CMC 356. Fuente: Autores.



Figura 167. Banco de prueba #2 con IED's SIEMENS® y PC. Fuente: Autores.



Figura 168. Rack de comunicación ELSYTEC. Fuente: Autores.



Figura 169. Laboratorio de Protecciones UPS. Fuente: Autores.

# **ANEXO 2**

## **DISEÑO DEL RACK DE COMUNICACIÓN**



