Revista Tecnocientífica URU
Universidad Rafael Urdaneta
No. 18 Enero - Junio 2020
Depósito Legal: PPI 201402ZU4464
ISSN: 2343-6360

Diseño para la integración de la red industrial con la red corporativa en una empresa manufacturera de alimentos

Abdénago Roldán, Alejandro Saras, Esteban Yeager y Gilbeto Araujo

Escuela de Ingeniería de Telecomunicaciones. Facultad de Ingeniería. Universidad Rafael Urdaneta. Maracaibo, Venezuela.

Correo electronico: abdenagorp@gmail.com aasb3799@gmail.com

Recibido: 30-10-2019 Aceptado: 12-01-2020

Resumen

El propósito de la investigación fue desarrollar un diseño funcional que permitiera la integración de la red industrial y corporativa de una empresa manufacturera; siendo estas usadas en automatización y en servicios empresariales respectivamente. Fue motivada por las ventajas competitivas que proporciona el internet de las cosas en las industrias, en el marco de la Industria 4.0, como la telemetría y telecontrol. Para poder llevar este proyecto a cabo se realizó un trabajo exhaustivo sobre los criterios de diseño que respectaban, gracias a la caracterización y análisis de tráfico en la red industrial, así como evaluando la viabilidad de la integración en sí, por medio de un análisis de los riesgos relativos a estas y la estructuración de un diagrama funcional, el cual fue simulado. Para su óptima realización se trabajaron con base en las buenas prácticas dadas por las guías del Converged Plantwide Ethernet, y normas y estándares internacionales.

Palabras Clave: Integración, red industrial, red corporativa, Converged Plantwide Ethernet

Design for the integration of the industrial network with the corporate network in a food manufacturing company

Abstract

The intention of this research was to design a way to integrate the industrial and the corporative network from a food manufacturing enterprise. This was motivated by the competitive benefits that provides the Internet of Things and the Industry 4.0, like telemetry and telecontrol. For the accomplishment of this project, it was needed an exhaustive work concerned of the extraction of the design criteria, recollected by the characterization and the traffics analysis of the industrial network; and by evaluating the viability of the integration, performing a risk assessment and constructing a network diagram, which was simulated. In order to develop a respectable work, this was done under the good practices, like the Converged Plantwide Ethernet guides and the internationals norms and standards.

Keywords: Integration, industrial networks, corporative networks, Converged Plantwide Ethernet

Introducción

Las redes de comunicaciones es la forma en que se conoce a un conjunto de nodos bien interconectados por enlaces de comunicación, para la prestación de un servicio. Y es en cuanto a los tipos de servicios que se pueden categorizar en dos grandes ramas: aquellos que utilizan la tecnología de información (IT) y aquellos que utilizan la tecnología de la operación (OT).

La primera de estas se conoce como redes corporativas y prestan servicios comunes para las empresas como compartición de archivos o navegación en internet. La segunda en contraposición se denomina redes industriales, porque presta los servicios básicos para la comunicación de los equipos de automatización de procesos.

Estos dos tipos de redes por asuntos de políticas de seguridad y de calidad de servicio se han mantenido aisladas o desligadas una de la otra. Pero con la llegada de la Industria 4.0, en la era de la información, resulta una necesidad para las empresas modernas (con actividades industriales) la integración de ambas para poder adquirir mejores tiempos de respuesta y prestar diversos servicios entre ambos contextos, como configuración y monitorización remota.

Las empresas manufactureras, a diferencia de otros sectores como el de electricidad, han tenido un desarrollo industrial lento. Sin embargo, la empresa objeto de estudio de este documento manifestó su interés en realizar su diseño de integración en colaboración con los investigadores, para la adquisición de ventajas competitivas dada la innovación de esta tendencia.

En consecuente, se presenta un reporte con resultados alcanzados por una investigación que constó de la caracterización y análisis de tráfico de una red industrial, para su consiguiente análisis de riesgo y el diseño en sí de la integración. Este documento se acompaña con una breve fundamentación teórica y metodológica para que pueda ser asimilable y recreable.

Fundamentación Teórica

Redes de comunicaciones.

Conjunto de nodos geográficamente dispersos conectados mediante enlaces de comunicación [1], con el fin de que estos elementos sean capaces de compartir sus recursos en orden de la prestación de servicios [2], como la transferencia de archivos o información.

Redes industriales.

Son sistemas flexibles que permiten la comunicación de los equipos de los entornos industriales; tratan de garantizar transmisión en tiempo real, siendo interoperables y resistentes a ruidos electromagnéticamente agresivos [3]. Anteriormente se aislaban de los corporativos, pero se han decidido integrar con estos, por una serie de ventajas como centralización de alarmas por medios de Centros Operativos de Redes y de Seguridad de Red [4], y aumentos en respuesta de eventos [5]; siendo una prioridad para empresas de hoy en día [6].

Análisis de tráfico.

Acción que permite la optimización en el rendimiento de las redes, que se realiza de forma manual o mediante la intervención manual, y puede requerir variar escalas de tiempo [7]. Existen tres enfoques para su realización: inspección de paquetes, recolección de propiedades estadísticas y monitoreo basado en flujos; siendo el último la combinación de los dos primeros y la mejor práctica [8]. Conlleva tres fases: medición, modelado y control, que permiten definir el estado actual, y determinar los métodos de actualización y su implementación, respectivamente [9]. A raíz de los parámetros que se extraen de estas actividades, se conocen los requisitos de calidad de servicio (QoS) de la red [10].

Análisis de riesgo.

Es la piedra angular de cualquier programa de seguridad de información, como información sobre los factores internos y externos para comprender las amenazas afrentadas y diseñar los controles

adecuados [11]. Según el NIST 800-30 (2012) la evaluación de riesgos se compone de prepararse para la evaluación, realizarla, comunicar los resultados y mantenerla. Es importante conocer que para ellos las redes IT y OT tienen diferentes requerimientos de seguridad [12], respetando el mismo modelo de confidencialidad, integridad y disponibilidad, pero con mayor énfasis en la disponibilidad, por los cual debe construirse o diseñarse en ella una arquitectura[13].

Coverged Plantwide Ethernet (CPwE).

Es la guía que dicta las pautas relevantes de diseño e implementación necesarios para implementar con éxito tecnologías de red estándar e integrar IACS (sistemas de administración y control integrados) y redes comerciales Ha sido desarrollada por Cisco Systems y Rockwell Automation, contemplando a Ethernet/IP como protocolo industrial, y según esta debe adaptarse para admitir la IACS que este siendo evaluada [14].

Metodología

Nivel de la investigación.

En cuanto al grado de profundidad que se abarca el fenómeno [15], siendo los mas comunes exploratorios, descriptivos y explicativos, la investigación se considera de tipo explicativa para la empresa objeto de estudio. En esta se trabajó para responder el por qué, para qué y cómo se realizó el diseñó, haciendo relaciones causa-efecto. Siendo más específicos, se considera también de tipo proyectista, dado a que consiste en la elaboración de una propuesta o de un modelo, como solución a un problema o necesidad de tipo práctico a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y las tendencias futuras [16].

Diseño de la Investigación.

La estrategia general adoptada, dentro de las documentales, de campo y experimentales [15], se considera experimental por la manipulación de las variables de las tendencias actuales no comprobadas [16] para la organización objeto de estudio, para explicar comportamientos respectivos. Asimismo, se subclasifica como preexperimental por el bajo grado de control y aleatoriedad con que se asignan sujetos (Bernal, 2010), siendo un diseño de un caso único el trabajado [15], para poder demostrar la factibilidad de la propuesta previa a su implementación, y de esta forma evitar fallas o costos innecesarios, resaltando su importancia.

Población y muestra.

La población; o el conjunto de elementos finitos del problema [15] es el conjunto de sedes a lo largo del país de la empresa manufacturera. La cual fue muestreada de acuerdo con los pasos descritos en [18], para obtener las sedes o partes de población seleccionada, siendo de forma no probabilística [15] al ser escogidos basándose en la localidad y cantidad de usuarios de estas.

Técnicas e Instrumentos de Recolección de Datos.

Las técnicas o procedimientos coherentes que conducen a generan información [19] fueron el análisis documental, observación y entrevistas. La revisión documental tuvo como fin enriquecer el marco teórico consultando fuentes secundarias como libros; la observación fue semiestructurada y simple para el primer objetivo, por no involucrarse y tener un esquema no limitativo [15], pero de forma directa; la observación fue indirecta para el segundo y cuarto, al requerir softwares para apreciar los atributos deseados; y la entrevista se realizó con un formato prediseñado [18] con un grupo de consultores la empresa.

Los instrumentos o los recursos para colectar información [15], que deben estar relacionados con la técnica utilizada [16] fueron una lista de cotejo para caracterizar la red, un diario de campo donde se hicieron anotaciones extras de la observación, una escala de estimación para evaluar los riesgos y una unidad de almacenamiento digital (computadora) para recopilar datos de los softwares y redactar los documentos productos de la investigación.

Análisis de los resultados

A continuación, se presentan una parcialidad de los resultados (por la extensión de estos) alcanzados de la investigación. Estos están ordenados de acuerdo con los objetivos planteados, los cuales han sido implícitamente descritos a lo largo de este documento.

Caracterización de la red industrial.

Se aplica la lista de cotejo, de las cuales se expondrán solo las respuestas negativas de la tabla (entendiendo que las positivas representan la idealidad), que son los puntos de mejora.

Tabla 1. Lista de Cotejo.

Característica deseada	Se cumple con la característica (SI/NO)
Los sensores en sitio son programables	NO
Existen PLC o PAC para cada una de las células de la red industrial	NO
Existen paneles de visualización para cada una de las células de la red industrial	NO
Existe un equipo de conmutación que relacione a todos los equipos de cada área de la red industrial	NO
Existe un panel principal para cada área de la red industrial	NO
Todos los protocolos en uso, en cada área, son Ethernet/IP	NO
Está claramente definido el nivel 2 (equipos de nivel de área) en la red industrial	NO
Existe un equipo de conmutación que comunique las áreas de la red industrial	NO
Existe un histórico centralizado para toda la zona de manufactura	NO
Existe un sistema SCADA centralizado para toda la zona de manufactura	NO
Está claramente definido el nivel 3 (equipos de nivel de zona de manufactura) en la red industrial	NO
Existe una zona desmilitarizada	NO
El único medio de interconexión es cableado Ethernet	NO
Existe una topología definida para la red industrial	NO

Fuente: Elaboración propia.

Por ello se considera que la empresa requería interconectar un grupo de subredes industriales e incluir una zona desmilitarizada previo a su integración. Adicionalmente de las notas del diario de campo se reconoce que los equipos que han de ser añadidos deben cumplir con las características de los equipos industriales como resistencia al polvo, humedad y variaciones de temperatura; actualizar los buses de campo y otros protocolos a Ethernet/IP con convertidores.

Analizar el tráfico y la calidad de servicio de la red industrial.

Se realizó el monitoreo y modelado. Para reconocer que los enlaces existentes son aptos de incorporar a la red industrial, sabiendo que en donde esta reposa, existe un área administrativa la cual posee

un enlace MPLS hacia la red corporativa seleccionada. Esto gracias a mediciones con el Wireshark, dimensionando el tráfico promedio que sería enviado; se consideraron las estadísticas de la transmisión, así como los protocolos que lleva, como muestran las siguientes figuras.

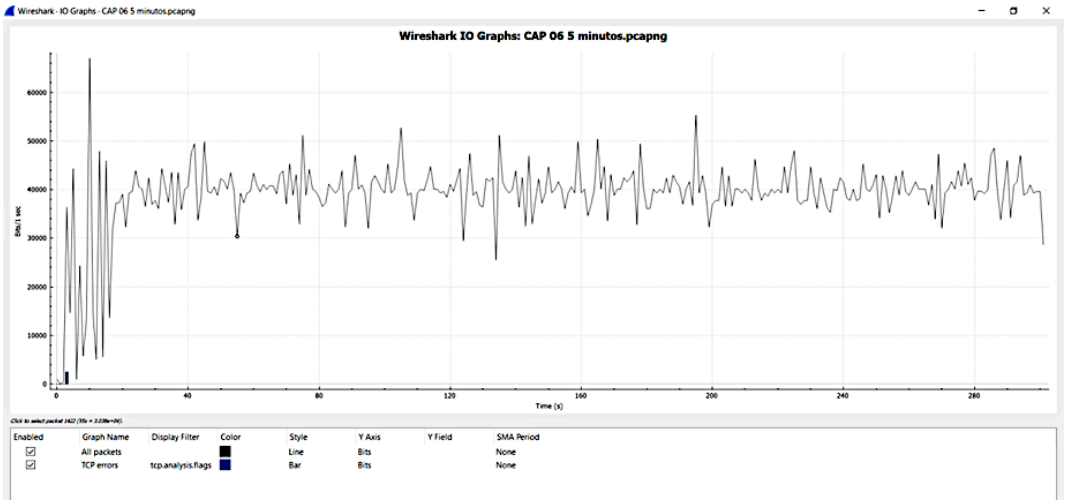


Figura 1. Bits por segundo en comunicación equipo a PLC con direcciones fijas.

Fuente: Elaboración propia

Wireshark · Protocol Hierarchy Statistics · CAP 06 5 minutos.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	7810	100.0	1471858	39 k	0	0	0
Ethernet	100.0	7810	7.4	109340	2899	0	0	0
Internet Protocol Version 6	0.1	5	0.0	200	5	0	0	0
User Datagram Protocol	0.1	5	0.0	40	1	0	0	0
DHCPv6	0.1	5	0.0	470	12	5	470	12
Internet Protocol Version 4	96.6	7543	10.3	150920	4001	0	0	0
User Datagram Protocol	0.2	12	0.0	96	2	0	0	0
NetBIOS Name Service	0.2	12	0.0	600	15	12	600	15
Transmission Control Protocol	96.2	7515	81.4	1197850	31 k	2507	50140	1329
EtherNet/IP (Industrial Protocol)	64.1	5008	71.2	1047550	27 k	0	0	0
Common Industrial Protocol	64.1	5008	55.5	817242	21 k	102	1843	48
CIP Connection Manager	0.1	6	0.0	188	4	6	188	4
CIP Class Generic	62.7	4900	55.4	815211	21 k	4900	815211	21 k
Internet Group Management Protocol	0.2	15	0.0	120	3	15	120	3
Internet Control Message Protocol	0.0	1	0.0	16	0	1	16	0
Address Resolution Protocol	3.4	262	0.5	7336	194	262	7336	194

Figura 2. Protocolos en comunicación equipo a PLC con direcciones fijas.

Fuente: Elaboración propia

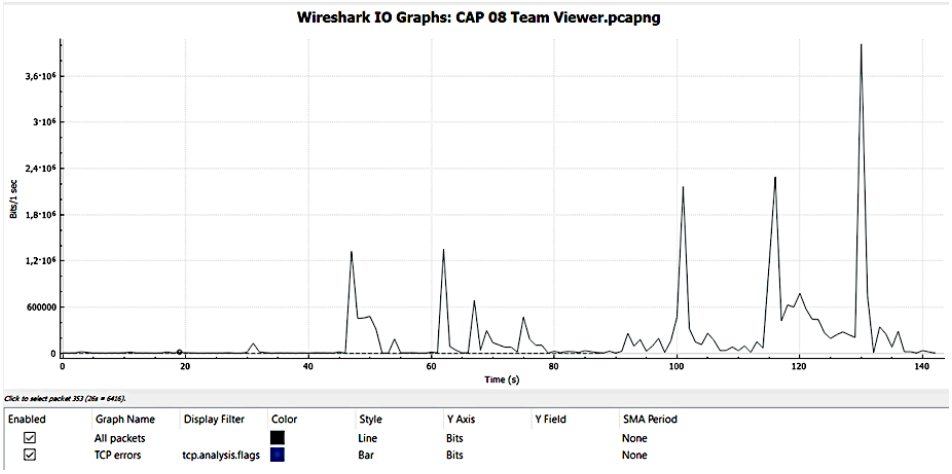
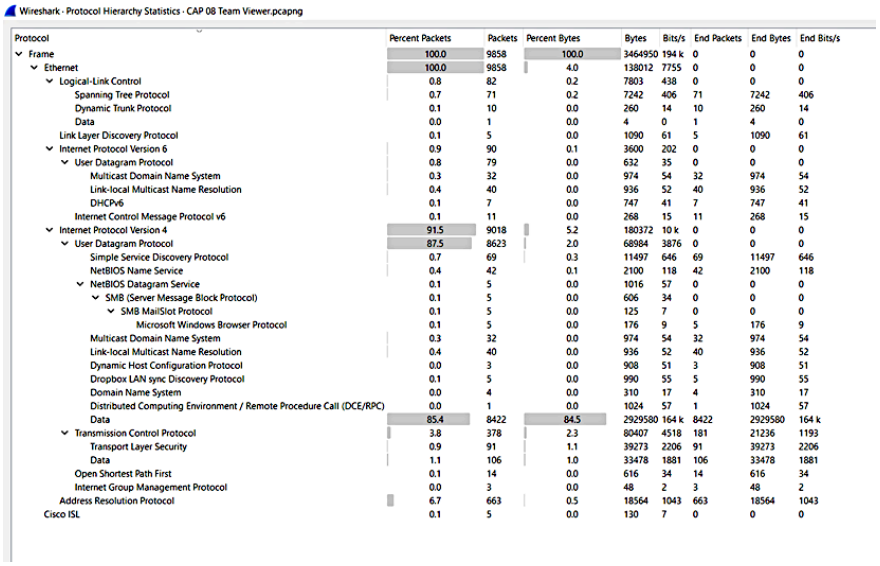


Figura 3. Bits por segundo con TeamViewer.



Wireshark · Protocol Hierarchy Statistics · CAP 08 Team Viewer.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	9858	100.0	3464950	194 k	0	0	0
Ethernet	100.0	9858	4.0	138012	7755	0	0	0
Logical-Link Control	0.8	82	0.2	7803	438	0	0	0
Spanning Tree Protocol	0.7	71	0.2	7242	406	71	7242	406
Dynamic Trunk Protocol	0.1	10	0.0	260	14	10	260	14
Data	0.0	1	0.0	4	0	1	4	0
Link Layer Discovery Protocol	0.1	5	0.0	1090	61	5	1090	61
Internet Protocol Version 6	0.9	90	0.1	3600	202	0	0	0
User Datagram Protocol	0.8	79	0.0	632	35	0	0	0
Multicast Domain Name System	0.3	32	0.0	974	54	32	974	54
Link-local Multicast Name Resolution	0.4	40	0.0	936	52	40	936	52
DHCPv6	0.1	7	0.0	747	41	7	747	41
Internet Control Message Protocol v6	0.1	11	0.0	268	15	11	268	15
Internet Protocol Version 4	91.5	9018	5.2	180372	10 k	0	0	0
User Datagram Protocol	87.5	8623	2.0	68984	3876	0	0	0
Simple Service Discovery Protocol	0.7	69	0.3	11497	646	69	11497	646
NetBIOS Name Service	0.4	42	0.1	2100	118	42	2100	118
NetBIOS Datagram Service	0.1	5	0.0	1016	57	0	0	0
SMB (Server Message Block Protocol)	0.1	5	0.0	606	34	0	0	0
SMB MailSlot Protocol	0.1	5	0.0	125	7	0	0	0
Microsoft Windows Browser Protocol	0.1	5	0.0	176	9	5	176	9
Multicast Domain Name System	0.3	32	0.0	974	54	32	974	54
Link-local Multicast Name Resolution	0.4	40	0.0	936	52	40	936	52
Dynamic Host Configuration Protocol	0.0	3	0.0	908	51	3	908	51
Dropbox LAN sync Discovery Protocol	0.1	5	0.0	990	55	5	990	55
Domain Name System	0.0	4	0.0	310	17	4	310	17
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.0	1	0.0	1024	57	1	1024	57
Data	85.4	8422	84.5	2929580	164 k	8422	2929580	164 k
Transmission Control Protocol	3.8	378	2.3	80407	4518	181	21236	1193
Transport Layer Security	0.9	91	1.1	39273	2206	91	39273	2206
Data	1.1	106	1.0	33478	1881	106	33478	1881
Open Shortest Path First	0.1	14	0.0	616	34	14	616	34
Internet Group Management Protocol	0.0	3	0.0	48	2	3	48	2
Address Resolution Protocol	6.7	663	0.5	18564	1043	663	18564	1043
Cisco ISL	0.1	5	0.0	130	7	0	0	0

Figura 4. Protocolos con TeamViewer.

Fuente: Elaboración propia

De esta forma, la interrogación al PLC sería local con enlaces Ethernet, para servicios de telemetría y telecontrol; a distancia se puede compartir escritorio con una aplicación como TeamViewer para extender estos servicios con la integración.

Analizar los riesgos de la integración de la red industrial a la red corporativa de la empresa.

Se aplico la escala de estimación, gracias a la entrevista con los consultores de la empresa enfocados al área de seguridad, de automatización y el jefe de infraestructura. Obteniendo que, en el total de los 253 riesgos evaluados existe una predominancia de los perfiles de riesgos medios (165), sobre los altos (77) y bajos (11) como indica la figura 5. Esto, porque no se había conceptualizado la integración.

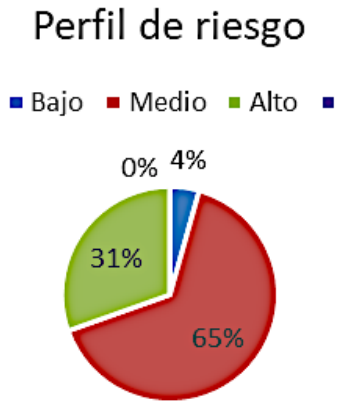


Figura 5. Perfiles de riesgos.

Fuente: Elaboración propia.

Estos pueden ser tratados con la aplicación de los controles identificados de acuerdos a las normas ISO 27001, NIST 800-30 e ITIL, y trabajos previos. En la figura 6 se manifiesta que la mayoría ha sido acorde a la estrategia de mitigación de probabilidad de ocurrencia, y la figura 7 es un ejemplo de controles para la integridad la información y sistemas.

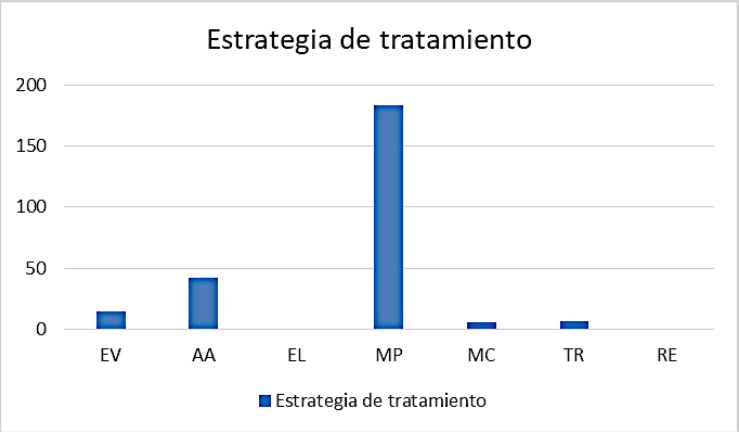


Figura 6. Estrategias de tratamiento.

Fuente: elaboración propia.

CONTROLES Y/O MECANISMOS TECNOLÓGICOS A IMPLEMENTAR (Basado en prácticas de ISO 27001, NIST 800-53, ITIL)	SISTEMAS Y DISPOSITIVOS DE CAMPO DE LA RED INDUSTRIAL (RED OT)											
	Cortafuegos DMZ	Switch CORE Sede Industrial	Sistema SCADA	Historiador SCADA	Switch SubRed Recepción	Switch SubRed Pasteurización	Switch SubRed Coagulación	PLC Principal	Paneles PC/PR/PP	Remoto TV1	Sensores	Actuadores
INTEGRIDAD DE LA INFORMACIÓN Y LOS SISTEMAS												
Definir políticas, normas y procedimientos para la gestión de equipos servidores			x	x								
Instalación y mantenimiento de SW Antivirus			x	x								
Instalación y mantenimiento de SW Antimalware			x	x								
Instalación y mantenimiento de SW de inspección de contenido	x		x	x								
Instalación y mantenimiento de SW AntiSpam			x	x								
Establecer un sistema de monitorización de los equipos y sistemas - memoria, discos, procesos.	x	x	x	x	x	x	x	x	x			
Establecer mecanismos de protección del firmware de los equipos y dispositivos	x	x			x	x	x	x	x	x	x	x
Establecer mecanismos para el manejo de errores	x	x	x	x	x	x	x					

Figura 7. controles de integridad de la información y sistemas.

Fuente: elaboración propia.

Diseñar una arquitectura de red para la convergencia de la red industrial con la red corporativa.

La última etapa fue la diagramación de un diseño jerárquico (arquitectura) con su simulación como indica la figura 8, en el cual se demuestra su viabilidad con un proceso de simulación en GNS3, donde los equipos PLC fueron vistos como huéspedes con un tráfico definido acorde a las redes industriales.

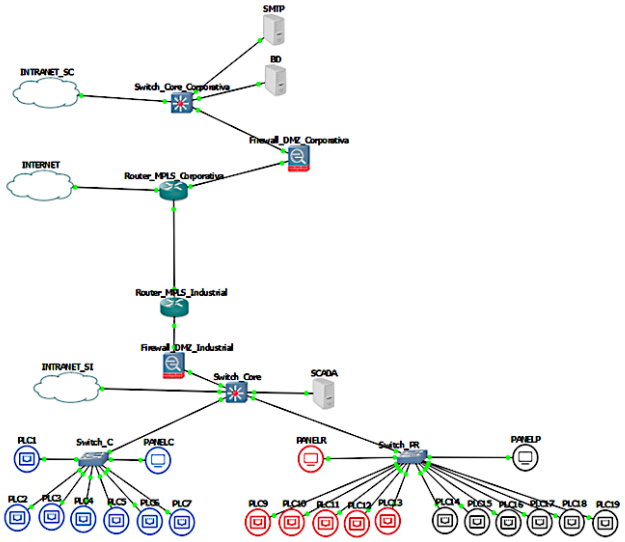


Figura 8. Simulación del diagrama de integración.
Fuente: Elaboración propia.

Conclusiones

Se resalta la importancia de la caracterización de una red como primera fase en cualquier diseño, en especial de una red de tipo industrial. Esto se debe a que normalmente las corporativas ya presentan bondades de interoperabilidad e integración, mientras que estas pueden verse disgregadas por áreas de procesos como en la empresa objeto de estudio.

El análisis de tráfico en las redes industriales es una tarea sencilla, sabiendo que estas son teóricamente determinísticas. No obstante, es importante conocer los protocolos en curso y la intensidad de tráfico intercambiada, para determinar la viabilidad de la integración sin degradación en la calidad de servicio (caso trabajado) o si es requerida la expansión de los enlaces existentes.

De igual forma el análisis de riesgo resulta imprescindible, sabiendo que las redes OT, normalmente están aisladas. A raíz de su integración se pueden considerar un gran número de amenazas de IT que podrían aprovecharse de las vulnerabilidades de los equipos industriales en sus configuraciones básicas. Sin embargo, esto siempre puede ser tratados bajo diferentes estrategias y controles según las normas que apliquen.

Extrayendo todos los datos descritos se pueden procesar para la elaboración de una arquitectura funcional, la cual debe ser simulada antes de su implementación por motivos prácticos como reducción de errores y costos. Esto depende del protocolo predominante, para Ethernet/IP, se recomienda la guía de Converged Plantwide Ethernet.

En síntesis, trabajando bajo lo indicado por las buenas prácticas se puede realizar un diseño funcional que pueda integrar las redes industriales y corporativas. A efectos de estos se pueden satisfacer

requerimientos de la empresa como configuración y monitorización remota, reducción de tiempos de fallas y similares.

Referencias Bibliográficas

[1] Briceño, J. (2005). Transmisión de Datos. Recuperado de: http://bdigital.ula.ve/RediCiencia/busquedas/DocumentoRedi.jsp?file=32381&type=ArchivoDocumento&view=pdf&docu=26115&col=11

[2] Correa, B. (2008). Propuesta de diseño e incorporación de la red LAN del bloque N de La Universidad del Zulia a la red WAN de la institución. (Tesis inédita de grado ingeniería). La Universidad del Zulia, Maracaibo, Venezuela.

[3] Vicario, C., Herrera, D., Gaitán, G., Zúñiga, M. (2014). Propuesta de una red industrial de monitoreo para facilidades eléctricas. (Tesis inédita de grado ingeniería). Universidad Nacional Autónoma de México, Ciudad de México, México.

[4] Guerrero, V., Yuste, R. Martínez, L. (2009). Comunicaciones Industriales siemens. Valencia, España: Marcombo.

[5] Brodersen, M. (2018). IT/OT Network Design. (White Paper). Cisco Systems.

[6] Harp, D., Gregory-Brown, B. (2015). IT/OT Convergence, Bridging the divide. (White Paper). Recuperado de: nexdefense.com

[7] Mortier, R. (2002). Internet traffic engineering. (Technical Report UCAM-CL-TR-532). Cambridge: University of Cambridge.

[8] Kasner, Z. (2015). Flow-Based Classification of Devices in Computer Networks. (Tesis inédita de grado ingeniería). Czech Technical University in Prague, Praga, República Checa.

[9] Aziz, Y., Naeem, M. (2008). Traffic Engineering with Multi-Protocol Label Switching Performance, Comparison with IP networks. (Tesis inédita de maestría). Blekinge Institute of Technology, Blekinge, Suecia.

[10] Bujlow, T. (2014). Classification and Analysis of Computer Network Traffic. (Tesis inédita doctoral). Aalborg University, Aalborg, Dinamarca

[11] Chapple, M., Seidl, D. (2017). Comptia CSA+ study guide. Indiana: John Wiley & Sons.

[12] Stouffer, K., Falco, J., Scarfone, K. (2007). Guide to Industrial Control Systems (ICS) security. Estados Unidos: National Institue of Standards and Technology

[13] Chhetri, S. Rashid, N., Faezi, S., Al Faruque, M. (2017). Security Trends and Advances in Manufacturing Systems in the Era of Industry 4.0. (Artículo científico). Univeristy of California, Irvine, Estados Unidos.

[14] Rockwell. (2011). Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. Cisco Systems & Rockwell Automation.

[15] Arias, F. (2012). El Proyecto de Investigación, Introducción a la metodología científica. Caracas: Episteme.

[16] Hurtado, J. (2010). Metodología de la investigación Holística. Caracas: Fundación Sypal.

[17] Tamayo, M., Tamayo, M. (2003). El proceso de la investigación científica. Caracas: Limusa Noriega.

[18] Bernal, C. (2010). Metodología de la investigación. Bogotá: Pearson.

[19] Del Cid, A. Méndez, R., Sandoval, F. (2011). Investigación, fundamentos y metodología. Ciudad de México: Pearson.