PhD Thesis

A study of the applicability of Software-Defined Networking in industrial networks

ELÍAS MOLINA MUÑOZ

eman ta zabal zazu

Universidad del País Vasco Euskal Herriko Unibertsitatea

Supervisor: Eduardo Jacob Taquet

Faculty of Engineering of Bilbao
Department of Communications Engineering
University of the Basque Country UPV/EHU
Bilbao, Spain 2017

Acknowledgments

First of all, I would like to express my gratitude to my thesis advisor, Prof. Dr. Eduardo Jacob, for helping me to improve my work through their advices and ideas. His great experience and enthusiastic interest for technology have been a constant motivation to me. I strongly thank him for providing me with the opportunity to work in the I2T Research Group, with a talented team of colleagues, in which I ended up learning a lot.

I extend my gratitude to the Zabalduz Program (PhD fellowship) for promoting the collaboration with the System-on-Chip Engineering S. L. company, which helped me to establish the overall direction of the research.

My heartfelt thanks also go to my workmates Igor, Alaitz, Christian, Jon, Jokin and Victor, who have been supportive and helpful during this endeavor. What I gained from this shared experience has been priceless.

Of course, this thesis is dedicated to my parents and brothers, whose endless love and sacrifice have always been the greatest inspiration for me in my pursuit for betterment.

Finally, my deepest acknowledgment goes to my wife and constant companion, Paola, for her understanding and infinite support during these years of study. Without her constant encouragement, I probably would never have finished this dissertation.

Advisors, colleagues, friends and family, to whom I owe my sincere gratitude, this is the least I could do in return for your kindness and generosity.

Abstract

Industrial networks interconnect sensors and actuators to perform measurement, supervision and protection functions in different domains, such as transportation or automation and control systems. These Cyber-Physical Systems (CPSs) generally rely on multiple networks, whether wired or wireless, to which demand industrial-grade requirements, where dependability, safety and performance characteristics of critical and non-critical services coexist. In such a scenario, the control and management functions should be tightly coupled to the different underlying conditions. Thus, industrial networks are evolving to meet new needs related to flexibility, maintainability, and adaptability, at the same time that the Quality of Service (QoS) and real-time constraints are not affected. However, traditional network control strategies generally fail to support for heterogeneous and dynamic environments.

After defining a set of requirements and discussing the shortcomings of the existing solutions, the analysis shows that a deeper and more flexible control can be achieved by means of a set of network functions operating independently from network hardware. In this way, the Software-Defined Networking (SDN) paradigm provides programmability for explicitly controlling the forwarding plane. This research explores the potential role and applicability of this paradigm and, specifically, the OpenFlow protocol, in industrial automation systems. To illustrate this approach, automation networks based on the IEC 61850 standard have been used as a case study. In particular, this standard is now one of the most widely accepted technologies for power grid communications, such as Substation Automation Systems (SASs), and it defines different services and protocols with stringent requirements that need to be fulfilled with advanced traffic engineering techniques.

Consequently, leveraging the flexibility of the software-defined networks, an OpenFlow-based control framework is proposed to improve the performance of modern SASs through management and monitoring tools that provide a global view of the network. Hence, different types of flows are handled according to their patterns, priorities and the network status.

Moreover, considering that SASs are considered mission-critical systems, as a failure can have serious economic and safety consequences, these infrastructures must be extremely reliable. The network robustness is strongly influenced by the implementation of redundancy and its ability of reacting to changes. However, Ethernet mesh networks, in which industrial applications tend to be supported, usually use redundant resources as backup solutions, being underutilized most of the time. On the contrary, the IEC 62439-3 standard defines the Parallel Redundancy Protocol (PRP) and the High-availability Seamless Redundancy (HSR) protocol, which provide zero recovery time in case of failure by using active redundant paths in Ethernet networks. Despite this, the management of PRP and HSR networks is static and inflexible, which, added to the bandwidth reduction due to data duplication, makes it difficult to efficiently control the network resources. Thus, this thesis proposes a novel SDN-based implementation of redundancy control techniques that effectively exploit mesh topologies and ensure adequate availability of industrial control applications. Specifically, it is discussed how the OpenFlow protocol allows an external controller to configure multiple redundant paths between dual-homed devices, as well as the analysis of redundancy influence on the performance of Wireless Local Area Networks (WLANs). As a result, critical services can be protected in interference and mobility situations.

The assessment of the adequacy of the solutions has been mainly conducted by emulating different topologies and traffic types. This way, the performance of different flow-based services has been presented. Furthermore, analytic models and extensive experiments have shown how latency is improved by reducing the number of hops with respect to spanning trees, as well as by load balancing in layer 2 networks. Also, a robustness analysis has been performed to determine the improvement achieved by using PRP in combination with OpenFlow. Another study has demonstrated the efficiency of combining HSR networks and traffic priority control, in comparison to the standard operation and other proposals. The promising results show that the proposed SDN model could significantly improve the performance of a typical industrial network and be effective in mission-critical systems.

Resumen

Las redes industriales interconectan sensores y actuadores para llevar a cabo funciones de monitorización, control y protección en diferentes entornos, tales como sistemas de transporte o sistemas de automatización industrial. Estos sistemas ciberfísicos generalmente están soportados por múltiples redes de datos, ya sean cableadas o inalámbricas, a las cuales demandan nuevas prestaciones, de forma que el control y gestión de tales redes deben estar acoplados a las condiciones del propio sistema industrial. De este modo, aparecen requisitos relacionados con la flexibilidad, mantenibilidad y adaptabilidad, al mismo tiempo que las restricciones de calidad de servicio no se vean afectadas. Sin embargo, las estrategias de control de red tradicionales generalmente no se adaptan eficientemente a entornos cada vez más dinámicos y heterogéneos.

Tras definir un conjunto de requerimientos de red y analizar las limitaciones de las soluciones actuales, se deduce que un control provisto independientemente de los propios dispositivos de red añadiría flexibilidad a dichas redes. Por consiguiente, la presente tesis explora la aplicabilidad de las redes definidas por software (*Software-Defined Networking*, SDN) en sistemas de automatización industrial. Para llevar a cabo este enfoque, se ha tomado como caso de estudio las redes de automatización basadas en el estándar IEC 61850, el cual es ampliamente usado en el diseño de las redes de comunicaciones en sistemas de distribución de energía, tales como las subestaciones eléctricas. El estándar IEC 61850 define diferentes servicios y protocolos con altos requisitos en términos de latencia y disponibilidad de la red, los cuales han de ser satisfechos mediante técnicas de ingeniería de tráfico. Como resultado, aprovechando la flexibilidad y programabilidad ofrecidas por las redes definidas por software, en esta tesis se propone una arquitectura de control basada en el protocolo OpenFlow que, incluyendo tecnologías de gestión y monitorización de red, permite establecer políticas de tráfico acorde a su prioridad y al estado de la red.

Además, las subestaciones eléctricas son un ejemplo representativo de infraestructura crítica, que son aquellas en las que un fallo puede resultar en graves pérdidas económicas, daños físicos y materiales. De esta forma, tales sistemas deben ser extremadamente seguros y robustos, por lo que es conveniente la implementación de topologías redundantes que ofrezcan un tiempo de reacción ante fallos mínimo. Con tal objetivo, el estándar IEC 62439-3 define los protocolos Parallel Redundancy Protocol (PRP) y High-availability Seamless Redundancy (HSR), los cuales garantizan un tiempo de recuperación nulo en caso de fallo mediante la redundancia activa de datos en redes Ethernet. Sin embargo, la gestión de redes basadas en PRP y HSR es estática e inflexible, lo que, añadido a la reducción de ancho de banda debida la duplicación de datos, hace difícil un control eficiente de los recursos disponibles. En dicho sentido, esta tesis propone control de la redundancia basado en el paradigma SDN para un aprovechamiento eficiente de topologías malladas, al mismo tiempo que se garantiza la disponibilidad de las aplicaciones de control y monitorización. En particular, se discute cómo el protocolo OpenFlow permite a un controlador externo configurar múltiples caminos redundantes entre dispositivos con varias interfaces de red, así como en entornos inalámbricos. De esta forma, los servicios críticos pueden protegerse en situaciones de interferencia y movilidad.

La evaluación de la idoneidad de las soluciones propuestas ha sido llevada a cabo, principalmente, mediante la emulación de diferentes topologías y tipos de tráfico. Igualmente, se ha estudiado analítica y experimentalmente cómo afecta a la latencia el poder reducir el número de saltos en las comunicaciones con respecto al uso de un árbol de expansión, así como balancear la carga en una red de nivel 2. Además, se ha realizado un análisis de la mejora de la eficiencia en el uso de los recursos de red y la robustez alcanzada con la combinación de los protocolos PRP y HSR con un control llevado a cabo mediante OpenFlow. Estos resultados muestran que el modelo SDN podría mejorar significativamente las prestaciones de una red industrial de misión crítica.

Laburpena

Sare industrialek sentsoreak eta eragingailuak interkonektatzen dituzte monitorizazio, kontrol eta babes funtzioak aurrera eraman ahal izateko ingurune ezberdinetan, besteak beste, garraio sistemetan edo industria automatizazioan. Sistema ziberfisiko hauek orokorrean sare anitzen gainean lan egiten dute, haridunak eta haririk gabekoak, hauen kontrol eta kudeaketa sistema industrialaren eskakizunei egokituak egon behar direlarik. Hau horrela izanda, malgutasunari, mantentzeari eta moldakortasunari lotutako eskakizunak agertzen dira, zerbitzu kalitatea bermatuak izan behar diren bitartean. Sare tradizionalen kontrola ordea ez da modu egokian moldatzen gero eta dinamikoak eta heterogeneoak diren inguruneetara.

Sare eskakizun batzuk definitu ondoren eta egungo soluzioen mugak aztertu eta gero, sare dispositiboekiko independentea izango den kontrola, sare horien malgutasuna handituko lukeela ondorioztatzen da. Hau horrela izanda, tesi honek software bidez definitutako sareen (bere ingeleseko sigletatik, Software-Defined Networking, SDN) ezargarritasuna aztertzen du industria automatizazio sistemetan. Azterketa hau aurrera eramateko, IEC 61850 estandarrean oinarritutako automatizazio sareak hartu dira kasu azterketa moduan, zeinak energia banaketa sistemetan, azpi-estazio elektrikoetan adibidez, hedatuta dauden. IEC 61850 estandarrak zerbitzu eta protokolo ezberdinak definitzen ditu, latentzia eta erabilgarritasun eskakizun handiak bete behar dituztenak trafiko ingeniaritza teknikak erabiliz. Ondorioz, software bidez definitutako sareen malgutasuna eta programagarritasuna aprobetxatuz, tesi honetan OpenFlow protokoloan oinarritutako kontrol arkitektura bat proposatzen da, zeinak sare kudeaketa eta monitorizazio teknologien bitartez, lehentasunaren eta sarearen egoeraren araberako trafiko politikak zehazteko gai dena.

Gainera, azpi-estazio elektrikoak azpiegitura kritikoen baitan kokatzen dira, alegia sare horietan gertatutako akats batek galera ekonomiko, fisiko eta materialak eragin ditzake. Hau horrela izanda, sistema hauek seguruak eta sendoak izan behar dira, beraz gomendagarria da topologia erredundanteen ezarpena, akatsen aurrean erreakzio denbora minimoak lortzeko. Helburu hori lortzeko, IEC 62439-3 estandarrak ethernet sareetan errekuperazio denbora nulua bermatzen duten Parallel Redundancy Protocol (PRP) eta High-availability Seamless Redundancy (HSR) protokoloak definitzen ditu. Hala ere, PRP eta HSR protokoloetan oinarritutako sare kudeaketa estatikoak eta zorrotzak, datuen bikoizketak eragindako banda zabalaren murrizpenarekin batera, zaila egiten du baliabideen kudeaketa eraginkorra. Horrexegatik, tesi honek SDN paradigman oinarritutako erredundantzia kontrola proposatzen du amaraun topologien aprobetxamendu eraginkorra bermatzeko, monitorizazio eta kontrol aplikazioen erabilgarritasuna bermatzen duen bitartean. Zehazki, OpenFlow protokoloarekin, sare-kanpoko kontrolatzaile batek, sare interfaze ugaridun gailuen artean (haririk gabeko inguruneetan barne) bide erredundanteak eratzeko erak aztertzen dira. Modu honetan, zerbitzu kritikoak interferentzia eta mugikortasunaren aurrean babestea bilatzen da.

Proposatutako ebazpenen egokitasunaren ebaluaketa, trafiko mota eta topologia ezberdinen emulazioaren bitartez egin da bereziki. Era berean, analitikoki eta esperimentalki aztertu da jauzi kopuruen murrizpenak latentzian duen eragina spanning tree-rekin alderatuta, baita 2. mailako zama banaketa ere. Horrez gain, PRP eta HSR protokoloek, Openflow bidezko kontrol batekin, sare baliabideen eraginkortasunean eta sendotasunean eskaintzen duten hobekuntza aztertu da. Lortutako emaitzak egiaztatzen dute SDN ereduak eginkizun kritikoetako sare industrialetako zerbitzuak nabarmenki hobetu ditzakeela.

Resumen extendido

Introducción

Las redes industriales permiten la comunicación en tiempo real entre aplicaciones que requieren un alto grado de fiabilidad y seguridad. Como ejemplo representativo de sistemas de misión crítica, las *Smart Grids* engloban procesos de supervisión y control de las infraestructuras de generación y suministro eléctrico, en los que cumplir rigurosos requisitos de latencia y disponibilidad. Por otro lado, se demandan nuevas prestaciones relacionadas con la flexibilidad, mantenibilidad y adaptabilidad a las condiciones existentes en dichos sistemas. Sin embargo, las estrategias de red tradicionales no se adaptan eficientemente a entornos dinámicos y heterogéneos. Sin embargo, la gestión de redes basadas en PRP y HSR es estática e inflexible, lo que, añadido a la reducción de ancho de banda debida la duplicación de datos, hace difícil un control eficiente de los recursos disponibles. Esto puede ser una limitación importante, teniendo en cuenta que los sistemas de control y automatización tienden a integrar servicios que generan grandes cantidades de datos. En efecto, tal y como se indica en (Li, F. et al., 2010), las redes eléctricas existentes no implementan tecnologías de red adaptativas, las cuales permitirían tener un control en tiempo real de la resiliencia y utilización de los recursos disponibles. Además, según los autores, dichas tecnologías deberían estar basadas en soluciones abiertas y estandarizadas.

Dadas las limitaciones de las infraestructuras de red tradicionales, este trabajo explora la aplicabilidad de las redes definidas por software (SDN) a las redes de automatización industrial, tales como las subestaciones eléctricas basadas en el estándar IEC 61850. Por consiguiente, con el objeto de incorporar programabilidad a la red, en este trabajo se propone una arquitectura SDN que, incluyendo funcionalidades de monitorización y control, permite implementar calidad de servicio, mecanismos de seguridad y gestión de la redundancia.

Planteamiento y objetivos de la investigación

Con el propósito de ofrecer unas prestaciones de red adecuadas, las funciones de control y gestión deben ser conscientes de los recursos disponibles, así como de los requerimientos específicos del tráfico. Así, el planteamiento de la tesis resultante es:

- *El uso de tecnologías SDN permite a los sistemas industriales obtener un mejor control de los recursos de red, al mismo tiempo que posibilitan cumplir los requerimientos de calidad de servicio. Además, un enfoque basado en un control de tráfico basado en flujos permite a las aplicaciones de misión crítica operar con alta disponibilidad.*

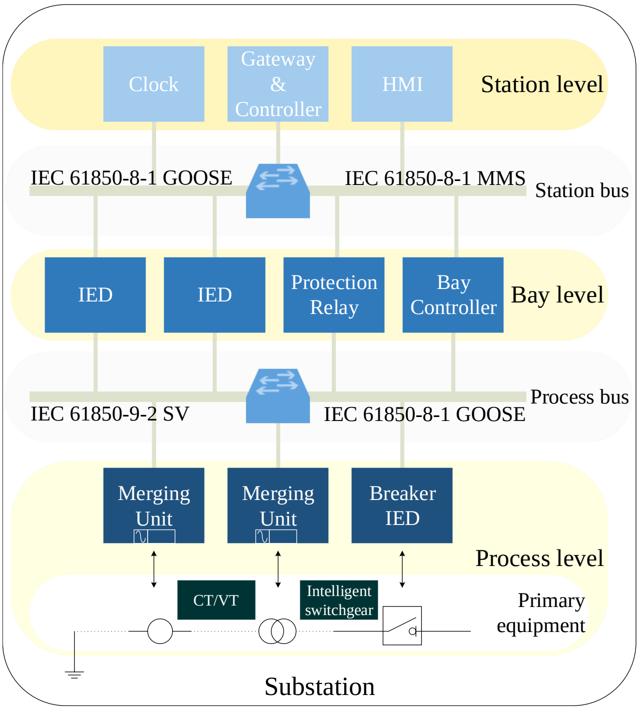
De este modo, esta disertación está motivada por las siguientes cuestiones:

- ¿Cómo impacta el uso de las SDNs a las redes industriales, tales como las basadas en el estándar IEC 61850?
- ¿Podrían las SDNs mejorar las prestaciones de los protocolos de redundancia de red?

Análisis del estado del arte

El principal objetivo del estándar IEC 61850 *Power Utility Automation* es flexibilizar el diseño de los sistemas de automatización de subestaciones, así como facilitar la interoperabilidad entre dispositivos de distintos fabricantes. Dicho estándar define, entre otros aspectos, los servicios y requisitos de diversos protocolos de comunicaciones, de forma que se distinguen diferentes clases de tráfico. Por tanto, es esencial la gestión del tráfico de datos para garantizar las prestaciones de diferentes servicios con exigentes requisitos. Posteriormente, se muestra una arquitectura lógica de la red de área local de una subestación basada en el estándar IEC 61850.

Se han analizado multiples funcionalidades exigidas en este tipo de infraestructuras, tales como medidas de restricción y priorización del tráfico. Sin embargo, el establecimiento de políticas de control de tráfico



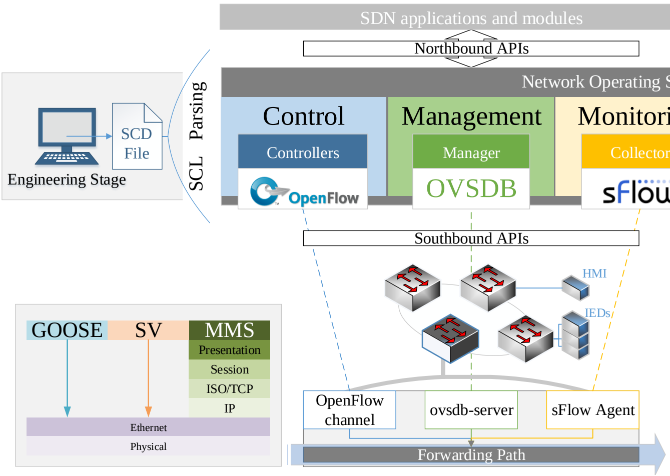
Esquema de tres niveles usado en subestaciones IEC 61850.

de alto nivel mediante métodos tradicionales requiere operar con configuraciones de bajo nivel específicas de los fabricantes de dispositivos de red, lo cual hace difícil obtener un comportamiento flexible y reconfigurable. Además, se ha de proveer alta disponibilidad para aquellos servicios críticos haciendo uso de redundancia dinámica en entornos cableados e inalámbricos. Sin embargo, esto es difícil de lograr haciendo uso de mecanismos de redundancia poco eficientes (p.ej., protocolos de *spanning tree*), o mediante un encaminamiento de los datos independiente del tipo de tráfico (p.ej., únicamente basado en direcciones MAC origen y destino o protocolos como PRP o HSR). Dichos objetivos podrían facilitarse a través de un control centralizado que haga uso de protocolos estandarizados.

Por ello, y de acuerdo a la Recomendación ITU-T Y.3300, el término Software-Defined Networking (SDN) se define como "un conjunto de técnicas que permiten programar, orquestar y gestionar los recursos de red, lo que facilita el diseño, provisión y operación de los servicios de red de una forma dinámica y escalable”. En (Kim & Feamster, 2013) se resumen las posibilidades de mejora en la gestión a través de este paradigma, pudiendo llevar a cabo un control flexible del plano de datos mediante tecnologías estandarizadas.

Propuesta para aplicar las SDNs a las redes industriales

Se propone una solución SDN que permite implementar mecanismos automatizados de ingeniería de tráfico en los sistemas IEC 61850, consiguiendo un control de la red más flexible. En la siguiente figura se ilustran los diferentes elementos de la arquitectura propuesta, incluyendo la pila de protocolos existente en los sistemas IEC 61850. Así, el protocolo OpenFlow junto con otras tecnologías de monitorización y gestión son usados para establecer políticas de tráfico acorde a su prioridad y estado de la red.



Arquitectura SDN propuesta.

Además, se mapea la información de configuración de una subestación, y se traslada a la plataforma de gestión y control. Por tanto, se consigue unificar el proceso de diseño de la infraestructura eléctrica con la configuración de la red. Esta propuesta resulta apropiada para automatizar la administración de una red, lo cual fue visto como necesario por (Ingram et al., 2011), donde se sugiere que “la complejidad de la configuración de la red de datos para subestaciones grandes hace que la gestión automatizada de *switches* sea una opción atractiva [...] herramientas de automatización podrían ser implementadas para extraer información de filtrado VLAN y multicast para configurar *switches* de múltiples fabricantes".

Algunas de las características principales de esta solución son:

- Filtrado de tráfico y calidad de servicio: la arquitectura permite, de forma centralizada, la generación e instalación automática de reglas de encaminamiento, así como el establecimiento de políticas de control de consumo de ancho de banda para diferentes tipos de flujos.

- Despliegue de políticas de seguridad: la plataforma permite establecer reglas que restrinjan el tráfico de los dispositivos desconocidos. Además, pueden determinarse umbrales de monitorización asociados a diferentes flujos de forma que, en caso de ser sobrepasados, se establezcan las acciones pertinentes

- Uso eficiente de recursos redundantes y mejora de protocolos de redundancia activa: la solución propuesta permite computar los caminos más cortos entre los diferentes nodos finales, así como balancear la carga en la red. Por otro lado, se consigue un mejor rendimiento de los protocolos PRP y HSR en términos de disponibilidad y consumo de recursos.

Validación

Como resultado, la evaluación de la idoneidad de las soluciones ha sido llevada a cabo, principalmente, mediante la emulación de distintas topologías y tipos de tráfico. Se ha estudiado analítica y experimentalmente cómo afecta a la latencia el poder reducir el número de saltos en las comunicaciones con respecto al uso de un árbol de expansión, así como balancear la carga en una red de nivel 2. Se ha realizado un análisis de la robustez alcanzada con la combinación del protocolo PRP con un control llevado a cabo mediante OpenFlow. Asimismo, se ha presentado un estudio sobre la mejora de la eficiencia en el uso de los recursos de red al combinar redes HSR y un control del tráfico basado en la criticidad del mismo. Dicho estudio incluye la comparación con el comportamiento estándar del protocolo, así como con propuestas de otros autores.

Conclusiones

Las distintas contribuciones de la presente tesis muestran cómo una plataforma basada en tecnologías SDN permite configurar los elementos de una red industrial a través de una interfaz común. La arquitectura propuesta obtiene una visión global de la topología y recursos disponibles y se beneficia de la programabilidad de las SDN, automatizando la configuración de recursos y aportando técnicas de diagnóstico de las condiciones de red. Así, usar un agente externo permite llevar a cabo el control dinámico de flujos con diferentes prioridades, incluyendo filtrado y catalogación de tráfico, balanceo de carga, o servicios de seguridad de red.

Los resultados de la presente investigación han sido recogidos en diez publicaciones, de los cuales cinco[1] son artículos publicados en revistas indexadas en el Journal Citation Reports (JCR), y el resto en conferencias nacionales e internacionales.

Referencias

- F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, “Smart Transmission Grid: Vision and Framework,” *Smart Grid, IEEE Transactions on*, vol. 1, no. 2, pp. 168–177, Sep. 2010.
- H. Kim and N. Feamster, “Improving network management with software defined networking,” *Communications Magazine, IEEE*, vol. 51, no. 2, pp. 114–119, Feb. 2013.
- D. Ingram, P. Schaub, and D. Campbell, “Multicast traffic filtering for sampled value process bus networks,” in Industrial Electronics Society (IECON), Conference on, pp. 4710–4715, 2011.

[1] Uno de los artículos considerados ha sido aceptado por la revista científica Computers & Electrical Engineering, pero aún está pendiente de ser publicado.

For all resources, whatever it is, you need more.

The Twelve Networking Truths, RFC 1925

Contents

List of Figures

List of Tables

List of acronyms

ABR	Available-Bit Rate
ACL	Access Control List
ACSI	Abstract Communication Service Interface
AP	Access Point
AFDX	Avionics Full DupleX Switched Ethernet
APDU	Application Protocol Data Unit
API	Application Programming Interface
BDDP	Broadcast Domain Discovery Protocol
CBR	Constant Bit Rate
CCA	Controlled Channel Access
CENELEC	Comité Européen de Normalisation Electrotechnique
CEN	Comité Européen de Normalisation
CLI	Command Line Interface
COTS	commercial off-the-shelf
CPS	Cyber-Physical System
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DAN	Double Attached Node
DHCP	Dynamic Host Configuration Protocol
DMZ	demilitarized zone
DoS	Denial of Service
EMS	Energy Management System
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute

ForCES	Forwarding and Control Element Separation
GOOSE	Generic Object Oriented Substation Event
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HMI	Human Machine Interface
HSR	High-availability Seamless Redundancy
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electrical Device
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPFIX	IP Flow Information Export
IS-IS	Intermediate System to Intermediate System
IT	Information Technology
JSON	JavaScript Object Notation
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LN	Logical Node
LRE	Link Redundancy Entity
LSDU	Link Service Data Unit

MAC	Media Access Control
MAN	Metropolitan Area Network
MMS	Manufacturing Message Specification
MOM	Manufacturing Operations Management
MPLS	Multiprotocol Label Switching
MPTCP	Multipath TCP
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time To Repair
MU	Merging Unit
NCS	Networked Control System
NIST	National Institute of Standards and Technology
NMS	Network Management System
NOS	Network Operating System
OAM	Operations, Administration and Management
ONF	Open Networking Foundation
OSI	Open Systems Interconnection
OT	Operational Technology
OVSDB	Open vSwitch Database Management Protocol
OVS	Open vSwitch
PCE	Path Computation Element
PCF	Point Coordination Function
PLC	Programmable Logic Controller

PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
PWG	Public Working Group
QoS	Quality of Service
RBD	Reliability Block Diagram
RCT	Redundancy Control Trailer
REST	Representational State Transfer
RPVST+	Rapid Per-VLAN Spanning-Tree Plus
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
SAN	Single Attached Node
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition
SCD	Substation Configuration Description
SCL	System Configuration description Language
SCSM	Specific Communication Service Mapping
SDN	Software-Defined Networking
SGAM	Smart Grid Architecture Model
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPB	Shortest Path Bridging
SV	Sampled Value
TDMA	Time Division Multiple Access
TRILL	Transparent Interconnection of Lots of Links
TSCH	Time Slotted Channel Hopping

TSN	Time-Sensitive Networking
TTEthernet	Time-Triggered Ethernet
UCA	Utility Communication Architecture
VBR	Variable-Bit Rate
VLAN	Virtual LAN
VL	Virtual Link
WAMS	Wide Area Measurement System
WAN	Wide Area Network
WLAN	Wireless LAN
WSN	Wireless Sensor Network
XML	eXtensible Markup Language

Things are always at their best in the beginning

Blaise Pascal, Provincial Letters

1
Introduction

Contents

Traditional Industrial Control Systems (ICSs) are converging to advanced Cyber-Physical Systems (CPSs) that integrate monitoring, coordination, control and communication functions to interact with physical elements. In fact, CPSs are emerging in many different fields, being especially relevant in the context of automation systems where sensors, controllers and actuators use communication networks to exchange information about safety-critical[1] processes and physical functions.

This work is focused on applying the SDN paradigm into industrial systems in order to improve the control and robustness of critical data

[1] The term safety-critical systems is used to refer to those infrastructures where some actions or failures could cause damage to people or equipment, and result in significant economic losses. Examples of safety-critical systems include avionics, intelligent transportation systems, military equipment, medical devices, power grid control systems, etcetera.

traffic, as well as the efficiency of redundant, and even wireless, networks. The key terms that highlight the scope of this dissertation are:

Management of critical networks
High-availability
IEC 61850
IEC 62439
Industrial Ethernet networks
Industrial wireless networks
OpenFlow
Reliability
Seamless redundancy
Smart Grid
Software-Defined Networking
Substation automation

This chapter provides a brief overview of mission-critical industrial systems.

1.1 Background and context

Recently-coined terms, such as for example, Industry 4.0 [1], the Fourth Industrial Revolution or Industrial Internet, revolve around the use of CPSs; that is to say, complex architectures where physical entities or processes are remotely controlled by cyber-components. These components are in charge of performing the configuration of communication capabilities and the data-processing functions, as sketched in Figure 1.1. The purpose of this figure is to illustrate the communication between the physical domain, formed by networked nodes, and the cyber domain, where the control plane should ensure satisfactory performance in meeting different requirements related to system manageability, security, reliability, and so on. Figure 1.1 also shows a wide range of mission-critical applications, such as transportation, industrial automation systems or electrical power grids, and some illustrative scenarios that have received considerable attention in recent years. In particular, networks in power supply facilities are considered in this thesis as they have been identified as the spearhead of future industrial automation environments. Specifically, despite the fact that electric power systems comprise a variety of domains and subsystems, this thesis focus on Substation Automation Systems (SASs), and in particular, on those based on the IEC 61850 standard.

CPSs have emerged on the basis of ICSs, where data acquisition and processing elements of an Networked Control System (NCS) are tradi-

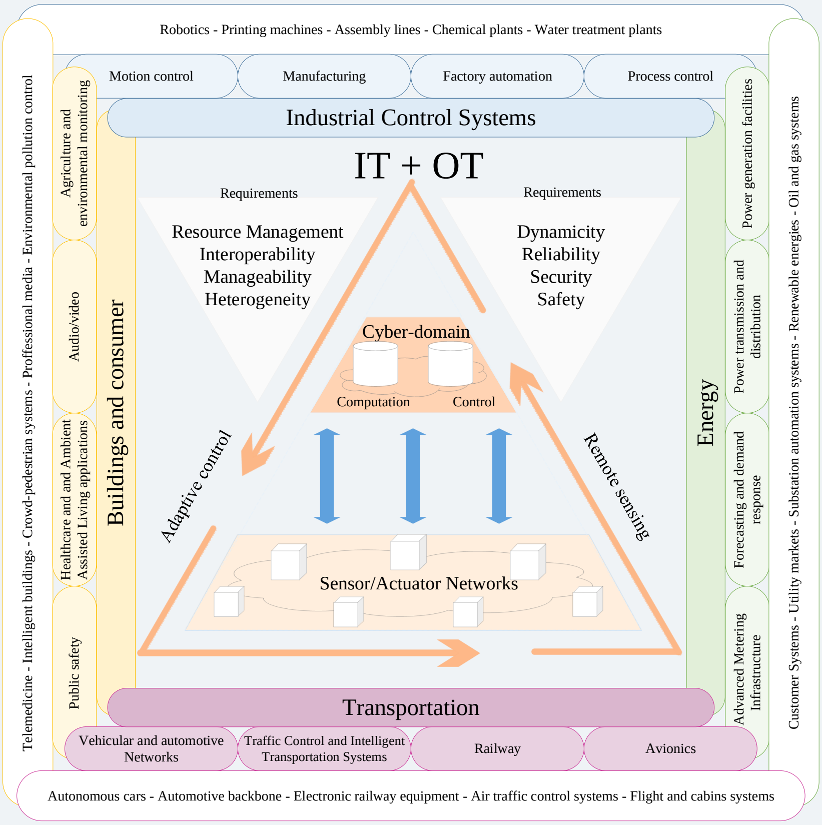

Robotics - Printing machines - Assembly lines - Chemical plants - Water treatment plants
Motion control
Manufacturing
Factory automation
Process control
Industrial Control Systems
IT + OT
Requirements
Resource Management
Interoperability
Manageability
Heterogeneity
Requirements
Dynamicity
Reliability
Security
Safety
Cyber-domain
Computation
Control
Adaptive control
Remote sensing
Sensor/Actuator Networks
Transportation
Vehicular and automotive Networks
Traffic Control and Intelligent Transportation Systems
Railway
Avionics
Autonomous cars - Automotive backbone - Electronic railway equipment - Air traffic control systems - Flight and cabins systems
Telemedicine - Intelligent buildings - Crowd-pedestrian systems - Proffessional media - Environmental pollution control
Agriculture and environmental monitoring
Audio/video
Healthcare and and Ambient Assisted Living applications
Public safety
Buildings and consumer
Energy
Power generation facilities
Power transmission and distribution
Forecasting and demand response
Advanced Metering Infrastructure
Customer Systems - Utility markets - Substation automation systems - Renewable energies - Oil and gas systems

Figure 1.1: CPS feedback operation, use cases and requirements.

tionally arranged in hierarchical levels and applications, as can be seen in the ANSI/ISA-95 model [2]:

- *Field*: Input/Output physical processes.
- *Control*: Programmable Logic Controllers (PLCs) and other intelligent devices.
- *Process control*: Human Machine Interface (HMI) and Supervisory Control And Data Acquisition (SCADA) functionalities.

- *Plant management*: Manufacturing Operations Management (MOM) and Batch execution systems.

- *Enterprise*: Enterprise Resource Planning (ERP) systems.

The differences between industrial and conventional networks have been described in surveys [3], [4]. It is remarkable the impact of service failure severity and the stringent latency requirements. In addition, these authors detailed specific industrial Ethernet stack implementations, and highlight the industrial wireless communication as an important current research area. Both studies reflected an evolution from heterogeneity of isolated networks towards heterogeneous systems that share the same network infrastructure, using the standard TCP/IP stack. According to Sauter et al. [3], a common integration strategy in heterogeneous network environments had been to introduce middleware schemes for translating protocols and dynamically adjust QoS parameters. However, these adaptation layers are usually complex and resource consuming. The same authors envisioned that a combination of Institute of Electrical and Electronics Engineers (IEEE) 802-based networking solutions in both wired and wireless domains tends to facilitate seamless network integration. Thus, converging technologies reduce the number of gateways and simplify the overall management.

In this way, nowadays advanced industrial systems are adopting multi-service networks to optimize the usage of resources. For example, focused on the interoperability, the use of the Ethernet standard (ISO/IEC/IEEE 8802-3) allows industrial systems to reuse existing Information and Communication Technology (ICT) management tools. Besides, since vendor dependence increases complexity in the management process based on non-open interfaces, proprietary legacy systems are being replaced, moving towards interoperable solutions. Yet, according to the IEC 61158 and IEC 61784 specifications, there are a plethora of Ethernet-based technologies that, among other topics, add real-time features on top of link layer. Due to this segmentation, today there is a growing need to harmonize the different Ethernet-based communications, and thereby to avoid vendor-specific implementations. The importance of this topic can be understood with emerging efforts, such as the IEEE 802.1 Time-Sensitive Networking (TSN) Task Group [5], whose goals are to provide reliable communication over Ethernet, ultra-low and deterministic end-to-end latency. This project is considered a new extended generation of the IEEE Audio Video Bridging (AVB) protocol (IEEE 1722) for general mission-critical scenarios.

In the same context, regarding Internet Engineering Task Force (IETF) initiatives, whose interest lies in the upper layers, the recently-formed Deterministic Networking (DetNet) group aims to establish time-sensitive solutions in Wide Area Networks (WANs).

1.2 Motivation and problem statement

From another point of view, until now, the design of industrial automation networks has been based on an isolation model. However, despite the previously mentioned levels representing a hierarchical architecture, a CPS tends to be designed as a network of interacting physical and computational elements that form a dynamic flatter information-driven infrastructure [6]. Thus, the significance of the CPSs lies on a fully integration between production processes and communications. As a result, emerging CPSs pose new challenges to the current network architectures, being necessary to design communication systems that enable dynamic performance, where changes in physical device settings involve responses from the network configuration.

Specifically, the Smart Grid, being a significant industrial case study, is a broad concept that encompasses monitoring, protection, and control of electric power systems. However, according to [7], “communication technologies are not yet mature for the revolution of transmission grids, and the existing grids lack enough compatibility to accommodate the implementation of spear-point technologies in the practical networks”. The same authors predicted that adaptive networks would allow open-standardized communication protocols to operate on a unique platform. As also stated by the authors, “real-time control based on a fast and accurate information exchange in different platforms will improve system resilience by enhancing the reliability and optimization of the transmission asset utilization”.

The cooperative interaction between network protocols and advanced control systems will provide a new ecosystem for future CPS applications. This gives the Software-Defined Networking (SDN) paradigm the opportunity to play a leading-edge role in building CPSs. Software-defined networks are those in which “the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network is abstracted from the applications” [8]. Standardized protocols, such as OpenFlow [9], Forwarding and Control Element Separation (ForCES, RFC 5810) or the combination of the Path Computation Element Protocol (PCEP, RFC 5440) and BGP Link-State Distribution (BGP-LS) schemes allow external entities to have a global view of the network. Particularly, the OpenFlow protocol, which has special relevance to this study, allows an independent controller to set and modify the network data paths by using flow-based forwarding rules.

SDN technologies are being commonly used in data center and telecom environments, whereas industrial networks are an application domain that have received little attention so far. The motivation for focusing on the latter is that the provided programmability may also be adequate to meet strict QoS constraints imposed by safety-critical systems. Besides, in industrial applications, it is necessary to develop mechanisms for ensuring network performance, including security and reliability, such that the provided services are not jeopardized. Besides, the design of industrial networks must meet the requirements of flows with different priorities, such as maximum latency, minimum throughput or maximum recovery time in case of failure. In terms of availability and robustness, “although the time latency associated with availability can vary, it is generally considered the most critical security requirement”, in accordance with the Guidelines for Smart Grid Cyber-Security [10] issued by the National Institute of Standards and Technology (NIST).

Therefore, the design of a network requires a robustness study, which is closely related to the use of techniques that minimize service downtime, frame losses, delay, jitter, and, in general, network vulnerabilities affecting the stability of the entire system. As a rule, network reliability and resilience are improved avoiding single points of failure and, toward this end, deploying redundant nodes and links reduces the interruption time in case of faults. Thus, redundancy is generally the most widely used methods for preventing the disruption of the normal operation of an infrastructure. Nevertheless, the fact is that nowadays Ethernet Local Area Networks (LANs), to which safety-critical environments are tending, are usually based on traditional spanning tree protocols that prevent loops at the expense of disabling redundant paths. Namely, they are configured in active-passive mode, so that protection links are used as spare elements. This, along with a forwarding scheme only based on Media Access Control (MAC) learning, means that traffic flows cannot be balanced or forwarded along the shortest paths, so that network resources are not efficiently utilized.

Furthermore, there are several reasons why the IEC 61850 standard has been chosen as a research subject. First, it is an evolving standard that includes, inter alia, communication services and network architectures based on Ethernet LANs for power automation systems. This standard defines protocols to transmit monitoring and control data, which pose stringent performance requirements (e.g. bandwidth or delay) on the underlying network infrastructure. This way, communication management systems have to deal with time-sensitive flows requiring minimal latency and loss of information. Indeed, another compelling reason to focus this thesis on the IEC 61850 standard is that it defines communication profiles that require seamless connectivity, which makes necessary the use of active redundancy strategies to reduce the recovery time in the presence of network failures. However, despite new insights have expanded the Ethernet standards to be redundant, there are not many options to provide zero recovery time in LANs. Among them, this study focuses on the Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) protocols, which have been recently standardized by the IEC and adopted by the IEC 61850 to protect critical services. However, it is necessary to improve performance of these technologies; for example, increasing the efficiency in bandwidth consumption is a primary goal of this work. To achieve this objective, the OpenFlow technology can be adopted. Therefore, it is a relevant and challenging case study to test new SDN-based approaches.

Moreover, even though wireless technologies have been proposed for automation systems from 1988 [11], existing radio technologies posed significant problems to be overcome in these environments. In this regard, industrial networks have traditionally used wired communications for transmission of critical information. However, as identified in [12], it emerges the need for wireless monitoring and control systems, which reduce installation and maintenance costs compared to wired ones.

Moreover, these scenarios more frequently require the interconnection of mobile nodes, as well as rapid network deployment and configuration. Therefore, although still in an early stage of development, wireless solutions offer numerous advantages for the industry automation. In particular, IEEE 802.11-based Wireless LANs (WLANs) will be analyzed in this work. In such a case, since wireless links suffer from unreliable data transmission due to non-deterministic factors, these networks should ensure continuity of operations, so that availability and performance are not affected.

From these motivations, several objectives have been addressed in this research.

1.3 Objective of the thesis

In order to contribute to the development of future Software-Defined Cyber-Physical Networks, the aim of this work is summarized below.

1.3.1 Thesis statement

For the purpose of maintaining proper network performance, management and control functions have to be aware of the network resources and traffic requirements. Limitations of traditional networking capabilities have led to the analysis of the potential benefits of SDN technologies on critical industrial networks (e.g., substation automation) and how the stringent requirements can be met. The resulting thesis statement is:

> *Using SDN technologies allows mission-critical systems to achieve greater levels of network resources management capabilities, while meeting QoS requirements. Moreover, demanding protection and control applications can operate with high reliability through a flow-based traffic processing approach.*

1.3.2 Research questions and aims

This dissertation is motivated by the following open issues[2]:

- How does the use of SDN technologies impact on industrial networks, such as IEC 61850-based systems? RQ1
- Could software-defined networks improve performance characteristics of redundancy protocols used in high-availability systems? RQ2

As a consequence, this thesis is structured into two separate dimensions, including the following research objectives:

- To study how to improve the network management and control of IEC 61850 networks by using SDN technologies.
  - With this aim, an overview of the communication model of this standard shall be provided.
  - In this research goal, it is necessary to analyze pros and cons of an SDN approach over the use of traditional networks for critical industrial infrastructures.
  - To define a software-defined architecture to provide advanced features to support the IEC 61850 protocol stack, such as QoS or security.
  - The proposed framework should implement monitoring and management tasks that build a global view of network utilization, allowing it to act quickly and accurately, and even providing new levels of network security.
- To provide a software-defined approach to efficiently control redundant topologies.
  - To achieve lower latencies, which is an essential requirement in critical, time-sensitive applications, it is necessary to ana-

[2] Margin notes are used to point out important concepts being discussed in the paragraphs next to them. For example, in this case, research questions are highlighted to draw the reader's attention.

lyze the relation between the network meshing and load balancing with the latency.

- It is required to determine the potential of the SDN paradigm in achieving a better utilization of available resources in situations of active redundancy; as well as to facilitate its management and increasing responsiveness, also considering the challenges of a centralized approach.
- To assess the overall effect of combining the OpenFlow and parallel redundancy protocols.
- To meet this objective, it is also necessary to study the possibility of resisting multiple network failures without interruption, by establishing multiple redundant paths.
- To consider heterogeneous network infrastructures, even considering the deployment of wireless technology in critical industrial environments.

The decision of choosing an SDN approach is supported by qualitative arguments throughout this dissertation. Otherwise, in order to address these research questions and to evaluate the proposals, this work relies on analytical and emulation-based results, which demonstrate the feasibility of them from a performance perspective.

1.4 Thesis outline

The structure of this document is made to reflect the two main objectives of the thesis. Thus, the remainder of this thesis is organized as follows:

Chapter 2: Literature review This chapter encompasses the state-of-the-art of Smart Grid communications. After giving a general description of electric power delivery systems in Section 2.1, Section 2.2 provides an overview of the basis of the IEC 61850 standard. Likewise, specific QoS metrics illustrate key requirements of industrial networks. Section 2.3 analyzes the relationship between redundancy and availability, and it presents a general review of layer 2 redundancy protocols, outlining the characteristics of PRP and HSR. Moreover, Section 2.4 explores the opportunities of wireless networks in critical systems. Also, Section 2.5 describes the main features of SDN and the OpenFlow protocol. Findings and requirements detailed throughout the chapter are summarized in Section 2.6.

Chapter 3: A proposal for applying SDN in industrial networks An application case is given in Section 3.1. Section 3.2 presents an overall architecture that fulfills requirements previously identified. The solution approach is detailed in Section 3.3, where the main control and management technologies used in the proposal, and the offered services are explained. Section 3.4 focuses on how the proposed architecture can be used in redundant networks, as well as its integration with PRP and HSR to enhance their performance.

Chapter 4: Validation and discussion This chapter contains the technical implementation of the proposals and it discusses the functional and performance evaluation results, demonstrating how an SDN framework can accommodate diverse and stringent requirements of industrial networks.

Chapter 5: Conclusion Finally, directions for further research and conclusions are drawn. In addition, this chapter lists the publications derived from this research.

This is state-of-the-art, for right now

Andrew Adamson, Shrek

2

Literature review

Contents

This chapter discusses related work and presents some characteristics and trends of the Smart Grid development. As a representative model, the IEC 61850 standard is focused on communication networks in power automation systems, which impose diverse industrial-grade requirements, detailed below. To facilitate an easier understanding of the needs and motivations of this research, throughout the document a series of margin notes will briefly highlight some relevant general network requirements. Once gathered all needs, qualitative design goals are specified at the end of this chapter.

2.1 Smart Grid

Electric utilities must accomplish the primary mission of providing power supply in transmission and distribution grids. Adding intelligence to the delivery processes is associated with quality management and cost efficiency of the whole energy system. Indeed, according to the definition of Smart Grid provided by the European Telecommunications Standards Institute (ETSI) [13], "a Smart Grid is an electricity network that can cost efficiently integrate the behavior and actions of all users connected to it –generators, consumers and those that do both –in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety".

Smart Grid industry makes use of ICT infrastructures for the management of the generation, storage, transmission, distribution and consumption of electrical energy to increase the efficiency of remote control and automation systems. Figure 2.1 illustrates the different systems that support an end-to-end Smart Grid architecture, being consistent with the Smart Grid conceptual model of the NIST [14] which includes seven functional domains:

- Markets
- Service Providers
- Customer
- Operations
- Generation
- Transmission
- Distribution

Communications in transmission and distribution infrastructures are crucial for proper operation of this large-scale CPS, where real-time power grid operations take place (e.g., control signals between transformers, relays, circuit breakers, etcetera), as well as the connection with back-office Energy Management Systems (EMSs) and Wide Area Measurement Systems (WAMSs). These operations include monitoring equipment and transformers, measuring power quality and fault management.

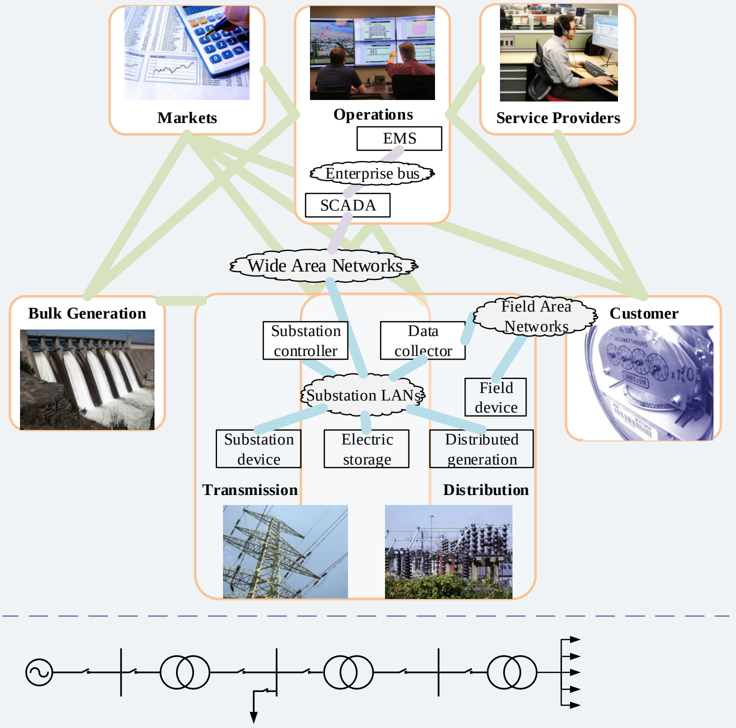


Figure 2.1: Smart Grid domains [14] and a simplified single line diagram of the grid model.

2.1.1 SGAM framework

The reference Smart Grid Architecture Model (SGAM), defined by the CEN–CENELEC–ETSI Smart Grid Coordination Group [15], can be used to identify and describe the mapping of the use case in question, SASs, into an entire Smart Grid architecture decomposed in a layered three-dimensional model (Figure 2.2). Each layer (interoperability dimension) includes the activities and actors in a plane with vertical (zones) and horizontal (domains) dependencies. The latter represent the "energy conversion chain", whereas the vertical axis reflects the "hierarchical levels of power system management". In focusing on ICT within substations, the relations in information, communication and, to a lesser extent on component layers, are:

- The first layer represents the data models and information exchanged between functions, services, and components. They can be identified by analyzing the information exchanged between the actors. It corresponds with the presentation and application layers in the Open Systems Interconnection (OSI) reference model.
- The communication layer, corresponding to the first five layers of the OSI model, consists of suitable protocols and mechanisms for exchanging that information and the data models allocated in the upper layer. It has to take into account the different service requirements.
- Finally, the component layer is derived from the actors involved in the use case, comprising physical components such as assets, devices, grid equipment and operators.

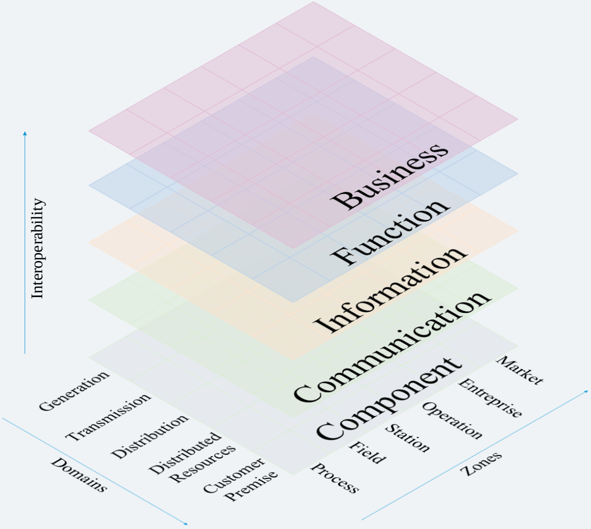


Figure 2.2: Entire layered three-dimensional model in agreement with the SGAM framework.

According to the domains that form the energy conversion chain, substations transfer power from the transmission to the distribution network. Hence, they include high-voltage (HV) and medium-voltage (MV) equipment; whereas among the zones of power system management, the use case is situated on the station zone. This zone encompasses the aggregation of the field level (equipment to monitor, protect and control) and connects with the operation zone (power control operation).

2.1.2 Convergence and standardization

Due to the fact that Operational Technology (OT) is generally associated with low latency and high-robustness requirements, power utilities and industrial plants have separated them from the Information Technology (IT) infrastructure, which includes a variety of complex computing, networking, and security systems. However, as introduced in Section 1.2, driven by the use of Ethernet and TCP/IP in automation systems, management functions tend to overlap, which means that maintenance and operating costs can be reduced by using common resources [16]. In this way, the IT and OT convergence implies that requirements, resources and security are managed in a consistent manner, which can be accomplished by employing a unified management interface.

From another point of view, power utility automation is a representative example of mission-critical system where interoperability is required for seamlessly transferring power control data. Among different standardization bodies, it is important to emphasize that the International Electrotechnical Commission (IEC) is currently the most important one in this area. While the Technical Committee 65 is responsible for standardizing industrial-process measurement and control systems, working groups of the IEC Technical Committee 57 have the purpose of providing a reference architecture for power management and acquisition and exchange of the associated information. Particularly, the IEC 61850 standard, entitled “Communication Networks and Systems for Power Utility Automation”, is being adopted worldwide for the design of electrical substations, and transmission and distribution networks. So, it is considered as a core IEC project for the Smart Grid Development [17]. Figure 2.3, based on [15], shows key IEC standards for the Smart Grid, where the IEC 61850 is placed in field and station levels of utility automation environments, whereas other standards, such as the IEC 61970 or the IEC 61968, are targeted to define common interfaces and data models for components in power systems, which are widely used in EMS by utilities worldwide. Also, IEC 61508 and IEC 62351 define safety and security aspects, respectively, which can be seen as common issues for all domains.

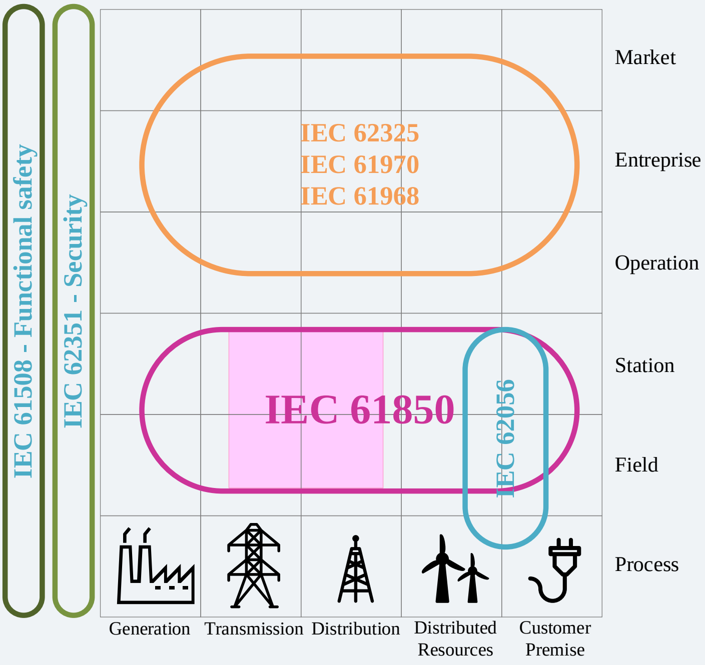


Figure 2.3: Domains of core IEC Smart Grid standards.

From a historical perspective, because of the variety of protocols emerging over the last decades to support power protection and control systems, the IEC 61850 was originally developed with the goal of unifying the Utility Communication Architecture (UCA) and European standards, and it is based on the earlier work of legacy protocols. Yet, besides the IEC 61850 and proprietary solutions, other standardized technologies should also be considered. The following ones have been among the most used in the communication of Remote Terminal Units (RTUs), SASs and control centers:

- Modbus TCP/IP specifies a master-slave communication model. It is considered too simple and inefficient. For example, slaves cannot start a new connection to the master, nor there are "common data formats between devices" [18].
- IEEE 1815 Distributed Network Protocol (DNP3) and IEC 60870-5-104 standards define protocols used for telecontrol in power system automation applications. They are mainly used for communicating RTUs or Intelligent Electrical Devices (IEDs) with a master station.

DNP 3.0 and IEC 60870-5-101 achieved wide market acceptance in USA and Europe, respectively. However, compared to these previous technologies, IEC 61850 is now more flexible and includes more functionalities, allowing the design of power automation system as a whole, beyond the pure protocol level between devices. Other specific advantages can be found in [18]. Moreover, in any case, IEC 61850-based systems generally include protocol converters to support legacy or other technologies, as specified in 61850-80-x documents (Table 2.1). For all these reasons, the IEC 61850 is one of the most advanced protocols for SCADA communications, and may be considered the successor to DNP3 and IEC 60870. In fact, although, as mentioned above, DNP3 is the de facto standard in the USA energy market, the IEC 61850 standard is increasingly defined as a future benchmark for local communications within a substation.

2.2 IEC 61850-based communication networks: a case study

The main purpose of the emerging IEC 61850 standard is to make substation automation flexible, expandable and cost-effective, by providing interoperability among devices from different manufacturers. As a consequence, the IEC 61850 specification avoids vendor-specific implementations, promoting technology-neutral ones. In this sense, the IEC 61850 communication stack is built on standard-based solutions, such as TCP/IP and Ethernet technologies. Besides this, the IEC 61850 relies on standardized protocols for basic services such as synchronization, security or redundancy.

Table 2.1 shows the structure of the IEC 61850 series, including technical reports (TR). Its first edition was published as an international standard in 2003 and restricted to intra-substation communications (LANs), whereas the second edition[1] covers areas beyond power substations, such as distributed generation systems (photovoltaic, wind and hydro power plants, fuel cells, etcetera) or communications between substations and remote operations centers. Moreover, the IEC 61850 Edition 2 specifies more stringent network requirements such as, for example, using the Precision Time Protocol (PTP, IEEE 1588-2008) instead of the Simple Network Time Protocol (SNTP, RFC 4330) in order to reduce synchronization accuracy. Also, regarding the network availability, the new specifications require higher redundancy for those critical assets which cannot tolerate data loss.

Table 2.1: IEC 61850 standard specifications.

Part	Title	Ed.- Date
-1 TR	Introduction and overview	2- 2013/03
-2	Glossary	1- 2003/03
-3	General requirements	2- 2013/12
-4	System and project management	2- 2011/04
-5	Communication requirements for functions and device models	2- 2013/01
-6	Configuration description language for communication in electrical substations related to IEDs	2- 2009/12
-7	Basic communication structure for substation and feeder equipment	
-7-1	– Principles and models	2- 2011/07
-7-2	– Abstract communication service interface (ACSI)	2- 2010/08
-7-3	– Common Data Classes	2- 2010/12
-7-4	– Compatible logical node classes and data classes	2- 2010/03
-7-410	– Hydroelectric power plants - Communication for monitoring and control	2- 2012/10
-7-420	– Distributed energy resources logical nodes	1- 2009/03
-7-510 TR	– Hydroelectric power plants - Modelling concepts and guidelines	1- 2012/03
-8-1	Specific communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3	2- 2011/06
-9-2	Specific communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3	2- 2011/09
-9-3	Precision time protocol profile for power utility automation	1- 2015/12
-10	Conformance testing	2- 2012/12
-80-1	Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104	1- 2008/12
-80-3 TR	Mapping to web protocols - Requirements and technical choices	1- 2015/11
-80-4	Translation from the COSEM object model (IEC 62056) to the IEC 61850 data model	1- 2016/03
-90-1 TR	Use of IEC 61850 for the communication between substations	1- 2010/03
-90-2 TR	Using IEC 61850 for communication between substations and control centres	1- 2016/02
-90-3 TR	Using IEC 61850 for condition monitoring diagnosis and analysis	1- 2016/05
-90-4 TR	Network engineering guidelines	1- 2013/08
-90-5 TR	Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118	1- 2012/05

[1] The first part of this edition was published in 2011.

Part	Title	Ed.- Date
-90-7 TR	Object models for power converters in distributed energy resources (DER) systems	1- 2013/02
-90-8 TR	Object model for E-mobility	1- 2016/04
-90-12 TR	Wide area network engineering guidelines	1- 2015/07

The IEC 61850 documents cover all topics related to the equipment and interfaces that globally define the configuration of a power substation, either internally or externally, including network engineering guidelines. For this work, the relevant parts of the standard are those focused on the definition of the information model and communication services. These parts are separated with the aim of achieving long-term stability with the set of mappings, found in IEC 61850-8-x and in IEC 61850-9-x, of data objects and services to communication layers. According to the IEC Technical Committee 57, this separation can be summarized as follows:

- IEC 61850
    - Object models
        - IEC 61850-7-3, 7-4, 7-410, 7-420
    - Service models
        - IEC 61850-7-2 ACSI and Generic Object Oriented Substation Event (GOOSE)
    - Profiles and mapping
        - IEC 61850-8 and IEC 61850-9

Before detailing information and communication aspects, it is appropriate to outline a possible logical structure of a substation. Moreover, it is noteworthy that an IEC 61850 compliant system must ensure that the demanding communication requirements specified in IEC 61850-5 are met, which are discussed below from Section 2.2.4.

2.2.1 Substation Automation Systems

Similar to the layered architecture defined in ISA-95 for general ICSs, IEC 61850-based SASs rely on high-speed data acquisition to monitor and track power electronic devices, and they are organized in the following levels:

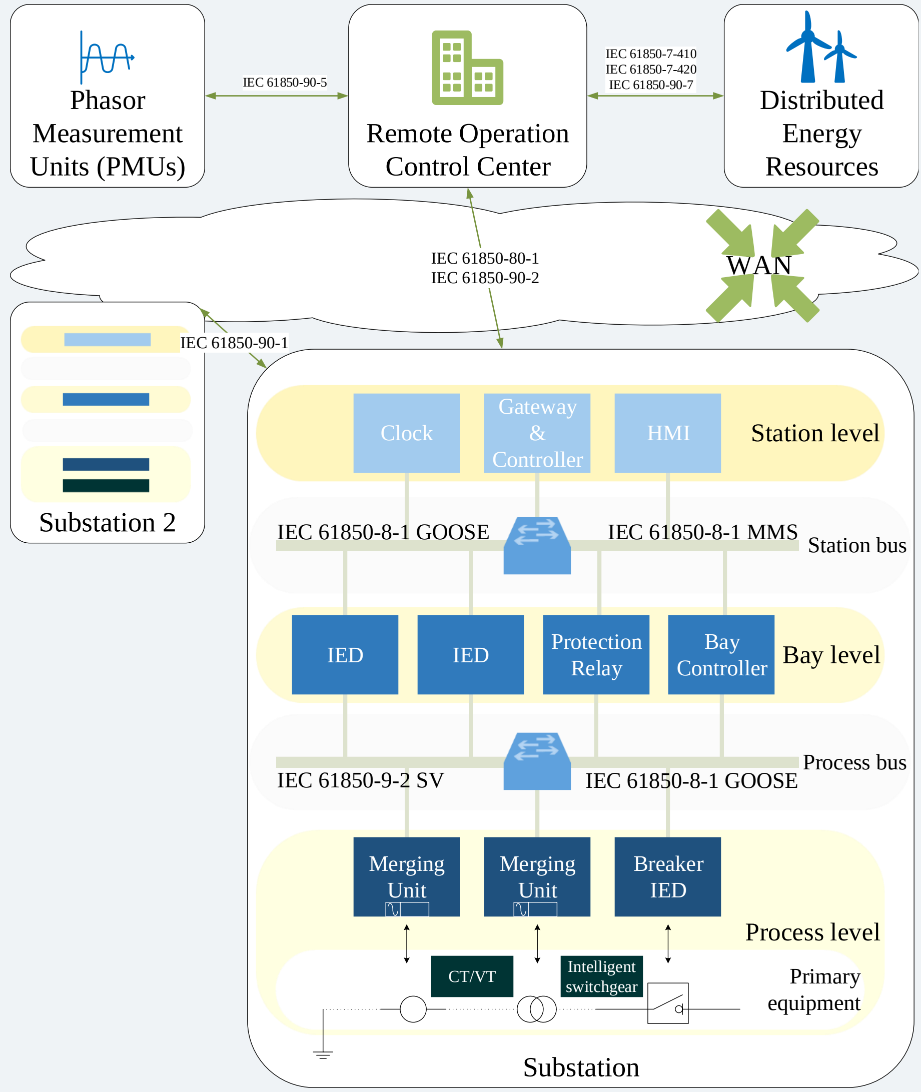


Figure 2.4: Three-level scheme used in IEC 61850-based systems.

- **Process** level: it includes primary equipment, such as instrument transformers, disconnectors or circuit breakers which, for example, are used to open and close switches in electrical switchyards.
- **Bay** level: it includes protection and control IEDs (e.g., sensors, relays, meters, etcetera).
- **Station** level: it is focused on operations and supervision functions, also including relays and gateways to communicate with control centers.

As represented in Figure 2.4, besides this logical architecture, a SAS consists of a process bus and a station bus[2], which allow sensor, monitoring, protection and control units to communicate to each other. The former bus handles data communication among primary process equipment and protective relays, while the station and bay levels are connected through the latter. While the transmission of critical data was generally done via dedicated wires, modern substation communication buses are based on the Ethernet technology in order to displace traditional serial data buses. Figure 2.4 shows different communication protocols (MMS, SV and GOOSE), which will be explained in detail in Section 2.2.3. Likewise, this figure also sketches interfaces for WAN connectivity, that is, to communicate control centers with substations, phasor measurement units or distributed energy resources.

2.2.2 Formal configuration language

The configuration of IEC 61850-based systems is based on object-oriented information modeling. Namely, for example, protection and control equipment are defined objects that exchange standardized data. The information models are included in IEC 61850-7-x documents, which lead to design substations in Logical Nodes (LNs), and characterize their data inputs and outputs following a standard naming convention. In addition, the IEC 61850-6 [19] defines the System Configuration description Language (SCL), based on eXtensible

[2] This is a logical network structure and station and process buses could fit into a single physical network.

Markup Language (XML) schema, to describe and exchange substation parameters, e.g., system topology or IED configurations.

Different SCL file formats are available depending on their objectives. More specifically, the Substation Configuration Description (SCD) files are intended to design and configure a whole substation, including the definition of client-server reports, “data sets”, and SV/GOOSE transmission parameters. Particularly, the communication section of an SCD file allows the definition of operational attributes such as IP addresses, destination MAC addresses or Virtual LAN (VLAN) parameters (i.e., VLAN-Identifier and VLAN-Priority) for each service exposed by a device. However, the current information model is not complete enough to represent the communication network in detail; for example, it does not describe the physical network topology. According to [20], the specification should integrate the network configuration in the unified engineering process of substation automation. In any case, according to the IEC 61850-6 clause 9, SCL files contain five sections: Header, Substation, Communication, IEDs and Datatype template. Below a partial example of an SCD file is given.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<SCL xmlns="http://www.iec.ch/61850/2006/SCL" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.iec.ch/61850/2006/SCL">
    <Header id="SCD Example">...</Header>
        <!--
            This section identifies the version and configuration of the SCL file.
        -->
    <Substation name="Substation_name">
        <!--
            This section defines the functional structure, and includes a list of the available logical nodes with their relation to the primary equipment.
            It can be used to build a single line diagram.
        -->
        <VoltageLevel name="E1">...
            <Bay name="Q1">
                <ConNode Nam="L1"/>
                <Device Nam="QA1" Type="CBR">
                    <LNode Inst="1" LNClass="CSWI" IEDName="AA1"/>
                    <Connection CNodeNam="L1"/>
                </Device>
            </Bay>
        </VoltageLevel>
        <VoltageLevel>...</VoltageLevel>
    </Substation>
    <IED name="LE_IED">
        <!--
            It contains the description and attributes of the different communication services, access points and logical devices and nodes.
        -->
    </IED>
    <Communication>
        <!--
            It determines the configuration of subnetworks (independent of the substation structure) and the connection of IEDs, including also their access points, network addresses and properties.
            It also allows the declaration of GOOSE/SV multicast subscriber information.
        -->
        <SubNetwork name="Subnetwork_name" type="8-MMS">.
            <Text>Station bus</Text>
            <BitRate unit="b/s" multiplier="M">10</BitRate>
        </SubNetwork>
    </Communication>
    <DataTypeTemplates>
        <!--
            This section declares the types of logical nodes and data models.
        -->
    </DataTypeTemplates>
</SCL>
```

This configuration language enables engineering tools for bottom-up system designs. A simple engineering design workflow is represented in Figure 2.5, where IEDs import and export SCL files that include the device-specific configuration data.

2.2.3 Communication services

In addition to the criticality-driven nature, different types of IEC 61850 services are expected. While the IEC 61850-7-2 defines the semantic of the so-called abstract services (Abstract Communication Service Interface, ACSI), the format and encoding of messages that contain the

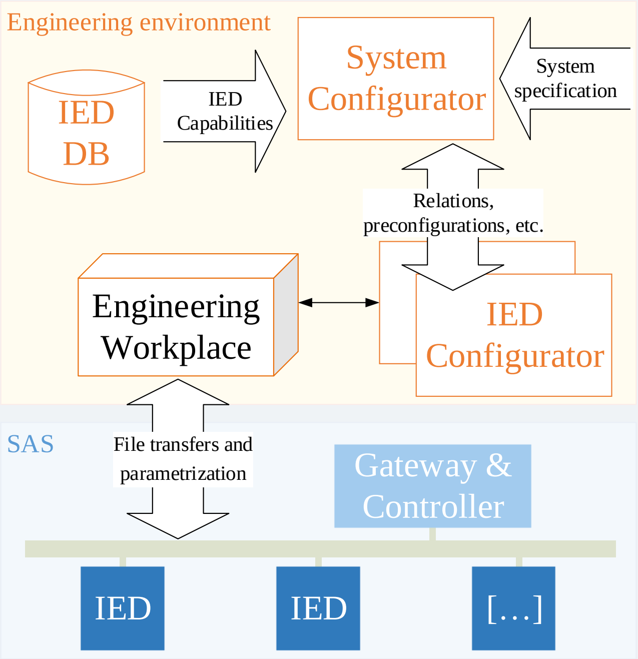


Figure 2.5: IEC 61850 engineering stage and workflow [19].

service parameters are defined in the Specific Communication Service Mapping (SCSM). Concretely, the IEC 61850-8-1 and IEC 61850-9-2 specifications describe communication profiles for teleprotection, measurement and control signals over packet-switched networks. These are mapped to a protocol stack that differentiates two models of communication, as shown in Figure 2.6.

2.2.3.1 Publisher/subscriber scheme

In this model, the following high-priority services are defined:

- IEC 61850-9-2 **Sampled Value (SV)**: analog measures of voltage and current samples generated by transducers. Thus, sequences of status measurements are periodically reported from Merging Units (MUs) to IEDs using unicast or multicast messages. If SVs

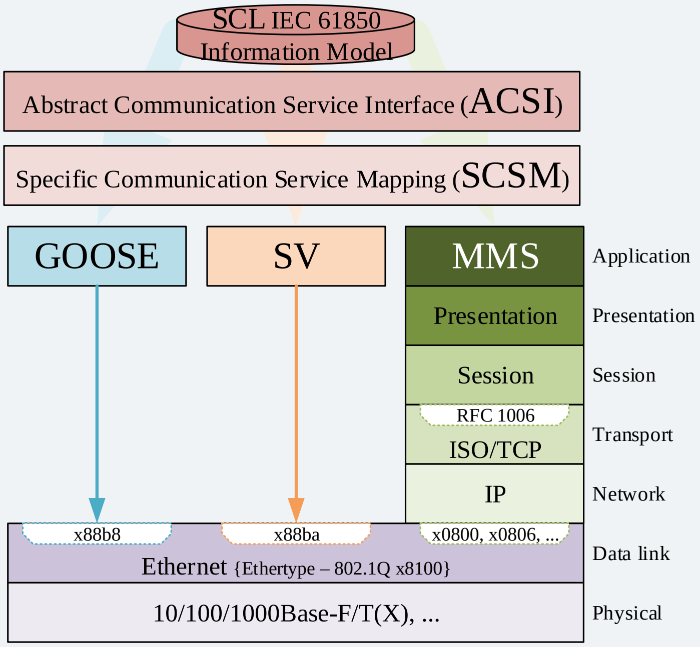


Figure 2.6: Different IEC 61850 communication protocols.

are transmitted in compliance with the 61850-9-2 SV-LE ("Light Edition", [21]) guideline, the frame size must be fixed to 126 bytes, at 4 kHz sampling rate for 50 Hz line frequency (80 samples per nominal cycle). This results in a steady-state rate of 4.032 Mbit/s per merging unit.

- IEC 61850-8-1 **GOOSE**: signals for control and protection operations (e.g., tripping or interlocking actions, as well as diagnostic functions). In this way, a device continuously transmits heartbeat multicast frames, which contains status information (e.g., breaker position indication) that is grouped into "data sets". But moreover, GOOSE frames are immediately sent upon certain events (e.g., notification of an alarm), being retransmitted several times to prevent possible network failures.

As respectively defined in 61850-9-2 and 61850-8-1, Figure 2.7 shows SV and GOOSE frame structures and Wireshark screenshots of example frames. Both Application Protocol Data Units (APDUs) are directly carried in the payload of link layer frames in order to reduce protocol overhead, and consequently, to increase the performance of real-time services. Hence, they are suitable for rapid exchange of time-critical data between MUs and IEDs.

Regarding communications outside the substations (Figure 2.4), that is, between substations or between substations (it is also applicable, for example, to power plants) and control centers, GOOSE and SV messages can be transmitted through tunnel technologies (IEC/TR 61850-90-1 and 61850-90-2) or by using Routable-GOOSE and Routable-SV (IEC/TR 61850-90-5), which are based on TCP or UDP over IP multicast.

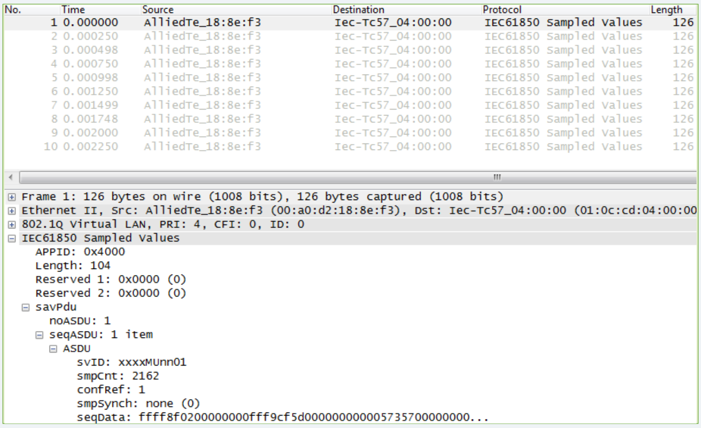
2.2.3.2 Client/server scheme

According to the IEC 61850-8-1 part, this scheme includes, among other data applications, the Manufacturing Message Specification (MMS) protocol (ISO 9506) to exchange, via unicast TCP connections, operational information (e.g., monitoring device information and reports). This low-priority information normally flows from IEDs to the substation administrator (e.g., substation central unit or SCADA), and it is not as low-latency demanding as the previous ones. In fact, according to [22], MMS communications are medium priority, and consist of unconfirmed messages collecting periodic information and confirmed messages for request/response interactions.

2.2.4 Bandwidth and latency requirements

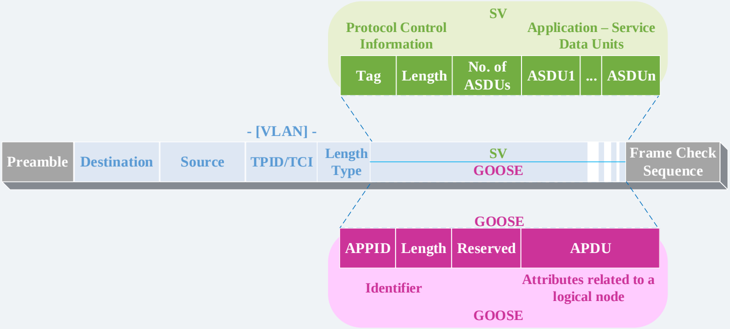
With regard to traffic patterns, like typical ICS applications, IEC 61850 devices generate periodic Constant Bit Rate (CBR) traffic, and aperiodic messages, both Variable-Bit Rate (VBR) and Available-Bit Rate (ABR) traffic.

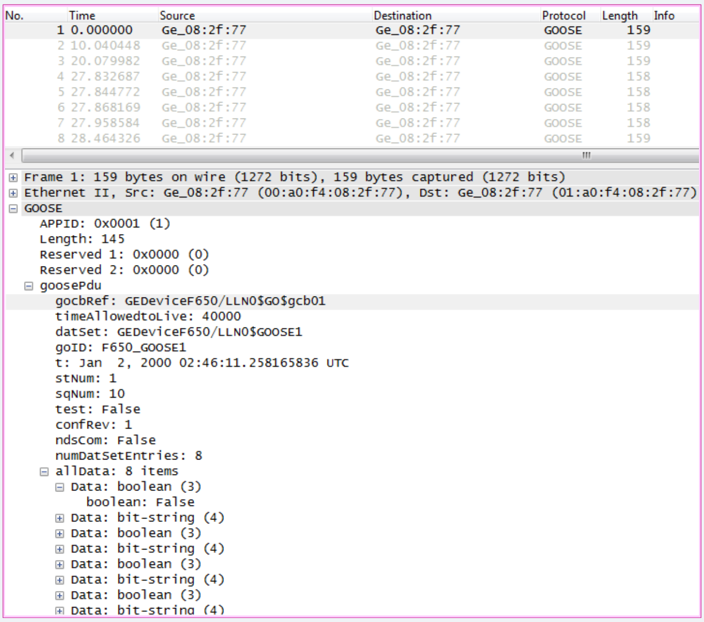
- CBR: SV is used to continuously send measures.



```
No.     Time        Source                 Destination          Protocol                  Length
      1 0.000000    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      2 0.000250    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      3 0.000498    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      4 0.000750    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      5 0.000998    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      6 0.001250    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      7 0.001499    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      8 0.001748    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
      9 0.002000    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126
     10 0.002250    AlliedTe_18:8e:f3      Iec-Tc57_04:00:00    IEC61850 Sampled Values     126

⊞ Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
⊞ Ethernet II, Src: AlliedTe_18:8e:f3 (00:a0:d2:18:8e:f3), Dst: Iec-Tc57_04:00:00 (01:0c:cd:04:00:00
⊞ 802.1Q Virtual LAN, PRI: 4, CFI: 0, ID: 0
⊟ IEC61850 Sampled Values
    APPID: 0x4000
    Length: 104
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ⊟ savPdu
      noASDU: 1
    ⊟ seqASDU: 1 item
      ⊟ ASDU
          svID: xxxxMUnn01
          smpCnt: 2162
          confRef: 1
          smpSynch: none (0)
          seqData: ffff8f0200000000fff9cf5d00000000000573570000000...
```





```
No.     Time          Source             Destination          Protocol   Length   Info
      1 0.000000      Ge_08:2f:77        Ge_08:2f:77          GOOSE        159
      2 10.040448     Ge_08:2f:77        Ge_08:2f:77          GOOSE        159
      3 20.079982     Ge_08:2f:77        Ge_08:2f:77          GOOSE        159
      4 27.832687     Ge_08:2f:77        Ge_08:2f:77          GOOSE        158
      5 27.844772     Ge_08:2f:77        Ge_08:2f:77          GOOSE        158
      6 27.868169     Ge_08:2f:77        Ge_08:2f:77          GOOSE        158
      7 27.958584     Ge_08:2f:77        Ge_08:2f:77          GOOSE        158
      8 28.464326     Ge_08:2f:77        Ge_08:2f:77          GOOSE        159

⊞ Frame 1: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
⊞ Ethernet II, Src: Ge_08:2f:77 (00:a0:f4:08:2f:77), Dst: Ge_08:2f:77 (01:a0:f4:08:2f:77)
⊟ GOOSE
    APPID: 0x0001 (1)
    Length: 145
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ⊟ goosePdu
      gocbRef: GEDeviceF650/LLN0$GO$gcb01
      timeAllowedtoLive: 40000
      datSet: GEDeviceF650/LLN0$GOOSE1
      goID: F650_GOOSE1
      t: Jan  2, 2000 02:46:11.258165836 UTC
      stNum: 1
      sqNum: 10
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 8
    ⊟ allData: 8 items
      ⊟ Data: boolean (3)
          boolean: False
      ⊞ Data: bit-string (4)
      ⊞ Data: boolean (3)
      ⊞ Data: bit-string (4)
      ⊞ Data: boolean (3)
      ⊞ Data: bit-string (4)
      ⊞ Data: boolean (3)
      ⊞ Data: bit-string (4)
```

Figure 2.7: SV and GOOSE frame structures and Wireshark screenshots.

	Protocol	Frame size (B)	Frames/s
Critical	SV	126	4000
	GOOSE	92-250	1-200
Non-critical	MMS	100-700	20-60
	SNMP	150-500	20
	Others	60-90	3

Table 2.2: Data traffic patterns of IEC 61850-based systems.

- VBR: GOOSE to periodically transmit messages and send data bursts upon the occurrence of a trigger.
- ABR: MMS to asynchronously transmit general purpose and supervisory control data.

Concerning the size and volume of data traffic, digital measurements are usually carried in small packets [4]. Data traffic patterns of systems operating under the IEC 61850 can be extracted from [23], [24] and are shown in Table 2.2, where SV messages are the most demanding ones due to their relatively high frequency.

Regarding latency, specific delay requirements for several industrial applications are summarized in [25]. In the case of IEC 61850-based systems, maximum transmission times depend on the protection and control applications thereof (the so-called "performance class"). Hence, according to the IEC 61850-5 specification [26], the most stringent services, such as SV raw data or GOOSE messages to provide teleprotection commands, or implement inter-tripping between circuit breakers, can tolerate a maximum "transfer time" (defined as depicted in Figure 2.8) of 3 ms, which must be guaranteed independently of the network condition. On the other hand, MMS may require up to 100 ms for "medium speed" messages. Table 2.5 lists different categories of message types and performance classes defined in [26].

Table 2.3: IEC 61850 services and transfer time requirements [26].

Function	Application	Message	Delay (ms)	Bandwidth	Priority
Raw data	Process bus	SV	<4	High	High
Trip	Protection	GOOSE	<3	Low	High
Other	Protection	GOOSE	10-100	Low	Medium-High

Function	Application	Message	Delay (ms)	Bandwidth	Priority
Medium speed	Control	MMS	<100	Low	Medium-Low
Low speed	Control	MMS	<500	Low	Medium-Low
File transfer	Management	MMS	>1000	Medium	Low
Command	Control	MMS	-	Low	Medium-Low
Time sync.	Phasors, SV	PTP	-	Low	Medium-High

It is necessary to consider that Table 2.5 shows communications constraints in terms of "transfer time", from which, according to the IEC 61850-10, 20% of the total transmission time is reserved for network latency, being the remaining 80% related to the processing times at the sender and receiver. Additionally, in accordance with the processing time for end nodes set forth in the IEC TR 61850-90-4 [23], the network has a maximum budget of 0.6 ms of latency. The network latency is affected largely by the layer 2 control technologies, including redundancy and multihoming ones, which are detailed in Section 2.3.3.

To achieve adequate performance in industrial networks and taking into account the bandwidth-sharing techniques in IEEE 802.3, latency reduction can be achieved by logical traffic filtering and prioritization[3]. Hence, for example, Virtual LAN (VLAN, IEEE 802.1Q) tags provide network segmentation and identify the priority of frames. Because of this, its use in IEC 61850 networks is recommended by [23]. More specifically, latencies caused by waiting for a lower-priority frame to egress a port are analyzed in [23].

R1
Traffic prioritization

Moreover, by and large, layer 2 multicast traffic is used by numerous industrial applications, as is the case with IEC 61850-based ones. Although using VLANs reduces traffic on the network, end hosts experience overload of unwanted frames on their respective VLAN. In such a scenario, one option is to support dynamic multicast filtering; for example, the Multiple Multicast Registration Protocol (MMRP, specified in IEEE 802.1Q) allows the dynamic configuration of multicast group subscriptions. That is to say, dynamic filtering allows end hosts to indicate to the network which addresses they are subscribed to, and then switches share this information with each other. The authors of [27] showed the expected network load reduction achieved in large industrial

[3] Margin annotations are used to summarize relevant requirements that should be satisfied in industrial networks.

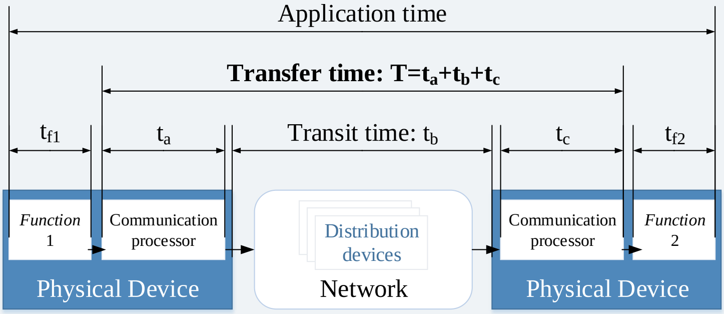


Figure 2.8: The definition of transfer time in IEC 61850-5 [26].

automation networks by using MMRP. However, dynamic multicast control protocols are poorly supported by current IEDs and, as stated in [28], the support for MMRP in Ethernet switches is almost non-existent. Moreover, according to the IEC 61850-90-4 [23], the use of this kind of protocol is not recommended. On the contrary, “static configuration in conjunction with tools that predict network performance for all segments is strongly recommended”. Therefore, “the whole traffic must be calculated before the substation is ever put into operation” to ensure predictable operation.

Reference [29] evaluated a VLAN-based substation using mathematical models for typical IEC 61850 traffic. On the other hand, Ingram et al. [24] analyzed that network segmentation may help to manage those networks whose resources are shared by process and station buses. Furthermore, rate limiting or policing mechanisms adjust the incurred frame latency in a switch. Besides, the authors experimentally verify the latency in an IEC 61850-based substation, where the network resources are shared among data with different priorities, such as SV, GOOSE along with competing background traffic, and they suggest that “port ingress rate limiting is one way of protecting against failures related to network flooding, but this also complicates network design and configuration”.

2.2.4.1 Predictability and timeliness

Hard real-time services require time-sensitive networks, whose control and management planes guarantee a low deterministic latency and jitter. Also, as stated in [30], to achieve a deterministic network, it must have a "formal verification of maximum end-to-end latencies" and "mechanisms to guarantee that ill-behaved end-systems will not interfere with well-behaved end-systems". Thus, using the OPNET Modeler software, the authors of [31] proposed a simulation model on basis of the Network Calculus (NC) framework[4] that allows network designers to identify bounded delays for intra-substation communications.

Switched Ethernet networks avoid collisions and, thereby, improve efficiency. However, despite being widely used in industrial applications, they are not able to guarantee a deterministic delay. In the case of avionics systems, the Avionics Full DupleX Switched Ethernet (AFDX), standardized in 2004 by the Aeronautical Radio Incorporated (ARINC) ARINC Specification 664 part 7 [32], is a suitable protocol for offering predictable timing behavior through the pre-establishment of the so-called Virtual Links (VLs). VLs are static paths previously computed by NC that, based on statistical multiplexing, guarantee a certain bandwidth, and limited latency and jitter. Each VL is identified by the packet's destination MAC address and defines a unidirectional stream. One of the main advantages of AFDX networks is to be based on commercial off-the-shelf Ethernet components with support for QoS. Indeed, it has been also considered to be applied in power substations [33]. However, according to [34], aircraft data and other mission-critical networks will evolve to unified systems that mix AFDX traffic and TCP/IP best effort services without using gateway functions. As an example, the SAE AS6802 Time-Triggered Ethernet (TTEthernet) standard [35] is another relevant technology used in aerospace and automotive industries. It is based on static time-triggered schedules and allows AFDX and synchronous time-triggered traffic to share the same network [36]. It is worth to remark that an IEEE 802.11 wireless extension of the SAE AS6802 standard was presented in [37]. Otherwise, the authors of [38] proposed another Time Division Multiple Access (TDMA) data link layer protocol that is compatible with existing Wi-Fi networks.

[4] A theoretical model that can be used to analytically evaluate real-time constrained applications.

Nevertheless, in any case, SAE AS6802 and AFDX standards impose static resource allocations. Hence, providing reconfiguration capability in the event of failures "is one of the next great challenges for avionic architectures" [39] and still applicable to Smart Grid applications.

R2
Flexible and reconfigurable network

2.2.5 Robustness and survivability requirements

The grace time of automation systems, namely the period that can be tolerated without degrading system performance, delimits the network recovery time. The IEC 62439 standard summarizes some examples of grace periods, as shown in Table 2.4.

Table 2.4: Examples of application grace time [40].

Applications	Typical grace time (s)
Uncritical automation, e.g. enterprise systems	20
Automation management, e.g. manufacturing, discrete automation	2
General automation, e.g. process automation, power plants	0.2
Time-critical automation, e.g. synchronized drives	0.02

With regard to the intended scope, the IEC 61850-5 specification [26] defines the maximum allowed communication recovery times depending on the class of service, as shown in Table 2.5.

Table 2.5: Requirements for recovery delay [26].

Communicating Partners	Service	Required recovery time
SCADA to IED Client-server	IEC 61850-8-1	400 ms
IED to IED interlocking	IEC 61850-8-1	4 ms
IED to IED, reserve blocking	IEC 61850-8-1	4 ms
Protection trip excluding Bus Bar protection	IEC 61850-8-1	4 ms
Bus Bar protection (GOOSE)	IEC 61850-9-2	Bumpless
Sampled measured values (SV)	IEC 61850-9-2	Bumpless

This way, to ensure no interruption in critical services, networks must have redundant components and be able to seamlessly restore communications in the event of a network failure; that is, to simultaneously duplicate a flow through different paths. The IEC 61850-90-4 [23] analyzes the behavior of robust topologies, including redundant trees, rings or mesh ones.

Since improving the availability and reliability of industrial networks is a major goal of this work, a detailed analysis is given in Section 2.3.

2.2.6 Network security requirements

Securing industrial CPSs is essential to ensure integrity and confidentiality for critical applications. The NIST identified [41] how to protect ICSs against common threats and vulnerabilities, suggesting countermeasures to reduce their risks. A thorough overview was given by Knowles et al. [42], who compared control system standards, guidelines and academic research to overcome cyber-security issues. Besides mechanisms for ensuring authentication and integrity of critical services [43], network security deeply depends on restricting physical and logical access to cyber-physical components, as recommended in most security standards (e.g., ISA-99/IEC 62443-1-3), such as:

- Traffic control between industrial control levels. Access Control Lists (ACLs), stateful packet inspection or application-gateway firewalls provide traffic filtering.
- Boundary protection, which can be obtained through demilitarized zone (DMZ) deployments to enforce the control policy for external information exchange.
- Mitigation of malicious attacks by using intrusion detection and prevention systems (IDS/IPS). A mitigation strategy must be performed after receiving an alarm from these systems.

With respect to power system operations, cyber-attacks to ICT and SCADA systems can cause malfunction of physical equipment and may result in blackouts. Hence, standardization bodies recommend prioritizing the promotion of Smart Grid cyber-security strategies. The IEC 62351 standard addresses security issues and specifies, in parts 4 and 6 [44], how to provide security mechanisms for IEC 61850 communication services, such as cryptographic algorithms or authentication certificates. Nevertheless, unlike MMS, “encryption is not recommended” for SV and GOOSE services due to their stringent latency requirements (transfer times below 3 ms), and therefore confidentiality is not mandatory. Likewise, this specification is also ambiguous regarding the need for ensuring data integrity and source authenticity. In this sense, several previous studies have analyzed possible attacks on GOOSE and SV protocols [45], [46] by taking advantage of the lack of authentication and encryption. Instead, "the communication path selection process (e.g., the fact that GOOSE and SV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges" [44]. Therefore, the generation of network policies should be appropriate to mitigate different vulnerabilities. Different cyber-security controls, such as access control, network isolation or monitoring will be proposed in Section 3.2.3.

R3
Traffic restriction

2.2.7 Network management and monitoring

Management plane functions generally include configuration, performance monitoring and maintenance. Typical industrial network configurations are mostly built on managed devices, which support priority queuing and access control protocols, being also necessary to implement physical redundancy. In the case of the Smart Grid, standardization bodies have published network engineering recommendations [23] for inter- and intra-substation communications, including traditional protocols that meet general network requirements. Regarding network management tools, reference [48] stated that being able to access all devices from a central location would facilitate faster troubleshooting and reconfiguration.

R4
Central management

2.2.7.1 Management protocols

Typically, network elements are managed by configuration tools based on proprietary Command Line Interfaces (CLIs) or Simple Network Management Protocol (SNMP, RFC 3411). In the case of SNMP, it allows Network Management Systems (NMSs) to get and set Management Information Base (MIB) parameters. Also, management functions can be implemented with the NETCONF (RFC 6241), that is, a protocol based on a Remote Procedure Call (RPC) paradigm that uses XML for encoding. According to [49], NETCONF poses numerous advantages over existing CLIs. On the other hand, it should be noted that multiple industrial networks comprise constrained devices, such as Wireless Sensor Networks (WSNs). Regarding the management of this kind of networks, the RFC 7547 [50] differentiates between centralized, distributed and hierarchical management. The authors of [51] studied how SNMP and NETCONF protocols can be used on resource-constrained Internet of Things (IoT) environments.

Regarding IEC 61850-based networks, MMS can be also used to obtain and manage communication configuration parameters. As a matter of fact, several LNs for the communication network are defined in IEC 61850-7-4 and IEC 61850-90-4, including a "bridge object model" to unify the supervision of communication, protection and control devices. For example, although its use is not widespread in network elements, some commercial switches (e.g., the Moxa PowerTrans PT-7528 series) integrate a built-in MMS server to facilitate network management. Nevertheless, this information model is very limited and it "is not sufficient to represent the comprehensive communication network" [20]. This prevents the information model of a switch from being viewed as an individual IED. Therefore, MMS is not a suitable alternative to traditional management protocols.

In any case, a further demand for NMSs is to consider "the configuration of the communication network in the unified engineering process of substation automation", as the authors of [20] suggested. In this regard, reference [52] included the commercial product "Cisco Connected Grid NMS" [53] as an approach that combines hardware and software to unify the monitoring and management functionalities. However, being a proprietary solution does not facilitate the interoperability, which is a major goal of the Smart Grid [14].

R5
Unified management

R6
Interoperable solution

2.2.7.2 Monitoring techniques

Besides mentioned requirements, it is also necessary to support performance and fault monitoring. This can be carried out with tools for traffic passive monitoring, such as:

- The sFlow standard (RFC 3176) operates via random packet sampling, such that sFlow agents (switches or routers) push messages, over UDP, containing their interface counters and sampled packets to an sFlow collector that is able to read packet headers for each flow. sFlow relies on a sampling-based method whose accuracy depends on the reporting interval specified in the agents. The estimation of the expected error can be extracted from [54]. Additionally, these authors concede that sFlow is suited to real-time traffic engineering, providing flexibility, scalability, low latency and advantages over other monitoring protocols such as the following ones. Figure 2.9 shows different agents (servers and network devices) sending sFlow datagrams to a sFlow collector and analyzer.

- The NetFlow protocol is a push-based monitoring technology developed by Cisco that has been superseded by the IP Flow Information Export (IPFIX) as a standard (RFC 7011). Reference [55] presented a lightweight adaption of IPFIX to be a suitable candidate for CPSs. However, it must be taken into account that visibility into layer 2 traffic is particularly important in the target application of this research. Therefore, one of the main advantages of sFlow is that it allows the monitoring of flows defined by layer 2 to layer 7 information of the OSI reference model, while on the contrary, NetFlow and IPFIX are oriented to collect IP traffic information, not allowing the determination of flows using layer 2 headers. In other words, NetFlow and IPFIX can be considered as WAN monitoring tools, whereas sFlow operates at the LAN level. Moreover, according to the authors of the paper [54], NetFlow is not suitable for low-latency network measurements. All of these features are indispensable for monitoring SV and GOOSE messages in IEC 61850-based substations.

- SNMP offers a widely accepted monitoring technology, and its use for polling statistics in substations is suggested by IEC 61850-90-4 [23]. For example, like most traditional NMSs, the PROFINET standard uses SNMP to retrieve Link Layer Discovery Protocol (LLDP, IEEE 802.1AB) data and thereby to extract the network topology of industrial networks. However, according to [56], “SNMP is not well suited for end-to-end measurements that are needed for performance metrics”. Additionally, the analysis of [57] is remarkable in showing a “passive flow monitoring framework for OpenFlow enabled experimental facilities” and discussing the advantages of sFlow over SNMP, such as “pushing counters is much more efficient than retrieving them using SNMP". In addition, sFlow uses the eXternal Data Representation (XDR, RFC 1832) data format, which is simpler than that used in SNMP (based on the exchange of ASN.1 objects, RFC 3641), "hence significantly reducing CPU overhead in switches and collectors", being more advantageous to monitor large networks. On the other hand, the Remote Network MONitoring (RMON, RFC 2819) specification is based on SNMP to improve network monitoring and traffic analysis. Nevertheless, as stated in [56], "the use of RMON has been limited due to the complexity and cost of the RMON probes".

- The OpenFlow protocol [9] itself allows the controller to retrieve counters per flows, ports and queues from controlled switches, so it could be an option for implementing the network monitoring task. For example, reference [58] uses this feature for traffic engineering purposes, and estimates a traffic matrix, namely, the traffic volume from every ingress point to every egress point. Nevertheless, these statistics are tightly associated with every flow entry installed on switches[5] and this is an inconvenience for anomaly detection processes, as discussed in [59].

Taking into account scalability aspects, monitoring protocols that rely on pull approaches (SNMP and OpenFlow) are usually less efficient than push-based mechanisms (sFlow and IPFIX), which do not require generating requests and maintaining session information to correlate requests and replies. As a consequence, among approaches that are supported by most network equipment vendors, it can be said that the sFlow protocol is the most adequate monitoring technique for the case study.

Furthermore, multiple Operations, Administration and Management (OAM) technologies, including heartbeat mechanisms for detecting liveness, have been standardized. For instance, some of the most representative technologies are IEEE 802.3ah (Ethernet in the First Mile), which provides Ethernet Link OAM, whereas end-to-end Ethernet OAM can be supported by IEEE 802.1ag (Connectivity Fault Management, CFM), as well as by the ITU-T Y.1731 standard, which offers a variety of OAM and management features. Also, Bidirectional Forwarding Detection (BFD, RFC 5880) provides continuity check

[5] The OpenFlow protocol will be further described in Section 2.5.1.

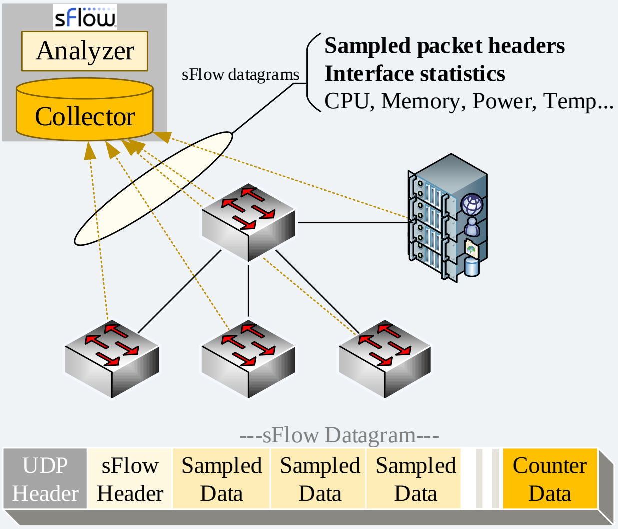


Figure 2.9: sFlow architecture and datagram encapsulation.

between two end-points. BFD is a UDP-based layer-3 protocol that is usually used for protection of tunnels, IP traffic or MPLS Fast Reroute.

2.3 Redundancy, load balancing, and high availability

According to [30], "the main task of safety-critical networks is to provide guaranteed delivery of all packets". Thus, to ensure robustness of mission-critical CPSs, underlying networks have to meet certain levels of reliability. Quantitative metrics for resilient control systems, including recovery time and performance degradation, are introduced in [60]. As the authors stated, redundancy is the most accepted method for maintaining continuous network operation. Indeed, legacy avionics systems, such as those based on the MIL-STD-1553 standard, already duplicated buses (wires and switches) in "hot backup" status, with only one of the buses active at a time.

In particular, this study focus on the Ethernet data link layer since, as previously mentioned, this technology is being selected for many critical projects which demand dependable communication infrastructures that meet stringent reliability requirements. In addition, as noted above, GOOSE and SV serve as examples of messages that are transferred without connection or confirmation via a TCP/IP stack. Because of this, although upper layers can provide redundancy and perform recovery actions, it is important to note that retransmission and coding techniques are not considered in this study as they counteract the delay requirements [61] and are not suitable for real-time communications. Therefore, although multipath transport protocols that support the simultaneous transmission of the same information in different paths may be mentioned, such as the Stream Control Transmission Protocol (SCTP) or variations of Multipath TCP (MPTCP) [62], they do not support the protection of IEC 61850 services.

This section outlines different restoration and protection techniques in connection with the availability of resources. Then, some of the most relevant protocols to provide redundancy in Ethernet networks are subsequently listed. A thorough review of Ethernet resilience techniques can be found in [63].

2.3.1 Types of redundancy

Redundancy takes two forms: temporal and spatial, while the first form replicates the information over time in a distributed manner, in the spatial redundancy the components (nodes and links) or data in a network are replicated, which is the object of study. Conventionally, two types of redundancy are distinguished:

- *Standby redundancy*: through passive resources, these redundant networks switch from an active to a secondary path. It may be distinguished between partial, which only overcomes the failed link or node, and global recovery, where the whole path is reconfigured (Figure 2.10 exemplifies these principles). In any case, two different schemes can be considered:

  - Protection schemes where standby paths are precomputed in a proactive way.
  - Restoration mechanisms that define recovery network elements reactively in the face of failures and changes in the network.

  Both approaches result in a certain communication downtime, but protection typically incurs in a lower recovery delay than restoration approaches.

- *Active or parallel redundancy*: multiple copies of the same data are transmitted along multiple paths simultaneously. The routes can be link-disjoint or node-disjoint for tolerance to link and node failures, respectively. The receiver expects incoming traffic on different routes, so it always receives the information transmitted as long as all paths do not fail simultaneously. This approach eliminates any downtime and ensures that no data are lost due to a single failure.

Regarding the disjoint paths problem, it can be formally defined as follows: given a connected, undirected graph $G = (\mathcal{N}, \mathcal{L})$ of a set $\mathcal{N}$ of N nodes and a set $\mathcal{L}$ of L weighted links, two nodes $s, t \in \mathcal{N}$, and an integer $k > 0$; find k paths $P_1, P_2, ..., P_k$ from s to t, such that the paths share no common links (or nodes). There are different possible criteria for finding the disjoint paths [64].

As can be drawn from the different redundant mechanisms, one of the main differences lies in the switchover time, in which time can be divided into:

1. Detection time based on monitoring the communication paths in order to detect failures. Common to all types.
2. Provision time: if any failure is detected, the network control plane must calculate an alternative path. It only affects the restoration case.
3. Switching time to the alternative path and the subsequent communication reestablishment. It generally does not influence in the case of parallel redundancy.

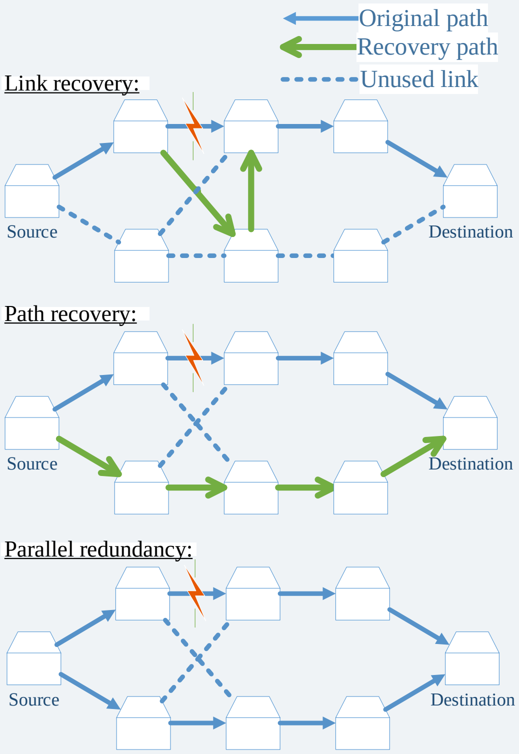


Figure 2.10: Types of redundancy and recovery mechanisms.

In the design of a network, different redundant methods must be determined on a risk-versus-reward trade-off, assessing the need to reduce recovery times and the number of redundant paths compared to other factors, such as management and deployment costs. Obviously, the use of concurrent paths also implies an increase of resources and parallelism management, so they are oriented toward critical use cases, like those mentioned in Section 1.1.

2.3.2 Availability calculation

The communication availability is essential for industrial applications, however it never can be totally guaranteed. It is defined in ITU-T Recommendation E.800 as follows: “availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided”. On the other hand, ITU-T Recommendation Y.1563 assesses performance parameters for the specific case of Ethernet service availability.

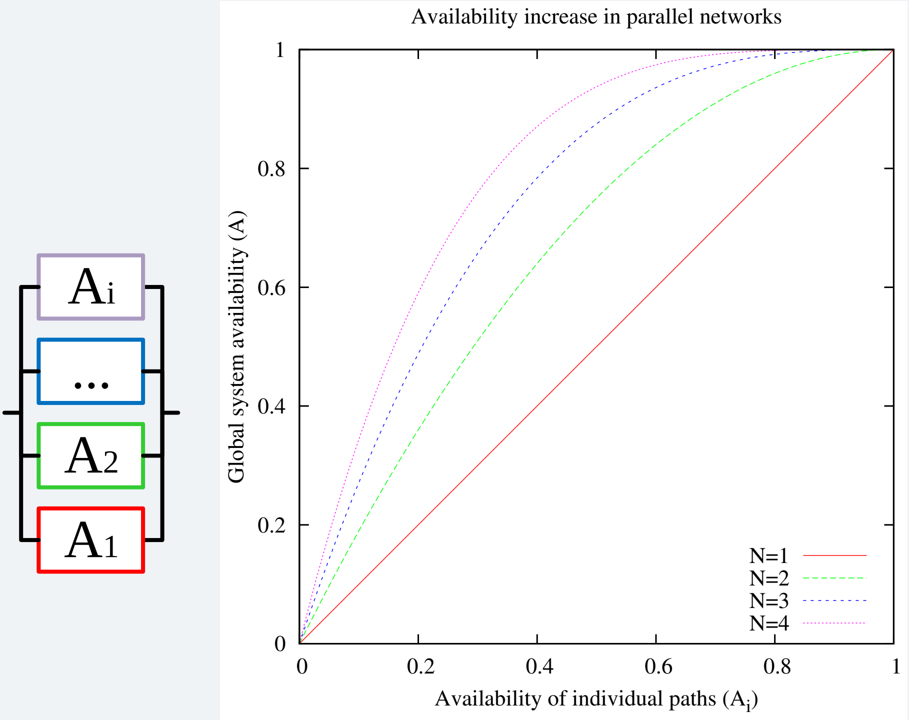


Figure 2.11: Availability model of parallel systems (comparing up to four redundant paths).

In [65], the authors illustrate an exhaustive analysis of network availability and different recovery methods, applied to several technologies. From a general view, the availability of the network ($A \in [0, 1]$) can be quantitatively defined by the parameters known as Mean Time to Failure (MTTF), Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) with the Equation 2.1. As can be understood, resilience and redundancy are closely related through fault detection and isolation techniques, which are covered by OAM tools. Depending on the fault nature, the failover period may be reduced and, therefore, the availability of a network is improved. This can be achieved by automating the prevention and detection of certain faults, while on occasions, the operators' diagnosis and decision-making will be totally necessary.

R7
High availability

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTTR} \tag{2.1}$$

Through an availability model based on Reliability Block Diagrams (RBDs), the impact of parallel redundancy on the overall network availability can be crudely estimated. Because the availability of a single path (A_i) is defined by summation of the individual availabilities of the network equipments and transmission links, the availability of parallel systems (A_p) may be calculated per the expression below:

$$A_p = 1 - \prod_{1}^{N}(1 - A_i) \tag{2.2}$$

Likewise, the unavailability ($U = 1 - A$, $U \in [0,1]$) of subsystems can be directly associated with the overall packet loss rate. Therefore, a redundant system reduces such rate with respect to a non-redundant one. For a parallel chain with unavailability q_1 and q_2,

$$U_{non-redundant} = q_1 \;\geq\; U_{parallel} = q_1 * q_2 \tag{2.3}$$

Relationship between redundancy and availability can be understood from Figure 2.11, which shows how the network availability is improved in accordance with a certain redundancy scheme. In this particular figure, up to four parallel paths are compared, assuming that the availability of each connection path is the same.

Regarding the packet loss ratio and following the model of Cena et al., [66], let M_G^L and M_R^L be, respectively, the number of packets generated by a source node and received by a destination node through a path $L \in A, B$, where A and B refer to individual paths, while AB is the combination of them. The sequence $d_i : i = 1...M$ indicates if a packet was successfully delivered, $d_i = 0$, or dropped, $d_i = 1$. Then,

- $M_d^L = \sum_{i=1...M} d_i^L$ is the amount of dropped packets on path L.
- In active redundancy schemes, packets are lost only when they are dropped on both redundant paths and, therefore, delivered packets $M_R^{AB} \geq max(M_R^A, M_R^B)$ and $M_d^{AB} = \sum_{i=1...M} d_i^A \wedge d_i^B$.
- Finally, the packet loss ratio is $\Upsilon_D^L = M_D^L / M$, and the probability of a packet loss event is $P(d_i^A) \wedge P(d_i^B)$, and it equals $P(d_o^A) \cdot P(d_j^B)$ if errors on A and B are statistically independent.

2.3.3 Spanning tree, link aggregation and other redundancy approaches

An overview of common layer 2 redundancy protocols is presented below.

2.3.3.1 Spanning tree-based protocols

Given that in the IEEE 802.3 Ethernet standard there is no mechanism to discard duplicated frames or any time-to-live field, the appearance of loops should be avoided. To that end, the most commonly applicable protocols for handling redundancy in Ethernet networks are based on the spanning tree approach. These techniques obtain loop-free topologies by disabling certain redundant links, and these passive resources are activated in the event of a network element failure.

There are several distributed spanning tree algorithms, either standard, such as for example the Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D) and the Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s), or proprietary, such as the Rapid Per-VLAN Spanning-Tree Plus (RPVST+) developed by Cisco. These two latter protocols enable load balancing as creating multiple instances of Spanning Tree Protocol per Virtual LAN. The advantages of MSTP with respect to RSTP in the effect of traffic interactions on SV and GOOSE messages were studied by Ingram et al. in [24]. In any case, switches running MSTP lack a global view of the network, and the resulting logical topologies do not take advantage of all physical redundant links, which therefore prevents the packets from being always forwarded through the shortest path. This shortcoming directly affects the latency of time-sensitive services and it will be examined in Section 3.3.

R8 Higher redundancy efficiency

Furthermore, another common shortcoming of these protocols is that they do not guarantee a deterministic failover behavior. For example, although a method to calculate the maximum recovery time in a ring configuration is provided in [40], the RSTP fault recovery time depends on the configuration parameters and the location of the fault.

A remarkable approach is developed in [67], where the authors rely on the MSTP protocol to define several trees and forward duplicated packets. However, it is a static configuration and the authors do not address the issue of how the receivers should discard duplicates. Also, as the authors claimed, this proposal “cannot be generalized for all the nodes of the network, since the duplication of messages induces overload”, but moreover, duplication depending on the traffic class would be more effective.

R9 Dynamic redundancy control

2.3.3.2 Link aggregation

End hosts with multiple interfaces, in which one or more may be active, increase reliability. On the one hand, Ethernet channel bonding allows multiple physical interfaces to bundle into a single logical one. Therefore, bonding reduces the failover time by providing resilience between ports in case of a link failure, as well as load balancing that increases bandwidth. Several technologies allow nodes to use multiple links jointly, such as, for example, the Link Aggregation Control Protocol (LACP, IEEE 802.1AX) or proprietary Multi-Chassis Link Aggregation (MC-LAG) implementations. The latter ones avoid a single point of failure by aggregating the capacity of multiple switches, thereby requiring a synchronization protocol between switches.

Despite the fact that solutions like LACP can be perfectly used for load balancing, they are not suitable for protecting services that require zero recovery time as they require “non-negligible amount of time for giving up on a path that has failed” [61].

2.3.3.3 Link-state routing protocols

Using Intermediate System to Intermediate System (IS-IS) routing to distribute link-state information has been recently proposed for layer 2 frame forwarding. The Transparent Interconnection of Lots of Links (TRILL, RFC 7176) and Shortest Path Bridging (SPB, IEEE 802.1aq) protocols rely on link-state routing algorithms to improve the Ethernet control plane. Unlike spanning tree-based techniques, both technologies enable shortest path forwarding in mesh topologies by calculating a hash based on, for example, Ethernet addresses, IP addresses and TCP/UDP port numbers of the packets. However, with these protocols, multipathing can only be carried out through equal cost paths and, according to [68], another disadvantage of the hashing technique is that “usually all links get the same percentage of the hash values and therefore all the paths need to have the same capacity”.

Despite the fact that both SPB and TRILL protocols has been mainly developed for large layer-2 fabrics (data center scenarios), they have been proposed to be used in industrial automation networks by [69], [70]. In the specific case of TRILL, it results in “an enhanced alternative to RSTP”; however it “is still unable to meet the required convergence time claimed by the Smart Grid requirements” [70]. Indeed, they are not conceived as active redundancy protocols. Hence, there are recent attempts [71] to build active protection paths in TRILL networks so that “when a link on the primary distribution tree fails, the preinstalled backup forwarding table will be utilized without waiting for the reconvergence, which minimizes the service disruption”.

2.3.4 IEC 62439: High-availability Ethernet protocols

As indicated above, a very low, or even zero, recovery time and packet loss rate are achieved by using spatial and temporal active redundancies. In this way, aforementioned redundancy mechanisms may not be appropriate, in terms of recovery time, to critical networks.

Besides proprietary or exclusive solutions, the Technical Committee 65 standardized in the IEC 62439 different techniques applicable to any industrial system to build high-availability networks. In particular, the IEC 62439 standard suite, entitled "High availability automation networks", includes a set of layer 2 redundancy control protocols for industrial environments. From a general point of view, they are grouped into two models:

- "Redundancy managed within the network" with devices singly attached to network devices, which implement redundancy management.
- "Redundancy managed in the end nodes" using doubly attached devices.

Otherwise, each included protocol is intended to be applied in specific applications (Table 2.4) and topologies; for example, ring topologies can be protected with the Media Redundancy Protocol (MRP), achieving lower convergence time with respect to RSTP.

Under this umbrella, it is interesting to note Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) technologies, which are able to provide zero recovery time in case of any single network failure. To achieve this, both protocols, defined in IEC 62439-3 [72], duplicate data and network resources. While in the MRP there is a ring manager that is in charge of controlling the redundant resources, in PRP and HSR redundancy management is implemented in the end devices, which are connected by active redundant links. The principles of these protocols will be described below, as well as the discussion of related work.

It is important to emphasize that PRP and HSR have been selected by the IEC 61850 Edition 2 [23] to avoid single point of failures and provide a minimal failover time, being suitable for protecting SV and GOOSE services. For example, [73] focuses on substation automation systems and it studies the performance of time synchronization services in RSTP and PRP networks where multiple network failures are simulated and, noticeably, PRP is much more tolerant to such failures.

2.3.5 Parallel Redundancy Protocol (PRP)

PRP (IEC 62439-3 Clause 4) guarantees seamless communication by simultaneously duplicating data in two networks. The management of redundant frames is fully implemented in the end nodes, called Double Attached Nodes (DANs). Thus, a DAN is connected to two independent LANs (see Figure 2.12) through interfaces with the same MAC address.

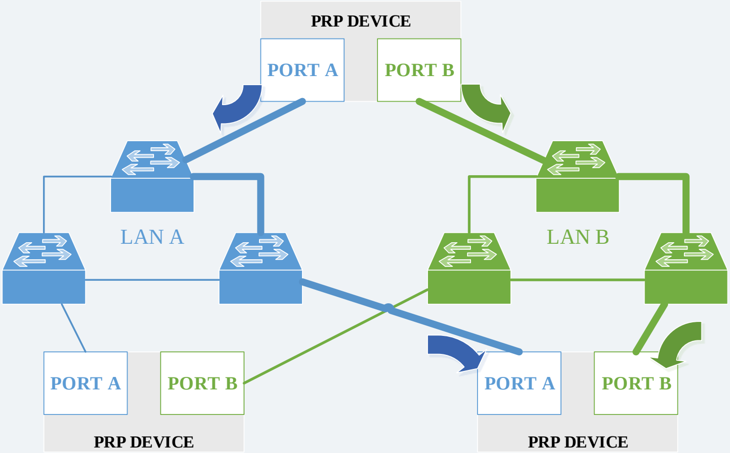


Figure 2.12: PRP network topology.

According to the specification, these networks must be identical in protocol at the Logical Link Control (LLC) level and their switches have to accommodate oversized frames (with length of up to 1532 bytes), since DANs extend the Ethernet header. Yet, these networks are protocol-agnostic and may have different topologies and performance, and even the PRP specification is independent of intrinsic redundancy used in the LANs[6]. Consequently, network switches can connect PRP incom-

[6] Like PRP, it should be noted that the above-mentioned AFDX protocol follows the same dual-redundancy transmission principle. However, to reduce wire runs and weight, AFDX only considers the use of cascaded star topologies.

patible nodes, which are called Single Attached Nodes (SANs). Besides, these off-the-shelf devices can become Virtual SANs by attaching to PRP proxies (denominated PRP RedBoxes), which do redundantly connect to both networks.

The specific PRP operation mode and the Ethernet frame specification described below.

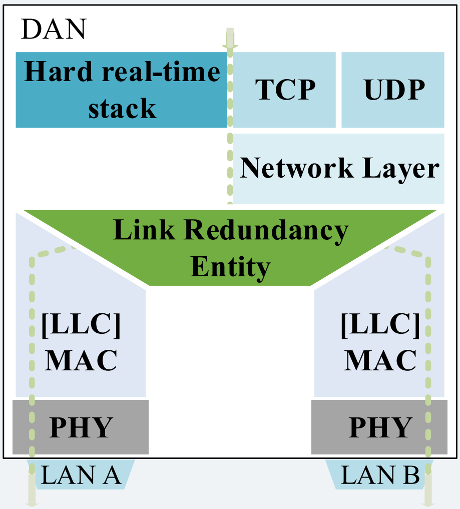


Figure 2.13: Scheme of a PRP device [72].

2.3.5.1 PRP operation process

A DAN implements a Link Redundancy Entity (LRE), which is responsible for managing the redundancy and duplicates transparently to the upper layers. A schematic PRP diagram is shown in Figure 2.13 according to the architectural model of an IEEE 802.1 bridge. In addition, PRP provides a mechanism for the network supervision, so that each DAN monitors the status of each LAN and other PRP devices. This facilitates the control of network errors, as well as discovering other DANs. To this end, multicast frames, identified by a specific Ethertype (0x88FB), are used. The PRP operation process is summarized in the following pseudo-code:

```
while true do
    send a multicast supervision frame;
    for every datagram received from upper layers do
        create two frames by adding an Redundancy Control Trailer (RCT)
          with the same sequence number and size field;
        calculate a new checksum per frame;
        send out the frames through its both ports at the same time;
    end
end
```

Algorithm 1: PRP sender node operation.

```
while true do
    receive multicast supervision frames;
    for every frame received on one of the two ports do
        check if the frame is a duplicate or not (MAC source address and
          sequence number);
    end
    if yes then
        discard the duplicate;
    else
        remove the RCT;
        transparently forward the received frame to its upper layers;
    end
end
```

Algorithm 2: PRP receiver node operation.

In other words, a PRP node works as follows:

- When the Entity receives a message from upper layers, it creates two frames by adding the so-called RCT and calculating a new checksum.
- The Entity sends out the frames through its both ports at the same time. These two frames traverse the two independent networks.
- At the destination node, the LRE has two operation modes to handle the received frames.
    - Duplicate Accept “for testing purpose” [72] or Duplicate Discard: the latter, which is the most common mode, ensures that the upper layer receives only the first data frame. For this purpose, the LRE must maintain a buffer of the first re-

ceived frames to recognize and discard duplicates. The buffer implementation affects the algorithm to detect duplicates, which is not specified by the standard. For instance, decisions about timeouts and buffer sizes must be consistent with network performance goals.

- In both cases, the LRE removes the RCT and forwards the received frame to its upper layers. In case that the duplicates are not discarded, upper protocols, such as IP and TCP protocols, can tolerate receiving and removing duplicates.

2.3.5.2 PRP Ethernet frame format

In order to enable detection of duplicated frames, each frame is extended by the RCT, 6 bytes long, structured as follows:

- Sequence number (16 bits): the source increments it for each frame sent, allowing a receiver to detect missing messages and permanent failures.
- LAN A/B label (4 bits): it identifies the network to which send the frame. The specification defines only the 0xA and 0xB codes.
- Link Service Data Unit (LSDU) size (12 bits): the LSDU is the content located between the Length/Type field and the Frame Check Sequence. This field indicates the size of the Link Service Data Unit [72] including the RCT.
- PRP suffix (16 bits): it coincides with the Ethertype (0x88FB).

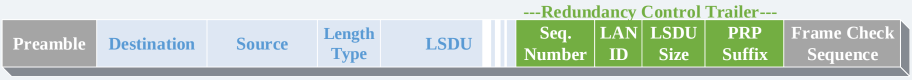


Figure 2.14: PRP frame format.

Figure 2.14 shows the PRP frame format.

2.3.5.3 Other characteristics and proposals for improvement of PRP

In general, PRP is not only useful for critical applications where data loss is not permitted, but also it may be relevant in situations where the loss rate may be relatively high, which may be applied to tolerate arbitrary faults, such as accidents, natural disasters, malicious attacks or blackouts.

It can be concluded that PRP is a simpler technique and more easily implementable than other approaches such as [74], which proposes a multiple path Ethernet scheme, along with congestion control and packet retransmission mechanisms in order to be able of transmit data through parallel paths in a reliable manner. However, PRP compliant devices duplicate all packets regardless of their priorities, which entails that the available network bandwidth is halved. This may be inefficient to meet requirements of the applications in many aspects, such as scalability. Consequently, it could be interesting to filter non-critical traffic in order to free resources.

R10
PRP efficiency enhancement

Otherwise, the approach presented in [70] combines PRP and TRILL networks, however this combination does not provide greater redundancy than conventional PRP deployments and, as asserted by the authors, there are situations where their "proposal cannot cope with the most stringent requirements". Accordingly, this paper encourages practitioners to supplement it by taking into account some principles of the PRP protocol. In order to maintain a very reliable networking infrastructure, multiple-failure scenarios will be analyzed in Section 3.3.3.

2.3.6 High Availability Seamless Redundancy (HSR) protocol

HSR (IEC 62439-3 Clause 5) can be considered a special version of PRP applied to certain topologies. Unlike PRP, HSR requires only an additional path between two nodes; on that ground, HSR is typically used in ring topologies, including rings of rings and mesh topologies. A single HSR ring network is composed of nodes connected to each other, with-out needing an intermediary. To this effect, HSR devices, also called DANs, incorporates a bridge function that forwards frames from port to port. All components must be HSR-aware so that legacy switches or general purpose nodes are not allowed. For this reason, SANs require the capabilities of a proxy (HSR RedBox) as depicted in Figure 2.15. Moreover, another proxy called QuadBox can connect HSR rings to each other. Specifically, two quadruple-port devices must be used to avoid single points of failure; both forward packets from ring to ring.

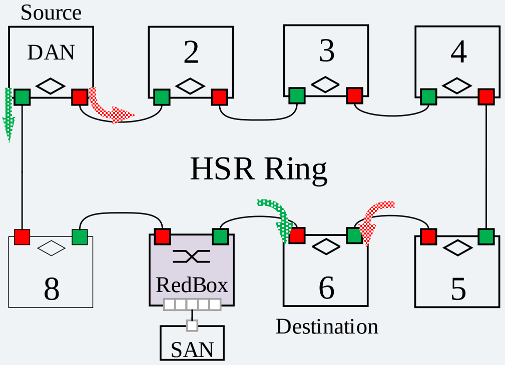


Figure 2.15: HSR network diagram.

2.3.6.1 HSR operation process

Regarding the operation, every node, which transmits in both directions of the ring, is responsible for detecting and removing duplicates from the network to prevent loops. The behavior of these nodes is summarized as follows:

- For unicast traffic:
    1. The LRE of the receiver removes the duplicated frames and passes the valid ones to upper layers.
    2. In case that the receiver does not operate properly and a sent frame returns to the sender, this must delete it to avoid loops.
- For broadcast/multicast traffic:
    1. Each node forwards frames from one port to another, and also it passes the filtered frames to upper layers, if applicable.

2. Broadcast/multicast frames traverse the complete topology before being removed by the sender.

In addition to the above, an HSR node is expected to support certain functionalities to improve the use of available resources, such as network segmentation and traffic prioritization through IEEE 802.1Q to differentiate services that require real-time processing. Moreover, similar to PRP, each DAN has a network supervision mechanism that generates layer 2 multicast frames with a specific Ethertype, 0x88FB, through its both ports.

2.3.6.2 HSR Ethernet frame format

As illustrated in Figure 2.16, a tag is added to the Ethernet frames by the sender so HSR devices can detect duplicates. These frames are identified by the Ethertype 0x892F and include the following fields:

- LAN Identifier (4 bits): it is necessary to handle complex networks that connects multiple PRP and HSR networks.
- LSDU size (12 bits): it specifies the size of the LSDU including the HSR header.
- Sequence Number (16 bits): it is incremented at each hop.

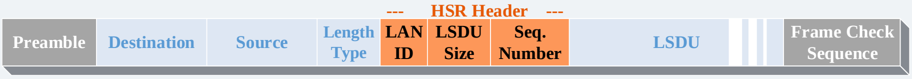


Figure 2.16: HSR frame format.

As in PRP, the introduction of an additional overhead due to the HSR header reduces the actual throughput.

2.3.6.3 Comparison between HSR and PRP

Differences between HSR and PRP make each one of them more appropriate in certain use cases, so the pros and cons of each protocol are summarized as follows:

- While the PRP scheme depends on the network elements and supports two independent LANs of any topology, HSR is limited to ring-based topologies[7].

- One limitation of PRP is that it is not strictly deterministic, since communication delays may vary depending on the topologies. In contrast, a major strength of HSR is that facilitates the determination of latencies, since it is only necessary to know the number of nodes and their corresponding switching time. However, on the other hand, ring topologies also present inherent limitations, such as the maximum number of hops that does not cause the maximum latency is exceeded.

- While PRP means a duplication of network equipment, HSR does not suppose this overhead, making it less expensive to deploy and maintain than PRP.

- The latter implies HSR works without dedicated Ethernet switches. By contrast, HSR nodes must implement switching function between their two ports. Accordingly, HSR should be implemented in hardware to meet acceptable time requirements; on the contrary, the PRP nodes can implement the LRE in software.

- These requirements are related to the flexibility to accommodate off-the-shelf devices: unlike PRP, SANs cannot be inserted in HSR topologies without using a RedBox, as mentioned before.

A further analysis of other IEC 62439 redundancy protocols can be found in [63]. Among them, the IEC 62439-4 Cross-Network Redundancy Protocol (CRP) and the IEC 62439-5 Beacon Redundancy Protocol (BRP) implement standby redundancy so that they do not provide a seamless

[7] The IEC 62439-3 specification also describes different robust topologies that employ PRP and HSR jointly.

communication. However, in contrast to PRP, they permit establishing cross-links between parallel LANs, which can be considered a limitation of PRP.

2.3.6.4 Network usage analysis of HSR

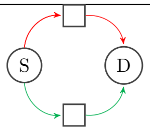
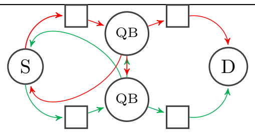
As discussed in [75], an upper latency bound exists in ring topologies, as a specific case of non-feedforward networks, if

$$\alpha \leq \frac{1}{H-1} \tag{2.4}$$

where α is the maximum utilization rate of any link and H the maximum path length. That is to say, the utilization rate decreases with increasing network size or, in other words, the number of hops is restricted by time constraints. This way, it is necessary to emphasize that the waste of bandwidth is one of the main drawbacks of HSR networks, since all frames are sent in both directions around the whole ring; "note that these are useless frames, which will later be removed from the network" [76]. In single HSR rings, duplication of traffic means that two unicast frames traverse the total number of links (L) in the network. Thus, the number of hops (h) is constant for all types of traffic and independent of the location of the source ('S') and the destination ('S'), as shown in 2.6 in Table 2.6. Consequently, frames generated by a node affect the overall network capacity. This is more noticeable when the topology consists of several rings, where unicast packets are also doubly transmitted along those rings that do not contain the destination node. In this case, the number of hops only depends on the location of the destination, as given in 2.6, where L_r is the number of links in each ring, and R is the ring containing the destination node.

One of the main goals of this work is to reduce the average number of hops per frame delivery and, therefore, to decrease the total network traffic. If network topologies are determined by the sets of nodes ($\mathcal{N}$) and links ($\mathcal{L}$), where end nodes ($\mathcal{N}_E$) generate and receive traffic; and for any pair of end nodes $i, j \in \mathcal{N}_E$, the source-destination pair is given by sd_i, j. Then, let $f(sd_{i,j})$ denote traffic flow sent from node i to node

Table 2.6: Number of hops in HSR networks.

Single ring		$h = L \quad (2.5)$
Coupled rings		$h = \sum_{r=1}^{R-1} 2L_r + L_R \quad (2.6)$

j, and $T_f[t]$ denote the number of frames generated by a flow f at time t. The above-mentioned goal can be expressed as follows:

$$\min \sum_{f \in \mathcal{F}, h} hT_{f,h} \tag{2.7}$$

where $T_{f,h}$ is the traffic volume due to the flow f ($\mathcal{F}$ is the set of all flows in the network) using paths with h hops.

2.3.6.5 Proposals for improvement of HSR

Reducing unnecessary traffic in HSR networks has been analyzed in [77], where MAC learning is implemented in QuadBoxes; whereas in [78], the authors introduced a traffic control node in charge of network monitoring and duplicating packets if necessary. With a similar approach, references [76], [79] proposed algorithms that remove duplicated frames to reduce throughput. Moreover, the latter proposes the creation of "virtual rings" that connect sources and destinations to restrict network traffic. Despite these proposals, no studies have focused on distinguishing types of services or providing methods of traffic control. In the proposal presented in Section 3.3.4, the OpenFlow technology is adopted to achieve this objective.

R11 Improvement of HSR performance and efficacy

2.4 Wireless industrial networks

It is becoming increasingly common to deploy industrial wireless networks, since they have numerous advantages, such as lower installation costs due to cabling reduction or enabling users and equipment mobility. In fact, the Industry 4.0 framework largely relies on the expansion of ubiquitous wireless sensor systems. However, wireless communications suffer from unreliable data transmission due to non-deterministic factors. Therefore, these networks have to ensure continuity of operations, so that availability and performance are not affected. Specifically, wireless automation requirements are specified in IEC 62657-1, differentiating them according to the critically of applications. According to [80], in 2006, there was no vendors had developed wireless networks for relay protection within a substation, which is one of the most demanding mission-critical and time-sensitive services in SASs (Table 2.5); whereas wireless communications could be used for the transmission of monitoring data. However, the same document envisaged that “future enhancements of wireless equipment robustness, security, and capabilities, particularly with meshed networks, could possibly meet the stringent requirements”.

Willing et al. [81] analyzed how mature wireless technologies, including IEEE 802.11, 802.15.1 or 802.15.4 standards, can be applied in industrial applications through robust network designs in error-prone channels. In the case of the Smart Grid systems, the opportunities posed by wireless sensor networks were assessed in [12], which described technical challenges, such as ensuring a certain latency or QoS. These challenges are associated with changes in the topology and connectivity due to the conditions of the physical layer. The propagation loss in power substations was also obtained in [12].

Furthermore, there are emerging wireless standards focused on providing industrial-grade reliability, such as WirelessHART (IEC 62591), ISA100.11a (IEC 62734) or WIA-PA (IEC 62601). They are all based on the IEEE 802.15.4e MAC layer, which uses Time Slotted Channel Hopping (TSCH) to provide reliable communication and deterministic latency. TSCH combines multi-channel TDMA with a very low cycle time, and frequency hopping. In addition, WirelessHART provides a reliable, connectionless transport service, whereas ISA100.11a supports unacknowledged and acknowledged services, and retry mechanisms to assure end-to-end delivery of messages based on UDP/IPv6. ISA100.11a is also capable of running TCP for non-real-time communications.

In these approaches, the "Network Manager" (following the nomenclature of WirelessHART) is responsible for configuring the network resources and managing routes between devices, so that field nodes need not be concerned with these tasks. WirelessHART has been proposed to be used in industrial CPSs [82], where the authors highlighted different research directions, among which hierarchical network architectures would enhance scalability. Thus, Lu et al. [82] proposed to divide large WSNs into multiple subnetworks and local network managers, which have to be coordinated with a global manager. Moreover, Lu et al. suggested establishing a unified codesign where the network resource allocation should be dependent on the control design.

These technologies are used at the sensor/actuator level for monitoring and automation applications. Therefore, all of them are aimed at short-distance (about 10 m) Wireless Sensor and Personal Area Networks. They can only achieve a low-data rate and, besides, they are not directly interoperable with Ethernet. As stated in [83], these issues may be overcome by using IEEE 802.11.

On the one hand, regarding the interoperability of Ethernet and Wi-Fi networks in industrial environments, reference [83] studies hybrid designs where link-layer frames are transmitted from wired backbones to the wireless channels and vice versa. On the other hand, unlike the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technique, the polling-based mechanism of IEEE 802.11, offers predictable communications and achieves shorter packet delay. This Controlled Channel Access (CCA) is based on the original Point Coordination Function (PCF) and "matches the requirements for automating various Smart Grid applications" [84]. In particular, the authors of [85] evaluated the latency of GOOSE messages defined in IEEE 802.11g wireless LANs, in the presence of interference previously characterized at different substations and scenarios. They "demonstrate suitability of an industrial WLAN for some innovative smart-distribution substation applications" [85].

There have also been proposals to integrate Real-Time Ethernet protocols into IEEE 802.11 networks by means of a scheduling function carried out by a managing node. For example, Ethernet Powerlink is used in [86] and a proprietary extension to PCF based on PROFINET IO (Industrial PCF, developed by Siemens) is studied in [87].

2.4.1 Redundancy in industrial WLANs

Previously mentioned WirelessHart, ISA100.11a and WIA-PA are mainly used in inherently redundant mesh networks with the aim of increasing redundancy, diversity and, hence, reliability. Moreover, the ISA100.11a standard includes the *duocast* feature, which allows a device to send packets to multiple APs and receive acknowledgements in the same time slot. In [88], the advantages of *duocast* are applied to industrial plants.

Otherwise, although IEEE 802.11 is not used in [89]–[91], they show the benefits of adopting redundancy in industrial wireless plants. Reference [89] decreases the failure probability by performing retransmissions that use different independent antenna and channels. As in PRP/HSR, the authors assume that the receivers may be responsible for processing multiple copies of the same packet. ReInForM [90] establishes multiple redundant paths, for which nodes have to be aware of the network topology and status. Hence, diverse information (e.g., desired reliability, channel quality and number of hops needed to reach destination) is added to the data packets, and it is needed to determine the transmission paths. Due to low-latency constraints, this approach is hardly applicable to industrial control systems. In fact, it should be taken into account that, despite reducing throughput, one of the benefits of sending redundant packets along multiple paths is not only avoiding retransmission, but also providing lower delay, which has been demonstrated in [91].

Furthermore, in spite of the fact that PRP was initially targeted to be used in wired Ethernet deployments, recent researches have proposed the use of PRP in wireless scenarios with the aim of increasing network resilience. Reference [87] proposes the use of PRP in hybrid topologies, where a node is connected through a primary wired link and a secondary wireless connection. As a consequence, although the wireless connection provides lower performance, it is valid as a backup mechanism. Rentschler et al. also proposed in [92] to communicate two PRP nodes via two different wireless channels, which operate as point-to-point links. As a result, lower error rate, latency and jitter are obtained. With the same approach, in paper [66] sending redundant frames is optimized with the addition of control messages, which prevent the transmission over lossy and erroneous channels.

These studies demonstrate the advantages of combining PRP and WLAN in applications with demanding availability requirements. However, point-to-multipoint connections and mobility scenarios have not been analyzed. Moreover, none of the above proposals is focused on the network management. On the other hand, in this study OpenFlow is proposed as the control mechanism (Section 3.3.3).

R12
Robust WLAN connectivity

2.5 OpenFlow and Software Defined Networking

This section provides an overview of the OpenFlow protocol, which emerged to develop a clean-slate network control architecture [93], [94] and it is the cornerstone of the SDN paradigm at present. The details of this paradigm are described later.

2.5.1 The OpenFlow protocol

From a historical perspective, OpenFlow was proposed in [94] as a promising solution to provide programmability and flexibility in campus networks. OpenFlow [9] is a protocol whereby a controller establishes the forwarding rules for flows arriving at a network device. Hence, a controller can access and establish the data path by adding, updating and deleting flow entries in the forwarding tables of switches, enabling data and control plane separation. In order to define the packet forwarding path, the forwarding rules are based on packet headers, input ports, priorities and instructions associated with each input flow.

Regarding the communication process between an OpenFlow switch and a controller, it is important to emphasize that these rules can be installed in two different ways:

- **Reactive mode**: in which the controller dynamically sets entries in response to requests from switches, through the so-called "packet-in" messages.
- **Proactive mode**: the flow tables are statically pre-populated by a controller, thereby reducing the flow insertion delay, which is required by time-sensitive scenarios.

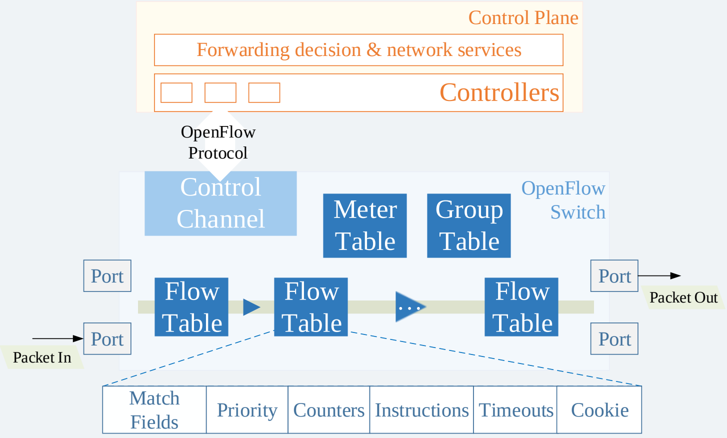


Figure 2.17: OpenFlow pipeline.

Figure 2.17 shows a scheme of an externally controlled switch and the OpenFlow rules of forwarding tables of switches, which contain multiple match fields (ingress port, metadata and packet headers), instructions and metadata that define the data path. Match fields enable a flow-level control scheme based on layer 2 to layer 4 headers. The number of possible fields from packets used to match against flow entries have increased as new versions of OpenFlow are released. Table 2.7 illustrates the 12-tuple supported by OpenFlow 1.0, to which new match fields have been added. For example, OpenFlow 1.1 introduced support for adding, modifying and removing Multiprotocol Label Switching (MPLS) labels; IPv6 match and header rewrite was added in OpenFlow 1.2; or, in the

Table 2.7: OpenFlow 1.0 match fields

Ingress Port	Ether Src	VLAN Id	IP Src	TCP-UDP Src Port / ICMP Type
	Ether Dst	VLAN Prior	IP Dst	TCP-UDP Dst Port / ICMP Code
	Ether Type		IP Proto	
			IP ToS bits	

current version (OpenFlow 1.5.1), flag bits in the TCP header (e.g., SYN, ACK and FIN) can be used to detect TCP connections.

With respect to the control channel, two scenarios are distinguished: in-band and out-of-band control planes. On the one hand, the former configuration does not need additional physical resources, whereas an out-of-band control plane may result expensive for wide-area networks with multiple controllers (detailed below). On the other hand, not separating control from data traffic may involve reliability issues as network failures affect both planes; in that event the control channel needs to be repaired before the controller can recover the data plane. Consequently, both approaches have advantages and disadvantages depending on the specific use case. For instance, Metropolitan Area Networks (MANs) and WANs (e.g., internet service providers or mobile backhaul networks) usually implement in-band solutions, while out-of-band control is more appropriate for LANs (e.g., data centers). Sharma et al. have studied extensively the failure recovery in OpenFlow networks and, in their paper [95], suggested a hybrid approach where out-of-band control is used in a failure free scenario, reverting to in-band control when the out-of-band network goes down.

Furthermore, it is noteworthy that the OpenFlow specification does not specify how control traffic paths should be implemented. Besides that, according to [96], network bootstrapping (including control channel setup) is a key issue of in-band facilities. The authors describe the control connection establishment phase after a Dynamic Host Configuration Protocol (DHCP) lease. However, they do not study the implications of mesh in-band networks. Precisely, typical configurations of in-band networks run a spanning tree protocol in the control VLANs to isolate the OpenFlow control and data traffic, as well as to prevent loops.

2.5.2 The SDN concept

According to Recommendation ITU-T Y.3300 [97], the SDN term is defined as “a set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner”. The necessity for software-defined networks first emerged in campus networks, with the introduction of OpenFlow, but now it is also used in data center and WAN environments.

Improving network management through SDN has been shown in different studies. As summarized in [98], traditional methods require network operators to deal with low-level vendor-specific configurations to enforce complex high-level network policies. On the contrary, management of software-defined networks are highly simplified as elements are controlled with standard protocols. Thus, SDN provides network programmability, which has actually “become a must for next-generation networks” [49]. Regarding the comparison with other legacy control technologies, there are several studies that provides an overview of advantages and disadvantages of SDN. For example, references [98], [99] presented a general overview, in which the programmability added by the SDN paradigm may ease network management, proposing techniques to improve network configurations and policy specification, focusing on reaction to frequent and continual changes to network state. Also, requirements that are emerging with the advent of this new paradigm are identified in [99].

In this way, the emerging SDN concept tends to homogenize the low-level interfaces. Unlike proprietary implementations, the control of vendor-neutral network devices is unified as the forwarding tables are configured by open controller-network device protocols. This improves the manageability and interoperability of heterogeneous cyber-physical networks. On the other hand, an important challenge is the compatibility of SDN with proprietary or legacy systems. For example, a preliminary proposal for the integration of the SDN concepts with the PROFINET standard is provided in [100].

As can be seen in Figure 2.18, which compares the traditional networking scheme with an SDN architecture, the control plane is generally decoupled from the data plane in software-defined networks. While in the traditional approach, distributed protocols (e.g., STP, OSPF or BGP) are used to exchange and propagate routing and topology information, which is used by network devices to establish the forwarding path; in a pure SDN solution the data plane consists of programmable switches, and all of the control functions are implemented in external entities. Obviously, there is the possibility of hybrid models.

Although OpenFlow [9] is the most prominent protocol to communicate both network planes, the so-called southbound Application Programming Interfaces (APIs), others technologies, such as ForCES, PCE, Interface to Routing System (I2RS) or OpFlex (by Cisco) define SDN interfaces. Actually, ForCES (RFC 3746), published in 2004, was the first attempt to standardize an open interface between the control and data planes. While ForCES separates both planes in one network element, maintaining the traditional network architecture, OpenFlow separates control plane from network devices and use a logically centralized controller. ForCES was proposed by the Internet Engineering Task Force (IETF) but was not significantly adopted by the vendors. For its part, the OpenFlow technology is being promoted, standardized, and supported by the Open Networking Foundation (ONF).

Moreover, in addition to the emergence of OpenFlow, different proposals have been published to remotely configure SDN switches. However, currently, there is no unified standard for managing all aspects of an SDN/OpenFlow device. Among other options, the OpenFlow Management and Configuration Protocol (OF-Config) could be highlighted; it is developed by the ONF and makes use of the NETCONF protocol. Nevertheless, the OF-Config protocol appeared recently and its degree of deployment is reduced. Another notable example is the Open vSwitch Database Management Protocol (OVSDB), standardized in [101], which uses a remote procedure call encoded in JavaScript Object Notation (JSON-RPC). Although OVSDB was initially supported by Open vSwitch (OVS), which is currently the most widely used software switch in virtualized environments, it is now being supported by vendors, such as Juniper, Arista, or Dell.

Summarizing the above, it can be said that, despite the purpose of eliminating vendor-centric solutions and ongoing efforts towards interoperable systems, this current lack of interoperability is an important

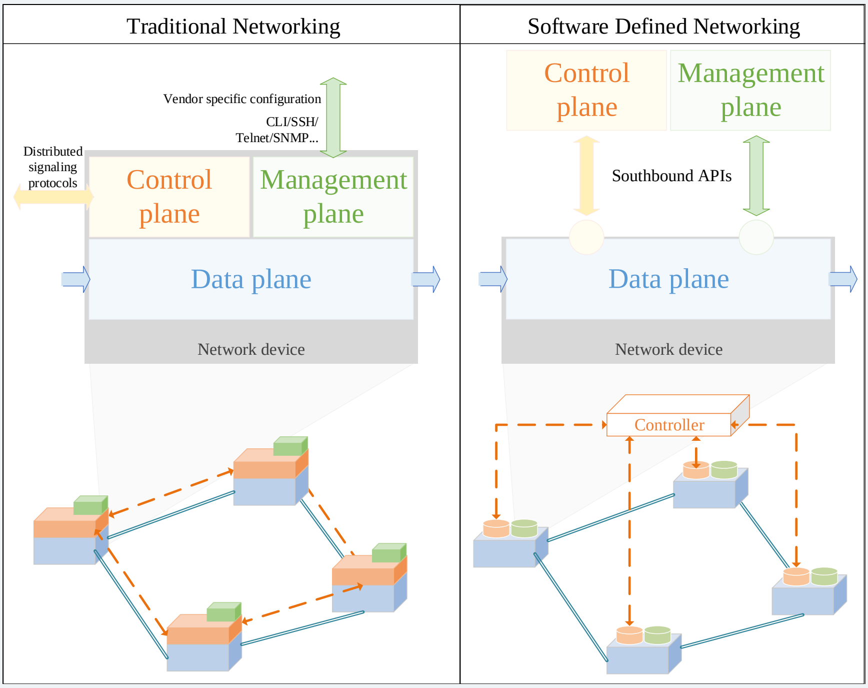


Figure 2.18: Traditional vs. software-defined architectures.

issue to support multi-vendor networks. Thus, there is still a need for close coordination between standardization bodies, industry forums and open-source projects, as stated in [102].

2.5.3 Evaluation of the OpenFlow specification and challenges of a logically centralized control

In contrast to traditional network models, programming the data path by external software enables the set up of forwarding policies according to awareness of the network state. Thus, a more efficient traffic engineering can be performed through a logically centralized entity having global visibility, enabling automated configuration based on network changes and external requirements.

On the other hand, the physically centralized approach initially proposed by OpenFlow could pose scalability and reliability concerns, as the controller could become a bottleneck and a single point of failure. However, as OpenFlow technology has advanced, new versions of the protocol have included features that improve the reliability of the centralized control plane, which makes it more profitable to be applied to industrial-grade networks, as will be described next. This section also presents several studies that have focused on the resilience and recovery issues of SDN facilities. Other issues related to the protection of control and management planes and SDN security challenges have not been considered in this thesis.

In this way, though the original SDN/OpenFlow centralized architecture seems to contradict with features identified in critical time-sensitive environments, these possible drawbacks can be overcome as summarized below:

- **Behavior during a control plane failure**: With respect to failures of the control channel, the initial version (1.0) of OpenFlow specified that, when a switch-controller connection goes down, the switch deletes all normal entries and matches flows according to the "emergency flow table". However, this table was removed in version 1.1, which defines two operation modes that are triggered by a connectivity interruption:

    - Fail secure mode, in which switches continue operating in OpenFlow mode, until they reconnect to a controller.

    - Fail standalone mode, where switches revert to a non-OpenFlow pipeline, performing Layer 2/Layer 3 switching functions. Switches that support both Operation and legacy forwarding operation (using the *OFPP_NORMAL* reserved port according to the OpenFlow specification [9]) are known as OpenFlow-hybrid switches.

- **Minimal latencies**: because the control plane is decoupled, being communicated via the OpenFlow protocol that runs over TCP, it may experience higher latencies than in monolithic approaches. Although the authors of [103] provide a quantitative study "on the non-negligible amount of control traffic in a SDN network running in reactive mode", it should be kept in mind that time-sensitive flows require a proactive behavior, where paths are precomputed, which does not introduce additional delays. This mode of operation is not required for non-critical traffic, such as MMS or Hypertext Transfer Protocol (HTTP). The importance of using a proactive operation mode in order to reduce communication latency is contrasted in [104].

- **Multiple controllers**: regarding scalability and the control plane fault tolerance, OpenFlow version 1.2 brought the possibility of connecting switches to multiple controllers, which enables load balancing and reduces recovery time during a controller failure. In a scenario with multiple controllers, master and slaves roles are assigned. Obviously, controllers must be coordinated between them to maintain a consistent global state; however, synchronization mechanisms are "outside the scope of the OpenFlow specification" [9]. References [105], [106] studied distributed and robust topologies, considering the optimal number and location of controllers in WANs. Likewise, in [107], the authors of the paper simulate the latencies between switches and a different number and locations of controllers to find the appropriate recovery process after link failures, proposing a robust architecture against disasters.

- **Fast failover groups**: with regard to the failover capability of an OpenFlow network, starting on version 1.1, the OpenFlow specification [9] defines group tables, oriented to implement "multipath or link aggregation" features. These tables also support the so called "fast failover group" entries as a protection mechanism. They are designed to accelerate the recovery process, by allowing OpenFlow switches to forward traffic to alternative paths without involving the controller. Fast failover groups are composed of a series of buckets, executing the first active one (flag *OFPPS_LIVE*). Specifically, buckets include the *watch_port* and *watch_group*[8] fields that indicate liveness. The port config bit *OFPPC_PORT_DOWN* and the port state bit *OFPPS_LINK_DOWN* indicate whether a port and a link are down, respectively. As a consequence, it is required to implement liveness monitoring and, according to the OpenFlow specification,

[8] A group is live if at least of one its buckets is live.

> this can be managed outside of the OpenFlow pipeline, either via “spanning tree or a keep-alive mechanism” [9]. In addition, it can be combined with a backup path computation proactively installed by the controller, so that the failover time is reduced.

Obviously, the reliability of SDN-based networks is related to the control plane availability. Improving the performance, reliability and scalability of the distributed control channel has already been studied [108]–[111], as well as determining how many controllers, topology and controller location, inter-controller communication, consistency and synchronization. Reference [108] analyzes the controller placement in SDN networks with respect to resilience, latencies and load balancing in the control plane, both from nodes to controllers and among controllers. Also, the survey presented in [109] includes an overview of several distributed control plane approaches, where the majority of research suggest architectures divided into domains each with their own controller, such as in HyperFlow [110] or in Kandoo [111]. Specifically, Kandoo proposes a hybrid configuration where local and global controllers work together to handle the data path according to the required network information. In this way, faster requests are managed by a local control services, reducing the amount of traffic on the global controllers. From a general point of view, the authors of [112] summarized different approaches that make these networks more robust, such as using multiple controllers, backup forwarding rules, as well as delegating the failure detection to the network devices.

2.5.4 Opportunities for SDN in industrial networks

After taking into account important aspects like scalability or reliability, the suitability of the SDN/OpenFlow paradigm is considered in order to meet the lack of programmability in previous networking architectures. Indeed, an SDN controller would be able to establish paths between sensors and actuators according to bandwidth, latency, redundancy, and safety considerations. As will be seen below, there are recent position papers that have envisaged proposals where the advantages of the SDN paradigm may be used for industrial networks.

One of the most prominent examples of the appropriateness of SDN technologies in the industrial context is that the CPS Public Working Group (PWG), formed by the NIST, has recently determined the adoption of SDN technologies to dynamically manage cyber-physical networks [43], due to the aforementioned reasons. Similarly, the DetNet group has adopted an SDN architecture to support the required traffic engineering capabilities for providing bounds on delay, jitter, and packet loss. In the same way, the 6TiSCH protocol [113] is another IETF initiative to centralize the flow scheduling and route computation tasks in time-sensitive wireless networks, and it considers that existing SDN protocols could be extended to address such needs.

2.5.4.1 Redundancy control

Recent projects have studied the use of OpenFlow in redundant topologies, in so far as it makes it possible to overcome some limitations of traditional redundancy protocols, such as configuring multiple failover end-to-end paths. Particularly, although the MPTCP is used for load balancing in OLiMPS [68], it is notable the shown interest for using OpenFlow in the computation and provision of multiple link disjoint paths. In addition, this paper studies the reactivity of the network architecture when some links go down. However, it is noteworthy that multipath approaches oriented to centralized load balancing are not usually applied to safety critical systems because, as stated in [114], "structural redundancy is typically not used to increase bandwidth, but to send redundant information over redundant paths", which is a primary focus of this research.

Moreover, traditional link aggregation protocols, such as LACP, are being combined with SDN, as studied in [115], where new possible scenarios are provided. The authors of this paper added LACP functionalities to a controller so that it takes care of its management but offloading LACP to the switches, further than leaving the management of LACP locally to the switches themselves or handling it entirely in the controller, which would lead to scalability issues.

2.5.4.2 SDN for Smart Grid communications

Regarding the use of SDN/OpenFlow as enabling technologies for the development of Smart Grid solutions, several studies have recently perceived opportunities for this integration, along with other SDN-related research applicable to IEC 61850 compliant systems. On the one hand, reference [116] experimentally evaluated the modularity and flexibility offered by an OpenFlow solution by analyzing how it can provide MPLS-like features and the coexistence of both technologies in the context of a Smart Grid application. Furthermore, taking into account that OpenFlow emerged for achieving network isolation to enable researchers to run experiments on production networks, the authors of [116] proposed using OpenFlow to test new technologies for Smart Grid development. However, this paper is not focused on the inter-substation environment.

On the other hand, regarding the scope of OpenFlow in IEC 61850 facilities, reference [117] is mainly focused automating the substation network configuration. However, with respect to maintenance of the operating network, it only contains ideas, as also identified in [118], such as the configurable packet inspection, dynamic monitoring, security policies and access control between connected IEDs, thereby enabling "the controller can easily manage traffic and curtail congestion events", or it can "open the door for control applications or recording tools driven by network events and traffic patterns". However, while both papers only suggest the opportunities without implementing a solution, many mentioned capabilities will be detailed in Chapter 3.

2.5.4.3 Wireless communication control

Prior to SDN/OpenFlow, the Control And Provisioning of Wireless Access Points (CAPWAP, RFC 5415) protocol enables a centralized management of wireless APs, being adequate for multi-vendor deployments. However, as identified by the ONF, this standard fails to address essential gaps, which can be filled with the combination of an SDN/OpenFlow-based control plane. Specifically, by using this approach would enable the network management and monitoring of unified, wired and wireless, infrastructures. For example, running both Open-

Flow and CAPWAP under the same controller could provide end-to-end control of QoS policies [119].

Route computation in a centralized way by an OpenFlow controller is similar to the Network Manager used in ISA100.11a, WirelessHART and 6TiSCH[9]. This manager is certainly the main component of those architectures and is responsible for configuring the network resources and managing routing between devices. Thus, "thanks to the centralized approach, field device complexity is kept low" [120]. Similarly, an OpenFlow controller is able to create, by using a common control interface, redundant paths based on the network status and information received from the network devices.

In relation to the object of study, SDN is being proposed [119] to transparently manage hybrid networks, where wireless and wired systems interact. Also, reference [121] uses OpenFlow for the mobility management in wireless mesh networks. Likewise, the OpenRoads project [122] uses OpenFlow to actively establish redundant wireless links, whether under Wi-Fi and WiMAX technology, achieving an uninterrupted communication in roaming situations. The detection and removal of duplicated packets by the receiver is performed by a Linux kernel module (called *nf_mobility*). This module provides a sequence number for connection (based on the 5-tuple: protocol, source and destination IP addresses and TCP/UDP ports).

OLiMPS and OpenRoads projects aimed at increasing the resilience where the duplication management function is relegated to the end nodes, as occurs in PRP. However, in contrast to PRP, these approaches are not compatible with those protocols that send data directly into lower layers; as occurs, for example, in the IEC 61850 standard, where GOOSE and SV services transport critical information and are mapped directly on layer 2 frames.

[9] 6TiSCH also supports distributed and hybrid approaches.

2.6 Summary

After the overview of network technologies used in industrial systems, and particularly in IEC 61850-based ones, multiple network functions have been identified as necessary to properly support the target application, which involves, among other things, meeting latency, priority, security and reliability constraints. In traditional switched Ethernet networks, the path computation is based on MAC learning over spanning trees, which is performed by means of distributed control protocols. In fact, distributed algorithms are well-suited for best-effort service delivery models [93]. Nevertheless, satisfying the goals of today's industrial applications requires the support of sophisticated functionalities, such as traffic engineering and restoration mechanisms. However, complex industrial networks are generally designed, configured and tested according to a predefined policy enforcement in order to meet high levels of performance and availability. In the majority of cases, this is carried out in a static way, requiring a great deal of manual configuration. Hence, despite the fact that fixed and dedicated infrastructures make easier to provide QoS guarantees for critical services, they do not support the adaptability demanded by reconfigurable CPSs [123]. Moreover, in agreement with [124]–[126], conventional fixed network protocols fail to address the dynamic aspects of CPS applications. To overcome this ossification, as the complexity of network management increases, it is necessary a control scheme that separates discovery, computation and decision processes from the data plane [93], [94].

As a result, a proper critical infrastructure design must be well adaptable to network conditions in order to provide the required performance and meet specific application needs. Thus, all of previously described requirements and shortcomings, which are listed in Table 2.8, demand a global control of network resources. Quality goals have been grouped into four broad categories for ease of understanding.

Table 2.8: Demands of target industrial networks.

Requirements		Qualitative design goals	
R1	Traffic prioritization	**Programmability: QoS and Security**	G1
R2	Flexible and reconfigurable network		
R3	Traffic restriction		
R4	Central management	**Manageability**	G2
R5	Unified management		
R6	Interoperable solution	**Interoperability**	G3
R7	High availability	**High availability and efficient utilization of resources**	G4
R8	Higher redundancy efficiency		
R9	Dynamic redundancy control		
R10	Efficiency improvement of PRP		
R11	Improvement of HSR control performance and efficacy		
R12	Robust WLAN connectivity		

Taking into account the arguments above, the SDN technologies can play an important role in the future cyber-physical networks. With this aim, several state-of-the-art control and management technologies have been analyzed to determine the best choice to build an SDN platform suitable for demanding environments like IEC 61850-based systems. Likewise, it is necessary to study the benefits that software-defined networks can offer to high-availability industrial systems, including wireless ones where connections are more susceptible to interference.

It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change.

Charles Darwin, On the Origin of Species

3

A proposal for applying SDN in industrial networks

Contents

After reviewing the state of the art and the main requirements of industrial networks, it is worth describing an application scenario where to apply the SDN architecture proposed in this chapter to provide automated control and provisioning of network resources. As indicated by the ISO/IEC/IEEE 42010 [127], a reference architecture must be purely abstract and its description should identify characteristics and features. So, first, logical building blocks that match specified qualitative goals are mapped onto a high-level conceptual representation. Then, an instantiation of the reference architecture achieved by substitution of the abstract entities with concrete elements, which meet the corresponding requirements[1], is described. Thus, Section 3.3 and Section 3.4 explain the features of the proposed solution, where the latter specifically focuses on the performance enhancement of redundancy management. This separation is because low latency and high availability challenges are especially important in this context.

3.1 Application scenario

Like any other infrastructure, in IEC 61850-based networks, nodes perform different protection and control functions, sending and receiving different data flows. To exemplify the situation, Figure 3.1 depicts a typical scenario where a switched Ethernet backbone hierarchically interconnects station, bay, and process levels. Moreover, monitoring and control systems may exchange data with external networks. As described in Section 2.2.1, this communication infrastructure comprises heterogeneous equipment, such as SCADA and HMI units for monitoring and visualization information from RTUs and IEDs, which, in turn, receive data from sensors and metering devices, and perform control and protection functions in power systems. In addition, Figure 3.1 also contains PRP/HSR and wireless communication technologies, which are present in today´s complex substations, as well as other devices, such as personal computers, printers, cameras, etcetera. This scenario could be used to support a variety of different types of traffic including, for example, SV, GOOSE and MMS messages, as well as others like FTP, HTTP or SNMP [23].

As described in [128], large-scale IEC 61850 systems can integrate more than 600 devices organized, for example, as a combination of ring and star topologies. There is a lack of interoperability in the deployment of such a variety of communication devices and characteristics, which usually leads to vendor-specific management systems. Furthermore, varying communication conditions, such as bandwidth or network load, may affect the message transfer performance. Thus, control functions should depend on network state information to make dynamic decisions, so resource monitoring is essential to maintain performance accordingly.

[1] Again, margin notes are used to improve readability as they highlight the qualitative goals and requirements considered in the architecture design.

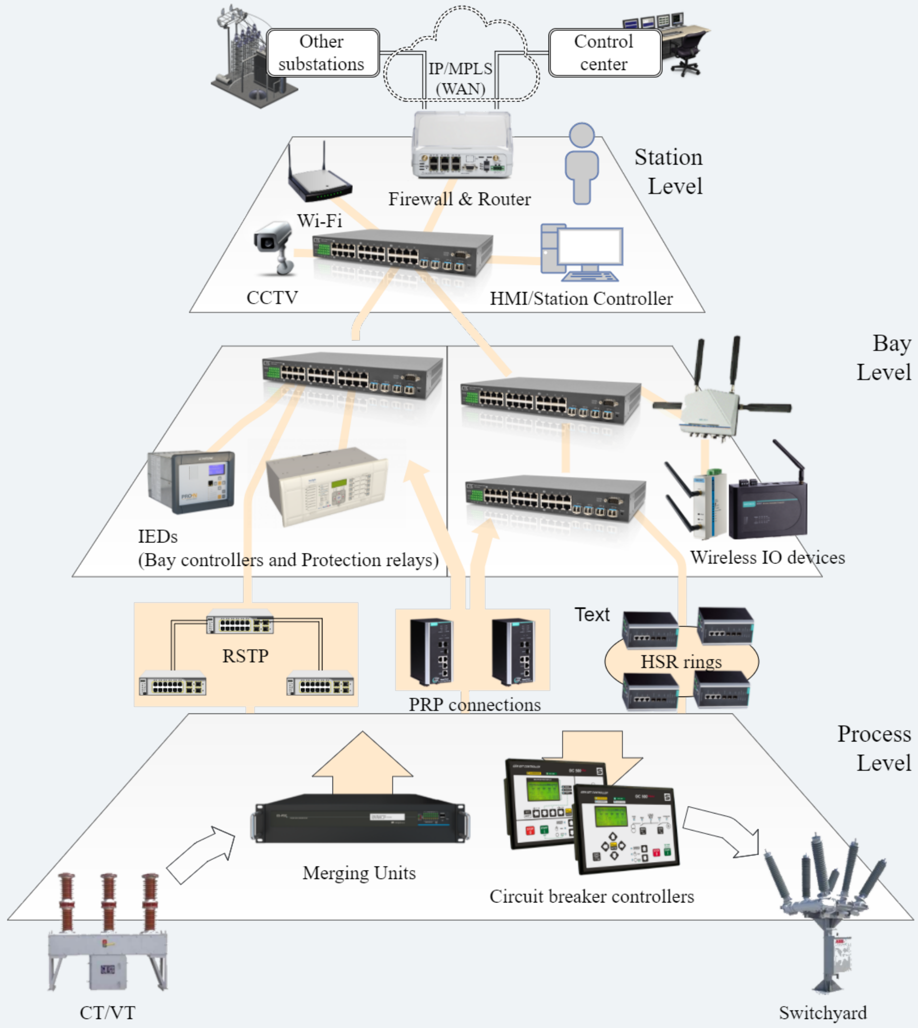


Figure 3.1: Substation communication scenario.

Nevertheless, in traditional networking, network condition monitoring and diagnosis are performed at device and port level, and data path is based on a predetermined profile. All packets are forwarded in the same way, and operational management tools (e.g., SNMP and web-interface based NMSs) need to configure VLAN and multicast MAC filters for all switches in the substation. Likewise, the static behavior of PRP and HSR can be a limitation when future smart grid scenarios tend to integrate changing and more bandwidth consuming services. As a consequence, a traditional approach is not able to efficiently meet the demands of modern control systems. On the contrary, an SDN-based approach to provision connectivity services in IEC 61850 systems can overcome these challenges and address new opportunities. Such an approach is presented below.

3.2 An SDN architecture to manage IEC 61850 network traffic

The proposed architecture, which is shown in Figure 3.2, is based on a complete Network Operating System (NOS)[2], which consists of a set of control, monitoring and management (CMM) functionalities:

- **Control plane**, which is responsible for computing and setting up routes and reacting to changes in network conditions.
- **Resource monitoring**, and its integration into the control plane, allows the system to act dynamically.
- **Management capabilities** with the aim of provisioning network resources, so that an external agent is responsible for creating, deleting or modifying operating parameters, such as interfaces, queues, etcetera.

The SDN architecture has to be designed in such a way as to agree with the qualitative arguments included in Table 2.8, as highlighted in the following margin notes. In this way, the NOS acts as a central interface where the control plane may receive diverse information, such as commands or status alerts, which are translated into flow entries to be automatically populated in the deployed networking devices.

[2] As defined in [129], a NOS provides “a uniform and centralized programmatic interface to the entire network”.

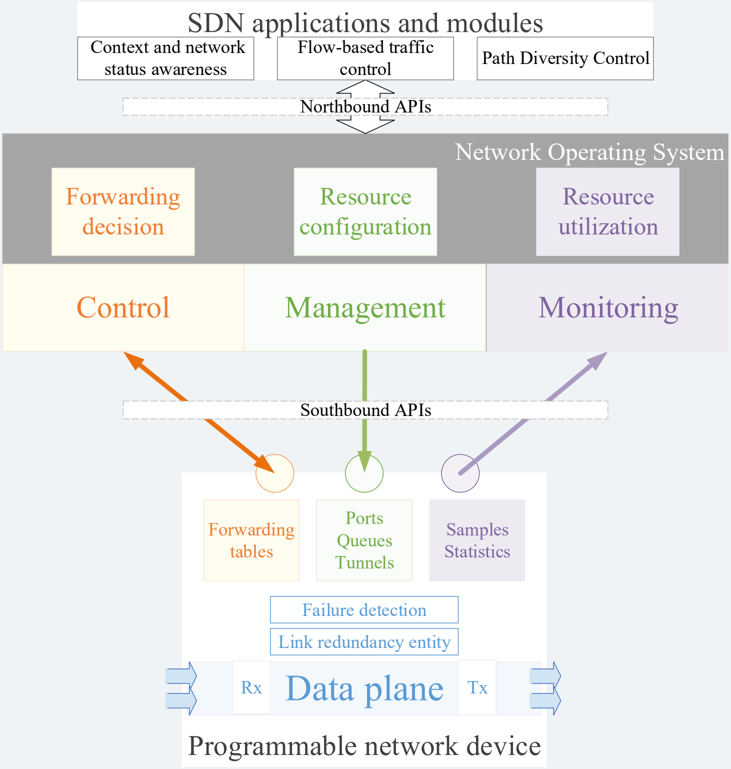


Figure 3.2: Proposed SDN architecture.

Then, it instantly varies the behavior of a network, being able, for example, to allocate resources to different type of traffic, exposing more paths to increase reliability, etcetera. As shown in Figure 3.2, applications written on top of the CMM architecture connect to each other via northbound APIs, whereas communication with network elements is performed through vendor-independent southbound APIs. The arrows between the network device and the NOS indicate the main direction of the flow of information, which can be grouped as follows:

G3
Interoperability

- Downstream (from the NOS to network devices): flow-level programming and network configuration.

- Upstream: feedback information from the network (i.e., packet-in, traffic flow statistics, device condition and failure reporting, etcetera).

It is necessary to note that certain control functions are delegated to these network elements. Thus, besides storing the flow tables, they provide distributed capabilities to enable, for example, failure detection and discovery mechanisms, or to support active redundancy.

The following is a description of the main functionalities to be provided by the architecture:

- **Context and network status awareness**. Analogous to control theory, where stability, observability and controllability are key concepts, the monitoring system receive real-time feedback and the platform allows network planners to define thresholds for triggering appropriate actions. Figure 3.3 outlines a control diagram where an adaptive system dynamically operates according to the received measures, events or triggers. For example, changes in network topology, bandwidth saturation or failures must be taken into account by the control plane to act consequently. Moreover, the NOS is also based on exogenous context information, which enables a unified method for configuring the communication network after the design phase of a SAS. By operating in this way, this forms a IT/OT convergence between substation and communication designs. There are commercial proprietary systems [53], of which there are no results or appraisals available, that address the integration of network management and control of IEC 61850-based substations without using the capabilities of SDN. On the contrary, the proposed framework facilitates the interoperability by relying on standard solutions, a main objective of IEC 61850 to avoid vendor-specific configurations.

G2
Manageability

- **Flow-based traffic control**. Unlike commercial off-the-shelf (COTS) switches that forward traffic based upon a spanning tree, the VLAN tag, and address learning processes, the SDN-based data path control processes the traffic according to flexible packet-forwarding rules, that can be exploited for implementing services such as:

G1
Programmability: QoS and Security

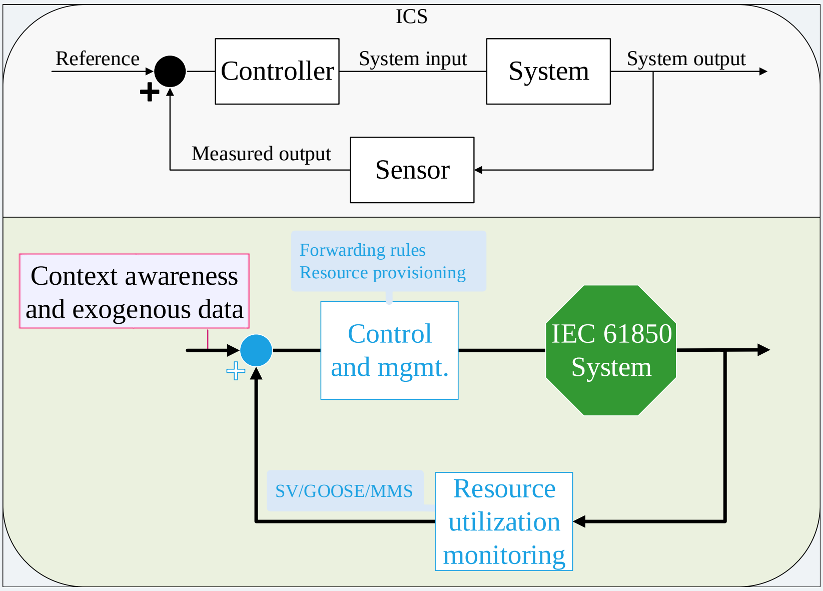


Figure 3.3: An SDN approach based on a control-loop feedback mechanism commonly used in ICSs.

- Traffic filtering policy enforcement: the ability to define the granularity of a flow (e.g., a flow could be defined as a combination of header fields, from layer 1 to layer 4) enables fine-grained control policies. This feature should also be present in PRP/HSR nodes to increase flexibility in inbound and outbound rules.
- QoS support: the CMM platform allows network designers to establish traffic shaping policies that distinguish flow types in a centralized manner, so that it is possible to take into consideration priority requirements of GOOSE or SV services.
- Layer 2 tunneling: although the platform disclosed herein is conceived in the context of switched LANs, it should be considered that new automation features may also need to traverse the WAN. Thus, it is necessary to set the appropriate parameters in network devices to establish tunneling (or encapsulation) techniques to transmit GOOSE or SV Ethernet frames between substations, and control centers.

- Network security: as analyzed in Section 2.2.6, security features built into network architectures are essential to any industrial deployment. Preventive protection through traffic isolation and access control mechanisms, should be augmented with anomaly detection mechanisms that react to threats.

➤ **Path diversity control**. The proposed scheme improves the network utilization through a network global view and dynamic actions, as follows.

G4
High availability and efficient utilization of resources

- Traffic forwarding and latency reduction: latency and jitter are affected by the number of hops and amount of traffic in layer 2 networks. Unlike spanning tree-based approaches, a combination of load balancing and multipath techniques takes advantage of partial mesh topologies to improve communication performance in time-sensitive environments. For example, in contrast to proposals based on static MSTP configurations [24], SDN can provide flexibility so that non-critical flows can be forwarded reactively with the aim of using underutilized routes.
- Performance improvement of PRP/HSR technologies: awareness of DAN/SAN, critical traffic and network status allows processing the data path and managing resources efficiently. Taking into consideration that PRP does not specify how to compute routes and instead of using this protocol in conjunction with common spanning tree technologies, it is proposed that the network control plane may be not agnostic about PRP nodes by introducing SDN-enabled switches. This choice is aimed at getting the best of both worlds: centralizing forwarding decisions and the implementation of the redundancy control mechanisms in the end nodes. With a similar approach, this SDN approach aims to efficiently improve HSR performance through flow-based multipath forwarding that ensures network reliability without introducing delay or inconvenience to critical data.
- Redundant wireless communication control: although wireless management systems must consider many factors, from the robustness point of view, wireless networks need to provide reliable data transfer in order to be used in safety-critical

applications. Therefore, the CMM platform has to deal with mobile devices through redundancy mechanisms that reduce interruptions.

In consequence, this approach takes advantage of having a global view of the network status to flexibly assign resources to different services. Figure 3.2 illustrates how the SDN framework centralizes the network intelligence and, as outlined, acts as a closed-loop feedback control that reconfigures QoS and routing policies according to changes, while guaranteeing security, reliability, and real-time requirements at the same time. Subsequently, the previously described features are illustrated by a specific solution.

3.3 Instantiation and solution features

While in the previous section the architectural capabilities have been correlated with the above-mentioned qualitative goals, main requirements identified in Chapter 2 have not yet been explicitly matched. Thus, following the recommendations for architecture descriptions defined in ISO/IEC/IEEE 42010, the previously-described architecture captures the essential attributes and provides a basis for instantiation of concrete components. Likewise, the ISO 15704 defines "the genericity dimension", which ranges from a "reference architecture" resembling generic building blocks, to a "particular architecture" that instantiates those generic blocks. Therefore, after an abstract description, control, monitoring and management functionalities can be particularized in the following way:

- **Control plane** composed of OpenFlow controllers[3] responsible for establishing forwarding rules at network switches. This involves, among others, the following tasks:
    - A discovery service module allows the controller to know the existing topology. To achieve this, the controller periodically sends LLDP and Broadcast Domain Discovery Proto-

[3] An OpenFlow-based control plane also supports a distributed architecture that increases the scalability and reliability of the network as the switches can be controlled by more than one controller.

  col (BDDP) packets to all controlled switches and receives returned packets from them. Hosts can be passively identified by examining their injected packet-in messages. An analysis of the control traffic in a topology discovery process for SDN networks is given in [130].

  - A path computation module, which determines a route from origin to destination and is capable of preventing loops.

- **Resource monitoring**: real-time passive measurement is based on distributed sFlow agents that constantly report traffic statistics into sFlow datagrams to the collector. Once analyzed the obtained information, the network state can be estimated and, consequently, a feedback loop allows the controller to react to changes in the network conditions, and adjust the resources as needed. In this way, considering the increasingly effective combination of sFlow and OpenFlow, some of the anomaly detection and actuation methods implemented in [59] are here placed in the context of substations.

- **Management capabilities**: the OVSDB protocol has been chosen to carry out management and configuration operations on the network devices as it allows the creation, configuration and deletion of ports, queues and tunnels of switches. In this way, the management agent exchanges requests and replies, in JSON-RPC objects, with the ovsdb-servers running on network devices. OVSDB

Figure 3.4 shows the instantiated architecture, including the above-mentioned components, along the IEC 61850 protocol stack. From the network device perspective, remote programmability features are achieved by supporting OpenFlow, sFlow and OVSDB protocols to interact with the centralized NOS, as well as by including PRP and HSR protocols for high availability. Using open-standardized communication protocols reduces reliance on vendor-specific appliances and facilitate seamless integration of independent implementations.

R4
Central management

R6
Interoperable solution

From another point of view, the reference SGAM has been applied for this instantiation. The methodology employed by the SGAM expedites the design of new structured power system developments. In fact, this method has facilitated the identification of the Smart Grid use case and

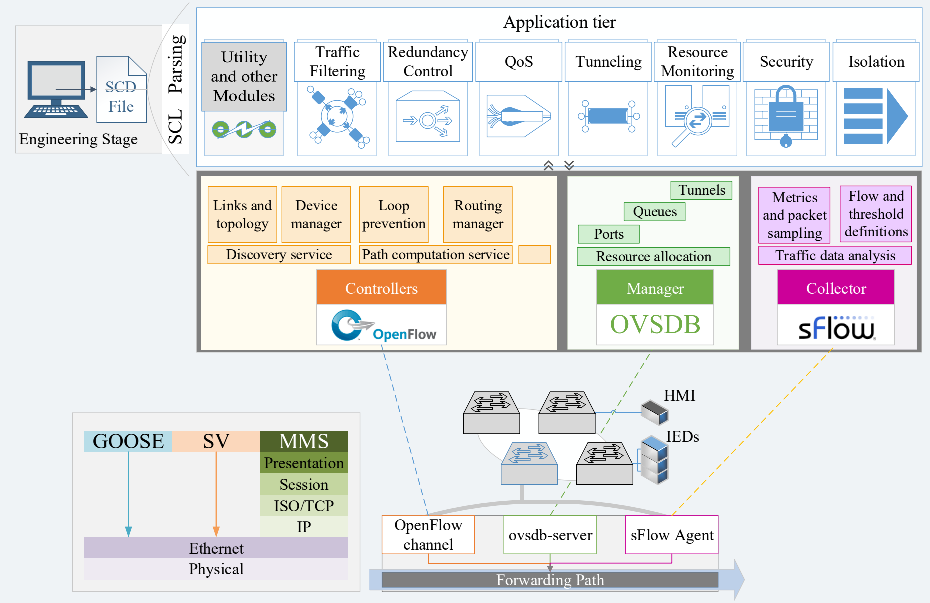


Figure 3.4: NOS functionalities.

the design of the solution disaggregated into specific data models, protocols, and control functions. Figure 3.5 shows the resulting transmission domain in the zones and layers of interest: information, communication and component ones. Moreover, the actual configuration attributes and rules of an IEC 61850 system can be integrated into the NOS, which is described in the following section.

In the following, general network functions provided by the architecture are particularized below. Since several requirements are intended to improve the use and availability of redundant systems, Section 3.4 particularly focuses on the suitability of this approach for high-availability networks.

3.3.1 Context and network status awareness

The following describes how the solution import SCL configuration files and gathers information on the state of the network.

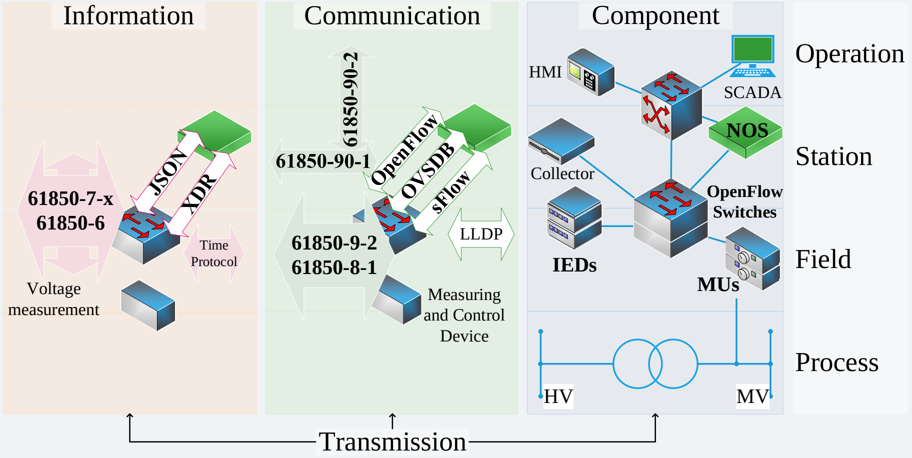


Figure 3.5: Information, communication and component for transmission domain according to the SGAM framework.

3.3.1.1 IEC 61850 integration

The proposed architecture benefits from the programmability feature of OpenFlow to map the IEC 61850 communication and data models,. Thus, SCL data parsing provides a mapping method between the engineering stage and the CMM platform. In this process, SCD files are translated into information that can be handled by the OpenFlow controller, obtaining accurate information about the substation configuration (Figure 3.6). This way, the controller can distinguish existing devices in the managed LAN and their data flow parameters, so it may automatically determine the logical topology of the substation, and decide how to route, modify or discard traffic flows, providing exactly the required performance.

Several properties are obtained after an appropriate SCD file parsing to build flow forwarding entries that are installed in switches, enabling IEDs to publish and subscribe information. Specifically, each IED section is parsed, for which there are a series of input subsections that define all external signals of interest identified by the name of the publisher IED (*iedName*). Figure 3.7 partially illustrates an SCD file, where elements

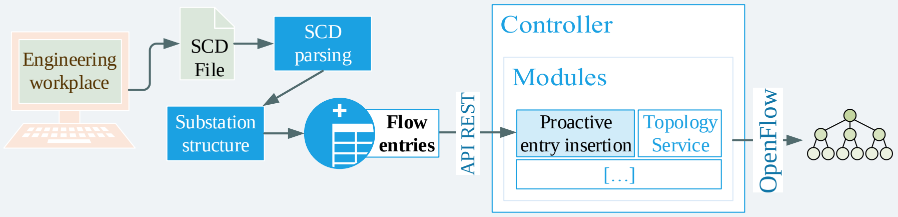
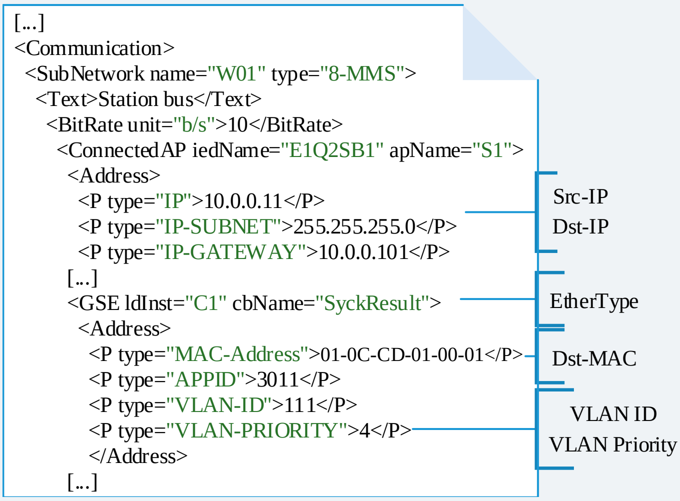


Figure 3.6: Parsing process flow.

and values mapped on OpenFlow fields can be identified. To establish the flows correctly, the controller has to know the connection between the switches and the IEDs (ports and physical topology). In particular, it is considered that the connection of each device with each switch in a network is known, so this information is statically incorporated in the controller logic. Namely, the controller has an a priori knowledge of IED connections, associating a particular IED with a concrete edge switch. This involves installing rules, which associate a publisher-subscriber flow to the corresponding input/output switch ports. Though inflexible, this choice, where a particular port is assigned to an IED, is preferable and makes it difficult the port swapping once the network is deployed. Another alternative to obtain the physical connection of IEDs is the approach described in [117], where the controller proactively communicates with IEDs by ICMP; likewise, this is suitable because static IP addresses are recommended [23]. Nevertheless, this restricts the use of simpler devices that only implement SV and GOOSE (layer 2 only devices), which is very common in process bus equipment.

Consequently, this proposal may be an appropriate tool to automate network administration, which is a need reinforced by [28], where the authors suggested that "the complexity of the data network configuration for a large substation makes automated management of network switches an attractive option [...] automated tools could be developed to extract this information to streamline the VLAN and multicast address filter configuration of Ethernet switches from multiple vendors". Moreover, despite the fact that [118] proposed to obtain network information derived from IED device configuration, the authors did not use the IEC 61850-6 standard, while a description of the SCD parsing is included

R5
Unified management



```
[...]
<Communication>
 <SubNetwork name="W01" type="8-MMS">
  <Text>Station bus</Text>
   <BitRate unit="b/s">10</BitRate>
    <ConnectedAP iedName="E1Q2SB1" apName="S1">
     <Address>
      <P type="IP">10.0.0.11</P>
      <P type="IP-SUBNET">255.255.255.0</P>
      <P type="IP-GATEWAY">10.0.0.101</P>
     [...]
     <GSE ldInst="C1" cbName="SyckResult">
      <Address>
       <P type="MAC-Address">01-0C-CD-01-00-01</P>
       <P type="APPID">3011</P>
       <P type="VLAN-ID">111</P>
       <P type="VLAN-PRIORITY">4</P>
       </Address>
     [...]
```

Figure 3.7: Mapping of SCL parameters in OpenFlow fields.

here. Also, taking into account proposals for enhancing IEC 61850 as found in [20], where several extensions related to network parameters and communication monitoring are defined to be included in IEC 61850-6, processing new SCL parameters may enable future scenarios that can be handled centrally.

3.3.1.2 Responsiveness and resources monitoring

R2
Flexible and reconfigurable network

In order to implement effective traffic control and meet strict QoS constraints, collecting real-time network state information is required to enable network-wide visibility and be responsive to network conditions. The proposed SDN scheme is reported on link utilization data and packet samples, so that it is able to detect network stress events during which delays may increase. This is possible because sFlow provides information about flows, communication interfaces and a number of other metrics describing the status of the device. This could be also used for link dimensioning for network planning purposes.

Regarding network failure detection, the platform is able to operate in two different modes: reactively or proactively triggered. The first case is a suboptimal approach where a controller-based restoration module is responsible for rearranging traffic in other paths when a *OFPT_PORT_STATUS* notification has been received (i.e., when a port or link goes down). More specifically, a failover manager module removes the flows entries that forwards traffic to the downed port so that the controller computes a new path as a new *packet-in* is received[4]. As studied in [95], in a flow restoration scheme the dependency on the centralized controller[5] made "carrier-grade reliability" difficult to achieve, suggesting to implement protection mechanisms. Effectively, a faster recovery is achieved with the pre-configuration of backup paths and switching automatically without the need of involving to the controller. With this aim, switches have to perform liveness detection where CFM or BFD sessions monitor different links or paths, respectively. In order to reduce the recovery time, transmit intervals of such sessions must be decreased.

3.3.2 Flow-based traffic control

Some exemplary traffic control features are described below.

3.3.2.1 QoS provisioning support

A QoS module makes possible to push flow rules that redirect specific traffic to different queues, which must be previously created and configured on the particular switch; in this case, the OVSDB protocol is used. As a result, OpenFlow actions are populated together with QoS policies[6], which can be exploited by all flow types including those whose

R1
Traffic prioritization

[4] It should be noted that, in the OpenFlow operation, if a network failure occurs and the affected flow entries are not modified or deleted, the associated idle timeout will not expire while packets are being received [9].

[5] Recovery time depends on failure detection, notification and reaction times.

[6] OpenFlow supports QoS [9] by setting the network Type of Service (ToS) bits and enqueuing packets. However, as the specification indicates, "queue configuration takes place outside the OpenFlow switch protocol, either through a command line tool or through an external dedicated configuration protocol".

data rate can be known a priori, such as SV (*SmpRate* field indicated during the engineering stage in the SCD files parsed).

With regard to the ingress rate control, the OpenFlow *meter* tables can be used to perform actions based on the observed rate of received packets. In particular, per-flow metering is based on *bands* that define rate and burst size parameters. If the specified bandwidth is exceeded, packets will be dropped or marked with DiffServ codepoint (DSCP) values. However, metering is an OpenFlow optional feature (available from version 1.3 onwards) and, for example, OVS does not currently support it.

3.3.2.2 Traffic filtering

Because GOOSE and SV frames are both multicast (SV can be also unicast), IEDs should be configured to subscribe or not to subscribe to certain services according to the SCD files, which is indicated by the *LGOS* and *LSVS* supervision logical nodes, as defined by the IEC 61850-7-4 specification. Additionally, in order to reduce the network load, switches should be configured to filter specific multicast MAC addresses and VLAN IDs only to determined ports, which is recommended by the IEC 61850 guidelines [23]. In the proposed architecture, the forwarding rules are automatically generated from SCD parsing and are installed into controlled switches. Therefore, this automatic and static behavior facilitates the deployment and implementation of a network, allowing the more critical traffic (only GOOSE and SV messages are predetermined by SCD files) to flow efficiently through the network.

R3
Traffic restriction

In this case, multicast flows are treated as a set of unicast paths as publishers and subscribers are known. The establishment of these forwarding rules is done by getting the union of shortest paths as follows:

1. For each subscriber to a GOOSE/SV service, a shortest path to the publisher node is obtained by using the Dijkstra algorithm.

2. Once collected all the paths, that is 1-to-1 correspondences between nodes, the distribution tree is formed by the union of them.

3. This process is repeated for each pair of publisher-subscribers and, hence, the final delivery tree reaches all the receivers from the senders.

The union of all shortest paths may not constitute a minimal tree interconnecting publisher and subscribers so, in order to achieve an optimal solution, it would be necessary to compute the whole set of the shortest paths and implement an algorithm for directed Steiner problems [131]. However, implementing these algorithms is considered to be out of the scope of this work.

3.3.2.3 Layer 2 tunneling

Unless MUs and IEDs implement R-GOOSE and R-SV (IEC 61850-90-5) to carry GOOSE and SV between substations, it is necessary to encapsulate the exchange of layer 2 messages over a WAN. The platform can create and manage different types of tunnels in a centralized and common way, which is achieved through OVSDB commands, as this cannot be provisioned by OpenFlow messages. The OpenFlow protocol does support the definition of logical ports (i.e., it is an abstraction and not necessarily a physical port [9]), which may perform encapsulation.

R4
Central management

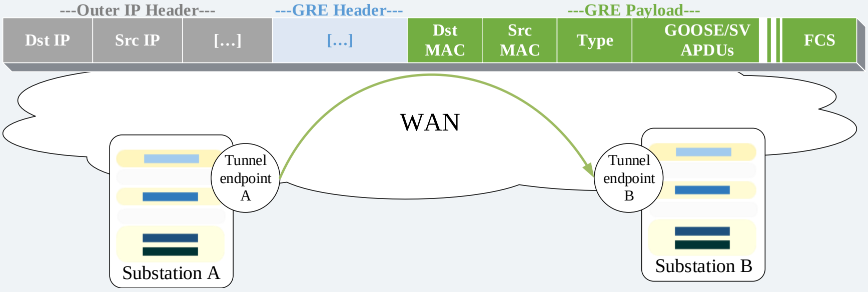


Figure 3.8: GOOSE/SV message exchange between substations by using tunneling functionality.

In particular, it is possible to forward Ethernet frames over a point-to-point Generic Routing Encapsulation (GRE, RFC 2784) tunnel, which is one of the techniques adopted by the technical report IEC 61850-90-1 to connect substation networks over a WAN. As shown in Figure 3.8, the transmission of GOOSE or SV application messages (APDUs) on top of an IP GRE tunnel can be provided between two substations. In this case, the *tunnel-id* OpenFlow match field maps the key field from the GRE header.

3.3.3 Network security

The following presents three protection mechanisms that are included in the proposed solution to enhance the network survivability.

3.3.3.1 Traffic isolation

Traffic isolation by network virtualization may be necessary to separate types of data in a substation, as previously mentioned (Section 2.2.4). The platform makes network virtualization easier by using a filter module that allows the creation of logical networks based on MAC addresses without using VLAN; although at the same time, if VLANs are used, VLAN IDs of each logical network can overlap each other. Therefore, the proposed layer 2 segmentation is oriented to create a better isolation among electrical circuit functions, and is an effective complement to the VLAN-based traffic segregation proposed by [23].

R3
Traffic restriction

In Figure 3.9, a diagram outlines an example where a network is partitioned into logical networks based on different data flows: for example, every MAC address of MUs in a process bus or a whole substation can be assigned to the same logical network and, at the same time, allocate each GOOSE or SV to a unique VLAN.

3.3.3.2 Anomaly detection

In this architecture, the sFlow collector detects when a certain threshold is exceeded for a specific flow and communicates it to the OpenFlow controller, which takes the appropriate actions. The platform allows network designers to specify flows (defined by MAC/IP addresses, Ethertype, VLAN, TCP/UDP ports, etcetera) and thresholds to moni-

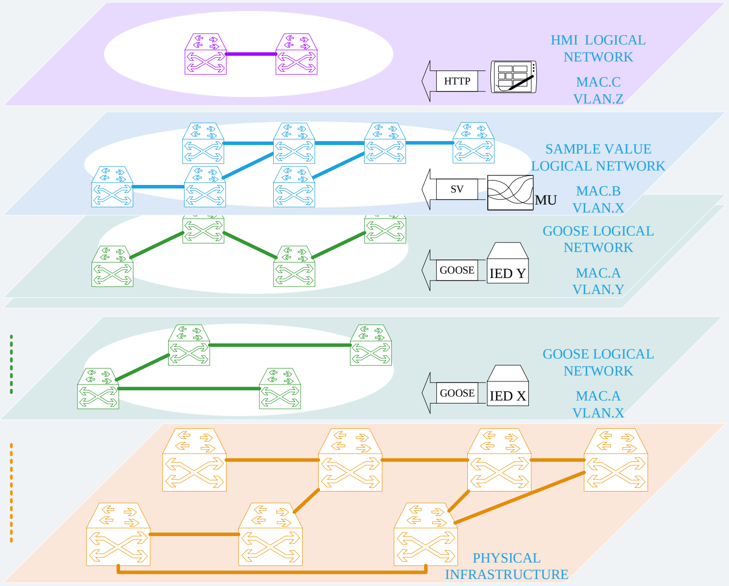


Figure 3.9: Example of network virtualization based on VLAN and MAC addresses.

tor them. By default, it establishes the SV rates obtained from the SCD configuration file to detect abnormal rates in the transmission of SVs to particular multicast MAC addresses.

Furthermore, with this feature, network designers can protect the connected nodes against Denial of Service (DoS) attacks. In particular, certain targets (for example, MAC addresses of IEDs or IPs of MMS servers) can be protected from one or multiple source addresses (distributed DoS). Once the OpenFlow controller is notified when this incoming traffic exceeds a predetermined amount, it will limit these specific packets. Figure 3.10 sketches the process by which an event-driven application written in node.js communicates with two northbound Representational State Transfer (REST) APIs in order to establish thresholds for different flows and deploy mitigation rules if appropriate.

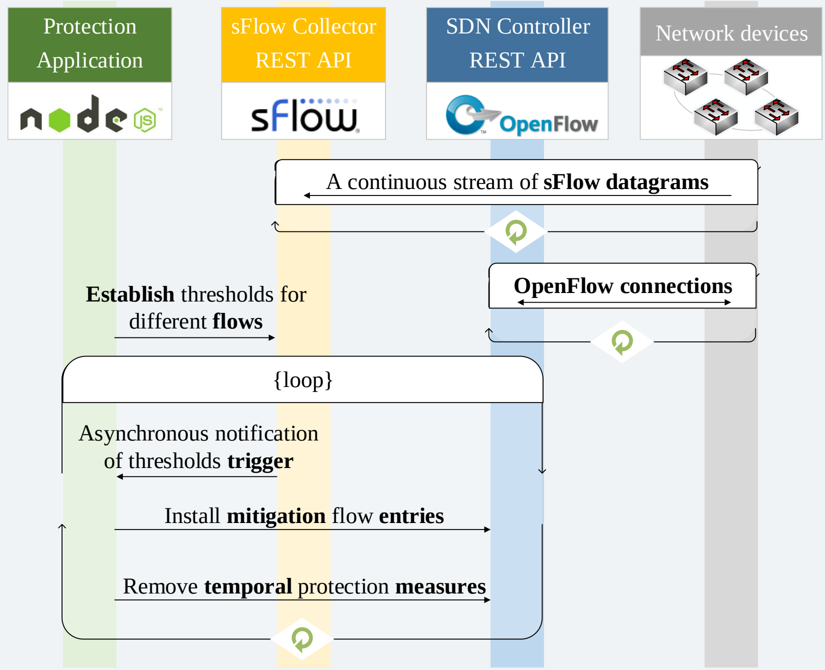

Protection Application
node js
sFlow Collector REST API
sFlow
SDN Controller REST API
OpenFlow
Network devices
A continuous stream of sFlow datagrams
OpenFlow connections
Establish thresholds for different flows
{loop}
Asynchronous notification of thresholds trigger
Install mitigation flow entries
Remove temporal protection measures

Figure 3.10: Traffic anomalies detection process.

3.3.3.3 Access control mechanisms

R3 Traffic restriction

Because of the lack of need for implementing authentication and encryption mechanisms for GOOSE and SV messages, references [45], [46] demonstrated opportunities to compromise the security of an IEC 61850 system with MAC spoofing attacks. For the purpose of solving these problems, a ACL module is used to enforce deny-by-default security policies and to limit ingress traffic according to the MAC source address, port and switch. Thus, the platform allows network planners to establish MAC ACLs statically so that only the enabled rules will be able to transmit and receive data. Moreover, using a device manager module, the controller continuously tracks and restricts the attachment of devices to only a single MAC Address (the first connected one), helping to avoid spoofing attacks and other traditional problems that may well occur when addresses are duplicated.

3.4 Performance enhancement of high-availability networks

This part of the work describes how the SDN/OpenFlow approach is able to manage path diversity in layer 2 critical networks. In point of fact, the main objective is to increase the manageability, and even the performance of high-availability Ethernet LANs to make the most of redundant topologies.

3.4.1 Reduction of Ethernet network latency

Obviously, the transmission of measurement and control data takes time, and depends on network features and configuration in addition to its current status. In order to meet timing requirements, latency analysis is a required procedure. There are several sources of latency of an Ethernet network. Although other parameters, such as QoS policies (priority queuing, classification of traffic, etcetera), also affects overall latency, the main ones are the following:

- Physical paths (either copper, fiber or radio links): elapsed time to traverse the physical medium.
- Store-and-forward latency, defined as *last bit in first bit out*. Otherwise, according to [23], using cut-through (bit forwarding) "reduces average latency but does not improve its worst case".
- Switch port-to-port latency: delay incurred by frames traversing the switch fabric.
- Queuing latency, which depends on the traffic pattern, and the output scheduling policy.

An analytical calculation of the worst case latency for Ethernet frames is detailed in [132], whereas these latencies are calculated for SV, GOOSE and MMS frames in [133]. With regard to the forwarding latency of an OpenFlow switch, it has not been increased, per se, when flow rules are already installed. It should be borne in mind that latency-critical data forwarding must be carried out proactively. Rotsos et al. [134] evaluated the switching performance of software and hardware Open-

Flow switches, which improve the switching performance. Additionally, Congdon et al. [135] implemented a model of forwarding prediction to reduce the OpenFlow forwarding latency, as well as the power consumption. These authors manage to reduce the low latency of a cut-through (bit forwarding, which is usual, for example, in HSR nodes) switch "by a factor of 3".

3.4.1.1 Shortest path forwarding: number of hops and connectivity

Obviously, previous factors must be multiplied by the number of switches that the data traffic has to traverse to reach the destination. That is to say, latency increases with the number of switches in series. Therefore, performance and real-time response depends on the number of hops per path. Concretely, given a connected, undirected graph (G), the average shortest path length is:

$$a_s = \sum_{s,t \in V} \frac{d(s,t)}{n(n-1)} \tag{3.1}$$

where V is the set of nodes in G, $d(s,t)$ is the shortest path from s to t, and n is the number of nodes in G.

In the proposed scheme, the OpenFlow controller is aware of the network topology through discovery services (Figure 3.4). Thus, an SDN controller is able to perform unicast data traffic forwarding along the shortest path in mesh topologies[7]. The effect of this change can be clearly seen in Figure 3.11.

Table 3.1 contains a comparison of the average path length (a) for different topologies[8]: rings, two-tier and three-tier designs, grids and full mesh networks. All except the last two of these networks can be found in data center, campus infrastructures and industrial automation networks. Grids and full mesh topologies have been included to complement the results in [69], where the authors obtain the minimum and maximum

[7] For example, an OpenFlow controller can be also configured to perform a traditional MAC learning function and install the forwarding rules accordingly.

[8] The number of end hosts has not been considered in the calculation, therefore only the distribution nodes are taken into account.

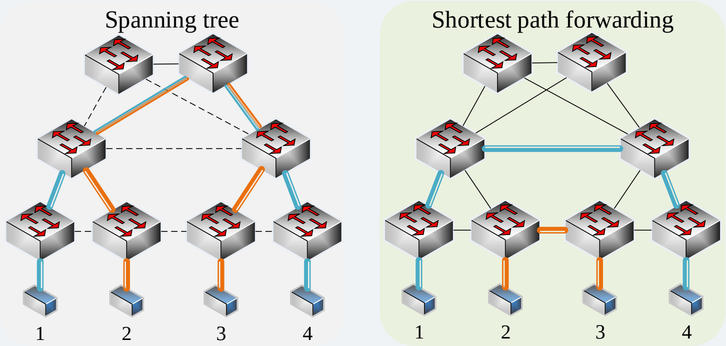


Figure 3.11: Comparison between spanning tree and shortest path forwarding in a mesh topology.

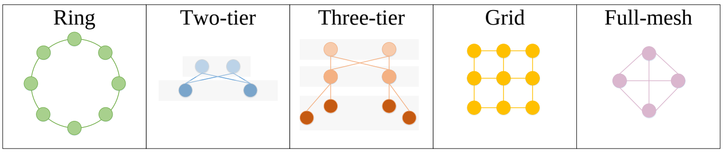
number of hops in SPB partial mesh networks without comparing them with spanning tree-based ones. All of this implies a latency improvement associated with the number of hops. This information complements and extends the analysis of the components of delay in IEC 61850 networks given in reference [136], which differently studied the latency of different flows along a specific a spanning tree topology.

R8 HIgher redundancy efficiency

Network robustness can be improved by increasing the connectivity of the network, where connectivity is the number of nodes to which a node is connected. Table 3.1 also includes the average connectivity degree, which is the average nearest neighbor degree of nodes with degree k. Each connection can be weighted by network characteristics (i.e., bandwidth). Thus, for a node i,

$$k^{w}_{nn,i} = \frac{1}{s_i} \sum_{j \in N(i)} w_{ij} k_j \tag{3.2}$$

where s_i is the weighted degree of node i, w_{ij} is the weight of the edge that links i and j, and $N(i)$ are the neighbors of node i. Table 3.1 collects each degree k with the value of average connectivity for unweighted networks. As can be seen, the connectivity of a spanning tree is substantially worse; for example, a full mesh topology becomes a star one when it is configured by a spanning tree protocol. Therefore, since the



Topology	Size	Spanning tree		Entire redundant network	
		a	k	a	k
Ring	5	2	1:2.0, 2:1.67	1.5	2:2
	10	3.67	1:2.0, 2:1.88	2.78	2:2
	15	5.33	1:2.0, 2:1.92	4	2:2
Two-tier	2,2	1.67	1:2, 2:1.5	1.33	2:2
	2,4	1.87	1:3.5, 2:2.5, 4:1.25	1.47	2:4, 4:2
core, edge	4,8	2.15	8:1.38, 1:6.8, 4:2.75	1.52	8:4, 4:8
Three-tier	2,2,4	1.93	1:5.33, 2:3.5, 6:1.16	1.86	1: 6.0, 2:3.32, 6:1.33
	2,4,8	2.24	8:1.63, 1:7.167, 6:2.17	2.09	8:2.5, 1:6.0, 2:8.0, 6:3.33
core, aggreg., edge	2,4,16	2.23	16:1.31, 1:13.5, 6:3.5	2.10	16:2.25, 1:6, 2:16, 6:6
Grid	3x3	2.61	1:2.25, 2:2, 3:2.17	2	2:3, 3:2.67, 4:3
	4x4	4.1	1:2.33, 2:2.33, 3:2	2.67	2:3, 3:3, 4:3.5
	5x5	4.85	1:2.91, 2:2.81, 3:2, 4:1.92	3.33	2:3, 3:3.11, 4:3.67
Full-mesh	5	1.6	1:4, 4:1	1	4:4
	10	1.8	1:9, 9:1	1	9:9
	15	1.87	1:14, 14:1	1	14:14

Table 3.1: Avg. shortest path length and connectivity for different networks.

spanning tree construction allows each host interface to communicate with another one along a single path, multipath connections and load balancing are infeasible. With the proposed approach, traffic can be spread among multiple paths of any length, including the shortest one and, as a consequence, the partial network load is reduced.

R8
Higher redundancy efficiency

3.4.1.2 Network load and traffic spreading

Paying attention to the queuing latency, in [133] and [132] the average latency due to queuing (L_Q) "is assumed to be" directly proportional to the network load ($Load_{Network}$), as indicated by the following formula:

$$L_Q = Load_{Network} * L_{SF(max)} \tag{3.3}$$

Where $L_{SF(max)}$ is the store and forward latency, which is the ratio of the size of the frames and the bit-rate capacity. From an experimental point of view, the traffic performance of a sampled value process bus is analyzed in [137], focusing on the maximum number of connected devices sending SVs without packet loss. The authors stated that "once sampled value frames are queued by an Ethernet switch, the additional delay incurred by subsequent switches is minimal”. However, the mentioned paper does not take into consideration a possible variation in the network load or load balancing techniques. Consequently, frames that are forwarded “in the same direction on the same path result in additional queuing delays”.

Therefore, flow-aware load balancing may prove beneficial to reduce traffic latency, meeting the IEC 61850 requirements. In fact, the OpenFlow controller dynamically sets up paths according to the existing resources (bandwidth usage monitoring) and data flows. Unlike spanning tree topologies, in this proposal data packets are spread among nodes and links. As a consequence, flows do not have to follow the same path in redundant topologies but they can be balanced through all the network resources.

R9
Dynamic redundancy control

Furthermore, a load balancer pool is created to enable the distribution of the traffic load in a set of members determined through a REST interface. The module offers load distribution for several protocols (UDP, TCP, or ICMP flows) to different servers. This functionality may be used in redundant systems, where data concentrators or gateways are balanced.

R4
Central management

3.4.2 Combination of PRP and OpenFlow

A full integration of PRP operation into an OpenFlow switch is proposed to enhance the control and adaptation ability with respect to the standard scheme.

3.4.2.1 A further active redundancy

In contrast to traditional deployments, and with the aim of creating multiple paths for pertinent data flows to achieve a better reliability, in this approach two different implementations are distinguished to establish more than a single path between PRP nodes:

- DAN-based operation mode: in which redundant paths are set in one or more LANs to which DANs are attached, so that a PRP node receives more than once the same frame through each LAN.

This is consistent with the IEC 62439-3 standard since the duplicated frames within 400 milliseconds must be handled by the LRE. While a common deployment is impaired when a second failure occurs in one LAN during the recovery period of the another one, in this proposal the performance is not degraded (without considering simultaneous failures in the node access links).

- SAN-based operation mode: it allows network designers to increase notably the availability without having to deploy a complete redundant system. In this way, a PRP node is connected to a single LAN, in which an OpenFlow controller configures more than one path for the transmission of the same content. Hence, a PRP device still receives duplicated frames through its only single interface, having to discard duplicates. This new operation mode reduces redundant resources (cabling and hardware) and, therefore, its capital and operational expenditures.

R7 High availability

In both cases, the OpenFlow controller pushes flow entries that replicate certain unicast traffic along predetermined multiple paths towards the destination. The first mode means an increase in the availability compared to a common PRP deployment based on, for example, Rapid Spanning Tree Protocol (RSTP), whereas the latter is not as robust as the first one since nodes are not doubled attached, but it involves an improvement over a traditional layer 2 LAN with non-PRP compliant nodes.

Furthermore, disasters and large-scale events may cause multiple points of failure, of which is difficult to determine complete knowledge in situations where the redundancy control protocol is delegated to the end nodes, such as defined by IEC 62439-3. Although, as previously described, PRP allows to control the network integrity and to detect errors, the provided mechanisms only are measured in a counter, which is typically accessible via the SNMP. This methodology may be complemented with the global view provided by an SDN controller, which can greatly improve the response performance in such extreme circumstances. This involves the integration of disaster management systems with the control plane, identifying non-affected routes and where the resource management system must take into account not only the availability of resources and policy, but also the QoS requirements of the application. This approach is clearly reflected in [138], where different disaster metrics are detected, evaluated and corrected by an OpenFlow controller.

3.4.2.2 Awareness of DAN/SAN and network status

In spite of the fact that, by default, multicast PRP supervision frames flood the LANs and reach all devices, they are only interpreted by PRP nodes. Although "a RedBox should be configured to stop the transfer of the supervision frames to the SAN devices, so there is no supervision frame flooding to the SANs" [139], this is not required for switches to which the SAN nodes are directly connected. Consequently, in addition to needlessly overloading the network, this traffic is received by them. For the purpose of reducing such traffic, a supervision frames filtering method that uses the device manager and ACL modules is proposed. Thus, periodically, the control plane obtains information about connected devices (attachment points and MAC/IP addresses), being aware of nodes that are SAN or DAN. Accordingly, the above-mentioned multicast frames are filtered at egress ports/switches. Therefore, it is ensured that the supervision flows, which are determined by the Ethertype (0x88FB) and a unique set of multicast addresses[9], only reaches devices with two interfaces; minimizing the amount of global traffic.

R10
Efficiency improvement of PRP

Other advantages are related to responsiveness and resources monitoring capabilities (Section 3.2.1), since they make use of flow statistics to adapt the network to the instantaneous needs, including the following actions:

- Enabling and disabling redundant paths according to the resource utilization; specifically, when a threshold is exceeded.
- Supervision frame rate checking, which is possible because the monitoring module retrieves counters about multicast frames and it checks that they are in line with the expected rates.

[9] The IEC 61850-8-1 and IEC 61850-9-2 specifications recommend specific MAC address ranges for multicast SV and GOOSE services: 01-0C-CD-04-00-00 ↔ 01-0C-CD-04-01-FF and 01-0C-CD-01-00-00 ↔ 01-0C-CD-01-01-FF, respectively.

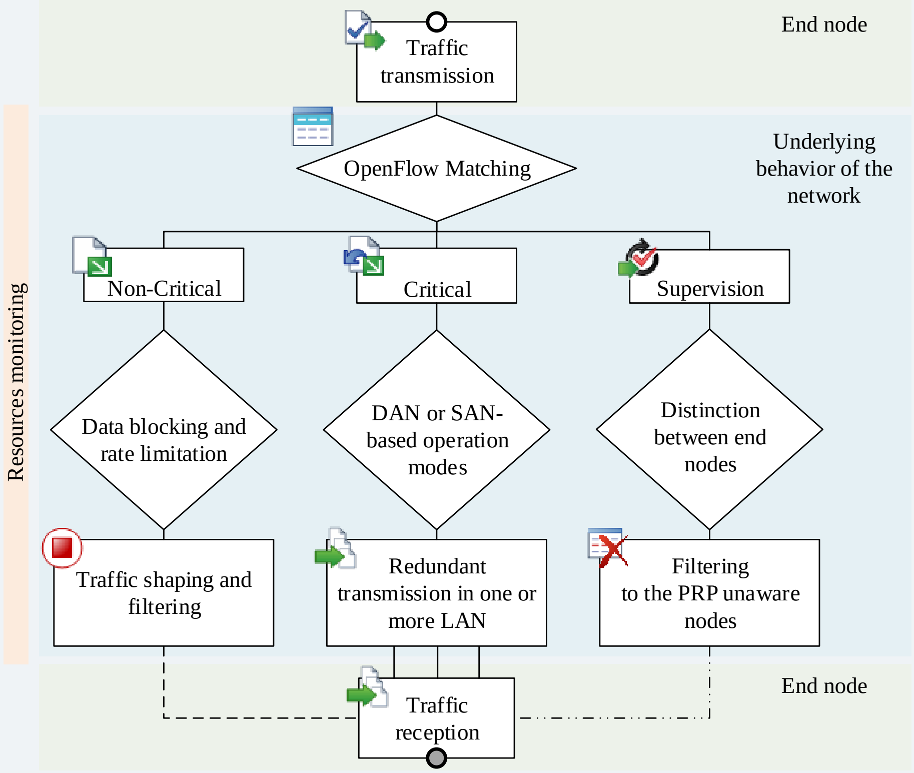

End node
Traffic transmission
OpenFlow Matching
Underlying behavior of the network
Resources monitoring
Non-Critical
Critical
Supervision
Data blocking and rate limitation
DAN or SAN-based operation modes
Distinction between end nodes
Traffic shaping and filtering
Redundant transmission in one or more LAN
Filtering to the PRP unaware nodes
End node
Traffic reception

Figure 3.12: Process flow for identifying and forwarding data traffic.

3.4.2.3 Critical traffic awareness

Contrary to what happens in traditional networks, the network control plane may be aware of the needs of PRP nodes. Therefore, unlike for non-critical traffic, parallel routes between sender and receiver nodes can be established for those frames that require very high availability. This is in accordance with the suggested in [114]: "while critical messages are sent in both directions, it is sufficient for non-critical messages to be sent in one direction only". This can be performed in two different modes:

- Data blocking: it prevents the non-critical traffic propagation in one of the LANs, which is performed by using the ACL module.

R10
Efficiency improvement of PRP

- Data rate limitation: as mentioned before, using the QoS module allows network designers to distinguish flow types by establishing traffic shaping policies in a centralized way.

Figure 3.12 illustrates the process flow for identifying and forwarding data traffic.

3.4.2.4 Traffic filtering policies in PRP nodes

In addition to the foregoing, it has also been studied how including an OpenFlow pipeline in PRP nodes allows them to distinguish data flows. Match fields that form forwarding rules enable the differentiation of flows requiring active protection from those which do not. Accordingly, traffic control in the end nodes is based on priority policies, that is, critical services will be protected with the PRP frame format; while services that tolerate communication disruptions will be transmitted without PRP encapsulation through one of the available interfaces. As a result, a node can distinguish between critical and non-critical flows, protecting them according to their needs. For example, some entries configured on a node PRP could include:

```
{"prp+of device": {
  "id": "prp_switch",
  "entries": [
   {"dl_type":"0x88B8","actions":"output:lre_prp"},
   {"in_port":"prp1-eth0","dl_type":"0x88B8","actions":"output:lre_prp"},
   {"in_port":"prp1-eth1","dl_type":"0x88B8","actions":"output:lre_prp"},
   {"dl_type":"0x0800","nw_dst":"192.168.60.2",
    "nw_proto":"17","tp_dst":161","actions":"output:prp1-eth0"}]}}
```

Specifically, the first rule determines that the incoming traffic with Ethertype *0x88B8*, corresponding to GOOSE frames, will be forwarded to the inner port *lre_prp*, which will append an RCT trailer to the frames and send them to the physical interfaces *prp1-eth0* and *prp1-eth1* (the following two rules set up the reverse path). On the other hand, the last rule determines that the UDP traffic, with IP destination address *192.168.60.2* and destination port *161*, will be directly forwarded by the *prp1-eth0* port.

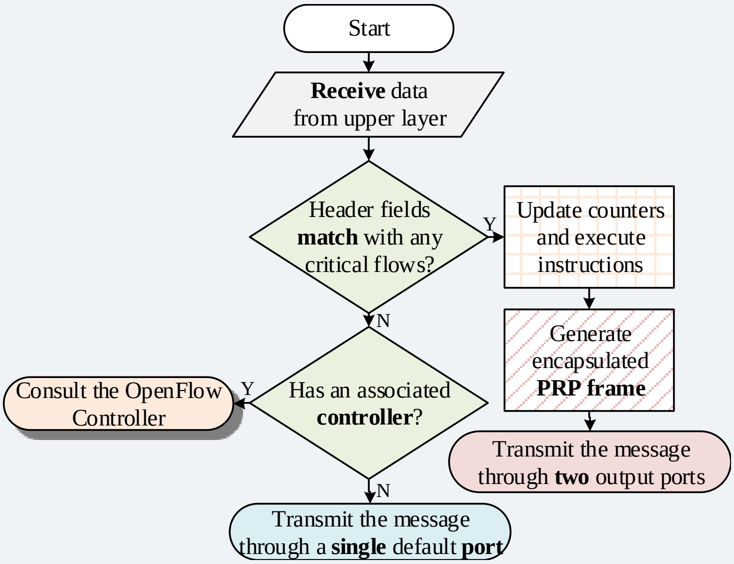

Start
Receive data from upper layer
Header fields match with any critical flows?
Y
Update counters and execute instructions
Generate encapsulated PRP frame
Transmit the message through two output ports
N
Has an associated controller?
Y
Consult the OpenFlow Controller
N
Transmit the message through a single default port

Figure 3.13: Traffic processing by combining PRP and OpenFlow technologies.

Figure 3.13 represents the data-flow processing in PRP nodes to distinguish critical and non-critical traffic. Although these policies are installed by using OpenFlow messages, the end nodes may be beyond the control of the controller.

3.4.2.5 Managing redundant wireless links

After showing how to ensure a high availability while improving the efficiency and effectiveness of PRP networks, the present proposal also aims to support wireless LAN connectivity for industrial environments. In particular, taking into account that PRP provides a high level of failure tolerance, each end node is assumed to be equipped with two interfaces, and connected to one or several IEEE 802.11 APs, and an OpenFlow controller establishes the forwarding rules in the networking devices (Figure 3.14). In this way, first, there is less chance of losing

R10
Robust WLAN connectivity

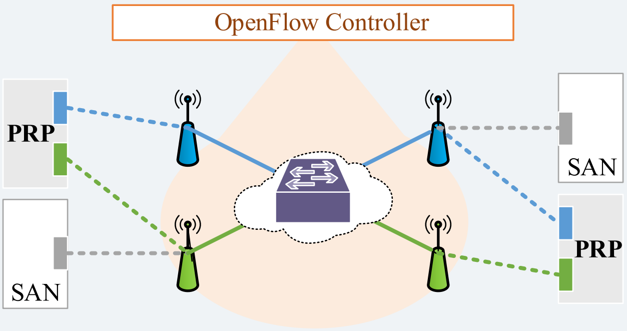


Figure 3.14: Wireless network with PRP nodes under OpenFlow control.

a higher priority packet due to interference or mobility; and second, OpenFlow-capable wireless forwarding devices, for example at the AP level, add fine grained control of the network traffic. In terms of robustness improvement, Section 4.3 will examine the benefits obtained in such a use case.

R12
Robust WLAN connectivy

.

3.4.3 Integration of HSR and OpenFlow

In the proposed solution, which is in line with the previous analysis, HSR networks consist of nodes whose control plane is managed by an OpenFlow controller. In the following, HSR+OF refers to a node that does not only implement HSR functionalities, but also a flow-based traffic processing founded on the OpenFlow data path. Figure 3.15 outlines the structure of an HSR+OF node, along with the main elements of a flow entry in an OpenFlow forwarding table [9]. Specifically, a node exposes its ports to the controller: two physical interfaces and an internal interface, hereinafter referred to as “HSR port”. The HSR port is attached to the external ports through two virtual interfaces and is responsible for handling duplicated frames.

Thus, the node implements two forwarding pipelines:

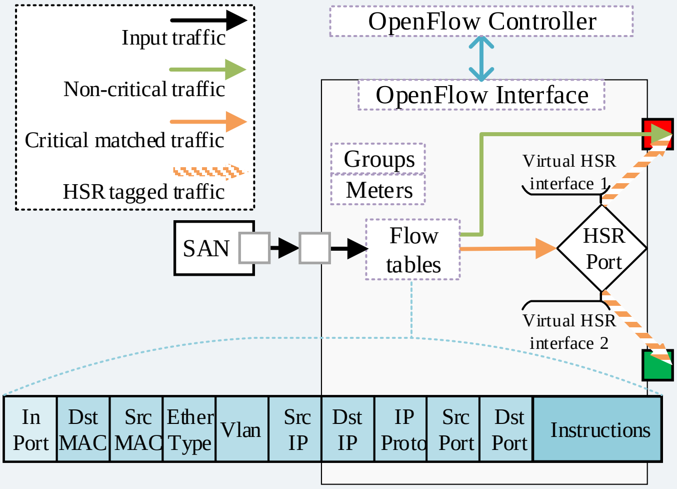


Figure 3.15: Forwarding in HSR+OF nodes.

- The simple pipeline forwards frames unchanged to one of the ring ports, as determined by the controller.

- The HSR pipeline protect higher priority flows by tagging and redundant forwarding. For example, matching the destination MAC address and the Ethertype could distinguish non-critical and critical GOOSE frames.

The configuration of an HSR+OF node may include, for example, the following configuration:

```
{"hsr+of device": {
  "ports": [
   {"s1-eth1": "Ring port 1"},
   {"s1-eth2": "Ring port 2"},
   {"s1-eth3": "Interlink to SAN"}
   {"veth1_1": "Virtual HSR interface 1"}
   {"veth1_2": "Virtual HSR interface 2"}
   {"hsr1": "HSR interface attached to veth1_1 and veth1_2"}
  ]}}
```

In this example, some flow entries may be the following:

```
{"Openflow flow table": {
  "entries": [
   {"in_port":"s1-eth1" , "dl_type":"0x892F",
    "actions":"output:veth1_1"}
   {"in_port":"s1-eth2" , "dl_type":"0x892F",
    "actions":"output:veth1_2"}
   {"in_port":"veth1_1" , "actions":"output:s1-eth1"}
   {"in_port":"veth1_2" , "actions":"output:s1-eth2"}
   {"in_port":"s1-eth3" , "dl_type":"0x88B8",
    "actions":"output:hsr1"}
   {"in_port":"s1-eth3" , "dl_type":"0x0800",
    "nw_dst":"192.168.40.11", "nw_proto":"17",
    "tcp_dst":102", "actions":"output:s1-eth1"}]}}
```

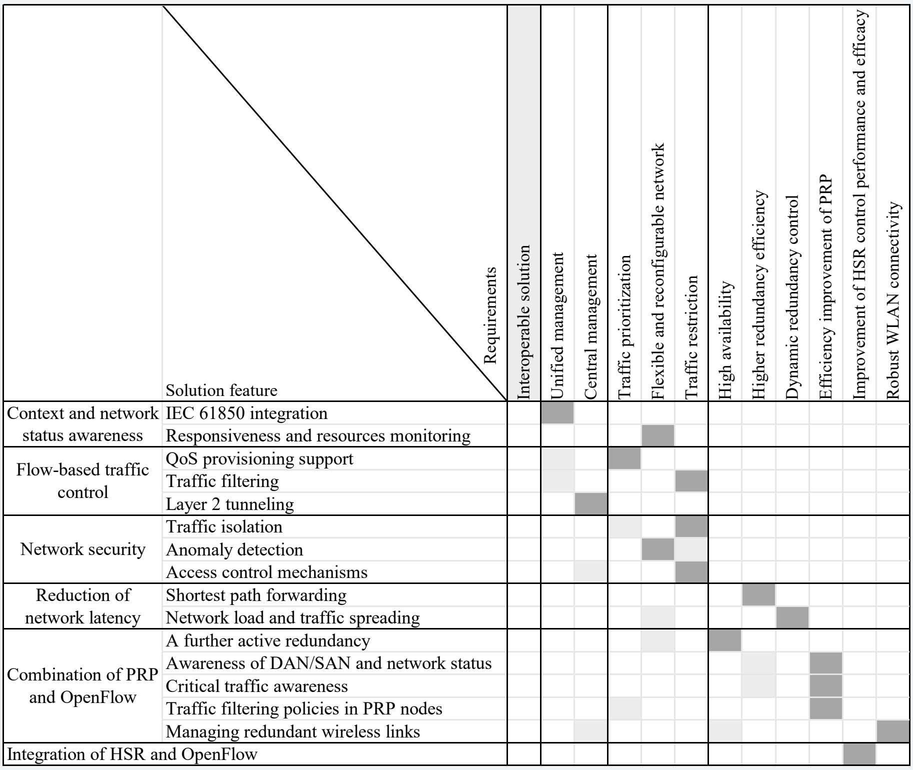
The first four entries allow the node to forward incoming HSR-tagged packets (Ethertype 0x892F) to the HSR pipeline (*veth* interfaces), and reversely pass from the HSR pipeline to the physical ring. The last two entries illustrate how to differentiate flows received from the SAN (*s1-eth3* interface). It should be noted that flow entries for latency-critical applications must be proactively installed, without introducing additional delays by a switch-controller interaction; and, besides, both pipelines are compatible with multicast and VLAN filtering or QoS reservation schemes.

With this scheme, the controller is able to decide whether forward data redundantly or not, changing the HSR forwarding rules in order to consider QoS priorities. A similar feature has been found in [140], which describes a policy framework for incoming frames; this policy may be drop, forward to certain ports, and forward without HSR tags. However, this so-called “Inbound Policy Operation” only checks source and destination MAC addresses, and the policy configurations are not tied to the whole node but to each port individually, with a maximum of 16 inbound configurations per port. Moreover, it is a proprietary solution, whereas with the presented method a node can be configured by an interoperable protocol like OpenFlow.

R11
Improvement of HSR control performance and efficacy

3.5 Summary

This chapter has described an SDN architecture that addresses the needs raised by new IEC 61850-based scenarios. By separating control and data planes, networking devices do not determine their own routing path, but CMM elements do it based on a centralized view of the current network state. The matrix shown in Figure 3.16 summarizes how the different functionalities are seen to respond to the targeted requirements, where the most relevant one is marked in dark gray.



	Requirements Solution feature	Interoperable solution	Unified management	Central management	Traffic prioritization	Flexible and reconfigurable network	Traffic restriction	High availability	Higher redundancy efficiency	Dynamic redundancy control	Efficiency improvement of PRP	Improvement of HSR control performance and efficacy	Robust WLAN connectivity
Context and network status awareness	IEC 61850 integration		■										
	Responsiveness and resources monitoring					■							
Flow-based traffic control	QoS provisioning support		▨		■								
	Traffic filtering		▨				■						
	Layer 2 tunneling			■									
Network security	Traffic isolation				▨		■						
	Anomaly detection					■	▨						
	Access control mechanisms			▨			■						
Reduction of network latency	Shortest path forwarding								■				
	Network load and traffic spreading					▨				■			
Combination of PRP and OpenFlow	A further active redundancy					▨		■					
	Awareness of DAN/SAN and network status								▨		■		
	Critical traffic awareness								▨		■		
	Traffic filtering policies in PRP nodes				▨						■		
	Managing redundant wireless links			▨				▨					■
Integration of HSR and OpenFlow												■	

Figure 3.16: Solution features/Requirements trace matrix.

In summary, the proposed approach provides features that are also present in traditional LANs, such as, for instance, VLAN and prioritization mechanisms, means of remote connectivity and security functions. In addition, this SDN architecture also offers other benefits including improved physical resource utilization, availability, etcetera. As a representative example, this preserves the benefits of PRP and HSR technologies, while making them more flexible and scalable, thereby reducing the need to over-provision links.

All life is an experiment. The more experiments you make the better

Ralph Waldo Emerson

4

Validation and discussion

Contents

This chapter details different validation activities conducted to evaluate and test the main contributions described in Chapter 3. For such purpose, the testbed environment that enables the performance evaluation of SDN/OpenFlow scenarios is detailed, and then the experiments and achieved results are discussed. Different network functions and improvement in network availability have been tested and demonstrated by using both emulation and analytical evaluations, which serve to analyze the appropriateness of the presented proposals. Finally, a summary of the results is given in Section 4.3, which also includes a correlation matrix that furnishes the connection between actual requirements, architectural design and validation criteria.

4.1 Practical implementation and testbed configurations

Firstly, tools used in the evaluation process, along with some GUIs, are presented. After that, test methodologies are described.

4.1.1 Software tools

The technical development is based on several open-source software projects and tools, as indicated below:

- **Mininet** software [141]: experiments have been run on the most widespread tool for emulating SDN-based networks, Mininet, by which it is possible to construct "virtual networks, running real kernel, on a single machine". Mininet allows the emulation of end hosts and software switches by using Linux lightweight virtualization techniques, in which processes run in isolated network namespaces[1]. Moreover, the OpenNet [143] simulation tool adds functionalities of the ns-3 simulator to Mininet. It implements Wi-Fi scan mechanisms to support layer-2 handover between APs working on two different frequency bands. As a result, wireless connections and mobile nodes have been evaluated. In addition, the NetAnim tool is useful to conduct a further analysis as it shows the transmitted frames and the movement of the nodes within the network when OpenNet is used (Figure 4.1).
- **OVS** software switch [144]: it has been used as OpenFlow networking device supporting the sFlow[2] and OVSDB protocols, as well. OVS executes a software application (ovsdb-server[3]) that is responsible for processing the OVSDB configuration protocol messages and configuring the switch accordingly. Regarding the configurable QoS parameters, OVS supports Hierarchy Token Bucket (HBT) and Hierarchical Fair Service Curve (HFSC) Linux classi-

[1] Performance fidelity and limitations of Mininet were studied in [142].

[2] OVS also supports NetFlow and IPFIX protocols, but they are less appropriate for monitoring IEC 61850 traffic, as justified in Section 2.2.7.

[3] For example, the ovsdb-client software can be used to interact with a running ovsdb-server process.

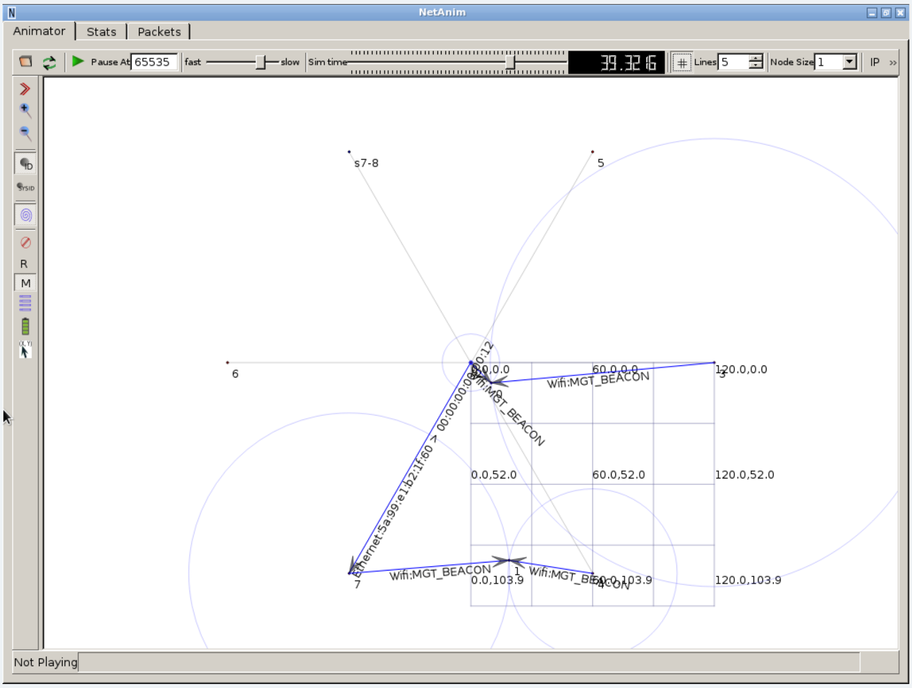


Figure 4.1: NetAnim visualization tool.

fiers. Both types allow the definition and configuration, for each queue and port, of the maximum rate shared by all queued traffic and the minimum guaranteed bandwidth. Other features supported by OVS such as, for example, LACP, have not been used.

- **sFlow-RT** collector: regarding the deployed resource monitoring method, an sFlow-RT application continuously receives sFlow datagrams from network devices, which have to be configured with the IP address of the collector, a packet sampling rate and an interface polling interval. sFlow-RT can be used to translate the sFlow datagrams into meaningful metrics, accessible through a REST API. Moreover, these metrics can be selectively sent to a visualization software, system such as Graphite, through which time-series data can be stored and displayed on a dashboard interface.

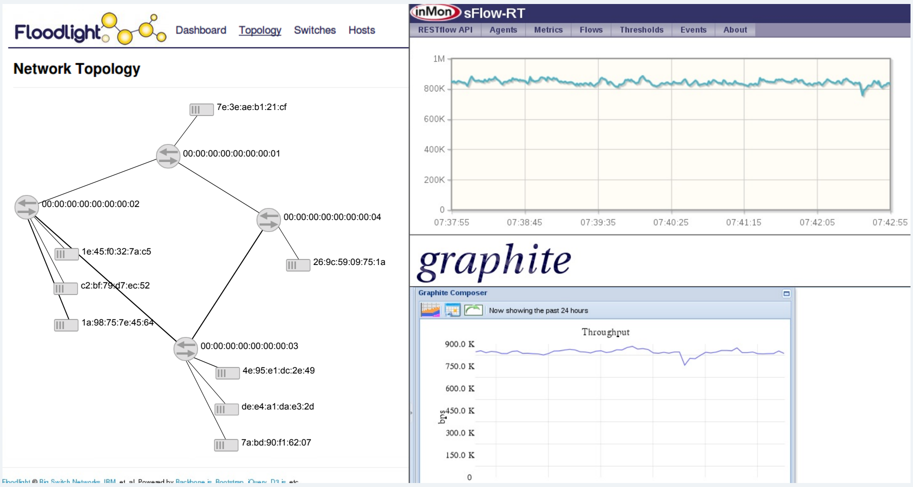


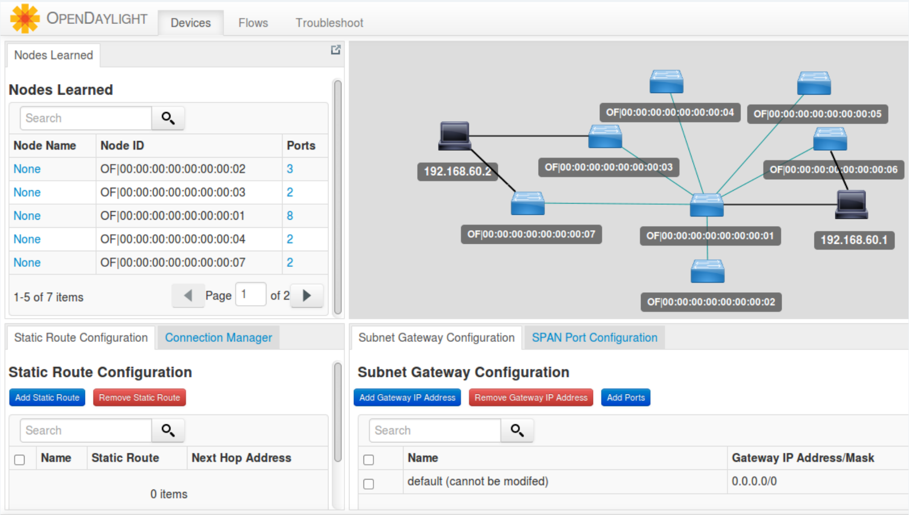
Figure 4.2: Screenshot of Floodlight, sFlow-RT and Graphite GUIs.

➤ As detailed below, two OpenFlow controllers, namely the **Floodlight** and **OpenDaylight** software projects, have been used in order to test different functionalities. They provide a fully functional control plane responsible for different tasks, such as the discovery and management of topologies and devices, route calculation and loop prevention. Besides, other notable modules used are as follows:

- The QoS Floodlight module published in [145] is used to determine rate limits associated with the OpenFlow match fields. It also offers a type-of-service scheme based on the definition of different priorities.

- The **MultipathODL** fork [146] enables link-layer multipath switching, which is specifically used to determine redundant paths for mission critical applications. It calculates multiple link disjoint paths per flow that are exposed as a path-finder service. Moreover, MultipathODL includes multipathing reactive flow handling that pushes, with each new flow, the forwarding rules to all switches on the paths. In addition, it provides different path calculators and selectors that may be linked to the dynamic network status, for example: "shortest path, random path, round robin path, maximum available bandwidth path, path with fewest flows or path with the highest capacity". These selectors can be chosen via a REST API.

Figure 4.2 includes screenshots of the Floodlight, sFlow-RT and Graphite GUIs used for displaying the network performance, and Figure 4.3 shows the OpenDaylight management application, which displays the network topology, information about the discovered devices and the installed flow rules.


OPENDAYLIGHT
Devices
Flows
Troubleshoot
Nodes Learned
Static Route Configuration
Connection Manager
Subnet Gateway Configuration
SPAN Port Configuration
Add Static Route
Remove Static Route
Add Gateway IP Address
Remove Gateway IP Address
Add Ports
Search
OF|00:00:00:00:00:00:00:04
OF|00:00:00:00:00:00:00:05
192.168.60.2
OF|00:00:00:00:00:00:00:03
OF|00:00:00:00:00:00:00:06
OF|00:00:00:00:00:00:00:07
OF|00:00:00:00:00:00:00:01
192.168.60.1
OF|00:00:00:00:00:00:00:02

Nodes Learned

Node Name	Node ID	Ports
None	OF|00:00:00:00:00:00:00:02	3
None	OF|00:00:00:00:00:00:00:03	2
None	OF|00:00:00:00:00:00:00:01	8
None	OF|00:00:00:00:00:00:00:04	2
None	OF|00:00:00:00:00:00:00:07	2

1-5 of 7 items Page 1 of 2

Static Route Configuration

☐	Name	Static Route	Next Hop Address

0 items

Subnet Gateway Configuration

☐	Name	Gateway IP Address/Mask
☐	default (cannot be modifed)	0.0.0.0/0

Figure 4.3: OpenDaylight GUI.

Moreover, a software implementation of PRP and HSR redundancy mechanisms is used:

- End nodes use the **PRP stack** published in [147], which runs on the Linux user space. Hence, each emulated host over Mininet can have two network interfaces virtualized in a single PRP interface, and therefore, it is able to detect and discard duplicated frames, as well as send PRP supervision messages every two seconds.

- The **HSR stack** and the generation of supervision multicast messages are supported in Linux kernel from version 3.13. An HSR+OF node overcomes several limitations of the current HSR module; for example, Quadbox's proxy capabilities and stacked HSR headers on top of VLAN are not yet supported. However, these features are provided HSR+OF nodes by delegating them to the OVS.

In summary, this whole architecture allows the emulation of switches supporting PRP and HSR protocols, and to assess different network topologies and traffic scenarios. The fact that all these studies have been conducted by emulating network topologies and using virtual devices rather than physical machines or networks could be considered as a limitation. For example, regarding the performance of PRP and HSR nodes, it could be improved from a hardware perspective, since hardware implementation is desirable to obtain a lower per-hop latency. Despite this, the hardware implementation is out of the scope of this work. In any case, for example, the average delay introduced by HSR pipeline over the simple pipeline has been obtained with a ping test between two end nodes connected through two switches, increasing the average round-trip time by 0.056 ms.

4.1.2 Emulation Conditions

Figure 4.4 shows a networking domain example that includes different network namespaces and virtual Ethernet pairs. Although OVS supports in-band control-plane configurations, the results presented here correspond to out-of-band configurations in which Mininet uses OVS to create a set of Ethernet switches that interact with an OpenFlow controller running on another machine, through independent network resources. Thus, OpenFlow traffic does not affect data plane operation and failures that affect control traffic are excluded from the analysis. As explained in Section 2.5.1, the implications of in-band schemes, where data and control planes share the same resources, have been studied by other authors. For example, in [148] the authors implement restoration and protection mechanisms in in-band OpenFlow networks and show recovery times for data and control traffic. Regarding controller redundancy, OVS allows interacting multiple controllers simultaneously, enabling backup schemes where bridges communicate preferentially with a master controller, otherwise with slave ones. Moreover, according to the OpenFlow and as detailed in Section 2.5.2, OpenFlow switches can be configured to change to "standalone mode" if the switch-controller connection fails, during which the switch behaves as a legacy one (without external controllers), or remain in "fail secure mode", in which switches drop the packets destined to controllers until they successfully connects to a controller.

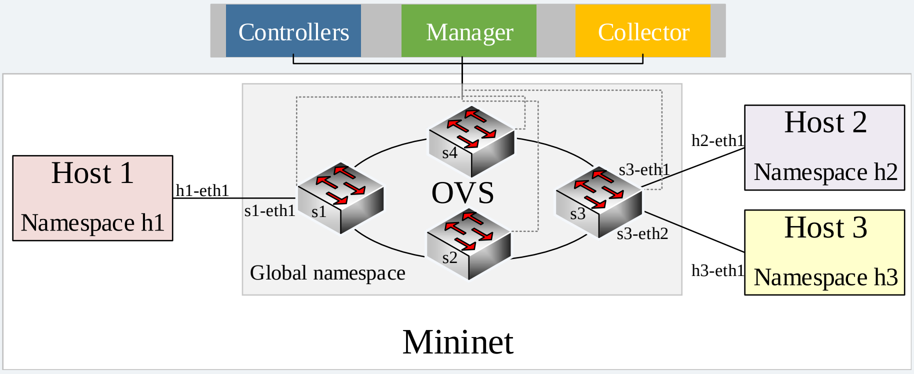


Figure 4.4: Testbed internal elements.

With regard to the emulation parameters, Linux Traffic Control and NetEm tools [149] serve to emulate various capabilities of links and set different network conditions, such as:

- To configure parameters of links and packet queues on interfaces, being possible to fix bandwidth constraints, which serves to characterize saturations. By contrast, despite being possible in NetEm, additional synthetic delays were not included.

- To characterize path performance degradation as NetEm allows the variable packet loss rate emulation. The smallest possible nonzero value causes 1 out of 43103448 packets to be randomly dropped [149]. In addition, Mininet was modified to enable decimal values of rate inputs.

Regarding traffic flows, different tools, such as ping, iperf or Netperf, have been used for generating ICMP, TCP and UDP flows. The latter type of traffic serves to obtain the recovery connection time; since, as defined in the RFC 6201 [150], test tools that offer monitoring the number of lost frames allow to know the recovery time of a system, calculated by the following expression:

$$R = \frac{\text{Lost frames}}{\text{Offered rate}} \tag{4.1}$$

As a result, sending a continuous packet stream would allow one to determine the packet loss rate when network elements fail, which enables the comparison of the recovery time and packet loss rate obtained with different technologies and conditions.

Additionally, to build scenarios where the hosts send and receive SV and GOOSE frames, the rapid61850 open-source project has been used. This project, published in [151], processes an SCD file to generate the data model and communications code required for an IED. This code implements the communications stack that allows IEDs to send predefined messages (with the indicated VLANs, Multicast addresses, etcetera), and they are able to encode and decode GOOSE and SV packets. In other words, the rapid61850 tool parses an SCD file and performs SCL schema validation, and then it generates C source code that models each IED existing in the SCD file, which, once complied, are included them in the emulation process.

Therefore, the emulation process allows to check the proper operation of a network design and validate the traffic engineering methods. In fact, it is possible to emulate the SV and GOOSE data communications of a substation without using any real IEDs, and test the proper operation of a network design and validating different traffic engineering methods. Moreover, since Mininet provides a Python API with which any topology can be defined, different scenarios are selected in accordance with the specific features and metrics being tested. Although there are approaches for modeling and simulating IEC 61850 networks and Smart Grid communications, as explored in [152], there are no industrial network simulators that integrate OpenFlow switches and inter-IED communication. Otherwise, the AMICI tool [153] combines network emulation with real-time software simulators. Indeed, the used emulation platform raises the possibility to integrate simulation tools to recreate physical processes such as the system described in the previously mentioned framework [153], which was proposed to analyze the security and reliability of interdependent infrastructures, such as the power grid and ICT.

4.2 Functional and experimental analysis

In this section, several emulation case studies and results serve to evaluate and validate the capabilities of the proposals.

4.2.1 Functional evaluation based on use cases

The proposed architecture heavily relies on flow-based traffic control functions (e.g., filtering). Representative examples of handling data flows in IEC 61850-based substation communication systems are shown below, which, making use of the Graphite software for real-time recording and graphing data, illustrate some of the advantages provided by the platform. The results are performed on a ring network, where the nodes are attached by edge links (100 Mbit/s) and switches are connected among themselves with trunk links (1 Gbit/s). This simple topology, extracted from [23], is widely used in real substations and, as described in this technical report, it may correspond to an architecture deployed in a 500/220/33 kV substation. Figure 4.5 shows how the following use cases represent different data flows that are transmitted on the same physical resources.

- **QoS provisioning support**: Figure 4.6 shows the throughput of multiple traffic streams in scenarios where the following rate thresholds are established:

    - TCP flow: 20 Mbit/s.
    - UDP flow: 2 Mbit/s.
    - SV flow: 4.5 Mbit/s.

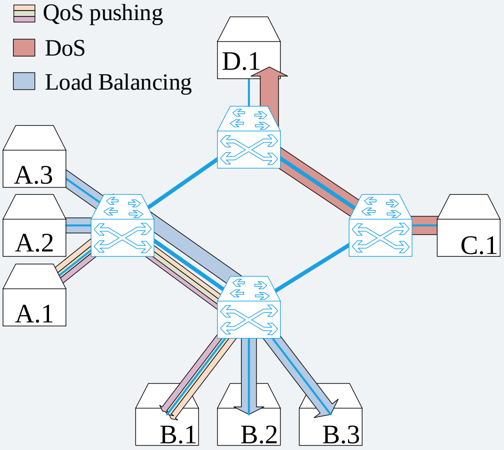


Figure 4.5: Testing network topology used in validation.

As verified, there are no QoS policies during the first 25 seconds; afterwards, the following egress rate limits are set during the next 20 seconds, from 09:02:50 until 09:03:10 (flows recover their previous rate when the traffic shaping is disabled).

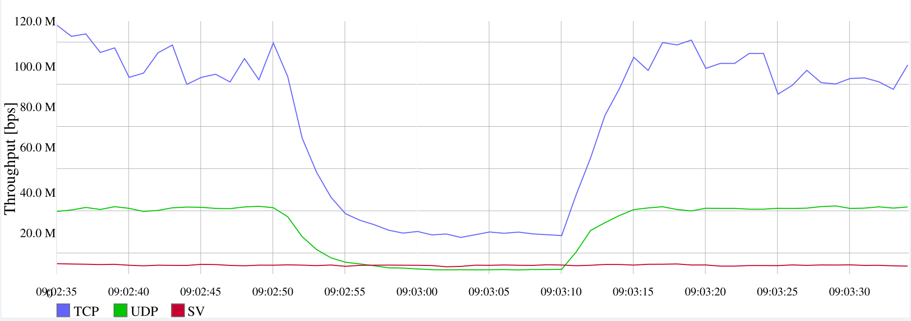


Figure 4.6: QoS effect for TCP, UDP and SV flows.

- **DoS attack detection and mitigation**: Figure 4.7 exemplifies a situation in which DoS attacks can be detected in near real-time. Through a simple ping flood attack, where a node is overwhelmed with ICMP Echo Request packets, it can be seen a first phase during which DoS control is disabled and a second phase with DoS control enabled; that is, the controller is configured to drop packets from an attacker. Then, the countermeasure is deactivated after a predetermined time period. Specifically, a threshold of 100 IP packets per second is set.

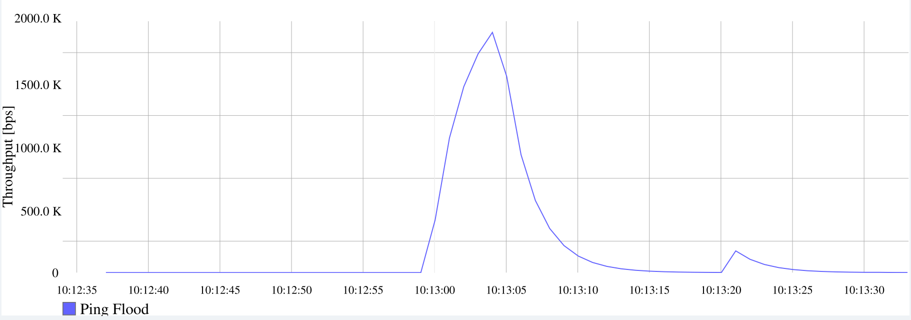


Figure 4.7: Detection of exceeded thresholds.

- **Load balancer pool**: the SDN controller holds a list of IP addresses and TCP/UDP ports of hosts configured as servers to which the incoming flows are distributed. In particular, Figure 4.8 shows the TCP throughput from two nodes to two different IP addresses (IP.1 and IP.2) even though, in principle, the application (iperf) had generated traffic to one and the same IP address (IP.100).

4.2.2 Path diversity control and latency reduction

The latency reduction is an important goal in the proposed solution, and is analyzed in the following validation test, where it is compared the effect of traffic interactions when frames are dynamically balanced. A two-tier network topology, widely adopted in real critical infrastructures, is used in the following tests, where end hosts and switches are connected through 100 Mbit/s full-duplex interfaces. Figure 4.9 shows two screenshots of the OpenDayLight web interface: the entire setup is given in Figure 4.9a, whereas Figure 4.9b displays the same topology,

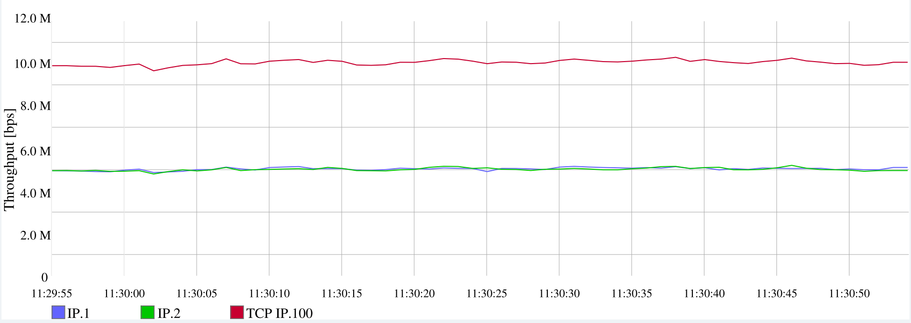


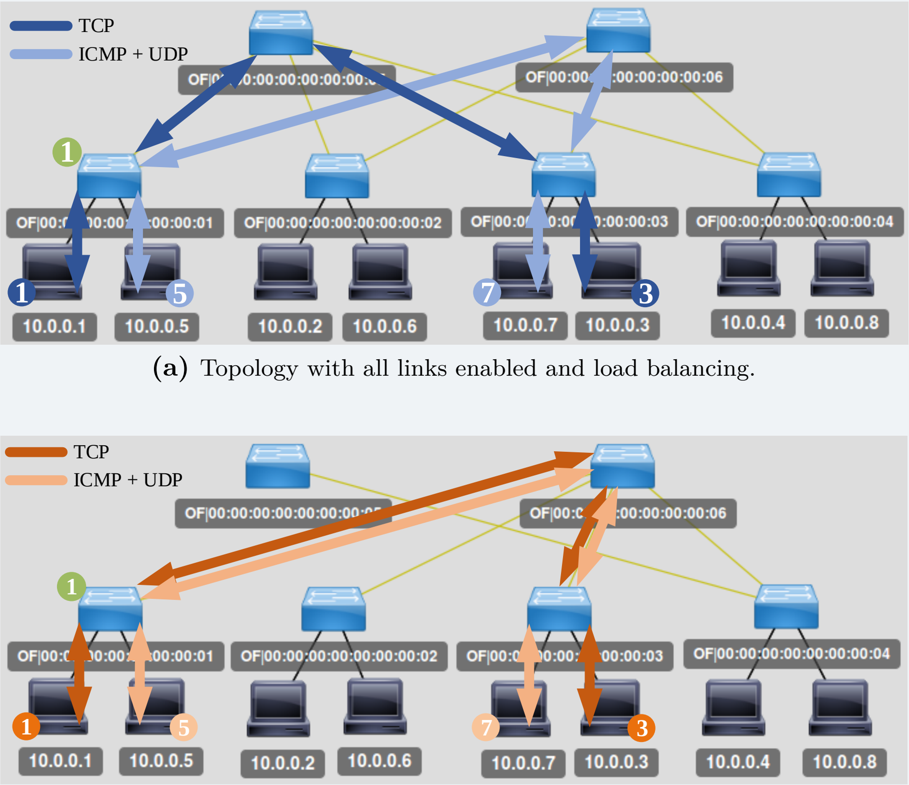
Figure 4.8: Load balancing effect over TCP traffic.

but where the switches run single-rooted RSTP, proving the reduction in the number of available links.

Traffic spreading among redundant paths allows to evaluate the impact in the network latency when different data flows are being transmitted at the same time. Specifically, ICMP, UDP and TCP streams are generated and may represent the interaction between critical real-time data and non-critical background ones. In this experiment, two incoming ports in switch ‘1’ (in green) receive the following traffic:

- UDP requests/responses and ICMP echo requests, respectively generated through Netperf and ping tools, are used to measure the round-trip latency. This final value is computed as the average of both services.
- A TCP connection injected with the iperf tool at different data rates. The data rates are limited by the output link capacities in the sender, and the edge switch has also installed an ingress policing rule to limit the maximum rate.

Nodes ‘1’ (in blue) and ‘5’ (in light blue) communicate with ‘3’ (in blue) and ‘7’ (in light blue), respectively, as depicted in Figure 4.9. The size of all packets transmitted by ‘1’ are fixed to 126 bytes, which is in compliance with the 61850-9 SV-LE specification; while frames sent by are fixed to 300 bytes, a typical value for MMS services [23]. Load balancing is based on destination MAC addresses so that, since ICMP messages



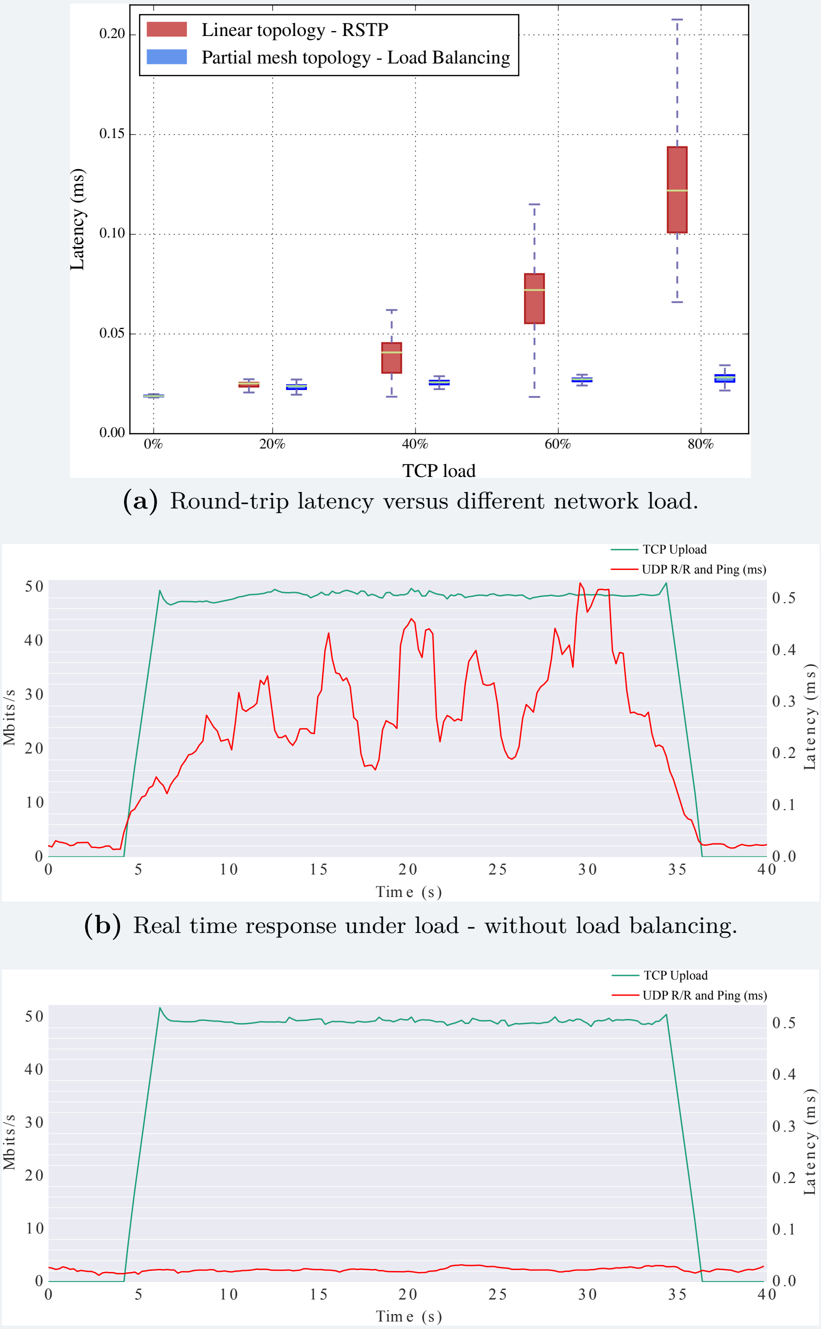
(a) Topology with all links enabled and load balancing.

(b) RSTP configuration where distribution switch 6 is root.

Figure 4.9: Two-tier network topology discovered by the OpenDayLight controller and flow paths..

and UDP datagrams provide no protection from duplication and no guarantees for delivery, traffic behavior is comparable to SV/GOOSE frames.

Figure 4.10a shows box plots including minimum, first quartile, median, third quartile and maximum value correspond to 30 samples from which information is collected for 10 seconds. These figures summarize the distributions of the round-trip latency for different data rates of TCP background connections (0, 20, 40, 60 and 80 Mbit/s). These statistics have been performed in 30 trials, each 10 seconds long. As a result, it



(a) Round-trip latency versus different network load.

(b) Real time response under load - without load balancing.

(c) Real time response under load - with load balancing.

Figure 4.10: Latency comparison with and without load balancing.

can be said that ‘1’-to-‘3’ transmission results in significant lower latency when traffic is balanced compared to the non-balanced case.

Moreover, Figure 4.10b and Figure 4.10c show two experiments where ‘5’ establishes a TCP connection that tries to consume all the bandwidth, limited in this case to 60 Mbit/s. These graphs compare the TCP goodput versus the *ping* and UDP request/response performance with and without load balancing.

As a summary, detailed experiments outline that latency grows quickly as TCP connection is set up for a linear topology, whereas latency is slightly affected in the balanced case. This load balancing can be configured statically (i.e., assigning links to critical and non-critical flows) or dynamically based on parameters such as the bandwidth available on the path.

4.2.3 Robustness analysis

Although jitter and packet loss can be reduced by queueing and prioritizing time-sensitive data streams, the loss of one or several time-critical messages can have impact on protection functions, as studied in [154]. Thus, inappropriate configurations, network congestion or high electromagnetic interference could cause packet losses. This section demonstrates the advantages that can be gained by controlling PRP and HSR networks with an SDN agent. Separate use cases are considered to assess the enhancement of robustness and the reduction of traffic in different scenarios.

4.2.3.1 Higher robustness against packet loss

With the aim of ensuring high-availability of mission-critical applications, sending and receiving frames through redundant paths enhance communication robustness. For instance, as mentioned before, PRP ensures that no messages are lost if one of the two established paths fails, avoiding downtime. This does not depend on using OpenFlow, but it corresponds to the overall availability of parallel systems, which is detailed in Section 2.3.

As a representative application of emerging industrial wireless networks, monitoring and control devices can be provided with redundant wireless interfaces to support robust transmissions. In particular, two use cases show how employing parallel connections increases the successful communication probability. The results presented here are obtained using the following topology (sketched in Figure 4.11) and network conditions:

- Using the IEEE 802.11g transmission standard, which operates in the 2.4 GHz band and at 22 Mbit/s average throughput.
- The channel assignment scheme allows two wireless interfaces of PRP nodes to operate on different channels. While it is true that the four non-overlapping channels 1, 5, 9, 13 (with 20 MHz separation between the center frequencies) are often used to prevent interference, the frequency diversity would increase if the nodes worked in different bands, e.g., 2.4 GHz and 5 GHz.
- Wireless nodes are configured to operate in an infrastructure mode served by several APs, which are star-wired to a distribution network through 100 Mbit/s full-duplex interfaces.

To show the robustness against interference, the availability of a service is studied when the probability of packet loss is the same, but statistically independent, for each wireless link which a node PRP is connected to. Figure 4.12a plots a comparison of the packet-loss robustness for a SAN and a DAN. Tests have been conducted under different packet loss rates and with UDP traffic; that is, an unreliable transport protocol.

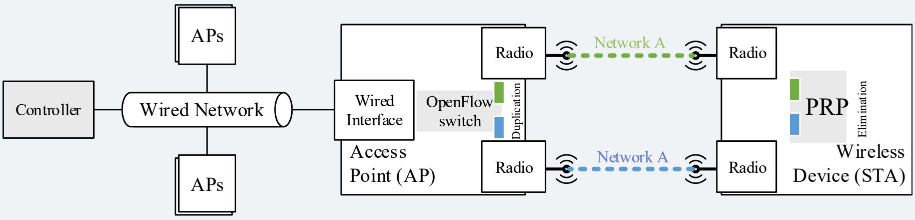


Figure 4.11: Application scenarios for the utilization of PRP in WLAN networks.

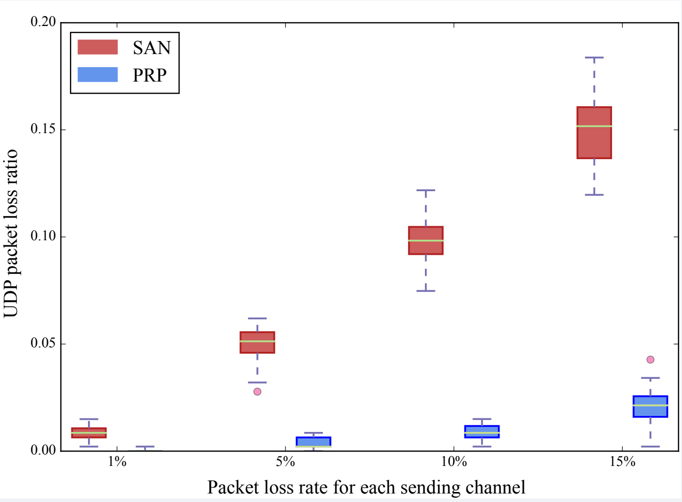
Moreover, in order to highlight the increase in the availability of TCP services (reliable transport protocol), Figure 4.12b shows the throughput of a TCP connection, limited to 1.05 Mbit/s by the sender.

4.2.3.2 Seamless roaming of mobile devices

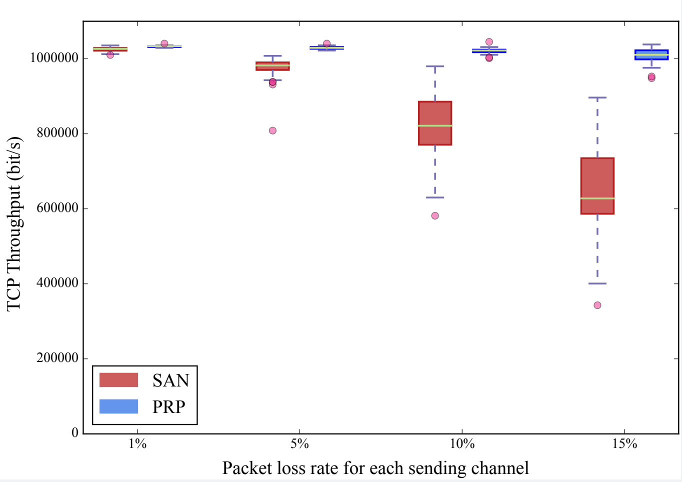
One of the goals proposed by the architecture is to provide mobility support with high reliability. This experiment illustrates the continuity of service during a handover process when simultaneous connections are established to different APs. Since, as discussed in [155], the SDN/OpenFlow technologies can optimize the provision of resources based upon predicting handover occurrences, it is also considered the possibility of proactively transmitting data before a change in the end node/AP connection. Nevertheless, the scanning and connection processes involves, in any case except when using PRP, a communication interruption, as shown in Figure 4.13b. In this case, it is necessary to note that OpenNet does not yet support IEEE 802.11r Fast Roaming standard or prescan mechanisms that select new APs before disconnection of current link to further shorten handover latency [143].

Particularly, Figure 4.13a represents three cases, in which a node receiving UDP traffic moves between two APs operating in different 802.11g channels.

- Node with a single interface (SAN):
    - The controller installs OpenFlow rules in the network elements so they operate as a traditional learning switches. This implies that a longer recovery time is seen, since the controller has to react to the data in a different link with the installation of new rules and changing or deleting the old ones.
    - The controller installs rules in the network elements so that the traffic is redundantly forwarded to the destination node by the APs in order to reduce the interruption period.
- Node with two interfaces (DAN) connected to two APs between which it moves. Thus, the node remains connected at all times, until it is out of range.

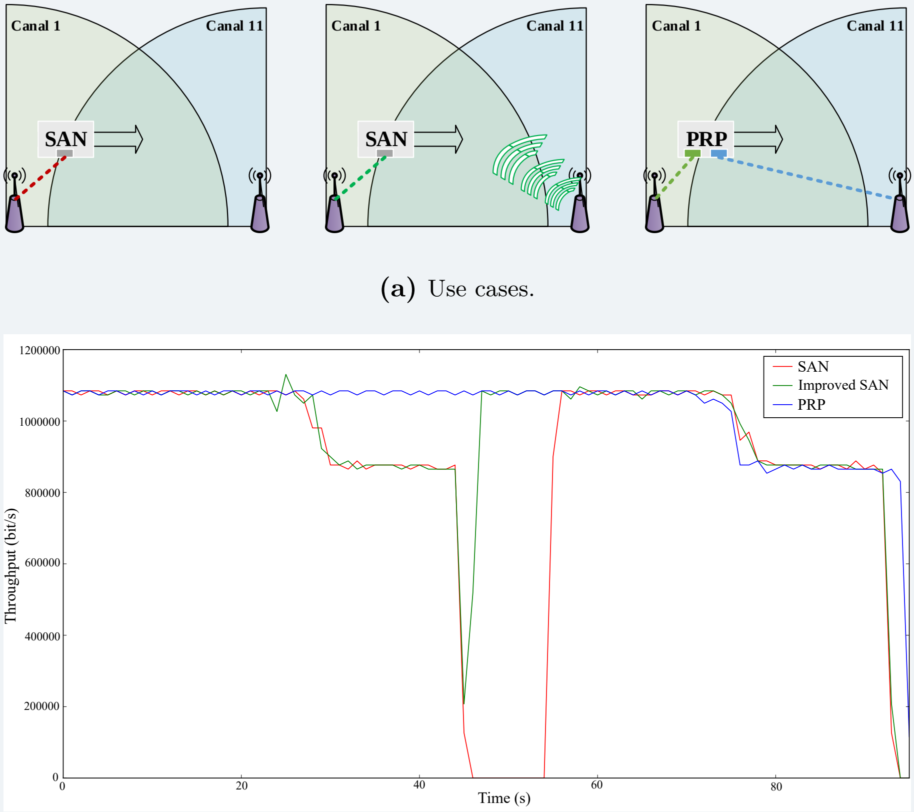


(a) Packet-loss robustness.



(b) TCP Throughput.

Figure 4.12: Influence of lossy wireless links on reliable and unreliable transport protocols.



(a) Use cases.

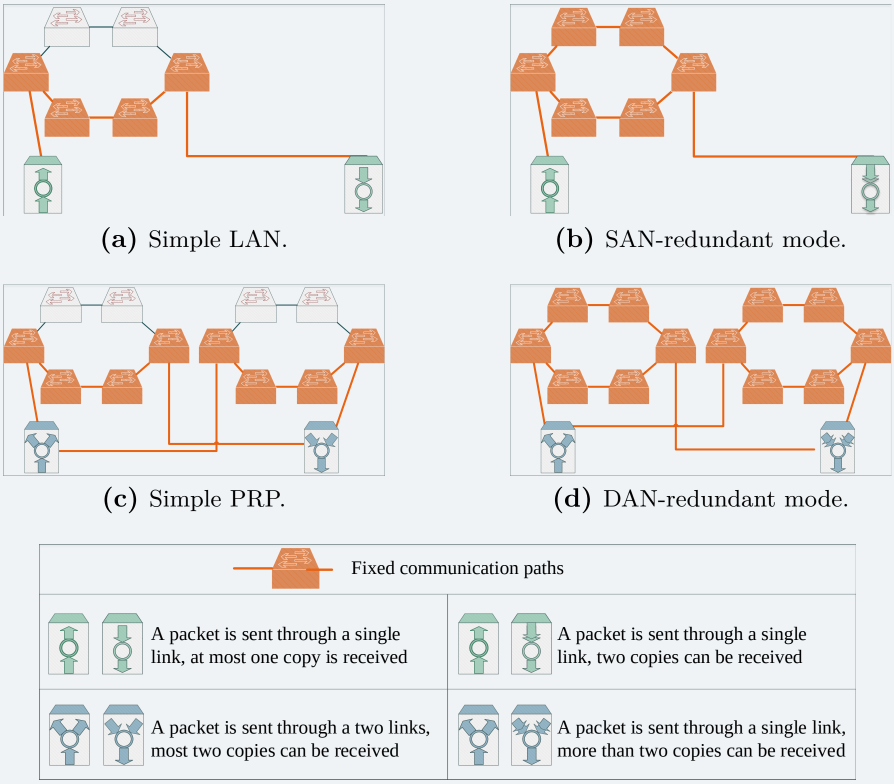
(b) UDP throughput.

Figure 4.13: Node connectivity in an AP roaming scenario.

It is important to emphasize that these three examples also serve to represent that one node supports the simultaneous transmission of PRP encapsulated and non-encapsulated frames, depending on the criticality of the data and network status. This means that, in non-critical flows, there is no longer a need for duplicating frames.

4.2.3.3 High survivability in multiple failure scenarios

In line with the above results, the present approach can significantly improve the availability and responsiveness over other traditional technolo-


Fixed communication paths
A packet is sent through a single link, at most one copy is received
A packet is sent through a single link, two copies can be received
A packet is sent through a two links, most two copies can be received
A packet is sent through a single link, more than two copies can be received

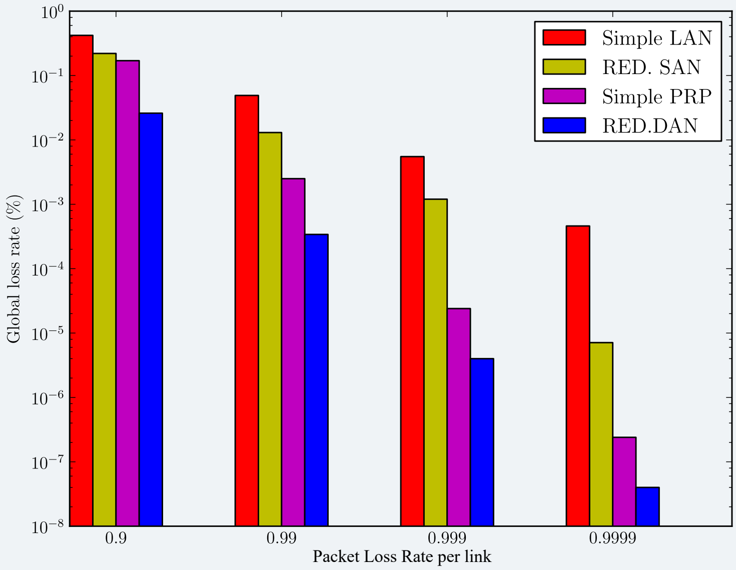
(a) Simple LAN. (b) SAN-redundant mode.

(c) Simple PRP. (d) DAN-redundant mode.

(e) Legend.

Figure 4.14: Test cases.

gies based on a single active path when multiple failures can cause network partitioning. Thus, the following validation experiments demonstrate the robustness provided by establishing multiple active paths in different lossy topologies and scenarios. As a test of concept, two identical and independent networks to which the PRP nodes are connected enable the creation of disjoint paths of equal cost, which reduces the possible number of cases and makes the understanding of them easier. Figure 4.14e describes the different cases to be considered, that is, there are four cases in which the number of possible receptions vary according to the established paths. The other figures in Figure 4.14 show how re-



	Global loss rate (%)			
PLR per link	**Simple LAN**	**RED. LAN**	**Simple PRP**	**RED. DAN**
0.9	4.2×10^{-1}	2.2×10^{-1}	1.7×10^{-1}	4.6×10^{-2}
0.99	4.9×10^{-2}	1.3×10^{-2}	2.5×10^{-3}	3.4×10^{-4}
0.999	5.5×10^{-3}	1.2×10^{-3}	2.4×10^{-5}	4.0×10^{-6}
0.9999	4.6×10^{-4}	7.1×10^{-6}	2.4×10^{-7}	4.0×10^{-8}

Figure 4.15: Comparison of the packet-loss robustness in different topologies.

dundancy is allocated. In all experiments, iperf was configured to send packets at a rate of 50 Mbit/s. A comparative evaluation in terms of recovery time is performed for the following cases:

- Simple LAN where only one path is established, Figure 4.14a.
- SAN-based operation mode, Figure 4.14b.
- Simple and common PRP deployment, Figure 4.14c.
- DAN-based operation mode with multiple redundancy in both LANs, Figure 4.14d.

As an outcome, Figure 4.15 (for the clarity of the figure, note the logarithmic scale of the vertical axis) shows the mean global loss rate, taking into consideration the same packet loss rate (PLR) per link, which can be expressed as follows for a link between two switches sw_1 andsw_2 connected on ports sw_1^1 and sw_2^1 respectively:

$$PLR_{sw_1 \rightarrow sw_2} = 1 - \frac{Packets\ received\ sw_2^1}{Packets\ transmitted\ sw_1^1} \tag{4.2}$$

which is inversely related to their availability, as also considered in [92]. These results show the reduction of global loss rate is achieved by using multiple parallel links. Therefore, this scheme allows the implementation of different robust topologies with extremely low packet losses.

4.2.4 Analysis of traffic reduction in HSR+OF networks

In this part, it is described how HSR+OF networks are tested. Specifically, an analytical model and experimental results show the throughput efficiency improvement of the proposed scheme.

As mentioned before, the available bandwidth of HSR conventional networks is reduced. However, with the HSR+OF approach, non-critical traffic traverses a single path, reducing the amount of data transferred, while only critical traffic is forwarded along two paths towards the destination node. As a result, the utilization of links varies with the type of traffic, critical or non-critical; and the location of senders and destinations. As analyzed in Section 3.3.1, the average shortest path length for a connected graph (G) is

$$a_s = \sum_{s,t \in V} \frac{d(s,t)}{n(n-1)} \tag{4.3}$$

The shortest pair of link-disjoint paths between a given pair of nodes is established for critical traffic. The well-known Suurballe algorithm [64] or the Bhandari's one [156] can be used to find an optimal solution. Algorithm 3 (where k is an integer for the number of paths) presents the pseudo code of the latter technique, which is simpler to implement than the Suurballe algorithm.

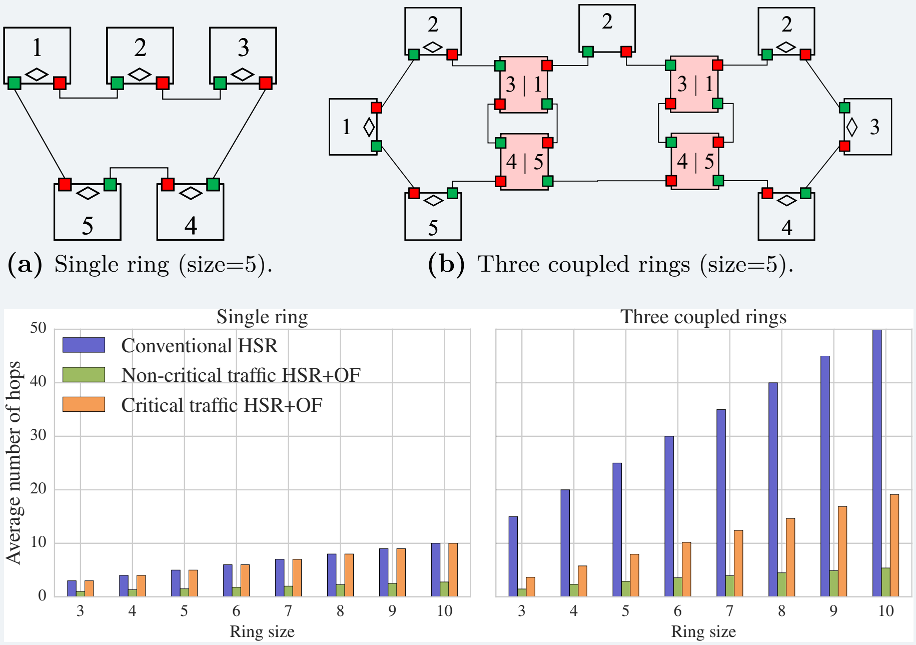
```
[Use a shortest path algorithm (e.g. Bellman-Ford) to find shortest paths
  allowing for negative links weights];
Find the shortest path $P_1$ from node $s$ to node $t$;
for $i = 2, \ldots, k$ do
    replace each link of all $P_x$ where $x < i$ with a reverse link of inverted link
      weight in the original graph;
    find the shortest path $P_i$ from node $s$ to node $t$;
    remove overlapping links to get $i$ disjoint paths $P_x$ where $x \leq i$;
end
```

Algorithm 3: Bhandari algorithm.

Figure 4.16 shows the reduction of the average number of hops per packet delivery with respect to the HSR scheme for single (Figure 4.16a) and coupled rings (a three-ring topology is considered, as shown in Figure 4.16b), where the rings size means the number of nodes in each ring.

The priority-aware scheme makes HSR+OF approach more efficient than the DVP algorithm [76], which, as far as this author knows, has been the most significant method for HSR performance until now. DVP establishes a pair of disjoint paths[4], but regardless of the requirements of the data flows. As a result, critical and non-critical traffic use the same network resources. Hence, the typical ratio of critical traffic to non-critical traffic [23], [24] affects the performance improvement achieved by the HSR+OF approach. Therefore, to quantify the improvement achieved, traffic patterns of IEC 61850-based systems (Section 2.2.4) are considered. Figure 4.17 compares DVP and HSR+OF for a three-ring topology when non-critical traffic patterns are more significant within the limits of the typical values. That is, the most favorable situation, in terms of saving resources, is analyzed. Additionally, it should be kept in mind that other related work [77], less effective than the DVP approach, reduces the HSR traffic at the expense of introducing a setup process,

[4] In this analysis, it has been considered the possibility that DVP could establish a shortest pair of disjoint paths, despite the fact that Nsaif et al. [76] do not describe whether these paths are the shortest ones or not. Moreover, it is necessary to note that the results in [76] are obtained for a specific topology and, unlike the HSR+OF approach, this reference does not include any analysis of single HSR rings, since such proposals do not reduce traffic in these cases.



(a) Single ring (size=5).

(b) Three coupled rings (size=5).

Figure 4.16: Reduction of the average number of hops.

which includes announcement and learning messages. Moreover, these proposals define special frames that are not included in the IEC 62439-3 standard.

4.2.4.1 Protecting critical flows

This validation test[5] aims to demonstrate that the proposed scheme the efficiency in bandwidth consumption. Specifically, it illustrates how the network is able to duplicate real-time critical information, just like the standard procedure, while it transmits non-critical traffic only along the shortest path, without HSR tag. Figure 4.18 shows this distinction when the connection (link ‘1’-‘2’) between ‘Source’ and ‘Destination’

[5] In the topology used here, all the emulated nodes and switches are interconnected by 100 Mbit/s full-duplex interfaces

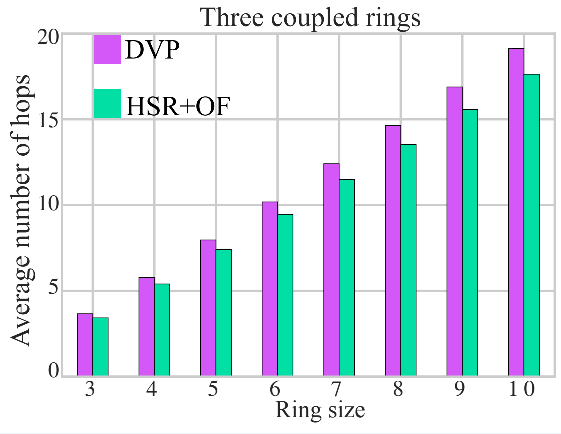
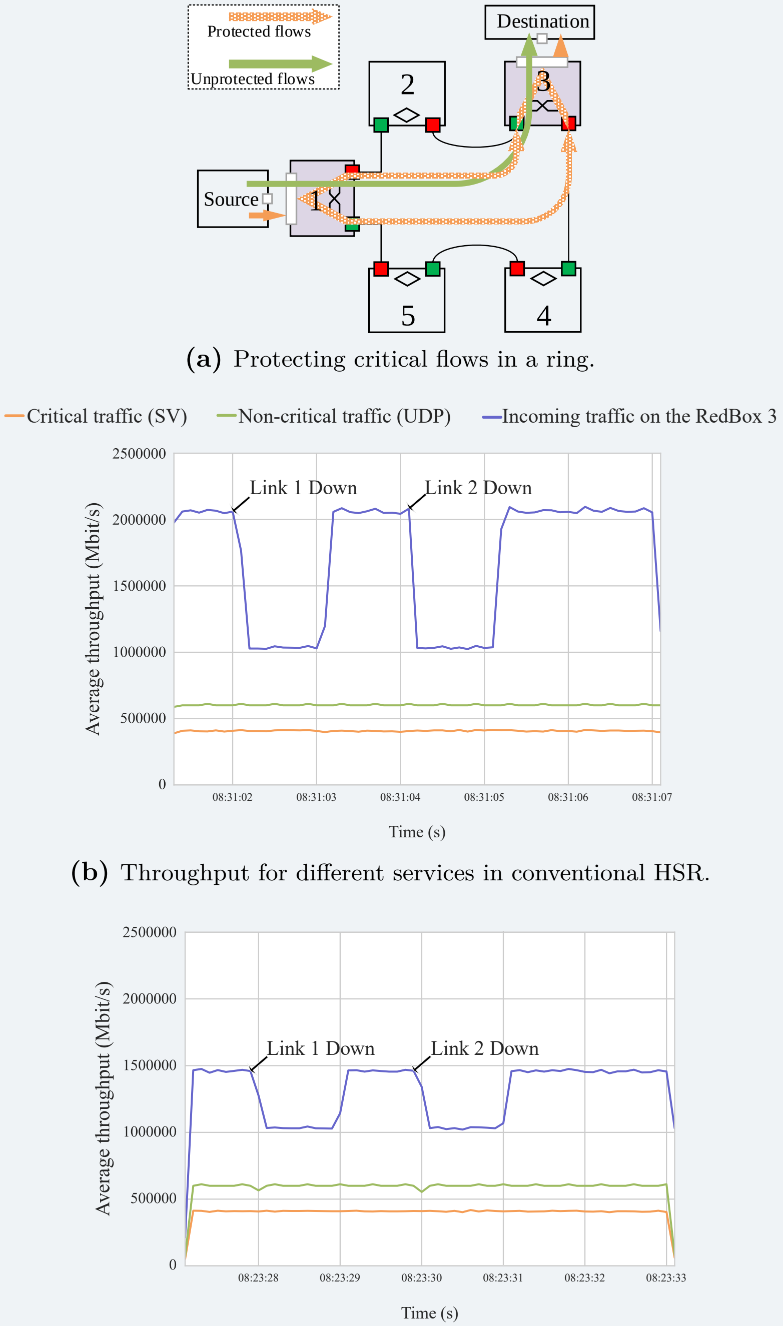


Figure 4.17: A comparison between DVP and HSR+OF for a three-ring topology considering data traffic patterns of IEC 61850-based systems.

goes down twice for several seconds. It is intended to highlight that no service disruption is still ensured only for time-critical services, since it can be checked that unicast SV frames [157] do not experience any loss of packets, whereas the UDP flow does suffer packet loss. Figure 4.18b also displays the decrease of incoming traffic on the destination RedBox, while in a traditional HSR network the available bandwidth is halved.

Furthermore, it is also shown that the recovery time can be reduced by using the “fast failover” OpenFlow feature, as occurs in the second interruption. Thus, the availability of non-critical services is improved. Figure 4.18b shows the average throughput, so packet loss is difficult to perceive. However, a detailed analysis of the frames received by Destination reveals a recovery time of 0.086 ms in a reactive recovery strategy, while fast-failover groups make it possible to reduce the recovery time to 0.004 ms. These recovery times represent a significant reduction over traditional spanning tree approaches such as RSTP (milliseconds at best).



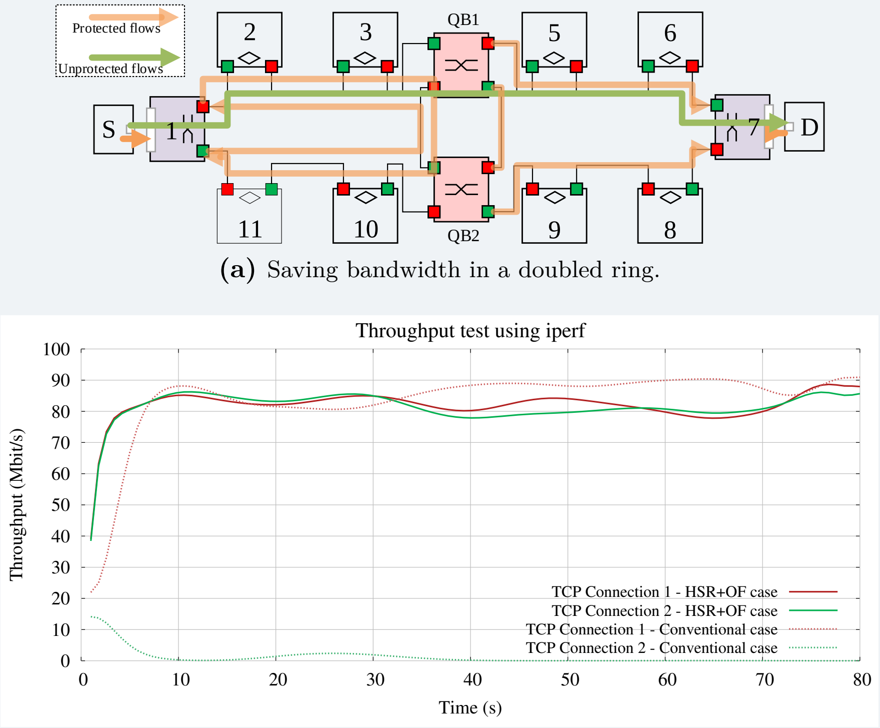
(a) Protecting critical flows in a ring.

(b) Throughput for different services in conventional HSR.

(c) Throughput for different services in HSR+OF approach.

Figure 4.18: Throughput rate based on the priority of the flows.

4.2.4.2 Exploting path diversity



(a) Saving bandwidth in a doubled ring.

(b) Increasing of throughput due to the lack of redundancy for non-critical flows.

Figure 4.19: Bandwidth performance under different settings.

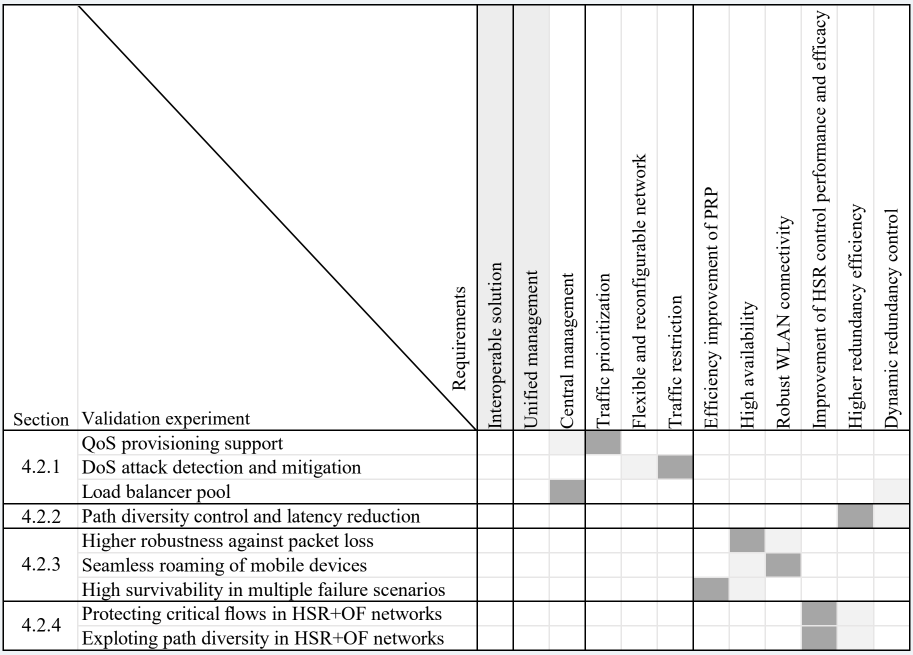
Controlling network resources is essential to maintain the required performance, since the interaction among different types of flows may affect to the latency of time-critical services. This experiment aims to measure the bidirectional bandwidth (in Figure 4.19a, from S to D, and vice versa) in a coupled ring topology, for which the iperf tool serves to measure the maximum achievable TCP bandwidth. As a result, the OpenFlow controller is able to balance the load, so that in this case TCP flows are transmitted through disjoint paths, enabling a better utilization of network resources. Figure 4.19b shows the sum of throughput achieved under the conventional approach and using a single path per flow. While in the former each TCP flow fully uses all links, the latter achieves higher throughput due to a lower bandwidth utilization for non-critical flows, since each flow is balanced and does not compete for bandwidth. Specifically, flow TCP-1 is transmitted through the nodes ‘1’, ‘2’, ‘3’, ‘QB1’, ‘5’, ‘6’ and ‘7’ and flow TCP-2 pass through nodes ‘7’, ‘8’, ‘9’, ‘QB2’, ‘10’, ‘11’ and ‘1’.

4.3 Discussion

Some conclusions are reported in this section. In order to facilitate the meeting of industrial communication requirements, and of the IEC 61850-based systems in particular, different QoS mechanisms should be considered, such as traffic prioritization, traffic filtering or a load balancer service. Indeed, they are according to the stringent criteria imposed by the IEC 61850 standard [23], which is reflected throughout the entire research. Consequently, the provided framework implements suitable management and traffic engineering techniques required to ensure adequate network performance. A reasonable test system has been provided to evaluate the effect of different parameters, such as network loading or redundancy, on network performance. Thus, once the test environment has been described, different parameters have been used in the performance evaluations.

Figure 4.20 connects the requirements, identified in Chapter 2 and taken as inputs to the proposal design, and validation tests. Although some tests inherently cover various requirements, the two main objectives of the experiments have been highlighted. As can be seen, those non-functional requirements associated with high availability and efficiency in the use of resources have been analyzed to a greater extent. On the other hand, the need for interoperability and the unified data management have been achieved in the SDN architecture design itself. Below are summarized the results of the tests.

First, three applications of the SDN framework have been validated: QoS pushing, DoS detection and load balancing, besides monitoring and resources management implicit to them. These different applications illustrate the usefulness of the flow-based approach. Other functionalities,



Section	Validation experiment / Requirements	Interoperable solution	Unified management	Central management	Traffic prioritization	Flexible and reconfigurable network	Traffic restriction	Efficiency improvement of PRP	High availability	Robust WLAN connectivity	Improvement of HSR control performance and efficacy	Higher redundancy efficiency	Dynamic redundancy control
4.2.1	QoS provisioning support			░	■								
	DoS attack detection and mitigation					░	■						
	Load balancer pool			■									░
4.2.2	Path diversity control and latency reduction											■	░
4.2.3	Higher robustness against packet loss								■	░			
	Seamless roaming of mobile devices								░	■			
	High survivability in multiple failure scenarios							■	░				
4.2.4	Protecting critical flows in HSR+OF networks										■	░	
	Exploting path diversity in HSR+OF networks										■	░	

Figure 4.20: Validation/Requirements trace matrix.

such as traffic isolation, tunneling or firewall are difficult to be represented in a visual manner.

Second, the results obtained from several experimental studies are related to the possibility of controlling all available network capacity. The fact of using certain OpenFlow controller capabilities represents, by default, an advantage with respect to traditional static spanning tree deployments where data do not have to follow the optimal path and, thereby, not achieving the optimal delay. By contrast, computing and setting the flow entries that, for example, form the shortest path in LANs can be considered essential for time-sensitive services. The proposal leverages path diversity to enable a service-aware flow control, which poses multiple advantages, such as a dynamic load-balancing or an appropriate failure recovery for critical and non-critical traffic.

Furthermore, improving the overall availability of critical services is a primary objective of new IEC 61850-based substations, so that active redundancy protocols are necessary to avoid retransmissions and recovery delays. To date, this is the first time that PRP and HSR features are included in OpenFlow networks. In this regard, the proposal increases flexibility in the deployments of highly available industrial networks by controlling, among other things, the redundant paths depending on the traffic class. This approach enables the possibility of using the PRP and HSR protocols as needed, reducing unnecessary traffic, which optimizes available resources. This can be an important limitation because the control and automation systems tend to integrate services that involve large volumes of data. Thus, end-to-end redundancy provisioning is based on traffic criticality, and several experiments have been conducted to illustrate the improvements in using parallel redundancy schemes controlled by an external entity that is not agnostic to network topology, conditions and traffic flows. The main objective of this performance analysis is to obtain significant results in terms of increased reliability, for example, by achieving zero the failover time in case of multiple simultaneous failures. Moreover, taking into account the benefits wireless solutions provide, the usability of the promising model which combines PRP and OpenFlow protocols in IEEE 802.11 networks has been shown in even the most demanding environments, such as in WLANs roaming scenarios where critical data must be properly managed and protected.

Concerning the HSR+OF approach, conducted analytical studies have demonstrated the versatility of this strategy, which affects resource consumption by reducing the number of links traversed from source to destination. Then, to illustrate the benefits of this approach, the effectiveness of the proposed priority-aware protection scheme is assessed in terms of throughput efficiency by analyzing in detail some particular cases. As a result, the bandwidth saving ratio obtained with this method is more effective than previous ones.

From another point of view, the bandwidth management has been carried out via traffic shaping, so that the resource reservation for different streams would be necessary in order to provide strict guarantees regarding message latency. Hence, a further analysis of the relations between network performance and QoS configurations, frame sizes or inter-frame arrival time will be addressed in future research. In addition, the impact that load balancing has on the network availability can be also examined in further research Other next steps for the future work are detailed in the next chapter.

We can only see a short distance ahead but we can see plenty there that needs to be done

Alan Turing, Computing Machinery and Intelligence

5 Conclusion

Contents

This chapter presents the summary and outlook of this work, and emphasizes the contribution of this thesis to the related research. Thus, next section reviews how the thesis statement has been addressed in the preceding chapters.

5.1 Thesis summary

Although the scope of industrial networks is extremely broad, ranging from smart factories to chemical industries and transportation domains, this thesis has chosen to focus on Smart Grid communications. In Smart Grid applications, situational awareness and adaptability are key features that simplify and enable flexible energy services. Besides this, with the increasing trend of developing highly efficient and reliable electric grids, as well as the integration of new distributed energy systems, there is a real need to move to new ICT solutions that adapt to specific constraints and dynamic changes. In particular, an IEC 61850-based system can be considered a representative example of critical cyber-physical infrastructure, which entails the deployment of robust topologies that fulfill strong latency and reliability requirements.

In the current context, in which SDN is being strongly considered in a variety of networking environments, it is of great significance to study the benefits and challenges of its application to future industrial infrastructures, and analyze how reliability and efficiency can be affected. Thus, the claim made in this thesis is that "using SDN technologies allows mission-critical systems to achieve greater levels of network resources management capabilities, while meeting QoS requirements. Moreover, demanding protection and control applications can operate with high reliability through a flow-based traffic processing approach". The assertion and associated research questions has been validated through the contribution of this thesis, which has been to study applicability of the SDN technologies to industrial networks, considering a twofold perspective: first, manage data flows in IEC 61850-based SASs, as a use case for ; and second, to improve performance of redundant Ethernet networks through SDN/OpenFlow techniques, since there are numerous mission-critical applications where packet loss or maximum recovery time requirements are particularly demanding, thereby requiring high-availability topologies.

In the first place, this study has provided a comprehensive overview of emerging needs and limitations of current networking technologies. In fact, after analyzing the issues involved in properly handling critical data communications, traditional networking strategies generally lack functionality to achieve adaptive systems as they are generally static and inflexible. Thus, based on the collected requirements, it has been proposed an SDN architecture which, unlike other authors [117] that first analyzed the possibility of exploiting the benefits of OpenFlow in IEC 61850-based substations, also incorporates management and monitoring capabilities to be aware of network configuration and traffic load in order to provide QoS for specific services.

Accordingly, an SGAM-based procedure is introduced for conceptualizing the development of a modular NOS, which configures data flows by parsing standard configuration files and diagnosing network conditions. This way, it has been proved to be able of handling an IEC 61850-based network efficiently, supporting the stringent communication requirements of power substations. This shows the benefits of using a logically centralized external agent that provides network control policies to be adaptable for different applications, and facilitate the dynamic resource management according to the network status, making the most of available resources. Concretely, this proposal includes automation techniques for performing a flow-based resource management that enable features such as traffic filtering, traffic shaping or security capabilities.

Furthermore, It has been concluded that avoiding single points of failure is essential for critical infrastructures. However, despite the fact that such networks have redundant resources, they are usually underused as active-passive configurations, mainly based on spanning tree protocols, which deteriorate the overall network performance. On the contrary, in order to facilitate compliance with strict time-sensitive requirements, an OpenFlow controller can be aware of the actual network topology and, thereby, multiple paths can be simultaneously, and efficiently, exploited. Thus, this proposal leverages the programmability provided by SDN technologies to dynamically control network resources and set several data paths between source and destination. As demonstrated, among other actors that affect performance, communication latency is reduced via load balancing as traffic spreading reduces the traffic interaction and network load. The latency reduction has been illustrated using both an analytical approximation and emulation tests.

In addition, the most representative standards for ensuring zero switchover time when a link or switch fails, PRP and HSR, pose diverse limitations due to the static replication of resources and information. In particular, PRP and HSR compliant devices are responsible for redundancy control and duplicate all traffic, regardless the type of service, which may cause an inefficient use of network resources. This implies significant drawbacks, such as providing unnecessary protection for non-critical data, which might cause network congestion or delays. Hence, an SDN approach is proposed to meet the existing necessities taking into account that an external network control can flexibly provide redundancy control and traffic prioritization. Specifically, the presented approach relies on the redundancy management capabilities of PRP and HSR nodes, along with flow-oriented control and flexibility features of OpenFlow. This choice is aimed at getting the best of both SDN and the implementation of the redundancy control mechanisms in the end nodes. In this manner, the redundancy degree can be established according to the actual requirements of critical and non-critical flows, so that the former are transmitted through active redundant paths, but the others do not, saving bandwidth and avoiding saturation of links. In particular, this has allowed, on the one hand, the provision of a higher level of redundancy between PRP nodes along multiple active paths in individual LANs, achieving a minimal disruption in case of multiple failures, which improves performance of traditional networks to which the PRP nodes are connected.

Moreover, an OpenFlow pipeline, based on the OVS software, has been incorporated into PRP/HSR nodes for filtering flows, as well as it has been also used as wireless APs. In fact, this thesis takes into account the emerging wireless technologies in industrial automation systems and, in order to reduce network downtime, the PRP is used in WLANs which are implemented under the SDN paradigm. It should be emphasized that, as far as the author is aware, no study has considered the potential impact of the SDN techniques on parallel redundancy Ethernet protocols, this being the first work on applying them to control PRP and HSR networks.

Regarding evaluation techniques, emulated network environments have enabled the evaluation of the proposed features, and the qualitatively discussion of the contributions, improvements and practical implications of the findings. Thus, the SDN approach presented in this work includes different added-value features providing mechanisms to meet the requirements specified by the IEC 61850 and IEC 62439 standards. These research findings support the hypothesis that using SDN technologies may become an appropriate solution to enable and enhance the development of mission-critical networks. Likewise, the network reliability improvement may enable new applications; especially those use cases that require minimum latency and loss of information.

In summary, after analyzing the applicability of SDN to critical CPS communications, the adoption of the SDN proposals would facilitate and address the current limitations identified in Chapter 2.

5.2 Future work

This thesis advances the understanding of SDN characteristics and performance for industrial network architectures, and has highlighted areas where further study is warranted. Firstly, some potential directions for extending this thesis are related to the opportunity of testing the novel contributions in field environments, thereby assessing their potential adoption and standardization. Other important topics for future research are listed below:

- **Hardware implementation**: performance tests undertaken using emulation techniques have allowed the reproduction of any topology where the network performance meets different requirements as, for example, specifying the link properties (bandwidth, loss, delay, and so on), without requiring a large amount of resources. For example, it must be taken into account that, at the present time, there is not available any commercial product that combines HSR and OpenFlow protocols. Hence, a software implementation tested in emulated networks has been appropriate to prove the advantages of this novel approach. Therefore, this study serves as a preliminary step to implement a hardware design, which is an interesting target for future work.

- **Integration of new control and monitoring algorithms**: other planned future activities include addressing some of the limitations of the current study. Although the performance results have demonstrated the usability of the all the aforementioned contributions and, thereby, the applicability of the SDN, the optimization of the existing solution is a future concern. Moreover, the proposed framework works as a NOS where new functionalities can be incorporated. Some improvements to be considered are given below.

- **Studying richer topologies**: with regard to network conditions and topologies, it could be expected to improve the results by considering more scenarios. For example, mixing PRP and HSR in redundant topologies could be considered in future research. In addition, it would be interesting to broaden the scope of IEEE 802.11

wireless networks analyzed, and consider the performance on IEEE 802.11s mesh networks, and under the IEEE 802.11n standard, as well as to consider QoS extensions. Concerning the use of PRP nodes with only one interface (SAN-based operation mode), experiments have use a standard PRP stack, without changes. However, it is clear that the protocol may be modified to reduce its overload and complexity: certain fields, for example, LAN ID, may not be necessary in this configuration mode. Otherwise, the work here presented manages unicast traffic redundancy; thus, it is considered necessary to study how the OpenFlow protocol may provide multicast traffic filtering along active redundant paths.

- **Guaranteeing bounded latency**: in another direction, it has been shown that a flow-based modeling approach helps meet the communication demands imposed by IEC 61850-based systems, such as latency or bandwidth. However, fulfilling stringent real-time application requirements could demand a predictable network performance with bounded response times, so that future work could include developing control services that conduct schedulability analysis. In order to perform flow scheduling of high priority traffic, it should be also necessary to implement synchronization mechanisms. These features are in line with the ongoing IEEE TSN and IETF DetNet projects, which are intended to provide the support of deterministic time-sensitive streams. Both standardization projects are currently exploring additional capabilities, such as spatial redundancy control or reservation protocols, to increase the reliability and determinism of industrial networks. It is necessary to mention that these projects are considering appropriate an SDN approach to carry out these goals, since external control agents enable the dynamic change of network policies and the adaptation of networks to traffic conditions in an automated way.

- **New application areas**: in general terms, this study has concentrated on the design of SDN communication infrastructures to support IEC 61850-based substations; however the application range could be extended to include more fields, such as WAN connecting SASs and utility companies, as well as to other ICSs whose traffic can be controlled by SDN controllers. Furthermore, despite SDN has drawn much research attention in the IT arena, it is in an early developmental stage and its adoption in traditional infrastructures is seen as a major challenge. Therefore, extensive experimental validation is required for mission-critical systems where, in addition, the long life cycles of industrial network equipment protect the investment already made. Thus, it can be assumed that resistance to change in IT systems, as well as organizational characteristics, such as "resources, size, centralization, formalization, complexity and expansion" [158], will affect the growing acceptance of SDN in existing CPSs.

5.3 Dissemination of results

Finally, it is remarkable that previously-mentioned contributions and research findings were published in different peer-reviewed journal articles during the development of this thesis. Publications arising from this work can be classified according their impact:

1. Journals indexed in published Journal Citation Reports (JCR):

    ➤ E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa, "Using Software Defined Networking to manage and control IEC 61850-based systems," *Computers and Electrical Engineering*, vol. 43, pp. 142–154, April 2015. Available: http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

    ➤ E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa, "Availability Improvement of Layer 2 Seamless Networks Using OpenFlow," *The Scientific World Journal*, Jan 2015. Available: http://dx.doi.org/10.1155/2015/283165

    ➤ E. Molina, E. Jacob, N. Toledo, and A. Astarloa, "Performance Enhancement of High-Availability Seamless Redundancy (HSR) Networks Using OpenFlow," *Communications Letters, IEEE*, vol. 20, no. 2, pp. 364–367, Feb 2016. Available: http://dx.doi/10.1109/LCOMM.2015.2504442

- N. Moreira, E. Molina, J. Lázaro, E. Jacob, and A. Astarloa, “Cyber-security in substation automation systems,” *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1552–1562, Feb 2016. Available: http://dx.doi.org/10.1016/j.rser.2015.10.124

- E. Molina and E. Jacob, “Software-Defined Networking in Cyber-Physical Systems: a survey,” *Computers and Electrical Engineering*, 2017, in press.

2. Publications in journals without impact factor and papers published in international conferences:

   - E. Molina, E. Jacob, and A. Astarloa, “Using OpenFlow to control redundant paths in wireless networks,” *Network Protocols and Algorithms*, vol. 8, no. 1, p. 90, May 2016. Available: http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

   - E. Molina, J. Matias, A. Astarloa, and E. Jacob, “Managing path diversity in layer 2 critical networks by using OpenFlow,” in *Network and Service Management (CNSM), International Conference on*, pp. 394–397, Nov 2015. Available: http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

   - N. Moreira, A. Astarloa, U. Kretzschmar, J. Lazaro, and E. Molina, “Securing IEEE 1588 messages with message authentication codes based on the KECCAK cryptographic algorithm implemented in FPGAs,” in *Industrial Electronics (ISIE), IEEE International Symposium on*, pp. 1899–1904, June 2014. Available: http://dx.doi.org/10.5296/npa.v8i1.8730

3. Peer-reviewed papers in national conferences

   - E. Molina, E. Jacob, and A. Astarloa, “Uso de OpenFlow para la gestión de caminos redundantes en redes inalámbricas,” in *Actas de las XII Jornadas de Ingeniería Telemática (JITEL)*, 2015, pp. 226–231. Available: http://jitel15.uib.es/static/actas-jitel-2015.pdf

- ➤ E. Molina, A. Astarloa, and E. Jacob, “Seguridad definida por software en subestaciones eléctricas,” in *I Jornadas Nacionales de Investigación en Ciberseguridad*, 2015, pp. 78–79. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=5469678

- ➤ E. Molina and E. Jacob, “Aplicabilidad de las redes definidas por software a los sistemas basados en el estándar IEC 61850,” in *III Congreso Smart Grids*, 2016, pp. 209–214.

4. Participation in other research activities

- ➤ E. Molina, “A study of the applicability of Software-Defined Networking in industrial networks,” in *Summer School Program, IEEE Communications Society*, 2016.

- ➤ E. Molina, “Un estudio sobre la aplicabilidad de las redes definidas por software a los sistemas industriales,” in *I Jornadas Doctorales de la UPV/EHU*, 2016. Available: http://www.ehu.eus/es/web/doktoregojardunaldiak/home

- ➤ E. Molina, “Aplicabilidad del concepto de Software-Defined Networking en redes industriales,” in *I & II Jornadas Zabalduz Eguna*, 2014-2015.

The work made in this thesis has been partially sponsored by the Spanish Ministry of Economy, Industry and Competitiveness (MINECO), under the S&N-SEC research project (“Despliegue seguro de servicios con Redes Definidas por Software y Virtualización de Funciones de Red” (01/01/2014 - 31/12/2016); and by the University of the Basque Country UPV/EHU under the Zabalduz research program.

6

References

[1] R. Drath and A. Horch, "Industrie 4.0: Hit or Hype?" *Industrial Electronics Magazine, IEEE*, vol. 8, no. 2, pp. 56–58, Jun. 2014. Available: http://dx.doi.org/10.1109/mie.2014.2312079

[2] Instrument Society of America, *ANSI/ISA 95.00.01-2010 Enterprise-Control System Integration - Part 1: Models and Terminology*. 2010.

[3] T. Sauter, "The Three Generations of Field-Level Networks - Evolution and Compatibility Issues," *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 11, pp. 3585–3595, Nov. 2010. Available: http://dx.doi.org/10.1109/TIE.2010.2062473

[4] B. Galloway and G. Hancke, "Introduction to Industrial Control Networks," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 2, pp. 860–880, May 2013. Available: http://dx.doi.org/10.1109/SURV.2012.071812.00124

[5] IEEE 802 project, "IEEE Time-Sensitive Networking Task Group." Available: http://www.ieee802.org/1/pages/tsn.html

[6] P. Leitão, A. W. Colombo, and S. Karnouskos, "Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges," *Computers in Industry*, vol. 81, pp. 11–25, 2016. Available: http://dx.doi.org/10.1016/j.compind.2015.08.004

[7] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, "Smart Transmission Grid: Vision and Framework," *Smart Grid, IEEE Transactions on*, vol. 1, no. 2, pp. 168–177, Sep. 2010. Available: http://dx.doi.org/10.1109/TSG.2010.2053726

[8] Open Networking Foundation (ONF), "Software Defined Networking: The New Norm for Networks," May 2012. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[9] Open Networking Foundation (ONF), "OpenFlow Switch Specification, version 1.5.1," Mar. 2015. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/

[10] National Institute of Standards and Technology (NIST), "NISTIR 7628. Guide-

lines for Smart Grid Cyber Security," Technical Report, 2010. Available: http://dx.doi.org/10.6028/NIST.IR.7628r1

[11] A. Lessard and M. Gerla, "Wireless communications in the automated factory environment," *Network, IEEE*, vol. 2, no. 3, pp. 64–69, May 1988. Available: http://dx.doi.org/10.1109/65.3275

[12] V. Gungor, B. Lu, and G. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 10, pp. 3557–3564, Oct. 2010. Available: http://dx.doi.org/10.1109/TIE.2009.2039455

[13] Smart Grid Coordination Group, "Standards for Smart Grids," CEN-CENELEC-ETSI, Technical Report, 2011. Available: http://www.etsi.org/images/files/Report_CENCLCETSI_Standards_Smart_Grids.pdf

[14] J. Bryson and P. Gallagher, "Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," *NIST Special Publication 1108r3*, 2014. Available: http://dx.doi.org/10.6028/NIST.SP.1108r3

[15] Smart Grid Coordination Group, "Smart Grid Reference Architecture," CEN-CENELEC-ETSI, Technical Report, 2012. Available: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Reference/_Architecture/_final.pdf

[16] S. M. Chemudupati Adithya; Kaulen, "The convergence of IT and Operational Technology," 2012. Available: http://ascent.atos.net/?wpdmdl=1069

[17] IEC Smart Grid Strategic Group (SG3), "Smart Grid Standardization Roadmap," Jun. 2010. Available: http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf

[18] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in *IEEE/PES Power Systems Conference and Exposition*, 2009. Available: http://dx.doi.org/10.1109/psce.2009.4840174

[19] IEC TC57, *Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs*, IEC 61850-6. Geneva, Switzerland.

[20] L. Zhu, D. Shi, and P. Wang, "IEC 61850-Based Information Model and Configuration Description of Communication Network in Substation Automation," *Power Delivery, IEEE Transactions on*, vol. 29, no. 1, pp. 97–107, Feb. 2014. Available: http://dx.doi/10.1109/TPWRD.2013.2269770

[21] UCA International Users Group, *Implementation guideline for digital interface to instrument transformers using iec 61850-9-2.* Raleigh, North Carolina, 2004. Avail-

able: http://tc57wg10.info/downloads/digifspec92ler21040707cb.pdf

[22] C. Lee, M. Park, J. Lee, and I. Joe, “Design and Implementation of Packet Analyzer for IEC 61850 Communication Networks in Smart Grid,” in *Computer applications for communication, networking, and digital contents*, vol. 350, Springer, 2012, pp. 33–40. Available: http://dx.doi.org/10.1007/978-3-642-35594-3_5

[23] IEC TC57, *Communication networks and systems for power utility automation - part 90-4: Network engineering guidelines*, IEC/TR 61850-90-4. Geneva, Switzerland, 2013.

[24] D. M. E. Ingram, P. Schaub, R. R. Taylor, and D. A. Campbell, “Network Interactions and Performance of a Multifunction IEC 61850 Process Bus,” *IEEE Transactions on Industrial Electronics*, vol. 60, no. 12, pp. 5933–5942, Dec. 2013. Available: http://dx.doi.org/10.1109/TIE.2012.2233701

[25] J. Farkas, B. Varga, E. Grossman, C. Gunther, P. Thubert, P. Wetterwald, J. Raymond, J. Korhonen, Y. Kaneko, S. Das, Y. Zha, F.-J. Goetz, and J. Schmitt, “Deterministic Networking Use Cases,” Internet Engineering Task Force, Internet-Draft, Mar. 2016. Available: https://tools.ietf.org/html/draft-ietf-detnet-use-cases-09

[26] IEC TC57, *Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models*, IEC 61850-5. Geneva, Switzerland, 2013.

[27] P. Ferrari, A. Flammini, S. Rinaldi, M. Rizzi, E. Sisinni, and G. Prytz, “On the use of multiple mac registration protocol in industrial networks,” in *Factory communication systems (wfcs), 2015 ieee world conference on*, 2015, pp. 1–8.

[28] D. Ingram, P. Schaub, and D. Campbell, “Multicast traffic filtering for sampled value process bus networks,” in *Industrial Electronics Society (IECON), Conference on*, 2011, pp. 4710–4715. Available: http://dx.doi.org/10.1109/IECON.2011.6120087

[29] Z. Zhang, X. Huang, B. Keune, Y. Cao, and Y. Li, “Modeling and Simulation of Data Flow for VLAN-Based Communication in Substations,” *IEEE Systems Journal*, In press. Available: http://dx.doi.org/10.1109/JSYST.2015.2428058

[30] P. Heise, F. Geyer, and R. Obermaisser, “Deterministic OpenFlow: Performance evaluation of SDN hardware for avionic networks,” in *Network and Service Management (CNSM), International Conference on*, 2015, pp. 372–377. Available: http://dx.doi.org/10.1109/CNSM.2015.7367385

[31] Y. Zhang, Z. Cai, X. Li, and R. He, “Analytical modeling of traffic flow in the substation communication network,” *IEEE Transactions on Power Delivery*, vol. 30, no. 5, pp. 2119–2127, Oct. 2015. Available: http://dx.doi.org/10.1109/TPWRD.

2014.2377475

[32] Aeronautical Radio Inc., *ARINC Specification 664: Aircraft Data Network, Part 7: Avionics Full Duplex Switched Ethernet (AFDX) Network*. Annapolis, USA, 2003.

[33] Z. Peng-yu, Z. Yan, L. Xiao-Sheng, P. Ji-wei, and Z. Zhen-feng, “A novel fast and deterministic substation communication network architecture based on AFDX,” in *Industrial Electronics Society (IECON), Conference on*, 2012, pp. 110–115. Available: http://dx.doi.org/10.1109/IECON.2012.6388823

[34] P. Heise, I. Gaillardet, H. Rahman, and V. Mannur, “Avionics Full Duplex Ethernet and the Time Sensitive Networking Standard,” May. 2015. Available: http://www.ieee802.org/1/files/public/docs2015

[35] SAE International, *AS6802: Time-Triggered Ethernet*. 2011.

[36] M. Jakovljevic and A. Ademaj, “Ethernet protocol services for critical embedded systems applications,” in *Digital avionics systems conference (DASC), IEEE/AIAA*, 2010. Available: http://dx.doi.org/10.1109/DASC.2010.5655310

[37] P. Gutierrez Peon, H. Kopetz, and W. Steiner, “Towards a reliable and high-speed wireless complement to TTEthernet,” in *Emerging Technology and Factory Automation (ETFA), IEEE*, 2014, pp. 1–4. Available: http://dx.doi.org/10.1109/ETFA.2014.7005311

[38] Y.-H. Wei, Q. Leng, S. Han, A. Mok, W. Zhang, and M. Tomizuka, “RT-WiFi: Real-Time High-Speed Communication Protocol for Wireless Cyber-Physical Control Applications,” in *Real-Time Systems Symposium (RTSS), IEEE*, 2013, pp. 140–149. Available: http://dx.doi.org/10.1109/RTSS.2013.22

[39] P. Bieber, F. Boniol, M. Boyer, E. Noulard, and C. Pagetti, “New Challenges for Future Avionic Architectures,” *AerospaceLab*, no. 4, pp. p. 1–10, May 2012. Available: https://hal.archives-ouvertes.fr/hal-01184101

[40] IEC 65C, *Industrial communication networks - High availability automation networks - Part 1: General concepts and calculation methods*, IEC 62439-1. Geneva, Switzerland, 2010.

[41] K. Stouffer, J. Falco, and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security,” *NIST Special Publication*, vol. 800, p. 82, 2014. Available: http://dx.doi.org/10.6028/NIST.SP.800-82r2

[42] W. Knowles, D. Prince, D. Hutchison, P. Disso, and K. Jones, “A survey of cyber security management in industrial control systems,” *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52–80, 2015. Available: http://dx.doi.org/10.

1016/j.ijcip.2015.02.002

[43] National Institute of Standards and Technology (NIST), *Framework for Cyber-Physical Systems, Release 1.0*. 2016. Available: https://pages.nist.gov/cpspwg/library/

[44] IEC TC57, *Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850*, IEC TS 62351-6. Geneva, Switzerland, 2006.

[45] J. Hoyos, M. Dehus, and T. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *Globecom Workshops, IEEE*, 2012, pp. 1508–1513. Available: http://dx.doi.org/10.1109/GLOCOMW.2012.6477809

[46] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE Protocol," in *Australasian Information Security Conference (AISC)*, 2014, pp. 17–22. Available: http://dl.acm.org/citation.cfm?id=2667510.2667513

[47] IEC TC57, *Communication networks and systems in substations - part 90-12: Wide area network engineering guidelines*, IEC/TR 61850-90-12. Geneva, Switzerland, 2015.

[48] Institute of Electrical and Electronics Engineers (IEEE), *Recommended Practice for Network Communication in Electric Power Substations*, IEEE Std 1615-2007. Geneva, Switzerland, 2007.

[49] A. Martinez, M. Yannuzzi, V. Lopez, D. Lopez, W. Ramirez, R. Serral-Gracia, X. Masip-Bruin, M. Maciejewski, and J. Altmann, "Network Management Challenges and Trends in Multi-Layer and Multi-Vendor Settings for Carrier-Grade Networks," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 4, pp. 2207–2230, Nov. 2014. Available: http://dx.doi.org/10.1109/COMST.2014.2327754

[50] U. Herberg, M. Ersue, D. Romascanu, and J. Schonwalder, "Management of Networks with Constrained Devices: Problem Statement and Requirements," Internet Engineering Task Force; RFC 7547, Oct. 2015. Available: https://rfc-editor.org/rfc/rfc7547.txt

[51] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of Resource Constrained Devices in the Internet of Things," *Communications Magazine, IEEE*, vol. 50, no. 12, pp. 144–149, Dec. 2012. Available: http://dx.doi.org/10.1109/MCOM.2012.6384464

[52] A. Luntovskyy, J. Spillner, and V. Vasyutynskyy, "Soft computing in computer and information science," A. Wiliński, E. I. Fray, and J. Pejaś, Eds. Cham: Springer International Publishing, 2015, pp. 293–308. Available: http://dx.doi.org/10.1007/

978-3-319-15147-2_25

[53] Cisco, “Connected grid design suite.” Available: http://www.cisco.com/c/en/us/solutions/industries/energy/external-utilities-smart-grid.html

[54] J. Suh, T. T. Kwon, C. Dixon, W. Felter, and J. Carter, “OpenSample: A Low-Latency, Sampling-Based Measurement Platform for Commodity SDN,” in *Distributed Computing Systems (ICDCS), IEEE Conference on*, 2014, pp. 228–237. Available: http://dx.doi.org/10.1109/ICDCS.2014.31

[55] C. Schmitt, T. Kothmayr, B. Ertl, W. Hu, L. Braun, and G. Carle, “TinyIPFIX: An efficient application protocol for data exchange in cyber physical systems,” *Computer Communications*, vol. 74, no. 15, pp. 63–76, 2014. Available: http://dx.doi.org/10.1016/j.comcom.2014.05.012

[56] T. Chen and L. Hu, “Internet performance monitoring,” *Proceedings of the IEEE*, vol. 90, no. 9, pp. 1592–1603, Sep. 2002. Available: http://dx.doi.org/10.1109/JPROC.2002.802006

[57] C. Argyropoulos, D. Kalogeras, G. Androulidakis, and V. Maglaris, “PaFloMon: A Slice Aware Passive Flow Monitoring Framework for OpenFlow Enabled Experimental Facilities,” in *Software Defined Networking (EWSDN), European Workshop on*, 2012, pp. 97–102. Available: http://dx.doi/10.1109/EWSDN.2012.13

[58] A. Tootoonchian, M. Ghobadi, and Y. Ganjali, “OpenTM: Traffic Matrix Estimator for OpenFlow Networks,” in *Passive and active measurement*, vol. 6032, Springer Berlin Heidelberg, 2010, pp. 201–210. Available: http://dx.doi.org/10.1007/978-3-642-12334-4/_21

[59] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, “Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments,” *Computer Networks*, vol. 62, no. 0, pp. 122–136, 2014. Available: http://dx.doi.org/10.1016/j.bjp.2013.10.014

[60] Q. Zhu and T. Basar, “Robust and resilient control design for cyber-physical systems with an application to power systems,” in *Decision and Control and European Control Conference (CDC-ECC), IEEE Conference on*, 2011, pp. 4066–4071. Available: http://dx.doi.org/10.1109/CDC.2011.6161031

[61] M. Popovic, M. Mohiuddin, D. C. Tomozei, and J. Y. L. Boudec, “iPRP - the Parallel Redundancy Protocol for IP Networks: Protocol Design and Operation,” *IEEE Transactions on Industrial Informatics*, In press. Available: http://dx.doi.org/10.1109/TII.2016.2530018

[62] I. Lopez, M. Aguado, C. Pinedo, and E. Jacob, “SCADA Systems in the Railway Domain: Enhancing Reliability through Redundant MultipathTCP,” in *Intelligent Transportation Systems, IEEE International Conference on*, 2015, pp. 2305–2310.

Available: http://dx.doi/10.1109/ITSC.2015.372

[63] M. Huynh, S. Goose, and P. Mohapatra, "Resilience technologies in Ethernet," *Computer Networks*, vol. 54, no. 1, pp. 57–78, 2010. Available: http://dx.doi.org/10.1016/j.comnet.2009.08.012

[64] J. W. Suurballe, "Disjoint paths in a network," *Networks*, vol. 4, no. 2, pp. 125–145, 1974. Available: http://dx.doi.org/10.1002/net.3230040204

[65] P. Cholda and A. Jajszczyk, "Recovery and Its Quality in Multilayer Networks," *Lightwave Technology, Journal of*, vol. 28, no. 4, pp. 372–389, Feb. 2010. Available: http://dx.doi.org/10.1109/JLT.2009.2031821

[66] G. Cena, S. Scanzio, A. Valenzano, and C. Zunino, "An enhanced MAC to increase reliability in redundant Wi-Fi networks," in *Factory Communication Systems (WFCS), IEEE Workshop on*, 2014, pp. 1–10. Available: http://dx.doi.org/10.1109/WFCS.2014.6837591

[67] S. Kubler, J. Robert, J.-P. Georges, and É. Rondeau, "Dual path communications over multiple spanning trees for networked control systems," *Engineering Applications of Artificial Intelligence*, vol. 25, no. 7, pp. 1460–1470, 2012. Available: http://dx.doi.org/10.1016/j.engappai.2012.05.001

[68] R. van der Pol, M. Bredel, A. Barczyk, B. Overeinder, N. van Adrichem, and F. Kuipers, "Experiences with MPTCP in an intercontinental OpenFlow network," in *TERENA Network Conference*, 2013.

[69] P. Ferrari, A. Flammini, S. Rinaldi, G. Prytz, and R. Hussain, "Multipath redundancy for industrial networks using IEEE 802.1aq Shortest Path Bridging," in *Factory Communication Systems (WFCS), IEEE Workshop on*, 2014, pp. 1–10. Available: http://dx.doi.org/10.1109/WFCS.2014.6837598

[70] J. M. Selga, G. Corral, A. Zaballos, and R. M. de Pozuelo, "Smart grid ICT research lines out of the European project INTEGRIS," *Network Protocols and Algorithms*, vol. 6, no. 2, pp. 93–122, 2014. Available: http://dx.doi.org/10.5296/npa.v6i2.5439

[71] M. Zhang, J. Pathangi, A. Ghanwani, A. Banerjee, and T. Senevirathne, "TRILL Resilient Distribution Trees," Internet Engineering Task Force; Internet Engineering Task Force, Internet-Draft, Jun. 2016. Available: https://tools.ietf.org/html/draft-ietf-trill-resilient-trees-05

[72] IEC 65C, *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*, IEC 62439-3. Geneva, Switzerland, 2012.

[73] P. Ferrari, A. Flammini, S. Rinaldi, E. Sisinni, and G. Prytz, "Advanced net-

works for distributed measurement in substation automation systems," in *Applied Measurements for Power Systems (AMPS), IEEE International Workshop on*, 2013, pp. 108–113. Available: http://dx.doi.org/10.1109/AMPS.2013.6656235

[74] N. Enomoto, H. Shimonishi, J. Higuchi, T. Yoshikawa, and A. Iwata, "High-Speed, Short-Latency Multipath Ethernet Transport for Interconnections," in *High Performance Interconnects, IEEE Symposium on*, 2008, pp. 75–84. Available: http://dx.doi.org/10.1109/HOTI.2008.13

[75] A. Charny and J.-Y. L. Boudec, "Delay bounds in a network with aggregate scheduling," in *Quality of future internet services: First cost 263 international workshop, qofis 2000 berlin, germany, september 25–26, 2000 proceedings*, J. Crowcroft, J. Roberts, and M. I. Smirnov, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 1–13. Available: http://dx.doi.org/10.1007/3-540-39939-9_1

[76] S. Nsaif and J.-M. Rhee, "DVP: A Novel High-Availability Seamless Redundancy (HSR) Protocol Traffic-Reduction Algorithm for a Substation Automation System Network," *Energies*, vol. 7, no. 3, pp. 1792–1810, 2014. Available: http://dx.doi.org/10.3390/en7031792

[77] I. Abdulsalam and J. Rhee, "Improvement of High-availability Seamless Redundancy (HSR) Unicast Traffic Performance Using Port Locking," in *Software Engineering (WCSE), World Congress on*, 2013, pp. 246–250. Available: http://dx.doi.org/10.1109/WCSE.2013.45

[78] M. Shin and I. Joe, "Performance improvement for the HSR ring protocol with traffic control in smart grid," in *Computer applications for graphics, grid computing, and industrial environment*, 2012, pp. 48–55. Available: http://dx.doi.org/10.1007/978-3-642-35600-1_7

[79] H.-D. Ngo, H.-S. Yang, D.-W. Ham, J. Rhee, Y. An, J. Han, Y. Lee, and N. Lee, "An improved High-availability Seamless Redundancy (HSR) for dependable Substation Automation System," in *Advanced Communication Technology (ICACT), International Conference on*, 2014, pp. 921–927. Available: http://dx.doi/10.1109/ICACT.2014.6779094

[80] Electric Power Research Institute (EPRI), "Assessment of Wireless Technologies in Substation Functions - Part II: Substation Monitoring and Management Technologies," Technical Report, Mar. 2006.

[81] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, Jun. 2005. Available: http://dx.doi.org/10.1109/JPROC.2005.849717

[82] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie, and Y. Chen, "Real-Time Wireless Sensor-Actuator Networks for Industrial Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1013–1024, May

2016. Available: http://dx.doi/10.1109/JPROC.2015.2497161

[83] A. Autolitano, D. Brevi, G. Cena, P. Cultrona, G. Marchetto, F. Rusina, S. Scanzio, R. Scopigno, and R. Sisto, "Wireless for the factory: The Wi-Fact analysis," in *Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), IEEE International Forum on*, 2015, pp. 403–410. Available: http://dx.doi.org/10.1109/RTSI.2015.7325132

[84] A. Abdrabou and A. Gaouda, "Considerations for packet delivery reliability over polling-based wireless networks in smart grids," *Computers & Electrical Engineering*, vol. 41, pp. 368–382, 2015. Available: http://dx.doi.org/10.1016/j.compeleceng.2014.12.003

[85] P. Parikh, T. Sidhu, and A. Shami, "A Comprehensive Investigation of Wireless LAN for IEC 61850 Based Smart Distribution Substation Applications," *Industrial Informatics, IEEE Transactions on*, vol. 9, no. 3, pp. 1466–1476, Aug. 2013. Available: http://dx.doi.org/10.1109/TII.2012.2223225

[86] L. Seno and S. Vitturi, "Wireless extension of Ethernet Powerlink networks based on the IEEE 802.11 wireless LAN," in *Factory Communication Systems (WFCS), IEEE Workshop on*, 2008, pp. 55–63. Available: http://dx.doi.org/10.1109/WFCS.2008.4638726

[87] P. Castello, P. Ferrari, A. Flammini, C. Muscas, P. Pegoraro, and S. Rinaldi, "A Distributed PMU for Electrical Substations With Wireless Redundant Process Bus," *Instrumentation and Measurement, IEEE Transactions on*, vol. 64, no. 5, pp. 1149–1157, May 2015. Available: http://dx.doi.org/10.1109/RTSI.2015.7325132

[88] T. Hasegawa and S. Yamamoto, "Design and execution of a Plant Wide ISA100 Wireless network for optimization of complex process industries," in *Society of Instrument and Control Engineers of Japan (SICE), Annual Conference of the*, 2015, pp. 158–163. Available: http://dx.doi.org/10.1109/SICE.2015.7285310

[89] A. Willig, "Redundancy concepts to increase transmission reliability in wireless industrial lans," *Industrial Informatics, IEEE Transactions on*, vol. 1, no. 3, pp. 173–182, Aug. 2005. Available: http://dx.doi.org/10.1109/TII.2005.852070

[90] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: reliable information forwarding using multiple paths in sensor networks," in *Local Computer Networks, Annual IEEE International Conference on*, 2003, pp. 406–415. Available: http://dx.doi.org/10.1109/LCN.2003.1243166

[91] M. Neely and E. Modiano, "Capacity and delay tradeoffs for ad hoc mobile networks," *Information Theory, IEEE Transactions on*, vol. 51, no. 6, pp. 1917–1937, Jun. 2005. Available: http://dx.doi.org/10.1109/TIT.2005.847717

[92] M. Rentschler and P. Laukemann, "Performance analysis of parallel redundant

WLAN," in *Emerging Technologies Factory Automation (ETFA), IEEE Conference on*, 2012, pp. 1–8. Available: http://dx.doi/10.1109/ETFA.2012.6489647

[93] A. Greenberg, G. Hjalmtysson, D. A. Maltz, A. Myers, J. Rexford, G. Xie, H. Yan, J. Zhan, and H. Zhang, "A Clean Slate 4D Approach to Network Control and Management," *SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 5, pp. 41–54, Oct. 2005. Available: http://doi.acm.org/10.1145/1096536.1096541

[94] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008. Available: http://dx.doi.org/10.1145/1355734.1355746

[95] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, "OpenFlow: Meeting carrier-grade recovery requirements," *Computer Communications*, vol. 36, no. 6, pp. 656–665, 2013. Available: http://dx.doi.org/10.1016/j.comcom.2012.09.011

[96] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, "Automatic bootstrapping of OpenFlow networks," in *Local Metropolitan Area Networks (LANMAN), IEEE Workshop on*, 2013, pp. 1–6. Available: http://dx.doi.org/10.1109/LANMAN.2013.6528283

[97] International Telecommunication Union (ITU), "Framework of Software-Defined Networking," Telecommunication standardization sector, Geneva, Switzerland, Jun. 2014.

[98] H. Kim and N. Feamster, "Improving network management with software defined networking," *Communications Magazine, IEEE*, vol. 51, no. 2, pp. 114–119, Feb. 2013. Available: http://dx.doi.org/10.1109/MCOM.2013.6461195

[99] J. Wickboldt, W. De Jesus, P. Isolani, C. Both, J. Rochol, and L. Granville, "Software-defined networking: Management requirements and challenges," *Communications Magazine, IEEE*, vol. 53, no. 1, pp. 278–285, Jan. 2015. Available: http://dx.doi.org/10.1109/MCOM.2015.7010546

[100] K. Ahmed, J. Blech, M. Gregory, and H. Schmidt, "Software Defined Networking for Communication and Control of Cyber-Physical Systems," in *Parallel and Distributed Systems (ICPADS), IEEE International Conference on*, 2015, pp. 803–808. Available: http://dx.doi.org/10.1109/ICPADS.2015.107

[101] B. Pfaff and B. Davie, "The Open vSwitch Database Management Protocol," Internet Engineering Task Force; RFC 7047 (Informational), Dec. 2013. Available: http://www.ietf.org/rfc/rfc7047.txt

[102] J. M. Halpern, "Standards collisions around SDN," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 10–15, Dec. 2014. Available: http://dx.doi.org/10.1109/

MCOM.2014.6979980

[103] A. Bianco, P. Giaccone, A. Mahmood, M. Ullio, and V. Vercellone, “Evaluating the SDN control traffic in large ISP networks,” in *IEEE International Conference on Communications (ICC)*, 2015, pp. 5248–5253. Available: http://dx.doi.org/10.1109/ICC.2015.7249157

[104] M. Fernandez, “Comparing OpenFlow Controller Paradigms Scalability: Reactive and Proactive,” in *Advanced Information Networking and Applications (AINA), IEEE International Conference on*, 2013, pp. 1009–1016. Available: http://dx.doi.org/10.1109/AINA.2013.113

[105] B. Heller, R. Sherwood, and N. McKeown, “The controller placement problem,” *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 473–478, Sep. 2012. Available: http://doi.acm.org/10.1145/2377677.2377767

[106] D. Hock, M. Hartmann, S. Gebert, M. Jarschel, T. Zinner, and P. Tran-Gia, “Pareto-optimal resilient controller placement in SDN-based core networks,” in *Teletraffic, International Congress on*, 2013, pp. 1–9. Available: http://dx.doi.org/10.1109/ITC.2013.6662939

[107] K. Nguyen, Q. T. Minh, and S. Yamada, “A Software-Defined Networking Approach for Disaster-Resilient WANs,” in *Computer Communications and Networks (ICCCN), International Conference on*, 2013, pp. 1–5. Available: http://dx.doi.org/10.1109/ICCCN.2013.6614094

[108] S. Lange, S. Gebert, T. Zinner, P. Tran-Gia, D. Hock, M. Jarschel, and M. Hoffmann, “Heuristic Approaches to the Controller Placement Problem in Large Scale SDN Networks,” *Network and Service Management, IEEE Transactions on*, vol. 12, no. 1, pp. 4–17, Mar. 2015. Available: http://dx.doi.org/10.1109/TNSM.2015.2402432

[109] Y. Jarraya, T. Madi, and M. Debbabi, “A Survey and a Layered Taxonomy of Software-Defined Networking,” *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1955–1980, Sep. 2014. Available: http://dx.doi.org/10.1109/COMST.2014.2320094

[110] A. Tootoonchian and Y. Ganjali, “HyperFlow: A Distributed Control Plane for OpenFlow,” in *Research on Enterprise Networking, Internet Network Management Conference on*, 2010, pp. 1–6. Available: http://dl.acm.org/citation.cfm?id=1863133.1863136

[111] S. Hassas Yeganeh and Y. Ganjali, “Kandoo: A Framework for Efficient and Scalable Offloading of Control Applications,” in *Hot Topics in Software Defined Networking (HotSDN), ACM SIGCOMM Workshop on*, 2012, pp. 19–24. Available:

http://doi.acm.org/10.1145/2342441.2342446

[112] A. Lara, A. Kolasani, and B. Ramamurthy, "Network Innovation using OpenFlow: A Survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 1, pp. 493–512, Jan. 2014. Available: http://dx.doi.org/10.1109/SURV.2013.081313.00105

[113] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: deterministic IP-enabled industrial internet (of things)," *Communications Magazine, IEEE*, vol. 52, no. 12, pp. 36–41, Dec. 2014. Available: http://dx.doi.org/10.1109/MCOM.2014.6979984

[114] IEEE LAN/MAN Standards Committee and others, *Standard for local and metropolitan area networks-frame replication and elimination for reliability*. 2014. Available: http://www.ieee802.org/1/pages/802.1cb.html

[115] M. Steinbacher and M. Bredel, "LACP Meets OpenFlow - Seamless Link Aggregation to OpenFlow Networks," in *TERENA Network Conference*, 2015. Available: https://tnc15.terena.org/getfile/1867

[116] A. Sydney, J. Nutaro, C. Scoglio, D. Gruenbacher, and N. Schulz, "Simulative Comparison of Multiprotocol Label Switching and OpenFlow Network Technologies for Transmission Operations," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 763–770, Jun. 2013. Available: http://dx.doi.org/10.1109/TSG.2012.2227516

[117] A. Cahn, J. Hoyos, M. Hulse, and E. Keller, "Software-defined energy communication networks: From substation automation to future smart grids," in *Smart Grid Communications (SmartGridComm), IEEE International Conference on*, 2013, pp. 558–563. Available: http://dx.doi.org/10.1109/SmartGridComm.2013.6688017

[118] J. Zhang, B.-C. Seet, T.-T. Lie, and C. H. Foh, "Opportunities for Software-Defined Networking in Smart Grid," in *Information, Communications and Signal Processing (ICICS), International Conference on*, 2013, pp. 1–5. Available: http://dx.doi/10.1109/ICICS.2013.6782793

[119] F. Granelli, A. Gebremariam, M. Usman, F. Cugini, V. Stamati, M. Alitska, and P. Chatzimisios, "Software defined and virtualized wireless access in future wireless networks: scenarios and standards," *Communications Magazine, IEEE*, vol. 53, no. 6, pp. 26–34, Jun. 2015. Available: http://dx.doi.org/10.1109/MCOM.2015.7120042

[120] P. Ferrari, A. Flammini, M. Rizzi, and E. Sisinni, "Improving simulation of wireless networked control systems based on WirelessHART," *Computer Standards & Interfaces*, vol. 35, no. 6, pp. 605–615, 2013. Available: http://dx.doi.org/10.1016/j.csi.2013.04.003

[121] P. Dely, A. Kassler, and N. Bayer, "OpenFlow for Wireless Mesh Networks," in *Computer Communications and Networks (ICCCN), International Conference on*,

2011, pp. 1–6. Available: http://dx.doi.org/10.1109/ICCCN.2011.6006100

[122] K.-K. Yap, T.-Y. Huang, M. Kobayashi, M. Chan, R. Sherwood, G. Parulkar, and N. McKeown, “Lossless Handover with n-casting between WiFi-WiMAX on OpenRoads,” *ACM Mobicom*, vol. 12, no. 3, pp. 40–52, 2009. Available: http://yuba.stanford.edu/~huangty/mobicom09demo.pdf

[123] N. G. Nayak, F. Durr, and K. Rothermel, “Software-defined environment for reconfigurable manufacturing systems,” in *Internet of Things (IoT), International Conference on the*, 2015, pp. 122–129. Available: http://dx.doi/10.1109/IOT.2015.7356556

[124] S.-Y. Lien, “Resource-Optimal Heterogeneous Machine-to-Machine Communications in Software Defined Networking Cyber-Physical Systems,” *Wireless Personal Communications*, vol. 84, no. 3, pp. 2215–2239, 2015. Available: http://dx.doi.org/10.1007/s11277-015-2560-6

[125] G. Kálmán, D. Orfanus, and R. Hussain, “Overview and Future of Switching Solutions for Industrial Ethernet,” *International Journal on Advances in Networks and Services Volume 7, Number 3 & 4, 2014*, vol. 7, no. 3, 2014.

[126] J. Kim, F. Filali, and Y.-B. Ko, “Trends and Potentials of the Smart Grid Infrastructure: From ICT Sub-System to SDN-Enabled Smart Grid Architecture,” *Applied Sciences*, vol. 5, no. 4, p. 706, 2015. Available: http://dx.doi.org/10.3390/app5040706

[127] ISO/IEC JTC 1/SC 7, *Systems and software engineering - Architecture description*, ISO/IEC/IEEE 42010. 2011.

[128] S. Chelluri, D. Rodas, and A. Harikrishna, “Integration considerations for large-scale iec 61850 systems,” in *5th international conference power system protection and automation*, 2010.

[129] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, “NOX: Towards an Operating System for Networks,” *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 3, pp. 105–110, Jul. 2008. Available: http://doi.acm.org/10.1145/1384609.1384625

[130] G. Tarnaras, E. Haleplidis, and S. Denazis, “SDN and ForCES based optimal network topology discovery,” in *Network Softwarization (NetSoft), IEEE Conference on*, 2015, pp. 1–6. Available: http://dx.doi.org/10.1109/NETSOFT.2015.7116181

[131] M. Charikar, C. Chekuri, T.-y. Cheung, Z. Dai, A. Goel, S. Guha, and M. Li, “Approximation algorithms for directed steiner problems,” *Journal of Algorithms*, vol. 33, no. 1, pp. 73–91, 1999. Available: http://www.sciencedirect.com/science/

article/pii/S0196677499910428

[132] Azarov, Max, “Worst-case Ethernet Network Latency for Shaped Sources,” Dec. 2005. Available: http://www.ieee802.org/1/files/public/docs2005/resb-azarov-WorstCaseLatency-051205.pdf

[133] X. Xu and Y. Ni, “Analysis of networking mode caused by GOOSE delay of smart substation,” in *Software Engineering and Service Science (ICSESS), IEEE International Conference on*, 2013, pp. 503–506. Available: http://dx.doi.org/10.1109/ICSESS.2013.6615359

[134] C. Rotsos, N. Sarrar, S. Uhlig, R. Sherwood, and A. W. Moore, “OFLOPS: An Open Framework for Openflow Switch Evaluation,” in *Passive and Active Measurement, International Conference on*, 2012, pp. 85–95. Available: http://dx.doi.org/10.1007/978-3-642-28537-0_9

[135] P. T. Congdon, P. Mohapatra, M. Farrens, and V. Akella, “Simultaneously reducing latency and power consumption in openflow switches,” *IEEE/ACM Transactions on Networking*, vol. 22, no. 3, pp. 1007–1020, Jun. 2014. Available: http://dx.doi.org/10.1109/TNET.2013.2270436

[136] B. Falahati, M. Mousavi, and M. Vakilian, “Latency considerations in IEC 61850-enabled Substation Automation Systems,” in *Power and energy society general meeting, IEEE*, 2011, pp. 1–8. Available: http://dx.doi.org/10.1109/PES.2011.6039138

[137] D. Ingram, P. Schaub, R. Taylor, and D. Campbell, “Performance Analysis of IEC 61850 Sampled Value Process Bus Networks,” *Industrial Informatics, IEEE Transactions on*, vol. 9, no. 3, pp. 1445–1454, Aug. 2013. Available: http://dx.doi.org/10.1109/TII.2012.2228874

[138] S. Song, S. Hong, X. Guan, B.-Y. Choi, and C. Choi, “NEOD: Network Embedded On-line Disaster management framework for Software Defined Networking,” in *Integrated Network Management, IFIP/IEEE International Symposium on*, 2013, pp. 492–498. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6573023

[139] G. Ditzel, “High Availability in EtherNet/IP Systems Using Parallel Redundancy Protocol (PRP),” in *Industry Conference, Annual Meeting*, 2014, pp. 1–16.

[140] Flexibilis, *FRS IPO Configurations - Application Note FLXN110*. 2014.

[141] B. Lantz, B. Heller, and N. McKeown, “A Network in a Laptop: Rapid Prototyping for Software-defined Networks,” in *Hot Topics in Networks (HotNets), ACM SIGCOMM Workshop on*, 2010, pp. 19:1–19:6. Available: http://doi.acm.org/10.

1145/1868447.1868466

[142] N. Handigol, B. Heller, V. Jeyakumar, B. Lantz, and N. McKeown, "Reproducible Network Experiments Using Container-based Emulation," in *Emerging Networking Experiments and Technologies, International Conference on*, 2012, pp. 253–264. Available: http://doi.acm.org/10.1145/2413176.2413206

[143] M.-C. Chan, C. Chen, J.-X. Huang, T. Kuo, L.-H. Yen, and C.-C. Tseng, "OpenNet: A simulator for software-defined wireless local area network," in *Wireless Communications and Networking Conference (WCNC), IEEE*, 2014, pp. 3332–3336. Available: http://dx.doi.org/10.1109/WCNC.2014.6953088

[144] B. Pfaff, J. Pettit, T. Koponen, K. Amidon, M. Casado, and S. Shenker, "Extending networking into the virtualization layer," in *Hot Topics in Networks (HotNets), ACM SIGCOMM Workshop on*, 2009. Available: http://conferences.sigcomm.org/hotnets/2009/papers/hotnets2009-final143.pdf

[145] R. Wallner and R. Cannistra, "An SDN approach: Quality of Service using Big Switch's Floodlight Open-Source Controller," in *Asia-pacific advanced network*, 2013, vol. 35, pp. 14–19. Available: http://dx.doi.org/10.7125/APAN.35.2

[146] Julian Bunn, "Experience with the OpenDaylight Controller in a multi-vendor 1 Tbps network," Dec. 2014. Available: http://supercomputing.caltech.edu/docs/Experience_with_OpenDaylight_Controller_at_SC14.pdf

[147] S. Meier and H. Weibel, "IEEE 1588 applied in the environment of high availability LANs," in *Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), IEEE Symposium on*, 2007, pp. 100–104.

[148] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, "In-band control, queuing, and failure recovery functionalities for openflow," *IEEE Network*, vol. 30, no. 1, pp. 106–112, Jan. 2016. Available: http://dx.doi.org/10.1109/MNET.2016.7389839

[149] S. Hemminger, "Network emulation with NetEm," in *Australia's National Linux Conference (LCA)*, 2005, pp. 18–23.

[150] R. Asati, C. Pignataro, F. Calabria, and C. Olvera, "Device Reset Characterization," Internet Engineering Task Force; RFC 6201 (Informational), Mar. 2011. Available: http://www.ietf.org/rfc/rfc6201.txt

[151] S. Blair, F. Coffele, C. Booth, and G. Burt, "An Open Platform for Rapid-Prototyping Protection and Control Schemes With IEC 61850," *Power Delivery, IEEE Transactions on*, vol. 28, no. 2, pp. 1103–1110, Apr. 2013. Available: http://dx.doi.org/10.1109/TPWRD.2012.2231099

[152] W. Li and X. Zhang, "Simulation of the smart grid communications: Challenges,

techniques, and future trends," *Computers & Electrical Engineering*, vol. 40, no. 1, pp. 270–288, Jan. 2014. Available: http://dx.doi.org/10.1016/j.compeleceng.2013.11.022

[153] B. Genge, C. Siaterlis, and M. Hohenadel, "AMICI: An assessment platform for multi-domain security experimentation on critical infrastructures," in *Critical information infrastructures security*, vol. 7722, B. H&auml;mmerli, N. Kalstad Svendsen, and J. Lopez, Eds. Springer Berlin Heidelberg, 2013, pp. 228–239. Available: http://dx.doi.org/10.1007/978-3-642-41485-5_20

[154] I. Ali and S. S. Hussain, "Control and management of distribution system with integrated {ders} via {iec} 61850 based communication," *Engineering Science and Technology, an International Journal*, pp. –, 2016. Available: http://www.sciencedirect.com/science/article/pii/S2215098616307753

[155] P. Dely, A. Kassler, L. Chow, N. Bambos, N. Bayer, H. Einsiedler, C. Peylo, D. Mellado, and M. Sanchez, "A software-defined networking approach for handover management with real-time video in WLANs," *Journal of Modern Transportation*, vol. 21, no. 1, pp. 58–65, 2013. Available: http://dx.doi.org/10.1007/s40534-013-0007-x

[156] R. Bhandari, *Survivable Networks: Algorithms for Diverse Routing.* Norwell, MA, USA: Kluwer Academic Publishers, 1998.

[157] IEC TC57, *Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)*, IEC 61850-7-2. Geneva, Switzerland, 2010.

[158] V. Lai and J. Guynes, "An assessment of the influence of organizational characteristics on information technology adoption decision: a discriminative approach," *Engineering Management, IEEE Transactions on*, vol. 44, no. 2, pp. 146–157, May 1997. Available: http://dx.doi.org/10.1109/17.584923