



HAL
open science

5G-based Grid Protection, Automation, and Control: Investigation, design, and implementation

Mohand Ouamer Nait Belaid

► **To cite this version:**

Mohand Ouamer Nait Belaid. 5G-based Grid Protection, Automation, and Control: Investigation, design, and implementation. Computer science. Université Gustave Eiffel, 2023. English. NNT: 2023UEFL2040 . tel-04300505

HAL Id: tel-04300505

<https://theses.hal.science/tel-04300505>

Submitted on 22 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

5G-based Grid Protection, Automation, and Control: Investigation, design, and implementation

Thèse de doctorat de l'Université Gustave Eiffel

Ecole Doctorale : *532 - MSTIC Mathématiques, Sciences et Technologies de l'Information et de la Communication*

Spécialité de doctorat: *Informatique*

Unité de recherche : *UMR 8049 - LIGM - Laboratoire d'informatique Gaspard-Monge*

**Thèse présentée et soutenue à l'Université Gustave Eiffel,
le 25/05/2023**

Mohand Ouamer NAIT BELAID

Composition du Jury

Salah-Eddine El Ayoubi

Professeur, CentraleSupélec, France

Rapporteur

Thi-Mai-Trang Nguyen

Professeure, Université Sorbonne Paris Nord, France

Rapportrice

Philippe Martins

Professeur, Télécom ParisTech, France

Examineur et Président du jury

Mariam Ait-Ou-Kharraz

Cheffe de Projet, Enedis, France

Examinatrice

Bertrand DECOCQ

Team and Program Manager, Orange, France

Examineur

Vincent Audebert

Chercheur Expert, EDF R&D, France

Co-encadrant de thèse

Boris Deneuille

Chercheur Expert, EDF R&D, France

Co-encadrant de thèse

Rami Langar

Professeur, ÉTS-Montréal, Canada & Université Gustave Eiffel, France

Directeur de thèse

Abstract

Title: 5G-based Grid Protection, Automation, and Control: Investigation, design, and implementation.

Keywords: Smart Grid, 5G Network, PAC systems, ILP, Virtualization, Orchestration, Edge computing, Cloud Computing.

The electric system undertakes critical changes due to the accelerated deployment of distributed energy resources (DERs), as well as newly introduced innovations like ubiquitous storage (batteries, Vehicle-To-Grid V2G), distribution automation, and internet of things (IoT). The resultant grid incarnates an evolution from a blind (i.e., limited observability), static, centralized, and unidirectional system to a highly-connected, dynamic, decentralizable, and bi-directional system, simply referred to as a *smart grid*. In order to guarantee the safety of people and assets and contribute to the quality of supply, grid substations and DERs follow static protection rules that limit the evolution of the electric system. To overcome this, adaptive protection, automation, and control (PAC) mechanisms are needed, with strict requirements on communications speed and reliability. The 5G cellular network is able to tackle those issues, by massive IoT connections and mission-critical services, offering a unique opportunity to rethink the operation mode of electrical PAC mechanisms.

The present dissertation proposes a new approach to design and implement PAC systems that overcome current limitations and allow for easier DER integration with better quality of supply and flexibility. In the first part, a new approach for designing and implementing PAC systems is described. The approach is based on advancements in operational and information technologies (OT/IT) to securely collect more data from deployed electrical equipment, while complying with communication constraints. The collected data is processed at different levels to propose the best possible solution, improving grid observability and enabling better coordination between components to quickly and effectively respond to any changes (fault, asset maintenance, etc.).

In the second part of the thesis, the routing of critical PAC traffic in a 5G network is modeled, then optimized. The goal is to respect the quality of service of PAC traffic with the least impact on the energy consumption of 5G nodes and existing network traffic. The PAC traffic routing is modeled using integer linear programming (ILP), resulting in a scheme that improves different parameters.

In the final part, three experiments are built to validate the proposed architecture and demonstrate 5G effectiveness in supporting various PAC-related use cases. The first experiment validates the possibility to use dedicated protocols for electrical systems in a 5G network infrastructure. Next, the second experiment implements a complete PAC system use case, using a hardware-in-the-loop (HiL) architecture to interface real telecom and PAC system components with a simulated grid model. The third experiment constructs a comprehensive case study with real electrical and telecom networks.

Résumé

Titre: Protection, automatisation et contrôle du réseau électrique basé sur la 5G : étude, conception et mise en œuvre.

Mots clés: Smart Grid, Réseau 5G, Systèmes PAC, ILP, Virtualisation, Orchestration, Edge Computing, Cloud Computing.

Le système électrique entreprend des changements critiques en raison du déploiement accéléré des ressources énergétiques distribuées (DER), ainsi que des innovations récemment introduites comme le stockage omniprésent (batteries, Vehicle-To-Grid V2G), l'automatisation de la distribution et l'Internet des objets (IoT). Le réseau qui en résulte incarne une évolution d'un système aveugle, centralisé et unidirectionnel vers un système hautement connecté, décentralisé et bidirectionnel, simplement appelé *smart grid*. Afin de garantir la sécurité des personnes et des biens, les DER suivent des règles de protection statiques qui limitent leur intégration au système électrique. Pour surmonter cela, des mécanismes de protection adaptatifs sont nécessaires, avec des exigences strictes en matière de vitesse et de fiabilité des communications. Le réseau de télécommunications 5G est capable de résoudre ces problèmes, par des connexions IoT massives et des services critiques, offrant une opportunité unique de repenser le mode de fonctionnement des protections électriques.

La présente thèse propose une nouvelle approche pour concevoir et mettre en œuvre des systèmes de protection, d'automatisation et de contrôle (PAC) qui surmontent les limitations actuelles et permettent une intégration plus facile des DERs. Dans la première partie, une nouvelle approche pour la conception et la mise en œuvre des systèmes PAC est décrite. L'approche s'appuie sur les progrès des technologies opérationnelles et de l'information (OT/IT) pour collecter en toute sécurité davantage de données à partir des équipements électriques déployés, tout en respectant les contraintes de communication. Les données collectées sont traitées à différents niveaux pour proposer la meilleure solution possible, améliorant l'observabilité du réseau et permettant une meilleure coordination entre les composants pour répondre rapidement et efficacement à tout changement.

Dans la deuxième partie de la thèse, le routage du trafic PAC critique dans un réseau 5G est modélisé, puis optimisé. L'objectif est de respecter la qualité de service du trafic PAC avec le moins d'impact sur la consommation énergétique des nœuds 5G et le trafic réseau existant. Le routage du trafic PAC est modélisé à l'aide de la programmation linéaire en nombre entier (ILP), ce qui donne un schéma qui améliore les différents paramètres.

Dans la dernière partie, trois expériences sont construites pour valider l'architecture proposée et démontrer l'efficacité de la 5G dans la prise en charge de divers cas d'utilisation liés aux PAC. La première expérimentation valide la possibilité d'utiliser des protocoles dédiés aux réseaux électriques dans une infrastructure 5G. Ensuite, la deuxième expérience met en œuvre un cas d'utilisation complet du système PAC, en utilisant une architecture hardware-in-the-loop (HiL) pour interfacier les composants réels du système de télécommunications et PAC avec un modèle de réseau simulé. La troisième expérience construit une étude de cas complète avec de vrais réseaux électriques et télécoms.

Contents

List of Figures	11
List of Tables	12
List of Acronyms	13
1 Introduction	23
1.1 Structure of the Dissertation	26
1.2 Publications	27
2 Background on Smart Grid and 5G Network Architecture	29
2.1 Introduction	29
2.2 Electrical Power System	31
2.2.1 Transmission Grid	32
2.2.2 Distribution Grid	33
2.2.3 Distribution PAC System	33
2.2.3.1 Definition	33
2.2.3.2 Interoperability Needs for Future PAC Systems	36
2.2.4 Distributed Energy Resources	36
2.2.5 EPS Threats and Faults	38
2.2.6 EPS Protection System	39
2.2.6.1 Background on Transmission Grid Protections	40
2.2.6.2 Background on Distribution Grid Protections	40
2.2.7 Impact of DERs on Distribution PAC Systems	44
2.2.7.1 Nuisance or false tripping	44
2.2.7.2 Protection blinding	45
2.2.7.3 Fuse-saving related issues	45
2.2.7.4 Unwanted islanding	46
2.3 5G Network Ecosystem	47
2.3.1 Features	47
2.3.2 5G network architecture	52
2.3.2.1 Typical RAN topology	52
2.3.2.2 Integrated Access Backhaul (IAB) topology	52
2.3.3 5G Network Concepts	53
2.3.3.1 Network slicing	53

2.3.3.2	SDN/NFV Paradigms	55
2.3.3.3	Mobile Edge Computing (MEC)	56
2.3.3.4	Virtualization	59
2.3.3.5	Orchestration of virtual functions	61
2.4	Conclusion	63
3	5G and Distribution Grid PAC Systems	64
3.1	Introduction	64
3.2	Related Works	67
3.2.1	Trends and Evolutions of PAC systems in Smart Grids	67
3.2.2	Current Research on the Integration of 5G Technology in Smart Grids	68
3.2.3	Main Industrial Works on next-generation of PAC systems	71
3.3	Communication Requirements of Next generation PAC systems	73
3.3.1	Quantitative Requirements	73
3.3.2	Qualitative requirements	74
3.4	Communication layer categories	76
3.4.1	Local Area Network	76
3.4.2	Neighborhood/Field Area Network	77
3.4.3	Wide Area Network	77
3.5	Proposed 5G-based architecture for PAC system	79
3.6	Developed PAC application : FLISR	80
3.6.1	Comparison between conventional and automatic FLISR system	81
3.6.2	Proposed FLISR stages	83
3.6.2.1	Fault detection	83
3.6.2.2	Fault location	84
3.6.2.3	DERs tele-decoupling	84
3.6.2.4	DER link reconfiguration	84
3.6.2.5	Fault Isolation	84
3.6.2.6	Power grid reconfiguration	84
3.6.2.7	Service Restoration	84
3.6.3	Use of 5G against unwanted islanding	84
3.6.3.1	Existing remote decoupling solutions	84
3.6.3.2	Wireless communication links limitation	86
3.6.3.3	5G based Remote decoupling	87
3.6.4	Dynamic Reconfiguration of Remote Decoupling Links	88
3.7	Conclusion	90
4	FLISR Traffic Management in 5G Mobile Networks	91
4.1	Introduction	91
4.2	Typical 5G-RAN Topology	92
4.2.1	System Model	92
4.2.2	Problem Formulation	95

4.2.3	Performance Evaluation	98
4.3	5G IAB-based RAN topology	102
4.3.1	System model	102
4.3.2	Problem formulation	105
4.3.2.1	Optimal Placement of FLISR virtual functions	105
4.3.2.2	Optimal FLISR traffic routing and link scheduling	107
4.3.3	Case study	110
4.3.4	Performance Evaluation	111
4.4	Conclusion	119
5	Hardware-in-the-Loop and Field Experiments	121
5.1	Introduction	121
5.2	5G-based Remote Decoupling Mechanism Implementation	122
5.2.1	Electrical Equipment	122
5.2.2	Telecommunication Equipment	124
5.2.3	Tests and results	125
5.3	5G NSA-based FLISR Application Experiment using a Simulated Distribution Grid	128
5.3.1	Grid layer	129
5.3.1.1	Used Distribution Grid	129
5.3.1.2	Used grid equipment	131
5.3.2	Communication layer	131
5.3.3	Application layer	132
5.3.4	Implemented FLISR Scenario	135
5.3.4.1	Phase 1	135
5.3.4.2	Phase 2	137
5.3.4.3	Phase 3	137
5.3.5	Tests and results	137
5.4	5G SA-based FLISR Application Experiment using a Real Distribution Grid	139
5.4.1	Concept Grid	139
5.4.2	Experiment Architecture	140
5.4.3	5G SA Network used for Field Testing	141
5.4.3.1	5G SA Core Network	141
5.4.3.2	5G Routers	143
5.4.3.3	BBU server: Tioga Pass server	145
5.4.3.4	AW2S RRU	145
5.4.4	Implemented FLISR Scenario	146
5.4.5	Tests and results	148
5.5	Conclusion	151
6	Conclusion and Perspectives	153
6.1	Contributions	153
6.2	Perspectives	155

Conclusion and Perspectives	153
Bibliography	158
7 Appendix	172
7.1 IEC 61850 standard	172
7.2 GOOSE protocol	173
7.3 Common Information Model (CIM)	174
7.4 Electrical Equipment Used in our Experiments	175
7.4.1 ABB protection relay REF 615 N	175
7.4.2 ABB voltage protection relay REU 615 A	175
7.4.3 dSpace MicroLabBox	176
7.4.4 ControlDesk	176
7.4.5 Scheneider Flair 23DM Fault passage indicator	176
7.4.6 Opal-RT real time simulator	177
7.4.7 RT-Lab control platform	177
7.4.8 Power Amplifier	178

List of Figures

1	Les industries qui bénéficieront le plus de la 5G [11]	18
2	Technologies OT/IT utilisées	18
3	Structure de la thèse	20
1.1	Industries that are most effective from 5G [11]	25
1.2	Used OT/IT technologies	25
1.3	Structure of the dissertation	26
2.1	Enhancement of key capabilities from 4G to 5G [158]	30
2.2	Different levels of the power grid	31
2.3	Map of high voltage lines in France [44]	32
2.4	MV/LV looped architecture.	34
2.5	The smart grid conceptual model and its relevant standards [167]	37
2.6	Flow of fault current in meshed power systems	40
2.7	Example of a voltage dip extent	41
2.8	The structure of an MV feeder	41
2.9	Protection system coordination in MV power system	42
2.10	Example of remote decoupling mechanism	44
2.11	False tripping of the relay of the feeder to which the DER is connected	44
2.12	Blinding of a protection relay	45
2.13	Effect of DER on fuse-recloser coordination	46
2.14	Example of an unwanted islanding situation	47
2.15	5G Network architecture	52
2.16	5G IAB network topology [139]	53
2.17	Usage scenarios of 5G and beyond [158]	54
2.18	The importance of key capabilities in different usage scenario [158]	55
2.19	edge computing reference architecture 3.0	57
2.20	Cloud/Edge Computing Architecture mapped to PAC systems in Smart Grids based on [45, 133]	59
2.21	Generic Virtualization Architecture	60
2.22	Virtual IED concept	62
2.23	Generic system orchestration and management Architecture	62
3.1	Evolution of PAC systems based on [27]	66
3.2	Communication requirements on Smart grid applications	75
3.3	Communication categories interconnection [101, 182, 7]	76

3.4	Coverage and data rate of each communication layer category	79
3.5	Proposed architecture for 5G-base PAC system	80
3.6	Example of PAC function deployment	81
3.7	Manual FLISR process execution time	82
3.8	Automatic FLISR process execution time	83
3.9	Proposed FLISR: Functions 1-6	85
3.10	Proposed FLISR: Function 7	85
3.11	The different range/latency capabilities of various wireless communication technologies [157]	87
3.12	5G-based remote decoupling mechanism	88
3.13	Loss of a wired Remote Decoupling link	89
3.14	Migration of a wireless Remote Decoupling link	90
4.1	5G-based FLISR using FlexRAN/FlexRIC.	93
4.2	Multiplexing between eMBB and uRLLC traffic.	94
4.3	Average traffic delay for $ F = 20$	100
4.4	Average power consumption per RU for $ F = 20$	101
4.5	FLISR traffic average delay.	101
4.7	Time execution evaluation.	102
4.6	Average power consumption per RU.	102
4.8	FLISR traffic management in the 5G-IAB network using FlexRAN/FlexRIC.	103
4.9	Case of study: initial topology (i.e., $\lambda = 1$)	111
4.10	Case of study: reconfiguration after fault $F1$ (i.e., $\lambda = 2$).	112
4.11	Case of study: reconfiguration after fault $F2$ (i.e., $\lambda = 3$).	112
4.12	Case of study: initial configuration restoration (i.e., $\lambda = 4$).	113
4.13	Optimization models' interactions	113
4.14	Average power consumption per base station.	115
4.15	Average number of slots to send eMBB traffic.	115
4.16	Average delay of FLISR traffic.	116
4.17	Average delay of FLISR traffic using different placement strategies.	116
4.18	Traffic routing cost using different placement strategies.	117
4.19	Average power consumption using different placement strategies.	117
4.20	Average delay of FLISR traffic while varying the number of reconfigurations.	118
4.21	Average traffic routing cost while varying the number of reconfigurations.	119
4.22	Average power consumption while varying the number of reconfigurations.	119
5.1	Simulink-based functional scheme using RTI I/O	123
5.2	The possible values of the three-phase voltages	124
5.3	Experiment simplified architecture	124
5.4	Experiment simplified architecture with 5G network	125
5.5	Remote decoupling experiment schema	126
5.6	Targeted architecture using a distribution grid	127
5.7	GOOSE measurements	127
5.8	Ping measurements	128

5.9	Experiment global architecture	129
5.10	20kV distribution grid simulated in Simulink	130
5.11	A zoomed part of the 20kV distribution grid (Substation1)	130
5.12	Physical deployment of the grid layer	132
5.13	Physical deployment of the communication layer	133
5.14	FLISR functions deployment	134
5.15	Detailed implementation of the application layer	134
5.16	Optimization process for FLISR function deployment	135
5.17	Delay of FLISR functions	138
5.18	Average delay and standard deviation of the FLISR process	138
5.19	5G NSA test network performance	139
5.20	Presentation of the Concept Grid test facilities on the Renardières site	140
5.21	Aerial view of the location of the various structures on the Renardières site	141
5.22	Detailed architecture of the experimental grid (normal operation)	142
5.23	Detailed architecture of the experimental grid (after reconfiguration function)	142
5.24	5G network deployment	143
5.25	Used 5G routers	144
5.26	message exchange during use case process	144
5.27	BBU server specifications	145
5.28	Use case process	147
5.29	How the relay are used during different message exchange	148
5.30	Remote decoupling delays	149
7.1	IEC 61850 communication profiles [9, 95]	173
7.2	Object oriented model of IEC 61850 standard [152, 31]	175
7.3	4 Steps to Real-Time simulation using RT-Lab	178

List of Tables

- 1 Évolution des systèmes électriques traditionnels vers des systèmes intelligents[137] 17
- 1.1 Evolution from traditional grids towards smart grids [137] 24
- 2.1 Different types of faults on MV grids 38
- 2.2 Fault appearance statistics on the MV grid [137] 39
- 2.3 Wired communication technologies for the smart grid. 50
- 2.4 Wireless communication technologies for the smart grid. 51
- 2.5 Comparison between edge and cloud architectures. 58
- 3.1 Comparison between conventional, current, and future PAC systems 65
- 3.1 *Cont.* 66
- 3.2 An overview of studies investigating the potential of 5G technology in smart grids 70
- 3.3 Industrial proofs of concepts for virtualized PAC systems. 71
- 3.4 PAC application communication requirements 78
- 4.1 Simulation parameters 99
- 4.2 Optimization Strategies 100
- 4.3 Average saving (%) with respect to EWoS 100
- 4.4 Simulation parameters 114
- 4.5 Optimization Strategies 114
- 4.6 Average saving (%) with respect to EWoS 115
- 4.7 Average gain (%) when using optimal placement of FLISR virtual functions instead of random placement. 116
- 4.8 Average gain (%) when using optimal placement of FLISR virtual functions instead of random placement. 118
- 5.1 Up link communication delay of RPi2 149
- 5.2 Up link communication delay of RPi3 150
- 5.3 Down link communication delay of RPi2 150
- 5.4 Down link communication delay of RPi3 and RPi1 151

List of Acronyms

3G : Third Generation
3GPP : 3rd Generation Partnership Project
4G : Fourth Generation
5G : Fifth Generation
AI : Artificial Intelligence
API : Application Programming Interface
BBU : Base Band Unit
CB : Circuit Breaker
CIGRE : International Council on Large Electric Systems
CIM : Common Information Model
CPRI : Common Public Radio Interface
CRE : Energy Regulation Commission
CU : Centralized Unit
DC : Data Center
DER : Distributed Energy Resource
DSO : Distribution System Operator
DTT : Direct Transfer Trip
DU : Distributed Unit
E2E : End-to-End
ECP : Edge Computing Platform
eMBB : enhanced Mobile Broadband
eMBB : enhanced Mobile Broadband
ePC : Evolved Packet Core
EPRI : Electric Power Research Institute
EPS : Electric Power System
ETSI : European Telecommunications Standards Institute
FCB : Feeder Circuit Breaker
FDD : Frequency Division Duplex
FLISR : Fault Location, Isolation, and Service Restoration
FPI : Fault Passage Indicators
FWA : Fixed Wireless Access
GOOSE : Generic Object-Oriented Substation Event
GPIO : General Purpose Input/Output
HiL : Hardware in the Loop

HSS : Home Subscriber Service
HTTP : HyperText Transfer Protocol
HV : High Voltage
IaaS : Infrastructure as a Service
IAB : Integrated Access and Backhaul
IBG : Inverter-Based Generators
ICT : Information and Communication Technologies
IEC : International Electrotechnical Commission
IED : Intelligent Electronic Device
ILP : Integer Linear Programming
IoT : Internet of Things
ISG : Industry Specification Group
IT : Information Technology
LAN : Local Area Networks
LF : Linux Foundation
LoS : Line of Sight
LTE : Long Term Evolution
LV : Low Voltage
MEC : Mobile Edge Computing
MIoT : Massive IoT
mMTC : massive Machine Type Communications
MNO : Mobile Network Operators
MV : Medium Voltage
NAN/FAN : Neighborhood/Field Area Network
NFV : Network Function Virtualization
NGMN : Next Generation Mobile Network
NIST : National Institute of Standards and Technology
NR : New Radio
NSA : Non-Standalone
NSA : Non-standalone
OCP : Open Compute Project
OCR : Over Current Relays
ONF : Open Networking Foundation
OT : Operational Technology
PAC : Protection, Automation, and Control
PLC : Programmable Logic Controller
PV : Photovoltaic
QoS : Quality of Service
RAN : Radio Access Network
RAT : Radio Access Technologies
RoCoF : Rate of Change of Frequency
ROI : Return on Investment
RRU : Remote Radio Unit

RTI : Real Time Interface
SA : Stanalone
SAIDI : System Average Interruption Duration Index
SBC : Single-Board Computers
SCADA : Supervisory Control and Data Acquisition
SCP : Short Circuit Power
SD-RAN : Software-Defined Radio Access Network
SDN : Software Defined Network
SG : Smart Grid
TDD : Time Division Duplex
TSO : Transmission System Operator
UE : User Equipment
UPF : User Plane Function
uRLLC : ultra Reliable Low Latency Communication
UVRT : Under Voltage Ride Through
V2G : Vehicle to Grid
VNF : Virtual Network Function
VPR : Virtual Protection Relay
WAN : Wide Area Network

Résumé long en français

L'électricité s'est imposée comme élément essentiel de la vie moderne. Elle apporte l'énergie aux foyers, aux entreprises et aux industries [170]. Le système électrique quant à lui, en constante évolution depuis plus d'un siècle, est un ensemble complexe composé d'installations de production, de lignes électriques de différents niveaux de tension sur lesquelles les clients consommateurs sont repartis de manière irrégulière. Le maintenir en fonctionnement implique d'assurer l'équilibre entre la production et la consommation [89], mais aussi de gérer de nombreux aspects comme assurer la stabilité dynamique et la qualité de l'approvisionnement électrique, maîtriser les chutes de tension, gérer les transites de puissance réactive ou encore assurer la protection des biens et des personnes. Le système électrique doit faire face à des fluctuations de la production intermittente d'énergies renouvelables (ex. : éolien, solaire, etc.), qui peuvent affecter sa stabilité et nécessiter des mécanismes de stockage d'énergie.

Tous ces défis qui ont fait l'objet de travaux et de consensus à l'échelle internationale restent à l'ordre du jour dans le contexte de la transition énergétique mondiale qui impose de faire évoluer, voire repenser le système électrique (voir Tableau 1). En effet le système électrique traditionnel est à sens unique, l'énergie circule des centrales électriques vers les consommateurs via les systèmes de transmission et de distribution. Ce modèle qui s'est révélé efficace par le passé trouve ses limites dans les défis du XXI^e siècle, dans un monde moderne, plus dynamique et plus complexe que jamais, dans lequel le système électrique doit s'adapter à l'évolution de la demande énergétique, intégrer de nouvelles sources d'énergie ou encore répondre efficacement et rapidement aux perturbations en temps réel. A ce titre les systèmes électriques intelligents bénéficieront de technologies avancées et de réseaux de communication plus performants pour une exploitation plus efficace, fiable et durable [22]. Ceci sera soutenu par des plates-formes numériques qui intègrent la gestion des énergies renouvelables, du stockage d'énergie, des véhicules électriques et d'autres applications de système de distribution pour équilibrer la demande et l'offre d'électricité, gérer les contraintes du système et améliorer sa résilience.

Table 1: Évolution des systèmes électriques traditionnels vers des systèmes intelligents[137]

fonctionnalité	Système traditionnel	Système intelligent
Capteurs/Relais	Électromécanique	Numérique
Communication	Unidirectionnelle	Bidirectionnelle
Production	Centralisée	Centralisée et Distribuée
Nombre de capteurs	Peu	Beaucoup
Surveillance	Manuelle	Automatisée
Restauration de service	Manuelle	Utilisation du centre de contrôle et de l'auto-guérison
Protection du système	Reconfiguration Manuelle	Adaptative
Contrôle et automatisation	Minimale	Généralisée

La norme de réseau cellulaire 5G a remplacé son prédécesseur 4G en offrant des vitesses plus rapides, une latence nettement inférieure et une plus grande capacité à prendre en charge le nombre croissant d'appareils numériques tels que les smartphones, les tablettes et les appareils IoT, sans risque de saturation du réseau [71, 36]. Si les offres 5G peuvent être accessibles au grand public, leur objectif premier est de servir les utilisateurs industriels. Pour le grand public, la 5G promet une connexion plus rapide qui peut sembler inutile vu le débit du réseau 4G. Mais ce dernier approche de la saturation dans les régions surpeuplées, ce qui signifie que la 5G peut permettre de désengorger la 4G. De plus, la 5G pourrait devenir une alternative à la fibre optique dans les zones moins denses, au bénéfice des foyers les plus isolés[110].

En tirant parti du potentiel de la 5G, les utilisateurs industriels peuvent créer de nouveaux services et améliorer les existants [171, 55]. L'un des avantages les plus importants concerne la logistique, où la 5G permet un suivi et une optimisation en temps réel du transport et de la livraison des marchandises. De plus, la flexibilité accrue offerte par les réseaux 5G permet une organisation de l'usine plus efficace et plus agile, améliorant ainsi la productivité. Le réseau 5G stable fournit également une base solide pour le développement de voitures autonomes et de nouveaux services de transport à l'avenir. De plus, dans le secteur de la santé, le fait de pouvoir connecter plus d'objets sur un réseau plus résilient, avec une latence divisée par dix, devrait favoriser le développement du suivi à distance des patients, pour mieux gérer les hospitalisations à domicile, la prévention contre les maladies, etc. La 5G peut également être utilisée pour piloter des drones, afin que les services de secours puissent les utiliser pour la prévention et pour soutenir les opérations de secours. La figure 1 met en évidence les secteurs qui bénéficieront le plus de la 5G.

Le réseau 5G devrait apporter des améliorations significatives aux systèmes électriques, notamment dans les domaines des systèmes de protection, d'automatisation et de contrôle

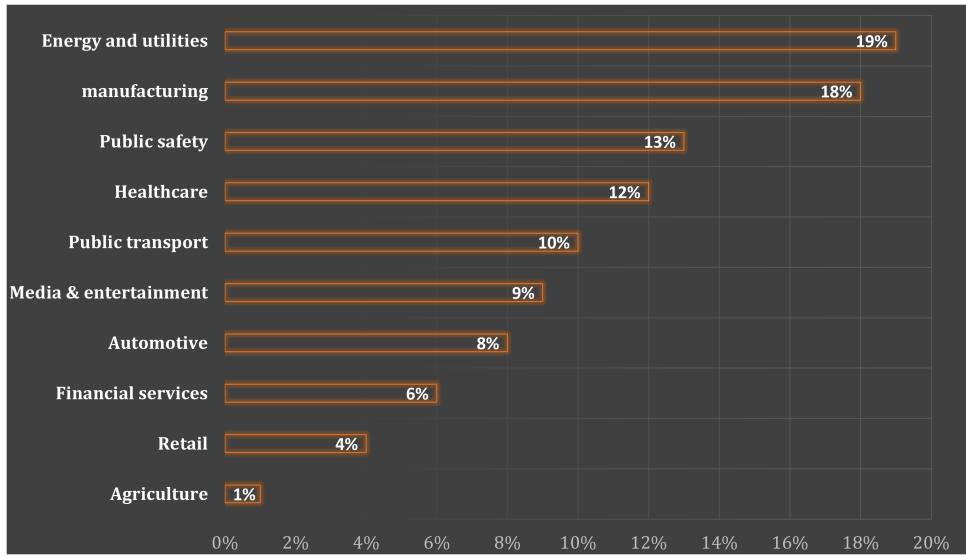


Figure 1: Les industries qui bénéficieront le plus de la 5G [11]

[33]. Par exemple, les relais de protection peuvent détecter et isoler les défauts en temps réel, tandis que les systèmes d'automatisation peuvent réagir rapidement aux conditions changeantes du système électrique. Les travaux universitaires et industriels existants indiquent que les propriétés souhaitées des futurs systèmes PAC (Protection, Automation, and Control) sont la flexibilité, la portabilité, la résilience et l'interopérabilité. Une tendance typique consiste à améliorer l'efficacité opérationnelle des futurs systèmes d'alimentation en intégrant les meilleures pratiques de mise en œuvre du monde IT (Figure 2), telles que l'informatique de pointe, la virtualisation et l'orchestration.

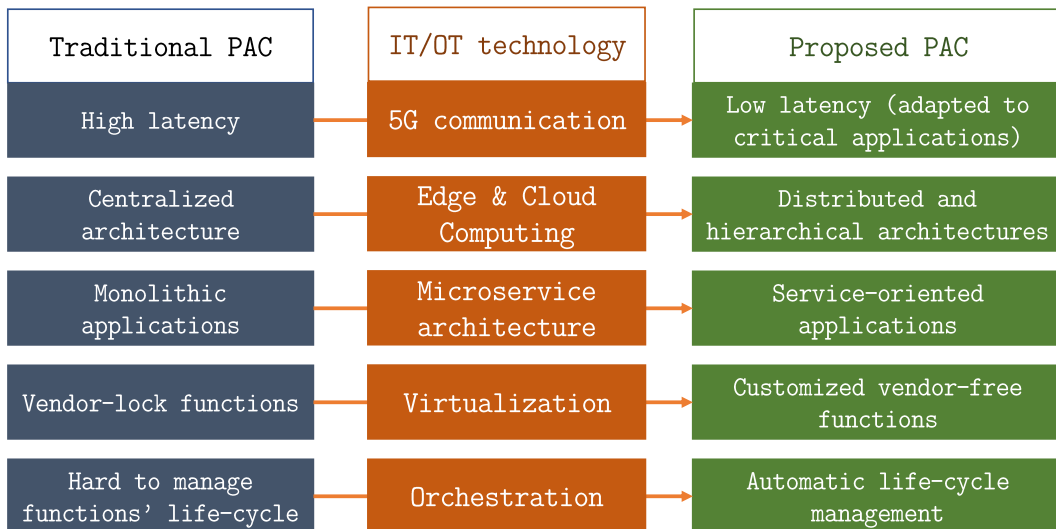


Figure 2: Technologies OT/IT utilisées

Le travail proposé présente une architecture de communication polyvalente qui exploite les capacités de la technologie 5G, de l'informatique de pointe et de la virtualisation pour fournir des services de communication sur mesure qui répondent à un large éventail d'exigences de performances exigées par diverses applications de système PAC.

Notre travail présente une nouvelle approche pour la conception de systèmes PAC

utilisant une architecture orientée données. L'objectif de cette approche est d'exploiter les capacités du réseau 5G pour collecter efficacement des données en temps réel. Des fonctions virtuelles sont déployées à différents niveaux du réseau de communication pour traiter les données et prendre des décisions optimisées. L'approche proposée répond aux limites des systèmes PAC actuels et fournit une solution efficace qui améliore les performances globales du système électrique. Nous proposons une architecture qui tire parti de l'informatique de périphérie [149] pour permettre le traitement local des données à proximité des équipements de réseau intelligent, améliorant ainsi la latence, la fiabilité et la sécurité. De plus, nous utilisons le concept de virtualisation pour créer des fonctions PAC indépendantes du matériel et du fournisseur [17]. Pour assurer la gestion du cycle de vie des fonctions virtuelles, nous avons utilisé l'orchestration, qui permet un déploiement et une manipulation efficaces de nos fonctions PAC [119].

Pour valider l'architecture proposée, nous avons mené à la fois des expérimentations hardware-in-the-loop (HiL) et sur le terrain, qui ont confirmé la capacité d'un réseau 5G à prendre en charge la communication critique d'un système PAC. Nos résultats démontrent le potentiel de notre approche pour améliorer les performances et la fiabilité des systèmes PAC.

Pour réduire l'impact du trafic critique PAC sur les flux existant dans le réseau 5G et réduire la consommation d'énergie dans les nœuds radio, nous avons conçu deux problèmes d'optimisation pour différents types de topologies de réseau 5G, à savoir la topologie typique avec une antenne gNB et la topologie avec un Backhaul sans-fil en utilisant plusieurs relais sans-fil de type Integrated Access and Backhaul (IABs). Notre objectif est de minimiser la consommation électrique des nœuds 5G alimentés par le système de distribution tout en assurant une acceptation optimale du trafic existant et en répondant aux exigences du trafic PAC critique. Nous avons adopté une approche de modélisation linéaire et formulé des fonctions d'objectif paramétrées pour obtenir un compromis optimal.

Structure de la thèse

Cette thèse est composée de six chapitres excluant cette introduction telle que présentée ci-dessous. La structure de la thèse est présentée dans la figure 3.

Le Chapitre 2 offre un aperçu complet des systèmes électriques et de leurs composants, essentiellement en lien avec les systèmes PAC. Ce chapitre se penche sur le fonctionnement des systèmes de protection électriques et identifie leurs limites. En explorant l'intégration de concepts IT/OT innovants, ce chapitre met en évidence le potentiel d'évolution des systèmes de protection électrique. De plus, il présente le réseau 5G et définit des concepts clés tels que l'Edge Computing, la virtualisation et l'orchestration, qui peuvent considérablement améliorer le fonctionnement des systèmes PAC.

Le Chapitre 3 présente le potentiel de la technologie 5G en tant qu'infrastructure de communication pour les applications PAC avancées. Ensuite, divers travaux académiques et industriels sur l'utilisation des technologies OT/IT pour les futurs systèmes PAC sont discutés. En outre, nous présentons un exemple de cas d'utilisation réel d'une applica-

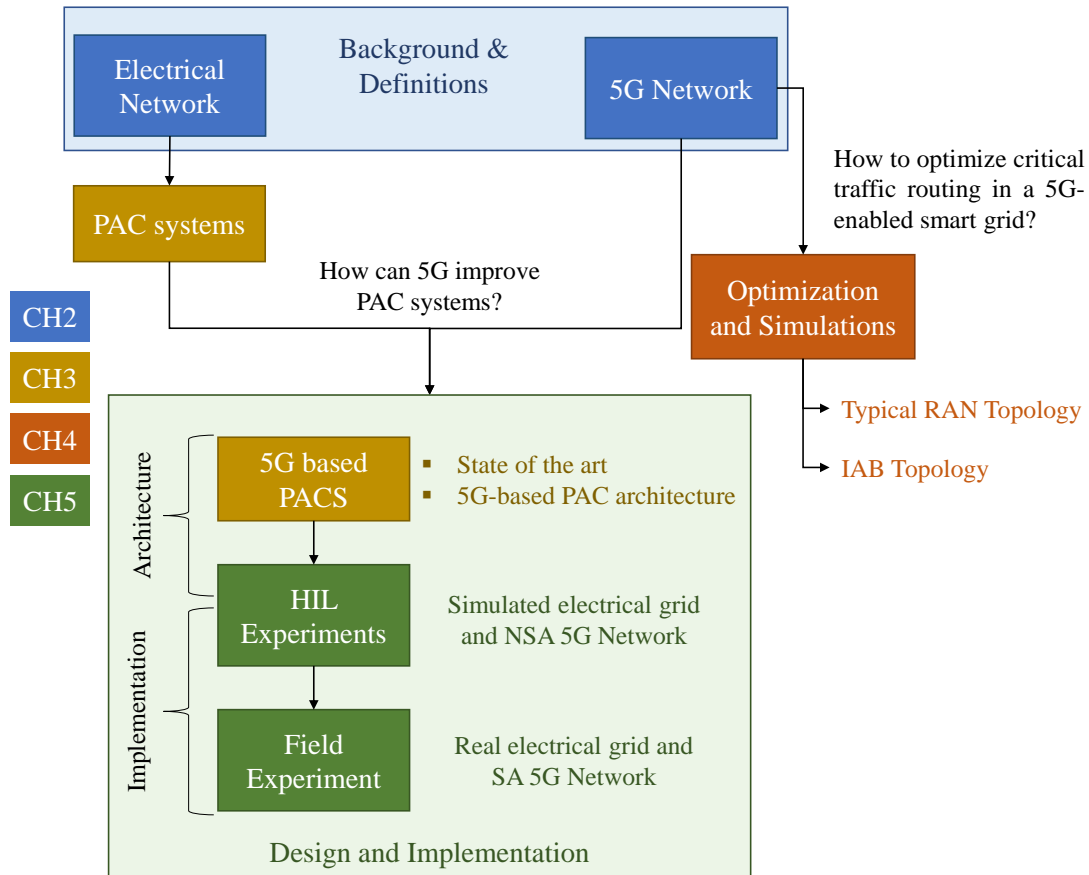


Figure 3: Structure de la thèse

tion PAC pour montrer comment l’exploitation de l’écosystème 5G peut améliorer les performances des schémas FLISR (Fault Location, Isolation, and Service Restoration) traditionnels. L’étude de cas donne un aperçu des implications pratiques des systèmes PAC basés sur la technologie 5G et met en évidence les avantages de cette approche par rapport à l’infrastructure de communication traditionnelle.

Le Chapitre 4 introduit de nouvelles architectures d’applications FLISR basées sur différentes topologies de réseau 5G et améliore la gestion du trafic en formulant des problèmes d’optimisation. Ces derniers sont conçus pour minimiser la consommation d’énergie des noeuds 5G, maximiser l’acceptation du trafic haut débit et répondre aux exigences de communication du trafic FLISR. Pour parvenir à un compromis optimal, notre approche consiste à développer des modèles linéaires et des fonctions objectives paramétrables.

Le Chapitre 5 commence par présenter la mise en œuvre réussie d’un mécanisme de découplage à distance, qui exploite pleinement le potentiel du réseau 5G pour améliorer la fiabilité et la sécurité du système de distribution. Ce mécanisme protège efficacement le système électrique contre les îlotages involontaires. Ensuite, nous mettons en évidence le potentiel d’un prototype FLISR basé sur la 5G utilisant une architecture HiL, qui facilite l’intégration transparente du matériel de protection réel dans un environnement de simulation. Les fonctions virtuelles du FLISR ont été développées à l’aide d’outils open source et basées sur une architecture de microservices, ce qui améliore la flexibilité du système

et réduit les dépendances vis-à-vis des fournisseurs de matériel/logiciel. Finalement, nous décrivons une expérimentation sur le terrain qui reproduit le processus FLISR mis en œuvre en utilisant un réseau 5G autonome (Standalone - SA) et un système de distribution réel. L'objectif est de vérifier l'efficacité d'un système FLISR basé sur un réseau 5G SA pour gérer un système électrique avec des ressources énergétiques distribuées. Les résultats obtenus démontrent que les exigences techniques pour l'application FLISR sont satisfaites. Les connaissances acquises peuvent contribuer au développement de systèmes de gestion de l'énergie basés sur la 5G plus efficaces et plus durables à l'avenir.

Dans le **Chapitre 6**, nous présentons les conclusions de nos travaux et proposons des orientations et des perspectives pour les futurs systèmes PAC basés sur un réseau 5G.

Publications

Les travaux de cette thèse ont donné lieu aux publications suivantes :

Journaux publiés

- Kabbara, N.*, Nait Belaid, M. O.*, Gibescu, M., Camargo, L. R., Cantenot, J., Coste, T., ... & Morais, H. (2022). Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges. *Energies*, 15(24), 9362.

Conférences internationales

- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar, "5G-Based Fault location, Isolation, and Service Recovery: Field experiment." 27th International Conference on Electricity Distribution (CIRED), Rome, Italy, Jun. 2023.
- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar "SD-RAN based Approach for Smart Grid Critical Traffic Routing and Scheduling in 5G Mobile Networks.", IEEE Global Communications Conference (IEEE GLOBECOM 2022), Rio-de-Janeiro, Brazil, Dec. 2022.
- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar, "Smart grid critical traffic routing and link scheduling in 5G IAB networks." IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2022), Singapore, Oct. 2022.
- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar, "Defining an MV/LV Protection, Automation, and Control system based on 5G network." CI-GRE 2022.
- M.O. Nait Belaid*, V. Audebert, V. Costan, and B. Deneuille, "Defining a Wide Area Protection System Using 5G Communication Technology." GCC CIGRE 2021.

- M.O. Nait Belaid*, V. Audebert, and B. Deneuille, "Designing a 5G Based Smart Distribution Grid Protection System." CIRED 2021: 1241-1245.

Il convient de mentionner que j'ai passé trois mois pendant ma thèse de doctorat au laboratoire MOSAIC [103] à l'Université d'Aalto en Finlande, dirigé par le professeur Tarik Taleb. La visite m'a donné accès à une communauté de chercheurs travaillant dans les domaines de l'optimisation linéaire et des réseaux mobiles, me permettant de bénéficier de leur expertise et d'approfondir mes propres connaissances.

Chapter 1

Introduction

Electricity is essential for modern life, powering homes, businesses, and industries [170] to establish an unprecedented welfare. The Electric Power System (EPS) has been around for over a century and has undergone significant changes over the years. The EPS comprises a complex set of production plants, electrical lines of different voltage levels, and irregularly distributed customers. Production must be constantly balanced with consumption to ensure stability and quality of supply [89]. This involves electrical constraints such as voltage drop, reactive power management, and protection against short-circuits. In addition, the electrical system is subject to fluctuations in intermittent renewable energy production (e.g. wind, solar energy, etc.), which can impact EPS stability and require energy storage mechanisms. Besides, adapted response and mitigation is required as the demand evolves constantly and unforeseen disruptions, like power outages or extreme weather conditions, threaten the grid. Effective monitoring and management of the electrical system are therefore essential to ensure a reliable and stable energy supply for end-users.

All these challenges are addressed in the context of ongoing efforts for a global energy transition, which imposed rethinking the electrical grid (see Table 1.1). The traditional electrical grid is a one-way system, where power flows from centralized power plants to consumers through transmission and distribution grids. This model has served well, but is no longer sufficient to meet the challenges of the 21st century. The modern world is more dynamic and complex than ever before, thus the need for an intelligent electrical system that can adapt to changing energy demands, integrate new energy sources, and respond to disruptions in real-time. The smart grid benefits from advanced technologies and communication networks for a more efficient, reliable, and sustainable energy supply [22]. This is empowered by a digital platform that integrates renewables, energy storage, electric vehicles, and other distribution grid applications to balance power demand and supply, reduce carbon emissions, and improve grid resilience.

Table 1.1: Evolution from traditional grids towards smart grids [137]

Feature	Traditional grid	Smart grid
Sensors/Relays	Electromechanical	Digital
Communication	Unidirectional	Bidirectional
Generation	Centralized	Centralized and Distributed
Number of sensors	Small	High
Monitoring	Manual	Automated
Service restoration	Manual and use a control center	Self-healing
Protection system	Manual reconfiguration	Adaptive
Control and automation	Minimal	widespread

The 5G cellular network standard is superseding its predecessor, 4G, by offering much more speed, significantly lower latency, and greater capacity to support the growing number of digital devices (smartphones, tablets, and IoT devices) without the risk of network saturation [71, 36]. For the general public, 5G promises a faster connection, which may seem unnecessary given existing speeds, but turns out to solve the congestion in dense regions, unclogging 4G. Moreover, 5G is an alternative to cumbersome and expensive deployments of fiber in remote areas, benefiting the most isolated homes [110]. Yet, 5G addresses primarily industrial users despite being available to the general public.

By leveraging the potential of 5G, industrial users can unlock endless possibilities to create new services and enhance existing ones [171, 55]. Logistics is amongst the prominent applications where 5G enables real-time monitoring and optimization of the transport and delivery of goods. Additionally, the increased network flexibility allows for more efficient and agile factory organization that improves productivity. Looking ahead, the stable 5G network provides a robust foundation for the development of autonomous cars and new transport services in the future. The health sector takes advantage of 5G-enabled massive connection of objects in a more resilient network, with a latency divided by ten, to encourage remote follow-up of patients, distant critical surgeries, adapted hospitalizations, disease prevention, etc. The 5G can also be used to pilot drones, adopted by emergency services for prevention and to support rescue operations. Figure 1.1 highlights sectors that stand to benefit the most from 5G.

The 5G network is expected to bring significant improvements to the electrical EPS as well, particularly in the areas of protection, automation, and control systems [33]. For instance, protection relays can detect and isolate faults in real-time, while automation systems can respond quickly to changing EPS conditions. Existing academic and industrial works indicate that the desired properties of future PAC (Protection, Automation, and Control) systems are flexibility, portability, resilience, and interoperability. A typical trend is to enhance the operational efficiency of future power systems by incorporating novel paradigms from the IT world (Figure 1.2, such as edge computing, virtualization, and orchestration).

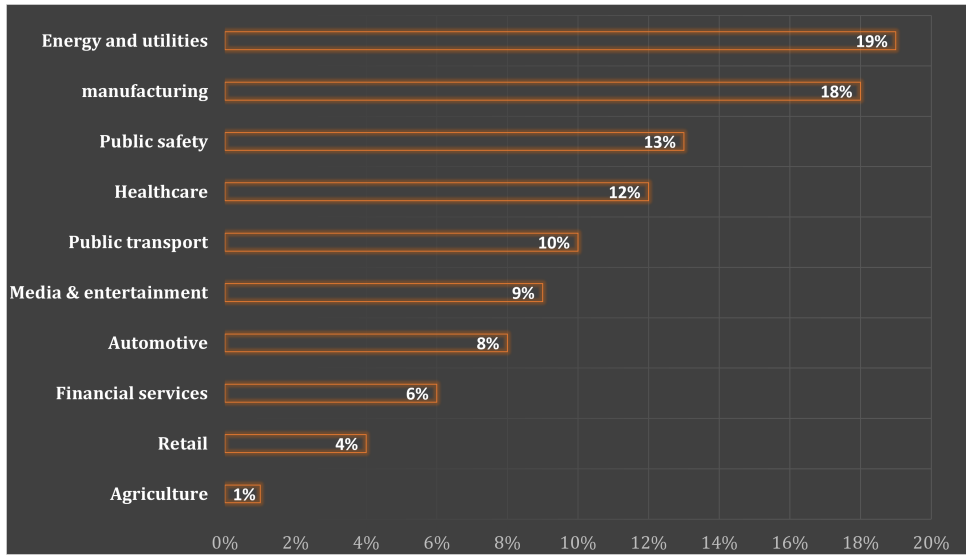


Figure 1.1: Industries that are most effective from 5G [11]

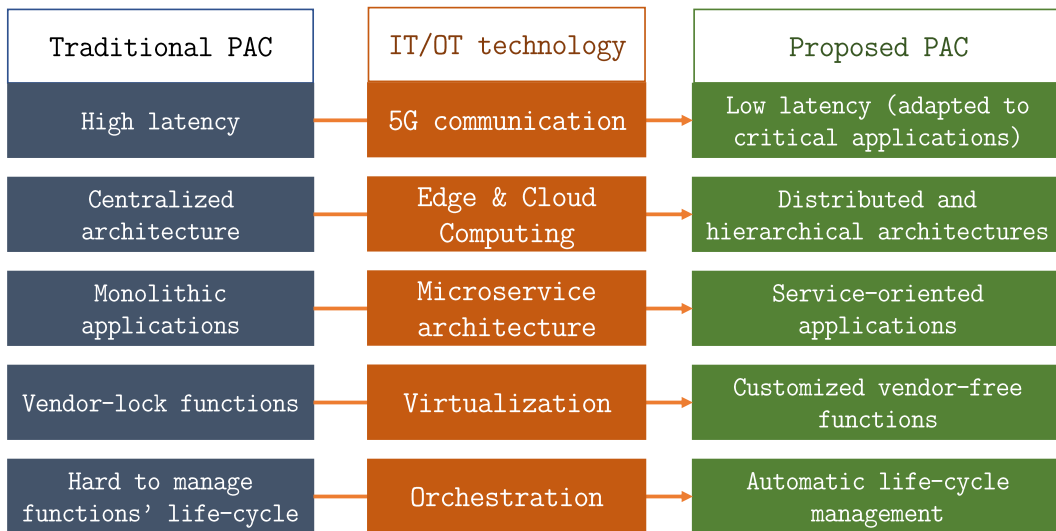


Figure 1.2: Used OT/IT technologies

The proposed work presents a versatile communication architecture that leverages 5G technology, edge computing, and virtualization capabilities to deliver tailor-made communication services that meet a wide range of performance requirements demanded by various PAC system applications.

A novel approach is presented for the design of PAC systems by shifting the focus towards a data-oriented PAC application. The limitations of current PAC systems are addressed to offer an effective solution that enhances the overall system performance. The objective is to exploit the capabilities of the 5G network to efficiently collect data at real-time. The architecture also leverages edge computing [149] to enable local data processing near smart grid equipments, enhancing latency, reliability, and security. In addition, we employ the virtualization concept to create agnostic PAC functions that are independent of hardware and providers [17]. Virtual functions are deployed at different levels of the communication network to process data and take optimized decisions. Orchestration is utilized to ensure the life-cycle management of the virtual functions, which enables an

efficient deployment and manipulation of our PAC functions [119].

To validate our proposed architecture, we conducted both hardware-in-the-loop (HiL) and field experiments, which confirmed the ability of a 5G network to support critical communications of a PAC system. The findings demonstrate the potential of our approach to enhance the performance and reliability of PAC systems.

To reduce the impact of PAC critical traffic on existing flows in the 5G network and lower energy consumption in radio nodes, we devised two optimization problems for different types of 5G network topologies, namely a typical one using gNBs for the 5G radio access network (RAN), and a topology with a wireless backhaul using integrated access and backhaul (IAB) nodes. Our objective is to minimize the power consumption of 5G nodes supplied by the distribution grid, while ensuring optimal acceptance of existing traffic, and meeting the demands of critical PAC traffic. We adopted a linear modeling approach and formulated parameterized objective functions to achieve an optimal trade-off.

1.1 Structure of the Dissertation

The dissertation spans over six chapters as summarized in Figure 1.3 and presented thereafter.

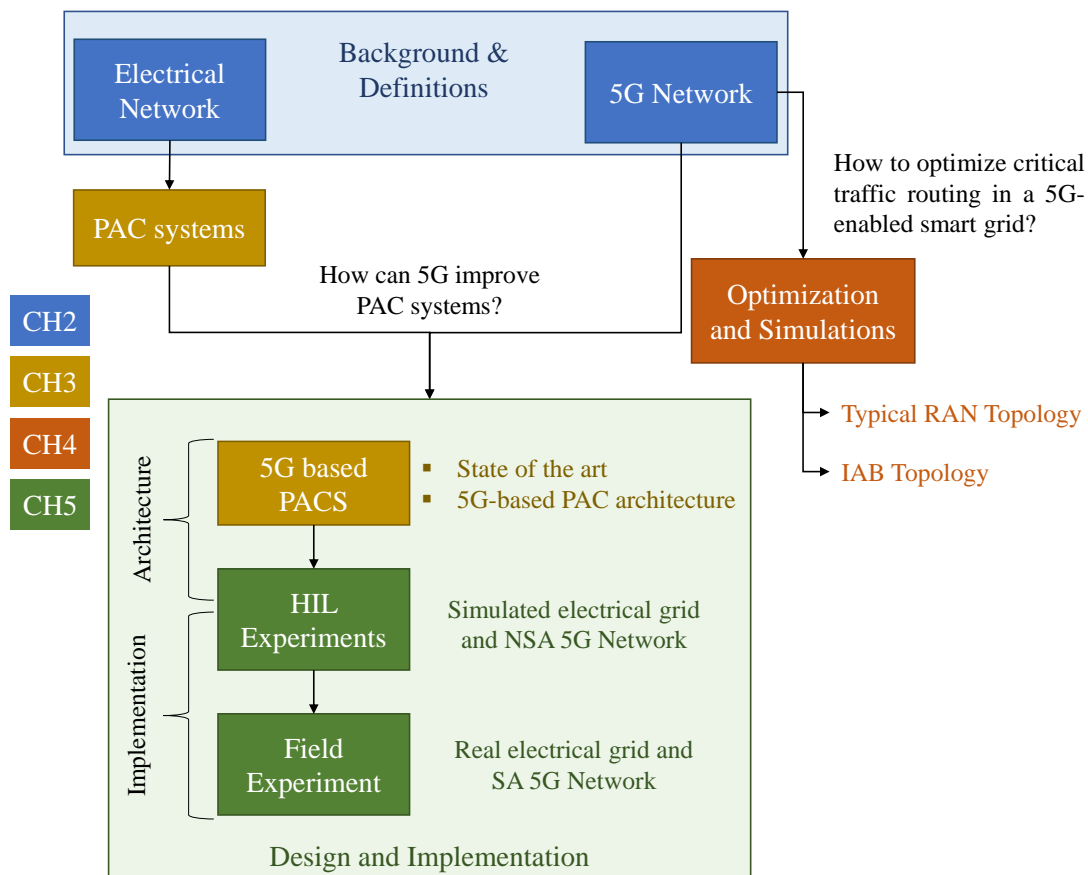


Figure 1.3: Structure of the dissertation

Chapter 2 offers a comprehensive overview of electrical systems and their compo-

nents, with a specific focus on PAC systems. This chapter delves into the nuances of power protection systems and identifies their existing limitations. The potential evolution of PAC systems are highlighted by exploring the integration of innovative OT/IT concepts. The chapter also introduces the 5G network and defines crucial concepts such as Edge Computing, Virtualization, Orchestration, and Network Slicing, which can significantly enhance the capabilities of PAC systems.

Chapter 3 demonstrates the potential of 5G technology as a communication infrastructure for advanced PAC applications. Then, various academic and industrial contributions on using OT/IT technologies for future PAC systems are discussed. A real example of a PAC application is presented to showcase how leveraging the 5G ecosystem can improve the performance of traditional fault location, isolation, and service restoration (FLISR) schemes. The case study provides insights into the practical implications of 5G-enabled PAC systems and highlights the benefits of this approach over traditional communication infrastructure.

Chapter 4 introduces new FLISR system architectures based on different 5G network topologies and addresses the challenge of flow control optimization in a multi-service scenario consisting of two services with heterogeneous requirements: enhanced mobile broadband (eMBB) and ultra-reliable low-latency communication (URLLC). The optimization problems are designed to minimize energy consumption, maximize eMBB traffic acceptance, and meet communication requirements for FLISR traffic, which is modeled as a URLLC service. Linear models with parameterized objective functions are developed to achieve the optimal trade-off.

Chapter 5 first demonstrates the successful implementation of a remote decoupling mechanism, harnessing the full potential of the 5G network for reliability and security of the distribution system and protection against unwanted islanding. Then, we highlight the potential of a 5G-based FLISR prototype utilizing HiL architecture, which facilitates the seamless integration of real protection hardware into a simulated environment. The FLISR virtual functions were developed using open-source tools and based on a micro-service architecture, which improves the flexibility of the system and reduces dependencies on hardware/software providers. Finally, we present a field experiment that replicates the implemented FLISR application using a standalone (SA) 5G network and a physical distribution grid. The goal is to verify the effectiveness of using FLISR system based on 5G SA network to manage an electrical network with DERs. Results demonstrate that the technical requirements for FLISR application are satisfied. Ultimately, the knowledge gained from this experiment pose a foundation for more efficient and sustainable 5G-based PAC systems in the future.

In **Chapter 6**, we draw conclusions from our work and offer insights into future directions for 5G-based PAC systems.

1.2 Publications

The work of this thesis has resulted in the following publications:

Published Journal Papers

- Kabbara, N.*, Nait Belaid, M. O.*, Gibescu, M., Camargo, L. R., Cantenot, J., Coste, T., ... & Morais, H. (2022). Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges. *Energies*, 15(24), 9362.

Conference Papers

- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar, "5G-Based Fault location, Isolation, and Service Recovery: Field experiment." 27th International Conference on Electricity Distribution (CIRED), Rome, Italy, Jun. 2023.
- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar "SD-RAN based Approach for Smart Grid Critical Traffic Routing and Scheduling in 5G Mobile Networks.", IEEE Global Communications Conference (IEEE GLOBECOM 2022), Rio-de-Janeiro, Brazil, Dec. 2022.
- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar, "Smart grid critical traffic routing and link scheduling in 5G IAB networks." IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2022), Singapore, Oct. 2022.
- M.O. Nait Belaid*, V. Audebert, B. Deneuille, and R. Langar, "Defining an MV/LV Protection, Automation, and Control system based on 5G network." CIGRE 2022.
- M.O. Nait Belaid*, V. Audebert, V. Costan, and B. Deneuille, "Defining a Wide Area Protection System Using 5G Communication Technology." GCC CIGRE 2021.
- M.O. Nait Belaid*, V. Audebert, and B. Deneuille, "Designing a 5G Based Smart Distribution Grid Protection System." CIRED 2021: 1241-1245.

It is worth mentioning that I spent three months during my PhD studies at MOSAIC lab [103] at Aalto University in Finland, headed by Professor Tarik Taleb. The visit provided me with access to a community of researchers working in the fields of linear optimization and mobile networks, allowing me to benefit from their expertise and deepen my own knowledge.

Chapter 2

Background on Smart Grid and 5G Network Architecture

2.1 Introduction

The smart grid is a complex system that includes a range of technologies and infrastructure components with the aim of optimizing system operations, reducing costs, improving the quality of supply and maximizing the integration of renewable energies. Advanced sensors and monitoring systems gather data on electricity supply, demand, and grid performance. This data is analyzed and processed using advanced algorithms to optimize energy distribution and management.

One of the key features of the smart grid is the ability to manage and control energy flows in real-time. This is achieved through the use of advanced automation and communication technologies, which can further detect power outages and reroute power flows to minimize disruptions. The smart grid can also integrate renewable energy sources, such as wind and solar generation, and manage their intermittency to ensure a stable and reliable energy supply.

Another key feature of the smart grid is the ability to enable demand response, a mechanism that incentivizes customers to adjust their electricity consumption during times of high demand or low supply, with the ultimate goal of stabilizing the generation and consumption balance, reducing strain on power system structures, and optimizing energy flow management. This can be achieved through price signals, which encourage consumers to shift their electricity use to off-peak hours, when energy is less expensive. Finally, Smart grids aim to enhance the quality of power supply by implementing mechanisms such as self-healing and by enabling grid operations in island mode

5G technology has the potential to revolutionize the operation of smart grids. Firstly, 5G technology can help enhance the communication infrastructure of smart grids. With the high throughput and low latency of 5G, communication between smart devices and PAC (Protection, Automation, and Control) systems can be more efficient and reliable. This can enable faster and more accurate data exchange, which leads to improved fault detection and response of smart grid protection systems, allowing utilities to react immediately and prevent potential power outages.

Secondly, 5G can enhance the situational awareness of PAC systems by leveraging advanced analytics and machine learning algorithms. 5G-enabled PAC systems can quickly analyze vast amounts of data from sensors and devices, providing utilities with real-time insights into the health of the grid.

Furthermore, 5G technology can facilitate the integration of renewable energy sources into smart grids by enabling real-time management of their variability. With the use of advanced algorithms and predictive analytics, 5G-enabled smart grids can accurately forecast energy generation and consumption, leading to optimized energy storage and distribution.

To provide advanced performance, the 5G technology is based on 8 technical requirements:

- Up to 10 Gbit/s data rate, 10 to 100 times more than 4G networks
- 1 millisecond latency
- 1,000 times more bandwidth per unit area
- Up to 100 times more connected devices per unit area (compared to 4G LTE)
- 99.999% uptime
- 100% coverage
- 90% reduction in network energy consumption
- Up to 10 years of battery life for low-power IoT devices

The key capabilities of 5G network are shown in Figure 2.1, compared with those of 4G.

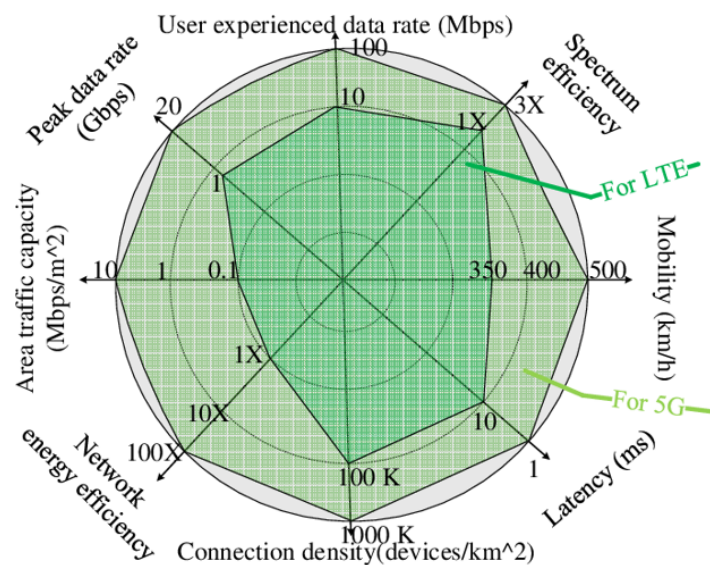


Figure 2.1: Enhancement of key capabilities from 4G to 5G [158]

This chapter is divided into two parts. In the first part, we provide an overview of the components that make up the electrical grid, with a focus on PAC systems. We begin

by introducing the transmission and distribution grid in Sections 2.2.1 and 2.2.2. Then we discuss the threats that surround the EPS and the faults they can cause in Section 2.2.5. We place a greater emphasis on the protection system in Section 2.2.6, as it plays a crucial role in ensuring the safe and efficient operation of power grids. We then introduce distribution PAC systems in Section 2.2.3, followed by a definition of distributed energy resources in Section 2.2.4 and their impact on distribution PAC systems in Section 2.2.7.

In the second part of this chapter, we focus on the main features and potential applications of the 5G network in the electrical grid. We begin by introducing the principal features and performances of the 5G network in Section 2.3.1. We then delve deeper into the key concepts of the 5G ecosystem, including virtualization, SDN/NFV, edge/cloud computing, orchestration, and network slicing, and their potential applications in the electrical grid in Section 2.3.3. Finally, we introduce two different 5G network topologies in Section 2.3.2: a typical one using gNBs for the 5G RAN and a topology with a wireless backhaul using IAB nodes.

2.2 Electrical Power System

In power systems, several voltage levels are defined that correspond to different stages. In France, large production plants typically generate electricity at voltage levels of approximately 15 to 25 kV, which then undergo multiple voltage transformations before reaching customers. The power travels first through the transmission system at 400 kV, classified as high voltage (HV), before transiting by intermediate levels of 225 kV, 90 kV, and 63 kV (also HV). Finally, the voltage is lowered to 15 kV/20 kV on the medium voltage (MV) distribution system before reaching the customers at 220 V/400 V on the low voltage (LV) distribution grid. Figure 2.2 provides a visual representation of the various voltage levels in the power grid.

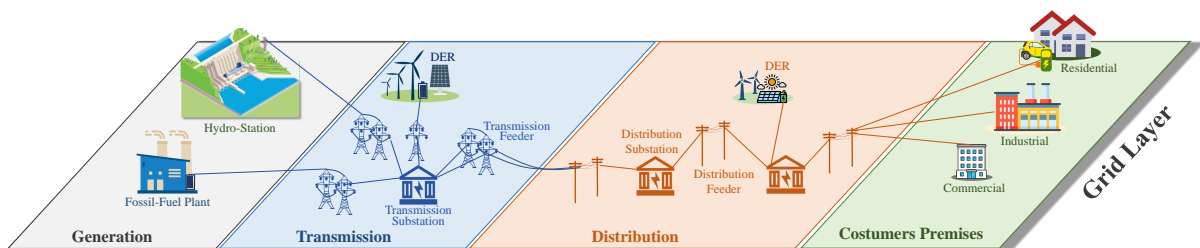


Figure 2.2: Different levels of the power grid

The use of high voltages limit voltage drops along the power lines, extending the range of electricity transmission. In addition, they allow an efficient energy transmission with minimal losses attributed to the *Joule* effect, which are directly proportional to the square of the effective current. Thus, by increasing the voltage level, the current decreases, resulting in reduced losses, even with the same power injection. We have:

- Voltage Drop: $V_d = I \times (R + jX)$, where I is the current flowing through the power line, R is the resistance of the power line, and X is the reactance.

- Joule Effect Losses: $P_j = I^2 \times R$, where P_j is the energy lost due to the Joule effect, I is the current flowing through the power line, and R is the resistance of the power line.

Based on these equations, it can be seen that increasing the voltage (V) will lead to a decrease in current (I) since the apparent power (S), defined by $S = P + jQ$ with active power P and reactive power Q , remains constant ($S = V \times I^*$). Therefore, increasing voltage reduces both voltage drop (V_d) and Joule effect losses (P_j) which are, respectively, proportional to the current (I) and its square (I^2). Thus, higher voltage levels are essential to efficiently transmit electrical energy over longer distances while minimizing energy losses.

2.2.1 Transmission Grid

The transmission system (between 63 kV and 400 kV) is operated, in France, by RTE as a meshed system, i.e. a node can be supplied via several lines; which has the advantage of maintaining an excellent quality of service even when a component is lost. The metropolitan transmission system represents approximately 100,000 km of power lines. Figure 2.3 presents a visual of the transmission system lines in France.



Figure 2.3: Map of high voltage lines in France [44]

In Europe, the power transmission grids are interconnected, which promotes energy

exchanges and mutual assistance in the event of an incident. This interconnection also enables the pooling of frequency adjustment resources, as it is more cost-effective for large electrical systems to maintain a frequency close to their set-point by sharing adjustment resources. In order to ensure continuous power supply, power transmission system operators must maintain an adequate amount of immediately available reserve power, typically generated by part-load or standby plants, that can quickly replace any lost electricity production.

However, the growth of interconnections has also brought new challenges, such as the need to harmonize regulations and technical standards across different countries and ensure proper management of cyber security risks. To address these challenges, policy makers and stakeholders are actively working to develop new frameworks and solutions that can enable the continued growth of interconnections while maintaining high levels of safety, reliability, and efficiency.

2.2.2 Distribution Grid

Enedis is the dominant operator in mainland France, managing nearly 95% of the public distribution system, whereas the remaining 5% is handled by local distribution companies. Enedis is responsible for a vast distribution grid of 1.4 million kilometers of lines, serving more than 36 million customers and over 536524 distributed production sites. To guarantee reliable energy distribution, Enedis operates an extensive infrastructure of 943000 secondary substations (MV/LV transformers) and 2,785 primary substations (HV/MV and MV/MV transformers), according to 2022 statistics [48].

The French distribution system operates radially despite being a meshed system (Figure 2.4). Under normal conditions, some switches are kept open to avoid loops as a preventive measure against wide failure propagation. Each sub-graph linked to a primary substation has a tree-like structure and is referred to as a *feeder*. The whole grid is then a spanning forest of multi-feeder trees rooted at primary substations. In the event of an incident, specific switches may be closed while others are opened to maintain radial operation. This reconfiguration effectively isolates the fault while ensuring that as many clients as possible are supplied. Another important reason for adopting this mode of exploitation is the relative simplicity of the protection system compared to meshed systems, where fault localization is more challenging. It is noteworthy that Enedis can loop its grid for brief periods to transfer part of the MV system from one substation to another.

2.2.3 Distribution PAC System

2.2.3.1 Definition

As power systems evolve, introducing novel PAC systems for improved support of operations becomes a necessity [14]. In this work, we formally define PAC systems as a cohesive set of power system functionalities that help protect, automate, and control the power grid across spanning field, process, and operational areas. PAC systems are based on three main components spread all over the power grid [30]: i) Functions located as

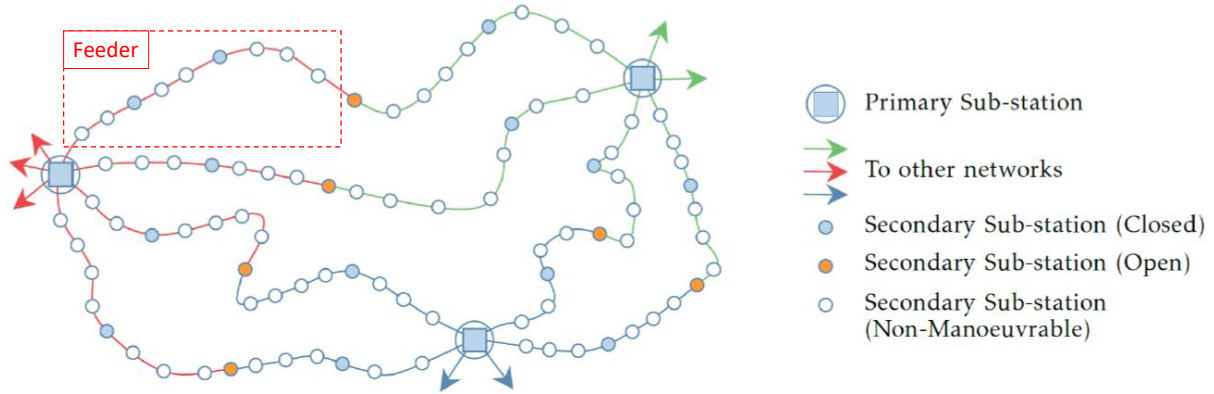


Figure 2.4: MV/LV looped architecture.

close as possible to the monitored structures (e.g., line or transformer protections); ii) Coordinated actions by local automation/control software (e.g., in electrical substations or DER plants); iii) Optimization by the grid operator control center (e.g., set of monitoring software, SCADA, management systems, energy markets) requiring a global macroscopic system view.

The french Energy Regulation Commission (CRE) defines the quality of energy by three different notions [142]:

- Quality of the voltage wave: includes disturbances concerning the shape of the voltage wave such as voltage dips or the harmonic ratio.
- Quality of service: covers the relationship between users and the associated system operator. This includes, for example, system Restoration delays and scheduled outage notifications.
- Continuity of supply: includes cuts and interruptions experienced by users. Ref. [15] defines the terms "brief outage" as a power supply interruption for a period between one second and three minutes, and "long outage" as a power supply interruption for any duration longer than three minutes. Outages of less than one second are not classified and are considered as voltage dips.

In accordance with the definition of quality of service and continuity of supply provided by the CRE, improving the observability of the electrical system through the utilization of a greater number of sensors to gather relevant information can facilitate enhanced coordination between the distinct components of a PAC system; ultimately resulting in a significant improvement in energy quality. This notion has been supported by various studies, such as the work of Yang et al [180] emphasizing the role of coordinated protection schemes in mitigating the impact of DER integration on distribution systems. Similarly, the research conducted by Dehghanpour et al. [37] highlights the benefits of increasing the observability of distribution grids through the use of advanced metering infrastructure.

However, conventional protection schemes (which constitute the first component of a PAC system) have limited coordination, which restrains many new uses, like the massive integration of DERs. Conventional protection design assumes:

- The Short circuit power (SCP)¹ is sufficiently high to ensure the operation of all HV, MV, and LV protections.
- The power system is sufficiently stable to allow fault clearance at each voltage level.
- Most of the generators are connected at the HV level, suggesting that MV and LV short-circuit currents are unidirectional.
- There is a very low risk of unwanted islanding situation.
- The loss of production in MV and LV levels in case of a fault remains very small.

The aforementioned considerations have become obsolete due to recent advancements in the distribution system, which have been extensively discussed in multiple studies. Article [69] highlights the issues coming along with the changes in the distribution system. An overview of major blackouts around the globe is presented, focusing on the initial disturbance and cascading effects. In 2019, several cascading events, triggered by a fault in the HV level, led to unwanted tripping of DER decoupling protections. This event resulted in the disconnection of approximately 1.1 million customers around London [86]. The use of connectivity and automation shall mitigate the risk of the occurrence of such blackout events and provide new opportunities for distribution system operators (DSOs).

Another limitation of conventional PAC systems lays on the hardware infrastructure, which incur a high-cost to upgrade (e.g., incorporate advanced features), sustain (e.g., during hardware malfunctions), and maintain given constantly evolving system requirements [94, 173]. Moreover, deploying such systems necessitates significant manual effort, leading to inconsistencies and a high risk of errors when not automatically validated.

The issues associated with PAC implementations have led to the emergence of software-defined PAC systems, which is the outcome of the convergence of the IT and power system domains. This idea, initially introduced by Lo et al. [112], has gained traction recently. According to [84], software-defined PAC systems can be formally defined as "an approach that involves decoupling PAC software from dedicated hardware by employing well-managed architectures that support heterogeneous, time-deterministic applications for protection, automation (e.g., SCADA), and control (e.g., closed- or open-loop) applications".

Beyond, in accordance with the energy transition paradigm, the digital transformation of the power industry is expected to significantly transform its management, reliability, and efficiency [51]. As a result, an increasing number of energy stakeholders are becoming interested in implementing adaptive systems, such as those offered by the IT sector (e.g., Virtualization Technology, Cloud/Edge Computing), which provide the necessary interoperability, reliability, and security for OT power assets [3]. Specifically, with regard to PAC systems, this pertains to the deployment of a multitude of hardware devices,

¹SCP refers to the maximum amount of current that can flow in an electrical system during a fault condition such as a short circuit. It is an important parameter in the design of a protection systems, as it helps to ensure that the equipment can safely handle the maximum possible fault current and that the protective devices can operate properly to isolate the fault and prevent damage to the system.

also known as Intelligent Electronic Devices (IEDs), that are vendor-lock free. The IEDs include functional logic as well as the associated information systems for monitoring and operating them in the field.

2.2.3.2 Interoperability Needs for Future PAC Systems

The smart grid is inherently complex and requires a significant number of smart devices and equipment that are mutually compatible to cover the entire grid structure [56]. The integration of information and communication technologies (ICT) into the power system has the potential to create an automated and self-healing smart grid model that can avert unnecessary blackouts caused by human errors or nature disasters[162]. However, describing and configuring the requisite data (e.g., primary asset data, IEDs) using various inter-operable ICT tools can be a time-consuming task. Conventional practices involve highly intricate documentation to decipher grid data (usually stored in memory registers), resulting in a lack of inherent interoperability features.

To streamline access to grid data, the IEC has released the principal standards, semantically defined for power systems: i) IEC 61850 (defined in section 7.1)² for power automation; ii) the common information model (CIM) that bundles power system operation and planning standards, comprising IEC 61970, IEC 61968, and IEC 62325; and iii) IEC 62056 for metering [66]. These standards provide a lingua franca (i.e., a common language) that facilitates interoperability (i.e., the exchange of information) [56], enabling the sharing of large-scale information without proprietary vendor lock-ins [153]. The national institute of standards and Technology (NIST) has developed a smart grid conceptual model, illustrated in Figure 2.5, that features seven domains: Customer, Service Provider, Distribution, Transmission, Bulk Generation, Market, and Operation [73].

The standardized information can be transmitted over multiple IEDs or hosts over the communication channels with no additional mapping of essential meta-data (e.g., value, unit, scale). Protocol (communication rules), Semantic (data meaning), and Syntax (data format) interoperability are all essential for future PAC systems operations. We particularly focus on IEC 61850 standard as we limit the scope of PAC applications in this research to those that can be embedded and formally modelled within IEDs (especially in digital substations, and distribution grid control systems).

2.2.4 Distributed Energy Resources

Power systems are experiencing drastic changes with the introduction of DERs, such as photovoltaics (PVs), wind turbines, and batteries; connected at MV and LV levels. The literature provides various definitions for DERs:

- DERs refer to a variety of technologies that generate electricity close to where it will be used [38].

²IEC 61850 is an international, well-established standard for specifying communication networks and systems in power utility automation. The main goals are to ensure interoperability among IED from multiple vendors and data exchange between physically separated subsystems performing different functionality [79].

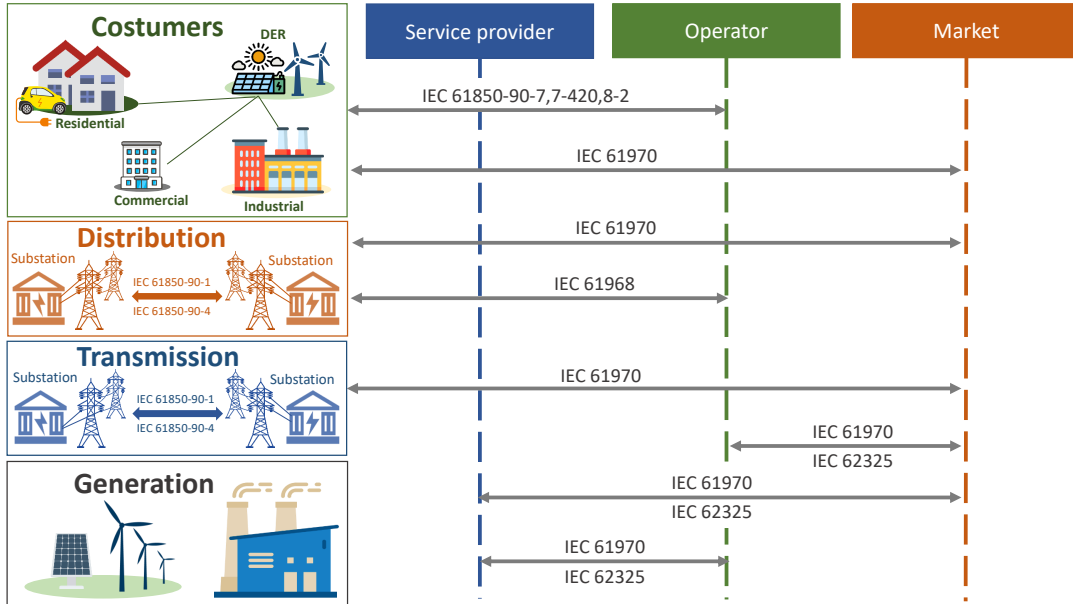


Figure 2.5: The smart grid conceptual model and its relevant standards [167]

- DERs bear the generation of electricity for on-site use, rather than transmitting energy over the electric grid from a large centralized facility [52].
- CIGRE (International Council on Large Electric Systems) defines DERs as all generation units with a capacity between 50 MW and 100 MW, usually connected to the distribution system and are neither centrally planned nor dispatched [154].
- IEEE defines DERs as the generation of electricity by facilities that are sufficiently smaller than central generating plants, allowing their connection at nearly any point in a power system [147].
- The authors of [5] gave a classification of DERs, with respect to their generation power range: i) Micro DER: 1 W - 5 kW; ii) Small DER: 5 kW - 5 MW; iii) Medium DER: 5 MW - 50 MW; iv) Large DER: 50 MW - 300 MW.

The massive integration of DERs at both MV and LV levels is actively transforming the traditional centralized, mostly static, uni-directional power systems into a grid supporting bidirectional flows of energy and information between different energy actors with much faster operating dynamics and limited predictability [29, 51]. Therefore, if the capacity of DERs approaches or surpasses the capacity of controllable sources, maintaining the supply and demand balance in the grid and avoiding congestion becomes an increasingly complex task with significant uncertainties [92]. Massive integration of DERs has been investigated in relation to the impact on grid stability and reliability, revealing that the increasing penetration of DERs may lead to voltage instability and overload in the distribution grid [123].

2.2.5 EPS Threats and Faults

All these threats induce faults in the system. In fault diagnosis theory, a fault refers to any deviation of a feature of the system, such as current, voltage, or frequency, from its normal operating condition [87]. When it comes to the electrical system, there are various types of faults that, in certain situations, can lead to power outages with major economic and societal consequences, including critical services interruption, production losses, health and safety risks, and security issues.

EPS extends over a wide geographic area, causing an exposure to a big variety of threats, classified to four categories [150]:

- Natural threats : can be stated in the order of appearance frequency as a cause for a blackout: windstorms, rainstorms, thunderstorms, blizzards, cyclones, ice storms, cold storms, heat waves, lighting strikes, earthquakes, tornados, drought, floods, hailstorms, landslides, tsunamis, wildfires and others.
- Accidental threats: technical failure, fire/explosion, human or animal interference, operation mistake, equipment defect or aging and maintenance error.
- Malicious threats: hacking, sabotage, terrorist attacks and acts of war.
- Emerging threats: geomagnetic storms³ (With the increasing interconnection of electrical grids between different countries, the length of transmission lines is also increasing, leading to larger geomagnetically induced currents.).

Table 2.1 describes the types of faults on MV grids while Table 2.2 presents their occurrence statistics.

Table 2.1: Different types of faults on MV grids

Type	Source	Location	DSO reaction	Impact on the customer
Auto Ex-tinguisher fault	Straw, bird, moisture	Overhead	-	voltage dip
Fugitive and semi-permanent	Branch, lightning, pollution	Overhead	Grid automation and maintenance	Power cuts (0.3-15s)
Permanent	Hardware failure, natural events	Underground and overhead	Automation and troubleshooting by technician	Power cuts (few seconds to several hours), voltage dip

³Geomagnetic storms are brief disturbances in earth’s magnetic field and atmosphere (aka the magnetosphere) caused by bursts of radiation and charged particles emitted from the sun [176]

Table 2.2: Fault appearance statistics on the MV grid [137]

Type		percentage	Global percentage
Non permanent	One phase	76%	96.6%
	Isolated phase to phase	3%	
	Phase to phase to ground	4%	
	three-phase	8%	
	Evolving	4%	
	Double one phase	5%	
permanent	One phase	67%	3.4%
	Isolated phase to phase	5%	
	Phase to phase to ground	4%	
	three-phase	7%	
	Evolving	17%	

2.2.6 EPS Protection System

The primary goal of a protection plan is to mitigate potential faults on the grid, which could endanger technicians, individuals, and connected equipment. A protection plan should cover all grid elements, including lines, transformers, generators, and busbars. To evaluate the associated performance, the following indicators can be used:

- **Sensitivity:** the ability of protections to detect faults, in particular very resistant faults which can jeopardize the safety of third parties.
- **Selectivity:** ensures that only the faulty part of the system is isolated without affecting the rest of the grid.
- **Speed:** evaluates system ability to respond quickly and minimize the negative impact of short-circuits.
- **Reliability:** refers to system capacity to avoid triggering unnecessary safety measures (security) and operate correctly in the event of a fault (safety).
- **Simplicity:** refers to how easy the system is to implement and maintain.
- **Cost-effectiveness:** evaluates the cost of the protection system, balancing effectiveness with affordability.

Finally, protection systems can vary depending on the grid structure, country, operator, insulation level, and line conductors (overhead or underground). Without loss of generality, we focus in this work on the fundamental protection scheme commonly used in many European countries as outlined in the B5/C6.26/CIREN Joint Working Group report [20]. It is important to note that this discussion will not cover generator protections, or decoupling protections which are discussed in Section 2.2.6.2.

2.2.6.1 Background on Transmission Grid Protections

The prevalence of the interconnected mesh topology in global power transmission grids poses a significant challenge for system protection. When a fault occurs, the fault current flows through multiple substations, creating a complex situation that makes it difficult to accurately locate the fault (Figure 2.6).

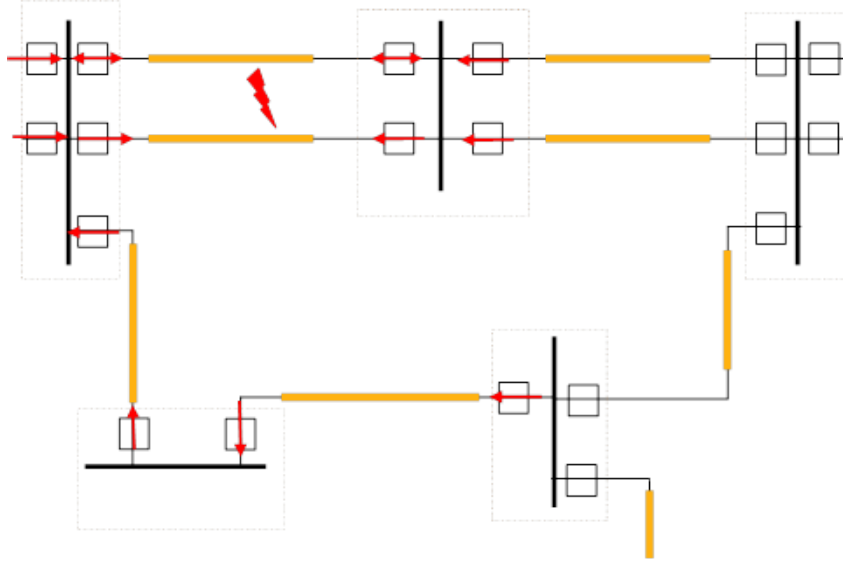


Figure 2.6: Flow of fault current in meshed power systems

Two of the commonly used protective measures are distance and differential protections, which can quickly eliminate most faults, including low resistance faults, in under 150 milliseconds [102]. While this process may cause a voltage dip⁴ across a large area, the incident duration typically corresponds to the time taken by the fault to be cleared, with an additional transient period lasting a few hundred milliseconds to recover the voltage nominal value. Figure 2.7 illustrates the potential extent of a voltage dip.

In order to ensure a stable and uninterrupted power supply, power plants must have the ability to withstand voltage dips and maintain a connection to the grid. This is achieved through under voltage ride through (UVRT) capabilities, which allow generators to remain connected even during a temporary drop in voltage.

2.2.6.2 Background on Distribution Grid Protections

Distribution grids worldwide are mostly operated in a tree-like structure (Figure 2.8), meaning that the supplied energy to a node follows a single path and originates from the *upstream grid* via the *feeder* (when DERs are not considered). As a result, it is possible to identify grid faults by monitoring the feeder.

The protection relays on the distribution network employ various measured quantities, such as current, frequency, and voltage, and compare them to predefined thresholds. When a fault appears on the grid, the relays initiate actions, such as tripping, based on specified time delay settings, the higher the measured fault current, the faster the tripping

⁴Voltage dip is defined as a 10 to 100% decrease in voltage amplitude over a time interval of 10 ms to 1 s

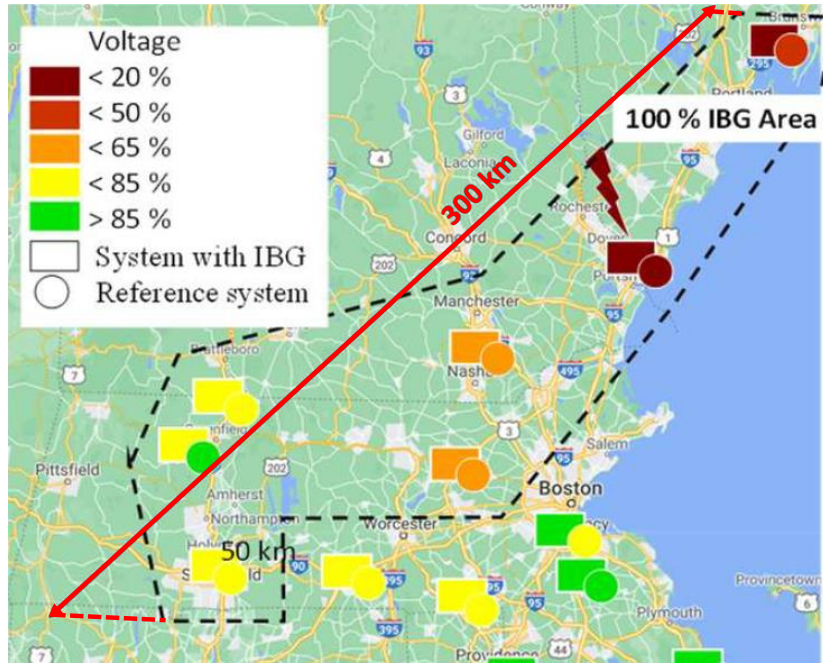


Figure 2.7: Example of a voltage dip extent

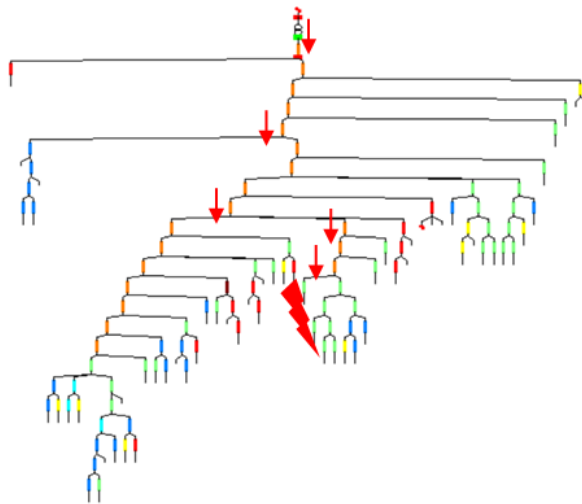


Figure 2.8: The structure of an MV feeder

action will occur. The protection relays will not sense the same fault current and trip in varied tripping delays, enabling a time-based selectivity mechanism that minimizes the impact on unaffected network segments while ensuring backup protection. Some time delay settings are coordinated with the transmission system to ensure global system coordination.

Moreover, a differentiation is drawn between protection plans for poly-phase faults and ground faults. Poly-phase faults are typically safeguarded with over-current protection (ANSI 51), which is designed with time selectivity to ensure that the closest protection device to the fault trips, as in Figure 2.9.

Ground fault protections depends on the neutral grounding system, which can incorporate various types of protection (such as over-current, directional, and wattmetric)

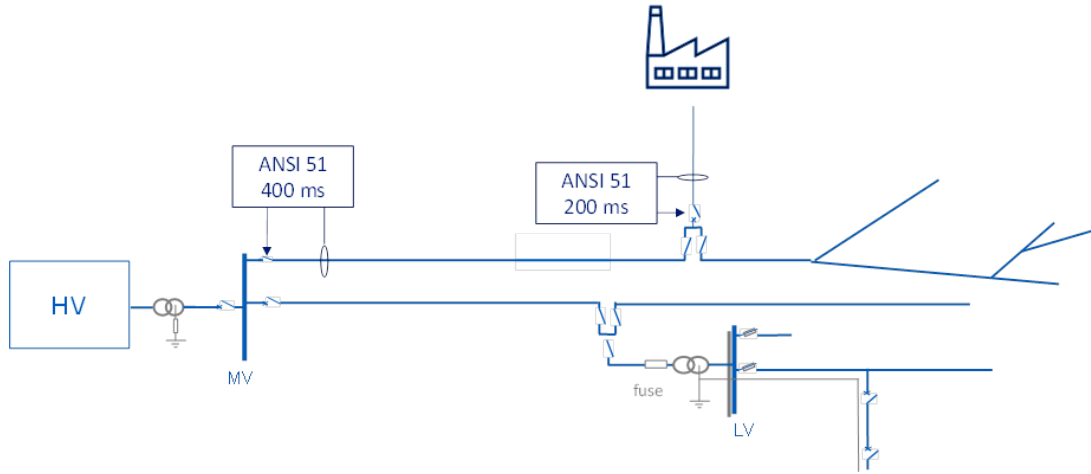


Figure 2.9: Protection system coordination in MV power system

using both current and voltage measurements. Additionally, a time-based selectivity (coordination) mechanism is used by the protections.

When a poly-phase or grounded fault occurs on the MV grid, resulting voltage disturbances last from a few milliseconds to one second, with a spread impact throughout the entire MV system.

Recent developments incorporate protection functions within multi-function digital relays, in addition to the role of fuses. However, digital protections are not commonly utilized in LV systems, and in certain cases, fuses and thermal-magnetic overcurrent circuit breakers may be the only means of protection.

Decoupling Protections :

EPS production sites are equipped with decoupling protections, also called interface protections, that automatically disconnect the means of production in case of a disturbance on the distribution system, especially during incidents.

Decoupling protections are a crucial safety feature in electricity production installations connected to distribution systems. According to EN 50549 [145], this means of automatic disconnection has the following main purposes:

- prevent the generation plant's electricity production from causing an overvoltage situation in the distribution system to which it is connected;
- detect involuntary islanding situations and disconnect the plant in this case. This helps to prevent damage to other equipment, both in generator facilities and the distribution system, due to out-of-phase reclosing and to allow for maintenance work after an intentional disconnection of a section of the distribution system;
- help to bring the distribution system into a controlled state in the event of voltage or frequency deviations beyond the corresponding regulation values

In their most common form, decoupling protections are passive and work by utilizing relays to monitor voltage and frequency measurements in real-time, comparing them to predetermined thresholds. When the measurements fall outside the authorized range, the

protection relays activate a trip signal to disconnect the generator from the distribution system. The time delay associated with the threshold ensures that the protection only trips when the disturbance is sustained, reducing the likelihood of false trips. Other criteria such as the RoCof (Rate of Change of Frequency) can be used to trigger the relays. Depending on the installation and operating conditions, the settings of these protection relays may be adjusted to optimize the system's performance while maintaining a high level of protection.

- Voltage and frequency ranges: The effectiveness of power protections depends on the voltage and frequency ranges specified for under/over voltage and frequency protections. By defining these settings, the risk of unwanted islanding can be reduced by setting the limit values closer to the nominal value, while the risk of untimely disconnection can be decreased by setting the limit values further from the nominal value. Fine-tuning these ranges is crucial for ensuring optimal protection while avoiding false disconnections.
- Operation time setting: The protections can be time-delayed, and the relay will only open a certain time after fault detection. Some decoupling protections, for example, are configured to trigger only after a delay of 1.5 second, which is slightly longer than the duration of a voltage dip caused by short circuit on the transmission (i.e., upstream) system. This time delay helps prevent untimely disconnection of DERs. However, other decoupling protections are set to be instantaneous, as is the case with most DERs currently connected to LV systems. In these cases, if a voltage dip occurs, the DER protections will trip immediately.

Numerous academic studies have been dedicated to developing methods for detecting unintentional islanding, resulting in the classification of several types of methods:

- Passive: only measure signals and compare them to pre-set thresholds;
- Active methods: involve slight modification on the inverter's control or add a physical element to destabilize any potential islanding. Implementing active methods may require additional hardware or software modifications, making them more complex and potentially more costly than passive methods.;
- Hybrid methods: combine the features of passive and active methods;
- Telecommunications-base methods: theoretically they are the most efficient and do not disturb the grid in normal operation. However, there is currently no communication method with the necessary characteristics that is both fast, reliable, and economical enough to be deployed on all MV and LV production sites. In France, protection type H.4 [50] and H.4.1 use this type of method. In this work, we investigate the use of 5G network to support telecommunication-based method.

Remote Decoupling To mitigate the risks of islanding and untimely disconnection using a telecommunication-based method, a viable option is to implement remote decoupling of DER mechanism through utility-controlled transfer trip (as illustrated in Figure 2.10). To prevent untimely disconnections, large voltage and frequency thresholds are established, and tripping is delayed until the circuit breaker of the MV feeder opens. Upon detecting this, the substation sends a decoupling order to the DER. Currently, in Metropolitan France, remote decoupling is available for producers with production exceeding 5MW, which requires a wired link between the DER and its MV substation. However, the threshold for remote decoupling in France Overseas is set at 1 MW.

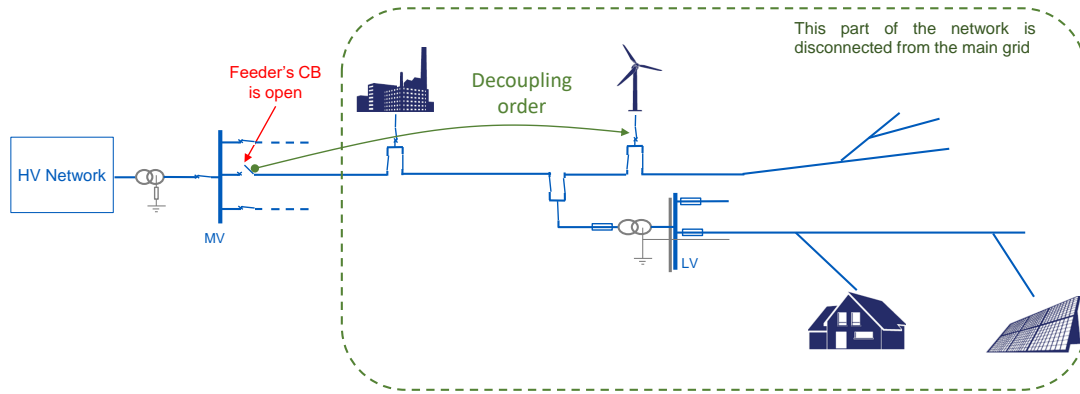


Figure 2.10: Example of remote decoupling mechanism

2.2.7 Impact of DERs on Distribution PAC Systems

DER integration into distribution grids affects the performance of MV and LV conventional protection schemes. The main protection issues under these conditions are presented in [166] and [28], and summarized below.

2.2.7.1 Nuisance or false tripping

The bidirectional flow of short-circuit currents is considered as the main protection concern related to the integration of DERs, as false tripping of non-directional over-current relays (OCR) can be caused. Figure 2.11 illustrates two adjacent distribution feeders, each protected by a dedicated OCR. Only one feeder has a DER generator.

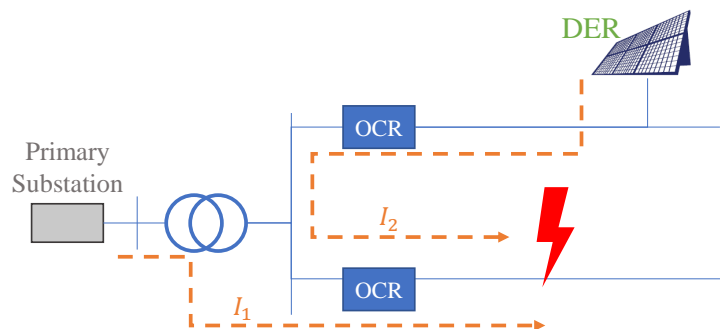


Figure 2.11: False tripping of the relay of the feeder to which the DER is connected

When a fault occurs in the feeder without DER, the substation will feed the fault with a short-circuit current I_1 , while the distributed generator will add another short circuit current I_2 . In the case where I_2 is considerable, the OCR that protects the healthy feeder could undergo a false tripping. This well-known issue can be solved with directional protection relays which need both voltage and current measurements.

2.2.7.2 Protection blinding

Protection system sensitivity can be decreased by the presence of one or more DERs connected to a faulty feeder. An example of blinding is illustrated in 2.12. The short-circuit current I_1 coming from the substation is weakened by the contribution of the short-circuit current I_2 from the DER. As a result, if the aggregate short-circuit current is below the OCR tripping threshold, the OCR will either not trip, or trip with a longer delay if inverse time curves⁵ are used.

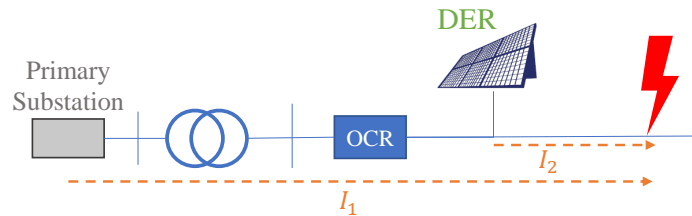


Figure 2.12: Blinding of a protection relay

The behavior of inverters under short-circuit conditions has been the subject of many publications [181, 127, 132, 163, 107]. They all converge on the fact that the behavior of inverter-based generators (IBGs) is very different from traditional directly-connected rotating synchronous generators, making the blinding difficult to study.

2.2.7.3 Fuse-saving related issues

Overhead distribution feeders are generally protected by reclosers⁶, sometimes associated to fuses. If a fault occurs on feeder protected by a fuse, the recloser must open quickly before the fuse blows. This prevents the fuse from melting and causing an extended outage, which would require replacement by technicians. In conventional distribution feeders (i.e. without DERs), recloser-fuse coordination is ensured assuming that the same short-circuit current flows through both the recloser and the fuse. However, in cases where a DER unit is also supplying power to the fault on the feeder (Figure 2.13), the short-circuit current flowing through the fuse would be higher than the one flowing through the recloser. This would result in the fuse melting before recloser opening, potentially leading to a violation of the fuse-save logic [91, 34].

⁵Inverse time curves determine the amount of time that must elapse at a specific current level before a certain action, such as tripping an OCR, is triggered.

⁶A recloser is an automatic switch that interrupts electrical power when a fault, such as a short circuit, occurs. It conducts a self-test of the electrical line to determine if the fault has been cleared. If the issue was temporary, the recloser resets automatically, and the electrical power is restored.

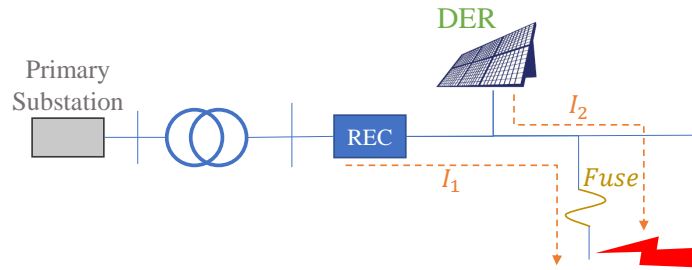


Figure 2.13: Effect of DER on fuse-recloser coordination

2.2.7.4 Unwanted islanding

According to the IEC 62116 standard [75], islanding corresponds to a situation in which a portion of the power system, containing customers and producers, is isolated from the main grid. Precautionary, when a segment is disconnected from the upstream grid, DERs (such as PVs and wind turbines) must stop supplying power. However, the load and the power produced on this portion of the grid may be balanced prior to the isolation event, i.e. the production is approximately equal to the consumption. In this case, when the source substation circuit breaker is opened (e.g. following a fault or a manual operation in the feeder), the grid portion separated from the upstream system remains energized. An island supplied by DERs is formed as highlighted in green in Figure 2.14. The island voltage and frequency become unstable, varying according to changes in production and consumption.

The development of DERs and self-consumption increases the probability of creating unintentional islanding, which results in various types of risks and damages, including:

- Failure to detect a fault, such as an electrical insulation fault⁷ that can remain powered by the DER, putting people at risk.
- Damage to the public grid and customer installations if voltage checks are not performed before reclosing, or unintentional islanding is eliminated by anti-islanding protections. This can cause two asynchronous electrical systems to be coupled, i.e. out-of-phase reclosing between the main grid and the island, resulting in serious material damage.
- Risks to utility line workers if supposedly de-energized lines are still powered by the DER.
- Power quality issues, as the unintentional islanding zone may operate under unsuitable power conditions for the loads.
- Protection failures due to the low fault current in unintentional islands, insufficient to operate fuses or over-current relay protection devices inside the island.

⁷An electrical insulation fault occurs when electric current leaks from one conductor to another that should not be electrically connected. This happens as a result of degraded or damaged insulation between the conductors and can result in hazards such as electric shock, fire, damage to equipment, and even loss of life.

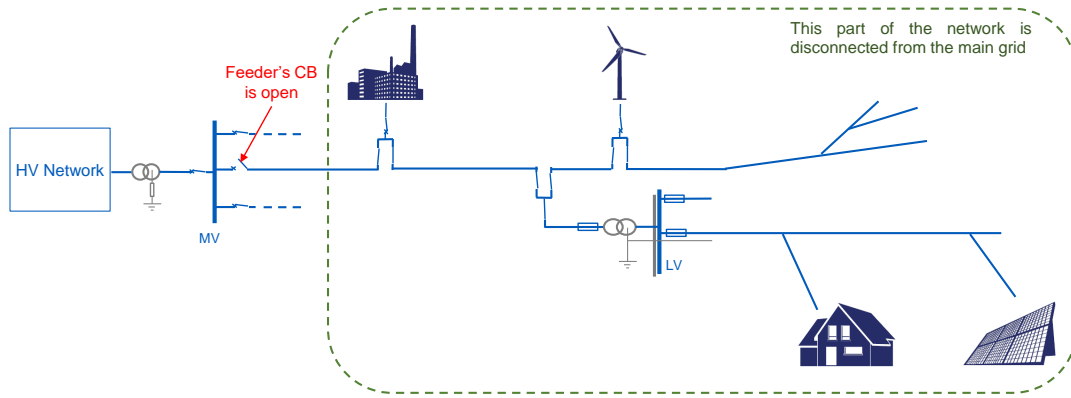


Figure 2.14: Example of an unwanted islanding situation

2.3 5G Network Ecosystem

In order to achieve next-generation energy system that integrates new services and functionalities, it is necessary to implement a specific digital communication layer [68, 124]. This layer enables communication between power, protection, and control devices, allowing for the most efficient configuration at all times [166]. Various technologies have been explored for implementing this communication layer, including optical fiber [164] and 4G mobile networks [97, 115]. While fiber meets communication requirements such as ultra-low latency, reliability, and service availability, it is expensive to implement and lacks the flexibility to easily connect new power plants. On the other hand, 4G technology offers the flexibility and scalability needed for integrating new nodes on the EPS, but is limited in terms of latency, speed, and reliability for advanced PAC applications. As a result, fifth-generation (5G) technology presents the ideal compromise by providing an ultra-reliable connection with slicing, as well as speed and latency comparable to those of optical fiber, while offering the same level of flexibility and scalability as 4G [63]. In addition, edge computing [165] near power plants reduces latency and bandwidth requirements and enhances security.

2.3.1 Features

Many are the characteristics to refer to 5G network as next-generation smart grid enabler. Some of these characteristics that will be detailed later in this section are, but not limited to, its software-defined nature, cognitive or AI capabilities, network intelligence, self-healing, global awareness, autonomous, etc. However, the main motivations to use 5G in the current grid system that will evolve into the next/proposed future generation of smart grid are [56, 144]:

- *Network Management Become Simpler:* The management of the communication network will be simplified by using the programmable 5G network [183]. The software defined network (SDN) controller, which uses advanced AI-based algorithms, will have a real-time global view of the next-generation PAC's communication network. It will dynamically adapt packet processing rules and policies in the infras-

tructure/data plane. Prior to 5G and without an SDN-based architecture, network orchestration and management requires physical or human intervention to change routing rules on communication devices.

- *Isolation of diverse traffic Types and Applications:* In the next generation PAC systems, a variety of traffic classes will be produced by IEDs such as current and voltage sensors, merging units, fault passage indicators, smart meters, and others. These traffic classes can generate either regular or irregular (i.e. event-based) data flows. To cater to the diverse needs of various applications, the 5G network is designed to support distinct and segregated traffic classes. [96].
- *Traffic prioritization:* Another major advantage of the 5G network is its ability to prioritize critical traffic based on different conditions. For instance, some PAC applications require the transmission of critical instructions and measurement data with both low latency and high reliability. The 5G network makes it possible to prioritize data flows [40], and allocate telecommunication resources dynamically to ensure that the most critical traffic gets the necessary resources. Furthermore, the SDN-based programmable controller provides a comprehensive network overview, enabling easy orchestration of traffic flows.
- *Virtual Network Slice:* 5G enables the creation of virtual network slices tailored for specific PAC applications, based on various factors such as the domain (generation, transmission, or distribution), geographical location, criticality of data, and type of consumer (e.g., individual, factory, hospital). For instance, a virtual network slice can be designed for distribution grid protection systems that adhere to stringent security measures, policies, management protocols, and quality of service (QoS) regulations.
- *Resilience:* Compared to wired communication, wireless communication allows for dynamic selection of the most reliable communication links and shortest data transmission paths. With the advancements in 5G technology, which boasts performance comparable to optical fiber, next-generation PAC systems can effortlessly attain greater flexibility in their communication networks while enhancing resilience.
- *Ultra-fast failure/fault Restoration:* Future generations of PAC systems will depend heavily on communication links. Therefore, ensuring the continuity of communication services and the rapid restoration of links during a crisis, such as congestion or interruption, will be crucial. The 5G network incorporates innovative technologies like SDN and NFV to expedite the restoration of communication links following a failure [40].
- *Standardization/Interoperability:* Interoperability is one of the foundations of the 5G network, enabled by implementing a microservices architecture and providing numerous interfaces with vendor-neutral access. As the IEDs are strategically placed throughout the expansive EPS and rely on the communication networks of different

operators, 5G interoperability is crucial to ensure that these devices can seamlessly exchange data with one another.

- *On-demand deployment of telecommunication resources:* By leveraging technologies such as NFV, SDN, and orchestration, the 5G network is equipped to deliver communication resources (including bandwidth, throughput, latency, and reliability) for PAC applications, precisely where and when needed. This approach effectively minimizes telecom network costs for grid operators who will only be charged for the consumed resources.

Table 2.3 and 2.4 provide an in-depth comparison of various wired and wireless telecommunication technologies. These tables highlight key factors such as bandwidth, range, reliability, and latency, which are crucial for evaluating the effectiveness of a communication network. By analyzing the data presented in these tables, it is evident that 5G technology outperforms other communication technologies in terms of speed, capacity, and latency.

Table 2.3: Wired communication technologies for the smart grid.

Technology	Standard/ protocol	Data rate	Coverage range	latency	Deployment cost	Energy consumption	Network
Fiber optic	PON	155 Mbps– 2.5 Gbps	60 km	Low	High	Medium	
	WDM	40 Gbps	100 km	Low	High	Medium	WAN
	SONET/SDH	10 Gbps	100 km	Low	High	Medium	
DSL	ADSL	1–8 Mbps	5 km	High	High	Medium	
	HDSL	2 Mbps	3.6 km	High	High	Medium	FAN
	VDSL	15–100 Mbps	1.5 km	High	High	Medium	
Coaxial Cable	DOCSIS	172 Mbps	<28 km				FAN
PLC	HomePlug	14–200 Mbps	<200 m	Low	Low - Medium	Medium	LAN
	Narrowband	10–500 kbps	<3 km	Low	Low - Medium	Medium	
Ethernet	802.3x	10 Mbps– 10 Gbps	<100 m	Low	- Migh	Medium	LAN FAN
				Medium			

Table 2.4: Wireless communication technologies for the smart grid.

Technology	Standard/ protocol	Data rate	Coverage range	latency	Deployment cost	Energy consumption	Network
Z-Wave	Z-Wave	40 kbps	<30 m	High	Low	Low	LAN
Bluetooth	802.15.1	721 kbps	<100 m	Low - Medium	Low	Low	LAN
ZigBee	ZigBee	250 kbps	<100 m	Low - Medium	Low	Low	LAN FAN
ZigBee Pro	ZigBee Pro	250 kbps	<1600 m	Low - Medium	Low	Low	LAN FAN
WiFi	802.11	2–600 Mbps	<100 m	Medium High	Low	Low	LAN FAN
WiMAX	802.16	75 Mbps	<50 km	Low - Medium	Medium	High	FAN WAN
Cellular	2G	14.4 kbps		High	Low	Low	
	2.5G	144 kbps		High	Low	Low	
	3G	2 Mbps	50 km	High	Low	Medium	FAN
	3.5G	14 Mbps		Low	Low	Medium	WAN
	4G	100 Mbps		Low	Low	Medium	
Satellite	5G	10Gbps		Low	Low	Medium	
	Satellite Internet	1 Mbps	<6000 km	Medium	High	High	WAN

2.3.2 5G network architecture

2.3.2.1 Typical RAN topology

The architecture of a typical 5G network is composed of three main components, namely the Radio Access Network (RAN), the core network, and the edge network.

The RAN is responsible for connecting user devices like smartphones and tablets to the 5G network. It is divided into three parts: the remote radio unit (RRU), the distributed unit (DU), and the centralized unit (CU). The RRU is responsible for receiving and transmitting radio signals to and from user devices. The DU processes the radio signals received from the RRU and transmits them to the CU. The CU manages and controls the RAN and interfaces with the core network.

The core network is in charge of managing and directing data traffic between the RAN and the internet or other networks. The edge network is an optional component that brings computing resources closer to end users and is used to provide low-latency services such as augmented reality, virtual reality, and autonomous vehicles. Together, these components form the standard topology of a 5G network.

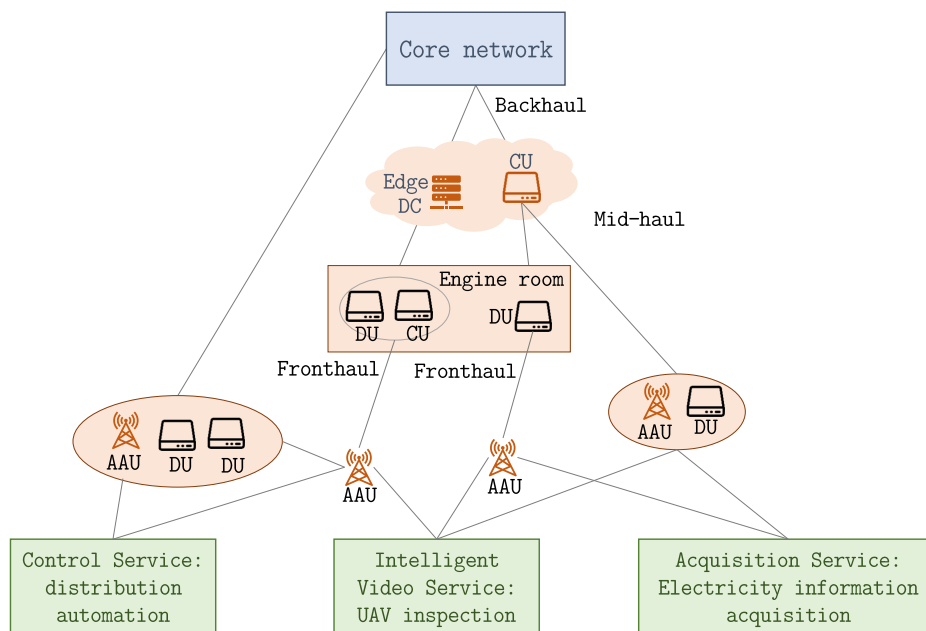


Figure 2.15: 5G Network architecture

2.3.2.2 Integrated Access Backhaul (IAB) topology

The IAB is an emerging technology that has been introduced in the 5G network architecture to improve the network's coverage and capacity. IAB allows the deployment of small cells in locations that were previously unreachable by the traditional macro base stations. IAB provides a cost-effective solution for network operators to expand their 5G network coverage and provide high-quality services to their customers.

The IAB topology consists of two main components 2.16: the IAB master node and the IAB slave node. The IAB master node acts as the controlling entity and is typically a macro base station, which coordinates the communication between the slave nodes and

the core network. The IAB slave node is a small cell that can function as both an access point and a backhaul node, which extends the network coverage and capacity.

In the IAB topology, the small cells are connected to the macro base station through a wireless backhaul link, which eliminates the need for a wired backhaul connection and simplifies network planning. The IAB topology also supports dynamic resource allocation and interference management, ensuring efficient utilization of network resources and high-quality user experience.

Overall, the IAB topology is a promising technology that enables 5G networks to expand their coverage and capacity in a cost-effective manner, while providing high-quality services to users.

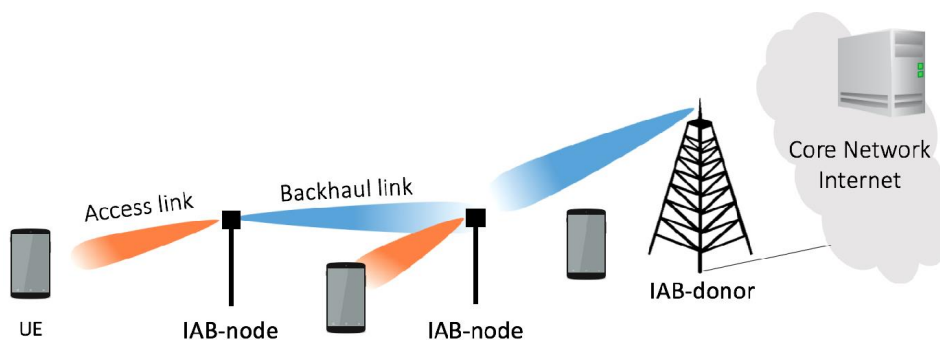


Figure 2.16: 5G IAB network topology [139]

2.3.3 5G Network Concepts

2.3.3.1 Network slicing

Network slicing technology has gained significant attention from research groups and standardization bodies, including NGMN [10], ONF [126], ITU-T [178], and 3GPP [168]. It was first introduced by the next generation mobile network (NGMN) Alliance in [10], revolutionizes traditional networking by enabling the coexistence of several self-contained logical networks on a common physical infrastructure platform. Unlike the traditional "one size fits all" approach, network slicing technology, as stated in [93], introduces a "one size per service" approach, providing value to application providers, vertical segments, and third parties without requiring a physical network infrastructure. Slices can be provisioned on-demand and each slice consists of a set of VNFs that vary significantly depending on the service requirements of that particular slice. The number of resources allocated to each slice depends on the type of service associated with it, as detailed in [6].

The overarching goal of 5G wireless technology is to cater to three distinct services with varying requirements: enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (uRLLC) [140]. Each service has unique applications and prerequisites [169], [185]. eMBB aims to provide exceptionally high data rates with high reliability for tasks such as augmented reality and remote presence. mMTC targets the connection of a large number of cost and energy-efficient devices. URLLC aims to provide a low-latency, ultra-reliable service with

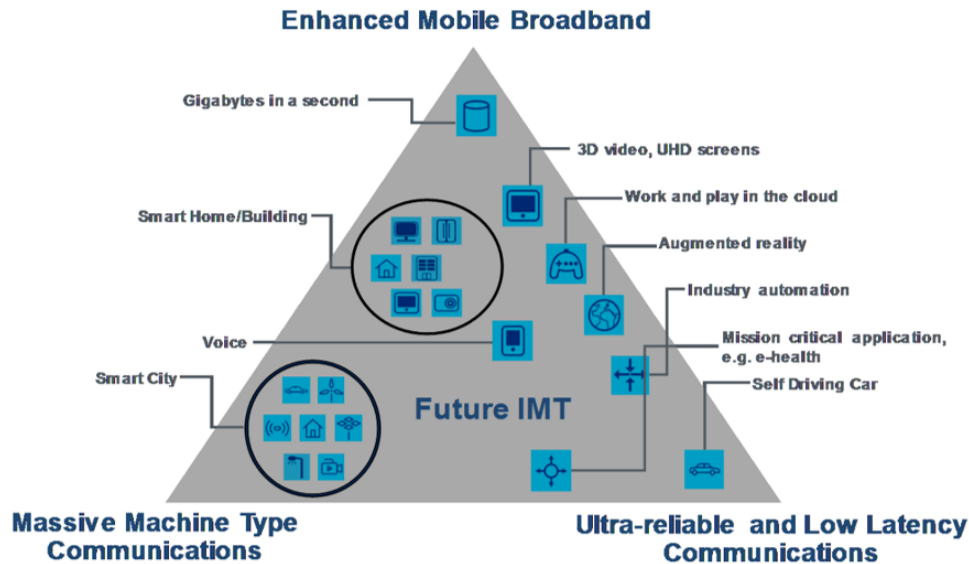


Figure 2.17: Usage scenarios of 5G and beyond [158]

relatively low data rates compared to mMTC. Based on the network slicing categories, Figure 2.17 depicts several potential use cases for 5G technology.

Network slicing is based on many conditions and principles. The most important and required are as follows [6]:

- Automation: the creation of a network slice in an automatic way without the need of manual intervention or fixed contractual agreements.
- Programmability: Third parties must be able to control the resources allocated to a slice through open APIs, enabling service-oriented customization and resource elasticity on demand.
- Isolation: Despite sharing the same physical infrastructure, network slices should provide a certain level of security and performance by isolating tenants from each other.
- Elasticity: Operations must be designed to maintain the required service level agreement under changing conditions.
- Customization: Network slices must efficiently allocate resources to tenants according to their service requirements.
- Hierarchical abstraction: Network slice resources allocated to a particular tenant can be partially or wholly traded to another third actor, following a hierarchical pattern.
- End-to-end (E2E): Network slicing inherently facilitates service delivery from service providers to the end-user/customer.

The importance of each key capability for the usage scenarios eMBB, uRLLC, and mMTC is illustrated in Figure 2.18.

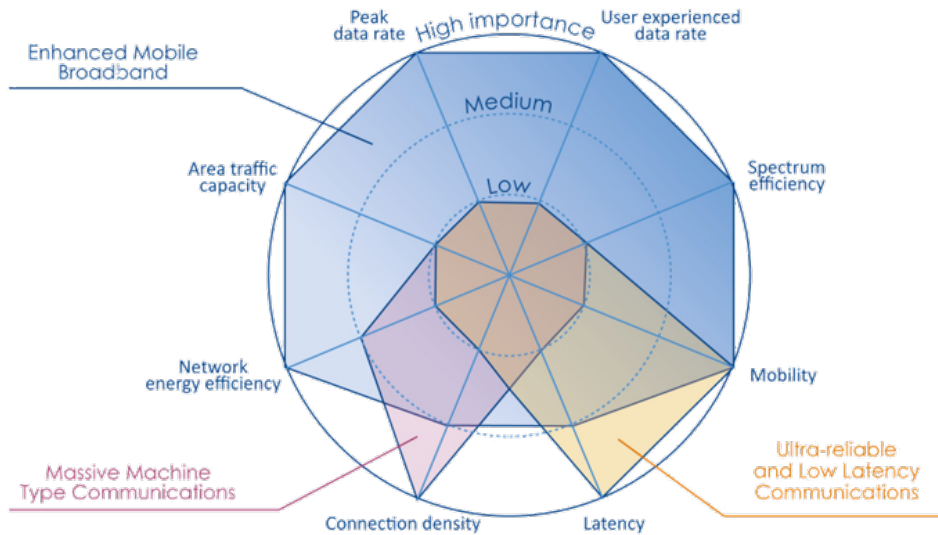


Figure 2.18: The importance of key capabilities in different usage scenario [158]

2.3.3.2 SDN/NFV Paradigms

Meeting the demands of new use cases requires a fresh perspective on telecommunication network architecture. The SDN and NFV paradigms are considered fundamental for the future vision of the 5G network [121]. Together, these complementary paradigms enable the creation of highly flexible 5G networks.

2.3.3.2.1 NFV :

This concept [122] offers a new approach to designing, deploying, and managing networking services, independent of hardware appliances. In this model, network functions are replaced by software running in a container, such as Docker or LXC, or in a virtual machine. The software-based infrastructure enables greater flexibility and scalability, while reducing costs associated with physical hardware. Overall, NFV provides a more flexible and agile approach to networking, enabling the rapid deployment of new services and reducing the costs and complexities associated with traditional hardware-based solutions.

The virtual network function (or VNF) must perform the same functions and behaviors as the original NF. Some examples of VNFs include firewalls, dynamic host configuration protocol (DHCP) servers, network address translation (NAT) servers, forwarding control, intrusion detection algorithms, domain name service (DNS), and more.

VNFs can be connected or combined to provide an optimal network communication service [146]. NFV introduces the following three major differences compared to current practice [70]:

- Separation of software from hardware
- Flexible network functions deployment

- Dynamic operation: scale the NFV performance dynamically and with great flexibility

SDN :

The SDN paradigm, which is standardized by the open networking foundation (ONF), involves separating the control logic from the forwarding network resources, and provides new ways to configure and build networks [155]. This enables network control to be programmable via open interfaces such as ForCES [39] and OpenFlow [104], and allows the underlying infrastructure to function as simple packet forwarding devices (i.e., the data plane) that can be programmed [122].

While traditional communication networks' architecture is decentralized and complex to manage, SDN enables easy deployment of virtual networks, efficient network programming, and dynamic configuration. SDN centralizes network intelligence in one network component and separates control plane from the underlying infrastructure (data plane). Together, SDN and NFV allow to break vertical software integration in communication network design.

In the following section, we delve into the concepts of Cloud/Edge computing that leverage virtualization technology to enable future PAC systems.

2.3.3.3 Mobile Edge Computing (MEC)

Edge computing is a type of network architecture that involves processing data at or near the physical location of the user or data source, providing cloud computing functionality and computing services at the network edge. This approach reduces latency and bandwidth usage by performing data processing closer to the source and enables real-time processing and analysis of data.

In the realm of mobile networks, multi-access or mobile edge computing (MEC) is a specific use case of edge computing designed for service providers. Its primary objective is to offload computing tasks to network edge nodes, such as base stations, wireless access points, and other devices, thereby bypassing the backhaul and core network. This approach facilitates highly efficient network operations and service delivery, particularly ultra-reliable communications with low latency and very high throughput. MEC systems follow a distributed deployment model, with each server serving a small scale and storing a limited amount of information, which enhances system reliability by eliminating any single point of failure. Technical and architectural standards for MEC have been primarily developed by the industry specification group (ISG) within the european telecommunications standards institute (ETSI) since 2014 [116].

The Edge Computing 3.0 reference architecture proposed by the Industrial Internet Industry Alliance is shown in Figure 2.19 [32]. The system consists of three layers:

- *Site layer*: comprises a variety of intelligent devices connected to the edge network, including mobile terminals, sensors, smartphones, smart cars, and cameras. These devices can function as both data providers and consumers, depending on the situa-

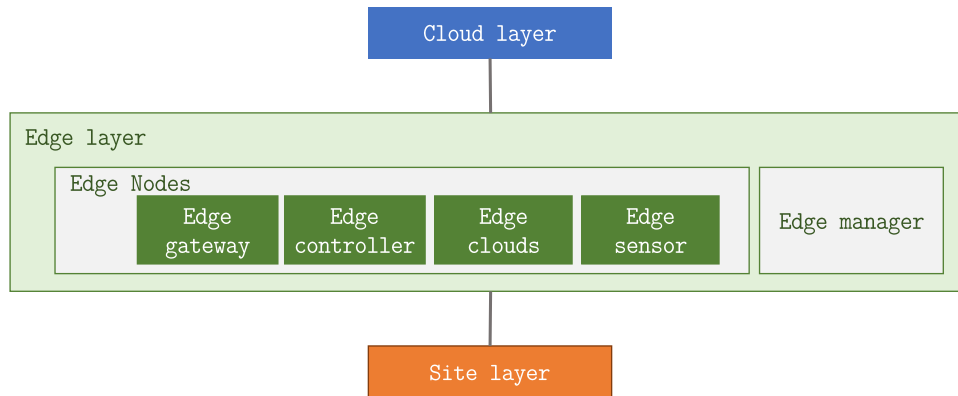


Figure 2.19: edge computing reference architecture 3.0

tion. Due to their limited computing power, the edge devices transfer the raw data they collect to the upper layer for processing and storage.

- *Edge layer:* Represents the core of the three-tier architecture and comprises multiple edge nodes located between the terminal and cloud layers. These nodes typically include base stations, access points, routers, switches, and gateways. The edge layer functions as a gateway for smart devices, processing and storing the data they collect. Data is aggregated and preprocessed at the edge layer before being uploaded to the cloud [159]. To facilitate real-time data analysis and intelligent processing, which is more secure and efficient than cloud computing, the Edge layer is often employed since it is closer to the user.
- *Cloud layer:* is a collection of powerful servers and devices that serve as the primary data processing center. Its crucial role is to handle large data analysis tasks such as optimization, prediction models, and decision support systems. The cloud layer also enables data persistence from the edge layer and performs complex tasks that require performance beyond the edge layer’s capabilities. Furthermore, the cloud layer has the potential to integrate global information, and its deployment topology and algorithms can dynamically adapt to the management policy, allowing for high flexibility. Table 2.5 provides a comparison between cloud and edge architectures, based on [18, 149, 2].

As part of the deployment of 5G, service providers will need to virtualize network functions, which will simplify network operations and improve flexibility and availability, resulting in new services and means. The MEC meets the performance and latency requirements of 5G networks and helps improve the customer experience. Adoption of an edge architecture for the 5G network can be realized by using an edge computing platform (ECP) defined by ETSI MEC and deploying a Distributed user plane function (UPF) defined by 3GPP.

The PAC system architecture mapped to the Cloud/Edge computing model comprises of three main layers, as shown in Figure 2.20. The lower layer represents the wide area measurement system, which collects data and sends it to a processing point located in the

Table 2.5: Comparison between edge and cloud architectures.

Evaluation Parameter	Edge Computing Architecture	Cloud Architecture
Latency	The low latency provided by the system ensures that real-time applications, such as monitoring frequency and verifying VAR (Voltage-Ampere Reaction) regulation to prevent power factor penalties, can be effectively handled.	The distance between the connected devices and cloud servers requires a multi-hop communication, which imposes a high communication delay, exceeding the maximum delay tolerated by certain real-time applications.
Bandwidth	Edge data filtering and pre-processing eliminate the need to send vast amounts of non-treated data to the cloud. This enables collecting more information on the grid and enriching forecasting models without increasing the communication service cost.	For accurate grid control, communicating devices such as IoT-based devices transmit large amounts of real-time raw data to the cloud. However, this increases the load on the communication network, leading to congestion and higher transmission delays, error rates, and OPEX of the telecommunication network.
Security / Privacy	As PAC systems handle an increasing volume of private and sensitive information on the power grid, data processing at the edge enables selecting which data should go through the cloud and which should remain local.	As the cloud can be managed by third parties, sending sensitive or private user data collected by connected IoT devices raises concerns regarding privacy and security.
Storage	Limited	Abundant
Computing power	Limited	Abundant

middle layer. The middle layer, which can be on-site or distributed throughout the communication network, analyzes the data and sends corrective orders to resolve local issues. The aggregated data is then sent to the central processing point in the upper layer, which has a system-wide visibility allowing the resolution of problems that require coordination. In order to ensure seamless management of each edge or cloud computing system model, it is necessary to have mechanisms in place to monitor and manage the various components, such as network infrastructure, computing resources, and applications.

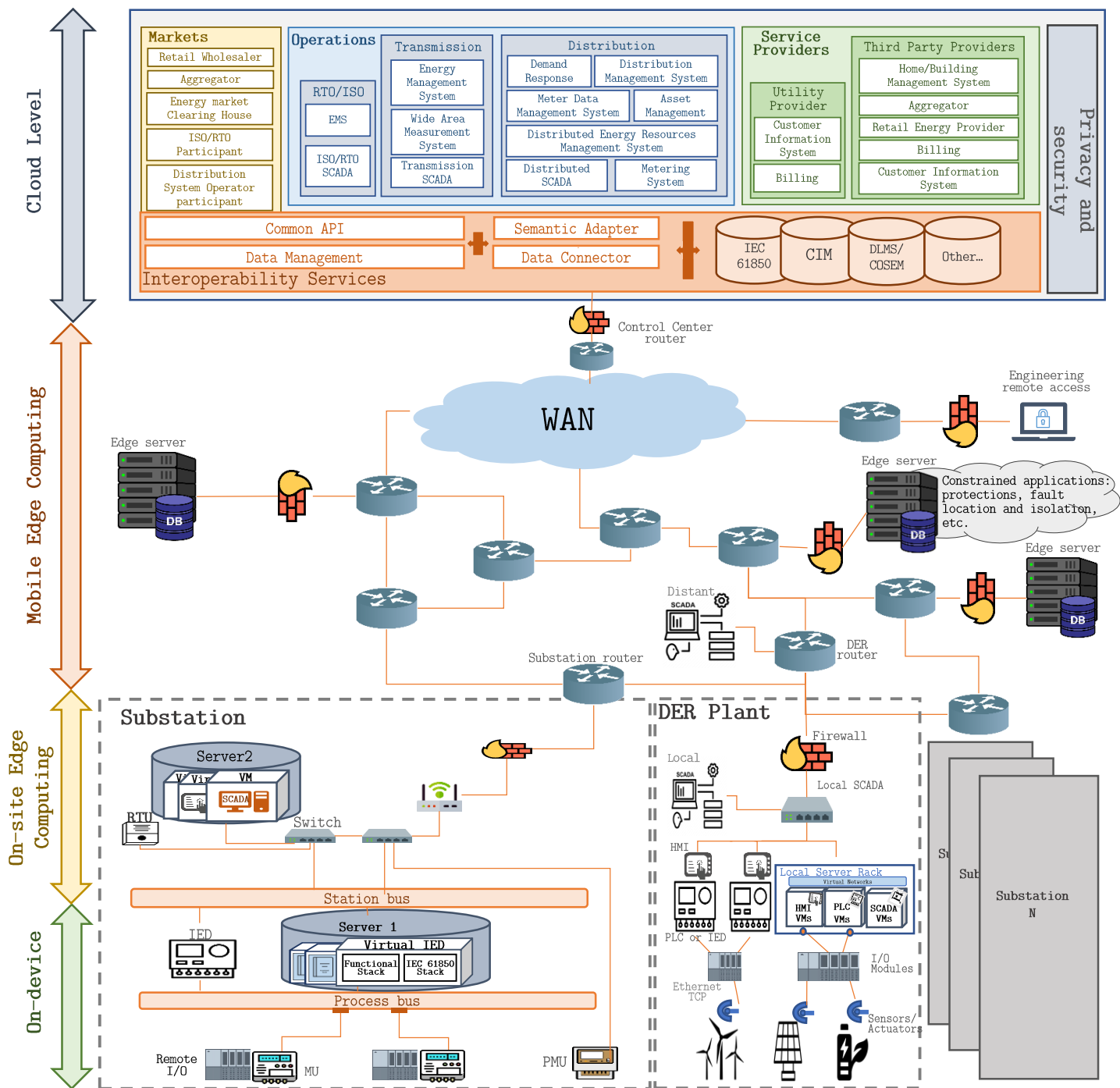


Figure 2.20: Cloud/Edge Computing Architecture mapped to PAC systems in Smart Grids based on [45, 133]

2.3.3.4 Virtualization

Virtualization, a long-standing practice in the IT field, is said to have originated in the late 1960s as a robust time-sharing solution for mainframe computers, according to [131]. This revolutionary concept enabled the optimization of costly, shared computing resources among multiple users. Over time, the concept of computing servers that support the simultaneous running of multiple isolated runtimes with legacy support (such as operating systems and libraries) became increasingly critical. As a result, virtualization techniques were widely adopted in the early 2000s, eventually becoming a standard in the computing

industry [131].

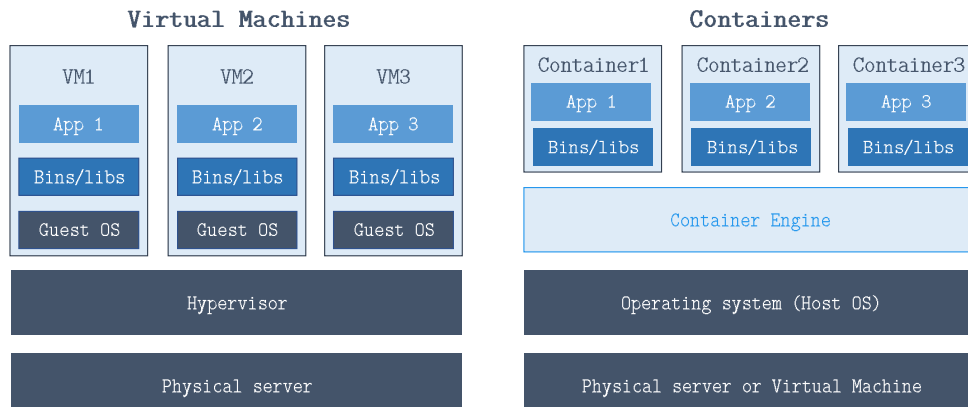


Figure 2.21: Generic Virtualization Architecture

Virtualization relies on software, which is represented by the virtualization hypervisor or container engine layer depicted in Figure 2.21, to mimic hardware-level functions and generate a corresponding 'virtual' or 'software-based' computing environment. The hypervisor plays a crucial role in dividing a single physical (host) hardware and allocating system resources, such as computing power, networking, and storage, among the isolated partitions.

The virtual computing system, commonly known as a 'virtual machine' or VM, provides a self-contained environment that emulates a physical computer. Each VM includes a guest operating system and running software applications that are isolated from the underlying host. This isolation ensures that any changes or issues that may occur within the VM do not affect the host system. Container technology is another popular form of virtualization that is gaining momentum in the IT industry. Containers share the host's kernel, which enables them to be more lightweight than traditional VMs and have less overhead. However, this shared kernel also limits the containers to the host operating system with less isolation. Containers are managed by a container engine, which orchestrates their deployment and scaling. This engine is more efficient than the hypervisor used in classical VMs, making containers more scalable and easier to manage [184].

2.3.3.4.1 Advantages of Virtualization: There are several types of virtualization, including desktop, server (primarily for use in data centers), operating system, networking, and network functions (NFV) in telecommunications [143]. This multidisciplinary adoption is driven by the numerous advantages of virtualization over traditional IT systems. These benefits can be summarized as follows:

- Optimizing resources usage
- Providing larger and more flexible processing and storage capacity
- Reducing the equipment costs (CAPEX) by replacing dedicated hardware with software implemented functions running on inexpensive "off-the-shelf" computing installations

- Reducing operation, and management costs (central remote monitoring)
- Enabling of infrastructure as a service (IaaS) and cloud computing paradigms
- Supporting legacy applications
- Providing disaster Restoration, High availability support
- Allowing simplified backup, cloning, and Snapshots

2.3.3.4.2 Virtualization for Critical Systems and the vIED Concept: Recently, there has been an increase interest in virtualization for real-time systems, particularly in industrial control systems (with virtualized programmable logic controllers PLCs) have gained popularity. According to [134], virtualized PLCs (i.e., a virtual machine or container with soft PLC runtime) have been found to be suitable, with response times ranging from 5-10 ms. The study in [47] provides a comprehensive overview of virtual PLC concepts and their real-time performance, evaluated using consolidated (dummy traffic) workloads.

A virtualized PAC system, also known as a software-defined system, relies on various IEDs that are bundled into logical or software entities and run on standardized hardware. The vIED instance, depicted in Figure 2.22, represents a container or VM that features functional business logic (e.g., droop control algorithms, overvoltage protection, or tap voltage regulator) and an IEC 61850 communication stack.

Recent versions of the VMWare hypervisor ESXI-RT have shown promising deterministic latency⁸ averaging at 3.5 microseconds for a total cycle time of 120 microseconds, as stated in [175]. These results meet the stringent requirements of protection and process control applications.

2.3.3.5 Orchestration of virtual functions

Orchestration plays a crucial role in the efficient digital lifecycle management, especially when transitioning to scalable and software-centric systems. The concept of system orchestration is widely used in various fields such as data centers, microservice architectures, and telecommunications networks. With the use of orchestration technologies, central supervision with remote support of software workloads distributed on heterogeneous devices can be achieved. It helps manage the entire lifecycle of IT infrastructure, including resource usage, scalability, and disaster Restoration policies, ensuring continuous system service delivery.

Figure 2.23 illustrates the key components of the system management tool. The physical layer encompasses primary grid asset I/O modules and standardized computing infrastructure such as IT servers. Each edge or on-premises software platform accommodates portable virtualized applications. With this architecture, edge node management can be conducted remotely at both the local edge level (e.g., digital substation, DER

⁸Deterministic latency refers to the predictable and consistent amount of time it takes for a system to perform a given operation or task.

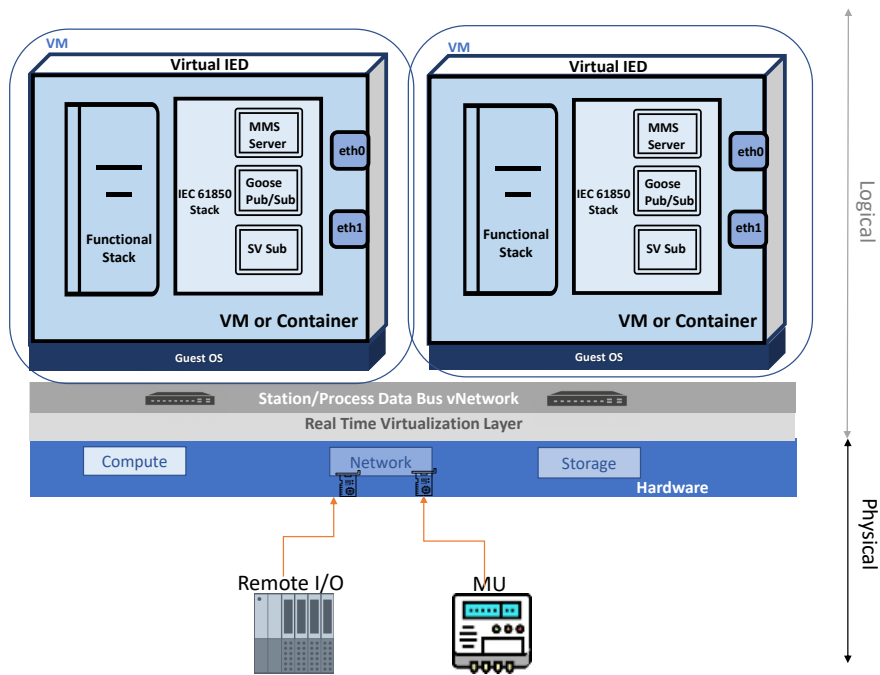


Figure 2.22: Virtual IED concept

plant) and the master node level (e.g., DSO Control Center) within the management plane level, providing flexible and efficient system management.

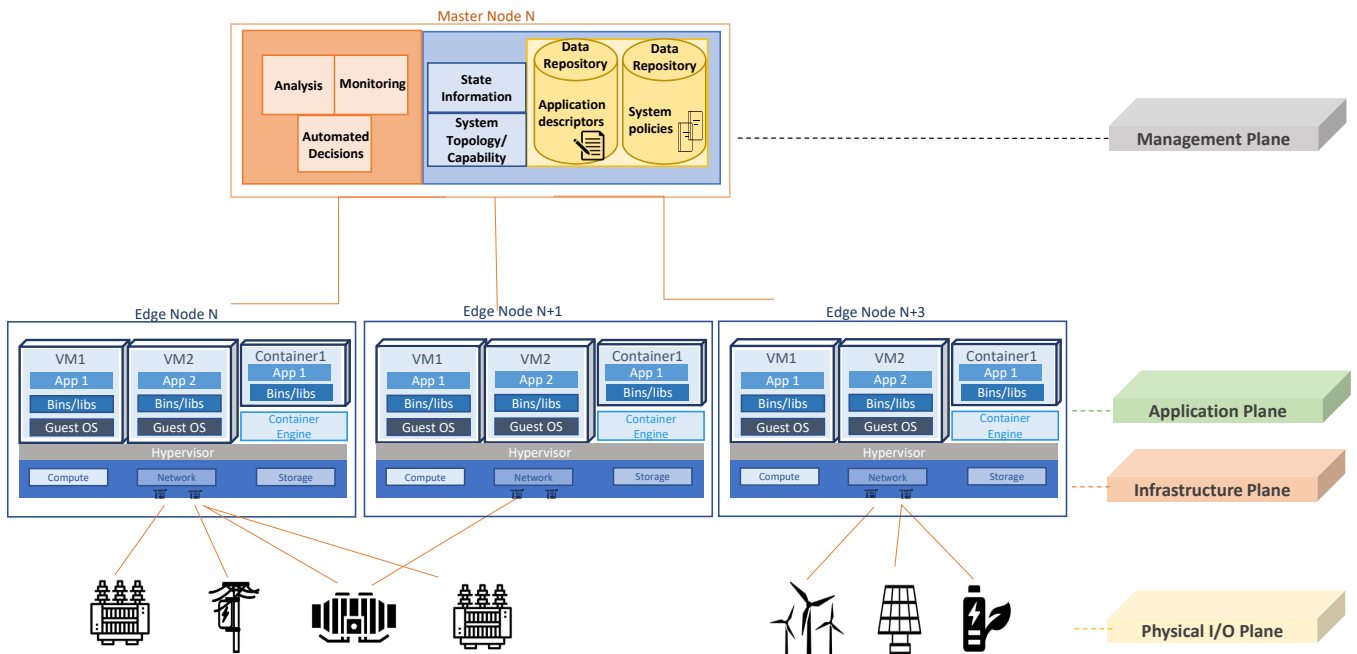


Figure 2.23: Generic system orchestration and management Architecture

All system states, capabilities, policies, and automated decisions required are available at the management plane level, with its primary elements centered around an information model. These elements include:

- **Monitoring:** which involves tracking the usage of hardware resources by edge nodes and the statuses of deployed applications (e.g., virtual IEDs).

- **Analysis:** analyzing the present states by referring to available application descriptors (computing, communication, performance needs) and predefined system policies (intrusion, hardware downtimes).
- **Automated Decisions:** issuing reconfiguration orders in case of system-level anomalies to ensure continuous system service availability.

Using such a model to manage a fleet of virtual IEDs can significantly reduce deployment efforts and optimize system performance. For instance, the tool enables easy deployment of new virtual PAC applications on edge nodes remotely from a central station, without requiring onsite interventions (provided physical I/O cabling is done). Moreover, if the virtual IEDs need an upgrade (e.g., firmware, configuration files) or hardware maintenance, the application can be temporarily redeployed to a different edge node with redirected data streams as needed. However, achieving deterministic compute resource behavior and implementing robust state and time synchronization techniques remain key research challenges.

2.4 Conclusion

In this chapter, we first provide an in-depth introduction of electrical grids and their components, with particular focus on PAC systems. We further explore the limitations of current power protection systems and examine how the integration of new OT/IT concepts can facilitate their evolution. We also introduce DERs and discuss associated challenges of integration at the distribution level. Our analysis indicates that the forthcoming generation of PAC systems will enable more widespread use of DERs.

The second part of this chapter delves into the potential use of the 5G technology to establish a telecommunication-based approach for detecting and mitigating unintentional islanding, as well as developing the next generation of PAC systems. Leveraging the benefits of virtualized and software-defined 5G networks, PAC systems can cater to evolving needs, support multiple applications and services, and ensure end-to-end security and privacy. Moreover, the integration of 5G with other emerging technologies like artificial intelligence, and edge computing can boost the performance and resilience of PAC systems even further.

Chapter 3

5G and Distribution Grid PAC Systems

3.1 Introduction

As stated in the previous Chapter, PAC (Protection, Automation, and Control) systems are critical EPS (Electric Power System) components, designed to protect assets, maintain the reliability and stability, and improve the overall efficiency of the power system.

Indeed, on one hand, protection schemes are designed to detect and isolate faults, which cause equipment damage, power outages, and even danger to human life. Consequently, they need to operate quickly and reliably to minimize the impact of faults on the power system. On the other hand, automation schemes are designed to improve the efficiency and reliability of the power system by automating various tasks. Finally, control schemes are designed to regulate the flow of power in the system, establishing power factor correction, reactive power and frequency control.

All these features are deployed in PAC systems across various spatial configurations, including local, regional, and wide-area. Local schemes protect and control equipment in a specific area of the power system. Regional schemes are designed to protect and control equipment across a specific region (multiple areas) of the power system. Wide-area schemes are designed to protect and control equipment across multiple regions of the power system and can involve communication between different power system operators. Table 3.1 shows a comparison between conventional, current, and future PAC systems.

The development and improvement of PAC schemes have been ongoing since the early days of power system engineering. Initially, protection schemes relied on electromechanical relays, which were manually operated and limited in their functionality. Over time, more advanced and automated protection schemes were developed, making use of digital relays, microprocessors, and communication technologies. Further technological advancements enabled the development of more sophisticated automation and control schemes, including those based on artificial intelligence and machine learning algorithms. These advanced schemes can provide greater flexibility, reliability, and efficiency, particularly in the context of modern power systems that rely on renewable energy sources, energy storage systems, and demand response process. In addition, improvement of PAC schemes

Table 3.1: Comparison between conventional, current, and future PAC systems

Features	Old PAC systems	Current PAC systems	Future PAC systems
Communication / Antenna orientation	Uni-directional (simplex)	Bi-directional (duplex)	Omni-directional / Beam forming
Supporting cell networks	Not supported	2G and 4G	2G, 4G, 5G and beyond
Device / Application Types	Not supported	MBB only	eMBB, uRLLC, mMTC, Hybrid (eMBB + uRLLC)
Network slicing	Not supported	Not supported	Supported
Control	Manual	Automated	Automated and AI-based
Customers / Users side interaction	Limited	Extensive	Unlimited
Instrument Type	Electrical	Numerical	Numerical and Software defined / driven / programmable
Flow control	Limited	universal	Ubiquitous / Pervasive
Customer participation	limited	Extensive with limited contribution	Unlimited with full participation in optimizing system operation
Metering system	Electromechanical	Digital	Digital, AI-based, and Software defined/driven/ programmable
Reliability and protection	Prone to failure and cascading outage; Estimated reliability	Adaptive reliability protection	Predictive reliability based on ML and real-time adaptive protection
Power restoration	Manual/Blind	Self-healing	Self-aware/ healing, autonomous
Grid topology	Radial	Radial	Mesh
Generation	Centralized	Centralized and low integration of DER	Smart generation with distributed architecture and massive DER integration
Response to action	Slow	Fast	Real-time
Operation and maintenance	Physical equipment check, time based maintenance	Remote monitoring, predictive and condition based maintenance	AI-base monitoring with smart supervision and Predictive condition based maintenance
Number of Sensors	Small number of sensors	many sensors	Large number of sensors
Sensor type	Electromechanical sensors	Smart sensor/ hardwired sensors	AI-based and programmable sensors
Latency	high (few minutes)	medium (few seconds)	very low (few milliseconds)
Security/ cyber attack	Less security issue	Secured but vulnerable to modern day cyber attack (DDOS)	Cyber defense system (AI-based grid monitoring and Security by design)
Standardization	-	Not much of work is done on smart grid standardization.	Multi-level interoperability
Protocol compatibility / connectivity	Non	Not with all protocols	Compatible with internet protocols and other protocols like PLC, SCADA.
Interoperability	-	Difficult to cope with different vendor specific devices and protocols.	No vendor-lock, open standards based applications and devices
Platform / Data center (DC) type	Non	Central DC	Central DC and distributed Edge-DC
Cost of communication network	Not expensive	Very expensive	Less expensive
Return on Investment (ROI)	Low	Medium	High
IoT with smart sensing	-	To a large extend	Ubiquitous / Pervasive
Resilience	Not expose to cyberattack but prone to failures	Not too much resistant to attacks and failures	Resilience against failures and malicious attacks can be achieved using AI algorithms

Table 3.1: *Cont.*

Features	Old PAC systems	Current PAC systems	Future PAC systems
Network Management	Complex, time consuming, and manual.	Complex, time consuming, and manual	Automatic / AI driven, and faster.
Granularity	Not attainable	Depend upon proprietary hardware	AI controllers can identify the traffic at every flow and packet level.
Scalability	Very limited	Limited (expensive and time consuming)	Unlimited (faster and cost effective)
Programmability	Not possible	Not programmable	Easily programmable with open interfaces

has also been driven by changes in regulatory and industry standards. Regulatory bodies have introduced new requirements for power system protection, automation, and control, particularly in the areas of cyber security and interoperability. Industry standards have also evolved, with new protocols and communication technologies being developed to improve the reliability and efficiency of PAC schemes. Figure 3.1 illustrates the evolution of PAC systems alongside the advancement in OT/IT and ICT technologies.

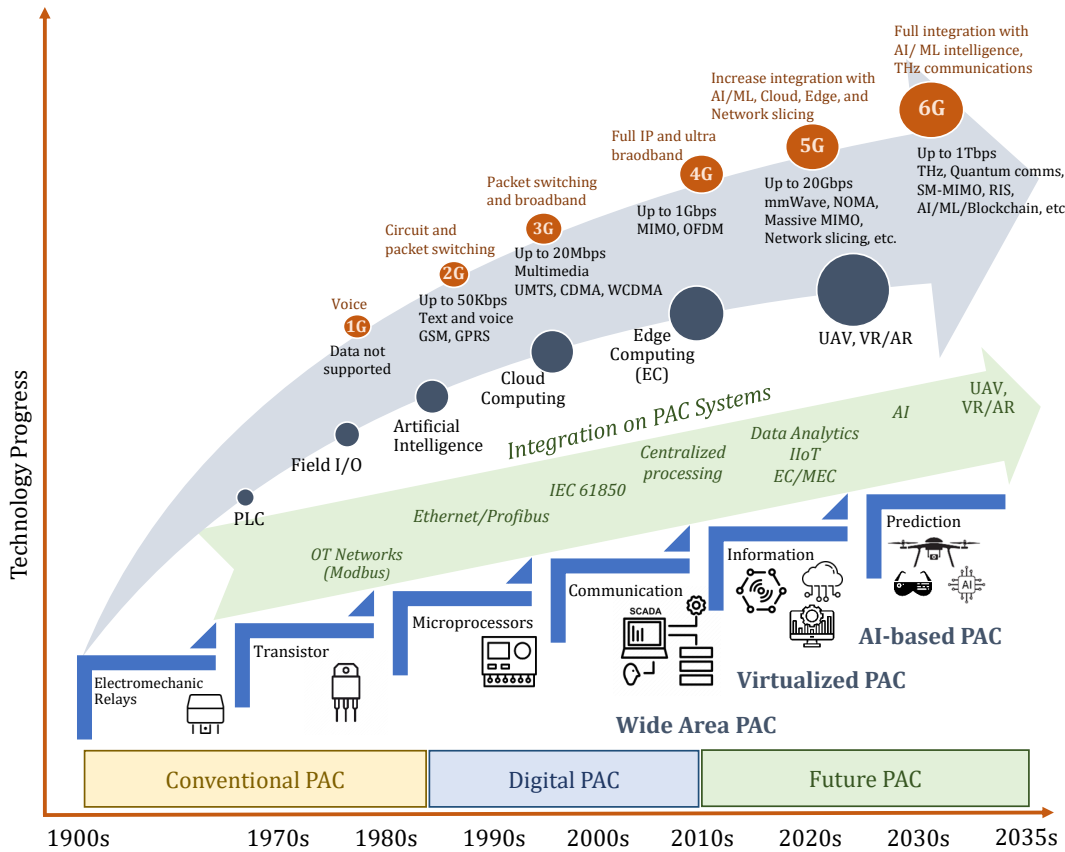


Figure 3.1: Evolution of PAC systems based on [27]

The remainder of this chapter is organised as follows: In Section 3.2, we provide an overview of recent trends and developments in PAC systems for smart grids. We also discuss current research on the use of 5G networks in EPS applications, as well as industrial works on next-generation PAC systems. Then, we highlight the communication requirements of PAC applications in Section 3.3. Next, in Section 3.4 we discuss the specificities of three communication layer categories: Local Area Network, neighborhood/field area

network, and wide area network. Furthermore, a 5G-based architecture to support next generation of PAC systems is proposed in Section 3.5. Finally, in Section 3.6, we showcase the effectiveness of our proposed approach by describing a new FLISR application built upon the proposed architecture.

3.2 Related Works

3.2.1 Trends and Evolutions of PAC systems in Smart Grids

Advancements in communication, information, and networking technologies have brought about changes in PAC design and architecture, a trend that has been observed in prior research discussed in the following paragraphs. Bo et al. [27] conducted a study on the evolution of power system protection and control, which covered the impact of technological advancements and included hybrid, wide area, and local protection and control architectures. These architectures can be coordinated to enhance system performance, and the authors proposed implementing this concept on a distributed real-time synchronized computing platform known as the 'power cloud.' While emphasizing the significance of interoperability¹ and openness of the platform, the authors did not explore the integration of such a platform and architectures with existing protection and control standards.

In their work, Phadke et al. [135] identified various opportunities and motivations associated with the recent development of Wide Area PAC systems, such as monitoring relay characteristics, supervising backup zones, implementing adaptive protections, and managing wide area disturbances. Similarly, the IEEE Power System Relaying Committee [85] examined recent advancements in centralized protection and control architectures and compared traditional (distributed) and various centralized architectures in terms of qualitative metrics (e.g., security, interoperability) and quantitative metrics (e.g., availability, reliability, cost), drawing on experience from a test trial.

Strasser et al. [162] conducted a survey on the requirements of future smart grids with respect to the concept of distributed intelligence in power systems, including the hardware/controller levels and local/coordinated optimizations. The survey also examined the use of software technologies for automation and control of power systems. However, the specific trends towards decentralization and the corresponding implementation technologies were not within the scope of [85, 162].

In their work, Birman et al. [25] examined the suitability of the cloud computing model for smart grid applications, addressing issues such as scalability, real-time operation, consistency, fault tolerance, privacy, and security. Although this research dates back to 2011, all these aspects are still highly relevant. The authors concluded that a dedicated data center or private dedicated internet for power systems is not cost-effective and proposed an integrated cross-sectoral solution. Kruger et al. [99] introduced the concept of 'grid function virtualization', drawing on similar concepts developed by the telecom-

¹Interoperability: Defined by the International Electrotechnical Commission (IEC) as: “*The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units*” [88].

munication industry. However, the authors focused on flexible distribution automation examples, such as state estimation, without discussing trends towards protection and control in digital substations or providing practical feedback from the telecommunication industry’s virtualization experience.

In summary, existing literature indicates that the desired properties of future PAC systems are flexibility, portability, resilience, and interoperability. The prevailing trend is to enhance the operational efficiency of future power systems by utilizing the advanced communication capabilities offered by 5G networks. These capabilities are expected to support seamless and real-time communication between devices, resulting in improved system monitoring, control, and management.

3.2.2 Current Research on the Integration of 5G Technology in Smart Grids

Numerous studies (summarized in Table 3.2) have thoroughly examined the potential of 5G technology in smart grid systems, identifying key challenges and proposing practical solutions to optimize integration and enhance the functionality of these systems.

Reka et al. [42] discuss the current wireless technologies and the architectural changes that have occurred over the past few years. Then, they emphasize the importance of reliable smart grid communication and discuss future roadmaps and challenges that must be addressed to achieve this goal. The work in [118] identifies key challenges that must be addressed for successful deployment of new smart grid services, and examines state-of-the-art 5G-based solutions that can enhance the applicability of smart grids. In [136], the authors focus not only on technical aspects but also on infrastructure and safety, electromagnetic compatibility, worker health, business models, and asset management.

In their article, LOUH et al. [114] investigate the potential of current 5G services to offer an adequate communication platform that enables the seamless integration of distribution grids into transmission systems. They focus on addressing the system’s resilience, particularly in black start scenarios where there is no power and the power autonomy of the towers has reached their maximum capacity. Furthermore, they propose a high-level communication architecture that includes various protection application scenarios.

Almasarani et al. explore how 5G technology can promote the development of advanced smart grid systems in the Kingdom of Saudi Arabia in their study [11]. They also examine the current state of smart grid technology and discuss security concerns surrounding machine-to-machine information on the smart grid. They propose several solutions to identify and mitigate cyber threats that could compromise the security and reliability of the power system.

Esenogho et al. present an innovative vision for a next-generation smart grid, which is powered by artificial intelligence and makes use of IoT and 5G technologies, in their recent article [56]. The authors argue that by combining Massive IoT (MIoT) with the advanced performance capabilities of 5G networks, the development of data-driven services for smart grids will be greatly enhanced, integrating cutting-edge AI techniques.

In their paper [120], Meng et al. begin by discussing the latest developments in the

5G physical layer, which provide the necessary communication requirements for 5G-based applications. They then explore key technologies such as 5G mobile edge computing, computational caching, and network slicing, and describe how these can be leveraged to enhance smart grid functionality. The paper also presents several logical network slicing architectures at the access network, transmission network, and core network levels, which could help to optimize the integration of 5G and smart grid systems.

Ghanem et al. [61] conducted an investigation on the application of 5G technology in smart grid critical applications, specifically in teleprotection. The study aimed to determine the 5G network capabilities required to meet the teleprotection application requirements. The results showed that meeting the requirements for category 1 teleprotection applications (latency less than 6 ms) may not be feasible in the near future. The main constraints preventing 5G from being a reliable and cost-effective option for this category are 5G synchronisation, rural coverage, long delays caused by the number of hops, and the lack of backup power supply. The success of 5G use cases in teleprotection is dependent on the cost to support uRLLC feature, which requires considering security, guaranteed QoS, redundancy, and adequate backup power supply.

Multiple experiments and case studies have been conducted to explore the potential of 5G technology in smart grids. In a distribution grid field experiment conducted at China Southern Power Grid, CAO et al. [177] explored the use of 5G NSA network with virtualization capabilities. The authors implemented two separate slices - a smart grid slice with differential protection and automation & control sub-slices, and an eMBB slice for public and business applications. The achieved results were promising, with an average latency of 8.3ms and 100% reliability, demonstrating the effectiveness of the 5G-based solution.

In [160], Joice maps the communication requirements of smart grid applications to the unique characteristics of 5G technology. To demonstrate the feasibility of these concepts, an energy distribution company in Brazil performed a Proof of Concept that included use cases associated with remote assistance (Digital Twin), teleprotection, and LV/MV pole transformer monitoring. The outcomes demonstrated that the 5G private network outperformed the 4G public network. The 5G network achieved a latency of approximately 40ms/54ms in the uplink/downlink direction.

In their recent publication [141], Porcu et al. introduce the concept of network applications (NetApps) as a new virtualization paradigm, with the potential to create a new market for information technology, small and medium enterprises, and startups. Furthermore, they showcase four 5G-compatible demonstrators that demonstrate the NetApps concept and the architecture that enables its implementation. These include automatic MV fault detection, real-time security monitoring for operators in HV substations, remote monitoring of DERs, and cross-border wide area monitoring.

In their article [105], Leligou et al. propose a conceptual framework and a set of approaches for leveraging the benefits of the 5G ecosystem and making it compatible with the next generation of smart grids. The proposed framework is developed under the Public Private Partnership (5G-PPP) framework and the European Commission-funded project H2020 ICT-762013 NRG-5 [128].

In summary, the examined works demonstrate that 5G technology, with its low latency, reliability, flexibility, and scalability, has the potential to enable various smart grid applications, particularly those related to PAC systems. The trend is to enhance the operational efficiency of future power systems by incorporating best implementation practices from the IT world, such as virtualization technology. This can enable the creation of a flexible and resilient power system infrastructure that can adapt to dynamic changes in energy demand and supply.

Table 3.2: An overview of studies investigating the potential of 5G technology in smart grids

Paper	Network	Experiment	Use Case	ICT concepts
[177]	Private 5G	Field	i) Differential protection; ii) Automation and control	Network slicing, Virtualization, Synchronization
[114]	/	/	i) Protection IEDs with monitoring and control, 5G as backhaul to private fibre optical network; ii) Multi-branches topology with hybrid underlying communication; iii) CPC, WAPC, WAMPAC	Synchronization, 5G LAN-virtual network, Network Slicing, resilience
[160]	Private 5G/ 4G public	Field	i) Teleprotection ; ii) Digital Twin; iii) LV/MV transformers monitoring	5G local networks
[136]	/	/	/	Network slicing, Infrastructure and security, Electromagnetic aspects, Business models, Asset management
[42]	/	/	/	Architecture 5G, Applications of 5G
[11]	/	/	/	WSN, Attacks on WSN, Security in 5G based SG, Cybersecurity strategy
[56]	/	/	/	Architecture 5G, Applications of 5G, SDN, NFV, Network Slicing, Distributed architecture
[141]	Private 5G	HiL	i) Automatic power distribution grid fault detection; ii) Remote inspection of automatically delimited working areas at distribution level; iii) Millisecond level precise distribution generation control; iv) Real-time wide area monitoring in a creative cross-border scenario	SBA, Edge/cloud separation, SDN/NFV, Orchestration
[120]	/	/	/	5G physical layer, Mobile Edge Computing, Computational caching, Network slicing
[118]	/	/	/	Cloud computing, Fog computing, Edge Mobile Computing, Network slicing, SDN/NFV
[61]	/	/	Teleprotection	Network Slicing, SDN/NFV
[105]	Private 5G	HiL/Field	i) AMI as a Service (AMIaaS); ii) Dispatchable Demand Response as a Service (DDRaaS); iii) Predictive Maintenance as a Service (PMaaS)	Cloud computing, Fog computing, Edge Mobile Computing, Network slicing (xMBB, uMtc, mMTC), SDN/NFV, Orchestration, Security, UAV/Drones
Our Work	Private 5G	HiL/Field	i) Remote decoupling; ii) FLISR	Cloud computing, Edge Computing, Virtualization, Orchestration

3.2.3 Main Industrial Works on next-generation of PAC systems

Alongside the research studies focusing on the use of 5G in smart grids, there has been a recent surge in the development of industrial pilots and proof of concepts for virtualized PAC systems, as shown in Table 3.3. The objectives of these endeavors have been diverse, ranging from proposing reference architectures and specifications to developing integrated hardware and software platform solutions. Such initiatives represent significant advancements in the practical implementation of virtualized PAC systems

Table 3.3: Industrial proofs of concepts for virtualized PAC systems.

Project Name	Lead	Scope	Virtualization Technology Used	Domain	Applications
SOGNO [133]	EU/LF Energy	Reference concept of a modular, interoperable service-oriented design of data-driven distribution automation systems	Docker Kubernetes	Distributed Automation	Aut- State Estimation, Power Control, Quality, Fault Localization, Load Forecasting
EU projects [138, 45]	EU	Re-utilizing [133]’s reference platform for virtual power plants and market based data exchanges	Docker Kubernetes [100]	Distributed Automation	Aut- Voltage, Frequency control
SEAPATH [106]	LF Energy	Reference concept/design and real time platform for industrial electricity system operators to execute their virtualized applications for automation and protection.	KVM [109]	Digital Substation	-
Centralized Substation Platform [53]	EPRI	Virtual computing platform for electric substations to support SCADA and management applications while meeting cybersecurity requirements	-	Digital Substation	-
Grid Management platform common design architecture GMP [1]	Dell, Intel, VMWare	Virtual computing platform running in edge substation or control center supporting legacy applications and security standards	VMware	Digital Substation, Distribution Automation	Grid -
Edge for Smart Secondary Substations [43]	Consortium	Reference architecture design for open, interoperable standards-based platform for digital secondary substations	-	Digital Substation	Secondary Substation Automation
Virtual Protection Relay (VPR) [148]	Kalkitech, Intel	VPR reference architecture hosting protection applications to benchmark against legacy applications and a framework to support onboarding of VPR	VMware	Digital Substation	Protection

A docker-based platform for containerized distribution grid automation domain was developed as part of the European project SOGNO [133], now part of the open-source

Linux Foundation (LF) Energy. The SOGNO project demonstrated the benefits of microservices, a lightweight, scalable software development architecture [21, 90], for distribution system operators' control center information systems. Several advanced soft RT functionalities (e.g., LV state estimator, fault isolation, power control) were validated in different field trials. The architecture proposed in [133] also envisioned an interoperability layer, with IEC 61850 protocol gateways and support of grid topology based on CIM (Common Information Model is defined in Section 7.3) data. Several European projects utilized the SOGNO reference architecture as part of their advanced smart grid platform implementations (e.g., EdgeFlex [45], Platoon [138]). However, SOGNO does not directly deal with virtualized IEDs at process levels or within substation domains.

Another project led by LF Energy, the SEAPATH project [106], mainly focused on providing a reference hard real-time platform running virtualized substation automation systems (and beyond). KVM [109], an open-source hypervisor, forms the base of the platform with docker support, advanced data processing technologies (e.g., Data Plane Development Kit DPDK [41]), and several integrated administration and security services. Testing the availability, performance, and reliability of the platform and virtualized automation applications based on lab measurements (with IEC 61850 communications) are within the envisioned scope of SEAPATH.

The Electric Power Research Institute (EPRI) surveyed specific considerations for centralized digital substation platforms [53]. The areas covered among others were cybersecurity support, intrusion detection, access control, network support, fault tolerance, firmware management, and scalability. A collaboration between Dell, Intel, and VMware aims to develop the proper hardware servers responding to the needs of centralized/virtualized substation PAC systems and power system operators' modernized control centers [1].

Recently, an international consortium of utilities, distribution grid operators, integrators, and IT technology experts was developed as part of the 'Edge for Smart Secondary Substations' project [43]. This consortium focuses on specifying reference technical hardware/software requirements and end-to-end application management for proactive secondary substations.

The VPR solution for hard RT² (Real-Time) requirements in substation automation was jointly developed by Intel, and Kalkitech [148]. The research analyzed response time (referring to IEC 61850 requirements) against different network configurations and resource allocations with parameter sensitivity studies. Furthermore, virtual networking redundancy and time synchronization requirements were discussed. Promising results were shown with time delays equivalent to existing protection systems.

Moreover, industrial products specialized in providing hardware-level centralization and virtualization of IEDs are being researched by leading vendors [172, 26, 98]. The interest in a microservice architecture (container-based) for substation protection applications was analyzed by [72]. Preliminary results showed multiple practical issues (mainly compatibility, resources, dependencies, and overhead) which made the transition to containerized protection non-straightforward. Industrial standardized servers (compli-

²real-time system whose operation is incorrect (*totally fails*) if results are not produced according to specified timing requirements

ant with IEC 61850-3 [76]) that can run virtualized IEDs have emerged, yet still lack proper installation and operation frameworks.

Summarizing, the current maturity of industry solutions for virtualized PAC systems is at its early stages (mainly through pilots and proofs of concept). The areas covered both deterministic latency (hard RT protection and control) as well as soft RT (mainly automation and SCADA, secondary substations). Some market-ready solutions exist but are limited to specific vendor implementations and hence do not fully harvest the advantages of virtualized PAC systems. The tool interfaces remain proprietary and easy to use frameworks are still lacking. Moreover, the maintainability and support of the platform itself and the responsibilities of the involved stakeholders (e.g., grid operators, virtualization platform maintainers, certification bodies) have yet to be explicitly addressed. Another observation concerns the proposals of different 'reference' architectures within these projects. Unless these diverse 'references' somehow converge, a significant complexity will be added for future PAC systems deployments.

3.3 Communication Requirements of Next generation PAC systems

For PAC applications, in order to provide a high-quality service, the communication infrastructure must meet certain quantitative and qualitative requirements [113, 67, 179, 13, 60, 62]. These include:

3.3.1 Quantitative Requirements

- *Latency*: This refers to the end-to-end transmission delay between PAC components. For mission-critical applications such as substations protection and control, and distribution automation, the maximum delay requirement must be met for efficient operation.
- *Bandwidth and RF spectrum limitations for PAC systems*: The communication infrastructure for PAC systems must be able to provide the necessary data rate required by the application. The bandwidth and RF spectrum of the communication channels must be considered, as different frequency ranges have different capabilities. High and medium frequency ranges can be used for short-distance communication that requires high data rates, while low-frequency ranges can be used for long-distance communication with various PAC components. Lower frequencies can penetrate linear and non-linear objects more easily, avoiding line of sight (LoS) constraints posed by higher frequencies.
- *Reliability*: This measures how successfully communication systems exchange messages in a timely manner according to their specifications. The more critical the application, the greater the required level of reliability. Additionally, PAC applications require different levels of reliability, so the communication infrastructure must

allow for different reliability levels for data exchange.

- *Throughput*: This is defined as the sum of the data rates that are delivered to all terminals (i.e., IEDs) in a network. PAC applications generate various types of data (text, pictures, audio, video, etc.) at different rates, so the required throughput by a PAC application depends on its characteristics.
- *Synchronisation*: is one of the main challenges in building time-critical PAC applications. Current communication technologies may not be sufficient to guarantee high accuracy synchronization ($< 3\mu s$ [61]) for some PAC applications. The radio part or fronthaul might be susceptible to weather and signal propagation noise. Network congestion can also exacerbate latency and impact synchronization. mobile network operators (MNOs) relying on GPS may face issues with jamming and weather conditions, which can result in errors in the IEDs. Furthermore, each IED can contribute to time error, creating synchronization difficulties. Additionally, TDD is more common in 5G networks, but achieving time synchronization is more challenging than in FDD.

3.3.2 Qualitative requirements

Qualitative requirements on SG applications are illustrated in Figure 3.2.

- *Data accuracy*: refers to error-free data that can be used as a reliable source of information. It is an essential data quality index that directly affects the efficiency, performance, and economic benefits of PAC applications.
- *Data validity*: ensures that data from various PAC components have undergone data cleansing and can be considered useful information.
- *Accessibility*: means that PAC application services are accessible to all customers without discrimination.
- *Interoperability*: measures the ability of various PAC components to exchange data and coordinate to perform a specific task. Interoperability is essential in both networks and PAC applications to ensure standard data exchange with the same meaning, and to integrate legacy communication equipment that does not support the latest communication protocols and security features.
- *Scalability*: The communication infrastructure should be scalable from both technical and economic standpoints. PAC systems rely more and more on ICTs and can include millions of customers and many connected devices. The telecom infrastructure should ensure the transition to scale while meeting different PAC application requirements.
- *Flexibility*: involves supporting communication requirements of diverse PAC applications and delivering various communication models with a high degree of flexibility and self-adaptability.

- *Security*: A PAC system is a critical infrastructure in which sensitive data are exchanged. Therefore, security, both physical and cyber-security, and privacy are essential for preventing any vulnerability to PAC assets. Securing connections between PAC devices increases bandwidth overhead and processing time required for each PAC application.
 - *Device authenticity*: Accessing services (e.g., manufacturing tests, software debugging) should be permissible with an approved procedure.
 - *Data confidentiality*: Associated with the generation, transmission, manipulation, and storage of private information on consumers generated dynamically by the various PAC services. This information should not be accessible to unauthorized persons.
 - *Data authenticity and integrity*: Ensures that customer information and transactions are reliable. It is crucial to confirm that the identity of both parties is as claimed by them for authenticity purposes.
 - *Customer privacy and security*: Consumer privacy protection is the main condition of current PAC infrastructure. Hence, PAC applications must ensure secure storage of customer data.

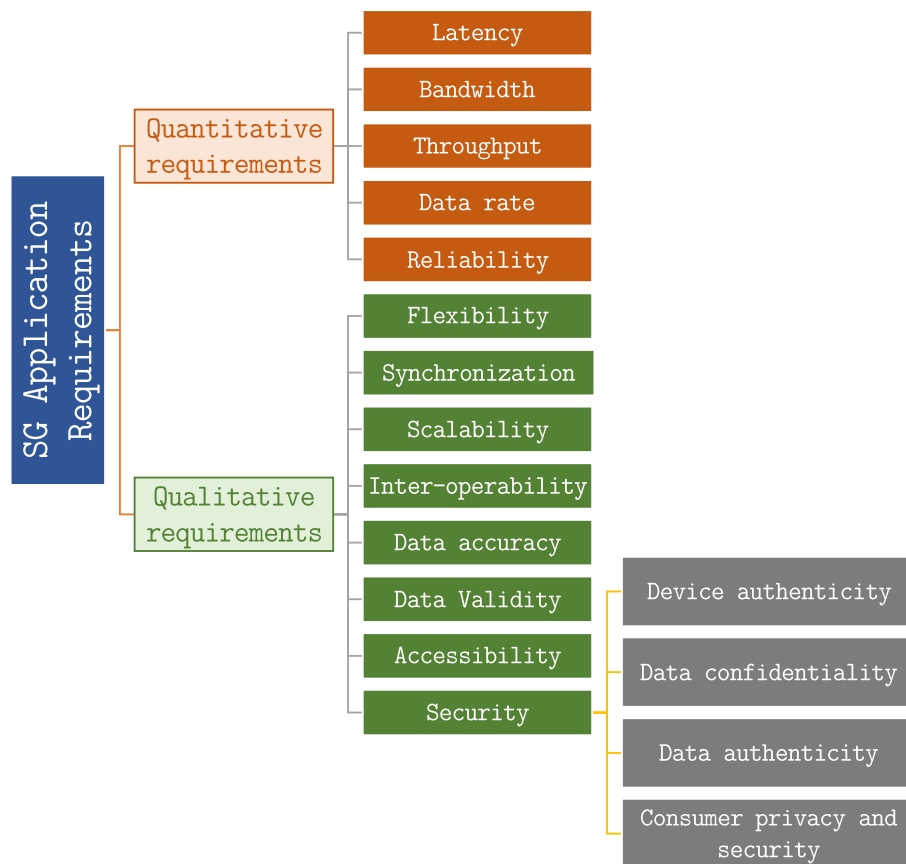


Figure 3.2: Communication requirements on Smart grid applications

3.4 Communication layer categories

PAC systems play a crucial role in power system operations by processing extensive amounts of data for critical applications. Reliable and real-time communication is imperative in PAC systems communication architecture, which is hierarchical and governs two extremities: a central-slow level and a local-fast level.

The local level guarantees simple, safe, and fast functions based on local information and operates on very fast timescales. The central level enables coordinated actions on a large scale, using complex algorithms, slower action times, and requires collecting information from dispersed grid components.

However, the downsides of this hierarchical structure were thoroughly studied by an IEEE Smart Grid Research group [14]. They recommended moving part of the "intelligent control" from the central-regional level to an intermediate-zonal level as a future vision by 2030. This new control architecture sets stringent communication requirements to ensure robust coordination and integration of heterogeneous smart grid elements.

The efficient, reliable, and flexible management of power grid operations requires the real-time exchange of meaningful information from different electrical grid components [68]. Basic communication categories in smart grids include wide area networks (WAN), neighborhood/field area network (NAN/FAN), and local area networks (LAN). These categories are interconnected hierarchically, as illustrated in Figure 3.3.

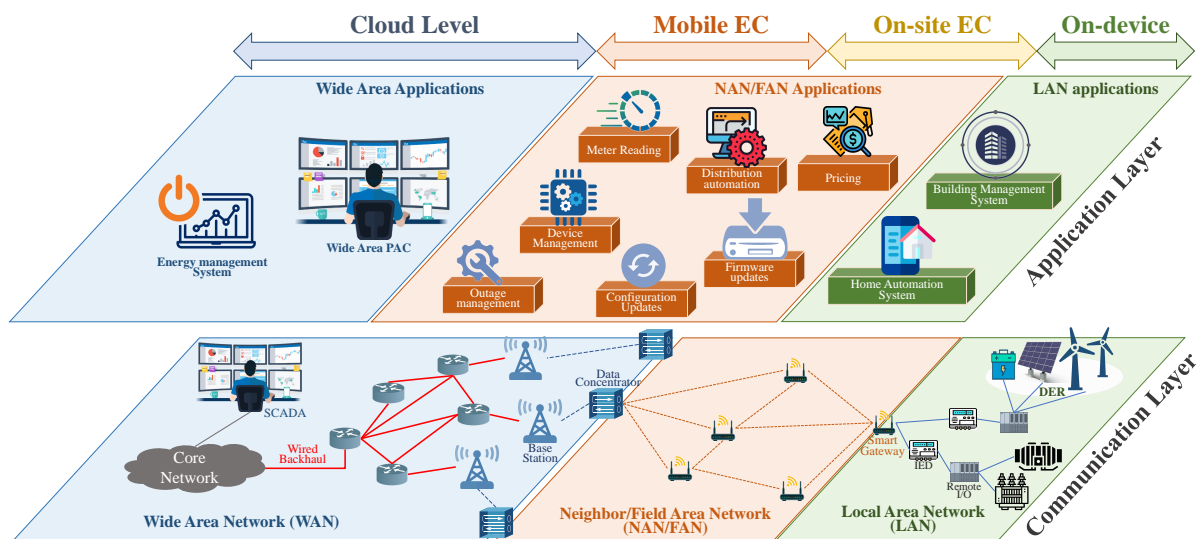


Figure 3.3: Communication categories interconnection [101, 182, 7]

The content of this section is summarized in Table 3.4, which illustrates communication requirements of various PAC applications.

3.4.1 Local Area Network

PAC system applications that are LAN-based facilitate data exchange between IEDs and a controller located in close proximity to the power grid, such as in a substation. A LAN can be connected to other stakeholders in the smart grid, such as an electric utility or third-party energy service provider, through a gateway. Since all data exchange

occurs in close proximity to the power grid, the communication requirements for LAN applications of PAC systems are low latency, high reliability, low cost, simplicity, and security. Furthermore, LAN networks can enable the Distribution System Operator (DSO) to perform NAN/FAN applications in the vicinity of the IEDs [65].

3.4.2 Neighborhood/Field Area Network

NAN and FAN are two types of networks within the distribution domain that support information flow between WAN and a LAN using either wireless or wired communications. They allow for the collection of data from different points on the electrical distribution grid for transmission to a data concentrator/substation, or vice versa. As a result, these applications require communication technologies that support higher data rates (ranging from 100 kbps to 10 Mbps) and larger coverage distances (up to 10 km). NAN/FAN enables a range of smart grid applications, such as smart metering, load management, distribution automation, pricing, outage management and restoration, or other customer-based applications [111, 174]. The NAN/FAN also enables services such as monitoring and controlling electricity delivery to each end-user, as well as distribution automation.

3.4.3 Wide Area Network

The Wide Area Network is essential to provide intelligent backbone networks with communication links covering long distances from control centers to NAN/FAN. This enables a range of smart grid applications, such as wide-area PAC and the transmission of high-frequency data from many measurement points. As a result, a well-coordinated control is allowed, significantly improving the stability of the power system. Furthermore, managing various IEDs can provide a range of services, such as substation automation, distribution grid automation, and outage management.

Wide area PAC applications represent a significant evolution to improve the operation of the EPS. They use system-wide information and selected local information to limit the propagation of large disturbances, offering higher data resolution and faster response times than traditional SCADA and EMS systems. While SCADA/EMS provides a cyclic measurement update interval of several seconds or even minutes, wide-area PAC applications provide high-resolution data. Real-time measurements are taken across the entire EPS by IEDs and sent to control centers, while instructions and commands are sent from control centers to IEDs.

Since WAN applications require a larger number of data points at high data rates (10 Mbps-1 Gbps) and long-distance coverage (10-100 km), optical communication is most often used as a communication medium due to its high capacity and low latency. Cellular can also be used because of its wide coverage range and high data rate. Satellite communications provide backup communications medium for critical sites.

Table 3.4 illustrates the communication requirements of various PAC applications [101, 8, 167, 57, 77, 83], and the coverage of each communication layer category considering the required data rate is depicted in Figure 3.4.

Table 3.4: PAC application communication requirements

Level	Communication Technologies		Application	Bandwidth	Latency	Reliability
	wired	wireless				
LAN	Coaxial Cable, Ethernet	Bluetooth, Transfer tripping		< 10 kbps	3–10 ms	> 99.99%
		ZigBee, GOOSE		-	4 ms	> 99.99%
		Z-wave, Sample Value SV 5G		80, 256 samples per 20 ms	-	-
		IED to IED interlocking		9.6–64 kbps	< 10 ms	> 99.99%
		IED to IED, reverse blocking		9.6–64 kbps	< 10 ms	> 99.99%
		AMI		UL 100 kbps	2–15 sec	> 98 %
		DER and ESS		DL 500 kbps		
		Meter reads		9.6–56 kbps	0.02–15 sec	> 98 %
		ZigBee Pro, Connects and disconnects		10 kbps	2–10 sec	> 98 %
		WiFi, Distribution system monitoring and maintenance		Low	0.1–300 sec	> 99 %
NAN	Coaxial Cable, Ethernet,	Cellular, Volt/VAR control		10–30 kbps	< 5 sec	> 99.5 %
FAN	DSL, Fiber optic,	LPWAN, Distribution system demand response (DSDR)		10–30 kbps	< 5 sec	> 99.5 %
		Satellite FLISR for distribution grids		10–30 kbps	< 4 sec	> 99.5 %
		Optimization for distribution grids		2–5 Mbps	few 100 ms	> 99.9 %
		Protection for microgrids		-	25–100 ms	> 98 %
				-	0.1–10 sec	> 99 %
		DR		14–100 kbps	0.5–600 sec	> 99.5 %
		DMS		9.6–100 kbps	0.1–2 sec	> 99 %
		Video surveillance		100–1000 kbps	1000 ms	> 99 %
		Wide-Area Situational Awareness (WASA)		600–1500 kbps	15–200 ms	> 99.9 %
		Outage management		56 kbps	2 sec	> 99.9 %
		Cellular, Wide-Area Monitoring PAC		10–100 kbps	< 10 ms	> 99.99 %
WAN	Coaxial Cable, DSL, Fiber optic	LPWAN, Adaptive islanding		-	< 100 ms	> 99.9 %
		Satellite Cascading failure control		-	< 5 sec	> 99.9 %
		Wide-area voltage stability control		-	< 5 sec	> 99.9 %
		SCADA		-	< 5 sec	> 99.9 %
		PMU-based state estimation		-	< 100 ms	> 99.99 %
		Dynamic state estimation		< 1 Mbps	10–200 ms	> 99.9 %
		Fault location		-	100 ms	> 99.9 %
				< 10 kbps	10 ms	> 99.99 %

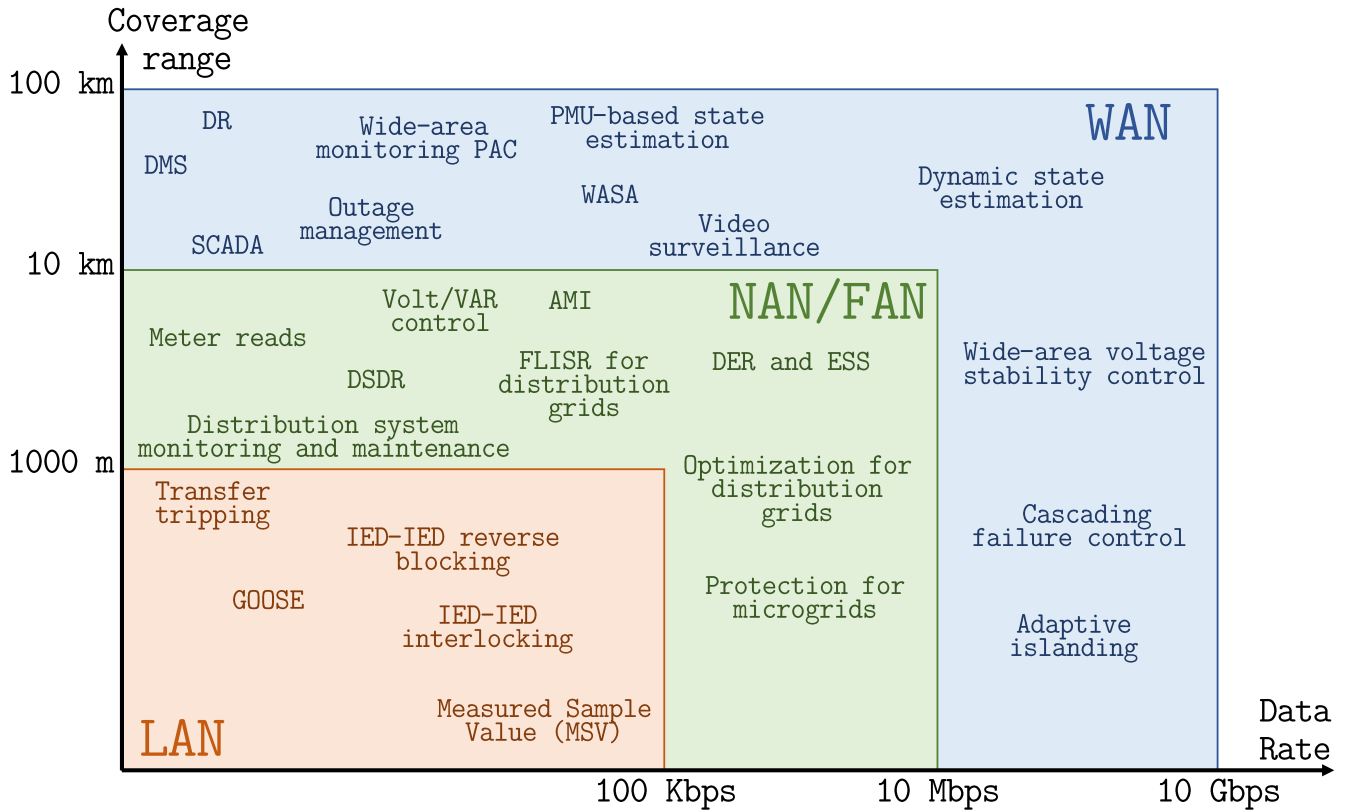


Figure 3.4: Coverage and data rate of each communication layer category

3.5 Proposed 5G-based architecture for PAC system

In this section, we present our proposed 5G-based architecture for PAC systems. It leverages edge computing and virtualization capabilities to deliver tailor-made communication services that meet a wide range of performance requirements demanded by various PAC system applications. The PAC functions are strategically deployed across three different levels - local, edge, or cloud - based on two main parameters: the application's criticality and the level of situational awareness.

To ensure a fine-grained approach based on use cases, the deployment of associated virtual functions in the proposed PAC system architecture, as illustrated in Figure 3.5, must adhere to a hierarchical organization [46]. This approach has a significant impact on function criticality and the level of situational awareness, which are the two primary factors used to determine the most suitable layer for deploying PAC functions. The lower layer comprises EPS devices forming a wide area measurement system, while the middle layer features a local controller that stores and analyzes the data to address local issues. The upper layer contains the central controller, which has a comprehensive system snapshot to address wide area problems.

The optimal deployment level for PAC applications is determined by the specific service requirements and performance objectives as illustrated in Figure 3.6. Applications with less stringent requirements (such as a global situational awareness of the distribution grid) with latency greater than 1 second, can be deployed at the cloud level. For applica-

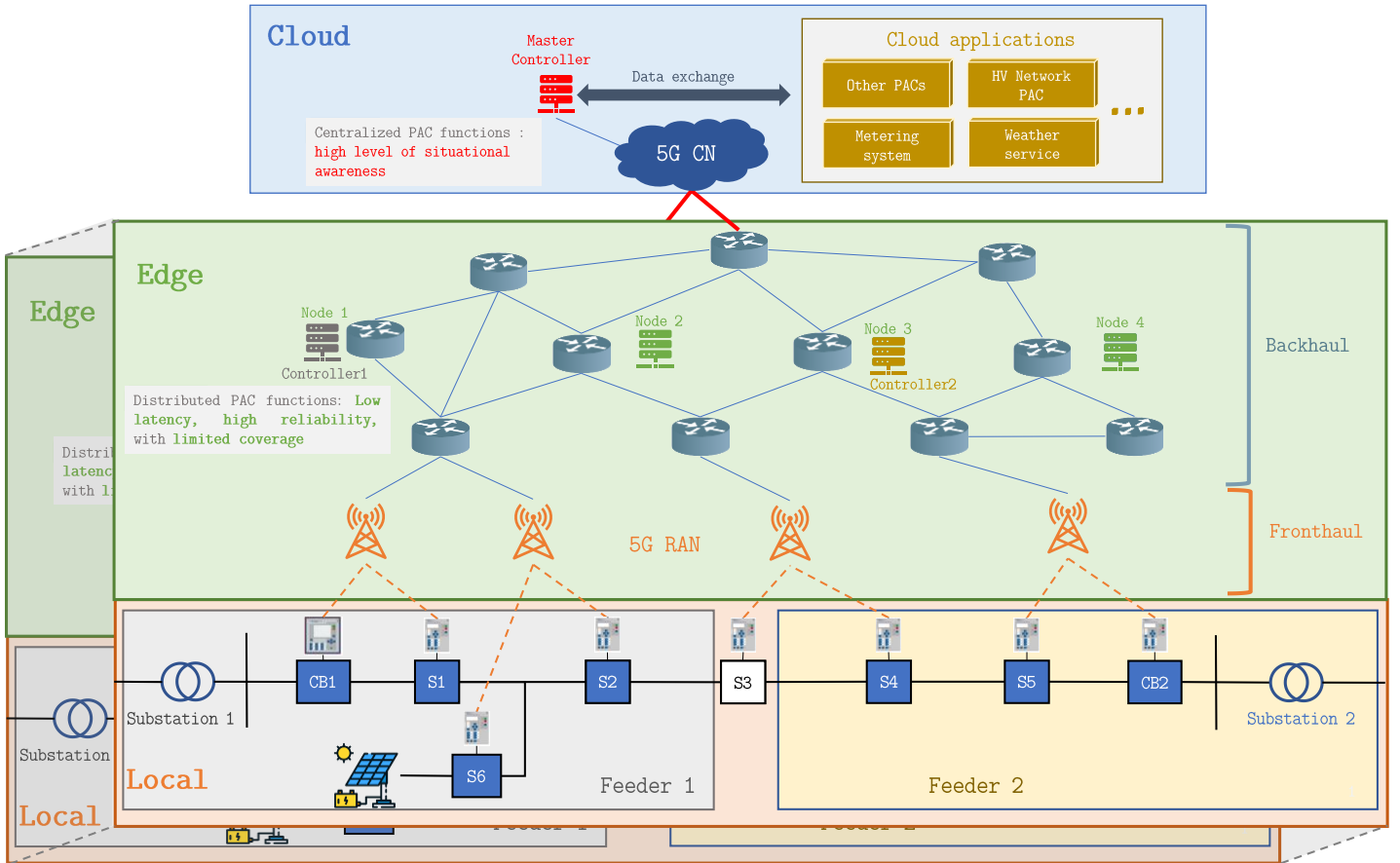


Figure 3.5: Proposed architecture for 5G-base PAC system

tions with an end-to-end latency between 5 milliseconds and 1 second and an operation scope centered on a single substation, the edge level is recommended (protection functions based on IED can be implemented at this level to optimize performance). Finally, for applications with very low latency requirements (less than 5 milliseconds) and a local operation scope, deployment at the radio site, as close as possible to the power network components, is necessary to ensure optimal performance.

3.6 Developed PAC application : FLISR

A FLISR (Fault Location, Isolation, and Service Restoration) application is a process used in power distribution grid to quickly detect and isolate faults in the system, and restore power to the affected areas [161].

The Fault Location stage involves identifying the location of the fault in the grid, while Isolation involves isolating the faulty section from the rest of the grid to minimize the impact of the fault. Finally, the Service Restoration stage involves restoring power to the affected areas by re-routing power from alternative sources or repairing the fault.

An efficient FLISR system is crucial to enhancing the reliability and quality of power supply grids by maximizing restored loads and minimizing the outage duration [186]. It is achieved through the use of advanced technologies such as smart sensors, real-time monitoring, and automation, which allow for faster and more accurate detection and isolation of faults.

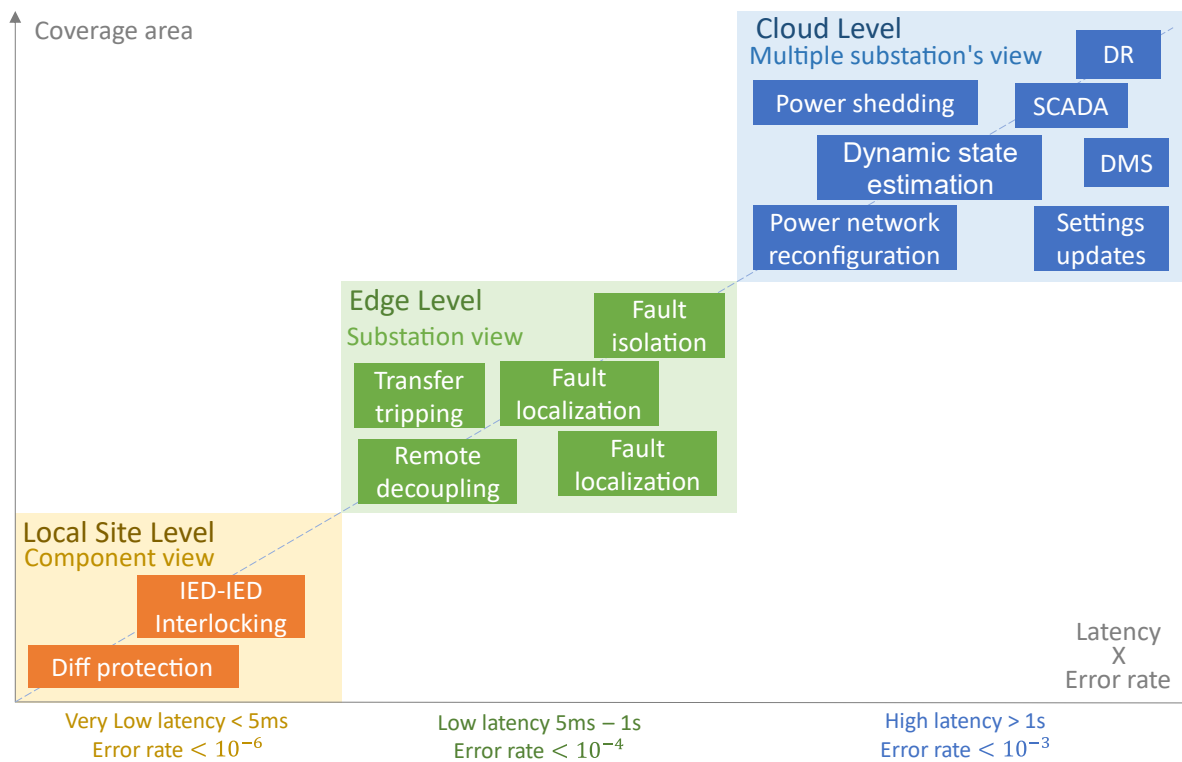


Figure 3.6: Example of PAC function deployment

3.6.1 Comparison between conventional and automatic FLISR system

Traditional FLISR relies on manual intervention to locate and isolate faults, whereas automatic FLISR uses advanced automation technologies to perform these tasks automatically. The Figures 3.7 and 3.8 show, respectively, the average time execution of conventional and automatic FLISR process. Here are some of the key differences between the two:

- **Fault detection and location:** In traditional FLISR, fault detection and location relies on manual inspection and testing of the grid, which can be time-consuming and prone to errors. In contrast, automatic FLISR uses advanced sensors and algorithms to detect and locate faults in real-time, which enables a much faster response time.
- **Isolation and system Restoration:** Once a fault is detected and located, traditional FLISR requires manual intervention to isolate the faulted section of the grid and restore power to the affected areas. This process can take a significant amount of time and requires skilled personnel. Automatic FLISR, on the other hand, uses advanced automation technologies to quickly isolate the faulted section and restore power to the affected areas, without the need for manual intervention.
- **Accuracy and reliability:** Traditional FLISR can be prone to errors, as it relies on human judgement and manual testing. In contrast, automatic FLISR is highly accurate and reliable, as it uses advanced algorithms and sensors to detect and locate faults in real-time.

- **Cost and scalability:** Traditional FLISR can be costly and difficult to scale, as it requires a significant amount of manual labor and skilled personnel. Automatic FLISR, on the other hand, is highly scalable and cost-effective, as it relies on advanced automation technologies that can be easily deployed and managed.

In summary, While traditional FLISR has been used for many years, it suffers from several limitations that make it less effective than automatic FLISR. Automatic FLISR offers faster, more accurate, and more reliable fault detection, isolation, and system recovery, making it an attractive option for power distribution networks seeking to enhance their resiliency and reliability.

The deployment of automatic FLISR can be democratized with the use of 5G technology, which provides a flexible, cost-effective, and easily deployable communication infrastructure even in isolated locations. Furthermore, the high reliability and low latency of 5G enable the integration of remote decoupling mechanism into the FLISR process, which protect the distribution grid against unwanted islanding and untimely disconnection. This allow a seamless integration of DERs in MV/LV systems.

On one hand, Virtualization facilitate the implementation of tailored virtual FLISR functions on IEDs without being restricted by software and hardware provider lock-ins. On the other hand, orchestration enhances the ability to manage the deployment and maintenance of virtual functions, leading to a more flexible and easily scalable FLISR application.

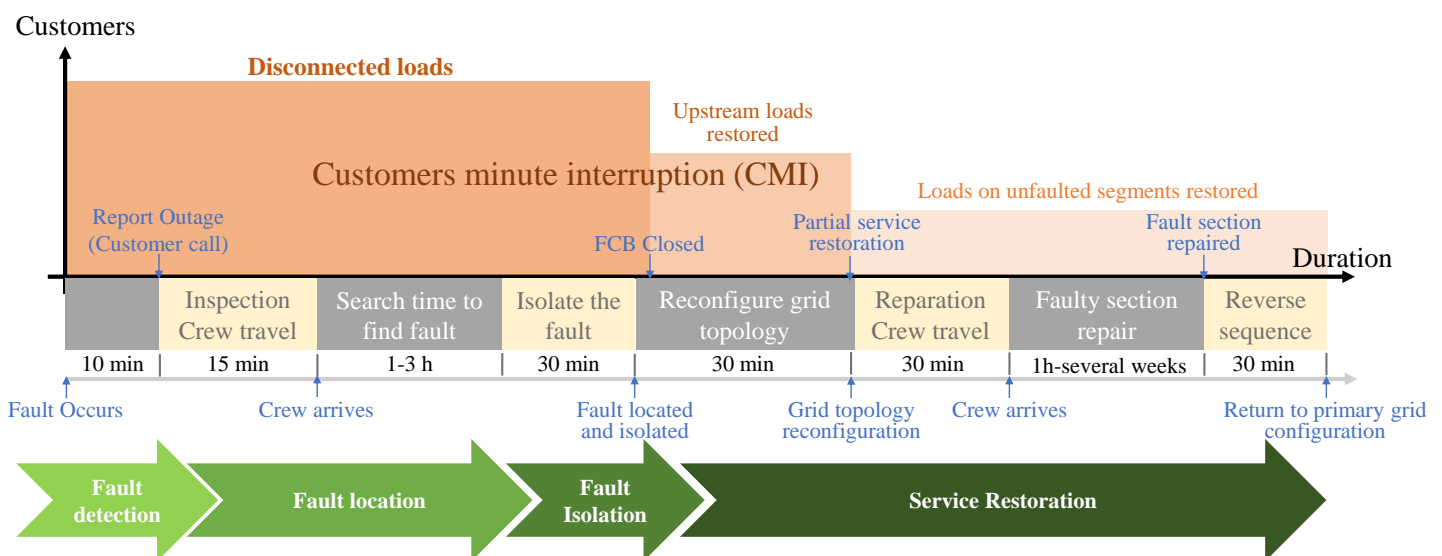


Figure 3.7: Manual FLISR process execution time

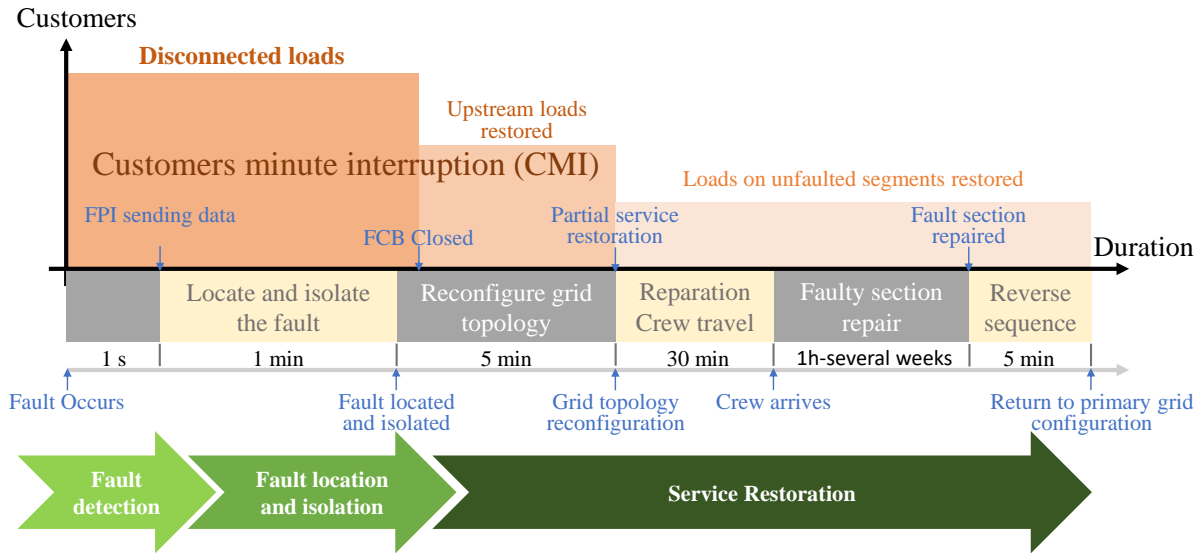


Figure 3.8: Automatic FLISR process execution time

The implementation and deployment of a new FLISR architecture across all MV and LV systems will result in additional CAPEX in the short term. This is due to the upgrade of distribution systems and the replacement of all switching and metering devices by compatible communicating IEDs. However, the long-term savings from reduced OPEX costs, time, and repair effort in the event of a failure should compensate for the initial costs.

An effective FLISR system will lead to greater satisfaction of existing customers, as well as attracting new ones needing a reliable power supply for their operations. This can be achieved by ensuring a reliable power supply for critical infrastructure such as hospitals and airports with high power quality. In addition, a well-functioning FLISR system can minimize the costs of penalties imposed on DSOs in the event of a power outage. In France, each minute gained or lost in the MV/LV system average interruption duration index (SAIDI) results in a bonus or penalty of 6.4 M€ for the DSO [35].

3.6.2 Proposed FLISR stages

Our proposed FLISR process is depicted in Figures 3.9 and 3.10. The figures illustrate a step-by-step sequence of actions that are taken when a fault occurs on the grid. This FLISR process involves seven specific functions that are outlined below:

3.6.2.1 Fault detection

When a fault occurs on the feeder, the feeder's protection relay is triggered, causing the feeder circuit breaker (FCB) to trip and open, thus disconnecting the faulty section from the power source. The fault passage indicators (FPIs) located along the feeder detect the fault and communicate the information to the feeder controller via their communication link. The faulty section of the feeder is then de-energized.

3.6.2.2 Fault location

The substation controller relies on data collected from various EPS components such as FPIs, FCBs, and switches, among others, as inputs for fault location algorithms.

3.6.2.3 DERs tele-decoupling

After the FCB opens, the substation controller sends a multicast direct transfer trip (DTT) signal to all DERs anti-islanding protection relays. This allows to disconnect the DERs from the grid to prevent them from injecting power into the grid while it is being restored.

3.6.2.4 DER link reconfiguration

When transferring a section of feeder F1 from substation S1 to be powered by feeder F2 in substation S2, all DERs in that section must be connected to substation S2. This ensures that when a fault occurs on feeder F2, the DERs receive the DTT signal from the substation S2 controller.

3.6.2.5 Fault Isolation

Once the fault location has been accurately determined, the affected section of the grid is isolated from both directions by opening the nearest upstream and downstream switches to the fault. As soon as the faulted section is isolated, the FCB can be closed and any upstream out-of-service loads can be restored.

3.6.2.6 Power grid reconfiguration

After isolating the power outage and before restoring the downstream out-of-service loads, the feeder controller assesses whether the out-of-service loads can be fully or partially transferred to a healthy feeder. If feasible, the power grid reconfiguration function is executed.

3.6.2.7 Service Restoration

The main goal of DSOs is to reconnect as many customers as possible within the shortest delay while minimizing the number of operations performed on grid elements, such as sectionalizers and tie switches. Once the fault is cleared, a reverse sequence of operations is carried out to return the distribution grid to its normal preset configuration.

3.6.3 Use of 5G against unwanted islanding

3.6.3.1 Existing remote decoupling solutions

The remote decoupling mechanism is a complex process that necessitates two agents, a sender and a receiver, as well as a reliable and speedy connectivity to guarantee transmission times of under 70ms, according to [49]. Until recently, achieving such a level of

connectivity required a dedicated wired telecommunication link such as copper or fiber optic link. However, the cost and deployment time involved in setting up these links have made them less popular, particularly with the obsolescence of leased line technologies.

Recently, IP-VPN links over fiber have been successfully tested. However, these links are still relatively costly and require fiber deployment to the DER site. This deployment often necessitates civil engineering work and lead times ranging from 3 to 12 months, which can be a limiting factor for connecting a new DER to the distribution grid.

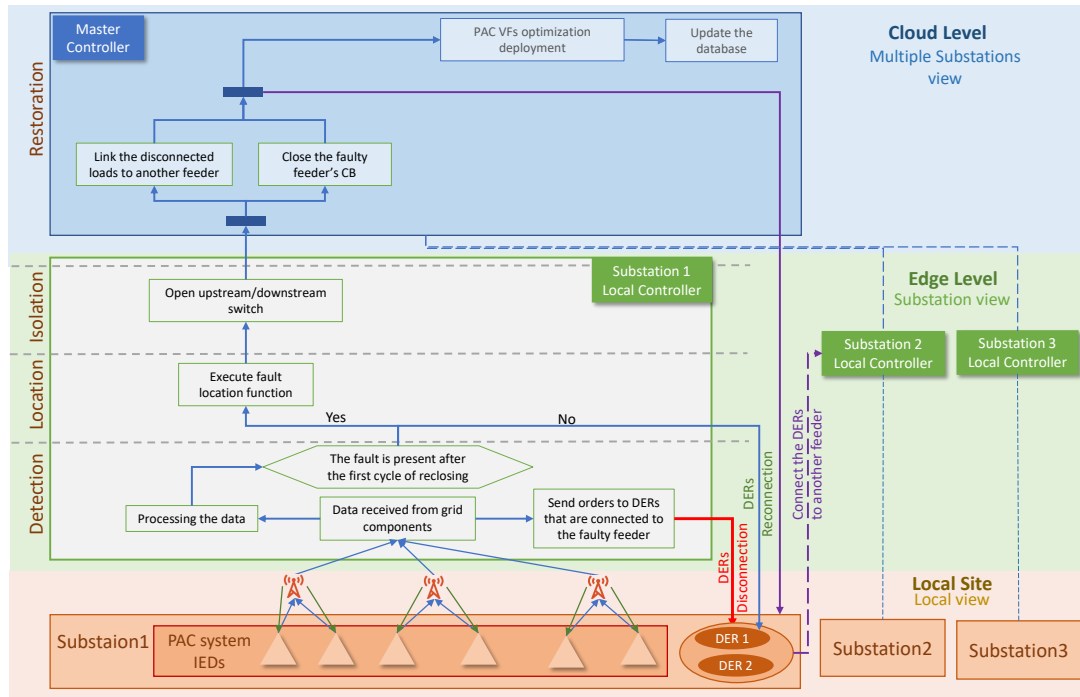


Figure 3.9: Proposed FLISR: Functions 1-6

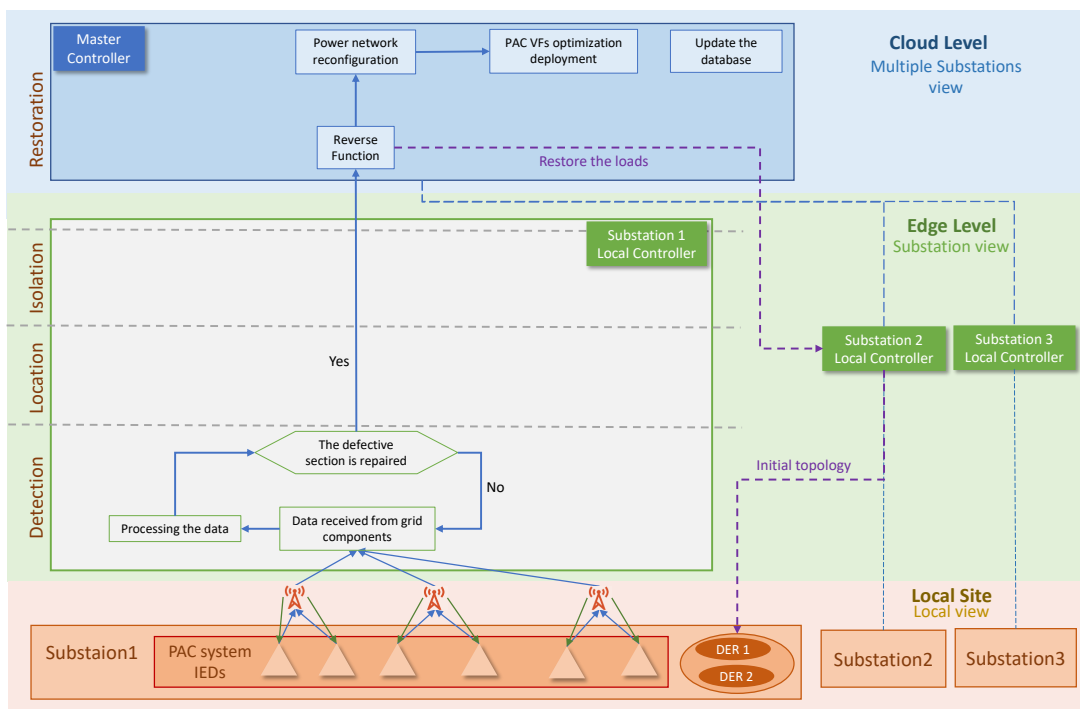


Figure 3.10: Proposed FLISR: Function 7

3.6.3.2 Wireless communication links limitation

To address the above challenges, stakeholders are exploring alternative connectivity options. For example, wireless technologies such as microwave and satellite links are being tested as potential solutions. While these technologies offer the advantage of faster deployment times compared to wired links, they also have limitations such as lower bandwidth and higher latency. In addition, the reliability of wireless links may be affected by factors such as weather conditions and interference.

- Cellular solutions, including 2G, 3G, and 4G technologies, are provided by mobile operators and offer good geographical coverage. However, while 4G networks offer relatively low latency with a round-trip time of 20 to 50ms, mobile operators cannot guarantee the required level of latency and reliability for critical applications. Moreover, the data connectivity architecture used in cellular networks can introduce high levels of network overhead, resulting in suboptimal latency between substations and DERs that are typically located within 20km of each other. This is because communications are routed through network nodes (such as the GGSN in the 3G architecture and the P-GW in the 4G architecture) which are often located at a national level. As a result, cellular solutions may not be the best option for time-critical DER applications that require low latency and high reliability.
- IoT solutions such as LoRaWAN, Sigfox, NB-IoT, and LTE-M are commonly used for wireless data transmission with connected objects. These solutions are designed to offer low power consumption for connected devices, but they may not offer the same level of performance as other solutions in terms of latency. While IoT solutions can provide reasonable latency, their primary focus is on power efficiency rather than low latency. As a result, IoT solutions may not be the best option for applications that require time-critical communication between substations and DERs. However, IoT solutions can be useful for non-critical applications that require low-power connectivity, such as monitoring and tracking applications.
- Microwave solutions can offer the required level of performance for time-critical communication between substations and DERs, but their implementation can be complex and costly. Microwave solutions require the deployment of infrastructure such as masts and directional antennas to enable direct transmission in "line of sight." These requirements can generate significant investment costs and delays. Furthermore, the scarcity of frequencies allocated to microwave solutions may discourage their use in some cases. Despite these challenges, microwave solutions may be a viable option for applications that require low-latency communication, particularly in situations where other solutions are not feasible. However, careful consideration of the costs and benefits of this technology is necessary before making a decision to deploy microwave solutions.
- Satellite solutions: historically, based on geostationary satellites (42,164 km orbit) with high latencies ($> 200ms$) which are incompatible with the need for remote

decoupling. However, new satellite solutions in low orbit offer variable latencies that are dependent on the distance to the closest satellite in the constellation. For example, the Starlink solution offers a minimum latency of 20ms, but the maximum latency can be as high as 88ms due to the current density of the constellation. While satellite solutions can provide reliable connectivity in remote areas, the variable latencies and associated costs of these solutions must be carefully considered before implementation. In particular, the costs associated with deploying and maintaining satellite solutions can be high, and the variable latency may make them unsuitable for some applications that require low latency. However, for applications that require connectivity in remote areas, satellite solutions may be the only viable option.

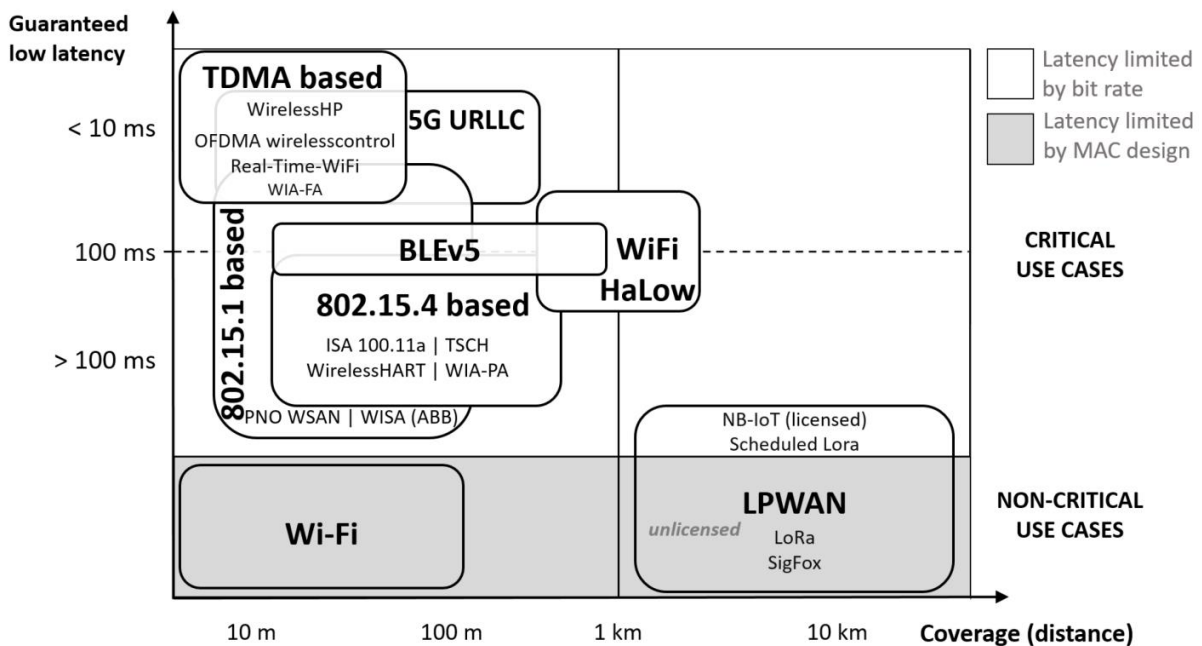


Figure 3.11: The different range/latency capabilities of various wireless communication technologies [157]

3.6.3.3 5G based Remote decoupling

Leveraging the high-speed and low-latency communication capabilities of 5G networks offers a promising solution for enabling remote decoupling in a more widespread manner. By using 5G-based communication architecture, it would be possible to reliably transmit critical control signals in real-time, enabling more DERs to be safely integrated into the electrical grid (Figure 3.12). This is particularly important for smaller DERs, which typically lack the advanced anti-islanding protections found in larger installations. Currently in French distribution grid, only large DERs (≥ 5 MW) are equipped with anti-islanding protections embedding tele-protections functionalities. The anti-islanding protections of small DERs (≤ 5 MW) are only based on local voltage and frequency measurements.

With the widespread adoption of 5G technology, it is expected that the cost of deploying 5G infrastructure will continue to decrease, making it a more viable option for remote

decoupling. Furthermore, 5G networks can be easily integrated into existing electrical infrastructure, reducing the need for additional equipment and infrastructure.

By enabling remote decoupling in more MV and LV systems, 5G technology can help to increase the resilience and efficiency of the electrical grid, as well as reducing the risk of power outages and improving the stability of the system. As the share of renewable energy sources, which are known to be more intermittent and less predictable than traditional fossil fuel-based power generation, increases in the grid, addressing the associated challenges becomes increasingly crucial.

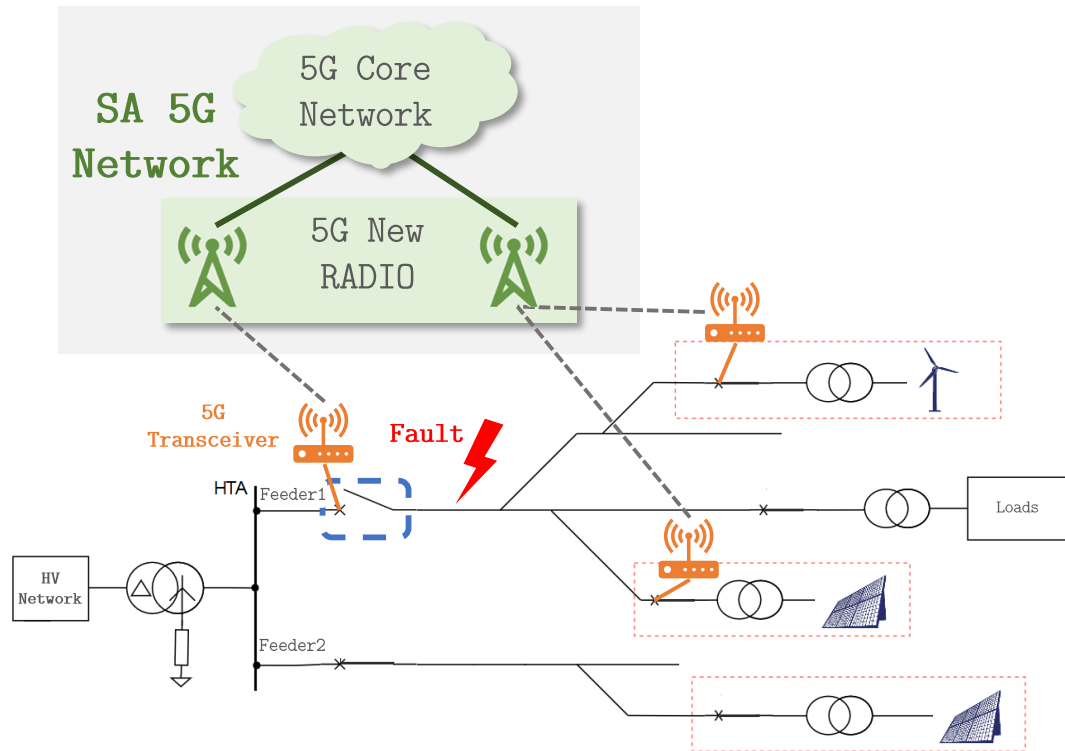


Figure 3.12: 5G-based remote decoupling mechanism

3.6.4 Dynamic Reconfiguration of Remote Decoupling Links

During a topology reconfiguration of an MV/LV system, it may be necessary to connect a DER to another substation to ensure proper distribution of power. This can be achieved through the use of remote switching devices, which can be controlled and monitored from a central location.

However, connecting a DER to another substation can also present challenges, particularly in terms of communication and control. In order to ensure the safe and reliable operation of the electrical system, it is important to have a robust communication infrastructure in place that can support the transfer of control signals and data between the DER and the substation.

Additionally, it may be necessary to adjust the settings and configurations of the DER to ensure that it is compatible with the new substation and the overall topology of the grid. This can involve updating protection settings, control logic, and other parameters to ensure that the DER operates safely and efficiently within the new configuration.

During a topology reconfiguration of an MV/LV system, the physical connectivity between the DER and the substation may change. If a wired remote decoupling link exists between the DER and the substation (Figure 3.13), and the DER is connected to another substation during this reconfiguration, the remote decoupling mechanism will be lost. This is because the wired link is physically connected to a specific substation, and if the DER is moved to another substation, the link will no longer be valid. In such a scenario, a new remote decoupling link will need to be established between the DER and the new substation to ensure the safe operation of the system. This can involve additional costs and lead times, which should be taken into consideration during the planning and implementation of topology reconfigurations.

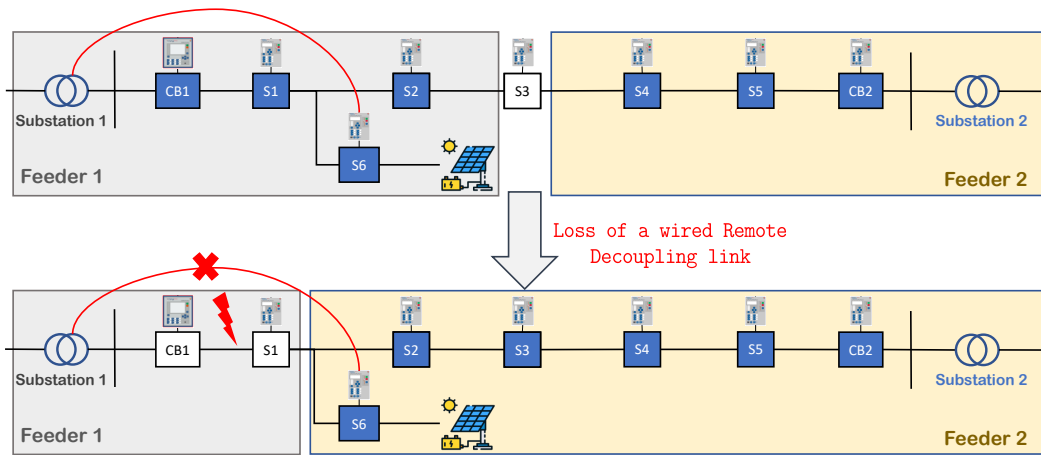


Figure 3.13: Loss of a wired Remote Decoupling link

In the case of a wireless link (Figure 3.14), it is possible to create a new remote decoupling link between the DER and the new substation to which it is connected during a topology reconfiguration of the MV/LV system. This is because wireless links are not limited by physical connections and can be established wherever there is wireless coverage. Therefore, if the DER is moved to a new substation, a new wireless link can be established to maintain the remote decoupling mechanism. However, it is important to ensure that the new wireless link provides the required level of performance in terms of latency, reliability, and security to maintain the safety and stability of the EPS.

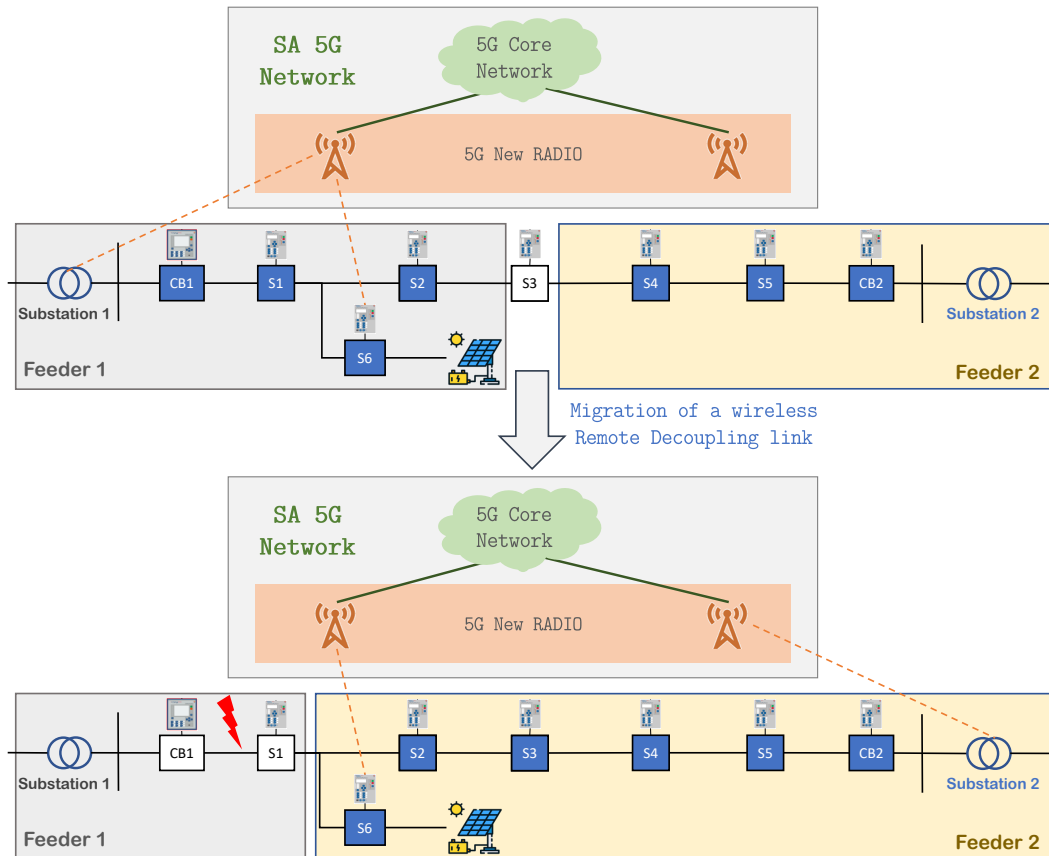


Figure 3.14: Migration of a wireless Remote Decoupling link

3.7 Conclusion

In this chapter, we have demonstrated the potential of 5G technology as a communication infrastructure to support advanced PAC applications and meet associated stringent requirements. Key concepts such as edge computing, virtualization, and orchestration have been presented and their roles in improving the performance of the communication network, while reducing deployment and management efforts, have been highlighted.

A real use case example of a PAC application has been presented to showcase how leveraging the 5G ecosystem can improve the performance of traditional FLISR application. Moving forward, in the next Chapter, we model the communication network and optimize its operation. We also develop experimental prototypes to evaluate the feasibility of using 5G as a communication technology for future PAC systems in Chapter 5. This work is important for the development of more efficient and reliable PAC systems, which can help improve the overall performance and resilience of power grids.

Chapter 4

FLISR Traffic Management in 5G Mobile Networks

4.1 Introduction

Distribution PAC systems target high safety and reliability levels, and address the need for better state-estimation, protection and control schemes. These systems also need to take into account the increase of DER penetration into power distribution grids [125], as a massive DER integration will have a considerable impact on the global power system stability. Challenges also arise from the customer side with the need to restore loads faster and more efficiently. To this end, the FLISR application utilizes the wide-area measurement and monitoring system to protect the power grid against disturbances that are beyond the scope of conventional PAC systems. Real-time data exchange from various IEDs are involved, requiring better communication technologies to mitigate any faults in the distribution grid [24]. Advanced FLISR applications can be enabled by the deployment of 5G networks that improve communication reliability, interoperability, and latency.

In this chapter, we present a management framework of the FLISR traffic transiting over a 5G network with a typical RAN (Section 4.2) and IAB-based (Section 4.3) topologies. The framework consists of a joint routing and link scheduling of FLISR traffic in the 5G-RAN taking into account the energy consumption. An Integer Linear Program (ILP) formulation, solved to optimality, is used to find the best trade-off between the achieved network throughput and energy consumption, while fulfilling the latency requirement of the FLISR traffic. Our approach is compliant with the software-defined radio access network (SD-RAN) paradigm, since it can be integrated as a flow control application on top of a SD-RAN controller. Test and results sections show that our proposed approach achieves significant gains in terms of energy consumption, flow acceptance, and end-to-end latency compared to baseline routing strategies.

To the best of our knowledge, we are the first to investigate the routing of FLISR traffic in 5G networks, and few are those that address the coexistence of eMBB and uRLLC services, while considering the energy consumption of 5G nodes. The main contributions of this chapter can be summarized as follows:

- We propose a cost-efficient 5G SD-RAN scheduler that optimally routes and schedules FLISR traffic while accommodating other flows with varying quality-of-service requirements, such as eMBB. This approach ensures the efficient use of network resources while maintaining the required level of service for different types of traffic.
- We demonstrate that our proposed traffic scheduler can be integrated as a control flow application on top of an SD-RAN controller, such as FlexRAN [59] or FlexRIC [151].
- We model the joint routing and link scheduling problem in 5G RAN as an ILP, whose objective is to ensure the best trade-off between the achieved network throughput and energy consumption, while meeting delay requirements of critical FLISR traffic.
- We compare our approach with several existing solutions and discuss the associated gains.

4.2 Typical 5G-RAN Topology

4.2.1 System Model

In this study, we utilized a centralized architecture built on cloud computing for the RAN (Radio Access Network) to improve network flexibility. The RAN architecture is divided into three entities, namely the centralized unit (CU), the distributed unit (DU), and the radio unit (RU). By implementing this approach, we can enable base-band central control and remote service functions for users, as one CU can manage several DUs. Additionally, the RU plays a crucial role in converting radio signals transmitted to and from the antenna into a digital signal that can be transmitted over the fronthaul to the DU.

Moreover, to manage the physical radio resources, an SD-RAN controller named *FlexRAN* [59] or *FlexRIC* [151] is suggested. The *FlexRAN/FlexRIC* controller consists of a master controller and one or more agents. The agent is positioned at every CU, while the master controller takes the responsibility of managing all the agents.

In this regard, we define a 5G Standalone network as an undirected graph, $G(E, V)$, commonly referred to as a connectivity graph where V is the set of nodes and E is the set of possible direct communication links. $V = C \cup D \cup H \cup S \cup I$, where C is the set of CUs, D the set of DUs, H the set of Remote Units (RUs), S the set of FLISR controllers, and I represents a set of servers located in the cloud. In Figure 4.1, we illustrate the connectivity of the grid components to the 5G network.

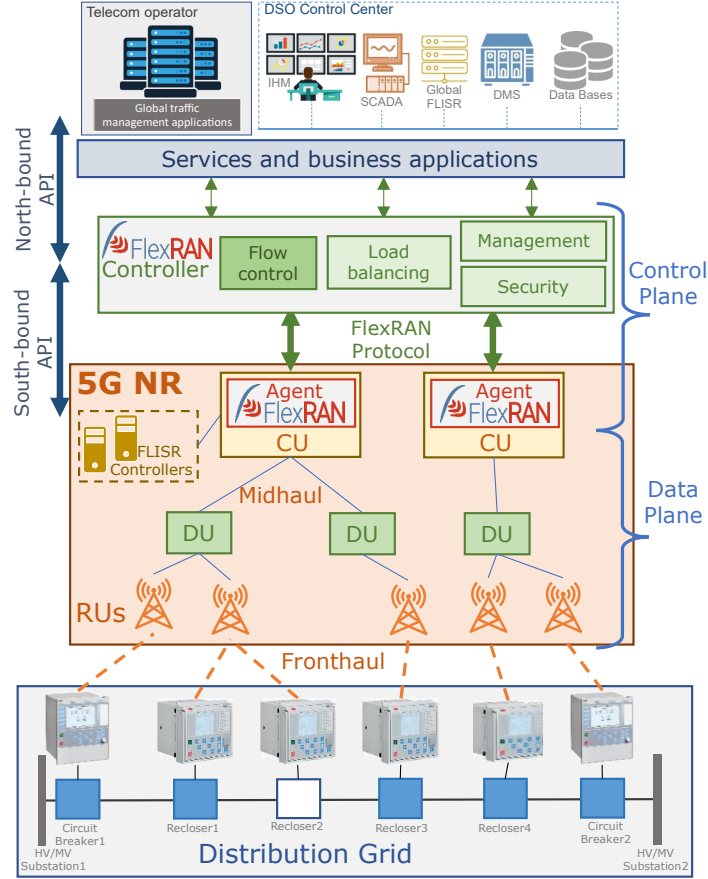


Figure 4.1: 5G-based FLISR using FlexRAN/FlexRIC.

Each node $h \in H$ has a circular transmission range $R_t(h)$ and an interference range $R_i(h)$. During the transmission of node h , all nodes residing in its transmission range receive the signal with sufficient power strength to allow for correct decoding with a high probability. An interference variable I is utilized for each pair of nodes $h, h' \in H$:

$$I_{h,h'} = \begin{cases} 1 & \text{if } h \text{ interferes with } h' \\ 0 & \text{Otherwise} \end{cases} \quad (4.1)$$

Each RU receives traffic from all connected users and routes it to either the 5G Core Network or a FLISR controller, depending on whether it is an eMBB or a FLISR traffic, respectively. It is assumed that each node $h \in H$ has a limited capacity to serve its connections, denoted by C_h . An RU can be in one of three states: Active (i.e., transmitting/receiving), Idle (i.e., on but not transmitting/receiving), or Off (i.e., not consuming power). According to experimental measurements reported in [16], an Active RU represents the peak power consumption, while an Idle RU consumes nearly 60% of its peak power consumption (assuming that a sleep control mechanism is implemented in the RU). Therefore, the following Power Consumption Model (PCM) for an RU h is derived:

$$PCM_h = \begin{cases} 100\% & \text{if } h \text{ is Active} \\ 60\% & \text{if } h \text{ is Idle (or ON)} \\ 0 & \text{Otherwise} \end{cases} \quad (4.2)$$

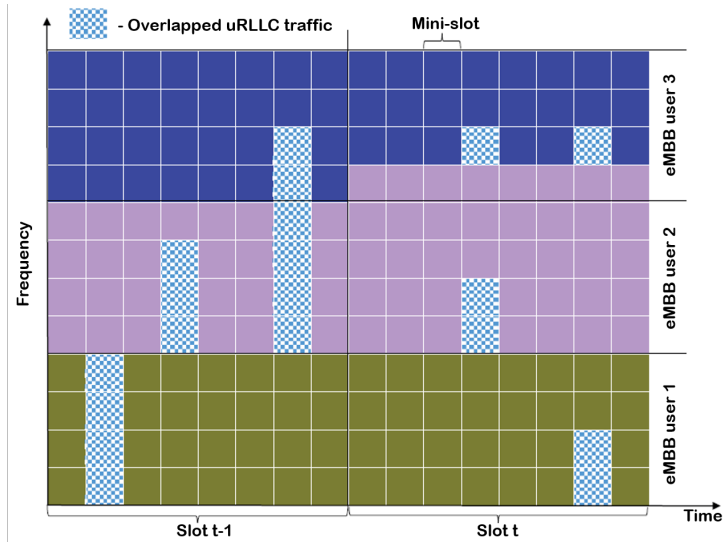


Figure 4.2: Multiplexing between eMBB and uRLLC traffic.

In addition, we assume that Physical Resource Blocks (PRBs) are assigned for eMBB traffic on a time-slot basis, while they are managed for uRLLC (i.e., FLISR traffic) on a mini-slot basis [19], as illustrated in Figure 4.2. Therefore, we consider a slotted, synchronized, and periodic 5G network with a time period of T . This time period is divided into $|T|$ time slots, where each time slot t is further divided into $|M|$ mini-slots of equal length to facilitate low-latency services.

We consider $|T|$ time slots to serve eMBB users, represented by $T = 1, 2, \dots, |T|$. We assume that FLISR traffic arrives at an RU in any mini-slot m of time slot t following a random process (i.e., Poisson process) and its payload size varies from 32 to 200 Bytes, as reported in [4]. Note that an RU that receives and sends traffic at least once in the period T will be idle during the whole period T and active during the slot/mini-slots where it sends eMBB/uRLLC packets. For the FLISR traffic, we consider IEC 61850 GOOSE packets with an average size of 200 Bytes.

In wireless networks, there are two types of channel access schemes: orthogonal and non-orthogonal. The former uses a puncturing technique, while the latter employs a superposition technique. For uRLLC (FLISR) users, appropriate mini-slots are can be allocated based on these schemes:

- Under the puncturing scheme, eMBB transmission is halted to schedule a uRLLC transmission
- Under the superposition scheme enables eMBB and uRLLC users to be served simultaneously in the same mini-slot, leveraging interference cancellation techniques.

In this work, we focus solely on the puncturing scheme as it enhances the reliability of uRLLC transmissions. Notably, FLISR traffic is critical to the smooth operation of the electrical system, and the superposition of eMBB traffic can lead to unmanageable interference and transmission errors, thereby jeopardizing the operation of the electrical system and leading to faulty situations.

RU is equipped with a set of $|K|$ subcarriers (SCs) with uniform bandwidth of B to cater to different users. It is important to note that in the wireless fronthaul, SCs are allocated to users (i.e., $k > 0, \forall k \in SC$), while in the wired part, SCs are not utilized (i.e., $k = 0, \forall k \in SC$).

In addition, we consider a set $L = LN \cup LP$ of users where LN is the set of eMBB users and LP is the set of power grid components that generate FLISR traffic. We also consider a set of flows $F = FN \cup FP$, where FN is the set of flows generated by the LN users, and FP is the set of flows generated by the LP users. Each flow f is represented by certain traffic demands: b_f in terms of required throughput and d_f in terms of maximum delay not to be exceeded. During the whole period T , each user $l \in LP$ sends its requests $f \in FP$ to a specific FLISR controller noted f_s . Without loss of generality, we assume that the traffic is uplink. This means that each originated traffic must be routed towards the set of servers located in the cloud I (if it is an eMBB traffic) or a FLISR controller (if it is a FLISR traffic).

To represent the user position within the network, we define a variable $a_{l,h}$ to indicate if a user $l \in L$ is within the coverage area of the RU $h \in H$ or not. A user l can be within the coverage area of many RUs.

$$a_{l,h} = \begin{cases} 1 & \text{if } l \text{ is within the coverage of } h \\ 0 & \text{Otherwise} \end{cases} \quad (4.3)$$

Taking into account all the above parameters, our routing and scheduling problem can be thus formulated as follows:

Given:

- A physical topology represented by the graph $G(V, E)$.
- A set of SCs K .
- A set of users L from which is generated a set of flows F , each flow f has specific throughput and delay demands (d_f and b_f).
- The coverage matrix A defined by the binary variable $a_{l,h}$ for $l \in L$ and $h \in H$.

Find: The optimal attachment of each user among L to one of the covering RUs, and the optimal routing and link scheduling of its corresponding traffic, that makes the best trade-off between achieving traffic requirements (i.e., in terms of throughput and delay) and reducing energy consumption (i.e., by switching off unused RUs).

In the following, we formulate our routing and scheduling problem as an ILP.

4.2.2 Problem Formulation

First, we analyze the resource allocation through two variables $x_{u,i,j,k}^{m,t}(fu)$ and $q_{e,i,j,k}^t(fe)$. The first indicates if the uRLLC (i.e. FLISR) traffic fu of user $u \in LP$ is routed from node $i \in V$ to $j \in V$ at mini-slot m of time slot t through the SC k . The latter is used to

know if eMBB traffic fe of user $e \in LN$ is routed from node $i \in V$ to $j \in V$ at time slot t through the SC k .

$$x_{u,i,j,k}^{m,t}(fu) = \begin{cases} 1 & \text{if } fu \text{ uses the edge } (i,j) \\ 0 & \text{Otherwise} \end{cases} \quad (4.4)$$

$$q_{e,i,j,k}^t(fe) = \begin{cases} 1 & \text{if } fe \text{ uses the edge } (i,j) \\ 0 & \text{Otherwise} \end{cases} \quad (4.5)$$

We also define the binary variable $w_{l,h}$ that decides whether the user $l \in L$ will be attached to the RU h or not.

$$w_{l,h} = \begin{cases} 1 & \text{if the } l \text{ is directly connected to } h \\ 0 & \text{Otherwise} \end{cases} \quad (4.6)$$

To indicate if an RU $h \in H$ is ON or not during the period T , we introduce another binary variable y_h defined by:

$$y_h = \begin{cases} 0 & \text{if } \sum_l w_{l,h} = 0; \forall h \\ 1 & \text{Otherwise} \end{cases} \quad (4.7)$$

We introduce the variable $zu_{h,k}^{m,t}$ to indicate if an RU h is using SC k during the mini-slot m of slot t to transmit FLISR traffic.

$$zu_{h,k}^{m,t} = \begin{cases} 0 & \text{if } \sum_u^{LP} \sum_{fu}^{FP} \sum_j^V x_{u,h,j,k}^{m,t}(fu) = 0; \forall h, k, m, t \\ 1 & \text{Otherwise} \end{cases} \quad (4.8)$$

We introduce the variable $ze_{h,k}^t$ to know if an RU h is using SC k during the slot t to transmit eMBB traffic.

$$ze_{h,k}^t = \begin{cases} 0 & \text{if } \sum_e^{LN} \sum_{fe}^{FN} \sum_j^V q_{e,h,j,k}^t(fe) = 0; \forall h, k, t \\ 1 & \text{Otherwise} \end{cases} \quad (4.9)$$

We introduce the variable $ze_{h,k}^{m,t}$ to indicate if an RU h is using SC k during the mini-slot m of slot t to transmit only eMBB traffic.

$$ze_{h,k}^{m,t} = \begin{cases} 1 & \text{if } ze_{h,k}^t - zu_{h,k}^{m,t} = 1; \forall h, k, m, t \\ 0 & \text{Otherwise} \end{cases} \quad (4.10)$$

To know if an RU h transmits eMBB traffic during the mini-slot m of t , we use the binary variable $ze_h^{m,t}$:

$$ze_h^{m,t} = \begin{cases} 0 & \text{if } \sum_k^K ze_{h,k}^{m,t} = 0; \forall h, k, m, t \\ 1 & \text{Otherwise} \end{cases} \quad (4.11)$$

The transmit power of each RU is allocated to resource blocks serving the users in the network. Consequently, the energy consumption of an RU h during a period T is given by P_h as follows:

$$P_h = \sum_m^M \sum_t^T \sum_k^K (ze_{h,k}^{m,t} + zu_{h,k}^{m,t}) + |M| \times |T| \times |K| \times y_h \times 0.6; \quad (4.12)$$

The throughput of the eMBB traffic is given by the ratio of the traffic successfully routed to $\{I\}$ and the number of required time-slots. Therefore, maximizing throughput can be achieved by minimizing the total number of slots used during the period T to transmit eMBB traffic.

Our ILP can be finally formulated as follows:

$$\mathcal{P}_1 : \text{Minimize} \left(\frac{\sum_h^H \alpha \times P_h}{|H| \times |K| \times |T| \times |M|} + \frac{\sum_h^H \sum_t^T \sum_m^M \beta \times ze_h^{m,t}}{|H| \times |T| \times |M|} + \frac{\gamma}{|FP|} \times \sum_{fu}^{FP} \frac{\text{delay}(fu)}{d_{fu}} \right) \quad (4.13)$$

where $|T|$ is the number of time slots in a period T and $\text{delay}(fu)$, as defined in (4.19), is the time it takes for FLISR flow $fu \in FP$ to reach the corresponding FLISR controller.

Subject to:

$$\sum_e^{LN} \sum_u^{LP} (x_{u,u,h,k}^{m,t}(fu) + q_{e,e,h',k}^t(fe)) \times I_{h,h'} \leq 1; \quad (4.14)$$

$$\sum_h^H \sum_k^K \sum_t^T q_{e,e,h,k}^t(fe) \geq 1; \quad (4.15)$$

$$\sum_h^H \sum_k^K \sum_m^M \sum_t^T x_{u,u,h,k}^{m,t}(fu) \geq 1; \quad (4.16)$$

$$\sum_k^K q_{e,e,h,k}^t(fe) \leq |K|; \quad (4.17)$$

$$\sum_k^K x_{u,u,h,k}^{m,t}(fu) \leq |K|; \quad (4.18)$$

$$\text{delay}(fu) = \sum_i^{CU} \sum_s^S \sum_k^K \sum_m^M \sum_t^T x_{u,i,S,k}^{m,t}(fu) \quad (4.19)$$

$$\times (t \times |M| + m) \leq \text{arrival}_{time}(fu) + d_{fu};$$

$$\sum_h^H w_{l,h} = 1; \quad (4.20)$$

$$\sum_j^V \sum_k^K \sum_m^M \sum_t^T x_{u,i,j,k}^{m,t}(fu) \leq 1; \quad (4.21)$$

$$\sum_j^V \sum_k^K \sum_t^T q_{e,i,j,k}^t(fe) \leq 1; \quad (4.22)$$

$$\sum_h^V \sum_k^K \sum_m^M \sum_t^T x_{u,h,j,k}^{m,t}(fu) = \sum_i^V \sum_k^K \sum_m^M \sum_t^T x_{u,j,i,k}^{m,t}(fu) \quad (4.23)$$

$$\sum_h^V \sum_k^K \sum_t^T q_{e,h,j,k}^t(fe) = \sum_i^V \sum_k^K \sum_t^T q_{e,j,i,k}^t(fe); \quad (4.24)$$

$$\sum_s^S \sum_u^{LP} \sum_i^{CU} \sum_k^K \sum_m^M \sum_t^T x_{u,i,s,k}^{m,t}(fu) = 1 \quad (4.25)$$

$$\sum_l^L w_{l,h} \leq C_h; \quad (4.26)$$

$$w_{l,h} \leq a_{l,h}; \quad (4.27)$$

$$x_{u,i,j,k}^{m,t}, q_{e,i,j,k}^t, z_t, z_{h,t}, y_h, w_{l,h} \in \{0, 1\}; \quad (4.28)$$

$$\alpha + \beta + \gamma = 1; \forall \alpha, \beta, \gamma \in [0, 1] \quad (4.29)$$

Constraint (4.14) avoids multi-usage of the same SC k by two interfering RUs at the same time-slot or mini-slot. Constraints (4.15) and (4.16) ensure that every served eMBB or uRLLC user get at least one resource block, while, (4.17) and (4.18) guarantee that the traffic demands do not exceed the maximal number of SCs of an RU. Constraint (4.25) ensures the reliability of FLISR traffic (i.e. all the FLISR flows are successfully routed to one of the available FLISR controllers within the period T). Constraint (4.19) keeps the delay of FLISR traffic under the maximum allowable delay, $arrival_{time}(fu)$ is the mini-slot at which the FLISR flow fu has arrived. Constraint (4.20) implies that each user is connected to one and only one RU. Constraints (4.21), (4.22) avoid loops while routing a flow originating from a user. Constraints (4.23), (4.24) refer to the flow continuity constraint, which ensures the routing path to be continuous. The number of flows that come into an element $v \in V$ is equal to what goes out of this element, except the node $\{I\}$ and the FLISR controllers $s \in S$ that process the packets. Constraint (4.26) implies not exceeding the capacity of an RU. Constraint (4.27) avoids attachment to a non-covering element. Constraint (4.28) indicates that the variables are binary. Constraint (4.29) shows that the parameters α, β, γ are weighting coefficients that determine the trade-off between the traffic throughput of eMBB traffic, the energy consumption of the RUs, and the average delay of FLISR traffic. For instance, assigning the value of 1 to α results in minimizing only the consumed energy without considering the traffic throughput or the average delay. Whereas assigning a value 1 to β or γ aims at focusing only on maximizing the throughput or minimizing the average delay, respectively. The objective function terms are normalized.

4.2.3 Performance Evaluation

In this section, we evaluate the efficiency of our proposed approach by performing several simulations according to the values shown in Table 4.1. The simulations are performed

Table 4.1: Simulation parameters

Parameters	Values
Nbr of RUs	3-15
Nbr of DUs	1-6
Nbr of CUs	1-3
Nbr of FLISR Controllers	1-5
Nbr of eMBB users	1-15
Nbr of Protections components	1-22
Nbr of Flows	3-72
uRLLC traffic ratio	10-90%
eMBB packet size	1500 Bytes
uRLLC packet size	180 Bytes
Link failure probability	0.001-0.1%
Link latency	1-5ms
Link bandwidth	10 Mbps - 1 Gbps
Nbr of subcarriers	12
Nbr of Slots	10, 20, and 30
Time slot duration	1ms
Nbr of mini-slots per slot	8
FLISR Traffic maximum delay	8-15ms
RU capacity C_h	10

on a PC with 32GB of RAM and an Intel Xeon Gold 6136 CPU @ 3.00 GHz with 4 cores. We solve our optimization problem formulated in the previous section using a Branch-and-Bound (B&B) algorithm to reach the optimal solution. Three performance metrics are considered to evaluate our strategy: i) The average delay of the FLISR traffic; ii) The average power consumption per RU; and iii) The execution time.

We compare our approach EWoS (Equal Weight Optimization Strategy) where α , β , and γ are initialized with the same value (i.e., 1/3) aiming to meet all the objectives together, with three baseline strategies 4.2:

- PMiS (Power Minimization Strategy) : initializes α , β , and γ as 1, 0, 0, respectively, aiming to minimize the average energy consumption per base station only.
- TMaS (Throughput Maximization Strategy): initializes α , β , and γ as 0, 1, 0, respectively, aiming to maximize the eMBB traffic throughput only.
- DMiS (Delay Minimization Strategy): initializes α , β , and γ as 0, 0, 1, respectively, aiming to minimize the average delay of the FLISR traffic.

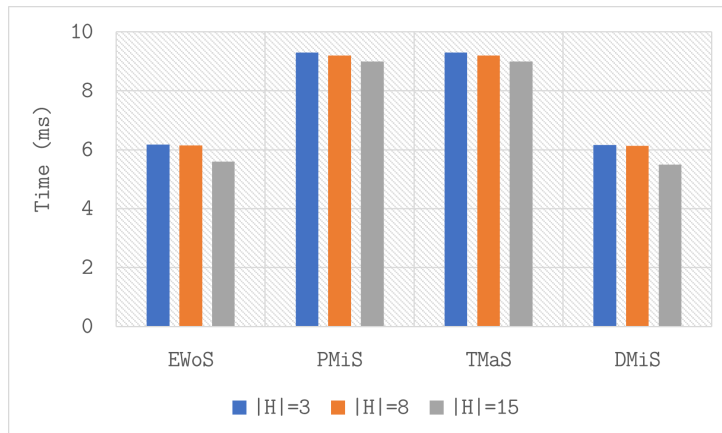
Table 4.2: Optimization Strategies

Strategy	α	β	γ
Power Minimization PMiS	1	0	0
Throughput Maximization TMaS	0	1	0
Delay Minimization DMiS	0	0	1
Equal Weight optimization EWoS	1/3	1/3	1/3

In Figures 4.3 and 4.4, our approach demonstrates a gain in delay of about 35% compared to the PMiS strategy while consuming only 5.5% more energy. Similarly, when compared to the DMiS strategy, our approach reduces energy consumption by 21% on average, albeit with a slight 1% increase in the average delay of FLISR traffic. Compared to the TMaS strategy, EWoS shows a gain in terms of energy consumption and FLISR traffic delay by about 24.11% and 32%, respectively. These outcomes demonstrate that our approach strikes a balanced trade-off between fulfilling traffic requirements, such as throughput and delay, and minimizing energy consumption. The average relative saving of each scheme with respect to EWoS is reported in Table 4.3.

Table 4.3: Average saving (%) with respect to EWoS

Strategy	PMiS	TMaS	DMiS
Energy consumption	-5.5%	24.11%	21%
eMBB Throughput	0.73%	-0.35%	1.89%
FLISR traffic delay	35%	32%	-1%

Figure 4.3: Average traffic delay for $|F| = 20$.

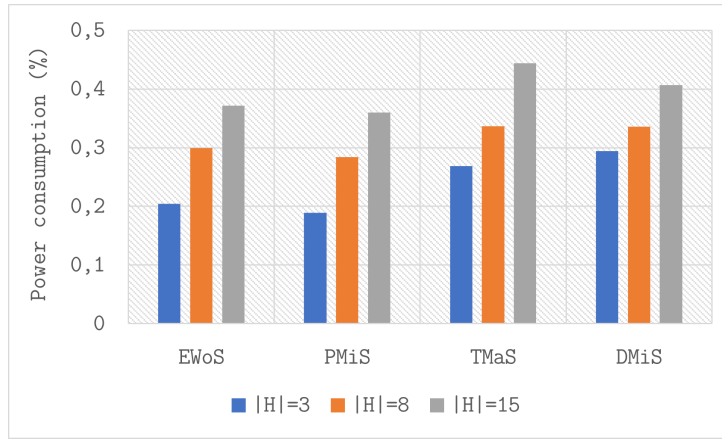


Figure 4.4: Average power consumption per RU for $|F| = 20$.

To further show the benefit of our approach, we report in Figure 4.5 the average delay of FLISR traffic when using EWoS. Our results demonstrate that our model consistently achieves stable outcomes while adhering to the maximum delay constraint, which ranges from $8ms$ to $15ms$ as reported in Table 4.1.

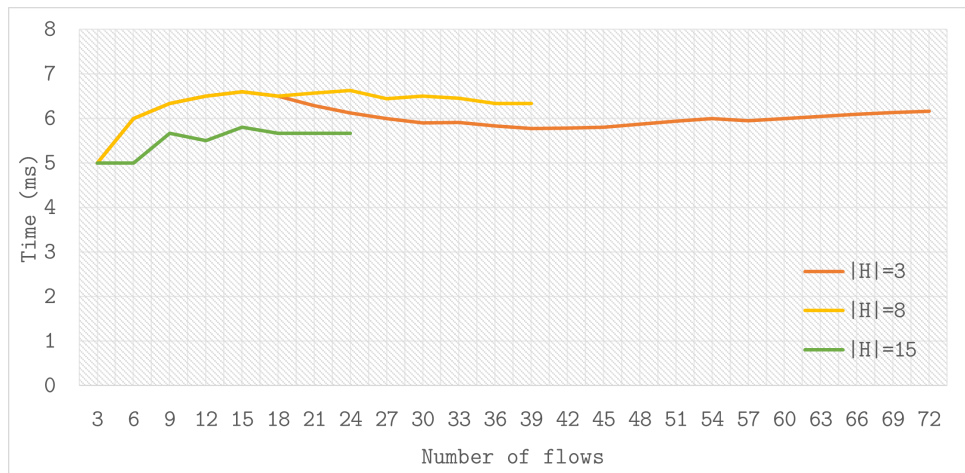


Figure 4.5: FLISR traffic average delay.

In Figure 4.6, we examine the relationship between the traffic amount and the energy consumption of RUs when using EWoS. Our results reveal that the power consumption increases in proportion to the number of flows present in the network. This outcome is attributable to the activation of more RUs when more flows are in use. Therefore, it is evident that the energy consumption of the network can be minimized by optimizing the number of activated RUs and their utilization.

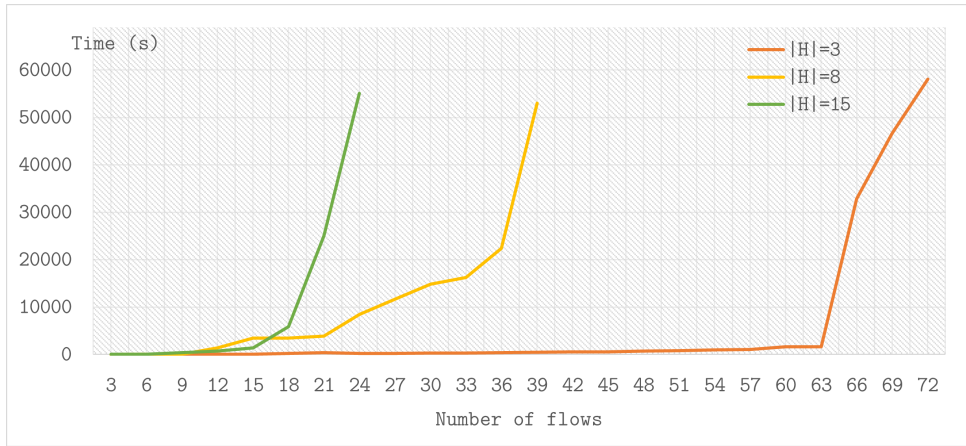


Figure 4.7: Time execution evaluation.

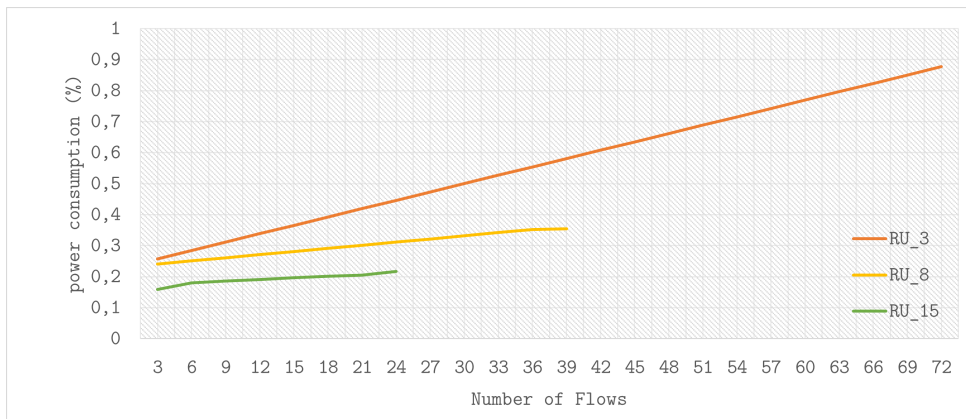


Figure 4.6: Average power consumption per RU.

In Figure 4.7, we investigate the effect of the number of flows, denoted as $|F|$, on the average execution time. As shown in the results, when a network has only three RUs, the curve rises exponentially when $|F| \geq 63$. Conversely, in a network with eight RUs (respectively, 15 RUs), the curve commences to rise exponentially when $|F| \geq 39$ (respectively, $|F| \geq 24$). The increase in the number of flows and RUs within the network amplifies the number of variables involved in our ILP formulation, which subsequently prolongs the execution time.

4.3 5G IAB-based RAN topology

4.3.1 System model

For this type of 5G-RAN topology, we consider a wireless RAN backhaul, composing of several IABs nodes and donors, as depicted in Figure 4.8. The IAB nodes act as 5G relays and IAB donors act as 5G gateways [54]. We represent a 5G-IAB network by an undirected graph $G(E, V)$ called a connectivity graph, where V is the set of nodes and E is the set of possible direct communication links. $V = I \cup D \cup N$, where I is a set of servers located in the cloud, D is a set of IAB donors, and N is a set of IAB nodes. Each base station $n \in D \cup N$ has a limited capacity to serve its connections, denoted by C_n . We

represent the graph G by a connectivity matrix, denoted by CM . Rows and columns of CM are labeled by the graph vertices V , with a 1 or 0 in position $(i;j)$ according to whether the node i and j are interconnected or not. Figure 4.8 shows how grid components are connected to the 5G network.

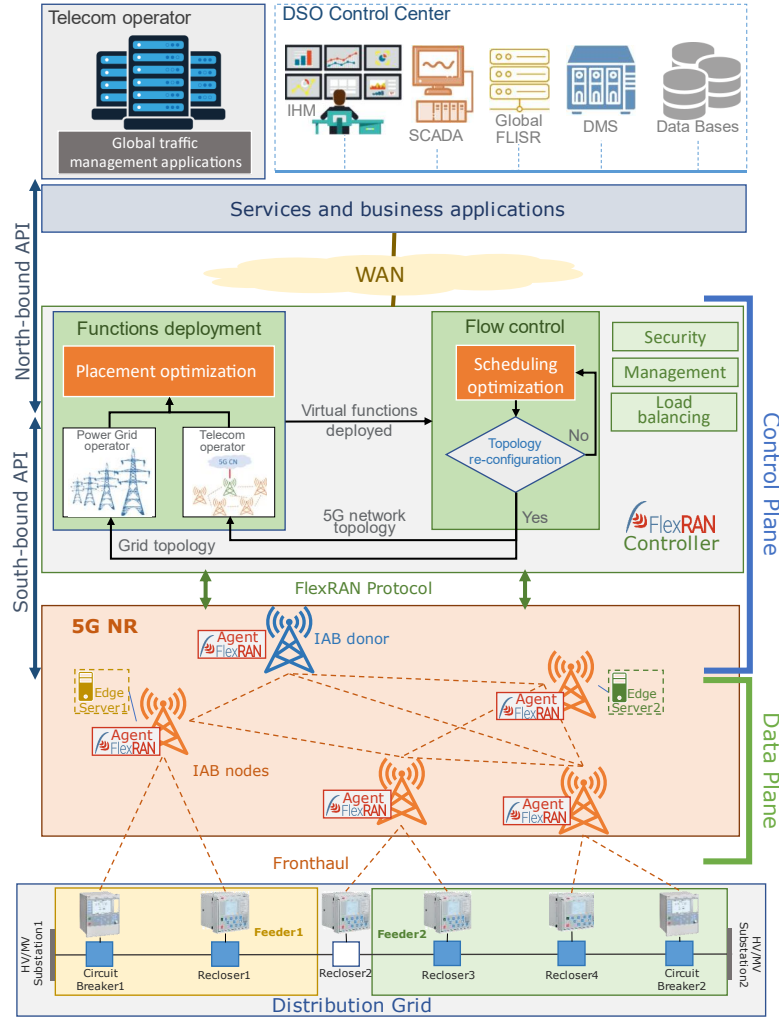


Figure 4.8: FLISR traffic management in the 5G-IAB network using FlexRAN/FlexRIC.

During the transmission of a base station $n \in D \cup N$, all the base stations residing in its transmission range, and thus representing its neighborhood denoted by NE_n , receive the signal from n with a power strength such that correct decoding is possible with high probability. A bidirectional wireless link exists between n and every neighbor $j \in NE_n$ and is represented by the directed edge $(j;n) \in E$. Each link $(j;n) \in E$ contains K subcarriers of uniform bandwidth B to support different users, and it is associated with a communication latency $l_{(j;n)}$, a failure probability $p_{(j;n)}$, and a bandwidth capacity $b_{(j;n)}$.

We denote by S the set of FLISR virtual functions deployed on the edge. Each FLISR virtual function $s \in S$ is associated with a deployment cost denoted s_c . We consider the “**Bump in the wire**” [64] deployment of Mobile Edge Computing (MEC), where MEC platforms are co-located at base stations $D \cup N$. Let H denote the set of MEC platforms ($H \subset D \cup N$). Each MEC platform $h \in H$ is associated with a resources capacity R_h to host FLISR virtual functions.

In addition, we consider a set $L = LN \cup LP$ of users where LN is the set of eMBB users

and LP is the set of power grid components that generate FLISR traffic. To represent the user position within the 5G-IAB network, we define a coverage matrix A where $A(l; n)$ indicates whether a user $l \in L$ is within the coverage area of the base station $n \in N \cup D$ (i.e. $A(l; n) = 1$) or not (i.e. $A(l; n) = 0$). Note that a user l can be within the coverage area of multiple base stations.

For each user $l \in L$, we consider a set of flows $F_l = \{f_{l_1}, \dots, f_{l_{|E_l|}}\}$. Each flow $f_{l_i} \in F_l$ is represented by certain traffic demands: minimum throughput $b_{f_{l_i}}$, required reliability $b_{f_{l_i}}$, and maximum delay $d_{f_{l_i}}$ not to be exceeded. Without loss of generality, we assume that the traffic is uplink. This means that f_{l_i} is transmitted from the source (i.e. user) $l \in L$ to a destination l_{dest} . The flow destination can be either a cloud server $se \in I$ if $l \in LN$ or a MEC platform $h \in H$ if $l \in LP$.

Given a connectivity graph, we use the conflict graph CG to represent the interference in G . Each vertex of CG corresponds to a directed link $(i; j)$ in the connectivity graph G . There is a directed edge from vertex $(i; j)$ to vertex $(a; b)$ in CG if and only if the transmission of link $(i; j)$ on subcarrier k interferes with the reception of the receiving node of link $(a; b)$ on the same subcarrier. The conflict graph CG is then fully defined by the interference matrix IM as follows:

$$IM_{(i;j),(a;b)} = \begin{cases} 1 & \text{if } (i; j) \text{ interferes with } (a; b) \\ 0 & \text{Otherwise} \end{cases} \quad (4.30)$$

Each IAB node will receive the traffic from all its attached users and then route it to the 5G Core Network (if it is an eMBB traffic) or to a FLISR virtual function (if it is a FLISR traffic).

In order to estimate energy usage, we assume that a base station can exist in three different states: Active (meaning it is either transmitting or receiving), Idle (which means it is turned on but not transmitting or receiving), and OFF. When the base station is in the Idle state, it is still using power, but at a level that is roughly 60% of its peak power consumption, according to experimental measurements outlined in [16]. We assume that sleep control mechanisms are implemented in the base station to achieve this level of power consumption. A base station will be considered Active during slots (or mini-slots) when it is processing eMBB (or uRLLC) packets and will be Idle during all other times, assuming it has sent and received at least one piece of traffic. Finally, if the base station is OFF, it will not use any power at all. As a result, we derive the following Power Consumption Model (PCM) of a base station $n \in D \cup N$ as follows:

$$PCM_n = \begin{cases} 100\% & \text{if } n \text{ is Active} \\ 60\% & \text{if } n \text{ is Idle (or ON)} \\ 0 & \text{Otherwise} \end{cases} \quad (4.31)$$

In terms of radio resource allocation, we make the assumption that resources for eMBB traffic are assigned on a time-slot basis, while resources for uRLLC (specifically, FLISR traffic) are managed on a mini-slot basis, as depicted in Figure 4.2. Two different schemes have been proposed in the literature for allocating appropriate mini-slots to uRLLC users:

the Orthogonal (or puncture) scheme, which involves stopping eMBB transmission to schedule a uRLLC user, and the non-orthogonal (or superposition) scheme, which allows eMBB and uRLLC users to be served in the same mini-slot using interference cancellation techniques. In our study, we only consider the Orthogonal scheme, which is preferable for ensuring reliable uRLLC transmissions. FLISR traffic is a critical component of the proper functioning of the electrical system, and allowing eMBB traffic to overlap in the same mini-slot could generate interference that could cause errors in FLISR transmission, potentially leading to failures in the communication chain that could compromise the operation of the electrical system.

In addition, we consider a slotted, synchronized, and periodic 5G-IAB network with period T . The period T is divided on $|T|$ time slots, each time slot t is divided into $|M|$ mini-slots of the same length in order to provide low latency services. We consider $|T|$ traditional Long Term Evolution (LTE) time slots for eMBB users represented by $T = \{1, 2, \dots, |T|\}$. We assume that FLISR traffics arrive at a base station at any mini-slot m of slot t , following a random process (e.g. Poisson process), and its payload size is varying from 32 to 200 Bytes[4].

4.3.2 Problem formulation

Our FLISR traffic management master problem can be divided into two correlated sub-problems, as follows:

4.3.2.1 Optimal Placement of FLISR virtual functions

In this first sub-problem, we aim to optimize the placement of FLISR virtual functions on the MEC platforms (co-located with a set of IAB nodes), while taking into consideration: i) 5G-IAB nodes energy consumption; ii) The cost of deploying FLISR virtual functions; iii) The Quality of Service (QoS) in terms of reliability and latency; and iv) The instantiation of FLISR virtual function following the grid topology reconfiguration.

Note that the virtual functions placement model is executed after each grid topology reconfiguration, and the set of grid topologies is denoted by Λ . We assume that the FLISR virtual functions are already deployed on the MEC platforms, thus the cost of virtual functions migration is not considered in this work.

Before presenting our ILP formulation for this sub-problem, let us introduce the variable $\phi_{l,i,j,\lambda}$ to indicate if a user l uses the edge $(i; j)$ to send its traffic in the grid topology λ or not.

$$\forall i, j \in V; l \in L; \lambda \in \Lambda : \phi_{l,i,j,\lambda} = \begin{cases} 1 & \text{if } l \text{ uses the edge } (i;j) \\ 0 & \text{Otherwise} \end{cases} \quad (4.32)$$

In addition to the FLISR virtual function set S and the set of MEC platforms H , we introduce the binary variable $v_{s,h}$, which determines whether a virtual function $s \in S$ will

be hosted on a specific MEC platform $h \in H$ or not, given a particular topology λ . It's worth noting that a virtual function can be hosted on multiple MEC platforms if required.

$$\forall s \in S; h \in H; \lambda \in \Lambda : v_{s,h,\lambda} = \begin{cases} 1 & \text{if } s \text{ is directly connected to } h \text{ on } \lambda \\ 0 & \text{Otherwise} \end{cases} \quad (4.33)$$

The conditions defined by Equations (4.34) and (4.35) ensure that every FLISR virtual function is deployed at least once, and the number of FLISR virtual functions hosted on any MEC platform $h \in H$ does not exceed its capacity limits.

$$\forall s \in S; \lambda \in \Lambda : \sum_h^H v_{s,h,\lambda} \geq 1 \quad (4.34)$$

$$\forall h \in H; \lambda \in \Lambda : \sum_s^S v_{s,h,\lambda} \times v_s \leq R_h \quad (4.35)$$

To indicate whether a base station $n \in D \cup N$ is used by a user $l \in L$ to send its traffic in any given topology $\lambda \in \Lambda$, we introduce another binary variable u_n , defined as:

$$\forall n \in N : u_n = \begin{cases} 0 & \text{if } \sum_\lambda^\Lambda \sum_l^L \sum_j^V \phi_{l,i,n,\lambda} + \phi_{l,n,i,\lambda} = 0 \\ 1 & \text{Otherwise} \end{cases} \quad (4.36)$$

The constraint defined by Equation (4.37) ensures that the latency of the established path between each power grid component $l \in LP$ and its corresponding FLISR virtual function is less than or equal to the latency d_l tolerated by component l . Constraint (4.38) ensures that the traffic passing through any communication link $(i; j) \in E$ in any topology $\lambda \in \Lambda$ does not exceed its bandwidth $b_{(i;j)}$. The reliability of the established path between each user $l \in LP$ and its corresponding FLISR virtual function is expressed in Equation (4.39).

$$\forall l \in L; \lambda \in \Lambda : \sum_i^V \sum_j^V \phi_{l,i,j,\lambda} \times l_{(i;j)} \leq d_l \quad (4.37)$$

$$\forall i, j \in V; \lambda \in \Lambda : \sum_l^L \phi_{l,i,j,\lambda} \times b_l \leq b_{(i;j)} \quad (4.38)$$

$$\forall l \in L; \lambda \in \Lambda : \prod_{(i;j) \in E} (1 - p_{(i;j)} \times \phi_{l,i,j,\lambda}) \geq p_l \quad (4.39)$$

However, constraint (4.39) is not linear, so, we perform the following transformation in order to linearize it.

$$\forall l \in L; \lambda \in \Lambda : \sum_i^V \sum_j^V \phi_{l,i,j,\lambda} \times \log(1 - p_{(i;j)}) \geq \log(p_l) \quad (4.40)$$

To ensure that users can communicate with their intended destinations without any loops or complications, we have defined constraints in equations (4.41), (4.42), and (4.43).

$$\forall j \in V; \lambda \in \Lambda : \sum_i^V \sum_l^L \phi_{l,i,j,\lambda} = \sum_n^V \sum_l^L \phi_{l,j,n,\lambda} \quad (4.41)$$

$$\forall l \in L; i, j \in V; \lambda \in \Lambda : \phi_{l,i,j,\lambda} \leq CM(i; j) \quad (4.42)$$

$$\forall l \in L; s \in S \cup I; i \in V; \lambda \in \Lambda : \phi_{l,s,i,\lambda} = 0 \quad (4.43)$$

After introducing all constraints and their respective transformations for our first sub-problem, the corresponding ILP formulation can be written as follows:

$$\begin{aligned} \mathcal{P}_{2.1} : \text{Minimize} & \left(\frac{\mu \times \sum_i^{N \cup D} u_i}{|D \cup N|} + \frac{\eta \times \sum_s^S \sum_h^H \sum_\lambda^\Lambda v_{s,h,\lambda}}{|S| \times |H| \times |\Lambda|} \right. \\ & \left. + \delta \times \sum_l^{LP} \frac{\sum_\lambda^\Lambda \sum_i^V \sum_j^V \phi_{l,i,j,\lambda} \times l_{(i,j)}}{d_l} \right) \\ \text{s.t} : & (4.32) - (4.43) \end{aligned} \quad (4.44)$$

$$\mu + \eta + \delta = 1; \forall \mu, \eta, \delta \in [0, 1] \quad (4.45)$$

Where μ , η , and δ are weighting coefficients, set by the Mobile Network Operators (MNOs), that determine the trade-off between the energy consumption, the deployment cost of FLISR virtual function, and the average delay of FLISR traffic, with values ranging between 0 and 1 and having a sum equal to 1 (i.e., $\mu + \eta + \delta = 1$). Note that the terms of the objective function are normalized.

The proposed objective function in (4.44) consists of minimizing the total energy consumption of 5G-IAB nodes, in addition to minimizing the deployment cost of FLISR virtual functions, while guaranteeing the QoS requirements of power protection components. It's worth noting that the terms of the objective function have been normalized to ensure fairness and avoid any bias.

4.3.2.2 Optimal FLISR traffic routing and link scheduling

After resolving the previous FLISR virtual functions placement problem $\mathcal{P}_{2.1}$, the set of MEC platforms, where each FLISR virtual function $s \in S$ is deployed can be determined. Let us denote by $H_s \subset H$ the resulting set. This set corresponds to the possible destination nodes when routing FLISR traffic flows, toward $s \in S$, in our second sub-problem. Indeed, once FLISR protection functions are optimally placed within the 5G-RAN, we need to route and schedule both eMBB and FLISR traffic optimally within the scheduling period T , as well as find the optimal attachment of each user to one of the covering base stations. This is the aim of our second sub-problem, formulated here-after.

We first introduce two binary variables to aid in our formulation: $x_{i,j,k}^{m,t}(f_u)$ and $q_{i,j,k}^t(f_e)$. The former indicates whether the uRLLC (i.e., FLISR) traffic flow f_u of user $u \in LP$ is routed from node $i \in V$ to node $j \in V$ at mini-slot m of time slot t through

subcarrier k . The latter is used to determine if the eMBB traffic flow f_e of user $e \in LN$ is routed from node $i \in V$ to node $j \in V$ at time slot t through subcarrier k .

$$x_{i,j,k}^{m,t}(f_u) = \begin{cases} 1 & \text{if } f_u \text{ uses the edge } (i;j) \\ 0 & \text{Otherwise} \end{cases} \quad (4.46)$$

$$q_{i,j,k}^t(f_e) = \begin{cases} 1 & \text{if } f_e \text{ uses the edge } (i;j) \\ 0 & \text{Otherwise} \end{cases} \quad (4.47)$$

We also define the binary variable $w_{l,n}$ which indicates whether the user $l \in L$ will be attached to the base station $n \in D \cup N$ or not.

$$w_{l,n} = \begin{cases} 1 & \text{if } l \text{ is directly connected to } n \\ 0 & \text{Otherwise} \end{cases} \quad (4.48)$$

To indicate whether a base station $n \in D \cup N$ is turned ON or OFF during period T , we introduce another binary variable y_n defined by:

$$\forall u, e, l \in L; i, j \in V; m \in M; t_1, t_2 \in T; k_1, k_2 \in K; f_u \in F_u; f_e \in F_e; \\ y_n = \begin{cases} 0 & \text{if } x_{i,n,k_1}^{m,t_1}(f_u) + q_{j,n,k_2}^{t_2}(f_e) + w_{l,n} = 0; \\ 1 & \text{Otherwise} \end{cases} \quad (4.49)$$

We introduce the variable $z u_{n,k}^{t,m}$ to indicate if a base station $n \in D \cup N$ is using subcarrier $k \in K$ during the mini-slot m of slot t to transmit FLISR traffic.

$$z u_{n,k}^{t,m} = \begin{cases} 0 & \text{if } \sum_u^{LP} \sum_i^{F_u} \sum_j^V x_{n,j,k}^{m,t}(f_{u_i}) = 0; \\ 1 & \text{Otherwise} \end{cases} \quad (4.50)$$

The variable $z e_{n,k}^t$ indicates whether a base station $n \in D \cup N$ is using subcarrier $k \in K$ during the slot t to transmit eMBB traffic.

$$z e_{n,k}^t = \begin{cases} 0 & \text{if } \sum_e^{LN} \sum_i^{F_e} \sum_j^V q_{n,j,k}^t(f_{e_i}) = 0; \\ 1 & \text{Otherwise} \end{cases} \quad (4.51)$$

We introduce the variable $z e_{n,k}^{m,t}$ to indicate if an IAB node $n \in D \cup N$ is using subcarrier $k \in K$ during the mini-slot m of slot t to transmit only eMBB traffic (i.e. avoid superposition).

$$z e_{n,k}^{m,t} = \begin{cases} 1 & \text{if } z e_{n,k}^t - z u_{n,k}^{m,t} = 1; \\ 0 & \text{Otherwise} \end{cases} \quad (4.52)$$

The transmit power of each IAB node is allocated to resource blocks serving the users in the network. Consequently, the energy consumption of a base station $n \in D \cup N$ during a period T is given by P_n as follows:

$$P_n = \sum_m^M \sum_t^T \sum_k^K (ze_{n,k}^{t,m} + zu_{n,k}^{t,m}) + |M| \times |T| \times y_n \times 0.6; \quad (4.53)$$

The throughput of the eMBB traffic is given by the ratio of the traffic successfully routed to cloud servers I and the number of required time-slots. Therefore, maximizing throughput can be achieved by minimizing the total number of slots used during period T to transmit eMBB traffic.

Hence, the ILP formulation of our second sub-problem can be written as follows:

$$\mathcal{P}_{2.2} : \text{Minimize} \left(\alpha \sum_n^{N \cup D} \frac{P_n}{|N \cup D| \times P_{max}} + \beta \frac{\sum_n^{N \cup D} \sum_t^T \sum_m^M \sum_k^K ze_{n,k}^{m,t}}{|N \cup D| \times |T| \times |M| \times |K|} + \gamma \frac{1}{|LP|} \sum_u^{LP} \sum_i^{F_u} \frac{\text{delay}(f_{u_i})}{|F_u| \times d_{f_{u_i}}} \right) \quad (4.54)$$

Where P_{max} is the maximum power that can be consumed by a base station during the period T . $\text{delay}(f_{u_i})$, as defined in (4.55), is the time it takes for FLISR flow $f_{u_i} \in F_u$ of user $u \in LP$ to reach the corresponding FLISR virtual function, and α, β, γ are weighting coefficients (set by the MNOs) that determine the trade-off between the energy consumption (first term of the above objective function), the traffic throughput (second term), and the average delay of FLISR traffic (third term), with values ranging between 0 and 1 and having a sum equal to 1 (i.e., $\alpha + \beta + \gamma = 1$). Note that the terms of the objective function are also normalized here. For instance, assigning the value of 1 to α results in minimizing only the consumed energy without considering the traffic throughput or the average delay. Whereas assigning a value 1 to β or γ aims at focusing only on maximizing the throughput or minimizing the average delay, respectively.

Subject to:

$$\forall u \in LP; f_{u_a} \in F_u : \left(\sum_i^V \sum_h^{H_{u_{dest}}} \sum_k^K \sum_m^M \sum_t^T x_{i,h,k}^{m,t}(f_{u_a}) \times (t \times |M| + m) - \text{arrival}_{time}(f_{u_a}) = \text{delay}(f_{u_a}) \right) \leq d_{f_{u_a}} \quad (4.55)$$

$$\forall i, j, v, w \in V; m \in M; t \in T; k \in K; e, u \in L; f_{e_b} \in F_e; f_{u_a} \in F_u : \left(x_{i,j,k}^{m,t}(f_{u_a}) + q_{v,w,k}^t(f_{e_b}) \right) \times I_{(i;j),(v;w)} \leq 1; \quad (4.56)$$

$$\forall i, j \in V; m \in M; t \in T : \sum_k^K \sum_u^{LP} \sum_{f_{u_a}}^{F_u} x_{i,j,k}^{m,t}(f_{u_a}) + \sum_k^K \sum_e^{LN} \sum_{f_{e_b}}^{F_e} q_{i,j,k}^t(f_{e_b}) \leq |K|; \quad (4.57)$$

$$\forall u \in LP; f_{u_a} \in F_u : \sum_i^{N \cup D} \sum_h^{H_{u_{dest}}} \sum_k^K \sum_m^M \sum_t^T x_{i,h,k}^{m,t}(f_{u_a}) = 1 \quad (4.58)$$

$$\forall i \in N \cup D; u \in LP; f_{u_a} \in F_u : \sum_j^{N \cup D} \sum_k^K \sum_m^M \sum_t^T x_{i,j,k}^{m,t}(f_{u_a}) \leq 1; \quad (4.59)$$

$$\forall i \in V; e \in LN; f_{e_b} \in F_e : \sum_j^V \sum_k^K \sum_t^T q_{i,j,k}^t(f_{e_b}) \leq 1; \quad (4.60)$$

$$\forall j \in D \cup N; \sum_i^{D \cup N} \sum_k^K \sum_m^M \sum_t^T \sum_u^{LP} \sum_{f_{u_a}}^{F_u} x_{j,i,k}^{m,t}(f_{u_a}) = \sum_n^{D \cup N} \sum_k^K \sum_m^M \sum_t^T \sum_u^{LP} \sum_{f_{u_a}}^{F_u} x_{n,j,k}^{m,t}(f_{u_a}) + \sum_u^{LP} |F_u| \times w_{u,j} \quad (4.61)$$

$$\forall j \in D \cup N; \sum_i^{D \cup N} \sum_k^K \sum_t^T \sum_e^{LN} \sum_{f_{e_b}}^{F_e} q_{j,i,k}^t(f_{e_b}) = \sum_n^{D \cup N} \sum_k^K \sum_t^T \sum_e^{LN} \sum_{f_{e_b}}^{F_e} q_{n,j,k}^t(f_{e_b}) + \sum_e^{LN} |F_e| \times w_{e,j} \quad (4.62)$$

$$\forall l \in L; \sum_n^{N \cup D} w_{l,n} = 1; \quad (4.63)$$

$$\forall n \in D \cup N; \sum_l^L w_{l,n} \leq C_n; \quad (4.64)$$

$$\forall n \in D \cup N; l \in L; w_{l,n} \leq A(l; n); \quad (4.65)$$

Constraint (4.55) keeps the delay of FLISR traffic under the maximum allowable delay, $arrival_{time}(f_{u_a})$ is the mini-slot at which the FLISR flow f_{u_a} arrived. Constraints (4.56) avoid multi-usage of the same subcarrier k by two interfering IAB nodes at the same slot or mini-slot. Constraint (4.57) guarantees that the traffic demands do not exceed the maximal number of subcarriers of a base station. Constraint (4.58) ensures the reliability of FLISR traffic (i.e. all the FLISR flows are successfully routed to one of the virtual functions within the period T). Constraints (4.59) and (4.60) avoid loops while routing a flow originating from a user. Constraints (4.61) and (4.62) refer to the flow continuity constraint, which ensures the routing path to be continuous. The number of flows that come into a base station is equal to what goes out of this base station. Constraint (4.63) implies that each user is connected to one and only one base station. Constraint (4.64) implies not exceeding the capacity of a base station. Constraint (4.65) avoids attachment to a non-covering base station.

4.3.3 Case study

To demonstrate our system model and problem formulation, we present our case study in Figure 4.9. The figure shows a distribution grid composed of 3 substations, each substation contains a feeder. On each feeder there are protection components and a set of supplied loads. The protection components are connected to the 5G-IAB network generating FLISR traffic which is classified as uRLLC traffic. The 5G-IAB network is composed of 15 base stations (i.e. 14 IAB nodes and 1 Donor) and 6 MEC platforms or hosts.

The distribution grid operates in its initial operation topology (i.e., $\lambda = 1$ in Figure 4.9) until the appearance of a fault $F1$ which generates a first reconfiguration of the grid (i.e., $\lambda = 2$ in Figure 4.10). The grid will operate in this second topology until the appearance of a fault $F2$, causing a second reconfiguration (i.e., $\lambda = 3$ in Figure 4.11). After repairing all the defective sections of the grid, a third reconfiguration of the grid is performed to retrieve the initial operation topology (i.e., $\lambda = 4$ in Figure 4.12). Topologies 2 and 3 allow for the supply of disconnected customers, after $F1$ and $F2$, respectively, via other feeders. Figures 4.9, 4.10, 4.11, and 4.12 depict the placement of FLISR virtual functions on each topology.

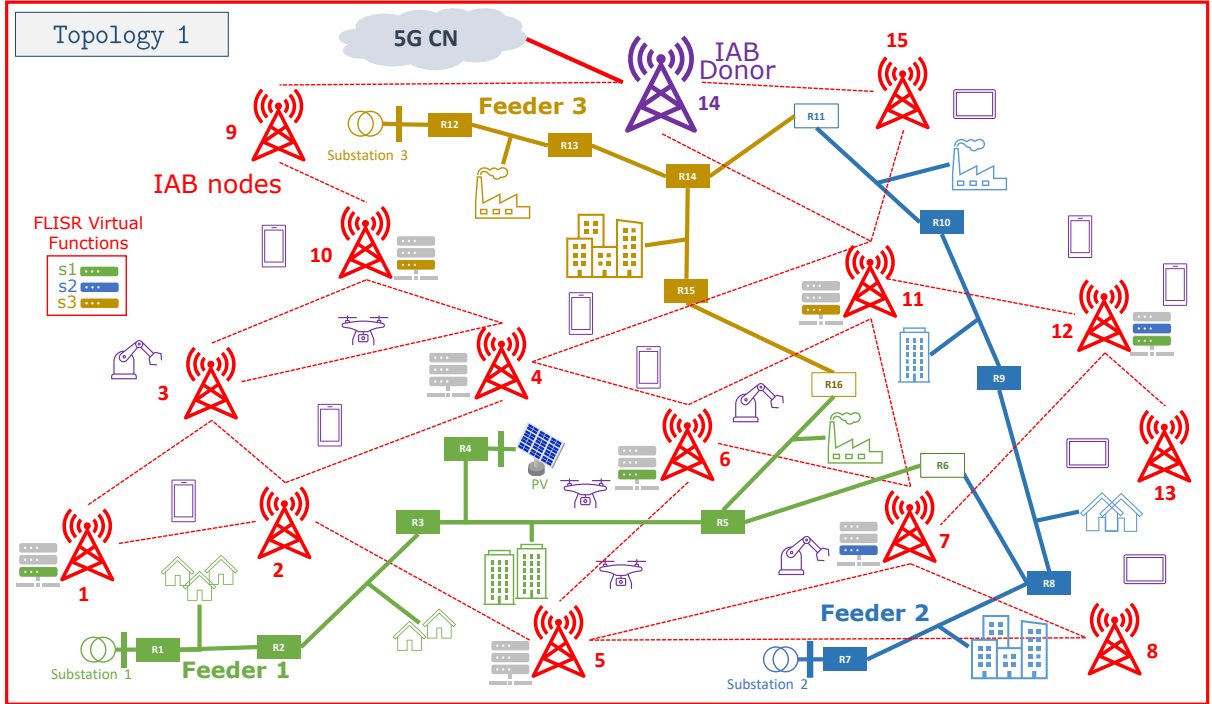


Figure 4.9: Case of study: initial topology (i.e., $\lambda = 1$)

In Figure 4.13, the interactions between the two optimization models are illustrated. The FLISR process consists of two distinct phases. Firstly, during the "Offline" phase, the system builds FLISR virtual functions and designs a resource blueprint that is adapted to the telecommunication requirements of each virtual function. Secondly, during the "Online" phase, there are two parts. The first part involves planning, where the virtual functions are deployed between the edge and cloud servers based on the placement model (i.e., $\mathcal{P}_{2.1}$). The second part involves control, where the link scheduling model (i.e., $\mathcal{P}_{2.2}$) is deployed and periodically executed to optimize the routing of critical FLISR traffic in real-time. Whenever there is a change in the distributed grid, resulting in a topology modification, the placement model is executed again to adapt the virtual functions deployment.

4.3.4 Performance Evaluation

In this section, we evaluate the efficiency of our proposed approach by performing several simulations according to the values shown in Table 4.4. The simulations are performed

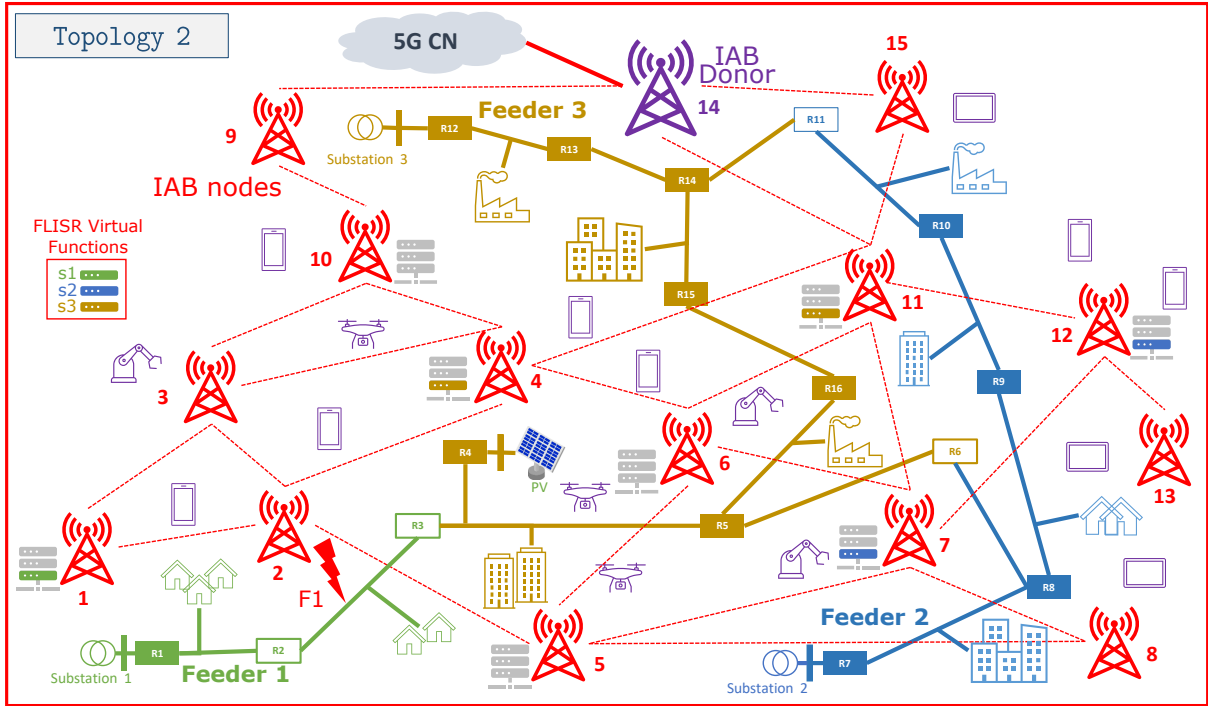


Figure 4.10: Case of study: reconfiguration after fault $F1$ (i.e., $\lambda = 2$).

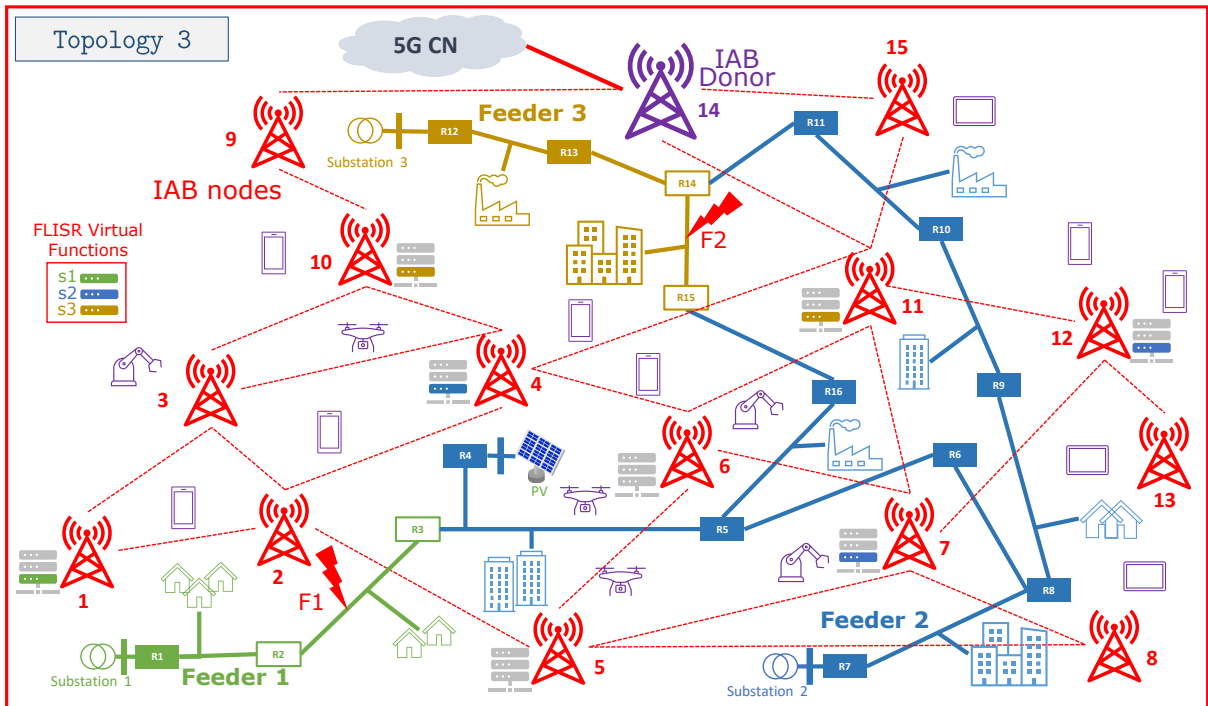


Figure 4.11: Case of study: reconfiguration after fault $F2$ (i.e., $\lambda = 3$).

on a PC with 32GB of RAM and an Intel Xeon Gold 6136 CPU @ 3.00GHz with 4 cores. We solve both optimization problems formulated in the previous section using a Branch-and-Bound (B&B) algorithm to reach the optimal solution. Three performance metrics are considered to evaluate our strategy: i) The average delay of the FLISR traffic; ii) The average power consumption per IAB node; and iii) The eMBB flow acceptance ratio. In addition, to gauge the effectiveness of our optimal FLISR traffic routing and link scheduling approach, we compare it with the case where random placement of FLISR

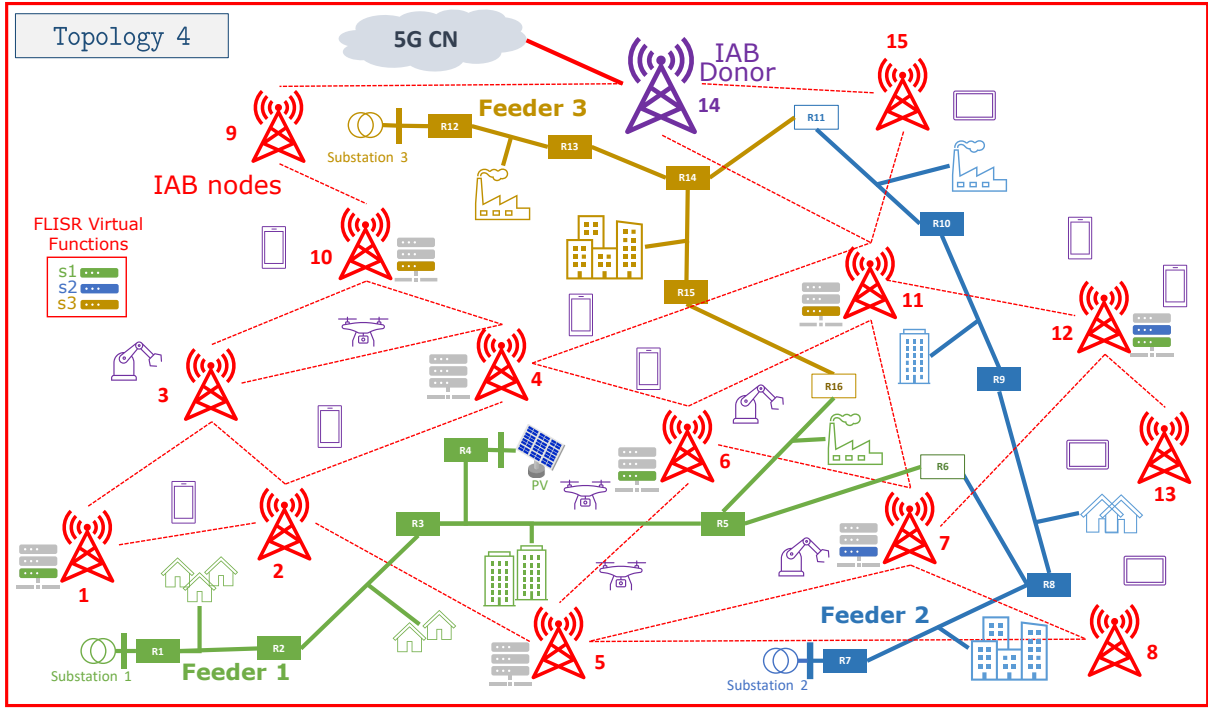


Figure 4.12: Case of study: initial configuration restoration (i.e., $\lambda = 4$).

virtual functions is considered (i.e., by solving $\mathcal{P}_{2.2}$ only) versus the case where optimal placement is considered (i.e., by solving both $\mathcal{P}_{2.1}$ and $\mathcal{P}_{2.2}$).

We considered different combinations of the parameters α , β , and γ related to the optimization problem $\mathcal{P}_{2.2}$. PMiS (Power Minimization Strategy) initializes α , β , and γ as 1, 0, 0, respectively, aiming to minimize the average energy consumption per base station only. TMaS (Throughput Maximization Strategy) initializes α , β , and γ as 0, 1, 0, respectively, aiming to maximize the eMBB traffic throughput only. DMiS (Delay Minimization Strategy) initializes α , β , and γ as 0, 0, 1, respectively, aiming to minimize the average delay of the FLISR traffic. In EWoS (Equal Weight Optimization Strategy), α , β , and γ are initialized with the same value (i.e., 1/3), aiming to meet all the objectives together.

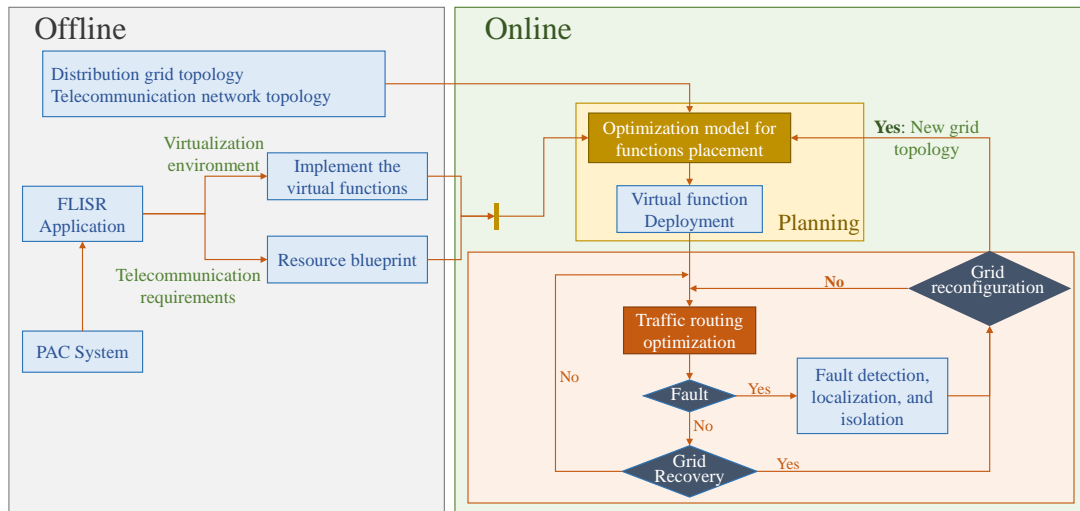


Figure 4.13: Optimization models' interactions .

Table 4.4: Simulation parameters

Parameters	Values
Nbr of IAB nodes $ N $	6-14
Nbr of Donors $ D $	1-3
Nbr of MEC platforms $ H $	1-6
Nbr of FLISR virtual functions $ S $	1-6
Nbr of eMBB users $ LN $	15
Nbr of Protections components $ LP $	16
Nbr of eMBB Flows $\sum_e^{LN} F_e $	5-25
Nbr of uRLLC Flows $\sum_u^{LP} F_u $	1-25
Link failure probability $p_{(i;j) \in E}$	0-0.01%
Link latency $l_{(i;j) \in E}$	0.5-5 ms
Link bandwidth $b_{(i;j) \in E}$	10-1000 Mbps
Nbr of subcarriers $ K $	12
Nbr of Slots $ T $	20
Nbr of mini-slots per slot $ M $	8
FLISR Traffic maximum delay	20 ms
IAB node capacity C_n	10
Number of topologies $ \Lambda $	4

Table 4.5: Optimization Strategies

Strategy	α	β	γ
Power Minimization PMiS	1	0	0
Throughput Maximization TMaS	0	1	0
Delay Minimization DMiS	0	0	1
Equal Weight Optimization EWoS	1/3	1/3	1/3

Figures 4.14, 4.15, and 4.16 show the impact of varying the number of uRLLC flows on average base-station energy consumption, FLISR traffic delay, and eMBB traffic throughput, respectively, for all considered topologies depicted in Figures 4.9, 4.10, 4.11, and 4.12. To explain easily the obtained results, we report in Table 4.6 the average relative saving of each scheme with respect to EWoS. We can see that, compared to PMiS, the EWoS approach consumed almost the same amount of energy (only a small increase of +1% is observed). However, it enhances the FLISR traffic delay and the eMBB throughput by 50% and 1.73%, respectively. Compared to the TMaS strategy, EWoS shows a gain in terms of energy consumption and FLISR traffic delay by about 14.11% and 58%, respectively. However, we observe 6% decrease of the eMBB throughput. Compared to the DMiS approach, the EWoS strategy allows a gain of 18.6% and 9.89% on the energy

consumption and the eMBB throughput, respectively. However, a small increase of 1% on the average delay of FLISR traffic is observed. According to these results, we can conclude that an MNO can target multiple objectives at the same time and achieve nearly the minimum energy consumption and minimum average delay of the FLISR traffic, while sacrificing almost 6% of the maximum network throughput by using an adequate choice of parameters.

Table 4.6: Average saving (%) with respect to EWoS

Strategy	PMiS	TMaS	DMiS
Energy consumption	-1%	+14.11%	+18.6%
eMBB Throughput	1.73%	-6%	+9.89%
FLISR traffic delay	50%	+58%	-1%

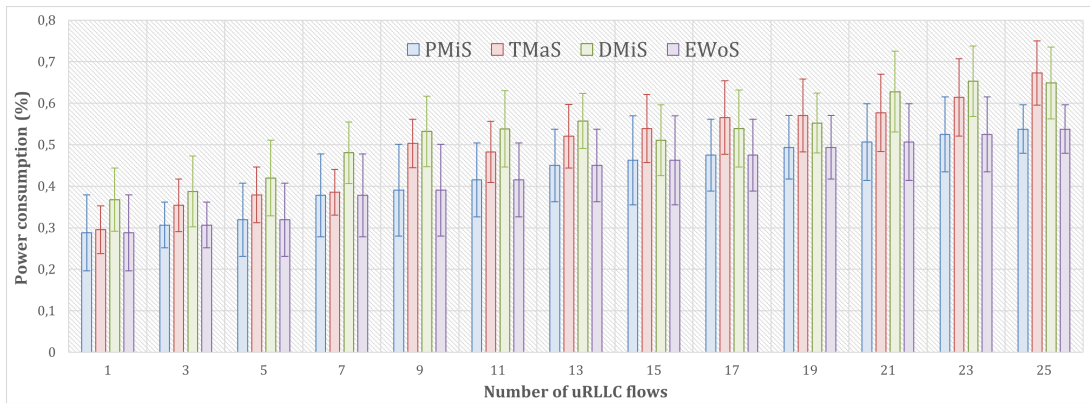


Figure 4.14: Average power consumption per base station.

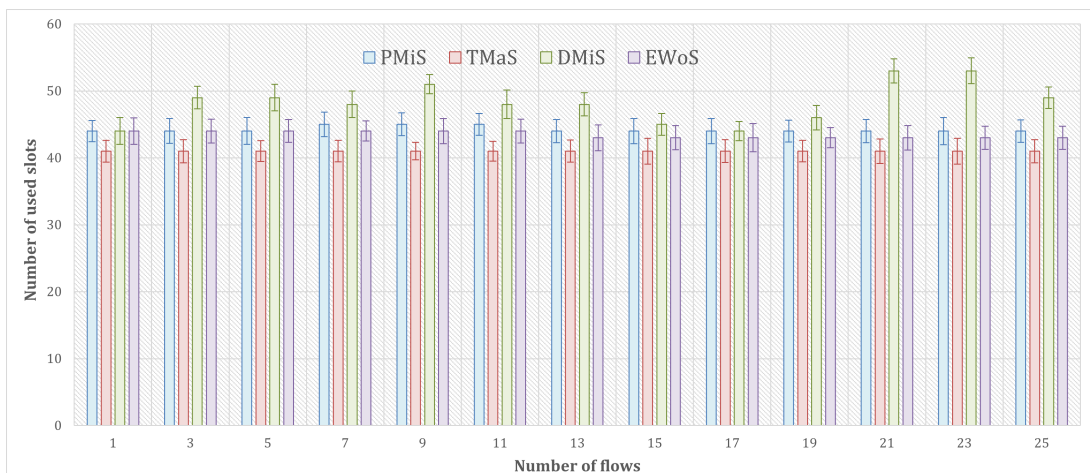


Figure 4.15: Average number of slots to send eMBB traffic.

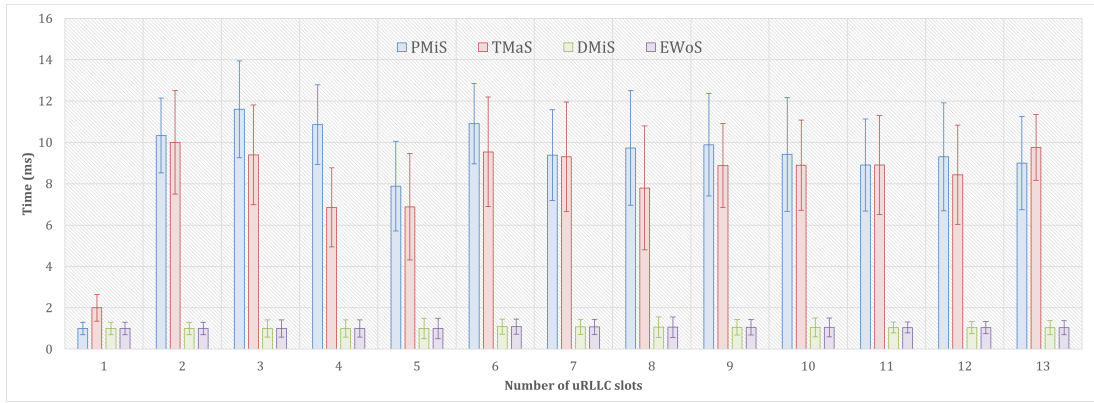


Figure 4.16: Average delay of FLISR traffic.

To further show the benefit of our EWoS approach, we compare in Figures 4.17, 4.18, and 4.19, the performance of our traffic routing and link scheduling approach under both random and optimal placement of FLISR virtual functions on different grid topologies. For each topology, we vary the simulation parameters following Table 4.4. The obtained gains are summarized in Table 4.7. Compared to the random placement of FLISR virtual functions, the optimal placement reduces the energy consumption, the average delay FLISR traffic, and the overall traffic routing cost by 14.5%, 21.7%, and 14.6%, respectively.

Table 4.7: Average gain (%) when using optimal placement of FLISR virtual functions instead of random placement.

Parameters	Grid topology				Average Gain
	$\lambda=1$	$\lambda=2$	$\lambda=3$	$\lambda=4$	
Energy consumption	18.1%	8.3%	15.6%	16.1%	14.5%
Average FLISR delay	28.9%	7.3%	27.1%	23.3%	21.7%
Cost value	18.3%	8.2%	15.9%	16.1%	14.6%

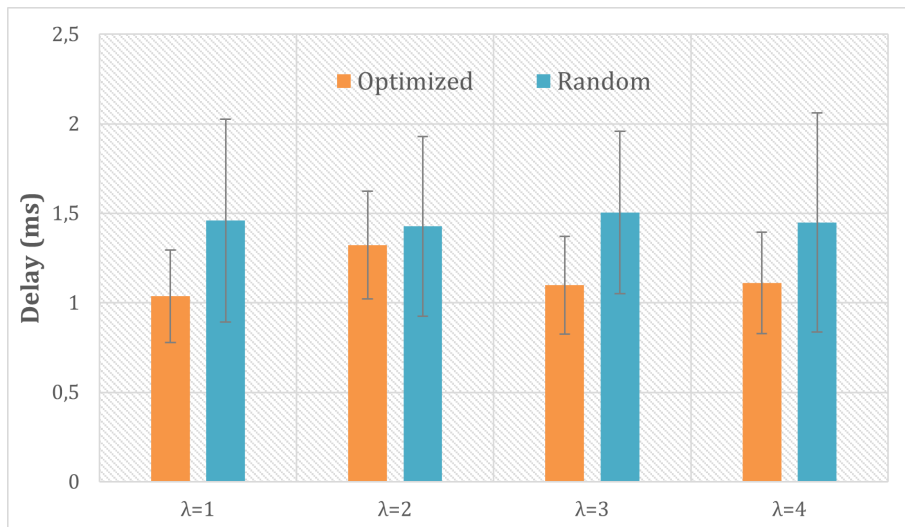


Figure 4.17: Average delay of FLISR traffic using different placement strategies.

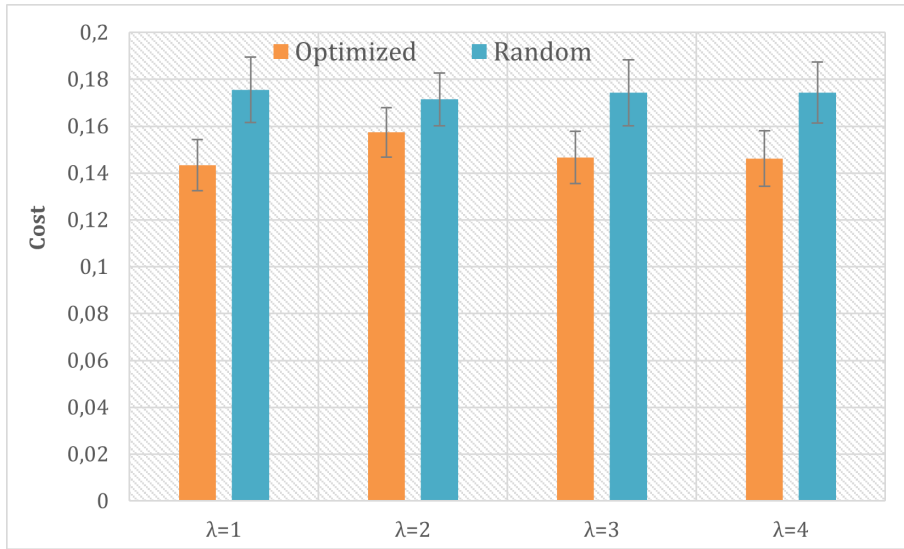


Figure 4.18: Traffic routing cost using different placement strategies.

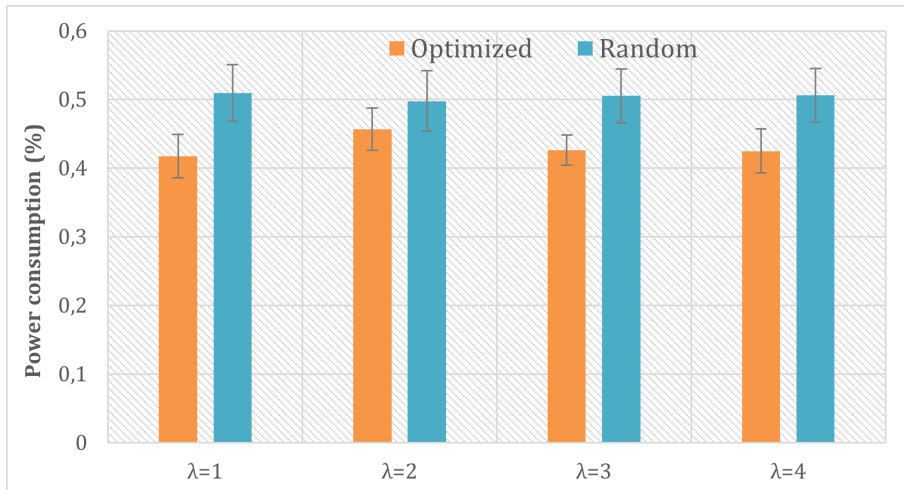


Figure 4.19: Average power consumption using different placement strategies.

In order to assess the impact of the number of reconfigurations on our EWoS approach, we conducted a comparative analysis as shown in Figures 4.20, 4.21, and 4.22. We compare the performance of our traffic routing and link scheduling approach under both random and optimal placement of FLISR virtual functions. For each fixed number of reconfigurations, we vary the remaining simulation parameters as specified in Table 4.4. Table 4.8 summarizes the gains obtained from the optimal placement of FLISR virtual functions, as compared to random placement. The optimal placement reduces the energy consumption, the average delay FLISR traffic, and the overall traffic routing cost by 21.58%, 40.42%, and 26.09%, respectively.

Although we explore a wide range of scenarios in our simulations, it's worth noting that in practice, the number of consecutive reconfigurations rarely exceeds three. Additionally, it's important to keep in mind that the model's execution time increases exponentially for values of λ greater than or equal to 13 ($\lambda \geq 13$).

Table 4.8: Average gain (%) when using optimal placement of FLISR virtual functions instead of random placement.

Number of topologies	Parameters		
	Avg delay	Cost	Power Consumption
$\lambda=1$	26.17%	17.64%	16.67%
$\lambda=2$	27.11%	20%	18%
$\lambda=3$	27.12%	22.11%	18.62%
$\lambda=4$	28.22%	23.36%	19.23%
$\lambda=5$	30.19%	24.6%	19.42%
$\lambda=6$	37.49%	25.65%	19.81%
$\lambda=7$	37.53%	27.04%	20.55%
$\lambda=8$	44.69%	28.57%	21.81%
$\lambda=9$	47.99%	30.14%	24.38%
$\lambda=10$	50.39%	30.51%	24.38%
$\lambda=11$	61.07%	30.87%	26.94%
$\lambda=12$	67.09%	32.59%	29.18%
Average Gain	40.42%	26.09%	21.58%

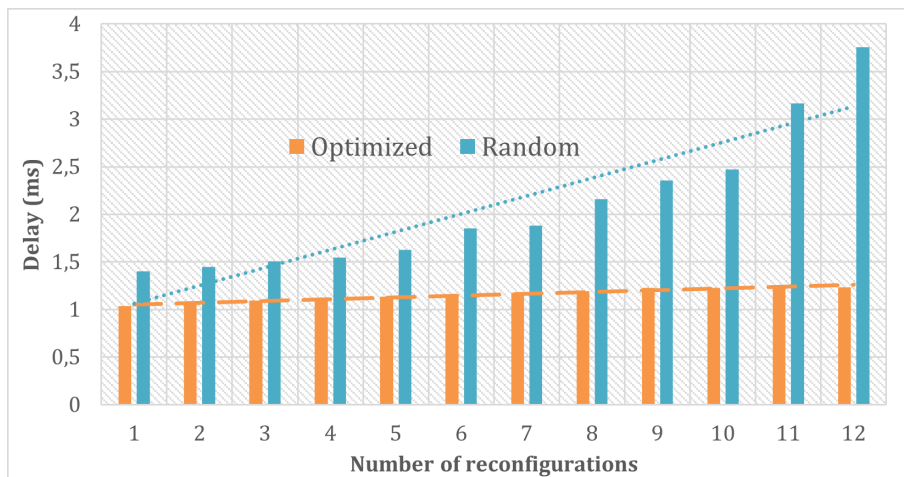


Figure 4.20: Average delay of FLISR traffic while varying the number of reconfigurations.

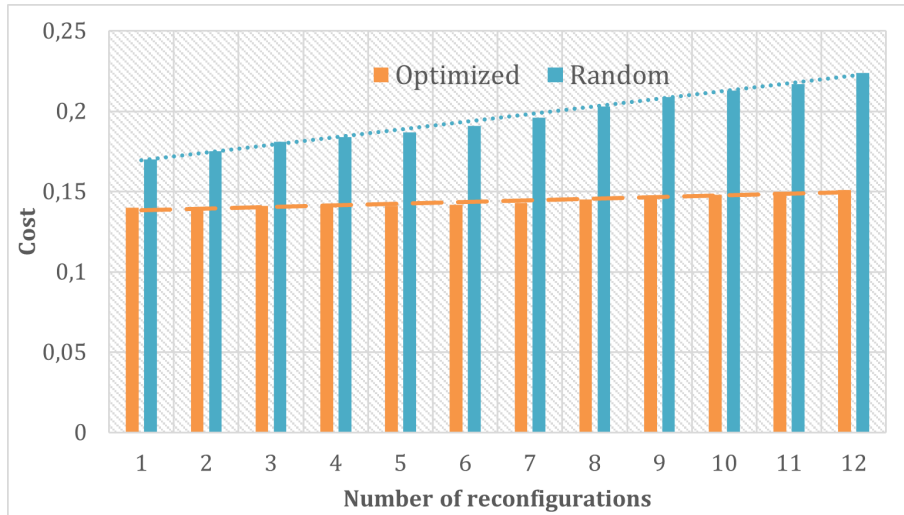


Figure 4.21: Average traffic routing cost while varying the number of reconfigurations.

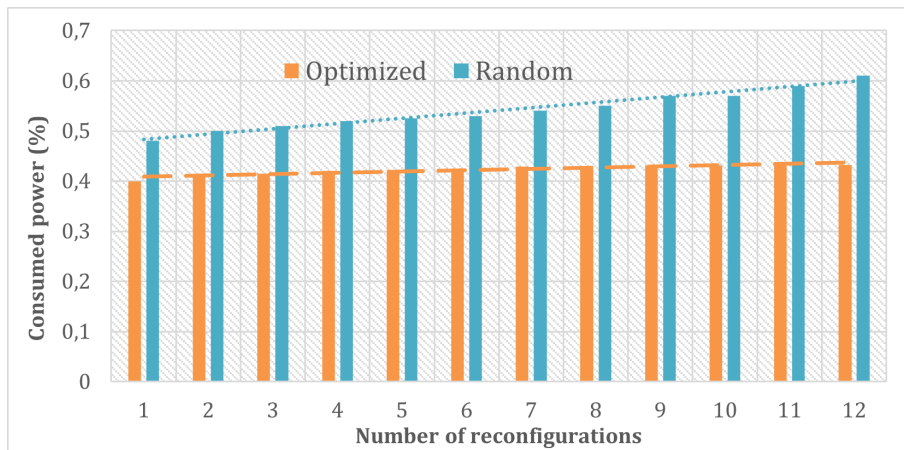


Figure 4.22: Average power consumption while varying the number of reconfigurations.

4.4 Conclusion

This chapter introduced new management frameworks of the FLISR traffic routing over a 5G network using both typical 5G-RAN and IAB-based architectures. Our approach is compliant with the software-defined radio access network (SD-RAN) paradigm, since it can be integrated as a flow control application on top of a SD-RAN controller, like FlexRAN or FlexRIC. The proposed frameworks involved formulating optimization problems with three primary objectives: minimize 5G nodes energy consumption, maximize eMBB traffic acceptance, and meet QoS requirements for the FLISR traffic. Simulation results verified the efficiency of the proposed solutions in small-scale scenarios. They allow the MNO to target multiple objectives at the same time using an adequate choice of parameters. The findings of this study provide valuable insights for the development of energy-efficient and high-performance FLISR applications in 5G networks.

To enhance our optimization models and tackle large-scale scenarios with more input parameters and variables, one could think using heuristics or reinforcement learning techniques to reduce execution times and tackle complex telecommunication networks and

distribution power systems. The plan was to leverage the previously developed linear models to train our reinforcement learning-based solutions. However, due to time constraints, we decided to shift our focus towards building different hardware-in-the-loop and field experiments and exploring the feasibility of utilizing 5G technology for PAC applications. This decision brought more added value to EDF R&D as will be shown in the next chapter.

Chapter 5

Hardware-in-the-Loop and Field Experiments

5.1 Introduction

In French distribution grids, only large DERs with a capacity of more than 5 MW are currently equipped with anti-islanding protections that incorporate the remote decoupling mechanism. Anti-islanding protections for small DERs (≤ 5 MW) are solely based on local voltage and frequency measurements. The adoption of a 5G-based communication architecture facilitates the extension of remote decoupling to more MV- and LV-connected power plants. This solution, compared to the existing methods, is cost-effective and easy to implement in areas that are difficult to access. Consequently, the probability of DERs experiencing unintended disconnections decreases and the risk of unwanted islanding is minimized, leading to improved integration of DERs into the MV and LV systems.

In this chapter, we present the findings from three experiments that we conducted. The first experiment¹, presented in Section 5.2, aims to address the unwanted islanding issue by leveraging a Hardware-in-the-Loop (HiL) architecture that integrates real hardware with digital simulations. To this end, we implement a remote decoupling mechanism, described in Section 3.6.3.3, using IEC 61850 GOOSE² messages over a 5G communication network and analyze the system response time.

The second experiment, described in Section 5.3, focuses on implementing the FLISR architecture proposed in Chapter 3.6.2. We design a prototype using off-the-shelf equipment, including protection components and fault passage indicators (FPIs). The prototype also includes a real-time HiL testing platform to simulate the dynamic behavior of the grid during HV or MV faults. The simulated distribution power system is connected to controllers hosted at the edge and cloud levels, where various FLISR functions are implemented. We establish the communication link using a 5G NSA (non-standalone) test network.

The third experiment, depicted in Section 5.4, is conducted as part of “Engage 5G &

¹The experiment was partly funded by the European Commission under the European Union Horizon 2020 program - grant agreement number 815074 (5G EVE project).

²Section 7.2 provide a comprehensive definition of the GOOSE protocol

Beyond” project [58]. Our objective is to demonstrate the potential benefits of utilizing a complete standalone (SA) 5G network as a communication layer for FLISR systems to enhance the management of a physical electrical system. The experiment seeks to explore the capability of a 5G SA network to provide low-latency and high-reliability communication between the various components of a PAC system, enabling quick and effective responses to faults or other grid events. By implementing a FLISR application, we aim to improve the reliability of the electrical system and reduce downtime caused by faults. The experiment also assesses the feasibility and practicality of integrating renewable energy sources, such as the photovoltaic DER, in smart grids.

In the following, we will describe these three experiments by presenting first the corresponding scenarios, then the associated testing results.

5.2 5G-based Remote Decoupling Mechanism Implementation

5.2.1 Electrical Equipment

In this experiment, we utilize a HiL architecture to connect physical protection relays with a simulated functional model. The model is created using an all-in-one development system and outlines the sequence of actions that occur in the event of a grid fault. The used electrical equipment includes:

- ABB protection relay REF 615 N.
- ABB voltage protection relay REU 615 A.
- dSpace MicroLabBox : an all-in-one development system that offers high performance and versatility while keeping low system costs. The implementation of control, test, and measurement applications is simplified, making it easier to develop new control concepts (defined in section 7.4.3).
- ControlDesk: is dSpace’s versatile and user-friendly instrumentation and experimentation software, specially designed for development simulators like MicroLabBox (defined in section 7.4.4).

The MicroLabBox comes with a complete dSPACE software suite, which comprises the Real-Time Interface (RTI) library for Matlab Simulink® to seamlessly integrate I/O into the model, and the ControlDesk software, enabling access to the application in real-time using graphical tools.

After installing the dSpace software package on the computer, we can easily access the RTI interface under Matlab Simulink. With this interface, Simulink models can be created to establish communication with MicroLabBox, utilizing the simulator’s inputs and outputs to facilitate the creation of complex simulations.

Using the RTI interface, we construct the scheme shown in Figure 5.1. A variety of inputs and outputs is used from MicroLabBox as follows:

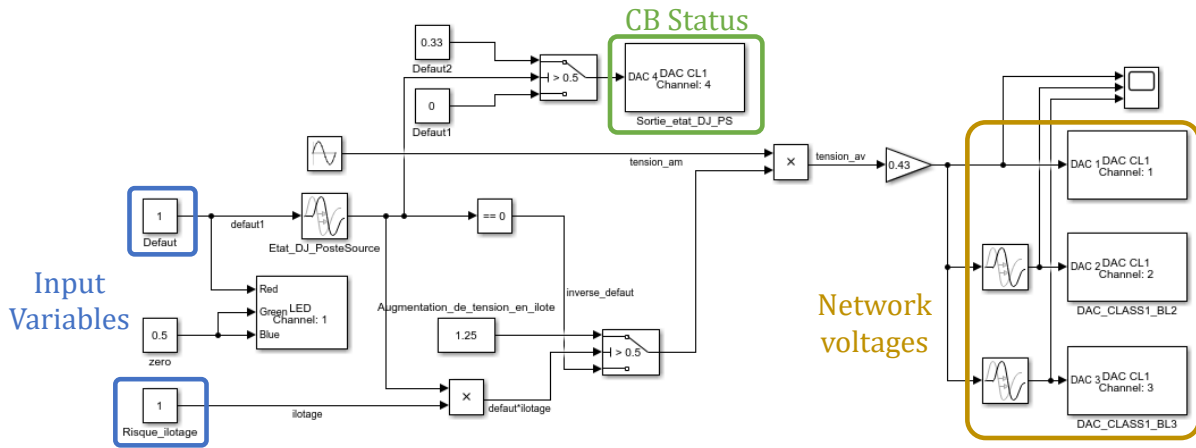


Figure 5.1: Simulink-based functional scheme using RTI I/O

- The variable "Sortie.etat-DJ_postesource" is a digital output that represents the status of the circuit breaker, transitioning from '0' to '1' within 500 ms after the variable "default" has changed to '1'. This delay is caused by the circuit breaker's time delay at the substation.
- "Command.DJ.centrale" is the decoupling order coming from the protection relay.
- "LED.BL1" is one of the 4 LEDs of the MicroLabBox. Its entries correspond to the 3 values of an RGB code (Red, Green, Blue). Each of the three RGB values (Red, Green, Blue) can range from 0 to 255. In this case, when the "Default" variable is 0, the RGB code will be (0, 128, 128), resulting in a blue LED. Conversely, when "Default" is 1, the code will be (255, 128, 128), which creates a pink LED.
- "DAC.CLASS1.BL1, BL2 and BL3" are the analog outputs that represent the three-phase voltages. They are connected to a digital-to-analog converter (DAC) that converts the digital signals into corresponding analog voltages. These analog voltages are then used to feed the voltage signals to the protection relay for processing and analysis.
- Three-phase voltages can take as values (Figure 5.2):
 - $\pm 4V$, if "Default" = "Risque_ilotage" = 0,
 - 0, if "Default" = 1 and "Risque_ilotage" = 0,
 - $\pm 5V$, if "Default" = "Risque_ilotage" = 1.

Once the Simulink diagram is completed and the parameters adjusted, the next step is to build the model. This is done by clicking on the "Build" button in Simulink, which compiles and transforms the model into code. Several files are then generated, including a .c file that corresponds to the generated C code, an .rta file (Real-Time Application), and an .sdf file (System Description File) that describes all the signals and parameters of the Simulink model. The .sdf file is the file used by ControlDesk, and it is loaded into the MicroLabBox to execute the model in real-time.

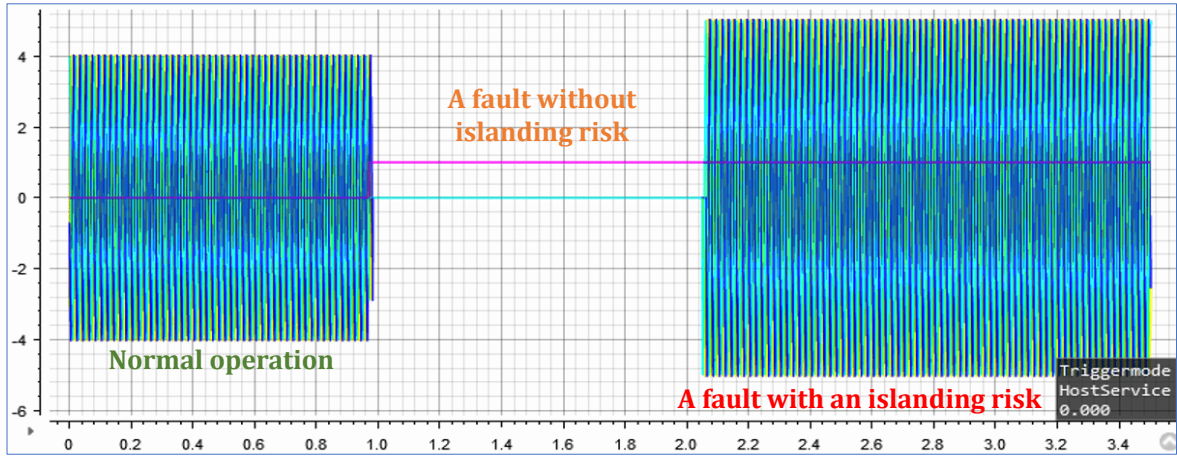


Figure 5.2: The possible values of the three-phase voltages

The voltage levels generated by the real-time simulator are insufficient to be directly interfaced with the protection relay. To overcome this issue, a voltage amplifier was introduced in the voltage measurement chain, as illustrated in Figure 5.3. This amplifier boosts the voltage to a suitable level for the protection relay to interpret the incoming signals.

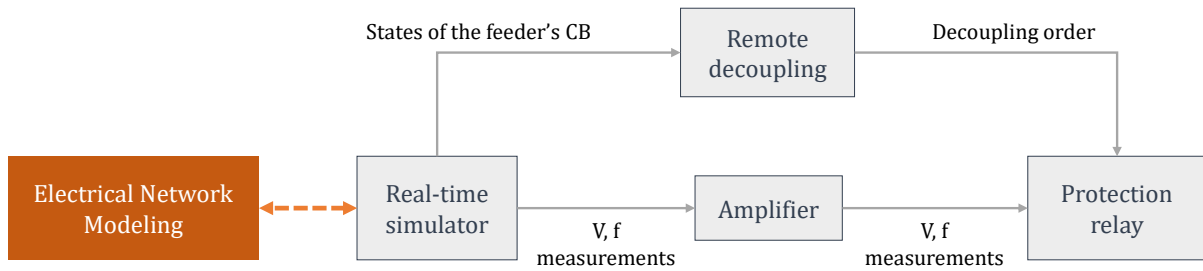


Figure 5.3: Experiment simplified architecture

5.2.2 Telecommunication Equipment

The 5G network used in this case study (Figures 5.4 and 5.5) is compliant with 3GPP R15 December 2018 and operates in TDD band n77 (3700 MHz) with a bandwidth of 100 MHz for the 5G new radio (NR), and FDD band n3 (1800 MHz) with a bandwidth of 20 MHz for the 4G radio. The core is based on NOKIA evolved packet core (ePC) and is a non-standalone (NSA) commercial core. The user equipment (UE) is a fixed wireless access (FWA) FastMile Gateway. To ensure reliable communication, a level 3 encapsulation is used to send GOOSE packets through an IP-based network.

Two SAR7705Hc routers are utilized for two purposes:

- Implementing level 3 encapsulation to enable the transmission of GOOSE messages from the Raspberry Pi to the Protection Relay. As 4G and 5G networks only support Layer 3 (IP), the routers are responsible for converting the Layer 2 messages into Layer 3 packets.

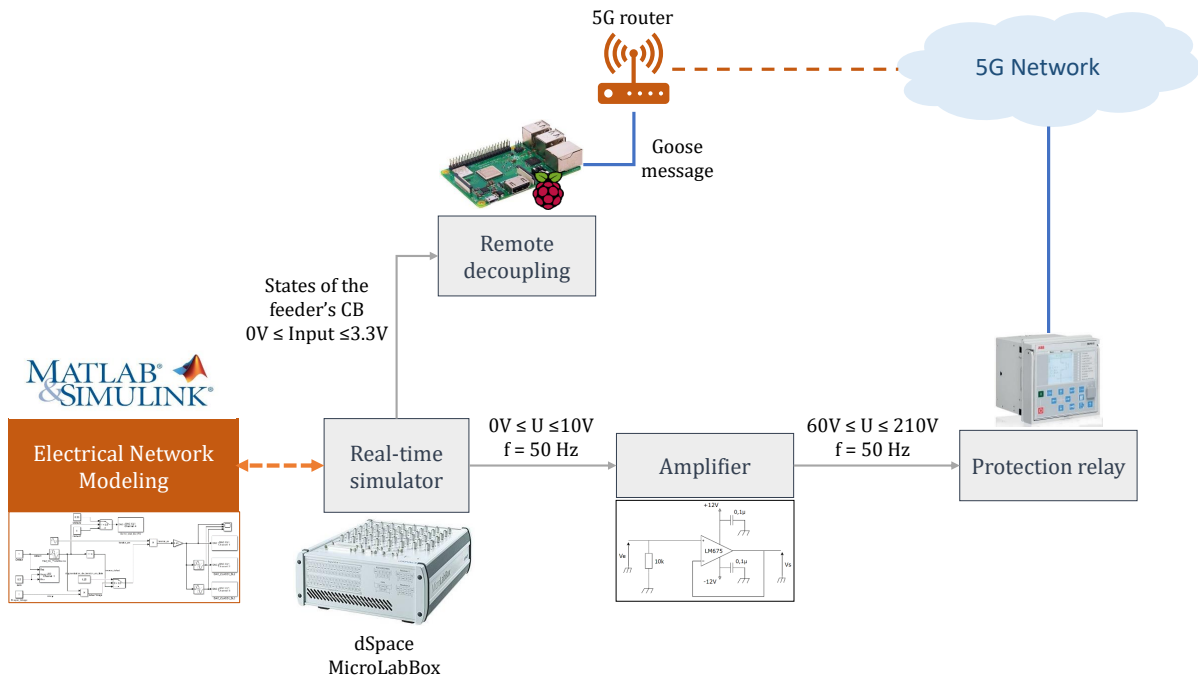


Figure 5.4: Experiment simplified architecture with 5G network

- Measuring data transfer performance between the devices. The routers are equipped with tools to evaluate network latency, jitter, and packet loss, which are essential in assessing the network's ability to reliably transmit real-time data.

The steps of the remote decoupling process, illustrated in Figure 5.6, are as follows:

- The circuit breaker of Feeder1 is opened.
- The status of the circuit breaker is sent to the Raspberry Pi, which is connected to a 5G router.
- The decoupling signal is transmitted through the 5G network.
- The protection relay receives and processes the decoupling signal.
- The PV circuit breaker is opened.

5.2.3 Tests and results

The two protection relays have distinct configurations. The ABB REF 615 relay is connected to the 5G network and has wide voltage and frequency thresholds. It receives a decoupling order from the Raspberry when the circuit breaker status changes from "0" to "1". On the other hand, the ABB REU 615 relay is designed with narrow voltage thresholds, making it highly responsive to voltage and frequency fluctuations.

The functional tests we performed are as follows:

- A voltage drop test after simulating a fault on the transmission system: The protection relay with instantaneous settings (REU 615) tripped, whereas the 5G-connected relay (REF 615) with delayed settings remained closed.

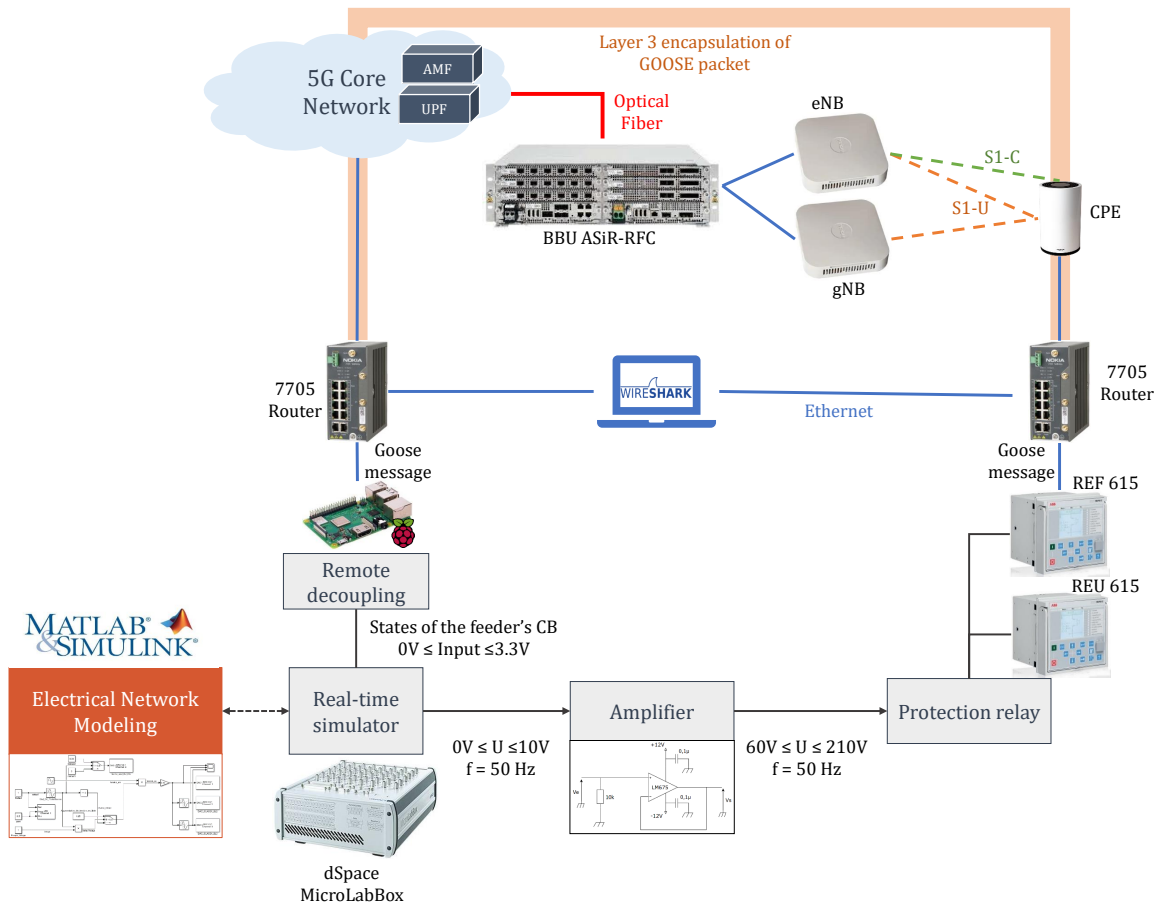


Figure 5.5: Remote decoupling experiment schema

- A voltage drop test after simulating the opening of the feeder circuit breaker (status changes from "0" to "1") : Both protection relays tripped. The relay with instantaneous settings (REU 615) opened due to voltage measurements, while the 5G-connected relay (REF 615) received a GOOSE decoupling command and reacted accordingly.

The performed tests helped to evaluate the performance and reliability of the protection relay with 5G connectivity in comparison to a traditional relay with instantaneous settings.

The GOOSE messages were transmitted exclusively from the core network to the protection device during the demonstration. To measure the delay, we utilized the Wireshark software on a PC connected to the mirror ports of two SAR 7705 routers. The average delay for the GOOSE messages was measured to be 7.5 ms and 8.5 ms over the 5G and 4G connections respectively. It's worth noting that there was no additional traffic on the test network, which helps explain the small difference in delay between the two network generations.

The measurement of two-way message delay was conducted using Ping traffic with the same size as the GOOSE packet. The time taken for the Ping packet to be sent and received was recorded and analyzed to evaluate the performance of the 5G and 4G networks. The results of the experiment are presented in Figures 5.7 and 5.8. The round

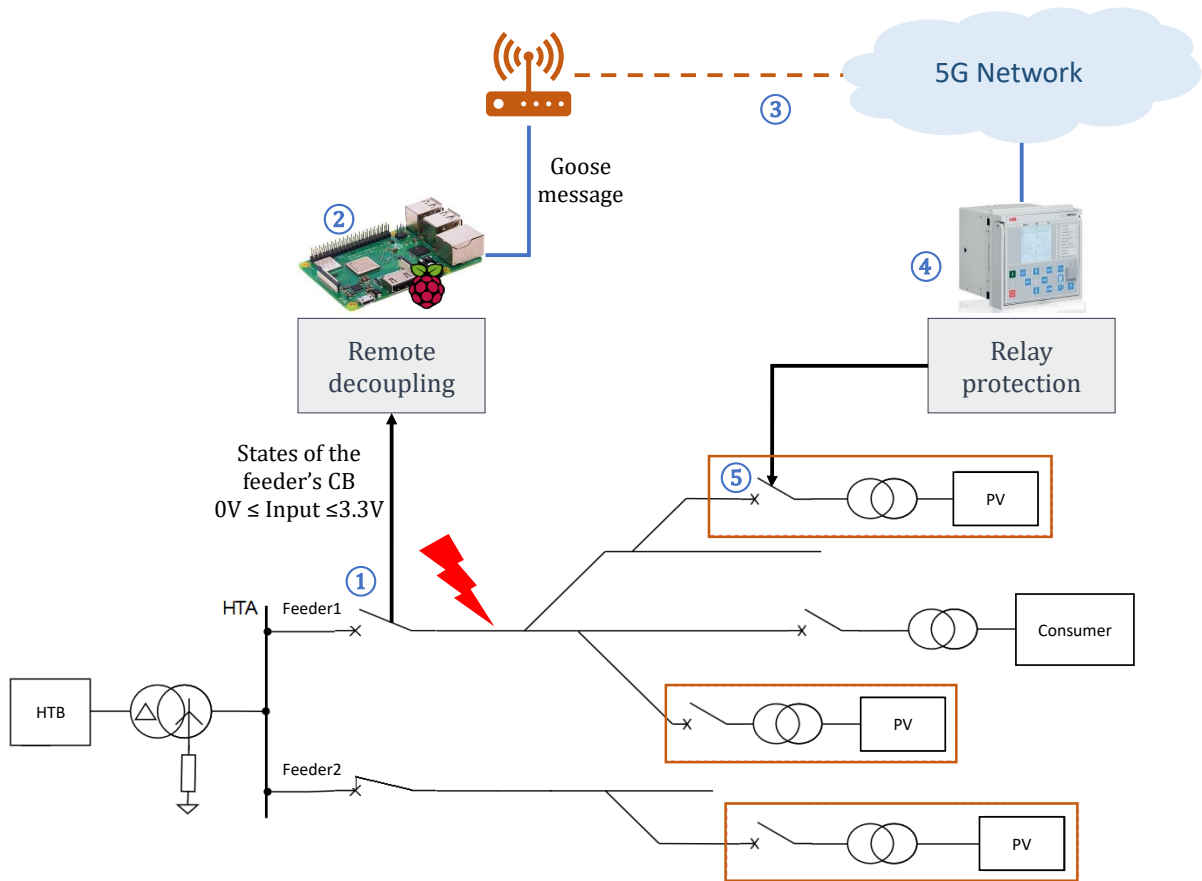


Figure 5.6: Targeted architecture using a distribution grid

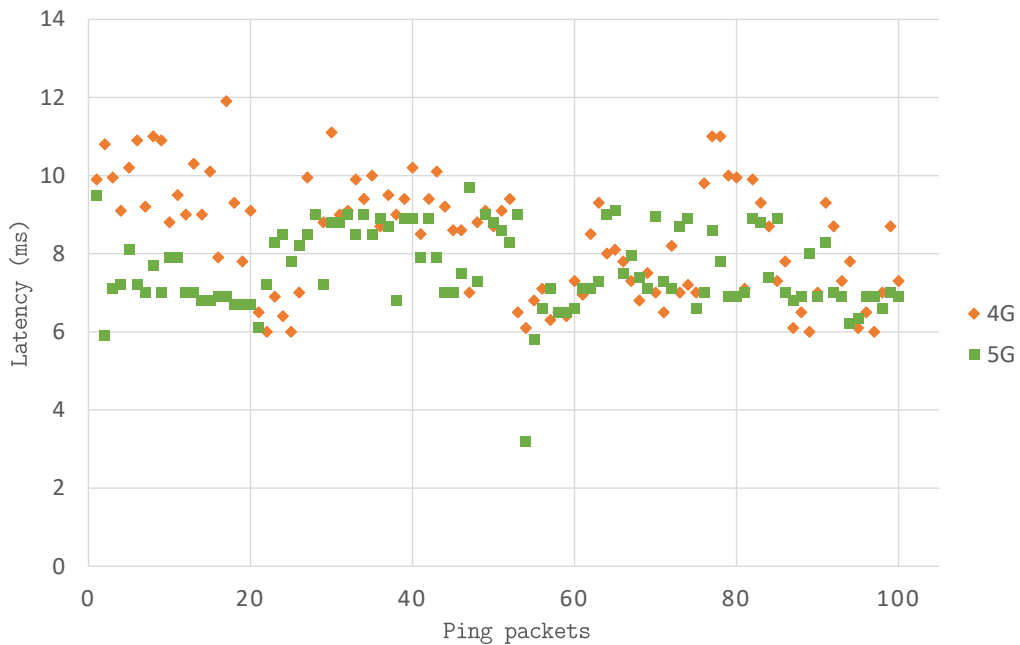


Figure 5.7: GOOSE measurements

trip average delay was found to be 23 ms on the 4G network and 13 ms on the 5G network, indicating a significantly improved performance on the 5G network compared to the 4G network.

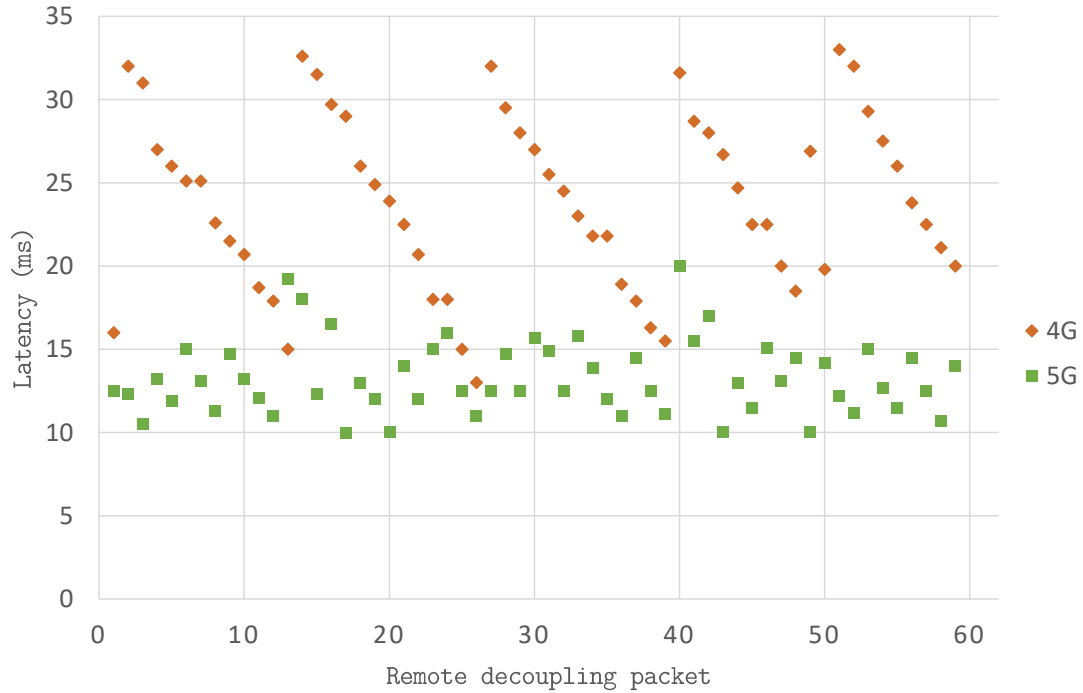


Figure 5.8: Ping measurements

5.3 5G NSA-based FLISR Application Experiment using a Simulated Distribution Grid

In this experiment, we implement the proposed FLISR application (defined in Section 3.6.2) using a simulated distribution grid. Our experiment involves three main layers, which are depicted in Figure 5.9.

The first layer is the grid layer, which includes a real-time simulator with an integrated Simulink model and a collection of physical protection components. The real-time simulator is connected to the physical equipment through analog or digital connections. Analog connections are used to transfer currents and voltages of the grid, while digital connections are used to communicate the status of various components of the simulated grid and receive control commands. The physical equipment consists of a set of power protection components such as protection relays and FPIs.

The second layer is the communication layer, which serves as an interface between the grid layer and the control layer. It comprises:

- Two SBCs (2 X Raspberry Pi 3) that function as digital gateways. These SBCs read the digital signals generated by physical or simulated power grid components and send the contained data to the controllers in the control layer through a 5G link. They also receive commands from the controllers (through a 5G link) and transform them into a digital signal that is transmitted to the physical or simulated power grid components.
- The 5G test network, which represents all the equipment that enables the transmission of data between the digital gateway and the control layer.

The third layer is the control layer, where data processing takes place, and decisions are made. This layer comprises local controllers deployed at the Edge level and a master controller deployed at the Cloud level. FLISR functions are deployed at two different levels (Edge or Cloud) based on two essential parameters:

- The required latency: If a fast response is needed, the function is deployed at the MEC level, which is closer to the physical equipment and can provide faster processing times.
- The level of situational awareness or the amount of data required for the function to operate correctly: If the function requires a more comprehensive view of the grid or more data processing power, it is deployed at the cloud level, which has more extensive computational resources and a broader view of the grid.

The role of local controllers is to analyze the collected data from the grid layer in order to send corrective orders to resolve local issues (i.e. FLISR functions 1,2,3 and 4: Fault detection, remote decoupling, fault location, and fault isolation) in the same substation, whereas, master controller which has a large system snapshot, uses aggregated data collected from local controllers to solve wide area problems (i.e. FLISR functions 5 and 6: Grid topology reconfiguration, system restoration).

5.3.1 Grid layer

5.3.1.1 Used Distribution Grid

The modeled distribution grid is a semi-urban with several unique features, including two 63/20 kV substations connected to each other via a coupling switch (SW_Coup).

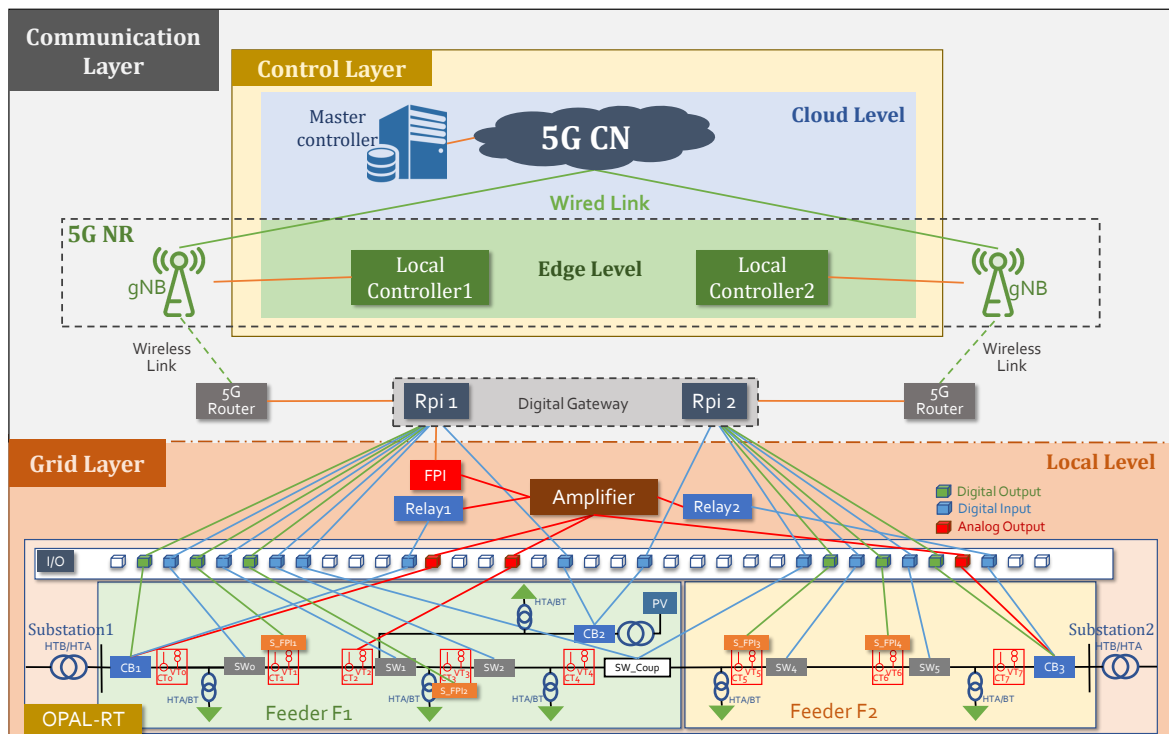


Figure 5.9: Experiment global architecture

About 65% of the electrical circuits are underground, while the rest are overhead. Each transformer is rated at 36 MVA, and the neutral is connected to the ground through an 80 Ohm resistance. Additionally, there is a 3 MW solar power plant (PV) connected to the grid (Feeder1 of substation1) through a circuit breaker (CB_PV). Earth Fault Over-current Protection is provided for the feeders of each substation (CB1 and CB2), while the PV plant is protected by a decoupling protection system with islanding detection (tele-decoupling) through the CB.PV. The real-time simulator includes current and voltage transformers placed in front of circuit breakers and switches to regulate the current and voltage of various subsections of the grid. Two ABB protection relays (as described in subsection 5.2.1) are also connected to the simulator, measuring the maximum current flowing through each phase. In the event of a grid fault, these relays will trip with a time delay and send opening orders to the appropriate circuit breaker (CB1 or CB2) through the simulator’s digital inputs.

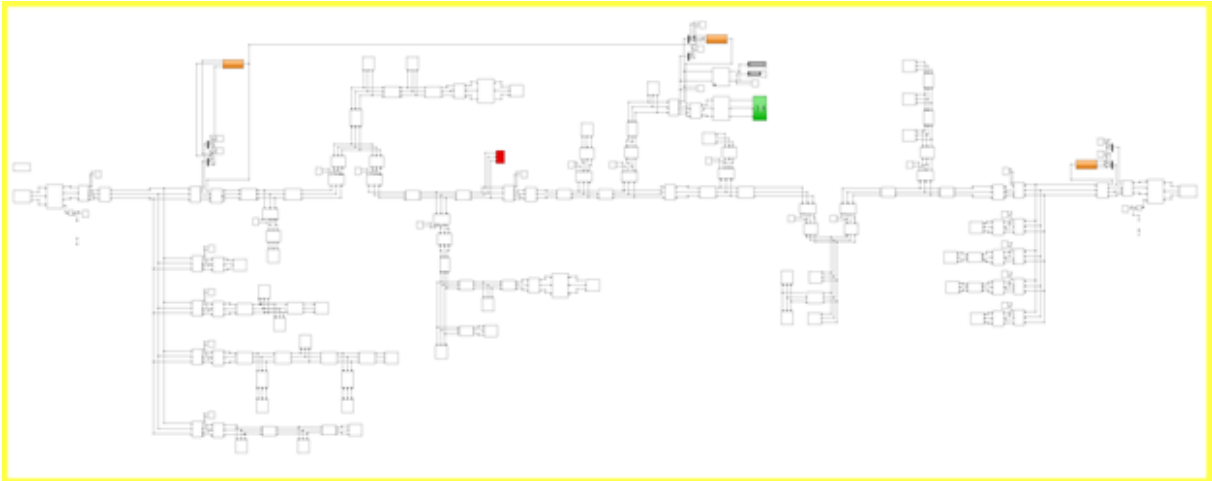


Figure 5.10: 20kV distribution grid simulated in Simulink

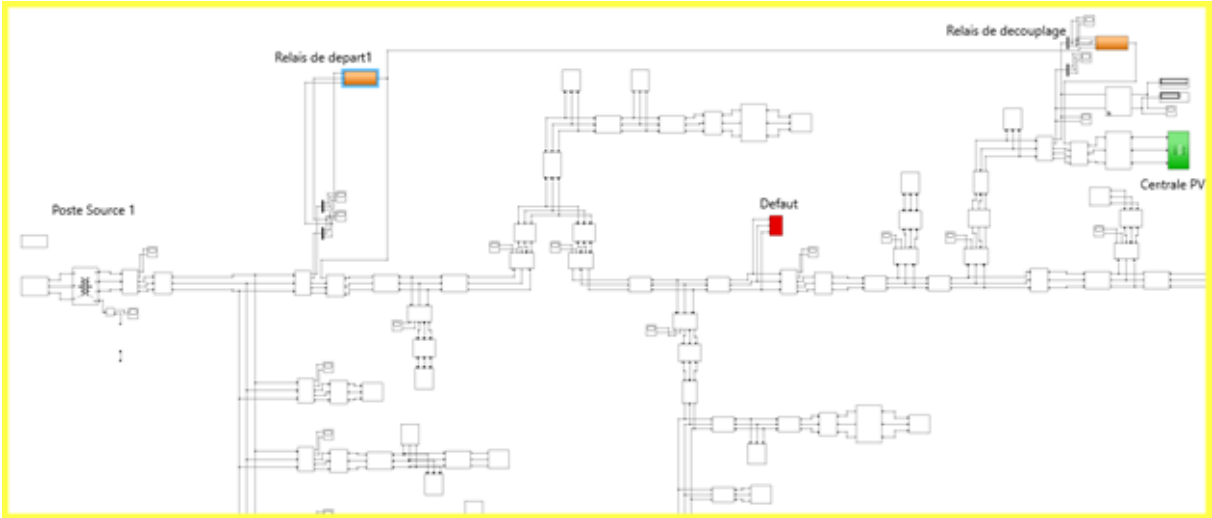


Figure 5.11: A zoomed part of the 20kV distribution grid (Substation1)

5.3.1.2 Used grid equipment

To model an electrical distribution grid, we utilized a HiL architecture and connected a range of protection components to a real-time simulator. These components included:

- ABB protection relay REF 615 N
- ABB voltage protection relay REU 615 A
- Schneider Flair 23DM Fault passage indicator: is a fault passage indicator that features a dual power supply and a voltage presence/absence relay (defined in section 7.4.5).
- Opal-RT real-time simulator: a real-time simulation that utilizes computer modeling to simulate the behavior of physical systems in real-time. We have integrated our Simulink model of a power distribution grid into a real-time simulator to achieve a higher level of realism. By using the input and output ports of the simulator, we are able to send and receive relevant signals, and perform control operations on the power grid in real-time. Finally, we observe and analyze the results obtained from the simulation (defined in section 7.4.6).
- RT-Lab control platform: is a software platform developed by OPAL-RT TECHNOLOGIES that allows for effective management and manipulation of real-time simulators. It provides a range of capabilities, including the ability to implement, edit, compile, run and analyze simulation models. RT-Lab is seamlessly integrated with MATLAB/Simulink, and once the Simulink models are loaded, any modifications must be made directly through the RT-Lab user interface (defined in section 7.4.7).
- Power Amplifier: Analog signals for current and voltage generated by simulated current and voltage transformers are transmitted via output ports of Opal-RT to protection equipment, including fault detectors and relays. However, due to the low power of these signals, they need to be amplified before transmission to the input of the protection equipment. To address this issue, an amplifier is used, which is placed between the analog outputs of Opal-RT and the analog inputs of the protection equipment.

5.3.2 Communication layer

Figure 5.13 illustrates the communication layer of the experiment. The 5G network in use is compliant with NSA standards, adhering to the 3GPP R15 December 2018 guidelines. Specifically, the 5G NR, as provided by Amarisoft Callbox [12], operates within the TDD band n78 (3500- MHz) and employs a 20 MHz bandwidth.

We used an NSA core [23] two 5G-compatible routers as UEs. Each SBC is connected to one of the routers through an ethernet cable. The 5G NR is connected to the core network using a fiber optic cable.

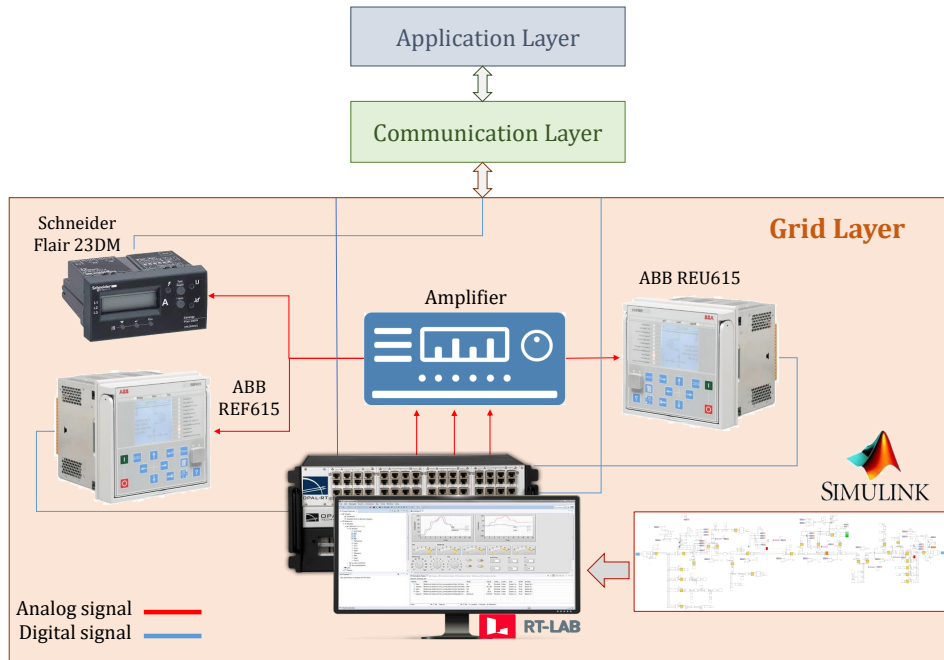


Figure 5.12: Physical deployment of the grid layer

5.3.3 Application layer

Figure 5.14 depicts the deployment of FLISR virtual functions at the application level, which can be deployed at the edge or cloud level as required and can migrate to optimize telecom performance. In our case study, we utilize a single cloud location and multiple edge locations, with an orchestration system managing the life-cycle of the virtual functions and an optimization model (presented in Chapter 4) determining the optimal location for each function. The detailed implementation of this architecture is illustrated in Figure 5.15.

The Kubernetes cluster, as depicted in Figure 5.15, consists of a central node, called the Master, and four worker nodes. The Master serves as the controller for the cluster, overseeing the deployment of virtual functions, known as pods, on the worker nodes. Each pod can contain one or more containers, and each container hosts one or multiple FLISR functions. We utilized Docker technology to build FLISR virtual functions, which are stored in a repository, allowing us to load them on-demand.

The Master node hosts several key components, including:

- A Python client that receives external commands from outside the cluster and forwards them to the Kubernetes API (application programming interface), such as receiving information from the optimization model to determine where to deploy each virtual function.
- Load balancers that expose the services of the different pods to the external network.
- A Master controller pod that hosts the reconfiguration and system restoration functions of the FLISR process.

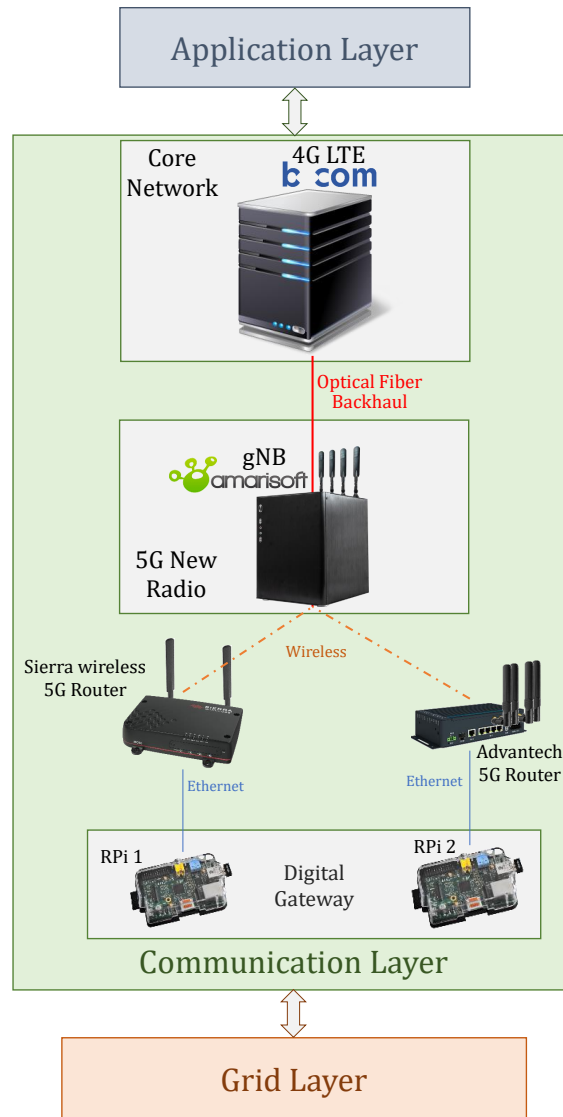


Figure 5.13: Physical deployment of the communication layer

- Prometheus server and Grafana pods, a duo of tools that collect diagnostic data from the worker nodes and present it on a dashboard.
- A Control plane containing the necessary components for the Master node to function as the cluster controller.

In our case study, we deploy worker nodes at the edge. Each worker node is equipped with an alert manager that sends diagnostic data, such as memory usage, CPU usage, and the number of hosted pods, to the Prometheus server. Additionally, the worker nodes may contain one or many edge controllers that host a set of FLISR functions, including Remote Decoupling, Fault Localization, and Fault Isolation, which have stringent communication requirements. The placement of these edge controllers is determined by the optimization model outlined in Section 4.3.2.1.

The Two Raspberry Pi boards serve as gateways for transmitting data from the digital outputs of the real-time simulator to edge controllers via GPIO pins and receiving commands from the edge controllers to route to the digital inputs of the real-time simulator. Each Raspberry Pi connects to a 5G router via an RJ45 link. The Python Server1 and

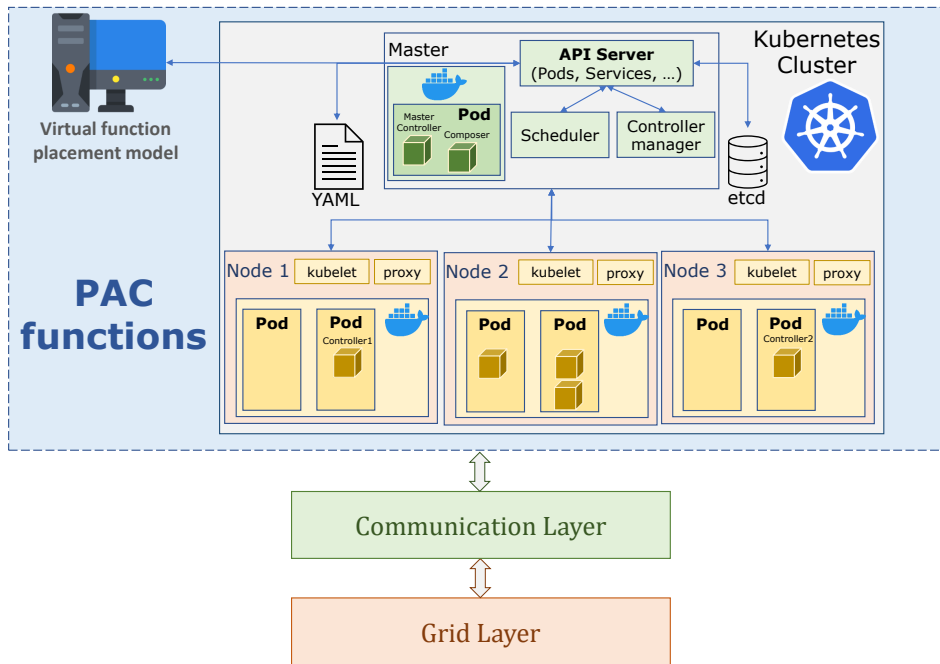


Figure 5.14: FLISR functions deployment

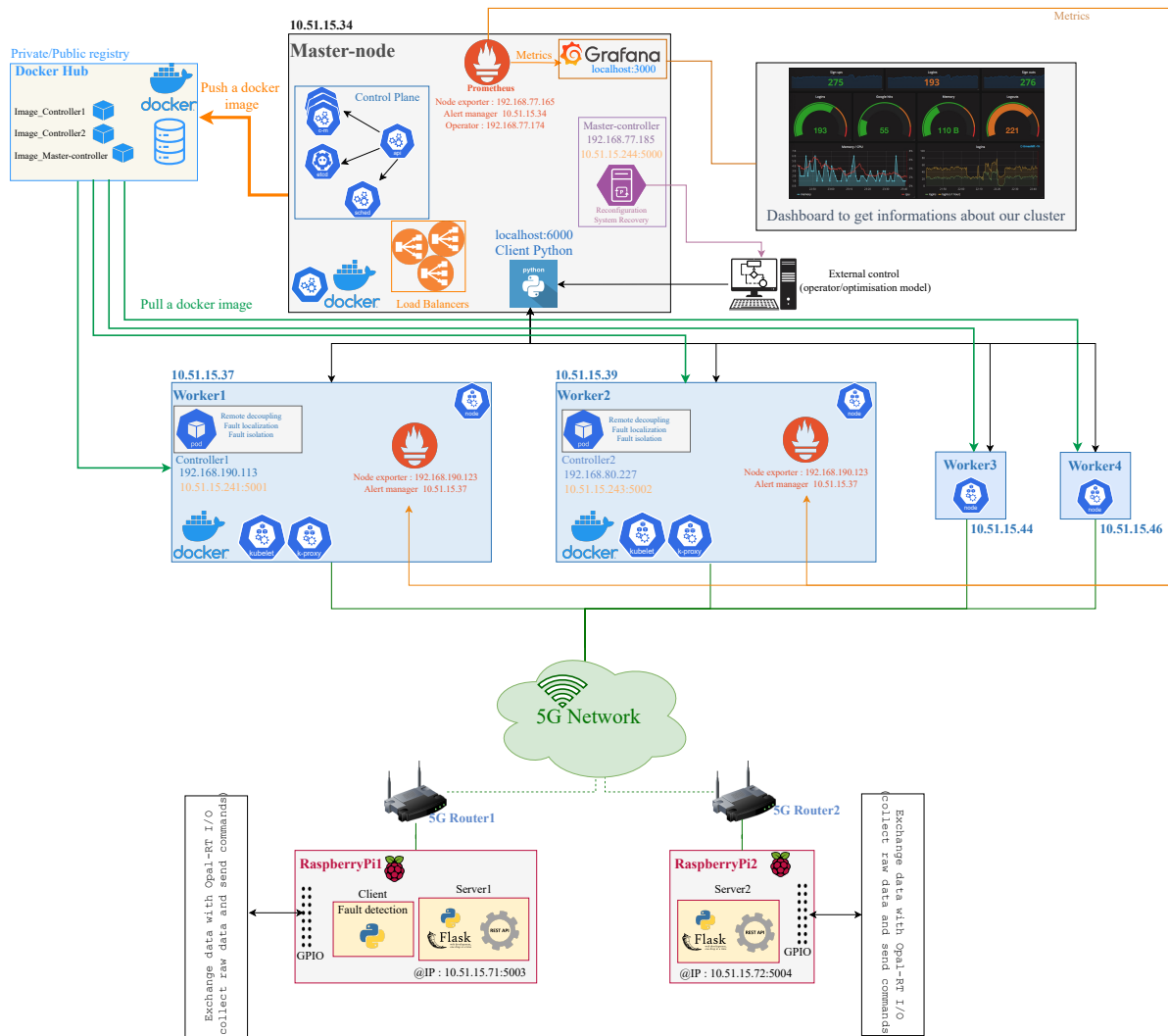


Figure 5.15: Detailed implementation of the application layer

Server2 codes act as REST APIs, which receive commands from virtual functions using the HTTP protocol. Moreover, the Python Client program in Raspberry Pi1 monitors the status of simulated protection equipment through the GPIO pins and triggers an alert, in the form of an HTTP request, when a fault occurs on the electrical grid. Finally, the alert is sent to the corresponding edge controller.

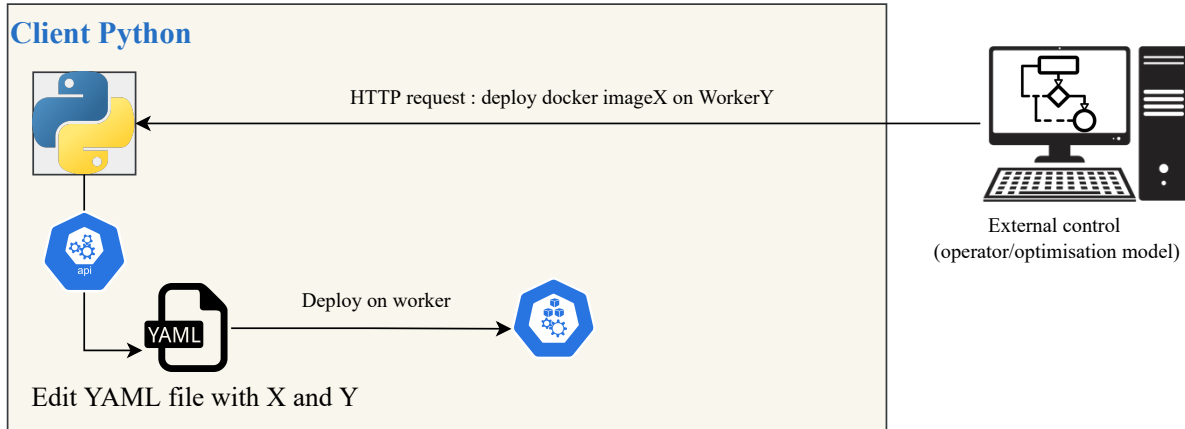


Figure 5.16: Optimization process for FLISR function deployment

Figure 5.16 illustrates how the virtual functions are deployed on the edge controllers. To determine the optimal placement of FLISR virtual functions, we utilize the optimization model developed in Section 4.3.2.1, which determines the appropriate pod for each function. The model is hosted on an external server and communicates with the Python client on the Master controller through HTTP requests. The Python client receives these commands and sends them to the Kubernetes API, which updates a YAML file and deploys it to the cluster to apply the changes. The YAML file includes information such as the desired number of replicas of the virtual functions, the location of the edge controller, and the resource allocation for each pod. Once the deployment is complete, the edge controllers receive the new pods and begin executing the FLISR functions. Additionally, the edge controllers may send diagnostic data, such as resource usage, to the Prometheus server for further analysis and monitoring. This deployment allows for efficient and flexible management of the virtual functions, enabling the cluster to dynamically adapt to changes in the power grid and optimize the performance of the FLISR application.

5.3.4 Implemented FLISR Scenario

The following scenario outlines the sequence of actions taken during a fault event in a distribution power grid. The scenario covers fault detection, remote decoupling, fault location and isolation, grid reconfiguration, and service restoration. The scenario is divided into three phases, detailed hereafter.

5.3.4.1 Phase 1

Before the fault, the distribution system is in its normal operation mode and the FLISR virtual functions are optimally deployed. The first phase starts at $t = 5s$:

- (a) A ground fault occurs between switches SW1 and SW2.
- (b) The current and voltage transformers in feeder F1 send instantaneous current and voltage values from each part of the grid to the physical protection components. The signals are received from the analog outputs of the real-time simulator, amplified by the amplifier, and then transferred to the protection components (FPI and protection relays). Simulated FPIs detect the fault and send a digital signal to the Raspberry Pi1 using the digital outputs of the simulator.
- (c) After detecting the fault in the feeder F1, a protection relay trips and sends a digital signal through the simulator digital inputs to open the circuit breaker CB1.
- (d) The notification of the CB1 tripping as well as the notification of fault detection by the physical/simulated FPIs are sent to the Controller1.
- (e) The Controller1 detects the occurrence of a fault in feeder F1 and notices CB1 tripping, so it sends a decoupling command to CB_PV (solar power plant circuit breaker).
- (f) At the same time, the Controller1 analyzes the signals received from grid FPIs and locates the fault.
- (g) To isolate the fault, Controller1 sends digital signals through the simulator digital inputs to trip SW1 and SW2, which are respectively the closest upstream and downstream switches to the fault location.
- (h) Controller1 sends closing command to CB1 in order to recover the upstream loads.
- (i) After checking that the second substation can support the feeder F1 disconnected loads, the master controller perform grid reconfiguration function, thus sends closing command to the coupling switch (SW3) so that the disconnected downstream loads will be re-energized by feeder F2.
- (j) Controller2 sends a closing command to CB_PV to recover a portion of downstream loads. As a result, all grid sections except the defective part are under voltage.
- (k) The master controller transmits the updated grid topology to the optimization model, which then computes the optimal placement of FLISR virtual functions. Upon completion, the optimization model sends an HTTP POST request to the Python client, prompting the redeployment of virtual functions into the optimal pods.

At the end of this phase, the topology of the power grid is modified, and the solar power plant is connected to feeder F2 instead of F1, controlled by Controller2 instead of Controller1.

5.3.4.2 Phase 2

The second phase of the scenario starts at $t=15st=15s$, where an earth fault appears between switches SW4 and SW5. The following actions are taken in this phase:

- (a) Controller2 follows the same steps as Controller1 in phase 1 to detect, locate, and isolate the fault.
- (b) Controller2 sends a remote decoupling command to CB_PV since the PV plant is connected to substation 2. Thanks to 5G communication, this level of flexibility is now possible, which is not the case in a conventional wired remote decoupling scheme.
- (c) Controller2 sends closing command to CB2 in order to recover the upstream loads.
- (d) After verifying that the defective portion of the grid in feeder F1 was not repaired, the master controller will not perform grid reconfiguration function.

After this second part of the scenario, a portion of the grid (between SW2 and SW5) is still not supplied.

5.3.4.3 Phase 3

In the final phase, after repairing all the defective portions of the grid, the master controller executes the restoration function to restore system's initial configuration. Next, transmits the updated grid topology to the optimization model, which computes the optimal placement of FLISR virtual functions. Once the optimization is complete, the model sends an HTTP POST request to the Python client, triggering the redeployment of virtual functions into their optimal pods.

5.3.5 Tests and results

Using Matlab Simulink blocks, we measured the following delays:

- Average remote decoupling delay (RD_D): the delay between the opening of FCB and CB_PV.
- Fault location delay (FL_D): the delay between the fault detection (by the FPIs) and the execution of the fault location function by the local controller.
- Average fault isolation delay (FI_D): the delay between the fault detection and the opening of the closest upstream and downstream switches to the fault.
- Average grid reconfiguration delay (NR_D): the delay between the fault detection and the execution of the power grid reconfiguration function.

The experimental results presented in this study, as shown in Figures 5.17, 5.18, and 5.19, demonstrate the high reliability of the 5G link, with 100% of packets successfully

reaching their destination. The achieved Avg_RD_D is below the maximum transmission time permitted by French regulations [49] (i.e., $< 70ms$). It should be noted that the Avg_NR_D of 100 ms was obtained with a limited configuration of only two substations. With the same architecture using a permanent 5G link in a full-scale configuration, such as with 50 substations, we anticipate that the average grid reconfiguration delay would be reduced from several minutes to just a few seconds. This level of improvement is possible thanks to the flexibility provided by 5G communication, which is not achievable with conventional wired remote decoupling schemes.

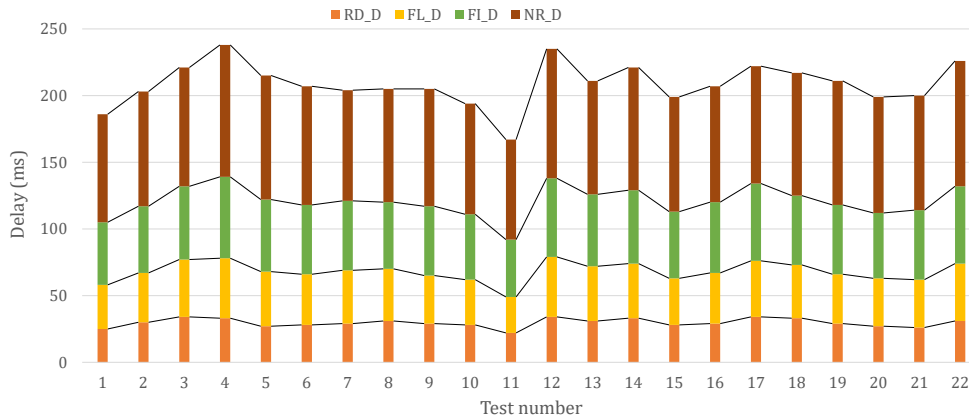


Figure 5.17: Delay of FLISR functions

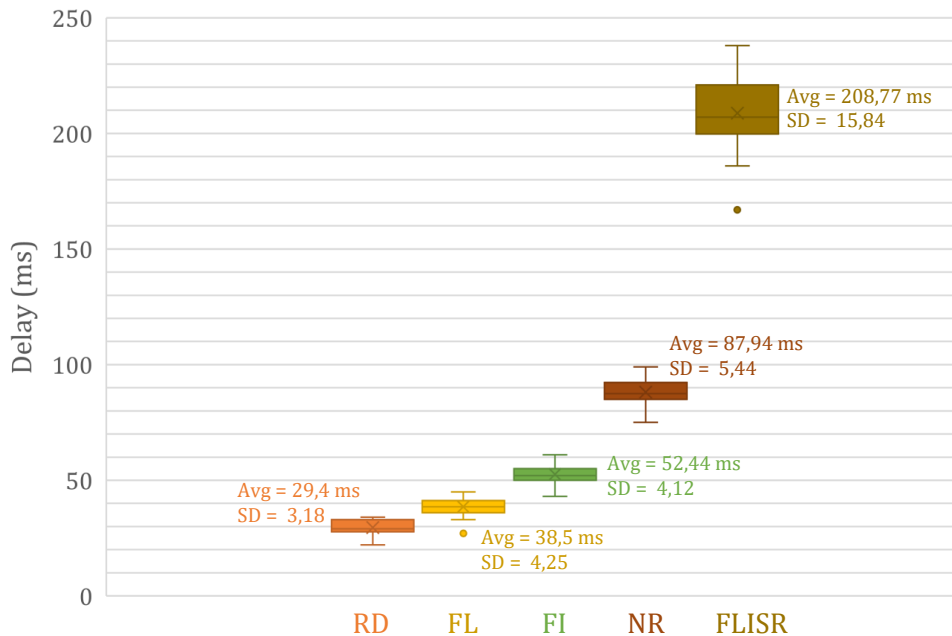


Figure 5.18: Average delay and standard deviation of the FLISR process

Figure 5.19 shows the performance of the 5G NSA test network in terms of packet delay in both the uplink and downlink directions, which are nearly equal.

In addition to the high reliability of the 5G link, the advanced FLISR system also leverage the use of virtualization and orchestration concepts to provide more flexibility in

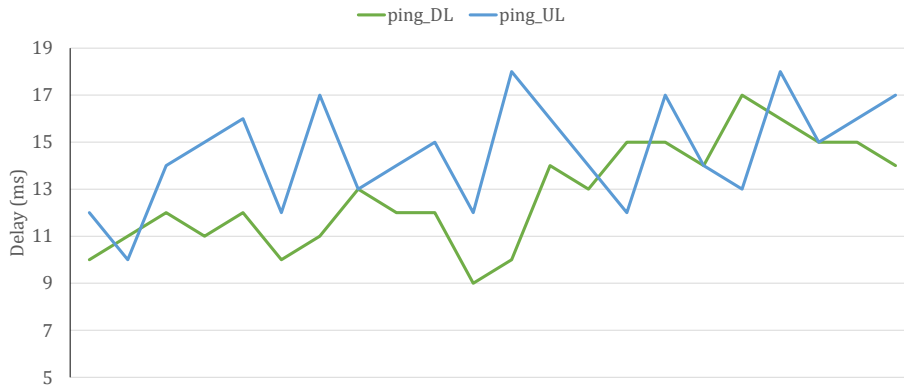


Figure 5.19: 5G NSA test network performance

its operations. Virtualization allows for the creation of virtual FLISR functions as docker containers that can be used to simulate physical resources. This enables the FLISR system to operate in a more agile and cost-effective manner as resources can be added or removed as needed, without the need for physical hardware changes.

Orchestration, on the other hand, refers to the automated management of the virtual FLISR functions to ensure they work together seamlessly. This means that the advanced FLISR system can be managed centrally, with automated processes being triggered when a fault is detected in the power grid. This allows for a faster response time and reduces the need for human intervention, increasing the reliability of the system.

Together, virtualization and orchestration provide the advanced application layer of FLISR system with the ability to quickly and efficiently adapt to changes in the power grid. This makes it more flexible and resilient in the face of faults, allowing for quicker restoration times and increased reliability.

5.4 5G SA-based FLISR Application Experiment using a Real Distribution Grid

In this section, we present our field experiments when deploying FLISR applications on a real 5G SA network and using a real distribution grid, namely Concept Grid.

5.4.1 Concept Grid

The Renardières R&D center, situated in Ecuelles, Seine-et-Marne, operates two research laboratories, namely "Concept Grid" and "Smart Substation Lab", where they have implemented a real-life electrical system with all the necessary components for various use cases. These components include a substation equipped with a 6 MVA transformer, multiple MV/LV transformer stations with 400kVA transformers and MV switching cells, a grid consisting of 3km of MV lines and 120 km of simulated lines, as well as a photovoltaic DER called "AgriPV".

In addition, this electrical system also features test resources that can generate faults

on the MV system, including single, two, or three-phase faults, and three neutral systems (resistive, compensated, or active). These resources facilitate the simulation of faults commonly encountered in the field, such as a fallen line, and enable the initiation of the FLISR process to manage them. The laboratories are also equipped with a control room that allows for the monitoring of test progress and the measurement of FLISR process performance.

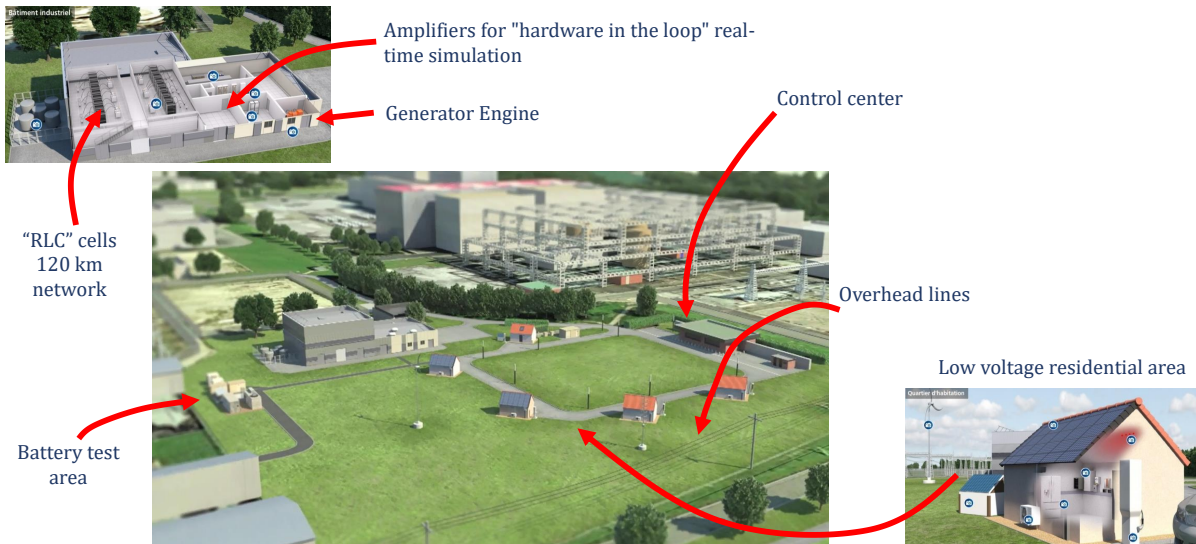


Figure 5.20: Presentation of the Concept Grid test facilities on the Renardières site

5.4.2 Experiment Architecture

Figure 5.21 displays the physical location of the electrical structures and telecom equipment utilized in the experiment at the Renardières site. These structures include:

- Building T.25, which houses the 5G infrastructure, including the 5G core and the Base Band Unit (BBU), as well as the control and command system for piloting tests and reporting measurements.
- A 5G Remote Radio Unit (RRU), situated on a mast close to Building T.25.
- Building T.18, the substation, where two 5G routers are installed and connected to Raspberries RPi1 and RPi3, located approximately 80m away from the antenna mast.
- Building P.26, the MV/LV Smart Substation Lab, which houses a 5G router and the Raspberry RPi2, situated approximately 280m away from the antenna mast.

The architecture of the MV/LV system consists of two feeders (Figures 5.22 and 5.23). The first feeder consists of a main artery supplied from the Concept Grid substation (BICG) on the "Moret" feeder to the closed area where the MV faults were generated, and a branch to the SSL laboratory (Smart SubStationLab) via ER14. The second Feeder (Episy) is also connected to the Concept Grid substation (BICG) and feeds the SSL



Figure 5.21: Aerial view of the location of the various structures on the Renardières site

laboratory (Smart SubStationLab) via AC3T. As shown in Figure 5.22, at the beginning of the tests, the Feeder's 1 (Moret) circuit breaker (CB1) is closed, while Feeder's 2 (Episy) circuit breaker (CB2) is open.

As part of this experiment, we generated a zero sequence fault (40A short-circuit between phase 1 of the Moret feeder and earth for 700 ms). The time and duration of the faults were controlled via a sequencer.

5.4.3 5G SA Network used for Field Testing

5.4.3.1 5G SA Core Network

com *Dome* is a proprietary software solution compliant with the 5G standard for private networks. It is designed to be scalable, flexible, and easy to manage, and can enhance productivity by providing advanced digitization, asset control, and automation. Additionally, it provides highly secure and reliable connectivity. some advantages and features of this solution:

- Deployment of industrial applications that require low latency.
- Full data control with a high level of security
- 100% software and cloud native implementation allowing fast and efficient configuration
- Guaranteed QoS with high performance

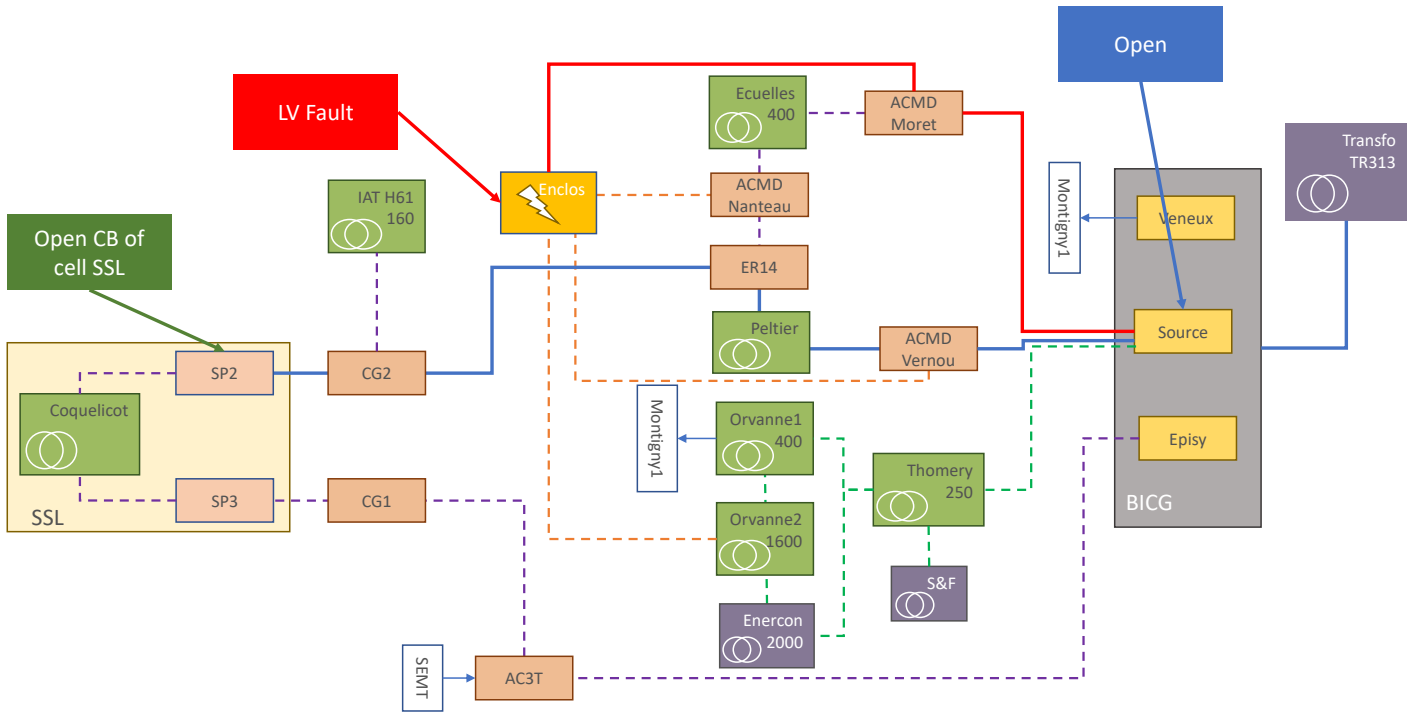


Figure 5.22: Detailed architecture of the experimental grid (normal operation)

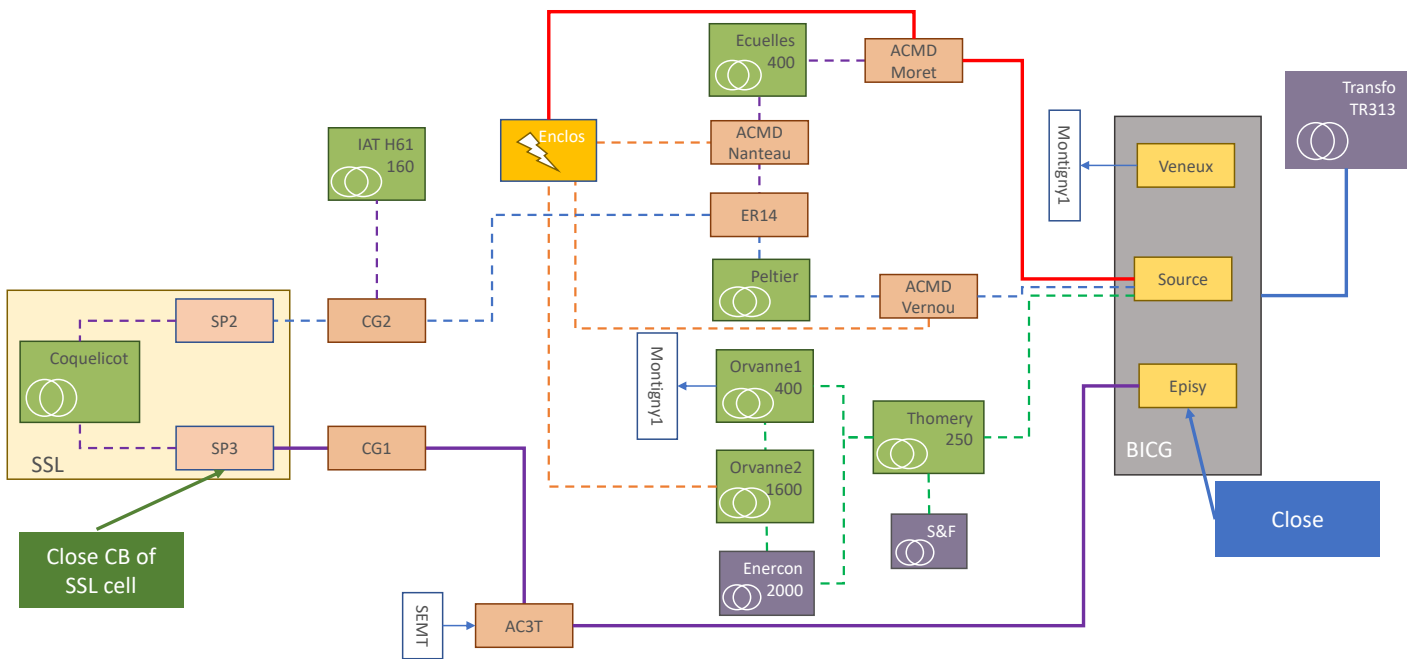


Figure 5.23: Detailed architecture of the experimental grid (after reconfiguration function)

- Compact and economical solution for private/corporate operators
- Core Network Control Plane:
 - 5G SA architecture
 - Quality of Service enforcement
 - Distributed deployment with Local Breakout
- Support edge computing deployment

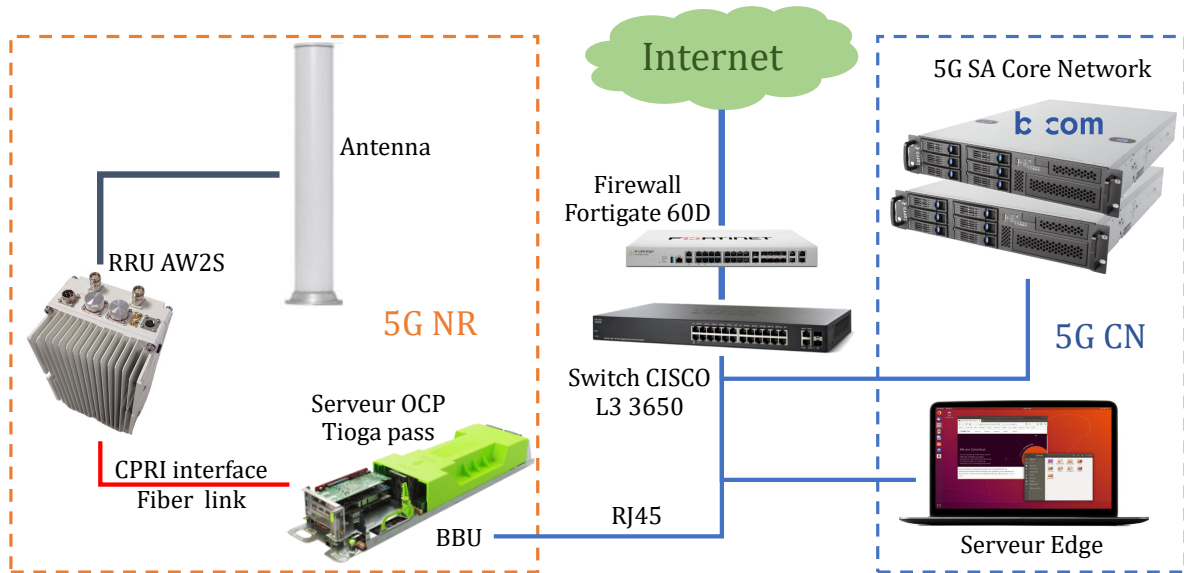


Figure 5.24: 5G network deployment

- 5G-NR RAN FR1 (below 7.125 GHz)
- Security:
 - SIM-based cellular
 - authentication (EPS-AKA, 5G-AKA)
- Deployment Platform:
 - Deployment on standard IT equipment
 - Container-based Network Functions
 - Kubernetes orchestration

5.4.3.2 5G Routers

To carry out our field experiment, we utilized three 5G routers (as illustrated in Figure 5.25) different brands. At present, no protection equipment is equipped with 5G connectivity. However, as the performance benefits of 5G networks are leveraged in the development of new PAC use cases, we anticipate the development of new equipment that integrates 5G connectivity. The lack of use cases and the high cost of 5G integration currently present major obstacles to this development. Nonetheless, we believe that continued research and development in this area will eventually overcome these barriers, paving the way for the widespread adoption of 5G-enabled protection equipment.

We then connected a Raspberry Pi device to each router, as illustrated in Figure 5.26. To enable direct access to each Raspberry Pi, we implemented port forwarding at the router level. This configuration allowed us to connect to each Raspberry Pi device using the IP address of the corresponding 5G router to which it was connected. Moreover, to



Figure 5.25: Used 5G routers

ensure seamless connectivity, we pre-configured and registered a SIM card for each router on the 5G core network HSS³ (Home Subscriber Service) function.

The communication between the controller and the three Raspberry Pi devices (RPi1, RPi2, and RPi3) responsible for controlling circuit breakers CB1, CB_PV, and CB2, respectively, is also shown in Figure 5.26. This exchange of messages occurs in response to an event, such as a fault on the grid. The messages are in the form of packets that are the same size as GOOSE messages in the IEC 61850 standard. The controller sends messages to the Raspberry Pi devices to turn the circuit breakers on or off, and the Raspberry Pi devices send messages to the controller to report the status of the circuit breakers. This communication is essential for the proper functioning of the system and allows the controller to monitor and control the circuit breakers remotely.

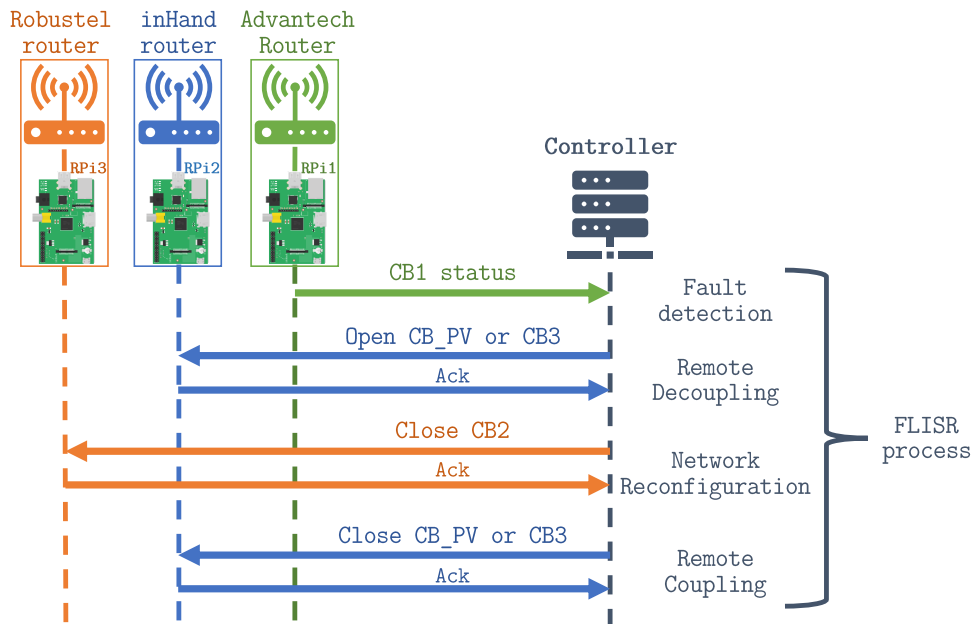



Figure 5.26: message exchange during use case process

³The HSS is a central database that stores information about the subscribers of a mobile network and is used to authenticate subscribers and authorize their access to the network.

5.4.3.3 BBU server: Tioga Pass server

The server used to host the BBU part of the 5G NR is a Mitac Tioga Pass E7278-S. The server is compatible with The Open Compute Project (OCP⁴) design. The Figure 5.27 shows some BBU server characteristics.



	Standard (E7278-S)	Advanced(E7278-A)	Ultra (E7278-U)
Processor	(2) Intel® Xeon® Scalable Processor, TDP 165W • Support both SkyLake SP and Cascade Lake SP, Intel® C621-AT chipset		
Memory	(12) DIMM slots, 6 channels • Up to 768 GB R-DIMM, DDR4 2933MT/s		
PCIe Extension	(2) FHHL PCIe Gen3 x16	(2) HHHH PCIe Gen3 x16	(1) FHHL PCIe Gen3 x16
Boot Drive (for OS)	80/110mm M.2 (SATA/PCIe Gen3 x4)		
Storage Extension	(1) 3.5" SATA HDD	(6) 2.5" 7mm SATA SSD	(4) 2.5" U.2 SSD (Hot Plug) (1) 2.5" 7mm SATA SSD (optional) ¹⁾
Mezzanine	(1) OCP NIC 2.0		
Management Port	(1) 1GbE RJ45, Intel i210, support NC-S		
BMC	ASPEED AST2500 • Support IPMI 2.0 and DMTF Redfish® 1.7 (DSP0266 1.7.0 Specification and Redfish Schema 2019.1)		
Dimension & Weight	D28.5" x W6.9" x H3.5" (724 x 175 x 89mm) / 17.6~18.7lbs (8~8.5kg)		
Power Supply	Centralized OCP power shelf (12V DC)		
OS Certification	VMWare • ESXi 6.7 U2/U3 • ESXi 7.0 Red Hat® • RHEL 7.6~7.x (x86_64 Arch) • Red Hat® OpenStack® 13.0 - 13.x (x86_64 Arch) • Red Hat® OpenStack® 14.0 - 14.x (x86_64 Arch) • Red Hat® Virtualization 4.2 - 4.3 (x86_64 Arch)		
Other Certification	SEBA Certified HW (before June 2020)		

Figure 5.27: BBU server specifications

5.4.3.4 AW2S RRU

A RRU is a type of wireless communication equipment that is used in mobile networks, such as a 5G network. It is typically used to transmit and receive wireless signals, and it is typically installed on a tower or other high structure in order to provide coverage over a large area. The AW2S RRU is a specific model of Remote Radio Unit that is manufactured by AW2S, some specification of the equipment are:

- Up to 2x20W RRH RF output
- 2×2 MIMO

⁴OCP is a worldwide network of technology leaders that promotes the utilization of open hardware and software. OCP has various initiatives and working groups dedicated to transforming hardware into a more efficient, flexible, and scalable form, providing more choices and customization options while reducing costs [129].

- CPRI⁵ input
- Support for multiple 2G, 3G, 4G and 5G RATs (Radio Access Technologies)
- Support for all standard TDD/FDD bands
- Personalization possible

In a 5G-Cloud RAN communication network, the BBUs process and modulate the digital signals transmitted to and from the wireless devices (the 5G router in our use case). The RRUs convert the digital signals into radio frequency signals to be transmitted over the air, and for converting the RF signals back into digital signals for processing by the BBUs. The CPRI interface allows communication between BBUs and RRUs. This digital baseband signals exchange is required for the operation of the 5G communication system. The interfaces provide a standard way for different manufacturers' equipment to interoperate and work together in a wireless network.

5.4.4 Implemented FLISR Scenario

Before the fault, the distribution grid is in its normal operating mode, the fault is triggered manually by a technician:

- (a) A ground fault appears when switch SW1 is closed (Figure 5.28-1), it propagates through feeder 1 and will be detected by circuit breaker CB1.
- (b) After detecting the fault, the CB1 circuit breaker will wait 250 ms before tripping (to avoid tripping on a transient fault) as shown in Figure 5.28-2.
- (c) When CB1 opens, a 48v signal is sent through a Phoenix Contact PLC-RPT-48DC/21AU relay module which activates a switch to allow a 5v signal to supply a GPIO pin of the Raspberry RPi1. RPi1 considers the analog signal (u) as a digital signal (d) (if $u \geq 3.3v$ then $d = 1$; else $d = 0$), if the digital signal is equal to 1, RPi1 sends a notification of fault occurrence and CB1 tripping to the controller. To ensure very low latency, udp protocol was used (Fault detection notification in Figure 5.26).
- (d) The Controller considers the occurrence of a fault in feeder F1 and CB1 tripping and sends a decoupling command to solar power plant circuit breaker CB_PV (Figure 5.28-3) through RPi2 (Remote decoupling command in Figure 5.26).
- (e) After disconnecting the F1 feeder and assuming that the fault is not yet repaired, the Controller sends a close command to CB2 via RPi3 (Grid reconfiguration command in Figure 5.26) in order to re-energize the disconnected loads. The photovoltaic plant is now connected to the F2 feeder as shown in Figure 5.28-4.

⁵The Common Public Radio Interface (CPRI) is a standardized interfaces for the connection of BBUs to RRUs in wireless communication systems. CPRI is used to transmit digital baseband signals between the BBUs and RRUs over fiber optic cables or other high-speed communication links.

- (f) Now that the solar power plant is connected to Feeder 2 (which has no fault), the Controller sends a close command to CB.PV via RPi2 (Remote coupling command in Figure 5.26) and couples the PV plant to the grid again(Figure 5.28-5).

The remote decoupling process is carried out between two protection equipment managed by RPi1 and RPi2 to achieve the inter-triggering between the circuit breaker CB1 on the feeder F1 and the circuit breaker CB.PV on the MV cell of the Smart Substation Lab (Building P.26) which serves the AGRI-PV photovoltaic farm.

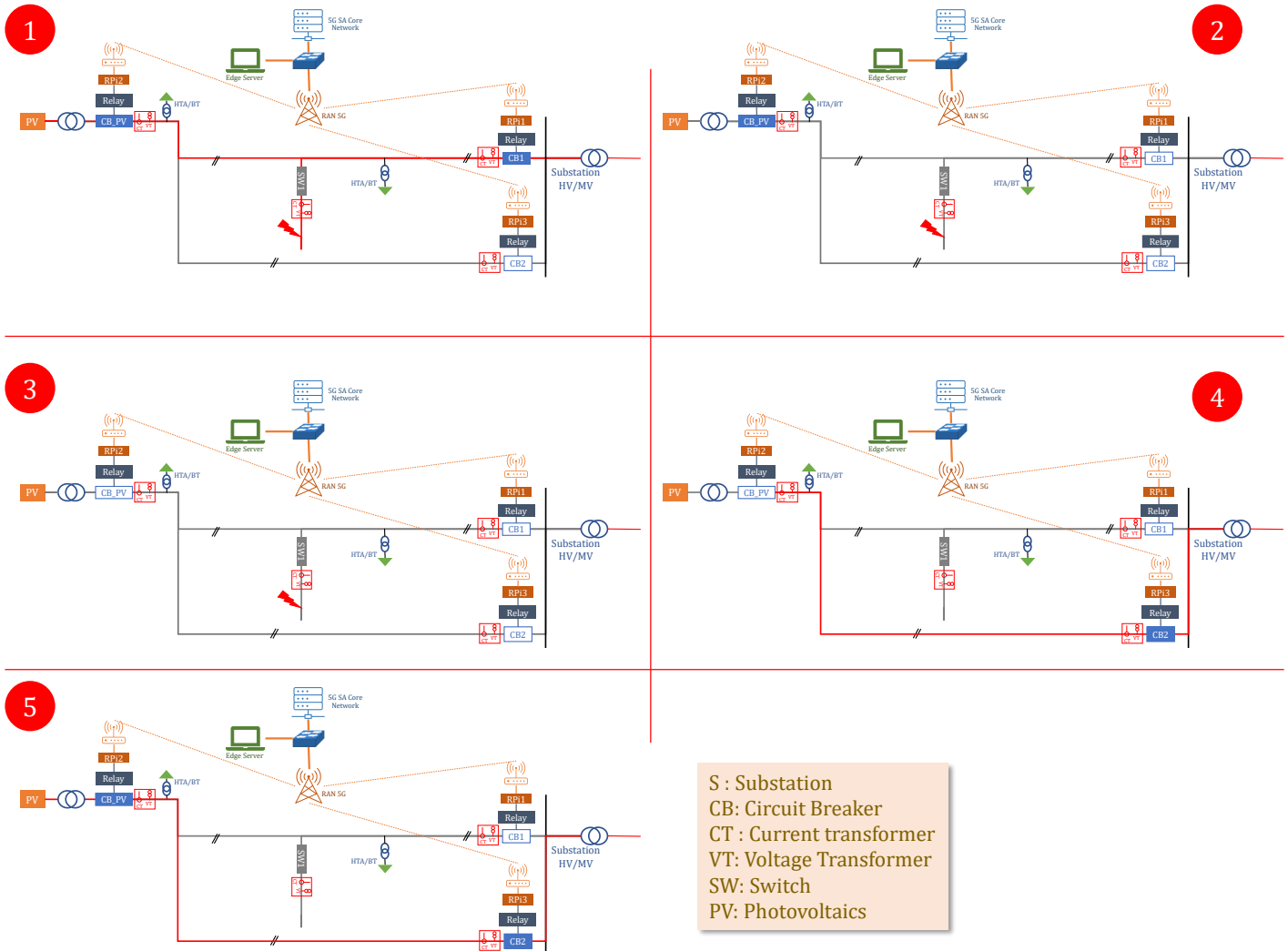


Figure 5.28: Use case process

Figure 5.29 shows the various relay systems used in the experiment. The fault detection assembly allows a 48V output, representing the status of CB1, to supply a 5V voltage to a GPIO pin on RPi1 so as not to damage it. The remote decoupling setup enables RPi2 to activate CB.PV with a 227V signal upon receiving a decoupling command from the controller. The output from the RPi2 pin is a 3.3V signal that activates a switch on the Seed relay shield [156], which has a 30V output. At the second relay, a 30V input activates a switch to produce a 227V output necessary for opening CB.PV. The grid reconfiguration and remote coupling assemblies operate similarly to the remote decoupling assembly, allowing to close CB2 and CB.PV, respectively. The Seed relay shield uses

solid state relays, which have faster switching speeds and longer lifetimes compared to electromechanical relays.

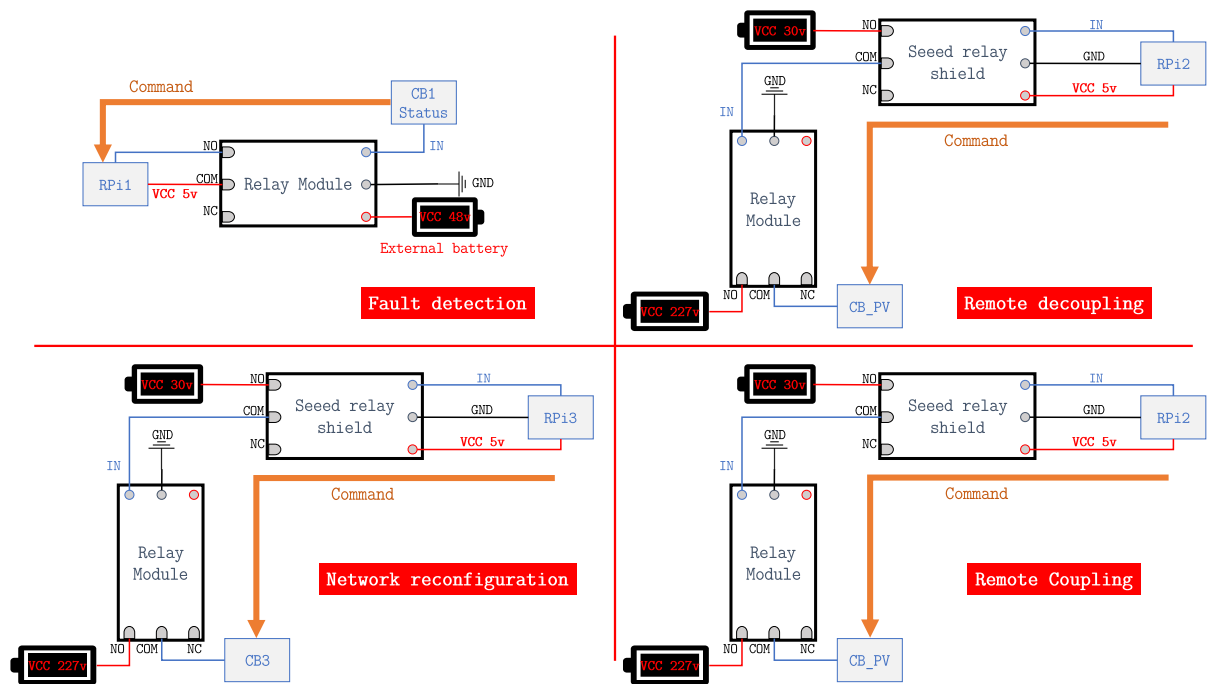


Figure 5.29: How the relay are used during different message exchange

5.4.5 Tests and results

The chart in Figure 5.30 demonstrates the time required for the decoupling command to be transmitted from Raspberry Pi RPi1 (after the detection of circuit breaker CB1 being opened) to RPi2, which subsequently triggered the opening of circuit breaker CB_PV. This process is crucial for maintaining the stability of the power grid, as it helps to prevent involuntary islanding and reduces the risk of the DER's protection systems activating prematurely. The resulting delay is within the maximum transmission time specified by French regulations (i.e. $< 70ms$) [49].

To evaluate the performance of the 5G link between the controller and each Raspberry Pi unit, we conducted communication tests and analyzed the results. Tables 5.1, 5.2, 5.3, and 5.4 show the results of communication tests performed to assess the quality of the connection between the controller and each Raspberry Pi unit. These tests were conducted using Internet Control Message Protocol (ICMP), with packet sizes and transmission intervals varying across the different tests. The results indicate that the connection is stable and reliable in both the upstream and downstream directions for all three Raspberry Pi units. Specifically, 500 packets were transmitted for each combination of packet size and transmission interval, and no packet loss was detected.

In Table 5.1 we evaluate the upstream link from RPi2 towards the controller. The maximum delay is 30.924 ms with a standard deviation of about 10.081.

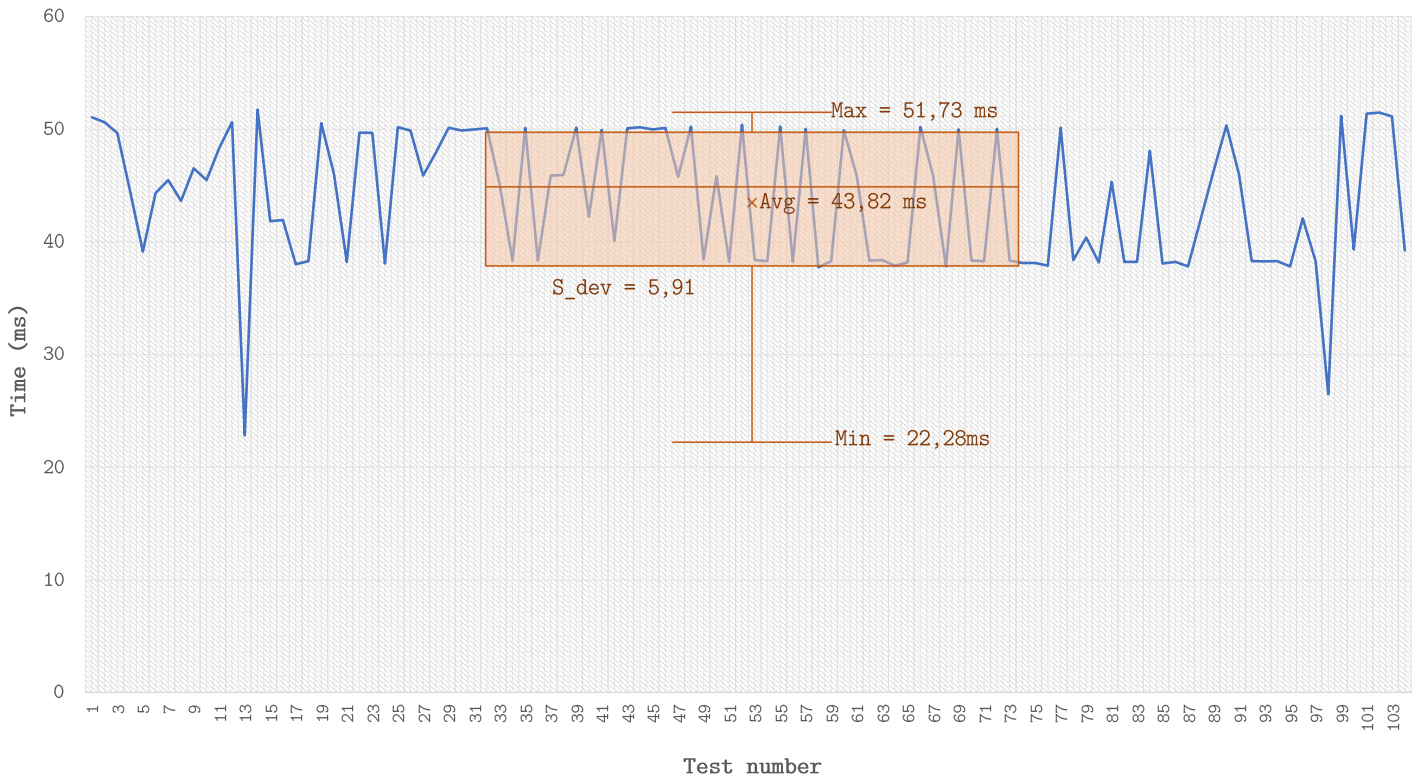


Figure 5.30: Remote decoupling delays

Table 5.1: Up link communication delay of RPi2

TI (ms)	PS (B)	PL	D_min (ms)	D_avg (ms)	D_max (ms)	SD
200	108	0	7,8605	15,5765	30,924	10,081
200	508	0	12,5925	18,8805	24,538	6,263
200	1008	0	15,1395	20,5505	26,703	6,063
500	108	0	7,576	13,041	24,8455	6,465
500	508	0	13,0685	18,601	25,062	6,231
500	1008	0	13,5555	20,374	25,396	5,805
1000	108	0	7,753	13,791	25,8525	7,174
1000	508	0	12,8295	17,933	22,5875	5,7
1000	1008	0	15,532	20,583	25,523	5,738

In Table 5.2 we evaluate the upstream link from RPi3 towards the controller. The maximum delay is 27.56 ms with a standard deviation of about 6.749.

Table 5.2: Up link communication delay of RPi3

TI (ms)	PS (B)	PL	D_min (ms)	D_avg (ms)	D_max (ms)	SD
200	108	0	6,183	16,517	24,938	6,744
200	508	0	10,294	18,7935	25,3535	7,058
200	1008	0	9,156	18,178	25,318	6,709
500	108	0	10,6235	16,9575	25,171	6,554
500	508	0	13,319	18,4065	23,162	5,619
500	1008	0	8,8835	18,2945	23,1495	6,444
1000	108	0	11,296	16,55	22,3715	6,27
1000	508	0	10,414	18,099	27,5665	6,749
1000	1008	0	9,765	18,087	23,321	6,044

In Table 5.3 we evaluate the downstream link from RPi2 towards the controller. The maximum delay is 27.5575 ms with a standard deviation of about 7.881.

Table 5.3: Down link communication delay of RPi2

TI (ms)	PS (B)	PL	D_min (ms)	D_avg (ms)	D_max (ms)	SD
200	108	0	6,9425	16,231	25,6	9,126
200	508	0	11,2405	17,2625	24,734	6,333
200	1008	0	12,4405	18,6595	24,5165	6,398
500	108	0	7,5195	17,2325	25,7965	8,375
500	508	0	11,4405	16,876	25,635	6,16
500	1008	0	12,5335	19,106	24,5405	6,275
1000	108	0	6,8605	17,667	27,5575	7,881
1000	508	0	11,411	16,8535	25,7145	6,236
1000	1008	0	12,956	19,2305	24,5245	6,244

In Table 5.4 we evaluate the downstream link from RPi3 towards the controller. The maximum delay is 24.995 ms with a standard deviation of about 6.493.

Table 5.4: Down link communication delay of RPi3 and RPi1

TI (ms)	PS (B)	PL	D_min (ms)	D_avg (ms)	D_max (ms)	SD
200	108	0	8,2875	14,6605	22,645	6,675
200	508	0	11,285	16,139	21,3465	5,74
200	1008	0	11,2505	16,3385	23,4705	6,269
500	108	0	8,737	16,3415	22,722	6,026
500	508	0	11,7095	16,522	21,3675	5,775
500	1008	0	10,204	16,4695	23,207	5,984
1000	108	0	8,515	16,079	24,995	6,493
1000	508	0	11,2245	16,475	21,424	5,609
1000	1008	0	11,7015	16,5655	23,408	6,011

The results from this experiment demonstrate that the technical requirements for FLISR application are satisfied. However, the configuration can be further improved by implementing a mission-critical oriented setup. This setup should leverage higher frequency bands, enabling the use of a numerology that better suits the demands of critical PAC applications. Additionally, a local breakout-based 5G architecture should be employed to facilitate the deployment of certain PAC applications at the edge computing level while others can be deployed at the cloud computing level. Furthermore, we can leverage the benefits of virtualization and network slicing to create a dedicated network infrastructure for PAC applications, ensuring they have the resources they need to operate smoothly. However, according to various private 5G network providers, network slicing may not be relevant for private networks due to its complexity and the effectiveness of QoS in meeting requirements.

5.5 Conclusion

In this chapter, we first demonstrated the successful implementation of a remote decoupling mechanism, utilizing the full potential of the 5G network to enhance the reliability and security of the distribution grid by protecting against unwanted islanding. Through rigorous testing, we have shown that a 5G-based communication system can meet the necessary delay and reliability requirements for this mechanism, even with the use of a NSA 5G network that did not incorporate network slicing. However, we recognize that there is room for improvement and anticipate that the implementation of a dedicated uRLLC slicing in a standalone 5G network would yield even better performance.

Furthermore, we highlighted the potential of a 5G-based FLISR prototype utilizing HiL architecture, which facilitates the seamless integration of real protection hardware into a simulated environment. By utilizing 5G NSA network, we have achieved high-performance communication, thereby allowing for greater flexibility and improved integration of DERs in MV and LV systems. We have also demonstrated the advantages of virtualization and

orchestration, which have streamlined the application layer management, enhancing the overall system's efficiency.

Finally, we showcased a field experiment on the FLISR application using 5G SA network. We begin by providing an overview of the research center where the experiment was conducted, followed by a detailed description of the used EPS, as well as the components of the 5G network. We utilized the application layer that was developed in the second experiment and modified it to suit the new electrical system's requirements. Adaptations were necessary to effectively control the EPS components that are not compatible with the 5G network. The findings confirmed the conclusions obtained previously, while validating the applicability of our approach on a 5G SA network with a real electrical system.

Chapter 6

Conclusion and Perspectives

Using cutting edge OT/IT technologies in future PAC systems brings various advantages, like minimizing power outage time, reducing blackout risks, increasing system reliability, improving DER integration, and reducing CAPEX and OPEX costs. Throughout this dissertation, we have investigated the use of a multi-level architecture supported by a 5G communication network to design and implement flexible, scalable, reliable, and secure PAC systems.

Incorporation of a cost-effective wireless remote decoupling mechanism into the FLISR process, expands its application to a larger number of connected DERs at MV and LV grids. This approach enhances power system security by minimizing the probability of unintended disconnection of DERs and reducing the risk of unwanted islanding. Thereby, this mechanism can facilitate the seamless integration of DERs into MV and LV networks, providing a more efficient and reliable power supply system.

Experiments on novel PAC systems were conducted in this work, contributing to the pioneering body of knowledge on the potential of 5G technology to significantly advance the future development of highly efficient and sustainable energy management systems. Collecting additional data from the power grid enhances the global system observability, while reducing latency improves the coordination of the protection components and empowers the establishment of a *logical*, rather than a *chronometric*, coordination framework. Additionally, using virtualization to build various PAC functions mitigates the issue of software and hardware vendor lock-in. The distribution of virtual functions between two levels, namely the edge and the cloud, enables the customization of their deployment based on telecommunication constraints and required coverage. Finally, utilizing orchestration to manage the life-cycle of virtual functions consolidates system maintenance, reinforcing horizontal and vertical scalability, as well as flexibility.

6.1 Contributions

Chapter 2 provides a comprehensive introduction to the key components composing the electrical system. The important role of protection systems is highlighted therein, alongside the challenges brought by the integration of DERs. In addition, the chapter explores various central concepts in the 5G ecosystem: *Edge computing* that enables data

processing close to electrical components; *virtualization* for PAC functions implementation avoiding vendor-lock issues; and *orchestration* for efficient life-cycle management of virtual functions. The chapter concludes by reviewing different types of 5G network topologies, providing readers with a well-rounded understanding of the subject matter.

Chapter 3 delves into both academic and industrial works centered around the utilization of OT/IT technology for the development of advanced PAC systems. The different sections explore the specific telecommunication requirements of various PAC applications and demonstrate how the exceptional performance of the 5G network can fulfill them. This chapter puts together a novel architecture based on a 5G infrastructure, which enables the implementation of a communicating PAC system. A FLISR application, designed following the proposed architecture, is presented for validation purposes. The case study provides valuable insights into the practical implications of 5G-enabled PAC systems and accentuates the advantages of the proposed approach over traditional communications.

Chapter 4 addresses the challenge of optimizing the routing of critical PAC traffic on a 5G network, while minimizing energy consumption and ensuring minimal impact on existing traffic. Our optimization framework, which utilized integer linear programming and parameterized objective functions tailored to different types of 5G topologies, namely typical one-hop 5G-RAN and IAB-based wireless backbone 5G-RAN, produced compelling results. Our simulations demonstrated that a MNO can achieve nearly the minimum energy consumption and average delay of PAC critical traffic, while sacrificing almost 6% of the maximum network throughput by using an adequate choice of parameters.

Chapter 5 first showcases two experiments developed using a HiL architecture, which enables interfacing physical PAC equipment with a simulated distribution system. Both experiments use a 5G NSA network with a 5G NR antenna and a 4G EPC core network. In the first experiment, a remote decoupling mechanism is implemented to safeguard the distribution network against unintentional islanding and simplify the integration of DERs. In the second experiment, a FLISR application is deployed to enhance the distribution system response to incidents. Virtual functions in this experiment are built as vendor-agnostic, using open-source tools based on a micro-service architecture. This chapter also presents a third experiment that focuses on the implementation of a FLISR application using a 5G SA network in a real distribution grid. Firstly, we provide an overview of the testing environment, including the used electrical and telecommunication equipment. We then describe the FLISR process and the adaptations we have made to enable the PAC components to use the 5G SA network for data exchange with the controller. In this experiment, a single controller was deployed at the Edge level to manage two feeders connected to the same HV/MV substation. Our findings demonstrate that the 5G network meets the technical requirements for PAC applications, as evidenced by the successful implementation of the FLISR application.

6.2 Perspectives

Our work involved designing and implementing a PAC application to assess the relevance of the 5G ecosystem for future PAC systems. The proposed architecture allows for the deployment of new applications such as state estimators, digital twins, and adaptive protections. As 5G architectures continue to evolve, with the deployment of network slicing, possibilities arise to establish more secure and reliable communication with dynamic telecommunication resource allocation. This development will enable DSOs to confidently use public 5G networks, reducing the cost of deploying new PAC applications based on the 5G communication network. A local breakout architecture (i.e., deploying user plane function (UPF) at the edge level) will enable more efficient deployment of virtual functions between local, edge, and cloud levels by minimizing latency and enhancing security and privacy.

The increasing efficiency of virtualization and orchestration systems is enabling more effective management of virtual PAC functions, a crucial development for the future of the power grid. With these systems, DSOs can set up white box platforms that offer customized functions tailored to the needs of their power grids without the risk of vendor lock-in. Moreover, advanced orchestration will simplify the management of virtual functions throughout their life-cycle, optimizing their deployment, maintenance, and overall performance.

The implementation of advanced and adaptable PAC systems can greatly enhance the secure integration of Distributed Energy Resources (DERs) into power grids. This, in turn, would significantly curtail the reliance on non-renewable energy sources, ultimately leading to a reduction in carbon emissions. By utilizing more versatile and responsive PAC systems, we can achieve a safer and more efficient energy system.

The data we collect will power machine learning algorithms that can accurately predict the behavior and the state of the electrical system, allowing for timely adaptation. As renewables become more prevalent and the electrical network operates in a decentralized manner, such predictions become increasingly crucial. By leveraging the insights gained from our distributed approach, we can optimize the performance of the network, ensure its stability, and improve the reliability of energy supply.

In this context, there are several key future steps for this work. For the short term, we plan to enhance our optimization models developed in Chapter 4 and tackle large-scale scenarios with more input parameters and variables. Using heuristics or reinforcement learning techniques can be efficient to reduce execution times and tackle complex telecommunication networks and distribution power systems. We also plan to adapt the virtual functions of PAC applications to comply with the IEC standards, ensuring their compatibility with existing systems and enabling wider adoption.

On medium term, we envision to develop and implement new PAC applications that leverage the architecture developed in Chapter 3, such as: Demand response, advanced energy management system, and wide-area protection system. We also envision to conduct a field experiment incorporating the new optimization models developed in Chapter 4, in order to validate its effectiveness and feasibility in real-world scenarios.

Finally, on the long term, we will further invest our efforts in the artificial intelligence based approaches for network and smart grid automation. This includes i) real-time state estimator, ii) distribution grid digital twin, and iii) predictive grid maintenance.

Bibliography

- [1] "Dell Technologies Grid Management Platform Common Design Architecture". <https://www.delltechnologies.com/asset/en-gb/solutions/business-solutions/briefs-summaries/dell-technologies-grid-management-common-design-arch-h18551.pdf>.
- [2] "How can smart grids benefit from edge computing?". en-GB. Available at <https://stlpartners.com/articles/edge-computing/smart-grids-edge-computing/>. (Visited on 08/12/2022).
- [3] "Power sector to spend \$5 billion on software by 2025". <https://about.bnef.com/blog/power-sector-to-spend-5-billion-on-software-by-2025/>. Aug. 2020.
- [4] 3GPP. "Study on New Radio Access Technology; Physical Layer Aspects". In: *Technical Report (TR) 38.802, V14. 2.0* (2017).
- [5] Thomas Ackermann, Göran Andersson, and Lennart Söder. "Distributed generation: a definition". In: *Electric power systems research* 57.3 (2001), pp. 195–204.
- [6] Ibrahim Afolabi et al. "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions". In: *IEEE Communications Surveys & Tutorials* 20.3 (2018), pp. 2429–2453.
- [7] Sheraz Alam et al. "Cognitive radio based smart grid communication network". In: *Renewable and Sustainable Energy Reviews* 72 (2017), pp. 535–548.
- [8] A. R. Al-Ali and Raafat Aburukba. "Role of Internet of Things in the Smart Grid Technology". en. In: *Journal of Computer and Communications* 3.5 (May 2015). Number: 5 Publisher: Scientific Research Publishing, pp. 229–233. DOI: [10.4236/jcc.2015.35029](https://doi.org/10.4236/jcc.2015.35029). URL: <http://www.scirp.org/Journal/Paperabs.aspx?paperid=57559> (visited on 08/03/2022).
- [9] Nasser Hasan Ali et al. "Comparisons process-to-bay level peer-to-peer network delay in IEC 61850 substation communication systems". In: *Journal of Electrical Systems and Information Technology* 1.3 (2014), pp. 266–275.
- [10] NGMN Alliance. "NGMN 5G White Paper v1. 0". In: *approved and delivered by the NGMN board, 17th Feb* (2015).

- [11] Ahmed Almasarani, MA Majid, et al. “5G-Wireless sensor networks for smart grid-accelerating technology’s progress and innovation in the kingdom of Saudi arabia”. In: *Procedia Computer Science* 182 (2021), pp. 46–55.
- [12] Amarisoft. *Amari Callbox*. <https://www.amarisoft.com/products/test-measurements/amari-lte-callbox/>.
- [13] Emilio Ancillotti, Raffaele Bruno, and Marco Conti. “The role of communication systems in smart grids: Architectures, technical solutions and research challenges”. In: *Computer Communications* 36 (Nov. 2013), pp. 1665–1697. DOI: [10.1016/j.comcom.2013.09.004](https://doi.org/10.1016/j.comcom.2013.09.004).
- [14] Anuradha M Annaswamy, Institute of Electrical and Electronics Engineers, and IEEE Standards Association. *IEEE vision for smart grid controls: 2030 and beyond*. en. OCLC: 861074253. New York, NY: Institute of Electrical and Electronics Engineers, 2013. ISBN: 978-0-7381-8458-6. URL: <http://ieeexplore.ieee.org/servlet/opac?punumber=6577606> (visited on 12/14/2021).
- [15] *Arrêté du 24 décembre 2007 pris en application du décret n° 2007-1826 du 24 décembre 2007 relatif aux niveaux de qualité et aux prescriptions techniques en matière de qualité des réseaux publics de distribution et de transport d’électricité*. 2015. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000017755016>.
- [16] Imran Ashraf, Federico Boccardi, and Lester Ho. “Power savings in small cell deployments via sleep mode techniques”. In: *2010 IEEE 21st International Symposium on Personal, Indoor and Mobile Radio Communications Workshops*. IEEE. 2010, pp. 307–311.
- [17] Shadi Attarha et al. “Virtualization management concept for flexible and fault-tolerant smart grid service provision”. In: *Energies* 13.9 (2020), p. 2196.
- [18] Leila Bagherzadeh et al. “Integration of cloud computing and IoT (CloudIoT) in smart grids: benefits, challenges, and solutions”. In: *2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE)*. IEEE. 2020, pp. 1–8.
- [19] Anupam Kumar Bairagi et al. “Coexistence mechanism between eMBB and uRLLC in 5G wireless networks”. In: *IEEE Transactions on Communications* 69.3 (2020), pp. 1736–1749.
- [20] Birgitte Bak-Jensen et al. “Protection of distribution systems with distributed energy resources”. In: (2015).
- [21] Armin Balalaie, Abbas Heydarnoori, and Pooyan Jamshidi. “Microservices architecture enables devops: Migration to a cloud-native architecture”. In: *Ieee Software* 33.3 (2016), pp. 42–52.
- [22] Ramazan Bayindir et al. “Smart grid technologies and applications”. In: *Renewable and sustainable energy reviews* 66 (2016), pp. 499–516.

- [23] Bcom. *Dome*. <https://b-com.com/en/accelerate/dome>.
- [24] MO Nait Belaid, Vincent Audebert, and Boris Deneuve. “Designing a 5G Based Smart Distribution Grid Protection System”. In: (2021).
- [25] Kenneth P. Birman, Lakshmi Ganesh, and Robbert van Renesse. “Running Smart Grid Control Software on Cloud Computing Architectures”. In: 2011.
- [26] H. BJÖRKLUN. “Experiences with the deployment of centralized protection systems using virtual protection relays for substations with large power electronic converters”, CIREC 2022 Paris Session”. en. In: (2022).
- [27] Z. Q. Bo et al. “Developments of power system protection and control”. en. In: *Protection and Control of Modern Power Systems* 1.1 (Dec. 2016), p. 7. ISSN: 2367-2617, 2367-0983. DOI: [10.1186/s41601-016-0012-2](https://doi.org/10.1186/s41601-016-0012-2). URL: <http://pcmp.springeropen.com/articles/10.1186/s41601-016-0012-2> (visited on 12/13/2021).
- [28] Math HJ Bollen and Fainan Hassan. *Integration of distributed generation in the power system*. Vol. 80. John Wiley & Sons, 2011.
- [29] Junwei Cao and Mingbo Yang. “Energy internet—towards smart grid 2.0”. In: *2013 Fourth international conference on networking and distributed computing*. IEEE, 2013, pp. 105–110.
- [30] “CAP R&D FEUILLE DE ROUTE R&D 2021/2024, RTE Report, France’s Transmission System Operator”. In: (2021).
- [31] IEC-International Electrotechnical Commission et al. “IEC TR 62357-1: Power systems management and associated information exchange – Part 1: Reference architecture, Edition 2.0”. In: (2016).
- [32] Edge Computing Consortium et al. *Alliance of Industrial Internet. Edge Computing Reference Architecture 2.0*. Tech. rep. Technical Report, 2017.
- [33] Mirsad Cosovic et al. “5G mobile cellular networks: Enabling distributed state estimation for smart grids”. In: *IEEE Communications Magazine* 55.10 (2017), pp. 62–69.
- [34] Edward Coster, Johanna Myrzić, and Wil Kling. “Effect of DG on distribution grid protection”. In: *Distributed generation 2* (2010).
- [35] CRE. *Délibération de la CRE du 21 janvier 2021 portant décision sur le tarif d’utilisation des réseaux publics de distribution d’électricité (TURPE 6 HTA-BT)*. <https://www.cre.fr/Documents/Deliberations/Decision/tarif-d-utilisation-des-reseaux-publics-de-distribution-d-electricite-turpe-6-hta-bt>.
- [36] Erik Dahlman, Stefan Parkvall, and Johan Skold. *4G, LTE-advanced Pro and the Road to 5G*. Academic Press, 2016.

- [37] Kaveh Dehghanpour et al. “A survey on state estimation techniques and challenges in smart distribution systems”. In: *IEEE Transactions on Smart Grid* 10.2 (2018), pp. 2312–2322.
- [38] *Distributed Generation of Electricity and its Environmental Impacts*. June 2022. URL: <https://www.epa.gov/energy/distributed-generation-electricity-and-its-environmental-impacts>.
- [39] Avri Doria et al. *Forwarding and control element separation (ForCES) protocol specification*. Tech. rep. 2010.
- [40] Nils Dorsch et al. “Intertwined: Software-defined communication networks for multi-agent system-based smart grid control”. In: *2016 IEEE international conference on smart grid communications (SmartGridComm)*. IEEE. 2016, pp. 254–259.
- [41] *DPDK*. <https://www.dpdk.org/>. Accessed: 2022-10-1.
- [42] Tomislav Dragičević, Pierluigi Siano, and SR Sahaya Prabakaran. “Future generation 5G wireless networks for smart grid: A comprehensive review”. In: *Energies* 12.11 (2019), p. 2140.
- [43] *E4S alliance: Secondary substation platform - SSP*. <https://www.ariadnagrid.com/blog/e4s-alliance-secondary-substation-platform-ssp/>. Oct. 2020.
- [44] EDF. *Le réseau de transport*. <https://www.edf.fr/groupe-edf/espaces-dedies/l-energie-de-a-a-z/tout-sur-l-energie/l-acheminement-de-l-electricite/le-reseau-de-transport>.
- [45] EU Horizon 2020 EdgeFLEX. *EdgeFlex*. <https://www.edgeflex-h2020.eu/>. Feb. 2022.
- [46] Salah Eddine Elayoubi et al. “5G RAN slicing for verticals: Enablers and challenges”. In: *IEEE Communications Magazine* 57.1 (2019), pp. 28–34.
- [47] Turan Elchuev. “Implementation of a Consolidated Virtual Industrial Control System, Masters Thesis”. en. In: (), p. 88.
- [48] ENEDIS. *Enedis OPEN DATA*. <https://data.enedis.fr/pages/accueil/>.
- [49] ENEDIS. *Enedis-NOI-RES_{13E}*. <https://fr.scribd.com/document/339252360/Enedis-Noi-Res-13e>.
- [50] ENEDIS. *Enedis-PRO-RES_{10E}*. <https://www.enedis.fr/media/2162/download>.
- [51] ENTSO-E. “The Cyber Physical System for the Energy Transition Digitalisation Challenges, Opportunities and Projects from TSOs and ENTSO-E”. In: (2019).
- [52] Environmental and Energy Study Institute (EESI). *Distributed generation*. URL: <https://www.eesi.org/topics/distributed-generation/description>.
- [53] EPRI. “Common Substation Platform: Utility Requirements Assessment - Part 1,2”. In: (2022).

- [54] Ericsson. *Integrated access and backhaul – a new type of wireless backhaul in 5G*. <https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/introducing-integrated-access-and-backhaul>.
- [55] Olaonipekun Oluwafemi Erunkulu et al. “5G mobile communication applications: A survey and comparison of use cases”. In: *IEEE Access* 9 (2021), pp. 97251–97295.
- [56] Ebenezer Esenogho, Karim Djouani, and A Kurien. “Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect.” In: *IEEE Access* (2022).
- [57] M. Faheem et al. “Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges”. In: *Computer Science Review* 30 (2018), pp. 1–30. ISSN: 1574-0137. DOI: <https://doi.org/10.1016/j.cosrev.2018.08.001>. URL: <https://www.sciencedirect.com/science/article/pii/S1574013718300856>.
- [58] ffftelecoms. *Engage 5G & Beyond*. <https://www.ffftelecoms.org/5g/soutien-du-comite-strategique-de-filieres-infrastructures-numeriques-projets-innovants-lies-au-developpement-de-la-5g/>.
- [59] Xenofon Foukas et al. “FlexRAN: A flexible and programmable platform for software-defined radio access networks”. In: *Proceedings of the 12th International on Conference on emerging Networking EXperiments and Technologies*. 2016, pp. 427–441.
- [60] Kinan Ghanem et al. “Bandwidth and security requirements for smart grid”. In: *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. IEEE. 2020, pp. 36–40.
- [61] Kinan Ghanem et al. “Challenges and promises of 5G for smart grid teleprotection applications”. In: *2021 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE. 2021, pp. 1–7.
- [62] Kinan Ghanem et al. “Communication requirements for future secondary substations to enable DSO functions”. In: *CIREN 2020 Berlin Workshop (CIREN 2020)*. Vol. 2020. IET. 2020, pp. 451–454.
- [63] Amitabha Ghosh et al. “5G evolution: A view on 5G cellular technology beyond 3GPP release 15”. In: *IEEE access* 7 (2019), pp. 127639–127651.
- [64] Fabio Giust et al. “MEC deployments in 4G and evolution towards 5G”. In: *ETSI White paper 24.2018* (2018), pp. 1–24.
- [65] MW Goldsmith et al. “Prepared for the Conn SMART”. In: *Marc Goldsmith & Associates LLC* (2011).
- [66] CEN-CENELEC-ETSI Smart Grid Coordination Group. “Smart Grid Coordination Group Smart Grid Reference Architecture”. In: (2012).

- [67] V. Gungor et al. “A Survey on Smart Grid Potential Applications and Communication Requirements”. In: *Industrial Informatics, IEEE Transactions on* 9 (Feb. 2013), pp. 28–42. DOI: [10.1109/TII.2012.2218253](https://doi.org/10.1109/TII.2012.2218253).
- [68] Vehbi C. Gungor et al. “Smart Grid Technologies: Communication Technologies and Standards”. en. In: *IEEE Transactions on Industrial Informatics* 7.4 (Nov. 2011), pp. 529–539. ISSN: 1551-3203, 1941-0050. DOI: [10.1109/TII.2011.2166794](https://doi.org/10.1109/TII.2011.2166794). URL: <http://ieeexplore.ieee.org/document/6011696/> (visited on 08/01/2022).
- [69] Hassan Haes Alhelou et al. “A survey on power system blackout and cascading events: Research motivations and challenges”. In: *Energies* 12.4 (2019), p. 682.
- [70] Bo Han et al. “Network function virtualization: Challenges and opportunities for innovations”. In: *IEEE communications magazine* 53.2 (2015), pp. 90–97.
- [71] Ying He et al. “Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach”. In: *IEEE Communications Magazine* 55.12 (2017), pp. 31–37.
- [72] Aki Hokkanen. “Scalable Software Platform Architecture for the Power Distribution Protection and Analysis”. en. In: (2020).
- [73] Ekram Hossain, Zhu Han, and H Vincent Poor. *Smart grid communications and networking*. Cambridge University Press, 2012.
- [74] Wei Huang. “Learn IEC 61850 configuration in 30 minutes”. en. In: *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*. College Station, TX: IEEE, Mar. 2018, pp. 1–5. ISBN: 978-1-5386-6127-7. DOI: [10.1109/CPRE.2018.8349803](https://doi.org/10.1109/CPRE.2018.8349803). URL: <https://ieeexplore.ieee.org/document/8349803/> (visited on 11/12/2021).
- [75] IEC. Feb. 2014. URL: <https://webstore.iec.ch/publication/6479>.
- [76] IEC. *Communication networks and systems for power utility automation - Part 3: General requirements*. International Electrotechnical Commission, 2013.
- [77] IEC. *Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models*. International Electrotechnical Commission, 2013.
- [78] IEC. *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*. OCLC: 861074253. International Electrotechnical Commission, 2009.
- [79] IEC. *Communication networks and systems for power utility automation – Part 7-1: Basic communication structure – Principles and models*. OCLC: 861074253. International Electrotechnical Commission, 2011.

- [80] IEC. *Communication networks and systems for power utility automation – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*. OCLC: 861074253. International Electrotechnical Commission, 2003.
- [81] IEC. *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*. OCLC: 861074253. International Electrotechnical Commission, 2011.
- [82] IEC. *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*. OCLC: 861074253. International Electrotechnical Commission, 2011.
- [83] IEC. *Communication networks and systems for power utility automation – Part 90-12: Wide area network engineering guidelines*. OCLC: 861074253. International Electrotechnical Commission, 2020.
- [84] *IEEE PSCC Subcommittee Study Group Meeting Minutes: "System Architectures Supporting the Virtualization of Substation Protection and Control Applications"*. <https://site.ieee.org/pes-pscc/files/2022/07/SG-P21-Meeting-Minutes-2022-01-10.pdf>. 2022.
- [85] "IEEE PSRC "Advancements in Centralized Protection and Control Within a Substation"". en. In: *IEEE Transactions on Power Delivery* 31.4 (Aug. 2016), pp. 1945–1952. ISSN: 0885-8977, 1937-4208. DOI: [10.1109/TPWRD.2016.2528958](https://doi.org/10.1109/TPWRD.2016.2528958). URL: <https://ieeexplore.ieee.org/document/7414482/> (visited on 12/02/2021).
- [86] *Investigation into 9 August 2019 power outage*. Ofgem. <https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage>. (Visited on 07/25/2022).
- [87] Rolf Isermann. *Fault-diagnosis applications: model-based condition monitoring: actuators, drives, machinery, plants, sensors, and fault-tolerant systems*. Springer Science & Business Media, 2011.
- [88] ISO. *International Technology for Learning, Education, and Training*. International Electrotechnical Commission Standard, Geneva, 2003.
- [89] Hussein Jumma Jabir et al. "Impacts of demand-side management on electrical power systems: A review". In: *Energies* 11.5 (2018), p. 1050.
- [90] David Jaramillo, Duy V Nguyen, and Robert Smart. "Leveraging microservices architecture by using Docker technology". In: *SoutheastCon 2016*. IEEE. 2016, pp. 1–5.
- [91] Akhtar Hussain Javed et al. "Review of Operational Challenges and Solutions for DER Integration with Distribution Networks". In: *2021 56th International Universities Power Engineering Conference (UPEC)*. IEEE. 2021, pp. 1–6.

- [92] YR Kaffle et al. “Towards an internet of energy”. In: *2016 IEEE International Conference on Power System Technology (POWERCON)*. IEEE. 2016, pp. 1–6.
- [93] Amal Kammoun et al. “End-to-end efficient heuristic algorithm for 5G network slicing”. In: *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. IEEE. 2018, pp. 386–392.
- [94] D Khajuria P; Samara-Rubio. “Power of Infrastructure Modernization”. en. In: *Intel Corporation* (Apr. 2021).
- [95] Rafiullah Khan et al. “Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid”. In: *Ieee Access* 5 (2017), pp. 11626–11644.
- [96] Young-Jin Kim et al. “Virtualized and self-configurable utility communications enabled by software-defined networks”. In: *2014 IEEE international conference on smart grid communications (SmartGridComm)*. IEEE. 2014, pp. 416–421.
- [97] Peng-Yong Kong. “Wireless neighborhood area networks with QoS support for demand response in smart grid”. In: *IEEE transactions on smart grid* 7.4 (2015), pp. 1913–1923.
- [98] P. KREUTZER and J. OLIVEIRA. “”Virtualization as an enabler for digital substation deployment”, CIREC 2022 Paris Session”. en. In: (2022).
- [99] Carsten Kruger et al. “Real-time Test Platform for Enabling Grid Service Virtualisation in Cyber Physical Energy System”. en. In: *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. Vienna, Austria: IEEE, Sept. 2020, pp. 109–116. ISBN: 978-1-72818-956-7. DOI: [10.1109/ETFA46521.2020.9211939](https://doi.org/10.1109/ETFA46521.2020.9211939). URL: <https://ieeexplore.ieee.org/document/9211939/> (visited on 11/18/2021).
- [100] *Kubernetes*. <https://kubernetes.io/>.
- [101] Murat Kuzlu, Manisa Pipattanasomporn, and Saifur Rahman. “Communication network requirements for major smart grid applications in HAN, NAN and WAN”. In: *Computer Networks* 67 (2014), pp. 74–88. ISSN: 1389-1286. DOI: <https://doi.org/10.1016/j.comnet.2014.03.029>. URL: <https://www.sciencedirect.com/science/article/pii/S1389128614001431>.
- [102] Techniques de l’ingénieur. *Réseaux de transport et de répartition - Systèmes et plans de protection, D4804 V1, 2010*. <https://www.techniques-ingenieur.fr/base-documentaire/energies-th4/reseaux-electriques-de-transport-et-de-repartition-42263210/reseaux-de-transport-et-de-repartition-d4804/>.
- [103] MOSAIC LAB. *MOSAIC LAB*. <http://www.mosaic-lab.org/>.

- [104] Adrian Lara, Anisha Kolasani, and Byrav Ramamurthy. “Network innovation using openflow: A survey”. In: *IEEE communications surveys & tutorials* 16.1 (2013), pp. 493–512.
- [105] Helen C Leligou et al. “Smart grid: a demanding use case for 5G technologies”. In: *2018 IEEE international conference on pervasive computing and communications workshops (percom workshops)*. IEEE. 2018, pp. 215–220.
- [106] *LF Energy Seapath*. <https://www.lfenergy.org/projects/seapath/>. Accessed: 2022-10-1.
- [107] Ruiqi Li et al. “A systematic evaluation of network protection responses in future converter-dominated power systems”. In: (2016).
- [108] Yingyi Liang and Roy H Campbell. *Understanding and simulating the IEC 61850 standard*. Tech. rep. 2008.
- [109] *Linux KVM*. https://www.linux-kvm.org/page/Main_Page.
- [110] Xiang Liu. “Evolution of fiber-optic transmission and networking toward the 5G era”. In: *Iscience* 22 (2019), pp. 489–506.
- [111] Chun-Hao Lo and Nirwan Ansari. “The Progressive Smart Grid System from Both Power and Communications Aspects”. In: *Communications Surveys & Tutorials, IEEE* 14 (Jan. 2012), pp. 1–23. DOI: [10.1109/SURV.2011.072811.00089](https://doi.org/10.1109/SURV.2011.072811.00089).
- [112] Thiago Berticelli Lo et al. “Cloud IEC 61850: Architecture and Integration of Electrical Automation Systems”. en. In: *2014 Brazilian Symposium on Computing Systems Engineering*. Manaus: IEEE, Nov. 2014, pp. 13–18. ISBN: 978-1-4799-8559-3. DOI: [10.1109/SBESC.2014.30](https://doi.org/10.1109/SBESC.2014.30). URL: <https://ieeexplore.ieee.org/document/7091159/> (visited on 11/04/2021).
- [113] G. López et al. “Paving the road toward Smart Grids through large-scale advanced metering infrastructures”. In: *Electric Power Systems Research* 120 (2015). Smart Grids: World’s Actual Implementations, pp. 194–205. ISSN: 0378-7796. DOI: <https://doi.org/10.1016/j.epsr.2014.05.006>. URL: <https://www.sciencedirect.com/science/article/pii/S0378779614001862>.
- [114] Amadou LOUH et al. “Seamless extension of fibre optical IP/MPLS network with 5G technology Releases allowing Business service segregation, Precision time synchronization and Critical teleprotection services in Utility distribution networks”. In: CIGRE. 2022.
- [115] Haoyang Lu et al. “A microgrid monitoring system over mobile platforms”. In: *IEEE Transactions on Smart Grid* 8.2 (2016), pp. 749–758.
- [116] Pavel Mach and Zdenek Becvar. “Mobile edge computing: A survey on architecture and computation offloading”. In: *IEEE communications surveys & tutorials* 19.3 (2017), pp. 1628–1656.

- [117] Ralph E Mackiewicz. “Overview of IEC 61850 and Benefits”. In: *2006 IEEE Power Engineering Society General Meeting*. IEEE. 2006, 8–pp.
- [118] S Moitaba Matinkhah and Wasswa Shafik. “Smart grid empowered by 5G technology”. In: *2019 Smart Grid Conference (SGC)*. IEEE. 2019, pp. 1–6.
- [119] Kashif Mehmood et al. “Intent-based network management and orchestration for smart distribution grids”. In: *2021 28th International Conference on Telecommunications (ICT)*. IEEE. 2021, pp. 1–6.
- [120] Sachula Meng et al. “Integration application of 5g and smart grid”. In: *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE. 2019, pp. 1–7.
- [121] Rashid Mijumbi et al. “Network Function Virtualization: State-of-the-Art and Research Challenges”. In: *IEEE Communications Surveys & Tutorials* 18.1 (2016), pp. 236–262. DOI: [10.1109/COMST.2015.2477041](https://doi.org/10.1109/COMST.2015.2477041).
- [122] Rashid Mijumbi et al. “Network function virtualization: State-of-the-art and research challenges”. In: *IEEE Communications surveys & tutorials* 18.1 (2015), pp. 236–262.
- [123] Njabulo Mlilo, Jason Brown, and Tony Ahfock. “Impact of intermittent renewable energy generation penetration on the power system networks—A review”. In: *Technology and Economics of Smart Grids and Sustainable Energy* 6.1 (2021), p. 25.
- [124] Hussein T Mouftah et al. “Smart grid communications: Opportunities and challenges”. In: *Handbook of Green Information and Communication Systems* 2013 (2013), pp. 631–663.
- [125] MO NAIT Belaid et al. “Defining a Wide Area Protection System Using 5G Communication Technology”. In: *Proc. of GCC Conference*. 2021.
- [126] *Network Slicing*. 2019. URL: <https://opennetworking.org/wp-content/uploads/2019/01/Network-Slicing-and-Private-LTE.pdf>.
- [127] Tobias Neumann and István Erlich. “Short circuit current contribution of a photovoltaic power plant”. In: *IFAC Proceedings Volumes* 45.21 (2012), pp. 343–348.
- [128] *NRG5*. <https://5g-ppp.eu/nrg-5/>. Accessed: 2023-1-5.
- [129] OCP. *Open Compute Project (OCP)*. <https://www.opencompute.org/>.
- [130] OPAL-RT. *OP5650*. <https://wiki.opal-rt.com/display/HDGD/OP5650>.
- [131] Oracle. *Brief History of Virtualization*. https://docs.oracle.com/cd/E26996_01/E18549/html/VMUSG1010.html.
- [132] Y Pan et al. “Impact of inverter interfaced distributed generation on overcurrent protection in distribution systems”. In: *2011 IEEE Power Engineering and Automation Conference*. Vol. 2. IEEE. 2011, pp. 371–376.

- [133] Marco Pau et al. “A Service Oriented Architecture for the Digitalization and Automation of Distribution Grids”. en. In: 10 (2022), p. 14.
- [134] Diogenes Javier Perez et al. “How Real (Time) Are Virtual PLCs?”. en. In: (), p. 8.
- [135] Arun G. PHADKE et al. “Improving the performance of power system protection using wide area monitoring systems”. In: *Journal of Modern Power Systems and Clean Energy* 4 (July 1, 2016). ISSN: 2196-5420. DOI: [10.1007/s40565-016-0211-x](https://doi.org/10.1007/s40565-016-0211-x). URL: <https://doi.org/10.1007/s40565-016-0211-x> (visited on 07/25/2022).
- [136] Alexandre PINHEL et al. “Reflections on the Potential use of 5G Technologies in the Electric Sector”. In: CIGRE. 2022.
- [137] *Plan de protection des réseaux HTA - B.61-21 - Principes*. 1994.
- [138] *Platoon EU Project*. <https://platoon-project.eu/>.
- [139] Michele Polese et al. “Integrated access and backhaul in 5G mmWave networks: Potential and challenges”. In: *IEEE Communications Magazine* 58.3 (2020), pp. 62–68.
- [140] Petar Popovski et al. “5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view”. In: *Ieee Access* 6 (2018), pp. 55765–55779.
- [141] Daniele Porcu et al. “Demonstration of 5G solutions for smart energy grids of the future: a perspective of the Smart5Grid project”. In: *Energies* 15.3 (2022), p. 839.
- [142] *QUALITÉ DE L'ÉLECTRICITÉ*. 2019. URL: https://assets.rte-france.com/prod/public/2020-09/RTE_Rapport%20qualite%20electricite%202019_0.pdf.
- [143] Redhat. *What is virtualization?* <https://opensource.com/resources/virtualization>.
- [144] Mubashir Husain Rehmani et al. “Software defined networks-based smart grid communication: A comprehensive survey”. In: *IEEE Communications Surveys & Tutorials* 21.3 (2019), pp. 2637–2670.
- [145] *Requirements for generating plants to be connected in parallel with distribution networks Connection to a LV distribution network. Generating plants up to and including Type B =* <https://www.en-standard.eu/bs-en-50549-1-2019-requirements-for-generating-plants-to-be-connected-in-parallel-with-distribution-networks-connection-to-a-lv-distribution-network-generating-plants-up-to-and-including-type-b/>, author=EUROPEAN STANDARDS.
- [146] *Reseaux : comprendre le SDN et le NFV*. URL: <https://www.solutions-numeriques.com/reseaux-comprendre-le-sdn-et-le-nfv/>.
- [147] I El-Samahy and Ehab El-Saadany. “The effect of DG on power quality in a deregulated environment”. In: *IEEE Power Engineering Society General Meeting, 2005*. IEEE. 2005, pp. 2969–2976.

- [148] Dean Samara-Rubio, Graham McKenzie, and Prithpal Khajuria. “White Paper: ”A Paradigm Shift in Power System Protection””. en. In: *Intel Corporation, Kalkitech* (2022).
- [149] Farzad Samie, Lars Bauer, and Jörg Henkel. “Edge computing for smart grid: An overview on architectures and solutions”. In: *IoT for smart grids* (2019), pp. 21–42.
- [150] Nikolaos Sapountzoglou. “Fault detection and isolation for low voltage distribution grids with distributed generation”. PhD thesis. Université Grenoble Alpes, 2019.
- [151] Robert Schmidt, Mikel Irazabal, and Navid Nikaein. “FlexRIC: an SDK for next-generation SD-RANs”. In: *Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies*. 2021, pp. 411–425.
- [152] Artem Schumilin et al. “A Consistent View of the Smart Grid: Bridging the Gap between IEC CIM and IEC 61850”. In: *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. IEEE. 2018, pp. 321–325.
- [153] K. Schwarz and I. Eichbaeumle. “IEC 61850, IEC 61400-25, and IEC 61970: Information models and information exchange for electric power systems”. In: (2004).
- [154] Adolf Schweer and J Tzschope. “Impact of increasing contribution of dispersed generation on the power system; Einfluss zunehmender dezentraler Stromerzeugung auf das elektrische Energieversorgungssystem”. In: *Elektrizitaetswirtschaft* 98 (1999).
- [155] *SDN architecture*. 2014. URL: https://opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf.
- [156] Seed. *Seed RPi Shield Relay*. https://raw.githubusercontent.com/SeedDocument/Relay-Shield_V2.0/master/res/Relayshieldsch.pdf.
- [157] Amina Seferagić et al. “Survey on wireless technology trade-offs for the industrial internet of things”. In: *Sensors* 20.2 (2020), p. 488.
- [158] M Series. “IMT Vision–Framework and overall objectives of the future development of IMT for 2020 and beyond”. In: *Recommendation ITU 2083* (2015).
- [159] Weisong Shi et al. “Edge computing: Vision and challenges”. In: *IEEE internet of things journal* 3.5 (2016), pp. 637–646.
- [160] Joyce Meireles SIQUEIRA. “5G and the Power System Applications Requirements”. In: CIGRE. 2022.
- [161] Renato A Spalding et al. “Fault Location, Isolation and service restoration (FLISR) functionalities tests in a Smart Grids laboratory for evaluation of the quality of service”. In: *2016 17th International Conference on Harmonics and Quality of Power (ICHQP)*. IEEE. 2016, pp. 879–884.

- [162] Thomas Strasser et al. “A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems”. en. In: *IEEE Transactions on Industrial Electronics* 62.4 (Apr. 2015), pp. 2424–2438. ISSN: 0278-0046, 1557-9948. DOI: [10.1109/TIE.2014.2361486](https://doi.org/10.1109/TIE.2014.2361486). URL: <https://ieeexplore.ieee.org/document/6915899> (visited on 02/11/2022).
- [163] Miaomiao Sun, Hui Wang, and Xiaorong Zhu. “Fault characteristics of photovoltaic power station and its influence on relay protection of transmission line”. In: *5th IET International Conference on Renewable Power Generation (RPG) 2016*. IET. 2016, pp. 1–5.
- [164] Jonathan Sykes et al. “Sharing direct fiber channels between protection and enterprise applications using wavelength division multiplexing”. In: *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*. IEEE. 2018, pp. 1–8.
- [165] Tarik Taleb et al. “On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration”. In: *IEEE Communications Surveys & Tutorials* 19.3 (2017), pp. 1657–1681.
- [166] Vishnuvardhan Telukunta et al. “Protection challenges under bulk penetration of renewable energy resources in power systems: A review”. In: *CSEE journal of power and energy systems* 3.4 (2017), pp. 365–379.
- [167] Lilia Tightiz and Hyosik Yang. “A Comprehensive Review on IoT Protocols’ Features in Smart Grid Communication”. In: *Energies* 13.11 (2020). ISSN: 1996-1073. DOI: [10.3390/en13112762](https://doi.org/10.3390/en13112762). URL: <https://www.mdpi.com/1996-1073/13/11/2762>.
- [168] *TR 23.799: Study on Architecture for Next Generation System*. 2016. URL: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3008>.
- [169] Hugo Tullberg et al. “The METIS 5G system concept: Meeting the 5G requirements”. In: *IEEE Communications magazine* 54.12 (2016), pp. 132–139.
- [170] Roberto Turconi, Alessio Boldrin, and Thomas Astrup. “Life cycle assessment (LCA) of electricity generation technologies: Overview, comparability and limitations”. In: *Renewable and sustainable energy reviews* 28 (2013), pp. 555–565.
- [171] Hanif Ullah et al. “5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases”. In: *IEEE Access* 7 (2019), pp. 37251–37268.
- [172] Jani Valtari and Sushil Joshi. “White Paper: ‘Centralized Protection and Control’, ABB”. en. In: (2019).
- [173] Lizhi Wang et al. “Software-Defined Microgrid Control: The Genesis of Decoupled Cyber-Physical Microgrids”. en. In: *IEEE Open Access Journal of Power and Energy* 7 (2020), pp. 173–182. ISSN: 2687-7910. DOI: [10.1109/OAJPE.2020.2997665](https://doi.org/10.1109/OAJPE.2020.2997665). URL: <https://ieeexplore.ieee.org/document/9099877/> (visited on 07/08/2022).

- [174] Wenye Wang, Yi Xu, and Mohit Khanna. “A survey on the communication architectures in smart grid”. en. In: *Computer Networks* 55.15 (Oct. 2011), pp. 3604–3629. ISSN: 1389-1286. DOI: [10.1016/j.comnet.2011.07.010](https://doi.org/10.1016/j.comnet.2011.07.010). URL: <https://www.sciencedirect.com/science/article/pii/S138912861100260X> (visited on 08/01/2022).
- [175] Welotech. “Substation Modernization: Current to Future Online Webinar”. In: (2022).
- [176] *What Are Geomagnetic Storms?* URL: <https://www.sciencealert.com/geomagnetic-storms>.
- [177] CAO Y et al. “5G wireless communications for smart grid: a PACS case with network slice”. In: CIGRE. 2020.
- [178] *Y.3011: Framework of network virtualization for future networks*. 2012. URL: <https://www.itu.int/rec/T-REC-Y.3011-201201-I>.
- [179] Y.Q. Yan et al. “A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges”. In: *Communications Surveys & Tutorials, IEEE* 15 (Jan. 2013), pp. 5–20. DOI: [10.1109/SURV.2012.021312.00034](https://doi.org/10.1109/SURV.2012.021312.00034).
- [180] Hui Yang, Fushuan Wen, and Gerard Ledwich. “Optimal coordination of overcurrent relays in distribution systems with distributed generators based on differential evolution algorithm”. In: *International transactions on electrical energy systems* 23.1 (2013), pp. 1–12.
- [181] Shan Yang and Xiangqian Tong. “Integrated power flow and short circuit calculation method for distribution network with inverter based distributed generation”. In: *Mathematical Problems in Engineering* 2016 (2016).
- [182] Rong Yu et al. “Cognitive radio based hierarchical communications infrastructure for smart grid”. In: *IEEE network* 25.5 (2011), pp. 6–14.
- [183] Jianchao Zhang et al. “Opportunities for software-defined networking in smart grid”. In: *2013 9th International Conference on Information, Communications & Signal Processing*. IEEE. 2013, pp. 1–5.
- [184] Qi Zhang et al. “A Comparative Study of Containers and Virtual Machines in Big Data Environment”. In: *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. 2018, pp. 178–185. DOI: [10.1109/CLOUD.2018.00030](https://doi.org/10.1109/CLOUD.2018.00030).
- [185] Shunliang Zhang. “An overview of network slicing for 5G”. In: *IEEE Wireless Communications* 26.3 (2019), pp. 111–117.
- [186] Aboelsood Zidan et al. “Fault detection, isolation, and service restoration in distribution systems: State-of-the-art and future trends”. In: *IEEE Transactions on Smart Grid* 8.5 (2016), pp. 2170–2185.

Chapter 7

Appendix

7.1 IEC 61850 standard

IEC 61850 is an international, well-established standard for specifying communication networks and systems in power utility automation. Its main goals are to ensure interoperability between multiple vendor IEDs and the data exchange between physically separated subsystems performing different functionality [79].

IEC 61850 consists of three main elements:

- **Data Model:** Partitioning each IED into modular independent components and sub-layers which allows to perform individual replacements without affecting the entire system [74]. The standard defines the common ‘Classes’ that will be used to specify different semantic data objects allowing the modeling and description of a large amount of electrical network information (including electrical protections, electro-technical equipment, power quality equipment, DER, etc) in a homogeneous way (using Logical Devices (LD), Logical Nodes (LN), Data Objects (DO), Data Attributes (DA)).
- **Communication:** Describing Abstract Communication Service Interfaces (ACSI) (IEC 61850-7-2 [80]), based on the functional requirements in IEC 61850-5 [77], facilitates the information exchange within the control system (to perform a certain function), between IEDs, as well as towards external remote information systems. The standard then specifies the procedures to map the abstract stack to the real communication protocol stack, including Sample Value (SV), Manufacturing Messaging Specification (MMS) and Generic Object-Oriented Substation Event (GOOSE) (IEC 61850-8-1 [81]/ IEC 61850-9-2 [82]).
- **Engineering and Testing:** The standard supports an increased maintainability and operational gains by providing standardized engineering tools for specifying, configuring, and testing control systems (IEC 61850-6 [78]). The files exchanged with the vendors are in standardized digital eXtensible markup language (XML) format (covering specifications, models, and functionalities supported by the equipment and the substation configuration). Costs and time for specific developments are reduced or even avoided with a better interpretation of the standard.

The main protocols of the IEC 61850 standard are: MMS (Manufacturing Message Specification), GOOSE (Generic Object-Oriented Substation Event) and the SMV (Sampled Measured Values).

- The MMS protocol (part 8: IEC 61850-8-1) is used for monitoring.
- The GOOSE protocol (parts 7: IEC 61850-7-2, and 8: IEC 61850-8-1) is used to exchange information between protection relays, as well as for tripping and blocking circuits. It is also used for status updates and sending commands.
- The SMV protocol (part 9: IEC 61850-9-2) transports digitized instantaneous values of the quantities of a power supply system (mainly voltages and currents).

7.2 GOOSE protocol

The GOOSE protocol is a feature of the IEC 61850 standard which is based on the User Datagram Protocol (UDP) as shown in Figure 7.1. Unlike TCP (Transmission Control Protocol), the flow is unidirectional, data transmission is done without notifying the receiver, who does not need to send an acknowledgment.

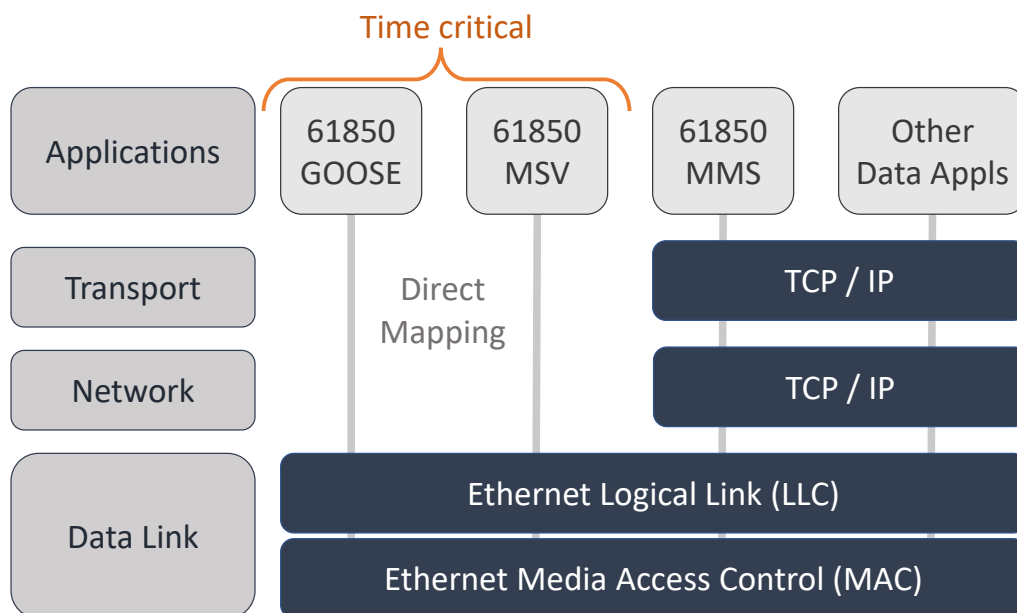


Figure 7.1: IEC 61850 communication profiles [9, 95]

GOOSE uses multicast (one to many) communications based directly on Ethernet allowing IEDs to communicate with each other. The GOOSE protocol is based on Publisher/Subscriber mode instead of the traditional Server/Client mode, ie the message is sent by an IED to all potential receivers. The transmission frequencies vary according to the mode of the system: normal mode or during a change of situation.

7.3 Common Information Model (CIM)

In the field of transport and distribution grid, the CIM model aims to allow software to exchange information on an electrical network. It defines a common vocabulary and description of the energy sector. The information model describes the basic components used for energy supply.

An information model is composed of several layers and has 2 distinct modeling levels:

- The real device is divided into logical devices,
- Logical devices are divided into logical nodes, data objects and attributes.

The complete structure of the information model is shown in Figure 7.2. The different layers of the information model are as follows [117, 108]:

Physical Device (IED): The physical device, also called IED (Intelligent Electronic Device), is the monitoring or control device, which is equipped with a microcontroller and a graphical interface, and which connects to the network. In the context of the IEC 61850 standard, this term designates a device implementing one of the communication protocols of the standard.

Logical Device (LD): Each IED can contain one or more logical devices. They constitute the first level of functions' repartition supported by the IED.

Logical Node (LN): it's smallest part of a function that can exchange data. The IEC 61850 standard assigns a logical node to each function in substation equipment. Logical nodes are virtual representations of devices. They are grouped based on functionality.

Data Object (DO): A logical node contains data objects that represent specific information, for example a state or a measurement. The data objects defined for a specific logical node are grouped into categories by "Functional Constraints" (FC):

- Description: common information on the logical node;
- Status: process or function status,
- Measures: measured or calculated analog data;
- Control: data that is changed by commands;
- Settings: function parameters of a logical node.

Data Attribute (DA): Each data object contains a set of elements called data attributes

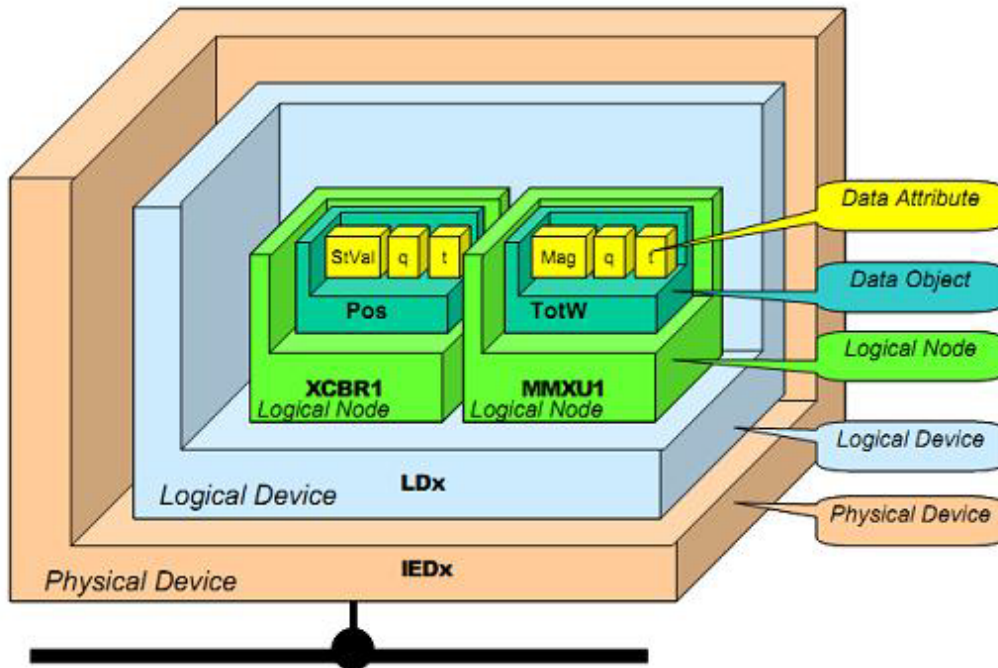


Figure 7.2: Object oriented model of IEC 61850 standard [152, 31]

7.4 Electrical Equipment Used in our Experiments

7.4.1 ABB protection relay REF 615 N

The REF615 is a relay designed to provide protection, control, measurement, and supervision of overhead lines and power cables in public and industrial power distribution systems. It is suitable for a wide range of distribution network topologies, including radial, ring, and mesh configurations, with or without distributed power generation. The REF615 is available in several standard configurations, referenced from A to N, with the N configuration offering the highest level of functionality. Notable features of the REF615 include precise fault detection and location capabilities, support for advanced protection algorithms, and extensive communication capabilities with SCADA (Supervisory Control and Data Acquisition) systems. Additionally, the REF615 offers a range of protection and metering functions based on voltage, frequency, and power, with both directional and non-directional overcurrent and ground fault protection. It also includes an extensive range of ground fault protection functions, with a unique multi-frequency admittance-based protection for better sensitivity and selectivity. Advanced and fast short circuit and ground fault location is available as an optional feature. The REF615 supports IEC 61850 editions 1 and 2, and integrates network protocols that provide seamless failover against failure, namely High-Availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP).

7.4.2 ABB voltage protection relay REU 615 A

The REU615 is a versatile relay designed for voltage and frequency-based protection and monitoring in utility and industrial power distribution systems, including networks with

distributed power generation. It is an ideal solution for automatic and manual voltage regulation, as well as for busbar undervoltage and overvoltage monitoring, load shedding, and load restoration. The REU615 comes in two standard configurations, A and B, with customizable options available to suit specific application needs. Notable features of the REU615 include a removable plug-in unit for easy installation and testing, and a large graphical display that shows customizable Single Line Diagrams (SLDs), which can be accessed locally or through an easy-to-use web browser-based HMI. The REU615 is designed to provide reliable and efficient voltage protection and monitoring, with standard configurations that allow for quick and easy installation, while also providing customization options for more specialized applications.

7.4.3 dSpace MicroLabBox

The dSpace MicroLabBox is an all-in-one development system that offers high performance and versatility while keeping system costs low. It simplifies the implementation of control, test, and measurement applications, making it easier to develop new control concepts. With more than 100 I/O channels of various types, the MicroLabBox is suitable for use in mechatronics research and development, including but not limited to applications in smart grids, robotics, medical engineering, electric motor controls, renewable energies, automotive, and aerospace engineering.

This compact system boasts high computing power and very low I/O latencies, ensuring excellent real-time performance. The MicroLabBox's programmable FPGA (Field-programmable gate array) provides flexibility, enabling the execution of extremely fast control loops needed for electric motor control or active vibration and noise control.

The MicroLabBox comes with a complete dSPACE software package, including the Real-Time Interface (RTI) library for Simulink® to integrate I/O into the model, and the ControlDesk software, which allows access to the application while it's running in real-time using graphical tools.

7.4.4 ControlDesk

ControlDesk is dSpace's versatile and user-friendly instrumentation and experimentation software, specially designed for the development of simulators like MicroLabBox. It enables real-time visualization and measurement of various variables and facilitates the modification of parameters of the Simulink-designed model. Additionally, it allows easy configuration of the simulator's inputs and outputs, providing users with maximum control and flexibility. With its intuitive interface, ControlDesk makes it easy to analyze and optimize simulations, making it an indispensable tool for simulation-based testing and research.

7.4.5 Schneider Flair 23DM Fault passage indicator

The Flair 23DM is a fault passage indicator that features a dual power supply and a voltage presence/absence relay. Additionally, it includes advanced functions like an am-

meter/voltmeter, and is rated for operation with an external 24-48 VDC voltage source. Communication is facilitated through an RS485 serial link using the Modbus protocol, providing access to states and measurements as well as remote parameter-setting capabilities.

7.4.6 Opal-RT real time simulator

Real-time simulation utilizes computer modeling to simulate the behavior of physical systems in real-time. We have integrated our Simulink model of a power distribution network into a real-time simulator to achieve a higher level of realism. By using the input and output ports of the simulator, we are able to send and receive relevant signals, and perform control operations on the power grid in real-time. Finally, we observe and analyze the results obtained from the simulation.

OPAL-RT TECHNOLOGIES is a well-known company in the realm of real-time simulations. EDF has recently procured a hardware platform model, OP5650, along with a license for the control software platform, RT-LAB, and necessary accessories from the company to facilitate its research projects. The OP5650 platform consists of two primary sections: an upper section containing the analog and digital signal input/output modules, and a lower section containing the multi-core processor computer and FPGA.

The real-time simulator is designed to be highly customizable, allowing for specific input/output needs to be met. It boasts a modular design, with a chassis that can hold up to eight signal conditioning and analog/digital conversion modules. Each module provides 16 analog channels and 32 digital channels, enabling the management of up to 128 fast analog signals and 256 digital signals. For a comprehensive overview of the simulator's features, refer to the official documentation provided by Opal-RT[130].

7.4.7 RT-Lab control platform

RT-Lab is a software platform developed by OPAL-RT TECHNOLOGIES that allows for effective management and manipulation of real-time simulators. It provides a range of capabilities, including the ability to implement, edit, compile, run and analyze simulation models 7.3. RT-Lab is seamlessly integrated with MATLAB/Simulink, and once the Simulink models are loaded, any modifications must be made directly through the RT-Lab user interface. This integration streamlines the simulation process and facilitates the implementation of complex models, making it easier for users to focus on the simulation results rather than the underlying implementation details.

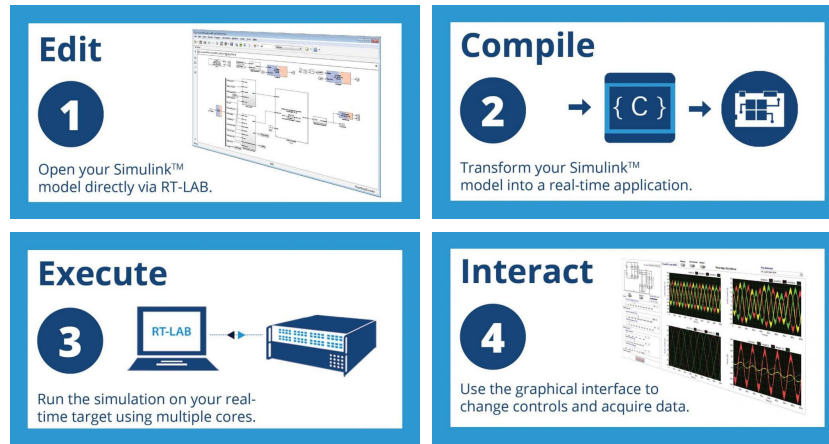


Figure 7.3: 4 Steps to Real-Time simulation using RT-Lab

7.4.8 Power Amplifier

Analog signals for current and voltage generated by simulated current and voltage transformers are transmitted via output ports of Opal-RT to protection equipment, including fault detectors and relays. However, due to the low power of these signals, they need to be amplified before transmission to the input of the protection equipment. To address this issue, an amplifier is used, which is placed between the analog outputs of Opal-RT and the analog inputs of the protection equipment. At the EDF laboratory, we use an amplifier from "OPAL-RT TECHNOLOGIES" that is fully compatible with the Opal-RT simulation platform. This amplifier is specifically designed for real-time simulations of power networks, motors, and DER emulators.

