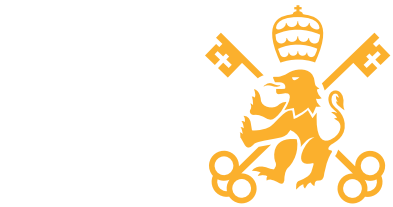

COMILLAS

UNIVERSIDAD PONTIFICIA

ICAI ICADE CIHS

Contribution to the analysis and evaluation of the digitalisation of smart grids

by

Néstor Rodríguez Pérez

supervised by

Dr. Javier Matanza Domingo

Dr. Gregorio López López

A document submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at

ICAI School of Engineering

Comillas Pontifical University

Madrid, 2024

Start by doing what's necessary; then do what's possible; and suddenly you are doing the impossible. - Saint Francis of Assisi

Declaration

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

Néstor Rodríguez Pérez
Madrid, January 2024

Acknowledgement

Soy de los que creen que los grandes logros que uno alcanza en la vida son resultado de una mezcla de trabajo, perseverancia, oportunidad, y de las personas de las que uno se rodea.

Le debo todo lo que soy y todo lo que he conseguido en mis 27 años de vida a mis padres, Carmen y Blas, así como a mi hermana, Lidia. Su cariño, apoyo, y sacrificio me han ayudado a afrontar todos los retos que me he propuesto y a convertirme en la persona que soy actualmente. Me han dado acceso a la mejor preparación posible, tanto escolar como universitaria, sin las cuales esta tesis doctoral no habría sido posible.

Asimismo, esta tesis tampoco habría sido posible sin mis dos directores, Javier Matanza y Gregorio Lopez, a los que puedo llamar amigos y, como ellos dicen, ”padres académicos”. Les estoy muy agradecido por la confianza depositada en mí al ofrecerme la oportunidad de realizar el Doctorado y de participar en grandes proyectos de investigación, y por todo su apoyo a lo largo de estos casi cuatro años. Ambos son mi ejemplo a seguir, no solo a nivel profesional, sino también personal.

También quisiera agradecer el apoyo de mis compañeros en el IIT, por mantener un ambiente excelente para realizar investigación de alta calidad. En particular, quisiera agradecer a los investigadores Rafael C., Lukas, y José Pablo, con los que he trabajado más estrechamente durante esta etapa predoctoral, y cuyo apoyo y experiencia también han resultado fundamentales para la finalización de esta tesis. También, agradecer a mis compañeros de la segunda planta del IIT; es un placer trabajar a vuestro lado cada día.

Por último, pero no por ello menos importante, quisiera agradecer a mis amigos el haberme apoyado en este gran reto que supone un Doctorado, por estar ahí en los buenos y malos momentos, y por hacer sencillo el desconectar y descansar del trabajo.

Muchas gracias, a todos, por todo,

Néstor

Abstract

Digitalisation is the main vehicle to make the grid smarter and face the challenges of the energy transition. This digitalisation involves the widespread implementation of sensors and actuators in the distribution grid, connectivity, and data processing technologies, having an impact on multiple activities of Distribution System Operators (DSOs).

This PhD thesis aims to address some of the aspects significantly related to the digital transformation of distribution grids to increase the effectiveness of this process. To achieve this, this PhD thesis first identifies the key technologies and challenges associated with this transformation. Based on this, it proposes a framework for measuring the level of digitalisation in distribution grids and develops a methodology for conducting quantitative Scalability and Replicability Analyses (SRA) of Information and Communication Technologies (ICT) in smart grid solutions. Since the high scalability and replicability of ICTs may also have a negative impact, the thesis explores the potential impact of cyberattacks on highly scalable and replicable devices, such as high-wattage IoT devices and distributed energy resources control devices. Finally, the increased penetration of distributed energy resources and the cybersecurity risk require better coordination between system operators. For this, the last part of this thesis identifies and discusses the communication and data model standards that system operators may adopt to enhance coordination and system resilience.

The examination of the main technologies used in the digitalisation of distribution grids and their applications shows that disruptive technologies such as digital twins, inspection and immersive technologies, Artificial Intelligence (AI), or Internet of Things (IoT) can transform the monitoring of Low Voltage (LV) networks, predictive maintenance, optimise investments and planning activities, or increase labour productivity, among others. In terms of challenges, the main ones associated with digitalisation affect cybersecurity, core processes, and the electric power ecosystem in general. These challenges must be properly addressed to fully leverage the advantages and benefits of new technologies.

To assess the level of digitalisation in distribution grids, 16 indicators are proposed. Unlike previous research that focused on performance evaluation, these indicators specifically examine the digitalisation aspects. They are categorised according to the pillars of digitalisation, including sensors and actuators, connectivity, data processing, and digital culture. These indicators are aligned with the guidelines set forth in Article 59.1 of the EU Directive 2019/944 and with the Joint Research Center DSO Observatory. They are designed to be applicable regardless of the use cases, requiring minimal data input, and could be used to establish causal relationships between performance and digital infrastructure.

To facilitate the digitalisation process through the deployment of scalable and replicable solutions, a step-by-step methodology for conducting ICT Scalability and Replicability Analysis (SRA) in smart grids is developed. To validate this methodology, it is applied to two real case studies using the OMNeT++ network simulation framework. Case study A

examines a self-consumption monitoring and control system that implements the Modbus TCP protocol to communicate with electricity storage and solar PV assets. Case study B analyses an indoor conditions monitoring system based on wireless M-Bus for the implementation of an energy management system. The results of the ICT SRA are presented using ICT scalability and replicability maps, a new concept that allows a quick overview of the analysed scenarios and an efficient estimation of the feasibility of unexplored scenarios. The methodology proves to be an effective way to analyse wired and wireless ICT, providing a comprehensive SRA of ICT systems for various scenarios.

To evaluate the potential impact of massively compromising internet-connected devices present in smart grids, two studies using DigSilent PowerFactory are conducted in this PhD thesis. The first study examines the replicability of Manipulation of Demand through IoT (MaDIoT) attacks in two different power system models: the PST-16 model, which represents a simplified version of Europe, and the IEEE 39-Bus model, which represents New England (North America). This study highlights the differences in the success and impact of the attacks between the two models, thus expanding and complementing previous research that focused primarily on American power system models. The second study evaluates the replicability of MaDIoT attacks in a power system that incorporates distributed solar PV generation, resulting in lower probability of success. Furthermore, it analyses the impact of MaDIoT 3.0 attacks in different scenarios. MaDIoT 3.0 attacks are introduced in this thesis as an evolution of the original MaDIoT attacks, and combine attacks on both the demand and Distributed Energy Resource (DER) devices.

Finally, this thesis examines the protocols and standards commonly used in recent European projects for data exchange between system operators. It discusses the utilisation of these protocols and standards for exchanging specific types of information, with a particular focus on the Common Information Model (CIM), which provides a great coverage of technical information but needs further development, and two alternative communication mechanisms (publish-subscribe and client-server), whose characteristics must be considered when developing an ICT architecture.

Resumen

La digitalización es el principal vehículo para hacer la red más inteligente y afrontar los retos de la transición energética. Esta digitalización implica la implementación generalizada de sensores y actuadores en la red de distribución, conectividad y tecnologías de procesamiento de datos, lo que tiene un impacto en múltiples actividades de los Operadores de Sistemas de Distribución (DSO).

Esta tesis doctoral aborda algunos de los aspectos más relacionados con la transformación digital de las redes de distribución con el objetivo de aumentar la eficacia de este proceso. Para lograrlo, esta tesis identifica primero las tecnologías clave y los desafíos asociados con esta transformación. En base a esto, propone un marco para medir el nivel de digitalización en las redes de distribución y desarrolla una metodología para realizar Análisis cuantitativos de Escalabilidad y Replicabilidad (SRA) de las Tecnologías de la Información y la Comunicación (TIC) en soluciones de *smart grids*. Dado que la alta escalabilidad y replicabilidad de las TIC pueden también tener un impacto negativo, la tesis explora el impacto potencial de los ciberataques en dispositivos altamente escalables y replicables, como dispositivos IoT de alto consumo y dispositivos de control de recursos energéticos distribuidos. Finalmente, la mayor penetración de los recursos energéticos distribuidos y el riesgo de ciberseguridad requieren una mejor coordinación entre los operadores del sistema. Para ello, la última parte de esta tesis identifica y analiza los estándares de comunicación y modelos de datos que los operadores de sistemas pueden adoptar para mejorar la coordinación y la resiliencia del sistema.

El análisis de las principales tecnologías utilizadas en la digitalización de las redes de distribución y sus aplicaciones muestra que tecnologías disruptivas como los gemelos digitales, las tecnologías de inspección e inmersión, la IA o el Internet de las Cosas (IoT) pueden transformar la monitorización de las redes de Baja Tensión (BT) , mantenimiento predictivo, optimizar las inversiones y la planificación de actividades, o aumentar la productividad laboral, entre otros. En términos de desafíos, los principales asociados a la digitalización tienen que ver con la ciberseguridad, los procesos centrales y el ecosistema del sector eléctrico en general. Estos desafíos deben abordarse adecuadamente para aprovechar plenamente las ventajas y beneficios de las nuevas tecnologías.

Para evaluar el nivel de digitalización de las redes de distribución se propone un conjunto de 16 indicadores. A diferencia de trabajos previos que se centraron en la evaluación del desempeño, estos indicadores examinan específicamente los aspectos de la digitalización. Se clasifican según los pilares de la digitalización, incluidos sensores y actuadores, conectividad, procesamiento de datos y cultura digital. Estos indicadores están alineados con lo recogido en el Artículo 59.1 de la Directiva Europea 2019/944 y con el *DSO Observatory* del *Joint Research Center*. Están diseñados para ser aplicables independientemente del caso de uso, requieren una recopilación mínima de datos y podrían usarse para establecer relaciones

causales entre el mejor funcionamiento de la red y la infraestructura digital.

Para facilitar el proceso de digitalización mediante el despliegue de soluciones escalables y replicables, se desarrolla una metodología para realizar paso a paso el SRA de las TIC en *smart grids*. Para validar esta metodología, se aplica a dos casos reales utilizando el simulador de redes de comunicación OMNeT++. El caso de estudio A analiza un sistema de monitorización y control de autoconsumo que implementa el protocolo Modbus TCP para comunicarse con baterías y el colector de datos de la generación solar fotovoltaica. El caso de estudio B analiza un sistema de monitorización de condiciones de interiores que usa el protocolo M-Bus inalámbrico para un sistema de gestión de la energía. Los resultados del ICT SRA se presentan utilizando mapas de escalabilidad y replicabilidad de las TIC, un nuevo concepto que permite una visión rápida de los escenarios analizados y una estimación eficiente de la viabilidad de escenarios no analizados. La metodología demuestra ser una forma eficaz de analizar las TIC, tanto cableadas como inalámbricas, proporcionando una SRA integral de sistemas TIC para diversos escenarios.

Para evaluar el potencial impacto de comprometer masivamente los dispositivos conectados a Internet presentes en las redes inteligentes, en esta tesis se llevan a cabo dos estudios utilizando DigSilent PowerFactory. El primer estudio examina la replicabilidad de los ataques de manipulación de la demanda a través de IoT (MaDIoT) en dos modelos de redes eléctricas distintos: el modelo PST-16, que representa una versión simplificada de Europa, y el modelo IEEE 39-Bus, que representa a Nueva Inglaterra (Norteamérica). Este estudio destaca las diferencias en el éxito y el impacto de los ataques entre los dos modelos, ampliando y complementando investigaciones anteriores que se centraron principalmente en los modelos de red estadounidenses. El segundo estudio evalúa la replicabilidad de los ataques MaDIoT en un sistema eléctrico que incorpora generación solar fotovoltaica distribuida, lo que resulta en una menor probabilidad de éxito. Además, analiza el impacto de los ataques MaDIoT 3.0 en diferentes escenarios. Los ataques MaDIoT 3.0 se presentan en esta tesis como una evolución de los ataques MaDIoT originales y combinan ataques tanto en dispositivos de demanda como de DER.

Finalmente, esta tesis examina los protocolos y estándares comúnmente utilizados en proyectos europeos recientes para el intercambio de datos entre operadores de red. Se analiza la utilización de estos protocolos y estándares para el intercambio de tipos específicos de información, con un enfoque particular en el *Common Information Model* (CIM), que proporciona una gran cobertura de información técnica pero necesita mayor desarrollo, y dos mecanismos de comunicación alternativos (publicación- suscripción y cliente-servidor), cuyas características deben ser consideradas a la hora de desarrollar una arquitectura TIC.

Contents

1 Introduction **1**

1.1 Motivation 3
1.2 Objectives of this thesis 5
1.3 Thesis outline 5

2 Digitalisation for Smart Grids: technologies and challenges **11**

2.1 Introduction 11
2.2 Digitalisation pillars 12
2.3 Impact of digitalisation on the electricity distribution sector 13
2.3.1 Core impact 14
2.3.2 Systemic impact 16
2.4 Key technologies and their applications 18
2.4.1 Digital twins 18
2.4.2 Inspection technologies 19
2.4.3 Immersive technologies 20
2.4.4 Big Data analytics, artificial intelligence and cloud computing 20
2.4.5 IoT 22
2.4.6 Blockchain 23
2.5 Challenges of digitalisation 24
2.5.1 Challenges in core processes and asset management 24
2.5.2 Challenges in the electric power sector 25
2.5.3 Challenges in cybersecurity and data privacy 26
2.6 Conclusions 29

3 Indicators of the digitalisation of distribution grids **31**

3.1 Introduction 31
3.2 State-of-the-art of Smart Grid indicators 32
3.3 Key indicators of digitalisation 38
3.3.1 Sensors and actuators indicators 38
3.3.2 Connectivity indicators 39

3.3.3 Data Processing indicators . . . 40
3.3.4 Indicators of digital culture . . . 41
3.4 Applicability . . . 42
3.4.1 Overview of the distribution grid . . . 43
3.4.2 Relation between performance and digital infrastructure . . . 44
3.5 Conclusions . . . 45

4 Scalability and Replicability Analysis of ICT in Smart Grids 46
4.1 Introduction . . . 46
4.2 Scalability and replicability: state-of-the-art . . . 48
4.2.1 Definitions and dimensions . . . 48
4.2.2 Literature review . . . 50
4.2.3 Trends and gaps . . . 55
4.3 Methodology description . . . 56
4.3.1 Map the ICT system into the SGAM . . . 56
4.3.2 Scalability questions and system characteristics . . . 57
4.3.3 Minimum requirements and technical constraints . . . 60
4.3.4 Development of scenarios . . . 61
4.3.5 Definition of Key Performance Indicators . . . 62
4.3.6 Development of a simulation model or experiment . . . 63
4.3.7 Run scenarios and analysis of results . . . 64
4.4 Application of methodology: case studies . . . 65
4.4.1 Case study A . . . 65
4.4.2 Case study B . . . 74
4.5 Conclusions . . . 85

5 Impact of cyberattacks to demand and distributed generation 86
5.1 Introduction . . . 86
5.2 State of the art . . . 87
5.3 Materials and methods . . . 88
5.3.1 Power system models . . . 89
5.3.2 Protection schemes . . . 91
5.3.3 MaDIoT bot characteristics . . . 91
5.3.4 Adversary model . . . 92
5.3.5 Criteria for attack success . . . 93
5.4 MaDIoT attacks in different power systems . . . 93
5.4.1 Attack model and Scenarios . . . 93
5.4.2 Results . . . 95
5.5 MaDIoT attacks and distributed energy resources: MaDIoT 3.0 . . . 101

5.5.1 Attack model and Scenarios . . . 103
5.5.2 Results . . . 105
5.6 Conclusions . . . 110

6 TSO-DSO data exchange for resilient operation 112
6.1 Introduction . . . 112
6.2 ICT architectures for TSO-DSO data exchange . . . 113
6.2.1 Interactions between electricity system actors . . . 113
6.2.2 ICT architectures in European projects . . . 115
6.3 Protocols and standards for data exchange: comparison and application . . . 123
6.4 Conclusions . . . 129

7 Conclusions, contributions, and future research 130
7.1 Introduction . . . 130
7.2 Summary . . . 130
7.3 Main conclusions . . . 131
7.4 Thesis contributions . . . 133
7.5 Future work . . . 135
7.6 Published and under-review work . . . 136
7.6.1 Conference presentations . . . 136
7.6.2 Journals (peer-reviewed) . . . 138
7.6.3 Papers under review . . . 140
7.7 Research projects . . . 141
7.8 International research stay . . . 142

A Relevant information for the ICT SRA of Case Study A 143
A.1 Modbus TCP . . . 143
A.2 Scalability analysis of baseline scenario . . . 144

B Relevant information for the ICT SRA of Case Study B 147
B.1 Wireless M-Bus . . . 147
B.2 Transmission medium model . . . 149
B.3 Comparison of impact of propagation models . . . 151
B.3.1 Propagation models . . . 151
B.3.2 Scenarios and settings for the comparative analysis of propagation models . . . 151
B.3.3 Simulation results . . . 152

C Distributed Generation in the PST-16 System 157

D TSO-DSO Coordination Schemes **160**

Bibliography **161**

List of Figures

1.1 Schematic representation of modern electricity systems. 2
1.2 Main research questions for this thesis. 3
1.3 Structure of the chapters and their relations with the appendixes. 10

2.1 Pillars of digitalisation of power grids 13
2.2 Interactions between electricity system actors. Based on the Smart Grid Conceptual Model by [41] 17

4.1 Types and subtypes of ICT scalability based on [116], [117]. 49
4.2 Dimensions of interoperability and related SGAM layers. 50
4.3 Quantitative Information and Communications Technologies (ICT) Scalability and Replicability Analysis (SRA) methodology proposed. 56
4.4 SGAM Framework. 57
4.5 Potential influence of scaling-up components in SGAM domains and zones. . 59
4.6 Types of communications between devices and/or systems to consider for the identification of potential bottlenecks. 62
4.7 Structure and visual representation of an ICT scalability and replicability map. 64
4.8 ICT system of case study A mapped into the Smart Grid Architecture Model (SGAM). Component and communication layers. 67
4.9 Simplified SGAM characterisation of the ICT system of case study A. 68
4.10 ICT Scalability and replicability map of case study A with the analysed scenarios. 71
4.11 Standard deviation of the total polling time for different BER and number of servers in scenario A2. 72
4.12 Standard deviation of the total polling time for different number of servers in scenarios A1 and A5. 73
4.13 ICT system of case study B mapped into the SGAM. Component and communication layers. 75
4.14 Simplified SGAM characterisation of the ICT system of case study B. 76
4.15 Baseline building block in Turku, Finland, for case study B. 77

4.16 Top view of the 3D model in OMNeT++ for the Positive Energy Block (PEB). 80
4.17 ICT Scalability and replicability map of case study B with the analysed scenarios. 81
4.18 Delivery ratio of scenario B7 depending on the standard deviation and mean (in minutes) of the Gaussian distribution used to determine the first transmission time of messages. 82
4.19 Delivery ratio, message error ratio, and gross delivery ratio of scenarios B1, B4.1, B4.2, B8, and B10. 83

5.1 Simplified diagram and main characteristics of the PST-16 benchmark model. 90
5.2 Success ratio for different scenarios when increasing the size of the botnet. . . 95
5.3 Frequency, voltages, and relative rotor angle of generators when attacking 500k bots in loads 30, 31, and 34 in the PST-16 system (EU-C scenario with high impact). Attack at t=1s (indicated by *). 98
5.4 Zoom to the frequency and relative rotor angle shown in Figure 5.3 for the first 10 s. Attack at t=1s (indicated by *). PST-16 system (EU-c scenario with high impact) 99
5.5 Frequency and voltages when attacking 500 k bots in loads 12, 16, and 28 in the IEEE 39-Bus system (US39 scenario with high impact). Attack at t=1s (indicated by *). 100
5.6 Evolution of MaDIoT attacks. 101
5.7 Simplified diagram of area C in the PST-16 system with distributed solar Photo Voltaic (PV) included. 102
5.8 Explanation of the pattern followed for the names of the scenarios. 104
5.9 Success ratio of traditional MaDIoT attacks (demand compromised) in the PST-16 system with and without DG. 105
5.10 Comparison of bus voltages in area C when Distributed Generation (DG) is connected. 106
5.11 Frequency, voltages, and relative rotor angle of generators in scenario 3C1500_0 (highest impact observed). Attack at t=0.5s (indicated by *) 107

6.1 SGAM Information–Communication layer of the ICT architectures implemented in SmartNet 116
6.2 SGAM Information–Communication layer of the ICT architectures implemented in the Spanish demo of Coordinet 118
6.3 SGAM Information–Communication layer of the ICT architectures implemented in the Greek demo of Coordinet 119
6.4 SGAM Information–Communication layer of the ICT architectures implemented in the Slovenian demo of TDX-Assist 120

6.5 Interoperable pan-European Grid Services Architecture (IEGSA). Source: own elaboration based on [217]. 121
6.6 Summary of the SGAM layers of the ”Flexibility Platform” demonstrated in EU-SysFlex 122

A.1 Simplified Modbus transaction between client and server 143
A.2 Dataframe transmitted with Modbus TCP over Ethernet 144
A.3 Time to complete the polling to all the servers connected for different BER values and number of servers 145
A.4 Standard deviation of the total polling time for different BER and number of servers 146

B.1 Wireless M-Bus protocol stack 147
B.2 Wireless M-Bus frame formats A and B 149
B.3 Top view of the scenarios considered. 153
B.4 BER-SNR for the propagation models studied. Scenario #1 154
B.5 BER-SNR for the propagation models studied. Scenario #2 155
B.6 Delivery ratio, message error ratio, and gross delivery ratio depending on the number of sensors, using different propagation models. Scenario #2 156

List of Tables

2.1 Summary of the main applications of key digital technologies in distribution grids. 18

3.1 Number of indicators and categories per reference, and their main objective and characteristics. 34
3.2 Benchmarking of main smart grid indicators in the literature 37
3.3 Indicators to evaluate the digitalisation of power distribution grids 38

4.1 Summary of the scope of analysis, strengths, weaknesses, and metrics for the main literature reviewed 54
4.2 Functional characteristics of the control and monitoring system studied in case study A. 68
4.3 Scenarios simulated for the ICT SRA of case study A. 69
4.4 Scenarios to be compared depending on the objective of the analysis for case study A. 70
4.5 Summary of characteristics of the sensors [167] and Edge Hub [168]. 76
4.6 Scenarios simulated for the ICT SRA of case study B. 78
4.7 Scenarios to be compared depending on the objective of the analysis for case study B 79

5.1 Summary of the characteristics of the IEEE 39-BUS and the PST-16 models. . 89
5.2 UFLS scheme applied for the 50 and 60 Hz models (frequency vs. load to be shed) 91
5.3 Considered Manipulation of Demand through IoT (MaDIoT) adversary model based on guidelines by [200]. 93
5.4 Considered MaDIoT attack model based on the modelling guidelines by [200]. 94
5.5 MaDIoT attack scenarios for the IEEE 39-Bus model (New England) and the PST-16 model (Europe). 95
5.6 Average impact on the system when successfully attacking 500k bots in the US39 and EU-C scenarios. 97

5.7 Initial conditions of the PST-16 system with DG in area C compared to the base PST-16 (without DG). . . . 103
5.8 Scenarios analysed for the PST-16 system with 546.5 MW (10% of demand in Area C) of distributed solar PV connected in Area C. . . . 104
5.9 Success ratio of MaDIoT 3.0 attacks on area C. . . . 108
5.10 Success ratio of MaDIoT 3.0 attacks on different areas. . . . 109
5.11 Success ratio of MaDIoT 3.0 attacks when considering six buses for the attacked demand. . . . 109

6.1 ICT architectures implemented in EU-funded projects. . . . 124
6.2 Summary of advantages/disadvantages of Client–Server (C-S) and Publish–Subscribe (P-S) communications. . . . 126
6.3 Summary of standards coverage and applicability for the exchange of specific types of information. . . . 128

A.1 Request and Response Protocol Data Unit (PDU) for Read Holding Registers function code . . . 144

B.1 Summary of wireless M-Bus transfer modes . . . 148
B.2 Configurations of the log-normal and ITU-R P.1238 models considered for comparison. . . . 152
B.3 Analysed scenarios. . . . 152

C.1 Installed capacity of Solar PV generation in Spain per voltage level. . . . 157
C.2 Estimated solar PV generation connected to <145kV for the years 2023 and 2030 in Spain. . . . 158
C.3 Distributed solar PV generation per bus of area C (PST-16) for THE years 2023 and 2030 . . . 159

D.1 Coordination schemes comparison among EU H2020 projects and [219] . . . 160

Acronyms

ADU Application Data Unit.

AI Artificial Intelligence.

AMI Advanced Metering Infrastructure.

AMQP Advanced Message Queuing Protocol.

API Application Program Interface.

APTs Advanced Persistent Threats.

AR Augmented Reality.

ASM Active System Management.

BER Bit Error Ratio.

BMS Battery Management System.

BSP Balancing Service Provider.

BUC Business Use Case.

C-S Client–Server.

CAPEX Capital Expenditure.

CDO Chief Data Owner.

CDR Cloud Demand Response.

CGMES Common Grid Model Exchange Specification.

CIM Common Information Model.

CISO Chief Information Security Officer.

CMP Commercial Market Party.

COV Coefficient of Variation.

DDoS Distributed Denial of Service.

DEP Data Exchange Platform.

DER Distributed Energy Resources.

DG Distributed Generation.

DiD Defence in Depth.

DL Deep Learning.

DNS Domain Name System.

DORA Digital Operational Resilience Act.

DoS Denial of Service.

DSO Distribution System Operator.

ECCo SP ENTSO-E Communication and Connectivity Service Platform.

EMPAIR Equipement Modulaire de Protection des Accès Industriels Répartis.

EMS Energy Management System.

ESaaS Energy Storage as a Service.

ESB Enterprise Service Bus.

ESMP European Style Market Profile.

EUCC European Cybersecurity Certification scheme.

EV Electric Vehicle.

FSK Frequency Shift Keying.

FSP Flexibility Service Provider.

FSSF File System Shared Folders.

GDPR General Data Protection Regulation.

GIS Geographical Information System.

GSM Global System Mobile.

HAN Home Area Network.

HEMRM Harmonised Electricity Market Role Model.

HEMS Home Energy Management Systems.

HTTPS Hypertext Transfer Protocol Secure.

HV High Voltage.

ICCP Inter-control Centre Communications Protocol.

ICT Information and Communications Technologies.

IEC International Electrotechnical Commission.

IEGSA Interoperable pan-European Grid Services Architecture.

IoT Internet of Things.

IPsec Internet Protocol security.

IQR Interquartile Range.

IT Information Technology.

JRC Joint Research Center.

KER Key Explotable Result.

KPI Key Performance Indicator.

LAN Local Area Network.

LIDAR Laser Imaging, Detection, and Ranging.

LM Local Market.

LoWPAN Low power Wireless Personal Area Networks.

LPWANs Low Powered Wide Area Networks.

LTE Long Term Evolution.

LV Low Voltage.

MaDIoT Manipulation of Demand through IoT.

MBAP Modbus Application Protocol.

mFRR Manual Frequency Restoration Reserve.

MIME Multipurpose Internet Mail Extensions.

ML Machine Learning.

MMS Manufacturing Message Specific.

MO Market Operator.

MQTT Message Queuing Telemetry Transport.

MTBF Mean Time Between Failure.

MTTF Mean Time To Failure.

MV Medium Voltage.

NAN Neighbourhood Area Network.

NPLC Narrowband Power Line Communications.

NRA National Regulatory Authority.

NRAs National Regulatory Authorities.

OFGR Over-Frequency Generator Rejection.

OPEX Operational Expenditure.

OSI Open Systems Interconnection.

OT Operational Technology.

P-S Publish–Subscribe.

P2P Peer-to-Peer.

PDU Protocol Data Unit.

PEB Positive Energy Block.

PED Positive Energy District.

PLC Power Line Communications.

PLR Packet Loss Rate.

PMUs Phasor Measurement Units.

PV Photo Voltaic.

QoS Quality of Service.

RAM Random Access Memory.

RES Renewable Energy Sources.

REST Representational State Transfer.

SCADA Supervisory Control And Data Acquisition.

SD Standard Deviation.

SFTP Secure SHell File Transfer Protocol.

SGAM Smart Grid Architecture Model.

SGCM Smart Grid Conceptual Model.

SNR Signal-to-Noise Ratio.

SO System Operator.

SOAP Simple Object Access Protocol.

SRA Scalability and Replicability Analysis.

SRM Shared Responsibility Model.

SUCs System Use Cases.

TLS Transport Layer Security.

TSO Transmission System Operator.

TSOs Transmission System Operators.

UAVs Unmanned Aerial Vehicles.

UDP User Datagram Protocol.

UFLS Under-Frequency Load Shedding.

V2G Vehicle-to-Grid.

VPN Virtual Private Network.

VPPs Virtual Power Plants.

VR Virtual Reality.

WAN Wide Area Network.

WS Web Services.

XML eXtensible Markup Language.

Glossary

G_{Rx} Gain of the receiver antenna.

G_{Tx} Gain of the transmitter antenna.

$L_f(n_f)$ Floor penetration loss factor that depends on the number of floors, n_f.

N_B Background noise.

$PL(d_0)$ Path loss at a reference distance d_0.

$P_0[W]$ Initial power of the signal in watts.

P_{Rx} Power of signal received.

P_{Tx} Initial power of transmission of a signal.

$P_z[W]$ Final power of the signal at distance z, in watts.

R_{eff} Effective reflectivity of the signal.

R_p Power reflection coefficient for P-polarized light.

R_s Power reflection coefficient for S-polarized light.

T_{eff} Effective transmission of the signal.

T_j Polling time in round j.

X_σ Zero-mean Gaussian distributed variable with standard deviation σ.

δ Loss angle.

λ Wavelength of the signal.

σ Standard deviation.

θ_i Angle of incidence.

d Distance between antennas.

f Frequency.

k Cosine of the angle of the refracted rays with respect to the normal.

n_1 Refractive index of medium 1.

n_2 Refractive index of medium 2.

n_{acc} Access number between 0 and 255 in wireless M-Bus.

n_f Number of floors between transmitter and receiver.

n Loss rate that depends on the environment.

t_{acc} Retransmission time interval for wireless M-Bus.

$t_{i,j}$ Time it takes for the client to request, received, and process all the necessary information from each servier i at round j.

t_{nom} Nominal transmission time for wireless M-Bus.

Chapter 1

Introduction

The energy transition is requiring, among other measures, the decarbonisation of the energy sector. This is leading to massive electrification of the energy demand and an increase in the use of renewable sources. In electricity distribution networks, this is translating into an increase in the number of Distributed Energy Resources (DER), Electric Vehicle (EV) charging points, and active participation of consumers (e.g., *prosumers*, demand response), which pose challenges for the operation of the network, that is required to be more dynamic. To face these challenges, the development of smart grids is key.

The smart grid can be defined as the application of Information and Communications Technologies (ICT) (understood as computer and electronic elements coupled with telecommunications) to the electricity grid [1] to improve its functioning (operation, quality of service, reliability, etc.). From an infrastructure point of view, a smart grid can be understood as the digitalisation of the electricity grid infrastructure to achieve better performance.

Digitalisation investments are the main vehicle to make the grid smarter and face the challenges of the energy transition [2]. However, this is a complex transformation process due to several factors. In many countries, such as Spain, the electricity transmission system, operated by a Transmission System Operator (TSO), only accounts for $\approx$ 4.4% of the total extension of the electricity system [3]. The remaining 95.6% constitute the electricity distribution system, which in Spain represents approximately one million kilometres of power lines, operated by more than 300 Distribution System Operator (DSO). This scale makes it difficult to achieve homogeneous levels of digitalisation, the use of the same technologies or interoperable ones, and to coordinate the operation between TSO and DSOs in a ever-evolving landscape where the operation of distribution systems is becoming more active due to the appearance of new types of customers. Figure 1.1 shows a simplified representation of modern electricity systems where new types of customers emerge.

For the effective development of smart grids through digitalisation, this process has to be analysed and evaluated through some of the different aspects it involves: which technologies

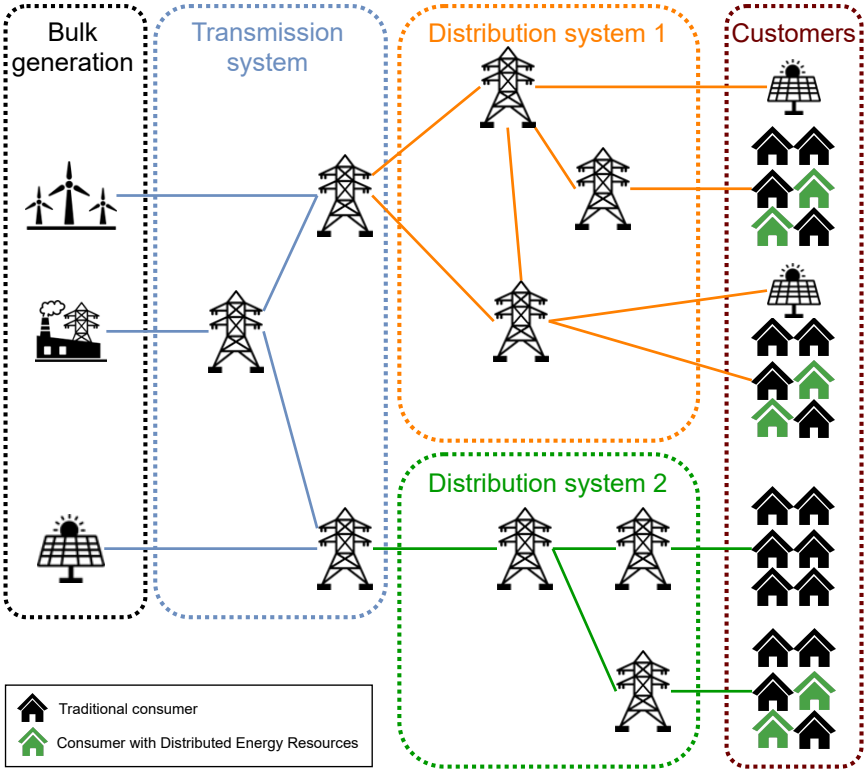

Figure 1.1: Schematic representation of modern electricity systems.

are driving this process; how to measure the overall level of digitalisation of a distribution grid; how, before their implementation, the scalability and replicability of the ICT involved can be analysed; what could be the impact of massively compromising internet-connected devices with a great potential for scalability and replicability in smart grids; and which protocols and standards can be used by system operators to exchange information for a more resilient operation.

The development of smart grids cannot be based on a single technological option. To make better decisions, DSOs need to be aware of how digitalised their grid is, which are the latest technologies and their added value to their activities. Since the remuneration of the distribution sector is regulated in Europe, National Regulatory Authorities (NRAs) also need to evaluate the advances in digitalisation made by DSOs for smarter grids [4].

These advances are strongly based on ICT. It is clear that smart grid solutions need to be highly scalable and replicable [5], [6] for their widespread deployment in the extensive distribution grid. However, it is not clear how to analyse the scalability and replicability of the ICT systems involved, which are an important part to consider [7] before implementing a solution.

At the same time, massive deployments of unsecured internet-connected devices in smart grids can be a threat to the entire electricity system. It is not so clear how this scalability

and replicability could affect power systems if devices (IoT, DER devices) get massively compromised in a cyberattack, and if the impact of such attacks would scale and replicate in the same way under different conditions or when performed in different power systems [8].

To increase system resilience and reliability under different conditions, DSOs and TSOs may need to exchange more information for normal system operation or for the implementation of system services mechanisms (e.g., flexibility markets) [9]. However, the wide range of standards and communication protocols make it difficult to select which communication protocols and information models are more suitable for the exchange of specific types of information.

This thesis addresses each of these essential aspects for the effective and efficient digitalisation of distribution grids in their evolution to smart grids.

1.1 Motivation

Digitalisation is driving most of the investments required by the electricity system to face the energy transition, involving the development of smart grids. However, the full digitalisation of the grid, which can be understood as the implementation of digital technologies for each and every node, is neither efficient nor cost-effective. For an effective digitalisation, it is necessary to tackle some of the aspects, presented in the form of research questions, related to this process. These research questions are outlined in Figure 1.2:

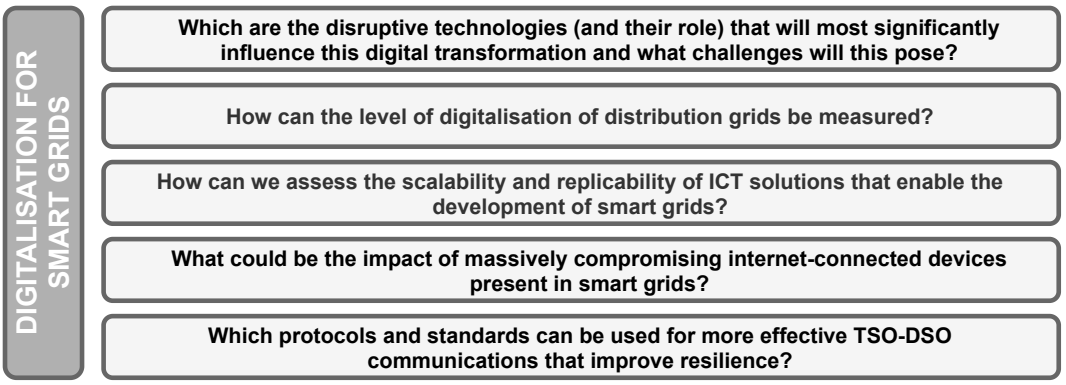

Figure 1.2: Main research questions for this thesis.

First, given the wide range of technologies that can be implemented for smart grids, it is necessary a preliminary identification of the main disruptive technologies and their impact on the activities of DSOs, as well as the challenges of this digitalisation process. This is translated into the following question: **Which are the disruptive technologies (and their role) that will most significantly influence this digital transformation and what challenges will this pose?**. The answer to this question sets the basis to analyse more in depth relevant aspects of the digitalisation of distribution grids.

In Europe, Article 59.1 of EU Directive 2019/944 [4] and the EU Action Plan *"Digitalising the energy system"* [2] highlight the need of indicators to monitor smart and digital investments in the electricity grid. As it will be more thoroughly detailed in Chapter 3, despite the fact that different organisations have made some proposals, none of them aims to directly measure the level of digitalisation (i.e., digital infrastructure), focusing more on its results in terms of performance. This raises the following research question: **How can the level of digitalisation of distribution grids be measured?**.

To digitalise the electricity grid, smart grid solutions need to be scalable and replicable. A Scalability and Replicability Analysis (SRA) is included in most EU-funded research projects [6]. However, the dependence of these solutions on Information and Communication Technologies (ICT) is increasingly making it necessary to include these in the scope of analysis. ICT must maximise the deployment possibilities and be able to support new devices and accommodate new services. As Chapter 4 will highlight, there is no clear approach for this type of analysis, which affects the clarity of the results. Therefore, this raises the following research question: **How can we assess the scalability and replicability of ICT solutions that enable the development of smart grids?**.

Although the scalability and replicability of ICT are desirable features from a techno-economic perspective, they can increase the cybersecurity risk. The massive deployment of IoT devices and Distributed Energy Resources (DER), with more relaxed cybersecurity measures than the Supervisory Control and Data Acquisition (SCADA) systems. However, as Chapter 5 will show, the negative impact that MaDIoT attacks could potentially have on different power systems needs further research [8]. This raises the question: **What could be the impact of massively compromising internet-connected devices present in smart grids?**.

Finally, not only to increase the resilience of the system against MaDIoT attacks but also to integrate DER and active demand into the operation of the system [9], allowing them to be participants in system services markets [10], more data exchange between system operators is necessary. Choosing the appropriate communication protocols and information models for exchanging specific types of information is challenging due to the extensive variety of standards and communication protocols available. Just in Europe, the number of alternative approaches followed by EU-funded research projects is high, as the analysis in Chapter 6 will show. This raises the following research question: **Which protocols and standards can be used for more effective TSO-DSO communications that improve resilience?**.

1.2 Objectives of this thesis

The general objectives of this thesis are to contribute to the analysis and evaluation of the digitalisation of smart grids, mainly from the ICT perspective, by proposing a set of indicators to measure the digitalisation of distribution grids and evaluating the scalability and replicability of the ICT involved, the impact of compromising insecure devices that can be massively deployed in this digitalisation process (e.g., IoT devices, solar PV inverters, etc.), and the different communication protocols and data models that can be used by system operators to exchange information for better overall operation.

The specific scientific objectives that were pursued to answer the research questions presented in the motivation can be summarised as follows:

- Identify the main technologies and challenges of the digitalisation of electricity distribution grids.
- Propose a framework to measure the digitalisation of distribution grids in an easy way and that allows the fair comparison of DSOs regardless of their size.
- Develop and apply a methodology to perform quantitative scalability and replicability analyses of ICT for smart grid use cases, identifying system requirements and constraints, and providing guidelines for the selection of metrics and the development of realistic scenarios. The methodology must be applicable to systems relying on different types of technologies (wired and wireless).
- Perform a simulation study of the impact on different power systems of cyberattacks to highly scalable and replicable devices. The devices to be considered include high-wattage IoT devices and control devices for distributed energy resources.
- Perform a qualitative study of the main communication and data model standards that system operators can use to exchange specific types of information.

1.3 Thesis outline

This thesis can be divided into four main parts, all related to the challenges of increasing the digitalisation of electricity distribution systems for the development of smarter grids, introduced in Chapter 2, setting up the context for the rest of the document.

The first part (Chapter 3) addresses the challenge of measuring the digitalisation of distribution grids in a simple way so that DSOs can be objectively compared in their efforts, and cause-effect relationships between investments and performance can be identified.

The second part (Chapter 4) focuses on the scalability and replicability of ICT for an efficient digitalisation, defining and applying a quantitative methodology to analyse these

aspects in a smart grid context. However, high scalability and replicability of ICT may be a threat to the power system if they have vulnerabilities and an attacker manages to compromise them.

The third part (Chapter 5) analyses the impact on the power system if an attacker manages to compromise high-wattage IoT devices in the demand (MaDIoT attack) and DER control devices (MaDIoT 3.0 attack), gaining insights about the scalability and replicability of the impact of these attacks under different conditions.

Finally, the last part (Chapter 6) deals with the challenge of improving the communications between system operators, which could be key to increasing the resilience of the system to minimise the impact of MaDIoT attacks and facilitate the integration of DER in system operation. It evaluates different protocols and standards for TSO-DSO data exchange, discussing their application for the exchange of specific types of information.

The document is structured in seven chapters and four appendices. The content addressed in each of them is briefly described in the following paragraphs, also indicating the related published / under review articles.

Chapter 2 provides an overview of digitalisation for smart grids, setting the context for the rest of the thesis. It discusses the main impact of this digitalisation for Distribution System Operator (DSO)s and the applications of the main digital technologies that are being implemented. Additionally, it also discusses the main challenges that this digitalisation poses. Some of these challenges are directly related to the topics addressed in subsequent chapters. The following journal article related to this chapter is under review:

- **Title:** Digitalisation of Distribution Grids: Technologies and Challenges for the Development of Smart Grids
  Authors: N. Rodríguez-Pérez, E. de Leyva Mérida , G. López, J. Matanza, J.P. Chaves Ávila, R. Cossent
  Journal: Renewable and Sustainable Energy Reviews JCR: Q1
  Status: First review.

Chapter 3 proposes a set of 16 indicators to measure the digitalisation of distribution grids in four main aspects (pillars of digitalisation): sensors and actuators, connectivity, data processing and digital culture. In contrast to other indicators, these are not focused on performance (output) but on the digital infrastructure implemented to improve performance (input). The potential applications of the proposed indicators are also discussed in this chapter. The following journal article related to this chapter was published:

- **Title:** Measuring the Digitalisation of Electricity Distribution Systems in Europe: towards the Smart Grid
  Authors: N. Rodríguez-Pérez, J. Matanza , G. López, R. Cossent, J.P. Chaves Ávila, C. Mateo Domingo , T. Gómez San Román, M.A. Sánchez Fornié

Journal: International Journal of Electrical Power and Energy Systems (IJEPES) Vol. 159, pp. 110009-1 - 110009-9, 2024. JCR: 5,200 Q1 (2022).
DOI: https://doi.org/10.1016/j.ijepes.2024.110009

Chapter 4 addresses how to perform the Scalability and Replicability Analysis (SRA) of ICT for smart grid solutions. It first presents the state-of-the-art of this topic to highlight trends and gaps. Then, a methodology to perform quantitative ICT SRA is described step by step. This methodology is validated by applying it to two case studies from the EU-funded RESPONSE project, using OMNeT++ simulation framework. Case study A implements the monitoring and control system (wired technology) for a self-consumption solution that consists of energy storage and solar PV generation. Case study B implements an indoor conditions monitoring system (wireless technology). For both cases, an ICT scalability and replicability map is generated to provide an overview of the scalability and replicability potential of the solutions. The following journal article related to this chapter was published:

- **Title:** ICT Scalability and Replicability Analysis for Smart Grids: Methodology and Application
  Authors: N. Rodríguez-Pérez, J. Matanza , G. López
  Journal: Energies 17, no. 3: 574. 2023. JCR: 3,200 Q3 (2022)
  DOI: https://doi.org/10.3390/en17030574

Chapter 5 evaluates the impact on the power system of cyberattacks to demand and distributed generation. It analyses the scalability and replicability of Manipulation of Demand through Internet of Things (MaDIoT) attacks by performing two studies. The first one analyses and compares their impact on power systems with different characteristics (IEEE 39 and PST-16 benchmark model). The second one introduces the concept of MaDIoT 3.0 attacks, which, apart from demand, include DER devices in the scope of the attack, and analyses their impact for different scenarios in the PST-16 system. The following journal articles related to this chapter were published / under review:

- **Title:** Confronting the Threat: Analysis of the Impact of MaDIoT Attacks in Two Power System Models
  Authors:N. Rodríguez-Pérez, J. Matanza, L. Sigrist, J. L. Rueda Torres, and G. López.
  Journal: Energies 16, no. 23: 7732. 2023. JCR: 3,200 Q3 (2022)
  DOI: https://doi.org/10.3390/en16237732

- **Title:** MaDIoT 3.0: Assessment of Attacks on Distributed Energy Resources and Demand in a Power System
  Authors:N. Rodríguez-Pérez, J. Matanza, L. Sigrist, J. L. Rueda Torres, and G. López.
  Journal: IEEE Transactions on Smart Grids
  Status: First review.

Chapter 6 discusses protocols and standards for TSO-DSO data exchange. These data exchanges improve the collaboration and coordination of System Operator (SO)s, improving their ability to tackle risks, such as the one by MaDIoT attacks analysed in the previous chapter. Data exchanges may take place because of the implementation of new market mechanisms (e.g., system services) or simply to improve the operation of the system. For this, this chapter first provides an overview of ICT architectures for TSO-DSO data exchange implemented in recent European projects, identifying common protocols and standards. Then, these are compared and their application for the exchange of specific types of information is discussed, focusing on the Common Information Model (CIM) in terms of data models, and on Publish-Subscribe and Client-Server mechanisms in terms of communication protocols. The following journal article related to this chapter was published:

- **Title:** ICT Architectures for TSO-DSO Coordination and Data Exchange: A European Perspective.
  Authors: N. Rodríguez Pérez, J. Matanza , G. López, J.P. Chaves Ávila, F. Bosco, V. Croce, K. Kukk, M. Uslar, C. Madina, M. Santos-Mugica
  Journal: IEEE Transactions on Smart Grid, vol. 14, no. 2, pp. 1300-1312, March 2023. JCR: 9,600 Q1 (2022)
  DOI: `https://doi.org/10.1109/TSG.2022.3206092`

Chapter 7 provides a summary of the contributions made in this thesis, presents some general conclusions, and identifies unresolved issues that can be explored in future research. Furthermore, it includes a list of all the papers that have been published in journals and conference proceedings as a result of this thesis. Finally, it also includes a list of all the research projects related to the topics addressed in which the Ph.D. candidate has been involved.

The document also includes a number of appendices in order to provide additional information to the interested reader. They are described, together with their relationship to the thesis chapters, in the following paragraphs:

Appendix A provides an overview of the Modbus TCP communication protocol, which is relevant for the ICT SRA of Case Study A carried out in Chapter 4, and a detailed analysis of one of the scenarios considered. The following conference article related to the content of this Appendix was presented:

- **Title:** Scalability evaluation of a Modbus TCP control and monitoring system for Distributed Energy Resources.
  Authors: N. Rodríguez Pérez, J. Matanza, G. López, and V. Stojanovic.
  Conference: IEEE PES International Conference on Innovative Smart Grid Technologies Europe - ISGT Europe 2022, Novi Sad (Serbia). 10–12 October 2022.
  DOI: `https://doi.org/10.1109/ISGT-Europe54678.2022.9960319`

Appendix B includes some relevant information for the ICT SRA of Case Study B carried out in Chapter 4. It provides an overview of the wireless M-Bus protocol, how the

transmission medium was modelled in OMNeT++, and a comparative analysis of different propagation models that justify the model used. The following conference articles related to the content of this Appendix were presented:

- **Title:** Scalability analysis of a wireless M-Bus system for smart metering and sensoring.
  Authors: N. Rodríguez-Pérez, J. Matanza, G. López, and M. Hajigholi.
  Conference: 15th IEEE PowerTech Conference - PowerTech 2023, Belgrade (Serbia) 25–29 June 2023.
  DOI: `https://doi.org/10.1109/PowerTech55446.2023.10202977`

- **Title:** Model the Path: Impact of Propagation Models on the Scalability of a Wireless M-Bus Sensoring System for Smart Grids.
  Authors: N. Rodríguez-Pérez, J. Matanza, and G. López.
  Conference: IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGrid Comm), Glasgow (UK), 31 October–3 November 2023.
  DOI: `https://doi.org/10.1109/SmartGridComm57358.2023.10333969`

Appendix C describes how the percentage of solar PV distribued generation for the year 20230 in Spain was estimated based on public sources of information. This percentage was used to include distributed solar PV in area C of the PST-16 system used in the analaysis of MaDIoT 3.0 attacks in Chapter 5.

Finally, **Appendix E** provides the equivalence of the nomenclature used among EU H2020 projects and the Active System Management (ASM) report when referring to market-based coordination schemes between TSOs and DSOs.

The whole structure of the thesis together with the relationships between chapters and the appendices is presented in Figure 1.3

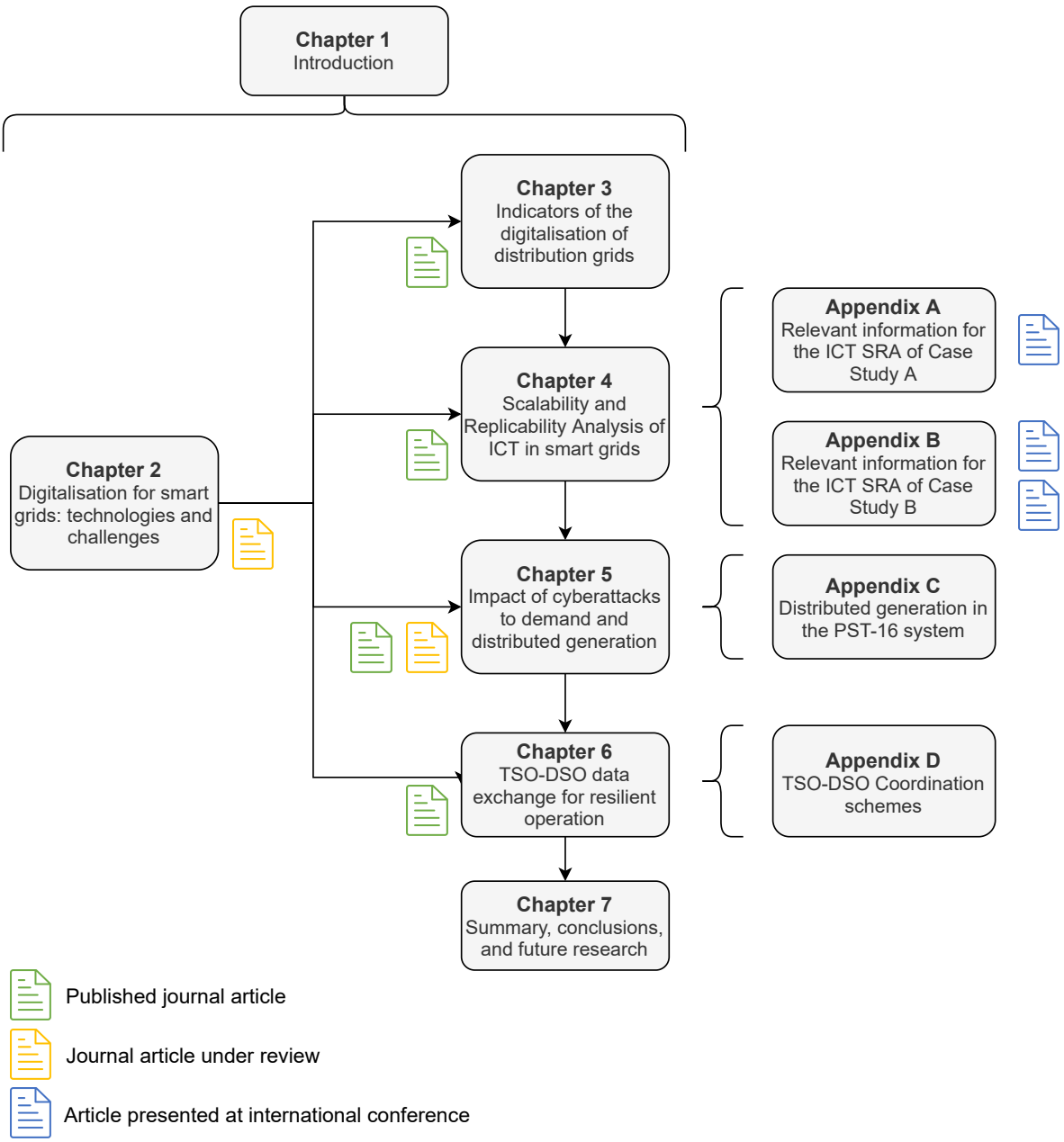

Figure 1.3: Structure of the chapters and their relations with the appendixes.

Chapter 2

Digitalisation for Smart Grids: technologies and challenges

2.1 Introduction

In recent years, the electricity sector has seen a significant shift towards digitalisation [11] to address the new operating challenges posed by the electrification of energy demand and the increasing penetration of DER and Renewable Energy Sources (RES) due to the ongoing energy transition. According to [12], approximately 18% of the total investment needed for decarbonisation in Spain is expected to be allocated to the digitalisation of the electricity system, which increases the pressure on the expected performance of the investments.

This digitalisation involves the widespread implementation of sensors and actuators, connectivity, and data processing technologies. Sensors and actuators allow the monitoring and operation of the grid remotely or in an automated way; the connectivity of these devices, enabled by communication technologies such as fiber optics or 5G, makes it possible to overcome barriers of data volume and time [13]; and data processing technologies, such as the cloud, Big Data, or Artificial Intelligence (AI), are essential for the development of smart grids [14] capable of processing the massive amount of data collected for decision making. In general, the large volume of data changes how information is obtained, analysed, and used, emerging new roles in companies, such as the Chief Data Owner (CDO), the Chief Information Security Officer (CISO) or data scientists, and requiring the development of a strong digital culture.

This chapter discusses the core impact of digitalisation on DSOs: on its organisation model, customer impact, and on grid processes and asset management. As the actors in the power sector are interconnected, the systemic impact of digitalisation must also be considered.

Since a wide range of technologies are involved in this transformation process, each offe-

ring unique opportunities and challenges, it is not always clear where these technologies add value for DSOs. For this, the main technologies are identified in this chapter and mapped against their main potential applications in the electricity distribution sector. Technologies such as digital twins, inspection and immersive technologies, AI, or Internet of Things (IoT) can transform the monitoring of Low Voltage (LV) networks, predictive maintenance, optimise investments and planning activities, or increase labour productivity, among others.

However, digitalisation also poses some challenges in terms of cybersecurity, for the core processes, and for the electric power sector in general. These challenges must be properly addressed to fully leverage the advantages and benefits of new technologies.

This section is structured as follows. Section 2.2 presents the pillars that support digitalisation in the electricity sector; Section 2.3 discusses the impact of digitalisation throughout the value chain of electricity distribution, distinguishing between the core and the systemic impact; Section 2.4 provides an overview of the applications of the main technologies that are being considered by Distribution System Operators (DSOs). Finally, Section 2.5 discusses the challenges that digitalisation brings to electricity grids, together with some recommendations to address these, and Section 2.6 draws the conclusions of the chapter.

2.2 Digitalisation pillars

In recent years, the electricity sector has seen a major shift towards digitalisation with the widespread installation of smart meters in many countries: more than 1.2 billion smart meters have been installed worldwide (Europe accounting for more than 123 million smart meters) [15]. This has enabled many DSOs to use big data techniques and Machine Learning (ML) algorithms to gain valuable insights from smart metering data [16], while also allowing consumers to access their consumption data with greater ease.

Apart from smart metering, many DSOs are currently deploying advanced supervision sensors in low voltage feeders [17], improving the detection of technical and commercial abnormalities, and Phasor Measurement Units (PMUs), which improve system control and monitoring [18], [19]. However, in general, distribution networks are not yet sufficiently digitalised to cope with the massive integration of DER that is expected.

Digitalisation of power distribution grids is mainly based on three key pillars: sensors and actuators, which are necessary to monitor and control the grid; connectivity, related to the ICT implemented for the communications of sensors and actuators with other systems; and data processing, related to the exploitation of the data collected.

Together with these, a fourth element for the digitalisation of distribution grids can also be considered: the digital culture of the DSO. The implementation of new digital solutions in the grid and the adoption of cybersecurity measures in all DSO activities can be made easier if the DSO hires digital professionals, provides its personnel with digital training and

the necessary tools, and allows customers to interact digitally. The DSO's digital culture can either facilitate or impede the implementation of technical solutions.

These pillars of digitalisation show a high level of interdependence, as shown by Figure 2.1; a significant development of one pillar usually requires an equivalent development of one of the others, increasing the number of use cases and applications of digitalisation. The deployment of a large number of sensors on either new or existing assets may necessitate the adaptation of the communications infrastructure necessary for collecting the data, as well as an increase in the computing and storage capacity of the servers responsible for processing and analysing the data. In terms of digital culture, the DSO should guarantee that the personnel involved have the appropriate tools and training to make the most of and maintain the new infrastructure.

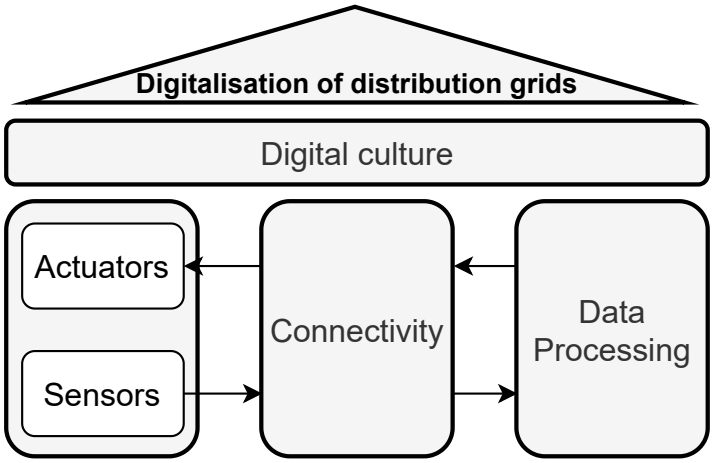

Figure 2.1: Pillars of digitalisation of power distribution grids.

2.3 Impact of digitalisation on the electricity distribution sector

The impact of digitalisation in the electricity distribution sector can be divided into two types: core impact and systemic impact. The core impact includes the effects that digitalisation has on the three main components of the value chain of a DSO: organisation, customer relations, and processes and asset management [20]. On the other hand, the systemic impact includes cybersecurity and risk management, which are aspects that are shared by all stakeholders in the electricity sector and require coordination and collaboration to take advantage of the benefits of digitalisation in a safe way.

2.3.1 Core impact

Impact on the organisational model

According to the Spanish Energy Club, digital transformation impacts companies in five key areas [21]: digital culture and leadership, skills and talent attraction, new ways of working, digital labour and workforce, and value creation.

To begin with, **digital culture and leadership** that promote a worker-centred perspective must be established. To achieve this, three elements are necessary:

- *Digital leadership* [22]. To adapt to the digital era, it is important for organisations to undergo restructuring. Leaders should place importance on the need for digital change and companies should take advantage of digital opportunities by motivating their teams and initiating projects. Additionally, employees should prioritise creating value rather than only pursuing personal goals.

- *Elimination of silos* [23]. It is essential to create teams that are multipurpose, non-hierarchical, and have the authority to manage projects from start to finish, thus moving closer to an agile work system.

- *Breaking through risk aversion*. Digital technology enables the ability to carry out small-scale demonstrations with a minimal financial risk if unsuccessful, yet still potentially yielding valuable results and experience.

Digital culture and leadership can be better achieved by attracting **digital talent**. Companies must be able to answer four key questions (*What?, Who?, Where?, How?*) when recruiting such personnel [24]. First, a thorough examination of the expertise needed for each job must be done (*What?*). Then, the company should fully understand the digital profiles available in the market (*Who?*), which nowadays is a global market. Companies should pay attention to indicators that demonstrate whether the sector (*Where?*) is conducive to the growth of this type of talent, such as the start-up environment or the appeal of the location. To answer the question ”How?”, companies must understand what motivates digital profiles and focus on their interests. Apart from attracting new talent, the capabilities of existing employees should not be disregarded. Training programs should be implemented to improve the skills of employees involved in digital projects and provide them with continuous learning opportunities.

Digitalisation also involves **new ways of working**. To exploit the advantages offered by digitalisation, companies must improve their flexibility and focus on creating value through collaborative and agile approaches to work [25], such as Scrum or Design Thinking [26].

The **digital workplace** redesigns processes to maximise productivity and prioritise employee experience [27]. This transition has been accelerated amid COVID-19. The adoption

of a digital workplace brings great benefits [28], [29]: improved productivity, better acquisition and retention of talent, higher level of innovation, and optimised costs.

Finally, it is crucial to have a culture that is dedicated to generating value beyond individual objectives. To achieve this, it is important to continuously measure the progress of the digitalisation process in order to enhance credibility and facilitate change management.

Customer impact

The new type of electricity consumer is adopting technologies that impact the electrical infrastructure (Electric Vehicle (EV), DER).

This culminates in the figure of the *prosumer*, who is able to generate, store and sell their energy to the grid [30]. The new business model for power grid agents will have to provide control, flexibility, and simplicity to these customers [31], [32].

The development of Virtual Power Plants (VPPs) [33] or the development of blockchain technologies for energy trading [34] could promote the provision of system services by customers. These services, when needed, could occasionally help DSOs operate more efficiently and safely without having to upgrade the grid infrastructure.

Impact on electricity grid processes and asset management

Electricity grids are made up of a wide variety of distributed devices, such as protections, smart meters, and transformers. For a long time, the connection of these assets has been progressive. An illustration of this is the introduction of Power Line Communications (PLC), which allowed the development of Advanced Metering Infrastructure (AMI). Digitalisation has the potential to enable the full integration of the assets of the electricity distribution network, improving operations and asset management in four main areas [21]: planning and investment, operation, maintenance, and asset life cycle.

The way in which digitalisation can affect each of these areas is briefly described in the following.

- **Planning and investment**. The electric power sector should consider how to develop new infrastructure to meet increasing demand, abrupt changes in consumer behaviour, or the connection of DERs. Digitalisation can help in the development of a planning activity that quickly adjusts and shifts to new trends and manages uncertainty by forecasting future scenarios, improving investment planning and decision making.

- **Operation**. The increasing penetration of DER results in greater variations in demand patterns and the possibility of bidirectional power flows that make it more difficult to operate the grid safely. The interconnection of assets through IoT will enable a more efficient operation. Grid operation will be much more automated through autonomous

decision-making systems, drastically reducing the response time in the event of incidents. Smart meters and network monitoring will provide real-time information to improve the Quality of Service (QoS) through the autonomous detection and localisation of faults [35], non-technical losses [36], and anomalous events in the network. By automating the response to incidents and contingencies, the variations in load flows and voltages derived from load disconnection problems, converters, or lines, would be reduced.

But digitalisation will not only have an impact on the remote operation of the grid. Field workers are highly dependent on process coordination, as they work in remote areas and under constantly changing conditions. As a result, the useful work performed on a working day corresponds to a medium-low percentage in relation to its duration. A digitalised workforce relies on digital technologies to improve productivity, as well as to operate in a fault-free and safe environment.

- **Maintenance**. It is possible to estimate when assets are likely to malfunction by using predictive maintenance, which can lead to an increase in asset productivity (i.e., utilisation) and availability, as well as a significant reduction in maintenance costs [37], [38]. The combination of Big Data, AI, and IoT will further improve predictive maintenance [39] by keeping track of Key Performance Indicators (KPIs) of assets, such as the Mean Time Between Failure (MTBF) or the Mean Time To Failure (MTTF) [40].

  In addition to this, the development of methods to control and monitor the growth of plant masses would increase efficiency, as it allows a more precise and optimised monitoring of vegetation growth around electrical infrastructure, thus avoiding possible incidents.

- **Asset's life-cycle**. Digitalisation can increase the profitability of end-of-life assets by reducing costs and minimising risks associated with asset abandonment processes. This could be achieved primarily through intelligent and unified management of the data generated during the life of the assets [21].

2.3.2 Systemic impact

The correct operation of the electricity system is achieved thanks to the cooperation of the different actors. The Smart Grid Conceptual Model (SGCM) developed by NIST [41] presents the interaction of up to seven domains: markets, operations, services provision, transmission, distribution, generation, and customer domain. The generation domain can be divided into bulk generation and DER. This last one is considered as a customer by the DSOs. Considering this, the main actors involved in the power sector and their communication and electrical flows are shown at a high level in Figure 2.2. In it, the service provider actor

refers to any entity that provides energy-related services such as energy and flexibility trading, balancing, DER aggregation, etc. The physical, cyber, and strategic connections within the power sector are evident, so the impact of digitalisation is not unilateral.

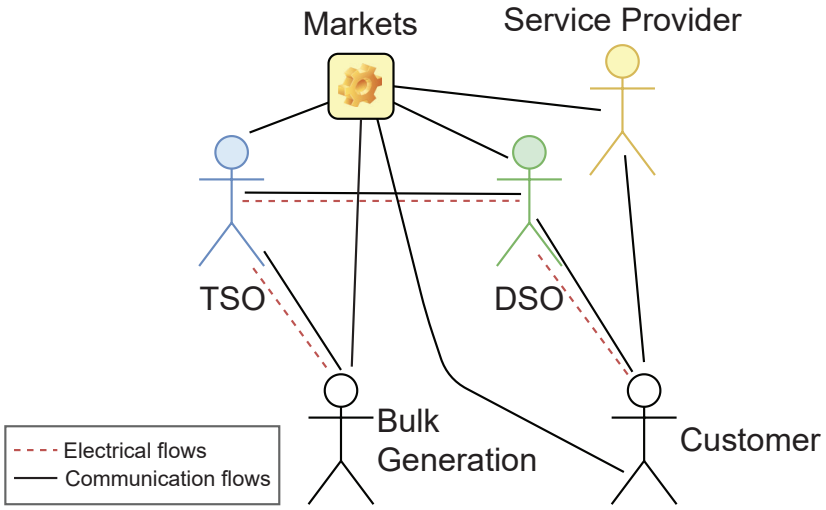

Figure 2.2: Interactions between electricity system actors. Based on the Smart Grid Conceptual Model by [41]

This interconnection between the actors in the power sector (both in the electricity and communication layers) makes cyber-resilience a major issue for the electric power sector. It also requires that the interconnected actors apply the same security levels to their processes. Digitalisation causes the expansion of the attack surface, creating new security risks that can be taken advantage of in a cyberattack. One of these risks is caused by the combination of Operational Technology (OT) and Information Technology (IT) technologies, which adopt different security measures, for the operation of the system. For example, a cyberattack on the IT environment can have a consequent impact on the OT environment [42].

The failure of a digital system or a cyberattack on an actor (including customers) can have a cascading effect on the entire electricity system (or parts of it) [43], causing blackouts with serious economic consequences. To achieve cyber resilience in the electric power sector, all stakeholders must work together and develop collective strategies.

2.4 Key technologies and their applications

This section examines, at a high level, the potential of technology to improve the fundamental activities and asset management of DSOs. Table 2.1 summarises the main applications of the key digital technologies in distribution grids.

Table 2.1: Summary of the main applications of key digital technologies in distribution grids.

	Digital twins	Inspection technologies	Immersive technologies	Big Data, AI, and Cloud	IoT	Blockchain
Optimisation of investment activities	X	X	X	X	X	
Predictive maintenance	X			X	X	
Dynamic and flexible planning	X			X	X	
LV network monitoring		X		X	X	X
Labour productivity and sustainability		X	X	X		X
Vegetation management		X	X	X		
Contingency analysis and incident response				X	X	X

2.4.1 Digital twins

A digital twin is a digital representation of a physical entity that uses platforms and two-way data exchanges to accurately reflect its real-world behaviour [44], [45]. Due to its complexity, the application of this technology by DSOs is mostly in the demonstration phase [46]. Digital twins would mainly add value to the following three activities:

- *Optimisation of investment activities*: Digital twins enable real-time monitoring of equipment quality [47]. This technology not only allows for continuous observation of asset and process dynamics but also makes it possible to detect unmeasured factors. As a result, decisions can be made about replacing equipment or improving processes, which can lead to savings in cost and time.

- *Predictive maintenance*: Through simulations and data collection, digital twins can be used to develop predictive maintenance strategies [48], [49]. Machine learning al-

gorithms, trained with these simulations, can improve the prediction of component failures, thus allowing for proactive maintenance interventions.

- *Dynamic and flexible planning*: The predictions and forecasts generated by the digital twins allow for dynamic and flexible planning [44], which is essential for preparing for the future grid landscape. Multiscenario simulations, taking into account the growing presence of DER [47] and customer participation in power markets, can help identify weak points in transmission and distribution systems that should be taken into account when creating resilient plans [50]. These models, combined with analytics, can systematise, automate, and simplify the decision-making process in planning activities.

2.4.2 Inspection technologies

Inspection technologies are those that allow the remote visual monitoring of the grid infrastructure. Unmanned Aerial Vehicles (UAVs), Laser Imaging, Detection, and Ranging (LIDAR) or thermal cameras are some inspection technologies that are increasingly being used in distribution grids for the following activities:

- *Optimisation of investment activities*: This technology eliminates the need for physical visits, thus reducing both time and paperwork. Additionally, they allow remote identification of land-related characteristics, facilitating decision-making processes for grid expansion or new infrastructure projects.

- *LV Network monitoring*: Digitalisation has a significant impact on the monitoring of LV networks, allowing greater surveillance and detection of irregularities. Thermal cameras can be used to identify overheated transformers [51], while UAVs can be incorporated into regular grid operations by using them for maintenance tasks without having to be physically present, specially in LV orverhead lines in rural areas.

- *Labour productivity and sustainability*: The use of inspection technologies in terms of labour productivity and sustainability is remarkable. UAVs are becoming a major factor in automating asset inspection and improving worker safety in difficult conditions, reducing the need for personnel displacement. This not only increases productivity but is also in line with sustainability objectives.

- *Vegetation management*: Vegetation management is a key factor in ensuring grid reliability, mainly in rural areas where overhead lines are more common. LIDAR systems, satellite technology [52], and UAVs [53] can be used together to create a 3D model of the surrounding vegetation. This could help to reduce the risk of accidents during maintenance activities and reduce the number of electrical faults caused by vegetation.

2.4.3 Immersive technologies

Immersive technologies, such as Virtual Reality (VR) and Augmented Reality (AR), offer a new way to visualise, monitor and work on the grid infrastructure. These technologies have the potential to increase situational awareness, facilitate real-time decision-making, and foster a more intuitive engagement of workers with data. More specifically, immersive technologies can be useful in the following contexts:

- *Optimisation of investment activities*: Similarly to digital twins, immersive technologies facilitate the evaluation of the condition and performance of grid equipment (e.g., using augmented reality to monitor overhead lines sag [54]). Decision makers can use this capability to identify the most suitable times for upgrades or replacements, helping to ensure that resources are allocated efficiently and that grid maintenance is cost-effective.

- *Vegetation management*: In field visits where the use of UAVs is not sufficient, the use of immersive technologies can provide greater security to the process through remote support and step-by-step guidance for the workforce.

- *Labour productivity and sustainability*: Immersive technologies offer a broad range of applications to enhance the efficiency and sustainability of field operations. AR technology provides many opportunities, from scanning QR codes on a smartphone to get instructions for maintenance tasks to using augmented vision through wearables [20], such as smart glasses, which allow operators to work hands-free while receiving remote support, thus reducing the risk of the most dangerous tasks [55]. Furthermore, by equipping these devices with geolocation systems, operators can be tracked in real time when working in remote areas. With regard to VR technology, workers can be trained in secure virtual environments where they are not exposed to high voltages, overcurrents, or falls from high heights.

2.4.4 Big Data analytics, artificial intelligence and cloud computing

Big Data analytics (or just Big Data) refers to computational techniques and procedures that allow the analysis of large volumes of data. The deployment of sensors and actuators in the distribution grid involves the massive collection of data that has to be processed using Big Data techniques to make decisions in different aspects and take full advantage of the digital infrastructure implemented. Related to Big Data, AI applications are increasing the insights extracted from collected data. AI encompasses various concepts, including ML and Deep Learning (DL). ML techniques make use of mathematical and statistical algorithms to uncover patterns and relationships in a dataset that may not be easily identifiable using traditional methods. This allows for more accurate predictions.

However, this requires large computing capabilities and the correct integration of the data collected. This is where the cloud adds value. The cloud allows the hosting and overseeing of a company's virtual infrastructure while seamlessly integrating all its resources.

Services such as Google Cloud, Amazon Web Services, and Microsoft Azure allow the integration of IoT sensor data in real time, allowing constant monitoring of the network. Furthermore, this technology improves the scalability of processes and virtual infrastructure and can provide access to AI, blockchain, VR, and quantum computing applications. However, the shared responsibility models of cloud providers should be considered. System operators should ensure that they follow a model that preserves privacy, data, algorithms, and connections with other clouds before moving large parts of their ICT into the cloud [56], [57].

Recently, as a complement to cloud computing and thanks to virtualisation technologies, the concepts of Edge and Fog computing have emerged. These concepts shift the computational load from the cloud to the connected devices that generate the data or that are closer to the sources. These novel architectures address the need to minimise the time spent transferring data to the cloud, processing it, and transmitting the results by processing the data locally, reducing, at the same time, the need for large-scale connectivity with central systems.

- *Optimisation of investment activities*: The use of Big Data makes it feasible to include variables in investment models and assessments that could not be quantified before. For example, variables that refer to environmental safety (e.g., vegetation expansion). Furthermore, the use of historical data would allow to predict administrative processing times for construction activity and costs.

- *LV Network monitoring*: These technologies must seamlessly integrate with IoT technologies. The huge amount of data generated by IoT devices will require the use of these technologies to process the data in real time to run applications for autonomous detection, location, and response to faults [58] and anomalous events in the network. By using Edge computing, sensors' data can be processed at secondary substations to detect, locate, and classificate LV faults, and for state estimation, fraud detection and power losses accountability [59], [60]. Additionally, cloud computing has enabled the integrated management of the LV network [61].

- *Predictive maintenance*: In order to process the large amount of sensor data, distributed computing may be necessary. Edge computing could be used to run predictive maintenance algorithms locally [59], [60], whereas Cloud computing allows access to large ML and DL maintenance algorithms. The Cloud provides an integrated management of all data through Key Performance Indicators (KPIs), which allows for centralised control of all deployed resources, saving time and money. Additionally, Big Data can use historical data or reports to recognise the typical behaviour of assets and calculate the risk of deviation from the baseline. These data are then fed to the ML algorithm,

which is responsible for forecasting changes in the state of the assets based on sensors' data [58], and for automating decision-making based on the history of state changes.

- *Dynamic and flexible planning*: These technologies enable the systematisation, automation, and simplification of decision-making processes in planning activities.

- *Automation and optimisation of contingency analysis and incident response*: The integration of IoT with the LV network enables a change to a much more automated system. This is further enhanced by the use of Big Data and ML algorithms, which will provide significant improvements in the analysis of contingencies [62], [63]. This combination of autonomous decision-making systems and real-time communications networks leads to a marked improvement in contingency analysis, allowing faster incident detection and autonomous incident response, thus reducing the time taken to replenish incidents. It would be possible to achieve uninterrupted supply through the development of incident prediction algorithms.

- *Vegetation management*: Through the use of Big Data, it is possible to process the necessary information from different sources to develop, using AI algorithms, predictive models of the growth of the vegetation mass.

- *Labour productivity and sustainability*: Cloud computing enables the management of the entire workforce from a single location. By combining it with Big Data analytics, it is possible to optimise and integrate the management of field resources. Advanced analytics can be used to predict risks in real time and alert field workers through their smartphones or smart glasses. Geolocation systems can be used to track the position of all resources, which, when combined with advanced analytics, allows for dynamic and efficient task allocation to workers and the optimisation of routes for increased productivity.

2.4.5 IoT

The digitalisation of the electrical distribution grid involves increasing its level of automation, which, in turn, depends on the widespread deployment of sensors and actuators with connectivity. The IoT is a further step in connecting assets and creating a real-time communication network. IoT is not a technology, but a widely used term in industry that encompasses a multitude of sensing, actuation, and communication technologies. It provides versatility and scalability, achieved through the combination of various communication technologies and physical media. This can range from using the power grid itself through PLC to using fiber optics or 5G technology in critical assets to achieve low latency [13], or using Low Powered Wide Area Networks (LPWANs) [64] to reach the most remote and isolated assets while reducing maintenance due to their low power consumption. To take full advantage of

this connectivity, it is usually necessary to develop router communication equipment that is specifically designed for electrical services, as the deployment conditions (e.g., secondary substations, power lines, etc.) can be challenging.

- *LV Network monitoring*: The use of communication technologies has enabled the provision of intelligence to assets through the IoT. This is made possible by using remotely managed meters and actuators (e.g., breakers, switches, tap changes, etc.) and the real-time monitoring of the network through sensors.

- *Predictive maintenance*: The IoT enables real-time tracking of operations through asset monitoring. By providing connectivity between sensors (temperature, humidity, vibration, power, or battery life) and maintenance systems, it is possible to process the data to evaluate the reliability of the deployed equipment.

- *Automation and optimisation of contingency analysis and incident response*: The full interconnection and monitoring of all grid assets through IoT devices and the use of 5G as communication technology allow real-time connection among them, reducing the delay in responding to critical incidents.

- *Planning and investment*: The continuous monitoring of assets through IoT provide a real-time understanding of the status and reliability of these assets, thus allowing optimal production planning and agile, secure and accurate decision-making.

2.4.6 Blockchain

Blockchain is a Peer-to-Peer (P2P) technology that facilitates decentralised data storage, sharing, and processing between participants in a network [65]. It consists of blocks, interconnected through cryptographic methods, that contain data, information, or transactions. Most applications of blockchain in the electricity sector focus on P2P energy trading [65]. However, this technology can also add value to the operation of distribution grids:

- *LV Network monitoring*: The use of blockchain can enable a secure and fast transaction settlement to manage grid constraints [65]. If an anomaly is detected, maintenance can be facilitated and paid instantly and automatically through Smart Contracts, allowing faster response times.

- *Automation and optimisation of contingency analysis and incident response*: The effect of increasing penetration of renewable energy and DER on grid stability requires new services and flexibility requirements [66], either to regulate electricity demand to better match supply, or to compensate for backup supply sources that can respond quickly in times of shortage. Blockchain technology can be used to ensure the balance between supply and demand by automating transactions and settlements between

agents. However, due to the disruptive nature of this new model, the integration of blockchain is, by the moment, mostly through pilot programmes with a selected group of participants and focused on specific functional applications.

- *Labour productivity and sustainability*: Smart contracts can be used to automate the supply chain of spare parts and maintenance equipment [67], thus making network infrastructure maintenance more efficient. When the predictive maintenance algorithm detects an imminent failure of an asset, the necessary equipment for its maintenance can be purchased automatically. This improves response times and maintenance productivity, as the dynamic task allocation algorithm can simultaneously alert the workforce about the failure.

2.5 Challenges of digitalisation

Despite the advantages and applications of digitalisation, it can also present some challenges for system operators.

2.5.1 Challenges in core processes and asset management

In order to make the most of the implementation of IoT devices and incorporate their data into operational and planning processes, DSOs may choose to create their own communication network (for example, using PLC or fiber optic technologies) or rent the infrastructure from a communications service provider. Any new implementation that requires ICT should be evaluated in terms of scalability and replicability, not only from a functional perspective (i.e., the solution performs as expected), but from an ICT perspective (i.e., the ICT infrastructure does not saturate). As mentioned previously in this chapter, the digitalisation of distribution grids involves the progressive deployment of a large number of devices (sensors and actuators). Before this deployment, DSOs should evaluate the scalability and replicability of the ICT that provides the connectivity between devices and data storage and processing systems. This means making sure that the infrastructure, without major updates, will be able to comply with the requirements of the different applications (for example, in terms of latency, throughput, etc.) when increasing its use. In addition, due to the large extension of distribution grids, DSOs should implement cost-effective solutions with a large replicability potential or whose elements provide a variety of different configurations (for example, devices offering wide interoperability).

A proprietary ICT infrastructure, although providing a great level of independence and control over communications, can be an insufficiently scalable and costly endeavour in terms of Capital Expenditure (CAPEX), while renting a third-party infrastructure could provide more scalability but also an increase in the Operational Expenditure (OPEX) and dependability on third parties.

A similar decision must be made regarding AI algorithms and Big Data, which require large computing and storage capacities; companies can choose between using public cloud computing providers, where the Shared Responsibility Model (SRM) of the provider should be taken into account, or using an on-premise cloud solution, which present more difficulties in terms of infrastructure scalability, cybersecurity, and expenses.

From an economic and technical point of view, the complete monitoring and automation of the distribution grid is not efficient. Solutions such as the implementation of edge computing in all secondary substations, the monitoring of all electrical equipment for maintenance purposes, or an accurate digital twin of all assets are unsustainable. DSOs should perform a preliminary assessment of assets to prioritise the most critical ones and implement the digital technologies that have a greater impact on the reliability and QoS metrics. For this, DSOs need to measure the digitalisation of their grids to draw conclusions about its impact and the cause-effect relationship between digitalisation and performance.

Finally, there will be some challenges to increase the digital culture of DSOs. Implementing the digital field force for distribution grids will present some difficulties. In addition to the expenses related to the purchase of technologies such as mobile applications, geolocation, immersive, and inspection technologies, DSOs will have to face some resistance to change from employees and teach them to use these tools proficiently and in a cyber-secure manner. In this regard, measuring digital culture through indicators would help DSOs identify the aspects to further work on.

2.5.2 Challenges in the electric power sector

Despite already being a highly interconnected system, digital technologies have increased the level of interdependence between the different actors and the risk of cascading effects, both in the physical (electricity system) and cyber (ICT) layers. To minimise it, it is essential for all the actors involved in the electric sector to collaborate, operate in a coordinated manner, and share best practices and incidents as soon as they occur. This should be accompanied by the development of flexibility mechanisms.

However, to encourage investment in digitalisation and the development of new solutions in the electricity sector, regulatory measures are needed [68]. Regulatory sandboxes could be used to encourage the use of innovative digital technologies to test and develop different flexibility services while maintaining regulatory oversight [69].

One challenge that the electric power sector is currently facing is interoperability. Interoperability can be defined as the ability of systems to exchange information and make use of that information. For this, the use of standards is key.

In Europe, the ICT implemented can be different from one area to another. In many cases, for the communication between Transmission System Operators (TSOs), DSOs, and other actors, custom-made platforms or protocols are developed to facilitate the integration of

the different systems. In other cases, existing platforms that support different standards and protocols, or that provides an API that can be easily adopted, are used.

To address this challenge at an European level, the BRIDGE initiative has proposed to develop a conceptual European data exchange model that involves elements of the platforms developed/used like functionalities, standardisation needs, etc. [70]. The use of different types of platforms in EU innovative projects so far makes it necessary to define the 'interoperability of platforms' [70] and identify those platforms with replicability and scalability potential at a European level, while ensuring General Data Protection Regulation (GDPR) [71] compliance and data owner's control over their data. In addition, these platforms should also comply with EU regulation including data exchange, such as Regulation 2017/2195 [72], Regulation 2017/1485 [73], and Regulation 2016/1388 [74]. The interoperability of platforms, together with data handling (data ownership, access, quality, and harmonisation), are considered the main challenges to address in this regard.

To address these challenges, the collaboration of the different stakeholders in the development of use cases [75] can be key. Regulation should take into account the emergence of new agents in the electricity sector (e.g., aggregators, energy communities, etc.) and clearly define their roles and responsibilities, armonising the approach to define roles in the Harmonised Electricity Market Role Model (HEMRM) [76], and including data management.

Finally, the adoption of Common Information Model (CIM) as the main information model can help to increase interoperability between systems within the same organisation and with other actors of the sector. However, more collaboration in the development of CIM extensions is needed [70].

2.5.3 Challenges in cybersecurity and data privacy

Digitalisation in the electricity sector will increase the cyberattack surface and involve the management of a huge amount of data, in some cases including personal data, that must be properly secured. The utilisation of cloud solutions to manage these volumes of data could lead to less control over it (e.g., sensitive data not encrypted or anonymised) and an increase in the number of data breaches, which could have an effect on personal data protection. It is important to know the objective and final use of each piece of data collected, as well as if it involves personal data, so that the proper measures can be adopted to avoid leakages and comply, in Europe, with the GDPR.

The extensive use of IoT devices could be a major security risk [77], as these devices may not have any security measures in place [78] or adhere to different regulations (i.e., a non-aligned / fragmented legal framework) [79]. IoT devices deployed at the consumer level may be the target of cyberattacks with the objective of disrupting the normal operation of the power grid. This type of attack is called MaDIoT attack [80]. In addition to demand, the growing integration of DER also broadens the scope of potential attacks [81]. An attacker

compromising DER could affect the operation of the system [82]. In general, IoT devices in the demand and DER controllers can be a security challenge for grid operators because of two reasons:

- These devices have a deficient cybersecurity infrastructure [83] and, in the majority of cases, no physical security infrastructure.
- Controlling Advanced Persistent Threats (APTs), phishing, and other similar risks is more challenging than usual, since the infrastructure, public or private, is usually not owned by the distributors. For example, electric vehicle charging points are not continuously monitored by DSOs [84], [85].

At the moment of writing this thesis, in Europe, the European Union Agency for Cybersecurity (ENISA) is in the final stage of development of the European Cybersecurity Certification scheme (EUCC) [86] which will set some minimum security requirements for these devices.

In addition to this, collaboration between DSOs, TSOs, and other entities is essential to achieve systemic resilience. To create collective situational awareness and minimise the risk of cascading failures, detailed real-time information sharing and notification about incidents is necessary, as well as a coordinated response. To this end, European normative is evolving to encourage information sharing and cyber incident communication initiatives, such as the Digital Operational Resilience Act (DORA) [87] for the financial sector and the Network and Information Security 2 (NIS2) Directive [88]. NIS2 Directive, which includes the energy sector within its scope, introduces more security requirements, the obligation to report incidents to the designated national entity, and more extensive enforcement measures.

Focused on the electricity sector and the high level of interconnection of its stakeholders, the Network Code on Cybersecurity [89] [1] sets specific measures to address cybersecurity of cross-border electricity flows. It establishes minimum cybersecurity requirements, cross-border risk management processes, cybersecurity controls, a framework for cybersecurity information sharing, and the delineation of roles and responsibilities for the stakeholders involved, among other measures.

Nevertheless, just the compliance with cybersecurity regulation does not guarantee complete protection from cyberattacks. The fast pace of digitalisation in the electricity sector makes it difficult for regulation to keep up with the latest cyber threats and vulnerabilities. Hence, it is crucial to adopt a resilient and adaptable mindset, along with effective approaches to address systemic cyber risks.

In the past, cybersecurity was frequently overlooked compared to other risks and was usually under the responsibility of the IT department. This is changing. In electricity distribution, where reliability of supply is essential, cybersecurity cannot be managed independently. It must be integrated with business risks and throughout the entire organisation [90].

[1] Currently in draft phase. Expected to be adopted by the European Commission in the first quarter of 2024.

To minimise the cybersecurity risks and increase cyber-resilience, DSOs should consider the following:

- **Defence in depth and end-to-end cyber-resilience strategies**. The idea of Defence in Depth (DiD) entails structuring the risk management strategy across various levels, so that if one is compromised, another level will be implemented to prevent the attack from accessing sensitive data.
  Regarding end-to-end cyber-resilience strategies, cybersecurity should be a priority for all levels of an organisation, from the business level to the functional level. It should be incorporated into the strategy plans at the corporate level, and into enterprise risk management at the business level. At the functional level, it is important to consider cybersecurity when designing systems and architectures.

- **IT and OT integration and cooperation**. IT and OT systems are substantially distinct and thus their security needs are also different. IT security is mainly concerned with confidentiality, while OT security is more focused on integrity and availability. This can lead to security issues, which are often compounded by the lack of coordination and integration between IT and OT systems, and by the inefficient integration of modern and legacy technology [91]. IT and OT environments should converge and collaborate in terms of cybersecurity. To maximise cyber resilience of the electricity system, the cyber risk management model must take a systemic approach and incorporate the IT, OT, and IoT environments.

- **Development of a strong cybersecurity culture**. Integrating cybersecurity into all aspects and processes is essential for the development of a strong cybersecurity culture. It is crucial to provide cybersecurity training to employees, which can be achieved through activities such as threat response simulations. Cybersecurity is everyone's responsibility, and this message should be emphasised at all levels of the organisation.

- **Adaptation to technologies**. The ever-evolving nature of technology presents a persistent difficulty in ensuring the cyber-resilience of systems. However, this technological advance is also beneficial. For instance, ML and AI algorithms can help to detect cyberattacks and enable proactive defence strategies. Furthermore, quantum computing will revolutionise the encryption landscape [92]. It is important that all actors in the electric sector are aware of these changes and work together to ensure the resilience of the system.

2.6 Conclusions

The digitalisation of the electricity distribution sector can provide several benefits to the operation of distribution grids, but also pose some challenges.

Digitalisation will affect the organisational model of DSOs, requiring the development of a strong digital culture and leadership, the attraction of digital talent, and the implementation of new ways of working. The emergence of prosumers and the increasing connection of DER could require the development of mechanisms for the provision of system services, such as congestion management, to efficiently operate the distribution grid without requiring costly grid upgrades. Furthermore, the deployment of sensors and actuators, widespread connectivity, and high-capacity data processing technologies will have a positive effect on operation and asset management. It will also have an impact at the sector level (systemic impact), due to the high level of interconnection of the actors in the power sector, requiring more collaboration and cooperation of these in the digitalisation process.

In addition to the impact of digitalisation along the value chain of DSOs, this chapter has provided an overview of how key technologies can optimise core processes and asset management activities.

On the one hand, many technologies are currently being progressively implemented by DSOs. IoT in combination with Big Data, AI, and cloud computing, would have an impact on most of the main DSO activities involving planning, monitoring, operation, and maintenance; while inspection and immersive technologies were identified to play a relevant role in improving the productivity of field tasks and maintenance.

On the other hand, more disruptive technologies, such as digital twins or blockchain, need further development and testing. Digital twins can constitute a significant advancement towards smarter grids, although their connection with the physical world is one of their main challenges to address. Regarding the blockchain, its use by DSOs would be carried out through very specific use cases; most of its applications focus on energy trading, which is usually outside the competence of these entities.

Additionally, the main challenges that arise as a consequence of digitalisation were discussed. Digitalisation of distribution grids, to be cost effective, will require highly scalable and replicable solutions from both the functional and the ICT perspective. How to perform such scalability and replicability analysis for ICT is discussed in Chapter 4. The wide range of alternative technologies will require a detailed analysis of which is the best option for specific use cases. To be able to choose the best technological option, DSO employees will have to be updated with the new trends and receive the proper training; this may raise some resistance to change. In addition to this, DSOs should also know how digitalised their current grid is (Chapter 3), so that the digitalisation process can be more effective technically and economically.

At the level of the electric power sector, the different entities will need to increase the interoperability of their systems and platforms. This is the first step to develop better collaboration and coordination schemes that minimise the risk of the cascading effect of failures or cyberattacks, and that allow for the implementation of new use cases. For this, clear roles and responsibilities regarding data should be defined, and more collaborative work on the development of common information models is needed. The standards that can be used for TSO-DSO data exchange are discussed in Chapter 6.

Finally, probably one of the greatest challenges of digitalisation is cybersecurity. Digitalisation expands the attack surface, and the large volume of data involved makes it challenging to manage them with the proper level of security and privacy. IoT devices of consumers could be compromised to cause blackouts in the power system (for example, MaDIoT attacks, whose impact is analysed in Chapter 5). These attacks could also involve control devices of DER, which present several vulnerabilities. Although some regulation has been developed in Europe, DSOs will need to go further when adopting security measures, as threats may evolver faster than the normative. For this, DSOs should develop and implement defence in depth and end-to-end cyber-resilience strategies, improve the integration and cooperation of the IT and OT deployed, promote a strong cybersecurity culture, and take advantage of the new technologies, such as AI, to improve their cybersecurity.

Chapter 3

Indicators of the digitalisation of distribution grids

3.1 Introduction

In Europe, the distribution of electricity is regulated: a National Regulatory Authority (NRA) defines the remuneration scheme for DSOs, including incentives and penalties, based on aspects such as quality of service, CAPEX, OPEX, etc. However, the increasing digitalisation of distribution grids towards the development of smarter, more reliable, electricity grids, together with the objectives of higher energy efficiency and penetration of renewables, are requiring the evaluation of how ”smart” the grid is becoming, or needs to become, for the ultimate achievement of these objectives.

In the last decade, there has been an increasing interest in defining key performance indicators (KPIs) to be used in the evaluation of the ”smartness” of the grid [93], [94], its reliability [95], its continuity of supply [96], the performance of smart grid projects [97]–[99], the situational awareness effects [100], and the evaluation of flexibility markets in distribution systems [101].

In Europe, this interest was reflected in Directive 2019/944 of the European Parliament [4], which establishes in Article 59.1 that the NRAs shall evaluate how DSOs perform regarding the development of a smart grid that allows higher levels of energy efficiency and renewable energy; this evaluation should be based on a set of indicators and published in a periodic report with some recommendations. In this sense, the EU Action Plan ”Digitalising the energy system” [2] set the intention of the European Commission to ensure an appropriate regulatory framework and to support the work of defining common smart grid indicators so that NRAs can monitor smart and digital investments. Indicators must be defined by NRAs in a consultation process with the DSOs to check the feasibility of the implementation and reduce the regulatory risk of lack of data to compute them.

In general, the existing literature about smart grid Key Performance Indicator (KPI) [93], [94], [97], [102] covers almost all the aspects that can be expected in a smart grid. However, most of them focus on the performance of the grid and not on the evaluation of the means and infrastructure implemented that drive that performance, which at this moment is becoming reliant on digitalisation. They do not offer a comprehensive perspective on the extent of digitalisation in DSOs nor facilitate a fair comparison in this regard. A more digitalised grid does not necessarily mean a better or "smarter" grid. Indicators that focus exclusively on the digitalisation of electricity distribution grids are needed to be able to draw solid conclusions about the impact of digitalisation in distribution grids, to have the possibility of assessing the cause-effect relation between digitalisation investments and grid performance, to improve the ability to integrate new resources, and to measure and compare the digitalisation efforts of DSOs in a clear and objective way, regardless of their size.

This chapter proposes a set of indicators specifically orientated to measure the digitalisation of distribution systems to assess the digital capabilities and infrastructure put in place to achieve the grid performance levels. These indicators were externally reviewed in terms of feasibility and potential available data by three subject matter experts from three Spanish DSOs, in their personal capacity (not as DSO representatives).

Since this work is the result of collaboration with EU DSOs, and the EU Directive 2019/944 has created the need for smart grid indicators in Europe, the target area of this chapter is Europe, although all the proposed indicators would be applicable to a non-European distribution utility, as they are use case and regulatory agnostic.

Instead of using categories related to the operation of smart grids, the indicators in this chapter are classified according to the pillars of digitalisation of distribution grids presented in Chapter 2. These indicators, in contrast to most KPIs in the literature, are aimed at evaluating the digitalisation measures and infrastructures implemented by DSOs, and not the resulting performance of smart grids and demonstrations' success.

This chapter is organised as follows. First, a benchmark of the indicators proposed in the state-of-the-art is provided in Section 3.2. Section 3.3 describes the key indicators proposed for the measurement of digitalisation of power grids. These indicators are classified based on the pillars for digitalisation, including digital culture. Section 3.4 discusses the usefulness and advantages of these indicators for DSOs and NRAs. Finally, the main conclusions are drawn at the end of the chapter.

3.2 State-of-the-art of Smart Grid indicators

There are different proposals of indicators to measure multiple aspects of electricity distribution networks. In addition to academia [93], various organisations have made significant efforts to promote digitalisation. These include the Joint Research Center (JRC) of the Euro-

pean Commission through its DSO Observatory [103], [104], DSO associations [102], EU-funded projects [105] and, outside Europe, by the U.S. Department of Energy [106], [107] and SP Group [94]. This section provides a comparison of these references, which represent different points in time, and emphasises the rationale behind the digitalisation indicators proposed in the following sections of this chapter.

Table 3.1 quantitatively compares how many indicators are proposed by the main previous work and how many categories or dimensions are used by them to organise the indicators. It shows that the number of categories is approximately the same, in the range of 6-8, whereas the number of indicators significantly varies. On the other hand, the 16 digitalisation indicators proposed in this chapter are organised in four categories.

Table (3.2) outlines the various categories that have been used in the literature, summarising their scope. Digitalisation is a factor that is applicable to all of these categories.

Starting with the one that defines the lowest number of indicators, SP Group [94] provides a unique "Smart Grid index" to measure the "smartness" of distribution grids that is calculated based on seven "dimensions" or categories. Although it can be assumed that these dimensions are assessed based on multiple indicators, [94] does not enumerate them and just presents the final index. Despite authors in [94] state that all the information used to calculate the index was extracted from public sources, there is lack of transparency on how the different dimensions are measured, how the final index is calculated based on these, and which public sources of information were used. In addition to this, one single index may be useful to benchmark DSOs at a high level, but it does not provide enough information on what can be specifically improved by DSOs, which are the differences between them, or if they need further investments on digital technologies. This can also be misleading; as this "smartness" is expressed as a percentage, it would be difficult to interpret a 100% score and if that would mean that there would not be margin to improve.

The report of the Office of Electricity Delivery and Energy Reliability of the U.S Department of Energy [106] presents 134 metrics to measure the implementation progress of the Smart Grid from an industry perspective. These metrics were identified, discussed, and evaluated in terms of relevance by more than 140 experts in the field. The metrics in [106] are not exclusively focused on DSOs; they also consider other stakeholders in the electricity distribution field (e.g., smart grid startup companies, customers, etc.). The application of these metrics would raise some issues: first, many of the metrics present significant uncertainties regarding data availability, how they would be measured, and their usefulness to the analysis, such as *Number of products with end-to-end interoperability certification*, *Number of new standards*, or *Number of households with home area network*; second, the number of metrics is very high, they involve different stakeholders, and many of them are difficult to measure. The data collection process from all stakeholders would require a very significant effort, which would have to be considered when defining a final set of KPIs.

Table 3.1: Number of indicators and categories per reference, and their main objective and characteristics.

Reference	No. of categories	No. of indicators	Objective	Main characteristics
Dupont et al. [93]	6	59	Evaluate the ”smartness” of the grid, including indicators related to information exchange, advanced sensors, and other digital infrastructure.	Output indicators. Not only involves DSOs. Some depend on size of utility.
SP Group [94]	7	1	Measure the ”smartness” of distribution grids with a single index.	Output indicators. Difficult to interpret the single index.
DSO associations [102]	8	58	Assess the performance of smart grids through 8 KPIs and 58 indicators.	Mainly output indicators, difficult to interpret (complex formulas).
Fotopoulou et al. [105]	4	23	Performance assessment of smart grids.	Output indicators. Some are difficult to measure.
EU JRC DSO Observatory [103], [104]	6	48	Technical characteristics and performance of European DSOs.	Input indicators not focused on digital infrastructure. Some depend on size of utility
U.S. Department of Energy [106]	7	134	Measure the progress towards the smart grid considering different stakeholders in the electric sector.	Mainly output indicators. Not only involves DSOs. Difficult to measure.
U.S. Department of Energy [107]	21	38	Measure the progress towards the smart grid.	Mostly output, but also input indicators. Some depend on size of utility.
This chapter	4	16	Measure the digitalisation level of electricity distribution grids, supporting EU Directive 2019/944	Input indicators focused on digitalisation, independent of technology and size of the utility. No complex formulas.

As a continuation of the previous report, the Pacific Northwest National Laboratory elaborated the Smart Grid Status and Metrics Report [107] for the U.S. Department of Energy. It makes the distinction between "build metrics", that describe attributes that support the smart grid, and "value metrics", that describes the value of an outcome of a smart grid. It considers 21 metrics with a total of 38 sub-metrics, discussing deployment trends, projections, and recommendations for the future. Despite some of these indicators evaluate digitalisation as an input (e.g., *Percentage of substations with automation*), the majority aim to assess performance (output) and some of them are based on absolute numbers and not percentages, making it difficult to compare DSOs of different sizes (e.g., metrics such as *Number of microgrids in operation*, *Total number of advanced measurement devices* or *Number of meters planned or installed*).

The DSO Observatory of the EU JRC [103] measures 48 indicators that provide a very detailed view on the technical characteristics and performance of DSOs in Europe, but without focusing on the digital capabilities and infrastructure. It shows the great amount of technical information that can be provided by DSOs. However, most of these indicators only provide a general view of the characteristics of the distribution network and are dependent on the size of the DSO. Indicators such as the *total km of network lines per voltage level*, the *total number of connection points*, or the *percentage of PV installations connected per voltage level* provide information on the electrical infrastructure but they cannot be used to objectively compare DSOs of different sizes between them. For example, a large distribution network would have more kilometres of lines, more connection points and, probably, more distributed PVs per voltage level than a small one and, despite this, it would not necessarily mean that the larger distribution network is "smarter".

Dupont et al. [93] propose 59 key performance indicators to assess the "smartness" of a smart grid, including some indicators related to information exchange, advanced sensors, and other digital infrastructure. Some of these indicators also involve other stakeholders apart from DSOs (e.g., *Number of customers served by ESCO's*, *Flexibility that aggregators can offer to other market players*, etc.) and, as in [103], others would not provide an objective comparison of DSOs (e.g., *Number of microgrids in operation*, *Number of EV charging points*, etc.).

Fotopoulou et al. [105] propose 23 indicators for system operators to assess the performance of smart grids. These indicators are divided into four categories: technical, environmental, social, and platform engineering indicators. Technical indicators comprise mainly quality of service indicators, such as *Technical losses, Voltage deviation*, or *Harmonic distortion*; Environmental indicators focus on indicators such as *Direct CO2 emissions*; The social indicator proposed aims to measure the *Adoption/acceptance of proposed strategies*; and the last category, the platform engineering indicators, aims to evaluate the performance of the software and algorithms implemented based on different aspects, such as *Average CPU usage*, *User interface friendliness*, or *Tool accuracy*. The indicators in this last category, al-

though strongly related to digitalisation, are mainly focused on the performance (output) of implemented digital elements (software, algorithms) and not the degree of implementation of such elements (input). In addition to this, it would be difficult to measure this category for all the processes of a DSO.

Finally, DSO associations [102] propose 58 indicators that are involved in the calculation of eight key performance indicators. The descriptions of the indicators are not very detailed, just providing some high-level examples of how they could be measured. An indicator that exemplifies this well is indicator 3.2 *Grid Reconfiguration*, where the following example to measure it was given: "*Effectiveness in fault prevention (with respect to a baseline) weighted according to the relevance of the area*". This definition poses multiple questions: Who defines the baseline? Is it the same for everyDSO? What method is used to assign weights? Is there a standard methodology to assess the relevance of an area? In addition to this, the weights applied to each indicator for the calculation of the eightKPIs are not specified, so their adequacy and interpretation once calculated are unknown.

As Table 3.2 shows, previous works mainly focused on the performance and expected outcomes of a smart grid; aspects such as DER penetration and integration, system reliability, and additional products, services, and markets, are considered by most references. What all the categories or dimensions have in common is that they are being currently addressed through the digitalisation of the network, but they do not provide simple and specific indicators to measure this digitalisation. They may provide an overview of how much a distribution network resembles a smart grid, but lack detailed information on how this performance or "smartness" is achieved. Not all indicators may be used to effectively and objectively compare different distribution networks between them, and, when it is possible, the comparison would just provide a benchmark of distribution networks and the objectives to achieve, but without really assessing what infrastructure would be needed. With the high investment in digitalisation of distribution networks that is taking place in recent years, this becomes essential to efficiently achieve a smart grid; it would not make sense to increase the deployment of technologies at the electricity distribution level if it would not improve the performance, resilience or reliability of the grid.

Therefore, a set of indicators that allow the assessment of the level of digitalisation of distribution networks is needed to complement the indicators proposed in the literature, fill the information gap regarding which are the digitalisation inputs, and expand their potential usefulness for both the DSOs and NRAs. The indicators proposed in the following section would contribute to this by:

- Focusing on measuring the digital infrastructure and capabilities of a DSO (input), at different levels, that may have an impact on performance metrics (output) such as quality of service, reliability, energy equity indicators, etc. Therefore, these indicators are conceived to be analysed together with performance indicators. This way, NRAs

would find it easier to provide recommendations to comply with article 59.1 of EU Directive 2019/944.

- Being independent of the size of the DSO evaluated, so they would allow a more objective comparison between networks.

- Being simple and clearly defined, most of them as percentages, without involving complex formulas or weight-assignment methods.

- Including 12 new indicators (of 16) that have not been defined previously in the literature or whose scope is more specific than existing ones.

- Considering indicators related to the digital culture of the DSO, which, as commented in Chapter 2, is essential to fully leverage smart grid solutions.

- Being "affordable", in terms of effort, for DSOs. The proposed indicators have been qualitatively validated by three experts from Spanish DSOs. As mentioned above, [103] also shows that a significant amount of information can be provided by DSOs.

Table 3.2: Benchmarking of main smart grid indicators in the literature

	[103]	**[94]**	**[93]**	**[106]**	**[102]**	**[105]**	**[107]**
DER penetration and integration	X	X	X	X	-	-	X
Additional products, services, and markets	X	-	X	X	X	-	X
DSO-TSO coordination	X	-	-	-	X	-	X
Monitoring and control	X	X	-	-	X	-	X
Grid management tools	X	-	-	-	X	-	-
System reliability	X	X	X	X	-	-	X
Data analytics	-	X	-	-	-	-	-
Security	-	X	-	X	-	-	X
Customer empowerment	-	X	X	X	-	-	X
Asset optimisation	-	-	X	X	X	-	X
Quality of Service	-	-	X	X	-	X	X
Grid planning	-	-	-	-	X	-	-
Data access	-	-	-	-	X	-	-
Environment	-	-	-	-	-	X	-
Economic	-	-	-	-	-	X	X

Table 3.3: Indicators to evaluate the digitalisation of power distribution grids

Category	Indicator
A. Sensors and actuators	A1. % of nominal consumption power with smart meters deployed
	A2. % of primary substations and % of secondary substations with automation and remote control
	A3. % of remote control devices outside primary and secondary substations per voltage level (MV and LV)
	A4. % of nominal power corresponding to LV feeders that are monitored online
	A5. % of transformers that are remotely monitored
B. Connectivity	B1. % of primary substations and % of secondary substations with broadband communications and % of nominal power that they represent
	B2. % of DER that establish communications with the distribution network and % of nominal power that they represent
C. Data processing	C1. % of network observable per voltage level (MV and LV) through state estimation
	C2. % of information that is available in real-time/semi-real-time
	C3. % of network assets with digital twins
D. Digital culture	D1. Existence of a digitalisation plan and responsible people
	D2. % of employees and field workers that have completed internal training courses in digital technologies and cybersecurity in the last three years and % of employees currently enrolled in training courses.
	D3. % of field workers with access to documentation through connected devices
	D4. % of the distribution network documentation that is accessible digitally
	D5. Availability of a digital platform for consulting and carrying out procedures for users
	D6. % of network users registered in the metering data app and, with respect to this, % that are active users per month

3.3 Key indicators of digitalisation

Given the four key pillars of digitalisation introduced in Chapter 2 (Section 2.2), the proposed KPIs are classified based on these: sensors and actuators; connectivity; data processing; and digital culture indicators.

The indicators for each group are presented in Table 3.3 and briefly described and discussed in the following subsections. To offer a fair comparison betweenDSOs of different sizes, most indicators are expressed as a percentage. It is highlighted that, as the purpose of these indicators is to measure digitalisation and not directly performance, high percentages would not necessarily mean high performance or cost effectiveness. Further analysis could study how different levels of digitalisation measured through the proposed digitalisation indicators correlate or explain the improvements on utility's performance measured through performance indicators.

To be effectively interpreted, these digitalisation indicators will need a prior characterisation of the distribution network (type of area, voltage levels, etc.), since the digitalisation needs may be different. For example, the requirements and connectivity necessities for a rural electricity network and for a urban one would not be the same, so they cannot be directly compared. It should also be noted that these terms (i.e., rural, urban) may have a different meaning depending on the sector (ICT or electricity),DSO, or country. In Europe, a common nomenclature is still needed for the electricity and ICT sectors.

3.3.1 Sensors and actuators indicators

The indicators in this group aim to measure the digitalisation of the distribution system in terms of the deployment of sensors and actuators. These devices allow a faster, more automated, and more sustainable operation of the network.

A1 % of nominal consumption power with smart meters deployed. The deployment of smart meters allow users to measure their consumption accurately and remotely, and to modify their consumption and contracted power (if applicable) to adapt it to prices and actual use of the network. At the same time, smart meters also protect users against overloads. In addition to this, the DSO can use smart meter data to quickly and easily detect and locate supply interruptions, considerably improving the quality of service. This indicator can be divided into two parts: % of residential power with smart meters, and % of commercial and industrial power with smart meters.

A2 % of primary substations and % of secondary substations with with automation and remote control. The number of operators in charge of a power distribution area is limited and a maintenance crew is not always close to the location of the breakdown. This indicator, together with the following one, measures if, and to what extent, theDSO is able to remotely reconfigure the network and restore the service, by acting automatically or manually on the devices deployed from the control center.

A3 % of remote control devices outside primary and secondary substations per voltage level (MV and LV). To operate the network safely, it is necessary to install devices (e.g., switches and voltage control devices) at certain points of the network and not only in the primary and secondary substations. These devices enable the DSO to perform actions remotely and reduce downtime of the supply.

A4 % of nominal power corresponding to LV feeders that are monitored online. Monitoring LV distribution power lines can be key to improve network operation and reliability.

A5 % of transformers that are remotely monitored. Transformers are critical equipment that are in constant operation and that require a high initial investment. Having sensors that measure critical parameters of this equipment, such as oil temperature [108] and vibrations [109], can help to predict and, mainly, prevent failures before they occur through proper maintenance. In addition to ensuring the security of the distribution network and electricity supply, this can also lead to an extension of the useful life of transformers. This indicator could also be distinguished between transformers in primary substations and transformers in secondary substations.

3.3.2 Connectivity indicators

To support the deployment of sensors and actuators in the network, the control centers of DSOs must have the necessary communications infrastructure to securely send control commands and receive monitoring data. The faster and more distributed these communications, the more secure the electricity supply will be.

Therefore, two of the indicators in this section are related to the presence of broadband connectivity. What is considered broadband depends significantly on the technology used. In general, a broadband connection can be considered when the speed offered is higher than the offered by narrowband technologies such as narrowband power line communications (500 kbps) [110].

B1 % of primary substations and % of secondary substations with broadband communications and % of nominal power that they represent. Although, currently, it is not necessary to have broadband communications in all the substations and distribution transformers, this is something to consider in the coming years with the increasing connection of devices to the grid. With a broadband communication infrastructure, DSOs will be able to manage not only the devices deployed by themselves, but also all the energy management and generation/storage devices installed by users in the near future. Communications closer to real-time between control centers and primary substations and secondary substations (next indicator) will allow the DSO to increase its knowledge about the status of its network and will help to increase the number of possible functionalities and services for user participation and consumption.

B2 % of DER that establish communications with the distribution network and % of nominal power that they represent. This indicator refers to all the DER that establish communication with the DSO it in order to coordinate their actions for the safe and efficient operation of the network (e.g., providing services to the DSO). For example, Home Energy Management Systems (HEMS), Battery Management System (BMS), communications for EV charging infrastructure, generators or storage for self-consumption, etc. The existence of this communication gives users the possibility of having an active role in the electricity system if they wish.

3.3.3 Data Processing indicators

These indicators are related to the processing of the data generated by sensors, which were transmitted using connectivity capabilities and then translated into specific functionalities. Despite some additional indicators related to the amount of data processed (e.g., volume of information processed versus the volume of information collected during a period; number of uses cases based on advanced analytic) could be added, these have eventually been discarded due to the complexity of accurately and fairly measuring them from a practical point of view. The decision was made to give more importance to the applicability and measurement potential of the data processing indicators than to their completeness.

C1 % of network observable per voltage level (Medium Voltage (MV) and LV) through state estimation. The electrical distribution system is incredibly extensive geographically, so it is not economically or technically feasible to have every point of the system

monitored at every voltage level. Observable means that the DSO is able to know the functioning of the grid by analysing the data collected (voltage, current, power, etc.) By optimising the arrangement of sensors [111] and applying mathematical techniques with the available data, the state of the parts of the grid that are not being directly monitored can be estimated (i.e., power system state estimation) with a reduced error margin [112].

C2 % of information that is available in real-time/semi-real-time. This indicator measures the real-time and semi-real-time data processing capabilities of the DSO: what percentage of information within a day can be generated in less than 15 minutes from the moment the input data was collected.

C3 % of network assets with digital twins. The prediction on the behaviour of equipment or part of the network allows optimising the operation and making better decisions. This is can be done through the so-called "digital twins", introduced in Chapter 2, which can be understood as highly detailed models that replicate the functioning of physical systems to analyse, optimise, and manage them [45].

3.3.4 Indicators of digital culture

A highly digitalised distribution network cannot be properly leveraged if the people who interact with it (e.g., for planning, operation, or maintenance activities) do not have the necessary training and resources. Consequently, we foresee the following indicators regarding Digital Culture.

D1 Existence of a digitalisation plan and responsible people. The existence of a plan within the DSO to digitalise the distribution network implies that it has not only studied the weak points and aspects to improve the network, but also that the DSO is aware of the potential functionalities and services that users willing to participate actively could demand.

D2 % of employees and field workers that have completed internal training courses in digital technologies and cybersecurity in the last three years and % of employees currently enrolled in training courses. A DSO that cares about the continuous training and learning of its employees means that it values its human resources and knows that they constitute the basis for efficient and safe operation of the network. This remains essential even though new personnel with digital skills is hired, as new technologies and cyber threats are continuously emerging. That is why two indicators related to internal training are proposed: on the one hand, the % of employees who have taken a course related to digitalisation (technologies, digital skills, cybersecurity, etc.) in the last three years, to obtain information on the training received by staff in this

period, and, on the other hand, the % of employees who are currently taking a course, with the aim of having an overview of continuous training at a given time.

D3 % of field workers with access to documentation through connected devices. If technicians and maintenance crews can access all the information needed through a laptop, tablet or mobile phone, they will be much more agile and efficient in performing tasks than if they have to carry up-to-date papers and notebooks with the technical specifications of devices and equipment. Furthermore, it should also be possible for field workers not only to access this documentation but also to be able to edit it when finding inconsistencies with respect to reality.

D4 % of the distribution network documentation that is accessible digitally. In relation to the previous indicator, it is important that, apart from the operators deploying connected devices, the information needs to be available in digital format. This could be an indicator difficult to measure in certain cases. Alternatively, it could be estimated by consulting field workers about their use of documentation in digital format in their tasks.

D5 Availability of a digital platform for consulting and carrying out procedures for users. When users have the possibility to interact with DSOs easily and online, the barriers to their active participation are significantly reduced. It also helps to improve DSO's customer service and response time to incidents notified by users. This is a binary indicator: if the DSO does not have said platform, it would be 0, and 1 if it is available.

D6 % of network users who are registered in the metering data application and, with respect to this, % that are active users per month. The first step towards an active participation of users in the distribution network is that they show interest in their own electricity consumption. It could be considered active users those unique users who have accessed the application at least once in a month.

3.4 Applicability

The advantages and applications of the proposed indicators are numerous.

First, these indicators do not require a huge amount of input information and complex calculations in contrast with when measuring smart grid performance indicators: they are related to the digital infrastructure of the grid and not its resulting performance. For example, in [102], KPIs' formulas involve calculating different weights for the addends/summands, whereas the digitalisation indicators presented in this document are mostly percentages, much easier to calculate. Since the remuneration of DSOs is regulated, they carry out the accountability of network investments and maintain an inventory of the assets installed at primary

and secondary substations. Indicators such as *"A5. % of nominal power corresponding to LV feeders that are monitored online"* could be extracted by the DSO from already-available information. Other, such as *"A1. % of nominal consumption power with smart meters deployed"* and *"A2. % of primary substations and % of secondary substations with automation and remote control"* are already measured [103], [113]. Therefore, the process of measuring the proposed indicators would not be very time consuming.

Second, contrary to performance indicators, the measurement of these digitalisation indicators do not seek the maximisation of digitalisation but the optimisation of digitalisation. It may not be necessary to digitalise each and every point of distribution grids to achieve a good operation; once a certain digitalisation level is achieved, the marginal benefit (in operation, quality of service, reliability improvement of the grid, etc.) of implementing a specific digital technology may be lower than its cost.

Third, the proposed indicators have been categorised according to the pillars of digitalisation of power distribution grids and they are use-case-agnostic. Any smart grid solution would be related to, at least, one of these pillars. As mentioned in Chapter 2 (section 2.2), a significant development in one category (i.e., pillar of digitalisation) would typically require a similar improvement in at least another category. Therefore, to fully leverage these indicators, every category should be analysed considering the others.

Fourth, the proposed indicators were reviewed by three subject-matter experts and practitioners from three Spanish DSOs who provided feedback in their personal capacity and not as DSO representatives. The consulted experts significantly appreciated the necessity for indicators that measure the digitalisation of DSOs. They considered that data availability, in principle, would not be a problem to implement the proposed indicators, and positively valued their feasibility, highlighting the realism of the outcomes that could be expected from these.

And last but not least, the digitalisation indicators proposed here are in line with the recommendations of the DSO Observatory, an initiative supported by the European JRC that monitors how DSOs are evolving to foster the energy transition [103]. The DSO Observatory recommends following an European-wide approach to collect DSO technical data, and to research, at a policy level, on the adequacy of grid digitalisation versus grid expansion. The proposed indicators would provide more information on the digitalisation characteristics of DSOs that could be measured with different objectives that can be of great interest for NRAs and DSOs: A) to get a overview of the distribution system, B) to determine the relation between performance and digital infrastructure. These objectives are discussed below.

3.4.1 Overview of the distribution grid

By measuring the proposed indicators, the current state of the digital infrastructure of the grid could be summarised.

Sensors and actuators indicators provide information on how large the control and monitoring infrastructure in the field is. The larger this infrastructure is, the smarter the grid can become. With the increasing deployment of acder and new energy services, the distribution grid will require a wider range of actions and more information to guarantee the reliability of the grid.

Connectivity indicators show the level of readiness of the grid to communicate in a fast and reliable way, not only with sensors and actuators already deployed, but with new devices that may be installed in the future by the DSO or third parties.

Data processing indicators provide an idea of how good the DSO processes data and how the data of the sensors and actuators are used to ensure efficient and safe operation of the grid. For this category, it is extremely important to consider the two previous categories to obtain relevant good insights. If the scores in sensors and actuators, and connectivity are acceptable, but the scores for data processing are low (e.g., low observability of the grid), the DSO should improve its capacity to process grid data, so that the sensors and communication infrastructure can be better leveraged.

Digital culture indicators, despite being related to the corporate level of a DSO, show if the digitalisation of the distribution network is accompanied by the development of the digital capabilities of the DSO's personnel and customers. High scores in this category would show that employees and customers may find fewer difficulties and resistance to change when implementing new smart grid solutions and services.

3.4.2 Relation between performance and digital infrastructure

The full digitalisation of the distribution network may not be necessary to maintain an excellent performance and quality of service. In fact, digitalisation increases the cyber security risk and, over certain levels, performance may not improve. For example, the reliability of MV grids, regardless of the topology, does not increase significantly for automation degrees greater than 20-30% [114]. Whether the added value of a specific digitalisation investment is higher than its cyber security risk is something that should be evaluated case by case.

By measuring the digitalisation of different distribution grids, the relation between grid performance and digitalisation may be observed and leveraged to keep cost-effectiveness, avoiding overinvestments. It would also help to know if the areas that are being digitalised are those which require it the most. Large DSOs could carry out comparisons between their distribution zones with different levels of digitalisation and energy services and determine to what extent the digital infrastructure influences grid performance so that new investments can be better planned.

NRAs could also benefit from this. By measuring the proposed indicators in addition to performance indicators for all the DSOs, the NRA may get a clear view of which digitalisation indicators need to be developed in order to improve performance. With these insights, NRAs

could identify clusters of DSOs with similar digitalisation conditions and provide ad hoc recommendations or even design new regulatory schemes to promote specific investments that are shown to have a positive influence on grid performance.

3.5 Conclusions

So far, existing KPIs have focused on the performance and quality of service aspects of smart grids. However, nowadays, the main approach followed by DSOs to improve their performance indicators is the digitalisation of the grid and its processes. The set of indicators proposed in this chapter, specifically focused on digitalisation and not on performance, aims to answer the need of measuring the digitalisation level of distribution grids and to become a mean to determine which digital capabilities are driving the performance levels measured.

The proposed indicators are in consonance with the JRC DSO Observatory's recommendations to measure the digitalisation of DSOs and to facilitate the comparison of international experiences and best practices. They are agnostic to use cases, do not require a large amount of information, and could be leveraged by both NRAs and DSOs to get a complete view of the level of digitalisation of distribution grids and to identify cause-effect relations between performance and digital infrastructure.

The extensive use of these indicators among DSOs and NRAs could open new synergies. DSOs would be able to take advantage of other DSOs' experiences when considering different digitalisation alternatives and when estimating the success of innovative smart grid solutions. At the same time, NRAs would be better positioned to promote or discourage certain digitalisation investments. However, these benefits would only be experienced if regulators promote the adoption of the proposed digitalisation indicators, standardise the related data collection process, and disseminate their results, so that different experiences and learnings can be shared. This collaboration between stakeholders could improve the digitalisation process of distribution grids to better address the challenges of the Energy Transition.

Chapter 4

Scalability and Replicability Analysis of ICT in Smart Grids

4.1 Introduction

In the process of digitalisation of electricity distribution grids to smart grids, some solutions based on ICT will inevitably add more value than others. The digitalisation indicators presented in the previous chapter, when analysed together with performance indicators, could help identify those digitalisation investments with greater impact. However, to make this digitalisation more efficient and cost-effective, the ICT involved in smart grid solutions should be highly scalable and replicable.

To assess this, a SRA has to be performed. The purpose of a SRA is to detect any potential impediments and limitations that could prevent the solution from being just a one-off local demonstration [5].

The scalability and replicability of smart grid solutions are influenced by technical, economic, regulatory, and stakeholder acceptance factors [5], [115]. In various European projects, technical SRAs have focused on the impact on the power system, calculating indicators such as the decrease in network losses or the hosting capacity [116]. However, the ICT infrastructure used is also an important factor in the scalability of smart grids [7], as it can impose constraints on the scalability and replicability of the smart grid use case. For example, [116] shows that the reliability of MV grids, regardless of the topology, does not increase significantly for automation degrees higher than 20-30%; however, it may not be possible for the ICT used to match such scalability levels, or may depend on factors such as the topology or area to cover. Therefore, to gain a complete understanding of the technical scalability and replicability of a smart grid solution, the ICT part is essential to reduce the risk of having to upgrade the infrastructure in the near future.

Despite the fact that scalability and replicability concepts have already been applied to

ICTs in other fields, mainly to computer applications and operating systems [117], there are no clear guidelines for their application in a smart grid context. This lack of clarity leads to non-homogeneous analyses, which in turn affects the conclusions drawn.

The BRIDGE initiative at the European level provides high-level instructions, based on the SGAM [118], to perform a SRA regardless of the layer/dimension considered [119]. Nevertheless, [119] points out that more precise instructions and techniques can be created for each layer or kind of technology.

Also within the BRIDGE initiative, [120] has proposed a SRA methodology for smart grid projects. This methodology involves the identification of Key Exploitable Results (KERs) for each SGAM layer, with the aim of evaluating scalability and replicability as two overall indexes for each Key Explotable Result (KER). In terms of ICT, [120] suggests evaluating the use of open technology, standards, and communication protocols, as well as the interoperability of the systems, to determine if they can be replicated. To evaluate scalability, it is proposed to determine whether additional resources based on open standards would be necessary to expand the system. However, it is not clear how to carry out this mainly qualitative assessment and how to calculate and interpret the proposed scalability and replicability indices for ICT systems in smart grids.

Therefore, the execution of an ICT SRA can be challenging due to the absence of a well-defined approach and the wide range of factors to consider. This makes it difficult to ensure that the analysis yields the most useful insights.

Consequently, this chapter provides a common methodology for quantitative ICT SRAs so that the outcomes of such studies can be as beneficial as possible. For this, the concept of **ICT SRA map** is introduced in this thesis as a novel way of summarising SRA results, constituting a tool to determine the potential scalability and replicability of smart grid ICT systems, so that each future implementation does not have to reinvent the wheel. This methodology is validated and exemplified by applying it to two real case studies (one using wired technology and another one using wireless technology) from the EU-funded RESPONSE project.

This chapter is structured as follows. First, the state-of-the-art of ICT SRA is introduced in Section 4.2, including definitions and dimensions of scalability and replicability (4.2.1), the literature review (4.2.2), and the main trends and gaps identifed (4.2.3). Then, Section 4.3 describes the methodology developed to perform ICT SRA in smart grids. This is followed by the application of the methodology to two case studies in Section 4.4. Finally, in Section 4.5 the main conclusions are drawn.

4.2 Scalability and replicability: state-of-the-art

4.2.1 Definitions and dimensions

In general terms, the scalability of a system can be defined as its ability to increase its size, scope, or range; while replicability can be understood as the ability of a system to be implemented at a different location or time [116]. An SRA is the evaluation of these two concepts for a specific system or use case.

Scalability

A discussion is still open on whether the scalability and performance evaluations of ICT systems are two different things. Reference [121] considered them two different types of research, giving the scalability analysis more relevance. In some cases, scalability is considered just a characteristic of the system [122], [123] or a qualitative requirement [124]–[126].

On the other hand, it is true that scalability and performance are deeply related [117], [127]. Ultimately, a quantitative scalability analysis always constitutes a performance evaluation of a scaled-up version of the system. However, the opposite is not always true. A performance evaluation can be done without obtaining scalability insights; just to design the system for specific operation conditions.

Two general dimensions for the scalability of smart grid systems are differentiated in [116]: the scalability in size, when the system covers a larger area; and scalability in density, when parameters such as the number of elements involved are varied.

Focused on ICT, [117] defines different types of scalability for operating systems and local area networks:

- Load scalability: if the system works well with light and heavy workloads.
- Space scalability: if memory limits are not exceeded when increasing the number of elements in the system.
- Space-time scalability, if the system works well while significantly increasing the number of elements.
- Structural scalability: if the standards implemented do not constrain the system.
- Distance scalability: if the system works well with short and long distances
- Speed/distance scalability, if the system works well with short and long distances regardless of the speed required.

Figure 4.1 combines the scalability types defined by [116] and [117], providing the complete picture of ICT scalability.

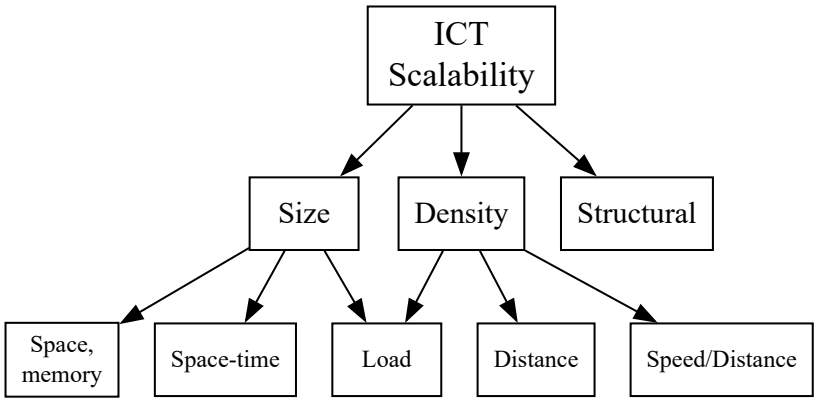

Figure 4.1: Types and subtypes of ICT scalability based on [116], [117].

Replicability

Regarding replicability, for ICT, the concept has been less explicitly assessed than scalability by the literature.

When considering smart grid systems, two dimensions were differentiated by [116] in the functional layer: intranational (that is, within the same country) and international replicability. However, these two dimensions are usually not considered directly when studying the replicability of ICT systems. For example, the ICT replicability study in [128] consists of a qualitative evaluation of alternative protocols; in other cases, the replicability study is understood as an evaluation of the levels of standardisation, interoperability, and network configuration [5], [129]–[131]. Among these, the interoperability of an ICT system can be analysed in three different SGAM layers: information, communication, and component layer. Figure 4.2 shows how, depending on the layer considered, the scope and type of interoperability analysed vary, distinguishing between semantic, syntactical, or technical interoperability [132].

Spatial dimensions can be addressed quantitatively by performing ICT performance evaluations of scenarios where the topology and environment of the communication network considered are similar to those found in a specific area. From a qualitative perspective, different aspects can be evaluated. The ICT systems implemented by DSOs may vary not only at an international level, but also at the regional level. Therefore, to easily replicate a smart grid system from an ICT point of view, a high level of interoperability of its components and systems is essential. In addition, the communications infrastructure in the area should also be evaluated. In some cases, communication technologies (e.g., 5G) may not be available and an alternative has to be used, which can be a problem if ICT components are not compatible with the alternative; in other cases, the original smart grid system may use a wireless protocol in a frequency band whose acquisition of a licence in another country could significantly increase implementation costs or that is already allocated for other use [133].

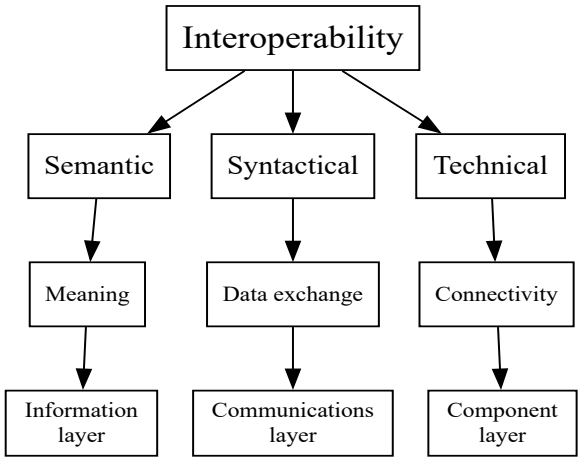

Figure 4.2: Dimensions of interoperability and related SGAM layers.

4.2.2 Literature review

In this section, previous work that has performed a scalability and / or replicability analysis of ICTs in smart grid contexts is reviewed. Since scalability analysis also constitutes a specific way of performance evaluation, references using the terminology ”performance evaluation” have been included, as long as the studies comply with the characteristics of a scalability or replicability analysis.

To better organise and promote the dissemination of knowledge and experience from different studies that address the scalability, replicability, or performance of different ICTs, the TICTA-C Initiative [134] has been developed. The TICTA-C Initiative makes the taxonomy of the literature reviewed publicly available on the Internet. The taxonomy is visually presented as a scheme and classifies each reference according to the use case it studies, providing information related to the type of analysis performed (quantitative, qualitative, or both), and the technologies studied. Furthermore, the metrics used in the literature are classified according to whether they are qualitative or quantitative and on whether the ICT analysed is wired, wireless, or other. TICTA-C is conceived to be collaborative, so the taxonomy can be expanded by submitting new references through a Web form.

Table 4.1 summarises the scope of the analysis and the quantitative metrics of the main references reviewed.

The following subsections detail and discuss the characteristics and scope of analysis of a number of references, divided into use cases.

A Energy Storage as a Service (ESaaS) and VPPs

References [128], [135] proposed a two-step approach to carry out an ICT scalability analysis within the InteGrid project. It combined a first qualitative SGAM-based analysis to identify potential bottlenecks, with a quantitative analysis that determines the operational limits

through simulations. Regarding replicability, the process was the same as the one followed for the qualitative scalability analysis but comparing different ICT alternatives [128]. However, qualitative ICT comparisons do not really provide many insights about the replicability potential of a specific ICT system.

B Flexibility aggregation, ancillary services and demand response

Within the EU-funded InterFLEX project [136], the analysis performed was qualitative and scalability-focused, not addressing replicability. It defined conceptual scenarios, including real-time and deferred operation, and analysed them using the SGAM and information about ICT attributes. The relevance of these attributes was previously determined through questionnaires to the stakeholders involved in the use case. The results in [136] are a set of general recommendations and prerequisite rules to be considered when scaling up the architectures. However, the specific ICTs implemented were not analysed, so the SRA lacks specific scalability insights of the technologies implemented.

On the other hand, the EU-funded WiseGRID project [130] qualitatively analysed the replicability of the information and communication layers of the WiseGRID ICT tools. Standardisation, interoperability, and network configuration factors were assessed at a high level for every tool. The WiseGRID tools implemented protocols such as Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), OCPP1.6 and CHAdeMO, and the CIM. In this case, the specific ICTs were considered in the replicability analysis.

Yamada et al. [137] evaluated the scalability of an aggregator-to-consumer Wide Area Network (WAN) Web Service communications (OpenADR and IEEE 1888 Web Services) for fast automatic demand response. To emulate the delay of the Internet WAN, it used queuing theory and communication simulation equipment, measuring the delay in completing the aggregation of resources, since it was identified as the main bottleneck. The main disadvantage of this approach is that the extrapolation (i.e., replicability) of the results obtained in [137] can be challenging when considering other locations for the use case, as the speed of the Internet connection can differ.

Matanza et al. [138] analysed the use of power-line communications for the transmission of OpenADR signals for demand response. The analysis was focused on latency in several communication environments (background and impulsive noise sources, channel attenuation, and multipath effects), concluding that this technology would be more suitable for ”slow” demand response programs (e.g., day-ahead) rather than real time markets.

Yaghmaee et al. [139] defined a Cloud Demand Response (CDR) model and propose a communication model to evaluate the communications performance of both the CDR and distributed demand response models when implementing different communication strategies (hop-by-hop, end-to-end, and intermediate catching) in a clustered wireless mesh network. For the analysis, it considered different cluster sizes and Bit Error Ratio (BER), which provided valuable information on the scalability and replicability of the system.

C Grid control/monitoring

Kenner et al. [140] discussed two architectures to collect data from energy analysers: one using the Modbus TCP/IP protocol and the other using a RESTful web service architecture. They analysed the performance of these architectures with respect to latency, needed bandwidth, and scalability. However, they just compared the performance of the two alternative architectures without reaching the limits set by the operational requirements of the use case and, therefore, without fully assessing the scalability potential of the technologies.

Bian et al. [141] co-simulated the power and communications network to assess the performance of remotely controlling a switch. The approach followed by [141] for this assessment constitutes a quantitative way of analysing replicability: latency was calculated for a 100km fiber-optic cable with different background traffic assumptions (0-50-100%). The analysis showed that when channel usage reaches 100%, the performance of communications is significantly worse (i.e., high latencies), which may affect critical smart grids applications. Therefore, utilisation peaks should be considered when using the same communications infrastructure for multiple purposes.

Garau et al. [142] quantitatively analysed the performance of wireless and hybrid wireless-wired communications network for voltage regulation and fault protection applications. It showed that the hybrid approach, even under ideal conditions, may present latencies that cannot be accepted for critical smart grid applications. On the other hand, it claimed that wireless technologies such as WiMAX, WiFi, and Long Term Evolution (LTE), may satisfy smart grid requirements. Nevertheless, [142] did not consider any scalability scenarios or other aspects (e.g., interference) that could significantly affect the performance of wireless technologies under real conditions; an SRA would be necessary to ease the extrapolation of these research results to future implementations.

D Advanced Metering Infrastructure (AMI)

Zhou et al. [143] performed a high-level qualitative and a deep quantitative scalability analysis of three different AMI architectures (one centralised and two distributed). However, the focus was on the cost rather than on performance.

Reference [144] proves how important a scalability analysis is not only for pilots but for already-implemented infrastructures to expand its use and functionalities. It analysed the performance of three AMI technologies (hybrid fiber optic - WiMAX, fiber optic - LTE, and 900-MHz RF) when used in parallel for price-induced controls, distribution automation, demand response, and Vehicle-to-Grid (V2G) applications.

On the other hand, [145] shows the importance of assessing the replicability of ICT in smart metering, and its correlation with scalability. It quantitatively analysed the operating limits of PLC PRIME smart metering networks under different scenarios combining replicability (urban and residential areas) and scalability (small, medium, and large buildings) parameters.

E Other smart grid applications

Reference [146] shows the importance of choosing appropriate metrics when performing an quantitative scalability analysis. It analysed and compared the impact that different levels of penetration and applications of DER have on up to nine hybrid Home Area Network (HAN)-Neighbourhood Area Network (NAN) communication networks; it shows that the maximum DER penetration achieved varies depending on which performance metric is taken as reference (latency or Packet Loss Rate (PLR) in [146]).

Reference [147] followed an alternative approach to analyse the scalability of six hybrid HAN-NAN communication architectures for generic distributed smart grid applications; instead of increasing the number of devices involved (scalability in size), [147] increased the size of the User Datagram Protocol (UDP) packet (scalability in density). It compares the results with the initial performance requirements with respect to latency, throughput, and PLR. The authors conclude that the Low power Wireless Personal Area Networks (LoWPAN)-based hybrid architectures would satisfy all requirements regardless of packet size and data rate. For Narrowband Power Line Communications (NPLC)-Ethernet and NPLC-WiMAX, it shows that, only for certain data rates and packet size ranges, performance can satisfy the requirements.

Meeuw et al. [148] analysed the performance limits of a blockchain-based local energy market for its implementation in a community microgrid in Walenstadt, Switzerland. This analysis allows some replicability insights; given the transactions per second required by the market, and its level of decentralisation, results in [148] allow the deduction of the minimum data rate required so that the communication infrastructure can be designed properly.

Table 4.1: Summary of the scope of analysis, strengths, weaknesses, and metrics for the main literature reviewed. Qn-Quantitative; Ql-Qualitative; S-Scalability; R-Replicability

Use case	Ref.	Scope				Strengths	Weaknesses	Metrics
		QnS	QlS	QnR	QlR			
A	[128], [135]	X	X		X	SGAM analysis allows identification of potential bottlenecks	Replicability analysis just compares ICT alternatives. No real distinction between replicability and scalability in the analysis.	Link usage (%), Round-trip time
B	[130]				X	Standardisation, interoperability, and network configuration factors are assessed. The specific ICTs are analysed.	High-level analysis of the ICTs.	-
	[136]		X			SGAM analysis allows identification of potential bottlenecks. As it requires the involvement of stakeholders, information may be more accurate.	Provides general recommendations and pre-requisite rules; the specific ICTs used are not analysed. Relevance of attributes may be biased if there are few stakeholders.	-
	[137]	X				Combines queuing theory and communication simulation equipment.	Extrapolation of results (replicability) can be difficult, as the speed of the internet may vary between locations.	Aggregation delay
	[138]			X		Replicability analysis in several communication environments (background and impulsive noise sources, channel attenuation and multipath effects.)	No scalability in size analysis	Latency, round-trip time.
	[139]	X		X		Considers different cluster sizes and BER, providing scalability and replicability insights. Compares analytical and simulation results.	Performance is not compared against baseline requirements of the use case.	Throughput, No. of message transmissions, No. of TCP/UDP update messages
C	[140]	X				Analysis considers latency, needed bandwidth, and scalability.	Operational limits are not reached during analysis, so the scalability potential of the technologies is not fully assessed	Latency
	[141]			X		Considers different background traffic. Shows that utilisation peaks should be considered when analysing a communications infrastructure.	Only one end device (switch) is considered in the analysis. No scalability scenarios to see the impact in a wider area.	Latency
D	[143]	X	X			Deep quantitative scalability analysis. Provides a cost scalability analysis.	Lacks analysis of the technical performance of technologies.	Cost of implementation, accumulated bandwidth distance product (ABDP)
	[144]	X				Highlights the importance of carrying out a scalability analysis to take advantage of already-implemented infrastructures. Considers requirements and characteristics of the smart grid applications analysed.	Difficult-to-interpret graphs of results (both axis represent time)	Latency, throughput
	[145]	X		X		Correlates the scalability of the technologies with the replicability analysis carried out. Considers urban and residential scenarios and also small, medium, and large buildings.	-	Time to read all meters, time to register all meters
E	[146]	X				Shows how the maximum DER penetration varies depending on the performance metric taken as reference	Needs further analysis on what has an impact on packet loss rate.	Latency, throughput, packet loss rate (PLR)
	[147]	X				Scalability in density analysis. Comparison of performance with initial requirements.	No scalability in size analysis.	
	[148]			X		Allows the deduction of the minimum data rate required to properly design the infrastructure for different scenarios.	It does not really provide an ICT SRA, but a tool to set the minimum requirements of the ICT infrastructure.	Latency, throughput

4.2.3 Trends and gaps

As Table 4.1 shows, the literature has focused mainly on the quantitative analysis of ICT for various use cases. In this type of analysis, latency, throughput, and reliability metrics are used as main indicators, regardless of the type of technology analysed. However, a notable gap in the state-of-the-art is the clear relationship between the selected metrics and the unique requirements or constraints of each use case. This may blur the scalability analysis since conclusions may differ depending on the selected metrics.

To address this gap, a more comprehensive framework to assess scalability in a context-sensitive way has to be developed. This involves understanding how the choice of metrics should align with the particular characteristics and objectives of each ICT system, ultimately leading to more nuanced scalability analyses. Analysis results must also allow to determine if the system is scalable or replicable in specific scenarios.

However, not all ICT systems, or at least not all of their elements, may be suitable for a quantitative scalability analysis. In some cases, due to the functional characteristics of the system, technical performance limits may be expected to provide a scalability potential higher than that expected in a real implementation. For this reason, a previous analysis that identifies potential bottlenecks, even at a high level, would be convenient to determine the usefulness of a quantitative analysis that could focus only on the most critical components.

On the other hand, quantitative replicability analysis has been focused on analysing different conditions for communications (e.g., BER, modulation technique, etc.), or topologies (e.g., rural and urban environments for smart meters). For wireless communications, aspects such as background noise and obstacles (e.g., building walls) have not been considered in most cases, despite being relevant for replicability and having a deep impact on performance.

When scalability is not the objective of the analysis but is considered just another metric that characterises an ICT system, the calculation method is not specified or is qualitatively defined in general terms, without considering the different types of scalability that an ICT system may present. This is also observed in the SRA guidelines provided at the European level [120], where the approach to calculate the scalability and replicability indexes is not described in detail.

For this reason, a detailed methodology to carry out an SRA of the ICT systems involved in smart grids is proposed in the next section, so that the appropriate metrics can be selected based on the technology and requirements of the use case, and the results can be used to get insights about the scalability and replicability of the ICT system for different scenarios.

4.3 Methodology description

The methodology developed to perform a quantitative ICT SRA is summarised in Figure 4.3 and described below. It consists of up to seven steps that cover from the characterisation of the ICT system and the definition of the scope of the analysis, to the visualisation of the ICT SRA results through scalability and replicability maps.

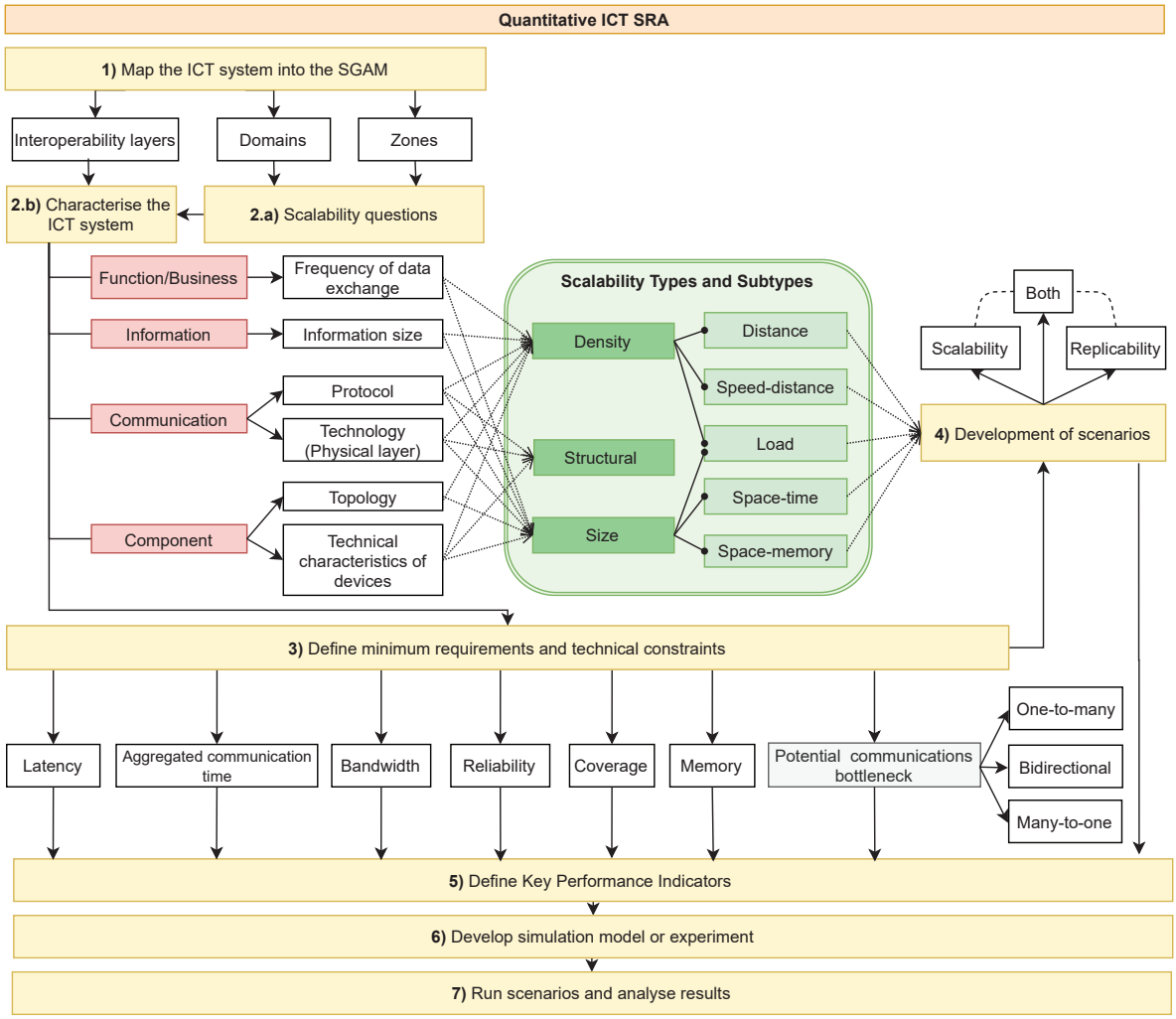

Figure 4.3: Quantitative ICT SRA methodology proposed.

4.3.1 Map the ICT system into the SGAM

The first step for the SRA is to obtain information about the implemented ICT, the topology, and the functioning of the system. This information can be mapped into the SGAM [118]. The SGAM is a model for the interoperability of smart grid solutions that uses two axes (domains and zones), and five interoperability layers, as shown in Figure 4.4. In the first axis of

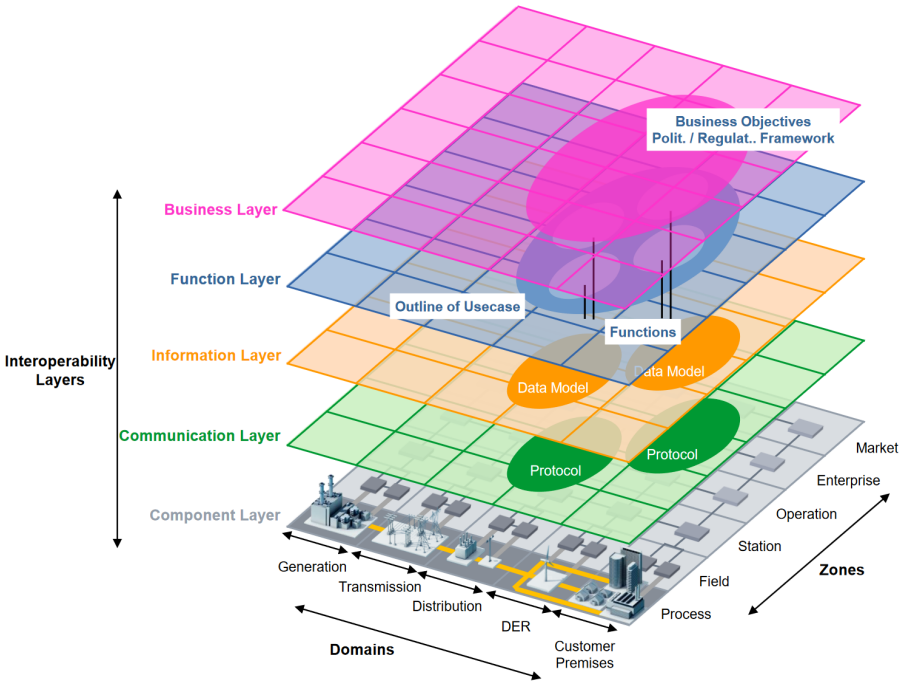

Figure 4.4: SGAM Framework. Source:[118]

the SGAM, the "Domains" of the electrical sector are represented, that is, the current chain that electricity follows from its generation to its consumption (generation, transmission, distribution, DER, and customer premises). In the second axis, the "zones" are shown, which are the same for each domain and allow information management to be classified (field, station, operation, enterprise and market) and include equipment and physical spaces (process). These two axes are applied to five interoperability planes or layers: component, communication, information, function, and business.

A preliminary map that includes the components and communication layers would be sufficient for this step of the methodology to determine the scope and characteristics of the SRA. Obtaining the whole map is a complex task that requires time and which is only useful if the scope of the SRA has already been set.

4.3.2 Scalability questions and system characteristics

Based on the SGAM, some initial scalability questions can be asked in order to determine how a scaled-up version of the system would be. This can be done by observing the domains and zones involved. To characterise the system from an ICT perspective, the focus would be on the interoperability layers.

Scalability questions

Scalability questions are a set of simple initial questions to try to answer during the characterisation of the ICT system under study, to determine the scope of the ICT SRA. If all the scalability questions can be answered without testing or performing simulations, then a quantitative SRA is not necessary.

To formulate these questions, the value chain of the electricity system should be considered. In general, domains grow larger as they become closer to electricity customers. That is to say, electricity consumers are in the order of millions, DER may be in the order of thousands/millions, distribution grids must provide service to both consumers and DER (i.e., distribution customers), and transmission grids connect bulk generation with distribution grids.

From a scalability point of view, scaling-up in one domain may affect the domain immediately above it. An example is the smart metering deployment by DSOs, which in many countries are in charge of this process. Millions of smart meters have been deployed at the customer level in many countries, but DSOs are the ones providing the means to monitor them. Another example would be the implementation of a TSO-DSO coordination scheme managed by the TSO in countries where there is only one TSO and hundreds or thousands of DSOs: the TSO would have to provide the necessary scalability to replicate such coordination scheme with each DSO.

Zones within a domain also have this characteristic. From process to market, the number of components is expected to decrease. In the smart metering example, data collectors had to be deployed at the secondary substation level (field zone), which use the router deployed at primary substations (station level) to send the data to the central system (operation level). Therefore, in each zone, the ICT scalability is supported by the component that provides the connection in an upper zone.

This potential influence of scaling-up components in SGAM domains and zones is illustrated by Figure 4.5.

Scalability questions can then be formulated taking into account these zone and domain aspects. Two general examples would be:

- Will the communications between the station and field zone work properly if the number of field devices increases?
- Will the TSO operation system be able to cope with an increment in the amount of data exchanged with the DSO operation system?

Characterise the ICT system

As indicated in the first step, to formulate the scalability questions it is necessary to have a description of the component layer of the system in the SGAM. As the ICT system is

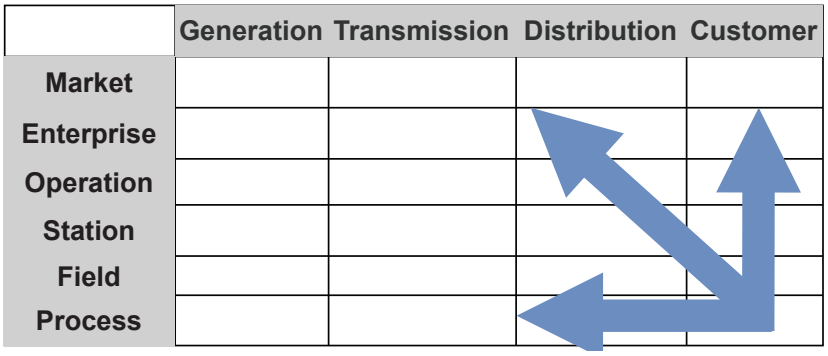

Figure 4.5: Potential influence of scaling-up components in SGAM domains and zones. Note: Customer includes DER and consumers.

characterised for each SGAM layer, some of the scalability questions can be evaluated again and even discarded.

The **component layer** provides two pieces of information. The first one is the topology of the ICT system implemented, which is essential to know the communication links, potential information flows, and in which zones they are placed. This is relevant for scalability in size analysis.

The second piece of information is the technical characteristics of the devices, which, even with missing information, can give an idea of the type of ICT implemented (i.e., wired or wireless) and the capacity of the devices. Depending on the amount of information available, this can be relevant for all types of scalability analysis.

The **communication layer** is built on top of the component layer, providing essential information for conducting a quantitative ICT SRA, regardless of the type of scalability considered. This layer indicates the communication technology (physical layer) used by each link in the component layer and the communication protocol that is implemented. ICT systems will be wired, wireless or hybrid. Depending on this, different key performance indicators will be used during the analysis.

Regarding the communication protocol, it determines how the components will exchange the information and may be key to the scalability and replicability of the system. If the protocol is proprietary, the replicability of the system will be affected, and if the specification is not freely accessible, it can be a huge obstacle to perform a quantitative SRA, which can end up excluding these links from the scope of analysis.

The **information layer** indicates the data models and the information exchanged between components through the communication links. This would set the size of the information to be considered in the analysis to which to sum the overhead in the messages that may be added by the communication protocol implemented. This information is essential for performing a quantitative scalability analysis (in density and in size), since it affects potential requirements such as the latency and can be related to the existence of bottlenecks.

Finally, the **function and business layers** are related to the services provided by the system. This will give the frequency of data exchange, which is essential for determining if the quantitative SRA is necessary, as it is related to the scalability in size and density. For example, some functions can require exchanging information once per day (e.g., daily market results), while others may need further resolution (e.g., monitoring of resources). The higher the frequency of exchange, the higher the probability of communication bottlenecks when scaling up the system to reasonable levels. In all likelihood, a once-per-day, non-essential exchange would need to scale up to disproportionate levels before experiencing information bottlenecks. The other way around, frequent, time-sensitive exchanges of large volumes of information would increase the probability of information bottlenecks.

4.3.3 Minimum requirements and technical constraints

Once the characteristics of the system have been obtained for all the layers of the SGAM, the functional requirements and technical constraints must be examined. These are typically provided by the function/business layers, which specify the frequency of data exchange (i.e., the first requirement for the system); by the component layer, if the technical specifications of the devices and systems implemented are available; or by the communication technology employed. Each smart grid solution will have different requirements [149] and, in all likelihood, the ICT will have been selected to fulfil all the requirements of the use case [150]. However, this compliance should be checked when scaling up and replicating the system.

For the analysis of ICT systems, these requirements can be related, but not limited, to the following:

- *Latency*. When an application requires real-time communication, latency is typically the most important factor to take into account, making it the primary performance measure for the system, as it can affect the reliability of the smart grid [151], [152] and is an essential requirement when designing control schemes for DER [153]. Scalability requires that, as the system grows, latency should remain below the limit set by the application. Replicability involves making sure that the system can maintain the same latency level under different conditions.

- *Aggregated communication time*. The aggregated communication time is the total time taken for all communications within the system over a given period. For example, a smart metering data collector may need to collect all smart meters' data in less than 15 minutes. Scalability and replicability involve maintaining aggregated communication times below the limit under different conditions.

- *Bandwidth*. The bandwidth indicates how much data can be transmitted through the communication channel in a given time. This can constitute a very important require-

ment when the communication channel is shared with other applications. As the system scales, it should keep the bandwidth used at acceptable values.

- *Reliability*. This concept is related to the system's ability to correctly deliver the information that is transmitted. This is an important requirement in all ICT, but especially in those that rely on wireless communications, as the signal may not reach its destination under certain conditions (e.g., heavy wheather). Data loss can reduce the stability of the grid [153] and have an economic impact on the grid [154]. A scalable and replicable system must be able to maintain high reliability regardless of size and conditions.

- *Coverage*. It refers to the geographical or network extent to which the communication system can serve effectively. It is a very important requirement in wireless communications to guarantee scalability and replicability and is deeply related to the reliability of the system.

- *Memory*. Memory usage refers to the Random Access Memory (RAM) and storage consumption of the components that make up the system. Scalability requires efficient memory management of the different components to face increasing loads and avoid information bottlenecks that end up affecting the final application of the system.

In large ICT systems, data collection and analysis of these requirements may be an extremely complex task. However, the scalability of a system is usually determined by those components that could potentially generate communication bottlenecks, so by restricting the scope of the ICT SRA to these critical components and their direct connections, the scalability of the entire system can be analysed. To identify potential information bottlenecks, a fast and simple approach is to analyse the system topology: as Figure 4.6 shows, information bottlenecks may appear in components that receive information from many components (many-to-one communications), send information to many components (one-to-many communications), and communicate bidirectionally with other components. In addition to this, when identifying potential information bottlenecks, the frequency of information exchange must be considered. As mentioned previously, the higher this frequency, the higher the likelihood of an information bottleneck when scaling up the system.

4.3.4 Development of scenarios

The scenarios analysed during the ICT SRA should cover a wide range of possible conditions for the replication of the system. For each scenario, its scalability in size (i.e., increasing the number of users, devices, or systems) should be evaluated. The conditions or characteristics that define each scenario must be identified for each SRA and may be related to the ICT used, to the place where the system is implemented (environment), the devices deployed and the functional characteristics of the system for the use case under study. At least one condition

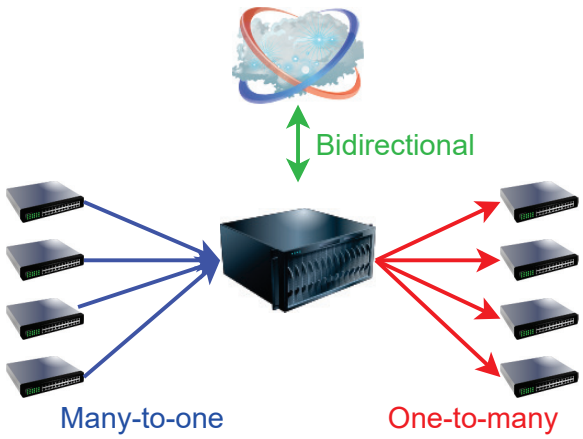

Figure 4.6: Types of communications between devices and/or systems to consider for the identification of potential bottlenecks.

should be different from one scenario to another so that the impact on performance can be better assessed.

The type of ICT used (i.e., wired or wireless) may set conditions such as the topology of the system (wired technologies may allow for bus or star topology), distance or area to be covered, or the BER. In addition to this, some communication protocols can be configured in different ways, which may fit larger-scale versions of the system more effectively.

The environment in which wireless communications are deployed can have a major effect on their performance. Different scenarios should be taken into account, including various types and sizes of obstacles, interference, and ambient noise.

The deployed devices could also provide some interesting scenarios for analysis. If the solution involves multiple types of device, scenarios with different shares of each type could be assessed. An interesting scenario could be defined to analyse the effect on performance when a different communication protocol is used on devices that are compatible with multiple protocols and standards, as long as the functionality of the use case is not affected.

Finally, functional characteristics could also be the basis for some scenarios. For example, for the analysis of scalability in density, different information sizes could be considered. However, it is important that the functional characteristics that are modified as part of a scenario do not alter the minimum requirements of the use case. That is, in a comprehensive SRA, an scenario should not involve changing any of the requirements by which the performance of the ICT system is to be evaluated.

4.3.5 Definition of Key Performance Indicators

When applying the methodology proposed, the KPIs defined for the specific ICT system under analysis must have the following main characteristics:

- They must allow to evaluate whether the ICT system meets the minimum requirements identified previously. Therefore, the KPIs should be related to these requirements and technical constraints.
- It must be possible to measure or calculate them in all the scenarios analysed.
- For each KPI defined, an acceptance threshold must be stated. This, again, is determined by the requirements of the use case.

4.3.6 Development of a simulation model or experiment

The are two main approaches to perform quantitative SRAs of ICTs: performance tests with actual or emulated hardware and software, or simulations.

Conducting a SRA through laboratory tests or emulated hardware/software can be very precise, but it often requires a large financial investment to acquire the necessary equipment. In certain cases, the lack of resources for the analysis requires the simulation of some components [140]. In other cases, equipment is used to replicate the performance of a particular system involved (e.g., internet delays in [137]). This approach can be cost-effective when researching platforms or software [148], [155], [156], since the wide range of cloud providers allows creating production-like environments and collecting statistical data.

The most cost-effective and efficient way to conduct an ICT SRA is through simulations. This method is usually much faster to set up than a laboratory setting and provides a great deal of flexibility for exploring various scalability and replicability scenarios. When the technology being studied is wireless, simulations are practically the only way to carry out a comprehensive SRA, as it would require a large amount of resources to do so in an experiment.

Three main communication network simulators are typically used: NS-3 ([126], [142], [146], [147], [157]), OPNET ([126], [141], [144], [158]), and OMNeT++ ([135], [145]).

NS-3 is a widely used, open source, discrete event network simulator, primarily employed in academia, that is centered on internet systems (wired and wireless). Despite its popularity, it is more challenging to use than other simulation frameworks due to the lack of graphical user interface tools [159].

Riverbed Modeler (formerly OPNET) is a commercial discrete event network simulator that offers a variety of validated models for different types of networks and technologies. This simulator provides a user-friendly graphical interface to configure and run simulations [159].

OMNeT++ is an open source discrete event simulation platform designed for the simulation of wired and wireless communication networks. It has a variety of open source extensions that increase its capabilities.

Apart from communication network simulators, MATLAB, Simulink, and Octave can also be used to evaluate the performance of ICT [139], [143], [160]–[162].

The simulation software chosen for the analysis will be based on the knowledge and preferences of the user, the characteristics of the analysis, and the availability of free models [159].

4.3.7 Run scenarios and analysis of results

Regardless of the approach selected for the analysis (simulation or experiment), the results of the ICT SRA can be represented in an ICT scalability and replicability map so that the main conclusions of the analysis can be drawn quickly and efficiently. This is a novel way of visualising ICT scalability and replicability results, being, together with the methodology, a contribution of this thesis, and constitutes a valuable tool when considering scaling up or replicating the system in the future.

Figure 4.7 shows an example of the structure and visual representation of an ICT scalability and replicability map. In the example, the SRA identified five key conditions to be considered in the scenarios, which are placed in the left column of Figure 4.7. There are a total of 12 values for these conditions, placed in the right column of Figure 4.7: conditions 1 and 2 can adopt three exclusive values each, whereas conditions 3, 4, 5 can adopt two exclusive values each. Therefore, 12 scenarios are the minimum number of scenarios for the SRA (for each scenario to change at least one condition value).

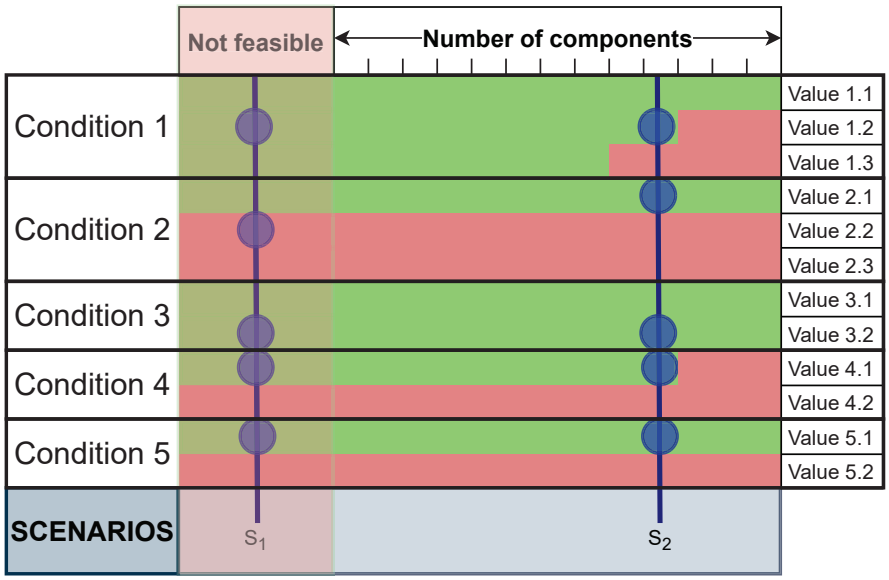

Figure 4.7: Structure and visual representation of an ICT scalability and replicability map.

The scenarios are represented by a vertical line placed corresponding to the maximum number of components (i.e., sensors, servers, etc.) the system would support while fulfilling all the requirements set for the system. For each scenario, its conditions are represented graphically by a blue circle. If the system does not comply with the requirements in a scenario

for any number of components considered, it is placed in the "Not feasible" zone of the map (S_1 in Figure 4.7).

Regarding the colours in Figure 4.7, green colour means that the system is, in general, scalable and replicable in that range of number of components when the system is under that specific condition, while the red colour indicates that the system would not meet the minimum requirements. Therefore, when analysing a scenario, the maximum number of components supported by the system will be determined by graphically placing the scenario where all the conditions (i.e., blue circles) are in a green area.

For simplicity, only two scenarios (S_1 and S_2) are exemplified in Figure 4.7. For example, condition 1 could represent *Information size* with three possible values (*value 1.1* = 2 Bytes, *value 1.2* = 4 Bytes, and *value 1.3* = 8 Bytes). Green and red bars in Figure 4.7 show that, in a scenario considering *value 1.3* instead of *value 1.2*, the ICT system would support the connection of fewer components. This can be visually seen by moving the blue circle of value 1.2 one step below (adopting value 1.3), entering into a red area, meaning that the system would not comply with the minimum requirements for that number of components. The maximum number of components when condition 1 adopts value 1.3 is determined by the green area.

Placing the ICT SRA results in a scalability and replicability map not only facilitates the task of summarising the results of the analysis and its conclusions, but also the analysis of the impact of each scenario's condition on the scalability and replicability of the system.

4.4 Application of methodology: case studies

Below, the quantitative ICT SRA methodology is applied to two case studies (A and B) that use wired and wireless technologies, respectively, to validate its applicability.

4.4.1 Case study A

This case study examines the monitoring and control system for a self-consumption solution demonstrated in Dijon, France, as part of the EU-funded RESPONSE project. The demonstration site will contain several energy storage assets, with a total capacity of 510 kWh, and a PV power plant of 228 kWp. The operation of electricity storage is aggregated through a BMS, while the solar PV generation is just monitored using a data logger. The objective of the system is to maximise the self-consumption ratio of one building by monitoring the solar PV generation and managing the charging / discharging of the batteries hourly, as indicated by EDF, the provider of the solution. If this system is scaled-up, it could potentially provide service to more than one building or involve more assets. In addition to this, if it works well under different conditions, it could be implemented in more places. To assess

this, an ICT SRA should be carried out. The ICT SRA methodology presented in the previous section is applied to this case and described below.

Step 1): Map the ICT system on the SGAM

Figure 4.8 shows the component layer of the SGAM for the system. It consists of four main elements: the cloud, Equipement Modulaire de Protection des Accès Industriels Répartis (EMPAIR), the BMS, and the PV data logger.

The BMS device is responsible for the management of the batteries deployed to provide electricity when needed, while the PV data logger is responsible for the management of the solar PV panels installed.

The EMPAIR is a device that implements a set of hardware and software methods for cybersecurity. It can be installed either in electrical substations (station/field zone of the DSO) or in renewable power plants (field zone of the customer domain). To communicate with the BMS and PV data logger, Modbus TCP protocol is used. EMPAIR is compatible with different communication protocols (IEC 61850 Manufacturing Message Specific (MMS), MQTT, IEC 60870-5-104, Modbus TCP/IP) and Application Program Interface (API) thanks to GeneSys, a control software for embedded applications.

The Cloud hosts an Energy Management System (EMS) named Clevery, developed by EDF, for the optimisation of energy production. It communicates with the EMPAIR by means of IEC 61850 MMS and a Virtual Private Network (VPN) tunnel.

Step 2.a): Scalability and replicability questions

Some initial scalability and replicability questions arise when observing Figure 4.8:

1. What would be the effect of placing the EMPAIR in the distribution domain? This would mean increasing the size of the Local Area Network (LAN) or, in other words, increasing the distance (i.e., the length of the Ethernet cables) between the connected devices. There may be a maximum distance under which the operational requirements cannot be satisfied.

2. What would be the effect of increasing the number of devices connected to EMPAIR? This question could also be studied in combination with the previous one. When placed at a PEB level, the results would show the maximum number of devices that can be controlled within a building; when placed at a Positive Energy District (PED) level, the operational contour defined by the distance and number of devices could be obtained.

Taking into account these questions, Modbus TCP communications over Ethernet in the system is the key part for the SRA, as the connection between the cloud and the EMPAIR does not raise any significant questions, since it provides scalability by design: the connection of

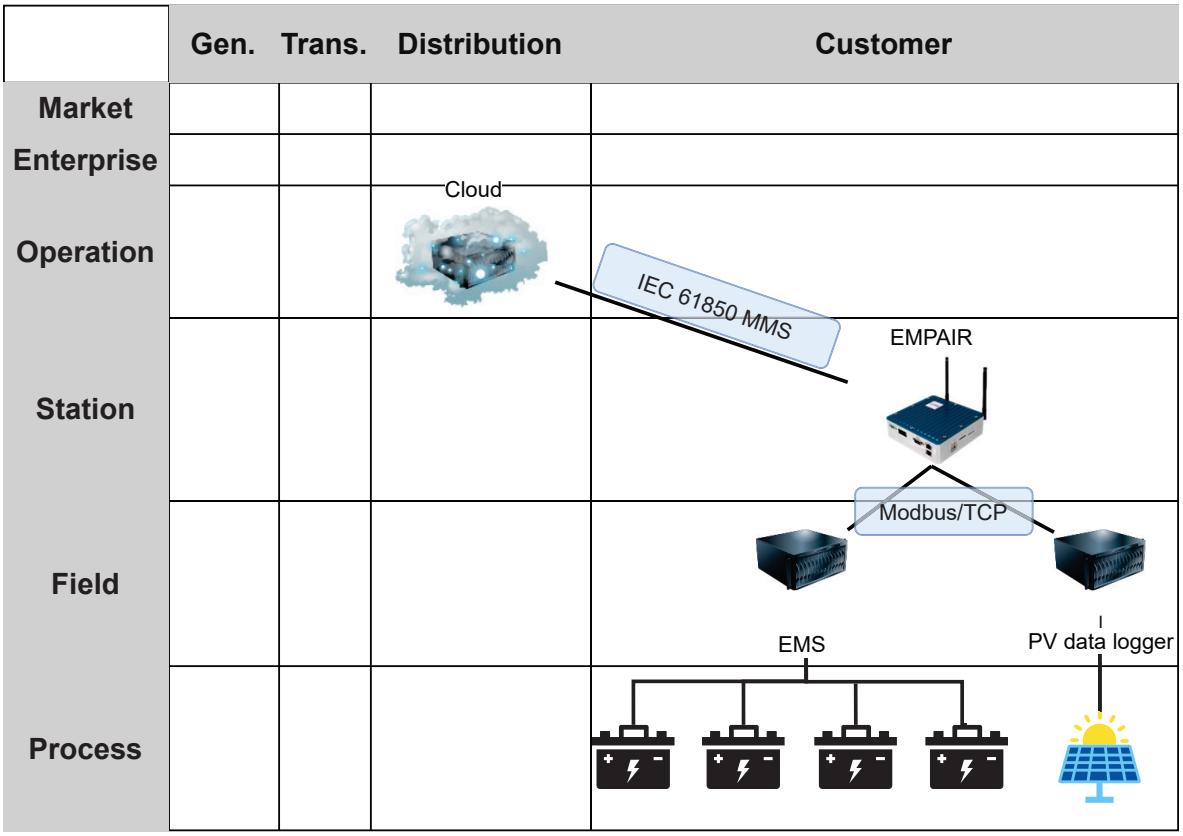

Figure 4.8: ICT system of case study A mapped into the SGAM. Component and communication layers.

more EMPAIR devices to the Cloud would not mean a challenge for the system. Therefore, the focus of the SRA will be the communications between the BMS, PV data logger and the EMPAIR device.

Step 2.b): Characterise the ICT system

The simplified SGAM layers of the DER control and monitoring system are depicted in Figure 4.9. An EMPAIR device is responsible for controlling and monitoring the solar PV and EMS (component layer). This is done through Modbus TCP, which uses Ethernet connections between devices (communication layer). An overview of the Modbus TCP protocol can be found in Appendix A.1. Measurements (battery and generation), control commands, and alarms are transmitted using the Modbus Protocol Data Unit (Modbus functions). The server for each type of information, its frequency of exchange, size, and the modbus function used to transmit the data are outlined in Table 4.2. These characteristics were given by the solution provider. The ultimate goal is to optimise the self-consumption of the PEB where the solution is implemented (business layer).

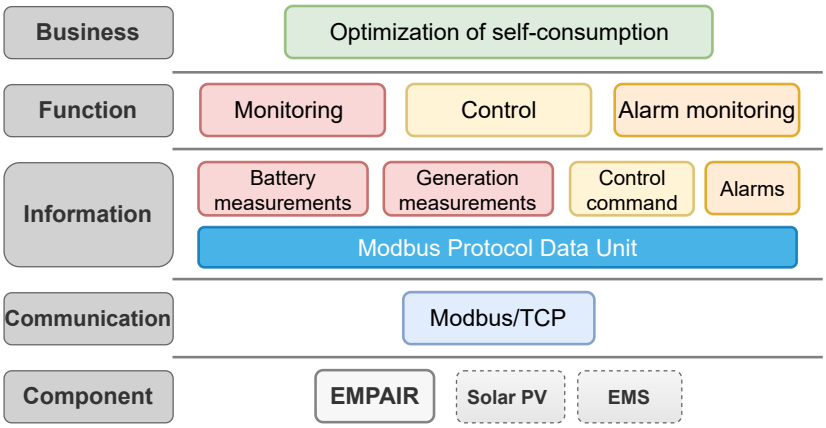

Figure 4.9: Simplified SGAM characterisation of the ICT system of case study A.

Table 4.2: Functional characteristics of the control and monitoring system studied in case study A.

Server	Information	Frequency of exchange	Size(B)	Modbus function
BMS	Measurements	1/h	48	0x03
	Alarms	1/min	1	0x01
	Control	1/h	16	0x10
PV data logger	Measurements	1/min	4	0x03
	Alarms	1/min	1	0x01

Step 3): Minimum requirements and technical constraints

The EMPAIR client can only establish a Modbus TCP connection with one server at once. According to the exchange frequency shown in Table 4.2, the control and monitoring system must take an average of one minute to request all connected servers (to finish the poll). This would constitute the main functional requirement for the system when scaling up. The use of Ethernet cables (in this case, Cat-5e UTP cable) would set a distance constraint, as they can only be used up to a maximum of 100m.

Step 4): Development of scenarios

To assess the scalability of the system under different conditions, all the scenarios will be analysed for, at least, the range of 2-192 servers in steps of 10 and for 24 h of simulation time. Two is the minimum number of servers deployed in the real implementation of the system. Table 4.3 shows the scenarios developed for the SRA of the ICT system in case

study A, where scenario A1 is the baseline scenario for the analysis. The parameters or conditions that determine the scenarios are the topology of the ICT system (star vs bus), the distance client-server, the type of devices (% of devices BMS - % of devices PV data logger), the BER, and the processing delay (time for the client to process the server's response).

Table 4.3: Scenarios simulated for the ICT SRA of case study A.

#	Topology	Distance [m]	Device types	BER	Processing delay [ms]
A1	Star	20	50-50%	10^{-12} 10^{-6} 10^{-5}	9
A2	Star	20	100-0%		9
A3	Star	20	0-100%		9
A4	Star	20	50-50%		4.5
A5	Star	20	50-50%		13.5
A6	Star	20	50-50%		0
A7	Star	100	50-50%	10^{-12}	9
A8	Bus	≤100	50-50%	10^{-12}	9
A9	Bus	≤100	100-0%	10^{-12}	9
A10	Bus	≤100	0-100%	10^{-12}	9

The main purpose of scenarios A2 and A3 is to evaluate the replicability of the system if only one type of server is considered (only BMS for A2, and only PV data logger for A3) with respect to the baseline.

Scenarios A4, A5, and A6 study the performance of the system if the client processes messages faster (A4), slower (A5), or if its process time is negligible (A6). To study the impact of BER on performance, the first six scenarios (A1-A6) will consider BER of 10^{-12}, 10^{-7}, 10^{-6}, and 10^{-5}. Although Ethernet transmission generally provide a BER of 10^{-12}, higher values represent worst-case scenarios, which must be considered for the replicability analysis.

Scenario A7 studies the performance of the system if the distance between the client and the servers is pushed to the limits of Ethernet ($\approx 100m$).

Finally, scenarios A8-A10 analyse what happens if the topology of the system is "bus" instead of "star", while keeping the distance to less than 100m.

Table 4.4 summarises the scenarios that should be considered to assess the impact on the performance of the ICT system in different aspects.

Table 4.4: Scenarios to be compared depending on the objective of the analysis for case study A.

Scenarios	Objective
A1-A2-A3 A8-A9-A10	Impact of device type
A1-A4-A5-A6	Impact of processing delay
A1-A7	Impact of distance
A1-A8 A2-A9 A3-A10	Impact of topology

Step 5): Define KPIs

The main requirement is that the EMPAIR must be able to request all the necessary information from all the servers in one minute. Therefore, the main KPI would be related to the time taken to complete the polling process, or polling time. As demonstrated in (4.1), the polling time in round j, (T_j), is calculated as the sum of the time it takes for the client to request, receive, and process all the necessary information from each server i at round j, for a total of N connected servers.

$$T_j = \sum_{i=1}^{N} t_{i,j} \tag{4.1}$$

To truly assess the performance of the system, thousands of rounds must be studied. Therefore, the average polling time for all rounds and its Standard Deviation (SD) have to be calculated as KPIs. If the system manages to keep the average polling time to 60s, but its Coefficient of Variation (COV) is higher than 0.5% (SD of 300ms), the client may be missing information from some of the servers in some rounds.

Step 6): Simulation model

The OMNeT++ simulator [163] was used to model the Modbus TCP network connecting EMPAIR to the BMS and the solar PV data logger. Modbus TCP is an application layer communication protocol for client-server communications between devices. The EMPAIR acts as the client and the BMS and PV data logger as the servers.

The client is assumed to be connected to the servers via a 100 Mbps Ethernet Cat-5e UTP cable, which has an estimated transmission rate of $2 \cdot 10^8$ m/s [164]. The client, depending on the type of server, sends up to three types of request with different characteristics (Table 4.2): *read measurements*, *read alarms*, and *write control commands*.

The processing delay in the baseline scenario (A1) was set to 9ms ($\sim$ 111 requests/s), which is an intermediate value between an ESP8266 chip and a Raspberry Pi [165].

The client can only establish a connection with one server at a time. After connecting, it requests the alarm values (which have the same frequency of exchange for both types of server) and assesses whether it should send any other requests after receiving the response. The polling time should be one minute. To compensate for any polling-time deviations from 60s, the client is programmed to use the last polling-time error for each new round. The priority of requests is: alarms, measurements, and then control commands. However, the client does not request more than two information objects in the same connection, as in the actual implementation.

Step 7): Results

The results of the analysis of the scenarios in case study A are presented in Figure 4.10, which provides the ICT scalability and replicability map of the Modbus TCP system analysed. The scenarios are placed graphically on the map depending on the maximum number of servers they would support, indicating with a blue circle their characteristics. It shows the impact that the type of device, the topology, the BER, and the processing delay have on the scalability and replicability of the system.

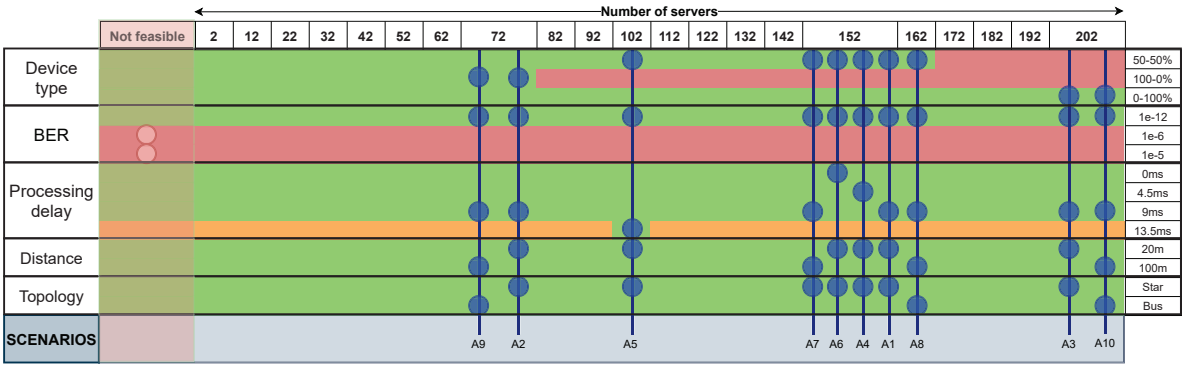

Figure 4.10: ICT Scalability and replicability map of case study A with the analysed scenarios.

Starting with the type of device, Figure 4.10 shows that increasing the share of BMS devices with respect to PV data loggers significantly reduces the number of servers that can be connected to the EMPAIR. In the baseline scenario, A1, which connects 50% of BMS and 50% of PV data logger, the maximum number of servers is 152 (a more detailed analysis of the baseline scenario can be found in Appendix A.2. This maximum increases to 202 servers when they are 100% PV data loggers (scenario A3) and decreases to 72 servers when they are 100% BMS devices. This is very interesting because it means that, although scenario A2 does not have margin to add 10 BMS to the operation of the system, it could add 4 BMS and 76 PV data loggers (converting scenario A2 to A1). It can be said that, in this case, from a functional point of view, one BMS device would be equivalent to 12.66 PV data loggers.

This can be explained by the functional characteristics presented in Table 4.2: once an hour, a BMS has to send more information (48 Bytes of measurements, which require more time to be transmitted) than a PV data logger. When this happens, the requirement of keeping a polling time of 60s must still be fulfilled, limiting the scalability of the system.

Although the limit of 152 servers in A1 (50-50% devices) can be increased to 162 by changing the topology of the system from star to bus, this change in the topology would not have any effect when all the servers are of the same type (scenario A9 with respect to A2, and A10 with respect to A3). Therefore, the topology has almost no impact.

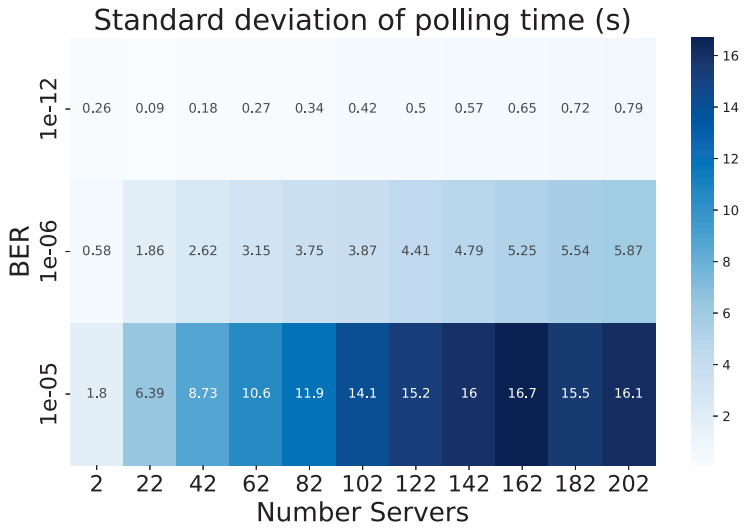

Figure 4.11: Standard deviation of the total polling time for different BER and number of servers in scenario A2.

Despite the fact that the type of device has a large impact, it is the BER of the Ethernet transmission that is determinant. Figure 4.11 shows the standard deviation of the polling time for scenario A2 (100% of BMS) for different BER and number of servers. It can be observed that only BER of 10^{-12} can provide some scalability to the system (72 servers in scenario A2, maximum SD of 300ms). This is aligned with the Ethernet standard (IEEE 802.3 [166]) which sets $BER \leq 10^{-12}$ for reliable operation.

With respect to processing delay, it obviously has an impact on the scalability and replicability of the system. Figure 4.12 shows the standard deviation of the polling time for scenarios A1 (baseline) and A5 (13.5 ms processing delay). A 42% increase of the processing delay decreases the maximum number of servers in 33% (from 152 to 102 servers). This increase in processing delay is translated into the same percentage increase in the SD of the polling time up to 182 servers, as shown by Figure 4.12. Since the processing delay affects all the requests made by the client (EMPAIR), regardless of the type of server, it can be expected to always have an impact on the scalability of the system. This means that, for example, the

scenario A2 analysed before would have a maximum number of servers lower than 72 when increasing the processing delay. For this reason, the scalability and replicability map depicted in Figure 4.10 shows an orange bar for a processing delay of 13.5 ms. If the impact on the SD keeps its proportionality, the maximum number of servers in scenario A2 is estimated to be 52 servers for a processing delay of 13.5 ms.

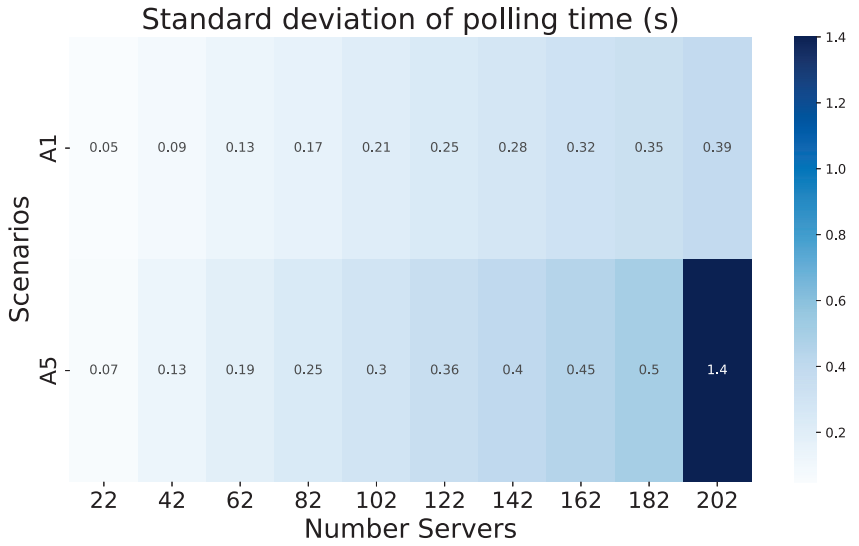

Figure 4.12: Standard deviation of the total polling time for different number of servers in scenarios A1 and A5.

Therefore, the ICT SRA results show that the scalability and replicability of the Modbus TCP control and monitoring system for DER are mainly determined by the type of connected devices and the processing delay of the client. When scaling-up the system, it is advisable to aggregate the operation of batteries under the less number of BMS possible, since the more BMS are connected to the EMPAIR, the less solar PV data loggers can be implemented. Regarding the processing delay, the upgrading of the EMPAIR device to better processing capabilities would increase scalability, but it would also increase the cost for this device. This could make sense if more than one building is included in the operation, since the system is found to be very scalable when the Ethernet cable is up to 100m long. This would allow the system to provide service to more than one building with multiple battery and solar PV assets, while using just one EMPAIR device. Although the bus topology increased the scalability of the system in one scenario, it had no impact on others, so it cannot be firmly stated which topology would be better for scaled-up deployments; therefore, the most appropriate topology can be selected based on the specific conditions of the deployment area, providing a great replicability potential.

4.4.2 Case study B

This case study examines the indoor conditions monitoring system implemented in a PEB consisting of 96 dwellings in Turku, Finland, as part of the EU-funded RESPONSE project. This solution deploys one sensor per apartment to measure the temperature and humidity conditions, which are sent to the EMS application in the Cloud through a data collector. The objective is, on the basis of the collected data, to regulate and optimise energy consumption while keeping comfortable conditions for the inhabitants of a residential building. Through the analysis of the scalability and replicability of the metering system, it could be optimised for its future implementation in other areas of the city (with different conditions), or at the city district level.

Step 1): Map the ICT system on the SGAM

Figure 4.13 illustrates the system mapped into the component layer of the SGAM. It is made up of three main components: Edge Cloud, Edge Hub, and Edge Sense.

The Edge Sense [167] is a wireless sensor that is placed in apartments to measure temperature and humidity. Therefore, it is in the customer domain and the process zone of the SGAM, as shown by Figure 4.13. It transmits these data multiple times each hour to the Edge hub via wireless M-Bus. Wireless M-Bus is a communication protocol mainly defined at the application, data link, and physical layers of the Open Systems Interconnection (OSI) model. An overview of the main characteristics of the wireless M-Bus protocol is provided in Appendix B.1.

The Edge Hub [168] is a building access point device that offers both Global System Mobile (GSM) and wireless M-Bus connectivity. It would be placed at the station/field zone of the SGAM. This allows the collection of sensor data and makes it available to the energy management service in the cloud. Although it constitutes a potential application for the future, this specific use case did not involve the provision of services to the DSO, so the Edge Cloud is considered to be in the operation zone of the customer domain.

Step 2.a): Scalability and replicability questions

By observing Figure 4.13, some initial scalability and replicability questions arise.

1. What would be the effect of increasing the area to be covered by the Edge Hub? This would mean increasing the distance between the Edge Sense devices and the Edge Hub, as well as increasing the number of sensors.

2. What would be the effect of increasing the number of sensors connected to the same Edge Hub? Since modifying the distance will be very limited by the wireless communication, increasing the number of sensors connected to a single Edge Hub could pose a

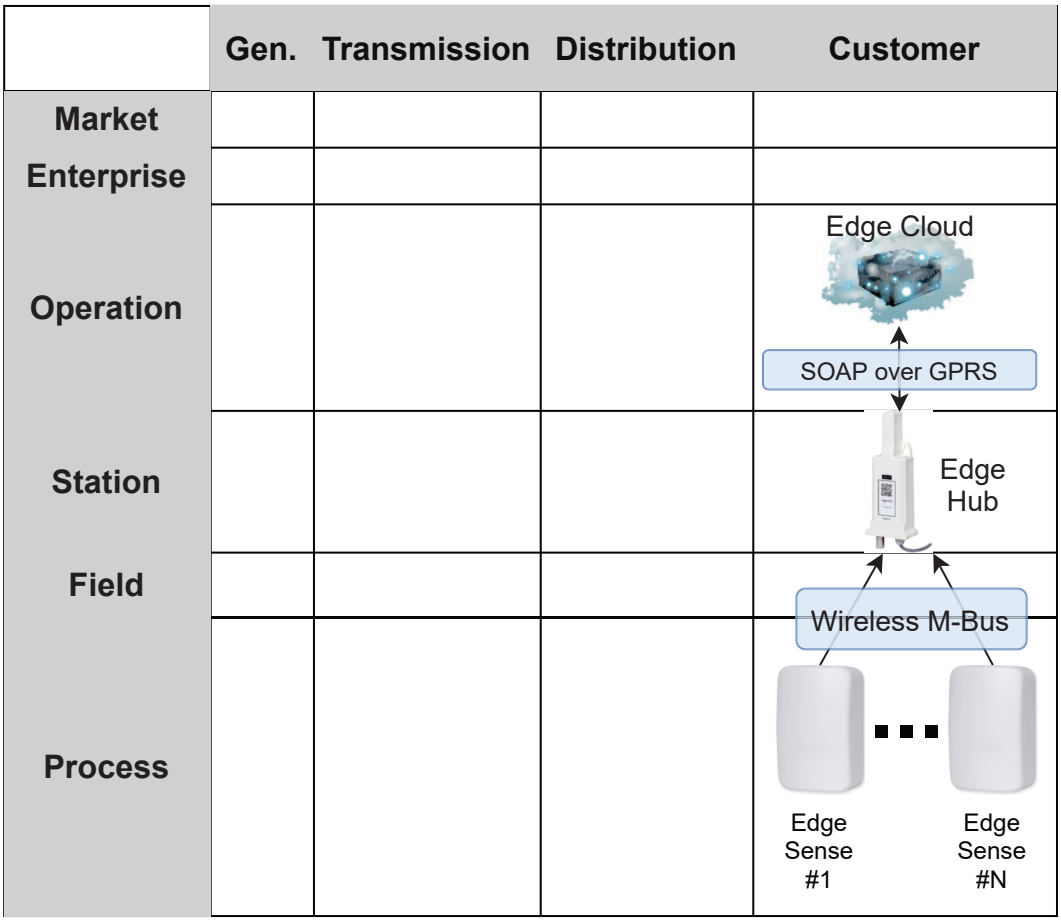

Figure 4.13: ICT system of case study B mapped into the SGAM. Component and communication layers.

significant challenge: the wireless medium is shared by all the sensors, and all of them need to send their measurements at a minimum time interval.

Based on these questions, the wireless M-Bus communications of the system is the key part for the SRA, as the connection between the Edge Hub and the cloud does not pose any significant questions about scalability and replicability. Therefore, the focus of the SRA will be the communications between the sensors and the Edge Hub.

Step 2.b): Characterise the ICT system

The simplified SGAM layers of the Wireless M-Bus system analysed in case study B are depicted in Figure 4.14. Table 4.5 outlines the technical characteristics of the multiple sensors that communicate with a single Edge Hub. The purpose of the system is to monitor the indoor conditions in order to optimise energy consumption and achieve the desired indoor climate while using the minimum energy possible. The messages transmitted by the Wireless M-Bus

are expected to be of a few bytes in size, containing information such as indoor temperature and humidity.

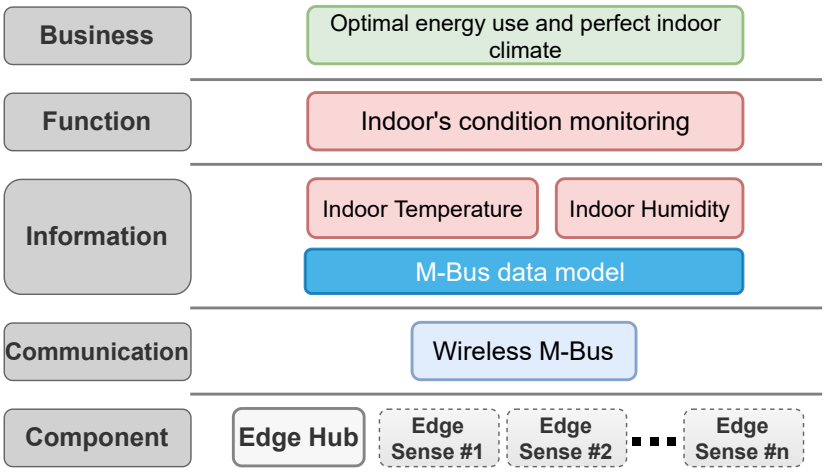

Figure 4.14: Simplified SGAM characterisation of the ICT system of case study B.

Table 4.5: Summary of characteristics of the sensors [167] and Edge Hub [168].

	Edge Hub	**Sensors**
Standards	EN 13757-3/4:2013, and OMS 4.0.2	EN 13757-3/4:2013, and OMS 4.0.2
Frequency	868.3 and 868.95 MHz	868.3 and 868.95 MHz
Sensitivity	–112 dBm for S-mode	<14dBm
Antenna	External	Dual Internal Diversity

Step 3): Minimum requirements and technical constraints

The optimisation algorithm requires data frequently. Sensors must provide new measurements at least every 15 minutes, which is a common time interval for smart meters. Therefore, the Edge Hub has to be able to receive measurements from all the sensors deployed in $\leq$ 15 minutes (aggregated communication time); if it takes more time, some sensors' measurements will be missed. This means that the Edge Hub constitutes a potential information bottleneck of the ICT system. Since wireless communications share the transmission medium (i.e., the air), some factors should be considered for the SRA:

- Presence of obstacles to the wireless transmission, such as walls, objects, etc.

- Presence of background noise due to other devices.

- Probability of message collision. If sensors send information to the Edge Hub at the same time, messages will collide and be missed. To avoid this, wireless M-Bus defines a first-transmission and retransmission scheme. To achieve a probability of reception of 95%, each message must be sent at least twice within the update period (15 minutes). Based on the EN 13757-4:2019 specification, the first transmission time for the baseline system will be defined by a uniform distribution between 0 and 300s (5min). The retransmission time interval, t_{acc}, of each message is determined by (4.2). The nominal transmission time (t_{nom}) is set to 300s and n_{acc} is the access number, which must be between 0 and 255. Each sensor randomly generates a new n_{acc} when installed and increases it by one every 15 minutes, restarting when it reaches 255.

$$t_{acc} = \left(1 + \frac{|n_{acc} - 128| - 64}{2048}\right) \cdot t_{nom} \tag{4.2}$$

Step 4): Development of scenarios

Figure 4.15 shows the baseline building block (96 dwellings, 2500m^2) of the system.

Figure 4.15: Baseline building block in Turku, Finland, for case study B.

To assess the scalability of the system under different conditions, all the scenarios developed will be analysed for, at least, the range of 96-192 sensors in steps of 12. 96 is the minimum number of sensors because this is the number expected to be deployed in the actual implementation. Table 4.6 shows the scenarios developed for the SRA of the ICT system in case study B, where scenario B1 is the baseline scenario for the analysis. The parameters that determine the scenarios are the area to be covered by the system, the thickness of the walls of the buildings, the size of the information transmitted, the background noise, and the statistical distribution considered to determine the first transmission time of the messages.

Table 4.6: Scenarios simulated for the ICT SRA of case study B.

#	Area [m^2]	Wall thickness [cm]	Information size [B]	Background noise [dBm]	Statistical distribution
B1	2500	10	38	-90	Uniform
B2	2500	10	19	-90	Uniform
B3	2500	10	57	-90	Uniform
B4.1	2500	10	38	-70	Uniform
B4.2	2500	10	38	-60	Uniform
B5	2500	10	38	-90	Gaussian
B6	2500	10	19	-90	Gaussian
B7	2500	10	57	-90	Gaussian
B8	2500	20	38	-90	Uniform
B9	5000	20	38	-90	Uniform
B10	5000	10	38	-90	Uniform
B11.1	5000	10	38	-70	Uniform
B11.2	5000	10	38	-60	Uniform
B12	5000	10	38	-90	Gaussian

Scenarios B2 and B3 are load scenarios (scalability in density), as the information size is modified to 50% (B2) and 150% (B3). Scenarios B4.1 and B4.2 constitute replicability scenarios, as the background noise is changed to -70 and -60 dBm, respectively.

Previously, it was mentioned that the first transmission time for the messages in the baseline system is defined by a uniform distribution between 0 and 300s (5 minutes). An interesting replicability scenario would be what the performance of the system would be if, instead of a uniform distribution, a Gaussian distribution was implemented. Scenarios B5, B6, and B7 are equivalent to B1, B2 and B3 but with a Gaussian distribution. The means considered for the distribution are (in minutes): 2.5, 5, 7.5 and 10; whereas the standard deviations considered are: 2.5, 5, and 7.5. Therefore, twelve distributions can be analysed for scenarios B5, B6, and B7.

To study the performance when increasing the thickness of the walls of the building, which can be significant in wireless communications, scenario B8 considers an increase of 10cm of the wall thickness. Baseline thickness is 10 cm, which is approximately the thickness

of the walls in the actual demonstration site in Turku (Finland), where buildings are designed for a cold climate. Therefore, increasing wall thickness can be considered a worst-case scenario that would guarantee a very high replicability potential if the system works well under these conditions. While keeping the conditions of scenario B8, scenario B9 doubles the area to be covered by the solution (scalability in density and size). This would mean considering two building blocks as the one shown by Figure 4.15. With the only exception of this larger area, scenarios B10, B11.1, B11.2, and B12 are homologous to scenarios B1, B4.1, B4.2, and B5, respectively.

Table 4.7 summarises the scenarios that should be considered to assess the impact on the performance of the ICT system.

Table 4.7: Scenarios to be compared depending on the objective of the analysis for case study B

Scenarios	**Objective**
B1-B2-B3 B5-B6-B7	Impact of information size
B1-B4 B10-B11	Impact of background noise
B1-B5 B2-B6 B3-B7 B10-B12	Impact of the statistical distribution of first-transmission time
B1-B8 B9-B10	Impact of wall thickness
B1-B10	Impact of area size

Step 5): Define KPIs

Since the most restrictive requirement is that the Edge Hub must get data from all the sensors every 15 minutes, the reliability of the wireless M-Bus communications must be assessed.

For this, the three main KPIs taken into account are the delivery ratio of the network, the message error ratio, and the gross delivery ratio. The delivery ratio (4.3) measures the proportion of messages with new data that are received (i.e., not including retransmitted messages) and correctly processed by the Edge Hub, while the message error ratio (4.4) measures the proportion of messages received with errors (including retransmitted messages) due to interference.

$$Delivery\ ratio = \frac{\#Messages\ processed}{\#New\ data\ messages} \tag{4.3}$$

$$Message\ error\ ratio = \frac{\#Erroneus\ messages}{\#Messages\ received} \tag{4.4}$$

The gross delivery ratio (4.5), on the other hand, measures the proportion of messages that reach the Edge Hub, including those with errors, with respect to the total number of messages that have been sent by sensors (including retransmitted messages).

$$Gross\ delivery\ ratio = \frac{\#Messages\ received}{\#Messages\ sent} \tag{4.5}$$

Step 6): Simulation model

The wireless M-Bus network is simulated using the OMNeT++ simulator [163]. The sensors and the Edge Hub were modelled according to their technical specifications [167], [168] (Table 4.5).

The wireless M-Bus communications are modelled considering the following characteristics:

- Transfer S-mode of wireless M-Bus is used.
- Messages have a total size of 38B in the baseline scenario.
- Communications are unidirectional (i.e., S1 mode); from the sensors to the Edge hub. Characteristics of S1 mode can be found in Appendix B.1.
- Sensors take new measurements every 15 minutes.
- The only impediments to the wireless signals taken into account are the walls and floors of the buildings, supposing that they are constructed of concrete. To this end, the 3D model of the PEB, depicted in Figure 4.16 (top view), was created in OMNeT++.

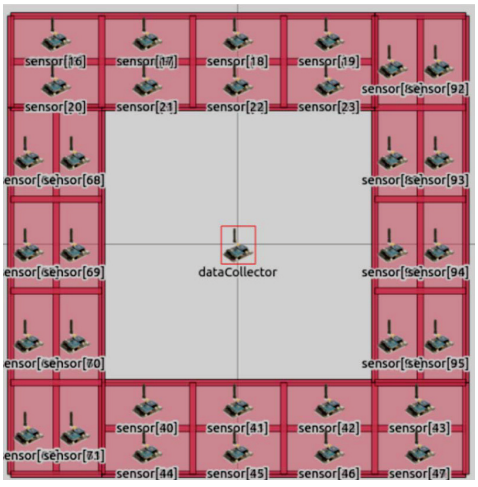

Figure 4.16: Top view of the 3D model in OMNeT++ for the PEB.

- The transmission medium model implements three models included in the INET library [169]: the free-space path loss model (FSPL), the Isotropic Dimensional Background Noise model (background noise model), and the dielectric obstacle loss model. The formulation of these models described in Appendix B.2. The FSPL model + obstacles is chosen for the simulation because it provides a realistic performance level compared to other models in similar environments (log-normal, ITU-R P.1238) when an empirical model is not possible. The analysis of the impact of different propagation models on the scalability analysis is presented in Appendix B.3.

Step 7): Results

The results of the analysis of the scenarios in case study B are presented in Figure 4.17, which provides the ICT scalability and replicability map of the wireless M-Bus system analysed. The scenarios are placed graphically on the map depending on the maximum number of sensors they would support, indicating with a blue circle their characteristics.

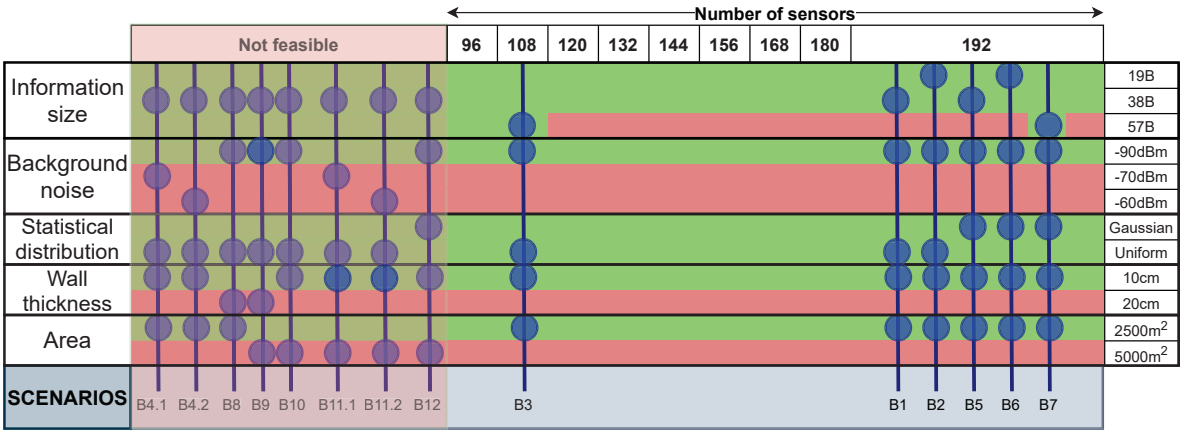

Figure 4.17: ICT Scalability and replicability map of case study B with the analysed scenarios.

Starting with scenarios that allow for the scalability of the system, the effect of the size of the information is remarkable. The baseline size (38B) and a smaller one (19B) do not have an impact on the scalability of the system, allowing it to scale up to 192 sensors, while a larger one (57B) limits the scalability to 108 sensors (scenario B3). This is explained by the low data rate of the S-mode in wireless M-Bus (16,384 kbps) and the use of a uniform distribution of 5 min for the first transmission. Larger messages require longer transmission times, increasing the probability of message collision as the number of sensors increases.

However, scenario B7 manages to overcome this limitation imposed by the size of the information. This scenario allows the deployment of up to 192 sensors by using a Gaussian distribution instead of a uniform distribution for the first transmission time of messages. Figure

4.18 shows that this is true for all the Gaussian distributions considered and that outstanding performance can be expected when the standard deviation time is 7.5 min. This means that, when replicating the solution, if a larger amount of information needs to be transmitted per sensor (for example, because they include additional measurements or other data), a better approach would be to configure the sensors to follow a Gaussian distribution instead of a uniform one for the first transmission.

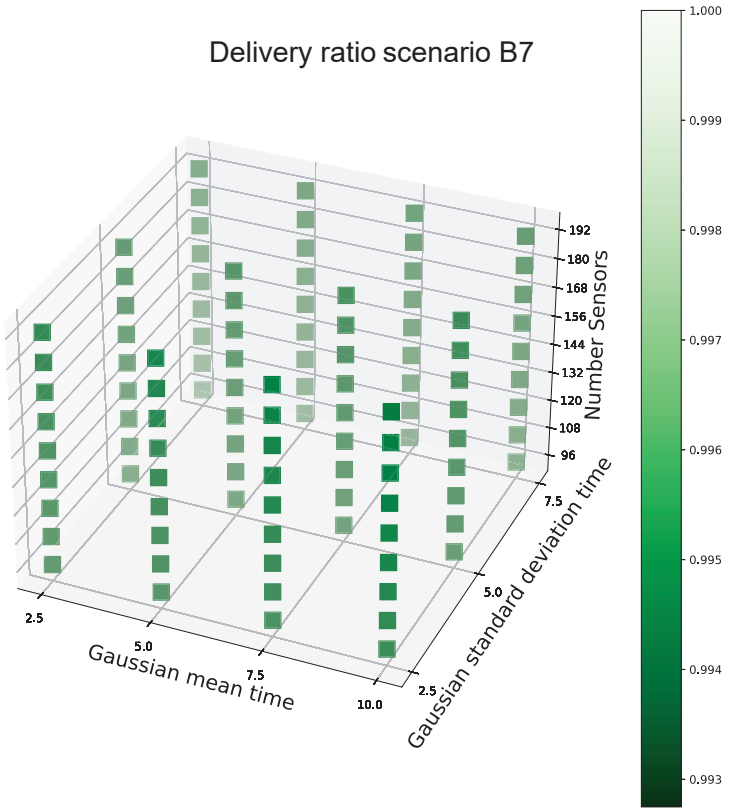

Figure 4.18: Delivery ratio of scenario B7 depending on the standard deviation and mean (in minutes) of the Gaussian distribution used to determine the first transmission time of messages.

It should be noted that 57% of the scenarios studied would not allow the scalability and replicability of the ICT system. This means that the system would have to reduce the number of sensors from the demonstration's 96 sensors in order for the system to be replicated in scenarios B4.1, B4.2 and B8-B12. By considering these scenarios, it is possible to gain useful knowledge about the scalability and replicability of the wireless M-Bus system. For this, Figure 4.19 plots the delivery ratio, the message error ratio, and the gross delivery ratio of the baseline scenario (B1) and scenarios B4.1, B4.2, B8 and B10. In it, it can be seen that the delivery ratio and message error ratio are mainly influenced by the conditions set for the scenarios (no influence of the number of sensors is observed), whereas the gross delivery

ratio, which is related to message collision, decreases slightly when increasing the number of sensors (except for B8).

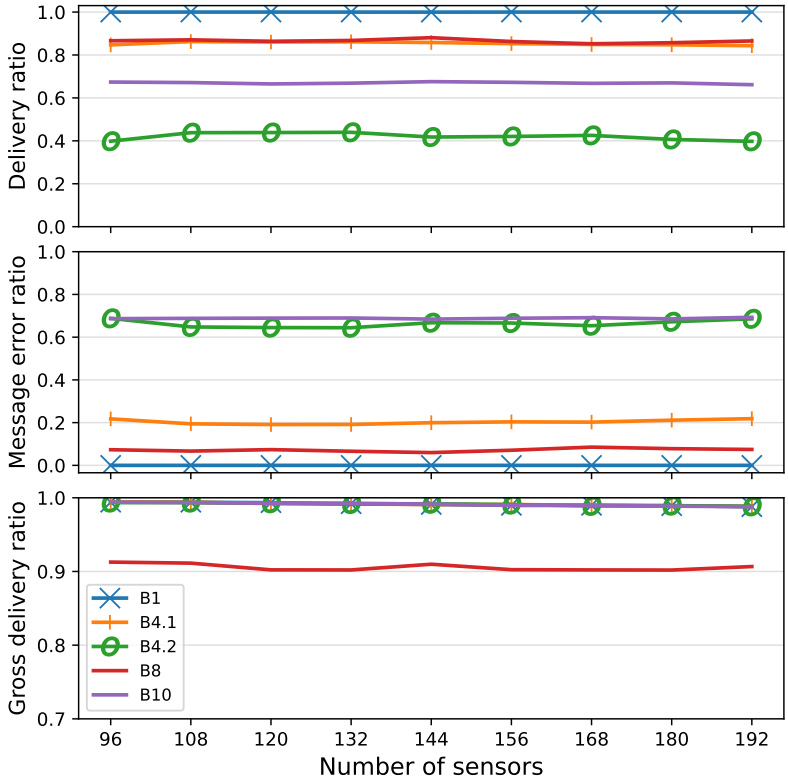

Figure 4.19: Delivery ratio, message error ratio, and gross delivery ratio of scenarios B1, B4.1, B4.2, B8, and B10.

Scenarios B4.1 and B4.2 in Figure 4.19 show that the impact of background noise is significant. In urban settings, a background noise level of -90dBm is considered acceptable and has no effect on the system analysed. However, if the noise is higher, such as -70 or -60 dBm, the system's capabilities will be significantly reduced. Although the delivery ratio is close to the acceptable threshold (0.9) in scenario B4.1, its message error ratio is excessive ($\approx$ 0.2) for the use case. Regarding scenario B4.2, less than half of the new measurements are received, showing an extremely poor performance.

The impact of wall thickness is shown by scenario B8 in Figure 4.19. Increasing the wall thickness from 10cm (B1) to 20cm (B8) implies a decrease in the delivery ratio of $\approx$ 0.15. Despite this could be considered a moderate decrease (the delivery ratio in scenario B8 is close to the acceptable threshold of 0.9), in this case the impact on the gross delivery ratio should also be considered. This ratio is $\approx$ 0.9 for scenario B8, which means that approximately 10% of the messages do not reach the data collector. Since this ratio remains quite stable regardless of the number of sensors, the main cause for non-received messages is not message collision but the thickness of the obstacles, which prevent messages from reaching

their destination.

Scenario B10 in Figure 4.19 shows the impact on performance of increasing the deployment area from $2500m^2$ to $5000m^2$. Despite the gross delivery ratio remains invariant with respect to B1 (low impact of message collision or lost messages), the delivery and message error ratios are much worse (both are ≈ 0.7). These ratios show an interesting fact: although 70% of the messages are not properly processed due to the presence of errors, the remaining 30% that do not contain errors account for 70% of the measurements that need to be processed. This could mean that the data collector cannot process the messages from the sensors that are further away, since the obstacles and background noise that the signal encounters on its way decrease the Signal-to-Noise Ratio (SNR) at the receiver, which increases the BER, and that a second data collector is necessary, which would require further analysis. These results, together with those presented in a preliminary analysis of this system [170], indicate that the system presents a high density scalability: As long as the area of deployment does not increase from $2500m^2$, the system would be able to support at least 384 sensors [170]. However, the performance of the system is deeply affected when scaling in area size.

Therefore, the boundaries for the scalability and replicability of the wireless M-Bus system for smart metering and sensoring using just one data collector are determined by the size of the information to be transmitted (which can be overcome by implementing a Gaussian distribution for the first transmission), by the background noise of the environment, by the size of the area to be covered, and by the thickness of walls. If the information sent in every message is 38B or less (e.g., using compressed formats), a large number of sensors can be potentially deployed (at least, 192 sensors) in an area of $2500m^2$ as long as the background noise is kept to common levels (-90dBm) and the thickness of the concrete walls is 10cm or less. Before replicating the solution, the background noise of the site should be measured to make sure there is not too much interference. Regarding wall thickness, concrete walls of more than 10 cm in residential buildings are difficult to find, considering that the actual demonstration building has approximately this thickness and is located in Finland (cold climate). Thus, the wall thickness is not expected to limit the replicability of the solution; the fact that it works well with concrete walls of 10 cm makes it very replicable under more favourable conditions (e.g., warmer areas). However, these aspects should be checked when considering the replication of the system, when changing its characteristics, and when scaling up in density.

4.5 Conclusions

The inclusion of ICT in the scope of a technical SRA would allow a complete understanding of the scalability and replicability of smart grid solutions, which are increasingly dependent on ICT.

This chapter has presented a novel methodology to quantitatively perform an ICT SRA in a smart grid context. This methodology uses SGAM as a basis to characterise the system and define the scope of the analysis, as a quantitative approach may not be necessary in all cases. The proposed methodology does not depend on the use case, communication technology, or the quantitative approach (simulations or experiments) selected.

To validate this methodology, it was applied to two case studies comprising solutions that use different communication technologies and that are demonstrated in the EU-funded RESPONSE project. Case study A analyses the scalability and replicability of a Modbus TCP control and monitoring system for DER, while case study B analyses a wireless M-Bus system for smart metering and sensoring.

The ICT SRA results of both case studies are summarised by their corresponding ICT scalability and replicability maps, a novel concept introduced for this type of analysis. These maps allow for a quick overview of the scalability and replicability of an ICT system and for an efficient way of estimating the feasibility of potential scenarios that were not explicitly considered during the SRA.

The application of the methodology shows its effectiveness in analysing, in a structured way, the scalability and replicability of an ICT system by focusing on the most critical links, which are identified by a prior characterisation of the system. The clear identification of requirements and constraints allows to get clear conclusions about the scalability and replicability of the system and the main factors that have an impact on these, regardless of the type of ICT (wired or wireless), as it could be seen in section 4.4.

Chapter 5

Impact of cyberattacks to demand and distributed generation

5.1 Introduction

ICT scalability and replicability in smart grids are desirable features from a techno-economic perspective, as they reduce the need for costly infrastructure upgrades and deployment times. However, the potential cyber risk assumed may be related to this scalability and replicability; highly scalable and replicable ICT systems may present vulnerabilities that can be exploited by malicious actors, potentially having unauthorised access to a large number of devices that may alter the operation of the grid. These attacks could be equally scalable and replicable.

Taking into account the large scalability and replicability capabilities of IoT devices at the consumer level, cyberattacks may not only target utilities' Supervisory Control And Data Acquisition (SCADA) systems [171] but try to exploit the vulnerabilities of these devices [172]. In addition to being more vulnerable than SCADA systems, the surface of attack of electricity demand is larger, and high-wattage devices such as charging points for electric vehicles are not continuously monitored by SOs [84], [85]. As mentioned in Chapter 2, IoT devices generally have lower levels of security [78] and, when massively compromised, can be used to reduce the security margins of the system, cause load shedding, or cause a cascading failure that results in a wide area blackout [80], [173], [174]. This chapter will be devoted to the analysis of the effect of attacks in the power system to this type of devices.

In [175], the authors presented the concept of internet-based load altering attack, identifying direct and indirect loads that could be compromised through the internet, such as data centers, demand side management loads, and loads directly managed by customers (e.g., air conditioning, washing machines, etc.).

The term MaDIoT attack was first introduced by Soltan et al. [80] as an attack that disrupts the normal operation of the power grid by altering the power demand using IoT

devices to which the attacker has access.

Apart from demand, the increasing connection of DER to distribution grids also expands the range of possible attacks [81], [176]. If a malicious actor gains control over DER (e.g., by compromising an inverter [177]), it could impact the functioning of the system [82], [178]. Communication technologies commonly used in the control and monitoring of DER, such as Modbus, which was the technology analysed in the SRA of section 4.4.1, can be compromised in a cyberattack (e.g., reconnaissance, data modification and Denial of Service (DoS)) [176], [179], [180].

This chapter analyses the scalability and replicability of MaDIoT attacks by conducting two studies. The first study assesses the replicability potential of MaDIoT attacks by analysing and comparing their impact on power systems with different characteristics. For this, the IEEE 39 test system and a simplified model of the European power system (PST-16) are used. These systems differ mainly in their size (network and demand) and generation mix.

The second study expands the concept of MaDIoT attacks to include DER devices within the scope of the attack. We have called this combination of attacks against demand and DER devices MaDIoT 3.0 attacks. In addition to this, the impact of demand attacks on the PST-16 system with solar PV DG connected is analysed, so that the replicability of these attacks in these types of systems, which are becoming more common, can be studied.

This chapter is structured as follows. Section 5.2 briefly presents the state of the art of MaDIoT attacks. Section 5.3 describes the basic power system models used, the protection schemes included for the simulation of the attacks, the MaDIoT bot characteristics, the adversary model, and the criteria to consider an attack successful. Then, Section 5.4 analyses MaDIoT attacks in different power systems, whereas Section 5.5 presents the analysis of MaDIoT 3.0 attacks. Finally, Section 5.6 outlines the main conclusions.

5.2 State of the art

Load-altering attacks [175], [181] and MaDIoT attacks [80] can disrupt the normal operation of power grids by altering the demand using IoT devices to which the attacker has access. These attacks can cause local outages due to load shedding and the actuation of generators' protections [173], [182]–[186], or alter the energy market [187]. However, the success and impact of these attacks may depend on the power system analysed [8].

Soltan et al. [80] studied these attacks on the Polish grid model and concluded that these attacks may be scalable, causing local outages and large blackouts on the grid. However, [184] later suggested the possibility that the model analysed was not N-1 secure, which would lead to an overestimation of the impact of attacks.

Huang et al. [184] showed that causing a wide-area blackout in a large North American regional system through evenly distributed MaDIoT attacks is extremely challenging; even

if the grid was previously put in a vulnerable state, such attacks would only lead to partial blackouts due to the disconnection of a portion of the loads (via Under-Frequency Load Shedding (UFLS) protection) and generators (via Over-Frequency Generator Rejection (OFGR) protection). After this, the system would quickly recover its stability.

In [188], the authors studied scenarios in the IEEE 39-Bus system assuming that the attacker had advanced knowledge of the topology of the system and the estimated generation/demand for each node; this would allow the launch of more sophisticated attacks targeting the most vulnerable nodes, which received the name of MaDIoT 2.0 attacks. The results in [188] presented success rates between 67 and 91% in causing widespread blackouts; however, the criteria used to consider an attack successful were unclear, and the likelihood that an attacker has the required system knowledge and resources is presumably low.

In addition to demand devices, DER communications [189] and devices can also be the target of cyberattacks [81] to disrupt the normal operation of the power system.

Attacks on DER can cause problems with voltage regulation [83] and transient frequency instability [176], [190]. Solar PV installations can be disconnected from the system by compromising inverters and breakers or by inducing low, high, or zero voltage conditions [191]. These attacks may represent a higher risk than attacks on SCADA devices or monitor points [190], although to really cause an instability problem at the power system level, massive amounts of DER (e.g., $\geq$ 35% of solar PV penetration in California [192]) must be compromised.

The potential impact of a combined attack on demand and DER devices has not been studied in previous work. One could expect that attacking demand and DER would have a greater impact on the system or, at least, a greater success ratio than performing an equivalent attack only on demand in a system without DER. However, the benefits that the connection of DER provide to power systems must be considered.

5.3 Materials and methods

Similarly to [80], [184], [188], the studies presented in following sections use simulations to analyse the impact of MaDIoT attacks on power systems. These studies have been carried out within the framework of the EU-funded project eFORT.

The software used for the simulations is DIgSILENT PowerFactory 2022 SP3 (22.0.6.0).

In the following, a brief description of the base test systems used can be found, followed by an explanation of the protection schemes implemented for the analysis of MaDIoT attacks, the bot characteristics, the adversary model, and the criteria for attack success.

5.3.1 Power system models

Two different base systems are used for the analysis: the IEEE 39-bus system and the PST-16 benchmark system. Table 5.1 provides a summary of the characteristics of these models.

Table 5.1: Summary of the characteristics of the IEEE 39-BUS and the PST-16 models.

	IEEE 39-BUS	**PST-16**
Frequency (Hz)	60	50
Areas	1	3
Number of buses	39	66
Base active load (MW)	6097.1	15565
Base reactive load (Mvar)	1408.9	2225
Generators	10	16
Generation type	hydro, thermal	hydro, thermal, and nuclear
Max. active power generation (MW)	14535	18220
Line capacity (MVA)	With USA/Canada: 1231	Areas A-C: 1572 Areas B-C: 2476 Areas A-B: 2585
Voltage level (kV)	345	380, 220, 110

IEEE 39-Bus

It represents the New England power system, consisting of 39 buses, with a total base load of 6097.1 MW of active power and 1408.9 Mvar of reactive power (default conditions of the model in PowerFactory), which are the initial conditions of the system (before the attack) for the study in section 5.4. Since it is an American system, the electrical frequency is set to 60 Hz. This system has a maximum active power generation of 14535 MW, of which 8500 MW are provided by the generator representing the interconnection with USA/Canada in bus 39. However, the support of this USA/Canada connection is fixed at 1000 MW. Therefore, the actual maximum active power capacity of IEEE-39 is 6035 MW, and the available reserve would be 938 MW, since 1000 MW of demand are supplied by the interconnection. The interconnection bus (bus 39) is connected to the rest of the system through two power lines with a total capacity of 1231 MVA. In the initial conditions, the load connected to bus 39 consumes 1104 MW, and only 19% of the capacity of the interconnection lines is used.

Regarding the load model, the default dynamic load model of the IEEE-39 system model in PowerFactory is used.

PST-16 (Simplified European Model)

The PST-16 Benchmark System [193] consists of three areas (A, B, and C) and 66 buses, with a total base load of 15565 MW of active power and 2225 Mvar of reactive power, which are the initial conditions of the system (before the attack) for the studies in section 5.4 and section 5.5. The maximum active power generation of the PST-16 system is 18220 MW. Since it represents a European system, the electrical frequency is set to 50Hz.

For this system, the constant impedance load model is used [193]. Regarding the modelling of generators, the ones used by the base model were not altered. Details on the generator model and grid diagram can be found in [193].

Figure 5.1 shows a simplified diagram of the PST-16 system. Area A represents the north of Europe, with a high share of hydro generation, and areas B and C represent central and south Europe, respectively, with high shares of thermal and nuclear. As Figure 5.1 shows, area C concentrates the loads, so power has to be transferred from area A and B to area C through two long tie-lines. The capacity of the line connecting areas A-C is 1572 MVA, for B-C it is 2476 MVA, and for A-B it is 2585 MVA. Under the initial conditions (before perfoming the MaDIoT attacks), the loading of these interconnection lines is 110.1%, 17.3%, and 37.2%, respectively. The base conditions of the PST-16 system can be considered to correspond to the peak demand conditions, since it represents 85% of the generation capacity.

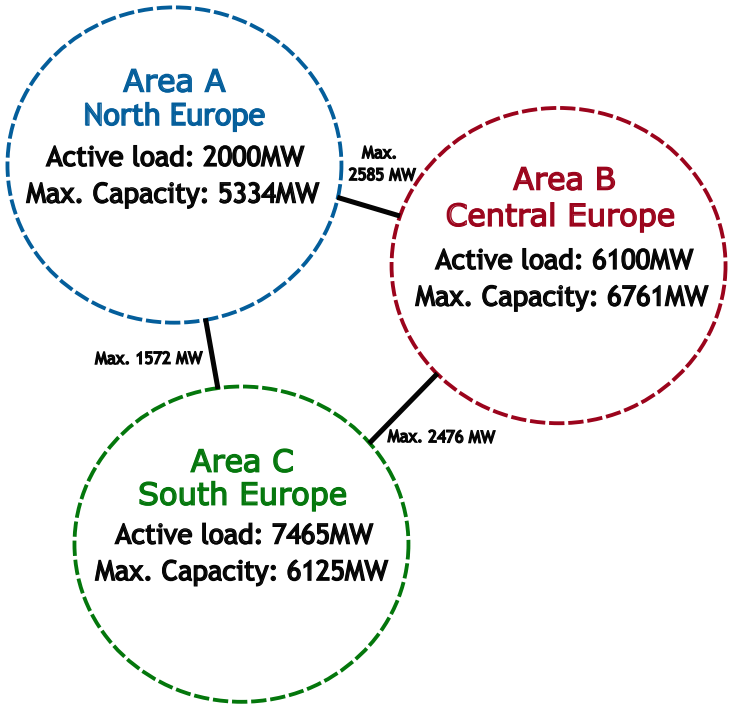

Figure 5.1: Simplified diagram and main characteristics of the PST-16 benchmark model.

5.3.2 Protection schemes

Four protection types that are relevant to the study were implemented in the test systems: overvoltage protections, undervoltage protections, an UFLS scheme, and an OFGR protection scheme. These are the only protections implemented in the simulated systems.

Overvoltage and undervoltage protections

These protections disconnect the loads when voltage is above (F59 phase overvoltage protection) or below (F27 phase undervoltage protection) a pre-defined value. Overvoltage protections are configured to trip when voltage exceeds 1.1 p.u for 10s, whereas undervoltage protections trip when voltage is below 0.85 p.u for 10s.

UFLS Protection

This protection scheme gradually disconnects loads from the system as the frequency drops below certain levels, as shown in Table 5.2. The actuation of the protection is instantaneous for each frequency level.

Table 5.2: UFLS scheme applied for the 50 and 60 Hz models (frequency vs. load to be shed)

Frequency Threshold (Hz)	**49** **59**	**48.8** **58.8**	**48.6** **58.6**	**48.4** **58.4**	**48.2** **58.2**	**48** **58**
Load-shed (%)	5	5	10	10	10	10

OFGR Protection

To protect the generators, the protection trips when the frequency at the generation bus reaches 51.7 Hz (PST-16) or 61.7 Hz (IEEE 39), which are values similar to those used in [184]. These protections disconnect the corresponding generator from the system.

5.3.3 MaDIoT bot characteristics

For the analyses, it is assumed that every compromised load (i.e., bot, in the cybersecurity jargon) consumes 3 kW of active power as in [188]. This could be the case of, for example, EV chargers. Trying to keep the power factors similar to those in the baseline test systems, the attack is considered to also imply a variation in the reactive power. The power factor of the demand (inductive) for the IEEE 39-bus and PST-16 systems is 0.97 and 0.99, respectively. Therefore, the reactive power of the bot is considered to be 0.69 kvar for the IEEE 39-bus system and 0.42 kvar for the PST-16 system.

For the demand, only MaDIoT attacks that increase power consumption are considered, as in [188]. Therefore, if, for example, 500k bots are compromised, the theoretical demand increment in the system would be 1500 MW; the actual increment during the simulation would depend on the load model. As in previous works [80], [184], [188], it is assumed that target devices can be compromised. Thus, the specific botnet (i.e., a group of bots) architecture is out of scope. However, it can be assumed that the devices are somehow compromised (e.g., they are accessible from the Internet and keep default passwords), and then malware is installed on them to allow remote command and control, as in the case of the famous Distributed Denial of Service (DDoS) attack orchestrated against the Domain Name System (DNS) provider Dyn back in 2016, which used millions of IoT devices infected with the Mirai malware [194], [195] and managed to put the Internet against the ropes.

5.3.4 Adversary model

Regarding the attacker, in [188] it is presumed to know details of the grid, such as its topology and power flows, so that voltage stability indexes can be calculated, identifying the most vulnerable nodes. This is justified by studies that state that much information can be obtained through openly available information [196] or by using satellite images (for example, Google Maps) [197]–[199]. This process can be very time-consuming, and it is extremely complex to check its accuracy to perform a power flow analysis. Furthermore, the attacker would need to have access to devices at all the nodes of the system or target specific nodes and try to find devices connected to those nodes that can be compromised.

However, an attacker may already have a botnet to exploit without knowing exactly where the bots are connected electrically but with a good idea of their proximity (e.g., by mapping the IPs). For this reason, it is considered in this document that the attacker does not have advanced knowledge of the grid, significantly reducing the amount of work the attacker would need to carry out before the attack and, therefore, increasing the possibility for the power system to suffer an attempt of MaDIoT attack.

Table 5.3 presents the adversary model according to the modelling guidelines provided by [200]. As mentioned previously, the adversary knowledge would be oblivious and the attacker does not have physical access to the assets (non-possession adversary access). MaDIoT attacks are targeted attacks (the objective are high-wattage IoT devices in section 5.4 and, additionally, solar PV inverters in section 5.5), and the attacker is considered to have substantial resources, tools, and skills to carry out the attack (class II). It should be noted that it is assumed that the attacker has managed to compromise the devices and install malware that allows for command and control, so that the attacker can control a massive number of devices. Since this kind of attack has already been reported in previous work, the feasibility of the attack is not within the scope of the studies presented in this chapter, which instead focus on the impact that these attacks may have on the power system.

Table 5.3: Considered MaDIoT adversary model based on guidelines by [200].

	Attack Model
Adversary knowledge	Oblivious
Adversary access	Non-possession
Adversary specificity	Targeted attack
Adversary resources	Class II

5.3.5 Criteria for attack success

For all the analyses and systems in this chapter, the attack is considered successful if, at the end of the simulation, loads have been disconnected (tripping of UFLS, overvoltage, or undervoltage protections) or if generators had to be disconnected (OFGR protections). This criterion is similar to that in [183], which considered an attack successful if it trips at least one over/under frequency protection relay, even if the impact is not catastrophic.

5.4 MaDIoT attacks in different power systems

This section focuses on the impact of MaDIoT attacks on different power systems (IEEE 39 and PST-16, introduced in subsection 5.3.1). This way, the replicability and scalability of the impact of MaDIoT attacks on an American grid and a European grid can be evaluated considering that IEEE 39 and PST-16 are quite different in size (39 and 66 buses, respectively), type of generation, initial demand ($\approx$ 6 GW and $\approx$ 15.5 GW, approximately), interconnection capacity, and generation capacity (Table 5.1). These models are selected for the analysis because different power system models including different electrical topologies, demand distributions, generation structures, and exhibiting different dynamic behaviour may have a different impact on the success of MaDIoT attacks.

5.4.1 Attack model and Scenarios

The attack model, following the modelling guidelines provided by [200], is presented in Table 5.4. The frequency of MaDIoT attacks is considered to be iterative, as multiple attempts would be needed to achieve the desired impact. The real-time detection of MaDIoT attacks by the system operator is extremely difficult to achieve [80], [201] since the attacked devices are not under the control of system operators, so the reproducibility and discoverability of the attack can be classified as a multiple-times attack. The functional level of the attack can be considered level 1 (the manipulation of control equipment / networks) or level 2 (supervisory equipment, local networks overseeing processes), according to [200]. The attacked assets

would be high-wattage devices connected via IoT, whose equivalent to the classification in [200] would be field controllers and human–machine interfaces. The attack techniques used by the attacker would be the modification of control logic (to activate high-wattage devices), wireless compromise, and Denial-of-Service of the power grid (final objective of the attack). Since the attacker needs to obtain unauthorised access to modify control commands, the attack premises are communications and protocols, as well as asset control commands. With respect to the attacker, the adversary model presented in subsection 5.3.4 is considered (the attacker does not have advanced knowledge of the grid).

Table 5.4: Considered MaDIoT attack model based on the modelling guidelines by [200].

	Attack Model
Attack frequency	Iterative
Attack reproducibility and discoverability	Multiple-times
Attack functional level	Level 1 or 2
Attacked asset	Field controllers, human–machine interfaces
Attack techniques	Modify control logic, wireless compromise, and Denial-of-Service to the power grid
Attack premise	Cyber: communications and protocols, and asset control commands

To consider that bots are close to each other and to study a worst-case-like scenario, the analysed attacks in this section only affect three nodes. These nodes and, therefore, the loads attacked, are selected randomly every time a simulation is executed, in a Monte Carlo-like way, as opposed to the approach in [188], where the most vulnerable nodes were targeted. In the analysis, those executions compromising the same loads for the same scenario (repeated results) are discarded.

For the PST-16 system, the attacked nodes belong to the same area since the closer they are, the greater the expected impact on the system [188]. Attacks are carried out at $t = 1\ s$ at the same time; this only affects the simulation time, since the simulation already starts with the system in steady state (result of running a power flow with the initial demand indicated in Table 5.1)

Table 5.5 shows the scenarios considered for the analysis for each test system. For each one, the botnet size varies in the range [50 k, 500 k], scaling-up in 50 k steps, and the simulation time is 21 s to keep the computational load at acceptable levels. For the PST-16 system, a total of nearly 1500 simulations are performed, while the IEEE 39-Bus accounts for 424 simulations.

Table 5.5: MaDIoT attack scenarios for the IEEE 39-Bus model (New England) and the PST-16 model (Europe). Only demand is compromised. Botnet size measured in total number of bots (e.g., 50k = 50 thousand bots)

Scenario	Test System	Area	Botnet Size	# Nodes Attacked
US39	IEEE 39	-	[50 k, 500 k]	3
EU-A	PST-16	A	[50 k, 500 k]	3
EU-B		B		
EU-C		C		

5.4.2 Results

The simulation results for the scenarios defined in Table 5.5 are presented and discussed below.

Success Ratio

To provide an overview of the results and ease the comparison of the two models, Figure 5.2 shows the success ratio (the number of successful attacks divided by the total number of attacks) of the MaDIoT attacks simulated for the scenarios presented in Table 5.5. In this figure, the differences in the success ratios between the US39 scenario and the EU scenarios are noticeable. This was expected, as they present different characteristics.

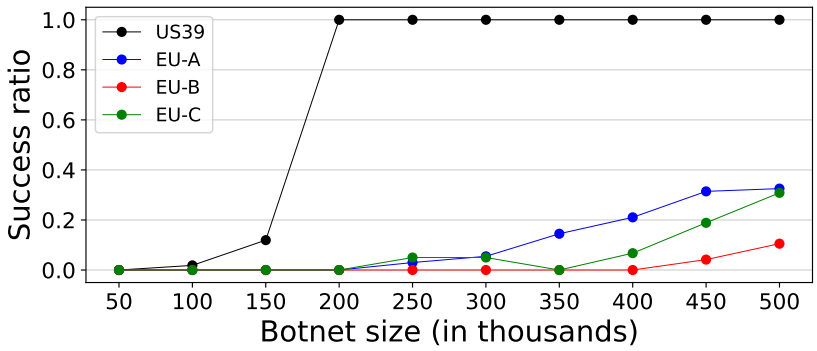

Figure 5.2: Success ratio for different scenarios when increasing the size of the botnet.

For the US39 scenario, it is remarkable that all the simulated attacks that compromised more than 150 k bots were successful. In fact, the difference between 150 k and 200 k (in theory, increasing from 450 MW to 600 MW) is significant, going from 10% success probability to 100%. The generation in IEEE-39, without the interconnection with USA/Canada, has in theory a margin of 938 MW to reach its generation limit, which, from the frequency point of view, should be enough to face attacks of up to 300k bots. However, after analysing the

simulations carried out for 300k bots, it was observed that generation does not increase fast enough after the attack to avoid the activation of first-step UFLS protections in some loads, since the attack compromises the loads at the same time. The consideration of an attack as successful if it trips at least one protection is behind the high success ratios. This means that, under the conditions assumed, it does not matter if the buses affected are close between them when compromising more than 150 k bots: the attack will always activate UFLS protections in the IEEE-39 system. Therefore, the attacker does not need advanced knowledge of the grid: by performing its attack during the peak demand hour, when the generation of the system has little margin, the success ratio could be high. It may seem like this contradicts the results presented in [188]; however, it should be taken into account that the study in [188] considered a daily load pattern for the grid, so its results may aggregate the success ratio of carrying out MaDIoT attacks during valley demand hours and during peak demand.

On the other hand, with respect to the PST-16 system, MaDIoT attacks start to be successful in the EU-A and EU-C scenarios for botnets > 200 k bots and, for the EU-B scenario, for botnets > 400 k. Although EU-A and EU-C end up having a similar success ratio (≈30%) for the largest botnet size considered, the maximum success ratio for the EU-B scenario is significantly smaller (≈10%). As Figure 5.1 shows, areas A and C are the areas with the highest gap between generation capacity and demand: area A has more generation than demand, while area C needs to import power from outside the area.

Therefore, Figure 5.2 shows that the number of bots needed to have a successful attack is lower in the IEEE 39-Bus system than in the PST-16, as it is also a smaller system with fewer generation capacity.

Impact of MaDIoT Attacks on Test Systems

Despite the fact that IEEE 39-Bus and the PST-16 grid models present different success ratios to the MaDIoT attacks, the success ratio is not tantamount to the degree of the impact (the number of loads and/or generators disconnected): a 100% success ratio may be achieved activating just one protection whereas a 30% success ratio may involve a wide area blackout.

Table 5.6 shows the average generation and demand disconnected in successful MaDIoT attacks to 500k bots in the US39 and EU-C scenarios (EU-C is the highest impact scenario for the PST-16 model). The IEEE-39 is a smaller system, with less generation, so the relative magnitude of compromising 500k bots (in theory, 1500 MW) is higher than in the PST-16 system. Therefore, it could be expected a higher impact on IEEE-39 than in PST-16. However, this table shows that although the average demand affected is similar in both scenarios, in the US39 scenario generation is not disconnected (OFGR) and the disconnection of demand was observed to be due to the activation of UFLS protections. On the other hand, in the EU-C scenario the disconnection of demand is mainly due to undervoltage protections, although the dynamics caused by the attack also activate some UFLS protections.

Table 5.6: Average impact on the system when successfully attacking 500k bots in the US39 and EU-C scenarios.

Scenario	Botnet Size	Average Generation Disconnected	Average Demand Disconnected
US39	500 K	0 MW	983.64 MW
EU-C	500 K	1515.28 MW	938.84 MW

To compare the impact on the two systems, two high-impact cases (one per model) have been selected for analysis. Both cases represent attacks to 500k bots (in theory, 1500 MW, as the load model has to be considered). The results of these two cases are plotted in Figures 5.3, 5.4 and 5.5, which are discussed below.

Figure 5.3 plots the frequency (Hz), the voltages (p.u), and the relative rotor angle of generators (with respect to the reference generator) against time when compromising a total of 500 k bots within loads 30, 31, and 34 in the PST-16 model (one high-impact EU-C scenario). The time of the attack (t = 1 s) is indicated by "*" in the x-axis. For the frequency and voltages, only the information for six buses is plotted, including the buses to which the attacked loads are connected, to keep the figure visually simple. Regarding the relative rotor angle, only three generators from area C are represented. Additionally, for each plot in the figure, the first activation of each type of protection is represented by a red-dotted vertical line (except for the OFGR protection, for which the three activations are shown).

Figure 5.3 shows how the attack significantly destabilises the PST-16 system. Figure 5.4 shows a zoom on the frequency and the relative rotor angle during the first 10 seconds of the case shown in Figure 5.3. Starting with the frequency, the attack has, at first, a reduced impact that is noticeable for a few seconds; a slight oscillation between the areas is observed, but the system manages to confine frequency variations and is apparently stable. Nevertheless, by t = 15 s, area C diverges from the other two areas. The frequency of bus C10, which has generation connected, drops suddenly to 46 Hz at around t = 18.5 s. These frequency variations about 12 s after the attack are explained by the loss of the rotor angle stability of the system.

The middle plot of Figure 5.3 clearly shows the immediate high impact that the attack has on the voltages of area C. It is worth recalling that area C, prior to the attack, was already working under what could be considered peak-demand conditions and that, under these conditions, the area was already dependent on the power imports from the other two areas: before the attack, the line A-C was working at 110% of its capacity (max. 1572 MVA), and line B-C was working at 17.3% (max. 2476 MVA). The voltages of the buses attacked drop significantly to just above the limit configured for the tripping of the undervoltage protections. However, due to the sudden increase in demand caused by the attack, the system loses rotor

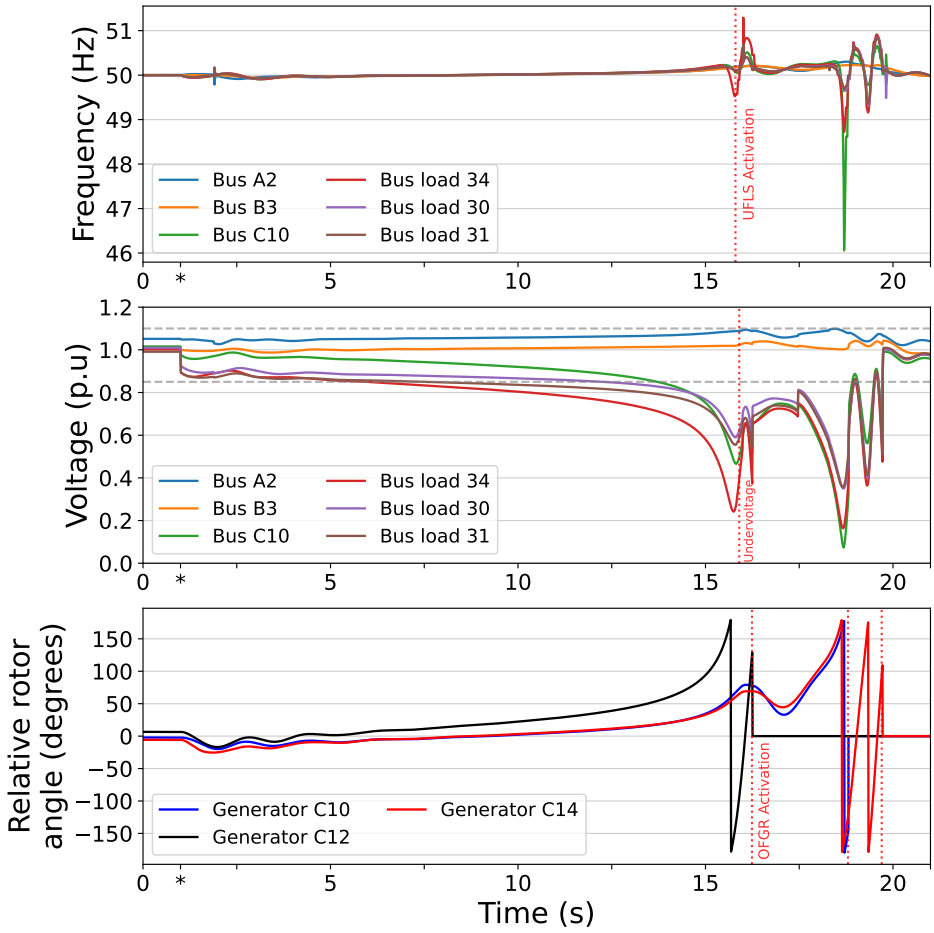

Figure 5.3: Frequency, voltages, and relative rotor angle of generators when attacking 500k bots in loads 30, 31, and 34 in the PST-16 system (EU-C scenario with high impact). Attack at t=1s (indicated by *).

angle stability and goes into voltage collapse. The bottom plot of Figure 5.3 shows that the rotor angles in the generators of area C start to diverge with respect to the reference generator after some initial oscillations. Therefore, the system experiences a rotor angle stability problem that leads to a voltage collapse.

Since voltages drop below 0.85 p.u for more than 10s (Figure 5.3), undervoltage protections start tripping (indicated by the red-dotted line in the voltage plot), disconnecting loads from the system. The actuation of undervoltage protections, together with the UFLS (red-dotted line in the frequency plot) and OFGR (red-dotted lines in the relative rotor angle plot) protections in the frequency domain, are among the main causes for the oscillations in the 15–20 s interval. After the actuation of the protections, the system seems to recover by t = 20 s but with rather low voltage levels (e.g., at Bus C10). By that time, nearly 2.9 GW of generation has become disconnected from the system due to the OFGR scheme. However,

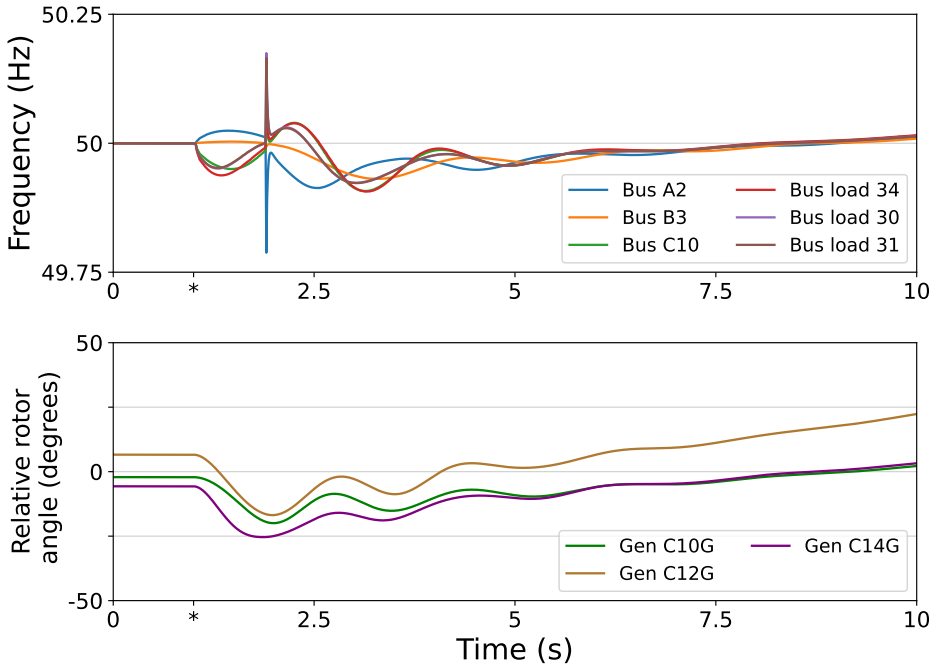

Figure 5.4: Zoom to the frequency and relative rotor angle shown in Figure 5.3 for the first 10 s. Attack at t=1s (indicated by *). PST-16 system (EU-c scenario with high impact)

the impact could be different if further protection features were implemented (e.g., distance protection with/without out-of-step protection). In this case, despite facing an increase in the demand due to the attack (theoretically, 1500 MW, but, in practice, less due to the load model), the system ends up with around 3 GW less demand than before the attack (≈20% decrease), due to the disconnection of loads (UFLS and undervoltage protections). This means that not only the equivalent to the extraordinary demand caused by the attack had to be disconnected from the system but also that more loads had to be disconnected for the system to recover. The loads disconnected include the ones attacked (loads 30, 31, and 34),

Similarly to Figure 5.3, Figure 5.5 plots the frequency and voltages when attacking 500 k bots in loads 12, 16, and 28 in the IEEE 39-Bus system (one high-impact US39 scenario), indicating with a red-dotted vertical line when the UFLS protections activate.

In the case plotted, the immediate impact of the attack on the frequency and voltages of the system is significant. It can be observed that the frequency drops by 1 Hz in approximately three seconds. Below 59 Hz, the UFLS scheme starts actuating, as described in Table 5.2. This softens the drop in frequency; only when it reaches ≈58.6 Hz does the system start to increase the frequency. However, the recovery is slow. In this case, the system manages to keep all voltages within limits, so the only protections tripping are the UFLS protections. These protections shed about 1.1 GW of loads along the system. Nevertheless, despite disconnecting loads, the total demand of the system increases by 76 MW with respect to the

demand before the attack (≈1.2% increase). This means that, practically, the amount of demand disconnected is equivalent to the demand increase provoked by the attack. However, the shedding also affects legitimate loads as UFLS protections make no distinction. Compared to the EU-C case analysed in Figure 5.3, the relative impact is smaller because the system manages to maintain its stability, despite the relative magnitude of the attack being greater than in the EU-C case.

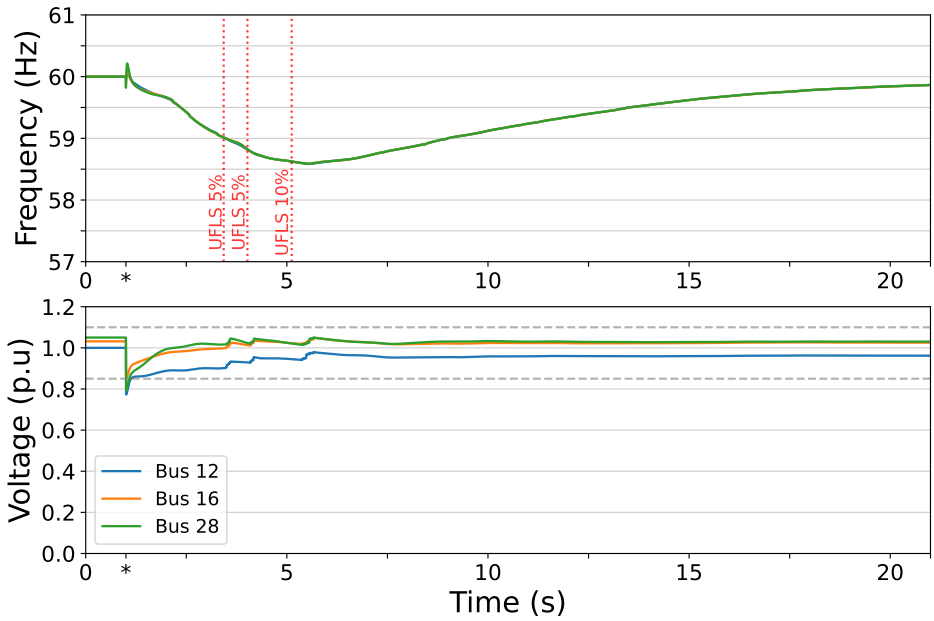

Figure 5.5: Frequency and voltages when attacking 500 k bots in loads 12, 16, and 28 in the IEEE 39-Bus system (US39 scenario with high impact). Attack at t=1s (indicated by *).

Therefore, although any attack compromising any three buses in the IEEE 39-Bus system may be successful, its impact could be relatively low, equivalent to the magnitude of the attack. On the other hand, destabilising the PST-16 system is more difficult as it is larger and has more resources to face the attack; however, as discussed, a successful attack can significantly affect the stability of the system, causing the partial disconnection of loads and generation.

The results presented also show the different types of impact that MaDIoT attacks have on different grids (i.e., replicability of the attacks). In the case presented for the PST-16 system, the attack mainly affects rotor angle instability in area C (area attacked in the analysed case) and voltages, whereas for the IEEE 39-Bus system the main impact was on the frequency, since it does not have enough generation capacity for large attacks.

It should be noted that these results correspond to a scenario where demand is high, and the attack affects only three electrical nodes that are relatively close among them. In the PST-16 system, the success ratio and impact of the attack can be expected to be lower when the

attack is distributed among a greater number of nodes (while keeping the same botnet size), when initial demand is low, or when distant nodes are the ones affected (for example, when only one node per area is attacked in the PST-16 model). Therefore, not only the size, but also the location of the attack has an impact on the survival of the system, i.e., whether or not the attack can destabilise the power system. For IEEE-39, location aspects may not affect the impact that much, as its main problem is in the frequency domain, not having the proper generation to face the attack.

5.5 MaDIoT attacks and distributed energy resources: MaDIoT 3.0

Modern electricity grids are increasing the penetration of DER, many of which are being installed by *prosumers*.

This section analyses the replicability of the impact and success of MaDIoT attacks in the PST-16 system (simplified European system) with distributed solar PV generation connected to area C; and the success and impact on the power system when attacking the connected solar DG together with demand. In this study, only the PST-16 system is used with the same initial demand as in the previous study (Table 5.1). The consideration of DER devices as potential targets of the attack has received the name of MaDIoT 3.0 attacks in this chapter, as an evolution of MaDIoT [80] and MaDIoT 2.0 [188] attacks (Figure 5.6).

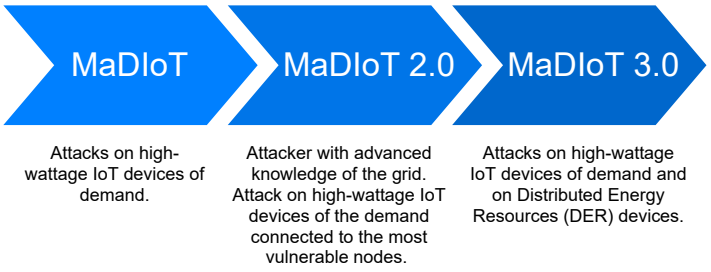

Figure 5.6: Evolution of MaDIoT attacks.

To perform this analysis, and to be able to compare the impact of connecting DG, distributed solar PV generation was connected to buses that have loads, but not bulk generation, in area C of the PST-16 model. This area was selected because of:

a) Its representation of southern Europe in the PST-16 benchmark model. Spain's available data on distributed solar PV penetration can be extrapolated (see Appendix C).

b) Its mismatch between active load and maximum bulk generation capacity (Figure 5.1). Area C has less generation capacity available than other areas.

c) The success ratio of common MaDIoT attacks in this area is around 30% (Figure 5.2) without distributed generation. This allows for a better comparison of the impact of the attack when considering solar PV generation.

Figure 5.7 shows a simplified diagram of area C of the PST-16 system with the placement of distributed solar PV generation.

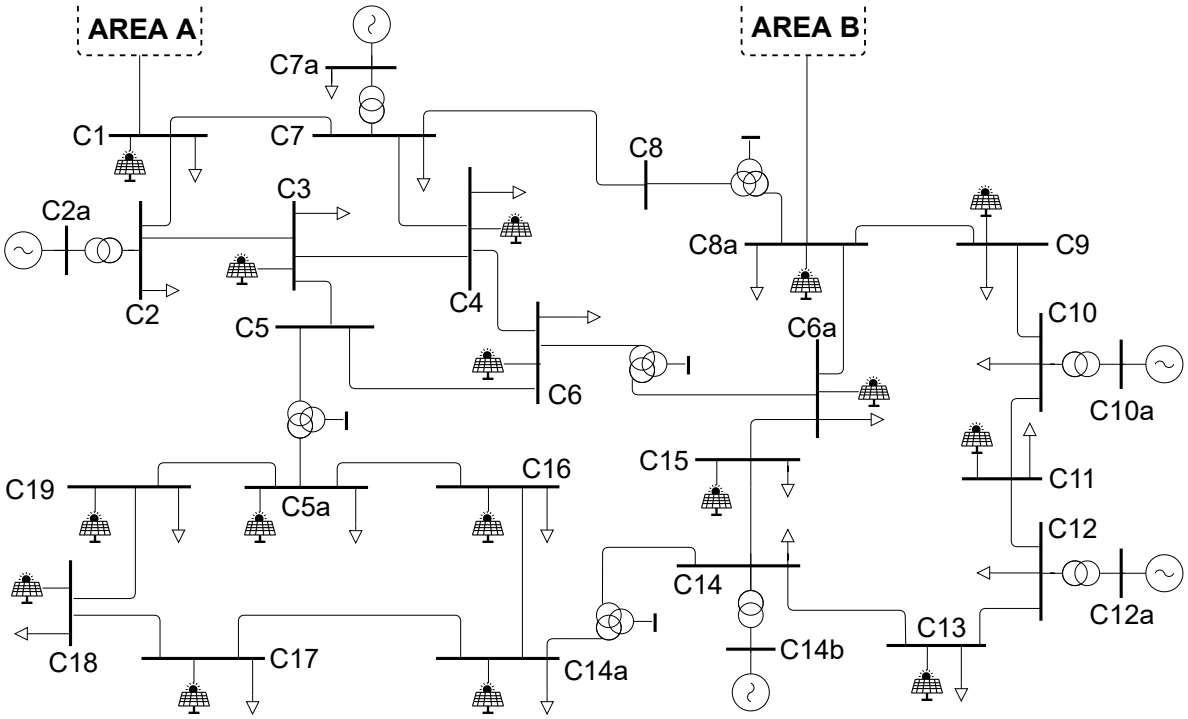

Figure 5.7: Simplified diagram of area C in the PST-16 system with distributed solar PV included.

The penetration degree of DG that is applied in the study corresponds to the one estimated for Spain for the year 2030 (10% of the instant power of the demand supplied with distributed solar PV). Since area C could represent the South of Europe, this value was calculated by extrapolating actual data about solar PV generation in Spain (connected to up to 145kV).

To estimate the penetration level of distributed solar PV in Spain in 2030, first it is necessary to estimate the current level (year 2023), to be use as a basis. For this, data updated by the Spanish regulator on March 2023 was used [202]. Then, for 2030, the percentage was calculated based on the information published by the Spanish TSO (i.e., *Red Eléctrica de España*) on the generation that is awaiting its start-up and has permission to connect to the distribution network; it is safe to assume that this generation will be operational by 2030 [203]. It is estimated that, by 2030, the penetration level of distributed solar PV will be 10%. Appendix C describes how the estimated value of 10% was obtained, and Table C.3 in the appendix shows the solar PV power that is connected to each bus in area C, summing up

546.5 MW in total. For simplicity, this generation was modelled in PowerFactory as *static generators* with constant reactive power control. Since DG is included, bulk generation has to decrease. It was assumed that the penetration of distributed solar PV in Area C (546.5 MW) reduces the number of bulk generators in two generation units (approximately, 433 MWs of generation under initial conditions). The maximum active power limit of bulk generation in the PST-16 system is reduced in 900 MW, which should not be a problem since there is still enough reserve to face attacks.

Table 5.7 shows the initial conditions (before the attack) for the PST-16 system with DG in area C and compares them with the initial conditions of the base PST-16 system (without DG).

Table 5.7: Initial conditions of the PST-16 system with DG in area C compared to the base PST-16 (without DG).

	PST-16 with DG in area C	**Base PST-16 (without DG)**
Active load (MW)	15565	15565
Reactive load (Mvar)	2225	2225
Max. Active power (MW) limit (bulk generation)	17316.2	18220
DG in area C (MW)	546.5	0
Interconnection loading (%)	Areas A-C: 109.3% Areas B-C: 13.7% Areas A-B: 37.3	Areas A-C: 110.1% Areas B-C: 17.3% Areas A-B: 37.2%

5.5.1 Attack model and Scenarios

The attack model for an attack on DER would be similar to that of high-wattage IoT devices in the demand (Table 5.4). However, control servers could also be part of the compromised assets, and attack techniques would also include *"module firmware"* [200] to modify the control objectives of DG inverters. With respect to the attacker, the adversary model presented in subsection 5.3.4 remains unchanged.

Table 5.8 summarises the characteristics of the scenarios analysed in this section. To improve the readability and understanding of the analysis of results, the name of each scenario follows the pattern depicted in Figure 5.8. On average, each scenario counts with 165 simulations.

As in the study presented in section 5.4 the nodes to which the compromised loads are connected are selected randomly every time a simulation is executed, in a Monte Carlo-like

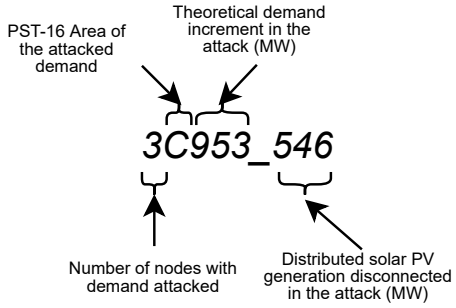

Figure 5.8: Explanation of the pattern followed for the names of the scenarios.

way. Regarding the attack to DG, the simulation program selects those nodes whose DG power, when aggregated, is equal to the indicated value in the scenario. This means that there are no partial disconnections of DG within the same bus: if the bus is selected, all its DG is disconnected in the attack.

Table 5.8: Scenarios analysed for the PST-16 system with 546.5 MW (10% of demand in Area C) of distributed solar PV connected in Area C.

Scenario	**Attack on demand**				**Attack on DER**		**Total**
	Area	**No. nodes**	**Botnet size**	**MW**	**Area**	**MW**	**(MW)**
3C1500_0	C	3	500k	≈ 1500	–	0	≈ 1500
3C1350_0	C	3	450k	≈ 1350	–	0	≈ 1350
3C1200_0	C	3	400k	≈ 1200	–	0	≈ 1200
3C953_546	C	3	318k	≈ 953	C	546.5	≈ 1500
3C1225_225	C	3	408k	≈ 1225	C	225	≈ 1450
3C525_525	C	3	175k	≈ 525	C	525	≈ 1050
3A953_546	A	3	318k	≈ 953	C	546.5	≈ 1500
3B953_546	B	3	318k	≈ 953	C	546.5	≈ 1500
6C1500_0	C	6	500k	≈ 1500	–	0	≈ 1500
6C953_546	C	6	318k	≈ 953	C	546.5	≈ 1500
6C1500_546	C	6	500k	≈ 1500	C	546.5	≈ 2046

The first three scenarios (3C1500_0, 3C1350_0, and 3C1200_0) aim to evaluate the impact of traditional MaDIoT attacks (i.e., only demand is compromised) on the system with distributed solar PV generation. Since the connection of DG modifies the initial state of the system from the one used for the analysis in the previous section, a different response to the attack and different success ratios can be expected.

The next three scenarios (3C953_546, 3C1225_225, and 3C525_525) allow the analysis of the impact of MaDIoT 3.0 attacks that combine demand and DG attacks performed at the same time. This means that the attacker manages to increase the demand and, at the same time, disconnects solar PV DG.

In addition to this, five additional scenarios are considered to get further insights about the impact of MaDIoT 3.0 attacks. Two scenarios (3A953_546 and 3B953_546) allow to analyse the impact when the compromised demand and the compromised DG do not belong to the same area. This may be the case if an attacker only managed to find and exploit vulnerabilities in technologies, systems, or devices that were replicated more extensively in certain regions. The remaining three scenarios (6C1500_0, 6C953_546 and 6C1500_546) allow to analyse the impact of doubling the number of nodes attacked while keeping the botnet size invariant.

5.5.2 Results

The results for the scenarios defined in Table 5.8 are presented and discussed below.

Impact of connecting distributed generation

Figure 5.9 shows the success ratios of MaDIoT attacks in scenarios 3C1500_0, 3C1350_0, and 3C1200_0 compared to the success ratios previously obtained for the base PST-16 system model (without distributed solar PV connected, section 5.4).

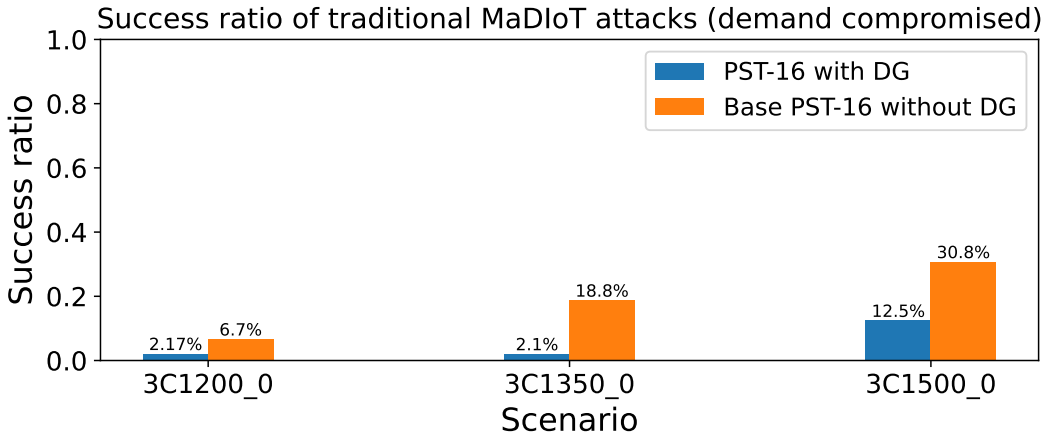

Figure 5.9: Success ratio of traditional MaDIoT attacks (demand compromised) in the PST-16 system with and without DG.

It can be seen in Figure 5.9 that, for the three scenarios, the success ratio of traditional MaDIoT attacks in the system with solar PV DG connected in area C is significantly lower than in the system with only bulk generation. In fact, the success ratio only becomes relevant when 500k bots are attacked (3C1500_0).

The results presented in section 5.4 showed that the attack in area C mainly affected rotor angle instability and voltages. As Figure 5.10 shows, the connection of DG in area C increases the voltages of the nodes (average increase of 0.99%), putting the system in a better initial state to face the attack. Furthermore, the DG units added to area C were modelled in PowerFactory as static generators with constant reactive power control. This would explain the decrease in the success ratio.

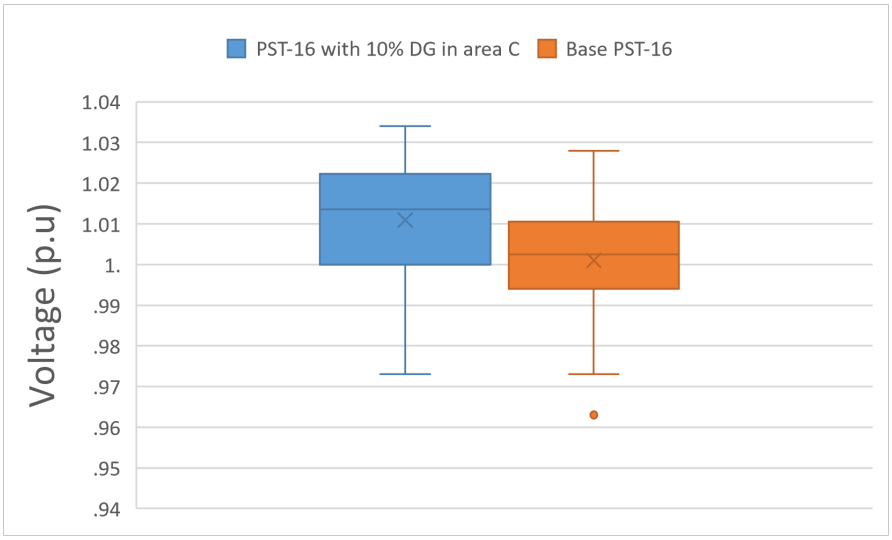

Figure 5.10: Comparison of bus voltages in area C when DG is connected.

However, it was previously mentioned that the success ratio may not be indicative of the impact of the attack. To gain an understanding of the magnitude of the attack's impact on the PST-16 system with DG, the simulated case with the most significant effect is analysed below.

Figure 5.11 plots the frequency (Hz), the voltages (p.u), and the relative rotor angle (degrees) of generators in area C (with respect to the reference generator) against time when facing an attack defined for scenario 3C1500_0. The time of the attack (t = 0.5 s) is indicated by "*" in the x-axis. For the frequency and voltages, only the information for five buses is plotted, including the buses to which the attacked loads are connected (loads 27, 30 and 34 connected to buses C13, C14a and C16, respectively), to keep the figure visually simple. Regarding the relative rotor angle, only three generators of area C are represented. The red-dotted line in the voltage plot shows when the undervoltage protections are activated.

The results in Figure 5.11 show that the attack has a lessened effect on the frequency of PST-16, with it dropping below 50 Hz for a few seconds before returning to the nominal value. Additionally, the voltage of the targeted buses decreases, with bus C13 dropping to just above the limit of the undervoltage protections (0.85 p.u). However, it goes below this limit by $t \approx 6s$, which causes the activation of the protections after ten seconds, as indicated by the red-dotted line.

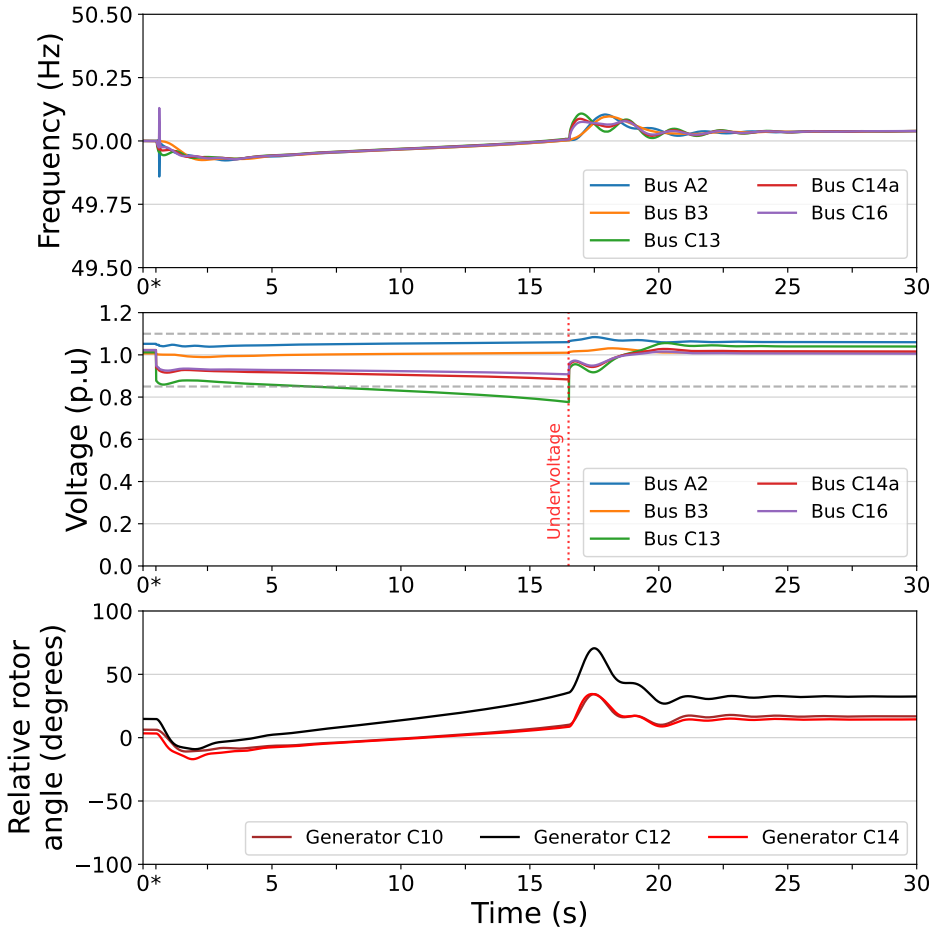

Figure 5.11: Frequency, voltages, and relative rotor angle of generators in scenario 3C1500_0 (highest impact observed). Attack at t=0.5s (indicated by *)

As before, this is related to rotor angles, which are affected by the attack, as shown in the bottom plot of Figure 5.11. The rotor angles in the generators of area C start to diverge with respect to the reference generator right after the attack, causing a progressive decrease in the voltages of the area. The activation of the undervoltage protections by $t \approx 16s$, disconnecting 600 MW of demand, provokes a disturbance in the rotor angles and a slight desynchronisation of the frequency of the areas of the system. However, the undervoltage protections have the desired effect and avoid voltage collapse: voltages return to normal operation values and the rotor angles recover stability without the actuation of OFGR protections. In this case, by the end of the simulation, the system ends up with 188 MW less demand than before the attack (1.2% decrease). This is a much lower impact than the one analysed in Section 5.4 for the system without DG (20% decrease).

In addition to this case, it was simulated a case in which the same loads that were attacked in Section 5.4 are targeted for the system with DG; the results obtained show that the attack

would not be successful (i.e., no protections were activated) under these new conditions. The same way around, when simulating the case just presented in Figure 5.11 in the base PST-16 system (without DG), the attack is successful and provokes the disconnection of $\approx 2GW$ of generation and the protections disconnect a large number of loads, decreasing the demand of the system in $\approx$ 13% with respect to the initial demand. This shows the great positive effect that the presence of just 10% of distributed solar PV generation in area C has on the stability of the PST-16 system when facing MaDIoT attacks, modifying their scalability and replicability in this system.

Impact of MaDIoT 3.0 attacks

Once it has been analysed the impact that connecting solar PV DG to area C of PST-16 has on the success ratio of traditional MaDIoT attacks in this system, the impact of performing combined attacks targeting high-wattage IoT demand and solar PV inverters (MaDIoT 3.0 attacks) is assessed.

Table 5.9 shows the success ratio of MaDIoT 3.0 attack scenarios in area C. The highest success ratio in this table is achieved by scenario 3C953_546, with 3.91% of successful attacks. This is lower than the success ratio obtained for scenario 3C1500_0 (12.5%), despite both scenarios are equivalent in terms of total power affected ($\approx 1500MW$, in theory). This means that the amount of demand attacked, distributed in just three nodes, has a greater influence on the success ratio than attacking all the DG connected to area C (546.5 MW). This can also be appreciated in scenario 3C525_525, with a null success ratio when decreasing the amount of demand attacked. This is because, while demand attacks are focused on three nodes in this study, the 546.5 MW of DG that are attacked are distributed along area C (multiple nodes, as presented in Figure 5.7), having less impact.

Table 5.9: Success ratio of MaDIoT 3.0 attacks on area C. Below, for comparison, success ratio of traditional MaDIoT attacks in the PST-16 with DG.

Scenario	Success ratio
3C953_546	3.91%
3C1225_225	1.79%
3C525_525	0%
3C1500_0	12.5%
3C1200_0	2.17%

However, this does not mean that the attack on DG has no effect: scenario 3C1225_225 shows that increasing the demand attacked while decreasing the amount of DG attacked would not guarantee more success with respect to scenario 3C953_546. In terms of impact,

protections in 3C1225_225, in general, disconnect less loads than in 3C953_546, having a lesser effect on the system.

On the other hand, apart from the DG in area C, an attacker may only have access to high-wattage IoT devices of the demand of other areas (A and B) for different reasons (e.g., socioeconomic aspects, better replicability of the systems, etc.). To assess this, Table 5.10 shows the success ratio of MaDIoT 3.0 attacks when the targeted demand is in different areas of the PST-16 system (A, B or C). The three scenarios define attacks on the same amount of demand and DG.

Table 5.10: Success ratio of MaDIoT 3.0 attacks on different areas.

Scenario	Success ratio
3A953_546	4.76%
3B953_546	0%
3C953_546	3.91%

While attacks on demand of areas A and C have similar success ratios (4.76% and 3.91%, respectively), if the attacked demand is in area B, the success ratio based on the simulated attacks is 0%. These differences between areas are in line with the success ratios presented before in Figure 5.2 for traditional MaDIoT attacks, where the success ratios of attacking only 1500 MW demand (500k bots) in A and C are also similar between them, and higher than for area B. Therefore, performing multiple-area MaDIoT 3.0 attacks do not really increase the success ratio in the PST-16 system under the analysed conditions.

Finally, the success ratio of MaDIoT 3.0 attacks is evaluated when doubling the number of nodes to which the attacked demand is connected (from three to six). This would be the case if the vulnerable high-wattage IoT devices are more distributed along area C (i.e., better regional replicability). This also allows to slightly equate the conditions of the attacked demand to the conditions of the attacked DG (more distributed), which was identified as one of the main causes for the different impact of the two targets. Table 5.11 shows the success ratios for scenarios 6C1500_0, 6C1500_546 and 6C953_546.

Table 5.11: Success ratio of MaDIoT 3.0 attacks when considering six buses for the attacked demand.

Scenario	Success ratio
6C1500_0	0%
6C1500_546	13.33%
6C953_546	0%

It is remarkable that merely attacking demand in six nodes dilutes the success ratio to

0%, compared to the 12.5% obtained when considering three nodes (3C1500_0 in Figure 5.9). This means that the PST-16 system manages to face the attack without the activation of any of the protections in the system. To increase the success ratio, it should be combined with attacks to the DG to increase the impact on voltages, as scenario 6C1500_546 shows. In this case, less demand per node is compromised (but in more nodes), and all the DG is attacked, achieving a success ratio of 13.3%.

The results presented in this section provide interesting scalability and replicability insights about the connection of DG to area C of the PST-16 system and its impact on MaDIoT 3.0 attacks. Traditional MaDIoT attacks, where only demand is compromised, do not replicate the success and impact in the PST-16 system when 10% DG is connected to area C, due to the change in the initial conditions of the system (e.g., higher initial voltages in area C due to the connection of DG).

When performing MaDIoT 3.0 attacks in the PST-16 system, it was observed that the amount of demand attacked had a greater influence on the success ratio than the attacked DG, although the latter was relevant to achieve some success. On the other hand, attacking the demand of areas different from where DG is attacked would not increase the success ratio of the attack under the analysed conditions for PST-16. In the same way, distributing the attacked demand between more buses would significantly decrease the success ratio, unless larger attacks are performed.

5.6 Conclusions

High-wattage IoT devices at the consumer level of electricity grids, as well as devices involved in the control of DER, could be new attack vectors, since they would be deployed along power systems. Therefore, knowing to what extent MaDIoT attacks could affect different types of systems, under different conditions, becomes essential as the number of these devices increases.

This chapter has first analysed the replicability of MaDIoT attacks in two power system models representing a simplified version of Europe and New England (PST-16 model and the IEEE 39-Bus model, respectively), expanding and complementing the studies performed by previous work. Then, the replicability of MaDIoT attacks in the PST-16 system with distributed solar PV generation was assessed, as well as the impact of MaDIoT 3.0 attacks, which combine attacks to demand and DG.

For the traditional MaDIoT attacks, the results have shown how the success ratio of the attacks depends on the power system affected. The IEEE 39-Bus system presents success ratios of up to 100%, while the maximum success ratio obtained for the PST-16 system is around 30% and depends on the area attacked. However, a more detailed analysis of high-impact cases has shown that higher success ratios do not necessarily mean a higher impact

for these systems. The PST-16 system is larger and has more resources to face the increase in demand caused by the attack, but a high-impact attack can cause a blackout equivalent to 20% of the initial demand, experiencing an impact greater than the magnitude of the attack. In the IEEE 39-Bus system, where the same attack is larger in relative terms, the analysed high-impact case just resulted in an impact equivalent to the magnitude of the attack, since its main problem is related to its power generation capacity.

However, the connection of distributed solar PV generation to area C of the PST-16 system increased the voltages by $\approx 1\%$ on average, changing the response of PST-16 system to the attack and thus not replicating the same success and impact, significantly reducing both. Regarding MaDIoT 3.0 attacks, demand had a greater influence on the success of the attack than the DG, mainly due to the different concentration of these. Distributing the attacked demand among more buses or attacking the demand in areas different from the one with the attacked DG would result in a lower success ratio in the PST-16 system. This means that, under the analysed conditions for the PST-16 system, the local scalability and replicability (i.e., deployment in few nodes) of vulnerable high-wattage IoT devices in the demand become more relevant for MaDIoT 3.0 attacks than regional replicability (i.e., deployment distributed within the area or between areas of the same system).

High-wattage IoT devices and the equipment involved in the operation of DER should comply with cybersecurity standards and regulation, and undergo strict tests to minimise the risk of being compromised and used in a MaDIoT type of attack. At the system operation level, TSOs and DSOs should consider these attacks in their cyber risk management plans. TSOs and DSOs should also collaborate, be coordinated, and exchange information between them for a more efficient, reliable, and secure operation of the electricity system.

Chapter 6

TSO-DSO data exchange for resilient operation

6.1 Introduction

The complexity of DER integration and the increasing volume of available data make it necessary to develop and implement communication architectures that are efficient and interoperable to exchange information between the different actors of the power system. In Europe, better cooperation between the TSO and the DSO for the overall optimisation of the system is identified as of great importance [204].

The provision of system services by DER and/or demand could be a way for SOs not only to avoid costly upgrades of the grid, but to increase system resilience against MaDIoT 3.0 attacks analysed in Chapter 5.5. Through the real-time activation of these services, SOs could try to minimise or even eliminate the harmful consequences of these attacks.

However, to make this a reality, further improvements in coordination and information exchanges between all stakeholders (and especially those involving TSOs and DSOs) is necessary. In recent years, many EU-funded research projects have focused on this, developing data platforms and ICT architectures so that SOs can exchange data and coordinate their actions efficiently and reliably [205].

The academic literature has focused mainly on business and functional aspects when addressing this aspect [10], [206]–[209]. However, the ICT component is becoming more relevant, as the standardisation and interoperability level of the ICT systems deployed will deeply affect the final cost of implementation of a TSO-DSO coordination scheme [210]. In addition to this, in Europe, the interconnection of power systems from an electrical point of view also requires reliable communication exchanges between operators.

Regarding ICT, Lambert et al. [211] presents a general ICT architecture for data exchange using commonly used protocols in Europe. However, different ICT advances have

been made in the last few years, some of which are discussed in this chapter. At the information layer, reference [212] mainly reviews how CIM has been implemented by different European projects and which gaps are still present for interoperability. Reference [213] presents a description of each data exchange in a TSO- DSO coordination scheme, describing the type of data, the importance, the time domain, and source/user of the data, but without discussing the communication protocols and standards for each data exchange.

To achieve effective data exchange between the stakeholders of the electric power ecosystem, a previous identification and exchange of data models, protocols, platforms, etc. that can be used is needed. Then, SOs and service providers must agree on communication protocols and platforms, as well as increase the interoperability of their systems.

As a contribution to this process, this chapter analyses some of the ICT architectures for the coordination of SOs demonstrated in five EU H2020 projects: SmartNet [214], CoordiNet [215], TDX-Assist [216], INTERRFACE [217], and EU-Sysflex [218]. These architectures are analysed at the communication and information layer of the SGAM, analysing the coverage of the most widely used information standards for the exchange of specific types of information and discussing the adequacy of two alternative types of protocols (publish-subscribe and client-server) for different data exchanges, so that common approaches and gaps are identified and discussed.

This chapter is structured as follows. Section 6.2 introduces and describes the ICT architectures for TSO-DSO data exchange used in the EU H2020 projects mentioned above. Section 6.3 analyses and compares the application of the different communication protocols and standards used in these projects. Finally, Section 6.4 outlines the main conclusions of the chapter.

6.2 ICT architectures for TSO-DSO data exchange

6.2.1 Interactions between electricity system actors

The development of system services would require two essential things: a market, so that the conditions are the same for all the providers and the most cost-effective solutions can be selected; and better coordination and information exchange between all the stakeholders.

The design of the market, and who operates it, determines the communication flows and operational and information exchange processes that will take place between the participants, especially the SOs, for the acquisition and activation of services. In the specialised literature, the different market, operational, and information exchange designs are known as coordination schemes [10].

Coordination schemes can be defined from a market or ICT perspectives. The Active System Management (ASM) report [219] defined the coordination schemes focusing on

TSO–DSO communication in general. However, different EU-funded projects consider different market models under different names. For example, the CoordiNet project, in general, considered separate markets for balancing and congestion management, while SmartNet considered a joint market for balancing and congestion management. On the other hand, the INTERRFACE project provides integration of different markets (e.g., congestion and wholesale, or congestion and balancing) and different options for TSO-DSO coordination [220]. The equivalent coordination schemes discussed in the ASM report [219] and the H2020 projects SmartNet, CoordiNet, and INTERRFACE are presented in Table D.1 in Appendix D.

The analysis of the different TSO-DSO coordination schemes is not within the scope of this chapter. However, since these involve the establishment of communication links between SOs, it is necessary to have an idea of their approach in terms of ICT. At a high level, and considering ICT, two main approaches can be distinguished:

1. **Common market platform**: There is a unique platform that is operated by either the TSO (requiring the DSO to send its constraints) or by an independent operator (requiring both the TSO and DSO to send their constraints). For these communications of constraints and other market information to SOs, the same platform or an additional one may be used.

2. **Multiple market platforms**: This consists of a Local Market (LM) platform for the DSO and one central market platform for the TSO. Depending on the coordination scheme, these markets may operate in different ways, affecting the communication needs. At a high level, two common ways of operation are:

   (a) LM dispatches the units located at the distribution level and the central market dispatches the remaining flexibility available at the distribution level together with the flexibility at the transmission level. Therefore, the markets are decoupled and not synchronised in real time.

   (b) LM and the central market dispatch their own resources but require coordination between TSO and DSO (e.g., the TSO may provide set points to the DSO).

Among the different models, the centralisation of the market (i.e., common platform) currently constitutes the main one implemented [10]. However, other schemes could allow the provision of local services to DSOs, improving the resilience of the distribution grids, and improve cost efficiency by having a more liquid market and economies of scale [209]. These benefits, compared to those provided by the centralisation of the market, could be high enough to neglect the ICT costs required for the transition. In fact, ICT costs may not be a barrier to choosing one model or the other [221].

6.2.2 ICT architectures in European projects

In this section, the ICT architectures implemented in the demonstrations deployed in different European research projects are reviewed, focusing on the information and communication layers of the SGAM. For simplicity, only the demos focused on congestion management are considered; in terms of ICT, other types of services should not involve great changes at the high level.

SmartNet

The aim of the Horizon 2020 funded project SmartNet (2016-2019) was to provide architectures for TSO-DSO coordination for system services. Of the three demos carried out in this project, only the Danish and Spanish demos had congestion management as one of their use cases.

The ICT architectures presented in [222] mainly propose a set of data models and standards that could be used for each communication link, but do not specify the communication protocol or technology for each specific demonstrator, due to the lack of information regarding ICT requirements for the use cases. Nonetheless, [222] does assess which links may require wired or wireless technologies based on latency and security requirements. The architectures for the Danish and Spanish pilots are briefly described below for the congestion management use case and summarised jointly in Figure 6.1:

1. *Danish pilot* [223]. In this pilot, congestion management is done through aggregated consumption shifting and load curtailment mechanisms of 30 summer houses. In this pilot, the common TSO-DSO market coordination scheme of SmartNet is applied.

   Two different ICT systems are employed: *system A*, which includes the IoT hardware deployed in the houses that mostly use non-standard protocols and which is out of the scope of this analysis; and *system B*, which is related to the LV grid and uses International Electrotechnical Commission (IEC) standards.

   Within *system B*, the standards proposed for market-related communications (requirements, bids, and market results) are CIM standards (IEC 62325, IEC 61968, and IEC 61970). For the communications between the Commercial Market Party (CMP) management system and the DER aggregator's management system, as they are related to network operation (activation signals), the standards include IEC 61850, IEC 60870-5-101/104, IEC 60870-6/TASE.2 (Inter-control Centre Communications Protocol (ICCP)), OpenADR, IEC 62056 (DLMS/COSEM) as well as a Representational State Transfer (REST) architecture. Excluding REST, these standards are also proposed for the technical communications between DER units and aggregators. Regarding physical connections, only the link between the market management system and the CMP's trading system would require a wired connection [222].

2. *Spanish pilot* [224]. This pilot tested the *Shared balancing responsibility model* of SmartNet with the provision of local flexibility services to solve local congestion. Although the DSO manages the local market, it must meet the set-points established by the TSO. Despite implementing a different coordination scheme, the ICT architecture proposed is similar to the Danish pilot.

   For congestion management, the direct communication between TSO and DSO would be done using CIM-based standards such as IEC 61968 and IEC 61970. For market-related communications, CIM (IEC 62325) is also proposed. Finally, communications with the DER aggregator and units consider IEC 61850, IEC 60870-5-101/104, ICCP/TASE.2, OpenADR and DLMS/COSEM as in the Danish pilot. In terms of physical connections, only the communications between the CMP's trading system and the aggregator would require a wired connection [222].

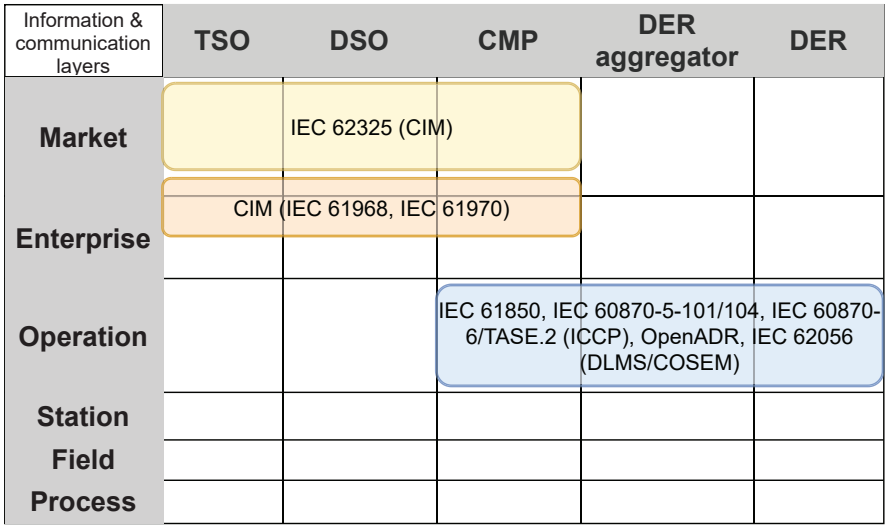

Figure 6.1: SGAM Information–Communication layer of the ICT architectures implemented in SmartNet

CoordiNet

The CoordiNet project (2019-2022) aimed to demonstrate how TSO and DSO can coordinate to use the same grid resources for different services. For this, three demos were implemented: Spain, Greece and Sweden. These pilots consider different use cases, including congestion management by the acquisition of flexibility services. In CoordiNet, data models and common interfaces were built on ENTSO-E CIM profiles and followed the Common Grid Model Exchange Specification (CGMES) [225].

1. *Spanish pilot*. The CoordiNet platform is made up of two main elements: the central or common platform, and the local platform.

   The CoordiNet common platform is on TSO's premises and is based on two already-existing TSO systems: GEMAS, which clears and operates the market, including the execution of the congestion management market considering the DSO High Voltage (HV) and MV networks; and eSIOS, which publishes and receives market information, acting as an interface between market agents, CoordiNet common platform, and GEMAS system.

   On the other hand, the CoordiNet local platform is on DSO's premises and is only one of the five modules that make up the DSO platform. The other modules are day-ahead operation, intraday operation, observability, and communications.

   In this pilot, short-term congestion management has three parts: aggregation of congestion preconditions, activation of flexibility resources, and supervision of resource activation [225].

   For the aggregation of congestion preconditions, the protocol proposed for communications between systems is the IEC 62325-504 (Web Services (WS), using CIM).

   The activation of flexible resources includes the congestion market clearing and the communication of results to the stakeholders. For this, the protocols used depend on the link:

   - Flexibility bids are sent by DER to the CoordiNet platform using IEC 62325-504.
   - Results of the congestion market are sent to the DSO platform using the MQTT, and to the TSO through GEMAS/ eSIOS.
   - Once definitive results are obtained, the CoordiNet common platform sends the activation signals to Flexibility Service Provider (FSP) (IEC 62325-504, ICCP) and notifies SOs to supervise the activation.

   Finally, during the supervision of resource activation, the TSO and the DSO will send resources' monitoring data to the CoordiNet common platform, which processes them and passes settlement processes to the relevant FSPs using IEC 62325-504. The aggregator of FSPs would use MQTT to monitor the state of the unit every five minutes.

   The communication between aggregators and the local market is done through XML files, using ad-hoc REST services.

   Figure 6.2 presents, at a high level, the ICT architecture proposed in this pilot through its mapping into the SGAM's Information–Communication layer.

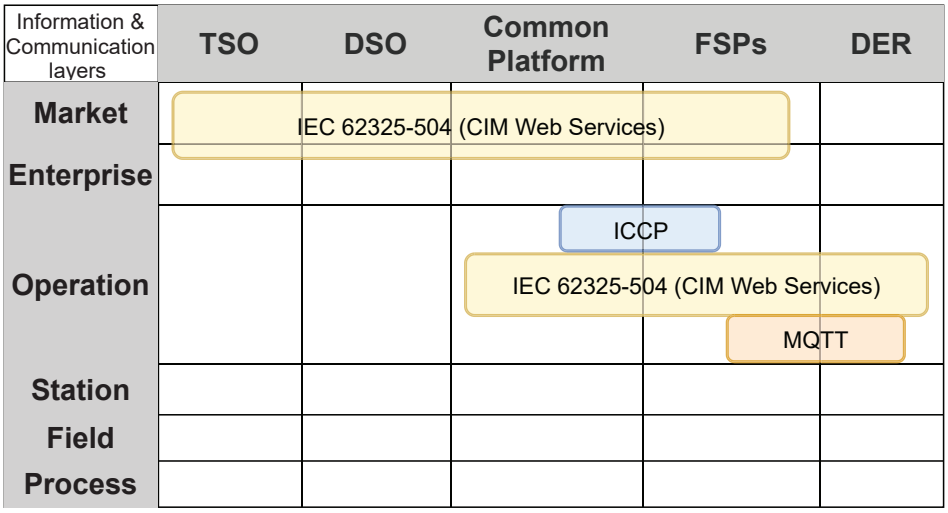

Figure 6.2: SGAM Information–Communication layer of the ICT architectures implemented in the Spanish demo of Coordinet

2. *Greek pilot*. The CoordiNet platform consists of two platforms: the TSO-DSO collaboration platform, for the exchanges between the SOs; and the market platform, for the communications between the different market participants. Both systems use an Enterprise Service Bus (ESB) as a communication middleware, but they are independent of each other since TSO-DSO information exchange goes beyond market-related communications and different security measures might be required.

   In the TSO-DSO collaboration platform, two protocols connect the TSO and DSO's systems with the ESB:

   - ICCP (IEC 60870-6/TASE.2), using Internet Protocol security (IPsec) through a VPN. This would be the case of the TSO's SCADA and EMS.
   - Secure SHell File Transfer Protocol (SFTP). Used by different DSO's systems (e.g., metering, SCADA, etc.) and the TSO's Geographical Information System (GIS).

   As for the communications between the ESB of the collaboration platform and other systems (e.g., market platform, DSO support tools, metering and control microservices, etc.) would be done using MQTT or a REST API, implementing Transport Layer Security (TLS).

   Regarding the market platform, the communications between market participants (market operator, forecast provider, TSO-DSO collaboration platform and FSPs/aggregators) would rely on MQTT/REST API.

   Figure 6.3 shows the summarized ICT architecture proposed in this pilot mapped into

the SGAM's communication layer.

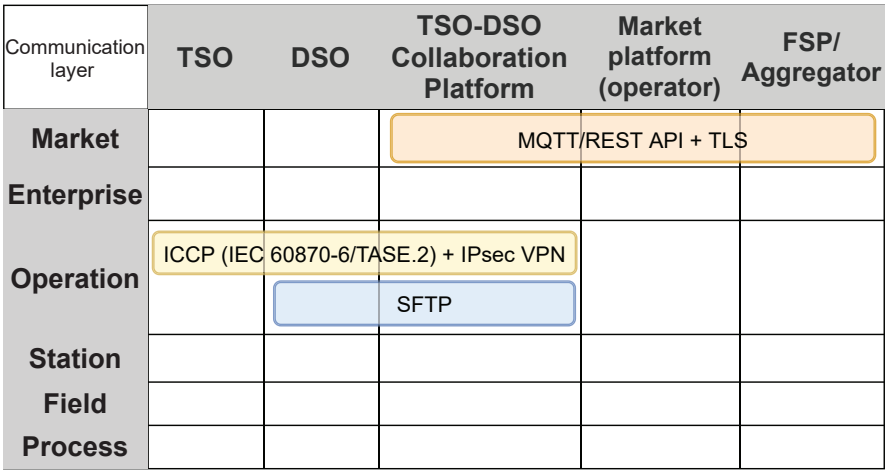

Figure 6.3: SGAM Information–Communication layer of the ICT architectures implemented in the Greek demo of Coordinet

TDK-Assist

The Horizon 2020 funded project TDX-Assist (2017-2020) aimed to develop an ICT architecture for data exchange coordination between TSO and DSO for the integration of renewable energy sources in the European marketplace using various demos in EU member states [226].

The new balancing challenges faced by SOs are typically caused by the increasing amount of distributed generation. This requires enabling an active role at the DSO level so that TSOs can coordinate with DSOs for the necessary balancing mechanisms. In the Slovenian demo of TDX-Assist, the use of DERs for balancing in a market environment was proposed and evaluated in the project using a novel Business Use Case (BUC) methodology [226] based on the IEC 62913-1 blueprint use case method endorsed by IEC SyC Smart Energy WG 6. To address different balancing market situations in the project, various scenarios were considered. The first represents the much-needed data exchange between the TSO, the DSO, and the BSP. In the second alternative scenario, data is exchanged directly between the TSO and the DSO, where the DSO also acts as the Balancing Service Provider (BSP). This BUC was implemented in Slovenia to validate the required CIM-based data modelling and exchange mechanisms between DSOs and TSOs.

The ICT architecture implemented in the Slovenian demo [227] for the communication between the TSO, which hosts the market platform, and the DSO (also acting as the BSP), was based on the ICCP link and the ENTSO-E Communication and Connectivity Service Platform (ECCo SP), as depicted in Figure 6.4. It could be considered that it follows common market model with the DSO and TSO (through the market platform) exchanging data as real-time information. In this case, ICCP, being a SCADA-to-SCADA protocol, is used for real-time

data exchanges between the DSO's SCADA and the TSO. The rest of the data is exchanged through ECCo SP using two alternative technological ways: AMQP and File System Shared Folders (FSSF) for large file exchanges (e.g., topology data).

To collect real-time measurements at the DSO level and send the activation signals needed for the tested balancing mechanism, MQTT is used by the DSO, making sure the CIM data model is implemented as a customized payload profile for the semantic layer. Through the MQTT broker, this data is also made available to other applications at the control centre level, such as the power quality monitoring system. For its exchange through ECCo SP, an MQTT/AMQP adapter was implemented by the respective DSO in the TDX-Assist demo.

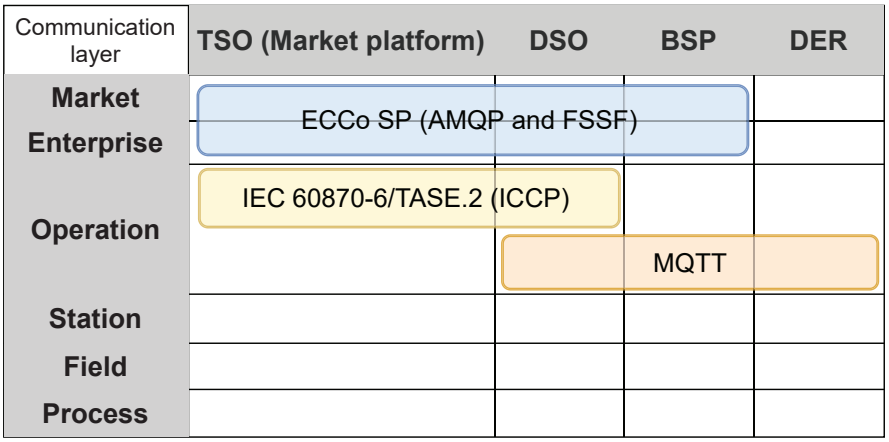

Figure 6.4: SGAM Information–Communication layer of the ICT architectures implemented in the Slovenian demo of TDX-Assist

INTERRFACE

The INTERRFACE project (2019-2022) created a "TSO-DSO-Consumer INTERFACE aRchitecture" to provide innovative grid services for an efficient power system. It focused on the coordination processes between TSOs and DSOs for procuring balancing, other ancillary services, and congestion management. These services should be acquired by TSOs and DSOs at both the transmission and distribution levels, allowing for a more efficient use of the power network, a greater presence of demand response, and an increased hosting level of renewable generation.

With this aim in mind, INTERRFACE supported digitisation as the key driver for resource optimisation from the SOs' perspective and active market participation from the FSPs' perspective. IEGSA was the digital tool specifically designed and developed for this [217] as shown in Figure 6.5. It acts as the interface between the SOs and the customers.

INTERRFACE had multiple demonstration areas and theoretical TSO-DSO coordination plans (referred to as "options") for balancing and congestion management markets. Here it

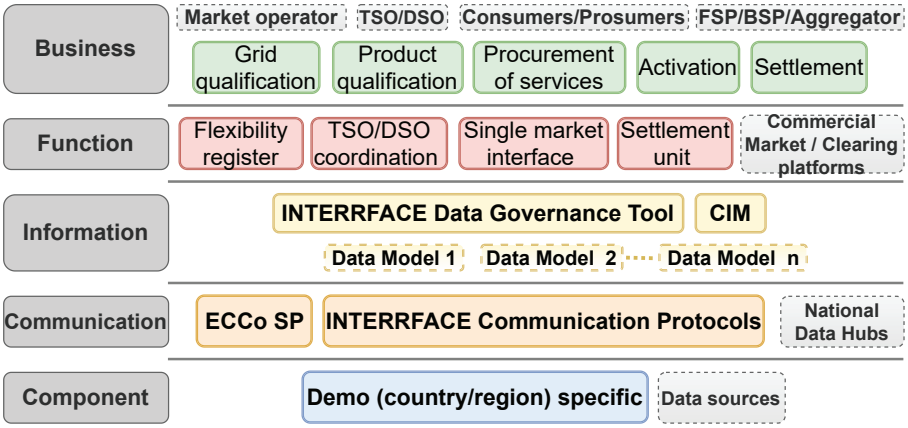

Figure 6.5: IEGSA. Source: own elaboration based on [217].

is only mentioned the 'Single Flexibility Platform' demonstrator, which is part of option 3 in [228]. This demonstrator involved three countries (Estonia, Finland, Latvia), and TSOs and DSOs from each of these. Its purpose is to facilitate the exchange of flexibility across country borders, to combine existing balancing products with congestion management products, and to expand the market by including distributed flexibility with locational bid information. It also introduced two new actors that are part of the IEGSA framework - the 'Flexibility Register' and the 'TSO-DSO Coordination Platform'.

The two actors, together with system operators and providers of flexibility, engage in tasks such as managing flexibility resources and bid location data, network topology management, handling resource and grid qualification, pre-qualification of products, and choosing bids, among other responsibilities.

EU-Sysflex

The EU-SysFlex project (2017-2021) was focused on creating a pan-European system that can effectively coordinate the use of flexibilities to integrate renewable energy sources. The project provided proposals in the areas of market design, system operation, and data management, and some of these proposals were tested in various demonstrations.

The German demonstration can be categorised as a decentralised common TSO-DSO market model (SmartNet nomenclature [222]). This model was designed and tested for congestion management and voltage control. It involved processes such as informing the SOs about the availability of flexibilities, selecting the necessary ones to resolve grid congestion by each SO, calculating the maximum flexibility potential for the upstream SO, and activating the flexibility for its own needs and in response to requests from the upstream SO [229].

An illustration of this is the "Flexibility Platform" demonstrator, which is essentially an integrated flexibility market model (SmartNet nomenclature [222]). Although it could be operated by the TSO, DSO, or jointly by them, it was designed so that a third party could

also assume the role of Market Operator (MO). This integrated approach does not imply the existence of a single platform per country or region. In contrast, different platforms could compete. However, this requires extra interoperability between platforms.

But even within one platform, the mix of all the functionalities and external integrations is complex. As many as 31 functional processes associated with the flexibility market were identified, which can be incorporated into the Flexibility Platform. These processes include registering flexibility requirements and capabilities, pre-qualifying flexibility suppliers, ranking flexibility offers, managing requests for flexibility activation, baseline calculation, verifying delivered flexibilities, and so on.

The primary goal of EU-Sysflex was to make it easy for all stakeholders to access the marketplace. This involves creating unified market regulations and enabling smooth data exchanges. The Flexibility Platform is available to any flexibility provider and any SO, and is able to manage any type of flexibility product, including ”joint products” (which can be used for various purposes and by different SOs). To achieve this, much focus must be placed on data management, including secure exchange of confidential information.

Elering’s Estfeed data exchange platform was used in the demonstrator for all data exchanges (Figure 6.6). The Estfeed protocol [230] is based on Simple Object Access Protocol (SOAP) and REST. Data users and data sources communicate with Estfeed adapters using Hypertext Transfer Protocol Secure (HTTPS) protocol. Estfeed messages are encoded using Multipurpose Internet Mail Extensions (MIME) multipart format. The header of the message must contain metadata in EXtensible Markup Language (XML) format, while the payload can be in any format.

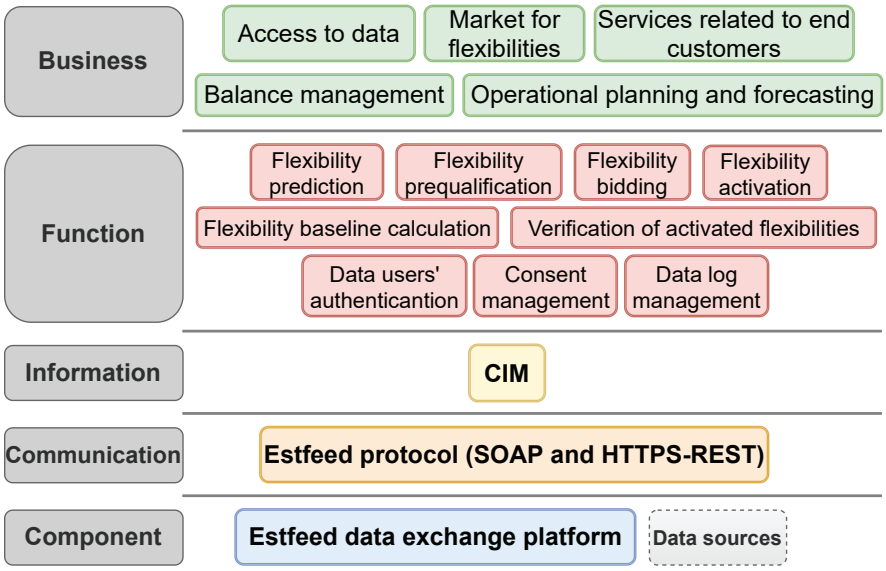

Figure 6.6: Summary of the SGAM layers of the ”Flexibility Platform” demonstrated in EU-SysFlex

The Flexibility Platform eliminates the need for explicit coordination between TSOs and DSOs; the platform handles all interactions between them. All SOs utilise the platform to exchange pertinent information. In this way, joint procurement of flexibilities that create synergies can be enabled through coordinated grid impact assessment, socio-economic bid optimisation, and value stacking.

"Flexibility Platform" demonstrates a list of System Use Cases (SUCs) elaborated specifically for flexibility data exchange. These SUCs, include flexibility prediction, prequalification, bidding, activation, baseline calculation, and verification of activated flexibilities. Additionally, other data management demonstrators have implemented 'process-agnostic' SUCs such as data users' authentication, consent and data log management, etc. The IEC 62559-2 standard template was used to describe the use cases [231] and the SGAM framework was used to model them. A standards gap analysis was performed for each SUC and two use cases were modelled in CIM (EU-SysFlex referred to this as the "CIMification" process [232]).

6.3 Protocols and standards for data exchange: comparison and application

Section 6.2 has shown the wide range of ICT options to implement similar use cases that require the information exchange between SOs. Table 6.1 summarises the ICT architectures of the EU-funded projects analysed.

All the projects analysed in the previous section used CIM as information model. CIM aims to facilitate the exchange of grid and market data between organisations, as well as the exchange of data between systems within a single organisation [233]. The core of CIM is mainly defined in two families of standards: IEC 61970 standards [234], that aim to define EMS Application Program Interfaces (APIs), and IEC 62325 standards, which define CIM for energy market communications.

Table 6.3 summarises the potential coverage and applicability of CIM and other standards (IEC 61850 and IEC 61968) for the exchange of information that may be necessary for emerging use cases.

IEC 61850 is a set of communication and information standards that is widely used by DSOs for the automation of substations. However, through IEC 61850-7-420 [235], it also defines information exchanges between DER (including EMS) and distribution automation systems. Therefore, its adoption by DER operators and manufacturers could facilitate the exchange of DER structural data (i.e., characteristics of the DER connected), which is relevant for their correct integration into the operation and planning of the distribution grid.

Table 6.1: ICT architectures implemented in EU-funded projects. C-S: Client-Server ; P-S: Publish-Subscribe

Approach	Demo	Protocol/Platform	Type	Communication link	Information exchanged
Market platform interacts with TSO and DSO for network constraints and needs	SmartNet Denmark	IEC 62325	C-S	TSO-DSO-MMS MMS ↔ CMP	Reserve needs, market bids, and activation
		IEC 61968, IEC 61970	/	TSO-DSO- Market Management System	Network constraints
		COSEM, ICCP, IEC 61850 (MMS)	C-S	CMP ↔ DER aggregator	Asset activation.
		OpenADR, IEC 61850 (GOOSE, SV)	P-S	DER aggregator ↔ DER units	DER characteristics
Common platform interacts with DSO platform to exchange needs and constraints	CoordiNet Spain	IEC 62325-504 (CIM WS)	C-S	DER generation ↔ Common Platform Common platform ↔ FSPs Common platform ↔ DSO platform	Flexibility bids. Activation signals and settlement processes DSO needs and constraints
		ICCP	C-S	Common Platform ↔ FSPs (Market)	Activation signals
		MQTT	P-S	FSPs ↔ DER units	Congestion market results. Unit monitorization.
Common platform also includes interactions between TSOs and DSOs	INTERRFACE "Single Flexibility Platform"	ECCo SP	P-S C-S	Flexibility register function TSO-DSO Coordination function Single market interface function Settlement unit function	
		INTERRFACE Communication Protocols			
LM by DSO must meet set-points by TSO	SmartNet Spain	IEC 62325	C-S	DSO ↔ Market Management System Market Management System ↔ CMP Trading System DSO ↔ Market Management System Market Management System ↔ CMP Trading System	Market clearing, bids, prequalification, and reserve needs
		COSEM, ICCP, IEC 61850 (MMS)	C-S	CMP Trading System ↔ DER Aggregator	Asset activation and confirmation
		OpenADR, IEC 61850 (GOOSE, SV)	P-S		
Market platform for market info and TSO-DSO platform for other	CoordiNet Greece	ICCP	C-S	TSO-DSO platform ↔ SCADA and EMS	TSO-DSO coordination
		SFTP	C-S	TSO-DSO platform ↔ DSO's systems and TSO's GIS	
		MQTT	P-S	TSO-DSO platform ↔ Market platform, other systems	
		HTTPS (REST API)	C-S	Market platform ↔ Market operator, forecast provider, FSPs/aggregators	Market-related communications
Common platform handles all the required interactions between TSOs and DSOs	EU-SysFlex "Flexibility platform"	Estfeed Platform	P-S C-S	All interactions	/
Common market platform is used for real-time data exchange between TSO-DSO	TDX-Assist Slovenia	ICCP	C-S	DSO ↔ TSO (market platform)	Real-time data
		ECCo SP (AMQP and FSSF)	P-S C-S	DSO ↔ TSO (market platform)	Meter and grid data (i.e., field measurements)
		MQTT	P-S	DER, smart meters ↔ DSO	Real-time measurements and activation signals.

IEC 61968 standards aim to define information exchanges between distribution systems. IEC 61968-11 [236] and IEC 61968-13 [237] provide CIM extensions for the exchange of modelling information (i.e., network models) and distribution network data. Some of these extensions are used not only internally or between DSOs, but also to exchange information (e.g., DER structural data or forecasts) with other stakeholders (TSO, customers, etc.).

Regarding the core CIM standards, they aim to cover a wide variety of information. Starting with the ones defining EMS APIs (IEC 61970 standards), IEC 61970-301 [238] sets out the basic CIM, providing a model to represent the main objects used in utility operations. Despite its limitations, some of its packages, such as the "Operational Limits" package or the "Availability" profile could be useful for the exchange of temporary limits on balancing capacity bids [239]. IEC 61970-302 [240] provides an extension ("Dynamics" package) for the exchange of models for stability analysis, becoming relevant for the accurate inclusion of DER in such studies (for example, for the analysis of MaDIoT 3.0 scenarios). IEC 61970-452 [241] defines the parts of CIM that are necessary for state estimation and power flow applications, whereas IEC 61970-456 [242] outlines the contents and procedures to exchange the steady-state solutions of these and other applications. These two last standards are used together with IEC 61970-457 [243], which is based on IEC 61970-302 to provide a data model for the exchange of information of the dynamic models used in different dynamic studies.

To make it easier for TSOs to share operational and grid planning information, the CGMES was created. This is reflected on the IEC 61970-600-1 & 2 standards [244], [245] and is necessary for the implementation of network codes related to capacity calculation, congestion management, and system operation. However, for its application by DSOs, the compliance of CGMES profiles with distribution requirements should be validated [239].

As for market-related communications based on CIM, IEC 62325-351 [246] (also known as European Style Market Profile (ESMP))is applicable to European style electricity markets, defining data models to comply with European regulations, whereas IEC 62325-301 [247] extends CIM for energy market communications. ESMP constitutes the basis for the IEC 62325-451-*X* series: IEC 62325-451-2 [248] is used for the scheduling business process; IEC 62325-451-4 [249] provides a model for the transmission of aggregated data that enables market settlement and reconciliation; IEC 62325-451-5 [250] defines the model for the business processes of problem statement and status request; and IEC 62325-451-6 [251] defines the model for the publication of market information.

Despite the great advances in interoperability that the CIM standards provide, there are still some practical issues that may arise when developing a system. These issues can be related to CIM extensions, the harmonisation of other standards when connecting multiple systems or applications, and the validation of model instances [252]. The gap analysis in EU-SysFlex [232] concluded that CIM coverage may need to be improved when dealing with data hubs, data portability, sub-meter data, data aggregation and anonymisation, consent management, data logs exchange and authentication information, data exchange between DERs

Table 6.2: Summary of advantages/disadvantages of C-S and P-S communications.

Communication paradigm	Type of information exchanges	Advantages/Disadvantages
C-S	Synchronous	- Well-defined interfaces (API REST) - Waste of communication resources if information updates are not frequent or not synchronised
P-S	Asynchronous	- Lightweight protocols. Communication is more effective since transactions occur only when updates are available.

and SOs (e.g., by harmonising CIM and IEC 61850 [253]), and when implementing other flexibility services besides balancing. On the other hand, no CIM extensions are necessary for congestion management if the Manual Frequency Restoration Reserve (mFRR) type product is used to provide this service.

Two primary ICT strategies can be identified when implementing a data exchange system: one involves the creation of new platforms (i.e., custom-made) that can be integrated with existing SO's systems (e.g., CoordiNet); and the other involves the use of an external Data Exchange Platform (DEP) such as ECCo SP or Estfeed (e.g., INTERRFACE, EU-SysFlex).

Centralised market schemes do not present significant technical challenges for data exchange, as there is only one market platform that interacts with the different stakeholders. However, meeting data exchange requirements can be challenging, particularly when the scheme requires real-time synchronisation of multiple platforms or processes with different actors. This would be more difficult to implement, as it requires seamless communication between markets.

At the communication layer, two paradigms are typically used for communication protocols: Client-Server (C-S) (i.e., request-response) and Publish-Subscribe (P-S). The advantages and disadvantages of both paradigms are numerous [254] and are summarised in Table 6.2. The most suitable one depends on the data exchanged and the connected systems.

In the C-S paradigm, the client regularly polls the server to obtain its status through clearly defined interfaces. This implies that, unless updates are frequent or the communication is synchronised, memory, computing, and energy resources may be wasted during certain times. In terms of reliability, the server response confirms that the client request was properly received and processed.

Typically, exchanges of market data take place at predetermined times, such as when a market process is about to be initiated or cleared. As the number of agents involved in

a process can be large (Figure 2.2), a web service architecture such as HTTP-based REST ensures a high degree of interoperability, synchronous communication, and the establishment of well-defined procedures through APIs. This is particularly evident in SmartNet and the Spanish demo of CoordiNet, where the market requests bids from the CMPs/DERs through WS. On the other hand, in P-S, messages are received by the subscribers of the topic as they are published on that topic, with a broker acting as an intermediary. This is useful when the same communication needs to be sent to multiple recipients without pre-determining the time or frequency. However, publishers cannot determine if the message was received successfully by all subscribers, as the broker decouples them from the publisher.

In certain market data subclasses, such as generation and appliance data, and meter data, it is necessary to communicate information quickly and to multiple entities at the same time. In these cases, a publish-subscribe protocol like MQTT [255] may be more suitable. This protocol is widely used in IoT devices with limited communication capabilities due to its low message overhead, latency, and quality of service options. This allows the broker to guarantee that the message is received by all subscribers, even avoiding duplicates.

In the Spanish demonstration of CoordiNet, MQTT is employed by FSPs to observe the activation of DERs (many-to-one communications). Nevertheless, for data exchanges between a limited number of platforms/systems (i.e., not field devices), where communications are not expected to be heavily restricted, AMQP may be a more suitable choice than MQTT. AMQP [256] is based on queues (similar to topics) and provides additional security and control over messages. To enhance scalability and reliability at an enterprise level, it is recommended to implement AMQP and restrict the use of MQTT to edge connections [257] (e.g., meter data from DERs, activation signals, etc.). This approach was followed by the Slovenian demonstration of TDX-Assist, to use ECCo SP between the DSO and the market platform in the TSO.

Two main options for exchanging grid data are identified: ICCP and DEPs. The ICCP standard [258] provides a C-S service model for the direct transfer of time-sensitive data between control centres through wide and local area networks, including time-series data, control operations, scheduling information, etc. Although ICCP is traditionally used for the exchange of grid data between TSO and DSO [211], its standard version is considered a legacy protocol that lacks sufficient protection and has a large attack surface [259], [260]. Therefore, the use of DEPs as an alternative is increasing for centralised schemes, so that the system to access meter, grid, and market data can be the same and new agents can easily connect without a major investment in an ICCP connection. Some of these DEPs, such as Estfeed, have their own protocol [230] that defines a 'Publish' protocol and a 'Request-Response' protocol to meet the requirements of the different agents and data exchanges, as well as adapters for data hubs and applications; others, such as ECCo SP, are compatible with different protocols, such as AMQP, WS, and FSSF [261], which may already be used by SOs.

Table 6.3: Summary of standards coverage and applicability for the exchange of specific types of information. Source: Own elaboration based on [239] and standards specifications.

Category	Information	IEC 61850	IEC 61968		IEC 61970						IEC 62325						
		IEC 61850-7	IEC 61968-11	IEC 61968-13	IEC 61970-301	IEC 61970-302	IEC 61970-452	IEC 61970-456	IEC 61970-457	CGMES (IEC 61970-600-1 & 2)	IEC 62325-451-4	IEC 62325-451-5	IEC 62325-451-6	IEC 62325-451-7	IEC 62325-451-2	IEC 62325-301	ESMP (IEC 62325-351)
Services, markets, and network requirements	Market result												X	X			
	Product prequalification results																X
	Market participant pre-qualification information																X
	Basic participant information																X
	Invoicing data										X						
	Settlement data										X		X				
	Aggregated data																X
	Network data of distribution system			X						X			X				
	Network demand forecast			X						X			X				
	Network information						X			X							
	Network reconfiguration data												X				
TSO-DSO Information exchange	Flexibility resources													X			
	Flexibility resources qualification results										X	X	X	X	X		
	Scheduling process: activation signal correction/counter action														X		
	Execution order														X		
	Baselines reports												X				
	Connection state forecast									X							
	DER Structural data	X	X	X		X											
	Development plans for distribution networks						X			X							
	Dynamic Line Rating forecast for overhead lines												X				
	Energy clearing results										X				X	X	X
	Flexibility needs										X				X	X	X
	Forecast data			X						X			X				
	Grid congestion status											X				X	
	Limits and margins for capacity (by zone)															X	X
	Grid constraints assessment												X				
	Network characteristics (internal) information						X			X							
	Temporary limits on balancing capacity bids				X								X				
	Power flow simulation						X	X	X	X							
	Resource optimisation information														X		
	Short circuit power forecast													X			
	State estimation data						X	X									
	System parameter control schema/instructions						X	X									

6.4 Conclusions

The electrification of energy demand and the increasing penetration of DER pose some challenges to SOs in terms of operation that allows the possibility of acquiring and activating new system services faster and cheaper than network upgrades. The implementation of these services will require better coordination between TSOs, DSOs, and service providers, which at the same time requires more interoperability between systems for a better data exchange between entities.

Since this is currently the scope of many research projects, this chapter has reviewed seven ICT architectures for data exchange implemented in five EU-funded projects, identifying common protocols and standards based on the type of data and communication link.

Among the different coordination schemes developed for new market mechanisms, the ones involving multiple platforms can be the most challenging from the ICT point of view, requiring seamless real-time synchronisation of different market platforms or processes. However, this real-time synchronisation would also provide a basis for improving the daily operation of the electricity system.

The CIM is the main data model used for data exchange between SOs and other entities. It covers technical information for DSOs, TSOs and other agents, such as DER operators, as well as market-related information. However, this coverage is in many cases partial and more collaboration is needed on the definition of CIM extensions that can be widely applied, not limited to specific use cases or entities. Furthermore, to improve the interoperability of systems and platforms, CIM would need to be better harmonised with other widely used standards such as IEC 61850. This harmonisation could facilitate data exchange between DER and SOs, improving their integration into the operation of the system, and enabling mechanisms to minimise the risk of MaDIoT 3.0 attacks.

In terms of communication protocols, C-S mechanisms are appropriate for the communication of synchronous market processes (WS or https-REST) and grid data (ICCP, DEPs). However, in this last case, the standard ICCP is considered a legacy protocol that should be replaced by more modern and secure protocols or, directly, by using DEPs.

For real-time market and meter data exchanges, P-S protocols can be, in general, conveniently implemented. However, MQTT is better for communications with field/remote devices, and AMQP for the communications between larger systems/platforms, because of their design characteristics.

As an alternative to point-to-point connections between systems and ad-hoc platforms, existing DEPs could provide faster and more cost-effective use case implementations because of their interoperability potential. However, they should prove to be scalable and replicable, guaranteeing low communication latencies for those data exchanges requiring real-time capabilities; otherwise, a mixed approach may be more convenient.

Chapter 7

Conclusions, contributions, and future research

7.1 Introduction

This last chapter summarises all the content and conclusions developed in this thesis, lists all main contributions, and proposes future lines of work that are left open for further research.

The chapter is divided into four main sections. Section 7.2 presents a qualitative overview of all the topics discussed in this document. Section 7.3 explains the main conclusions that can be extracted from the whole document. Section 7.4 outlines the main contributions that have emerged from the research conducted. Lastly, Section 7.5 suggests potential lines of work to further advance the knowledge developed in this thesis.

7.2 Summary

This thesis can be divided into four parts, all focused on the difficulties associated with enhancing the digitalisation of electricity distribution systems to facilitate the advancement of smarter grids. These challenges are introduced in Chapter 2, which establishes the context for the rest of the document.

The first part (Chapter 3) contributes to address the challenge of measuring the digitalisation of distribution grids in a straightforward way. This is important to objectively compare the efforts of DSOs and to establish cause-effect relationships between investments and performance.

The second part (Chapter 4) focuses on the scalability and replicability of ICT for an efficient digitalisation. It proposes a quantitative methodology to assess these aspects within the context of a smart grid. However, it is important to note that while the high scalability

and replicability of ICT can be advantageous, they can also pose a risk to the power system if there are vulnerabilities and an attacker can exploit them.

The third part (Chapter 5) analyses the consequences for the power system in the event that a hacker successfully compromises high-wattage IoT devices in the demand (MaDIoT attack) and DER control devices (MaDIoT 3.0 attack). This analysis provides information on the scalability and replicability of the impact of these attacks under various conditions.

The last part of this thesis (Chapter 6) focuses on improving the communication between system operators. This is crucial to enhance the resilience of the system and reduce the impact of MaDIoT attacks. In addition, it aims to facilitate the integration of DER in system operation. This part examines various protocols and standards for TSO-DSO data exchange and explores their suitability for exchanging specific types of information.

7.3 Main conclusions

All the conclusions that have been drawn throughout the chapters are summarised in the following paragraphs:

- Although digitalisation of distribution grids offers numerous advantages, including enhanced operational efficiency, it also presents some challenges that need to be addressed. The rise of *prosumers* and the integration of DER necessitate the implementation of new technologies for control, monitoring, and system service provision to optimise grid operation without needing costly upgrades of the electrical infrastructure. The digital transformation of DSOs requires a robust digital culture, effective leadership, and the attraction and training of employees with digital skills. The deployment of sensors, connectivity, and data processing technologies positively influences the main activities of DSOs, but it will also require greater collaboration within the power sector. The scalability and replicability of ICT systems, the proper selection and configuration of technologies, and the resistance to change by employees, in addition to the deficient security of IoT and DER devices, significantly increase the cybersecurity risk, which is identified as one of the main challenges. DSOs must go beyond cybersecurity regulation and adopt comprehensive defence strategies, foster a cybersecurity culture, and take advantage of new technologies to improve cybersecurity measures in an ever-evolving threat landscape.

- The proposed digitalisation indicators, mainly focused on the digital infrastructure rather than overall performance, address the imperative to evaluate the digitalisation level of distribution grids. Aligned with the EU Directive 2019/944 and the JRC DSO Observatory, these indicators facilitate comparisons and the identification of best practices. In particular, they are use-case-agnostic, data-efficient and of interest for both

National Regulatory Authorities (NRAs) and DSOs to comprehensively assess digitalisation levels and discern cause-effect relationships between performance and digital infrastructure. Widespread adoption of these indicators could foster synergies, enabling DSOs to benefit from shared experiences and NRAs to strategically guide digitalisation investments. However, the realisation of these benefits depends on the regulatory promotion, the standardisation of data collection processes, and the public dissemination of results.

- The inclusion of ICT within the scope of a SRA to comprehensively evaluate the scalability and replicability of solutions may be key for the development of smart grids, given their increasing dependence on these technologies. The quantitative methodology proposed for conducting an ICT SRA in a smart grid context is agnostic to use cases and communication technologies, ensuring flexibility for the analysis, as demonstrated when applied to two real case studies involving different communication technologies. ICT SRA results are presented through ICT scalability and replicability maps, a novel concept that facilitates a quick overview of the scenarios analysed and an efficient estimation of the feasibility of unexplored ones. The application of the methodology demonstrates its effectiveness in systematically analysing the scalability and replicability of ICT systems, offering clear insights into critical links, requirements, constraints, and influencing factors, regardless of the type of technology (wired or wireless).

- The analysis of MaDIoT attacks on two different power system models reveals different success ratios and impact, showing that higher success ratios do not necessarily correlate with greater impact in the systems analysed. The connection of distributed solar PV generation alters the response of the PST-16 system, reducing both the success and the impact of the attack. MaDIoT 3.0 attacks, which combine attacks on demand and DER, highlight the predominant effect of concentrated demand attacks (vulnerable devices with great local scalability and replicability) on the probability of success in the PST-16 system under the conditions analysed. High-wattage IoT devices and DER equipment must follow stringent cybersecurity standards and undergo rigorous tests to mitigate the risk of compromise. At the system operation level, TSOs and DSOs should incorporate MaDIoT attacks into their cyber risk management plans and increase collaboration, coordination and information exchange to improve the efficiency, reliability, and security of electricity systems.

- The coordination and data exchange between TSOs, DSOs, and service providers is crucial to meet the challenges posed by the electrification of energy demand and the increasing connection of DER without incurring costly network upgrades. A seamless data exchange requires systems to be interoperable. Common protocols and standards are identified in seven ICT architectures for data exchange implemented in EU-funded

projects. A decentralised data exchange approach can be a potentially challenging but operationally beneficial scheme, requiring real-time synchronisation of multiple platforms. The Common Information Model (CIM) serves as the primary data model but requires further collaboration to provide comprehensive coverage of information and harmonisation with widely used standards, such as IEC 61850. Communication protocols following Client-Server (C-S) mechanisms, are deemed suitable for synchronous market processes and grid data exchanges, and more modern protocols can replace legacy protocols like ICCP. Publish-Subscribe (P-S) protocols, such as MQTT and AMQP, are suggested for direct communications with field or remote devices, and for the communications of larger systems or platforms at the business layer, respectively. Centralised data exchange platforms could facilitate cost-effective and interoperable implementations, contingent on scalability and low-latency considerations for real-time data exchanges, which should be analysed.

7.4 Thesis contributions

The contributions of this thesis are in line with the objectives that were set out in Section 1.2. Here, each of the objectives is evaluated based on the results presented in this thesis.

- **Objective:** *Identify the main technologies and challenges of the digitalisation of electricity distribution grids.*
  Chapter 2 identifies the main technologies for the digitalisation of distribution grids and maps them against the main applications. It also discusses the challenges that digitalisation poses in terms of cybersecurity, core processes, and for the electric power ecosystem in general.

- **Objective:** *Propose a framework to measure the digitalisation of distribution grids in an easy way and that allows the fair comparison of DSOs regardless of their size.*
  Chapter 3 proposes a total of 16 indicators to measure the digitalisation of distribution grids, and not their performance, which was the focus of previous work. The indicators are organised according to the digitalisation pillars (sensors and actuators, connectivity, data processing, and digital culture), and are in consonance with Article 59.1 of EU Directive 2019/944 and Joint Research Center DSO Observatory's recommendations; they are agnostic to use cases, do not require a large amount of information, and could be used to identify cause-effect relations between performance and digital infrastructure.

- **Objective:** *Develop and apply a methodology to perform quantitative scalability and replicability analyses of ICT for smart grid use cases.*
  Chapter 4 described a step-by-step methodology to perform ICT SRA in smart grids.

To validate this methodology, is is applied to two real case studies, using OMNeT++ as simulation tool. Case study A analyses a monitoring and control system that relies on wired technology (Modbus TCP) for a self-consumption solution; Case study B analyses an indoor conditions monitoring system based on wireless technology (wireless M-Bus). ICT SRA results are presented through ICT scalability and replicability maps, a novel concept that facilitates a quick overview of the scenarios analysed and an efficient estimation of the feasibility of unexplored ones. The methodology proves to be an efficient way to analyse wired and wireless ICT, providing a comprehensive SRA of ICT systems for different scenarios.

- **Objective:** *Perform a simulation study of the impact on different power systems of cyberattacks to highly scalable and replicable devices. The devices to be considered include high-wattage IoT devices and control devices for distributed energy resources.*
  Chapter 5 conducts two studies regarding this objective. The first one analyses the replicability of MaDIoT attacks (i.e., attacks to demand) in two different power system models (the PST-16 model, representing a simplified version of Europe; and the IEEE 39-Bus model, representing New England), highlighting the differences that the attacks present both in terms of success and impact. This expands and complements previous work that was mainly focused on American power system models. The second study assessed the replicability of MaDIoT attacks when the power system has distributed solar PV generation. It also analyses the impact of MaDIoT 3.0 attacks, which are introduced in this thesis as an evolution of the original MaDIoT attacks by combining attacks to both the demand and DER devices.

- **Objective:** *Perform a qualitative study of the main communication and data model standards that system operators can use to exchange specific types of information.*
  Chapter 6 identifies common protocols and standards used for data exchange between system operators in recent European projects. Their application for the exchange of specific types of information is discussed, focusing on the Common Information Model (CIM) and two alternative communication mechanisms.

Finally, the knowledge generated by this thesis is of interest to the scientific community; a proof of this is the number of publications that this work has entailed. A list of those publications can be found in Section 7.6.

7.5 Future work

This thesis leaves a number of open issues that could be further explored in future studies. Some of these are outlined below:

- To measure the relationship between digitalisation and performance of distribution grids, it should be quantified the specific relevance of each proposed indicator for each performance indicator considered (e.g., weight assignment); in the same way, this relevance should also be quantified for the different generic smart grid use cases. DSOs would have to be willing to measure the indicators and, to validate the framework, the correlation between clusters of similar DSOs (from the digitalisation perspective) and performance could be analysed.

- Regarding the SRA of ICT for smart grids, it would be interesting to study the applicability of the methodology using a co-simulation approach (e.g., simulating the communications and the power layer) or hardware-in-the-loop.

- For the analysis of MaDIoT attacks, future work may consider the dynamics and protection schemes of large electricity distribution systems connected to transmission systems. This would require the development of an integrated transmission and distribution system model, which would also require a large computational capacity. The consideration of both the transmission and distribution systems is an interesting research line to explore in the future. Other interesting future research work goes along the line of including automatic or manually induced operator actions, such as re-dispatches, to avoid, for instance, line overloads that could lead to subsequent line trippings and initiate a cascading outage. Such mitigation actions have not been considered in previous works. Sequential attacks (increasing/decreasing demand in time during the same attack) also represent interesting future research lines.

- Regarding information exchanges between system operators, future research needs to analyse the data intensiveness required for a good coordination between operators. The analysis of the SGAM component layer of the ICT architectures would also be of great interest so that component costs could be estimated and used in a cost-benefit comparison. Furthermore, the use of cybersecurity standards for information exchange would be an interesting research topic.

7.6 Published and under-review work

The published work produced as a consequence of the current research is shown in the following sections.

7.6.1 Conference presentations

- **Title:** Scalability evaluation of a Modbus TCP control and monitoring system for Distributed Energy Resources.
  Authors: N. Rodríguez Pérez, J. Matanza, G. López, and V. Stojanovic.
  Conference: IEEE PES International Conference on Innovative Smart Grid Technologies Europe - ISGT Europe 2022, Novi Sad (Serbia). 10–12 October 2022.
  Status: Published and presented at the conference.
  DOI: `https://doi.org/10.1109/ISGT-Europe54678.2022.9960319`
  Abstract: Modbus TCP is a communication protocol widely used to communicate with energy assets such as inverters or data loggers. The communications technologies involved in the management of distributed energy resources (DER) should prove their ability to include new units in the operation while fulfilling functional requirements. This paper studies the scalability performance of Modbus TCP protocol over Ethernet to monitor and control DER in a positive energy district (PED) environment. This use case is part of an Innovative Element (IE) being demonstrated in the city of Dijon within the RESPONSE project. The analysis was carried out considering different bit error ratios (BER) and number of servers. As performance indicator, the time spent by the client to poll all the servers (i.e., polling time) was measured, as it is the most restrictive functional requirement in the use case analysed, requiring it to be one minute. Simulation results show how increasing BER and the number of devices in the network impact the total polling time. Despite the average polling time complied with the required one in most cases, its standard deviation significantly increased with BER. If the transmission medium presents a low BER, Modbus TCP has a great scalability potential to control and monitor devices that require data exchanges every minute. In addition, the maximum number of devices to keep a good performance is considered appropriate for its application in a PED environment. Future works may assess the impact of distance or topology on use case's performance.

- **Title:** Scalability analysis of a wireless M-Bus system for smart metering and sensoring.
  Authors: N. Rodríguez-Pérez, J. Matanza, G. López, and M. Hajigholi.
  Conference: 15th IEEE PowerTech Conference - PowerTech 2023, Belgrade (Serbia) 25–29 June 2023.

Status: Published and presented at the conference.
DOI: https://doi.org/10.1109/PowerTech55446.2023.10202977
Abstract: Wireless M-Bus communication protocol has emerged as one way of implementing smart metering for smart grids and cities. To determine possible applications of this technology in these contexts, its scalability and replicability potential must be analysed so that its limitations can be considered.
This paper studies the scalability performance of a wireless M-Bus that collects data from sensors deployed at dwellings in a cluster of buildings of the city of Turku, as part of the RESPONSE project. The simulation model developed for this analysis considered building obstacles and the retransmission scheme of wireless M-Bus. To assess performance, three main indicators were used: delivery ratio, message error ratio, and gross delivery ratio.
Simulation results show how the position of the data collector, the number of sensors deployed, and the area to be covered, have an impact on the different performance indicators. The wireless M-Bus system is found to be highly scalable in density for a reduced area. For large area deployments, performance declines dramatically, regardless of the position of the data collector.
Future research may compare results when considering different propagation models and also when changing environment characteristics such as walls' width.

- **Title:** Model the Path: Impact of Propagation Models on the Scalability of a Wireless M-Bus Sensoring System for Smart Grids.
Authors: N. Rodríguez-Pérez, J. Matanza, and G. López.
Conference: IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGrid Comm), Glasgow (UK), 31 October–3 November 2023.
Status: Published and presented at the conference.
DOI: https://doi.org/10.1109/SmartGridComm57358.2023.10333969
Abstract: This paper analyses the impact of the propagation model on the outcomes of a scalability analysis of a wireless M-Bus system simulated in OMNeT++. Four path loss models are compared: Free Space Path Loss (FSPL) model with obstacle-related losses, the ITU-R P.1238 model, and two configurations of the log-normal model used by previous studies in similar contexts. Performance is assessed using three main indicators: delivery ratio, message error ratio, and gross delivery ratio.
Results show that, although all the propagation models considered validate the baseline implementation of the system, performance differences emerge when scaling it up. The two configurations of the log-normal models may provide a too-optimistic scalability potential, while the ITU-R model may provide a pessimistic one. The high influence of the propagation model in the scalability results of the system is demonstrated, as

other factors, such as message collision, prove to have no impact on scalability for the scenarios analysed.
Future research may compare other standardised propagation models or consider the inclusion of more than one data collector.

7.6.2 Journals (peer-reviewed)

- **Title:** ICT Architectures for TSO-DSO Coordination and Data Exchange: A European Perspective.
  Authors: N. Rodríguez Pérez, J. Matanza , G. López, J.P. Chaves Ávila, F. Bosco, V. Croce, K. Kukk, M. Uslar, C. Madina, M. Santos-Mugica
  Journal: IEEE Transactions on Smart Grid, vol. 14, no. 2, pp. 1300-1312, March 2023. JCR: 9,600 Q1 (2022)
  Status: Published (March 2023). Online since September 2022
  DOI: `https://doi.org/10.1109/TSG.2022.3206092`
  Abstract: The coordination between system operators is a key element for the decarbonization of the power system. Over the past few years, many EU-funded research projects have addressed the challenges of Transmission System Operators (TSO) and Distribution System Operators (DSO) coordination by implementing different data exchange architectures. This paper presents a review of the ICT architectures implemented for the main coordination schemes demonstrated in such projects. The main used technologies are analyzed, considering the type of data exchanged and the communication link. Finally, the paper presents the different gaps and challenges on TSO-DSO coordination related to ICT architectures that must still be faced, paying especial attention to the expected contribution of the EU-funded OneNet project on this topic.

- **Title:** Confronting the Threat: Analysis of the Impact of MaDIoT Attacks in Two Power System Models
  Authors:N. Rodríguez-Pérez, J. Matanza, L. Sigrist, J. L. Rueda Torres, and G. López.
  Journal: Energies 16, no. 23: 7732. 2023. JCR: 3,200 Q3 (2022)
  Status: Published (November 2023)
  DOI: `https://doi.org/10.3390/en16237732`
  Abstract: The increasing penetration of Internet of Things (IoT) devices at the consumer level of power systems also increases the surface of attack for the so-called Manipulation of Demand through IoT (MaDIoT) attacks. This paper provides a comparison of the impact that MaDIoT attacks could have on power systems with different characteristics, such as the IEEE 39-Bus (New England) and the PST-16 system (simplified European model), by assuming that the attacker does not have advanced knowledge of the grid. The results for the IEEE 39-Bus system expand and complement

the results obtained by previous work. The simulation results show that these systems present significant differences between them with respect to the success probability of an attack, being in general much higher for the IEEE 39-Bus system. In the PST-16 system, the required number of bots to obtain a certain success probability varies depending on the area attacked. However, a high probability of success does not necessarily mean a high impact on the system. This paper shows that the response to the high-impact MaDIoT attacks of the two models considered is very different as the initial impact of the attack on the system also differs, mainly affecting rotor angles in the PST-16 system, and the frequency in the IEEE 39-Bus.

- **Title:** ICT Scalability and Replicability Analysis for Smart Grids: Methodology and Application
  Authors: N. Rodríguez-Pérez, J. Matanza , G. López
  Journal: Energies 17, no. 3: 574. 2023. JCR: 3,200 Q3 (2022)
  Status: Published (January 2024)
  DOI: `https://doi.org/10.3390/en17030574`
  Abstract: The essential role of Information and Communication Technologies (ICT) in modern electricity grids makes it necessary to consider them when evaluating the scalability and replicability capabilities of smart grid systems. This paper proposes a novel step-by-step methodology to quantitatively perform an ICT scalability and replicability analysis (SRA) in a smart grid context. The methodology is validated and exemplified by applying it to two real case studies that are demonstrated in the EU-funded RESPONSE project and comprise solutions relying on different communication technologies. The results of the proposed methodology are summarised through ICT scalability and replicability maps, which are introduced in this paper as a quick way of obtaining an overview of the scalability and replicability capabilities of an ICT system and as an efficient way of estimating the feasibility of scenarios not covered in the SRA.

- **Title:** Measuring the Digitalisation of Electricity Distribution Systems in Europe: towards the Smart Grid
  Authors: N. Rodríguez-Pérez, J. Matanza , G. López, R. Cossent, J.P. Chaves Ávila, C. Mateo Domingo , T. Gómez San Román, M.A. Sánchez Fornié
  Journal: International Journal of Electrical Power and Energy Systems (IJEPES) Vol. 159, pp. 110009-1 - 110009-9, 2024. JCR: 5,200 Q1 (2022).
  Status: Published (August 2024).
  DOI: `https://doi.org/10.1016/j.ijepes.2024.110009`
  Abstract: This paper proposes a set of digitalisation indicators focused on measuring the different digital capabilities and infrastructure of electricity distribution systems, as opposed to previous indicators which have mainly focused on performance and quality

of service aspects.
The indicators are classified according to the pillars of digitalisation: sensor and actuator, connectivity, data processing, and digital culture. They are use-case-agnostic and do not require a huge amount of information. In addition to this, three possible new applications of these indicators for distribution system operators and regulatory authorities are identified and discussed.
The extensive use of these indicators in Europe could allow the development of fruitful collaborations between distribution system operators, allow the identification of cause-effect relations between grid performance and digital infrastructure, and improve the replicability of innovative smart grid solutions. However, this will only be possible if regulators promote the adoption of the proposed indicators and the dissemination of their results.

7.6.3 Papers under review

- **Title:** Digitalisation of Distribution Grids: Technologies and Challenges for the Development of Smart Grids
  Authors: N. Rodríguez-Pérez, E. de Leyva Mérida , G. López, J. Matanza, J.P. Chaves Ávila, R. Cossent
  Journal: Renewable and Sustainable Energy Reviews JCR: Q1
  Status: First review.
  Abstract: Digitalisation in the electricity sector can provide several benefits to the operation of distribution grids, but also pose some challenges in terms of cybersecurity, for the core processes, and for the electric power ecosystem in general. This paper provides an overview of how key technologies can optimise core processes and asset management activities and discusses the main challenges that arise as a consequence of digitalisation. Technologies related to Internet of Things, Big Data, advanced analytics, and cloud computing have a great potential to help develop the smart grid concept in distribution grids. For this, however, the electricity sector should increase their systemic resilience through the adoption of defence-in-depth strategies, coordination of information and operation technologies, and end-to-end cybersecurity strategies.

- **Title:** MaDIoT 3.0: Assessment of Attacks on Distributed Energy Resources and Demand in a Power System
  Authors:N. Rodríguez-Pérez, J. Matanza, L. Sigrist, J. L. Rueda Torres, and G. López.
  Journal: IEEE Transactions on Smart Grids JCR: 9,600 Q1 (2022)
  Status: First review
  Abstract: The increasing penetration of Distributed Energy Resources (DER) expands the cyberattack surface of power systems. This paper analyses the impact and success

of MaDIoT 3.0 attacks, which combine attacks to high-wattage IoT devices in the demand with attacks to DER devices that end up in the disconnection of these resources from the system.
The results indicate that the inclusion of distributed solar PV generation in the system reduces the success ratio and impact of load-altering MaDIoT attacks when compared to the same system without distributed generation. For Madiot 3.0 attacks, the demand had a more significant influence on the attack's success than the DG. Distributing the attacked demand across more buses or targeting the demand from other areas would decrease the probability of success. Therefore, the local scalability and replicability of high-wattage demand devices become more critical than their distributed deployment on a regional scale.

7.7 Research projects

The contributions of this thesis were part of the work developed by the PhD candidate in the following projects:

- **RESPONSE. integRatEd Solutions for POsitive eNergy and reSilient CitiEs**
  Funding: European Union Horizon 2020. Grant agreement No. 957751
  Beginning - Finish Dates: October 2020 - September 2025
  Webpage: `https://h2020response.eu/`

- **eFORT- Establishment of a FramewORk for Transforming current EPES into a more resilient, reliable and secure system all over its value chain**
  Funding: European Union Horizon Europe. Grant agreement No. 101075665
  Beginning - Finish Dates: September 2022 - August 2026
  Webpage: `https://efort-project.eu/`

- **OneNet- One network for Europe**
  Funding: European Union Horizon 2020. Grant agreement No. 957739
  Beginning - Finish Dates: October 2020 - September 2023
  Webpage: `https://www.onenet-project.eu//`

- **IELECTRIX - Indian and European Local Energy CommuniTies for Renewable Integration and the Energy Transition**
  Funding: European Union Horizon 2020. Grant agreement No. 824392
  Beginning - Finish Dates: May 2019 - October 2022
  Webpage: `https://ielectrix-h2020.eu/`

- **EUniversal - Market enabling interface to unlock flexibility solutions for cost-effective management of smarter distribution grids**

Funding: European Union Horizon 2020. Grant agreement No. 864334
Beginning - Finish Dates: February 2020 - July 2023
Webpage: https://euniversal.eu/

- **EU-INDIA Smart Grid Platform Handbook**
  Funding: Far-Sighted Regulation Global Association
  Beginning - Finish Dates: September 2021 - January 2022
  Webpage: https://www.iit.comillas.edu/publicacion/informetecnico/en/279/Smart_grid_replication:_handbook_for_India

- **Digitalisation of electricity distribution networks in Spain**
  Funding: Fundación Naturgy
  Beginning - Finish Dates: November 2020 - April 2021
  Webpage: https://www.iit.comillas.edu/publicacion/informetecnico/en/257/La_digitalizaci%c3%b3n_de_las_redes_el%c3%a9ctricas_de_distribuci%c3%b3n_en_Espa%c3%b1a

- **Participation in the Smart Secondary Substation Working Group of FutuRed (Spanish platform of electricity networks)**
  Beginning - Finish Dates: 2020-2021

7.8 International research stay

To obtain the International Mention, the PhD candidate did a International Research Stay at TU Delft (Netherlands) for three months (15th April - 15th July 2023) in the Electrical Sustainable Energy Department under the supervision of Dr. Jose Luis Rueda Torres.

Appendix A

Relevant information for the ICT SRA of Case Study A

A.1 Modbus TCP

Modbus TCP is an application-layer communication protocol for client-server communications between devices that runs on the TCP/IP protocol stack over Ethernet. Modbus TCP defines a Protocol Data Unit (PDU) that contains two pieces of information: the function code and the payload (i.e. the information to be sent). Communications through Modbus follow the request-response mechanism; the client indicates to the server (i.e., request), through the function code, what kind of action must be done, and provides additional information in the data attached (e.g., amount of registers needed). Then, the server processes the client's request, performs the required action, and sends a response to the client. Figure A.1 shows a simplified diagram of Modbus transactions between client and server.

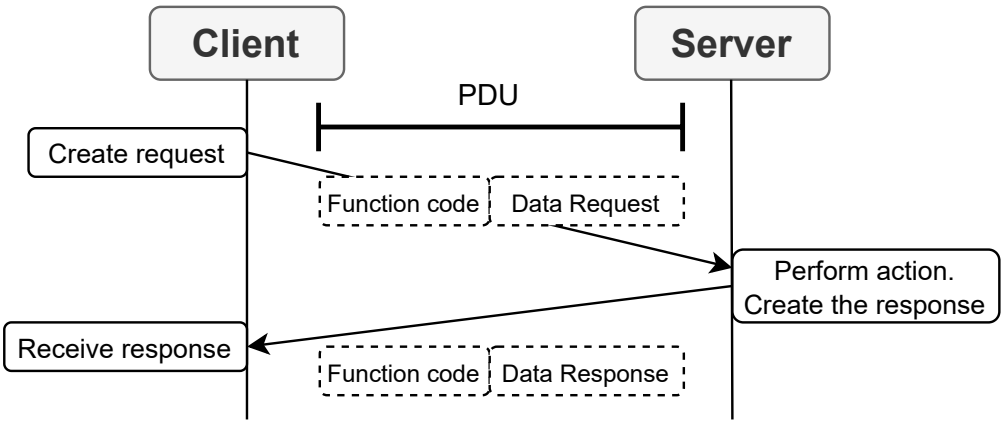

Figure A.1: Simplified Modbus transaction between client and server

Modbus defines up to 21 function codes. For each function code, the PDU of both the request and response are specified and must be ≤ 253 bytes. Table A.1 shows, as an example, the breakdown of the PDU for function code 03, "Read Holding Registers", which is one of the functions considered in the simulation model developed and used for the analysis in Chapter 4.

Table A.1: Request and Response PDU for Read Holding Registers function code

	Request	**Response**
Function code	1 Byte	1 Byte
Starting address	2 Bytes	1 Byte
Quantity of registers (N)	2 Bytes (max. 125 registers)	N x 2 Bytes

To transmit a message, a Modbus Application Protocol (MBAP) header (7 bytes) must be added to the PDU, forming the Application Data Unit (ADU). As Modbus runs over TCP/IP and Ethernet, which work at different communication layers, the final message transmitted through the Ethernet cable contains the information needed by each of the layers. Figure A.2 shows the different headers that constitute the dataframe for Modbus requests and responses.

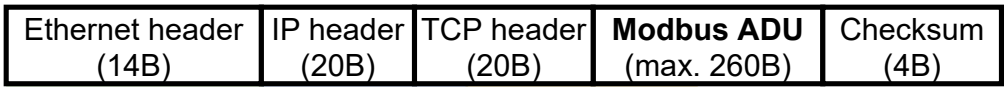

Figure A.2: Dataframe transmitted with Modbus TCP over Ethernet

A.2 Scalability analysis of baseline scenario

In this appendix, the simulation results to evaluate the performance of the Modbus TCP system when scaling up the baseline scenario considered in Chapter 4 are discussed in detail.

The distribution of the time it takes for the client to complete the polling of all servers (i.e., polling time) is shown in Figure A.3 for different values of BER and number of servers.

For BER=10^{-12}, the client can maintain an average polling time of 60s for all the servers considered. Although this is also true for BER =10^{-6}, the Interquartile Range (IQR) becomes noticeably larger when more than 32 servers are connected. One cause for this is because the higher the number of servers and BER, the less time the client has to poll each server and the more messages contain errors, requiring their retransmission. For BER=10^{-5}, the IQR does not only increase, but is also displaced over the required polling time of 60s when more than 132 servers are connected.

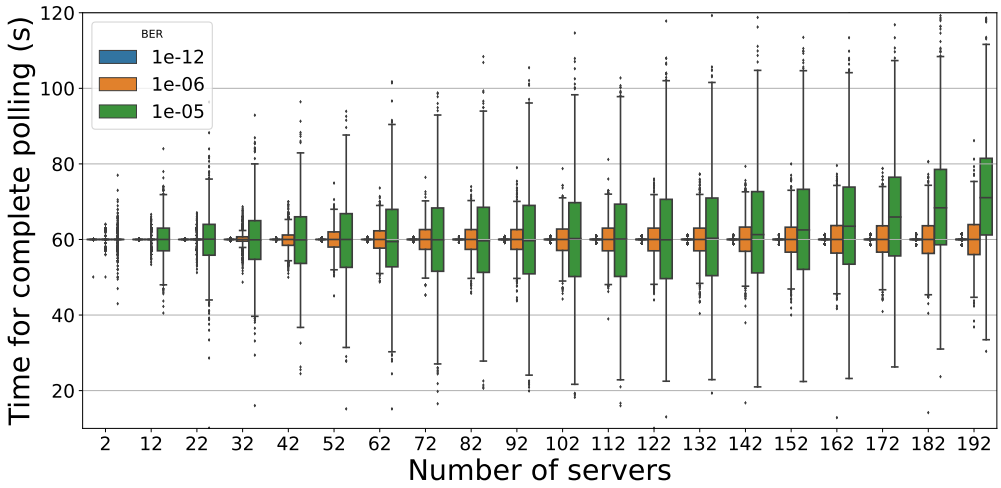

Figure A.3: Time to complete the polling to all the servers connected for different BER values and number of servers

As commented in Chapter 4, the client tries to keep the average polling time to one minute by compensating time deviations. Time deviations have two main causes: jitter, or variable delay, and BER. In Figure A.3 the influence of both factors on the polling time can be differentiated. For BER=10^{-12}, deviations with respect to the polling time will be mainly caused by jitter, as BER is so low that it rarely causes retransmission of messages. When increasing the number of servers, the number of messages per minute also increases, hence the added effect of jitter will be greater, which makes the outliers slightly more noticeable. On the other hand, for the other two BER considered (10^{-6} and 10^{-5}), the main cause for polling time deviation is the BER itself, that makes it necessary to resend erroneous messages.

The effect of compensating polling time deviations, when successful, would be translated into a symmetry with respect to an horizontal axis defined by the 60s mark in Figure A.3, so that the average is equal to that value. For BER=10^{-5}, asymmetry starts being noticeable for more than 112 servers. This means that the number of erroneous messages is so high that delays will not be fully compensated. Successive rounds would accumulate these delays, increasing the amount of data missed by the client.

To clearly determine the performance limits of the system based on specific statistics, Figure A.4 shows the SD of the polling time for the BER considered. In this figure, the impact of increasing BER can be appreciated.

For BER=10^{-5}, the SD of the polling time starts to stabilise coinciding with the beginning of the asymmetry in Figure A.3 (> 112 servers), reaching its peak for 142 servers. This peak means that the system has reached the performance limit; the client cannot poll all the servers in one minute on average, as it cannot compensate for time deviations. Above this number of

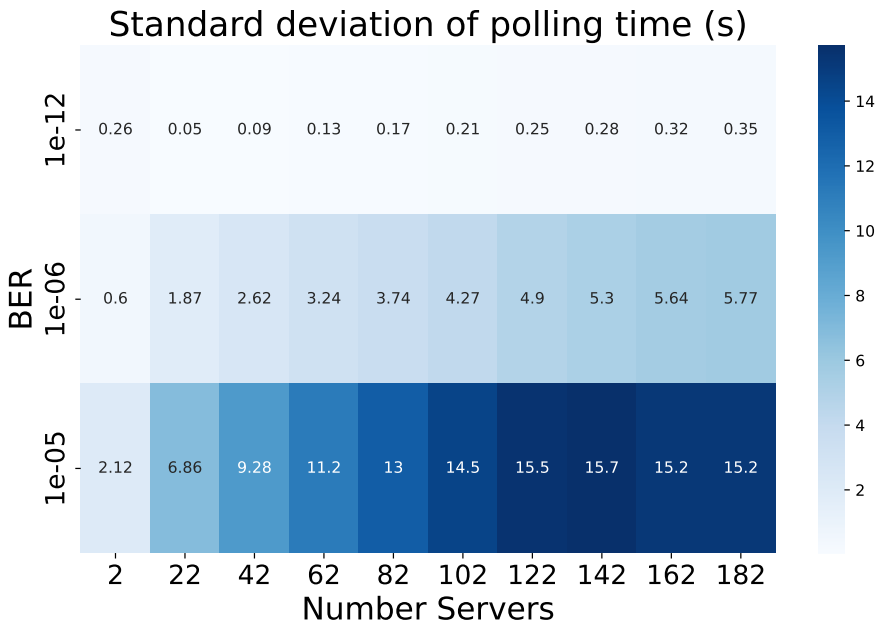

Figure A.4: Standard deviation of the total polling time for different BER and number of servers

servers, SD will be mainly influenced by the BER.

On the other hand, when the BER is lower (10^{-12} and 10^{-6}), the Modbus system does not reach its performance limit, as the SD of the polling time increases along with the number of servers. However, for BER=10^{-6}, Figure A.3 shows that the SD is beginning to stabilise, so the maximum number of servers that determines the performance limit of the system (peak of the SD) may be around 200 and 220.

However, the fact that, under some conditions, the system does not reach its limits and maintains an average polling time of one minute does not mean that its performance is acceptable for the use case under study. The maximum coefficient of variation (COV) allowed is considered to be 0.5% (maximum SD of 300ms). Considering this, when the BER of the transmission medium is 10^{-6} and 10^{-5}, the operation of the Modbus TCP system would not be appropriate for any number of servers. However, if the BER is low (10^{-12}), up to 142 servers could be operated by a single client within the same Modbus TCP network, in case they are 20m away from the client. For this BER, despite the COV for two servers (0.26s) is close to the maximum allowed, this is observed to be exclusively caused by polling times below 60s in Figure A.3; if these outliers below the 60s mark are not considered, the expected SD would be 0.005s.

Appendix B

Relevant information for the ICT SRA of Case Study B

B.1 Wireless M-Bus

The protocol stack for wireless M-Bus is shown by FigureB.1. Although layers 3-6 of the Open Systems Interconnection (OSI) model are not explicitly defined and implemented in wireless M-Bus, the EN 13757-3:2013 standard, which defines the application layer, also includes the definition of the transport layer to be applied under certain conditions [262].

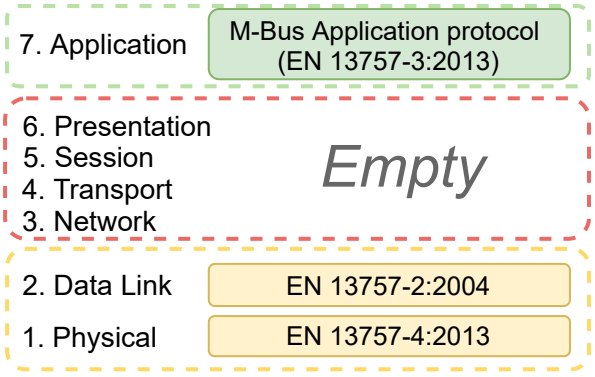

Figure B.1: Wireless M-Bus protocol stack

Networks implementing wireless M-Bus follow a star topology where one device collects data from multiple meters or sensors. The wireless M-Bus protocol has six different transfer modes, which are summarised by Table B.1. At the same time, some of these modes can be divided into submodes depending on whether the communications are unidirectional or bidirectional between sensors and data collectors.

The structure of a wireless M-Bus frame is shown by FigureB.2. It consists of a preamble

Table B.1: Summary of wireless M-Bus transfer modes

Mode	Frequency band (MHz)	Bit rate (kbps)	Brief description of use
S-Stationary	868	16,384	Data sent several times a day to a stationary/mobile concentrator.
T-Frequent Transmit	868	66,67	Data sent every few seconds to a walk-by or drive-by data collector
R-Frequent Receive	868	2,4	Each meter sends the data to the collector in a different frequency channel to avoid interferences
C-Compact	868	50 or 100	Similar to T, but it takes less energy to transmit the same information
N-Narrowband VHF	169	2,4; 4,8; 6,4; 19,2	For a long range, narrowband system
F-Frequent Receive and Transmit	433	2,4	Bidirectional communication with NRZ encoding

(header+sync) and a payload that depends on the format implemented, A or B, defined by EN 13757-4:2019. The main difference between formats is in the data field of the second and optional blocks. Format A can be used in any of the modes presented in Table B.1, whereas format B can only be optionally used in modes C, N, and F [263].

For the analysis conducted in Chapter 4, the wireless M-Bus network uses transfer mode S1 (i.e., unidirectional communications) and, therefore, format A for the messages.

According to EN 13757-4:2019 specification, the modulation used by the wireless M-Bus protocol in transfer mode S is Frequency Shift Keying (FSK) modulation. To consider the BER in the simulation model, a lookup table is generated using the SNR-BER relation shown by (B.1), which is provided by [264], where the SNR is expected in linear units.

$$BER = \frac{1}{2} e^{\frac{-SNR}{2}} \tag{B.1}$$

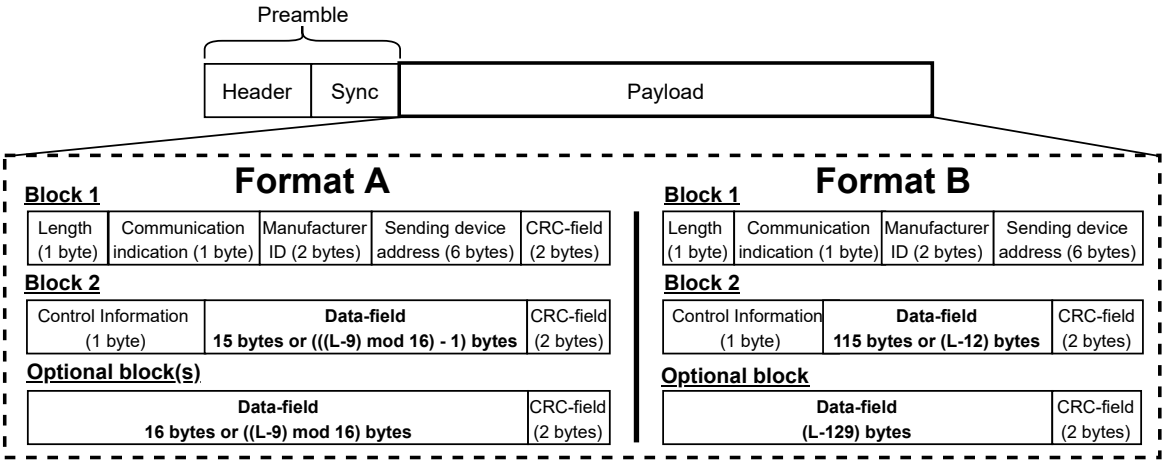

Figure B.2: Wireless M-Bus frame formats A and B

B.2 Transmission medium model

To simulate the impact that obstacles (i.e., building's walls and floors) have on the wireless M-Bus network performance studied in 4.4.2, three models from the INET framework [169] are used: path loss model, obstacle loss model, and background noise model.

The path loss model allows to use an algorithm that simulates the power decrease of the signal as it propagates through the medium. Ideally, an empirical propagation model of the demonstration site would be the best approach to evaluate the performance of wireless communications, since it would capture most of the effects that have an impact on the signal [265].

The obstacle loss model provides algorithms to simulate the power decrease when the signal is reflected by obstacles' surfaces and when it is absorbed.

The background noise model describes how the noise affecting the communication channel may change over space and time.

For the **path loss**, the free-space path loss model (FSPL) is used (B.2).

$$FSPL = \left(\frac{4\pi d}{\lambda}\right)^2 \tag{B.2}$$

Where d is the distance between antennas and λ is the wavelength of the signal.

As its name points out, the FSPL model considers the line-of-sight path through free space, without any obstacles. In order to characterise the dielectric and reflection losses not modelled by the FSPL model, the dielectric obstacle loss model from INET is used. This model considers the orientation, material, shape, and position of obstacles in the path to compute the dielectric and reflection losses of the signal.

Without entering into the geometric details involved in the calculation, the **dielectric losses** factor caused by an obstacle is given by (B.3).

$$P_z[W] = P_0[W] \cdot e^{\frac{-4\delta\pi z}{\lambda}} \tag{B.3}$$

Where P_z is the final power of the signal at distance z, P_0 is the initial power, and δ is the loss angle.

Regarding the losses due to the **reflection** of the signal on obstacles, the model uses the Fresnel equations, assuming that the signal is unpolarized. The effective transmission of the signal (T_{eff}) can be calculated as shown by (B.4).

$$T_{eff} = 1 - R_{eff} = 1 - \frac{1}{2} \cdot (R_s + R_p) \tag{B.4}$$

Where R_{eff} is the effective reflectivity and R_s and R_p are the power reflection coefficient for S-polarized (B.5) and P-polarized (B.6) light, respectively.

$$R_s = \left| \frac{n_1 cos(\theta_i) - n_2 k}{n_1 cos(\theta_i) + n_2 k} \right|^2 \tag{B.5}$$

$$R_p = \left| \frac{n_1 k - n_2 cos(\theta_i)}{n_1 k + n_2 cos(\theta_i)} \right|^2 \tag{B.6}$$

In (B.5) and (B.6), n_1 and n_2 are the refractive indices of medium 1 (i.e., the air) and 2 (i.e., concrete), respectively; θ_i is the angle of incidence, and k (cosine of the angle of the refracted rays with respect to the normal) is given by (B.7).

$$k = \sqrt{1 - \left(\frac{n_1}{n_2} \cdot sin(\theta_i) \right)^2} \tag{B.7}$$

Therefore, the power of the signal received (P_{Rx}) is calculated by applying to the initial power of transmission (P_{Tx}) the gains of the transmitter and receiver antennas (G_{Tx} and G_{Rx}, respectively), the FSPL factor, the dielectric losses, and the effective transmission of the signal due to reflection on obstacles (T_{eff}) in linear units:

$$P_{Rx} = P_{Tx} \cdot G_{Tx} \cdot G_{Rx} \cdot FSPL \cdot e^{\frac{-4\delta\pi z}{\lambda}} \cdot T_{eff} \tag{B.8}$$

Finally, to consider the impact of **background noise**, on performance, the Isotropic Dimensional Background Noise model from INET is used. This model considers that noise does not change over space, time, and frequency. It is assumed that the baseline background noise will be $10^{-12}W$ (-90dBm). The relation between background noise (N_B), the signal-to-noise ratio (SNR) in linear units, and P_{Rx} is expressed by (B.9)

$$SNR = \frac{P_{Rx}}{N_B} \tag{B.9}$$

B.3 Comparison of impact of propagation models

In this appendix section, the performance of the wireless M-Bus system is analysed and compared when using three different propagation models: log-normal path-loss model, ITU-R P.1238 indoor model [266], and free-space model complemented with dielectric and reflection losses due to obstacles.

B.3.1 Propagation models

Apart from the free-space model with dielectric and reflection losses that was described in B.2, two different propagation models are considered: log-normal path loss model and ITU-R P.1238 indoor model.

Log-normal path loss model

The path losses in this model are given by Eq.B.10.

$$PL(d)[dB] = PL(d_0)[dB] + 10nlog\left(\frac{d}{d_0}\right) + X_\sigma \tag{B.10}$$

Where $PL(d_0)$ is the path loss at a reference distance, d_0; n is the loss rate, which depends on the environment; d is the distance between transmitter and receiver; and X_σ is a zero-mean Gaussian distributed variable with standard deviation σ (in dB).

ITU-R P.1238 Indoor Model

The path losses in this model are given by Eq.B.11 [266].

$$PL(d)[dB] = PL(d_0)[dB] + 10nlog\left(\frac{d}{d_0}\right) + L_f(n_f) \tag{B.11}$$

Where, for $d_0 = 1m$, $PL(d_0)[dB] = 20log(f) - 28$ with frequency, f, in MHz; and $L_f(n_f)$ is the floor penetration loss factor in dB that depends on the number of floors, n_f, between transmitter and receiver.

According to [266], n can increase to around 4 for a typical indoor environment where the signal encounters obstacles and walls. For $f = 0.9GHz$ in a residential environment, $L_f(n_f)$ takes the values of 9, 19, and 24dB when n_f is 1, 2 and 3 floors, respectively.

B.3.2 Scenarios and settings for the comparative analysis of propagation models

To carry out the comparison of propagation models, these have been configured based on the settings used by the literature in similar contexts.

Table B.2 shows the values for the configuration of the path loss models studied. Two variations for the log-normal model are considered. Log-normal #1 is taken from [267], which studies the performance of wireless M-Bus in a common indoor environment in residential buildings; on the other hand, log-normal #2 takes its values from [268], where an indoor-to-street scenario is considered. Regarding the ITU-R P.1238, the path loss exponent, n, can take values between 2 (commercial environment) and 3.3 (office environment) for a 900 MHz signal [269], and up to 4 in certain cases [266]. Here, $n = 3$ is taken, based on path loss exponents in [268], [270].

Table B.2: Configurations of the log-normal and ITU-R P.1238 models considered for comparison.

Model	**d0**	**n**	σ	**Ref.**
Log-Normal #1	1m	2.97	3dB	[267]
Log-Normal #2	1m	3	7dB	[268]
ITU-R P.1238	1m	3	-	[266], [268], [270]

Regarding simulated scenarios, Table B.3 summarises the characteristics of the scenarios studied and Figure B.3 shows a top view of the area considered for each scenario. Scenario #1 is the baseline scenario (same as in section 4.4.2): one cluster of buildings with 96 sensors deployed and the data collector placed at the center of the cluster. Scenario #2 represents the scalability scenario, where up to 384 sensors are distributed among four clusters of buildings, with the data collector placed at the center of the area of the four clusters.

Table B.3: Analysed scenarios.

Scenario	**No. of clusters**	**Floors per building**	**Data collector's location**
#1	1	3	Center of one cluster
#2	4	3	Center of four clusters

B.3.3 Simulation results

In this section of Appendix B, the simulation results showing the performance of the wireless M-Bus system under the assumption of the different propagation models are presented and discussed.

Figure B.4 and Figure B.5 (scenario #1 -baseline- and #2 -scalability-, respectively) show two plots each. The bottom plot shows the SNR got by the data collector for each sensor that successfully sends a message. For each propagation model, this is plotted over the theoretical

Figure B.3: Top view of the scenarios considered.

curve corresponding to the SNR-BER relation of FSK modulation, which is the one used by wireless M-Bus in transfer mode S [264]. For visual simplification, of the two log-normal models considered, only the log-normal #1 is shown. On the other hand, the top plot in the figures shows the number of sensors sending messages within each SNR range.

Figure B.4 shows that, except for the ITU-R P.1238 model, the propagation models considered present an SNR higher than 17.5 dB for this scenario, which requires a very low BER and a high probability of receiving all the messages correctly. Thus, there are practically no red and black points in the figure. On the other hand, when using the ITU-R P.1238 model, the SNR range is approximately between 10 and 20 dB, with a strong concentration in the 10-15 dB range. Despite the BER being significantly higher when using ITU-R P.1238, the data collector managed to receive all the information from the 96 sensors in the cluster for this case. Therefore, in the baseline scenario, all the propagation models studied provide acceptable performance results. These results contrast significantly with those in scenario #2.

Figure B.5 shows the BER-SNR curve of the models when scaling up the system (scenario #2). With respect to scenario #1, the BER-SNR of log-normal #1 now has values in the SNR range plotted, although it is observed that most of the sensors would have an SNR higher than 15 dB.

Figure B.6 plots the KPIs for the different propagation models analysed in scenario #2. Starting with the delivery ratio, when any of the log-normal models is applied to the propagation medium, it can be observed that the data collector manages to get all the necessary measures from all the sensors (delivery ratio $\approx$ 1). The FSPL+obstacles and the ITU-R P.1238 models, on the other hand, provide a delivery ratio below 0.8, which would not be acceptable in a real implementation, as the data collector would miss more than 20% of the

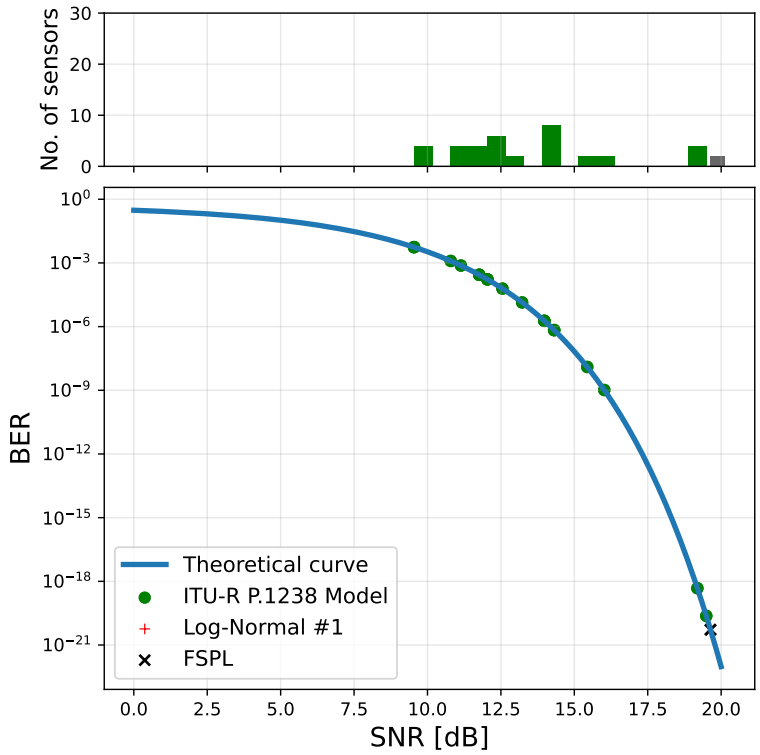

Figure B.4: BER-SNR for the propagation models studied. Scenario #1

information sent by the sensors, which is represented by the message error ratio plot in Figure B.6. In addition to this, in all likelihood the missing sensors would always be the same ones: those presenting a low SNR and, therefore, high BER in Figure B.5.

In the message error ratio plot in Figure B.6 it can also be appreciated the effect of increasing the standard deviation of the Gaussian distribution in the log-normal models. Log-normal #2, which has a $\sigma = 7dB$, presents a message error ratio ≈ 0.1, whereas log-normal #1 ($\sigma = 3dB$) presents a close-to-null error ratio.

Regarding the gross delivery ratio, Figure B.6 shows that it decreases when increasing the number of sensors deployed, regardless of the propagation model used. This is because the message collision probability, which is related to this ratio, does not depend on the propagation model, just on the number of sensors. It must be highlighted that, despite collision probability increases with the number of sensors deployed, it is observed that it does not have an impact on the delivery ratio for any of the models analysed. This means that the main cause for the data collector not being able to collect the information from all the sensors would be the reception of messages with errors and not a large number of sensors. Therefore, the scalability analysis of the system is significantly influenced by the propagation model defined for the simulation. If the model cannot be adjusted empirically, a good approach would be to use the FSPL model with obstacle-related losses when the obstacles can be modelled in an

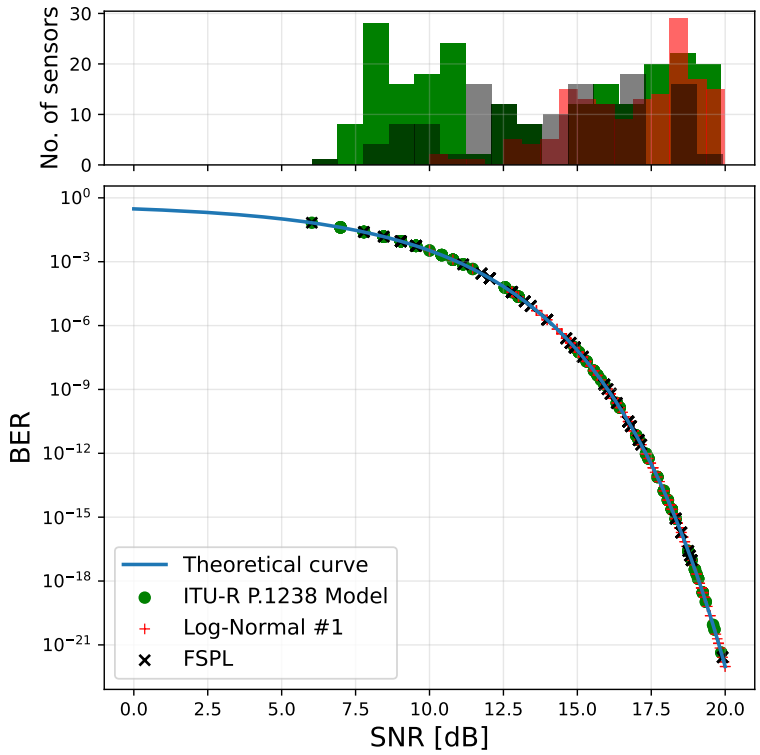

Figure B.5: BER-SNR for the propagation models studied. Scenario #2

acceptable way, hedging the risk of getting too optimistic scalability results. Therefore, this is the approach selected for the analysis in section 4.4.2. If obstacles cannot be fairly modelled, for an indoor environment it is observed that the ITU-R P.1238 model would constitute an even more conservative approach for the analysis, as results in [271] also point out.

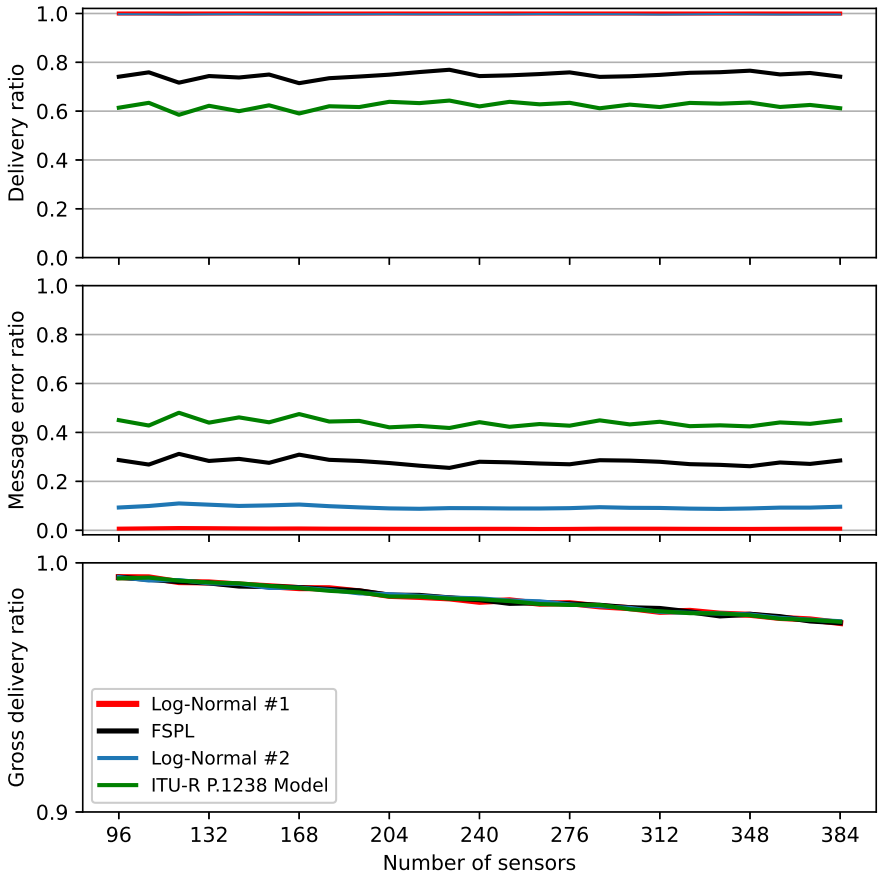

Figure B.6: Delivery ratio, message error ratio, and gross delivery ratio depending on the number of sensors, using different propagation models. Scenario #2

Appendix C

Distributed Generation in the PST-16 System

The penetration of solar PV per voltage level in Spain on March 2023 is shown by Table C.1 [202]. For the study, only the solar PV connected to <145kV is considered (i.e., distributed solar PV).

Table C.1: Installed capacity of Solar PV generation in Spain per voltage level. Date: March 2023. Source: [202]

Voltage (kV)	**Solar PV Generation (GW)**	**% of solar PV**
$0 \leq V < 1$	1.67	9.56%
$1 \leq V < 36$	2.92	16.72%
$145 \leq V \leq 400$	10.27	58.8%
$36 \leq V < 72.5$	1.31	7.50%
$72.5 \leq V < 145$	1.29	7.41%

By considering the current electricity generation capacity of Spain, and the generation that is pending its start-up, but that has the permission to connect to the system [203], the percentage of solar PV connected to <145kV over the total generation capacity can be estimated for both the years 2023 and 2030, when it is assumed that all this expected generation will be already connected. Table C.2 shows this estimation for the years 2023 and 2030 in Spain.

5.96% and 9.79% of distributed solar PV penetration equals to 365 MW and 599 MW of the total generation capacity in area C of the PST-16 system model. Since only the load buses which do not have bulk generation connected are considered for the deployment of

Table C.2: Estimated solar PV generation connected to <145kV for the years 2023 and 2030 in Spain. Source: Own elaboration based on public data from [202] and [203].

Scenario	**Solar PV<145kV**		**Total Generation Power (GW)**
	(GW)	**(%)**	
2023	7.191	5.96	120.64
2030	24.65	9.79	251.904

distributed solar PV (see Figure 5.7), the total amount of demand to which distributed solar PV would be connected is 5.46 GW. Therefore, with these values in mind, the percentage of this demand that could be supplied by distributed solar PV would be 6.68% and 10.97% for 2023 and 2030, respectively. These values are rounded down to 5 and 10%. For the analysis presented in Chapter 5 (section 5.5), only the 2030 scenario is considered, with 10% of demand supplied by distributed solar PV.

Table C.3 shows the distributed solar PV that would be connected to each load bus for the years 2023 and 2030.

Table C.3: Distributed solar PV generation per bus of area C (PST-16) for THE years 2023 and 2030

Bus	**2023 (5%)**	**2030 (10%)**
C1	30 MW	60MW
C3	30 MW	60MW
C4	25 MW	50MW
C5a	3 MW	6MW
C6	25 MW	50MW
C6a	30 MW	60MW
C8a	25 MW	50MW
C9	25 MW	50MW
C11	20 MW	40MW
C13	30 MW	60MW
C14a	2 MW	4MW
C15	25 MW	50MW
C16	1 MW	2MW
C17	0.5 MW	1MW
C18	1 MW	2MW
C19	0.75 MW	1.5MW

Appendix D

TSO-DSO Coordination Schemes

Table D.1 provides the equivalence of the nomenclature used among EU H2020 projects and ASM when referring to market-based coordination schemes between TSOs and DSOs.

Table D.1: Coordination schemes comparison among EU H2020 projects and [219]. Based on [222], [272]

ASM [219]	**SmartNet**	**CoordiNet**	**INTERRFACE**
Option 1	-Local ancillary services market model -Shared balancing responsibility model	-Multi-level -Fragmented -Central -Local	-1A -1B -1C
Option 2	-Common TSO-DSO ancillary services market model	- Common -Integrated	-2A -2B
Option 3	-Centralised ancillary services market model -Local ancillary services market model	-Local -Distributed -Central	-3A -3B -3C -3D
Out of scope	-Local ancillary services market model -Integrated flexibility market model	-Multi-level -Fragmented -Central -Local	

Bibliography

[1] A. Sendin, M. A. Sanchez-Fornie, I. Berganza, J. Simon, and I. Urrutia, *Telecommunication networks for the smart grid*. Artech House, 2016.

[2] European Commission, "Digitalising the energy system - EU action plan," en, European Commission, Strasbourg, Tech. Rep., Oct. 2022, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0552&from=EN (visited on Jan. 12, 2023).

[3] FutuRed, *8 Cifras clave de la redes eléctricas en España*, Spanish, 2023, [Online]. Available: https://www.futured.es/las-redes-electricas-espana/ (visited on Jan. 9, 2024).

[4] E. Union, *EU Directive 2019/944*, en, Code Number: 158, Jun. 2019, [Online]. Available: http://data.europa.eu/eli/dir/2019/944/oj/eng.

[5] L. Sigrist, K. May, A. Morch, P. Verboven, P. Vingerhoets, and L. Rouco, "On Scalability and Replicability of Smart Grid Projects—A Case Study," en, *Energies*, vol. 9, no. 3, p. 195, Mar. 2016, ISSN: 1996-1073, DOI: 10.3390/en9030195.

[6] A. Rodríguez Calvo, "Scalability and replicability of the impact of smart grid solutions in distribution systems," PhD Thesis, Comillas Pontifical University, Madrid, Spain, 2017.

[7] S. Ma, H. Zhang, and X. Xing, "Scalability for Smart Infrastructure System in Smart Grid: A Survey," en, *Wireless Personal Communications*, vol. 99, no. 1, pp. 161–184, Mar. 2018, ISSN: 0929-6212, 1572-834X, DOI: 10.1007/s11277-017-5045-y.

[8] B. Singer, A. Pandey, S. Li, L. Bauer, C. Miller, L. Pileggi, and V. Sekar, "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 38–55, DOI: 10.1109/SP46215.2023.10179343.

[9] F. Capitanescu, "Are we prepared against blackouts during the energy transition?: Probabilistic risk-based decision making encompassing jointly security and resilience," *IEEE Power and Energy Magazine*, vol. 21, no. 3, pp. 77–86, 2023, DOI: 10.1109/MPE.2023.3247053.

[10] L. Lind, R. Cossent, J. P. Chaves-Ávila, and T. Gómez San Román, "Transmission and distribution coordination in power systems with high shares of distributed energy resources providing balancing and congestion management services," en, *Wiley Interdisciplinary Reviews: Energy and Environment*, vol. 8, no. 6, Nov. 2019, ISSN: 2041-8396, 2041-840X, DOI: 10.1002/wene.357.

[11] K. Vu and K. Hartley, "Effects of digital transformation on electricity sector growth and productivity: A study of thirteen industrialized economies," *Utilities Policy*, vol. 74, p. 101 326, 2022, ISSN: 0957-1787, DOI: https://doi.org/10.1016/j.jup.2021.101326.

[12] A. Amores, L. Álvarez, O. Álvarez, J. Chico, A. Longueira, H. Sánchez, M. Sánchez, A. Díaz, and I. Azabal, "Hacia la descarbonización de la economía: La contribución de las redes eléctricas a la transición energética," Monitor Deloitte, Tech. Rep., 2018.

[13] S. R. S, T. Dragičević, P. Siano, and S. S. Prabaharan, "Future generation 5g wireless networks for smart grid: A comprehensive review," *Energies*, vol. 12, no. 11, 2019, ISSN: 1996-1073, DOI: 10.3390/en12112140.

[14] N. M. Kumar, A. A. Chand, M. Malvoni, K. A. Prasad, K. A. Mamun, F. Islam, and S. S. Chopra, "Distributed energy resources and the application of ai, iot, and blockchain in smart grids," *Energies*, vol. 13, no. 21, 2020, ISSN: 1996-1073, DOI: 10.3390/en13215739.

[15] A. De Paola, N. Andreadou, and E. Kotsakis, "Clean Energy Technology Observatory: Smart Grids in the European Union - 2023 Status Report on Technology Development Trends, Value Chains and Markets," *Publications Office of the European Union, Luxembourg*, 2023, ISSN: 1831-9424, DOI: 10.2760/237911.

[16] C. Athanasiadis, T. Papadopoulos, G. Kryonidis, and D. Doukas, "A review of distribution network applications based on smart meter data analytics," *Renewable and Sustainable Energy Reviews*, vol. 191, p. 114 151, 2024, ISSN: 1364-0321, DOI: https://doi.org/10.1016/j.rser.2023.114151.

[17] L. Suárez-Ramón, P. Arboleya, J. Lorenzo-Álvarez, and J. M. Carou-Álvarez, "Evolution of electrical distribution grids toward the smart grid concept," in *Technologies for Integrated Energy Systems and Networks*. John Wiley & Sons, Ltd, 2022, ch. 8, pp. 187–214, ISBN: 9783527833634, DOI: https://doi.org/10.1002/9783527833634.ch8.

[18] M. R. Shadi, M.-T. Ameli, and S. Azad, "A real-time hierarchical framework for fault detection, classification, and location in power systems using pmus data and deep learning," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107 399, 2022, ISSN: 0142-0615, DOI: https://doi.org/10.1016/j.ijepes.2021.107399.

[19] M. A. A. Sufyan, M. Zuhaib, M. A. Anees, A. Khair, and M. Rihan, "Implementation of pmu-based distributed wide area monitoring in smart grid," *IEEE Access*, vol. 9, pp. 140 768–140 778, 2021, DOI: 10.1109/ACCESS.2021.3119583.

[20] E. A. d. Leyva Merida, "Analysis of the impact of digitalisation in the electricity distribution sector in Spain," es-ES, M.S. thesis, Comillas Pontifical University, 2020.

[21] C. E. de la Energía (ENERCLUB), "Digitalización en el sector energético español," Tech. Rep., 2020.

[22] M. Temelkova, "Skills for digital leadership-prerequisite for developing high-tech economy," *International Journal of Advanced Research in Management and Social Sciences*, vol. 7, no. 12, pp. 50–74, 2018.

[23] P. Farahani, C. Meier, and J. Wilke, "Digital supply chain management agenda for the automotive supplier industry," *Shaping the digital enterprise: Trends and use cases in digital innovation and transformation*, pp. 157–172, 2017.

[24] R. Strack, S. Dyrchs, Á. Kotsis, and S. Mingardon, *How to Gain and Develop Digital Talent and Skills*, en, 2017, [Online]. Available: https://www.bcg.com/publications/2017/people-organization-technology-how-gain-develop-digital-talent-skills (visited on Dec. 26, 2023).

[25] I. Vokony, I. Taczi, and M. Szalmane Csete, "Agile digitalization evolution in the energy sector, taking into account innovative and disruptive technologies," *Renew. Energy Power Qual. J*, vol. 20, pp. 584–589, 2022.

[26] S. Snow, J. Happa, N. Horrocks, and M. Glencross, "Using design thinking to understand cyber attack surfaces of future smart grids," *Frontiers in Energy Research*, vol. 8, 2020, ISSN: 2296-598X, DOI: 10.3389/fenrg.2020.591999.

[27] M. Attaran, S. Attaran, and D. Kirkland, "The need for digital workplace: Increasing workforce productivity in the information age," *International Journal of Enterprise Information Systems (IJEIS)*, vol. 15, no. 1, pp. 1–23, 2019.

[28] A. Haddud and D. McAllen, "Digital workplace management: Exploring aspects related to culture, innovation, and leadership," in *2018 portland international conference on management of engineering and technology (PICMET)*, IEEE, 2018, pp. 1–6.

[29] R. Peña-Casas and D. Ghailani, "The impact of digitalisation on job quality in the electricity, hospital and public administrations sectors in eight EU countries," DIGIQU@LPUB, European Social Observatory, Deliverable D3.2, Sep. 2023, [Online]. Available: https://www.ose.be/digiqualpub/files/deliverables/2023_digiqualpub_Deliverable3.2_Digitalisation&JobQuality.pdf.

[30] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 1675–1684, 2018.

[31] J. Rodríguez-Molina, M. Martínez-Núñez, J.-F. Martínez, and W. Pérez-Aguiar, "Business models in the smart grid: Challenges, opportunities and proposals for prosumer profitability," *Energies*, vol. 7, no. 9, pp. 6142–6171, 2014, ISSN: 1996-1073, DOI: 10.3390/en7096142.

[32] R. Moura and M. C. Brito, "Prosumer aggregation policies, country experience and business models," *Energy Policy*, vol. 132, pp. 820–830, 2019.

[33] E. Ropuszynska-Surma and M. Weglarz, "The virtual power plant–a review of business models," in *E3S web of conferences*, EDP Sciences, vol. 108, 2019, p. 01 006.

[34] N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu, X. Du, and M. Guizani, "When energy trading meets blockchain in electrical power system: The state of the art," *Applied Sciences*, vol. 9, no. 8, 2019, ISSN: 2076-3417, DOI: 10.3390/app9081561.

[35] S. Dutta, S. K. Sahu, M. Roy, and S. Dutta, "A data driven fault detection approach with an ensemble classifier based smart meter in modern distribution system," *Sustainable Energy, Grids and Networks*, vol. 34, p. 101 012, 2023.

[36] E. U. Haq, C. Pei, R. Zhang, H. Jianjun, and F. Ahmad, "Electricity-theft detection for smart grid security using smart meter data: A deep-cnn based approach," *Energy Reports*, vol. 9, pp. 634–643, 2023, 2022 9th International Conference on Power and Energy Systems Engineering, ISSN: 2352-4847, DOI: https://doi.org/10.1016/j.egyr.2022.11.072.

[37] W. J. Lee, H. Wu, H. Yun, H. Kim, M. B. Jun, and J. W. Sutherland, "Predictive maintenance of machine tool systems using artificial intelligence techniques applied to machine condition data," *Procedia Cirp*, vol. 80, pp. 506–511, 2019.

[38] S. Selcuk, "Predictive maintenance, its implementation and latest trends," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, vol. 231, no. 9, pp. 1670–1679, 2017.

[39] M. Compare, P. Baraldi, and E. Zio, "Challenges to iot-enabled predictive maintenance for industry 4.0," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4585–4597, 2020, DOI: 10.1109/JIOT.2019.2957029.

[40] M. Moleda, B. Malysiak-Mrozek, W. Ding, V. Sunderam, and D. Mrozek, "From corrective to predictive maintenance-a review of maintenance approaches for the power industry," *Sensors*, vol. 23, no. 13, 2023, ISSN: 1424-8220, DOI: 10.3390/s23135970.

[41] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr, V. Y. Pillitteri, T. L. Brewer, N. T. Golmie, D. H. Su, A. C. Eustis, D. G. Holmberg, and S. T. Bushby, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," en, National Institute of Standards and Technology, Tech. Rep. NIST SP 1108r3, Oct. 2014, NIST SP 1108r3, DOI: 10.6028/NIST.SP.1108r3.

[42] D. Acarali, M. Rajarajan, D. Chema, and M. Ginzburg, "Modelling dos attacks and interoperability in the smart grid," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, 2020, pp. 1–6, DOI: 10.1109/ICCCN49398.2020.9209671.

[43] V. S. Rajkumar, A. Ştefanov, A. Presekal, P. Palensky, and J. L. R. Torres, "Cyber attacks on power grids: Causes and propagation of cascading failures," *IEEE Access*, vol. 11, pp. 103 154–103 176, 2023, DOI: 10.1109/ACCESS.2023.3317695.

[44] M. Jafari, A. Kavousi-Fard, T. Chen, and M. Karimi, "A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future," *IEEE Access*, vol. 11, pp. 17 471–17 484, 2023, DOI: 10.1109/ACCESS.2023.3241588.

[45] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in *Transdisciplinary perspectives on complex systems*, Springer, 2017, pp. 85–113.

[46] J. P. Chaves, R. Cossent, T. Gómez, G. López, J. Matanza, C. Mateo, N. Rodríguez, and M. Á. Sánchez, *Digitalisation of electricity distribution networks in Spain*, Spanish, Sep. 2021, [Online]. Available: https://www.fundacionnaturgy.org/publicacion/la-digitalizacion-de-las-redes-electricas-de-distribucion-en-espana/.

[47] T. Cioara, I. Anghel, M. Antal, I. Salomie, C. Antal, and A. G. Ioan, "An overview of digital twins application domains in smart energy grid," *arXiv preprint arXiv:2104.07904*, 2021.

[48] G. Zhang, C. Huo, L. Zheng, and X. Li, "An Architecture Based on Digital Twins for Smart Power Distribution System," in *2020 3rd International Conference on Artificial Intelligence and Big Data (ICAIBD)*, May 2020, pp. 29–33, DOI: 10.1109/ICAIBD49809.2020.9137461.

[49] R. van Dinter, B. Tekinerdogan, and C. Catal, "Predictive maintenance using digital twins: A systematic literature review," *Information and Software Technology*, vol. 151, p. 107 008, 2022, ISSN: 0950-5849, DOI: https://doi.org/10.1016/j.infsof.2022.107008.

[50] T. Liu, H. Yu, H. Yin, Z. Zhang, Z. Sui, D. Zhu, L. Gao, and Z. Li, "Research and Application of Digital Twin Technology in Power Grid Development Business," in *2021 6th Asia Conference on Power and Electrical Engineering (ACPEE)*, Apr. 2021, pp. 383–387, DOI: 10.1109/ACPEE51499.2021.9436946.

[51] T. Mariprasath and V. Kirubakaran, "A real time study on condition monitoring of distribution transformer using thermal imager," *Infrared Physics and Technology*, vol. 90, pp. 78–86, 2018, ISSN: 1350-4495, DOI: https://doi.org/10.1016/j.infrared.2018.02.009.

[52] H. Wang, Y. Zhong, B. Chen, Z. Zhuang, and L. Chen, "Application of satellite technology in smart grid," in *2022 International Seminar on Computer Science and Engineering Technology (SCSET)*, 2022, pp. 164–167, DOI: 10.1109/SCSET55041.2022.00047.

[53] J. Toth and A. Gilpin-Jackson, "Smart view for a smart grid — Unmanned Aerial Vehicles for transmission lines," in *2010 1st International Conference on Applied Robotics for the Power Industry*, Oct. 2010, pp. 1–6, DOI: 10.1109/CARPI.2010.5624465.

[54] M. Y. Sermet, I. Demir, and S. Kucuksari, "Overhead power line sag monitoring through augmented reality," in *2018 North American Power Symposium (NAPS)*, 2018, pp. 1–5, DOI: 10.1109/NAPS.2018.8600565.

[55] D. V. João, P. Z. Lodetti, M. A. I. Martins, and J. F. B. Almeida, "Virtual and Augmented Reality Applied in Power Electric Utilities for Human Interface Improvement – A Study Case for Best Practices," in *2020 IEEE Technology Engineering Management Conference (TEMSCON)*, Jun. 2020, pp. 1–4, DOI: 10.1109/TEMSCON47658.2020.9140129.

[56] R. Duncan, "A multi-cloud world requires a multi-cloud security approach," *Computer Fraud & Security*, vol. 2020, no. 5, pp. 11–12, 2020.

[57] M. Lane, A. Shrestha, and O. Ali, "Managing the risks of data security and privacy in the cloud: A shared responsibility between the cloud service provider and the client organisation," *Bright Internet Global Summit 2017*, 2017.

[58] D. Syed, A. Zainab, A. Ghrayeb, S. S. Refaat, H. Abu-Rub, and O. Bouhali, "Smart grid big data analytics: Survey of technologies, techniques, and applications," *IEEE Access*, vol. 9, pp. 59 564–59 585, 2021, DOI: 10.1109/ACCESS.2020.3041178.

[59] C. Jinming, J. Wei, J. Hao, G. Yajuan, N. Guoji, and C. Wu, "Application prospect of edge computing in smart distribution," in *2018 China International Conference on Electricity Distribution (CICED)*, 2018, pp. 1370–1375, DOI: 10.1109/CICED.2018.8592104.

[60] N. R. Pérez, M. A. Sanz-Bobi, and A. S. Paniagua, "Analysis of an edge-computing-based solution for local data processing at secondary substations," in *2021 IEEE Madrid PowerTech*, 2021, pp. 1–6, DOI: 10.1109/PowerTech46648.2021.9494971.

[61] X.-S. Zhou, J.-W. Mi, Y.-J. Ma, and Z.-Q. Gao, "Cloud Computing Technology in Smart Grid," *DEStech Transactions on Engineering and Technology Research*, no. icmeca, Jul. 2017, ISSN: 2475-885X, DOI: 10.12783/dtetr/icmeca2017/11958.

[62] S. Yang, B. Vaagensmith, and D. Patra, "Power Grid Contingency Analysis with Machine Learning: A Brief Survey and Prospects," in *2020 Resilience Week (RWS)*, Oct. 2020, pp. 119–125, DOI: 10.1109/RWS50334.2020.9241293.

[63] F. Schäfer, J.-H. Menke, and M. Braun, "Evaluating machine learning models for the fast identification of contingency cases," en, *Applied AI Letters*, vol. 1, no. 2, e19, 2020, ISSN: 2689-5595, DOI: 10.1002/ail2.19.

[64] M. Abbasi, S. Khorasanian, and M. H. Yaghmaee, "Low-Power Wide Area Network (LPWAN) for Smart grid: An in-depth study on LoRaWAN," in *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*, Feb. 2019, pp. 022–029, DOI: 10.1109/KBEI.2019.8735089.

[65] M. Nour, J. P. Chaves-Ávila, and Á. Sánchez-Miralles, "Review of blockchain potential applications in the electricity sector and challenges for large scale adoption," *IEEE Access*, vol. 10, pp. 47 384–47 418, 2022, DOI: 10.1109/ACCESS.2022.3171227.

[66] S. Cantillo-Luna, R. Moreno-Chuquen, H. R. Chamorro, V. K. Sood, S. Badsha, and C. Konstantinou, "Blockchain for distributed energy resources management and integration," *IEEE Access*, vol. 10, pp. 68 598–68 617, 2022, DOI: 10.1109/ACCESS.2022.3184704.

[67] X. Zhang and M. Fan, "Blockchain-based secure equipment diagnosis mechanism of smart grid," *IEEE Access*, vol. 6, pp. 66 165–66 177, 2018, DOI: 10.1109/ACCESS.2018.2856807.

[68] J. Rossi, A. Srivastava, D. Steen, and L. A. Tuan, "Study of the european regulatory framework for smart grid solutions in future distribution systems," in *CIRED 2020 Berlin Workshop (CIRED 2020)*, vol. 2020, 2020, pp. 800–802, DOI: 10.1049/oap-cired.2021.0230.

[69] M. Correa, T. GOMEZ, and R. Cossent, "Local flexibility mechanisms for electricity distribution through regulatory sandboxes: International review and a proposal for spain," in *2021 IEEE Madrid PowerTech*, 2021, pp. 1–6, DOI: 10.1109/PowerTech46648.2021.9494866.

[70] B. R. a. D. M. WG, "BRIDGE TSO-DSO Coordination report," BRIDGE, Tech. Rep. D3.12.f, Dec. 2019.

[71] E. Commission, *Eu commission regulation 2016/679: General data protection regulation (gdpr)*, en, Dec. 2016, [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[72] E. Commission, *Eu commission regulation 2017/2195*, en, Dec. 2022, [Online]. Available: http://data.europa.eu/eli/reg/2017/2195/oj.

[73] E. Commission, *Eu commission regulation 2017/1485*, en, Dec. 2021, [Online]. Available: http://data.europa.eu/eli/reg/2017/1485/2021-03-15.

[74] E. Commission, *Eu commission regulation 2016/1388*, en, Dec. 2016, [Online]. Available: http://data.europa.eu/eli/reg/2016/1388/oj.

[75] *Smart Grid Use Cases*, English, Github Repository, 2022, [Online]. Available: https://smart-grid-use-%20cases.github.io.

[76] e. ENTSO-E EFET, "The Harmonised Electricity Market Role Model," Tech. Rep., 2022, [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/EDI/Library/HRM/Harmonised_Role_Model_2022-01.pdf (visited on Dec. 27, 2023).

[77] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," en, *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, Jun. 2019, ISSN: 18745482, DOI: 10.1016/j.ijcip.2019.01.001.

[78] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *2019 IEEE Symposium on Security and Privacy (SP)*, May 2019, pp. 1362–1380, DOI: 10.1109/SP.2019.00013.

[79] A. Di Felice, *Defining the way forward for IoT security and certification schemes*, Oct. 2019, [Online]. Available: https://www.digitaleurope.org/wp/wp-content/uploads/2019/10/Position-on-IoT-security-and-certification-schemes-FINAL-FOR-APPROVAL.pdf (visited on Jan. 9, 2024).

[80] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 15–32.

[81] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," in *2017 North American Power Symposium (NAPS)*, Sep. 2017, pp. 1–6, DOI: 10.1109/NAPS.2017.8107267.

[82] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment," en, *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 3, pp. 274–282, Sep. 2020, ISSN: 2398-3396, 2398-3396, DOI: 10.1049/iet-cps.2019.0084.

[83] R. S. de Carvalho and D. Saleem, "Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources," in *2019 Resilience Week (RWS)*, vol. 1, Nov. 2019, pp. 226–231, DOI: 10.1109/RWS47064.2019.8972000.

[84] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable?" *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[85] A. Mokarim, G. B. Gaggero, and M. Marchese, "Evaluation of the impact of cyber-attacks against electric vehicle charging stations in a low voltage distribution grid," in *14th IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2023)*, Glasgow, 2023.

[86] E. U. A. for Cybersecurity (ENISA), *Cybersecurity – security requirements for ICT product certification*, Oct. 2023, [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en (visited on Dec. 29, 2023).

[87] E. Commission, *Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014*, en, Sep. 2020, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.

[88] E. Commission, *EU directive 2022/2555 (NIS 2 Directive)*, en, Dec. 2022, [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[89] E. Commission, *EU electricity supply – sector-specific rules on cybersecurity (network code)*, Oct. 2023, [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13101-EU-electricity-supply-sector-specific-rules-on-cybersecurity-network-code-_en (visited on Jan. 5, 2024).

[90] V. Pillitteri and T. Brewer, *Guidelines for smart grid cybersecurity*, en, Sep. 2014, DOI: https://doi.org/10.6028/NIST.IR.7628r1.

[91] E. Commission, *Commission Recommendation on cybersecurity in the energy sector*, English, Apr. 2019, [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf.

[92] Y. Li, P. Zhang, and R. Huang, "Lightweight quantum encryption for secure transmission of power data in smart grid," *IEEE Access*, vol. 7, pp. 36 285–36 293, 2019, DOI: 10.1109/ACCESS.2019.2893056.

[93] B. Dupont, L. Meeus, and R. Belmans, "Measuring the "smartness" of the electricity grid," in *2010 7th International Conference on the European Energy Market*, IEEE, 2010, pp. 1–6.

[94] A. Bok Soon and S. Kwong Mian, *Smart Grid Index "How smart is your grid?"* 2018.

[95] P. Venemans and M. Schreuder, "A method for the quantitative assesment of reliability of smart grids," en, in *CIRED 2012 Workshop: Integration of Renewables into the Distribution Grid*, Lisbon, Portugal: IET, 2012, pp. 117–117, ISBN: 978-1-84919-628-4, DOI: 10.1049/cp.2012.0757.

[96] M. J. C. de Mendonca, A. O. Pereira, M. M. H. Bellido, L. A. Medrano, and J. F. M. Pessanha, "Service quality performance indicators for electricity distribution in Brazil," *Utilities Policy*, vol. 80, p. 101 481, 2023, ISSN: 0957-1787, DOI: https://doi.org/10.1016/j.jup.2022.101481.

[97] W. J. Harder, "Key Performance Indicators for Smart Grids," en, M.S. thesis, University of Twente, 2017.

[98] A. Janjic, S. Savic, G. Janackovic, M. Stankovic, and L. Velimirovic, "Multi-criteria assessment of the smart grid efficiency using the fuzzy analytic hierarchy process," *Facta universitatis - series: Electronics and Energetics*, vol. 29, pp. 631–646, Dec. 2016, DOI: 10.2298/FUEE1604631J.

[99] L. Z. Velimirović, A. Janjić, and J. D. Velimirović, "Smart Grid Project Efficiency Assessment," in *Multi-criteria Decision Making for Smart Grid Design and Operation: A Society 5.0 Perspective*. Singapore: Springer Nature Singapore, 2023, pp. 27–44, ISBN: 978-981-19-7677-3, DOI: 10.1007/978-981-19-7677-3.

[100] L. Ge, Y. Li, S. Li, J. Zhu, and J. Yan, "Evaluation of the situational awareness effects for smart distribution networks under the novel design of indicator framework and hybrid weighting method," *Frontiers in Energy*, vol. 15, no. 1, pp. 143–158, 2021, DOI: 10.1007/s11708-020-0703-2.

[101] R. Acosta, C. Wanigasekara, S. Lehnhoff, and J. Gomez, "Evaluating distribution system flexibility markets based on smart grid key performance indicators," in *Proceedings of 2023 3rd Power System and Green Energy Conference, PSGEC 2023*, 2023, pp. 393–400, DOI: 10.1109/PSGEC58411.2023.10255889.

[102] CEDEC, E.DSO, Eurelectric, and GEODE, "Smart Grid Key Performance Indicators: A DSO perspective," Tech. Rep., 2021.

[103] G. Prettico, A. Marinopoulos, and S. Vitiello, "Distribution System Operator Observatory 2020: An in-depth look on distribution grids in Europe," JRC, European Comission, Tech. Rep., 2021, [Online]. Available: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/distribution-system-operator-observatory-2020.

[104] G. Prettico, A. Marinopoulos, and S. Vitiello, "Guiding electricity distribution system investments to improve service quality: A european study," *Utilities Policy*, vol. 77, 2022, DOI: 10.1016/j.jup.2022.101381.

[105] M. Fotopoulou, D. Rakopoulos, and S. Petridis, "Development of a multi-dimensional Key Performance Indicators' framework for the holistic performance assessment of Smart Grids," in *ECOS 2022 - The 35th International Conference on Efficiency, Cost Optimization, Simulation and Environmental Impact of Energy Systems*, Copenhagen, Denmark, Jul. 2022, DOI: 10.5281/zenodo.7249154.

[106] E. Incorporated, "Metrics for Measuring Progress Toward Implementation of the Smart Grid," Office of Electricity Delivery and Energy Reliability, Washington, DC, Tech. Rep., Jun. 2008, [Online]. Available: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Smart_Grid_Workshop_Report_Final_Draft_07_21_09.pdf.

[107] P. J. Balducci, M. R. Weimar, and H. Kirkham, "Smart grid status and metrics report," Jul. 2014, DOI: 10.2172/1168929.

[108] H. de Faria, J. G. S. Costa, and J. L. M. Olivas, "A review of monitoring methods for predictive maintenance of electric power transformers based on dissolved gas analysis," *Renewable and Sustainable Energy Reviews*, vol. 46, pp. 201–209, Jun. 2015, DOI: 10.1016/j.rser.2015.02.052.

[109] S. Saponara, L. Fanucci, F. Bernardo, and A. Falciani, "Predictive diagnosis of high-power transformer faults by networking vibration measuring nodes with integrated signal processing," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 8, pp. 1749–1760, Aug. 2016, DOI: 10.1109/tim.2016.2552658.

[110] F. E. Abrahamsen, Y. Ai, and M. Cheffena, "Communication technologies for smart grid: A comprehensive survey," *Sensors*, vol. 21, no. 23, 2021, ISSN: 1424-8220, DOI: 10.3390/s21238087.

[111] B. S. Roy, A. Sinha, and A. Pradhan, "An optimal PMU placement technique for power system observability," *International Journal of Electrical Power and Energy Systems*, vol. 42, no. 1, pp. 71–77, Nov. 2012, DOI: 10.1016/j.ijepes.2012.03.011.

[112] J. Zhao, J. Qi, Z. Huang, A. P. S. Meliopoulos, A. Gomez-Exposito, M. Netto, L. Mili, A. Abur, V. Terzija, I. Kamwa, B. Pal, and A. K. Singh, "Power system dynamic state estimation: Motivations, definitions, methodologies, and future work," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3188–3198, Jul. 2019, DOI: 10.1109/tpwrs.2019.2894769.

[113] European Commission. Directorate General for Energy. and Tractebel Impact., "Benchmarking smart metering deployment in the EU-28: Final report.," en, LU, Tech. Rep., 2020, [Online]. Available: https://data.europa.eu/doi/10.2833/492070.

[114] A. Rodriguez-Calvo, R. Cossent, and P. Frias, "Assessing the potential of MV automation for distribution network reliability improvement," en, *International Transactions on Electrical Energy Systems*, vol. 27, no. 10, e2383, Oct. 2017, ISSN: 20507038, DOI: 10.1002/etep.2383.

[115] G. Fotis, C. Dikeakos, E. Zafeiropoulos, S. Pappas, and V. Vita, "Scalability and replicability for smart grid innovation projects and the improvement of renewable energy sources exploitation: The flexitranstore case," *Energies*, vol. 15, no. 13, p. 4519, 2022.

[116] A. Rodriguez-Calvo, R. Cossent, and P. Frías, "Scalability and replicability analysis of large-scale smart grid implementations: Approaches and proposals in europe," *Renewable and Sustainable Energy Reviews*, vol. 93, pp. 1–15, Oct. 2018, DOI: 10.1016/j.rser.2018.03.041.

[117] A. B. Bondi, "Characteristics of scalability and their impact on performance," en, in *Proceedings of the second international workshop on Software and performance - WOSP '00*, Ottawa, Ontario, Canada: ACM Press, 2000, pp. 195–203, ISBN: 978-1-58113-195-6, DOI: 10.1145/350391.350432.

[118] CEN-CENELEC-ETSI Smart Grid Coordination Group, *Smart Grid Reference Architecture*, Nov. 2012.

[119] R. Cossent, L. Alacreu, J. P. Chaves, and M. Serrano, "Draft methodological guidelines to perform a scalability and replicability analysis," H2020 BRIDGE, Tech. Rep. D3.12, Dec. 2019.

[120] Scalability and Replicability Task Force, "BRIDGE Guidelines for implementing the prescribed technology: Additional subroutines and requirements. Scientific background and state of the art," H2020 BRIDGE, Tech. Rep., Nov. 2021.

[121] J. Hennessy, "The future of systems research," *Computer*, vol. 32, no. 8, pp. 27–33, 1999, DOI: 10.1109/2.781631.

[122] B. Sörries, "Communication technologies and networks for Smart Grid and Smart Metering," *CDG 450 Connectivity Special Interest Group (450 SIG)*, Sep. 2013.

[123] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. P. Chen, "A survey of communication/networking in Smart Grids," en, *Future Generation Computer Systems*, vol. 28, no. 2, pp. 391–404, Feb. 2012, ISSN: 0167739X, DOI: 10.1016/j.future.2011.04.014.

[124] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," en, *Computer Communications*, vol. 36, no. 17-18, pp. 1665–1697, Nov. 2013, ISSN: 01403664, DOI: 10.1016/j.comcom.2013.09.004.

[125] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, "Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IoT)," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1505–1515, Jun. 2018, ISSN: 2327-4662, DOI: 10.1109/JIOT.2017.2781251.

[126] J. Haapola, S. Ali, C. Kalalas, J. Markkula, N. Rajatheva, A. Pouttu, J. M. M. Rapún, I. Lalaguna, F. Vazquez-Gallego, J. Alonso-Zarate, G. Deconinck, H. Almasalma, J. Wu, C. Zhang, E. P. Muñoz, and F. D. Gallego, "Peer-to-Peer Energy Trading and Grid Control Communications Solutions' Feasibility Assessment Based on Key Performance Indicators," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, Jun. 2018, pp. 1–5, DOI: 10.1109/VTCSpring.2018.8417871.

[127] P. Jogalekar and C. Woodside, "A scalability metric for distributed computing applications in telecommunications," in *Teletraffic Science and Engineering*, vol. 2, Elsevier, 1997, pp. 101–110.

[128] J. Le Baut, "Technical Scalability and Replicability of the InteGrid smart grid functionalities," en, H2020 InteGRID, Tech. Rep. D8.1, 2019, p. 377.

[129] K. Angelakoglou, N. Nikolopoulos, P. Giourka, I.-L. Svensson, P. Tsarchopoulos, A. Tryferidis, and D. Tzovaras, "A Methodological Framework for the Selection of Key Performance Indicators to Assess Smart City Solutions," en, *Smart Cities*, vol. 2, no. 2, pp. 269–306, Jun. 2019, ISSN: 2624-6511, DOI: 10.3390/smartcities2020018.

[130] F. Plaiogiannis, V. Banos, L. Lombarto, S. Meir, I. Benítez, P. Mullor Ruiz, A. Zambrano, and E. Pastor, "Scaling up and Replication Roadmap," H2020 WiseGRID, Tech. Rep. D18.1, Apr. 2020.

[131] D. I. Makrygiorgou, N. Andriopoulos, I. Georgantas, J. Rong, I. Moraitis, E. P. Calatayud, and M. S. Matoses, "Scalability and replicability analysis of smart grid projects: Insights from the h2020 crossbow project," *Frontiers in Energy Research*, vol. 11, p. 1 167 517, 2023.

[132] V. Maagøe, "Interoperability," English, IEA 4E EDNA, Tech. Rep., Oct. 2022, p. 41, [Online]. Available: https://www.iea-4e.org/wp-content/uploads/2022/10/EDNA-Studies-Interoperability-Final.pdf.

[133] G. López, J. I. Moreno, H. Amarís, and F. Salazar, "Paving the road toward Smart Grids through large-scale advanced metering infrastructures," *Electric Power Systems Research*, vol. 120, pp. 194–205, 2015, ISSN: 0378-7796, DOI: https://doi.org/10.1016/j.epsr.2014.05.006.

[134] N. Rodríguez-Pérez, *Taxonomy of ICT sCalability and replicabiliTy Analyses - Collaborative Initiative (TICTA-C)*, Jul. 2022, [Online]. Available: https://tictac-initiative.github.io/.

[135] S. Potenciano Menci, J. Le Baut, J. Matanza Domingo, G. López López, R. Cossent Arín, and M. Pio Silva, "A Novel Methodology for the Scalability Analysis of ICT Systems for Smart Grids Based on SGAM: The InteGrid Project Approach," en, *Energies*, vol. 13, no. 15, p. 3818, Jul. 2020, ISSN: 1996-1073, DOI: 10.3390/en13153818.

[136] S. Potenciano Menci, F. Kupzog, B. Herndler, J. Le Baut, and M. Calin, "Scalability and replicability analysis (SRA) for all use cases v1.0," H2020 InterFLEX, Tech. Rep. D3.8, Dec. 2019.

[137] T. Yamada, K. Suzuki, and C. Ninagawa, "Scalability analysis of aggregation web services for smart grid fast automated demand response," in *2018 IEEE International Conference on Industrial Technology (ICIT)*, Feb. 2018, pp. 1285–1289, DOI: 10.1109/ICIT.2018.8352363.

[138] J. Matanza, S. Kiliccote, S. Alexandres, and C. Rodríguez-Morcillo, "Simulation of low-voltage narrow-band power line communication networks to propagate openadr signals," *Journal of Communications and Networks*, vol. 17, no. 6, pp. 656–664, 2015, DOI: 10.1109/JCN.2015.000112.

[139] M. H. Yaghmaee, A. Leon-Garcia, and M. Moghaddassian, "On the Performance of Distributed and Cloud-Based Demand Response in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 5403–5417, Sep. 2018, ISSN: 1949-3061, DOI: 10.1109/TSG.2017.2688486.

[140] S. Kenner, R. Thaler, M. Kucera, K. Volbert, and T. Waas, "Comparison of smart grid architectures for monitoring and analyzing power grid data via Modbus and REST," en, *EURASIP Journal on Embedded Systems*, vol. 2017, no. 1, p. 12, Dec. 2017, ISSN: 1687-3963, DOI: 10.1186/s13639-016-0045-7.

[141] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and Y. Wu, "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," in *2015 IEEE Power & Energy Society General Meeting*, IEEE, 2015, pp. 1–5.

[142] M. Garau, G. Celli, E. Ghiani, F. Pilo, and S. Corti, "Evaluation of smart grid communication technologies with a co-simulation platform," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 42–49, 2017.

[143] J. Zhou, R. Qingyang Hu, and Y. Qian, "Scalable Distributed Communication Architectures to Support Advanced Metering Infrastructure in Smart Grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1632–1642, Sep. 2012, ISSN: 1558-2183, DOI: 10.1109/TPDS.2012.53.

[144] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and D. Shi, "Performance evaluation of communication technologies and network structure for smart grid applications," en, *IET Communications*, vol. 13, no. 8, pp. 1025–1033, 2019, ISSN: 1751-8636, DOI: 10.1049/iet-com.2018.5408.

[145] L. González-Sotres, C. Mateo, P. Frías, C. Rodríguez-Morcillo, and J. Matanza, "Replicability Analysis of PLC PRIME Networks for Smart Metering Applications," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 827–835, Mar. 2018, ISSN: 1949-3061, DOI: 10.1109/TSG.2016.2569487.

[146] J. Zhang, A. Hasandka, S. M. S. Alam, T. Elgindy, A. R. Florita, and B.-M. Hodge, "Analysis of Hybrid Smart Grid Communication Network Designs for Distributed Energy Resources Coordination," in *2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb. 2019, pp. 1–5, DOI: 10.1109/ISGT.2019.8791581.

[147] J. Zhang, A. Hasandka, J. Wei, S. Alam, T. Elgindy, A. Florita, and B.-M. Hodge, "Hybrid Communication Architectures for Distributed Smart Grid Applications," en, *Energies*, vol. 11, no. 4, p. 871, Apr. 2018, ISSN: 1996-1073, DOI: 10.3390/en11040871.

[148] A. Meeuw, S. Schopfer, A. Wörner, V. Tiefenbeck, L. Ableitner, E. Fleisch, and F. Wortmann, "Implementing a blockchain-based local energy market: Insights on communication and scalability," en, *Computer Communications*, vol. 160, pp. 158–171, Jul. 2020, ISSN: 01403664, DOI: 10.1016/j.comcom.2020.04.038.

[149] P. Rengaraju, C.-H. Lung, and A. Srinivasan, "Communication requirements and analysis of distribution networks using wimax technology for smart grids," in *2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2012, pp. 666–670, DOI: 10.1109/IWCMC.2012.6314284.

[150] S. Hanna, S. Rohjans, P. Heeren, and J. Rolink, "Supporting the requirements-based selection of suitable communication protocols in smart grids," in *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2022, pp. 1–5, DOI: 10.1109/ISGT-Europe54678.2022.9960466.

[151] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, no. 1, 2019, ISSN: 2411-5134, DOI: 10.3390/inventions4010022.

[152] I. Mashal, O. A. Khashan, M. Hijjawi, and M. Alshinwan, "The determinants of reliable smart grid from experts' perspective," *Energy Informatics*, vol. 6, no. 1, p. 10, Apr. 11, 2023, ISSN: 2520-8942, DOI: 10.1186/s42162-023-00266-3.

[153] M. Klaes, J. Zwartscholten, A. Narayan, S. Lehnhoff, and C. Rehtanz, "Impact of ict latency, data loss and data corruption on active distribution network control," *IEEE Access*, vol. 11, pp. 14 693–14 701, 2023, DOI: 10.1109/ACCESS.2023.3243255.

[154] D. Niyato, P. Wang, Z. Han, and E. Hossain, "Impact of packet loss on power demand estimation and power supply cost in smart grid," in *2011 IEEE Wireless Communications and Networking Conference*, 2011, pp. 2024–2029, DOI: 10.1109/WCNC.2011.5779440.

[155] D. Ottolini, I. Zyrianoff, and C. Kamienski, "Interoperability and Scalability Trade-offs in Open IoT Platforms," in *2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC)*, Jan. 2022, pp. 1–6, DOI: 10.1109/CCNC49033.2022.9700622.

[156] A. M. Del Esposte, F. Kon, F. M. Costa, and N. Lago, "InterSCity: A Scalable Microservice-based Open Source Platform for Smart Cities:" en, in *Proceedings of the 6th International Conference on Smart Cities and Green ICT Systems*, Porto, Portugal: SCITEPRESS - Science and Technology Publications, 2017, pp. 35–46, ISBN: 978-989-758-241-7, DOI: 10.5220/0006306200350046.

[157] M. El Soussi, P. Zand, F. Pasveer, and G. Dolmans, "Evaluating the Performance of eMTC and NB-IoT for Smart City Applications," in *2018 IEEE International Conference on Communications (ICC)*, May 2018, pp. 1–7, DOI: 10.1109/ICC.2018.8422799.

[158] D. Bian, M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Assessment of communication technologies for a home energy management system," in *ISGT 2014*, Feb. 2014, pp. 1–5, DOI: 10.1109/ISGT.2014.6816449.

[159] K. Mets, J. A. Ojea, and C. Develder, "Combining power and communication network simulation for cost-effective smart grid analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1771–1796, 2014.

[160] F. Malandra and B. Sansò, "Performance Evaluation of Large-scale RF-Mesh Networks in a Smart City Context," en, *Mobile Networks and Applications*, vol. 23, no. 4, pp. 912–920, Aug. 2018, ISSN: 1383-469X, 1572-8153, DOI: 10.1007/s11036-017-0958-y.

[161] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent Edge Computing for IoT-Based Energy Management in Smart Cities," *IEEE Network*, vol. 33, no. 2, pp. 111–117, Mar. 2019, ISSN: 1558-156X, DOI: 10.1109/MNET.2019.1800254.

[162] P. K. Sharma, S. Rathore, and J. H. Park, "DistArch-SCNet: Blockchain-Based Distributed Architecture with Li-Fi Communication for a Scalable Smart City Network," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 55–64, Jul. 2018, ISSN: 2162-2256, DOI: 10.1109/MCE.2018.2816745.

[163] OMNeT++, *Omnet++ discrete event simulator*, [Online]. Available: https://omnetpp.org/ (visited on Dec. 27, 2023).

[164] Ackspace, *Cat5 Technical Sheet*, [Online]. Available: https://ackspace.nl/w/images/b/b1/Cat5_reference_sheet.pdf (visited on Mar. 7, 2022).

[165] E. Gamess, B. Smith, and G. Francia III, "Performance Evaluation of Modbus TCP in Normal Operation and Under A Distributed Denial of Service Attack," en, *International journal of Computer Networks & Communications*, vol. 12, no. 2, pp. 1–21, Mar. 2020, ISSN: 09752293, DOI: 10.5121/ijcnc.2020.12201.

[166] "Ieee standard for ethernet," *IEEE Std 802.3-2022 (Revision of IEEE Std 802.3-2018)*, pp. 1–7025, 2022, DOI: 10.1109/IEEESTD.2022.9844436.

[167] Egain, *Egain Sense Technical Sheet*, Jun. 2020, [Online]. Available: https://wwwegainio.cdn.triggerfish.cloud/uploads/2020/06/egain-techspecs_egain-sense-908_version-a_2020-1.pdf (visited on Oct. 28, 2022).

[168] Egain, *Egain Edge Hub Technical Sheet*, Jun. 2020, [Online]. Available: https://wwwegainio.cdn.triggerfish.cloud/uploads/2020/06/egain-techspecs_913-edge-hub_version-a_2020-1.pdf (visited on Oct. 28, 2022).

[169] INET, *INET Framework -An open-source OMNeT++ model suite for wired, wireless and mobile networks.* [Online]. Available: https://inet.omnetpp.org/ (visited on Nov. 2, 2022).

[170] N. Rodríguez-Pérez, J. M. Domingo, G. L. López, and M. Hajigholi, "Scalability analysis of a wireless m-bus system for smart metering and sensoring," in *2023 IEEE Belgrade PowerTech*, 2023, pp. 1–6, DOI: 10.1109/PowerTech55446.2023.10202977.

[171] C. Bruno, L. Guidi, A. Lorite-Espejo, and D. Pestonesi, "Assessing a potential cyber-attack on the italian electric system," *IEEE Security & Privacy*, vol. 13, no. 5, pp. 42–51, 2015, ISSN: 1558-4046, DOI: 10.1109/MSP.2015.99.

[172] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial, and industrial IoT (in)security: Attack taxonomy and case studies," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 199–221, 2022, ISSN: 2327-4662, DOI: 10.1109/JIOT.2021.3079916.

[173] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, Orlando FL USA: ACM, Dec. 4, 2017, pp. 303–314, ISBN: 978-1-4503-5345-8, DOI: 10.1145/3134600.3134639.

[174] M. P. Goodridge, A. Zocca, and S. Lakshminarayana, "Analysis of cascading failures due to dynamic load-altering attacks," in *14th IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2023)*, Glasgow, 2023.

[175] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011, ISSN: 1949-3061, DOI: 10.1109/TSG.2011.2160297.

[176] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6695–6709, 2023, DOI: 10.1109/JSYST.2023.3305757.

[177] A. S. Musleh, J. Ahmed, N. Ahmed, H. Xu, G. Chen, J. Hu, and S. Jha, "Development of a collaborative hybrid cyber-physical testbed for analysing cybersecurity issues of der systems," in *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2023, pp. 1–6, DOI: 10.1109/SmartGridComm57358.2023.10333908.

[178] P. Linnartz, A. Winkens, and A. Ulbig, "Assessing the impact of cyber attacks manipulating distributed energy resources on power system operation," *arXiv preprint arXiv:2207.07968*, 2022.

[179] A. Mumrez, G. Sánchez, G. Elbez, and V. Hagenmeyer, "On evasion of machine learning-based intrusion detection in smart grids," in *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2023, pp. 1–7, DOI: 10.1109/SmartGridComm57358.2023.10333966.

[180] W. Lin, M. R. Saifuddin, and B. Chen, "The design and implementation of a cyber exercise on epic microgrid testbed," in *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2023, pp. 1–7, DOI: 10.1109/SmartGridComm57358.2023.10333919.

[181] M. Mahrukh and M. S. Thomas, "Load altering attacks- a review of impact and mitigation strategies," in *2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON)*, 2023, pp. 397–402, DOI: 10.1109/REEDCON57544.2023.10150456.

[182] Y. Dvorkin and S. Garg, "Iot-enabled distributed cyber-attacks on transmission and distribution grids," in *2017 North American Power Symposium (NAPS)*, 2017, pp. 1–6, DOI: 10.1109/NAPS.2017.8107363.

[183] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2018.

[184] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against iot demand attacks," in *28th USENIX security symposium (USENIX Security 19)*, 2019, pp. 1115–1132.

[185] S. Lakshminarayana, S. Adhikari, and C. Maple, "Analysis of iot-based load altering attacks against power grids using the theory of second-order dynamical systems," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4415–4425, 2021, DOI: 10.1109/TSG.2021.3070313.

[186] M. P. Goodridge, S. Lakshminarayana, and C. Few, "Analysis of load-altering attacks against power grids: A rare-event sampling approach," in *2022 17th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, IEEE, 2022, pp. 1–6.

[187] T. Shekari, C. Irvene, A. A. Cardenas, and R. Beyah, "Mamiot: Manipulation of energy market leveraging high wattage iot botnets," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '21, Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, pp. 1338–1356, ISBN: 9781450384544, DOI: 10.1145/3460120.3484581.

[188] T. Shekari, A. A. Cardenas, and R. Beyah, "Madiot 2.0: Modern high-wattage iot botnet attacks and defenses," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 3539–3556.

[189] K. Chan, Y. Kim, and J.-Y. Jo, "Der communication networks and their security issues," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, pp. 0785–0790, DOI: 10.1109/CCWC54503.2022.9720774.

[190] I. Zografopoulos, C. Konstantinou, N. G. Tsoutsos, D. Zhu, and R. Broadwater, "Security assessment and impact analysis of cyberattacks in integrated t&d power systems," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, ser. MSCPES '21, Virtual Event: Association for Computing Machinery, 2021, ISBN: 9781450386081, DOI: 10.1145/3470481.3472706.

[191] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. R. Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada, "A review of cyber–physical security for photovoltaic systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, 2022, DOI: 10.1109/JESTPE.2021.3111728.

[192] D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Assessing cyber-physical risks of iot-based energy devices in grid operations," *IEEE Access*, vol. 8, pp. 61 161–61 173, 2020, DOI: 10.1109/ACCESS.2020.2983313.

[193] J. L. Rueda, J. C. Cepeda, I. Erlich, A. W. Korai, and F. M. Gonzalez-Longatt, "Probabilistic approach for risk evaluation of oscillatory stability in power systems," in *PowerFactory Applications for Power System Analysis*, ser. Power Systems, F. M. Gonzalez-Longatt and J. Luis Rueda, Eds., Springer International Publishing, 2014, pp. 249–266, ISBN: 978-3-319-12958-7, DOI: 10.1007/978-3-319-12958-7_11.

[194] A. Borys, A. Kamruzzaman, H. N. Thakur, J. C. Brickley, M. L. Ali, and K. Thakur, "An evaluation of iot ddos cryptojacking malware and mirai botnet," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 725–729, DOI: 10.1109/AIIoT54504.2022.9817163.

[195] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110, ISBN: 978-1-931971-40-9, [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[196] A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos, "Open source intelligence for energy sector cyberattacks," in *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, D. Gritzalis, M. Theocharidou, and G. Stergiopoulos, Eds., Cham: Springer International Publishing, 2019, pp. 261–281, ISBN: 978-3-030-00024-0, DOI: 10.1007/978-3-030-00024-0_14.

[197] C. Arderne, C. Zorn, C. Nicolas, and E. E. Koks, "Predictive mapping of the global power system using open data," *Scientific Data*, vol. 7, no. 1, p. 19, Jan. 15, 2020, ISSN: 2052-4463, DOI: 10.1038/s41597-019-0347-4.

[198] H. Kim, D. Olave-Rojas, E. Álvarez-Miranda, and S.-W. Son, "In-depth data on the network structure and hourly activity of the central chilean power grid," *Scientific Data*, vol. 5, no. 1, p. 180 209, Oct. 23, 2018, ISSN: 2052-4463, DOI: 10.1038/sdata.2018.209.

[199] W. Medjroubi, U. P. Müller, M. Scharf, C. Matke, and D. Kleinhans, "Open data in power grid modelling: New approaches towards transparent grid models," *Energy Reports*, vol. 3, pp. 14–21, Nov. 2017, ISSN: 23524847, DOI: 10.1016/j.egyr.2016.12.001.

[200] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.

[201] E. Martel, R. Kariger, and P. Graf, "Cyber resilience in the electricity ecosystem: Principles and guidance for boards," *Center for Cybersecurity and Electricity Industry Community, World Economic Forum*, 2019, [Online]. Available: https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf.

[202] Comisión Nacional de los Mercados y la Competencia (CNMC). "Información mensual de estadísticas sobre producción de energía eléctrica a partir de renovables, cogeneración y residuos." Spanish. (Jun. 1, 2023), [Online]. Available: https://www.cnmc.es (visited on Jul. 6, 2023).

[203] Red Eléctrica de España. "Consulta el estado de las solicitudes." Spanish. (May 31, 2023), [Online]. Available: https://www.ree.es/es/clientes/generador/acceso-conexion/conoce-el-estado-de-las-solicitudes (visited on Jul. 6, 2023).

[204] C. of European Energy Regulators (CEER), "CEER Position Paper on the Future DSO and TSO Relationship," Tech. Rep. C16-DS-26-04, Sep. 2016.

[205] B. D. M. WG, "European energy data exchange reference architecture," BRIDGE, Tech. Rep., 2021.

[206] A. G. Givisiez, K. Petrou, and L. F. Ochoa, "A Review on TSO-DSO Coordination Models and Solution Techniques," en, *Electric Power Systems Research*, vol. 189, p. 106 659, Dec. 2020, ISSN: 03787796, DOI: 10.1016/j.epsr.2020.106659.

[207] S. I. Vagropoulos, P. N. Biskas, and A. G. Bakirtzis, "Market-based TSO-DSO coordination for enhanced flexibility services provision," en, *Electric Power Systems Research*, vol. 208, p. 107 883, Jul. 2022, ISSN: 03787796, DOI: 10.1016/j.epsr.2022.107883.

[208] R. Silva, E. Alves, R. Ferreira, J. Villar, and C. Gouveia, "Characterization of TSO and DSO Grid System Services and TSO-DSO Basic Coordination Mechanisms in the Current Decarbonization Context," en, *Energies*, vol. 14, no. 15, p. 4451, Jul. 2021, ISSN: 1996-1073, DOI: 10.3390/en14154451.

[209] H. Gerard, E. I. Rivero Puente, and D. Six, "Coordination between transmission and distribution system operators in the electricity sector: A conceptual framework," *Utilities Policy*, vol. 50, pp. 40–48, 2018, ISSN: 0957-1787, DOI: https://doi.org/10.1016/j.jup.2017.09.011.

[210] M. Stefan, A. Zegers, and F. Kupzog, "Ict aspects of tsodso interaction data exchange and ict requirements along organizational interaction between tso and dso," *ISGAN: International Smart Grid Action Network*, 2018.

[211] E. Lambert, H. Morais, F. Reis, R. Alves, G. Taylor, A. Souvent, and N. Suljanovic, "Practices and Architectures for TSO-DSO Data Exchange: European Landscape," en, in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe*, Sarajevo, Bosnia and Herzegovina: IEEE, Oct. 2018, pp. 1–6, ISBN: 978-1-5386-4505-5, DOI: 10.1109/ISGTEurope.2018.8571547.

[212] A. Bytyqi, S. Gandhi, E. Lambert, and N. Petrovič, "A Review on TSO-DSO Data Exchange, CIM Extensions and Interoperability Aspects," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, pp. 309–315, Mar. 2022, ISSN: 2196-5420, DOI: 10.35833/MPCE.2021.000770.

[213] S. Skok, A. Mutapčić, R. Rubesa, and M. Bazina, "Transmission power system modeling by using aggregated distributed generation model based on a tso—dso data exchange scheme," *Energies*, vol. 13, no. 15, 2020, ISSN: 1996-1073, DOI: 10.3390/en13153949.

[214] *SmartNet Project*, en-GB, [Online]. Available: http://smartnet-project.eu/ (visited on Dec. 14, 2023).

[215] *Coordinet Project*, en, [Online]. Available: https://coordinet-project.eu (visited on Dec. 14, 2023).

[216] *TDX-ASSIST Project*, [Online]. Available: http://www.tdx-assist.eu/ (visited on Dec. 14, 2023).

[217] *Interrface Project*, [Online]. Available: http://interrface.eu/The-project (visited on Dec. 14, 2023).

[218] *EU-SysFlex Project*, en-US, [Online]. Available: https://eu-sysflex.com/ (visited on Dec. 14, 2023).

[219] CEDEC, EDSO, ENTSO-E, EURELECTRIC, and GEODE, "TSO-DSO Report: An integrated approach to active system management," Tech. Rep., 2019.

[220] H. INTERRFACE, "Definition of new/changing requirements for Market Designs.," Tech. Rep. Deliverable 3.2, 2020.

[221] P. Kuusela, P. Koponen, I. Kockar, and H. Xu, "An ICT cost comparison of different market structures for distributed ancillary services," en, in *CIRED 25th International Conference on Electricity Distribution*, Madrid, 2019, p. 5.

[222] S. Horsmanheimo, H. Kokkoniemi-Tarkkanen, P. Kuusela, L. Tuomimäki, C. A. Andersen, J. Dall, F. Pröstl Andrén, M. Stephan, F. Kupzog, J.L. Baut, K. N. Gregertsen, I.C.R. Tardy, G. Mathisen, D. Ectors, R. Rodríguez, C. Arrigoni, F. Zanellini, F. Corti, D. Moneta, M. Esser, G. Samen Curtis, and M. Pardo, "ICT Architecture and Design Specification," H2020 SmartNet, Tech. Rep. Deliverable 3.2, Apr. 2017, p. 135.

[223] Armin Ghasem Azar, Henrik Madsen, Rune Grønborg Junker, Zohreh Alizadeh, Hanne Binder, Adrián Ibañez, Stig B. Mortensen, Jacob Andreasen, Claus Amtrup Andersen, Thomas Saabye, Jacob Dall, Loui Algren, Miguel Marroquin, Giulia De Zotti, Thomas Kieldsen, Stig Holm Sørensen, and Razgar Ebrahimy, "Results of Pilot B (Denmark)," H2020 SmartNet, Tech. Rep. Deliverable 5.2, Apr. 2019, p. 88.

[224] M. Pardo, M. Duarte, C. Madina, J. Jimeno, M. Marroquín, A. Ibáñez, E. Estrade, and L. Jones, "Results of Pilot C (Spain)," H2020 SmartNet, Tech. Rep. Deliverable 5.3, Apr. 2019, p. 62.

[225] C. Bauschmann and J. Köhlke, "Interoperable Platforms for procuring system services from consumers, storage and generators: Specification of the interfaces linking the markets for grid services, the advanced monitoring tools for grid operation and the flexibility provided. V1.0," H2020 CoordiNet, Tech. Rep. Deliverable 2.4, Feb. 2021, p. 67.

[226] M. Radi, G. Taylor, J. Cantenot, E. Lambert, and N. Suljanovic, "Developing Enhanced TSO-DSO Information and Data Exchange Based on a Novel Use Case Methodology," *Frontiers in Energy Research*, vol. 9, p. 259, 2021, ISSN: 2296-598X, DOI: 10.3389/fenrg.2021.670573.

[227] N. Suljanovic, A. Souvent, G. Taylor, M. Radi, J. Cantenot, E. Lambert, and H. Morais, "Design of Interoperable Communication Architecture for TSO-DSO Data Exchange," en, in *2019 IEEE Milan PowerTech*, Milan, Italy: IEEE, Jun. 2019, pp. 1–6, ISBN: 978-1-5386-4722-6, DOI: 10.1109/PTC.2019.8810941.

[228] H. INTERRFACE, "TSO-DSO-Consumer INTERFACE aRchitecture to provide innovative Grid Services for an efficient power system," Tech. Rep. Deliverable 3.1.

[229] A. Tkaczyk and K. Kukk, "New big data collection, storage, and processing requirements as identified from the EU-SysFlex use cases," H2020 EU-SysFlex, Tech. Rep. Deliverable 5.3, Oct. 2020.

[230] Estfeed, "Estfeed Protocol v3," en, Technical Specification Y-1029-15, 2020, p. 38.

[231] E. Suignard, R. Jover, W. Albers, J. Budke, and K. Kukk, "Description of data exchange use cases based on IEC 62559 methodology," en, H2020 EU-SysFlex, Tech. Rep. Deliverable 5.2, Oct. 2020, p. 311.

[232] K. Kukk, L. Winiarski, B. Requardt, E. Suignard, C. Effantin, S. Sochynskyi, A. Tkaczyk, E. Lambert, P. Anton, O. Rossøy, N. Good, R. Jover, K. Trees, and W. Albers, "Proposal for data exchange standards and protocols," en, H2020 EU-SysFlex, Tech. Rep. Deliverable 5.5, Apr. 2021, p. 175.

[233] E. P. R. I. (EPRI), "Common Information Model Primer: Third Edition," en, Tech. Rep. 3002006001, Jul. 2015, p. 188.

[234] *IEC 61970:2022 SER series*, International Standard, 2022, [Online]. Available: https://webstore.iec.ch/publication/61167 (visited on Dec. 27, 2023).

[235] *IEC 61850-7-420:2021*, International Standard, 2021, [Online]. Available: https://webstore.iec.ch/publication/34384 (visited on Dec. 27, 2023).

[236] *IEC 61968-11:2013*, International Standard, 2013, [Online]. Available: https://webstore.iec.ch/publication/6199 (visited on Dec. 27, 2023).

[237] *IEC 61968-13:2021*, International Standard, 2021, [Online]. Available: https://webstore.iec.ch/publication/34213 (visited on Dec. 27, 2023).

[238] *IEC 61970-301:2020+AMD1:2022 CSV Consolidated version*, International Standard, 2022, [Online]. Available: https://webstore.iec.ch/publication/74467 (visited on Dec. 27, 2023).

[239] A. Kapetanios, V. Sakas, K. Kotsalos, N. Suljanovic, F. Oliveira, C. Ivanov, S. Happ, M. Haghgoo, E. Anderson, C. Augusto, and F. Bosco, "Report on Extended Data, Platform and Service Interoperability," en, OneNet Project, Tech. Rep. D5.6, 2022, [Online]. Available: https://www.onenet-project.eu//wp-content/uploads/2022/12/OneNet_D5.6_v1.0.pdf.

[240] *IEC 61970-302:2018*, International Standard, 2018, [Online]. Available: https://webstore.iec.ch/publication/29470 (visited on Dec. 27, 2023).

[241] *IEC 61970-452:2021*, International Standard, 2021, [Online]. Available: https://webstore.iec.ch/publication/64844 (visited on Dec. 27, 2023).

[242] *IEC 61970-456:2021*, International Standard, 2021, [Online]. Available: https://webstore.iec.ch/publication/68054 (visited on Dec. 27, 2023).

[243] *IEC 61970-457:2021*, International Standard, 2021, [Online]. Available: https://webstore.iec.ch/publication/31929 (visited on Dec. 27, 2023).

[244] *IEC 61970-600-1:2021*, International Standard, 2021, [Online]. Available: https://webstore.iec.ch/publication/63866 (visited on Dec. 27, 2023).

[245] *IEC 61970-600-2:2021*, International Standard, 2021, [Online]. Available: https://webstore.iec.ch/publication/63867 (visited on Dec. 27, 2023).

[246] *IEC 62325-351:2016*, International Standard, 2016, [Online]. Available: https://webstore.iec.ch/publication/25128 (visited on Dec. 27, 2023).

[247] *IEC 62325-301:2018*, International Standard, 2018, [Online]. Available: https://webstore.iec.ch/publication/31487 (visited on Dec. 27, 2023).

[248] *IEC 62325-451-2:2014*, International Standard, 2014, [Online]. Available: https://webstore.iec.ch/publication/6843 (visited on Dec. 27, 2023).

[249] *IEC 62325-451-4:2017*, International Standard, 2017, [Online]. Available: https://webstore.iec.ch/publication/29116 (visited on Dec. 27, 2023).

[250] *IEC 62325-451-5:2015*, International Standard, 2015, [Online]. Available: https://webstore.iec.ch/publication/21818 (visited on Dec. 27, 2023).

[251] *IEC 62325-451-6:2018*, International Standard, 2018, [Online]. Available: https://webstore.iec.ch/publication/60715 (visited on Dec. 27, 2023).

[252] H. J. Kim, C. M. Jeong, J.-M. Sohn, J.-Y. Joo, V. Donde, Y. Ko, and Y. T. Yoon, "A Comprehensive Review of Practical Issues for Interoperability Using the Common Information Model in Smart Grids," en, *Energies*, vol. 13, no. 6, p. 1435, Mar. 2020, ISSN: 1996-1073, DOI: 10.3390/en13061435.

[253] A. Schumilin, C. Duepmeier, K.-U. Stucky, and V. Hagenmeyer, "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)*, Aug. 2018, pp. 321–325, DOI: 10.1109/SEAA.2018.00059.

[254] C. Rodríguez-Domínguez, K. Benghazi, M. Noguera, J. L. Garrido, M. L. Rodríguez, and T. Ruiz-López, "A Communication Model to Integrate the Request-Response and the Publish-Subscribe Paradigms into Ubiquitous Systems," en, *Sensors*, vol. 12, no. 6, pp. 7648–7668, Jun. 2012, ISSN: 1424-8220, DOI: 10.3390/s120607648.

[255] OASIS, *MQTT Version 5.0*, A. Banks, E. Briggs, K. Borgendale, and R. Gupta, Eds., Mar. 2019, [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html.

[256] OASIS, *OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0*. Oct. 2012, [Online]. Available: https://docs.oasis-open.org/amqp/core/v1.0/amqp-core-complete-v1.0.pdf.

[257] J. E. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate, and P. Manzoni, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Jan. 2015, pp. 931–936, DOI: 10.1109/CCNC.2015.7158101.

[258] International Electrotechnical Commission, *IEC 60870-6-503:2014*, en, Jul. 2014, [Online]. Available: https://webstore.iec.ch/publication/3760.

[259] M. Franz, "ICCP Exposed: Assessing the Attack Surface of the "Utility Stack"," en, in *SCADA Security Scientific Symposium*, 2007, p. 15.

[260] M.J. Rice, G.K. Dayley, C.A. Bonebrake, and L.J. Becker, "Secure ICCP," Pacific Northwest National Laboratory, U.S. Department of Energy, Tech. Rep., Jun. 2017.

[261] J. Bartol, T. Kodek, A. Souvent, F. Oliveira, E. Lambert, N. Petrovič, and N. Suljanović, "Utilization of ECCo SP for secured and reliable information exchange between system operators," in *2019 27th Telecommunications Forum)*, Nov. 2019, pp. 1–4, DOI: 10.1109/FOR48224.2019.8971052.

[262] OMS, *Open Metering System Specification Vol.2: Primary communication issue 4.1.2 / 2016-12-16*, en, Dec. 2016, [Online]. Available: https://oms-group.org/fileadmin/files/download4all/specification/Vol2/4.1.2/OMS-Spec_Vol2_Primary_v412.pdf (visited on Dec. 19, 2023).

[263] F. Lavra, "Telit Wireless M-Bus 2013 Part 4 User Guide," en, Telit Communications, Tech. Rep., Jan. 2016, [Online]. Available: https://www.iot.com.tr/uploads/pdf/Telit_Wireless_M-bus_2013_Part4_User_Guide_r14.pdf (visited on Dec. 19, 2023).

[264] J. G. Proakis, M. Salehi, N. Zhou, and X. Li, *Communication systems engineering*. Prentice Hall New Jersey, 1994, vol. 2.

[265] S. Kurt and B. Tavli, "Path-Loss Modeling for Wireless Sensor Networks: A review of models and comparative evaluations.," *IEEE Antennas and Propagation Magazine*, vol. 59, no. 1, pp. 18–37, Feb. 2017, ISSN: 1558-4143, DOI: 10.1109/MAP.2016.2630035.

[266] I. T. U. (ITU-R), *Recommendation ITU-R P.1238-11: Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 450 GHz*, en, 2021.

[267] P. Masek, K. Zeman, Z. Kuder, J. Hosek, S. Andreev, R. Fujdiak, and F. Kropfl, "Wireless m-bus: An attractive m2m technology for 5g-grade home automation," in *Internet of Things. IoT Infrastructures*, Springer International Publishing, 2016, pp. 144–156, ISBN: 978-3-319-47063-4.

[268] J. Andersen, T. Rappaport, and S. Yoshida, "Propagation measurements and models for wireless communications channels," *IEEE Communications Magazine*, vol. 33, no. 1, pp. 42–49, Jan. 1995, ISSN: 1558-1896, DOI: 10.1109/35.339880.

[269] H. A. Obeidat, A. A. S. Alabdullah, E. A. Elkhazmi, E. A. Elkhazmi, W. Suhaib, O. Obeidat, M. S. Alkhambashi, M. Mosleh, M. F. Mosleh, N. T. Ali, Y. A. S. Dama, Z. Z. Abidin, R. A. Abd-Alhameed, and P. S. Excell, "Indoor environment propagation review," *Computer Science Review*, 2020, DOI: 10.1016/j.cosrev.2020.100272.

[270] T. S. Rappaport, *Wireless communications: Principles and practice, 2/E*. Pearson Education India, 2010.

[271] A. Kaya, B. De Beelde, W. Joseph, M. Weyn, and R. Berkvens, "Geodesic path model for indoor propagation loss prediction of narrowband channels," *Sensors*, vol. 22, no. 13, p. 4903, Jan. 2022, ISSN: 1424-8220, DOI: 10.3390/s22134903.

[272] G. Boultadakis, P. Mann, P. Butkus, N. Appleman, M. Gianluigi, D. Siface, M. Rossi, M. Baron, J. P. Chaves, K. Glennung, I. Vaitiekuté, N. Savvopoulos, P. Josefsson, A. Sanjab, and K. Kessels, "Coordination schemes, products and services for grid management," CoordiNet and INTERRFACE, Joint Paper.