CYPRESS

Report D1.3 describing the benchmarks

Task 1.3 - Project Report

Adrien Godfraind, Sami Ben Mariem, Vincent Rossetto, Frédéric Sabot, Pierre Henneaux, Yves Vanaubel

Date: 2022-11-15

Contents

Executive Summary

This document is the third deliverable of the "Cyber-Physical Risk of the bulk Electric Energy Supply System" (CYPRESS) project.

The work presented in this document has been performed in the frame of the first work package, WP1, titled "*Criteria and benchmarks for cyber-physical risk management*". The main objective of WP1 is to generalize and adapt the concepts currently used in reliability management of electric power and energy systems so that they can correctly cover the cyber-threats from various system wide control and communication layers while accounting for a large number of small active devices connected closer to the system edge. This work package should ensure coherence of the modeling and validation approaches to be used in both WP2 and WP3.

More precisely, this document is the result of the work performed during the third task (T1.3) of this work package. This task firstly aims at identifying a reduced number of benchmark test power systems from the power systems literature to be used in the CYPRESS project. It also seeks to make specific choices for modeling the cyber-layers that need to be added to these benchmarks. The modeling choices at the cyber-layer are guided by current and anticipated communication systems used by transmission system operators internally and for exchanging information with neighboring system operators and with edge power devices. The benchmarks selected in this task will be used in WP2 and WP3 for the purpose of cyber-physical security assessment and enhancement respectively.

This document starts by focusing on the power system part of the Task 1.3 objectives. Chapter 2 opens with a section dedicated to transmission test systems. It presents criteria that transmission test systems should meet to be selected for the next tasks of the project, then it describes the studied and selected benchmark test power systems and potential modifications of these systems to ensure that they meet most criteria. The chapter continues with distribution test systems by presenting selected distribution test systems. Finally the chapter concludes by making the link with the cyber layer, *i.e.* by describing the interconnections of the power systems with the cyber layer.

Chapter 3 focuses on the cyber part. Since the project aims at, among other things, carrying out digital tests and simulations on test systems representing Cyber-Physical Power Systems in their entirety, this chapter investigates what cyber components should be present in the cyber layer of Cyber-Physical Power Systems. Indeed, in the literature, there is a lack of reference ICT test systems to represent this cyber layer. This chapter starts by presenting the proposed modeling of cyber layer and then introduces the components that compose the cyber layer, such as components involved in the control, protection and monitoring of electrical equipment, the communication standards used in electrical substations, etc, in order to integrate them in the selected test power systems.

In addition to this report, a git repository containing the data of test power systems that were selected in the context of the task as well as a table summarising transmission test systems available in the literature can be found at the following link: `https://github.com/adriengodfraind/CYPRESS`.

Author Contributions

Table 1 lists all the authors that have contributed to this report. Adrien Godfraind is the main author of this report, he contributed to the entire document and coordinated the work with the other co-authors. Frédéric Sabot provided significant improvements and corrections to Chapter 2 and co-wrote Section 2.1. Sami Ben Mariem and Vincent Rossetto provided valuable inputs regarding the cyber part and co-wrote the entire Chapter 3 with Adrien. Pierre Henneaux contributed to Section 2.1.2.1 and to the data completion of some selected power test systems with Frédéric. Finally, Yves Vanaubel managed the whole task together with Adrien and provided valuable advice on the writing of the document and the upstream research.

Author	Affiliation
Adrien Godfraind	Haulogy
Sami Ben Mariem	Université de Liège
Vincent Rossetto	Université de Liège
Frédéric Sabot	Université libre de Bruxelles
Pierre Henneaux	Université libre de Bruxelles
Yves Vanaubel	Haulogy

Table 1: List of authors

List of acronyms

- AS: Autonomous System
- BGP: Border Gateway Protocol
- CPPS: Cyber-Physical Power System
- DMZ: DeMilitarized Zone
- DNP: Distributed Network Protocol
- DTLS: Datagram Transport Layer Security
- GMLC: Grid Modernization Laboratory Consortium
- GOOSE: Generic Object Oriented Substation Events
- GPS: Global Positioning System
- HMI: Human-Machine Interface
- HTTP: Hyper-Text Transfer Protocol
- HVDC: High-Voltage Direct-Current
- ICCP: Inter-Control Center Communications Protocol
- ICT: Information and Communication Technologies
- IDS: Intrusion Detection System
- IEC: International Electrotechnical Commission
- IED: Intelligent Electronic Device
- IEEE: Institute of Electrical and Electronics Engineers
- IP: Internet Protocol
- LAN: Local Area Network
- MAC: Media Access Control
- MPLS: Multi-Protocol Label Switching
- MTDC: Multi Terminal Direct Current
- OSPF: Open Shortest Path First
- PLC: Programmable Logic Controller

- RTS: Reliability Test System
- RTU: Remote Terminal Unit
- SCADA: Supervisory Control And Data Acquisition
- SV: Sampled Value
- TCP: Transmission Control Protocol
- TLS: Transport Layer Security
- TSO: Transmission System Operator
- UDP: User Datagram Protocol
- VAR: Volt-Ampere Reactive
- VLAN: Virtual Local Area Network
- VPN: Virtual Private Network
- WAN: Wide-Area Network

List of Figures

List of Tables

1

Introduction

For a number of years, the energy sector has been in full transition and this is particularly noticeable in the electric power systems. More and more elements of the power grid are intelligent and connected, which leads the community to talk about *smart grids* or Cyber-Physical Power Systems (CPPS) [1], [2]. We are seeing more and more distributed generation, decentralized control, intelligent loads and buildings, autonomous software, etc. being part of the power grid and its management [3]. All these are enabled and empowered by information and communication technology (ICT), so that the latter is more and more present in power systems. From generation to consumption, passing through transmission and distribution, there is clearly an increasingly tight connection between power systems and ICT networks [4].

This growing interconnection calls for the research and development of new protection and control algorithms [5] to plan and operate the power system, optimize its use or protect it against the multitude of new threats that are emerging with the addition of the cyber layer to the physical grid. Indeed, while the ICT presents an enhancement that enables, among other things, complex controls in smart grids, it also introduces additional complexity, new sources of failure and security threats [4].

This is why the "Cyber-Physical Risk of the bulk Electric Energy Supply System" (CYPRESS) project has been initiated. The objective of this project is to develop new knowledge, methods and tools necessary to guarantee the security of supply through the electricity transmission grid. These developments aim to address cyber threats by integrating them into a coherent probabilistic risk-management approach. The latter has been explored in the literature and is beginning to be used in practice, but the "cyber-vulnerability/physical grid stability limits" interactions have hardly been explored. This is why this objective of developing knowledge, methods and tools in the cyber-physical reliability management of the transmission system has been initiated.

Within the framework of this project, it is planned to carry out digital tests and simulations on test systems representing the Cyber-Physical Power Systems in their entirety. Task 1.3 - of which this document is the result - contributes to this achievement as it aims at selecting benchmark test systems that will be used for the above mentioned purposes. More specifically, the task aims firstly at identifying a reduced number of benchmark test power systems from the power systems literature to be used in the CYPRESS project. The task also seeks to make specific choices for modeling the cyber-layers that need to be added to these benchmarks. The bench-

marks selected in this task will be used in WP2 and WP3 for the purpose of cyber-physical security assessment and enhancement respectively. This document is organised as follows.

Chapter 2 focuses mainly on the power system part of the Task 1.3 objectives. The first section is dedicated to transmission systems and presents selection criteria that transmission test systems should meet to be selected as benchmarks for this project. Then, it describes test systems found in the literature that are of greatest interest, the reasons for this interest and, for some of them, the section explains the modifications that were made to make them satisfy a larger set of criteria. The chapter continues with distribution test systems (Section 2.2) by presenting selected distribution test systems. Finally Section 2.3 makes the link between the physical power system and the cyber layer, the latter being the focus of the next chapter. In particular, this section describes the interconnections of the power systems with the cyber layer.

Chapter 3 focuses on the cyber part of the Task 1.3 objectives. This chapter investigates what cyber components should be present in the cyber layer of Cyber-Physical Power Systems. It starts by presenting the proposed modeling of cyber layer (Section 3.1). Then Section 3.2 aims at providing more insights on the design of benchmark test systems for the cyber part of power systems infrastructure. Indeed, contrarily to power systems, there is a lack of reference ICT test systems to represent this cyber layer in the literature. Section 3.2 thus describes the components that compose the cyber layer of the power grid, such as components involved in the control, protection and monitoring of electrical equipment, the communication standards used in electrical substations, etc. Finally, Section 3.2.3 presents constraints and advice for infrastructure design, inspired by the industry, which will allow to define a realistic test system relevant to the operators.

2

Benchmark test power systems

This chapter focuses on the power system part of the Task 1.3 objectives. It mainly aims at describing the benchmark test power systems that were studied and selected and whose data were potentially completed during the course of this task.

First, the chapter opens with a section dedicated to transmission test systems (Section 2.1). This section starts by presenting the criteria used for the selection of these test systems. Then, it gives descriptions of the systems that interested us the most, the reasons for this interest and, for some of them, explain the modifications made by CYPRESS project members to make them satisfy a larger set of criteria. As for Section 2.2, it deals with distribution test systems and describes a few systems that could be of interest for the project. Finally, the chapter concludes with Section 2.3 describing the interconnection of the power system with the cyber layer -which will be the focus of the next chapter- and the concept of node-breaker modeling. The idea is to link the two chapters by presenting an overview of the different interconnection points between the physical and cyber domains.

The data that could be found for the systems described in this chapter is available online, at the following address[1]: `https://github.com/adriengodfraind/CYPRESS`. These data were obtained from a variety of power system test cases repositories and databases. The main ones are the Texas A&M University's Electric Grid Test Cases [6], the University of Washington's Power Systems Test Case Archive [7], the Illinois Center for a Smart Electric Grid's power cases [8], the PyPower library [9], the *Power Grid Lib* benchmark library [10], the Matpower database [11] and the *BetterGrids* Grid Data Repository [12]. Note that we have collected the files that might be useful, both the original system data files, some of its more popular modifications as well as the versions that was modified as part of the task. However, for some of the slight adaptations that can be found in one work or another, they can either be found in the papers cited in the report, or in other papers that are not mentioned here.

[1] Note that as the project progresses, several versions of the same test system could be developed and published on this git.

2.1 Transmission test systems

One of the objectives of Task 1.3 was to design a small set of transmission test systems to be used in the remaining of the project. For this, an exhaustive table summarising test systems available in the literature has been built. This table has been made available online[2]. Test systems should satisfy a number of criteria to be used in the project. These criteria are listed in Section 2.1.1. However, it was found that none of the available test systems satisfied all our criteria. So, we selected a few systems that satisfied most criteria and modified/complemented as needed. The selected test systems and their modifications are detailed in Section 2.1.2.

Some honorary mentions are also given in Section 2.1.3. These systems satisfy a majority of our criteria, but they were not modified to satisfy all criteria. They might however be modified and used in future work if needed. Finally, Section 2.1.4 lists large (more than 100 buses) test systems available in the literature. These systems will be used towards the end of the project to assess the scalability of the developed methodologies. It was thus found premature to select (and modify) specific test systems.

2.1.1 Selection criteria

System size First, concerning the size, it is useful to work with different sized systems. We should thus select, for example, a system with less than 10 buses, a system with 10 to 30 buses, another one with 30 to 100 buses, and one with more than 100 buses. Indeed, the 10-bus system can be used to test first ideas and debugging. The 10-to-100-bus systems can be used to test more elaborated methodologies. And the large system(s) can be used for performance and scalability studies.

Available data It is of course more convenient to use test systems for which data are available. In this project, the necessary data are static data (for power flow studies), economic data (for optimal power flows studies) and dynamic data (for stability studies). Other relevant data are reliability data (*e.g.* failure and repair rates, for use in security assessments), load profiles and generation forecasts/meteorological data (for weather-dependent energy sources).

Represents a "real" power system By this, we mean two things. First, electrical elements should represent physical assets. For example, a double line should be represented by two lines in parallel and not by a single line of equivalent impedance. This allows *e.g.* to perform N-1 security assessment. Similarly, generators connected on the same bus should not be replaced by an equivalent generator. Second, knowing the type (nuclear, steam, hydro, wind, etc.) of generators is also useful as it allows to more easily fill missing data if necessary.

Represents a modern grid The system should include renewable generation, distributed energy resources and/or HVDC connections since the CYPRESS project aims to study nowadays and future power grids.

Can be operated in an N-1 secure manner The N-1 criterion still forms the basis of most TSOs' security guidelines. Also, the CYPRESS project aims at developing probabilistic risk management techniques. Applying probabilistic methods on a grid with (important) N-1 security issues would not make sense. Indeed, the most important contributors to the total risk would obviously be the N-1 issues (that typically have a higher probability than N-k issues). Thus, it would be impossible to demonstrate the added value of (more complex) probabilistic methods over deterministic methods.

Node-breaker modeling The system should be available as a node-breaker model. The concept of node-breaker modeling is explained in Section 2.3.2. It is very interesting to work with systems having such topological flexibility because the cyber layer that will be added to these benchmarks needs (among other things) these elements to interact with the physical layer. However, it should be noted that it is complicated to find datasets with node-breaker modeling. That is to say, some papers describe how the authors developed a node-breaker model for a certain system but these data are difficult to find.

Includes distribution Cyber and/or physical events taking place at the distribution grid level can have cyber-physical impacts at the transmission level. Therefore, although the CYPRESS project focuses mainly on transmission, distributions systems are also considered. Systems that include both a transmission and a distribution side are a plus.

[2] `https://github.com/adriengodfraind/CYPRESS`

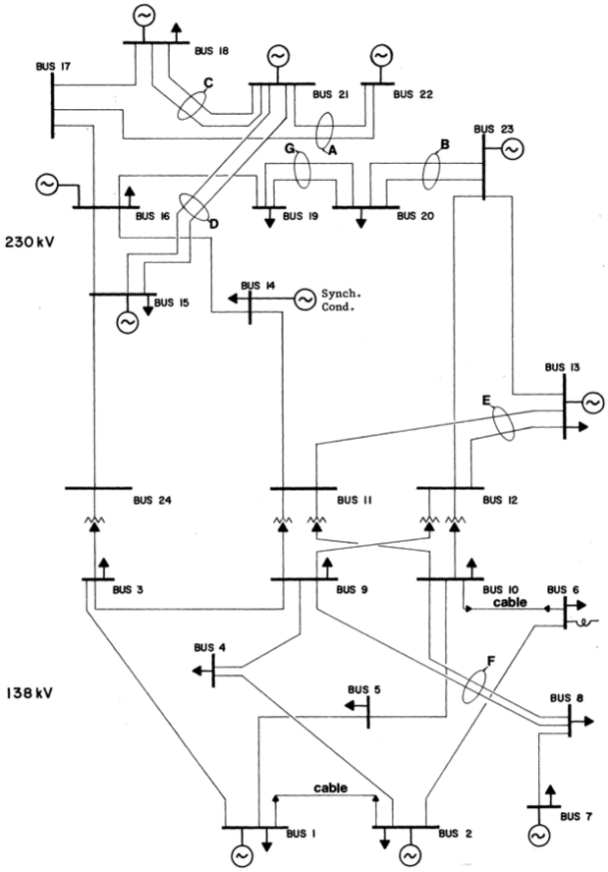


Figure 2.1: IEEE Reliability Test System-1979. [18]

Used in cyber-physical studies Systems that have already been used in cyber-physical studies are given priority.

Multi-area system It is a good idea to select systems divided in several areas so that it can represent several TSOs, even though it is not a restricting criterion since the division can be done by the project members if needed. However, it is an interesting feature.

2.1.2 Selected systems

The systems that satisfied most of the criteria listed above are discussed in this section. These systems were modified/complemented as needed and the following subsections give the reasons for their choice, as well as the adaptations made to them.

2.1.2.1 IEEE Reliability Test System

The first system that was selected is the IEEE Reliability Test System. The IEEE RTS system is mainly used for bulk power system reliability evaluation studies. It allows to analyze power system operations strategies and issues, including unit commitment, economic dispatch, load flow and associated economic and reliability impacts [13]. The main idea behind this system is to enable comparative studies on new reliability techniques (especially in the case of multi-area systems) [14]. The IEEE RTS is also often used for planning studies and studies related to new technologies (*i.e.* renewable integration, HVDC/MTDC systems and electrical vehicles) [15].

Besides the various versions for which data has been slightly adapted to focus on one or another criterion in the different projects using the IEEE RTS, there exist 4 main versions of this system. The first version was published in 1979 and contains 24 buses, as can be seen in Figure 2.1. This version was modestly updated in 1986 with, among other things, its size being doubled by joining two identical RTS-79 models with a tie line [16]. Then, in 1996, a new version was published [17] with the possibility to have 3 areas of interconnected RTS 24-bus systems, as can be seen in Figure 2.2.

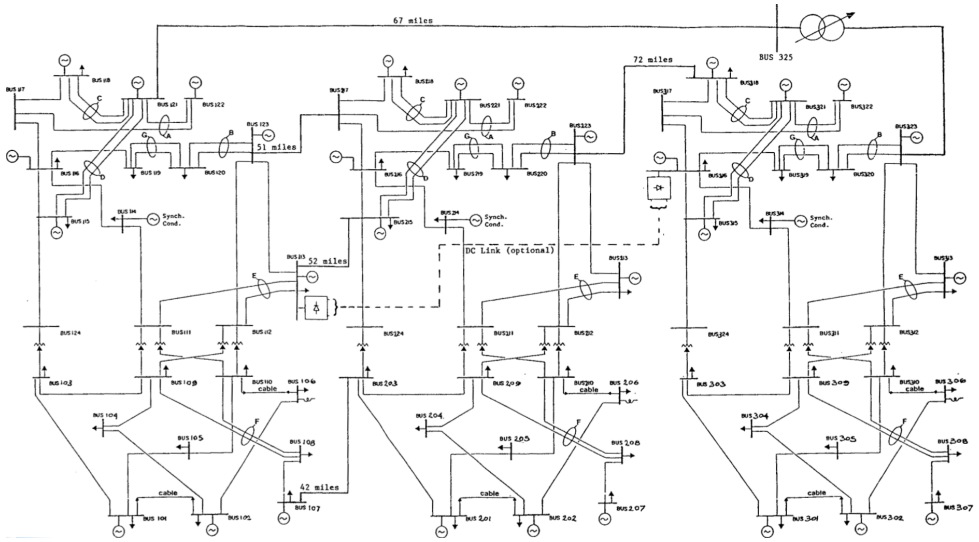


Figure 2.2: IEEE Three Area Reliability Test System-1996. [17]

Finally, the most recent version is the IEEE RTS from the Grid Modernization Laboratory Consortium (RTS-GMLC) [13]. This version is an update of the RTS-96 and was published in 2019. It proposes a generation mix more representative of modern power systems by replacing several coal, nuclear and oil generating units with natural gas generations and by integrating solar and wind generations as well as energy storage. This version also updates load profiles, generators characteristics, etc. Also, it made congestion issues more frequent by removing some lines, reducing some line limits and by slightly increasing the load at some buses [19].

The RTS-GMLC contains 73 nodes, 106 transmission lines and 158 generators (93 synchronous machines, 61 wind and solar plants (31 of which are rooftop aggregates), 3 synchronous condensers and 1 storage unit). Figure 2.3 displays the grid layout of the system, where the three areas can be observed. This layout was mapped to an arbitrary geographical location in order to obtain spatio-temporally consistent wind, solar and load data (with forecasts integrated) [15]. The RTS-GMLC data can be found in the following GitHub repository: `https://github.com/GridMod/RTS-GMLC`.

Reasons to choose this system

This system was chosen because it meets several of the criteria listed in Section 2.1.1.

System size There are 24- and 73-bus versions of this network (single-area and three-area versions). This system is thus both in the 10 to 30-bus system and the 30 to 100-bus system categories.

Available data A lot of data is available for the RTS. These data contain static data, economic data, reliability data (also including the number off days of planned maintenance per year), as well as load and generation profiles (including geographical data to generate new generation profiles). However, some dynamic data are missing. This is discussed later in this section.

Represents a "real" power system The RTS does not contain equivalent lines and generators. Also, the types of each generator is given.

Represents a modern grid As written here-above, there is a very recent version of the system (RTS-GMLC), which takes into account new characteristics of power grids, such as a modern generation fleet.

Can be operated in an N-1 secure manner All versions of the RTS are statically N-1 secure. When adding dynamic data, it should be checked that the system is also dynamically secure.

Node-breaker modeling Two different node-breaker representations have been developed for the 24-bus version of the RTS [20], [21]. Ref. [20] defines the type of configuration (double breaker, breaker-and-a-half and ring buses) of each substations, however, it does not specify how the elements are connected to those

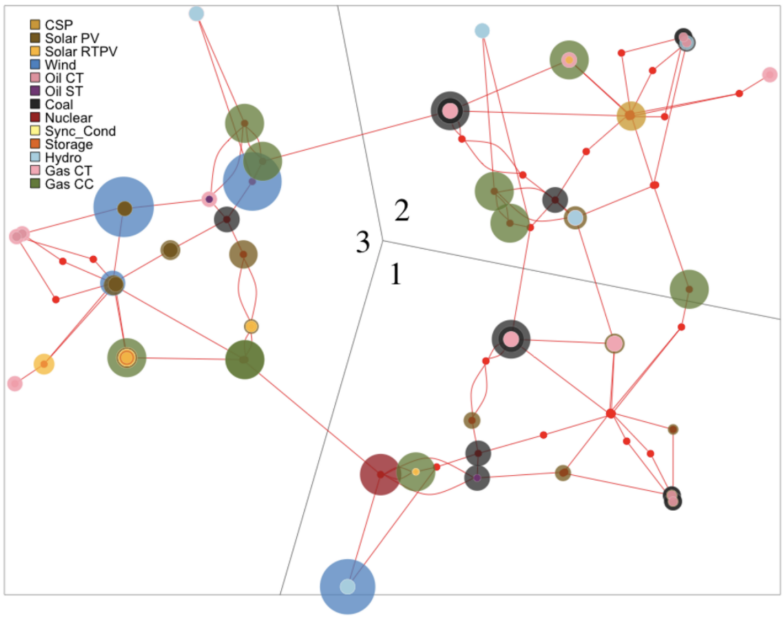


Figure 2.3: Grid layout of the RTS-GMLC, annotated with the relative size and location of RTS-GMLC generation capacity. [13]

substations. Ref. [21] is a relatively old publication, however it fully specifies how elements are connected. It should be noted that these substation configurations have been included in the RTS-96 paper [17]. However, in the discussion of [17], it was noted than those configurations were often unnecessarily complex and unreliable (especially for buses 9 to 12). Modified configurations were however not proposed in the closure to discussion. We thus propose to keep the substation configurations proposed in [20] and to redefine how elements are connected to the substations. This is detailed later in this section.

No node-breaker representation currently exists for the three-area versions of the RTS, but they could be defined relatively easily. Some substation configurations would however need to be adapted to account for the additional lines (interconnections) and decommissioned lines (in the GMLC version).

Used in cyber-physical studies This system has already been used in cyber-physical power system studies. For example, in [22], [23], some researchers develop a benchmark test system for cyber-physical reliability studies by extending buses of the IEEE RTS into substations with ICT features. The example of the cyber system extension for substation 7 is given in Figure 2.4.

Multi-area system Then the IEEE RTS is known to contain three areas, so that it responds to the "multi-TSOs" feature that could be interesting to study. But it is also possible to focus on one area at a time.

Popularity Finally, this system is very popular and widely used in the power system community, so that a large amount of data is available (data that can be found in various versions depending on the studies, so that it is possible to pick the version that is the most relevant with the project's objectives).

Missing features

As detailed above, dynamic data and detailed substations configurations are the only missing feature of the RTS for our project.

Some publications added dynamic data to the RTS-96. For example, Ref. [14] proposed a dynamic model of the RTS-96 and implemented it using SimPowerSystems, a Simulink library for power systems. It modelled exciters with IEEET1 models, steam governors with IEEEG1 models (with an optional four-mass model for the governor shaft), and hydro governors with IEEE GOVHYDRO1 models. The same parameters are used for all controllers of a same type. Power system stabilisers (PSSs) are added to all generators, but are not tuned (*i.e.* all PSSs have the same parameters) which is unrealistic. Ref. [24], [25] proposed an alternative dynamic model of the RTS-96 based on [26]. Such a dynamic model was implemented in Eurostag in [27]. Three different sets of parameters are used for synchronous machines of thermal generators (one for oil, one for coal, one for nuclear), and a

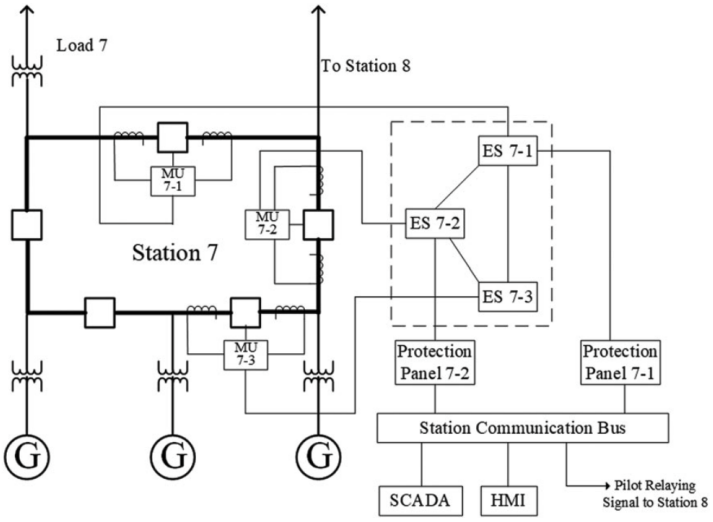


Figure 2.4: Cyber-system extension for substation 7 of the IEEE RTS. [23]

single set of parameters is used for synchronous machines of hydro generators. All generators are equipped with simplified AC4A excitation systems. Regarding turbine-governor systems, two different models are used for thermal units (one for large units and one for small units), and a single model is used for hydro units.

Dynamic data for the RTS-GMLC does however not yet exist. So, new data has to be added to model the more modern generators, *i.e.* for gas, wind and solar.

Adding system dynamic data

Dynamic data for thermal and hydro units of the RTS-GMLC can be directly taken from [24]–[26]. However, dedicated dynamic models will have to be developed for wind and solar (considering both rooftop and concentrated installations) generators.

Adding detailed substation configurations

As discussed above, Ref. [20] proposed substation configurations (double-breaker (2-B), breaker-and-a-half (B-1/2) and ring substations) for the RTS-79 but did not detail how lines and generators are connected to those substations. Ref. [21] also proposed substation configurations for the RTS-79, but those were unrealistic (unnecessarily complex and unreliable). We thus keep the configurations proposed in [20] and specify how elements are connected using the following rules listed in decreasing order of priority.

- In B-1/2 substations, generators and lines are mixed when possible. In other words, the "shared breakers" are connected to one line and one generator instead of being connected to two generators for example.
- When this is not possible (*i.e.* there are more lines than generators), double lines share a common breaker.
- Loads are assumed to be connected via two redundant transformers. In B-1/2 substations, the transformers share a common breaker. In ring substations, the transformers are placed in adjacent slots. For 2-B substations, placement does not matter.
- Loads are connected last.
- Elements are placed in alphanumerical order. For B-1/2 substations, the order is (i) above shared breaker 1, (ii) below shared breaker 1, (iii) above shared breaker 2, etc. For ring substations, elements are placed clockwise.

Additionally, to limit the differences between the different versions of the RTS (GMLC vs 96, and one- vs three-area), the following hypothesis are made.

- Solar and wind sources are connected via the distribution transformers. Due to their large size (around 800 MW each), the wind farms at buses 122, 303 and 317 are connected to the high-voltage side in a 2-B arrangement.
- Interconnections are connected to substations in a 2-B arrangement.

Table 2.1: Definition of the breaker-and-a-half substation configurations in the one-area RTS. Note that line L11-13 is removed in the GMLC version.

BUS	Shared breaker #								
	1		2		3		4		5
1	G1	L1-2	G2	L1-3	G3	L1-5	G4	/	/
2	G1	L1-2	G2	L2-4	G3	L2-6	G4	/	/
3	L1-3	L3-9	L3-24	/	/	/	/	/	/
9	L3-9	L4-9	L8-9	L9-11	L9-12	/	/	/	/
10	L5-10	L6-10	L8-10	L10-11	L10-12	/	/	/	/
11	L9-11	L10-11	L11-13	L11-14	/	/	/	/	/
14	G1	L11-14	L14-16	/	/	/	/	/	/
15	G1	L15-16	G2	L15-21-1	G3	L15-21-2	L15-24	/	/
16	G1	L14-16	L15-16	L16-17	L16-19	/	/	/	/
17	L16-17	L17-18	L17-22	/	/	/	/	/	/
18	G1	L17-18	L18-21-1	L18-21-2	/	/	/	/	/
21	G1	L21-22	L15-21-1	L15-21-2	L18-21-1	L18-21-2	/	/	/
23	G1	L12-23	G2	L13-23	G3	L20-23-1	G4	L20-23-2	G5

Table 2.2: Definition of the ring substation configurations in the one-area RTS.

Bus	Element			
	1	2	3	4
4	L2-4	L4-9	/	/
5	L1-5	L5-10	/	/
6	L2-6	L6-10	/	/
8	L7-8	L8-9	L8-10	/
12	L9-12	L10-12	L12-13	L12-23
19	L16-19	L19-20-1	L19-20-2	/
20	L19-20-1	L19-20-2	L20-23-1	L20-23-2
24	L3-24	L15-24	/	/

- The substation configurations in the three zones of the RTS are identical.

Based on these rules and hypothesis, detailed substation configurations can be derived. Tables 2.1 and 2.2 respectively give the detailed configurations of the B-1/2 and ring substations for the one-area RTS. The three-area version can easily be extrapolated from the above hypotheses. Substations 7, 13 and 22 are 2-B substations and are thus not further detailed. Note that for brevity, the load transformers are not included in the tables.

2.1.2.2 Roy Billinton Test System

The second system that was selected to go further is the Roy Billinton Test System (see Figure 2.5). This system is a well-known test system developed at the University of Saskatechewan by Prof. Roy Billinton for educational and research purposes [28]. It has been used for a wide range of reliability studies associated with planning, operation and inclusion of new technologies in the power grid. It contains 6 buses including 2 generator buses, 5 load buses, 9 transmission lines and 11 generating units (connected to the 2 generator buses) for an installed capacity of 240 MW and a peak load of 185 MW. In the original version, the generating units consist of 5-MW, 20-MW and 40-MW hydro power plants and 10-MW, 20-MW and 40-MW thermal power plants. The original version is provided with power flow data, reliability data and cost data [15], [29].

The RBTS was extended (twice) by its authors to include distribution systems. The first time in [30] (1991), they selected 2 load buses (buses 2 and 4) and designed distribution systems for each while in [31] (1996), they extended buses 3, 5 and 6 by developing the necessary distribution and sub-transmission systems. The resulting system can be seen in Figure 2.6.

Reasons to choose this system

This system was chosen because it meets several of the criteria listed in Section 2.1.1.

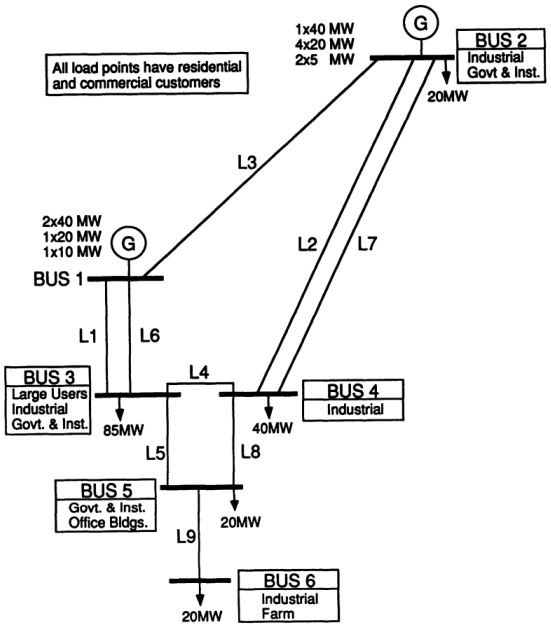


Figure 2.5: Single-line diagram of the Roy Billinton Test System (first version, 1989). [28]

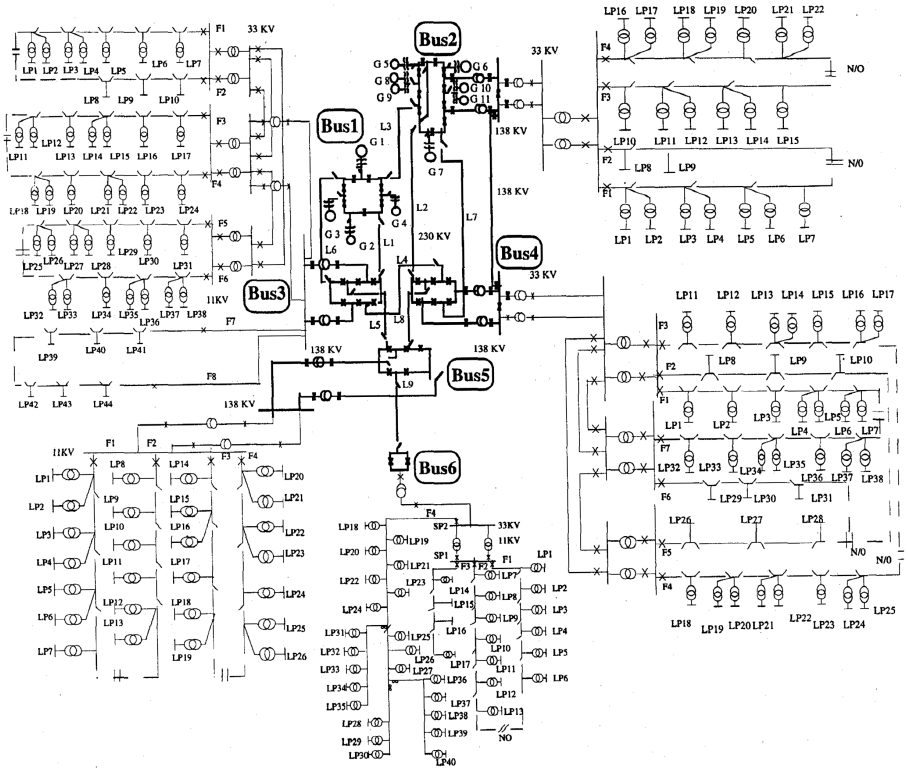


Figure 2.6: Complete single-line diagram of the RBTS (1996). [31]

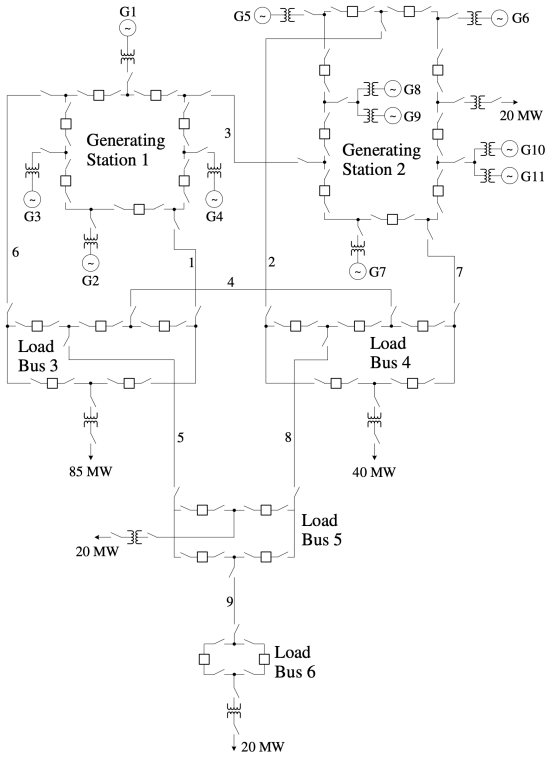


Figure 2.7: Extended single-line diagram of the RBTS. [32]

System size First of all, the idea was to select systems of different sizes and to have at least one system containing less than 10 buses, the version without distribution of the RBTS contains 6 buses, which answers this idea.

Available data Similarly to the RTS, a lot of data is available for the RBTS. These data contain static data, economic data, reliability data, and load and generation profiles. There are however no dynamic data. These have been added as discussed later in this section.

Represents a "real" power system The RBTS does not contain equivalent lines and generators. Also, the types of each generator is given.

Can be operated in an N-1 secure manner Similarly to the RTS, the RBTS is statically N-1 secure (except that bus 6 is lost after the loss of line 9). When adding dynamic data, it should be checked that the system is also dynamically secure.

Node-breaker modeling There is no node-breaker version of the RBTS as such, however in the first paper describing the system the authors propose an extended version with station configurations for the load and generator buses. These station configurations include circuit breakers and can be seen on the extended single-line diagram in Figure 2.7. This extension is provided with station equipment data (reliability data such as failure rate, outage duration, maintenance time, ...) [29]. Furthermore, in the distribution systems developed in [30], [31], all breakers are identified.

Includes distribution As stated here-above, the RBTS has been extended by its creators in order to include distribution. According to them, the RBTS extended with distribution systems in [31] has all the main facilities, such as generation, switching stations, transmission, sub-transmission and radial distribution systems found in a practical system[3]. It also contains four voltage levels: 230, 138, 33 and 11 kV.

[3]Note that this paper is from 1996. Therefore, it may not have all the main facilities found in practical systems of today and may need to be adapted (especially by integrating DERs).

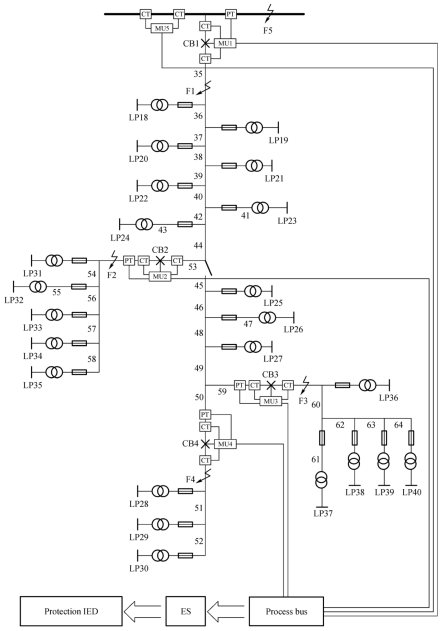


Figure 2.8: Architecture of IEC 61850 for RBTS. [33]

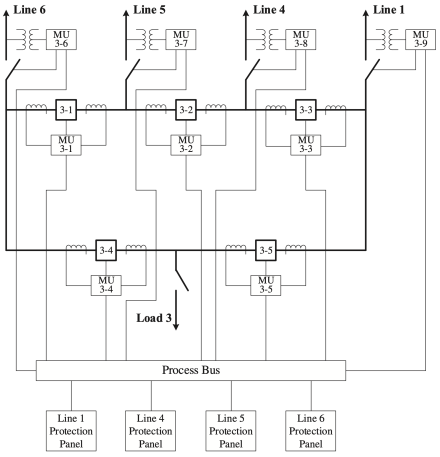


Figure 2.9: The protection system for bus 3 of the RBTS. [32]

Used in cyber-physical studies The RBTS has already been used in cyber-physical power system studies. In [33], they use the RBTS to demonstrate and implement a technique for reliability evaluation of modern substation and distribution systems. To do so, they use the 1996 version of the RBTS, *i.e.* the version from [31] with each bus (except bus 1) having been extended with a distribution or sub-transmission system. They decided to develop an IEC 61850 based protection system on the main feeder line 4 of bus 6. It is composed of circuit breakers, Merging Units, Ethernet Switches and protection IEDs (designed based on the IEC 61850 standard), as can be seen in Figure 2.8. In [32], H. Lei and C. Singh (*i.e.* the authors of [22], [23]) propose a methodology for considering the effect of cyber-malfunctions in substations on power system reliability. In order to do this, buses 3, 4 and 5 of the original RBTS are extended to include detailed substation protection system configurations with modern architecture (see Figure 2.9 for bus 3 extension).

Finally, it is a well known test system and a reference for several reliability studies in the literature.

Missing features

A disadvantage of the RBTS is that it does not really represent a modern system, it does not contain renewable energy, power electronics-based generation or HVDC lines and concerning the distribution, 1991 and 1996 versions do not include any distributed energy resources. However, for the moment, no CYPRESS member plans to use a modified version of the RBTS with renewable generation at the transmission level in the context of the project. The primary goal of the RBTS is to perform first simulations, methodology tests, etc. on a system where results are easy to interpret. Thus, it is not critical to have a complete modern version of this system and we did not do the work of adapting it during the task.

Concerning the dynamic data, no work on the dynamic aspects of power grids was found using the RBTS as a test system, and therefore no extension of the system with dynamic data was found. We therefore did the work of adding the dynamic data, as explained in the following section.

Adding system dynamic data

The following general procedure has been followed to add dynamic data to the RBTS. First, add generic dynamic data to all generators. If the generation type (nuclear, gas, wind, etc.) is known, slightly less generic data can be used. Second, verify that the system is (dynamically) N-1 secure.

More specifically, the following dynamic data have been added to the RBTS. Synchronous generators are represented with a "four winding" model[4] (one field winding, one d-axis damper winding and two q-axis damper windings). Excitation systems are represented by an IEEET1 model, and the governor is represented with BPA

[4] We do not recommend a specific saturation model as this usually depends on the software used.

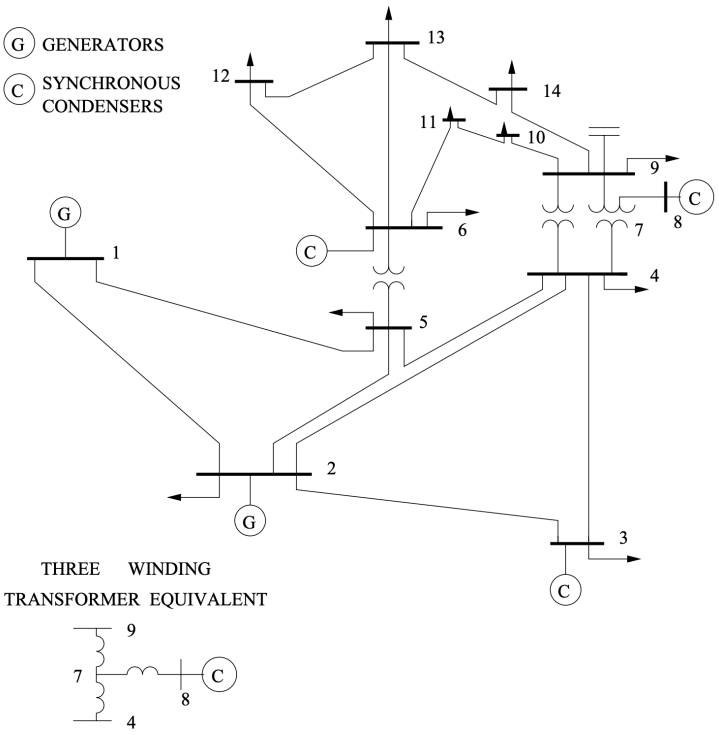


Figure 2.10: IEEE 14-bus system. [36]

GG (also known as WSCC type G) model as in [34]. A different turbine-governor model is however used for hydro units as they have a fundamentally different behaviour than other types of units. The model used is a GOVHYDRO1 model. Most parameters are taken from annex D of [35]. This annex contains typical data for different types of machines (hydro, nuclear, coal, gas) and a wide range of rated powers (5 MW to 1.3 GW). So, for each generators of the test systems, parameters were taken from a machine in [35] that has the same type and that has the closest rated power. For hydro units, those parameters are completed with the ones in [26].

2.1.3 Honorary mentions

At the time of the writing of this report, the systems listed in Section 2.1.2 were deemed appropriate for most studies expected to be performed in the project. This section however lists other test systems that satisfy a large portion (but not all) of our criteria, and might thus be used in the future. Similarly to the previous section, we give for each system its advantages and the criteria that are not satisfied. But contrarily to the selected systems, these systems were not modified to satisfy the criteria.

2.1.3.1 IEEE 14-bus system

The IEEE 14-bus test system represents a portion of the American Electric Power System (in the Midwestern US) as of February 1962. As can be seen in Figure 2.10, it consists of 14 buses, 21 lines, 3 transformers and 5 generators with exciters and Automatic Voltage Regulators [36].

The most common application with this system is state estimation (*i.e.* studies related to state estimation methods, PMU placement, data processing) but it is also the most used system for protection studies (protection system coordination, fault detection, short circuit analysis) and for cyber-security studies. Furthermore, it is the second most used system for control studies (voltage and frequency control, hierarchical microgrid and smart grid control, distributed and decentralized control, Automatic Generation Control (AGC)) and it has been used for other types of studies as well [15].

Reasons to choose this system

This system meets several of the criteria listed in Section 2.1.1.

Available data The IEEE 14-bus test systems includes the most important data, *i.e.* static and dynamic data. The original version does not include dynamic data, but they are available in [37], [38]. Moreover, according to [15], the system has been used in 16% of stability studies (transient, angular, frequency or voltage) from IEEE Transactions journals' papers. This test system however does not include other data such as economic data, load profiles and reliability data.

Represents a "real" power system In the IEEE 14-bus test system, parallel lines and generators are replaced by equivalents. However, the type of each generator (steam, gas, hydro or nuclear) is well defined. It can be noted that only 2 out of the 5 synchronous machines are generators. The others are synchronous condensers. Such large proportion of synchronous condensers is quite unusual.

Can be operated in an N-1 secure manner The IEEE 14-bus test system is statically N-1 secure. We did not check whether the dynamic data proposed in [37], [38] lead to a dynamically secure system.

Node-breaker modeling This system has already been modified in some research works to obtain a node-breaker version. In [39] they extend 2 buses into substation with node-breaker modeling. The system is also extended in [40], where the author builds on the expansion done in [41], which consists in using some of the typical substation topologies (ring bus, double breaker, breaker-and-a-half and transfer bus configurations) to expand each bus.

Used in cyber-physical studies It has already been used in cyber-physical power system studies, including studies concerning cyber-attacks. Indeed, in [42], they have developed a cyber-power modeling and simulation testbed to analyze the impact of cyber events on the power grid and they used the IEEE 14-bus system to simulate 3 cyber-attack case studies (Communication line outage, DoS and Man-in-the-Middle). In [43], they propose countermeasures to detect 2 kinds of Coordinated Cyber-Physical Attacks and demonstrate the implementation of CCPAs in smart grid and the effectiveness of countermeasures on several IEEE test systems, including the 14-bus. It is also used in several other CPPS studies. In [44], the authors introduce a model for a cyber-physical power system, based on the IEEE 14-bus system, that includes (the CPPS model) the cyber, control, and corporate IT subsystems.

Popularity The IEEE 14-bus system is one of the most widely used systems in the power system field, making it a trustworthy benchmark system. Indeed, the authors of [15] claim that it is the third most used system for power system studies after having analyzed almost 2500 related journal papers (from IEEE Transactions on Power Systems, on Power Delivery, on Energy Conversion, ...) released between 1986 and 2019.

Missing features

Originally, the IEEE 14-bus system does not contain "modern" elements. However it is possible to add them, as has been done in [45], where renewable energy sources are added to the system. They did this to test their developed framework to evaluate the voltage instability sensitivities of power system buses to increase in renewable energy (RE) penetration.

2.1.3.2 New England 39-bus test system

The IEEE 10-generator 39-bus test system, or New England test system, is an approximate representation of the New England 345 kV system [46]. This system, that can be seen in Figure 2.11, consists of 39 buses, 19 loads and 10 generators, with one of these generators that represents the aggregation of a large number of generators. It is broadly used for small signal stability studies and dynamic stability analysis. Actually, it is the most used system for stability analysis according to [15]). It is also used in planning and control studies and in studies that include new technologies [15]. Note that according to [47], the New England test system has already been equipped with a protection system and used to study the impact of hidden failures on cascade propagation and to demonstrate intelligent control techniques for vulnerability assessment.

Reasons to choose this system

Available data The IEEE 39-bus test systems includes the most important data, *i.e.* static and dynamic data. The original version of the IEEE 39 system includes dynamic data of the generators with exciters but without governors. Ref. [37] proposed a new set of data that includes governors and more modern exciter models. This test system however does not include other data such as economic data, load profiles and reliability data.

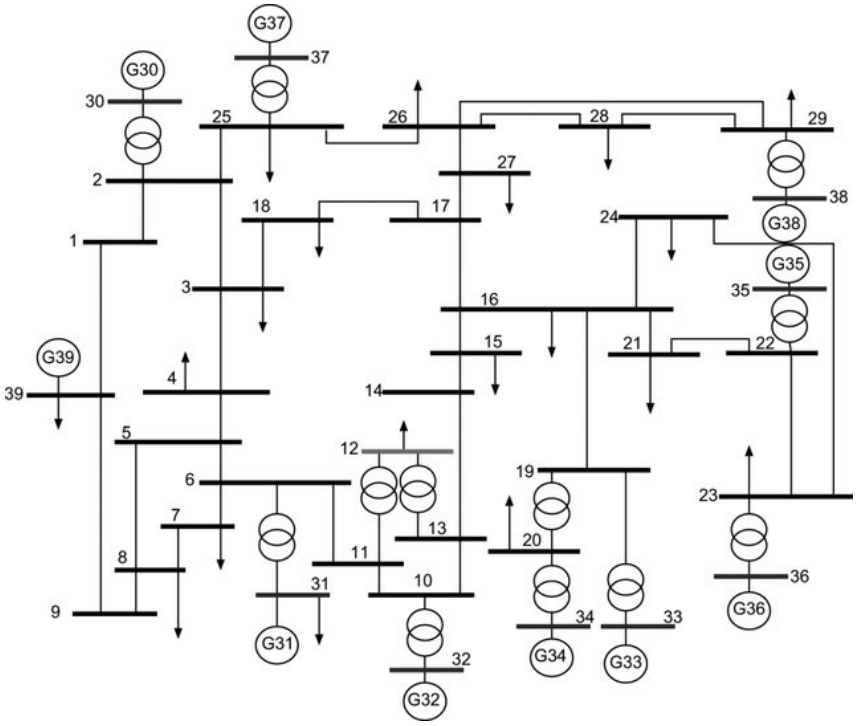


Figure 2.11: Single-line diagram of the New England 39-bus test system. [48]

Represents a "real" power system In the IEEE 39-bus test system, parallel lines and generators are replaced by equivalents. However, the type of each generator (steam, gas, hydro or nuclear) is well defined.

Can be operated in an N-1 secure manner The version of the IEEE 39-bus test system proposed in [37] is not dynamically secure. Indeed, an important difference this version and the original lies in the generator connected to bus 39. In the original version, bus 39 is an equivalent of a neighbour system (the New York Power System (NYPS)), so the generator is an equivalent a many remote generators and thus has a very high inertia. In the new version, it represents a classical generator with a typical inertia. This causes the new version to be N-1 insecure. Indeed, the loss of a single generator can cause the frequency to drop below the first under-frequency load shedding threshold. We thus recommend to use the new version (that is more complete and more modern), but to keep the old inertia value[5].

Also, the test system is not secure against the loss of line 16-19. Indeed, the loss of this line creates a small island (composed of buses 19, 20, 33 and 34) that can easily collapse. A possible solution to this issue is to replace line 16-19 by a double line.

Used in cyber-physical studies The IEEE 39-bus test system has already been used in studies of cyber-physical power systems. In [49], the test system is used to demonstrate a cyber attack scenario on the *Smart City Testbed* of Washington State University. It is also used by the authors of [50] to analyze the performance of cyber-physical power systems under cyber attacks. In this work, the system was partitioned into 3 regions with each region monitored and operated by a control center and the control centers being interconnected through optical network and cooperating to estimate the state and to asses the functionality of the whole CPPS.

Popularity The New England test system is a well known system that is a popular choice for IEEE working groups' reports and is part of the most used systems in power system studies [14], [15].

Missing features

Originally, the system does not contain elements found in current systems, such as renewable energy. However, some have incorporated these types of generation into the system for their respective studies. For instance in

[5]Some other comments regarding [37]: the rated power of generators 38 and 39 are inconsistent with the load flow results (e.g. generator 39 produces 1000 MW but has a rated power of 911 MW). Also, the loss of generator 38 causes the frequency to drop below 49 Hz (or 59 Hz in a 60 Hz-system). Using a droop of 10% instead of 5% can alleviate this issue.

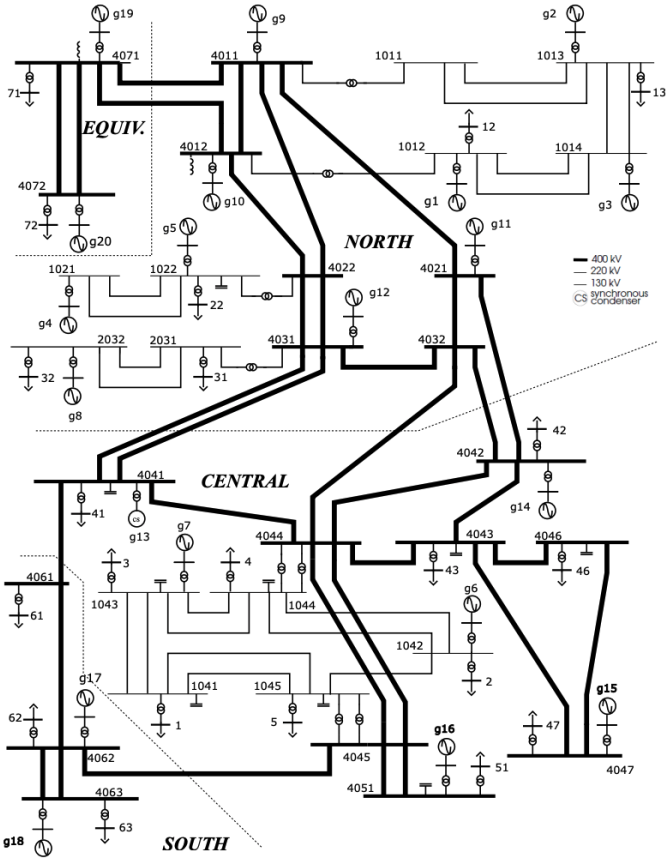


Figure 2.12: Single-line diagram of the Nordic test system. [58]

[45], in addition to doing this for the IEEE 14-bus system, they added renewable energy sources to the New England test system. Another example can be found in a set of papers [51]–[55], where the authors propose three versions of the IEEE 39-bus system dynamic model to study the fundamental dynamics of modern power grids in the presence of power electronics interfaces. In addition to using data from the system dynamics, their papers (as well as the associated summary report and repository) propose a modern version of the system. Indeed, in 2 of the 3 proposed versions, elements such as wind turbines and an energy storage system connected to a voltage source converter are introduced.

Concerning the multi-area criterion, as stated in Section 2.1.1 describing the selection criteria, the division can be done by the project members if needed. Originally, the New England 39-bus test system does not contain different regions, but in the cyber-physical study [50] described briefly in the corresponding paragraph above, they divided the system into 3, giving an idea of what could be done if needed in the CYPRESS project.

2.1.3.3 Nordic Test System

The Nordic test system is a fictitious system that has similarities with the Swedish and Nordic power grids and that has been developed for voltage stability studies by the IEEE PES Task Force on "Test Systems for Voltage Stability Analysis and Security Assessment" [15], [56]. This system, that is displayed in Figure 2.12, is an upgrade of the former so-called Nordic 32 test system ([57]) in which dynamic models and parameters were adjusted to make them more representative for voltage stability studies. It has been mainly used to study various aspects of voltage instability, including contingency evaluation, voltage security assessment, instability detection and emergency control, but also for new technology studies [15], [58].

The Nordic test system contains 74 buses, 52 lines, 19 generators, 1 synchronous condenser, 22 loads at distribution level and 11 (switched) shunts. Each generator is equipped with Automatic Voltage Regulator, Power System Stabiliser and Over-Excitation Limiter models while each load is controlled by the Load Tap Changer of its distribution transformer [59]. The models used are those already found in short-term dynamic studies. They are complemented with an appropriate representation of load power restoration (under the effect of automatic load tap changers and/or thermostatic load control), over-excitation limiters, and discrete controls triggered by

voltage drop (such as automatic switching of shunt compensation, modified load tap changer control, or undervoltage load shedding). The system consists of 4 areas: *North* with hydro generation and some load, *Central* with much higher load and thermal power generation, *Equiv* connected to *North* (includes a very simple equivalent of an external system) and finally *South* with thermal generation and which is rather loosely connected to the rest of the system [58].

Reasons to choose this system

This system meets several of the criteria listed in Section 2.1.1.

Available data The Nordic test systems includes the most important data, *i.e.* static and dynamic data. Indeed, since its first publication, the system has been accompanied by data on the dynamics of its components as it is originally intended for transient stability and long term dynamic simulations[6]. Note that it is supposed to have similar dynamic properties to the Swedish and Nordic power grids. In addition, the new version [58] has adjusted the dynamic models and parameters to be more representative of modern power systems. The Nordic test system however does not include other data such as economic data and load profiles (although it provides two possible operating points), nor reliability data.

Represents a "real" power system The Nordic test system does not contain equivalent lines, but generators connected to the same buses are replaced by equivalents. Also, the types of each generator is given.

Can be operated in an N-1 secure manner The Nordic test system is statically and dynamically secure.

Includes distribution As written above, the system involves some distribution buses. Nevertheless, the problem is that the distribution grids are represented as aggregated loads in this model. Fortunately, there exists a toolbox called *TDNetGen* that is able to generate a complete combined Transmission & Distribution system using the Nordic Test System and replacing these aggregated loads with detailed distribution grid models [60]. This toolbox is described in more detail in Section 2.2.1.4 below.

Used in cyber-physical studies The following work on CPPS using the Nordic32 test system (*i.e.* the "old" version) could be found. In [61] the authors study a model-based approach to assessing the cyber-risks in a cyber-physical system. They provide some results concerning a quantitative assessment of cyber-risks in such systems and in order to do that they use the Nordic32 extended with measurement, protection and control, all in compliance with the standard IEC 61850 for interoperable substations. The complete model used in their study can be found in an archive[7]. This archive contains a high-performance agent-based simulation engine used for stochastic simulation of complex cyber-physical systems as well as the set of models (*json* files) related to the Nordic32 extended with a models of SCADA and substations instrumentation/measurement, compliant with IEC 61850.

Multi-area system As stated above, the Nordic 32 test system is composed of 4 areas, with each area having different characteristics such as different generation types and more or less loads. This division can be observed on the single-line diagram of Figure 2.12.

Missing features

Some components and controls were not considered by the Task Force that upgraded the Nordic system [58]. Among other things, they say that the models of important components could be considered in future extensions such as: alternative Over-Excitation Limiter models, HVDC links, (converter-interfaced) generation distributed in distribution grids, etc. Nevertheless, the models have been extended in some studies to cover other dynamic phenomena and consider modern grid elements [58]. For example, in [59], they replace synchronous generators of the Nordic Test System by aggregated solar-PV systems in order to investigate the impact of solar-PV generation on Long-Term Voltage Stability. In [62] they study the optimization of both the placement and controller parameters for Battery Energy Storage Systems to improve power system oscillation damping and they use the Nordic Test System (and the New England 39-bus system) to do that. In [63], the impact of greater penetration level of renewable energy sources, *i.e.* of inverter-based generation, is investigated regarding the system dynamics (with a focus on voltage stability). To do so they modify the Nordic Test System

[6] It thus includes on-load tap changers (OLTCs) and overexcitation limiters (OXLs) that are usually not found in other test systems.
[7] `https://openaccess.city.ac.uk/id/eprint/19330/`.

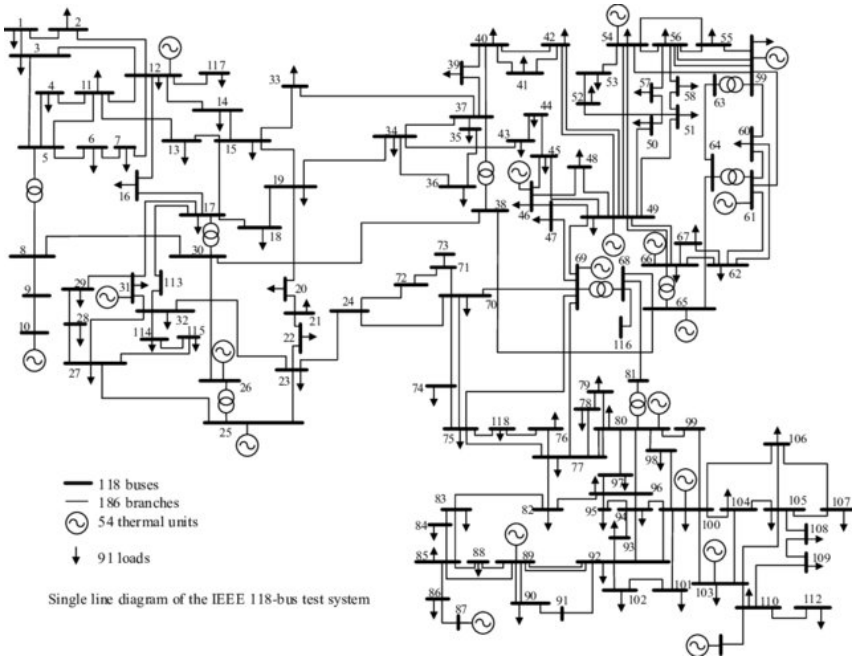


Figure 2.13: IEEE 118-bus system. [65]

in order to achieve a share of 35% of renewable sources and thus a 35% share of power electronics. Another example of a study that modified the system to incorporate modern grid elements is found in [64], where they add wind generation and HVDC links in order to apply and compare two control methods for HVDC frequency support.

2.1.4 Large transmission test systems

As mentioned above, it was decided to select at least one large (more than 100 bus) system in order to allow performance and scalability tests further in the project and to highlight certain aspects that would not be observable on small and medium-sized systems. Three systems are briefly described in this section. The idea was to start by listing the trustworthy systems that are widely used by the power systems community and for which a fair amount of reliable data was available. The choice of a (or several) specific system(s) will be done later in the project.

2.1.4.1 IEEE 118-bus system

The IEEE 118-bus test system represents an approximation of a portion of the American Electric Power System (in the Midwestern US) as of December 1962. It consists of 118 bus, 19 generators, 35 synchronous condensers, 186 branches, 9 transformers and 91 loads as can be seen in Figure 2.13.

According to the power system literature, the IEEE 118-bus has mostly been used in planning studies but also a lot in state estimation studies. It has also been used in cyber-security studies [15]. For example, as mentioned in Section 2.1.3.1, the authors of [43] propose countermeasures to detect 2 kinds of Coordinated Cyber-Physical Attacks and demonstrate the implementation of CCPAs in smart grid and the effectiveness of countermeasures on several IEEE test systems, including the IEEE 118-bus.

There is a modified version of this system that includes dynamic data and which contains 54 synchronous machines equipped with IEEE type-1 exciters [37], [38]. This version contains 172 buses, 185 transmission lines, 76 transformers and 91 constant impedance loads.

Note that there is also an "European version" of the IEEE 118 [66], [67]. In this version, the system was modified in accordance with European standards such as a 50 Hz nominal frequency as well as the use of conventional voltage levels and conductor dimensions.

Figure 2.14: South Carolina 500-bus system. [6]

2.1.4.2 ACTIVSg500 (South Carolina)

As a second system of larger size, it was decided to select the ACTIVSg500 system in order to be able to test future tools on a system of even larger size than the previous one. This test system, also known as the *South Carolina 500-Bus system*, was developed as part of the US ARPA-E[8] GRID DATA research project [68] and designed by algorithms described in [69]. Indeed, this system is entirely synthetic and was built from public information and a statistical analysis of real power systems in order to be statistically similar to real transmission system models but without modeling any actual lines. It does not represent the actual South Carolina grid but its generation and load profiles are similar to those in that region.

This system, represented in Figure 2.14, contains 56 generators, 597 transmission lines and 200 load. Furthermore, it is provided with dynamic generator data and generator cost data for optimal power flow studies.

2.1.4.3 ACTIVSg2000 (Texas)

The last large transmission test system that is proposed is the largest of the selection, *i.e.* the ACTIVSg2000 test case. As it was the case for the ACTIVSg500 system, this 2000-bus power system test case is entirely synthetic, was developed as part of the US ARPA-E GRID DATA research project [68] and designed by algorithms described in [69]. This system is built on the footprint of Texas, it contains 1500 substations as well as 287 lines at 345 kV and 1813 lines at 115 kV. The case includes power flow data but also parameters for transient stability and geomagnetic disturbance studies.

In [70], the authors have modelled the communication infrastructure of this synthetic grid to create a complete cyber-physical model of the power system. Their communication model is based on information gathered from the synthetic power grid model as well as network topologies used in substations, utility control centers and balancing authorities such as the Electricity Reliability Council of Texas.

2.2 Distribution test systems

As mentioned in Section 2.1.1, cyber and/or physical events in the distribution grid can have impacts at the transmission level. This is why, although the CYPRESS project focuses mainly on transmission, distributions systems are also considered. After looking at whether the transmission test systems had already been extended with distribution, we took a look at existing distribution test systems in the literature that could be integrated with the selected transmission systems.

[8]Advanced Research Projects Agency - Energy

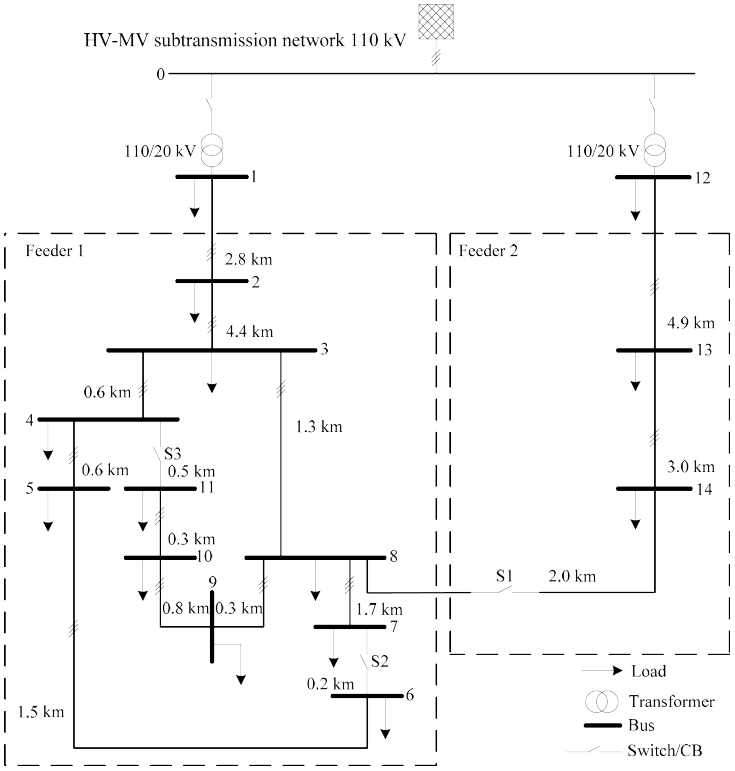


Figure 2.15: Single-line diagram of the CIGRE MV benchmark system - No generation. [79]

This section begins by proposing some interesting distribution test systems. After that, it concludes with a more detailed presentation of the work done by *N. Pilatte, P. Aristidou and G. Hug* [60] on the Nordic Test System to create combined transmission and distribution systems.

Note that besides the systems mentioned in this section, there are other systems that might be of interest. Examples include the IEEE Test Feeders developed by the Test Feeder Working Group of the Distribution System Analysis Subcommittee [71], [72], the power system models provided in the United Kingdom Generic Distribution System collection [73], the Electric Power Research Institute test circuits [74], but also the systems developed in the SimBench project [75]–[77].

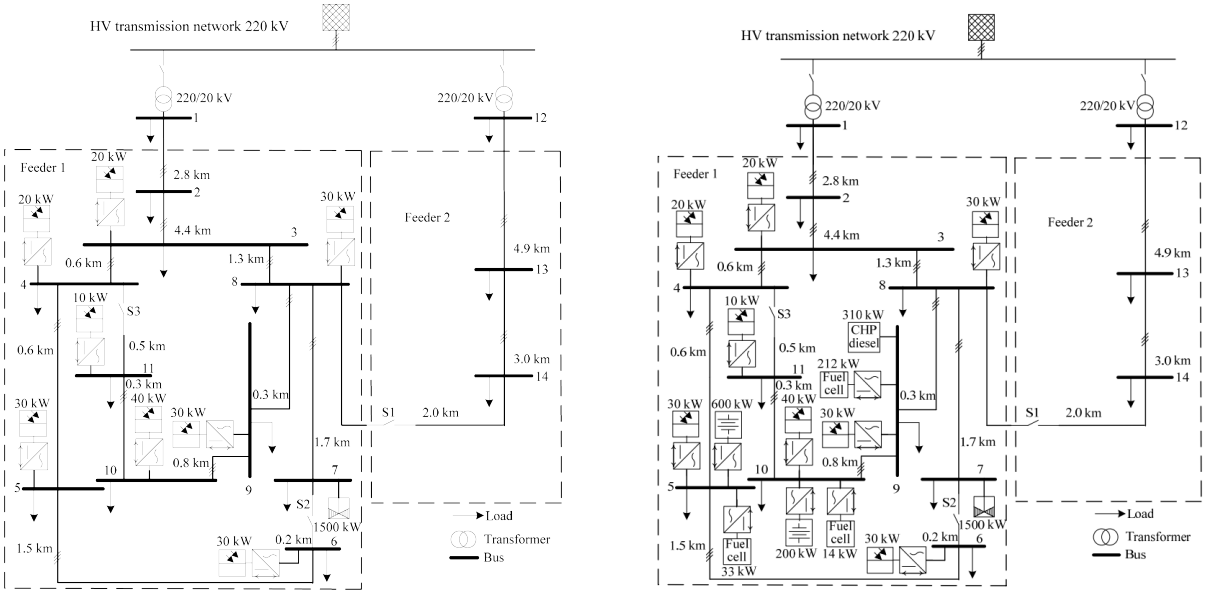
2.2.1 Selected systems

2.2.1.1 CIGRE MV System

The CIGRE Task Force C6.04.02 has developed three benchmark grids in order to deal with studies mainly concerned with the Distributed Energy Resources (DER) integration in electric power systems. Their purpose is to facilitate the analysis and validation of new methods and techniques aiming to enable the economic, robust and environmentally responsible integration of DER [78], [79]. Among these systems, there is a medium voltage system to represent distribution, it can be seen in Figure 2.15. The latter is derived from a real MV system in southern Germany supplying a small town and the surrounding rural area. When creating the MV benchmark system, this real system was adapted to become more user friendly and flexible while keeping its original realistic character [80].

As can be seen, the system is composed of 2 feeders operating at 20 kV that connect the 220 kV (sub-)transmission grid to the 14 buses MV system via transformers. Switches[9] S1, S2 and S3 enable to change from a meshed to a radial grid. Finally, DER can be added at any node of the system and different types of DER can be added such as PVs, residential fuel cells, wind turbines, CHP diesel and CHP fuel cells [80]. *Pandapower*'s documentation proposes 3 versions of this MV benchmark: the version depicted in Figure 2.15, without generation, that shown in Figure 2.16a, with 8 PV generators and 1 wind turbine and finally the version of Figure 2.16b

[9]Note that in the remainder of this document, the term "disconnector" will be preferred to "switch" when referring to a device that is used to completely de-energized an electrical circuit for service or maintenance. The term "switch" will be used to refer to the network component discussed in Chapter 3.



(a) With PV and wind.

(b) With all DER.

Figure 2.16: Single-line diagram of the CIGRE MV benchmark system with DER. [79]

containing all DER, *i.e.* 8 PV generators,1 wind turbine, 2 batteries, 2 residential fuel cells, 1 CHP diesel and 1 CHP fuel cell.

2.2.1.2 CIGRE LV System

In addition to the MV grid described above, the CIGRE Task Force C6.04.02 has also developed a LV system [78], [79], the single-line diagram of which is shown in Figure 2.17. As can be seen from the diagram, the LV system is connected to the 20 kV medium voltage grid via 3 feeders. These feeders divide the LV grid into 3 radial sub-systems of 400 V, a residential sub-system, an industrial sub-system and a commercial one.

Note that the CIGRE Task Force C6.04.02 has also developed a high voltage system. The latter can easily be combined with the above-described distribution systems for a complete study. The pandapower code [79] can be used to generate all 3 test systems.

2.2.1.3 SimBench's semi-urban MV system

The third distribution test system that was selected, and which may be added to the transmission later in the project, comes from the SimBench's dataset [75], [76]. More precisely, it is the SimBench's semi-urban MV system, that can be seen in Figure 2.18. This system, with a rated voltage of 20 kV, consists of 120 buses and 118 lines and is connected to the high voltage grid via a single substation. The grid has a high penetration of photovoltaic and wind generation and also contains hydro and biomass.

Its selection was made via the graphical user interface offered by SimBench. In fact, to facilitate the selection of systems, the SimBench's GUI offers a list of use cases, with for example "Voltage and reactive power optimization", "Failure simulation", "Ancillary services from distribution grids", "Local congestion management", etc. Here, an interesting choice to study the cyber-physical interdepencies seemed to be the use case "Grid automation with local or decentralized controllers". Once the use case is chosen, SimBench proposes a system of a certain voltage level, with a certain urbanization character (urban, rural, mixed, ...) and according to a certain present or future scenario of renewable energy resources deployment. Here, by selecting the use case "Grid automation with local or decentralized controllers", the system proposed by SimBench was the semi-urban medium voltage system, whose scenario corresponds to a future grid with a normal increase of DERs. The grid was generated based on information on the nature of MV systems from literature reviews, on real data from German grids and on consideration of the requirements of the use case. The data is synthetic and do not represent a real power system.

Although being quite recent (2019), this test system has already been used in a cyber-physical study. In [81], they present a methodology to model and determine the state of the interconnectors in cyber-physical electrical

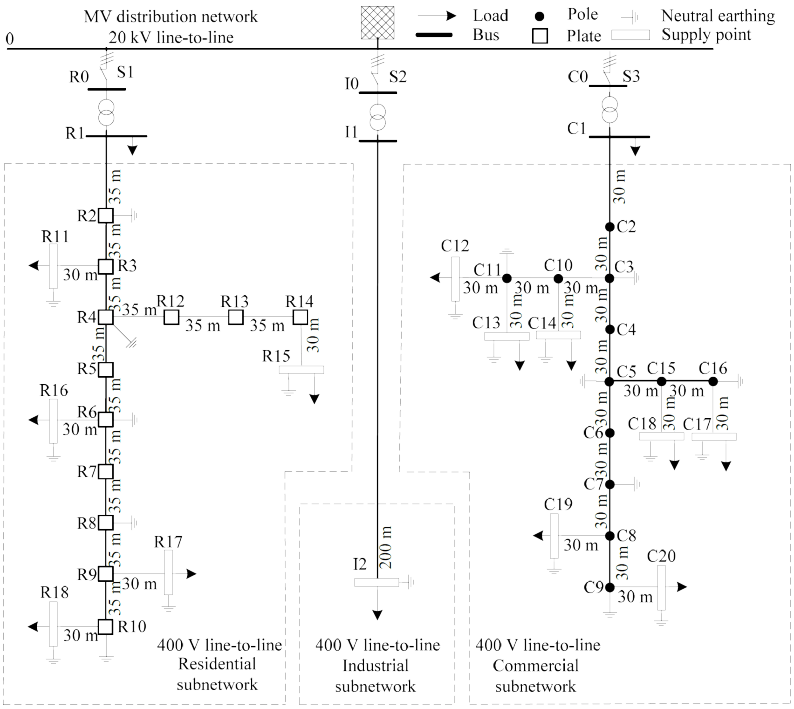


Figure 2.17: Single-line diagram of the CIGRE LV benchmark system. [79]

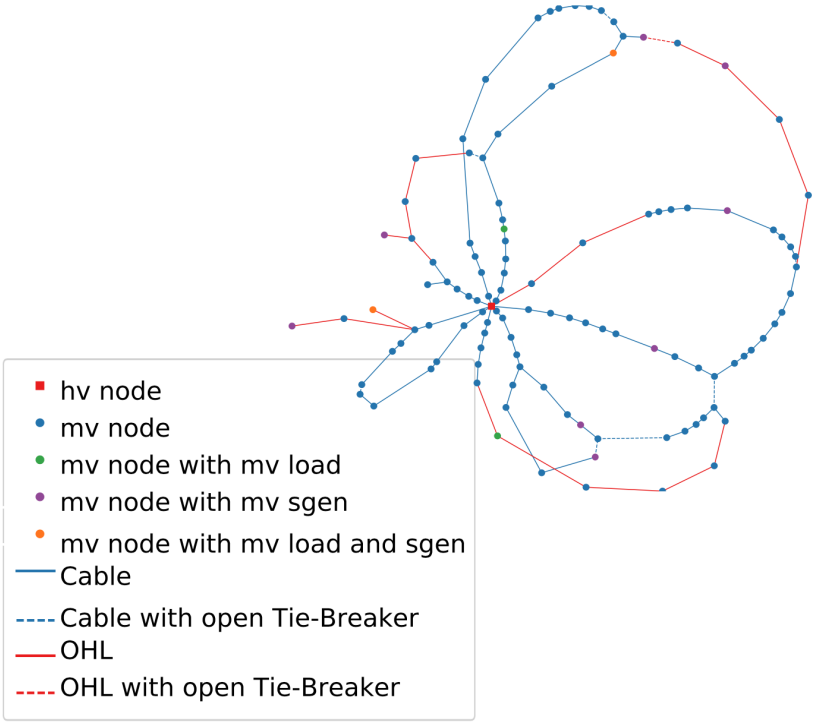


Figure 2.18: SimBench's semi-urban power grid. [75]

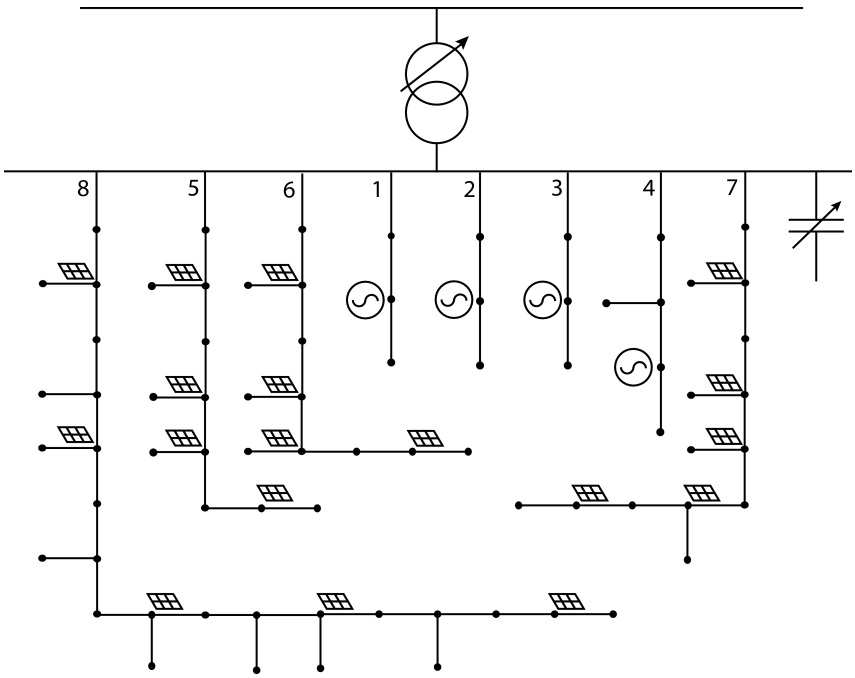


Figure 2.19: Distribution Grid topology - TDNetGen. [60]

systems and develop this methodology based on the MV semi-urban SimBench's system. The authors define an interconnector as "a technical instance that exists in two or more subsystems. These instances are physically, virtually, geographically or logically dependent on all subsystems the interconnectors connects. Focusing on the subsystems power system and ICT, an example of an interconnector is controllable generation".

2.2.1.4 TDNetGen

As introduced in Section 2.1.3.3 related to the Nordic Test System, there exists an interesting toolbox to be used in order to combine Transmission and Distribution Grid models and use the resulting system as one of the benchmark test power systems. This toolbox, *TDNetGen*, is an open-source MATLAB toolbox able to generate synthetic, large-scale, combined transmission and distribution grid models. According to *TDNetGen*'s designers, the test system models that are generated with the toolbox are highly customizable, which allows users to select certain desired characteristics, such as the level of renewable energy penetration, the size of the final system, etc.

TDNetGen is powered by MATPOWER (which is a stead-state analysis and planning tool) but in order to use the generated system with other simulation software, the toolbox allows users to build a custom exporter to any format. For now, it provides 2 custom exporters, one for ARTERE (power flow program developed at ULiège) and one for RAMSES (academic time-domain, dynamic simulation software). Indeed, it is possible to generate dynamic data even if the toolbox is based on MATPOWER. To perform a dynamic simulation, dynamic data for the transmission grid generators and controllers and for the distributed generators are required. The dynamic data is taken from the Nordic Test System document for the transmission side. However, for the distributed generators at the distribution grid level, [82] is used to model those on lines 1 to 4 as small synchronous machines while the distributed PV system model of [83] is used to model the distributed generators on lines 5 to 8.

As it is, the toolbox generates the combined T&D test system using the Nordic Test System model (see Section 2.1.3.3) and replacing the aggregated transmission grid loads with a detailed distribution grid model derived from the United Kingdom Generic Distribution System[10] [73] and customized to accommodate increased distributed generators penetration. The topology of this distribution grid is shown in Figure 2.19.

The toolbox is available at `https://github.com/apetros/TDNetGen`, the paper [60] gives detailed information and explanation of the parameters and it is important to note that the data can be freely modified and

[10]The United Kingdom Generic Distribution System (UKGDS) is a collection of power system models representative of UK distribution grids and that was developed by the Centre for Sustainable Electricity and Distributed Generation (SEDG).

shared.

2.3 Merging with the cyber layer

As its name indicates, the "CYber-Physical Risk of the bulk Electric energy Supply System" (CYPRESS) project not only addresses the physical security aspect of the electric power supply system, but it does so by considering its interdependence with the cyber system that is connected to the physical layer to form the cyber-physical power system.

Therefore, after having studied and selected test power systems that represent only the physical part of the above-mentioned CPPS, the remainder of this deliverable deals with the cyber layer to be integrated to these physical test systems. This cyber layer is the main focus of Chapter 3 and, before getting there, the present section links the two domains by discussing the cyber-physical interconnection of CPPSs.

As a reminder, the cyber layer refers to the information and communication technology (ICT) system whose presence enables the communications, computations, and storage of data used to plan and operate the physical system [84]. Indeed, this ICT layer contains components that enable control loops[11] to be implemented in the power grid. It can be found at various points in the composite power system and Section 2.3.1 presents these points where the physical and cyber worlds interconnect with each other. After that, Section 2.3.2 closes the chapter by presenting the concept of node-breaker modeling.

2.3.1 Interconnection points

The control and protection principles of electric power systems as well as the main computational applications involved are given in Chapter 2 of [84], while the present section introduces the cyber-physical interconnection points that emerge from it. It gives a reminder of some of the relevant elements that enable to make the link with Chapter 3. However, the reader who is interested in more detailed explanations can read [84]'s Sections 2.3.1 for control systems, 2.3.2 for protection systems and 2.4 for the main computational applications.

The present section is divided according to the location of the so-called interconnection points, *i.e.* substations, (industrial or residential) loads and generation plants.

2.3.1.1 Substations

Substations are a fundamental component of the power grid and they correspond to a really crucial point for the protection, control and monitoring of the grid. Therefore, the ICT layer that they contain plays an essential role in these operational functions.

One of the main control loops in the transmission grid is reactive power compensation and is carried out notably in substations, where the voltage is controlled by injecting or absorbing reactive power in the substation by using VAR compensation devices such as *Static Var Compensators* or *Static Synchronous Compensators*. There is also the possibility to act on transformers to control the power system. Indeed, by controlling the voltage ratio (resp. the phase angle difference) of tap-changing transformers (resp. phase-shifting transformers), one can control the voltage (resp. the active power) in the grid.

Note that in addition to the automatic control loops, the substations are also controlled and monitored from remote control centers by the TSOs. Their most common actions are to modify the set-points of tap-changing and phase-shifting transformers, and to open and close circuit breakers in the substation in order to change the grid topology. They also sometimes switch lines out of service to redirect power flow.

In addition to control systems, substations also contain protection systems. Such systems contain measurement devices (*e.g.* voltmeter and ampere meter) and instrument transformers (*i.e.* transducers that bring the measured current or voltage value in the range of common measurement devices) to detect a fault. The fault is then analysed by a protection relay that sends a tripping signal to its circuit breaker if needed, allowing the latter to de-energise the faulted element by isolating it from the grid. There are several types of protection systems[12] and for some of them, communication is needed to gather measurements while, for the others, local control is sufficient.

[11] A control loops uses sensors to measure physical quantities (*e.g.* voltages and currents), controllers to process the measurements of the sensors and make decisions and actuators to implement the decisions of the controllers (*e.g.* open a circuit breaker to protect an electric device) [84].

[12] The main ones are mentioned and explained in [84].

The AC-DC (or DC-AC) converter substations, where the HVDC lines are connected, are also interconnection points where the cyber layer plays a role. Indeed, the power electronics enabling the conversion must be managed to allow control of the active power flowing through the HVDC line, and in some cases, also control of the injection/absorption of reactive power into the AC grid.

It should be noted that for substation devices, some papers and manufacturers (*e.g.* SIEMENS [85]) use the term "primary equipment" to refer to the electrical equipment forming the main body of the power system, such as busbars, power lines, power transformers, but also instrument transformers or circuit breakers. Whereas "secondary equipment" refers to the equipment that controls, regulates, protects and monitors the primary equipment, *i.e.* the devices that form the *Substation Automation System* (cf. Section 3.2.2) [86]–[89].

2.3.1.2 Generation

The ICT infrastructure used to monitor, control and optimize the operation of generation units is called the *Generation Management System*. The control enabled by such an infrastructure mainly corresponds to actions on the active and and reactive power output of generators, *e.g.* by opening or closing a valve, increasing or decreasing the exciter current, etc. To enable these actions, data are collected via local measurements (*e.g.* from the generator's terminal or from its rotor speed sensor) for some types of control loops and, for other types of control loops, via wide-area communication, which allows the transfer of data from substations and control centers. An example of the latter is when a TSO monitors the grid from a remote control center and may perform redispatching, meaning that he communicates updated set-points for the generating unit, in order to prevent unacceptable operating conditions. Indeed, a generation management system allows both for the remote monitoring and control through a SCADA functionality as well as the local monitoring and control [84].

2.3.1.3 Loads

Some (residential or industrial) end-users connected to the distribution grid also have their electricity infrastructure connected to an ICT system. The occurrence of these systems at the consumer level is growing with the transition to smart grids and the increasing reliance on *Advanced Metering Infrastructures* (AMIs). Such an infrastructures refer to the digital (smart) meters that record the electricity consumption of consumers at a fine temporal resolution in order to provide real-time meter readings. In an AMI, a *Meter Data Management System* (MDMS) controls the smart meter's configuration and connects to an AMI head-end device that forwards commands and aggregates data from the meters via the infrastructure [84].

2.3.2 Node-breaker modeling

In order to incorporate a cyber layer into the test power systems described in this chapter, the modeling of the test systems needs to be quite detailed and represent some of the elements involved in the interconnection points, such as protection systems.

Typically, power test systems are represented with bus-branch models. Such models represent each substation with a single bus for each nominal voltage level. There is no information about the breakers, their configuration and how they will intervene during contingencies. The model is in compact form and all components are named by the buses to which they are connected [90].

With node-breaker modeling, stations with a normal bus-branch configuration need to be transformed into a node-breaker topology, which is done by creating a mapping of each station into its constituent elements. This results in models representing the substations in a complete way, with for example elements such as circuit breakers, disconnectors, branches or shunts being modelled individually and connected via nodes. In consequence, the nodes, breakers and substation disconnectors are explicitly included in the system model and the components are referred to by their own name (ID). We also talk often about "full topology" [90]. A mapping example can be seen in Figure 2.20.

For CPPSs, the advantage of having a node-breaker model is that detailed system configurations and protection system schemes can be introduced. In this way, by developing a system bus into a more detailed substation, ICT elements can be added to the detailed model of that substation, for example.

2.3.2.1 Substation arrangements

Note that the node-breaker model of a substation is built based on the bus arrangement of that substation, or in other words, on the topology of circuit breaker connections [91]. There exist many different station configu-

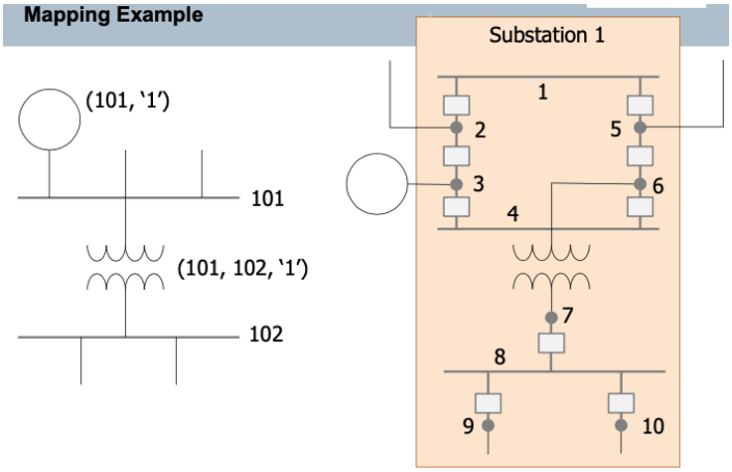


Figure 2.20: Bus-branch to node-breaker mapping example. [90]

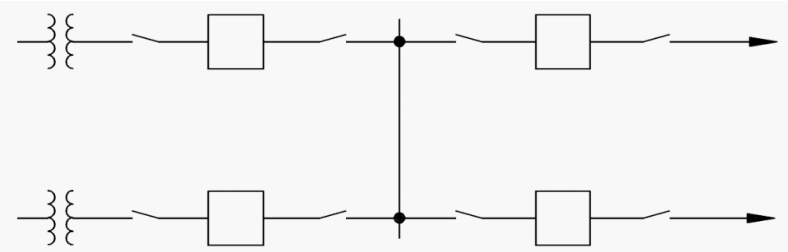


Figure 2.21: Typical one line diagram of the single bus, single breaker arrangement.[93]

rations, each of which having its advantages and disadvantages. The more common station arrangements are briefly described in the following [20], [92].

Single bus, single breaker arrangement

In a single bus substation configuration, all circuits are connected to one main bus, which is permanently energized. This arrangement, that can be seen in Figure 2.21, requires only one breaker per connection, *i.e.* each outgoing line is served by only one breaker.

The advantages of such an arrangement are that it is the simplest, in concept and operation, and the least expensive to build. Furthermore, it only requires small land area and is easily expandable.

The main disadvantages are that the single bus configuration offers the lowest reliability of all arrangements and that the failure of a circuit breaker when there is a fault on the protected line causes the loss of the entire substation. In addition, the only way to maintain a circuit breaker is to take that terminal out of service. However, note that this may not be a problem if the load served by this terminal has another power source or can be temporarily switched to other circuits [92], [93].

Main and transfer arrangement

In a main and transfer bus substation arrangement, there are two independent buses, the main bus and the transfer bus (Figure 2.22. In normal operation, the main bus is energized and each terminal is fed through its own breaker from this main bus while the bus tie breaker is open.

When one breaker is maintained, the bus tie breaker is closed and the disconnector between the breaker and the transfer bus is closed. During maintenance, the is no outage on any terminal and the terminal served from the transfer bus is protected through the bus tie breaker.

The main advantages of such an arrangement are its low initial cost, its flexible operation and the fact that the maintenance of breaker or line relays only modify slightly line protection, through the bus tie breaker.

Its disadvantages are that an additional breaker is required for the bus tie, a separate bus protection is required for each bus, switching is not easy when a breaker is taken out of service for maintenance and breaker or bus failure causes the loss of the entire station until the fault is isolated [92], [93].

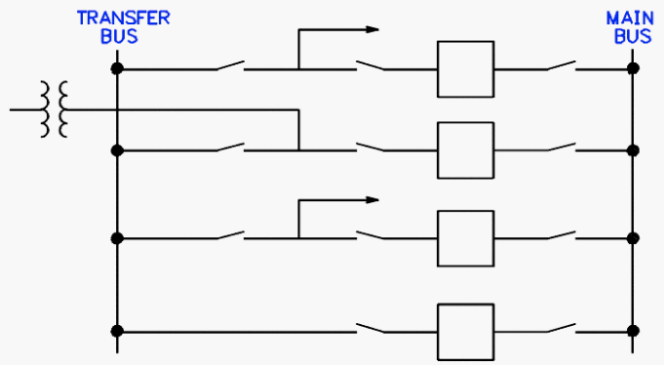


Figure 2.22: Typical one line diagram of the main and transfer arrangement.[93]

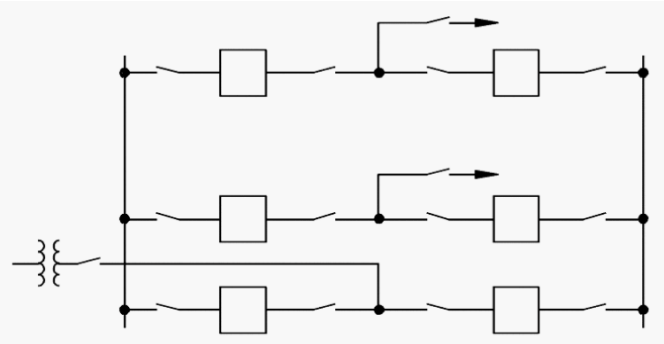


Figure 2.23: Typical one line diagram of the double bus, double breaker arrangement.[93]

Double bus, double breaker arrangement

In a double bus, double breaker arrangement, there are two main buses, each normally energized and two breakers are used for each terminal, as can be seen in Figure 2.23.

The main advantages of this arrangement are its flexible operation and high reliability, which is increased by the fact that each connection is served by two breakers. Furthermore, either of the main buses can be removed at any time for maintenance and the failure of a bus does not remove any circuit from service.

In contrast, this type of configuration is more expensive since it requires two breakers per circuit and the protective relaying must trip two breakers to isolate a faulted line from the substation [92], [93].

Ring bus arrangement

The ring bus configuration can be seen in Figure 2.24. It consists of a closed loop with each bus section separated by a circuit breaker. In order to increase the reliability and flexibility, each section supplies only one circuit.

The ring bus arrangement has the advantages of not being expensive as it requires only one breaker per connection and of offering flexible operation for breaker maintenance without interrupting load or requiring complex switching. Furthermore, the failure of a breaker takes only two circuits out of service in normal conditions and each circuit is served by two breakers.

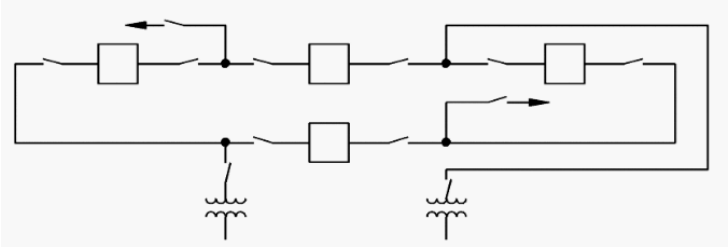


Figure 2.24: Typical one line diagram of the double bus, double breaker arrangement.[93]

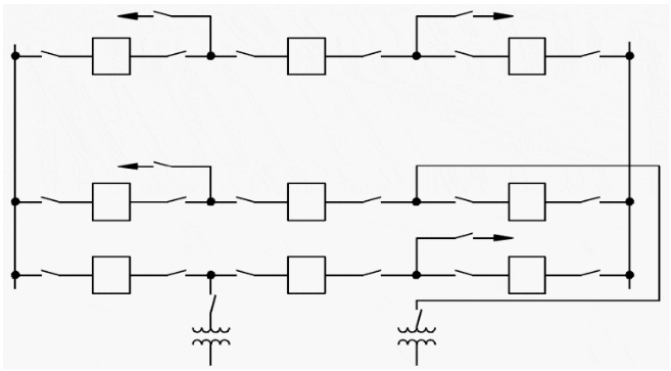


Figure 2.25: Typical one line diagram of the double bus, double breaker arrangement.[93]

On the other hand, automatic reclosing circuits are rather complex in such arrangements and they require voltage devices on all circuits because there is no definite potential reference point [92], [93].

Breaker-and-a-half arrangement

A breaker-and-a-half substation configuration is formed of two main buses that are normally energized. Between these buses there are three circuit breakers and between every two breakers is a circuit, as can be seen in Figure 2.25. Thus, such arrangement uses three breakers for every two circuits.

Its advantages are the flexible and simple operation it offers and its high reliability. Furthermore, the failure of a bus-side breaker only removes one circuit from service, the failure of a bus does not remove any from service and either of the main buses can be removed for maintenance at any time.

The drawbacks are that it requires 1.5 breakers per circuit and that the protective relaying is complex since the middle breaker must react to either of its associated circuits. Finally, the failure of this middle breaker causes the loss of an unfaulted circuit [92], [93].

3

Cyber layer

One of the intentions of this project is to carry out digital tests and simulations on test systems representing cyber-physical power systems in their entirety, *i.e.* test systems containing both the physical and cyber layers of CPPSs. Regarding the physical layer, the previous chapter presented some test power systems, taken from the literature, that will be used in the project. For the cyber layer, the selection process is different. Indeed, in the literature, there is a lack of reference ICT test systems to represent this cyber layer. It is therefore necessary to investigate what ICT components are involved in the control, protection and monitoring of electrical equipment, which communication standards are used in electrical substations, which different types of communication networks exist and which elements they contain, ... or, more globally, what cyber components are present in the cyber layer of Cyber-Physical Power Systems.

This chapter therefore aims to present the result of these investigations. First of all, with a view to the future modeling and simulation of the components presented in this chapter, Section 3.1 briefly presents the proposed way of modeling the cyber layer in practice. This simple proposition corresponds to a high level modeling and is merely intended to give an idea of what will be done in practice with the list of cyber components built up as the chapter progresses.

Then, Section 3.2 gives an insight into how to build a cyber system in the context of CPPSs. It begins by introducing the elements constituting the cyber layer of the power grid, starting with the ICT components typically found in communication networks (Section 3.2.1), and then focusing on the devices specialized in substation automation (Section 3.2.2. Finally, the chapter closes on a State-of-the-Industry about the power grid ICT infrastructure (Section 3.2.3).

3.1 Modeling the cyber layer

In order to simulate cyber-physical power systems, it is important to define a way to model the cyber layers that should be added to the benchmark test power systems.

A common approach in networking is to model the cyber layer as a graph composed of vertices connected by

edges. The vertices represent intermediary or terminal cyber devices, such as routers, switches or Remote Terminal Units (RTUs) while the edges represent the communication channels connecting these devices [1], [70].

From a programming point of view, the idea is to model a graph by creating a collection of objects (which can be serialized and represented in a standard form, *e.g.* the JSON format) *nodes* and *links* to represent the vertices and edges of a graph respectively. A *node* therefore corresponds to a cyber device, such as a router, switch or RTU, while a *link* corresponds to a communication channel connecting cyber devices [70]. In such a collection of *node* and *link* objects, each object is accompanied by attributes characterising it and enabling the respective element to be modelled and digitally simulated. As an example, a *link* object has attributes such as a source node, a destination node, a bandwidth, a type of link, etc.

All *link* objects have the same attributes, which are given at the beginning of Section 3.2.1. Concerning the *node* objects, they have different attributes depending on the device that corresponds to a specification of the *node*. These attributes are given in the following sections.

Note that in this chapter, the terms for the different cyber components -whose modeling is relevant to the project- are defined as they are encountered. Their definition is accompanied by the list of attributes useful for their modeling and this is presented in the form of a color box as shown just below.

Name of the component
Definition of the component.
Attributes:
- *First attribute*
- *Second attribute*
- *...*

3.2 Cyber components selection

The integration of cyber-components into the control and monitoring of critical infrastructures is not recent. Yet, the literature lacks a rigorous, widely adopted, state-of-the-art methodology that would allow operators to model their whole cyber-physical infrastructure. As mentioned above, a good example of such hole in the literature is the absence of reference test systems for the cyber part that would allow researchers to benchmark their tools. This results in a very slow adoption of new cyber technologies by operators that are not very receptive to completely theoretical results and that fear unexpected behavior of their infrastructure.

This section aims at providing more insights on the design of benchmark test systems for the cyber part of power systems infrastructure. As a first step, Sections 3.2.1 and 3.2.2 will elaborate on the typical components that are involved in the control and monitoring of the cyber-physical power grid. In contrast with traditional power-system components, the heterogeneity of cyber-components, mainly due to vendor-specific hardware and software implementation of devices, as well as the fast evolution in the technologies involved makes this task particularly tedious. Yet, this task is of crucial importance in order to derive a relevant and realistic reference test system.

From this point, there is still very little knowledge on how the cyber components interact and integrate into the whole cyber-physical infrastructure. In addition, almost all of cyber-components are microprocessor-based and may perform various tasks at once. This is particularly true when considering the advent of virtualization and emulation techniques. The purpose of Section 3.2.3 is to narrow the scope of what is conceivably possible in terms of infrastructure design. Indeed, this section will present constraints and advice, inspired by the field, which will allow to define a realistic test system relevant to the operators.

3.2.1 Traditional ICT components

This section aims at providing a characterization of typical state-of-the-art ICT components. As ICT components might appear in various forms, often performing multiple task at once, the section will focus on processes, being a task that is being run by an ICT device in a particular scenario. A process might either be run on a general-purpose computing unit, concurrently with other processes, in a vitalized environment or not, or might be run on its dedicated, optimized piece of hardware.

Note that a first component that composes any type of communication network is the communication channel connecting devices. As introduced in Section 3.1, these channels are represented by *link* objects. The attributes for modeling them are the following:

Link attributes:

- Source node
- Destination node
- Top-level OSI layer number
- Protocol per OSI layer - OSI Layer 7 (DNP3, ICCP, HTTP, Modbus), OSI layer 4 (TCP, UDP), OSI layer 3 (IP), OSI Layer 2.5 (MPLS), OSI Layer 2(Ethernet), OSI Layer 1 (fiber, microwave, cellular, serial)
- Bandwidth (bits per second)
- Drop rate
- Error rate

3.2.1.1 Local Area Networking

A Local Area Network (LAN) is a typically small-sized computer network used for interconnecting devices that are geographically close to one another, *e.g.* within a same building. In technical terms, a LAN is a layer-2 network, *i.e.* a network connecting hosts such that they can communicate without messages going through a router. LANs rely on layer-2 (data link) protocols such as Ethernet, which includes wired Ethernet and Wi-Fi, and the Point-to-Point Protocol (PPP) [94]. The latter is however only used for the very small LAN connecting two routers via a direct wire. Typical home or corporate LANs are built over Ethernet. Typical LAN devices include switches and wireless access points.

(L2) Switches The simplest form of LAN is a point-to-point connection, which presents the strong limit of 2 devices on the LAN. Switches are used to build bigger LANs by providing a way for more than 2 devices to communicate with each other. Switches can connect to other switches, to hosts and to routers, access points and other networking devices. Switches forward packets according to the layer-2 header of the TCP-UDP/IP networking stack. They ignore all headers from higher layers. Forwarding is based on the MAC address of the receiver. Switches learn the binding between MAC address and port to forward on by observing the sender's MAC address for incoming packets. With this information, they fill a MAC address table. Switches rely on the Spanning Tree Protocol (STP) to create a loop-free virtual topology to forward packets on. This is necessary to avoid catastrophic endless traffic loops taking up all the links' bandwidth. These techniques cannot be used to build large networks as any topological change requires the costly recomputation of a spanning tree over the entire LAN. This is why larger networks are built by interconnecting LANs with routers [94].

(L2) Switch
A (layer-2 or L2) switch is a device used for packet forwarding over a Local Area Network. It forwards packets according to the destination MAC address found in the packets' layer-2 header ignoring all headers from higher-layer protocols.
Attributes:
- Supported bandwidth per port
- Number of ports (used to connect switches or other devices)
- MAC address table

Wireless Networking While core networks are built over wired technology, wireless technology is particularly prevalent at the edge of the network. The typical use case is to connect several Wireless Access Points (WAP) to routers or switches to offer connectivity between mobile terminals such as laptops and smartphones and the rest of the network, including other mobile devices connected to WAPs and devices that simply use a wired connection. The typical protocol used is Wi-Fi (IEEE 802.11), which is used for wireless transmission of Ethernet frames. Mobile networking technology (3G, 4G, 5G) is also used for Internet connectivity but is uncommon in corporate WANs. Wireless communication is more sensitive to interference and will thus present higher error rates which reduces the effective bandwidth, and causes higher delays. In addition, they require specific

protocols for the handover of clients from one access point to the other and for multiplexing of the shared communication channel, i.e. a range of electromagnetic frequencies.

Wireless Access Points (WAP)
Wireless access points are devices that forward the packets to/from wireless devices from/to the wired network to which they are connected.
Attributes:
- Total available bandwidth
- Maximum number of clients
- Communication protocol: Wi-Fi, Bluetooth, 4G, ...
- (Optional) Protocol for the handover of clients to another access point

VLAN Virtual LANs (VLANs) are used to improve the scalability issues of layer-2 networking and provide additional isolation, which is desirable for security purposes. Indeed, segmenting traffic into smaller isolated networks limits the amount of places where it could be captured by an attacker. The idea behind VLANs is to add an additional identifier to Ethernet frames identifying the virtual LAN of the sender. These tags are typically added by the switch to which the sender is directly connected. It can also be inserted by the sender itself. Switches will only forward frames to devices belonging to the same VLAN. They will compute one spanning tree per VLAN, which will improve performance in case of topology changes. Inter-VLAN communication is not possible without going through a router (or a L3 switch - more on this below) [94].

L3 Switches As traditional layer-2 switches ignore packets layers higher than layer 2, their functionality and adaptability are quite limited. Their single purpose is packet switching on a LAN. For a finer-grain traffic management, it is sometimes useful to have access to layer-3 information. For example, they can perform inter-VLAN IP-based routing without sending all inter-VLAN traffic to a router like a L2 switch would. They can offer various capabilities that are typical of routers such as IP-based routing. The main difference is that L3 switches are not meant to be used for interconnecting LAN. Although they sometimes can even participate in the same routing protocols as routers, *e.g.* OSPF [95], they will not have a WAN port and offer all the same functionalities, making them unfit to be used as router replacements.

L3 Switch
A layer-3 or L3 switch is a switch that offers additional functionalities based on layer-3 packet headers. In particular, it supports inter-VLAN communication without going through a router [95].
Attributes:
- Supported bandwidth per port
- Number of ports (used to connect switches or other devices)
- MAC address table
- Buffer size and occupancy rate
- (Optional) Association between ports and VLAN tag
- (Optional) Association between IP addresses and VLAN tags
- (Optional) Forwarding table

3.2.1.2 Wide Area Networking

Wide Area Networks (WAN) are large scale networks used to interconnect several LANs. Due to scalability issues inherent to layer-2 networking, WANs do not use the Spanning Tree Protocol to build a loop-free forwarding plane. Instead, a set of routers, which are layer-3 devices, exchange dynamical topological information in order to build forwarding tables. These tables contain a mapping between ranges of IP addresses and the action to take in order to forward packets on the shortest path towards these addresses (according to some performance metric). This is done with routing protocols such as RIP or OSPF [94].

Power systems communication requirements A pervasive, highly available, and well-designed communication network will help enable increased reliability and availability while also reducing operational expenses [96]. Indeed, a secure and highly reliable data network reaching the edge of the grid is required to deliver operators with crucial real-time information, and let them operate the grid remotely in real time. For instance, TSOs and

DSOs typically require an efficient WAN infrastructure to interconnect all the different LANs that they manage. Typically, each substation and control center are independent LANs connected to a single WAN to allow end-to-end connectivity between each device. The WAN can either be private infrastructure (routers, switches, cables...) owned by the operator, which is more costly, or a Virtual Private Network (VPN) over a provider's WAN.

Border Gateway Protocol (BGP) For very large networks (at the scale of Internet Service Providers), intra-domain routing protocols such as OSPF are not sufficient to provide adequate performance due to the large number of routers exchanging topological information. Such networks are thus subdivided into smaller networks called Autonomous Systems (AS). Within an AS, routing protocols such as OSPF are used and a best route among ASes (according to economic criteria) is established through the Border Gateway Protocol (BGP) [94].

Router
A router is a layer-3 device used for forwarding packets along the shortest path (in terms of a given cost metric). Routers discard all headers below layer 3 and forward packets according to the destination IP address contained in the L3 header.
Attributes:
- Number of ports (used to connect routers or other devices)
- Supported bandwidth per port
- Buffer size and occupancy rate
- Interfaces - which IP address that is assigned to each physical port of the device
- (IP) Forwarding table
- (Optional) MPLS forwarding table

Virtual Private Networks (VPNs) VPNs are a technology to provide connectivity between isolated networks by routing inter-network traffic through a larger network that is not under control of the isolated networks' owner. This large network could simply be the Internet, as IP-in-IP tunnels only requires configuring routers at the isolated networks' edges. The main disadvantages of this approach are privacy and performance concerns from traffic being routed through the public Internet. While encryption can help ensure confidentiality, it would still be better to have the traffic be isolated from public Internet traffic. Furthermore, Quality of Service (QoS) can not be guaranteed with this technology. Indeed, a best-effort service is not sufficient for time-sensitive applications such as SCADA traffic.

Multi-Protocol Label Switching (MPLS) Thus, the provider network would most likely be an ISP's private network configured to use Multi-Protocol Label Switching (MPLS) technology to build opaque tunnels between the two remote locations. With this technology, an additional MPLS header is added to the packets at the provider's edge to add a stack of tags to them. Routers configured to use MPLS will forward these packets according to the tag on top of the stack. Tags can be added and removed from the stack to allow specifying intermediate hops for fine-grain traffic control [94].

Software Defined Networking (SDN) A modern alternative to MPLS for building VPNs is Software Defined Networking (SDN) which allows to program special SDN switches via a logically centralized controller in order to be able to program all the switches at once in order to perform a specific tasks. SDN switches have a flow forwarding table. This table contains rules for modifying and forwarding packets according to attributes spanning over headers at layers 2,3,4. When the switch receives a packet that does not match any rule, it reaches out to the controller that will instate a new rule according to its programming [97]. An ISP may use SDN to provide VPNs isolating each client's traffic. It may even ensure physical isolation throughout its entire network if required. SDN offering more flexibility both in terms of QoS and cost for the VPN provider, it has become more prevalent in recent years. VPN solutions based on SDN are often referred to as SD-WAN (Software-Defined Wide Area Network).

SDN Switch
SDN switches are centrally controlled through a (logically) centralized controller and forward packets according on rules spanning over L2,3,4 headers set by the controller in their flow tables [97].
Attributes:
- Supported bandwidth per port
- Number of ports (used to connect switches or other devices)
- Flow table

SDN Controller
The SDN controller is logically centralized entity (which can be distributed to avoid introducing a single point of failure). It configures SDN switches by filling their flow tables. The rules are derived from a single program defining the forwarding logic for the entire Software-Defined Network [97].
Attributes:
- Complete forwarding logic for the network

3.2.1.3 Network Security

Some network devices act in a transparent fashion to provide security services. They are invisible to communicating hosts and have the single purpose of guaranteeing security properties. They typically could be removed from the network without causing communication problems. Their removal would however make cyber-attacks more likely to succeed in compromising all or part of the system. Among this family of network devices, the most common are firewalls and Intrusion Detection Systems (IDS).

Firewalls Firewalls are devices that discriminate between allowed and forbidden traffic. According to a set of rules, they either forward the packet normally or drop it completely. The rules are usually based on layers 3 and 4, typically the sender and receiver's IP addresses and TCP or UDP ports. Advanced firewalls may also look at other type of information, including application data. Firewalls dropping packets based on application contents are called Deep Packet Inspection (DPI) firewalls. DPI is made difficult by the prevalence of encryption. A DPI firewall cannot deal with true end-to-end encryption. There however exist schemes where the clients get configured to allow the firewall to act as a Man-In-The-Middle (MITM) encrypting/decrypting packets. These provide better filtering at the cost of breaking end-to-end confidentiality.

Firewall
Firewalls are devices that observe the network packets that go through them and only transmit them towards their receiver if the communication is allowed according to the firewall's rules. Packets that are not allowed are simply discarded [98].
Attributes:
- The set of rules on which traffic is to be forwarded or discarded

DeMilitarized Zones (DMZs) A standard way to use firewalls to improve security of a corporate network is to logically separate devices that must be accessible from outside of the company's network from the rest of the corporate LAN. To do so, one makes use of a topology such as the one shown on figure 3.1.

All devices that must be accessible from the WAN are placed into the DMZ while the others are kept within the LAN. All unsolicited packets coming from the WAN towards the LAN are to be dropped. This mechanism ensures that devices that have no good reason for being reachable from the WAN remain isolated from unsolicited communication originating from it.

Intrusion Detection System (IDS) IDS refers to a collection of devices and/or pieces of software designed to detect that a network intrusion has occurred - i.e., malicious activity or policy violation. This is not to be mixed with the behavior of a firewall. While firewalls prevent intrusions, IDSs try to report them when they have already occurred. Typical IDS are made up of one or several sensors as well as a manager. The manager decides whether an alarm needs to be raised to the operator depending on the information coming from the sensors. Network IDSs (NIDS) passively listen to network traffic and raise an alarm when signs of an intrusion are detected [99].

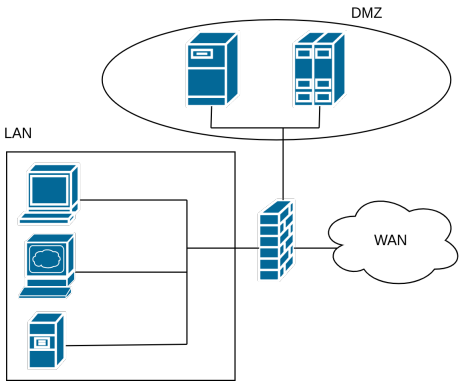


Figure 3.1: DMZ architecture

NIDS enable the system to detect a wide range of well-known attacks or unauthorized actions from legitimate users to attackers. Several techniques can be used to perform intrusion detection. Some NIDSs can be configured with explicit rules that should trigger an alarm while some other NIDS devices can run DPI algorithms to check traffic content against a database of attack signatures. Both strategies can be combined [99].

NIDS
A Network Intrusion Detection system NIDS is a device that passively listens to network traffic and raises an alarm upon detection of an anomaly, i.e. indication of an intrusion.
Attributes:
- Explicit rules describing scenarios that should raise an alarm
- Database of attack signatures

Virtual Routing and Forwarding (VRF) VRF refers to a technology included in routers that enables multiple instances of a routing table to exist in a virtual router. It enables segmentation capabilities as IP networks can be divided without the need of an extra router.

3.2.2 Substation Automation Components

This section presents the different components that are part of an electrical substation's cyber layer, playing a role in substation automation. Substation automation systems comprise a collection of hardware and software components that are used to monitor and control the substation electrical equipment, both locally and remotely. They include, among other things, metering and monitoring devices, protection relays, tap changers (to change transformer taps in response to a voltage change) and Human Machine Interfaces (HMIs) that provide local access to substation equipment [84]. A substation automation system also automates some repetitive, tedious and error-prone activities to increase the overall efficiency and productivity of the system.

The electrical automation industry was initially making extensive use of proprietary protocols developed by device manufacturers. Although they work especially well with devices of the same manufacturers, their lack of interoperability along with vendor dependency soon became a problem for electrical companies. As a result, proprietary protocols have been replaced by popular standard protocols in the industry. Older proprietary protocols such as Modbus are still used in legacy substation automation systems. However, most of the electrical companies in Europe have adopted communication infrastructures compliant with the IEC 61850 standard.

This standard and the components involved in IEC 61850-compliant substations are discussed in Section 3.2.2.2. However, before this, Section 3.2.2.1 introduces other components traditionally present in legacy substations and that are still present despite the innovations of recent years and the standardisation of substation automation.

3.2.2.1 Legacy Components

In legacy substations, the control and monitoring of electrical equipment is mainly done via sensors and actuators that are connected to devices called Remote Terminal Units (RTUs), which send data from the electrical equipment to the SCADA and receive control commands from it. Indeed, the RTUs are directly connected to the

primary equipment and monitor the positions of the circuit breakers as well as the current, voltage or temperature of the lines and equipment. In parallel, these units allow the control of equipment such as tap changers or capacity banks and allow operators to perform supervisory control and data acquisition functions remotely.

Remote Terminal Units The Remote Terminal Units (RTUs) are devices that exchange data and control signals with the control center SCADA system. They are mainly used for wider geographical telemetry and control of the field equipment. Most often, RTUs are not meant to execute control loops and control algorithms but more to interface with remote master stations for directly/indirectly relaying monitoring information and control signals from/to field equipment. They are mostly meant to perform simple data collection tasks with very small amounts of computations and execute the instructions provided by master stations or intelligent electronic devices. This involves small translation tasks to ensure that the targeted field equipment receives valid instructions. Note that although, traditionally, the RTU communicates back to some central station, it is also possible to communicate on a peer-to-peer basis with other RTUs. The RTU can also act as a relay station to another RTU that may not be accessible from the central station [100]. It should also be noted that modern RTUs typically support the IEC 61131-3 programming standard for Programmable Logic Controllers (PLCs) that allows them to execute small process control units such as PID, Alarming, Filtering, Trending, etc. [84], [99].

Remote Terminal Unit
A Remote Terminal Unit (RTU) is a stand-alone data acquisition and control unit that monitors and controls equipment at a remote location. Its primary task is to control and acquire data from field equipment at the remote location and to transfer this data back to a central station.
Attributes:
- List of primary equipment to which it is connected
- Supported protocols
- Number and type of physical ports on the device: serial, USB, Ethernet, ...
- Supported bandwidth: aggregated and for a given port

Then, although they are not involved in substation automation, it is important to talk about Phasor Measurement Units, as these are components that are most often installed in substations (and at generation plants), although they are mostly used for Wide-Area monitoring applications.

Phasor Measurement Units (PMUs) To define the state of a power system one can use the set of voltage magnitudes and voltage phase angles of all buses in the system. The voltage magnitude-voltage phase angle pair of a bus forms the so-called voltage phasor. To calculate these voltage phasors, but also the current phasors, Phasor Measurement Units are used. These devices provide synchronised measurements of the voltage phasor at a bus and of the current phasors in the branches connected to that bus [101], and can also be used to measure the frequency. The digital sensors of a standard PMU are capable of sampling 60 to 120 data points per second [102]. In order to estimate the phasors' components values, PMUs need to use a common time source for synchronization. This synchronization feature is most often provided by a Global Positioning System (GPS) signal. Note that the resulting synchronized measurement of phasors are also called *synchrophasors*.

Originally, a PMU is a standalone instrument composed of 3 sub-systems: the data acquisition part, the digital signal processor and the synchronisation system. The data acquisition part carries out the conditioning, sampling and analog-to-digital conversion of the input signals, the digital signal processor implements the measurement procedures and the synchronisation system provides the time reference [103].

PMUs are used in recently developed Wide-Area Monitoring and Wide-Area Control systems, offering new possibilities for power system control and real-time voltage stability assessment [101]. Furthermore, various PMU applications (*e.g.*, wide-area visualization, oscillation detection, and voltage stability) have been proposed to improve the power grid reliability [102].

Phasor Measurement Unit
A PMU measures the voltage and current phasors at different buses of a power system synchronized by a common timing signal.
Attributes:
- Sampling rate
- Number of analog inputs

3.2.2.2 IEC 61850

The IEC 61850 consists of a suite of standards that address different aspects of modern substation automation. It provides general guidelines for the organization of a substation's architecture and defines a series of protocols for intra-substation communication as well as some communication protocols for communication with control centers and other substations.

It is not limited to these protocols. The standard also defines in details a standard model for each of the functionalities enabling the operation of a generic substation. In addition to that, it also addresses all the necessary hardware requirements for substation devices as well as modeling languages to exchange about substation or device architectures.

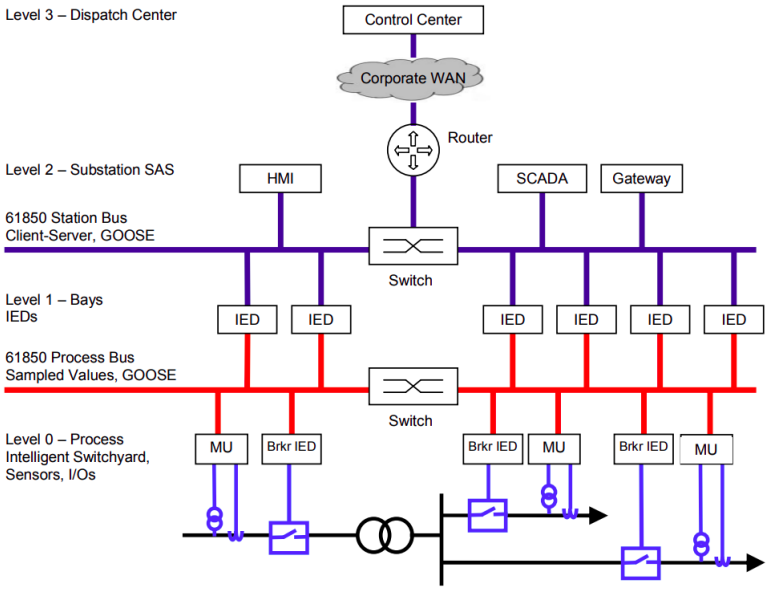


Figure 3.2: IEC61850 substation architecture. [104]

General architecture guidelines As can be seen in Figure 3.2, an IEC 61850-compliant substation is organised into 3 levels of devices connected via 2 levels of communication buses. Those 3 levels of devices are the following:

- Process level: Contains all switchgear, such as circuit breakers and switches, measuring devices such as current or voltage transformers and also Merging Units. The function of this level is to extract the information from sensors or transducers in the substation and send them to bay level devices. It also receives control commands from the latter and execute them appropriately [105], [106].
- Bay level: Consists of protection, control and monitoring units per bay[1]. Those units are mostly Intelligent Electronic Devices and they collect data from the same bay and/or from different bays and perform actions on the primary equipment[2] in their own bay [105], [106].
- Station level: Contains equipment for controlling and monitoring the whole station, such as HMI or SCADA system [106].

As mentioned above, 2 levels of communication buses connect those layers. A communication bus is a generic term describing a mean of connecting devices so that they may send messages to one or more devices connected to the same bus. Although not specified by the standard, in practice, the typical networking component that would fit this task is an Ethernet switch. The standard mandates that the bus is capable of transmitting Ethernet frames.

- The process bus connects the process level devices to bay level devices. It interconnects the IEDs within a same bay and carries real-time measurements for protection called Sampled Values (SV) [104].

[1] A bay is a power line within an electrical substation which connects a circuit to a busbar.

[2] As a reminder (cf. Section 2.3.1.1), primary equipment refers to the electrical equipment forming the main body of the power system while secondary equipment refers to the equipment that controls, monitors and protects the primary equipment.

- The station bus is used to allow the communication of station level devices such as the Human Machine Interface (HMI)[3] or the local SCADA relay and bay level devices. It interconnects all bays with the station level and carries control information such as measurement, interlocking and operations [104].
- Communication with devices outside the substation is done over a Wide-Area Network (WAN). The standard does not mandate the specifics of this network. In practice, it can either be a privately owned network or a Virtual Private Network (VPN) relayed over the public Internet.

Merging Unit
Merging Units (MUs) are used as an interoperable interface between primary and secondary equipment to record the measured values of the instrument transformers. Then, it digitizes these values and sends them along to one or more protection devices via a SV data stream over fiber optical Ethernet [85].
Attributes [107], [108]:
- Number of (analog) current and voltage inputs
- Number of binary inputs
- Number of binary outputs (used for tripping, executing local or remote control actions of a breaker or a disconnector, ...)
- Number and type of communication connectors (*e.g.* 2 Ethernet ports)
- Communication protocols supported
- Internal real-time clock (can be free-running or synchronized from an external source)
- Memory capacity (some MUs are able to store some data in their nonvolatile memory)

Intelligent Electronic Devices Broadly speaking, the term "Intelligent Electronic Device" (IED) defines any electronic device with intelligent function in substation automation. More precisely, IEDs are devices integrated with microprocessor-based technologies and that can collect and record information on many different parameters of a systems. Their architecture enables to run complex logic programs in a very short amount of time and, to reliably make complex decisions on abnormal situations. Their diffusion began in the 1980s, when these multi-functional devices started replacing the single-function instruments, thanks to the possibility of redefining the functionalities by simply redesigning the software [103].

The functions of a typical IED can be classified into the following main areas:

- Protection
- Control
- Monitoring
- Metering
- Communication

There are therefore many types of IEDs, depending on the function(s) they perform. For instance, it is possible that a Phasor Measurement Unit is designed in an IED. Indeed, according to the concepts proposed by the IEC 61850, the different functions of a PMU can be performed by different devices inside the substation, with the voltage and current signals acquisition done via suitable transducers and Merging Units, leaving the functionality of synchrophasor or frequency estimation to the IED. In this case, the operation of the PMUs described above is slightly different. Merging Units are used to collect the sensor signals in the field. They digitise and time-tag the electrical signal samples before sending them as packets through the process bus as SVs to an IED enabled to behave as a PMU [103]. As an example of IED with protection function, there are the protective relays, which, according to IEEE, are relays "whose function is to detect defective lines or apparatus or other power system conditions of an abnormal or dangerous nature and to initiate appropriate control circuit action" [109]. In substations, some protective relays are directly connected to protection devices (conventional solution) while others are connected to MUs through process buses (process bus solution) [85].

With the advent of new micro-processors technologies and the increasing spread of IEDs, it became necessary to define a standard to regulate the changes in progress [103]. The concept of Intelligent Electronic Device was thus standardized in the framework of the IEC 61850 standard which includes, among other things, an abstract data model for IEDs. As explained in [84], this data model provides a hierarchical structure of data attributes that represent the various devices and functions present in substations. These data attributes uniquely

[3] A Human Machine Interface is an interface to the operator of the substation.

identify device information, status information, device settings, measured values, and control actions within a substation.

Intelligent Electronic Device (IED)
Attributes:
- Function(s) performed by the IED
- Periodicity of GOOSE & SV messages
- Set of logical nodes supported by the IED

GOOSE stands for Generic Object-Oriented Substation Event. This protocol is used for sending messages over the process bus. It is used for sending status data to a group of listeners over Ethernet. It generally works in a synchronous fashion, *i.e.* data is collected, summarized and sent periodically, typically with a period of 4 ms or lower. However, a sender may also occasionally send messages spontaneously if an event occurs, *e.g.* a protection IED informs all IEDs on the process bus that it has triggered a breaker for protection.

Sampled Value Similarly to GOOSE, Sampled Value (SV) uses a publisher-subscriber mechanism. Messages are sent periodically by the publisher device to all its subscribers over the process bus. The frequency of messages is exactly defined but depends on two parameters: the frequency of the measured signal and the number of values sampled over the period of said signal.

MMS The IEC 61850 standard defines a precise nomenclature of devices and their functionalities. Physical devices such as IEDs are divided into smaller logical devices which are themselves subdivided into logical nodes, which represent elementary functionalities, *e.g.* break a line, or measure a specific voltage. The MMS protocol defines the format of messages to query for this specific information and control the functionalities defined by logical nodes. MMS runs over TCP on the station bus. Typically, MMS messages will be exchanged between the SCADA relay and IEDs.

Communication with control centers While IEC 61850 defines protocols for the communication between control centers and substation, this part of the standard is fairly recent (2016) and not much in application as this is typically handled by the SCADA system. IEC/TR 61850-90-2:2016 is mostly concerned with guidelines about the security of gateways and SCADA proxies and does not really deviate from the traditional SCADA-based approach by mandating new communication formats and is mostly a set of guidelines for the translation, data aggregation and transport between substations and control centers.

3.2.3 State-of-the-Industry

While industrial standards such as IEC 61850 attempts to regulate and unify industrial processes and operations, the standards often fail to provide complete requirements that will rule any of the design choices made by the operators. As a consequence, the expertise and experience of industrial actors often leads to some state-of-the-art practical choices that are not always properly documented in the standards. This must be considered with particular care as it will directly impact the realism of the chosen benchmark systems and thus, to which extent they will be relevant for the industrial field. In addition, standards often take as granted the fact that operators will integrate the latest cutting-edge technologies. This is particularly wrong for the power grid operators that are often not keen on updating their running infrastructure with novel technologies that are not well established in the field. In this context, validating how realistic are the chosen benchmarks with the eyes of experienced industrial actors is of crucial of importance.

3.2.3.1 CISCO Validated Design – Overview

CISCO is a world leader in the field of IT infrastructures design and implementation. Gaining from their experience in helping power grid operators with designing and securing their rapidly evolving IT infrastructure, they have properly documented and described a comprehensive industrial validated design that takes into considerations the various needs and constraints of the field.

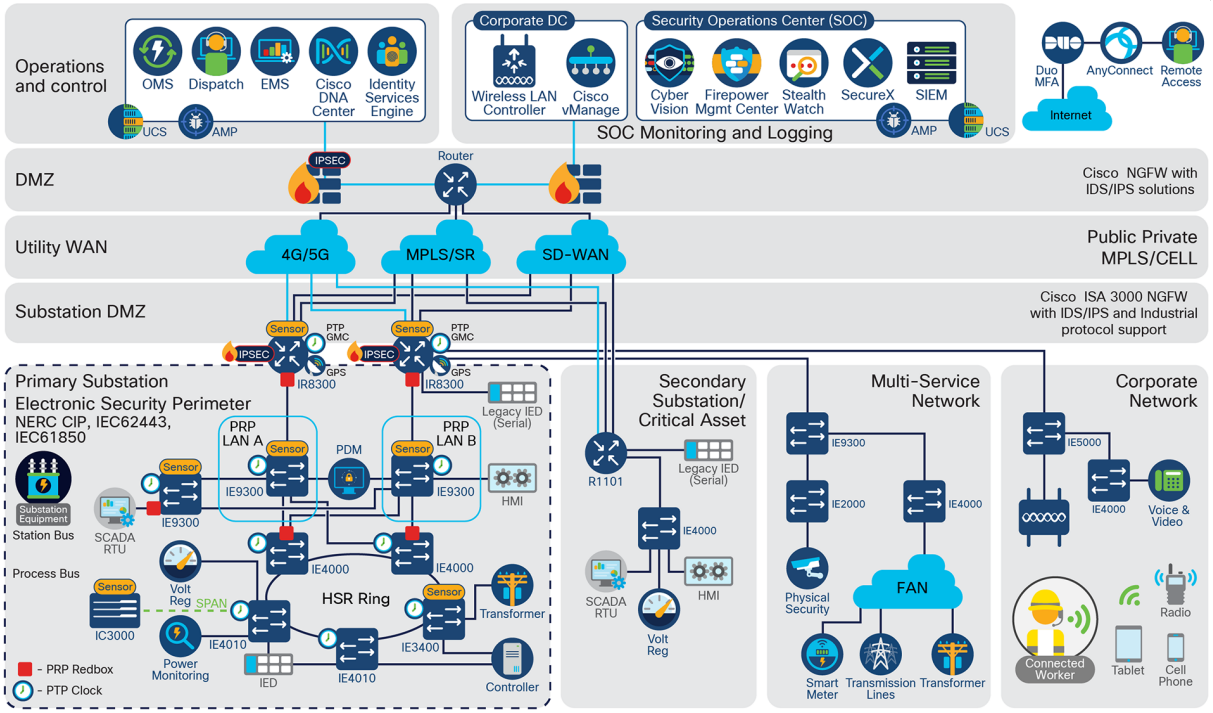


Figure 3.3: Grid IT infrastructure - CISCO Overview. [96]

Figure 3.3 describes how the CISCO validated design divides the cyber infrastructure of cyber-physical power systems [96].While all parts should respect various requirements regarding security and performance *-e.g., bounded transmission delays, etc -* , some zones illustrated in this figure do not require designs strictly specific to the field of power systems. For instance, the Operation and Control Center, the DeMilitarised Zones or the Utility WAN are not designed with any particular capabilities that goes beyond the state-of-the-art approach described in Section 3.2.1.

3.2.3.2 CISCO Validated Design – Substation Automation Architecture

As a complement to IEC 61850 standard that already participates in specifying the architecture of Substation system *-i.e., Station bus, Process Bus, etc.-*, CISCO attempts to specify some additional topological guidelines for enhancing substations security.

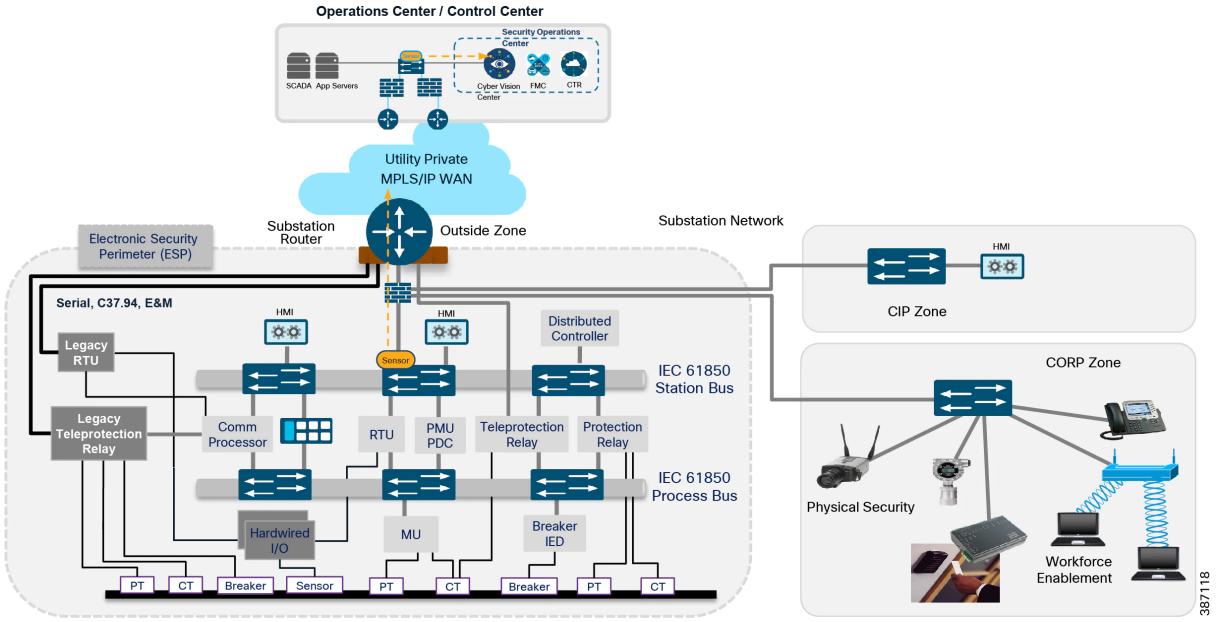


Figure 3.4: Substation Automation - CISCO Validated Architecture. [96]

Figure 3.4 illustrates those guidelines while taking into considerations IEC 61850 requirements. As such, it considers the recent migration of Substation Automation networks towards Ethernet-based-connectivity as specified by IEC 61850 while still considering legacy components.

Substation Automation Security To increase overall security of substation automation systems, CISCO provides additional content to clarify substation cyber-security requirements. As such, they divide these requirements into Group 1 - Basic Security Requirements and Group 2 - Enhanced Security Requirements.

Requirements of Group 1 can be further decomposed into:

- Network Segmentation is an architectural approach that divides a network into multiple segments, each acting as its own small entity. This allows administrators to control the flow of communication between segments based on granular policies, to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security through access control mechanisms.

  As represented in Figure 3.4, CISCO advises to further divide substations into logical zone, each having their own unique security requirements: (1) the Critical infrastructure Perimeter (CIP), (2) the Corporate Substation (CORPSS), the Electronic Security Perimeter (ESP), and (3) the Outside zone. Then, all external routable connectivity with those zone should pass through an identified Electronic Access Point dealing with inbound/outbound access permissions, detection of known or suspected malicious communications, etc. This can be implemented using L2 VLANs, L3 VRFs, Firewall interfaces and/or security contexts and Security Group Tags. (see section 3.2.1.3)

- Access Control refers to mechanisms and processes that aims at selectively restrict the access to a place or resource to some pre-defined authenticated and authorized actors. The authentication and authorization procedures might vary from simple validation of log-in credentials to very complex mechanisms preventing from starving critical applications. Typical examples are DHCP Snooping, Dynamic ARP Inspection (DAI), and IP Source Guard.

- Data Privacy & Secure connectivity ensure the integrity and confidentiality of both data that are transmitted and stored. Typical examples of such mechanisms are data encryption algorithms, checksums and hashes as well as security protocols such as TLS, DTLS, IPSec, etc.

- Network Availability refers to the structural property of a network describing its ability to relay data. It is a key requirements critical cyber-physical systems as operators more and more rely on the network to relay critical commands to components of the system. Guarantees on availability and thus, reliability of the network are typically achieved through redundancy. Indeed, redundancy in network components allows to mitigate failures and enhance the overall resiliency of the network. For instance, IEDs, such

as protective relays, with two network interfaces typically apply redundancy by sending the same traffic simultaneously through both interfaces. This type of redundancy is also known as parallel redundancy and it offers zero-time recovery, essentially not interrupting the traffic at all. Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) both provide redundancy at the Ethernet Layer and are typically applied underneath protocols such as GOOSE whSystemsich requires real-time delivery characteristics.

Requirements of Group 2 can be further decomposed into:

- Auditability & Logging
- Intrusion/Threat Detection & Prevention

Electronic Security Perimeter (ESP) Zone This zone contains all the active components necessary for proper functioning of the Critical Infrastructure. As such, the components in this zone are the most valued and trusted resources on the Substation network. This zone provides limited network connectivity to industrial components such as IEDs and Protection Relays. Outbound communications from this part of the system must be strictly controlled. For instance, any communication between this zone and any lower-security zone should leverage a `Pull model`, i.e. devices in this high-security zone will send the information to listeners in the low-security zones rather than answering unsolicited requests (which should be blocked) from them. Inbound connections into the ESP zone are discouraged except for business-critical applications.

CISCO advises to further segment the ESP zone, using VLANs:

- OT SCADA VLAN - This VLAN restricts communications to SCADA-like traffic such as Modbus, DNP3, IEC 61850 GOOSE.
- Network Management VLAN - This VLAN restricts communications to network managament traffic.
- Remote Workforce VLAN - This VLAN restricts communications to outbound traffic coming from partners/third party crews for them to gain access to the internet.
- Physical Security VLAN - This VLAN restricts communications to traffic generated by video surveillance systems, physical access systems, etc.
- Black Hole VLAN - This VLAN is used to black hole all unused ports.

As interactions between the substation automation system, corporate networks and the outside world are usually handled on the station level, a high level of security at that level is vital to the security of the whole system. Thus, all communication from the outside world to a substation should be protected by using a firewall and/or VPN-enabled channel.

Critical Infrastructure Perimeter (CIP) Zone This zone acts as a DeMilitarized Zone (DMZ) (see section 3.2.1.3) between the Corporate Substation Zone (CORPSS) and the ESP Zone. Indeed, it has a Firewall security level between both zones which allows proxied user-level access from the CORPSS towards the ESP zone, leveraging an information security hardened bastion host. Inbound connectivity to this zone can be provided using Remote Access VPN clients (see section 3.2.1.2). However, user connected to the CIP zone should be restricted to allow connectivity only to the Bastion Host. Then, the Bastion host will be responsible for proxying all user-level connectivity between the CORPSS zone and the ESP. Access to and from other resources within the CIP zone are significantly restricted to ensure the integrity of these resources and their interactions with the ESP zone.

Corporate Substation (CORPSS) Zone This zone acts as a remote gateway to the corporate/enterprise network for basic connectivity to business resources such as email servers, file servers, etc but also general access to the Internet via the Outside Zone. As such, traffic from this zone is supposed to only access other corporate assets directly leaving through the Outside Zone. Access to higher-security zones such as CIP and ESP from this zone should be strictly limited and controlled through access restrictions and additional credentials.

Outside Zone The Outside zone connects the Substation topology to the rest of the infrastructure *-i.e., owned by the operators or provided by a third-party Service Provider*. This zone is considered as not to be trusted. Therefore, the traffic that pass through this zone should be encrypted, authenticated, and preferably initiated from one of the other zones (ESP, CIP, and CORPSS).

Bibliography

[1] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.

[2] P. A. Oyewole and D. Jayaweera, "Power system security with cyber-physical power system operation," *IEEE Access*, vol. 8, pp. 179 970–179 982, 2020.

[3] P. Palensky, E. Widl, and A. Elsheikh, "Simulating cyber-physical energy systems: Challenges, tools and methods," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 3, pp. 318–326, 2013.

[4] S. C. Müller, H. Georg, J. J. Nutaro, *et al.*, "Interfacing power system and ict simulators: Challenges, state-of-the-art, and case studies," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 14–24, 2016.

[5] H. Georg, C. Wietfeld, S. C. Müller, and C. Rehtanz, "A hla based simulator architecture for co-simulating ict based power system control and protection systems," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, IEEE, 2012, pp. 264–269.

[6] *Electric Grid Test Cases*, Texas A&M University Engineering. [Online]. Available: `https://electricgrids.engr.tamu.edu/electric-grid-test-cases/`.

[7] *Power Systems Test Case Archive*, University of Washington - College of Engineering. [Online]. Available: `https://labs.ece.uw.edu/pstca/`.

[8] *Power Cases*, Illinois Center for a Smarter Electric Grid (ICSEG), 2022. [Online]. Available: `https://icseg.iti.illinois.edu/power-cases/` (visited on 08/04/2022).

[9] *PYPOWER*, 2022. [Online]. Available: `https://github.com/rwl/PYPOWER/tree/master/pypower` (visited on 08/04/2022).

[10] *Power Grid Lib - Optimal Power Flow*, IEEE PES Task Force on Benchmarks for Validation of Emerging Power System Algorithms, 2022. [Online]. Available: `https://github.com/power-grid-lib/pglib-opf` (visited on 08/04/2022).

[11] *Matpower - A Power System Simulation Package for MATLAB and Octave*, 2021. [Online]. Available: `https://github.com/MATPOWER/matpower/tree/master/data` (visited on 08/04/2022).

[12] *BetterGrids database*, BetterGrids Project, 2022. [Online]. Available: `https://db.bettergrids.org/` (visited on 08/04/2022).

[13] C. Barrows, A. Bloom, A. Ehlen, *et al.*, "The IEEE reliability test system: A proposed 2019 update," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 119–127, 2019.

[14] A. Moeini, I. Kamwa, P. Brunelle, and G. Sybille, "Open data IEEE test systems implemented in SimPowerSystems for education and research in power grid dynamics and control," in *2015 50th International Universities Power Engineering Conference (UPEC)*, IEEE, 2015.

[15] S. Peyghami, P. Davari, M. Fotuhi-Firuzabad, and F. Blaabjerg, "Standard test systems for modern power system analysis: An overview," *IEEE Industrial Electronics Magazine*, vol. 13, no. 4, pp. 86–105, 2019.

[16] R. N. Allan, R. Billinton, and N. Abdel-Gawad, "The IEEE reliability test system-extensions to and evaluation of the generating system," *IEEE Transactions on Power Systems*, vol. 1, no. 4, pp. 1–7, 1986.

[17] C. Grigg, P. Wong, P. Albrecht, *et al.*, "The IEEE reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Transactions on power systems*, vol. 14, no. 3, pp. 1010–1020, 1999.
[18] Probability Methods Subcommittee, "IEEE reliability test system," *IEEE Transactions on power apparatus and systems*, no. 6, pp. 2047–2054, 1979.
[19] K. W. Hedman, R. P. O'Neill, E. B. Fisher, and S. S. Oren, "Optimal transmission switching with contingency analysis," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1577–1586, 2009.
[20] F. Yang, A. S. Meliopoulos, G. J. Cokkinides, and Q. B. Dam, "Effects of protection system hidden failures on bulk power system reliability," in *2006 38th North American Power Symposium*, IEEE, 2006, pp. 517–523.
[21] R. Billinton, P. K. Vohra, and S. Kumar, "Effect of station originated outages in a composite system adequacy evaluation of the ieee reliability test system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-104, no. 10, pp. 2649–2656, 1985. doi: 10.1109/TPAS.1985.319105.
[22] H. Lei and C. Singh, "Developing a benchmark test system for electric power grid cyber-physical reliability studies," in *2016 International conference on probabilistic methods applied to power systems (PMAPS)*, IEEE, 2016, pp. 1–5.
[23] H. Lei, Y. Chakhchoukh, and C. Singh, "Framework of a benchmark testbed for power system cyber-physical reliability studies," *International Transactions on Electrical Energy Systems*, vol. 29, no. 1, e2692, 2019.
[24] P. Henneaux, J. Song, and E. Cotilla-Sanchez, "Enhancing test power systems for dynamic cascading outage simulations," in *2014 IEEE Conference on Technologies for Sustainability (SusTech)*, 2014, pp. 107–114. doi: 10.1109/SusTech.2014.7046228.
[25] C. Lassetter, E. Cotilla-Sanchez, and J. Kim, *Enhanced IEEE RTS-96 test case w/ synthesized dynamic parameters*, Zenodo, May 2016. doi: 10.5281/zenodo.51001.
[26] E. Johansson, K. Uhlen, G. Kjølle, and T. Toftevaag, "Reliability evaluation of wide area monitoring applications and extreme contingencies," in *17th Power Systems Computation Conference*, 2011.
[27] P. Henneaux and P.-E. Labeau, "Offsite power reliability assessment for nuclear power plants: An application of dynamic reliability to power systems," in *Advanced Concepts in Nuclear Energy Risk Assessment and Management*, ch. 7, pp. 257–278. doi: 10.1142/9789813225619_0007.
[28] R. Billinton, S. Kumar, N. Chowdhury, *et al.*, "A reliability test system for educational purposes-basic data," *IEEE Transactions on Power Systems*, vol. 4, no. 3, pp. 1238–1244, 1989.
[29] W. Li *et al.*, *Reliability assessment of electric power systems using Monte Carlo methods*. Springer Science & Business Media, 2013.
[30] R. N. Allan, R. Billinton, I. Sjarief, L. Goel, and K. So, "A reliability test system for educational purposes-basic distribution system data and results," *IEEE Transactions on Power systems*, vol. 6, no. 2, pp. 813–820, 1991.
[31] R. Billinton and S. Jonnavithula, "A test system for teaching overall power system reliability assessment," *IEEE transactions on Power Systems*, vol. 11, no. 4, pp. 1670–1676, 1996.
[32] H. Lei and C. Singh, "Power system reliability evaluation considering cyber-malfunctions in substations," *Electric Power Systems Research*, vol. 129, pp. 160–169, 2015.
[33] H. Hayati, A. Ahadi, and S. M. M. Aval, "New concept and procedure for reliability assessment of an IEC 61850 based substation and distribution automation considering secondary device faults," *Frontiers in Energy*, vol. 9, no. 4, pp. 387–398, 2015.
[34] P. Demetriou, M. Asprou, J. Quiros-Tortos, and E. Kyriakides, "Dynamic IEEE test systems for transient analysis," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2108–2117, 2017. doi: 10.1109/JSYST.2015.2444893.
[35] V. Vittal, J. McCalley, P. Anderson, and A. Fouad, *Power System Control and Stability*, ser. IEEE Press Series on Power and Energy Systems. Wiley, 2019, isbn: 9781119433712.
[36] N. Mithulananthan, C. A. Cañizares, and J. Reeve, "Indices to detect hopf bifurcations in power systems," in *Proc. of NAPS*, Citeseer, vol. 2, 2000, pp. 15–23.
[37] P. Demetriou, M. Asprou, J. Quiros-Tortos, and E. Kyriakides, "Dynamic IEEE test systems for transient analysis," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2108–2117, 2015.
[38] P. Demetriou, M. Asprou, J. Quiros-Tortos and E. Kyriakides, *Dynamic IEEE Test Systems*, https://www2.kios.ucy.ac.cy/testsystems/, University of Cyprus, KIOS Research and Innovation Centre of Excellence, 2022.
[39] B. Park and C. L. Demarco, "Optimal network topology for node-breaker representations with ac power flow constraints," *IEEE Access*, vol. 8, pp. 64 347–64 355, 2020.

[40] B. H. Bringeland, "A substation level state estimator for local data processing-algorithms for power system monitoring," M.S. thesis, NTNU, 2017.
[41] A. G. Expósito and A. de la Villa Jaen, "Reduced substation models for generalized state estimation," *IEEE Transactions on Power Systems*, vol. 16, no. 4, pp. 839–846, 2001.
[42] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.
[43] R. Deng, P. Zhuang, and H. Liang, "Ccpa: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.
[44] A. A. Jillepalli, D. C. de Leon, B. K. Johnson, *et al.*, "Metics: A holistic cyber physical system model for IEEE 14-bus power system security," in *2018 13th International Conference on Malicious and Unwanted Software (MALWARE)*, IEEE, 2018, pp. 95–102.
[45] B. B. Adetokun, J. O. Ojo, and C. M. Muriithi, "Reactive power-voltage-based voltage instability sensitivity indices for power grid with increasing renewable energy penetration," *IEEE Access*, vol. 8, pp. 85 401–85 410, 2020.
[46] T. Athay, R. Podmore, and S. Virmani, "A practical method for the direct analysis of transient stability," *IEEE Transactions on Power Apparatus and Systems*, no. 2, pp. 573–584, 1979.
[47] J. Bialek, E. Ciapessoni, D. Cirio, *et al.*, "Benchmarking and validation of cascading failure analysis tools," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4887–4900, 2016.
[48] F. R. Gomez, A. D. Rajapakse, U. D. Annakkage, and I. T. Fernando, "Support vector machine-based algorithm for post-fault transient stability status prediction using synchronized measurements," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1474–1483, 2010.
[49] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," *Electronics*, vol. 5, no. 3, p. 40, 2016.
[50] Y.-n. Wang, Z.-y. Lin, X. Liang, W.-y. Xu, Q. Yang, and G.-f. Yan, "On modeling of electrical cyber-physical systems considering cyber security," *Frontiers of Information Technology & Electronic Engineering*, vol. 17, no. 5, pp. 465–478, 2016.
[51] Y. Zuo, M. Paolone, and F. Sossan, "Effect of voltage source converters with electrochemical storage systems on dynamics of reduced-inertia bulk power grids," *Electric Power Systems Research*, vol. 189, p. 106 766, 2020.
[52] Y. Zuo, G. Frigo, A. Derviškadić, and M. Paolone, "Impact of synchrophasor estimation algorithms in ROCOF-based under-frequency load-shedding," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1305–1316, 2019.
[53] Y. Zuo, F. Sossan, M. Bozorg, and M. Paolone, "Dispatch and primary frequency control with electrochemical storage: A system-wise verification," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, IEEE, 2018.
[54] A. Derviškadić, Y. Zuo, G. Frigo, and M. Paolone, "Under frequency load shedding based on PMU estimates of frequency and ROCOF," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, IEEE, 2018.
[55] G. Frigo, A. Derviškadić, Y. Zuo, and M. Paolone, "PMU-based ROCOF measurements: Uncertainty limits and metrological significance in power system applications," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 10, pp. 3810–3822, 2019.
[56] T. Van Cutsem, M. Glavic, W. Rosehart, *et al.*, "Test systems for voltage stability analysis and security assessment," IEEE, Tech. Rep., 2015.
[57] CIGRE Working Group 38.02.08, "Long term dynamics. Phase II. Final report.," CIGRE, Tech. Rep., 1995.
[58] T. Van Cutsem, M. Glavic, W. Rosehart, *et al.*, "Test systems for voltage stability studies," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 4078–4087, 2020.
[59] E. Munkhchuluun, L. Meegahapola, and A. Vahidnia, "Long-term voltage stability with large-scale solar-photovoltaic (PV) generation," *International Journal of Electrical Power & Energy Systems*, vol. 117, p. 105 663, 2020.
[60] N. Pilatte, P. Aristidou, and G. Hug, "Tdnetgen: An open-source, parametrizable, large-scale, transmission, and distribution test system," *IEEE Systems Journal*, vol. 13, no. 1, pp. 729–737, 2017.
[61] O. Netkachov, P. Popov, and K. Salako, "Quantitative evaluation of the efficacy of defence-in-depth in critical infrastructures," in *Resilience of Cyber-Physical Systems*, Springer, 2019, pp. 89–121.
[62] Y. Zhu, C. Liu, K. Sun, D. Shi, and Z. Wang, "Optimization of battery energy storage to improve power system oscillation damping," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 3, pp. 1015–1024, 2018.

[63] E. Heusinger, J. Porst, A. Raab, M. Luther, and S. Samaan, "Impact of inverter-based generation on voltage stability in a modified Nordic test system," in *2021 IEEE Kansas Power and Energy Conference (KPEC)*, IEEE, 2021, pp. 1–5.
[64] D. Obradovic, M. Dijokas, T. Van Cutsem, R. Eriksson, M. Ghandhari, and A. Tosatto, "Assessment of HVDC frequency control methods in the nordic test system," in *Proc. CIGRE conference*, 2020.
[65] P. Fernández-Porras, M. Panteli, and J. Quirós-Tortós, "Intentional controlled islanding: When to island for power system blackout prevention," *IET Generation, Transmission & Distribution*, vol. 12, no. 14, pp. 3542–3549, 2018.
[66] H. Barrios, A. Roehder, H. Natemeyer, and A. Schnettler, "A benchmark case for network expansion methods," in *2015 IEEE Eindhoven PowerTech*, IEEE, 2015.
[67] *A Benchmark Case for Network Expansion Methods*, IAEW RWTH Aachen University, 2021. [Online]. Available: `https://www.iaew.rwth-aachen.de/go/id/ivfsh/?lidx=1` (visited on 08/01/2022).
[68] *Grid data - Generating Realistic Information for the Development of Distribution and Transmission Algorithms*, Advanced Research Projects Agency - Energy. [Online]. Available: `https://arpa-e.energy.gov/technologies/programs/grid-data` (visited on 08/02/2022).
[69] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Transactions on power systems*, vol. 32, no. 4, pp. 3258–3265, 2016.
[70] P. Wlazlo, K. Price, C. Veloz, *et al.*, "A cyber topology model for the Texas 2000 synthetic electric power grid," in *2019 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, IEEE, 2019, pp. 1–8.
[71] K. P. Schneider, B. Mather, B. Pal, *et al.*, "Analytic considerations and design basis for the ieee distribution test feeders," *IEEE Transactions on power systems*, vol. 33, no. 3, pp. 3181–3188, 2017.
[72] *IEEE PES Test Feeder*, IEEE, 2022. [Online]. Available: `https://cmte.ieee.org/pes-testfeeders/` (visited on 07/28/2022).
[73] *United Kingdom Generic Distribution System*, Centre for Sustainable Electricity and Distributed Generation, 2015. [Online]. Available: `https://github.com/sedg/ukgds` (visited on 07/22/2022).
[74] *EPRI Test Circuits*, Electric Power Research Institute (EPRI), 2021. [Online]. Available: `https://sourceforge.net/p/electricdss/code/HEAD/tree/trunk/Distrib/EPRITestCircuits/` (visited on 07/25/2022).
[75] S. Meinecke, D. Sarajlić, S. R. Drauz, *et al.*, "Simbench—a benchmark dataset of electric power systems to compare innovative solutions based on power flow analysis," *Energies*, vol. 13, no. 12, p. 3290, 2020.
[76] *SimBench - Benchmark*, SimBench Consortium, 2019. [Online]. Available: `https://simbench.de/en/` (visited on 07/22/2022).
[77] *SimBench - Github*, SimBench Consortium, 2021. [Online]. Available: `https://github.com/e2nIEE/simbench` (visited on 07/22/2022).
[78] K. Strunz, S. Barsali, and Z. Styczynski, "Developing benchmark models for integrating distributed energy resources," in *Power Engineering Society General Meeting*, 2006.
[79] *CIGRE Networks - pandapower*, `https://pandapower.readthedocs.io/en/v2.6.0/networks/cigre.html`, Fraunhofer IEE and University of Kassel, 2021.
[80] H. Ergun, I. B. Sperstad, B. Espen Flo, *et al.*, "Probabilistic optimization of T&D systems planning with high grid flexibility and its scalability," 2021.
[81] A. D. Patil, J. Haack, M. Braun, and H. d. Meer, "Modeling interconnected ICT and power systems for resilience analysis," *Energy Informatics*, vol. 3, no. 1, pp. 1–20, 2020.
[82] G. Valverde and T. Van Cutsem, "Model predictive control of voltages in active distribution networks," *IEEE Transactions on Smart Grid*, vol. 4, no. 4, pp. 2152–2161, 2013.
[83] R. Elliott, A. Ellis, P. Pourbeik, J. Sanchez-Gasca, J. Senthil, and J. Weber, "Generic photovoltaic system models for wecc-a status report," in *2015 IEEE Power & Energy Society General Meeting*, IEEE, 2015, pp. 1–5.
[84] E. Karangelos, K. Thoelen, F. Faghihi, *et al.*, "CYPRESS: Report D1.1 describing the selected performance metrics,"
[85] *Process bus solution for substation automation systems*, Siemens, 2022. [Online]. Available: `https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/protection-relays-and-control/general-protection/process-bus.html` (visited on 09/05/2022).
[86] T. Buhagiar, J.-P. Cayuela, A. Procopiou, and S. Richards, "Poste intelligent-the next generation smart substation for the french power grid," 2016.

[87] M. M. Rao, M. J. Thomas, and B. Singh, "Transients induced on control cables and secondary circuit of instrument transformers in a gis during switching operations," *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1505–1513, 2007.
[88] C. Sun, Y. Zhang, and S. Qu, "Research on secondary system of smart substation," in *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, vol. 394, 2018, p. 042 118.
[89] Y. Liu, "Generic substation event monitoring based on IEC 61850 and IEEE 1588 standards," Ph.D. dissertation, 2015.
[90] *Node-Breaker Modeling Representation*, [Webinar], North American Electric Reliability Corporation, 2016. [Online]. Available: `https://www.nerc.com/comm/PC/Model%20Validation%20Working%20Group%20MVWG%202013/December%202016%20-%20Node%20Breaker%20Model%20Representation%20Webinar.pdf`.
[91] G. T. Heydt, N. Nimpitiwan, A. Bose, Y. Zhang, A. S. Meliopoulos, and Q. Dam, "New implications of power system fault current limits," *PSERC Publication*, pp. 05–62, 2005.
[92] Paul M. Anderson, *Power System Protection (IEEE Press Series on Power Engineering)*. Wiley-IEEE Press, 1999.
[93] *Six common bus configurations in substations up to 345 kV*, Electrical Engineering Portal, 2019. [Online]. Available: `https://electrical-engineering-portal.com/bus-configurations-substations-345-kv#:~:text=5.-,Breaker%2Dand%2Da%2DHalf,as%20diagrammed%20in%20Figure%207.` (visited on 11/14/2022).
[94] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed. Pearson, 2016, isbn: 978-0-13-359414-0.
[95] B. L. Shinder, *Computer Networking Essentials*. Pearson Education, 2001, isbn: 1587130386.
[96] I. Cisco Systems, "Cisco grid security 3.1 design guide," *Cisco Validated Design*, 2020.
[97] B. L. Shinder, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Pearson, 2015, isbn: 0134175476.
[98] M. Goodrich and R. Tamassia, *Introduction to Computer Security*, 2nd. Pearson, 2018, isbn: 0133575470.
[99] S. Ben Mariem, V. Rossetto, V. Guler, A. Godfraind, and L. Mathy, "CYPRESS: Report D1.2 describing the selected threats and components,"
[100] G. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.
[101] J. F. Baalbergen, M. Gibescu, and L. van der Sluis, "Coordinated agent-based control for online voltage instability prevention," *International Transactions on Electrical Energy Systems*, vol. 24, no. 11, pp. 1541–1561, 2014.
[102] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.
[103] A. Monti, C. Muscas, and F. Ponci, *Phasor Measurement Units and Wide Area Monitoring Systems*. Academic Press, 2016.
[104] J. Mcghee and M. Goraj, "Smart High Voltage Substation Based on IEC 61850 Process Bus and IEEE 1588 Time Synchronization," *2010 First IEEE International Conference on Smart Grid Communications*, pp. 489–494, 2010.
[105] R. Gupta, "Substation automation using IEC61850 standard," in *Fifteenth National Power Systems Conference (NPSC), IIT Bombay*, 2008, pp. 462–466.
[106] M. A. Aftab, S. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *International Journal of Electrical Power & Energy Systems*, vol. 120, p. 106 008, 2020.
[107] *Relion®Substation Merging Unit SMU615 - Technical Manual*, ABB, 2019. [Online]. Available: `https://library.e.abb.com/public/586023a61b7945339ab942bf4b41831a/SMU615_tech_758407_ENb.pdf?x-sign=ykOEusIwdW8l2q8OLZjy+F9szweTz8IZxoUQTdfPEafg6te58Rc8qkGUhYe0RSRO` (visited on 04/28/2022).
[108] *SIPROTEC Merging Unit 6MU805 - Manual*, Siemens, 2018. [Online]. Available: `https://cache.industry.siemens.com/dl/files/459/109742459/att_956306/v1/6MU805_Manual_A5_V040303_us.pdf` (visited on 04/28/2022).
[109] J. L. Blackburn and T. J. Domin, *Protective relaying: principles and applications*, 4th ed. CRC press, 2014.

This project is supported by the Belgian Energy Transition Funds