CYPRESS

Modeling for cyber-physical risk assessment

Task 2.1 - Project Report

Efthymios Karangelos, Mahdi Bahrami, Frédéric Sabot

Date: September 2024

Contents

Executive Summary

The CYPRESS project aims at developing novel knowledge, methods and tools needed to help ensure the security of supply through the transmission grid, while accounting for the specific nature of cyber-threats and integrating them into a coherent probabilistic risk management approach. It is articulated along three research themes, aiming to develop: i) novel models and benchmarks for computer simulation and laboratory testing of the cyber-physical electric power system security of supply, ii) techniques for assessing the cyber-physical security of electric energy supply, and iii) techniques for enhancing the cyber-physical security of electric energy supply. The project scope falls entirely within the category of "fundamental research" within the meaning of Regulation (EU) No 651/2014 because it is experimental and theoretical work undertaken essentially with a view to acquire new knowledge on the foundations of phenomena or observable facts. The project is not intended to develop commercial tools.

The work presented in this document has been performed in the frame of CYPRESS WP2, titled "Cyber-physical risk assessment of transmission systems". The objective of CYPRESS WP2 is to develop a coherent methodology for the *ex ante* assessment of the cyber physical risks facing the electric power system. The document is the outcome of task T2.1 titled "Modeling for cyber-physical risk assessment". The task was defined with two complementary modeling objectives. Firstly, to address the question of cyber-physical dynamic equivalent models allowing to abstract away smaller or neighbouring parts of a system while studying its behavior from a more global perspective. The precise scope here was to investigate how one could leverage existing approaches that allow to abstract away the physical behavior of the system sub-part in question, so as to also reflect their *cyber*-physical behavior. The second objective was to extend the scope of the physical benchmarks deemed relevant in task T1.3 so as to fit the needs of transmission grid cyber-physical risk assessment.

Chapters 2 and 3 relate to the first objective, namely the development of cyber-physical dynamic equivalent models to represent the behavior of sub-parts of the electric power grid. The work reported in both these chapters focuses specifically in the case of distribution grids. This has been identified by the researchers working in task 2.1 as the most relevant use case for representing external systems in the context of transmission level cyber-physical risk assessment. First, chapter 2 reviews and qualitatively assess different cyber-physical threats that may act on the distribution level of the electric power grid. The point here is to identify cyber threats that may have a noticeable impact as "seen" from the transmission grid. Then, chapter 3 details and demonstrates a chosen approach for the derivation of a simpler equivalent model of a distribution grid, on the basis of a corresponding detailed model. This approach could be used to develop alternative equivalent distribution grid models under the threats identified in chapter 2.

Chapter 4 documents the outcome of the effort to extend the scope of the benchmark systems

identified in Task 1.3, so as to fit the needs for cyber-physical risk assessment at the transmission level. It has to be noted that, from the onset of this effort, it was decided not to restrict the scope to the benchmarks identified in Task 1.3. The reason for this was the fact that the available description of such benchmarks was too generic to effectively distinguish them from any other academic benchmark. It was therefore decided to attempt to develop a generic process to extend the scope of any physical power grid benchmark with an inventory of the cyber infrastructure that allows monitoring and controlling the transmission system.

Author contributions

Efthymios Karangelos is the author of chapters 1 and 4 and editor of the report. Frédéric Sabot is the author of chapter 3 and co-editor of this report. Mahdi Bahrami is the author of chapter 2 of this report. Rick Loenders provided valuable comments on an early draft of chapter 4.

Author	Affiliation
Efthymios Karangelos (Task leader)	Université de Liège
Mahdi Bahrami	
Frédéric Sabot	Université Libre de Bruxelles

Table 1: List of Authors

1

Introduction

Security assessment is a function of paramount importance for the planning and operation of electric power systems. It aims at quantifying a set of selected metrics so as to ascertain whether or not the supply of electricity is acceptably secure. It can be performed *ex-ante* so as to inform planning and operational decision-making processes, as well as *ex-post* so as to evaluate the planning and operational processes themselves. In recent years, the transition towards low carbon electric power systems along with the significant growth in computational capabilities are causing a paradigm shift in electric power system security assessment. Deterministic approaches and criteria are progressively considered sub-standard. A risk-based approach taking into account the likelihood and potential impact of the threats facing the power grid (*e.g.*, the forced outage of system components, forecasting errors, extreme weather events, etc.) is practically acknowledged as necessary [1].

An important feature of the risk-based approach to power system security assessment is that it can be applied to many different types of events. For example, the same metric can be used to express the risk associated to potential wind power forecasting errors and/or the simultaneous outage of multiple transmission lines. In spite of the fact that these categorically different events may have different occurrence likelihood and modeling requirements, this allows to reason on their relative significance and effectively prioritize the use of limited security-enhancing resources. The application of a risk-based approach for electric power system *cyber*-physical security assessment seems to be a straightforward choice. The power system cyber-physical threat landscape is not only very broad but also dynamically evolving. Reasoning on the relative significance of alternative credible cyber-physical threats and the relative usefulness of countermeasures acting on the cyber sub-system or/and physical power grid can be achieved on the basis of risk metrics. The caveat is that power system cyber-physical risk assessment comes with additional modeling requirements.

On top of the large-scale and complex physical power grid, which in itself is challenging to model efficiently, a representation of the cyber sub-system and of its inter-dependency with the physical grid

is the minimum additional requirement[1]. Addressing this minimum requirement is complicated by the proliferation of so-called "smart technology" across all layers of the modern electric power system; from the core activities of bulk electricity generation, transmission, and through active distribution towards the edge activities of the grid end-users.

Modeling the cyber-physical behavior of the distribution level seems to be a necessity, in light of the increasing population of so-called electricity *prosumers*. These modern end-users actively interact with the electrical power system by owning and operating distributed generation resources and storage devices, participating in demand-side response schemes *etc.*. All such emerging activities are facilitated by proprietary *Information & Communication Technology* (ICT) with unknown functionalities and potentially untrustworthy cybersecurity properties. The prosumer ICT therefore belongs in the electric power grid cyber-physical threat surface and thus in the modeling scope for cyber-physical risk assessment. In addition to the large population of ICT devices with unknown properties, the modeling challenge is further complicated by the institutional separation of electricity transmission and distribution, which prohibits the open exchange of information between *Transmission System Operators* (TSOs) and *Distribution System Operators* (DSOs). There is therefore a need to model the aggregate dynamic behavior of the distribution level and do so in an adaptive manner that reflects both the inherent variability in the physical behavior of distributed renewable generation and the cyber-physical threats that could propagate upstream towards the bulk power system.

Focusing next at the bulk power system level, there is a lack of publicly available integrated cyber-physical benchmarks. Benchmarks for the physical part of the electric power grid exist in the public domain since several decades, and this has significantly benefited research and development of risk-based security assessment methods. The cyber sub-system of the power grid is a fast evolving system whose ICT components are continuously updated, hence less prone to standardization in the form of benchmarks. At the same time, transparency in the properties of the cyber sub-system and its inter-dependency with the physical power grid can be considered as detrimental to cyber-physical security and this prohibits the open publication of private benchmarks. Addressing the resulting modeling gap is a prerequisite for developing efficient methods for cyber-physical risk assessment.

This report documents the efforts of the CYPRESS consortium towards addressing the aforementioned modeling challenges for power system cyber-physical risk assessment. Chapter 2 reviews cyber-physical threats acting at the distribution level and qualitatively discusses the potential of such threats to further compromise the security of the bulk power system. Chapter 3 addresses the technical question of deriving distribution system dynamic equivalent models, that may be integrated in transmission level risk assessment studies and while reflecting the cyber-physical behavior of the distribution level. Chapter 4 reports on the exercise of complementing physical power system benchmarks with an inventory of the cyber infrastructure allowing to monitor and control the transmission grid.

[1] Modeling the exogenous strategies of independent adversaries (a.k.a. cyber attackers) that actively seek to identify and exploit known or unknown vulnerabilities of the cyber-physical system is also a relevant, yet not absolutely necessary, sub-task for cyber-physical risk assessment.

2

Relevant cyber-physical threats acting on the distribution system

This chapter reviews malicious attacks against the ICT components of power distribution systems, as well as of system end-users connected at the distribution level. The goal is to qualitatively identify cyber threats against distribution systems that may potentially impact the physical operation of the bulk power system. Models and data describing the behavior of the distribution system under such identified threats can then be shared from the distribution system operator to the transmission system operator so as to inform the process of cyber-physical risk assessment at the level of the bulk power system.

2.1 Cyber-attacks against the *Distribution Automation System* (DAS)

The DAS consists of cyber-enabled devices as well as standard communication protocols [2]. It includes a control center, wired and wireless communication networks, and *Feeder Remote Terminal Units (FRTUs)*. FRTUs can be used for communication with several devices in the distribution primary network, such as capacitor banks, or line reclosers [3]. DAS collects operational data from field devices and uses these for the purpose of system monitoring and control. Communication networks play a critical role in DAS. The cybersecurity of communications between distribution control center and DAS components is a crucial issue for *Distribution System Operators* (DSOs). This two-way data-flow could be compromised by malicious actors. The threat landscape[1] against the DAS includes attacks [4]:

[1] The threat landscape is the complete set of cyber-physical threats facing a cyber-physical system. As new (unknown) cyber-physical vulnerabilities may be discovered at any moment, the threat landscape should be considered as a dynamic set.

Manipulating the protection settings of field devices, such as relays or reclosers. If cyber-attackers change the proper settings of protective IEDs, two different possibilities may occur. When a fault occurs on the distribution feeder, a compromised protective IED could not detect the fault, and would, in turn, fail to operate. In this situation, the backup protection should operate and clear the fault. The other possibility is that the compromised IED maloperates. In other words, it would operate when not desired. Cyber-attackers may target the protection coordination among protective devices. Similar to the first scenario, if the main protection fails to operate, its corresponding backup protection should undertake the task. Thus, assuming that the coordination among protective devices is disrupted, a larger part of the distribution system will be affected by faults.

Issuing trip commands to switching circuit breakers, reclosers, or *Remote Control Switches* (RCSs) After successful intrusion into the cyber network of DAS, the cyber attackers can immediately send trip commands to switching devices. Consequently, undesired outages would occur in the target distribution system. In other words, the protective devices would experience maloperation (undesired tripping) owing to cyber attacks [5]. If the cyber-attackers coordinately launch this attack against several distribution systems, a significant amount of load demand will be disconnected from the power grid. This situation could potentially cause problems for power system dynamic stability.

Manipulation of measurement data. Cyber-attackers can falsify the measurements made in DAS so as to impact the distribution system. To achieve this goal, they can perform different malicious actions. For instance, they can manipulate operation data, such as voltage measurement, reactive power measurement, and feeder status [4]. In addition, the attackers could inject malicious data into DAS. These types of malicious actions can mislead DAS to make wrong decisions. For instance, upon occurrence of a fault on a distribution feeder, the Fault Detectors (FDs) sensing the fault current report it to the control center [6]. Attackers can manipulate cyber-enabled FDs to mislead the system operator to erroneously find fault locations. Cyber-attackers might try to mask the locations of physical outages by preventing the DAS from performing correct fault location. Alternatively, they might compromise the FDs in normal conditions to mislead the operator about the presence of faults.

Denial of Service (DoS) attacks against DAS. Cyber-attackers can render the DAS communication network unavailable. To this end, the attackers can use DoS attack strategies [7]. Switching devices (such as CBs, reclosers, RCSs) play a crucial role in the fault isolation and load restoration processes [8]. Cyber-attackers could disrupt the fault management process in the target distribution network by launching DoS attacks. For instance, attackers could flood targeted RCSs by sending unnecessary requests to them. In addition, they could overload their communication channel. As a consequence, the RCSs would not be reachable by the control center, and the operator, in turn, would not be able to isolate the faulty area from the rest of the network. Therefore, the faulty area would be extended [4]. In this situation, the customers' interruption duration would be significantly increased. In addition, this might even lead to distribution feeder de-energization. In this regard, if such cyber attacks were to be launched simultaneously, a sudden decrease in load demand would occur, which would have the potential to impacting the bulk system. As another important example for DoS attacks against DAS, the attackers can target the communication link between the control center and FDs. In the case of fault occurrence on DS feeders, DoS attacks could disrupt fault location task of DAS [6]. In this condition, the control center would not receive the fault location information. As a result, the service restoration to affected customers could not be started. To conduct this type of cyber attacks against DAS, the attackers have to be aware of fault locations. It is almost impossible for cyber-attackers to predict the locations of normal faults. However, cyber-attackers could launch hybrid attacks, including man-made faults on DS feeders and targeting the FDs' communication network by DoS attacks.

Table 2.1: EV load demand (GW) for different penetration levels and power charging rates [11]

EV Penetration Rate	Level 2 Chargers			Level 3 Chargers	
	7.2 kW	11 kW	19 kW	40 kW	240 kW
10%	1.44	2.2	3.8	8	48
20%	2.88	4.4	7.6	16	96
30%	4.32	6.6	11.4	24	144
40%	5.76	8.8	15.2	32	192
50%	7.2	11	19	40	240

2.2 Cyber-attacks against electric vehicle ecosystem

In line with the de-carbonization of transportation systems, a rapid transition from internal-combustion-engine vehicles to *Electric Vehicles* (EVs) is being made. As a result, the number of EVs is increasing. EVs are considered as a high-wattage demand-side appliance [9]. EVs are, to some extent, a controllable and/or price responsive load. Further, *Vehicle-to-Grid* (V2G) programs can be implemented by DSOs to allow EVs with the appropriate techonology to also send power back to the grid, thus behaving as a *Distributed Energy Resource* (DER). The cyber space of EV ecosystems is complex and consists of multiple actors interacting with one another through physical or cyber connections.

Given all these characteristics, the EV ecosystem can be viewed as an ideal attack surface for cyber-attackers seeking to disrupt the electric power grid. Cyber-attackers can easily collect some of the required data using the apps or websites of EV service providers. Using these data, they can plan and launch cyber attacks against EV ecosystems. According to [10], cyber-attackers could intercept and/or compromise the following types of data:

- Energy demanded or usage by EVs.
- EV information, such as battery capacity, charging rate, *etc.*.
- EV charging process parameters, such as charging prices and charging sessions *etc.*.

Cyber-attackers can target the amount of load demanded by EVs. Actually, the cyber attacks against EV ecosystem could lead to sudden drop or increase in the total load of the DS through different cyber attack scenarios. The extent to which DSs and TS can be impacted by such cyber attacks depends on several factors. Obviously, in order to disrupt TS operation, the changes in load demanded by EV users must be significant. To compare the load demanded by EVs with the total system load, the following example can be considered. According to [11] the total load demand of Manhattan is about 2100 MW, while there are 2 million cars. Obviously, the amount of EV load directly depends on the EV penetration rate. The amount of EV load for different EV penetration rates and power charging levels is given in Table 2.1. This analysis assumes that all of the EVs are charged at the same time, and there is no limit on the number of charging points.

Cyber-attacks against the EV ecosystem can be classified into the following categories.

Cyber attack against EV users charging behavior. Cyber attackers could cause spike or sharp drop in load demanded by EVs through manipulating EV charging prices. At the limit, this may cause a surge towards charging points and all of these could become occupied at the same moment. For instance, cyber-attackers could encourage EV users to charge their EVs during high-demand periods by lowering the charging prices. When a large number of EVs are charged in an uncoordinated way, the imbalance between generation and demand can cause a frequency drop [12]. To conduct this type of cyber attacks, Man-in-the-Middle (MITM) attacks can be launched between different entities of EV ecosystem, including Electric Vehicle Charging Stations (EVCSs), EV management system, EV aggregator, and EVs.

Denial of charging (DoC) attack. Malicious actors could stop the charging of EVs when they are in plug-in mode. To achieve this goal, they can disrupt EV charging process by launching attacks against EV charging infrastructures such that they become unavailable to EV users [10]. In addition, they could send fake charging requests to the charging management system [13]. Thus, legitimate EV users are deprived from charging, and charging points remain unoccupied. Such attacks could cause a significant drop in EV load demand if attackers launch this attack on a large EV fleet. Consequently, over-frequency protection might operate, and frequency-sensitive components, such as generation units, would be disconnected from the grid.

DoS attacks against EV ecosystem. DoS attacks may cause delays or interruptions in the transfer of data exchanged among different entities in EV ecosystem. Consequently, charging or discharging process of EVs can be disrupted. For instance, if the data exchanged between EV users and EV aggregator becomes unavailable due to DoS attacks, the EV owners would not be able to receive updates on the EV charging prices [14]. Therefore, they might reconsider charging/discharging decisions. This could shift EV loads from off-peak to on-peak periods.

Malware spread from EVs to EVCSs. The interaction between a plug-in EV and EVCS could be exploited by hackers as an entry point to launch cyber attacks potentially disrupting the power grid [15]. In a more sophisticated attack, a compromised EVCS can be exploited by attackers to spread malware across a network of EVCSs. For example, the attackers could disconnect all compromised EVCSs at once. This could cause a significant power mismatch between generation and demand, which would in turn threaten the system stability.

2.3 Cyber-attacks against DERs

With the growing penetration of DERs in DSs, the number of components in DSs owned and controlled by third-parties is increasing rapidly. DER units are equipped with communication and smart technologies. This makes the system vulnerable to malicious attacks. Notice that most of the installed PV units are privately owned. In addition, the owners are not usually aware of cybersecurity risks, and they, in turn, do not take security measures. Doing so is mostly the responsibility of the manufacturer. Thus, cyber attackers might use the opportunity to exploit a common-mode vulnerability for disrupting power system operation. Using this strategy, they could cause voltage regulation issues. DER cybersecurity can be studied at device-level and grid-level interactions. Additionally, to analyze the vulnerabilities of DERs, all possible cyber attacks should be taken into account. As most of the DERs are power electronics-based, cybersecurity of power electronic systems is now regarded as a heightened concern for the ongoing transition to renewable energy sources. Cyber-attackers could perform a range of malicious actions against DERs [16], such as:

Attack against inverter and algorithms. Targeting the inverter and its algorithms, attackers could perform different malicious actions including manipulating inverter set-points, shutting down the units, or causing damages. These cyber attacks could lead to over/undervoltage and unexpected power factor adjustments. In addition, the cyber attacks could potentially impact output power of DERs. As the DERs are operated in isolated and grid-connected modes, the attackers could impact DS by compromising a large number of DERs, especially when the power grid relies on DER production (*e.g.*, on-peak time or even at noon with low load, low inertia and high share of renewable PV production).

Targeting the grid by compromising DER units. Using this strategy the attackers aim at disrupting the grid operation. For example, after compromising the control system of DERs, they can simultaneously disconnect them from the grid. Similarly, they could cause an abnormal condition in the grid, and subsequently force the DER units to be disconnected. Indeed, voltage violations in DSs drive DER

protection system to disconnect the unit from the grid. Each of possible cyber attack scenarios against DERs could impact the grid. However, most of the scenarios can cause only local impacts [16]. In contrast, disconnecting a large number of DER units from DER-rich distribution grids would affect the transmission system.

2.4 Cyber-attacks against Advanced Metering Infrastructures

Advanced metering infrastructure (AMI) provides information such as customer power consumption, voltage, current, power factor, power flow to DSOs. In addition, AMI enables DSO to perform control actions such as connecting or disconnecting end-use customers from the power system. AMI consists of the following components [17]:

- Smart meter.
- Customer gateway.
- Communication networks.
- Head-end.[2]

Considering that these components are mainly installed at the end-user premises, cyber-security concerns relate to the energy usage pattern of customers and energy-related information. Indeed, the number of installed smart meters at homes and buildings to measure the amount of power consumption is expected to be many millions [18]. Thus, cyber attacks against AMI could potentially impact the energy delivery system. In particular, the cyber attacks directed at AMI have the potential to impact TS operation through several cyber attack scenarios, including:

Disconnecting/connecting commands to smart meters. If cyber attackers issue disconnect commands to a large number of smart meters, millions of customers will be disconnected from the grid simultaneously, which leads to a sudden decrease in load demand. Additionally, they could frequently connect and disconnect a large number of compromised smart meters. This attack type in turn could cause power grid instability [18].

Falsifying the energy prices. Using this strategy, cyber attacks aim at shifting loads to the times undesirable for the grid. This could lead to significant change in energy usage pattern of customers affecting the DS operation [19]. As a consequence, demand side energy management is disrupted. In addition, these attacks could cause secondary impacts, such as line congestion in DS and/or TS [20]. Notice that such an attack could of course also impact EV charging.

2.5 Cyber-attacks against the voltage regulation system

In this part, the impacts of cyber attacks on the DS voltage regulation are reported. In principle, the cyber attacks against voltage regulation system in distribution systems should be less harmful to transmission grids. The reason for this lies in controlling the voltage locally on distribution networks. In other words, these types of cyber attacks mainly lead to local impacts on local grids.

[2] The head-end performs data verification and preliminary processing.

Targeting voltage regulation devices. There are several components that contribute to voltage regulation in DSs, such as step voltage regulation, load ratio control transformers (LRTs), and shunt capacitors [21]. An LRT connects the distribution medium voltage level to a higher voltage level. It receives the required information from the sensors placed on distribution feeders, and accordingly regulates voltage through switching their taps at the secondary voltage level. Cyber attackers could launch an attack against tap-controller system. In consequence, voltage violation would occur on the distribution feeders. ''Unnecessary tap change'' is the most impactful cyber attack against LRTs, which results in over/under voltage at feeder nodes. In the case of capacitor banks, cyber attackers could switch them on/off, thereby changing their configuration [22]. This malicious action changes the voltage profile of distribution feeders.

Targeting the capability of DGs to regulate voltage. As discussed earlier, the DER units can provide ancillary services to regulate voltage in DSs. This is often done by the power-electronics equipment. The attackers could cause voltage violations on the customer-side grid, where a large number of DERs have been placed. In response to voltage violation, the protection function of grid-connected DERs will operate by changing the output power of the DERs, and this, in turn, would make the situation worse.

DoS attacks against voltage regulation. In order to coordinate different voltage controllers in a DS, communication networks are deployed. Therefore, the attackers could target the communication network by launching DoS attacks, such as causing data transfer delay, dropping legitimate packets, or blocking the communications among the local voltage controllers and the control center. Delayed or missing information could lead to abnormal voltage on distribution feeders.

3

Equivalent modeling distribution grids for transmission level risk assessment

Distribution grids have historically had a passive role in the organisation of the electricity sector. With the energy transition, this is quickly evolving as a growing share of the electricity production is done via distributed energy resources (DERs). In parallel, new "smart loads" are appearing in distribution grids. Smart loads are loads that are controlled by digital technologies in order to be more "grid-friendly". A typical example is the use of smart chargers for electric vehicles (EVs) allows EVs to preferentially charge when load is low and/or to alleviate grid constraints. While smart devices are useful and even necessary to reach our climate goals, they introduce new vulnerabilities in power grids. In consequence, it may be necessary to also model the dynamic behavior of such sub-systems in order to accurately assess the cyber-physical risk facing the transmission system. This of course comes at extreme computational cost, given the expansion of the modeling scope. A possible solution is the representation of distribution sub-systems through dynamic equivalent models. This chapter explores this alternative.

3.1 Literature review

Modelling distribution grids is complex due to the sheer amount and variety of elements that are connected to them, and due to the low visibility of those elements. Indeed, a national transmission grid typically connects dozens up to hundreds (depending on the size of the country[1]) of power plants whose power outputs can directly be measured by the TSO. Distribution grids however can connects up to millions of houses, each with dozens of appliances.

[1] See e.g. [23] for a breakdown of the number of power plants per voltage level in Great Britain

This complexity explains why transmission utilities have long been using very simple load models[2]. Since the beginning of the century, there has been renewed interest in load modelling, first, due to the failure to reproduce some blackouts in post-mortem analysis in grids with high share of motor loads [24, p11-12], and more recently, due to increasing penetration of DERs and smart loads.

The most commonly-used load models (in industry and academia) are reviewed in section 3.1.1. However, the most difficult and critical part of load modelling is not to choose a given model but to define adequate parameters for the chosen model such that it represents as best as possible the reality. Section 3.1.2 thus reviews the techniques that can be used to estimate the parameters of those load models.

3.1.1 Commonly-used load models

Static load models are the simplest and thus most commonly-used load models. Static (or time-invariant) load models are used to represent loads whose power demand instantaneously changes after a change in supply voltage and/or frequency at the connecting bus [24]. They can generally be written in the form

$$\begin{cases} P = f_P(U, f) \\ Q = f_Q(U, f) \end{cases} \tag{3.1}$$

where P and Q are the active and reactive power demand of the load, U is the voltage at the load, f is the frequency at the load, and f_P and f_Q are arbitrary functions. The most famous example is the ZIP load model that consist in a constant impedance (Z), constant current (I) and constant power (P) load in parallel, mathematically described (for the frequency-independent version) by

$$\begin{cases} P = P_0 \left[\alpha_0 + \alpha_1 \dfrac{U}{U_0} + \alpha_2 \left(\dfrac{U}{U_0} \right)^2 \right], \quad \alpha_0 + \alpha_1 + \alpha_2 = 1 \\ Q = Q_0 \left[\beta_0 + \beta_1 \dfrac{U}{U_0} + \beta_2 \left(\dfrac{U}{U_0} \right)^2 \right], \quad \beta_0 + \beta_1 + \beta_2 = 1 \end{cases} \tag{3.2}$$

Motor load models are dynamic models that represent loads with a significant share of motor load. They are often used in grid that are susceptible to fault-induced delayed voltage recovery (FIDVR). Indeed, when a short-circuit occurs in a grid, it leads to low voltages in the neighbouring area. Motors near the short-circuit are thus unable to draw enough electric power and thus slow down. When the short-circuit is cleared, motors draw additional active and reactive power in order to get back to their initial speed. This inrush of power demand negatively impacts voltage stability and can cause FIDVR events and even loss of stability. Such behaviour cannot be represented with static load models and thus requires more complex models. Models of varying complexities are reviewed in [24]. An example is the Western Electricity Coordinating Council (WECC) composite load model (CLM) [25]. The CLM is shown in Fig. 3.1. It consists in an on-load tap changer (OLTC), and equivalent feeder impedance, four different types of dynamic induction motor models, and electronic and a static (i.e. ZIP) load. A more detailed description is given in [25]. It can be noted that this model is mostly used in the US as the North American Electric Reliability Corporation (NERC) is progressively making the use of this model mandatory in dynamic stability studies [26]. The interested reader is referred to [24], [27] for more detailed and exhaustive review of static and motor loads.

Active distribution network (ADN) models focus on modelling DERs and/or smart loads. They are thus of great interest in this project as DERs and smart devices are an important target of cyber-attacks. ADN models can significantly vary in complexity. The simplest model is a constant power

[2] From a transmission system perspective, load and distribution system can be seen as synonyms (large industrial loads that are directly connected to the transmission system will typically have a dedicated model and are not considered in this report).

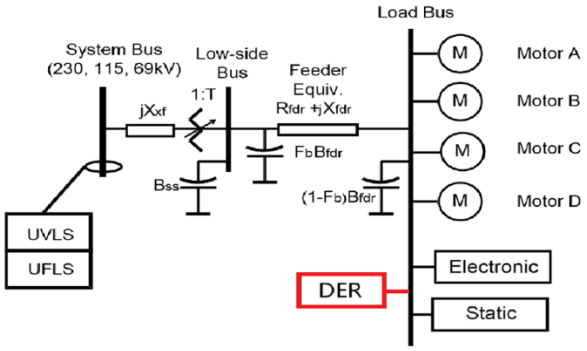


Figure 3.1: WECC composite load model [25]

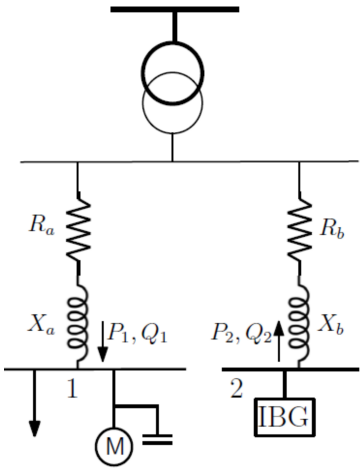


Figure 3.2: Example of an ADN model [28]

load with a step change in power drawn. The step change could represent the disconnection of many DERs, the simultaneous start of charge (e.g. due to a cyber-attack) of many EVs, etc. More complex ADN models include the WECC CLM (in its latest version) as it include a model of DERs (Fig. 3.1)[3]. Complex ADN models are often composite-type loads, i.e. are made of multiple aggregated models behind equivalent impedances as shown for example in Fig. 3.2.

Black-box models refer to models obtained with machine-learning (ML) techniques. The advantage of these models is that they do not require any information about the topology, connected assets, controls, etc. of the modelled distribution network. They are thus often used when only (time-series voltage and power) measurements at the point of common coupling (PCC) between the transmission and distribution grid are available. The disadvantage is that large-disturbances and cyber-attacks are (hopefully) rare events, it can thus be difficult to obtain enough useful measurements to train a machine learning model. Black-box models can also be used with simulated data instead of measurement data, however, ADN models (also called grey-box models in this context) can be preferred as they provide results which are easier to interpret.

Transmission and distribution (T&D) simulations explicitly represent all buses of a distribution system (down to a given voltage level) instead of using equivalent models. They theoretically allow for the best possible accuracy, however, they have significantly higher data and computation time requirements than the other methods. They are thus only used in small grids with a very large share of DERs

[3]It makes sense to represent both motors and DERs in a load model as they tend to interact. Indeed, motors tend to cause FIDVR events, and DERs often trip themselves when low voltages occur.

(e.g. Hawaii [29]), or as a benchmark in academic problems. T&D simulations can be performed using a single simulator or by coupling a transmission-focused simulator with (usually multiple instances of) a distribution-focused simulator [30].

3.1.2 Defining the parameters of load models

As mentioned above, having detailed load models is only useful if adequate values are set for the parameters of the models. Again, this is very challenging as load models aim to represent a large number of assets over which TSOs (and DSOs) have little visibility. Moreover, some load models can have a high number of parameters, e.g. the WECC CLM has more than 100. This section thus reviews the approaches available from the literature to define the parameters of load models.

Fitting approaches are a range of techniques in which the parameters of a load model are fitted such that the load model behaves as close as possible to a reference for a given set of disturbances, i.e. such that it's time response fits the reference. The reference behaviour can be defined either from measurements of the real load or from simulation results (in the latter case, we talk about model reduction or dynamic equivalents). Again, large disturbances are rare, so it might be difficult to obtain a diverse set of disturbances to fit the model with[4]. This is especially true for cyber disturbances. However, measurements should be used to validate simulations results when available.

Parameter fitting can be defined as searching a vector of parameters $\boldsymbol{\theta}$ that satisfies

$$\min_{\boldsymbol{\theta}} F(\boldsymbol{\theta}) = \frac{1}{d}\sum_{j=1}^{d}\left[F_P(\boldsymbol{\theta}, j) + F_Q(\boldsymbol{\theta}, j)\right] \tag{3.3}$$

$$\text{with } F_P(\boldsymbol{\theta}, j) = \frac{1}{N}\sum_{t=1}^{T} w_P(j,t)\left[P(\boldsymbol{\theta}, j, t) - \hat{P}(j,t)\right]^2 \tag{3.4}$$

$$F_Q(\boldsymbol{\theta}, j) = \frac{1}{N}\sum_{t=1}^{T} w_Q(j,t)\left[Q(\boldsymbol{\theta}, j, t) - \hat{Q}(j,t)\right]^2 \tag{3.5}$$

$$\boldsymbol{\theta}^L \leq \boldsymbol{\theta} \leq \boldsymbol{\theta}^U \tag{3.6}$$

where P (resp. Q) is the active (resp. reactive) power consumed by the load (often defined at the PCC), $\hat{P}$ and $\hat{Q}$ are the reference active and reactive power consumed by the load, w_P and w_Q are arbitrary weight functions, and $\boldsymbol{\theta}^L$ and $\boldsymbol{\theta}^U$ are lower and upper bounds on the parameters of the dynamic equivalent. The index j refers to the jth disturbance in the training set, and index t refers to time.

The model can either be a physical model (motor load, ADN, etc., sometimes referred to as grey-box models) or a ML model (black-box models). As if is often impossible to derive an analytical formulation for $F(\theta)$, derivative-free or metaheuristic techniques need to be used to solve the optimisation problem. For grey-box models, differential evolution and particle swarm optimisation are commonly used. For ML models, the appropriate ML techniques are used depending on the type of ML model chosen.

Component-based approaches are based on surveys that estimate what share of the load that is consumed by different categories of loads (e.g. residential vs. industrial, paper mill vs. steel mill). Rules of association can then be used to translate those shares into parameters for a given load model. In the literature, most rules target static load models or the WECC CLM [31]. Defining new rules of association requires a significant amount of expert knowledge and lab testing (to model individual classes of loads). Such approaches might thus prove difficult to apply to new load models and to emerging issues such as cyber-threats.

[4] It should be noted that the best parameters for a load model will change with the operating conditions of the load as different kinds of devices tend to be connected at different time of the day. This renders even more difficult the measurement gathering issue.

3.2 Selected approach

Based on the above discussion, the fitting approach has been chosen for this project as it is the most flexible and thus allows us to easily incorporate cyber elements in the load models. The main challenge with this approach is to define an adequate reference $\left((\hat{P}(j,t),\hat{Q}(j,t))\right)$ to train the model. As already discussed, real measurements won't be available for most potential cyber-attacks, so simulation results need to be used. It is frequent in the literature to use fully-detailed models of distribution grids to generate the reference signals for the considered disturbances (see e.g. [32]). Such models explicitly represent all electrical buses (down to a given voltage level) of the distribution network and assume know dynamic models for all the connected elements. In practice however, the data necessary to build such model are often unavailable even for the DSOs, especially dynamic data. This issue has only recently been addressed in [28], [33], [34]. Based on those work, we proposed a new framework that is described below. The remaining of this section is based on a paper we published during the project [35].

The framework consists in two main parts. In the first part, a detailed model of the considered distribution grid is built and probability density functions (pdfs) are defined for each of the parameters of the detailed model. Indeed, while it is difficult to have a detailed model with known parameters, it is very possible to define a model with uncertain parameters. Due to lack of data, the pdfs of the parameters will be relatively wide to represent the possible range of values that the parameter could realistically take. For example, industrial motors typically have a stator resistance between 0.01 and 0.05pu [28], so the pdf of the "stator resistance" parameter of the load model could be defined as a uniform distribution[5] on [0.01, 0.05] pu. Monte Carlo (MC) simulations are then performed on a predefined set of training disturbances to assess the impact of the uncertain modelling of the load on its behaviour. Thus, instead of having a single value for $\hat{P}(j,t)$ and $\hat{Q}(j,t)$, we obtain pdfs from the MC simulations. Then, for each disturbance and point in time, we can compute statistical indicators such as the ith percentile $\mathscr{P}_{P,i}(j,t)$ (resp. $\mathscr{P}_{Q,i}(j,t)$) of the active (resp. reactive) power likely consumed by the load and the associated standard deviation $\sigma_P(j,t)$ (resp. $\sigma_Q(j,t)$).

In the second part, we build two dynamic equivalents of the distribution system model to bound the uncertain behaviour of the distribution grid: one (referred to as the 5-equivalent) that fits the 5th percentile of the active and reactive power of the distribution system, and one that fits the 95th percentile as shown in Fig. 3.5 (other percentiles can of course be computed). It should be noted that percentiles are computed individually for each disturbance and each point in time. Those percentiles are thus synthetic and represent an envelope of the possible behaviours of the distribution grid, not a likely behaviour. To build those dynamic equivalents, an optimisation problem similar to (3.6) can be defined:

$$\min_{\boldsymbol{\theta}} F(\boldsymbol{\theta}) = \frac{1}{d}\sum_{j=1}^{d}\left[F_P(\boldsymbol{\theta},j)+F_Q(\boldsymbol{\theta},j)\right] \tag{3.7}$$

$$\text{with } F_P(\boldsymbol{\theta},j) = \frac{1}{N}\sum_{t=1}^{T}\left[\delta_{i,P,j,t}\frac{P(\boldsymbol{\theta},j,t)-\mathscr{P}_{P,i}(j,t)}{\sigma_P(j,t)}\right]^2 \tag{3.8}$$

$$F_Q(\boldsymbol{\theta},j) = \frac{1}{N}\sum_{t=1}^{T}\left[\delta_{i,Q,j,t}\frac{Q(\boldsymbol{\theta},j,t)-\mathscr{P}_{Q,i}(j,t)}{\sigma_Q(j,t)}\right]^2 \tag{3.9}$$

$$\boldsymbol{\theta}^L \le \boldsymbol{\theta} \le \boldsymbol{\theta}^U \tag{3.10}$$

with

$$\delta_{5,P,j,t} = \begin{cases} 1 & \text{if } P(\boldsymbol{\theta},j,t) \le \mathscr{P}_{P,i}(j,t) \\ \frac{1}{2} & \text{if } P(\boldsymbol{\theta},j,t) > \mathscr{P}_{P,i}(j,t) \end{cases} \tag{3.11}$$

[5] Uniform distributions are often used when little data are available. They tend to give conservative results as they assume extreme values (inside the support of the pdf) as likely as average values.

$$\delta_{95,P,j,t} = \begin{cases} 1 & \text{if } P(\boldsymbol{\theta}, j, t) > \mathscr{P}_{P,i}(j,t) \\ \frac{1}{2} & \text{if } P(\boldsymbol{\theta}, j, t) \leq \mathscr{P}_{P,i}(j,t) \end{cases} \tag{3.12}$$

and with the term $\delta_{i,Q,j,t}$ that has a similar definition. This factor results in a lower penalty for the equivalent that fits the 95th percentile if it consumes too much power and in a lower penalty for the 5-equivalent if it consumes too little. This leads to more conservative bounds on the behaviour of the distribution system. Different coefficients can be used if deemed necessary. In our tests, the differential evolution (DE) algorithm was used to solve the optimisation problem, although other algorithms could potentially have been used. DE is stopped once sufficient accuracy is reached, i.e. when

$$F_P(\boldsymbol{\theta}, j) \leq 1 \text{ and } F_Q(\boldsymbol{\theta}, j) \leq 1 \tag{3.13}$$

3.3 Example application on an ADN model

In order to illustrate our proposed framework, we now use it to define the parameters of an ADN model and show how to use the model in transmission studies. The transmission study considered in this example is the computation of critical clearing times (CCTs) of generators. In [35], we also showed that our approach can be used in the more difficult (i.e. sensitive to modelling accuracy) problem of cascading outage simulation, we refer the interested reader to the publication for more technical details and to [6] for implementation details.

3.3.1 Test case

The distribution system considered in this example is based on the CIGRE medium voltage (MV) network shown in Fig. 3.3a. For this specific network, the static data is known but no dynamic data is available. We are currently working on an application where even static data is unknown [36]. Realistic pdfs have thus been assigned to all the dynamic parameters of the model. It can be noted that we made some modification to the CIGRE MV network, most notably, we increased its DER penetration to 50%.

The considered dynamic equivalent (i.e. load model) is a relatively simple model made of one load bus connected to the transmission grid by an equivalent impedance and a distribution transformer as shown in Fig. 3.3b. The load bus consists of an exponential load, two first-order inductor motor models (to allow for partial stalling of motors), and two inverter-based generation (IBG) models (one that represents PV units, and one that represents wind). As the model of IBGs in the dynamic equivalent represent an aggregate of the many DERs from the full distribution model, their models have been slightly modified to allows for partial tripping (e.g. the power output of the model can be reduced by say 30% to represent the fact that 30% of the DERs might have tripped following a disturbance). An overview of the IBG model is shown in Fig. 3.4

Finally, the transmission system considered in this example is the IEEE 39-bus test system [38], [39] but with all loads replaced by copies of the CIGRE MV network (for full T&D simulations used as a benchmark) or by our dynamic equivalent. Some synchronous generators where removed from the transmission network to account for the fact that 50% of the load is now satisfied by DERs.

3.3.2 Training the dynamic equivalent

It is common to "train" an equivalent by connecting it to an infinite bus to which voltage (and possibly angle and frequency) disturbances are applied [24], [28], [32]. However, we found that connecting it to a synchronous machine that has roughly the same rating as the total gross load through a line with an impedance of 0.1 pu leads to equivalents which are more accurate in transmission studies. This is because it allows for easier incorporation of FIDVR events into the training set of the equivalent. It should be noted that the synchronous machine and line do not aim to be an equivalent of the

[6] `https://fredericsabot.github.io/publications/isgt2023`

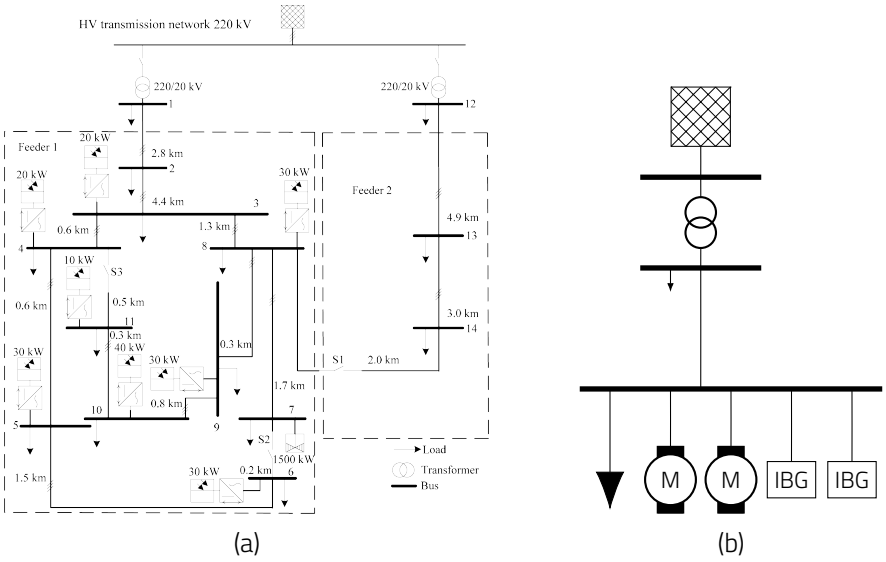


Figure 3.3: (a) CIGRE MV network with solar and wind generation [37], (b) Dynamic equivalent

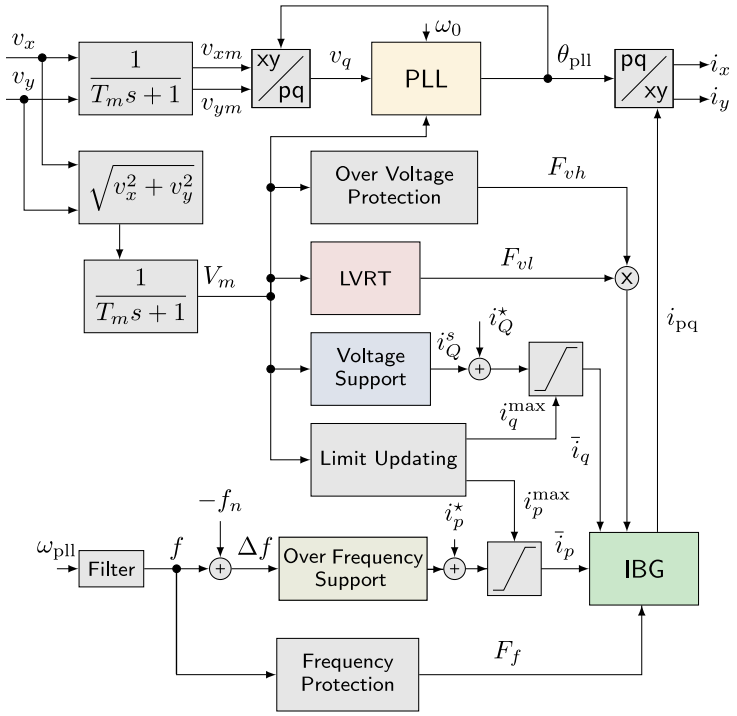


Figure 3.4: Overview of the IBG model, adapted from [34]

Table 3.1: Training disturbances

Id	Voltage dip (pu)	Duration (ms)
1	0.2	100
2	0.2	200
3	0.3	100
4	0.3	200
5	0.4	100
6	0.4	200
7	0.5	100
8	0.5	200
9	0.7	100
10	0.7	200
11	0.8	200
12	0.8	500
13	0.9	500
14	0.9	1000

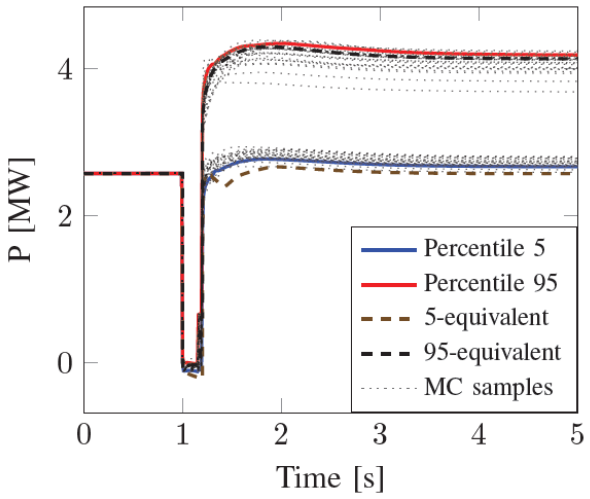


Figure 3.5: Reduced (dashed) *vs* unreduced (dotted and full) models – disturbance 6

transmission system as seen from the distribution system. Indeed, as shown later in this section, we obtained accurate results when using the equivalents in different locations of the transmission system with varying system strength (i.e. some places located close to synchronous machines and some located remotely). In [35], we even showed that equivalents trained this way are adequate to be used in simulations of cascading outages during the system strength can significantly vary as machines are disconnected.

The training disturbances used in this example are impedant short-circuits of different durations applied at the PCC leading to more or less severe voltage drops (representing short-circuits on the transmission system that are more or less close to the considered distribution network) as listed in Table 3.1.

The behaviour of the CIGRE MV network and its dynamic equivalents for the disturbance 6 (voltage drop to 0.4 pu during 200ms) are shown in Fig. 3.5. As dynamic data is uncertain for the full network, MC simulations show multiple likely behaviours (dotted lines). We then compute the 5th and 95th percentiles of the behaviour of the full model and use each of them as a reference to train two dynamic equivalents (dashed lines).

Table 3.2: CCTs computed using dynamic equivalents and probabilistic T&D simulations

Generator	CCT 5-95 bounds (ms)	
	Equivalents	T&D
30	[550, 616]	[554, 631]
31	[240, 264]	[244, 255]
32	[200, 214]	[200, 210]
35	[214, 244]	[220, 234]
37	[244, 264]	[242, 260]
38	[180, 210]	[184, 194]
39	[634, 700+]	[648, 700+]

3.3.3 Using the equivalents in transmission studies

We now show how the developed models can be used in transmission studies. In this example, the study performed in the computation of CCTs of generator. The CCT is the maximum clearing time of a short-circuit occurring at the generator terminal that can be allowed before the generator loses synchronism with the rest of the system. The CCT of a generator is usually computed by simulating progressively longer short-circuits on the generator until it loses synchronism. However, in our case, we built two dynamic equivalents (a 5- and a 95-equivalent), so we will perform the CCT calculation twice: once using the 5-equivalent for all loads, and once with the 95 equivalent[7]. This gives two values for every CCT. The actual value most likely falls in the range between the two computed values.

Table 3.2 shows the ranges computed for the CCTs of all generators of the IEEE 39 network. The table also shows the 90% confidence intervals of those CCTs computed with full (probabilistic, since dynamic data is uncertain) T&D simulations. It shows a very good agreement between results obtained with the equivalents and the T&D simulations, although the ranges computed with the equivalents are slightly wider.

3.4 Conclusion

In this chapter, we build two dynamic equivalents based on high and low percentiles of the behaviour of an uncertain distribution grid model. Those equivalents were then used to build statistics-informed bounds on the results of (transmission) stability studies. We showed that those intervals match actual confidence intervals that could be obtained using probabilistic T&D simulations in CCT computations and simulations of fast cascading outages. Perspectives for future work include considering other kinds of loads (e.g. variable-speed drives), and DERs (e.g. combined heat and power plants) in the equivalents as well as distribution grids facing cyber-physical threats; and assessing and improving the robustness of the equivalents to varying operating conditions.

3.5 Acknowledgement

Computational resources have been provided by the Consortium des Équipements de Calcul Intensif (CÉCI), funded by the Fonds de la Recherche Scientifique de Belgique (F.R.S.-FNRS) under Grant No. 2.5020.11 and by the Walloon Region. We would like to thank Gilles Chaspierre for providing us with the codes used in his previous work.

[7] This implicitly assumes a strong correlation between the uncertainties in the models of all distribution grids of the network. In practice, it might be extremely difficult to estimate what part of load modelling uncertainty has strong correlation between loads at different locations (e.g. temperature dependence, devices from a same manufacturer) and what part is independent. However, assuming strong correlations will most likely lead to conservative results as it will often lead to more severe events (e.g. all DERs in a zone disconnect).

4

Towards cyber-physical benchmarks for transmission system risk assessment

4.1 Introduction

The development of methods and tools for electric power transmission system risk assessment has relied on the public availability of numerous benchmarks. The physical characteristics of these benchmarks range in various ways: from smaller academic systems useful to demonstrate the first principles of new ideas/methodologies to larger realistic systems useful to validate scalability and real-life applicability; from systems relying on conventional generation resources (*i.e.*, nuclear, coal, oil, gas and hydro) to systems featuring a large penetration of modern renewables; from systems featuring limited transmission capacity and challenged by static (in)security to systems featuring limited voltage control capability and/or inertia and challenged with dynamic (in)security; from single-area, single-TSO, transmission level systems to multi-area, multi-TSO and multi-DSO transmission and distribution level systems; from systems fitting the legacy single-utility vertical organization for the planning & operation of generation, transmission and distribution to systems organized according to modern decentralized approaches featuring electricity prosumers and active distribution networks. As reviewed in [39], the vast majority of such benchmarks concerns only the physical layer of the system, with the cyber sub-system of the power grid remaining out of scope. This chapter documents the results of our effort to extend the scope of the benchmark systems identified in [39] to fit the needs of cyber-physical risk assessment at the transmission level.

4.1.1 Literature review

To set the stage, we briefly introduce here the few notable exceptions of electric power grid cyber-physical benchmarks that have been published in peer-reviewed journals or conference proceedings. Notice that we introduce such publications in chronological order. Further notice that we exclude from this review publications concerning testbeds that combine software and hardware to model the cyber-physical electric power grid.

Stefanov and Liu extended the physical model of the IEEE 39-bus benchmark with a model for its SCADA system [40]. This cyber sub-system model features three distinct hierarchical levels, the substation level, the control centre level and the (highest) transmission operator level. This model includes the population of ICT devices for every such level, with all substations sharing a common architecture. Models for the behavior of these ICT devices are also included, permitting the co-simulation of the cyber-physical power grid. Unfortunately the resulting cyber-physical model of the electric power grid seems to be proprietary.

Weaver *et al.* proposed a set of ICT devices facilitating transmission protection, control and communication applications on top of the WECC 9-bus, 3-generator transmission system model [41]. A novel feature of the so-called resulting "8 – Substation" model was the consideration of alternative physical and cyber topologies per substation. Further, in addition to the population of ICT devices composing the cyber sub-system, this work also developed an ontology as well as a modeling format. The proposed set of ICT devices, including functional descriptions and identifiers for respective commercially available hardware, remains to date accessible online[1].

Jillepalli *et al.* developed the so-called "METICS" cyber-physical model on top of the IEEE 14-bus benchmark system [42]. The modeling scope and the level of detail in the representation of the cyber sub-system is apparently extended with respect to the "8-Substation" model. Indeed, the METICS model appears to include additional operational and non-operational functionalities (indicatively, Phasor Measurement Units, Billing Department, Historian, Enterprise Workstations, *etc.*). However, the physical representation of the transmission grid seems to remain at the bus – branch resolution, which begs a question on the level of detail for the modeling of individual ICT components. This model is publicly available only in the format of some high-level drawings.

Reference [43] attempts to introduce a model of the communication network topology for a large-scale synthetic[2] model of the Texas Electric Power Grid. Although the synthetic grid in question has 2000 nodes, the communication network model seems to be generated only for the sub-grid of the McAllen zone which consists of 71 substations. In order to represent the communications network of this grid, the authors generate a population of links and nodes with specified attributes. Sub-classes of the node object represent selected power grid ICT components and specifically switches, routers, firewalls, relays, RTUs, relay controllers and cyber nodes (*e.g.*, office computer, card reader, *etc.*).

The transmission grid communication network topology is also the scope of the generative model introduced in [44]. The authors explore the use of several alternative algorithms so as to generate random graphs that match the graph characteristics (as in sparsity, amount of cyclic structures, connectivity between higher degree nodes and lower degree nodes) of a real-life power grid communication network. While the resulting graphs may indeed bare similarity to the original graph, it is unclear how one could populate the ICT infrastructure for protection and control on top of these.

A tool for the generation of synthetic cyber-physical electric power distribution systems has been presented in [45]. This tool includes a simplified representation of the distribution level cyber subsystem, mapping each node of the physical system to a single host and a single switch.

Most recently, Shashank *et al.* introduced a set of algorithms to develop a graph representation of cyber-physical interactions in an electric power transmission system [46]. The resulting graph includes instrument transformers, digital relays and engineering workstations as additional nodes on top of the physical system graph. It is noteworthy that the starting point for the application of these algorithms is a file contaning the data for the physical grid in bus – branch resolution. The algorithms

[1] `https://github.com/cptlc/cptl-models/tree/master/cypsa-8sub`

[2] A synthetic model of the Texas Power Grid is similar but not the same as the original Texas Power Grid.

complement this minimal input with the necessary additional detail based on known standard practices. Unfortunatelly this paper includes neither a precise documentation that would enable to reproduce the proposed algorithms nor any pointer to code implementing these.

4.1.2 Intended contributions

The cyber sub-system of the electric power grid facilitates the broad spectrum of control, communication, computation and data warehousing applications that are necessary to operate the grid with acceptable security and while enabling the trade of electrical energy as a commercial commodity. With a view on cyber-physical risk assessment at the transmission level, we define a scope of work that focuses on the operation of the transmission grid. Concretely, it includes the population of ICT devices that compose the grid's Substation Automation Systems (SASs), Regional and National Control Centres (RCCs/NCCs) and allow these digital entities to communicate. This scope is aligned with [40], [41].

Our primary intended contribution is to provide an inventory of cyber assets complementing the inventory of physical assets of an available transmission grid benchmark and the respective cyber-physical power grid graph. Rather than focusing on a specific case study, we develop a process that works in a system-agnostic manner and considers the grid topology, represented at the bus-branch resolution, as a minimal required input. The output of this process can be leveraged in conjunction with freely-chosen models for the cyber and physical components of the power grid in order to develop and/or demonstrate methods and tools for electric power transmission system cyber-physical risk assessment. To this end, we envision the public release of the accompanying code that implements the developed process, allowing for user-specified design choices to be integrated as optional inputs. We document here all such optional design choices along with an overview of the respective alternatives. Notice finally that, as a side-contribution, we extend the *Hyper Heterogeneous Multi Graphs* (H2MGs) formalism introduced in [47] with additional hyper-edge clases relevant for cyber-physical rather than physical power system modeling.

4.2 Cyber-physical power grid modeling overview

In order to represent the power grid cyber and physical infrastructure in an integrated manner, we adopt the so-called *Hyper Heterogeneous Multi Graphs* (H2MGs) modeling formalism. As introduced in [47], the H2MG is a structure consisting of *hyper-edges* and *addresses*. Addresses bear no properties but rather serve as interfaces between hyper-edges of various *classes* and *orders*. All hyper-edges belonging in the same class are of the same *order*, meaning that they have the same number of ports and thus can connect to the same number of addresses (through which they interface with other hyper-edges of the same/different class). The original application of the H2MG formalism in [47] was developed for the bus-branch representation of the physical power grid and distinguishes between *bus, generator, load, shunt, line* and *transformer* hyper-edge classes.

We first extend this set of hyper-edge classes so that it is also compatible with the representation of a physical power grid in the node-breaker resolution, by adding the switchgear (*i.e.*, *breaker* and *disconnector*) hyper-edge classes. We further introduce additional hyper-edge classes so as to also represent the cyber sub-system of the electric power grid. A particular challenge is that the properties of the cyber sub-system components are far more versatile than those of the grid's physical components. We define hyper-edge classes for generic cyber sub-system components that are inspired from the typical properties of commercially available devices. Notice that contrary to the physical components of the grid that share a common port type (electrical terminal), a single component of the cyber sub-system may host interface ports of different types (*e.g.*, analogue input/output ports, Ethernet ports, *etc.*) for exchanging messages of various formats. We identify the number of different ports per type, along with the message formats (and respective communication protocols supported) as part of the hyper-edge class definition.

4.3 Converting the grid topology at the node-breaker resolution

Since several decades, the bus-branch resolution has been considered as an adequate level of modeling detail for electricity markets, steady-state power system security assessment studies and power system optimization applications. It indeed allows to represent steady-state power flow across the major components of the grid and while containing the grid model to a relatively modest size. Suggestions to migrate to the finer node-breaker model in steady-state security assessment and planning applications have recently appeared [48]. The node-breaker modelling resolution represents in greater detail the topology of power transmission substations by additionally including the switchgear that connects the grid's main components.

Using this resolution is necessary towards the development of a cyber-physical power grid benchmark. Indeed, sensors and/or instrument transformers feed the power grid's cyber sub-system with data refering to precise points within a particular *bay*[3] of a substation rather than at an aggregate bus. Moreover, the actuators commanded by the cyber sub-system open and close the grid's switches and circuit breakers to connect/disconnect distinct circuits. The issue is however that most physical power grid benchmarks, including the ones surveyed in [39], have only been published in the bus-branch resolution. To address this issue, we have developed a process to convert from the bus-branch resolution to the node-breaker resolution and implemented this process in the Julia programming language.

In the H2MG formalism, we integrate switchgear, instrument transformers and sensors by creating respective hyper-edge classes as shown in Table 4.1. The switchgear (*i.e.*, switch and circuit breaker) classes are of order six. Any switch or breaker has a pair of electric power terminals connecting to respective addresses of the physical power grid. We recall here that circuit breakers serve to promptly interrupt a protected circuit in case of a detected fault conditions. (Disconnect) switches serve to guarantee that an electrical circuit is de-energized so as to avoid any risk. Although the electrical end-effect is similar, the functional difference is represented by the additional attribute 'Breaking Capacity (kA)' of the circuit breaker hyper-edge class. Foreseeing the possible redundancy in the cyber sub-system architecture the remaining two (cyber) port pairs of a breaker/switch allow its point-to-point interconnection for cyber input and output exchange with two redundant interface units. Through these interconnections, switchgear devices can communicate their open/close status and receive commands.

In order to facilitate modeling the data acquisition that supports the operation of the power grid, in the lower part of Table 4.1 we already introduce hyper-edge classes for *Current Transformers* (CTs), *Voltage Transformers* (VTs). Although the physical quantity in the scope of such devices differs, at the considered representation granularity it remains possible to define hyper-edge classes sharing the same attributes. More specifically, we define hyper-edge classes of order three. In addition to a primary winding representing the connection of these devices to the respective HV circuit, two analog output (cyber) ports allow again the possibility for redundant point-to-point connections for communicating analog output upstream in the cyber sub-system. We also introduce an additional generic hyper-edge class of order five. This can be used to represent the various *Non-electrical Sensors* (NeS) (*e.g.*, temperature sensors, pressure sensors, *etc.*) that furnish several measurements from the physical power grid towards its cyber sub-system. Notice finally that we avoid introducing an additional hyper-edge class for the electrical nodes of the power grid. Rather, we simply re-purpose the already available bus class.

In order to populate our graph with these additional hyper-edges, engineering design choices regarding the detailed power grid physical topology remain to be made. A first choice concerns the grouping of the buses of the bus-branch model into substations for the node-breaker model. The default choice implemented in the accompanying code is to group pairs of buses connected via a transformer into the same substation and separate pairs of buses connected via a transmission line into

[3] The term bay refers to the set of equipment connecting a single circuit to the busbars of a substation (as in switches, circuit breakers and instrument transformers, earth switches *etc.*). Formally, a bay is defined in the as *"the part of a substation within which the switchgear and control-gear relating to a given circuit is contained" [49].*

Table 4.1: Additional hyper-edge classes for node-breaker modeling resolution

Name	Attributes	
Circuit Breaker	ID	String
	Open	Boolean
	Normally Open	Boolean
	Nominal Rating (A)	Positive Real
	Short-Circuit Rating (kA,s)	2× Positive Real
	Breaking Capacity (kA)	Positive Real
	Port Types	2× Physical Terminals
		2× Digital Input
		2× Digital Output
Switch	ID	String
	Open	Boolean
	Normally Open	Boolean
	Nominal Rating (A)	Positive Real
	Short-Circuit Rating (kA,s)	2× Positive Real
	Port Types	2× Physical Terminals
		2× Digital Input
		2× Digital Output
CT/VT	ID	String
	Port Types	1× Primary Winding
		2×Analog Output
NeS	ID	String
	Port Types	1× Sensor
		2× Analog Output
		2× Digital Output

different substations. Our code can also input a user-provided substation grouping. The second choice concerns the substation detailed topology. The developed software supports the six most common arrangements [50] shown in Fig. 4.1, namely the: (a) single bus – single breaker, (b) main bus – transfer bus, (c) double bus – single breaker, (d) double bus – double breaker, (f)breaker and a half, and,(e) ring bus options. By default, the developed converter uses the double bus – single breaker arrangement. The user may specify a preferred alternative for every bus of the original bus-branch input model. Conceivably, for some specific cyber-physical power grid modeling application it may suffice to only represent a sub-part of the grid in node-breaker resolution. The obvious advantage of doing so would be the containment of the model size. To allow for such option, the user may specify to retain a subset of the grid's buses in bus-branch resolution.

Figure 4.2 plots the graph for the IEEE 14 bus test system in: (a) the original bus-branch resolution, (b) hybrid resolution, while adopting the double bus – single breaker arrangement for the substation corresponding to bus 12 of the original bus-branch model and (c) full node-breaker resolution, with the default double bus – single breaker option used for all substations. Indicatively, the original bus-branch model includes 14 buses and 0 breakers/disconnectors, the hybrid representation includes 26 buses (nodes) and 15 breakers/disconnectors while the full node-breaker representation includes 68 buses (nodes) and 69 breakers/disconnectors.

4.4 Fully-digital substations

With a view on the ongoing digitisation of the electric power grid and the increasing prevalence of the IEC61850 standard [51] we choose to focus on so-called fully-digital substations and while adopting the IEC61850 functional architecture shown in Fig. 4.3.

The IEC61850 architecture features three distinct levels for data exchange between the digital devices implementing the required measurement, monitoring, protection and control functions. The *process level* lies at the bottom of this architecture and provides interface functionalities concerning the acquisition of data from instrument transformers and/or modern sensors[4], as well as the issuing of commands towards the actuators of the power grid's physical components. The middle *bay level* implements protection and control functions on the basis of local and/or remote data with a scope of a distinguishable substation bay. At the top, the *station level* facilitates the interfaces between the different bays of a substation as well as between the substation bays and local/remote operating and monitoring devices. Table 4.2 lists in detail the data exchange categories represented as circled numbers in Fig. 4.3[5]. As an example, consider that the power grid operator at the control centre decides to open a specific circuit breaker. The implementation of such decisions includes data exchanges → (10) → (6) → (5) towards the substation station level, the respective bay level control application and the respective process level actuator.

The essential cyber component for the implementation of the functional architecture shown in Fig. 4.3 is the so-called *Intelligent Electronic Device* (IED). Formally, an IED can be defined as "any device incorporating one or more processors with the capability to receive or send data/control from or to an external source" [53]. With reference to Figure 4.3, IEDs implement the process-level and bay-level functionalities [54]. Cyber devices at the station level, facilitating data handling, security and user interaction, are typically not considered as IEDs. The respective devices will be henceforth collectively referred to as *Automation Devices* (ADs). Last but certainly not least, *Networking Devices* (NDs) are the media for all intra-substation and inter-substation communications.

It is important to note here that a modern IED is multi-functional. A single physical piece of equipment can integrate multiple so-called *logical nodes* and perform several so-called *logical functions* at different levels of the IEC61850 functional architecture [55]. For a given physical substation and set of functions, multiple valid sets of physical IEDs, each performing a specific sub-set of functions, can

[4] We refer the reader to [52] for an overview of modern sensor technologies that can be deployed as an alternative to conventional instrument transformers.

[5] Remote data exchanges outside a single substation are identifiable in gray color.

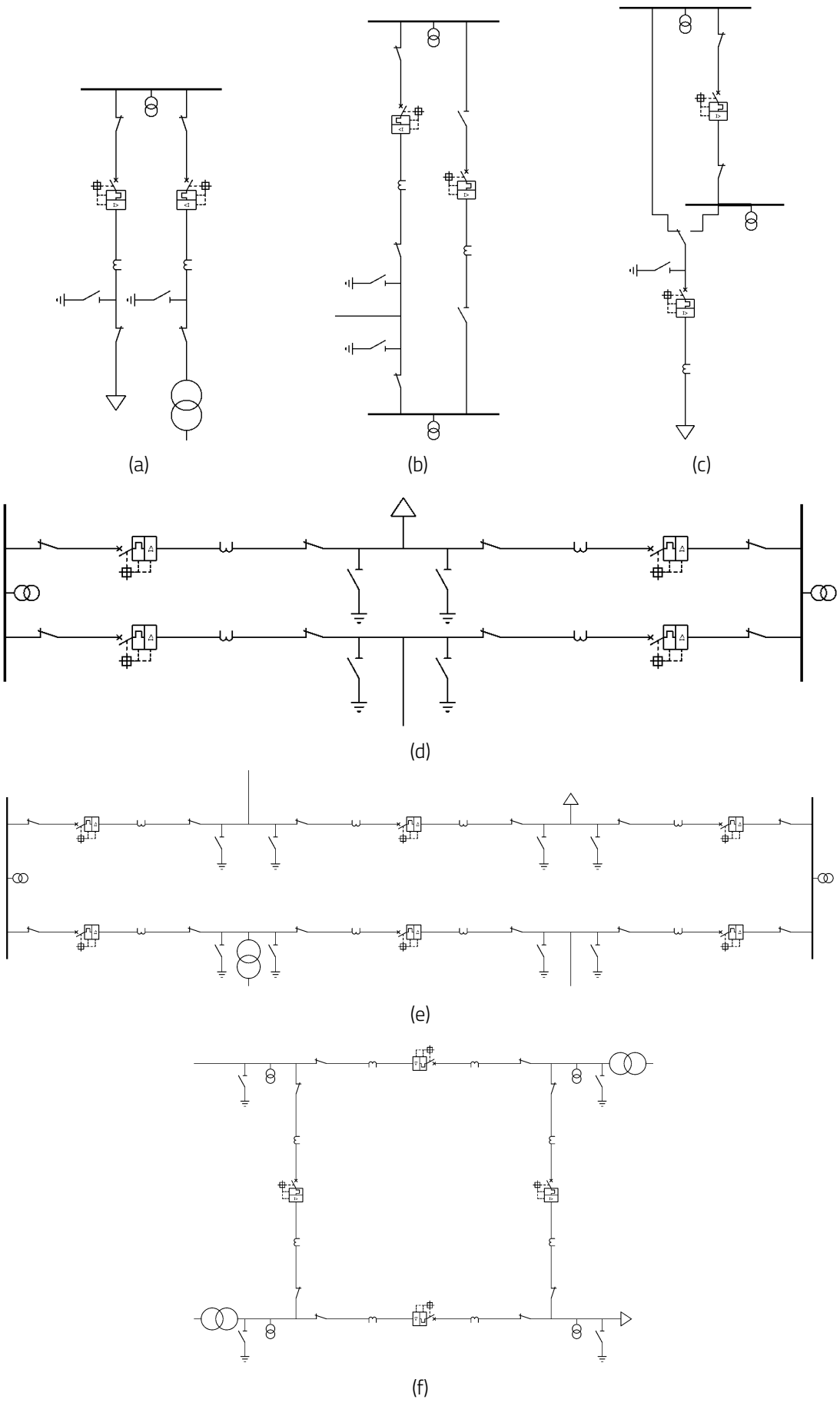
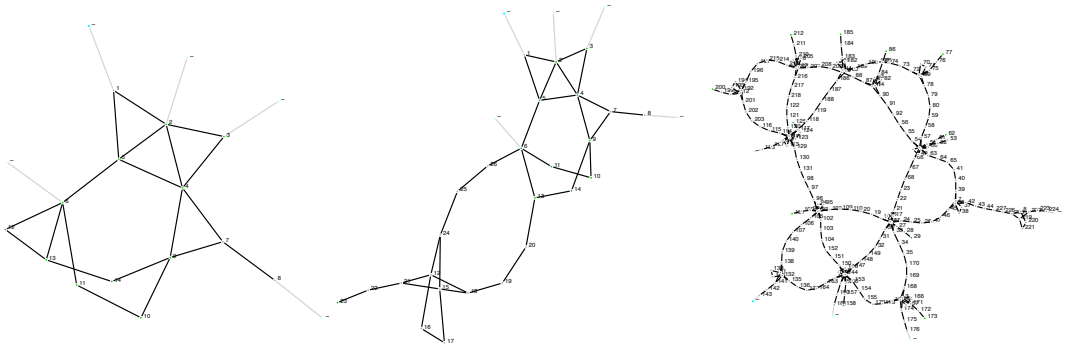


Figure 4.1: Alternative substation arrangements



(a) Bus – branch (b) Hybrid (c) Node – breaker

Figure 4.2: IEEE 14 bus network graph variants

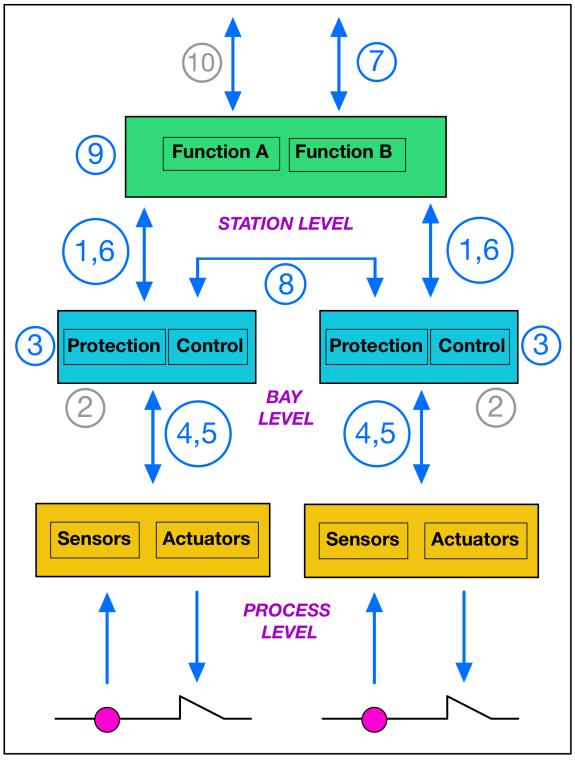


Figure 4.3: IEC61850 substation functional architecture

1	Protection data exchange between bay and station level.
2	Protection data exchange between bay level and remote protection.
3	Data exchange witin bay level.
4	Current & Voltage Transformer instantaneous data exchange between process and bay level.
5	Control data exchange between process and bay level.
6	Control data exchange between bay and station level.
7	Data exchange between substation (level) and remote engineering workspace.
8	Direct data exchange between the bays, especially for fast functions.
9	Data exchange within station level.
10	Control-data exchange between substation (devices) and remote control centre.

Table 4.2: IEC 61850 architecture data exchange categories

be defined [56]. The assignment of specific functions into a set of physical IEDs requires in practice to also consider the complexity of the functions to be implemented, regulatory requirements (*e.g.*, for stand-alone billing equipment), budget restrictions, the physical (building) layout of the substation in question, its criticality to the power grid *etc.*. The interested reader is referred to the documentation of the practical experience of designing fully-digital transmission substations in [57]–[64], which reveals the scope of such considerations.

In the context of extending a given physical power grid academic benchmark with a model for its cyber infrastructure, there is limited potential to take such practical engineering factors into account. To circumvent this issue, we make the choice to consider designs wherein any IED implements one or several functions at a single level of the IEC61850 functional architecture only. That is, we distinguish between process-level IEDs and bay-level IEDs, Fig. 4.4 . We further document and discuss practically relevant alternatives for allocating the functions of any single functional level to (a single or multiple) IEDs and introduce respective hyper-edge classes in the H2MG formalism based on the typical properties of commercially available devices. In the accompanying code, we implement a default choice for every functional level and allow the user to specify an alternative preference per substation and functional level.

4.4.1 Process-level IEDs

At the process level, IEDs implement the interface with sensors, instrument transformers and actuators. A first design choice towards defining the architecture of a fully digital substation concerns the allocation of the process-level functions to a number of physical IEDs. As mentioned, there are several valid alternatives for such allocation [65], [66].

Interfaces with instrument transformers and/or modern current/voltage sensors can be implemented by a *Stand-alone Merging Unit* (SaMU) IED. More specifically, the functionality of a SaMU is to collect the current and voltage signals from the instrument transformers and/or sensors, merge and broadcast them over the Ethernet in the standardised digital format of a *Sampled Values* (SV)

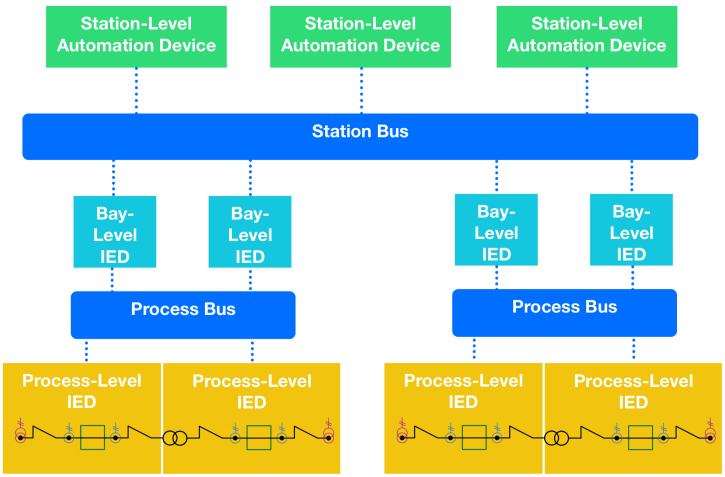


Figure 4.4: Fully-digital substation ICT architecture overview

message. In order to be able to represent such device type in physical power grid H2MG, we add an additional hyper-edge class with the attributes shown in the top tier of Table 4.3. It can be understood that commercially available SaMU IEDs differ in terms of the type and number of input/output ports they may host, in terms of the sampling rates and broadcast rates they can support, in terms of their physical dimensions *etc.*. In the (high)-level abstraction of the cyber-physical power grid H2MG, we define a typical device that can receive up to 4 analog (current) inputs and 4 analog (voltage) inputs to broadcast SV messages out of 2 redundant Ethernet ports.

Applications related to interfacing with primary transmission equipment (*i.e.*, breakers, switches, transformers, *etc.*) can be allocated to a so-called *Switchgear Interface Unit* (SIU) IED. This type of device has the capability to both send and receive inputs and outputs communicating (i) the position of breakers, disconnectors, transformer taps *etc.* upstream towards the bay/station levels, (ii) commands to change positions downstream towards actuators. SIUs communicate upstream over the process-level Ethernet (*i.e.*, the process bus) by exchanging *Generic Object Oriented Substation Event* (GOOSE) messages. GOOSE messages sent by SIUs typically contain status values and are either periodical or event driven (burst). The second tier of Table 4.3 lists the attributes of the additional hyper-edge class that we introduce in the H2MG formalism in order to be able to represent SIU IEDs. Again, we define a typical device by surveying the specifications of existing SIU IEDs. It can interface with up to 8 position sensors/actuators through respective input/output ports and also exchange GOOSE messages over 4 additional ports.

Applications related to interfacing with sensors measuring non-electrical quantities, for instance oil pressure and temperature can be allocated into a so-called *Non-electrical Interface Unit* (NeIU) IED. Raising alarms triggered by thresholds on the measured quantities is a potential additional functionality of such a device. In the H2MG formalism, we define an NeIU hyper-edge class offering such additional functionality and therefore potentially publishing both periodical and event-triggered GOOSE messages. The third tier of Table 4.3 lists the attributes defining an H2MG hyper-edge class as per the typical NeIU device. It is also possible to combine the interface applications of SAMUs, SIUs and NeIUs into a multi-purpose process level IED, the so-called *Process Interface Unit* (PIU) IED type integrates all interface applications at the process level. To allow for such design option, we create the hyper-edge classes listed in the bottom tier of Table 4.3.

Notice finally that in addition to the message formats, and respective communication protocols, listed in Table 4.3 we consider that all process-level IEDs support the reception of *Precision Time Protocol Synchronisation* (PTP Sync) messages for time synchronization as well as *Substation Configuration Language* (SCL) files containing configuration data.

Table 4.3: Process-level IED Hyper-Edge Classes

Name	Attributes	
SaMU	ID	String
	Port Types	4× Analog Input (current) 4× Analog Input (voltage) 2× Ethernet
	Message Format(s)	SV
SIU	ID	String
	Port Types	8× Digital Input 8× Digital Output 2× Ethernet
	Message Format(s)	GOOSE
NeIU	ID	String
	Port Types	4× Analog Input (non-electrical) 2× Ethernet
	Message Format(s)	GOOSE
PIU	ID	String
	Port Types	4× Analog Input (current) 4× Analog Input (voltage) 8× Digital Input 8× Digital Output 4× Analog Input (non-electrical) 2× Ethernet
	Message Format(s)	SV, GOOSE

Table 4.4: Bay-level IED Hyper-Edge Classes

Name	Attributes	
BL-IED	ID	String
	Port Types	4× Ethernet 2× Fiber Optic
	Message Format(s)	SV, GOOSE, MMS

4.4.2 Bay-level IEDs

At the bay level, IEDs implement metering and recording, protection and control functions [67]. Similarly to the process level, there is no unique mapping between the functions and the IEDs used to implement them. It is however typical to distinguish between *Bay Control Units* (BCUs) implementing control, metering and recording functions and *Protection Units* (PUs) implementing protection functions. The alternative is to group all bay-level functions into a single *Protection Control Monitoring Recording Unit* (PCMRU) [65].

Bay Control Units (BCUs) [68] perform a variety of tasks including (i) the reception of *Manufacturing Message Specification* (MMS) data from the station level including commands to be applied on the primary equipment of the bay, (ii) transmission of MMS data containing measurements, reports, status information towards the station level, (iii) publication of GOOSE messages including control commands towards the process level IEDs, (iv) subscription to GOOSE messages and SV messages from process level IEDs, and (v) implementation of automated control workflows and execution of predefined control sequences. *Protection Units* (PUs) subscribe to (SMV/GOOSE) messages broadcasted by process level IEDs[6], evaluate predefined functions using the content of such messages and issue GOOSE messages containing trip/close commands towards process level IEDs interfacing with the circuit breakers of a bay. Commercially available PUs are further distinguishable according to the primary asset they are designed to protect (e.g., busbar, line, transformer, etc.) as well as the types of the protection functions they implement (e.g., overcurrent protection, distance protection, differential protection, etc.). *Protection Control Monitoring Recording Units* (PCMRUs) combine all aforementioned functionalities.

Modern IEDs are typically capable of performing several thousand logical functions. It is important here to acknowledge that different (configurations of) metering and recording, protection and control functions are suitable for different power systems and operating contexts. Indeed, choosing (the configurations of) such functions requires careful and laborious study of the respective power system and the environment within which it is anticipated to operate. This can be recognized as a limiting factor to the development of a generally relevant map of the interface between the primary equipment of the power transmission grid and its cyber sub-system. Our pragmatic approach facing such limitation is to introduce a generic bay-level IED hyper-edge class with attributes referring to its available ports for communication. We inevitably leave the specification of the precise functions implemented by bay-level IEDs for a specific use-case of the cyber-physical power grid H2MG. Table 4.4 summarises the definition of the bay level IED (BL-IED) hyper-edge class[7].

4.4.3 Station-level Automation Devices

At the station level, ADs facilitate interface-related and process-related functions which concern the operation of the overall substation equipment rather than the equipment of a distinguishable bay. A

[6] As seen in Fig. 4.3 potentially also from remote substation bays.

[7] Again, although not listed in this table, we consider that all bay-level IEDs support the reception of PTP Sync messages for time synchronization as well as SCL files containing configuration data.

typical example of a process-related function is the tripping of multiple breakers across several substation bays according to a bus differential protection scheme. Interface-related functions allow the monitoring and control of the substation both at local and remote level. Station-level ADs are distinguishable in terms of the role/function they implement, the types of ports they host as well as the protocols they support. We distinguish respective new hyper-edge classes for the H2MG formalism on the basis of such differences. In order to introduce these additional hyper-edge classes, it is useful to briefly describe the main function/role implemented by each distinct station-level automation device.

Time synchronization is essential to enable the coordination required for the operation of the electric power grid. It is achieved through the exchange of timing information in a (nested) master-slave hierarchy. At the top of this hierarchy lies the *grandmaster* clock, which uses the Ethernet to disseminate a global time reference around a substation in the form of a so-called *Precision Time Protocol* (PTP) *Sync* message [69]. The top tier of table 4.5 defines the respective hyper-edge class, featuring two (redundant) Ethernet Ports for outgoing PTP Sync messages as well as a GPS Antenna allowing the potential reception of incoming synchronization messages from a GPS satellite. In the accompanying code, we populate the station level of every substation with duplicate (redundant) grandmaster clocks.

Remote monitoring and control functionalities are facilitated by a *Gateway*. The Gateway device enables communications between a substation's internal network and external systems (for instance the power grid's control centre and/or the ICT devices of other substations for teleprotection applications). Beyond being a connection point, the gateway provides protocol connection functionalities. Further, a *secure* gateway may also implement crucial cybersecurity functionalties (*e.g.*, firewalling, intrusion detection, intrusion prevention, *etc.*). In order to be able to represent gateway devices, we define a new hyper-edge class of order 10 in the H2MG formalism, as listed in the second tier of table 4.5. In the accompanying code, we populate the station level of every substation with a single gateway device.

Local interface functionalities relate to monitoring and operating the substation's physical and cyber infrastructure. We distinguish three (types of) enabling devices, namely the *Human-Machine Interface* (HMI), *Server Computer* and *Engineering Workstation*. The HMI device can be seen as the port through which the human substation operator interacts with the substation's electrical equipment. The Server Computer can be seen as the back-office for the local/remote interaction with the substation's electrical equipment. It collects real-time substation data from IEDs and sensors, hosts the necessary software applications for monitoring, reporting, alarm management and data management and additionally facilitates the control of the substation's equipment. Finally, the Engineering Workstation allows the configuration and management of the substation's IEDs, including the performance of diagnostic tests and firmware updates. The third to last tiers of Table 4.5 introduce the properties of the hyper-edge classes used to represent these three types of devices. In the accompanying code, we populate the station level of every substation with a single HMI, Server Computer and Engineering Workstation.

4.4.4 Networking Devices

In modern digital substations communications happen over Ethernet LANs, which offer high-speed, reliable data exchange. In order to represent these communication networks in the cyber-physical power grid H2MG, it is first necessary to add new hyper-edge classes corresponding to the common networking devices.

A *Twisted Pair Ethernet Cable* is the physical medium typically used to establish a connection between any two network devices within the same substation. Similarly, a *Single-Mode Fiber Optic Cable* is the physical medium for communications over longer distances, *e.g.* between substations and the control centre. We add a generic *network link* hyper-edge class of order two in the H2MG formalism. The precise cable type can be treated as an optional hyper-edge attribute. An *Ethernet Switch* is the networking device used to connect multiple devices and thus form a network. We similarly add a

Table 4.5: Station-level AD Hyper-Edge Classes

Name	Attributes	
Grandmaster Clock	ID	String
	Port Types	2× Ethernet 1× GPS Antenna
	Message Format(s)	PTP
Gateway	ID	String
	Port Types	6× Ethernet 2× Fiber Optic 2× USB
	Message Format(s)	SV,GOOSE, MMS DNP3, Modbus, SNMP TCP/IP, SNMP, HTTP/HTTPS
HMI	ID	String
	Port Types	2× Ethernet 2× USB 1× HDMI
	Message Format(s)	GOOSE, MMS
Server Computer	ID	String
	Port Types	6× Ethernet 2× Fiber Optic 2× USB
	Message Format(s)	SV,GOOSE, MMS DNP3, Modbus, SNMP TCP/IP, SNMP, HTTP/HTTPS
Engineering Workstation	ID	String
	Port Types	2× Ethernet 4× USB 1× HDMI
	Message Format(s)	SCL files

generic *network switch* hyper-edge class with 24 Ethernet ports.

4.4.5 Network Topologies

The substation network is typically divided into two main segments as shown in Fig. 4.4; the *process bus* and the *station bus*. In practice, the segmentation of the process and station buses may be physical or virtual. We opt for the physical segmentation design and populate the power-grid cyber-physical benchmark with the set of network devices (*i.e.*, network links and switches) necessary to implement distinguishable process and station buses. The additional choice to be made concerns the topology for the process-level and station-level communication networks.

In the most simple alternative, the process/station bus network could be arranged as per the single-star topology. This option relies on a single network switch to act as a central hub to which each IED/AD connects through a separate network link. It follows that every transmission goes through the network switch that has to forward every frame towards the destination device by means of the respective link. This arrangement allows multiple exchanges to occur at the same time [70]. Although cost effective this topology does not offer any security. Redundant topologies, corresponding to implementations of the *Parallel Redundancy* and *High-availability Seamless Redundancy* Protocols (respectively, PRP and HSR) have therefore prevailed. Both these protocols achieve seamless redundancy with zero switch-over time and no packet loss for single point network failures [71], [72].

The PRP uses a double-star topology, meaning two independent identical paths for data exchange. It implies duplicate redundant network links and switches. The sender(receiver) sends(receives) all frames through both redundant networks. The handling (detection and removal) of duplicate frames is managed by the protocol interface. On the other hand, the HSR connects the IEDs/ADs of the process-/station- bus in a ring topology. Each outgoing frame is sent by its sender in two copies towards both directions of the ring, with the second frame to arrive being discarded at the destination. In the accompanying code, we implement by default the HSR at the process-level of every bay and the PRP at the station level of every substation. The code also allows the user to specify an alternative preference per substation and functional level.

4.4.6 Digital substation design cheat sheet

As already mentioned, in order to design a fully digital substation certain choices have to be settled. In real life systems, such design choices are settled by carefully studying the particular application and are subject to several *"non-electrical"* constraints (*e.g.*, budget, construction delays, workforce availability, *etc.*). In order to generate the population of cyber sub-system components enabling the fully digital substations of a power grid benchmark, it appears necessary to make similar choices. Table 4.6 presents the alternatives that are supported in the accompanying code for the extension of a power grid benchmark into a cyber-physical power grid H2MG. A selection between these alternatives, universally across the grid or at the substation resolution, can be provided as input by the user. The default choices implemented in the accompanying code are distinguished in bold in Table 4.6.

4.5 Transmission Control Centers

Transmission control centres constitute the computational infrastructure overseeing the bulk power grid operation. This infrastructure collects and processes operational data coming through (digital) substations to monitor the state of the power grid in a nearly-continuous rate. It additionally integrates decision support functionalities allowing to assess the current security level of the power grid, to efficiently choose remedial actions given any violation of the system security limits, to perform *what-if* analysis against postulated operating conditions and to prepare relevant countermeasures. Further, it also implements control functionalities either in direct mode (*e.g.*, opening of a breaker as part of a pre-defined automated remedial action scheme), in operator-supervised mode (*e.g.*, remote

Table 4.6: Digital substation design options

Process level IEDs	(a) SAMU + SIU + NeIU
	(b) PIU
Bay level IEDs	(a) BCU + PU
	(b) PCMRU
Functional redundancy	(a) only at the process level
	(b) only at the bay level
	(c) at the process + bay levels
Process bus topology	(a) Single Star
	(b) Double Star (PRP)
	(c) Ring (HSR)
Station bus topology	(a) STAR
	(b) Double Star (PRP)
	(c) Ring (HSR)

opening of a breaker by the control room operator) or operator-manual mode (*e.g.*, instructing a substation engineer to open a breaker). In the modern, deregulated power system era transmission control centres also serve to coordinate the operation of the market entities in the interest of the system security.

4.5.1 Hierarchical organization

Given the scale of the systems in question and the complexity of the tasks at hand, hierarchical organization becomes the natural choice for the efficient functioning of transmission control centres. Towards completing the cyber-physical power grid H2MG representation, we adopt the hierarchical organization illustrated in Fig. 4.5. At the top of this hierarchy lies a so-called National Control Centre (NCC) with master authority. Its main responsibilities concern the system balancing, the cross-border power exchange as well as the coordination of the operation of regional control centres. Multiple Regional Control Centres (RCCs) have sub-master authority over different parts of the grid. A single selected RCC acts as a back-up to the NCC. This organization is of course inspired from real-life electric power systems, wherein both geographical locations as well as the grid topology and voltage levels are used to define the perimeter of distinct RCCs. The interested reader may find historical information on the hierarchical organization adopted in Belgium and France in [73] and [74], respectively.

The challenge is once again to transpose the related practical considerations from the real-world to the context of an academic power grid benchmark, and do so in a system agnostic manner. We have investigated several alternatives for the association of substations into RCCs and the NCC. In the absence of any information on the considered system, the default option implemented in the accompanying code is to associate all substations in two control centers, namely a single NCC and its back-up. An additional option is to integrate a user-defined allocation of substations into control centers in the form of an additional input file. Further, we have also implemented an option that relies on the availability of geographical coordinates for the system buses. As per this alternative, we

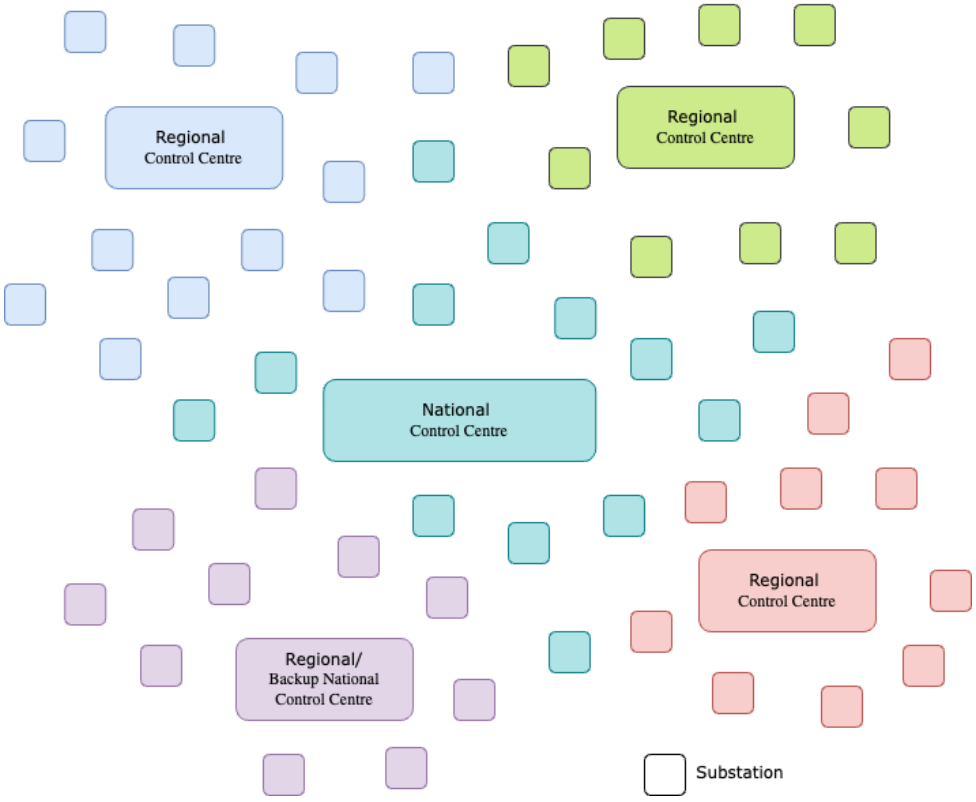


Figure 4.5: Control Centre Organization

only allocate substations including the highest system voltage level inside the perimeter of the NCC. Following this, the remaining substations are clustered into RCCs according to the k-means algorithm and while only considering the substation coordinates as features. The resulting RCC with the largest number of allocated substations acts also as a back-up to the NCC. A final (experimental) implemented alternative relies on the power grid physical topology. As per this alternative, we once again allocate all substations including the highest system voltage level inside the perimeter of the NCC. As a next step, we remove the respective buses from the grid case file and search for distinct topological islands. The buses connected to any distinct island are allocated to a distinct RCC. Again, the resulting RCC with the largest number of allocated substations is also the back-up NCC.

In our developed cyber-physical graph, the designation of a control center as an NCC, back-up NCC or RCC concerns both its ICT infrastructure as well as its connections through external Wide Area Networks (WANs). The NCC and its back-up connect to any substation and RCC. Further, these two types of control centers may also have external connections to external entities (*e.g.*, the market operator). In contrast, RCCs only connect to the specified substations within their perimeter as well as the NCC/back-up NCC.

4.5.2 Cyber infrastructure

In order to complete the cyber-physical power grid H2MG with hyper-edges corresponding to the cyber infastructure of the grid's NCCs/RCCs, let us first define respective typical architectures. The cyber components included in our typical control centre architecture are:

- a *Video Projection System*, displaying a real-time overview of the grid status, including its single-line diagram, power flow solution, relevant alarms and alerts, *etc.*.

Table 4.7: Control Centre Infrastructure Specification

	National CC	Regional CC
Video Projection system	✓	✓
Balancing desk	✓	x
Grid Monitoring desk	✓	✓
Security Assessment desk	✓	✓
Security Control desk	✓	✓
SCADA server	✓	✓
EMS server	✓	✓
Historian server	✓	✓
Market Interaction server	✓	x
Inter CC Interaction server	✓	✓
Training Simulator server	✓	x

- Groups of HMIs forming operator desks related to several tasks, such as real-time grid monitoring, generation/demand balancing, security assessment and control, look-ahead mode planning, *etc.*.
- Server Computers supporting all computational applications necessary to operate the grid and specifically:
  - the *SCADA* server for monitoring, control and alarm management applications.
  - the *EMS* server for topology processing, state estimation, load flow, security analysis *etc.* applications.
  - the *Historian* server for the storage and retrieval of the large amounts of data related to the operation of the power grid.
  - a *Market Interaction* server.
  - an *Inter-Control-Centre Interaction* server.
  - a *Training Simulation* server.
- a Gateway.

In order to generate the respective hyper-edges, it is first necessary to identify the respective classes. Hyper-edge classes for HMIs, Server Computer and the Gateway device have already been introduced in Table 4.5. For simplicity, we reduce the Video Projection System to its essential component and namely an imaging device accessible through cable connections (either Ethernet or HDMI). Next, it is necessary to define the degree of redundancy for each component of the cyber infrastructure. We consider that any component of the control centre cyber-infrastructure, with the exception of the non-critical Training Simulator server, is indeed replicated to ensure the required overall high service availability for the control centre. It is further necessary to define the topology of the control centre LAN. In our model, we consider a redundant star topology wherein each network component has two independent links to a central network switch. Finally, Table 4.7 summarizes the difference in the specification between NCCs and RCCs.

4.6 Concluding discussion

This chapter documents the results of the effort to extend the scope of available benchmarks for the physical bulk power system so as to enable cyber-physical risk assessment. At the start of this

CYPRESS activity, we made the choice of focusing on the cyber sub-system facilitating the operation of the transmission grid. As this particular part of the cyber infrastructure directly interacts with the power transmission grid it is the obvious primary modeling requirement for assessing the cyber-physical risk facing the said system. Cyber-physical threats acting on agents and systems interfacing the transmission grid, for instance power generators and/or the electricity market operator, can alternatively be represented through their potential effect on the physical behavior of the interfacing agents and systems.

The challenges of extending a bulk power system physical benchmark with a representation of the transmission grid cyber sub-system should not be understated. First and foremost, available benchmarks do not represent the physical properties of the transmission grid in the level of detail required to directly focus on identifying/modeling the enabling cyber infrastructure. Indicatively, detailed node – breaker topologies, assignment of buses into substations and substations in control centres, as well as protection principles, rules and settings are examples of the missing information. Even with such information available, there is no one-to-one mapping between a physical grids and its cyber infrastructure. The actual cyber infrastructure of real-life transmission grids has been designed while taking into account several practical considerations that cannot be transposed on the benchmark systems. Additionally, it is non-public information due to its criticality for cybersecurity and cyber-physical security reasons.

Facing such challenges, the concrete step that we take here is from the single-line diagram of a physical transmission grid at the bus–branch resolution to a *Hyper Heterogenous Multi Graph* of a cyber-physical transmission grid. The latter includes an asset inventory for the cyber components of substations and transmission control centres and maps information (*i.e.*, measurement and command) exchanges between cyber↔cyber components and cyber↔physical components. We believe that this is indeed usable for power grid cyber-physical risk assessment in several ways. In the simplest way, without detailed representation of the behavior of all components of the cyber sub-system, it could still be used to represented postulated cyber threat scenarios. Indeed, a sufficient way of representing such scenarios could be to only model the assumed maloperation of the concerned cyber sub-system components. For cyber components that are not affected by the threat and operate as intended, the physical model of the system may be sufficient. In a more advanced way, it may of course also be used in conjunction with freely chosen models of the cyber and physical system components in a co-simulation framework.

In other words, we consider the result of this effort as a stepping stone in the pathway for cyber-physical risk assessment and we hope that others may wish to build on top of it. With this motivation, we envision the public release of the accompanying code that implements the process described here in the Julia programming language. We also believe that the documentation of all the choices we had to make in this document may help other researchers that are also pursuing the question of modeling for cyber-physical risk assessment. It is worthwhile to acknowledge at this stage a particular choice that has been left implicit in the previous parts of this chapter. The developed cyber-physical H2MG does not include any explicit cybersecurity devices. Our primary motivation for doing so was to provide a blank-page where one may wish to add/study the effects of any particular cybersecurity device. We must also acknowledge however that our choice was affected by the fact that information on the cybersecurity measures in place on actual power systems is scarce, for obvious reasons.

Bibliography

[1] G. Kjølle, S. Jakobsen, F. Baldursson, S. Galant, and L. Haarla, "State of the art on reliability assessment in power systems," GARPUR consortium, Tech. Rep., 2014.

[2] D. E. Nordell, "Communication systems for distribution automation," in *2008 IEEE/PES Transmission and Distribution Conference and Exposition*, IEEE, 2008, pp. 1–14.

[3] C. Liao, C.-W. Ten, and S. Hu, "Strategic FRTU deployment considering cybersecurity in secondary distribution network," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1264–1274, 2013.

[4] I.-S. Choi, J. Hong, and T.-W. Kim, "Multi-agent based cyber attack detection and mitigation for distribution automation system," *IEEE Access*, vol. 8, pp. 183 495–183 504, 2020.

[5] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1035–1044, 2019.

[6] M. H. Kapourchali, M. Sepehry, and V. Aravinthan, "Fault detector and switch placement in cyber-enabled power distribution network," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 980–992, 2016.

[7] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 931–941, 2009.

[8] M. Farajollahi, M. Fotuhi-Firuzabad, and A. Safdarian, "Simultaneous placement of fault indicator and sectionalizing switch in distribution networks," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2278–2287, 2018.

[9] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyber-attack vector viable?" *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[10] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 1, pp. 478–487, 2020.

[11] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi, "Electric vehicle attack impact on power grid operation," *International Journal of Electrical Power & Energy Systems*, vol. 137, p. 107 784, 2022.

[12] N. Bhusal, M. Gautam, and M. Benidris, "Cybersecurity of electric vehicle smart charging management systems," in *2020 52nd North American Power Symposium (NAPS)*, IEEE, 2021, pp. 1–6.

[13] A. Shafee, M. Nabil, M. Mahmoud, W. Alasmary, and F. Amsaad, "Detection of denial of charge (DoC) attacks in smart grid using convolutional neural networks," in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, 2021, pp. 1–7.

[14] D. Niyato, D. T. Hoang, P. Wang, and Z. Han, "Cyber insurance for plug-in electric vehicle charging in vehicle-to-grid systems," *IEEE Network*, vol. 31, no. 2, pp. 38–46, 2017.

[15] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical system security of vehicle charging stations," in *2019 IEEE Green Technologies Conference (GreenTech)*, IEEE, 2019, pp. 1–5.

[16] J. Ye, A. Giani, A. Elasser, *et al.*, "A review of cyber–physical security for photovoltaic systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, 2021.

[17] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure (AMI)," in *2008 IEEE power and energy society general meeting-conversion and delivery of electrical energy in the 21st century*, IEEE, 2008, pp. 1–5.

[18] J. C. Foreman and D. Gurugubelli, "Identifying the cyber attack surface of the advanced metering infrastructure," *The Electricity Journal*, vol. 28, no. 1, pp. 94–103, 2015.

[19] P. A. Giglou and S. N. Ravadanegh, "Defending against false data injection attack on demand response program: A bi-level strategy," *Sustainable Energy, Grids and Networks*, vol. 27, p. 100 506, 2021.

[20] E. Ustundag Soykan and M. Bagriyanik, "The effect of SMiShing attack on security of demand response programs," *Energies*, vol. 13, no. 17, p. 4542, 2020.

[21] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, *et al.*, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2015.

[22] D. Choeum and D.-H. Choi, "OLTC-induced false data injection attack on volt/var optimization in distribution systems," *IEEE Access*, vol. 7, pp. 34 508–34 520, 2019.

[23] S. Gordon, "Dynamic interactions between voltage and frequency events in future power systems," Ph.D. dissertation, University of Strathclyde, 2024.

[24] CIGRE Working Group C4.605, "Modelling and aggregation of loads in flexible power networks," CIGRE, Tech. Rep., 2014-02.

[25] EPRI, "Technical reference on the composite load model," Tech. Rep., 2020-09.

[26] B. P. Administration, "Bpa annual data exchange model data requirements & reporting procedures," Tech. Rep., 2024-08. [Online]. Available: `https://www.bpa.gov/-/media/Aep/transmission/reliability-and-nerc-standards/bpa-mod-032-model-data-requirements-reporting-procedures.pdf` (visited on 2028-08-22).

[27] NERC Load Modeling Task Force, "Dynamic load modeling," NERC, Tech. Rep., 2016-12. [Online]. Available: `https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/Dynamic%20Load%20Modeling%20Tech%20Ref%202016-11-14%20-%20FINAL.PDF` (visited on 2022-08-12).

[28] G. Chaspierre, "Reduced-order modelling of active distribution networks for large-disturbance simulations," Ph.D. dissertation, Université de Liège, 2020-10.

[29] Electranix, "Hawaiian electric island-wide pscad studies (stage 2 system impact study)," Tech. Rep., 2021-06.

[30] 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.

[31] EPRI, "Technical reference on the composite load model," Palo Alto, CA, Tech. Rep. 3002019209, 2020-09.

[32] N. Fulgêncio, C. Moreira, L. Carvalho, and J. Peças Lopes, "Aggregated dynamic model of active distribution networks for large voltage disturbances," *Electric Power Systems Research*, vol. 178, 2020.

[33] G. Chaspierre, G. Denis, P. Panciatici, and T. Van Cutsem, "A dynamic equivalent of active distribution network: Derivation, update, validation and use cases," *IEEE Open Access Journal of Power and Energy*, vol. 8, pp. 497–509, 2021.

[34] J. Vorwerk, T. Zufferey, P. Aristidou, and G. Hug, "Using quantile forecasts for dynamic equivalents of active distribution grids under uncertainty," in *11th Bulk Power Systems Dynamics and Control (IREP 2022)*, Banff, Canada, 2022.

[35] F. Sabot, P. Henneaux, I. S. Lamprianidou, and P. N. Papadopoulos, "Statistics-informed bounds for active distribution network equivalents subject to large disturbances," in *2023 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, 2023-10. DOI: 10.1109/ISGTEUROPE56780.2023.10408629.

[36] F. Sabot, P. Henneaux, I. S. Lamprianidou, P. N. Papadopoulos, and K. Bell, "Impact of active distribution networks on power system stability - a case study," in *CIGRE Paris Session 2024*, 2024-08.

[37] CIGRE Working Group C4.04, "Benchmark systems for network integration of renewable and distributed energy resources," CIGRE, Tech. Rep., 2014-04.

[38] 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.

[39] A. Godfraind, S. Ben Mariem, V. Rossetto, F. Sabot, P. Henneaux, and Y. Vanaubel, "Report D1.3: Describing the benchmarks," CYPRESS consortium, Tech. Rep., 2022.

[40] A. Stefanov and C.-C. Liu, "ICT modeling for integrated simulation of cyber-physical power systems," in *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, IEEE, 2012, pp. 1–8.

[41] G. A. Weaver, K. Davis, C. M. Davis, *et al.*, "Cyber-physical models for power grid security analysis: 8-substation case," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, IEEE, 2016, pp. 140–146.

[42] 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.

[43] 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.

[44] O. Boyaci, M. R. Narimani, K. Davis, and E. Serpedin, "Generating connected, simple, and realistic cyber graphs for smart grids," in *2022 IEEE Texas Power and Energy Conference (TPEC)*, IEEE, 2022, pp. 1–6.

[45] L. Wang, J. Halvorsen, S. Pannala, A. Srivastava, A. H. Gebremedhin, and N. N. Schulz, "CP-SyNet: a tool for generating customised cyber-power synthetic network for distribution systems with distributed energy resources," *IET Smart Grid*, vol. 5, no. 6, pp. 463–477, 2022.

[46] S. S., G. Gurrala, P. Sastry, and V. Katewa, "Cyber-physical modeling and vulnerability assessment of substations for transmission system operator," *Electric Power Systems Research*, vol. 235, p. 110 769, 2024, ISSN: 0378-7796. DOI: https://doi.org/10.1016/j.epsr.2024.110769. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779624006552.

[47] B. Donon, F. Cubelier, E. Karangelos, *et al.*, "Topology-aware reinforcement learning for tertiary voltage control," *Electric Power Systems Research*, vol. 234, p. 110 658, 2024, ISSN: 0378-7796. DOI: https://doi.org/10.1016/j.epsr.2024.110658. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779624005443.

[48] Contingency Subgroup of the Modeling SPS and Relays Ad-Hoc Task Force., *Node-breaker white paper*. Western Electricity Coordinating Council, 2024.

[49] International Electrotechnical Commission, *Electropedia IEV ref 605-02-09*, 1983.

[50] J. D. McDonald, *Electric power substations engineering*. CRC press, 2003.

[51] International Electrotechnical Commission, "Communication networks and systems for power utility automation," *IEC Std*, vol. 61850, 2013.

[52] Working Group K15 of the Substation Protection Subcommittee, "Centralized substation protection and control," IEEE PES Power System Relaying Committee, Tech. Rep., 2015.

[53] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, "SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)," Gaithersburg, MD, USA, Tech. Rep., 2011.

[54] J. C. Lozano, K. Koneru, N. Ortiz, and A. A. Cardenas, "Digital Substations and IEC 61850: A Primer," *IEEE Communications Magazine*, vol. 61, no. 6, pp. 28–34, 2023.

[55] A. Apostolov and B. Vandiver, "Functional testing of IEC 61850 based IEDs and systems," in *IEEE PES Power Systems Conference and Exposition, 2004.*, 2004, 640–645 vol.2.

[56] B. Kasztenny, J. Whatley, E. Udren, J. Burger, and M. Finney D ark Adamiak, "IEC 61850: A practical application primer for protection engineers," in *60th Annual Georgia Tech Relaying Conference*, 2006. [Online]. Available: `https://www.gevernova.com/grid-solutions/multilin/pr/gatech/2006/iec61850_practical_application_primer_protection_eng.pdf`.

[57] J. Bettler, J. Silva, D. Morman, *et al.*, "Case studies of IEC 61850 process bus systems using GOOSE and sampled values: Recent installations and research," in *proceedings of the 47th Annual Western Protective Relay Conference, Spokane, WA*, 2020.

[58] T. Charton, D. Binon, V. Leitloff, L. Xu, and T. Shono, "Findings of CIGRE W11G B5.69 on experience gained of Process Bus in PACS," *PAC World Magazine*, no. 66, 2023. [Online]. Available: `https://www.pacw.org/findings-of-cigre-wg-b5-69-on-experience-gained-of-process-bus-in-pacs`.

[59] B. Heimisson, "LANDSNET's road to fully digital transmission system," *PAC World Magazine*, no. 66, 2023. [Online]. Available: `https://www.pacw.org/landsnets-road-to-fully-digital-transmission-system`.

[60] C. Polanco, I. Otarola, and A. Uzcategui, "Redundancy techniques in a Digital IEC 61850 substation PAC system," *PAC World Magazine*, no. 58, 2021. [Online]. Available: `https://www.pacw.org/redundancy-techniques-in-a-digital-iec-61850-substation-pac-system-2`.

[61] W. Caman, I. Otarola, A. Uzcategui, and A. Bittencourt, "Improving a Protection, Automation and Control (PAC) system in a digital IEC 61850 substation: The case of San Miguel digital substation," *PAC World Magazine*, no. 54, 2020. [Online]. Available: `https://www.pacw.org/improving-a-protection-automation-and-control-pac-system-in-a-digital-iec-61850-substation-the-case-of-san-miguel-digital-substation`.

[62] V. Leitloff, O. Lopez, J.-M. Boisset, M. Merley, and X. Michaut, "Towards an industrial deployment of Fully Digital PACS at RTE," *PAC World Magazine*, no. 66, 2023. [Online]. Available: `https://www.pacw.org/towards-an-industrial-deployment-of-fully-digital-pacs-at-rte`.

[63] H. Vardhan, R. Ramlachan, W. Szela, and E. Gdowik, "Deploying digital substations: Experience with a digital substation pilot in North America," in *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, 2018, pp. 1–9.

[64] K. Hinkley and C. Mistry, "First digital substation in TransGrid – Australia: A journey, business case, lessons," *The Journal of Engineering*, vol. 2018, no. 15, pp. 1135–1139, 2018. DOI: https://doi.org/10.1049/joe.2018.0171. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/joe.2018.0171.

[65] A. O. Pires, H. Leon, L. de Marchi Pintos, P. Montaner, C.-P. Teoh, and R. Ananth, "Process Interface Units (PIU) and its advantages for full digital substations," in *2022 Saudi Arabia Smart Grid (SASG)*, 2022, pp. 1–7.

[66] D. Dolezilek, P. Lima, G. Rocha, A. Rufino, and W. Fernandes, "Comparing the cost, complexity, and performance of several in-service process bus merging unit solutions based on IEC 61850," in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, 2020, pp. 1–6.

[67] T. Xu, X. Yin, D. You, H. Yu, Y. Wang, and H. Hou, "Bay level IED modeling and realizing using IEC 61850," in *2008 IEEE/PES Transmission and Distribution Conference and Exposition*, 2008, pp. 1–7.

[68] G. M. Asim Akhtar, M. Sheraz, and M. W. Ahmed, "Bay Control Unit in an IEC 61850 environment: A generalized and systematic process flow for optimized configuration," in *2022 IEEE Electrical Power and Energy Conference (EPEC)*, 2022, pp. 157–163.

[69] R. Moore, R. Midence, and M. Goraj, "Practical experience with IEEE 1588 high Precision Time Synchronization in electrical substation based on IEC 61850 Process Bus," in *IEEE PES General Meeting*, 2010, pp. 1–4.

[70] A. Apostolov, "Communications in IEC 61850 based substation automation systems," in *2006 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, IEEE, 2006, pp. 51–56.

[71] N. Moreira, E. Molina, J. Lázaro, E. Jacob, and A. Astarloa, "Cyber-security in substation automation systems," *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1552–1562, 2016.

[72] J. Gaspar, T. Cruz, C.-T. Lam, and P. Simões, "Smart substation communications and cybersecurity: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2023.

[73] J. M. Delforge, F. Denis, J. Ernould, and J. P. Waha, "Power system control organization in Belgium – hierarchical structure of the control centres," in *CIGRE International Conference on Large High Voltage Electric Systems*, 1978-08.

[74] J. Augé, R. Fernandez, A. Merlin, and F. Broussolle, "The new real-time computerized control system in the National Control Centre of Electricité de France," in *CIGRE International Conference on Large High Voltage Electric Systems*, 1984-08.

This project is supported by the Belgian Energy Transition Fund