

Graph-based Impact Analysis of Cyber-Attacks on Behind-the-Meter Infrastructure

Immanuel Hacker^{1,2*}, Ömer Sen^{1,2}, Florian Klein-Helmkamp², Andreas Ulbig^{1,2}

¹Digital Energy Fraunhofer FIT, Aachen, Germany

²IAEW at RWTH Aachen University, Aachen, Germany

*E-mail: immanuel.hacker@fit.fraunhofer.de

Keywords: cyber-physical systems, cyber-attacks, cyber-resilience, smart grids, SGAM, ontology

Abstract

Behind-the-Meter assets are getting more interconnected to realise new applications like flexible tariffs. Cyber-attacks on the resulting control infrastructure may impact a large number of devices, which can result in severe impact on the power system. To analyse the possible impact of such attacks we developed a graph model of the cyber-physical energy system, representing interdependencies between the control infrastructure and the power system. This model is then used for an impact analysis of cyber-attacks with different attack vectors.

This paper is a preprint of a paper submitted to 14th Mediterranean Conference on Power Generation Transmission, Distribution and Energy Conversion (MEDPOWER 2024) and is subject to Institution of Engineering and Technology Copyright. If accepted, the copy of record will be available at IET Digital Library

1 Introduction

The energy transition has led to two developments that increase the significance of Behind-the-Meter (BTM) infrastructure. On the one hand, electrification of the heating and mobility sectors, and on the other, decentralised energy production through photovoltaic (PV) systems. Additionally, storage systems are increasingly integrated to enable economically optimal combined utilisation of production and consumption. These BTM installations are interconnected through Information and Communications Technology (ICT) infrastructure often via the internet, due to the requirements from various stakeholders. The applications that necessitate this connectivity are highly diverse. The simplest example is the customer's need to remotely control activities such as charging their own Electric Vehicle (EV) or heating their house. However, more complex applications such as dynamic electricity tariffs, which control BTM devices based on market prices, are already a reality. From the perspective of network operators, due to the new challenges for the electricity grid, it is crucial that BTM installations can be controlled in a grid-serving manner to ensure the safe operation of the electricity grid at all times. These applications are either implemented directly via the customer's internet connection using Home Energy Management System (HEMS) or through a dedicated advanced metering infrastructure. The interconnection of the installations is imperative to implement these applications. However, the networking of many small assets via a common ICT infrastructure or a common software stack carries the risk that in the event of a cyber-attack, a large number of assets may be simultaneously affected, which could cumulatively have a significant

impact on the power system. Therefore, we propose a method to quantitatively assess this impact for various attack scenarios.

1.1 Related Work

The goal of this paper is to use approaches from the Semantic Web (SW) to build the graph model, therefore the related work section focuses on SW technologies are being explored in many areas for data modelling and describing semantic relationships between entities and attributes. Much research has also focused on how this technology can be connected to smart grid research areas. Several approaches exist to build ontologies for power systems using Resource Description Framework (RDF). For instance, [1] focuses on multi-domain energy systems, while [2] concentrates on micro-grid communities and on the service side of the system. Both use SW technologies, but not with the purpose of bridging different domains and enable cyber resilience research. The proposed models do not consider a holistic framework for describing smart grid use cases with all associated layers in both cases. In particular, they lack the connection to the Smart Grid Architecture Model (SGAM), which brings the concept in line with a widely used way to describe use cases, making the models much more accessible for researchers. [3] uses the SGAM as basis for an ontology designed for threat modelling. Although this work involves modelling cross-domain inter-dependencies of cyber-physical systems, it does not utilise SHACL, which allows validation through rules. In contrast to the work presented, our paper proposes an approach that provides a holistic picture that presents a complete framework and shows how SW technologies can be useful in all steps of definition, description, validation, and evaluation. One of these additional aspects is a rule-based augmentation for transforming power systems in Cyber Physical Energy System (CPES). [4] presents an approach of graph-based modelling for CPES and emphasises the need for an automated augmentation process. However, the work focuses only on a specific Supervisory Control and Data Acquisition (SCADA) use case and does not utilise SW technologies.

2 Modelling Approach

The goal of the graph model is to not only describe the power system but also the ICT infrastructure, and the functional design of the cyber-physical system. The reason is that the resulting model should be a holistic approach for all aspects of the smart grid and should be expandable to future applications. Furthermore, a goal of this model is to provide a basis for exchange scenarios in the research community.

2.1 Smart Grid Architecture Model

We chose to start off with an existing model, which offers a categorisation we can build up on and therefore ensure that an enhancement of the model happens in a consistent and interoperable way. The SGAM is categorised along three dimensions (Fig.: 1) the *Domains*, *Zones* and, the *Interoperability Layer*, the individual objects in our model are mapped to these dimensions[5]. The intent of SGAM is a holistic approach to model use cases in smart grids. Therefore, the original use case differs from the one in this paper as we want to model a system with instantiated models, not just a generic use case. An advantage of this approach is that use cases, developed with SGAM, can easily be transferred to models for analysis. The main advantage of using SGAM is its division into various interoperability layers. This allows, for example, the examination of information flows independently of the protocols used, enabling a more universally applicable investigation. Similarly, the functions that different actors in an application have are considered independently of the hardware. This stringent structuring allows for the impact analysis of different attack-vectors on various subareas of the cyber-physical energy system, such as a specific protocol or an attack on a particular functional actor.

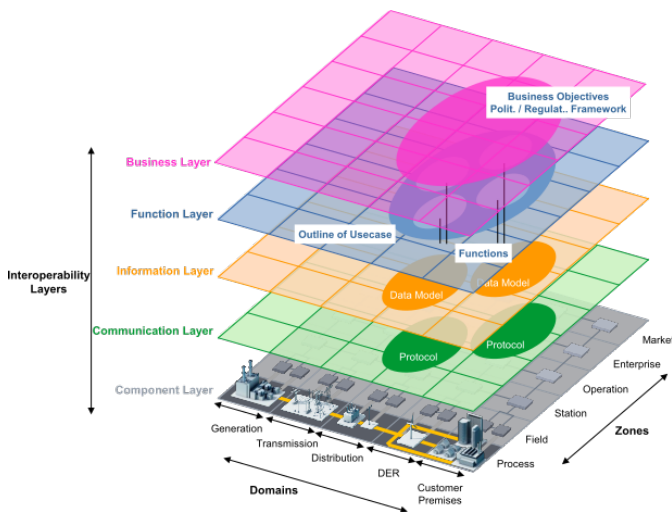


Fig. 1 Visualisation of the Smart Grid Architecture Model showing the three-dimensional structure of the model[5].

2.2 Closed World Assumption

The Open World Assumption (OWA) and Closed World Assumption (CWA) are two contrasting principles on how to model data. Hereby the OWA allows unknown or unrepresented data, so the absence of information is not considered evidence of absence and, therefore, not as invalid. The OWA is often used in SW applications. Still, because we need to verify that all the needed information for the later applications exists in the appropriate form, we follow the CWA considering that a statement is true only if it is explicitly stated and all unknown information is considered false. Shape Constraint Language (SHACL) allows us to follow the CWA.

3 Semantic Web Technologies

In the following, we will present SW based technology, used in this paper. SW references the idea of a version of the internet where the information is linked and machine-readable so that the knowledge can be accessed and used by software tools. To realise this vision, different technologies have been developed over the years, where the main challenges they tried to solve have been interoperability between different data sources and domains of knowledge.

3.1 Resource Description Framework

The RDF is the main standard in the field of SW to represent the information and the relationship between different objects. Every information is represented by a triple consisting of a *Subject*, *Predicate* and, *Object*. An example would be "John hasAge 25": the resource John has the attribute age which has the value 25. Instead of a value, the object can be another resource which creates a Knowledge Graph (KG) representing the relationship between the different references. Graphs have been proven to be a sophisticated way to model smart grids, in comparison to relational databases[4, 6]. The references used in RDF are Uniform Resource Identifier (URI)s, so the linkage of data even outside the KG is possible. RDF Schema (RDFS) are a mechanism in RDF to define classes, properties and, basic constraints in KG, therefore allowing us to build class hierarchies. Because of the wide usage of RDF, frameworks and tools for handling the data and automated reasoning are widely available. As well as a high compatibility with different data formats for storage like XML and TURTLE, listing 1 shows an extract from such a TURTLE file.

3.2 SPARQL Protocol And RDF Query Language

SPARQL Protocol and RDF Query Language (SPARQL) is designed to interact with RDF graphs and supports simple and complex graph pattern matching which enables sophisticated querying capabilities to analyse relationships between objects. In addition to information extraction, SPARQL also allows graph modification by adding, deleting, and changing data.

3.3 Shapes Constraint Language

An important challenge of the SW is to ensure data quality and interoperability, to tackle this, constraints can be specified and validated with SHACL. Although RDFS already provides capabilities for simple constraints, SHACL provides a formal syntax and vocabulary for expressing these constraints and offers a more expressive and flexible validation mechanism compared to RDFS. Shapes define the expected patterns and constraints, which can be rules like required properties, data types and, value ranges. An example where these are more advanced than RDFS is checking for cardinality and value ranges which is essential for the KG we want to build. Because the constraints are defined separately from the data graph, different shapes can be applied for the validation of a data graph depending on the context of the investigation, for example, if a detailed model of the communication network is needed or just abstract communication channels.

4 Ontology

The ontology section outlines the way we modelled the data for this paper, split into the domains: power system, communication network and operational technology. To do so, we show components of the ontology based on SGAM, entailing the interoperability layers which we use to organise the KG. Using this approach enables the independent design of the interoperability layers for rapid prototyping and error detection.

4.1 Power System

The degree of detail that we envision is to model the component layer describing the power system with power flow calculations in a stationary time horizon. Therefore we begin by modelling the power system in sufficient detail to enable these simulations, the data is mainly in the *Component Layer*. However, it is important to note that the model can be enhanced in the future to address additional needs. We started off by modelling the power system based on the data model of *PandaPower*[7] as one of the most common open source frameworks used, so the compatibility to import models from other tools is quite high. The original data model is a relational model, in contrast to the graph model we use, which closely resembles the character of the system and allows us to use graph algorithms. Furthermore RDFS enables us to build a class hierarchy with inheritance and SHACL lets us define specific constraints for the classes. This already exhibits several benefits over using the original model because, as with the SHACL based validation, errors in the KG can be found, which wouldn't be checked otherwise, ensuring data quality. Listing 1 shows the *Turtle* representation of a static generator; it defines the parent class in RDFS and the properties, including the allowed value range, for example, the active power has to be a negative value because positive values are defined as power consumption.

Listing 1 Representation of the RDFS and SHACL shapes of a static generator in *Turtle*.

```
errol:StaticGenerator
  rdf:type rdfs:Class ;
  rdf:type sh:NodeShape ;
  rdfs:label "Static_generator" ;
  rdfs:subClassOf errol:GenerationConsumption ;
  sh:and (
    [
      sh:path errol:p_mw ;
      sh:maxInclusive "0"^^xsd:decimal ;
    ]
  ) ;
  sh:property [
    rdf:type sh:PropertyShape ;
    sh:path errol:q_mvar ;
    sh:datatype xsd:decimal ;
    sh:description "reactive_power" ;
    sh:maxCount 1 ;
    sh:minCount 1 ;
    sh:name "q_mvar" ;
  ] ;
  sh:property [
    rdf:type sh:PropertyShape ;
    sh:path errol:type ;
    sh:datatype xsd:string ;
    sh:description "sgen_type" ;
    sh:maxCount 1 ;
    sh:name "type" ;
  ] ;
  sh:targetClass errol:StaticGenerator ;
```

4.2 Control Infrastructure

The control infrastructure of the layers *function*, *Information*, and *communication* but also of the physical ICT infrastructure like hosts the systems are running on and the network components. Because we mainly focus on internet based solutions the internal infrastructure of the internet service provider is out of scope. Figure 2 shows the simplified KG used in this paper for one household with a remote controllable heat pump. *errol*, the acronym for "Energy Resilience Research Ontology Library", is the namespace used for the newly developed ontology and indicates classes and predicates we defined. *errol:HouseHold* is a subclass of *errol:AssetGroups*, which implements the idea of *Zones* from SGAM for an instantiated model, in this example an household is equivalent to *station*. Functional actors are elements which represent one functional entity in the system like a HEMS. Hereby the functions can be abstracted from the technical implementation, an functional actor may be implemented on a specific controller or may be implemented in a distributed manner. [8] describes a similar implementation to achieve the abstraction of the functional layer. Functional blocks are the concrete implementations of individual functions of a functional actor. A functional actor can hold multiple functional blocks simultaneously. In a HEMS, for example, one functional block might be self-consumption optimisation, while another functional block could be the remote controllability of a smart home. In the example shown in figure 2,

there is a functional actor for the cloud backend of the HEMS provider and another for the HEMS within the smart home. Each of these has a functional block that implements remote controllability. The relationship between the functional blocks is realised through information object flows, which represent the flow of information and thereby the functional connections between the different actors.

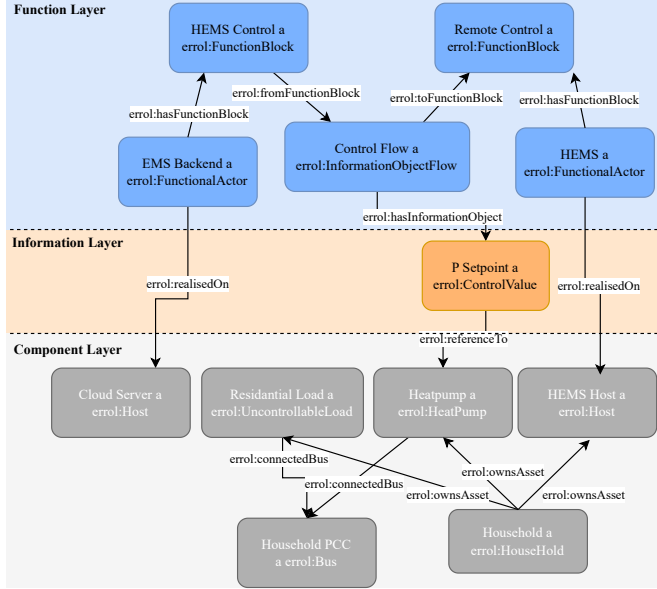


Fig. 2 Simplified visualisation of the KG used in this work, consisting of a HEMS solution.

These flows are directed, making the direction of the information flow clear. As a result, control direction and monitoring must be represented in two separate information flows. The transmission of measurement values has been omitted in this example, as it is not relevant for the intended impact analysis. These elements are all part of the *function layer*. Each information object flow references the information objects that are being transmitted. *errol:ControlValue* is a subclass of *errol:InformationObject*, specifically for control signals. Information objects can stand alone or reference physical components, such as in this example, a heat pump whose power output can be controlled. In this way, the information objects represent the relationship between the functional layer and the physical components. Furthermore the hosts on which the functional actors are realised are added in the component layer, which allows for analysis of the dependency of applications on the physical ICT infrastructure.

5 Workflow of Impact Analysis for Cyber-Attacks

Figure 3 shows the workflow of the impact analysis developed in this work. The starting point for the investigations done in this work are *PandaPower*[7] models, which get imported into

the presented graph format. The power system model then gets validated against the SHACL shapes for the power system.

Following this the control infrastructure is augmented automatically based on predefined augmentation rules. This augmentation process contains the hardware of the control infrastructure as well the function blocks needed for the application and also the information flow between these function blocks. Furthermore, information like the manufacturer and firmware version can be added to identify the scope of a cyber-attack which may only work on a specific firmware version.

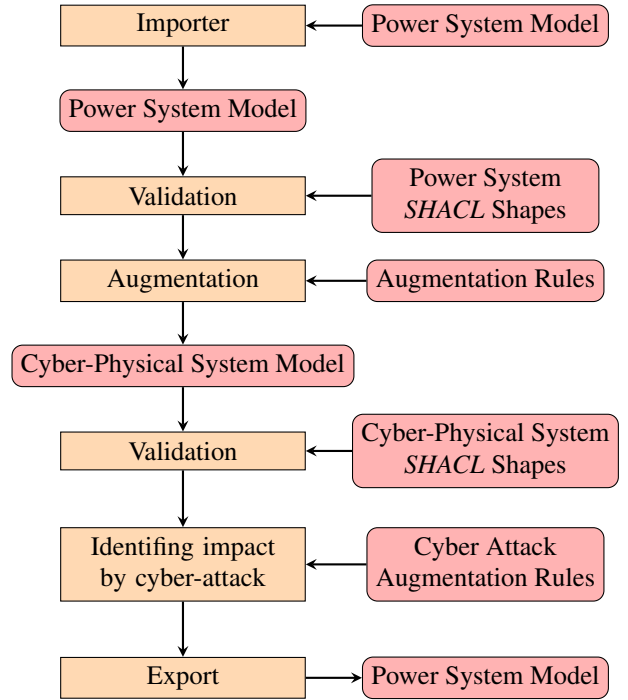


Fig. 3 The workflow starting from a *PandaPower* model showing the different steps, including the augmentation step, impact analysis, and export.

The augmentation rules allow probabilistic distributions, for example equip 30 percent of electric vehicles with a specific HEMS than connect these to a backend system depending on the manufacturer of the EV. SPARQL is the foundation of the augmentation engine, which allows the definition of augmentation rules in a declarative way which is a significantly more effective approach than solely imperative implementation the other parts are implemented in python. The main advantage of this approach is the possibility to make probabilistic rules with probabilistic behaviour. The augmentation rules are also realised as RDF graph, bringing the same advantages of validation and re-usability. Three kinds of rules are implemented *add* rules allowing adding new object based on templates, *change* rules allow to change or append a specific triple, and *delete* rules. A SPARQL query is used to define which elements should be modified or to which element the new objects should be connected. The probabilistic behaviour is defined by

two probabilities the first defines if the rule is applied for specific element and the second defines which template should be used. After the augmentation the result is a complete model of the cyber-physical energy system, which get validated by the corresponding SHACL shapes. The next step is the simulation of the cyber-attack, for this the type attack vector and the scope must be defined. The cyber-attacks used for this paper are also implemented as *change* rules in the augmentation engine. An example may be a compromised backend of an EV manufacturer allowing an attacker to arbitrarily control charging of connected EVs. Based on the connections modelled in the graph model the change in the *process zone* can be applied before exporting a power system model in the *pandapower* format. In the last step power flow simulations are performed to examine the impact of different attack vectors on the power system.

6 Case Study

In this section we present a case study conducted based on the framework, the case study was intentionally designed to be relatively straightforward, ensuring that it is easily understandable while primarily demonstrating the core functionality of the proposed method. In this case study we investigate the use case of remote controllable HEMS systems and the impact on the grid when the central control infrastructure of the HEMS provider gets compromised.

6.1 Scenario Description

The basis for the scenario are combined semi urban medium and low voltage grid from *SimBench*[9]. This benchmark case consists of one 110 kv transformer station and 110 secondary substations connected via a 20 kV network in a ring topology. Furthermore the low voltage grids have 8982 buses in total connected in radial topologies with 7823 households of which some also have PVs, Battery Storage Systems (BSSs), heat pumps and EVs connected to them, additionally commercial loads are part of the model. The benchmark case also contains production and load time series for the different units, for this paper we analysed the time steps with the highest and lowest sum of transformer loading. For the augmentation, every bus connected to a household load is defined as household point of common coupling (PCC) and a *errol:HouseHold* gets created, which then owns all units connected to this bus. If the household contains any controllable loads or production a HEMS consisting of a host, a functional actor, and the function block for remote contractility are added, as shown in figure2. Three different HEMS templates for different manufacturers exist, they get added which the probability of 50%, 30% and 20%. For each of the manufacturers a backend system gets created and the function blocks of the HEMS of this manufacturer get connected via an information object flow. For all controllable units *errol:controlValues* are created referencing the active power of the units, which then get connected to the corresponding information object flow. Because the objective of this case study is a worst case analysis of the impact of a

compromised HEMS operator for the grid, the augmentation rules identifies all values which are controllable by a specific backend and either set them to the maximal or minimal possible value. The underlying assumption for the BSS is that in normal operation the state of charge is not fully utilised, because of battery health concerns, and therefore the full power can be used for a short time attack. We analysed two attacks for each manufacturer one trying to maximise the load in the grid and one trying to minimise it.

6.2 Result and Discussion

Figure 4 shows the difference in the loading of the transformers of the secondary substations for the high load case. Every load gets compared to the loading in the scenario with out an attack. "Max. 1", for example, is the difference in load for the scenario that the attacker gains access to manufacture 1 and wants to maximise the load in the grid.

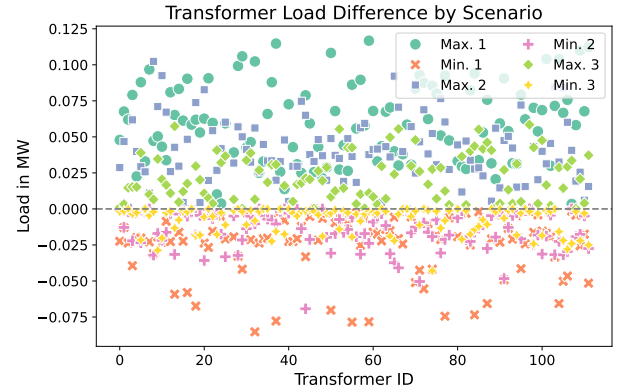


Fig. 4 Load difference of transformers in secondary substations for different attack scenarios in MW in the high load case.

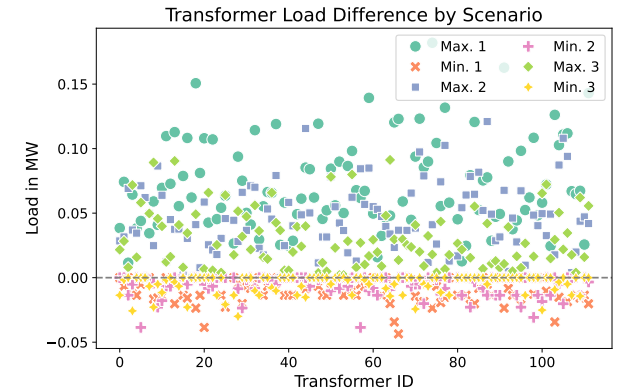


Fig. 5 Load difference of transformers in secondary substations for different attack scenarios in MW in the low load case.

Therefore the results for all maximising attacks are above zero and for all minimising attacks are below zero. As expected the attacks on manufacture 1 have the greatest impact in general because it was distributed with the highest probability in the augmentation process. Nevertheless, for certain substations,

this does not hold true because, by coincidence, a larger portion of the load connected to these substations is controllable by a different manufacturer. Figure 5 shows the corresponding results for the low load case. When comparing the results it can be seen that the maximising attacks in this case have a slightly greater effect with a load change up to 0.182 MW compared to 0.117 MW. The delta is mainly caused by turning off the PV production. On the other hand the impact of the minimising attacks is lower because in this case the total power of controllable loads is smaller and BSS with the goal of self consumption optimisation are already charging. In general it can be stated that the impact of the attacks does not lead to problematic grid states, i.e. violation of voltage or line and transformer limits. This is additionally supported by a specific analysis of the different voltage levels in the scenario. Figure 6 presents all medium and low voltage levels as box plots for the different attack scenarios. No clear deterioration can be observed, which is consistent with our experience from working with the *SimBench* models, as they exhibit a high robustness to voltage deviations. However, a study using real network models is necessary to demonstrate the specific impact on the networks. The presented results nevertheless showcase the functionality of the developed framework and the feasibility of it for these kind of analysis.

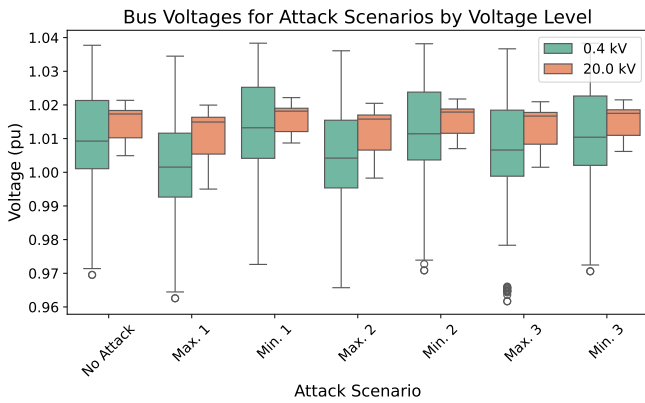


Fig. 6 Voltages of all busses differentiated by different voltage levels as box plots. For the different attacks scenarios in the high load case.

7 Conclusion and Future Work

This work presents a comprehensive approach to modelling and analysing the impact of cyber-attacks on interconnected BTM infrastructure within a cyber-physical energy system. By utilising Semantic Web technologies, SHACL, we have developed a graph model based on SGAM that effectively represents the interdependencies between control infrastructure and the power system. This model is used in our framework which automatically augments the control infrastructure to the electrical grid and allows the impact analysis of cyber-attacks. Our case study demonstrates the feasibility of the developed model and framework, showing that the analysed benchmark case is

not jeopardised by the examined attack vectors. Future work will focus on increasing the model's complexity to identify less obvious risks in future energy systems and integrating scenarios that are closer to real-world grid conditions. Additionally, the framework will be used to generate models of CPES as input data for more sophisticated simulation environments, such as co-simulation platforms, providing a foundation for the development of resilience-enhancing measures.

8 Acknowledgment

This work has received funding from the Federal Ministry of Education and Research (BMBF) under project funding reference 03SF0694A.



- [1] Devanand, A., Karmakar, G., Krdzavac, N., Rigo.Mariani, R., Foo.Eddy, Y.S., Karimi, I.A., et al.: 'OntoPowSys: A power system ontology for cross domain interactions in an eco industrial park', *Energy and AI*, 2020, **1**, pp. 100008. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S2666546820300082>
- [2] Chun, S., Jin, X., Seo, S., Lee, K.H., Shin, Y., Lee, I. 'Knowledge Graph Modeling for Semantic Integration of Energy Services'. In: 2018 IEEE International Conference on Big Data and Smart Computing (BigComp). (Shanghai: IEEE, 2018. pp. 732–735. Available from: <https://ieeexplore.ieee.org/document/8367218/>
- [3] Sandberg, H., Teixeira, A., Piatkowska, E.: 'Deliverable 2.3-Tools for smart grid cyber security', , 2016,
- [4] Klaer, B., Sen, O., der Velde, D.v., Hacker, I., Andres, M., Henze, M. 'Graph-based model of smart grid architectures'. In: International conference on smart energy systems and technologies (SEST). (, 2020.
- [5] Bruinenberg, J., Colton, L., Darmois, E., Dorn, J., Doyle, J., Elloumi, O., et al.: 'CEN -CENELEC - ETSI: Smart grid coordination group - smart grid reference architecture report 2.0'. (, 2012)
- [6] Jain, S., Groppe, S., Bhargava, B.K., editors. 'Semantic Intelligence: Select Proceedings of ISIC 2022'. vol. 964 of *Lecture Notes in Electrical Engineering*. (Singapore: Springer Nature Singapore, 2023). Available from: <https://link.springer.com/10.1007/978-981-19-7126-6>
- [7] Thurner, L., Scheidler, A., Schäfer, F., others: 'pandapower — An open-source python tool for convenient modeling, analysis, and optimization of electric power systems', *IEEE Transactions on Power Systems*, 2018, **33**
- [8] Neureiter, C., Lehnhoff, S., Engel, D.: 'A domain-specific, model driven engineering approach for systems engineering in the Smart Grid'. First edition ed. (Fredesdorf: MBSE4U, 2017)
- [9] Meinecke, S., Sarajlić, D., Drauz, S.R., others: 'Sim-Bench—A benchmark dataset of electric power systems to compare innovative solutions based on power flow analysis', *Energies*, 2020, **13**, (12). tex.article-number: 3290