energies

MDPI

Article

Assessing the Impact of Cybersecurity Attacks on Power Systems

Athanasios Dagoumas

Energy & Environmental Policy Laboratory, School of Economics, Business and International Studies, University of Piraeus, PC 18532 Piraeus, Greece; dagoumas@unipi.gr

Received: 4 December 2018; Accepted: 21 February 2019; Published: 22 February 2019

Abstract: Cybersecurity is an emerging challenge for power systems, as it strongly affects their reliability and the whole energy system cost. The paper uses several Unit Commitments (UC) models, applying different methods to tackle renewables' uncertainty. The selected power system is IEEE RTS 96. The UC models are used to assess the impact of different cybersecurity threats. The focus is to assess their impact on the total operating cost and the power grid adequacy to handle them. The comparison between the UC models shows that more robust UC models lead to higher total operating costs. The cost, unit dispatching, and energy mix evolution have a non-linear trend, depending on the power system characteristics and the cyberattacks types. However, the paper provides evidence of considerable price signals in the case of the examined cyberattacks. Each Transmission System Operator (TSO) should examine combinations of cyberattacks and operating conditions to identify crucial cases for system stability and power system cost operation. The applied methodology would also require substantial developments or supplementary approaches to assess cyberthreats at the distribution level.

Keywords: cybersecurity threats; unit commitment; uncertainty; power system; IEEE RTS 96

1. Introduction

Power systems are among the most complex and critical infrastructures of a modern digital society, serving as the backbone for its economic activities and security. It is therefore in the interest of every country to secure their operation against cyber risks and threats [1], as stated in the report of the European Commission's Smart Grids Task Force, as well as in the 'Cyber Security in the Energy Sector' report [2] published in 2017 by the Energy Expert Cyber Security Platform (EESCP), stressing the need for addressing the major challenges of cyber threats in the energy sector as well as providing the requirements for addressing appropriately cybersecurity. Potential cybersecurity threats could have cascading effects, leading to damage and power outages, as well as personal data breaches [3].

Over the last few decades, the power system has been modernized. This modernization concerns (i) market aspects, due to its liberalization, (ii) organizational aspects, due to the change of roles from the utilities, where central planning is replaced by decentralized operation with active participation of final consumers, as well as (iii) operational aspects, due to the evolution of smart technologies and communication protocols. Novel Internet of Things (IoT) nodes and smart meters are introduced in various parts of the energy grid, while existing SCADA systems are used for monitoring and control operations that are widely dispersed in case of energy transport and distribution networks. Furthermore, distributed control systems (DCS) are used for single facilities or small geographical areas, while remote terminal units (RTU) and programmable logic controllers (PLC) monitor system data and initiate programmed control activities in response to input data and alerts. Figure 1 provides the typical structure of a modern power system [4], as well as the communication among the different assets of the power system, in generation, transmission, distribution, and consumption.

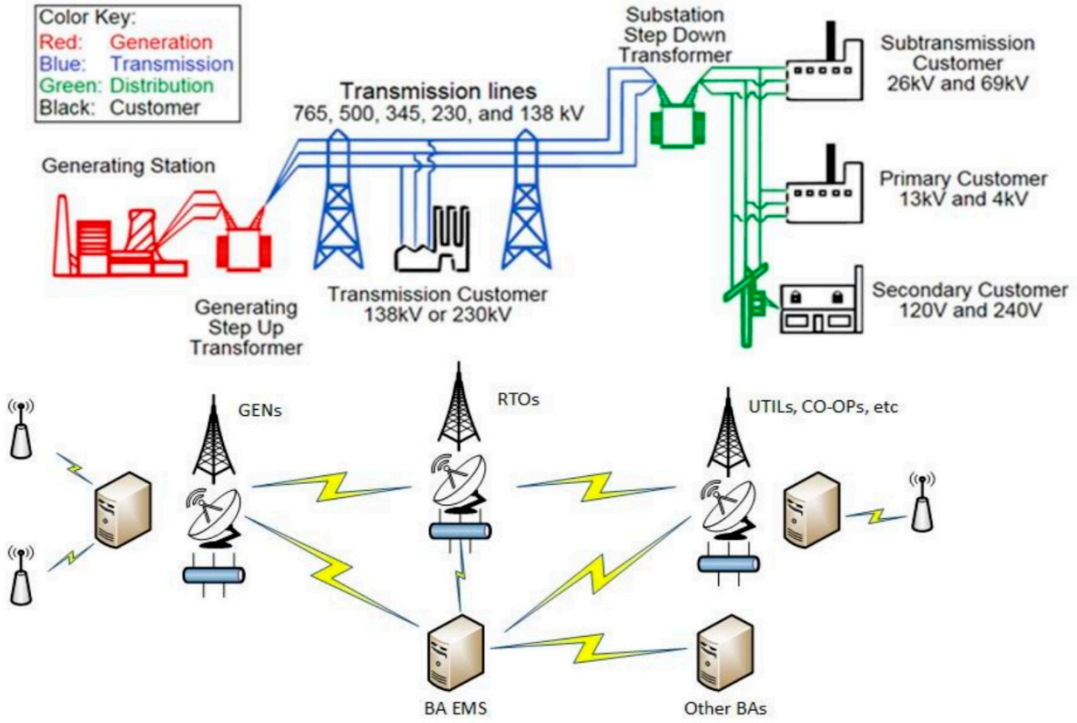


Figure 1. Typical structure of an electric power system (source: INL, 2016).

Cyber threats are evolving at a tremendous pace, exploiting capabilities created by the modernization of the power systems, as stated in the ENISA Smart Grid Threat Landscape report [5]. This is related to the transition from a centralized power system, based on large power stations and vertical integrated utilities, to a decentralized power systems model [6], as well as the complementary evolution of more advanced communication and digital systems. Modern power systems are becoming increasingly dependent on communication systems for their operations, and as a result increasingly susceptible to cyberattacks. As stated in the NIST report for Guidelines for Smart Grid Cybersecurity [7], while integrating information technologies is essential to building the smart grid and realizing its benefits, the same networked technologies add complexity and introduce new interdependencies and vulnerabilities to potential attackers and unintentional errors.

However, the development of smart power systems creates critical challenges, especially related to tackling rapidly evolving cybersecurity issues. This affects the capability of the Transmission and Distribution System Operators (TSOs and DSOs) to guarantee resilience, reliability, stability, security of supply, and power quality for the final users of electricity.

- Essential power system functions at risk from cyberattacks include:
- Electricity supply (generation) stability and reliability;
- Electricity transmission and distribution stability and reliability;
- Communication between systems or equipment;
- Information on the operating conditions of generation, transmission or distribution equipment;
- Black start capability;
- Equipment performance and ability to recover (backup systems).

Cyberattacks could affect not only system operators, but also market participants. For example, demand aggregators create billing systems for issuing invoices to their final consumers. Those systems, either using desktop computers, cloud services, or blockchain technology, are in danger of cyberattacks, which could considerably affect cash flows and finally the viability of market participants. Similar threats exist for participants that use peer-to-peer trading services. Although such types of threats

are possible and can have important effect, the threats that affect grid stability are considered more challenging due to their cascading effects.

A crucial issue in the assessment of cybersecurity threats is the identification of their impact on power systems' reliability and the whole energy system cost. This paper uses different unit commitment models, implementing different levels of robustness to tackle uncertain renewables generation, to assess the impact of the cybersecurity threats on the power systems. It provides price signals on the impact of the threats on the wholesale marginal prices and on the whole energy system costs. It identifies cases where black-out events are inevitable, estimating the overall cost of the interruption in energy service. The paper provides useful insights to the TSOs, as it provides price signals of the cyberthreats, enabling the identification of benchmark values for relevant equipment costs and tariff policies for producers and end users.

Sun et al. [8] provide a review of cyber systems in a smart grid, summarizing the cyber protection and cyber-physical system testbeds. The paper proposes a methodology for the detection of coordinated cyberattacks, which, however, is not holistic as there are unsolved cyber vulnerabilities that require further research. Mrabet et al. [9] provide a review of the cybersecurity requirements in smart grids, describing different types of severe cyberattacks. The paper proposes a cybersecurity strategy to detect and counter these critical attacks. Jarmakiewicz et al. [10] describe a cybersecurity protection approach for power grid control systems, by identifying key elements of the power system and their importance to power grid security. Shi et al. [11] provide a review of models, methods, and applications for the cyber-physical interaction in power systems. Poudel et al. [12] present a real-time cyber-physical system testbed for power system security and control, focusing on voltage stability and generation loss. Hammad et al. [13] present an offline co-simulation testbed for studies of power systems' cybersecurity and control verification. Liu et al. [14] present a novel model for the evaluation of the validity of active cyber-physical distribution system. The paper quantifies the impact of cyber faults on functionality validity during distribution automation.

The previous paragraph shows that the literature on cybersecurity issues in power systems is rapidly increasing. However, the papers mainly focus on the identification of security threats, rather than on the assessment on the actual operation and cost of the power systems. There are also a growing number of research papers on specific aspects of the power systems. Part et al. [15] focus on the implementation of cybersecurity strategy for safety systems of nuclear facilities. Gunduz and Jayaweera [16] provide a reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems. They present a probabilistic reliability model, concluding that impacts of cyber threats are considerable. However, they do not provide relative price signals but suggest that a relative quantitative assessment is required. Sundararajan et al. [17] provide a survey of challenges and solutions for distributed generation cyber-physical security. The paper identifies the key vulnerabilities, attacks and potential solutions for solar and wind units at the protocol level. Tellbach and Li [18] examine cyberattacks on smart meters in residential customers, concluding that integrity and confidentiality attacks cause monetary effects on the power grid, while availability attacks—besides monetary effects on the power grid—mainly aim at delaying or stopping the operation of smart meters. Ye et al. [19] provide a quantitative vulnerability assessment of cybersecurity for distribution automation systems. Potential physical consequences of cyberattacks are analyzed at two levels: the terminal device level and the control center server level. A game theory-based approach is used to examine the relationships among different vulnerabilities by introducing a vulnerability adjacency matrix. The results in a relatively small system demonstrate the reasonability and effectiveness of the proposed methodology. Venkatachary et al. [20] provide a review of the economic impacts of cybersecurity in the energy sector. However, the analysis is done in a top-down manner, without applying a detailed robust methodology that assesses the impacts of specific threats to the power system. Liu et al. [21] examine the impact of cyberattacks on the economic operation of power systems. Liu et al. [22] estimate the impact of three different possible cyber events on a physical power grid, using an integrated cyber-power modeling and simulation testbed. Poudineh

and Jamasb [23] examine the impact of electricity supply interruptions in case of the Scottish economy. They provide the sectoral interdependencies as well as the cost of energy not delivered. Considering that those interruptions could result from cyberattacks, the paper provides insights into related price signals.

Cybersecurity is affected by the structure of power systems, as well as by communication protocols and standards. Leszczyna [24] provides a review of standards with cybersecurity requirements for the smart grid. The paper assesses 17 standards, which are described from a cybersecurity requirements perspective and refer to the IEC smart grid architecture. Moreover, the relationships between cybersecurity requirements in different standards are analyzed and visualized. The role of communication standards is important, as shown in a paper that provides a technical overview and benefits of the popular IEC 61850 standard for substation automation [25]. Jarmakiewicz et al. [26] describe a cybersecurity protection approach for power grid control systems. The paper also discusses the verification process of the functionality provided by an implemented cybersecurity system. Cybersecurity is a challenge for different systems and applications, leading to the development of cybersecurity assessment models. A recent paper [27] describes a cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory in order to evaluate cybersecurity risk of particular applications. Zarreh et al. [28] describe a game theory-based cybersecurity assessment model for advanced manufacturing systems. The literature review revealed that cybersecurity in power systems is a challenging issue. Relevant papers are rapidly disseminating; however, they mainly focus on the identification of relevant threats and vulnerabilities, rather than on the quantification of their impact on the power system operation and cost. This gap is the focus of this paper, namely, to provide a quantitative assessment of the impact of cybersecurity threats. Towards providing robust price signals, robust methodologies must be selected. This is the reason that a Unit Commitment (UC) model has been chosen for this analysis. The aim of a UC algorithm is to determine which units will produce energy in each hour of a day to meet demand. The UC problem is complex as it incorporates several techno-economic constraints related to the production units and the transmission lines. The UC problem identifies the power units' dispatch, considering their operational and maintenance costs, their ramping capacity, their capability to provide ancillary services, and other techno-economic criteria. The UC problem is formulated as a Mixed Integer Linear Programming (MILP) problem, which is adequate to handle such complicated problems. The problem is solved in such a way that the overall fuel cost is minimized with respect to the system's and unit's constraints.

The applications of unit commitment models are also extended, as they are considered robust approaches to simulate the power systems operation. UC models examine—in most cases—a national power system or a small power system, providing insights into different challenges it faces. However, to our knowledge, there has been no attempt to quantify the impact of cybersecurity threats on power systems. Moreover, there are few cases providing a comparison among different UC models, which would be a useful step towards revealing the required level of detail for robust solutions and the impact of uncertainties on key variables. The Energy and Environmental Policy laboratory at the University of Piraeus has extensive experience in developing and extending UC models, but its work mainly concerns the Hellenic power system [29–31]. Considering that the assessment of cybersecurity threats is a challenging issue, the application of a common power system such as the IEEE RTS 96 with increased penetration of renewables has been selected, as this represents a large but more commonly used power system in the international community. This has led to the application and extension of UC models by the Renewables Energy Analysis Lab at the University of Washington [32].

The paper contributes to the literature by applying different UC models, differentiated by tackling uncertain renewable electricity generation, to estimate the impact of cybersecurity threats in a commonly used power system. The highlights of the paper are: (i) integration of cybersecurity threats in the Unit Commitment problem, (ii) comparison of different UC models on the IEEE RTS 96 power system, tackling differently the uncertainty of renewable electricity generation, (iii) assessment of the impact of cybersecurity threats in the power system cost and scheduling; and (iv) provision of useful

insights into the effects of cybersecurity threats on the total operating cost of a power system and its adequacy to handle them.

The rest of the paper is organized: Section 2 provides the methodology applied. Section 3 examines potential cyberattacks on the power system, identifying scenarios that will be described, simulated, and discussed in Section 4. Finally, Section 5 provides the main conclusions and highlights of the paper.

2. Methodology

The Renewables Energy Analysis Lab at the University of Washington has developed five different implementations of the Unit Commitment problem [33], where the basic formulation is described in Appendix A. The application of the UC models concerns the IEEE RTS-96 power system, shown in Figure 2. This power system includes, apart from thermal production units of various fuel (nuclear, coal-fired, diesel, natural gas) with 10,215 MW total installed capacity, renewable energy generation units from wind, whose power production is uncertain compared to other renewable technologies such as photovoltaics [33]. The whole system can be seen in the following layout.

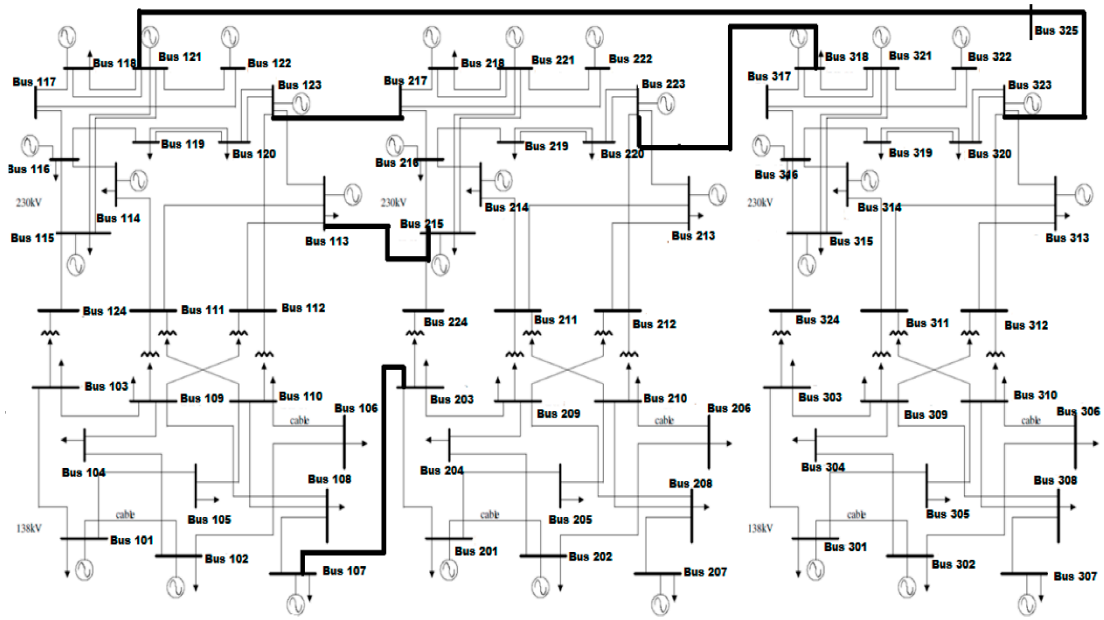


Figure 2. The electrical system IEEE RTS-96.

Renewable energy sources introduce uncertainty, due to the stochastic nature of the wind and the weather conditions in general. Transmission system operators must forecast the real generation from those renewable sources, affecting the stability of the power system, the strategy of energy market participants. We did not consider other renewable technologies, such as photovoltaics, as their power output can be forecasted with much higher accuracy, so the introduction of photovoltaics would lead to an upgrade of the net load at each bus rather than an introduction of uncertain renewables production. Photovoltaics, aside from the sunset effect, which affects the unit commitment problem and enhances the need for flexible ramping capacity, does not increase uncertainty in the dispatch of power units, as the uncertain power output from wind farms is doing.

The models developed by the Renewables Energy Analysis Lab, used for this paper, are the following: Deterministic unit commitment, Stochastic unit commitment, Improved interval unit commitment, Interval unit commitment, and Robust unit commitment. Each of those models uses a different mathematical procedure to forecast the anticipated renewable production. Some of them are more conservative than others. Consequently, those models are committing more thermal units, and the stability of the system is increased but with a higher total economic cost.

The UC models require a considerable amount of input data, which are described in Appendix B. The modelers have the option to change some constants in the data input program. Through those options, we can modify the penetration of the renewable sources, the variable cost, and ramping capabilities of thermal units, the capacities of the transmission lines, the wind profile and a penalty factor in the case of spilled wind production or unserved loads. In our research, we choose to have 30% of energy from wind power units, which is much higher than the current state of most power grids and a possible future power system of the next decades. Another decision is to go with the unfavorable or favorable wind profile. We have chosen the unfavorable wind profile.

2.1. Differences between the UC Models

2.1.1. Deterministic Unit Commitment Model (DUC)

This model uses only one forecast for the wind production, resulting from the elaboration of historical data. This model provides either conservative or very inefficient solutions in certain conditions. Therefore, the incapability of the model to tackle uncertainty of renewables production, leads to solution with limited robustness.

2.1.2. Stochastic Unit Commitment Model (SUC)

The stochastic model, instead of using a fixed forecast calculates the unit commitment for 10 different wind scenarios, assigning a weight on them based on the probability of each scenario. The model captures a certain level of unhedged uncertainty, which is quantified concerning expected unserved loads and spilled production [34].

2.1.3. Interval Unit Commitment Model (IUC)

This model implements a simplified representation of renewables uncertainty. The deterministic scenario is used a basis, on which an upper and a lower bound scenario for the wind energy production are identified. The model uses upper and lower bound forecasts in order to estimate the ramp-up and ramp-down limits for the thermal units, which leads to the commissioning of more power units and increase of the overall energy cost.

2.1.4. Improved Interval Unit Commitment Model (IIUC)

The Improved Interval Unit Commitment Model (IIUC) is an enhanced version of the previous model, where the upper and lower bounds are replaced by four scenarios. The two new scenarios incorporate more realistic slopes for the ramping capability of the thermal units. This approach is much more realistic because the previous extreme transition values are not possible in the real world. As a result, we anticipate that the IIUC solution will be less expensive than IUC.

2.1.5. Robust Unit Commitment Model (RUC)

The objective function of the model is the following, as presented in [35]:

$$\sum_{t=1}^{T}\sum_{i=1}^{I}(\alpha \cdot x_i(t) + suc_i(t)) + max\left\{\sum_{b=1}^{B} k_b \cdot g_{i,b}(t)\right\} \quad \forall\, t \le T,\ i \le I \tag{1}$$

The nomenclature for all UC models are provided in Appendix A. The objective function includes the startup cost and fixed production cost of the power units, as well as the variable production cost in the worst-case scenario, which stands as the main difference with the other models. The model is considered as a conservative unit commitment model with increased robustness, as it is based on the worst-case scenario. The model initially decides which units to be committed, based on their fixed and start-up costs. Then the output power of the power units is calculated to meet the reserves for the worst-case scenario [35].

2.1.6. Comparison of UC Models

Considering the theoretical model differences, a recent work [36] confirms those results. Figure 3 summarizes the differences between the models. Figure 3 shows that more robust UC models, being more "conservative" in constraints, led to the commitment of more power from dispatching units.

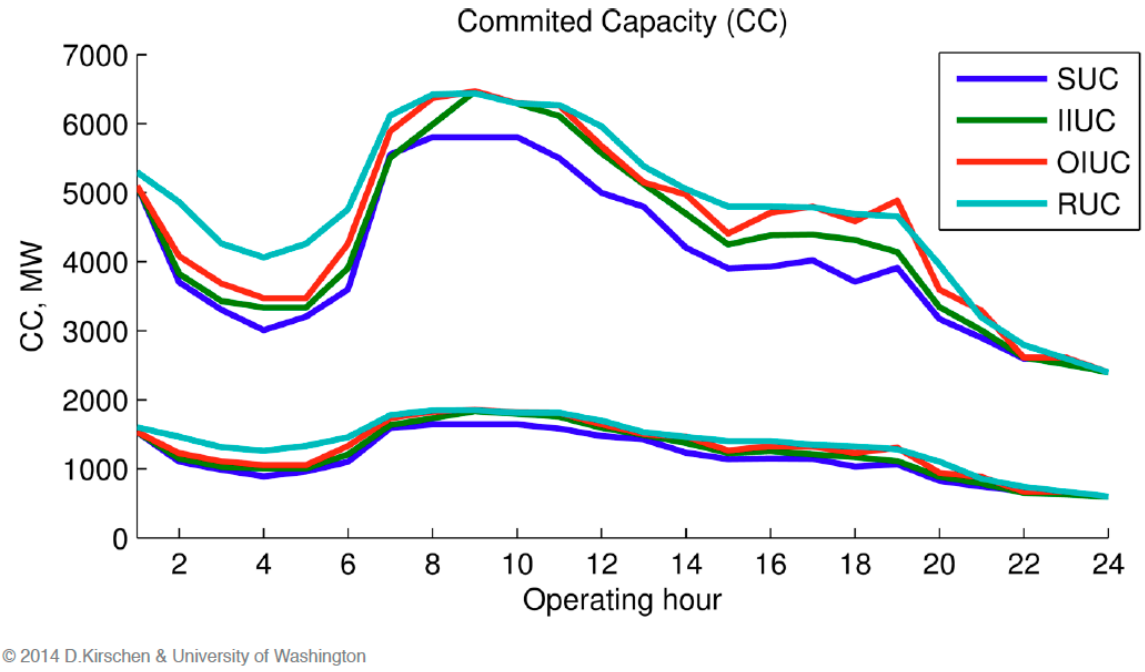


Figure 3. Committed capacity using different UC models and different wind profile (favorable for the upper group of lines and unfavorable for the lower group of values), source: Kirschen [34].

3. Cyberattacks on the Power System

The UC models will be demonstrated on dry-run scenarios of the IEE-RTS96 power system. The prototype will provide a set of different scenarios concerning cybersecurity threats. This section describes potential threats for the power systems. In order to identify the threats, it is important to describe the different Information and Communication Technologies (ICT), integrated within the power systems, with special focus on the TSO, which is responsible for the reliable operation of the transmission system.

Cybersecurity threats affect the capability of the Electrical Power System Operators to guarantee resilience, reliability, stability, security of supply, and power quality to the final users of electricity. Essential system functions at risk of cyberattacks for this demonstration include:

- electricity supply (generation) stability and reliability;
- electricity transmission stability and reliability;
- communication between systems or equipment;
- information on the operating conditions of generation, transmission equipment;
- black start capability.

More specifically, potential cybersecurity threats are:

- smart meters may be used by hackers as entry points into the broader power system;
- unauthorized interference on the measurement of electricity consumption (end-users);
- trip a power-generating unit or modify its schedule;
- cause a blackout in a big area of the grid;
- attack on the electricity market;

- disrupt the proper functioning of the system;
- attacks through the power system on civil infrastructure.

TSOs are responsible for the operation, maintenance, and expansion of the transmission systems. TSOs use Supervisory Control and Data Acquisition System (SCADA) for the high-level process supervisory management of transmission system facilities. SCADA systems are vital for system operators to monitor and control the electricity network. The fact that SCADA/EMS systems are now being interconnected and integrated with external systems creates new possibilities and threats. Those issues have been emphasized in the CIGRÉ joint working groups (JWG) D2/B3/C2.01 and D2.22 [37,38]. As part of the JWG efforts, the various interconnections of a substation were investigated [39]. An emerging challenge of the Transmission System Operators (TSOs) is to identify the vulnerabilities in the power systems, as well as how each cybersecurity threat affects independently and cumulatively those aims. This will help with the design of adequate security measures to ensure a cyber-secure system, which concerns the design of appropriate procedures and policies to tackle each threat, considering the relevant clauses of the ISO/IEC 27032:2012 and ISO 27001 standards.

The power units have installed Remote Terminal Units (RTU), using PLCs for their communication with the system operator. The communication protocols are based on international standards IEC60870-101 and IEC60870-104. The international standard IEC61850, which defines communication protocols for intelligent electronic devices at electrical substations, is an innovative standard, especially as it tackles multi-vendor interoperability [25]. The renewable units' RTUs communicate through ISDN or PSTN telecommunication services. Distributed generation units, such as photovoltaic units, are usually obliged to install a GSM/GPRS modem for communication purposes, while wind parks have an RTU for their communication with the dispatcher. Although the renewables do not participate in real-time dispatching in the same way with conventional thermal units, due to their stochastic nature, their rapidly growing share raises issues about the scaling-up of potential cybersecurity threats that could affect power systems reliability, security, and overall costs. Therefore, the identification of cybersecurity threats for relevant technologies for the main energy carriers of the future power system, namely natural gas, wind, and solar energy, is an important challenge. The same concerns are relevant in the identification of threats on indicative customers from different consumer types, using different telemetering devices (mainly for billing and profile patterns aims, rather than for dispatching purposes). The structure and communication protocol of power systems identify the potential threats. In case of the evolution of power line communication as a dominant communication method, or the transformation of a power system as an Internet-of-Things place, every device, plug, or connection point of the grid becomes vulnerable to potential cyberattack. This further enhances the importance of cybersecurity as a major challenge for a power system, as the threat is distributed at many levels and points, compared to the top-down consideration of cybersecurity that mainly focuses on attacks on power plants, central control systems, and high-voltage substations. The approach implemented in this paper, using the unit commitment model for assessing cyberthreats, can be robust for tackling top-down threats that affect system stability; however, the consideration of threats in a distributed manner would require considerable model improvements or use complementary approaches to tackle those challenges in more detail.

The communication of the thermal power plant with the central dispatching of the TSO is done through special software, called Real-Time Dispatching (RTD), providing instruction every 5 min, and the Automatic Generation Control system (AGC), which enables the provision of the required ancillary services in seconds, as depicted in Figure 4. The thermal units also have a Digital Control System (DCS), which provides several checks concerning its operation and communication with the substation and the dispatching center.

Several types of cyberattacks can take place. This work focuses on attacks on big plants that are dispatched by the Transmission System Operator (TSO), monitored through SCADA systems, and linked to the TSO-operated Automatic Generation Control system (AGC). The examined scenarios are described and discussed in the next section.

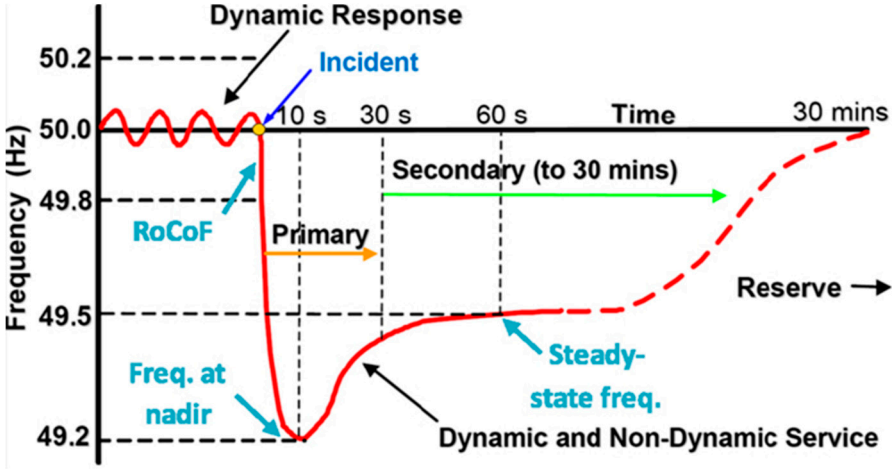


Figure 4. Frequency deviation following of activation of dynamic and non-dynamic ancillary services by a thermal power plant, linked to the AGC.

4. Results and Discussion

This section provides the results from the simulations. The examined scenarios focus on providing a comparison among the different UC models and secondly on the comparison among the different cybersecurity attacks.

Firstly, the different UC models have been run without any cyberattack, leading to baseline scenarios, entitled DCU_BAS, SUC_BAS, IIUC_BAS, and RUC_BAS for the deterministic, stochastic, improved internal, and robust UC models, respectively.

Secondly, we examined a Cyberattack 1 case with cyberattacks on three thermal units, 400 MW each, so 1200 MW in total. All three units have been scheduled to operate with the baseline scenarios, while the cyberattack was set to take place in the first hour of day, not enabling those units to operate for the whole examined day. A comparison among the first and second set of scenarios enables the provision of price signals on the cost of cyberattacks, as well as a comparison among the different UC models, incorporating a different level of robustness for tackling the stochastic and uncertain nature of the renewables.

Thirdly, another set of scenarios was examined using the RUC model, which is a robust model enabling the provision of price signals in cases where the transmission system operator (TSO) adopts a more conservative approach toon tackling uncertainties in the power system. This set of scenarios, Cyberattacks 1–4, examines different cases of cyberattacks. More specifically, the following cyberattack cases where examined: (1) cyberattacks in three thermal units, with 1200 MW total capacity, (2) cyberattacks in six thermal units, with 2400 MW total capacity, (3) cyberattacks in three wind farms, with 1200 MW total capacity, (4) cyberattacks in three thermal units, of 1200 MW, and three wind farms, of 1200 MW, with 2400 MW total capacity. In all cases, the thermal units and wind farms were scheduled to operate in the baseline scenarios. Figure 5 provides the evolution of hourly demand in the examined day, deviating between 4.3 and 7.4 GW.

Therefore, the examined cybersecurity attacks concern a considerable share of the generating capacity that is unable to meet the load. However, the examined system has 10.2 GW installed thermal plants, as well as 6.9 GW of wind farms; therefore, the examined cyberattacks are crucial to the power system stability and operating costs, but there is still spare capacity, with flexible ramping capability to meet such events. However, considering that the cyberattacks take place on dispatched thermal and RES plants, those attacks lead to increased operating costs, due to a change in the energy mix, as well as to start-up and shutdown costs for switching off the cyberattacked units and switching on new and more expensive units.

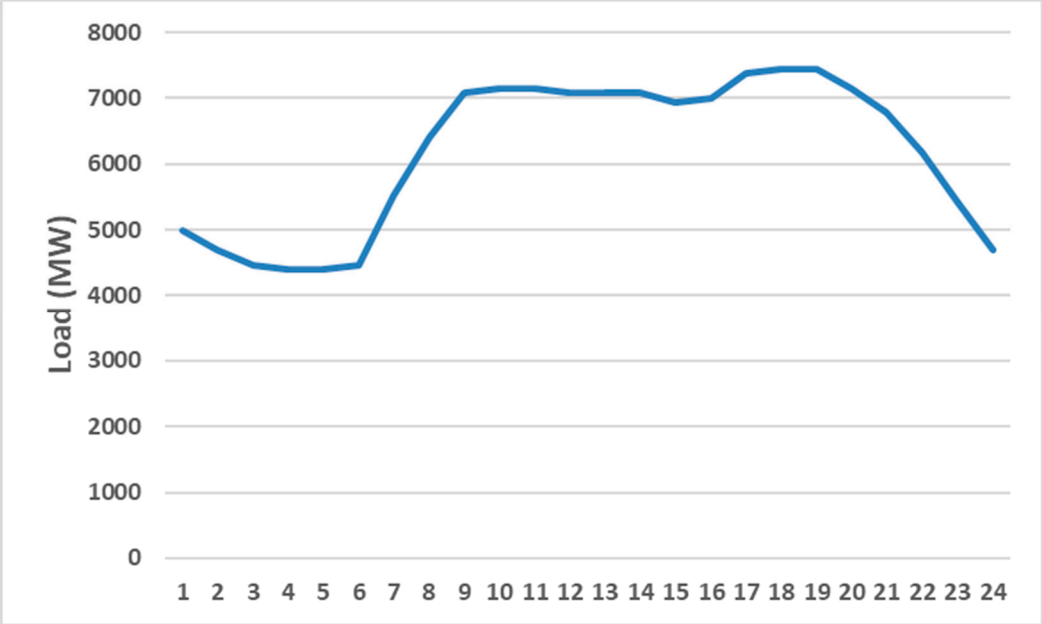


Figure 5. Evolution of hourly demand of the examined typical day.

Table 1 shows the evolution of the overall cost, as optimized in the objective function. The comparison among the different models shows that the incorporation of more technical constraints, as in the robust and stochastic models, compared to the deterministic solution, leads to a considerable increase in the cost. Through the implementation of the cyberattacks—in the case of Cyberattack 1 scenario, with attacks on three thermal units—the cost is further and considerably increased for all scenarios, especially for the stochastic and robust UC models. Results are from the interval UC models, as those models experienced difficulty in finding feasible solutions. The examined scenarios have also led to a considerable increase in the total computational time, especially in the case of the stochastic UC model. This has led the author to increase the convergence gap, which has led to a possible local minimum solution, rather than a global optimum, as can be seen in the increased cost compared to the robust UC model.

Table 1. Objective function cost (in USD) for different scenarios.

	Objective Function Cost
DUC_BAS	1,019,770
SUC_BAS	2,056,180
RUC_BAS	2,056,184
DUC_Cyber1	1,276,210
SUC_Cyber1	2,548,230
RUC_Cyber1	2,423,626
RUC_Cyber2	2,952,878
RUC_Cyber3	2,207,915
RUC_Cyber4	2,548,225

We further focused on the RUC model, examining different cyberattacks' scenarios. Table 1 shows that cyberattacks on thermal plants lead to considerably higher costs compared to attacks on wind plants. This is attributed to the fact that the attacked thermal plants were set to operate at their nominal capacity, due to their comparable cost, constituting base load plants. The enforced switching-off of those units, with a high capacity factor compared to renewables, led to the need for dispatching further units, as well as increasing the operation of more expensive units. Dispatching of units does not take place only for generating purposes, but also for providing the requested ancillary services for the

system stability. Especially in more robust UC models, such constraints lead to higher costs, as shown in Table 1, where Cyberattack 1, in the case of the deterministic model, is considerably less costly compared to the robust and stochastic UC models. Table 2 shows that different cyberattacks affect the dispatched units, leading to a different number of units that operate each hour. The importance of thermal plants is depicted in Figure 6, which shows the limited power generation from wind plants, which can justify the limited effect on the operational cost, compared to the thermal plants. However, in the case of different renewables generating profile, i.e., with photovoltaics that operate at peak hours with a high capacity factor and create a sunset effect, cyberattacks on their inverters could lead to considerable ramping needs.

Table 2. Number of thermal units dispatched for different scenarios using the RUC model.

	Units Committed				
	RUC_BAS	RUC_Cyber1	RUC_Cyber2	RUC_Cyber3	RUC_Cyber4
1	30	27	26	31	29
2	11	12	17	16	16
3	9	10	17	13	15
4	7	12	15	8	13
5	7	15	16	10	14
6	14	20	23	15	20
7	31	32	41	32	36
8	35	44	45	41	42
9	42	46	46	42	47
10	43	46	53	43	47
11	43	48	58	45	48
12	43	46	51	43	47
13	43	46	53	43	46
14	43	46	56	43	46
15	43	46	52	43	46
16	43	46	53	43	46
17	44	46	56	46	47
18	45	50	56	46	47
19	47	56	64	46	49
20	45	46	51	46	47
21	34	44	45	38	44
22	25	28	36	26	30
23	11	17	21	21	23
24	7	7	12	9	13

Therefore, cyberattacks on thermal units affect both start-up and shutdown costs, as well as generating and ancillary services costs. However, we cannot provide a generic conclusion that cyberattacks always have a higher impact on total operating costs, as renewables have a low operating cost, and therefore the decommissioning of those units might lead to a more expensive energy mix. However, the examined cases quantitate a higher impact on attacks on thermal units. Moreover, the examined cases using the RUC model show that they also affect the energy mix,—not only the dispatching of thermal plants but also the curtailment of wind plants. This is depicted indirectly in Table 3, which shows that the energy mix is changed as the curtailment of wind production changes. This can also be seen in Figure 7, which shows small but evident changes in the energy mix. However, those changes also depend on the topology of the network, the nodes of the cyberattacked units, their operating condition, and the interconnections among different nodes. Therefore, the operating cost, unit dispatching, and energy mix evolution show a non-linear trend on the effect of different scenarios. A clear outcome from the analysis is that each TSO should examine different combinations of cyberattacks with different operating conditions to identify cases that are more crucial for the system stability and the overall power system cost operation. The examined attacks show an increased cost for the power system operation and reveal the importance of base load plants. However, in the case of

power system operation in marginal conditions, namely with limited available capacity, the importance of flexible units with high ramping capacity might be more important.

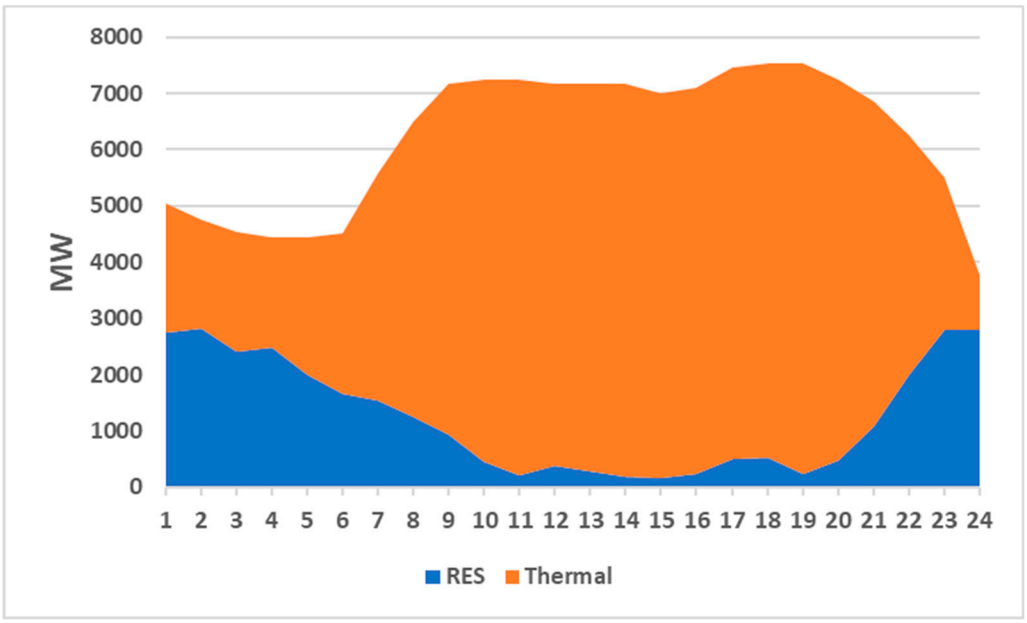
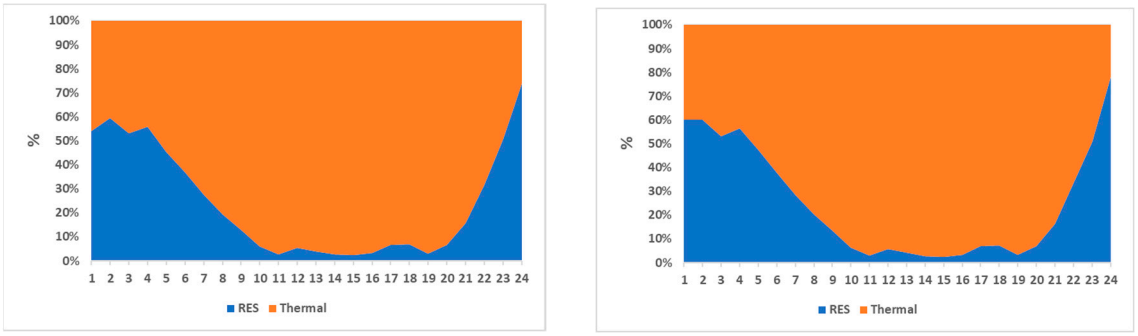


Figure 6. Evolution of hourly energy mix of the examined typical day for the RUC_BAS scenario.

Table 3. Energy mix for different scenarios with the RUC model.

	RUC_BAS	RUC_Cyber1	RUC_Cyber2	RUC_Cyber3	RUC_Cyber4
RES	20.20%	21.29%	20.63%	19.52%	19.83%
Thermal	79.80%	78.71%	79.37%	80.48%	80.17%
Total	100.00%	100.00%	100.00%	100.00%	100.00%



(**a**) (**b**)

Figure 7. *Cont.*

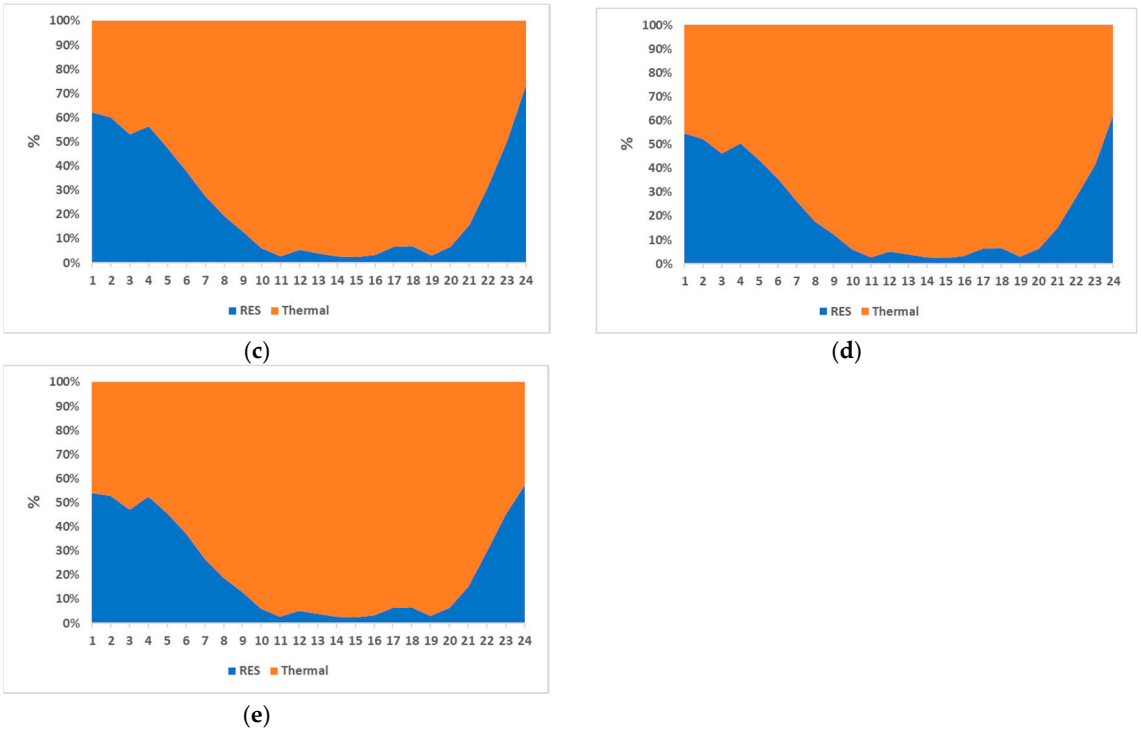


Figure 7. Evolution of hourly energy mix (in %) of the examined typical day for the (**a**) RUC_BAS, (**b**) RUC_Cyber1, (**c**) RUC_Cyber2, (**d**) RUC_Cyber3, and (**e**) RUC_Cyber4 scenarios.

5. Conclusions

This paper aims at assessing the impact of cybersecurity attacks on power systems. It uses different mixed-integer linear programming unit commitment models, which apply different methodologies to incorporate high levels of renewable energy production. The UC models, applying different methods to integrate the uncertainty from the renewables, are further extended to integrate cybersecurity threats, aiming to compare the UC models but also the effect of cybersecurity threats on different power capacity mixes and reliability uncertainty. Our focus is on the effects on the production side, hence the total operational cost, the average energy cost, the dispatch of power units, as well as the power grid adequacy to handle the cybersecurity threats. The selected power system is IEEE RTS 96.

The examined scenarios focus on providing a comparison of the different UC models and the different cybersecurity attacks. The comparison between the UC models confirmed our theoretical assumptions that more robust UC models mean higher total operating costs, due to the more conservative approach to tackle uncertain renewable electricity generation and the consideration of ancillary services. The examined cyberattacks take place on dispatched thermal and RES plants, leading to increased operating costs. This is attributed to the commissioning of more expensive units as well as the increased start-up and shutdown costs, due to the switching on new and more expensive units and the switching off the cyberattacked units. Moreover, the scenarios lead to an increase in the total computational time for finding the optimum solution. The results show that cyberattacks on thermal units affect both start-up and shutdown costs, as well as generating and ancillary services costs, leading to a higher impact compared to attacks on wind plants. However, the paper cannot provide a generic conclusion that cyberattacks on thermal plants always have a higher impact on total operating costs, as renewables have a low operating cost, and therefore the decommissioning of those units might lead to a more expensive energy mix.

The effects depend on the topology of the network, the nodes of the cyberattacked units, their operating condition, the interconnections among different nodes, and the ramping capacity of the available units. The cost, unit dispatching, and energy mix evolution have a non-linear trend that depends on the power system characteristics. The examined cases lead to considerable price signals on the potential effects of cyberattacks. However, each TSO should examine different combinations of

cyberattacks in different operating conditions to identify cases that are more crucial for the system stability and the overall power system operational costs. The approach implemented is useful for assessing cyberattacks at a system level. However, unit commitment modeling cannot quantify threats at the distributed level, unless considerable model developments are made and/or more detailed approaches are elaborated. This creates challenges for further research at the distribution level, which could be scaled up to be integrated at system level.

Funding: This work has been supported by the Horizon 2020 research project INTERFACE: TSO-DSO-Consumer INTERFACE architecture to provide innovative grid services for an efficient power system (Project Grant Agreement No. 824330).

Conflicts of Interest: The author declares no conflict of interest.

Nomenclature

A. Sets	
B	Index of generating unit cost curve segments, 1-B
I	Index of generating units, 1-I
J	Index of generating unit start-up cost, 1-J
L	Index of transmission lines, 1-L
S	Index of bus bars, 1-S
T	Index of hours, 1-T
B. Parameters	
a_i	Fixed production cost of unit i (\$)
B_{sm}	Admittance of transmission line between nodes s and m (S)
$d_s(t)$	Load demand at bus s (MW)
g_i^{down}	Minimum downtime of unit i (h)
g_i^{up}	Minimum up time of unit i (h)
$g_i^{down,init}$	Time that unit i has been down before t = 0 (h)
$g_i^{up,init}$	Time that unit i has been up before t = 0 (h)
g_i^0	Output of unit i at t = 0 (MW)
g_i^{max}	Rated capacity of unit i (MW)
g_i^{min}	Minimum output of unit i (MW)
$g_{i,b}^{max}$	Capacity of segment b of the cost curve of unit i (MW)
g_i^{on-off}	Onoff status of unit i at $t = 0$, equal to 1 if $g_i^{up,init} > 0$, otherwise 0
$k_{i,b}$	Slope of the segment b of the cost curve of unit i (\$/MW)
l_{sm}^{max}	Capacity of the transmission line between nodes s and m (MW)
$L_i^{down,min}$	Length of time that unit i has to be off at the start of the planning horizon (h)
$L_i^{up,min}$	Length of time that unit i has to be on at the start of the planning horizon (h)
M	Large number used for linearization
$ramp_i^{down}$	Ramp-down limit of unit i (MW/h)
$ramp_i^{up}$	Ramp-up limit of unit i (MW/h)
$suc_{i,j}^{cost}$	Cost steps in start-up cost curve of unit i (\$)
$suc_{i,j}^{lim}$	Time steps in start-up cost curve of unit i (h)
C. Variables	
$C_i(t)$	Operating cost of unit i at time t (\$)
$count_i^{down}$	Unit i downtime period counter
$g_i(t)$	Output power of unit i at time t (MW)
$g_{i,b}(t)$	Output power of unit i on segment b at time t (MW)
$suc_i(t)$	Start-up cost of unit i at time t (\$)
$w_{i,j}(t)$	Binary variable equal to 1 if unit i is started at time t after being out for j hours, otherwise 0
$x_i(t)$	Binary variable equal to 1 if unit i is producing at time t, otherwise 0
$y_i(t)$	Binary variable equal to 1 if unit i is started at the beginning of time t, otherwise 0
$z_i(t)$	Binary variable equal to 1 if unit i is shutdown at the beginning of time t, otherwise 0
$\theta_s(t)$	Voltage angle at bus s (rad)

Appendix A. Basic Formulation of the REAL UC Models

Formulation

The aim is to minimize the total generation cost of the thermal power plants, which is described in the following objective function [33]:

$$\sum_{t=1}^{T}\sum_{i=1}^{I} C_i(t). \tag{A1}$$

Equations (A2) and (A3) describe the binary logic. Specifically, Equation (A3) prohibits a unit starting up from being simultaneously shut down. Equation (A2) implements the logic that if a unit is starting up at time t, it cannot be on at time t - 1.

$$y_i(t) - z_i(t) = x_i(t) - x_i(t-1), \quad \forall\, 1 \le t \le T,\ i \le I \tag{A2}$$

$$y_i(t) + z_i(t) \le 1, \quad \forall\, t \le T,\ i \le I \tag{A3}$$

Equation (A4) defines the total cost for each unit i. The total cost is the summation of the startup cost of the units (if needed), the fixed cost, and the variable cost:

$$C_i(t) = \alpha \cdot x_i(t) + \sum_{b=1}^{B} k_b \cdot g_{i,b}(t) + suc_i(t), \quad \forall\, t \le T,\ i \le I. \tag{A4}$$

The total unit output is equal to the sum of the generation in each segment of the cost curve:

$$g_i(t) = \sum_{b=1}^{B} g_{i,b}(t), \quad \forall\, t \le T,\ i \le I \tag{A5}$$

Minimum unit output must be higher than the minimum output of unit i:

$$g_i(t) \ge g_i^{min} \cdot x_i(t), \quad \forall\, t \le T,\ i \le I. \tag{A6}$$

Unit output for each generation level:

$$g_{i,b}(t) \le g_{i,b}^{max} \cdot x_i(t), \quad \forall\, t \le T,\ i \le I,\ b \le B. \tag{A7}$$

Minimum up time constraints:

$$\sum_{t=1}^{L_i^{up,min}} (1 - x_i(t)) = 0, \quad \forall\, i \le I \tag{A8}$$

$$\sum_{tt=t}^{t+g_i^{up}-1} x_i(tt) \ge g_i^{up} \cdot y_i(t) \quad \forall\, L_i^{up,min} + 1 \le t \le T - g_i^{up} + 1, \quad i \le I \tag{A9}$$

$$\sum_{tt=t}^{T} (x_i(tt) - y_i(t)) \ge 0 \quad \forall\, T - g_i^{up} + 2 \le t \le T,\ i \le I, \tag{A10}$$

where $L_i^{up,min} = max\left\{0,\ min\left\{T, \left(g_i^{up} - g_i^{up,init}\right) \cdot g_i^{on-off}\right\}\right\}$

Minimum downtime constraints:

$$\sum_{t=1}^{L_i^{down,min}} x_i(t) = 0\,, \quad \forall\, i \le I \tag{A11}$$

$$\sum_{tt=t}^{t+g_i^{down}-1} (1 - x_i(tt)) \ge g_i^{down} \cdot z_i(t) \quad \forall\, L_i^{down,min} + 1 \le t \le T - g_i^{down} + 1, \quad i \le I \tag{A12}$$

$$\sum_{tt=t}^{T} (1 - x_i(tt) - z_i(t)) \ge 0 \quad \forall\, T - g_i^{down} + 2 \le t \le T, \quad i \le I, \tag{A13}$$

where $L_i^{down,min} = max\left\{0,\ min\left\{T, \left(g_i^{down} - g_i^{down,init}\right) \cdot \left(1 - g_i^{on-off}\right)\right\}\right\}$

Ramp-up and ramp-down constraints:

$$-\,ramp_i^{down} \le g_i(t) - g_i(t-1)\ , \quad \forall\, 2 \le t \le T,\ i \le I \tag{A14}$$

$$ramp_i^{up} \geq g_i(t) - g_i(t-1) \ , \ \forall\, 2 \leq t \leq T,\ i \leq I \tag{A15}$$

$$-ramp_i^{down} \leq g_i(t_1) - g_i^0, \ \forall\, i \leq I \tag{A16}$$

$$ramp_i^{up} \geq g_i(t_1) - g_i^0, \ \forall\, i \leq I. \tag{A17}$$

Equations (A18)–(A20) impose the constraints and calculate the startup cost of each unit i. Specifically, Equation (A18) sets the limitations for the calculation of the value of variable $w_{ij}(t)$, taking into account the initial conditions.

$$\begin{array}{l} w_{i,j}(t) \leq \sum_{tt=suc_{i,j}^{lim}}^{min\{t-1, suc_{i,j+1}^{lim}-1\}} z_i(t-j) + 1\ IF\left\{j \leq J-1 \bigwedge suc_{i,j}^{lim} \leq g_i^{down,init} + t - \right. \\ \left. 1 < suc_{i,j+1}^{lim}\right\} + 1\ IF\left\{j = J \bigwedge suc_{i,j}^{lim} \leq g_i^{down,init} + t - 1\right\}, \ \forall\, t \leq T,\ i \leq I,\ j \leq J \end{array} \tag{A18}$$

$$\sum_{j=1}^{J} w_{i,j}(t) = y_i(t), \ \forall\, t \leq T,\ i \leq I \tag{A19}$$

$$suc_i(t) = \sum_{j=1}^{J} suc_{i,j}^{cost} \cdot w_{i,j}(t), \quad \forall\, t \leq T,\ i \leq I, \tag{A20}$$

where symbol IF represents logical IF and symbol $\bigwedge$ symbolizes logical AND.

Equations (A21)–(A24) provide the transmission constraints of the power system. Equation (A21) defines the power balance in the electrical system. Equation (A22) provides the line flow limits. Equation (A23) provides the limits of the voltage angles, while Equation (A24) sets the voltage angle to zero at the reference bus.

$$\sum_{i=1}^{I} g_i(t) - \sum_{\{s,m\} \in L | m \rangle s} B_{sm} \cdot (\theta_s(t) - \theta_m(t)) - \sum_{\{s,m\} \in L | m < s} B_{sm} \cdot (\theta_m(t) - \theta_s(t)) \ \forall\, t \leq T, \ s \leq S \tag{A21}$$

$$-l_{sm}^{max} \leq B_{sm} \cdot (\theta_s(t) - \theta_m(t)) \leq l_{sm}^{max}, \ \forall t \leq T,\ \{s,m\} \in L \tag{A22}$$

$$-\pi \leq \theta_s(t) \leq \pi, \ \forall t \leq T,\ s \leq S \tag{A23}$$

$$\theta_s(t) = 0, \ \forall t \leq T \tag{A24}$$

Appendix B. Input Data for the IEEE-RTS96 System

All five models use the same Excel file as a data input file. That file includes all the tables needed for the calculations. GAMS read the input data through a small program, which provides the users with options to change some parameters before running the unit commitment model. In the following paragraph, we present briefly the options available and the data loaded from the Data input code (Renewable Energy Analysis Lab Library, 2017).

The following tables show the form of the input data as they are inserted into the model.

Thermal unit data:

Table A1. Units map gen_map(*i*,*s*): includes the position of each unit in the power system.

	s101	**s102**	**s103**	**s104**	**s105**
i1	1	0	0	0	0
i2	1	0	0	0	0
i3	1	0	0	0	0

Table A2. The capacity of segment *b* of the cost curve of unit *i* (MW): g_max(*i*,*b*).

Output Block (MW):			
	b1	b2	b3
i1	6.666667	6.666667	6.666667
i2	6.666667	6.666667	6.666667
i3	25.33333	25.33333	25.33333

Table A3. The slope of segment *b* of the cost curve for unit *i* ($/MW): k(*i*,*b*).

Cost ($/MW):	
	tr4
b1	28.967
b2	29.243
b3	29.703
b1	28.957
b2	29.233
b3	29.693

Table A4. Cost steps in start-up cost curve of unit *i* ($) suc_sw(*i*,*j*).

Start-up Cost ($):	
	tr4
j1	25
j2	28
j3	31
j4	34
j5	37
j6	40
j7	43
j8	46
j1	25
j2	28
j3	31
j4	34
j5	37
j6	40
j7	43
j8	46

Table A5. Time steps on start-up cost curve of unit *i* (h) suc_sl(*i*,*j*).

Start-up Blocks (h):								
	j1	j2	j3	j4	j5	j6	j7	j8
i1	1	2	3	4	5	6	7	8
i2	1	2	3	4	5	6	7	8
i3	1	2	3	4	5	6	7	8

Table A6. Time periods that unit *i* has been down before *t* = 0 (h): count_off_init(*i*).

Count "off" Init (h)
column1
0
0
0
1
17
4

Table A7. Time that unit *i* has been up before *t* = 0 (h): count_on_init(*i*).

Count "on" Init (h)	
	column1
i1	1
i2	400
i3	220
i4	0

Table A8. Fixed production cost for unit *i* ($): a(*i*)

No Load Cost ($)	
	tr4
i1	454.572
i2	454.562
i3	263.419

Table A9. Ramp-up limit of unit *i* (MW/h): ramp_up(*i*).

Ramp-Up Limit (MW/h)	
	tr4
i1	30.5
i2	30.5
i3	38.5

Table A10. Ramp-down limit of unit *i* (MW/h): ramp_down(*i*).

Ramp-Down Limit (MW/h)	
	tr4
i1	70
i2	70
i3	80

Table A11. Minimum time unit *i* has to be shut down (h): g_down(*i*).

Min. Down Time (h)	
	tr4
i1	1
i2	1
i3	2

Table A12. Minimum time unit *i* has to be up (h): g_up(*i*).

Min. Up Time (h)	
	tr4
i1	1
i2	1
i3	3

Table A13. Minimum output capacity of unit *i* (MW): g_min(*i*).

Min. Output (MW)	
	tr4
i1	4.0
i2	4.0
i3	15.2

Table A14. Output power of unit *i* at *t* = 0 (MW): g_0(*i*).

Output at *t* = 0 (MW)	
	column1
i1	20
i2	20
i3	70
i4	0
i5	0

Transmission line data

Table A15. Admittance of transmission line between nodes *s* and *m* (S): admittance(*l*).

1/X	
	column1
l1	7142.8570
l2	473.9336
l3	1176.4710

Table A16. Line map, line_map(*l*,*s*).

	s101	**s102**	**s103**	**s104**	**s105**
l1	1	−1	0	0	0
l2	1	0	−1	0	0
l3	1	0	0	0	−1
l4	0	1	0	−1	0

Table A17. Capacity of transmission line between nodes s and m (MW): l_max(*l*).

Capacity	
l1	175
l2	175
l3	175
l4	175

Demand load data

Table A18. Demand load on bus s (MW): d(*t*,*s*).

	s101	**s102**	**s103**	**s104**
t1	63.98618	57.25079	106.0823	43.78002
t2	60.16611	53.83283	99.74907	41.16628
t3	57.30105	51.26936	94.99911	39.20598

Wind plants data

Table A19. Wind plants map w_map(*w*,*s*).

	s116	**s117**	**s118**	**s119**
w3	1			
w4		1		
w5			1	
w6				1
w7				

Table A20. Capacity of wind plants (MW): w_capacity(w).

	Capacity
w1	300
w2	300
w3	600
w4	600

Table A21. Probabilities for each of the wind scenarios: prob(scen).

	Capacity
scen1	0.020000
scen2	0.160000
scen3	0.107273
scen4	0.241818
scen5	0.107273
scen6	0.150000
scen7	0.086364
scen8	0.000909
scen9	0.125455
scen10	0.000909

Earlier we mentioned that we have the option to select between a favorable and an unfavorable wind profile. The input data program selects the appropriate table each time according to our selection. The procedure is the same for both wind patterns.

Table A22. w_det_pu_1(t,w): includes the available wind power for each unit i calculated in per unit values.

Favorable						
			Deterministic			
Capacity	300	300	600	600	300	600
	w1	w2	w3	w4	w5	w6
t1	0.086380	0.211012	0.153027	0.154525	0.026973	0.485740
t2	0.043697	0.139327	0.139853	0.131191	0.076886	0.431102
t3	0.089033	0.151854	0.154940	0.179127	0.095984	0.370302
t4	0.304660	0.299134	0.273481	0.249978	0.064053	0.176555
t5	0.396127	0.299414	0.343453	0.178707	0.025651	0.066776

Table A23. Lower and upper bound of wind production: wind_robust_pu_1(t,w,robust) per unit values.

		UP	**DOWN**
		col1	col2
t1	w1	0.236872	0.000000
t1	w2	0.337008	0.109605
t1	w3	0.278299	0.042769
t1	w4	0.271115	0.030279
t1	w5	0.084981	0.000000
t1	w6	0.749222	0.254945

Table A24. Stochastic ramp-up and ramp-down rates of wind production: w_stoch_max_1(*t*,*w*,robust).

STOCHASTIC RAMPS		
	UP	DOWN
	col1	col2
w1	0.000000	−0.089880
w2	−0.012230	−0.065270
w3	0.121853	−0.117670
w4	0.001779	−0.104180
w5	0.131416	0.003539
w6	−0.032410	−0.312890
w7	0.010194	−0.025100
w8	0.033926	0.000792

Table A25. Probability for each scenario for each wind unit: wind_scenarios_1(*t*,*w*,scen).

		scen1	scen2	scen3	scen4	scen5	scen6	scen7
t1	w1	0.100862	0.072062	0.099023	0.080163	0.132368	0.061889	0.127721
t1	w2	0.181467	0.220213	0.187513	0.240498	0.191013	0.170966	0.213342
t1	w3	0.158785	0.121393	0.160644	0.144837	0.201459	0.128830	0.161325
t1	w4	0.169363	0.133267	0.176270	0.116373	0.163892	0.071113	0.171963
t1	w5	0.021053	0.000000	0.027147	0.000000	0.010517	0.000000	0.013856
t1	w6	0.488406	0.502584	0.442172	0.504939	0.484160	0.547880	0.481501
t1	w7	0.546199	0.593101	0.516420	0.615420	0.505618	0.549848	0.505922

References

1. SGTF EG2. Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity, Second Interim Report, Smart Grid Task Force Expert Group. 2018. Available online: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf (accessed on 29 January 2019).
2. EECSP. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP Expert Group. 2017. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (accessed on 29 January 2019).
3. European Commission. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Report. 2013. Available online: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed on 29 January 2019).
4. INL. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*; Idaho National laboratory: Idaho Falls, ID, USA, 2016.
5. ENISA. Smart Grid Threat Landscape and Good Practice Guide. 2013. Available online: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide (accessed on 29 January 2019).
6. ANL-GSS 15/4. Analysis of Critical Infrastructure Dependencies and Interdependencies, Argonne-Risk and Infrastructure Science Center, Argone National Lanoratory. 2015. Available online: http://www.ipd.anl.gov/anlpubs/2015/06/111906.pdf (accessed on 29 January 2019).
7. National Institute of Standards and Technology. Guidelines for Smart Grid Cybersecurity—Smart Grid Cybersecurity Strategy—Architecture and High-Level Requirements, Volume 1. 2014. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (accessed on 29 January 2019).
8. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 45–56. [CrossRef]
9. Mrabet, Z.E.; Kaabouch, N.; Ghazi, H.E.; Ghazi, H.E. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [CrossRef]
10. Jarmakiewicz, J.; Maślanka, K.; Parobczak, K. Development of Cyber Security Testbed for Critical Infrastructure. In Proceedings of the 2015 International Conference on Military Communications and Information Systems, Cracow, Poland, 18–19 May 2015.

11. Shi, L.; Dai, Q.; Ni, Y. Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electr. Power Syst. Res.* **2018**, *163*, 396–412. [CrossRef]
12. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. [CrossRef]
13. Hammad, E.; Ezeme, M.; Farraj, A. Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. *Int. J. Electr. Power Energy Syst.* **2019**, *104*, 817–826. [CrossRef]
14. Liu, W.; Gong, Q.; Han, H.; Wang, Z.; Wang, L. Reliability Modeling and Evaluation of Active Cyber Physical Distribution System. *IEEE Trans. Power Syst.* **2018**, *33*, 7096–7108. [CrossRef]
15. Park, J.K.; Suh, Y.S.; Park, C. Implementation of cyber security for safety systems of nuclear facilities. *Prog. Nucl. Energy* **2016**, *88*, 88–94. [CrossRef]
16. Gunduz, H.; Jayaweera, D. Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems. *Int. J. Electr. Power Energy Syst.* **2018**, *101*, 371–384. [CrossRef]
17. Sundararajan, A.; Chavan, A.; Saleem, D.; Sarwat, A.I. A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security. *Energies* **2018**, *11*, 2360. [CrossRef]
18. Tellbach, D.; Li, Y.F. Cyber-Attacks on Smart Meters in Household Nanogrid: Modeling, Simulation and Analysis. *Energies* **2018**, *11*, 316. [CrossRef]
19. Ye, X.; Zhao, J.; Zhang, Y.; Wen, F. Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems. *Energies* **2015**, *8*, 5266–5286. [CrossRef]
20. Venkatachary, S.K.; Prasad, J.; Samikannu, R. Economic Impacts of Cyber Security in Energy Sector: A Review. *Int. J. Energy Econ. Policy* **2017**, *7*, 250–262.
21. Liu, X.; Li, Z.; Shuai, Z.; Wen, Y. Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution. *IEEE Trans. Smart Grid* **2017**, *8*, 1023–1025. [CrossRef]
22. Liu, R.; Vellaithurai, C.; Biswas, S.S.; Gamage, T.T.; Srivastava, A.K. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2444–2453. [CrossRef]
23. Poudineh, R.; Jamasb, T. Electricity Supply Interruptions: Sectoral Interdependencies and the Cost of Energy Not Served for the Scottish Economy. *Energy J.* **2017**, *38*, 51–76. [CrossRef]
24. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. *Comput. Secur.* **2018**, *77*, 262–276. [CrossRef]
25. Mackiewicz, R.; Heights, S. Technical Overview and Benefits of the IEC 61850 Standard for Substation Automation. In Proceedings of the 2006 IEEE PES Power Systems Conference and Exposition (PSCE), Atlanta, GA, USA, 29 October–1 November 2006.
26. Jarmakiewicz, J.; Parobczak, K.; Maślanka, K. Cybersecurity protection for power grid control infrastructures. *Int. J. Crit. Infrastruct. Prot.* **2017**, *18*, 20–33. [CrossRef]
27. de Gusmão, A.P.H.; Silva, M.M.; Poleto, T.; Silva, L.C.; Costa, A.P.C.S. Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *Int. J. Inf. Manag.* **2018**, *43*, 248–260. [CrossRef]
28. Zarreh, A.; Saygin, C.; Wan, H.D.; Lee, Y.; Bracho, A. A game theory based cybersecurity assessment model for advanced manufacturing systems. *Procedia Manuf.* **2018**, *26*, 1255–1264. [CrossRef]
29. Dagoumas, A.; Polemis, M. An integrated model for assessing electricity retailer's profitability with demand response. *Appl. Energy* **2017**, *198*, 49–64. [CrossRef]
30. Dagoumas, A.; Koltsaklis, N.; Panapakidis, I. An integrated model for risk management in electricity trade. *Energy* **2017**, *124*, 350–363. [CrossRef]
31. Koltsaklis, N.; Dagoumas, A.; Panapakidis, I. Impact of the penetration of renewables on flexibility need. *Energy Policy* **2017**, *109*, 360–369. [CrossRef]
32. Renewable Energy Analysis Lab—Library. 2017. Available online: http://www2.ee.washington.edu/research/real/index.html (accessed on 29 January 2019).
33. Pandzic, H.; Dvorkin, Y.; Qiu, T.; Wang, Y.; Kirschen, D. *Unit Commitment under Uncertainty—GAMS Models*; Library of the Renewable Energy Analysis Lab (REAL), University of Washington: Seattle, WA, USA, 2017; Available online: http://www.ee.washington.edu/research/real/gams_code.html (accessed on 29 January 2019).
34. Dvorkin, Y.; Pandžić, H.; Ortega-Vazquez, M.A.; Kirschen, D.S. A Hybrid Stochastic/Interval Approach to Transmission-Constrained Unit Commitment. *IEEE Trans. Power Syst.* **2015**, *30*, 621–631. [CrossRef]
35. Bertsimas, D.; Litvinov, E.; Sun, X.A.; Zhao, J.; Zheng, T. Adaptive Robust Optimization for the Security Constrained Unit Commitment Problem. *IEEE Trans. Power Syst.* **2013**, *28*, 52–63. [CrossRef]

36. Kirschen, D. Variants of Stochastic Unit Commitment. 2014. Available online: http://gridoptics.org/fpgws14/files/workshop/Kirschen-SCUCVariantsSoftwareSession_GOWS_FY14.pdf (accessed on 29 January 2019).
37. CIGRÉ. *Security for Information Systems and Intranets in Electric Power Systems*; CIGRÉ joint working group JWG D2/B3/C2.01; CIGRÉ: Paris, France, 2007.
38. CIGRÉ. *Treatment of Information Security for Electric Power Systems*; CIGRÉ joint working group JWG D2.22; CIGRÉ: Paris, France, 2010.
39. Roche, P. *Cyber Security Considerations in Power System Operations*; CIGRÉ: Paris, France, 2005.