energies

MDPI

Article

A Case Study of an Industrial Power Plant under Cyberattack: Simulation and Analysis

Marilena Stănculescu [1,*], Sorin Deleanu [2], Paul Cristian Andrei [1] and Horia Andrei [3]

[1] Department of Electrical Engineering, University Politehnica of Bucharest, 060042 Bucharest, Romania; paul.andrei@upb.ro
[2] School of Applied Sciences and Technology, Northern Alberta Institute of Technology, Edmonton, AB T5G2R1, Canada; sorind@nait.ca
[3] Doctoral School of Engineering Sciences, University Valahia Targoviste, 130004 Targoviste, Romania; hr_andrei@yahoo.com
* Correspondence: marilena.stanculescu@upb.ro

Abstract: For critical infrastructures, technological developments regarding real-time data transmission and processing improve the system's operability and reliability. However, vulnerabilities are introduced in the case of implementing new remote access methods or where redundancy is low. At the national level, most critical infrastructures are connected, and, therefore, achieving a level of security and resilience is based on identifying a multitude of risks. In this respect, the reduction of risk to acceptable levels directly affects the quality of citizens' lives and decreases losses in the industry. This study starts from the threats to power systems, namely cyberattacks, which are much more dangerous, although less visible, to operators, and almost invisible to the public or the media. From this point of view, it was proved that the most vulnerable parts of the power system were human–machine interfaces, electrical equipment, Surveillance, Control, and Data Acquisition (SCADA) systems. This paper's main achievements include the simulation of cyberattacks on existing electrical equipment from a petrochemical plant (case study), which consists of modifying the remote data transmitted by the SCADA system. Two locations were submitted to simulated cyberattacks that were considered critical for the overall plant operation. Furthermore, the changes that occur following each fault resulting from the cyberattack and the influence of the electrical parameter changes upon the process flow were analyzed. Furthermore, by using Electrical Power System Analysis Software—ETAP—the changes that occur following each fault due to the cyberattack and the influence of the electrical parameter changes upon the process flow were analyzed. By considering the two malfunction events, the resilience assessment of the system was analyzed. In the second case, only partial resilience action, up to 40%, restored the operability of the industrial power plant.

Keywords: electro energetic system; critical infrastructure; SCADA; electric parameter; power transformer; simulation and analysis of cyber attack

Citation: Stănculescu, M.; Deleanu, S.; Andrei, P.C.; Andrei, H. A Case Study of an Industrial Power Plant under Cyberattack: Simulation and Analysis. *Energies* **2021**, *14*, 2568. https://doi.org/10.3390/en14092568

Academic Editor: Igor Kotenko

Received: 5 April 2021
Accepted: 27 April 2021
Published: 29 April 2021

1. Introduction

The technological evolution recorded in the transmission and online processing of the parameters of power systems over the last ten years has determined significant improvements in power systems' operability, control, and reliability.

Concurrently, vulnerabilities arise due to both new methods of remote access and reduced redundancy. For this reason, almost all the hardware and software components of a power system are potentially critical infrastructures, exposed to physical or informatics events naturally occurring or intentionally provoked. Critical infrastructure includes the energy system (electricity, oil, or gas), the transportation system, the water supply, and energy distribution.

Most national power systems are interconnected. The classical definition of power systems as power infrastructure networks has lost its validity, because nowadays, there is a significant presence of cyber components within the newer and much more complex configurations of power systems. There is a strong presence of cyber elements in all domains of power systems: generation, transformation, transmission, distribution, consumption. The concept of cyber-physical power systems has recently gained steam due to the continuous link and interaction between power equipment and cyber components at several levels and involving different information content. In recent years, there has been an increasing concern related to the protection of the critical infrastructures due the constant threat represented by cyberattacks. Consequently, relevant industries are adopting implementation measures and procedures to ensure their safety. For example, in [1], a security measure is presented based on the classification of past attack incidents against control systems and a big data analysis technique that processes the data generated from individual pieces of security equipment. One can conclude that there is integration between the power and cyber systems, in which the digital communications between the remote-control centers and power systems can satisfy the demand for protection, monitoring, and control [2–4]. Therefore, achieving the security and resilience of these interdependent critical structures requires the identification of a multitude of risks and their reduction to an acceptable level in order to minimally impact citizens' quality of life [5–7]. As presented in [8], security means physical security, i.e., the security of the power system against calamities or natural disasters and physical attacks carried out by individuals or organizations to destroy its key points and disrupt the system, as well as cybernetic security. Cybernetic security refers to protecting the power system against the threats of theft/destruction/manipulation of data or databases built on customer information or the handling of sensors and equipment for interruption of activity. A comprehensive study of how big data and machine learning can be introduced in electrical power grids and security concerns and their solutions is presented in [9]. Although different, the two areas (physical security and cyber security) are interconnected, with complex vulnerabilities. A possible attack aimed at the power system's malfunction is carried out on both planes simultaneously [10]. There are two types of relationships between the physical and the cyber structures composing the cyber-physical power system: direct and indirect interaction [11]. For the last kind of interaction, the failures recorded at the cyber structure level would not determine the immediate turning off of the power device, yet but downgrade its performance in the event of a failure or a failure involving an adjacent device.

The effectiveness of a critical infrastructure's resilience depends on the characteristics that define the resilience concept itself: ability to anticipate, absorb, adapt to, and recover quickly from a disruptive event. The protection and resilience of critical infrastructures are complementary and necessary concepts for implementing a comprehensive risk management strategy [12].

From the power system's point of view, it is necessary to measure resilience at both the producer and the distributor. The analysis of power systems with respect to risk management, emergencies, and cross-sectoral interoperability displays positive aspects resulting from the power system's interconnection with other critical infrastructures and reveals the limitations of these interdependencies. To achieve the desired level of security and resilience, interdependent critical infrastructure operators must act as partners in order to collectively identify priorities, namely, in order to achieve common goals, identify risks and reduce them to an acceptable level so that the direct effect on the quality of life of citizens will be minimal [13]. Although less visible to power system operators and almost invisible to the public or the media, cyber threats are much more dangerous. A cyberattack can lead to huge losses, which are economical and can also endanger people's safety by affecting certain aspects of human life. For example, power outages in a hospital may occur during surgery. Attacks on public traffic control systems can cause chaos, and even traffic accidents, at crowded intersections [12].

Therefore, it is necessary to conduct a cyber security analysis of these industrial control systems (ICS) to identify what kind of attacks could occur on an ICS before an unexpected situation arises. The syntagma "malware", used internationally for cyber threats, describes a software program intended to infiltrate a computer system to either damage the system or steal its data.

To deal with cyberattacks, [13] proposes a combined error of current and voltage, and a switching secondary controller is designed. A novel, model-independent, unified detection strategy based on disagreement Laplacian potential for effective identification of cyber anomalies in interconnected autonomous direct current (dc) microgrid (MG) cluster is presented in [14]. Power grid network protection must consider both cyber and physical aspects. In [15], a local cyber-physical power system is established based on the IEEE-9 bus system to quantify its operational dynamic vulnerability.

The Stuxnet malware is considered to be the first cyber weapon to be discovered in 2010 by the Kaspersky antivirus solution (Woburn 01801, MA, USA), [16]. The malware mentioned above has a software architecture, potentially effective against industrial control systems, human–machine interfaces, electrical devices, and SCADA systems, obviously posing a danger to critical infrastructures in the power system.

Numerous cases of successful cyberattacks are publicly available, together with predictions regarding their geopolitical impacts on longer term [17–21].

Cyber security specialists who developing the Kaspersky antivirus solutions applicable in the industry (i.e., power system included) predicted the following consequences: an increase in general and accidental malware infections, enhanced risk of targeted attacks requiring ransom, the practice of industrial cyber-espionage, the appearance of a new branch of crime that focuses on the development of attack services and hacking tools, new types of viruses, cyber criminals that take advantage of analyses of the vulnerabilities of industrial control computer systems published by security providers, the development of regulations on the subject cybersecurity, and industrial insurance [22,23]. A diversified system is more challenging to destabilize globally. On the other hand, a modular system has the advantage of flexibility. In the case of problems at critical points (e.g., large transformers), the replacement of the affected parts comes quickly at lower costs, because the company can afford to maintain a reserve stock without involving high logistical costs due to diversity of parts and manufacturers [24].

Intrusion Detection Systems in an Industrial Control System (ICS) network is currently done manually by security experts. Instead of manual intervention, it is important to update, in real time, the structures of attack graphs, to enable fast isolation of compromised network to secure the grid [25].

Currently, the implementation of SCADA at the level of connection stations containing power transformers aims for continuous surveillance monitoring and control of various equipment, online data acquisition, and processing, as well as performing operations such as:

- voltage control;
- load-balancing;
- overload situations management;
- protection of transformer faults;
- protection against faults on the bus.

The equipment from SCADA control centers receives data, sends commands to the remote equipment, or triggers alarms, if the received data exceeds the predefined safety limits [26–28]. An outside cyber attacker may try a variety of possible ways to enter the data acquisition, processing, and control system, especially looking for data transmission devices that have integrated wireless network antennas and processors (WWAN), looking for a connection to those devices that have been identified with security breaches and have not yet installed the necessary updates. Essentially, a cyber attacker needs to know the system components' architecture and operation to be able to change those parameters that can cause damage [29,30]. One of the most used ways to secure the information transmitted

in real-time by the SCADA is data encryption. The application of a performing encryption method leaves the initial information transparent only to the sender and receiver, presenting the perpetrators with a challenging task while trying to decipher it. The application of algorithms validated, especially by banking transactions, in SCADA provides enough protection by ensuring the confidentiality, integrity, and availability of data against cyberattacks [31,32]. The injection of false data has been demonstrated to be extremely detrimental to the smart power grids, causing economical and physical damages [33,34]. Assuming that, somewhere inside the power system, there could be malware that collects and transmits data as it propagates, waiting for the attack signal or meeting the predefined conditions in the source code to initiate the attack, this paper simulates a transformation station subjected to cyberattack by modifying the data transmitted remotely by the SCADA system. The study considers a petrochemical plant, while the energy parameters affecting the transformation stations at two different locations inside the plant are modified. The article has the following structure: after an overview of power system vulnerabilities, the SCADA system and the transmitted data structure are presented in Section 2. Two applications from Section 3, developed using the ETAP programming environment, simulate cyberattacks on critical power system components such as power transformers. Furthermore, the adverse effects produced by transmitting false values of the transformer's electrical parameters are evaluated. The last section contains the conclusions.

2. Critical Infrastructure of Power Systems and Vulnerability of Data Acquisition Systems

The power system has four subsystems: generation, transmission, distribution, and supply. The power system's various pieces of equipment have public and private owners, and are operated individually for given load conditions while obeying the standards. Such a system evolves towards the Intelligent Power System, whose structure appears in Figure 1. This model, suggested by the National Institute of Standardization and Technologies—NIST, has been adapted to the continuous developments recorded for information and telecommunication technologies, present in all systems and network components [35]. The contemporary evolution of power systems is towards the smart power grid (Smart Grid), based on decentralization and bidirectional exchange of energy and information. This system transition is necessary but challenging to implement because it must happen, whereas the national power system is in use, without interrupting electricity supply and without affecting users. The system conversion from a traditional power system based on a relatively small number of high-power plants to the decentralization and application of Smart Grid solutions improves its resilience. This eliminates the need for those plants which operate only during the daytime to support peak consumption. Such a mechanism requires the decentralization of a part of the generation at the national level to end consumers who have become prosumers (solar and wind sources in conjunction with battery storage) [36].

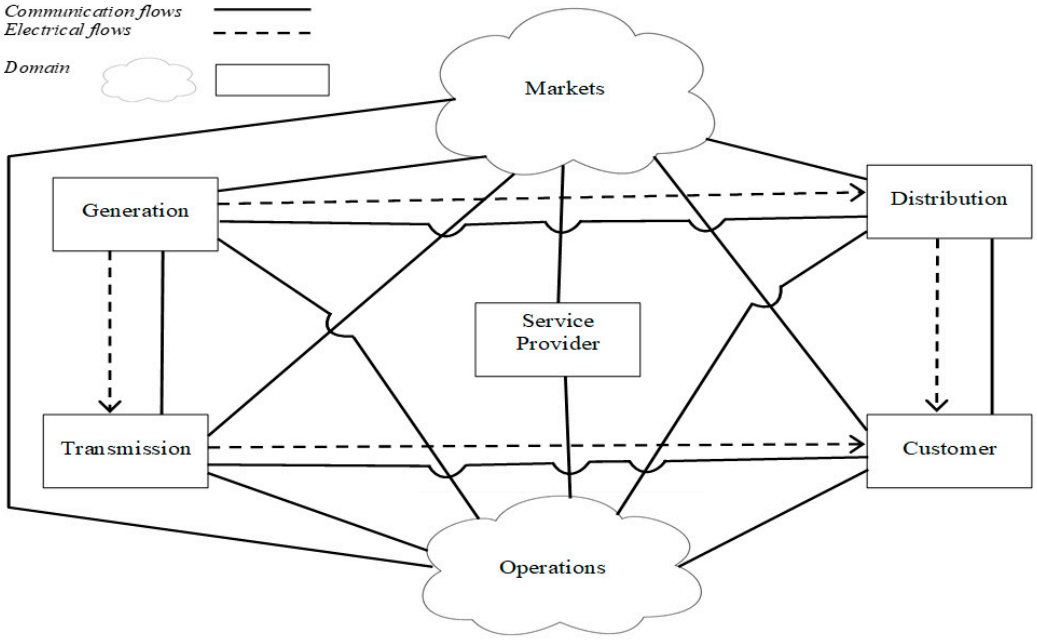

Figure 1. Electro energetic intelligent system and its interactions.

Changes in the spectrum of threats to the power system and the evolution of its components demonstrate the importance of implementing measures of reliability, operational safety, and interoperability from the design stage. One identified the following trends with a possible impact on the power system [37–41]:

- The implementation of information technology and telecommunications solutions, together with the increasing of the dependence of the power system on them, influences the performed operations positively in terms of speed and accuracy, determines fewer power outages of a small magnitude, and brings new vulnerabilities on the cyber side.
- The development of electronics involves small devices, with increased reliability and low energy consumption, but increases vulnerability to electromagnetic pulse.
- Interdependence between physical and cyber systems improves operational security but adds the possibility that a cyberattack may also affect physical systems.
- Outsourcing of equipment and services adds new vulnerabilities if nobody implements and uses appropriate security protocols.
- The evolution of the electric power system includes alternative methods of generation, energy storage, and decentralization; such a power system evolution involves rapid resilience, but adds new potential targets, with a lower level of security than a conventional plant and adds significant difficulties regarding the efficient and rapid coordination between all components involved.
- Standardization and flexibility of critical components has the potential to reduce the impact of a physical attack by rapidly changing affected components; however, in the event of a vulnerability, about which an attacker can easily find out details, the attack efficiency may increase and affect similar components.
- Coordination of assistance programs (e.g., spare parts stocks) limits the consequences of an attack and shortens the power outages, yet the large power transformers, built to order according to the customer specifications, has large sizes and is generally expensive. The power companies cannot afford to order such reserve transformers, given the financial and logistical burden.
- The implementation of new technologies instead of aging infrastructure can induce vulnerabilities due to disjunct or antagonist interests.
- Following all the adverse events of recent years, there is a growing trend for regulators and financial markets to recognize the security value, translated into incentives for security and resilience improvements.

Any power system is impossible to protect against all physical threats, given its size and the remote location of some of its components assessed as potential targets for cyberattacks, at least at certain times of the year. Thus, the most effective protection method against cyberattacks is the proactive collection of information by the relevant structures, in conjunction with law enforcement's action on preventing, deterrence, and annihilation of hostile actions on the power system before their occurrence. Such an event already took place in the United States on April 16, 2013. The attack, generically called the "Metcalf sniper attack", did not achieve its purpose, and the subject was not taken seriously by the media, which was a severe issue. The attackers cut the fiber optic in advance to make telecommunications impossible between the gas and electricity company Metcalf's "Pacific" substation, located in Coyote, California, and the authorities. Subsequently, the attackers opened fire on the 17 transformers within the station—those transformers became overheated after losing significant amounts of cooling oil. Nobody was injured or killed in this sabotage attempt, which was most likely carried out by professionals, because the authorities found no evidence, and the motivation behind the operation remained unknown. The attack did not achieve its goal, because the company managed to redirect electricity through other distribution lines to the region, thus avoiding a power outage while the station's repairs lasted a month. Such a precedent indicates the easiness of potential destabilization of a vital area of modern society: the critical power infrastructure. The attackers would not have managed such efficiency without inside information, so the Metcalf sniper attack cannot be considered a simple physical attack, but a combined one, in which the attackers exploited the vulnerabilities of the power system, with the help from inside (industrial espionage) or by illegally accessing the cyber system of the electricity company (cyberattack) [29,39,41]. Monitoring the self-integrity of the network used by the energy management systems (EMS, EMS/SCADA) for transferring the acquired data is a plus for both the company's security and the equipment's functionality. The proper selection and setup of SCADA systems ensure in-depth knowledge regarding the production's state of flow, service providing at any given time (i.e., including the electricity in the chain that forms the national power system), as well as the state of the equipment in terms of integrity and physical functioning but especially in terms of cybersecurity. SCADA systems are suitable for large environments, dispersed over some geographical regions. They comprise a command center that monitors and controls an entire technological process, a distribution system, a plant. For most operations, performed automatically, one may use Remote Terminal Units or Programmable Logic Controllers. At the same time, management decisions are taken in the command center based on the monitoring, control, and data acquisition system's graphic interface, as shown in Figure 2 [26,42,43].

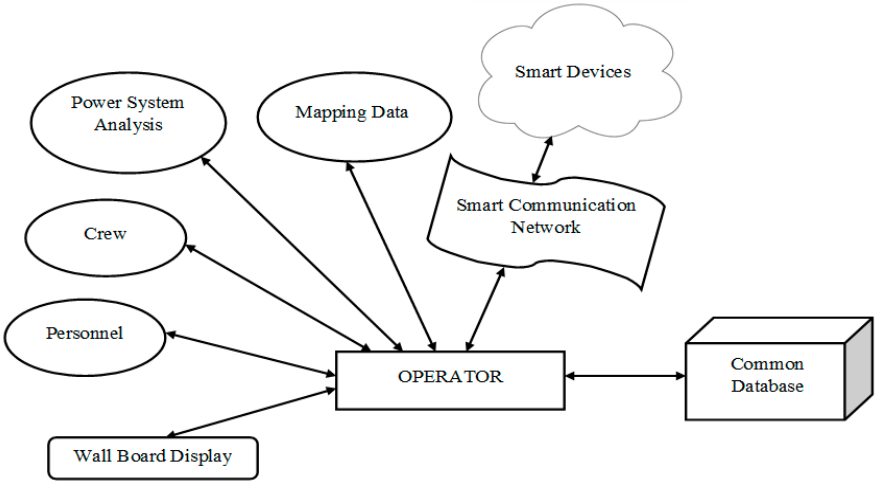

Figure 2. Structure of SCADA for power systems.

There is a clear example of vulnerability caused by the remote operation of assets through intelligent communication devices: the December 2015 attack on the Ukrainian power system focused on obtaining access data embedded in SCADA programs, followed by the remote control of operations. The combined consequences of exercised control, system disturbance, and malware installation made it challenging to return to normal operation states [44–46].

The cyber security architecture of monitoring, control, and data acquisition systems operates with the following terminology [47]:

1. The level/knowledge of the security structure refers to the level of training of the personnel responsible for cybersecurity, how well they know the system as a whole and in detail, and how effectively it copes with changes.
2. The level of potential adversaries refers to processes or actions that provide attackers with the tools and procedures to access the system, bypass the means of authentication or break them, and to find out further details about them through publicly available information.
3. Access/authentication refers to errors regarding the design, configuration, and implementation of the system that allow an attacker to have physical access to a part of the system or connect remotely to it.
4. Security weakness classifies as follows: defect - if the attacker manages to steal information, respectively, vulnerability, if a through a defect, the attacker receives access rights, as well.
5. Destructive potential refers to the level of potential damage caused once the attacker has access rights (e.g., changing parameters or shutting down equipment).
6. Detection refers to:
    - System access log.
    - Intrusion prevention.
    - Intrusion detection, if the attacked goes beyond the previous step.
    - Anti-malware solutions.
7. Recovery refers to the transition of the system back to the operating state, i.e., outstanding resilience that involves less significant damage.

Although the use of the term cyber resilience is vast, there is no consensus regarding its definition. From an organizational perspective, cyber resilience means "the ability to continuously deliver the intended outcome, despite adverse cyber events". Now, the organizational perspective refers to the ability level such as: supranational (i.e., a confederation of nations), national, regional, organizational (i.e., company), functional and technical [48]. The continuous deliverance requirement must reveal the presence of a completely functional "plan B", with the capability of fulfilling the outcome (i.e., the result of a business process in conditions of failure of the regular "plan A" following a successful cyberattack. In light of the cyber resilience definition presented above, adverse cyber events follow either "acts of God" (i.e., natural calamities) or "acts of man" (e.g., computer hacking, data deletion intentional or not), not necessarily separable. In the already mentioned reference [49], Bjorck et al. propose a delimitation between cybersecurity and cyber resilience using five aspects: *objective* (i.e., cybersecurity—to protect IT systems versus cyber resilience—assure the delivery of business), *intention* (i.e., cybersecurity—fail-safe versus cyber resilience—safe to fail), *approach* (i.e., cybersecurity—apply security from outside versus cyber resilience—built security from inside), *architecture* (i.e., cybersecurity—a single layer of protection versus cyber resilience—protection in multiple layers), and *scope* (i.e., cybersecurity—one organization versus cyber resilience—a cluster of organizations). In [50], Arghandeh et al. present several definitions of the resilience concept according to the application domains: infrastructure, economy, social, and/organizational. More precisely, there is a definition for power system cyber-physical resilience as the power system's ability to maintain the continuity in the electricity flow to customers following a priority sequence, appropriately responding in real-time to avoid interruption critical services.

The resilience represents the power system's ability to withstand disturbing events (e.g., perturbations, disruptions, disturbances, losses, adversity, anomalies, emergency, shocks, hazards, threats) and to have the capability of fast recovering and eliminate the effects caused by disturbances. In [51], the authors attempt to clarify the main differences between resilience and other concepts such as risk assessment, hazard, vulnerability, and robustness. In a thorough comparison, one presents the philosophical differences between the resilience and robustness of electrical power systems, highlighting that. In contrast, the resilience pleads for flexibility, adaptability, and agility in operation and control, as qualities of the service, the focus of assuring robustness targets the strength of the equipment coming from the design phase. Extreme robustness may lead to fragility. The reliability concept, defined as the power system's ability to deliver electricity of acceptable quality and for the contracted amount to the customers, although preceded by the concept of resilience, is still a significant preoccupation nowadays, being associated with the protection systems applied to substations [51,52]. In [51], Lei et al. propose a model for reliability assessment applied to a power substation build in conformity with the standard IEC 61850, assembled by using physical (i.e., transformers, circuit breakers, and transmission lines) in conjunction with cyber components (i.e., merging units, intelligent electronic devices, and process bus). The analysis of cyber-physical reliability appeals to the concept of the cyber-physical matrix. One can track the influence of the failure modes of individual components on the overall system. In [10,11], Falahati et al. evaluate the reliability of modern power systems, including the effect of the cyber system failure on the power system. There is a proposal to map the cyber system's failures to those recorded at the power system level. The primary outcome resulted in two optimization models meant to strengthen the cyber system's data connection and minimize the load shedding at the power system level. Reliability affected by cyber failures recorded at the protection system, treated by Lei et al. in [52], provides a quantitative dependency between the commutation time and service unavailability in the system.

Given the fact that an outside attacker must first enter the system and then know how the system works and what to change to cause damage, danger from the inside (employees or dissatisfied contractors or infiltrated by hostile states or competing companies) is much more likely to present itself, because such people know in detail the architecture and operation of the system components. The IT department of the electric utility company makes it easier to find such peeople by identifying the inside place of the launched attack, by implementing a source code control system (SCCS) that keeps track of changes made to the source code and allows the implementation of a previous variant, functional (without the lines of code that generated the malfunctions) in the back-up system.

An attacker tries all possible ways to enter the system, looking for devices that have integrated antennas and wireless network processors (WWAN), seeking to establish the connection to those devices identified with security breaches and that have not yet installed necessary updates.

Isolated targets connect to monitoring, control, and data acquisition systems via the GSM network, with bidirectional communication between the control center and the target being easy to intercept unless an encrypted communications system or a virtual private network is chosen, in which case Internet access becomes possible through the mobile operator.

3. Case of Study—Cyber Attack Simulation against Power Transformers

The present case of study refers to a significant portion of an intended petrochemical plant, a project that has now been abandoned. The name of the client cannot be disclosed for certain reasons, whereas the equipment modified data with respect to project documentation. The initial study started with a load flow, which provided the initial data for the further short-circuit analysis by using Electrical Power System Analysis Software—ETAP [53].

The ETAP Software Package, developed by Operational Technology International (OTI) has become an internationally standardized tool in Power System Analysis, addressing practically every single modeling and simulation problem in AC and DC systems. Demonstrated over more than two decades to be a very proficient software package, ETAP shortens the required calculation times, assuring a very high accuracy.

In the simulation procedure, one short circuit analysis was performed, with the following two purposes:

1. To verify the short circuit interruption capability for each breaker in the worst-case scenario of faulting each bus, i.e., theoretical, highly unlikely, yet necessary, for design purposes. The conclusion is that the breakers have the capability to withstand nominal currents, while safely interrupting the circuits in the case of the most severe faults, aka three-phase line to line to line.
2. Simultaneously, the optimization of the coordination between two or even three cascaded (i.e., connected in series, in a single path with the protected equipment) circuit breakers in such a way that, in the presence of three-phase short-circuits (L-L-L), the breaker closest to the fault trips first and eliminates the fault. In this way, the rest of the plant may potentially remain in operation if the process requires it. The coordination must exist for the short circuit current values obtained from the studies performed for all cases.

In Figure 3, the single-line schematic diagram of a full plant installation with the locations of possible security breaches is presented:

- Bus Z1—energizes the equipment used by the propylene installation
- Bus Z2—energizes the equipment used by the ethylene installation
- Bus Y1 and Bus Z3—energizes the equipment used by the methane installation.

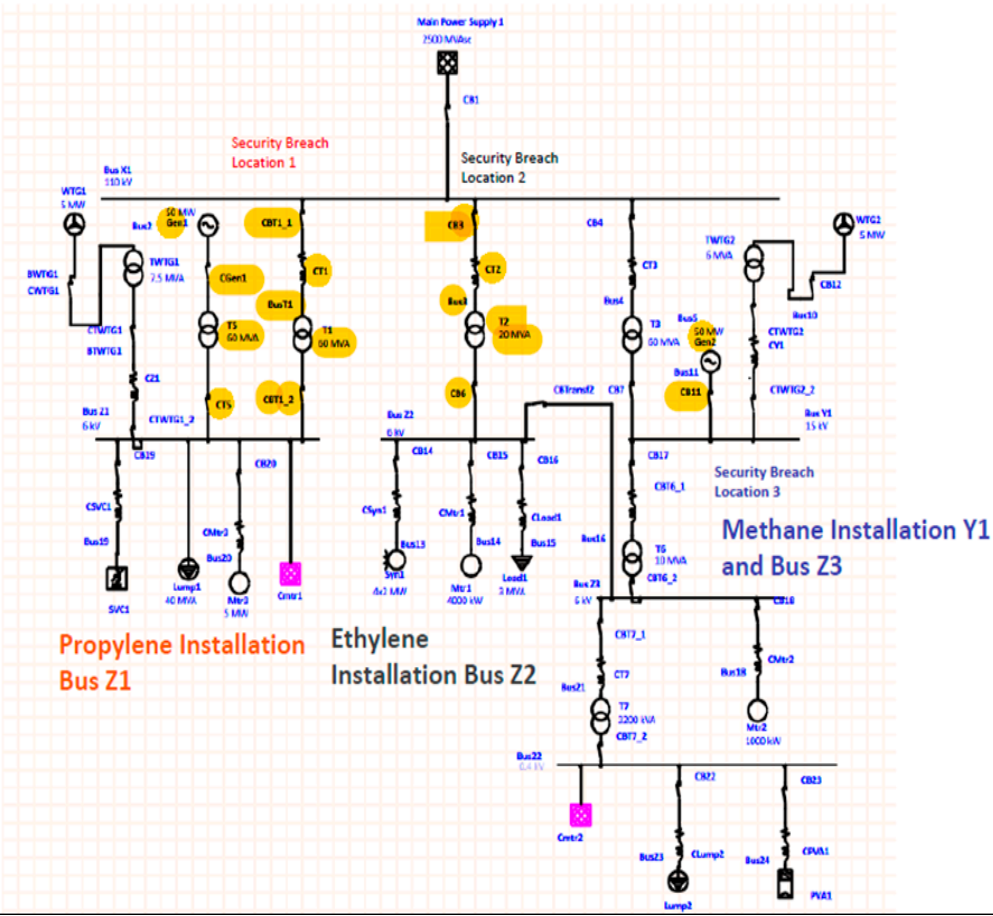

Figure 3. Full plant installation highlighting possible security breaches.

A three-phase fault at Bus Z1 may occur due to real system conditions or due to a security breach regarding the following equipment components: Transformer T1 and/or its breaker CBT1_2; Transformer T5 and/or its breaker CT5; Transformer TWGT1 and/or its breaker CTWGT1_2; Static VAR compensator and/or its breaker C19; Induction Motor Mtr3 and/or its breaker CMtr3.

A false temperature indication at the level of transformer T1 followed by its disconnection may result in the overloading of T5 or, indirectly, of GenZ1 1, and finally to the disconnection all the consumers connected to bus Z1.

3.1. Case 1—Simulation of a Possible Security Breach—Location 1

A three-phase fault at transformer T1 and its protective equipment (breaker CBT1_2), in conjunction with a three-phase fault at the transformer T5 and its protective equipment (breaker CT5), is shown in Figure 4.

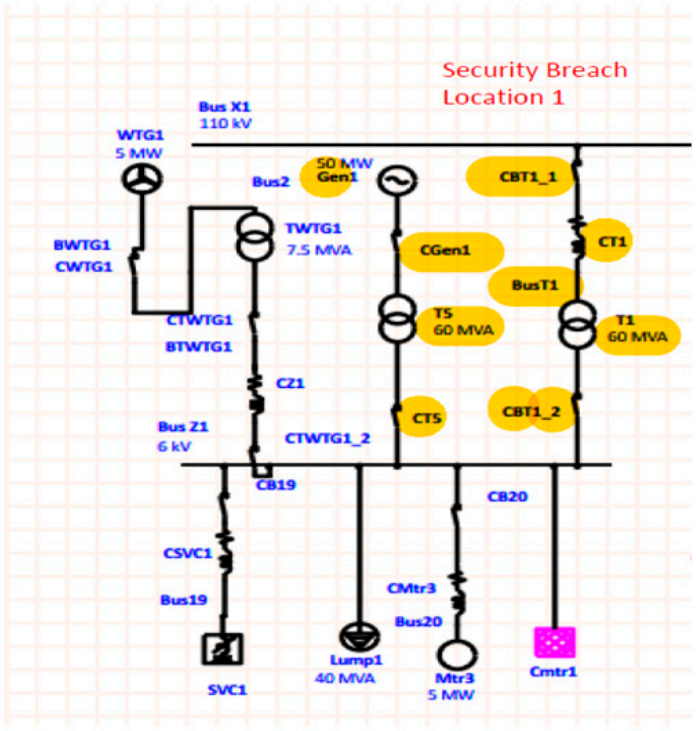

Figure 4. Security breach—Location 1.

The result places the propylene process installation out of operation. Initially, the total current absorbed by the electrical equipment belongs to the propylene installation, which, when operating at full capacity, is equal to 4650 A (at 6 kV).

The energy demanded by the propylene installation comes from mains using the transformer T1. The fully fast back-up required by the safety process imposed by the generator Gen1 is driven by a gas turbine and connected to the bus Z1 through the transformer T5. The nominal data for the transformers T1 and T5, and their percent impedance values, are given above. In Figures 5 and 6, the equipment data and impedance model, respectively, are presented for the transformer T1.

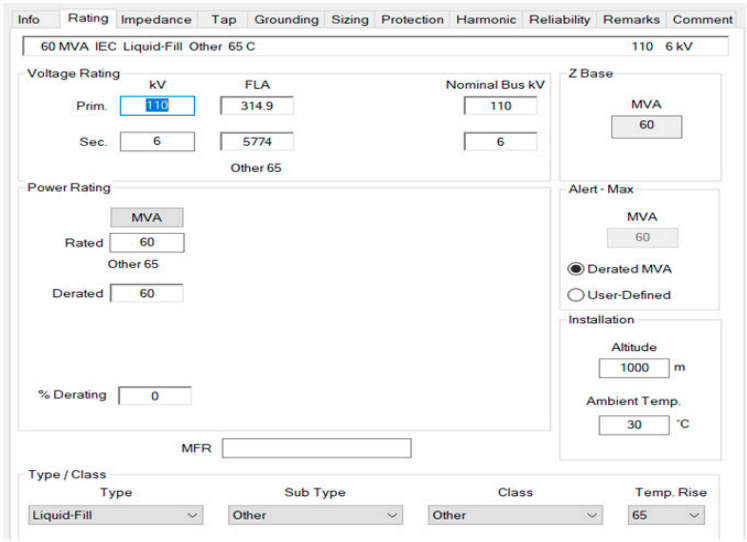

Figure 5. The nominal data for T1.

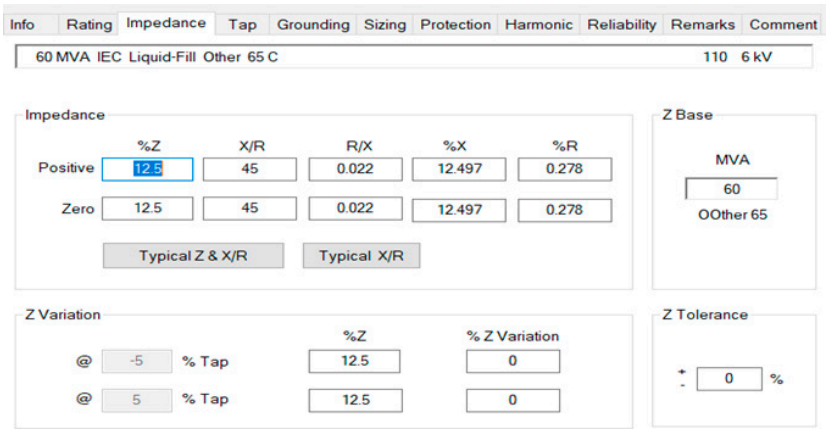

Figure 6. Percent impedance values for T1.

In Figures 7 and 8, the equipment data and impedance model, respectively, for the transformer T5 are presented.

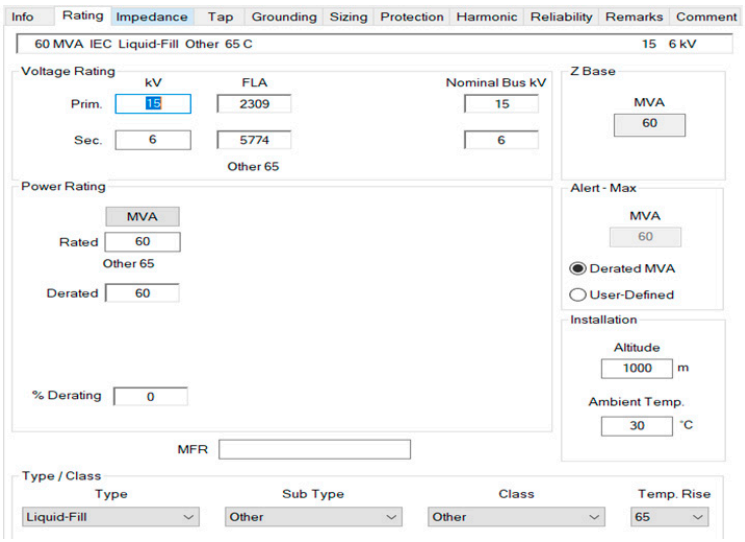

Figure 7. The nominal data for T5.

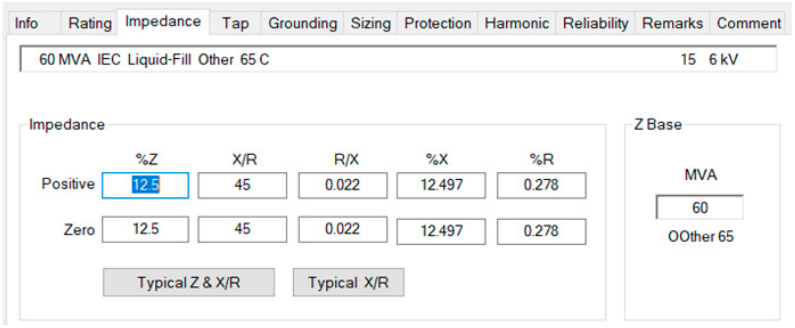

Figure 8. Percent impedance values for T5.

Interpretation of the Simulated Three-Phase Short-Circuit at Transformer T1

1. A cyberattack inducing a severe three-phase short-circuit at the transformer T1 or its breaker CTB1_2 results in a three-phase fault at the bus Z1, which can be safely eliminated by the breaker CTB1_2. Such an attack produces several adverse effects in the plant's whole distribution system, following excessive currents and voltage drops, whose values are presented in Figure 9, respectively, in Figure 10.

SHORT-CIRCUIT REPORT

3-Phase fault at bus: **Bus Z1**

Nominal kV = 6.000
Voltage c Factor = 1.10 (User-Defined)
Peak Value = 245.686 kA Method C
Steady State = 63.435 kA rms

Contribution		Voltage & Initial Symmetrical Current (rms)				
From Bus ID	To Bus ID	% V From Bus	kA Real	kA Imaginary	X/R Ratio	kA Magnitude
Bus Z1	Total	0.00	5.532	-93.909	17.0	94.072
Bus20	Bus Z1	0.94	0.661	-3.262	4.9	3.328
Bus19	Bus Z1	0.00	0.000	0.000	999.9	0.000
BTWTG1	Bus Z1	15.88	0.441	-2.549	5.8	2.586
BusT1	Bus Z1	92.56	1.053	-43.964	41.7	43.976
Bus2	Bus Z1	42.36	0.823	-20.111	24.4	20.127
Mtr4	Bus Z1	110.00	0.185	-1.173	6.3	1.187
Mtr5	Bus Z1	110.00	0.178	-0.944	5.3	0.961
Lump1	Bus Z1	110.00	2.191	-21.907	10.0	22.016
Mtr3	Bus20	110.00	0.661	-3.262	4.9	3.328
BWTG1	BTWTG1	40.31	0.441	-2.549	5.8	2.586
Bus X1	BusT1	92.64	0.057	-2.398	41.7	2.399
Gen1	Bus2	110.00	0.329	-8.044	24.4	8.051
PUA1	Bus24	98.52	0.000	0.000	0.0	0.000

Figure 9. Short-circuit report: three-phase fault at bus Z1.

Short-Circuit Summary Report

3-Phase Fault Currents

Bus		Device		Device Capacity (kA) Making				Short-Circuit Current (kA)				
ID	kV	ID	Type	Peak	Ib sym	Ib asym	Idc	I"k	ip	Ib sym	Ib asym	Idc	Ik
Bus Z1	6.000	Bus Z1	Bus					94.072	245.686				63.435
	6.000	CBT1_2	CB	360.000	130.000	156.072	86.362	94.072	245.686	87.877	118.559	79.585	
	6.000	CT5	CB	780.000	275.000	282.746	65.731	94.072	245.686	82.985	95.371	47.003	
	6.000	CTWTG1_2	CB	360.000	130.000	156.072	86.362	94.072	245.686	87.877	118.559	79.585	
	6.000	CB19	CB	360.000	130.000	156.072	86.362	94.072	245.686	87.877	118.559	79.585	
	6.000	CB20	CB	360.000	130.000	156.072	86.362	94.072	245.686	87.877	118.559	79.585	

Figure 10. Three-phase fault current.

2. Following the transformer T1 disconnection from the bus Z1 and the connection of the generator G1 through the transformer T5, the propylene installation's operation is fully re-established. However, a cyberattack targeting the transformer T5 or its breaker CT5, even eliminated by CT5, takes the full propylene installation out of function completely. The short circuit currents recorded for the three-phase fault recorded at bus Z1 have values very close to those displayed above.

3.2. Case 2—Simulation of a Possible Security Breach—Location 2

The simulation of a possible security breach at Location 2 appears in Figure 11: three-phase fault at the transformer T2 and its protective equipment (breaker CB6). Initially, the total current absorbed by the electrical equipment belonging to the ethylene installation, whereas operating at full capacity is equal to 1575 A (at 6 kV).

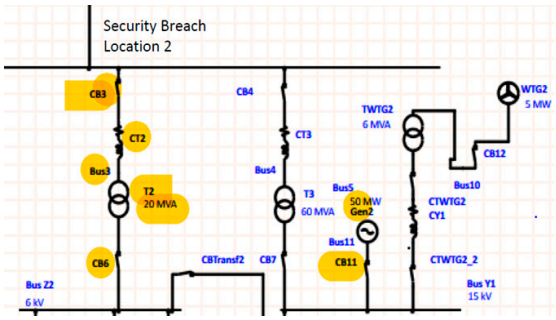

Figure 11. Security breach—Location 2.

The nominal data for the transformer T2, as well as percent impedance values, are presented in Figures 12 and 13, respectively.

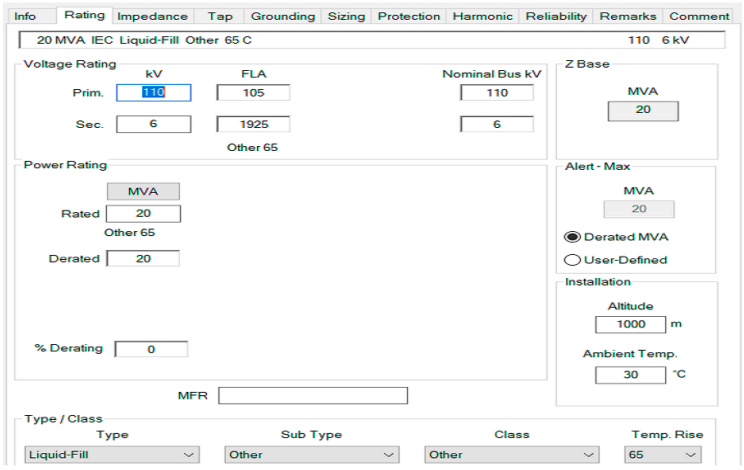

Figure 12. The nominal data for the transformer T2.

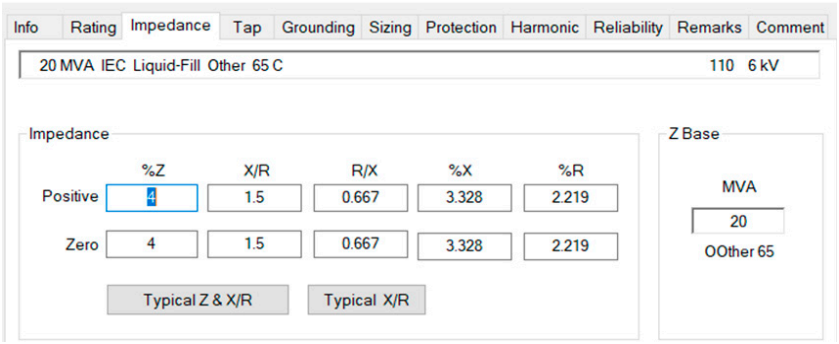

Figure 13. Percent impedance values for T2.

The energy demanded by the ethylene installation comes from mains using the transformer T2. A reduced (i.e., T6 rated at 10 MVA!) fast backup required by the process safety imposed the presence of the generator Gen2 (see Figure 11), driven by a gas turbine

and connected to the bus Y1. The generator Gen2 is the backup for methane installation connected to the bus Y1 and energized from the mains through the transformer T3.

Interpretation of the Simulation Three-Phase Short-Circuit at Transformer T2

1. A cyberattack inducing a severe three-phase short-circuit at the transformer T2 or its breaker CB6 results in a three-phase fault at the bus Z2, which can be safely eliminated by the breaker CB6. Such an attack produces several adverse effects in the plant's whole distribution system, following excessive currents and voltage drops, whose values appear presented in Figures 14 and 15.

SHORT-CIRCUIT REPORT

3-Phase fault at bus: **Bus Z2**

Nominal kV = 6.000
Voltage c Factor = 1.10 (User-Defined)
Peak Value = 126.211 kA Method C
Steady State = 57.665 kA rms

Contribution		Voltage & Initial Symmetrical Current (rms)				
From Bus ID	To Bus ID	% V From Bus	kA Real	kA Imaginary	X/R Ratio	kA Magnitude
Bus Z2	Total	0.00	22.359	-58.578	2.6	62.700
Bus15	Bus Z2	0.00	0.000	0.000	999.9	0.000
Bus14	Bus Z2	1.80	0.301	-2.544	8.5	2.561
Bus13	Bus Z2	0.85	0.210	-6.017	28.7	6.021
Bus3	Bus Z2	92.69	21.023	-38.115	1.8	43.528
Bus18	Bus Z3	0.64	0.097	-0.647	6.6	0.654
Bus21	Bus Z3	0.74	0.225	-1.035	4.6	1.059
Bus16	Bus Z3	88.38	0.503	-10.221	20.3	10.233
Mtr1	Bus14	100.00	0.301	-2.544	8.5	2.561
Syn1	Bus13	110.00	0.210	-6.017	28.7	6.021
Bus X1	Bus3	92.78	1.147	-2.079	1.8	2.374
Mtr2	Bus18	100.00	0.097	-0.647	6.6	0.654
Bus22	Bus21	24.07	0.225	-1.035	4.6	1.059
Bus Y1	Bus16	90.84	0.201	-4.088	20.3	4.093
PVA1	Bus24	25.57	0.000	-0.065	37320540.0	0.065
Bus Z3	Bus Z2	0.00	0.825	-11.903	14.4	11.931

Figure 14. Short-circuit report: three-phase fault at bus Z2.

Short-Circuit Summary Report

3-Phase Fault Currents

Bus		Device		Device Capacity (kA)				Short-Circuit Current (kA)				
				Making								
ID	kV	ID	Type	Peak	Ib sym	Ib asym	Idc	I"k	ip	Ib sym	Ib asym	Idc	Ik
Bus Z1	6.000	Bus Z2	Bus					62.700	126.211				57.665
	6.000	CB6	CB	360.000	130.000	156.072	86.362	62.700	126.211	60.921	62.698	14.822	
	6.000	CB14	CB	220.000	80.000	96.044	53.146	62.700	126.211	60.921	62.698	14.822	
	6.000	CB15	CB	220.000	80.000	96.044	53.146	62.700	126.211	60.921	62.698	14.822	
	6.000	CB16	CB	220.000	80.000	96.044	53.146	62.700	126.211	60.921	62.698	14.822	

Figure 15. Three-phase fault current.

2. With the transformer T2 disconnected from bus Z2, followed by the connection of the generator Gen2, the operation of the ethylene installation is re-established at reduced output, given the fact that the methane installation relies on mains through the transformer T3, eventually with some help from renewable energy sources (wind generator WTG2 and its transformer TWGT2). Such a scenario is valid, whereas T3, WTG2, and TWGT2 are fully operational.
3. However, a cyberattack, this time targeting the transformer T3 or its breaker CB7, takes the primary source for the methane installation (energized through bus Y1) out of operation, and the plant control room must decide whether to continue with ethylene production (energized through bus Z1) of methane. If the transversal couple breaker is not functional (i.e., faulty or under revision), then a cyberattack on transformer T2 or its breaker CB6 results in a complete stop for the ethylene installation.

3.3. Resilience Assessments

When performing resilience assessment, one must define the criteria that determine the metrics of resilience. In the literature, criteria are functions of time, carrying several names including performance, quality of service, the figure of matter, and service function [54,55].

Figure 16 displays a generic shape of a service function, highlighting three stable states (i.e., stable original state, disrupted state, and stable recovered state) and two transitory states. The transitions between the original stable state and the disrupted state following the disrupted event, respectively, between the disrupted state and the stable recovered state, are not mandatory linear because of the resilience action, as represented in Figure 16.

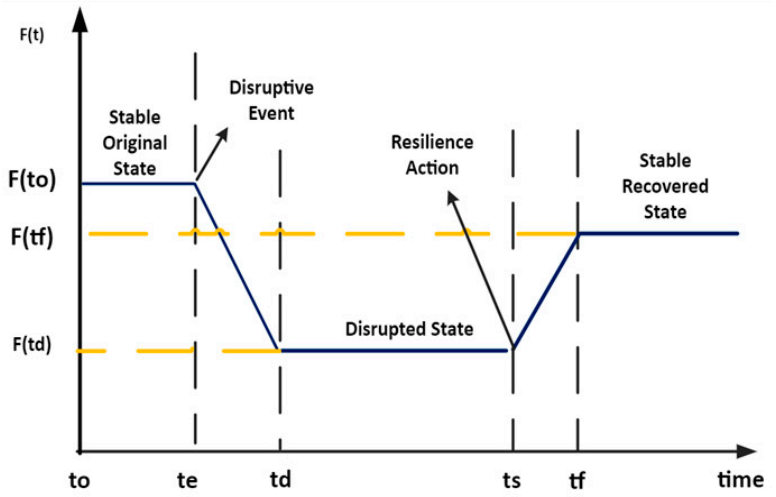

Figure 16. Service function depending on time.

By considering the two events presented in Sections 3.1 and 3.2, noted with e_j $j = 1, 2$, by choosing the service function as the percent input apparent power to the system $F(t_k)$, where t_k are the moments at which the system encounters actions or changes, the resilience can be defined as:

$$R(t_k, e_j) = \frac{F(t_k, e_j) - F(t_d, e_j)}{F(t_e) - F(t_d, e_j)} \quad (1)$$

According to Figure 16, t_0 is the time origin, t_e the moment when the disruptive event begins, t_d when the complete system's disruption, t_s the moment when the resilience action is applied, and t_f the time of complete or partial restoration of the service function.

For the case detailed in the Section 3.1, described as a fault at the transformer T1 and/or its protective equipment, namely the breaker CBT1_2, the service function is the percent apparent power demanded by the propylene installation. The scaling of the events from disruption to full restoration had the time represented in time units, as follows:

- The duration of the transient disruptive process: $t_d - t_e = 20$ units
- The duration of full disruption until the beginning of the resilience process: $t_1 - t_d = 60$ units
- The duration of the gas turbine startup and reaching the synchronous speed requited by the generator Gen1: $t_2 - t_1 = 40$ units
- The duration of the voltage built-up at the output of the generator Gen1 armature windings, assisted by the automatic voltage regulator: $t_3 - t_2 = 20$ units
- The duration of the process of synchronizing of the generator Gen 1 with the bus Z1, and paralleling to it: $t_4 - t_3 = 20$ units
- The duration of generator Gen1 field current adjustments for restoring the full apparent power demanded by the propylene installation: $t_f - t_4 = 20$ units

The full process of disruption–restoration in terms of time units and percent service function appears in Table 1.

Table 1. Simulation of a Possible Security Breach—Location 1.

Moment	t_e	t_d	t_1	t_2	t_3	t_4	t_f
(units)	0	20	80	120	140	160	180
Service function $F(t_k)$ (%)	100	0	0	30	70	90	100
Resilience	1.0	0.0	0.0	0.3	0.7	0.9	1.0

For the case detailed in the Section 3.2, the resilience action only partial (i.e., up to 40%) restores the operability of the ethylene installation, because the generator Gen 2 is shut down for the annual revision at the time of the disruptive event caused by the cyberattack, whereas the transformer T6 has only 8 MVA available. In this scenario, 4 MVA (i.e., 20%) come from the mains through the transformer T3, whereas the other 4 MVA (i.e., 20%) comes from renewable sources, respectively from the wind generator WGT2 through its transformer TWGT2.

The scaling of the events from disruption to full restoration had the time represented in time units, as follows:

- The duration of the transient disruptive process: $t_d - t_e = 20$ units
- The duration of full disruption until the beginning of the resilience process: $t_1 - t_d = 80$ units
- The duration of the power flow relocation through the transformer T3:$t_2 - t_1 = 20$ units
- The duration of the voltage built-up at the output of the generator WTG2 armature windings, assisted by the automatic voltage regulator, considering the wind turbine already in rotation: $t_3 - t_2 = 20$ units
- The duration of the process of synchronizing of the generator WTG2 with the bus Y1, and paralleling to it through the transformer TWGT2:$t_4 - t_3 = 20$ units
- The duration of generator WTG2 field current adjustments for delivering 4 MVA of apparent power demanded by the propylene installation:$t_f - t_4 = 20$ units

The full process of disruption–restoration in terms of time units and percent service function appears in Table 2.

Table 2. Simulation of a possible security breach—Location 2.

Moment	t_e	t_d	t_1	t_2	t_3	t_4	t_f
(units)	0	20	100	120	140	160	180
Service function $F(t_k)$ (%)	100	0	0	20	20	20	40
Resilience	1.0	0.0	0.0	0.2	0.2	0.2	0.4

Analyzing the schematic from Figure 3 in conjunction with the results from Table 2, one can conclude that the replacement of transformer T6, with higher ratings, for example 25 MVA, can provide the conditions for 100% service restoration in this case.

The graphs representing the time dependencies of the resilience in both cases in this study appear in Figures 17 and 18.

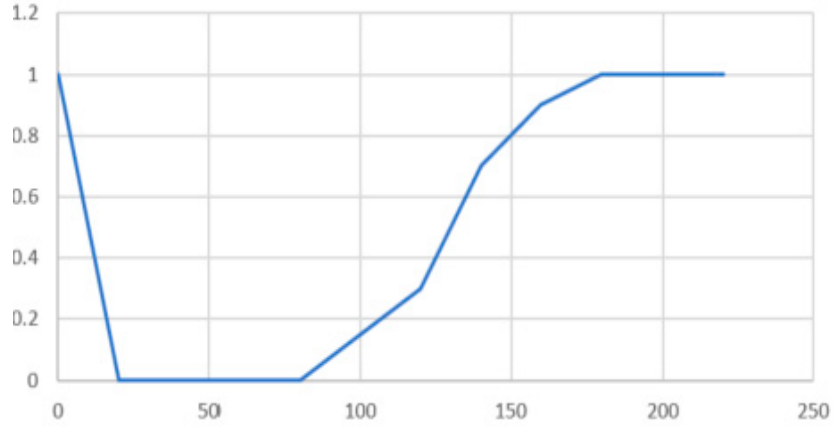

Figure 17. Resilience function depending $R(t)$ on time for disruption at Location 1.

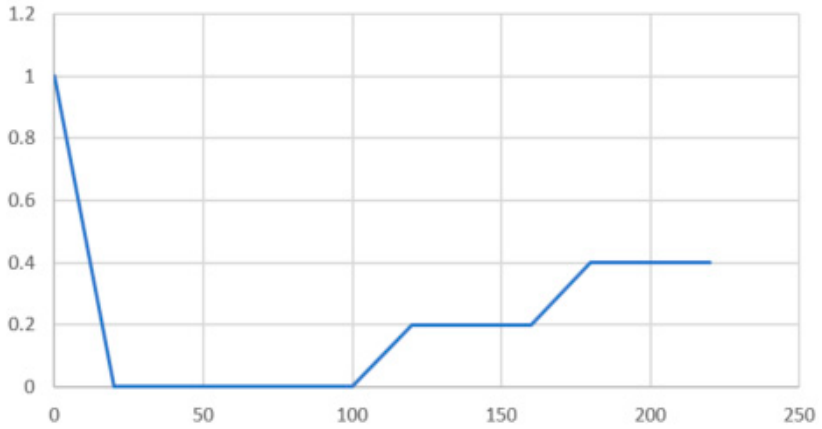

Figure 18. Resilience function depending on time for disruption at Location 2.

4. Conclusions

Nowadays, most national power systems are interconnected, and there is a strong presence of cyber and IoT components. For these reasons, simulation and analysis of industrial power plants under cyberattack constitutes a new and very important subject.

The present case study starts from the assumption that short-circuit conditions may appear following a breach in security in a petrochemical plant. For example, a three-phase fault at Bus Y1 may occur due to real system conditions or as a result of a security breach with respect to the following equipment components: Transformer T3 and/or its breaker CB7, Generator Gen 2 and/or its breaker CB11, Transformer TWGT2 and/or its breaker CTWGT2_2, Transformer T6 and/or its breaker C17.

An artificial short circuit combined with the poor conditions of coordination due to cyberattacks on the IPs belonging to the equipment components connected to a bus may result in the annihilation of all the installation energized from the other buses. The associated consequences may be severe: the transversal couple breaker may be tripped, resulting in much more disruption in the plant, through the disconnection of busses.

The study started with a load flow, providing the initial data for further short-circuiting analysis. The analysis relied on the ETAP Software Package, an internationally standardized tool in Power System Analysis, practically addressing every single modeling and simulation problem in AC and DC systems. This software has been demonstrated over more than two decades to be a very proficient software package, shortening the required calculation times and assuring a very high accuracy.

The short-circuit analysis had two purposes:

- To verify the short-circuit interruption capability for each breaker in the worst-case scenario of faulting each bus (i.e., theoretical, highly unlikely, yet necessary for design

purpose). The conclusion is that the breakers can withstand the nominal currents, whereas safely interrupting the circuits in case of the most severe faults. Moreover, from the obtained results, it the proper operation of every single equipment (e.g., generators, transformers, motors, loads, cables) can be observed; otherwise, ETAP would immediately highlight the place of malfunction by changing the text line(s) color to red and attaching proper flags.

- Meanwhile, the optimization of the coordination between two or even three cascaded (i.e., connected in series, in a single path with the protected equipment) circuit breakers, in such a way that, in the presence of three-phase short-circuits (L-L-L), the breaker closest to the fault trips first and eliminates the fault. In this way, the rest of the plant may potentially remain in operation if the process requires it.

In order to perform resilience assessment, the criteria that determine the metrics of resilience were defined and presented. For the case detailed in the Section 3.1, described as a fault at the transformer T1 and/or its protective equipment, namely the breaker CBT1_2, the service function is the percent apparent power demanded by the propylene installation. The scaling of the events from disruption to full restoration was represented in time using time units. Analyzing the schematic from Figure 3 in conjunction with the results from Table 2, it can be concluded that the replacement of the transformer T6 with one of higher ratings, for example 25MVA, can provide the conditions for 100% service restoration in this case. In the second case, the resilience action was only partial, at up to 40%, restoring the operability of the industrial power plant.

As future work, this problem can be solved by applying a procedure for encrypting and securing data, implemented in a simpler or more expensive platform, depending on the power system's desired level of protection.

Author Contributions: Conceptualization, M.S. and H.A.; methodology, M.S. and H.A; software, S.D.; validation, M.S., H.A. and S.D.; formal analysis, P.C.A.; investigation, M.S. and H.A.; resources, M.S, P.C.A. and H.A.; data curation, S.D.; writing—original draft preparation, H.A.; writing—review and editing, P.C.A., M.S., S.D.; visualization, M.S.; supervision, H.A. and M.S.; project administration, H.A.; funding acquisition, M.S. and H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Acknowledgments: The authors thank the "ETAP Canada" for providing the software used in simulations.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lee, S.; Huh, J.H. An effective security measures for nuclear power plant using big data analysis approach. *J. Supercomput.* **2019**, *75*, 4267–4294. [CrossRef]
2. 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]
3. Sun, C.C.; Liu, C.C.; Xie, J. Cyber-physical system security of a power grid: State-of-the-art. *Electronics* **2016**, *5*, 40. [CrossRef]
4. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State of-the-art. *Electr. Power Energy Syst.* **2018**, *99*, 45–56. [CrossRef]
5. Mohan, A.M.; Meskin, N.; Mehrjerdi, H. A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. *Energies* **2020**, *13*, 3860. [CrossRef]
6. National Infrastructure Advisory Council. Available online: https://www.dhs.gov/national-infrastructure-advisory-council (accessed on 10 October 2020).
7. Electric Grid Security and Resilience—Establishing a Baseline for Adversarial Threats. 2016. Available online: https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf (accessed on 17 March 2021).

8. Han, Y.; Wen, Y.; Guo, C.; Huang, H. Incorporating cyber layer failures in composite power system reliability evaluations. *Energies* **2015**, *8*, 9064–9086. [CrossRef]
9. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, M.S.H. Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
10. Falahati, B.; Fu, Y. Reliability assessment of smart grids considering direct cyber-power interdependencies. *IEEE Trans. Smart Grid* **2012**, *3*, 1515–1524. [CrossRef]
11. Falahati, B.; Fu, Y. Reliability assessment of smart grids considering indirect cyber-power interdependencies. *IEEE Trans. Smart Grid* **2014**, *5*, 1677–1685. [CrossRef]
12. Business Blackout. In *the Insurance Implications of a Cyber Attack on the U.S. Power Grid*; Lloyd's Emerging Risk Report; Lloyd's and the University of Cambridge, Centre for Risk Studies: Cambridge, UK, 2015.
13. Liu, X.-K.; Wen, C.; Xu, Q.; Wang, Y.-W. Resilient Control and Analysis for DC Microgrid System under DoS and Impulsive FDI Attacks. *IEEE Trans. Smart Grid* **2021**. [CrossRef]
14. Jena, S.; Padhy, N.; Guerrero, J.M. Cyber-Resilient Cooperative Control of DC Microgrid Clusters. *IEEE Syst. J.* **2021**. [CrossRef]
15. Jianfeng, D.; Jian, Q.; Jing, W.; Xuesong, W. A Vulnerability Assessment Method of Cyber Physical Power System Considering Power-Grid Infrastructures Failure. In Proceedings of the IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China, 20–24 November 2019; pp. 1492–1496. [CrossRef]
16. Energy Center. Available online: http://energy-center.ro/actualitate-news/911-dintre-sistemele-industriale-de-control-care-pot-fi-accesate-de-la-distanta-sunt-expuse-amenintarilor-cibernetice/ (accessed on 15 June 2020).
17. Langner, R. Stuxnet: Dissecting a cyber warfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [CrossRef]
18. The State of Security. Available online: https://www.tripwire.com/state-of-security/latest-security-news/electric-grid-vulnerabilities-abound/ (accessed on 12 July 2020).
19. The State of Security. Available online: https://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip/power-grid-security-vulnerabilities-call-on-utility-companies-to-unite-together/ (accessed on 13 July 2020).
20. Weird. Available online: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed on 13 July 2020).
21. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power systems on a cyber-physical environment. *Electr. Power Syst. Res.* **2017**, *149*, 156–168. [CrossRef]
22. Sullivan, J.E.; Kamenski, D. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *Electr. J.* **2017**, *30*, 30–35. [CrossRef]
23. BBC News. Available online: http://www.bbc.com/news/technology-30575104 (accessed on 14 August 2020).
24. Threat Landscape for Industrial Automation Systems in H1—2017. Available online: https://securelist.com/ksb-threat-predictions-for-industrial-security-in-2018/83186/ (accessed on 13 July 2020).
25. Sahu, A.; Davis, K. Structural Learning Techniques for Bayesian Attack Graphs in Cyber Physical Power Systems. In Proceedings of the IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2–5 February 2021; pp. 1–6. [CrossRef]
26. Edison Electric Institute. Available online: http://www.eei.org/ (accessed on 3 May 2020).
27. Radvanovsky, R.; Brodsky, J. *Handbook of SCADA/Control Systems Security*; CRC Press: Boca Raton, FL, USA, 2013.
28. NIST Special Publication 800-82, SCADA Systems for Electrical Distribution. Available online: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final (accessed on 5 March 2020).
29. Andrei, H.; Andrei, C.; Gaiceanu, M.; Stanculescu, M.; Arama, I.; Marinescu, I. Power Systems Recovery and Restoration Encouter with Natural Disaster and Deliberate Attacks, chapter 10. In *Power Systems Resilience, Modeling, Analysis and Practice*; Tabatabaei, M., Ravadanegh, S.V., Bizon, N., Eds.; Springer: Berlin/Heidelberg, Germany, 2019.
30. Andrei, H.; Gaiceanu, M.; Stanculescu, M.; Marinescu, I.; Andrei, C. Security evaluation of sensor networks, chapter 11. In *Recent Developments on Industrial Control Systems Resilience*; Tabatabaei, M., Pricop, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2019.
31. Kesler, B. The Vulnerability of Nuclear Facilities to Cyber Attack. Available online: http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI-v10-I1_Kesler.pdf (accessed on 3 January 2020).
32. Andrei, A.; Stănculescu, M. *Cryptography vs. Cryptanalysis*; Printech: Bucharest, Romania, 2014.
33. Andrei, H.; Gaiceanu, M.; Stanculescu, M.; Marinescu, I.; Andrei, C. Microgrid protection. In *Microgrid Architectures, Control and Protection Methods*; Tabatabaei, M., Kabalci, E., Bizon, N., Eds.; Springer: Berlin/Heidelberg, Germany, 2019.
34. Liu, X.; Li, Z. False data attacks, impact analyses and defense strategies in the electricity grid. *Electr. J.* **2019**, *30*, 35–42. [CrossRef]
35. Aoufi, S.; Derhab, A.; Guerroumi, M. Survey on false data injection in the smart power grid: Attacks, countermeasures and challenges. *J. Inf. Secur. Appl.* **2020**, *54*. [CrossRef]
36. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Available online: https://www.nist.gov/system/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf (accessed on 5 June 2020).
37. Boutin, V.; Feasel, M.; Cunic, K.; Wild, J. How Microgrids Contribute to the Energy Transition. Available online: https://sun-connect-news.org/fileadmin/DATEIEN/Dateien/New/9982095_12-01-16A_EN.pdf (accessed on 5 June 2020).
38. North American Electric Reliability Corporation and U.S. Department of Energy. High Impact, Low-Frequency Event Risk to the North American Bulk Power System. 2010. Available online: https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf (accessed on 10 June 2020).

39. Huang, T.; Pi, R.; Bompard, E.; Profumo, F.; Cuccia, P.; Fulli, G.; Masera, M. Analysis and visualization of natural threats against the security of electricity transmission system. *Sci. Bull. Electr. Eng. Fac.* **2017**, *17*. [CrossRef]
40. Xiang, Y.; Wang, L.; Zhang, Y. Adequacy evaluation of electric power grids considering substation cyber vulnerabilities. *Electr. Power Energy Syst.* **2018**, *96*, 368–379. [CrossRef]
41. Smith, R. Assault on California Power Station Raises Alarm on Potential for Terrorism. The Wall Street Journal 05 February 2014. Available online: https://www.wsj.com/articles/SB10001424052702304851104579359141941621778 (accessed on 11 October 2019).
42. Davarikia, H.; Barati, M.; Al-Assad, M.; Chan, Y. A novel approach in strategic planning of power networks against physical attacks. *Electr. Power Syst. Res.* **2020**, *180*. [CrossRef]
43. SCADA Systems for Electrical Distribution. Available online: https://www.electricaltechnology.org/2015/09/scada-systems-for-electrical-distribution.html (accessed on 11 October 2019).
44. Stanculescu, M.; Badea, C.A.; Marinescu, I.; Andrei, P.; Drosu, O.; Andrei, H. Vulnerability of SCADA and Security Solutions for a Waste Water Treatment Plant. In Proceedings of the IEEE 11th International Symposium on Advanced Topics in Electrical Engineering-ATEE, Bucharest, Romania, 28–30 March 2019.
45. Analysis of the Cyber Attack on the Ukrainian Power Grid, North American Electric Reliability Corporation, Electricity Information Sharing and Analysis Center. 2016. Available online: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (accessed on 11 October 2019).
46. Conway, M.; Bristow, J.; Doetzl, M.; Radigan, T. Lights Out in the Ukraine: Lessons Learned from a Successful Cyber Attack, ABB Power Generation Webinar. 2019. Available online: https://www.darkreading.com/vulnerabilities---threats/lessons-from-the-ukraine-electric-grid-hack/d/d-id/1324743 (accessed on 11 October 2019).
47. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2019**, *169*. [CrossRef]
48. Guide to Industrial Control Systems (ICS) Security. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.S800-82r2.pdf (accessed on 5 February 2020).
49. Bjorck, F.; Henkel, M.; Stirna, J.; Zdravkovic, J. *Cyber Resilience—Fundamentals for a Definition*; Advances in Intelligent Systems and Computing; Springer: Berlin/Heidelberg, Germany, 2015; Volume 353, pp. 311–316.
50. Arghandeh, R.; von Meier, A.; Mehrmanesh, L.; Mili, L. On the definition of cyber-physical resilience in power systems. *Renew. Sustain. Energy Rev.* **2016**, *58*, 1060–1069. [CrossRef]
51. Lei, H.; Singh, C.; Sprintson, A. Reliability modeling and analysis of IEC 61850 based substation protection systems. *IEEE Trans. Smart Grid* **2014**, *5*, 2194–2202. [CrossRef]
52. Lei, H.; Singh, C. Power system reliability evaluation considering cyber-malfunctions in substations. *Electr. Power Syst. Res.* **2015**, *129*, 160–169. [CrossRef]
53. Available online: www.etap.ca (accessed on 13 August 2020).
54. Ravadanegh, S.N.; Karimi, M.; Tabatabaei, M.N. Modeling, and analysis of resilience for distribution networks. In *Power Systems Resilience Modeling, Analysis and Practice*; Tabatabaei, M., Ravadaneghi, S.N., Bizon, N., Eds.; Springer: Berlin/Heidelberg, Germany, 2019.
55. Ashok, J.K. Analysis and Modeling of Resilience for Networked Systems. 2014. Available online: https://scholarsmine.mst.edu/masters_theses/7247 (accessed on 15 March 2021).