applied system innovation

MDPI

Article

Business Impact Analysis of AMM Data: A Case Study

Josef Horalek

Department of Information Technologies, Faculty of Informatics and Management, University of Hradec Králové, 500 03 Hradec Kralove, Czech Republic; josef.horalek@uhk.cz

Abstract: The issue of Automated Meter Management (AMM), an integral part of modern energy smart grid systems, has become a hot topic in recent years. With the current energy crisis, and given the new approaches to smart energy and its regulation, implemented at the level of the European Union, the gradual introduction of AMM as a standard for the regulation and management of the distribution system is an absolute necessity. Modern smart grids incorporate elements of smart regulation that rely heavily on the availability and quality of the data generated or used during AMM as part of the smart grid. In this paper, based on an analytical view of AMM as a whole and guided interviews with the sponsors of each service and owners of each dataset, criteria are proposed and a Business Impact Analysis (BIA) is implemented, the results of which are used to determine security measures for the safe and reliable running of the AMM system. This paper offers a unique view of the AMM system as an integral part of modern smart grid networks from a data-driven perspective that enables the subsequent implementation and fulfillment of security requirements by ISO/IEC 27001 and national security standards, as the AMM system is also a critical information system under the EU directive regarding the cybersecurity of network and information systems, which are subject to newly defined security requirements in the field of cybersecurity.

Keywords: security AMM; intelligent control; industrial security management; ISO 27001:2023; BIA; smart systems; cyber security in smart grids; smart metering; data privacy in smart grids

Citation: Horalek, J. Business Impact Analysis of AMM Data: A Case Study. *Appl. Syst. Innov.* **2023**, *6*, 82. https://doi.org/10.3390/asi6050082

Academic Editors: Claudio Zunino and Emmanuel Karapidakis

Received: 15 June 2023
Revised: 3 August 2023
Accepted: 7 September 2023
Published: 15 September 2023

1. Introduction

The electricity market in the Czech Republic is fully liberalized. All customers have the right to choose their electricity supplier and exercise their rights by metering their electricity consumption. The price of the commodity (electricity) is determined by the market. Activities of a monopoly nature, particularly with respect to the transmission and distribution of electricity and the provision of system services, are regulated. In the Czech Republic, there is an entity responsible for the central management and provision of metering data, referred to as the market operator (OTE, a.s.). Customers who use electricity for heating and water storage use a two-tariff system connected to a system for the remote control of appliances by means of a bulk remote control (hereafter referred to as an HDO). This system is used to directly remotely control groups of appliances according to set schedules that reflect the level of load on the network. At the same time, the system allows for tariff signals relating to the price of electricity supply to be transmitted to customers in a simplified form (differentiation between high and low price bands). As a result, customers in the Czech Republic have, for many years, enjoyed most of the benefits [1,2] that the EU hopes to obtain from the introduction of smart metering systems (also referred to as AMM). Distribution companies can thus also influence (optimize) the course of the daily load in distribution networks within the limits set by tariff schemes approved by the regulatory authority. At the same time, it should be noted that the potential for savings and the management of electricity consumption on the part of customers who do not use electricity for heating and storage water heating is low, given the share represented by this consumption in total household consumption and its time structure [3].

In smart grids, blockchain integration is often considered to offer greater security and reliability in various sectors. Robust prevention and detection mechanisms are essential for protecting these networks from cyber threats. Here, we present a brief overview of the key strategies used to prevent and detect cybersecurity breaches in these advanced systems. This involves preventing cybersecurity breaches in the area of blockchain-based authentication, which enables the use of decentralized identity management and blockchain cryptographic mechanisms to achieve secure user authentication and access control. This prevents unauthorized access to critical network components. Furthermore, it is necessary to ensure the security of smart contracts on the blockchain, with rigorous code reviews and auditing processes being implemented to ensure the security of smart contracts deployed on the blockchain. Eliminating vulnerabilities in smart contracts prevents the occurrence of potential exploits and breaches. Encrypting these communications is essential, and is most often achieved by deploying end-to-end encryption protocols to secure communication channels between network components, ensuring data confidentiality and integrity. With respect to process–technical approaches, regular software updates are required to remove known vulnerabilities and fix potential entry points for cyber attackers. Appropriate multi-factor authentication (MFA) techniques combine passwords with other authentication factors, such as biometrics or tokens, in order to strengthen user authentication and prevent unauthorized access. Topologically, the focus is on network segmentation: by dividing the network into secure segments, we limit access to sensitive areas and limit the damage an attacker can cause. The final component is thus the security audits themselves.

Another prong is cybersecurity intrusion detection, which uses intrusion detection systems (IDS) to monitor network traffic and identify suspicious activity or anomalies that are indicative of potential cyber-attacks. Next are behavior analysis systems, which use machine learning algorithms to analyze user and device behavior and detect deviations from normal patterns that could indicate a breach. Last but not least, it is possible to leverage blockchain technology to achieve an immutable audit trail, where the immutable nature of the blockchain is used to create an audit trail of all network activity, ensuring the transparent monitoring and investigation of potential security breaches. Real-time monitoring capabilities should also be mentioned for their ability to quickly detect and respond to cyber threats, thus reducing the amount of time an attacker has to penetrate a system. Then, threat intelligence feeds can be integrated to keep users up-to-date on emerging cyber threats, and implementing proactive measures against potential attacks is also important for effectively managing cybersecurity. The subsequent outputs from the BIA and from risk analysts themselves are collected in incident response plans, which are imperative to get right. Well-defined incident response plans describe the steps to be taken in the event of a cybersecurity breach and ensure a rapid and coordinated response. Integrating blockchain technology into smart grids offers robust security benefits. By combining preventative measures with advanced detection mechanisms, organizations can significantly reduce the risk of cyber-attacks, protect critical data, and ensure the smooth operation of smart grids.

Due to the dynamic development and availability of smart metering technologies, the fully fledged phased introduction of AMM, supported by national and European legislation, is realistic. However, the introduction of AMM as part of the smart grid entails specific risks from the perspective of DSOs, including the gradual emergence of norms and standards based on the EU directive Common Rules for the Internal Electricity Market [4], which addresses the technical risks of communication interference (electromagnetic compatibility, etc.). Cybersecurity is a significant risk for a new AMM-based system, as stated by D. Bhamare et al. in [5], where he presents a detailed analysis in the area of cybersecurity for industrial control systems; furthermore, A. AlDairi and L. Tawalbeh in [6], focusing on the importance of a cyber-attack analysis targeting the Smart City area (in which AMM undoubtedly falls), an E. Ismagilova et al. in [7], where they similarly discuss the importance of analysis and risk management. While the obsolete and replaced mass remote control (HDO) system is highly robust concerning the technologies used and prac-

tically unassailable by conventional means (possibility of physical separation of control systems; high-power and connection voltages required for signal generation), the cyber security of the new system is a challenge that needs to be addressed both process-wise and technology-wise. There are also opportunities for the use of Artificial Intelligence in this area, as discussed by T. Yigitcanlar et al. in [8] in a sub-oral literature review discussing the contributions and risks of Artificial Intelligence, where the intelligent power control system that is mentioned plays a significant role. Similarly, the use of AI is discussed by R. Nishant et al. in the context of global sustainability, etc. [9].

It is clear from the above that the deployment of the AMM system as a global solution for the efficient management of the generation, distribution, and consumption of electricity brings new risks in the area of cyber security.

The area of cybersecurity assurance at present often consists only of the implementation of security restraints and security baselines, which are logically related to the fulfillment of international security standards, especially ISO 27001 [10], and the recommendations of organizations such as ENISA or NIST. However, to optimize the deployment of uniform security measures and improve the perception of the ISO 27001 recommendations, it is necessary to identify the transformative assets: data and information. These assets need to be determined as objectively as possible in terms of their confidentiality, integrity, and availability, which is the cornerstone for the definition of appropriate security measures and is, therefore, the first aspect that this article addresses regarding the specific environment of AMM. However, given the complexity of the issue of cybersecurity and its impact on business objectives, there is a unique and unique approach to determining business impact analysis. This is due to the link between the relevance of homogeneous datasets and the business impacts, but also to the clear justification of the requirements to ensure adequate cybersecurity, as well as their financial costs. This complex approach, based on a data analysis of individual datasets, their impact on the company's business, and an interrogation of the service to cybersecurity, is an innovative issue that is either addressed separately or, more often than not, not at all. This complex approach presents an opportunity to link the technical cybersecurity perspective with a pure business perspective, as required not only by the spirit of standards and recommendations but by the roles of cybersecurity managers and security directors. The shortcomings of existing solutions and approaches can be summarised in a few points:

- An isolated view of cybersecurity and business requirements.
- Separate technology or organizational solutions.
- Identification of data assets and downstream services as primary assets.
- Use of technical and technological perspectives, without considering datasets.
- Insufficient consideration of business requirements.
- Insufficient process for mapping and exchange of data assets.

The approach and process presented below, developed as a case study, addresses the above shortcomings and limitations. The general advantage of the BIA then is that it can and does draw on generally available information and data, developed, e.g., as part of undergraduate and thesis work, supplemented by publicly guided interviews with the sponsors of individual data assets. The author's findings are then based on the collected data and information, supplemented by the author's specific knowledge of the distribution company environment where he worked as a security manager. Thus, the main research concerns the banning of publicly available information data flows, an assessment of their importance, and the synthesis of BIA documents as inputs for further security analysis and the design of continuity and recovery plans, etc.

The article is structured into interrelated logical units. The third chapter presents an analysis of the data used in the AMM system. The technical Object Identification System (OBIS) codes that are used to generate the uniform datasets are presented. These are described in detail, with an emphasis on their meaning, and a model of the data flow of the homogeneous datasets is presented. This is followed by a brief introduction to the prescriptions of data aggregation used for the operation of the whole AMM system, as an

important part of the Smart Grid, and for the systems of the regulator and the electricity market operator (EMO).

In the next chapter, the criteria for determining dataset values according to the CIA triad and the parameters for BIA are presented. The resulting values of the datasets discarded by the CIA triad and the results of the BIA are presented, and the reasons for and implications of the discarding of the different ascetics involved in the operation of the AMM system are discussed. The discussion chapter then outlines the most important performance requirements that emerged from the implemented BIA and CIA.

2. Materials and Methods

The basic research methodology was to analyze the scientific and technical approaches to address the cybersecurity of the Smart Grid system and its smart parts, which affect the low voltage level and the renewable parts in the form of AMMs. By synthesizing the obtained sub-techniques and procedures, a set of criteria for assessing the trustworthiness, availability, and integrity of each dataset were formed, compiling the most significant risks from the perspective of the grid operator, and information was gathered through repeated guided interviews to classify the significance of each dataset, technical means and risks in the BIA.

Related Works

A similar approach to that described above can be found in a broader range of solutions to the specific cybersecurity conditions of industrial and intelligent systems, as outlined in the following publications:

- M. Antunes et al. A Client-Centered Information Security and Cybersecurity Auditing Framework [11].
- M. Antunes et al. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal [12].
- Corallo et al. Cybersecurity in the Context of Industry 4.0: A Structured Classification of Critical Assets and Business Impacts [13].
- J. Oliveira et al. Failure Mode and Effect Analysis for Cyber-Physical Systems [14].
- Corallo Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level [15].
- V. Mullet et al. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0 [16].

The above-mentioned scientific publications unanimously confirm that a complete approach to impact analysis based on extended BIA methods is not only used but has significant scientific and research potential for tuning appropriate strategies to build a safe environment for information systems and data security. The issue of an effective approach to risk management in heterogeneous networks where the technical and data interconnection of the world of ICT and ICS and IoT occurs is a widely discussed and researched topic at present, and the subject of several scientific research topics, as can be concluded from the selected current outputs given below:

- Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence [17].
- K. Razikin et al. Cybersecurity Decision Support Model to Designing Information Technology Security System Based on Risk Analysis and Cybersecurity Framework [18].
- N. F. Syed et al. Traceability in Supply Chains: A Cybersecurity Analysis [19].
- F. Kitsios et al. Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry [20].
- V. Sobeslav et al. Security Consideration of BIA Utilization in Smart Electricity Metering Systems [21].

As mentioned above, smart metering and the whole complex AMM system are considered an integral part of the smart grid, and its security requirements and compliance need to be addressed from this perspective. This security and process perspective is currently the subject of a wide range of research projects and projects:

- Philips et al. A Review on Cyber Security in Metering Infrastructure of Smart Grids [22].
- M. Z. Gunduz et al. Cyber-Security on Smart Grid: Threats and Potential Solutions [23].
- W. Qiu et al. Multi-View Convolutional Neural Network for Data Spoofing Cyber-Attack Detection in Distribution Synchrophasors [24].
- Sun et al. Intrusion Detection for Cybersecurity of Smart Meters [25].
- I. Kawoosa et al. A Review of Cyber Securities in Smart Grid Technology [26].
- Lee et al. Data Privacy and Residential Smart Meters: Comparative Analysis and Harmonization Potential [27].
- N. K. Singh et al. End-User Privacy Protection Scheme from Cyber Intrusion in Smart Grid Advanced Metering Infrastructure [28].
- M. Orlando et al. A Smart Meter Infrastructure for Smart Grid IoT Applications [29].
- M. K. Hasan et al. Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations [30].
- T. S: Ustun Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages [31].
- J. Slacik et al. Broadband Power Line Communication for Integration of Energy Sensors within a Smart City Ecosystem [32].
- X. Xia et al. Detection Methods in Smart Meters for Electricity Thefts: A Survey [33].
- S. Vitiello et al. Smart Metering Roll-Out in Europe: Where Do We Stand? Cost Benefit Analyses in the Clean Energy Package and Research Trends in the Green Deal [34].
- Youssef et al. Analytical Analysis of Information-Centric Networking in Smart Grids [35].
- Kohout et al. Smart Metering Cybersecurity-Requirements, Methodology, and Testing [36].
- H. Kim et al. Intelligent Access Control Design for Security Context Awareness in Smart Grid [37].

The above overview of selected related works confirms that the issue of ensuring the security and effectiveness of heterogeneous systems connecting ICT, ICS, and IoT world is one of the most dynamically developing areas in the world of information and network security. It is necessary for homogeneous, specific types of communication and data to design such security measures, consisting of technical and organizational measures that do not affect the quality of transmitted data, considering the latency and stability requirements of the whole AMM system.

However, for the effective implementation of security solutions, it is necessary to correctly identify and classify the individual datasets and, subsequently, the technical resources that create, enrich, and exploit these datasets. For this reason, it is essential to use a data-centric view of the entire AMM system that identifies the types of data, their meaning, and their flow throughout the system. For this view of the data, it is necessary to use standard approaches and develop a data analysis and business view using BIA, the results of which can then determine the desired data quality and value, which, in turn, determines the deployment of sub-security solutions at the organizational and technology level. This basic view is presented in this article, which was prepared as a case study in cooperation with a distributor covering 2/3 of the distribution territory of the Czech Republic and having over 3 million customers.

3. Analysis of AMM Data

The AMM meter is classified as a static meter like all meters that measure electrical energy using electronic components without mechanically moving parts. Each static meter determines the readings using Object Identification System (OBIS) codes. Previously, these were only a few readings, which included voltage, current, and active energy values. At

present, it is also possible to determine from the meter data whether there has been a security breach, for example, by removing the cover or possibly attempting to tamper with the data with a magnet, from information in the meter's error register, as shown in the OBIS codes shown in Table 1.

Table 1. OBIS code registers.

OBIS Code	Magnificence	Description
1.0.12.4.0.255	U	The mean voltage value is the average of the combined values.
1.0.12.6.0.255	U max	Minimum voltage value. The meter measures or counts the combined voltage values every second and stores the maximum value in 15 min from three values.
1.0.12.3.0.255	U min	Minimum voltage value. The meter measures or counts the combined voltage values every second and stores the minimum value in 15 min from three values.
1.0.21.4.0.255	+P (+Ri) L1	The mean value of active sampling power per evaluation period (projection of the phasor onto the *x*-axis in quadrants I and IV) in phase 1.
1.0.22.4.0.255	−P (Ri) L1	The mean value of the active supply power for the evaluation period (projection of the phasor onto the *x*-axis in quadrants II and III) in phase 1.
1.0.23.4.0.255	+Q (+Rc) L1	The mean value of reactive power (inductive in active sampling) over the evaluation period (projection of the phasor to the *y*-axis in quadrants I and II) in phase 1.
1.0.24.4.0.255	−Q (−Rc) L1	The mean value of reactive power (capacitive when taking active power) for the evaluation period (projection of the phasor to the *y*-axis in quadrants III and IV) in phase 1.
1.0.31.4.0.255	I L1	The mean value of current per evaluation period in a phase.
1.0.41.4.0.255	+P (+Ri) L2	The mean value of active sampling power per evaluation period (projection of the phasor onto the *x*-axis in quadrants I and IV) in phase 2.
1.0.42.4.0.255	−P (−Ri) L2	The mean value of the active supply power for the evaluation period (projection of the phasor onto the *x*-axis in quadrants II and III) in phase 2.
1.0.43.4.0.255	+Q (+Rc) L2	The mean value of reactive power (inductive in active sampling) per evaluation period (projection of the phasor to the *y*-axis in quadrants I and II) in phase 2.
1.0.44.4.0.255	−Q (−Rc) L2	The mean value of reactive power (capacitive when taking active power) for the evaluation period (projection of the phasor to the *y*-axis in the III and IV quadrants) in phase 2.
1.0.51.4.0.255	I L2	The mean value of current per evaluation period in phase 2.
1.0.61.4.0.255	+P (+Ri) L3	The mean value of active sampling power per evaluation period (projection of the phasor onto the *x*-axis in quadrants I and IV) in phase 3.
1.0.62.4.0.255	−P (−Ri) L3	The mean value of the active supply power for the evaluation period (projection of the phasor onto the *x*-axis in quadrants II and III) in phase 3.
1.0.63.4.0.255	+Q (+Rc) L3	The mean value of reactive power (inductive in active sampling) over the evaluation period (projection of the phasor to the *y*-axis in quadrants I and II) in phase 3.
1.0.64.4.0.255	−Q (−Rc) L3	The mean value of reactive power (capacitive when taking active power) for the evaluation period (projection of the phasor to the *y*-axis in quadrants III and IV) in phase 3.
1.0.71.4.0.255	I L3	The mean value of current per evaluation period in phase 3.
1.0.1.8.0.255	+A	Electricity (work) consumption—description of the cumulative dial at the end of the evaluation period (consumption—from the PDS perspective) in the sum of 3 phases.
1.0.2.8.0.255	−A	Electricity (works) supply—description of the cumulative dial at the end of the evaluation period (supply—from the PDS perspective) in the sum of 3 phases.
1.0.1.8.1.255	+A T1	Electricity in tariff 1 (works) consumption—description of the cumulative dial at the end of the evaluation period (consumption—from the supply system operator perspective) in the sum of 3 phases.
1.0.1.8.2.255	+A T2	Electricity in tariff 2 (works) consumption—description of the cumulative dial at the end of the evaluation period (consumption—from the perspective of the supply system operator) in the sum of 3 phases.
1.0.1.8.3.255	+A T3	Electricity in tariff 3 (works) consumption—description of the cumulative dial at the end of the evaluation period (consumption—from the perspective of the supply system operator) in the sum of 3 phases.
1.0.1.8.4.255	+A T4	Electricity in tariff 4 (works) consumption—description of the cumulative dial at the end of the evaluation period (consumption—from the perspective of the supply system operator) in the sum of 3 phases.
1.0.0.2.1.255	IDTOU	Number of TOUs.
1.0.96.1.0.255	SNn	Serial number of the electrometer.
1.0.0.0.0.255	ckod	BAR code.
1.0.0.2.0.255	Firmware	Firmware version.

When reading values from the meter, the data file is normally divided into two parts: register reading and profile reading. Table 1, containing the OBIS register codes, shows an example of the first part of the meter register data file; this contains the state variables such as the states and maxima of the active energy consumed and delivered, as well as the voltage and current values on the individual phases or possibly the error registers. Each value is accompanied by a time stamp indicating the date on which the value was read. The second part of the data file contains the data from the LP15 m profile; these values are given in 15 min intervals in the file and are the mean value of the measured energy over a 15 min period. When performing a reading of these values, the period to be read is always defined so that the values are related to the values from the previous reading; see Table 2, showing OBIS codes profile LP15.

Table 2. OBIS codes profile LP15.

OBIS Code	Magnificence	Description
1.0.1.4.0.255	+P	The mean value of active sampling power per evaluation period (projection of the phasor onto the *x*-axis in quadrants I and IV) summed over 3 phases.
1.0.2.4.0.255	−P	The mean value of the active power of the supply for the evaluation period (projection of the phasor onto the *x*-axis in quadrants II and III) in the sum of 3 phases.
1.0.6.4.0.255	+Rc	Reactive power phase in Q2.
1.0.8.4.0.255	RC−	Reactive power phase in Q4.
1.0.5.4.0.255	Ri+	Reactive power phase in Q1.
1.0.7.4.0.255	Ri−	Reactive power phase in Q3.

3.1. AMM Datasets and Systems Entering the Analysis

For analysis purposes, it is first necessary to identify the datasets that need to be secured in the AMM measurement. For AMM measurements, security must be devised comprehensively across systems. AMM measurement is used today for so-called Type C measurements. Datasets flow through various systems across the entire structure of the organization; see Figure 1, containing a flow diagram of datasets. For the sake of simplicity, one part has been selected, and that is the path of the data sets from the measurement equipment to the customer. A description of each dataset is given as follows:

- LP15—This is the so-called "last profile", which contains the mean values of the performance in the interval of 15 min. This profile is mainly used to obtain better information about the consumption at the point of consumption for the customer and the trader. This profile can be used as a control element for validation, or it can be used to evaluate the maximum for future microservices and the under-supply for consumption. Thanks to AMM metering, the LP15 profile can be used to calculate consumption more accurately in case of complaints of a defective meter at the point of consumption.
- LP60—This is a 60 min profile, which is calculated as the arithmetic mean of the sum of the four LP15 values to obtain a profile at a 60 min interval. Its applicability is mainly in the area of monthly deviation billing to the electricity market operator (EMO) and is also provided as customer information. The calculation of LP60 is always performed as part of the validation in the Reading and Validation System.
- BW—This is the billing value data set, which is a copy of the meter registers. For billing purposes for type C metering, using AMM, the value of the Net Energy of Consumption or Production is used. This value always has a time stamp. As part of the reading, the values of all possible variables are always read from the meter, most of which are used for validation and verification purposes.
- ODP—This type of dataset is an instruction-type message sent to the meter for remote disconnection due to non-payment. It is not used much in practice at present, but in the future, it should be used in cases where the customer has not paid for the electricity consumed and has an inaccessible tapping point.

- PRIPO—The dataset operates on a similar principle as ODP, except that, in this case, it is a connection of the point of subscription, for example, after payment or overwriting the point of subscription.
- TAR—The TAR dataset contains tariff setting information, which will either be a message that sets a fixed switching of blocked appliances within the low and high tariff, or is a direct instruction to switch appliances on or off. The function in the meter replaces the existing bulk remote control system and the meter can also switch more types of appliances than was possible with the old-fashioned AMM metering, thanks to the attached relay box.
- BLOCK—The BLOCK dataset indicates the power limiting function. It is mainly used in microdevices where it is necessary to limit power generation in case of a large surplus of power in the network. It is also used if the maximum generation at a customer site is exceeded.

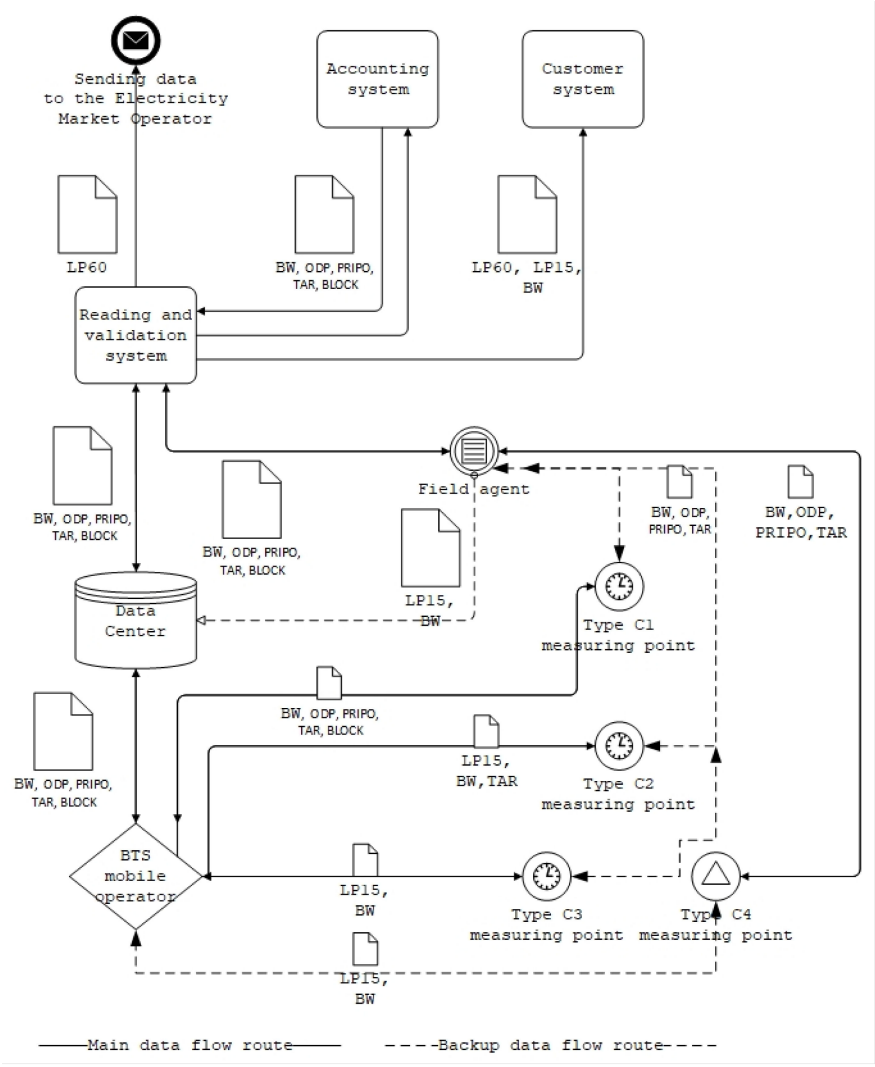

Figure 1. Dataset flow diagram.

The diagram shows where the information assets flow; the different systems have different functions and use the information assets in different ways. Meters at measuring point MP with C1, C2, C3 and C4 measurement types (MPC1, MPC2, MPC3, MPC4) have different integrated functions. For MPs with measurement types C1, C2, and C3, the meters have remote communication and thus allow the measurement of the LP15 waveform and BW registers, while for measurement type C4, the meter does not need remote reading and can be operated as a standard measurement type C meter by physical reading by a

field worker. The meter for metering types C1 and C2 has the possibility of remote tariff control (TAR) or remote setting by changing the TOU table. The meter for C1 type of metering should also have ODP and PRIPO functions, which are remote disconnection and connection, as well as the possibility of remote BLOCK power limitations. As one of the main links in the external service providers, there is a mobile operator and its BTS is included in the communication chain, which provides a means of communication between the data center and the meter. The transmission technology in this case may be heterogeneous and does not need to be specified for the data analysis. The data center (DCT) is designed to collect data and also forms a direct connection to the meters. All data are stored in the DCT when the reading is taken. The DCT should be sufficiently secure against external attacks; therefore, it should only be accessed by the internal network. The Readout and Validation System (RaVS) is the software used to operate the data center. In the readout system, readings are defined and scheduled, and various reports are run. As it is also a validation system, validation is performed of the data in the measured data sets. Also, the hourly LP60 data are calculated here and the data are sent to the Accounting System (US) or Customer System (CS). Further, for security reasons, the data intended for the Electricity Market Operator (EMO) are also sent through an intermediate link in the form of a data-sending application to the Electricity Market Operator. The Accounting System (AS) is used for billing consumption and all customer and employee records are kept here; it also deals with various operational matters such as meter installation and dismantling, disconnection, connection, and all meter servicing. The Customer Service (CS) system is set up to provide metering data to customers; here, it is possible to see the progress of the meter readings and part of the description of the registers. The application of sending data to EMO provides a means of communication with the market operator and sends sound data and messages to EMO. The last link is the field agent (FA), who performs physical periodic readings of MP with a C4 metering type, establishes disconnection following non-payment and parameterization of meters if necessary, and performs readings and adjustments for meters on MP with C1, C2, and C3 metering type in case of non-functional communication.

3.2. The Aggregation Principle

With AMM, the EMO measures data for production and consumption. Within the balance sheet, EMO then carries out post-aggregation, a process whereby deviations from the agreed values are calculated for the balance sheet groups of each settlement entity. These calculations are then used as the basis for the settlement of the deviations. This root-and-branch accounting is not only a legislative obligation, but, in the context of the AMM system and its integration into the overall Smart Grid system, has a direct impact on the end customer, where it influences their behavior in terms of electricity ownership and use, enables the distributor to personalize consumption offers, and ultimately increases the impact of the efficient use of electricity for small consumers by offering not only an instant overview of consumption and costs, but also the opportunity to adjust their behavior in terms of planning consumption for moments of surplus and offering savings in moments of high consumption and possible electricity shortages in the grid. The whole system then maintains the basic physical principles and saves transmission and distribution network costs by educating consumers. The clearing entity deviation is defined as the difference between the actual supply and actual consumption of electricity on the one hand and the total agreed supply and total agreed consumption of electricity on the other hand (1). Supply (generation) is always marked with a positive sign and consumption is marked with a negative sign. The deviation is always set in MWh with a resolution to three decimal places.

$$\mathrm{V}_{CE} = E_{CE}^{actual} - E_{CE}^{contr} \quad (1)$$

CE—Clearing entity.
V_{CE}—Clearing entity variance.
E_{CE}^{actual}—Actual supplied/extracted energy [MWh] (2).
E_{CE}^{contr}—Contracted energy [MWh].

$$E_{CE}^{actual} = \sum_{CTP \in CE} E_{supplied,CE}^{measured} - \sum_{CTP \in CE} E_{\text{extracted,CE}}^{measured} \quad (2)$$

Index $CTP \in CE$- expresses the set of all *CTPs* that the EMO has registered in the system to a particular clearing entity.

$E_{supplied,CE}^{measured}$ resp. $E_{\text{extracted,CE}}^{measured}$—the measured value of supply or extraction [MWh] in a given domestic CTP [MWh]; this value includes the positive or negative control energy that was actually produced/not produced/consumed and therefore must be measured.

According to the legislation, the actual quantity of electricity in the clearing entity in a trading hour is the sum of the quantity of electricity based on the data obtained from measurements using type diagrams at the points of consumption or transmission of the clearing entity and at the point of consumption and transmission of the electricity market participants for which the clearing entity has assumed responsibility for the deviation (3). The contracted quantity of electricity should be the sum of the quantity of electricity contracted by that clearing entity, along with other clearing entities, in a given trading hour, including the quantity of the contracted control energy.

$$E_{CE}^{\text{contracted}} = \sum_{ID \in CE} E_{\text{supplied},CE}^{\text{contracted}} - \sum_{ID \in CE} E_{\text{extracted},CE}^{\text{contracted}} + \sum_{ID \in CE} E_{\text{imp,CE}}^{measured} - \sum_{ID \in CE} E_{\text{exp,CE}}^{measured} + \sum_{ID \in CE} E_{\text{regulation,CE}}^{measured} \quad (3)$$

The index $\Sigma_{ID \in CE}$ expresses the set of all execution diagrams negotiated by a given clearing entity (or market participants for which it has assumed deviation responsibility) with other clearing entities.

$E_{\text{supplied,CE}}^{\text{contracted}}$ resp. $E_{\text{extracted,CE}}^{\text{contracted}}$ is the commercially negotiated resulting value of the clearing entity's obligation to deliver or withdraw electricity to/from the EC based on the registration of negotiated values in organized markets and the registration of domestic bilateral trades [MWh].

$E_{\text{imp,CE}}^{measured}$ resp. $E_{\text{exp,CE}}^{measured}$ is the commercially negotiated value of the commitment of the clearing entity to deliver or withdraw electricity to/from the EC based on the registration of cross-border bilateral contracts.

$E_{\text{regulation,CE}}^{measured}$ is the total value of the contracted control energy [MWh].

From the above, it is clear that the appropriate quality of data sets in the AMM system is essential for the proper functioning of the power system and the relationship between the generator, distributor, and end user.

4. Business Impact Analysis of AMM Datasets

Business Impact Analysis (BIA) is widely used to assess the impact on an organization when there is an interruption in the supply of products or services that are critical to its operations. It is primarily used as an input to business continuity management (BCM) and risk analysis. BIA primarily involves expert determination of the minimum levels of resources required to restore critical activities within specified times and levels.

The methodological evaluation of BIA for AMM purposes involves, in the first phase, the assessment of the value/quality of information assets using the Confidentiality, Integrity, Availability (CIA) triad. The task is to determine the significance of homogeneous data assets, which then influences the choice of protection level.

This is followed by the implementation of standard procedures for BIA, which starts by defining and qualifying the basic risks for BIA related to the area of reregulated electricity distribution service to end customers.

This is followed by the establishment of service availability parameters in the form of Maximum Tolerable Period of Disruption (MTPD), Medium Impact Period of Disruption (MIPD), and Maximum Tolerable Data Loss (MTDL.) In parallel with this, recovery parameters in the form of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be established. For uniform parameters, threshold values are established that reflect the legislative and regulatory requirements for this type of regulated business.

BIA focuses primarily on metering data as important datasets. Metering data are used by different distribution companies for settlement purposes with different market

participants, as well as to ensure grid stability, especially given the growth of small-scale renewables. Without these data, the energy market could not function, and the risk of grid instability would increase. Therefore, the analysis needs to assess the risk of their unavailability to the distribution company. As an example of a distribution company, ČEZ Distribuce, a.s., one of the three licensed distribution system operators, will be used in the currently deployed variant of meter communication with a point-to-point data center.

4.1. CIA Triad Security Classification

Before the BIA itself is carried out, it is necessary to carry out a classification and establish safety criteria. These criteria are determined according to the degree of severity of the impact on the operation of the organization. The main purpose is to make the subsequent design and associated measures clearer and simpler. The readings from the measuring equipment, which must be protected from misuse, will be entered as a data set. The security aspects are mapped to the CIA triad, and we use the A, B, C, and D grades to determine the importance of the datasets. The specific parameters are given in Tables 3–5.

Table 3. Availability criteria.

Class Availability	Security Classification	Description
A	[A; *; *]	Disruption of the availability of the information asset system is not acceptable, and even short-term unavailability must be addressed as soon as possible. Recovery should be within minutes; otherwise, the interests of the distribution system operator (DSO) may be critically compromised.
B	[B; *; *]	The unavailability of the information asset system must be restored within hours; otherwise, the interests of the DSO may be seriously compromised.
C	[C; *; *]	The unavailability of a system information asset should not exceed a period of one day. A longer outage may result in a partial compromise of the DSO's interests.
D	[D; *; *]	Data unavailability affects the interests of the DSO to an insignificant extent.

Table 4. Confidentiality criteria.

Class Availability	Security Classification	Description
A	[*; A; *]	The information assets are very confidential and if they were to be disclosed, this could have fatal consequences for the DSO and possibly the functioning of the distribution system.
B	[*; B; *]	Information assets are confidential, and their protection is mandated by law, the Civil Code, or GDPR.
C	[*; C; *]	Information assets are not public, and their disclosure would violate unbundling.
D	[*; D; *]	Information assets may only be disclosed under certain conditions set by law or the DSO's internal regulations.

Table 5. Integrity criteria.

Class Availability	Security Classification	Description
A	[*; *; A]	A disruption to the integrity of the information asset could ultimately affect the operation of the distribution system and the DSO.
B	[*; *; B]	Violation of the integrity of the information asset could limit the important interests and objectives of the DSO.
C	[*; *; C]	A breach in the integrity of the information asset could limit, in part, the interests and objectives of the DSO.
D	[*; *; D]	Violation of the integrity of the information asset does not significantly limit the interests and objectives of the DSO.

4.2. Guidelines for BIA

The BIA guides are always determined depending on the nature of the business of the organization for which the impact of a disruption of an information asset is being examined. For ČEZ Distribuce a.s. (ČEZd), the most valuable dataset is the measurement data; therefore, the BIA analysis guidelines must relate to the area of use of these assets.

Lawful and Contractual Obligations—Electricity metering is most often used by distribution companies, including ČEZd, as a basis for billing for electricity supply or consumption; therefore, these companies must comply with laws that mainly relate to doing business in the energy sector. At present, the continuous metering on MP type C metering, the operation of which will be in charge of AMM metering, is not yet mandatory. Its use will not be mandatory until 2027, and not all decrees and laws are fully prepared for this way of measuring electricity. The rights and obligations of operation within the framework of legislation are addressed as the main legal regulation by the Energy Act No. 458/2000 Coll. [38]; this Act incorporates the relevant European Union regulations and comprises the rules or conditions of doing business or exercising state administration in the energy sectors, which are the electricity, gas, and heating sectors, or the rights and obligations of natural and legal persons related thereto. There is also Decree No 359/2020 [39], formerly Decree No 82/2011, on electricity metering [40]; this Decree defines how electricity metering is to be carried out at individual consumption points. As of 2021, the C1, C2, and C3 methods of electricity metering with remote power transmission, and C4, with the possibility of installing remote power transmission, have been integrated into the decree.

The obligation to measure in this way starts on 1.7.2027, which puts even more pressure on introducing AMM as soon as possible. The Decree also sets out the rules for the transmission of measurement data and the conditions for each type of measurement. It also sets out the dates and scope of data transmission to the electricity market operator. The last part concerns the method of determining the compensation for unjustified electricity consumption. Decree No 540/2005 [41] is also important; this Decree sets out the required quality of supply and services related to regulated activities in the electricity sector, including the amount of compensation for non-compliance, the procedures and deadlines for claiming compensation, and the procedures for reporting compliance with the quality of supply and services. Decree No. 408/2015 on the Electricity Market Rules [42] defines how the electricity market is to operate, the financial settlements within the market, the format of data transmission, and the legal deadlines or penalties for non-compliance. It also covers provisions relating to the supply and generation of electricity, metering data, and supported resources.

Management and operation of the organization—Efficiency is particularly important in management and operations. In addition, it is also necessary to ensure operations in terms of safety and stability. Therefore, this aspect is important, because if an unexpected situation occurs in the organization, it is necessary that the organization has sufficient human resources and is able to resolve everything in the shortest possible time, before there is any major impact on the quality of the service delivered in the transmission of

measurement data. If the emergency requires the use of only part of the capacity, the risk of any impact on the functioning of the organization is minimal. However, if the emergency or failure of critical systems cannot be resolved even using all available capacity and resources, the consequences for the organization can be almost fatal.

Provision of necessary services—AMM metering data will mainly be used for customers with less electricity consumption, with a circuit breaker of up to 80 A, which is about 15% of electricity consumption in the Czech Republic, a minority share. However, as far as the number of customer points with this type of metering is concerned, there are 3.5 million customer points in the territory of ČEZ Distribuce, a.s. Therefore, the unavailability of a small number of consumption points will have only a small impact, will not affect the organization, and the limitation will be almost no problem for customers. However, if the data or service limitation affects more than 100,000 or even 1,000,000 subscriber points, this can be a big problem for the whole organization.

Loss of confidence—Credibility is very important for any organization, including ČEZ Distribuce, a.s. Even external presentation can play a role in the choice of strategy within the business and direction of the company. If there is some minor failure or glitch in, for example, communication, it may not have any major impact on the functioning of the organization and may not even have a major impact on the relationship with the customer, and thus the public. On the other hand, there may be a large-scale and long-lasting outage or a major loss of data. Should this happen, negative publicity may ensue, which may be dealt with at the national level or even by the government and could possibly result in a reduction in the value of the company or its sales and a large staff turnover.

Financial loss/interference with operations—The financial burden in the event of a data access problem by CEWD varies most according to the length of time for which the information asset is unavailable. If the unavailability of type C metering data for AMM meters is taken into account, a short data access failure or small amount of data loss may have almost zero financial impact on the organization. On the other hand, if there is a long-term outage or large data loss at 100,000 or more customer sites, the financial burden on the organization could be devastating. In particular, Decree No. 540/2005 [41], a Decree on the quality of electricity supply and related services in the electricity sector and the deadline for sending, and Decree No. 408/2015 [42], a Decree on the Electricity Market Rules, impose financial penalties for failures to provide data on time (4).

$$a \times p \times t = P \quad (4)$$

a—number of MPs.
t—time of overrun (hours).
p—penalty in (€).
P—penalty (€).

Based on the above guidelines for BIA, it is possible to identify five basic risks that will be assessed in the BIA. For each risk, the impacts of its possible implementation are defined and categorized (Table 6).

Table 6. Risk classification from the BIA guidelines.

Impact/Risk	Exceeding Lawful and Contractual Obligations	Disruption to the Management and Operation of the Organization	Loss of Confidence	Financial Loss/ Interference with Operations	Provision of Necessary Services
1—Low	May cause violations of internal policies, regulations, or contracts	May cause some restriction of operation for a short period in part of the organization.	Relationships within the organization or with some suppliers may deteriorate for a short period.	Directly or indirectly, this will lead to losses of several million crowns.	System and service limitations for several thousand people.
2—Medium	It can lead to administrative or civil proceedings and associated financial penalties.	May cause restrictions in important parts of the organization for a longer period.	May adversely affect relationships with the public or a wide group of people for a short period.	Directly or indirectly, this will lead to losses of tens of millions of crowns.	System and service limitations for tens of thousands of people.

Table 6. *Cont.*

Impact/Risk	Exceeding Lawful and Contractual Obligations	Disruption to the Management and Operation of the Organization	Loss of Confidence	Financial Loss/ Interference with Operations	Provision of Necessary Services
3—High	It may cause a breach of the law leading to criminal prosecution. Possible prohibition of activity—loss of license.	May cause temporary cessation of operations in important parts of the organization or a large part of it.	May very negatively affect public relations for a long period, with spillover to the national level or energy exchange.	Will lead directly or indirectly to losses of several hundred million crowns.	Extensive system and service limitations affecting several hundred thousand people.
4—Critical		May cause temporary cessation of operations in important parts of the organization or a large part of it.	Can have a lasting serious impact on relationships at the national level, and with customers and suppliers, and even have political implications.	Will directly or indirectly lead to losses of more than half a billion crowns.	Extensive restriction of essential systems or services to more than half a million persons.

It is now necessary to determine the Maximum Tolerable Period of Disruption (MTPD), Medium Impact Period of Disruption (MIPD), and Maximum Tolerable Data Loss (MTDL) parameters, which determine how data sets should be treated in the event of recovery and backup. Primarily, these parameters determine the business continuity management for information assets, as well as Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameters, where RPO is the time from which the last backup was taken, and RTO is the time needed to make the application available again. In determining these parameters, we assume the baseline conditions, where RPO <= MTDL, RTO <= MIPD, and RTO <= MTPD.

The Maximum Tolerable Period of Disruption (MTPD) is the maximum period of tolerance for unavailable or disrupted services that would have a high impact on ČEZ Distribuce, a.s. (Table 7).

Table 7. MTPD criteria.

Grade MTPD	Description
30M	High impacts are achieved within 30 min.
2H	Within 2 h, high impacts are achieved.
12H	Within 12 h, high impacts are achieved.
24H	Within 24 h, high impacts are achieved.
2D	High impacts are achieved within 2 days.
1W	High impacts are achieved within 1 week.
1WW	In more than 1 week, high impacts are achieved.

The Medium Impact Period of Disruption (MIPD) is the maximum period of tolerance for unavailable or disrupted of services that would result in a medium impact on ČEZ Distribuce, a.s. (Table 8).

Table 8. MIPD criteria.

Grade MIPD	Description
30M	Medium impacts are achieved within 30 min.
2H	Within 2 h, moderate impacts are achieved.
12H	Within 12 h, moderate impacts are achieved.
24H	Within 24 h, moderate impacts are achieved.
2D	Medium impacts are achieved within 2 days.
1W	Medium impacts are achieved within 1 week.
1WW	High impacts are achieved in more than 1 week.

The Maximum Tolerable Data Loss (MTDL) is the maximum time since the last data backup that is acceptable to ČEZ Distribuce, a.s. (Table 9).

Table 9. MTDL criteria.

Grade MTDL	Description
1H	It is backed up periodically at 1 h intervals.
1D	Backed up periodically at 1-day intervals.
1W	Backed up regularly at intervals of 1 week.
1WW	Backed up regularly at intervals of 1 month.

In order to implement the BIA, it is necessary to define input metrics to assess data unavailability, data loss, and data disclosure or modification from the perspective of the system sponsors (Table 10).

Table 10. BIA evaluation metrics.

Abbreviation	Description
30M	Unavailable data 30 min.
2H	Unavailable data 2 h.
12H	Unavailable data 12 h.
24H	Unavailable data 24 h.
2D	Unavailable dates 2 days.
1W	Unavailable dates 1 week.
1WW	Unavailable for more than 1 week.
B1	Missing backup 1 h.
B24	Missing backup 24 h.
BW	Missing backup week.
BM	Missing backup month.
BALL	Complete loss of data.
UDOUT	Unauthorized disclosure to strangers.
ER	Minor errors—various typos.
ERL	Major errors—incorrectly programmed data transmissions.
ERD	Deliberate data modification error.

5. Results

In the first stage of the analysis, the parameters of the CIA triad were determined, which determines the significance of the individual datasets that the company has and uses in AMM. The resulting evaluation was divided according to the type of metering; this type of metering was subsequently differentiated in accorfance with Decree No. 359/2020 Coll, based on whether it was a so-called continuous or non-continuous metering, whether it was generated or consumed, and whether two-tariff metering or a one tariff rate was used. The summary results are shown in Table 11.

Table 11. Classification of CIA triad of AMM datasets.

Type of Measurement AMM Data Set	C1 Production/ Consumption 1T/2Current	C2 Consumption 2T Continuous	C3 Consumption 1T Continuous	C4 Consumption 1T/2T Non-Continuous
LP 15	[B; B; A]	[C; B; B]	[C; B; B]	[C; B; B] *
LP60	[B; B; B]	[C; B; C]	[C; B; C]	[C; B; C] *
BW	[B; B; A]	[B; B; A]	[B; B; A]	[C; B; A] *
ODP	[B; A; A]	[B; A; A] **	[B; A; A] **	[B; A; A] **
PRIPO	[B; A; B]	[B; A; B] **	[B; A; B] **	[B; A; B] **
TAR	[A; A; B]	[B; A; B]	N/A	[B; B; B] **
BLOCK	[A; A; A]	N/A	N/A	N/A

* The dataset for a given type of measurement occurs only in exceptional cases when remote reading is implemented. ** The dataset is defined and provided exclusively manually by the field worker.

Description of the CIA triad assessment for each AMM dataset:

LP15—the LP15 dataset is characterized by "raw" data read from the measuring equipment. Its availability is not so important, as the availability is usually enough to get it up and running within a few days because it does not not billing values, but informative values. The only type of metering for which metering data are more important is C1 metering in the presence of electricity production at the point of consumption. Confidentiality is mandated by legislation for this asset in all cases; disclosing data could lead to a breach of GDPR and other laws. In unauthorized hands, they could be misused for commercial purposes. A breach of integrity could, in all cases, cause a reduction in the important interests of the DSO. In the case of a microgeneration or small-generation plant in C1 metering, problems could be created for the operation of the distribution system if a large number of load points are involved.

BW—in the case of meter readings, BW is a very important dataset, as it is a copy of the meter registers from which the data are subsequently used for billing. Therefore, a disruption in the availability of this asset should be resolved within hours, especially in cases where it is necessary to invoice the electricity consumed or generated based on the data. The difference is whether the unavailability of the information asset occurs at the middle of the month or at the end of the month, when it is a bigger problem. Confidentiality is mandated by law for this asset in all cases, as with LP15, and disclosure could also lead one to be in breach of GDPR and other laws. In unauthorized hands, data could be misused for commercial purposes. A breach of integrity on one information asset on one MP may not be such a problem for an organization. However, if an information asset is breached at thousands of sites, this can have serious implications for the functioning of the entire DS.

ODP—this dataset should not be unavailable for more than a few hours in most cases, because disconnection could occur, for example, due to the non-payment bound by binding deadlines from the trader, for which non-compliance is subject to high penalties. Fortunately, such remote disconnections are rare. Disclosure of this set of data could have fatal consequences for DS if published on many subscription sites. If information about the disconnection, its method, etc., were to fall into unauthorized hands, the security of the supply on the distribution system could be compromised, for example, by deliberately disconnecting a large number of customer sites from electricity. A breach of integrity in the case of this data file could lead to disconnection of unplanned MPs and consequently undermine confidence in the services of ČEZ Distribuce, a.s., and possibly lead to costly litigation.

PRIPO—this dataset should not be unavailable for more than a few hours in most cases, similarly to ODP, because the connection of the point of consumption is, for example, due to payment of the amount due, and this is determined by binding deadlines from the trader, where non-compliance carries high penalties. In addition, there could be complaints from the customer, who could claim damages from ČEZ Distribuce, a.s., based on the failure to connect on time. Fortunately, it is rare for such a variant of a site to be remotely connected, as in the case of ODP. Disclosure of this dataset could lead to fatal consequences for DS at many customer sites. If information about the connections, how they work, etc., were to fall into unauthorized hands, this could disrupt the security of the supply on the distribution system, for example, by the deliberately unplanned connection of a large number of customer sites to the network. However, in most cases, this would be a problem in combination with the disclosure of ODP information. A breach of integrity in this dataset could result in MPs that should have been connected not being connected. Subsequently, litigation against the owner of the MP could occur, but these cases would be rare.

TAR—this dataset should not be unavailable for more than an hour in most cases, because it is mainly used for the correction and connection of loads in the network. The dataset is mainly used to connect and disconnect electrical appliances in the network to ensure stability according to the electricity beign consumed or drawn. The only case where this does not occur is the C4 type of measurement where switching times are fixed using the TOU table. The disclosure of this dataset could have fatal consequences for DS in cases where it is disclosed at many load points. If information about the switching method were to fall into unauthorized hands, this could also lead to a disruption of supply security in the

distribution system, the deliberate unplanned connection of a large number of appliances, putting a strain on the distribution system and, as a consequence, blackouts could occur. A breach of integrity in the case of this dataset could result in the erroneous switching of appliances. This could lead to asymmetry in the network, excessive unplanned loading, and, in an extreme case, blackouts.

BLOCK—this dataset should not be unavailable for more than an hour in most cases, as is the case with TAR, as it is primarily used to control the active power output of power plants generating too much power on the grid. Therefore, its unavailability in case of a power surplus in the grid may cause the whole grid to fai. The disclosure of this dataset could have fatal consequences for the DS in cases where it is disclosed at many load points. If information about active power management method were to fall into unauthorized hands, the supply security in the distribution system could be compromised. Violations of dataset integrity could result in the mismanagement of active power at generators or microgenerators. This could lead to asymmetry in the network, excessive unplanned load on the network, and possibly blackouts.

LP60—this dataset is used in the case of measurement type C as information only. In the case of C1 metering, the production data can be used in the electricity market for spot prices. Confidentiality is mandated by law for this dataset in all cases; disclosure could be in breach of GDPR and other laws. In unauthorized hands, the data could be misused for commercial purposes. A breach of integrity could lead to the incorrect evaluation of some criteria in cases of C1 metering at generation plants; otherwise, a breach of integrity would have virtually no impact on the operation of the DS, although some customers might complain.

5.1. BIA Evaluation of the AMM System

The first step in establishing a BIA for an AMM system is to assess the risks in terms of availability, loss, disclosure, or errors in information from the single assets that sources or processes AMM data. The assessment was conducted through guided interviews with the sponsors of each dataset and validated against legislative and regulatory requirements. The results of the BIA from the perspective of the dataset sponsors are presented in Table 12. The input metrics were used as parameters to assess data unavailability, data loss, and data disclosure or modification from the perspective of the system user. The impact was classified according to the guidelines for risk classification from the BIA guidelines presented in Table 6, and the numerical expression corresponds to the indicated level of impact: 1—none; 2—low; 3—medium; 4—high; 5—critical. BIA evaluation metrics are presented in Table 10.

Table 12. BIA results from the perspective of the dataset sponsors.

Impact / Assets	30 M	2 H	12 H	24 H	2 D	1 W	1 WW	B 1	B 24	BW	BM	BALL	UDOUT	ER	ERL	ERD
BTS	1	2	3	3	4	4	5	1	1	1	1	1	3	1	4	5
DC	1	1	2	3	3	4	5	1	2	3	4	5	5	1	4	5
RVS	1	1	2	3	4	5	5	1	2	2	4	5	5	2	4	5
CS	1	1	1	1	2	2	3	1	1	2	3	4	5	1	2	3
EMO	1	2	3	3	3	4	4	1	1	2	3	3	5	2	4	5
AS	1	2	3	3	4	5	5	1	3	4	5	5	5	1	4	5
FA	1	1	2	2	2	3	4	1	1	2	2	3	3	1	3	4
MPC1	1	2	2	3	3	4	5	1	1	2	3	4	5	2	3	4
MPC2	1	1	2	2	3	4	5	1	1	2	3	4	5	2	3	4
MPC3	1	1	1	2	2	3	5	1	1	2	3	4	5	2	3	4
MPC4	1	1	1	1	2	3	4	1	1	1	2	4	5	2	3	4

Table 12 shows that short-term outages of up to 2 h in all parts of the system have no impact on the operation of ČEZ Distibuce, a.s. ČEZ Distibuce, a.s., will only run into major problems when various systems (assets) and applications are down for 2 h or more; of course, an outage of longer than a week has a critical impact on all systems and applications. This is mainly because Type C metering does not have the same priority as higher metering

types. The accounting system (AS) is the most sensitive system during an outage, and it is also a problem if the application used to send data to the Electricity Market Operator (EMO) is not working. Both ascetics have a medium impact on the company with as little as a 12-h outage. This is mainly because both systems are end-to-end, and it is less important when a linked system or application is not working because an alternative or temporary path can be integrated into the end-to-end systems to allow them work externally. Another reason is that, for example, the accounting system is operated by the largest number of employees, and all invoices and financial flows of the company are processed there; therefore, any system failure has a big impact on the economic functioning of ČEZ Distibuce, a.s. In the case of an application intended to be sent to EMO, medium impacts on the company can be communicated faster because there is a certain time limit for the transmission of data to OTE, and the penalties for non-compliance with the deadlines are fixed.

On the other hand, the customer system (CS) is only used to inform the customer and should never have more than a medium impact because customer registration in the system is voluntary and if the system drops out it will not affect all customers. For MPC1, the impact of an outage is worse over time, because it has more features that are used remotely and the distributor is required to place MPC1 at customer sites using electricity generation. OMC4 would be least impacted because there will be very few of these sites and they will probably be read at intervals of up to one year, like the existing C-type meters. As far as data loss is concerned, for all systems and applications, 1 h gap in backup will not threaten the organization much. The most problematic aspect is the accounting system (AS), which will have a medium impact on the operation of the company at 24 h. The only system that is not affected by a missing backup or data loss is BTS because no data are stored there and BTS only works to transfer information.

The biggest impact on data loss occurs in the Data Centre (DC) and the Reading and Validation System (RVS). If data from any of the systems are compromised, this could have a critical impact on all systems and applications in the company, except BTS and FA because the mobile operator in the form of BTS contains little information about the company's sensitive data. The risk of disclosure is also only moderate for FA field workers, as a field worker usually accesses the data of, at most, a few thousand people per year. In the context of error rate assessment, unit errors of system users or some anomalies in the system or application are not as much of a problem for ČEZ Distribuce, a.s. However, if there are system errors, the meters at the points of consumption and the field staff will have medium impacts, while the customer system (CS) has a rather low impact. Other systems are highly impacted by system errors. For deliberate errors, the impact on society ranges from high to critical in most systems and applications, as it can be assumed that such behaviors will always aim to cause as much harm to society as possible.

5.2. Risk Assessment by BIA Guidelines by Asset

5.2.1. BTS (BTS)

If continuous metering is installed on MP type C metering to the extent that it is gradually being built, remote readings will be taken at least at 95% of the sites and possibly more. Therefore, the mobile operator and its data transmission via BTS will be very important. Legal and contractual obligations are as folows: In case of a BTS failure or more, or, for example, if the operator carries out some modifications to the mobile network in a certain area and the meters stop being read as a result, there may be a violation of Decree No 359/2020 Coll., § 5, § 6, § 8 becausee the distributor would not fulfil the obligations of reading and timely transmission. In addition, there may be a breach of Decree No 540/2005 Coll., § 14, § 15, § 16, which provides for the quality of the service supplied. The number of such cases may range from hundreds of points of consumption to several thousand due to the expected installation of a larger number of meters with remote readings. The risk is, therefore, assessed as high. In a very extreme case, a violation of Act No 458/2000 Coll., Section 11 and Decree No 408/2015 Coll. Management and operation of the organization could occur: as the BTS outage of the mobile operator is an external

service, and so communication with external suppliers always takes longer than internal communication, there is also a form of uncertainty for the operator, as communication may not not be repaired in time for sites where legal deadlines need to be met. Cases where there is a communication outage with a large number of sites are very burdensome for the distributor. As it is assumed that large-scale outages cannot be covered by field staff and sending data by an alternative route, the risk of ČEZ Distribuce, a.s. is high. Loss of credibility is also a concern; in this case, it is considered that loss of credibility will be at an approximately medium level. The outage should never fully affect all the points of consumption on one BTS; furthermore, it is from an external supplier, and the impactwill be felt much more by the external entity than by ČEZ Distribuce, a.s., itself, which will not be fully responsible for the outage. In terms of financial loss/fisruption of activities, if we assume that an outage of services for some 1000 MP, which would require the loss of several BTS, according to the Czech Telecommunication Office, yhid eoulf numbrt about 16,000 for 4G networks throughout the Czech Republic. That works out to about 1 BTS per 60 users. ČEZ Distribuce, a.s., would be most vulnerable to this outage during the period at the beginning of the month, when it is necessary to provide data to EMO by a certain time. For Type C measurements, the same timeframes as for other continuous measurements will apply. Hence, data must be delivered within 7 working days, 18 h. If we assume that the problem would still occur in 1000 MP on the 7th working day after 18 h, then the penalty would be up to 300,000 €. Regarding the provision of essential services, if there is a communication outage due to problems in the mobile network, it should never affect more than a few thousand people, and this should only occur in a very limited number of cases. Following the experience of the pilot projects, such a large-scale outage can be expected once a year. In the area of critical service provision, this is rated as medium risk due to the small number of sites that will be affected. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 13.

Table 13. Asset BTS risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
High	High	Medium	High	High	2D	12 HRS	BM

5.2.2. Data Centre (DC)

Since, in the case of AMM metering, a huge amount of data will be stored in the data center, and these data are primarily important as a basis for electricity billing, it is important that there are as few missing data, preferably none, and that the service is as consistent as possible. *Legal and contractual obligations*: if there is an outage in the DCT, it will not be possible to carry out further processing of the real data, as the data will not be accessible. Therefore, such an outage will affect practically all applications, and there may be a violation of Decree No 359/2020 Coll. § 5, § 6, § 8, as the distributor could not fulfil the obligations regarding readings and their timely transmission. Furthermore, there may be a violation of Decree No. 540/2005 Coll., § 14, § 15, § 16, § 17, § 18, Act No. 458/2000 Coll., § 19, § 20 and Decree No. 408/2015 Coll. Again, however, this depends on the length of the outage and the state of the requirements in the systems of ČEZ Distribuce, a.s. If, however, a large loss of data was to occur as a result of damage to the DC, ČEZ Distribuce, a.s., could face huge problems, so this area must be assessed as critical. *Management and operation of the organization*: if the DC goes down, an organization like ČEZ Distribuce, a.s., could never provide data in an alternate way within an acceptable timeframe. The kind of fault in the DCT is also important, and whether data loss occurs. In terms of operations, this is probably the most delicate system, and can affect the operation of the entire company in certain cases. That is why the risk is identified as critical. *Loss of credibility*: in terms of loss of credibility, the DCT should be fully owned by ČEZ Distribuce, a.s., with only some parts managed by an external entity. Therefore, if there is a data breach or failure of the DC

involving a major outage, and ČEZ Distribuce, a.s., could not remedy this to a reasonable extent, there could be a critical loss of trust in the company for many years. *Financial loss/disruption of operations*: in financial terms, the financial loss could be astronomical if the worst were to happen, for example, a complete loss of data from the DC due to an accident or the loss of a large part of the data that could not be recovered. It is, therefore, not necessary to quantify the damage in this case, as the amounts could easily be billions of Euros. *Provision of essential services*: if the DC is down for a longer period than, for example, 1 h, the impact on the functioning of the whole organization would be quickly noticeable. If there is a large-scale outage or loss of data, millions of customers and power producers could be affected, so the aspect must be assessed as critical. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 14.

Table 14. Assets in data center: risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
High	Critical	Critical	Critical	Critical	1W	24 HRS	BW

5.2.3. Reading and Validation System (RVS)

The readout system performs data conversion and validation, so it is essential for this system that the DC is also operational. Without this, the RVS could not handle the data. *Legal and contractual obligations*: If the RVS fails, it will not be possible to subsequently provide data to other beneficiaries such as AS, EMO, and CS. Such an outage would affect virtually all downstream applications and may violate Decree 359/2020 §5, §6, §8 because the distributor could not meet its obligations to take readings and submit them promptly. Furthermore, there may be a violation of Decree No. 540/2005 Coll. § 14 § 15 § 16 § 17 § 18, Law No. 458/2000 Coll. § 19, § 20, and Decree No. 408/2015 Coll. Again, however, this depends on the length of the outage and the status of the requirements in the company's systems. However, if the outage were of a longer duration, this could have a strong impact on the company's operations. *Management and operation of the organization*: An outage or service limitation in the RVS can have a critical impact on the operation of the entire company. An alternate means of obtaining and verifying data to this extent is not possible. Therefore, care must be taken to get the application up and running as soon as possible. *Loss of credibility*: As far as loss of trust is concerned, everything is the same as in the case of DC, where the risk of loss of trust is critical because the application links directly to the DC, and its outputs flow to all relevant systems. Since the application is directly responsible for ČEZ Distribuce, a.s., its long-term non-functionality can have a substantial impact on the credibility of the whole company. *Financial loss/Disruption of operations*: There could be a breach of legal limits within billing or data transmission due to the application being non-functional for a prolonged period, for example, the first 7 days of the month. This could have a detrimental effect on the entire company, as compensation for the outage could go into the tens or maybe hundreds of billions of Euros. Therefore, the risk is rated as critical. *Provision of essential services*: An outage or service limitation at an RVS can affect almost all customers with Type C metering at any time, so this aspect must be rated as critical. Here, the length of the outage is also a major concern. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 15.

Table 15. Assets in reading and validation system risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
High	Critical	Critical	Critical	Critical	2D	24 HRS	BW

5.2.4. Customer System (CS)

This system can also only be operated in the form of an application; the data are provided to the customer for informational purposes only. *Legal and contractual obligations*:If continuous metering is implemented on the MP, the distributor is obliged to transfer the metering data to the customer according to Decree 359/2020 Coll. However, there is no penalty for violations of this Decree. *Management and operation of the organization*: This system is not completely central to the organization and its failure, even for a month, may not be dramatic for the company and its operation. *Loss of credibility*: An outage of this system can affect several thousand people, or, in some cases, tens of thousands of people. It is quite likely to damage the company's reputation, but not for long or in any fatal way. Therefore, there is a medium risk. *Financial loss/disruption of activities*: From this point of view, it is not certain whether there would be any sanctions from any customer on ČEZ Distribuce, a.s., due to the non-functionality of this system. However, any sanctions would probably be of a negligible amount. Therefore, the risk ranges from low to very low. *Provision of essential services*: In terms of service provisioning, tens of thousands of people may be affected by an outage of this service, but these are services that are not essential to the customer. Therefore, the risk is medium due to the number of customers affected by the outage. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 16.

Table 16. Assets in customer system risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
Medium	Low	Medium	Low	Medium	1WW	1WW	BM

5.2.5. Interface for Sending Data to EMO

This interface/application is the communication channel associated with the EMO, through which the LP60 data from the AMM measurement flow. For analysis, we consider only this function, as other information from billing, etc., flows directly from the AS. *Legal and contractual obligations*: If there is an EMO outage, it will not be possible to send real data because the OTE will not have access to them; therefore, such an outage will only affect non-compliance with § 5, § 6, § 7 of the Act No. 359/2020 Coll. because the distributor could not fulfil the obligations of timely transmission. Furthermore, there may be a violation of Decree No. 408/2015 Coll. However, again, this depends on the length of the outage and the status of the requirements in ČEZ Distribuce, a.s.'s systems. In terms of legal obligations, there is a roughly medium risk of non-compliance with legal obligations for this application for Metering Type C. *Management and operation of the organization*: The operation of this application does not have much impact on the operation of the organization because it is one of many specific applications within ČEZ Distribuce, a.s. The overall problem is that there is no way to replace this application without burdening the operation itself. *Loss of credibility*: In terms of loss of credibility, the risk is assessed as high because it involves communication with an external entity that is strategically important to the company. Furthermore, LP60 is sent from Type C metering through this application to evaluate the generation plants. *Financial loss/disruption of activities*: The financial loss in this case is similar to the calculation from the point dedicated to RVS. The required compensation, therefore, falls into the high category. *Provision of essential services*: With the dynamic development of micro-metering installations and the gradual expansion of AMM metering, a system outage or service limitation can affect more than 100,000 people. Therefore, this aspect is rated as high. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 17.

Table 17. Assets for the interface for sending data to EMO risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
Medium	Medium	High	High	High	2D	12 HRS	BM

5.2.6. Accounting System (AS)

This is a system in which everything is accounted for and contractually evaluated, and all personal data about customers are stored here. This is why it is one of the most sensitive systems. *Legal and contractual obligations*: If there is an AS outage, it will not be possible to subsequently bill customers for their electricity consumption, transmit billing data to EMO, handle disconnections and claims, or handle complaints. Such an outage will affect the vast majority of activities and may result in a violation of Decree 359/2020 Coll. because the distributor could not meet its obligations to transmit billing data promptly. Furthermore, Decree No. 540/2005 Coll. may be violated in almost all respects, as well as Law No. 458/2000 Coll. and Decree No. 408/2015 Coll. Again, however, this depends on the length of the outage and the status of the requirements in the US. However, if there is a system outage for an extended period, this could have a high impact on the company in terms of claims for financial damages. *Management and operation of the organization*: If there is a widespread outage of the AS, it could also halt the ability to take readings in the field, as readings requests would stop coming in, and there would be nowhere to send billing data. Most of the systems connected to the AS could stop working until everything is back up and running. Therefore, I would rate the risk associated with an outage as critical. *Loss of credibility*: There is a high risk of loss of credibility in a large-scale AS outage, as the outage would affect the operations of a large part of the business as well as customers; for this reason, the impact is rated as high. *Financial loss/Disruption to operations*: The financial loss does not need to be quantified here, as it could be astronomical in the extreme case of compensation payments; therefore, the the risk of impact is critical. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 18.

Table 18. Assets in accounting system risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
High	Critical	Critical	Critical	Critical	12 HRS	2D	B24

5.2.7. Field Worker Equipment (FWE)

For field worker performance, the designated field worker must receive work orders on his/her FWE on time. The field worker mainly handles the readings for sites with a C4 type of metering and also handles the reports of all MPs, including remediation in case of communication failure. *Statutory and contractual duties*: If there is an outage in the system associated with FWE, it will not be possible to bill the operational requirements in the field efficiently and there will be a violation of Decree No. 540/2005 Coll. The violation of other decrees would only occur in a few cases or in highly extreme cases, such as Decree No. 458/2000 Coll. and Decree No. 408/2015 Coll. *Management and operation of the organization*: In the event of a major outage of the FWE system, there would also be a deterioration in efficiency in the management of field workers, as well as the possibility of the incorrect handling of some requests that would have to be sent to field workers by an alternative route. However, fieldwork would not be as constrained due to the system's non-functionality. The impacts on ČEZ Distribuce, a.s., should not be more than moderate. *Loss of credibility*: If there is a widespread FWE outage, there could be a medium impact on

the organization. However, as this is a day-to-day activity that will affect certain isolated locations, trust in ČEZ Distribuce, a.s., will not suffer that much. *Financial loss/Disruption of activities*: Financial losses may only arise in the event of legal action due to financial harm to the customer or non-compliance with ordinances, but this should not exceed tens of millions of crowns, and these costs would only occur in extreme cases. However, this would put more strain on the company's operations and certain inefficiencies would result in increased costs. *Provision of essential services*: If a system outage or unavailability lasted for several days or even a week, it could affect, at most, several tens of thousands of people across the entire distribution territory of ČEZ Distribuce, a.s. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 19.

Table 19. Assets in field worker equipment risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
Medium	Medium	Medium	Medium	Medium	1WW	1W	BW

5.2.8. Measuring Point C1 (MPC1)

The continuous measurement category C1 with remote communication can be remotely limited or disconnected and the tariff control can also be controlled remotely. In case of communication failure, a field worker is sent to the site. Of all the C-type meters, safety is particularly important in this type of meter. *Legal and contractual obligations*: If MPC1 fails, it will not be possible to remotely read the electricity at MP, nor will it be possible to disconnect, connect and control the active power. If this happens at the wrong time at many sites, it may violate Decree No. 359/2020 Coll., No. 540/2005 Coll., as well as Act No. 458/2000 Coll. And Decree No. 408/2015 Coll. If the distributor does not control the load and generation at these customer sites, it could cause significant damage to the distribution network, and thus violate all standards of safe supply. Therefore, the risk is set as high. *Management and operation of the organization*: The management and operation of the organization could be significantly affected by the outage of several thousand sites as the company would not be able to remedy the situation on the ground with its forces. Depending on the nature and length of the outage, in extreme cases, there could be a significant impact on operations. *Loss of credibility*: As far as this aspect is concerned, a possible outage of the network due to its inability to be managed on OMs such as micro-sources could also have a large media impact because the security of electricity supply in some areas could be disrupted. Hence, the risk is high. *Financial loss/Disruption of activities*: There could only be a large financial loss if there is a communication failure involving several thousand sites at a time when power generation needs to be regulated. Unfortunately, it is not possible to precisely quantify the amount, but it could be worth several billion in the event of litigation. Therefore, the risk of impact is determined to be high. *Provision of essential services*: If an outage or disruption in communications with the generating plants causes the grid to crash, 100,000 people could be without power that morning. Therefore, the risk was rated as high. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 20.

Table 20. Asset at measuring point C1 risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
High	High	High	High	High	1W	24HRS	BM

5.2.9. Measuring Point C2 (MPC2)

In the case of continuous metering category C2 with remote communication, it is possible to remotely read and control the tariff control. In case of communication failure, a field worker is sent to the site. Of the Type C meters, this is one of the most numerous groups. *Legal and contractual obligations*: If the MPC2 fails, it will not be possible to remotely read the electricity at the OM; furthermore, the switching time will not be observed. If this happens at the wrong time, for many sites, there may be a violation of Decree No. 359/2020 Coll., No. 540/2005 Coll., Act No. 458/2000 Coll. and Decree No. 408/2015 Coll. If the distributor does not control the load at these customer sites, it could cause significant damage to the distribution network and thus violate all standards of safe supply. Therefore, the risk is set as high. *Management and operation of the organization*: A large-scale communication failure could have a major impact on the management and operation of the organization as tens of thousands of sites could be affected because the company would not be able to remedy the situation on the ground. Depending on the nature of the outage and the length, in extreme cases, there could be a substantial impact on operations. *Loss of credibility*: As far as this aspect is concerned, the potential failure of the network is due to its inability to be managed by the MP with blocked appliances. This could also have a large media impact because the security of electricity supply in some areas could be disrupted. For this reason, the risk is high. *Financial loss/Disruption of activities*: A large financial loss could only occur if there is a communication failure involving several thousand sites at a time when it is necessary to control loads by unplugging or switching on blocked appliances. Unfortunately, the amount cannot be precisely quantified, but could exceed several billion in the event of litigation. Therefore, the risk of impact is determined to be high. *Provision of essential services*: In terms of the number of points of consumption, this is the largest type of metering, so a significant impact on society can be expected in the event of a major communications outage in the form of unavailable services. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 21.

Table 21. Assets in measuring point C2 risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
High	High	High	High	High	1W	2D	BM

5.2.10. Measuring Point C3 (MPC3)

In the case of a Category C3, continuous measurement with remote communication, the MP can be read remotely, and in the event of communication failure, a field worker is sent to the site. Of the Type C metering, this is one of the most numerous groups of electricity meters. *Legal and contractual obligations*: If there is an MPC3 failure, it will not be possible to remotely read the MP. If this happens at the wrong time for many sites, there may be a violation of Decree No. 359/2020 Coll., and No. 540/2005 Coll., as well as Act No. 458/2000 Coll. and Decree No. 408/2015 Coll. Therefore, the risk is set as high. *Management and operation of the organization*: A large-scale communication failure could have a major impact on the management and operation of the organization, as tens of thousands of sites could be affected because the company would not be able to remediate the situation on the grounds. Depending on the nature of the outage and the length, in extreme cases, there could be a substantial impact on operations. *Loss of credibility*: Regarding this aspect, a possible communication outage with a large number of meters at MP could have a medium impact. A few tens of thousands of customers could have their bills delayed, meaning that it would not have such a heavy impact on the company's reputation. *Financial loss/Disruption to operations*: Major financial loss could only occur if communication with tens of thousands of sites is interrupted at the time of billing, when billing for consumption would be required and data must be sent to EMO. Unfortunately, the amount cannot be precisely quantified

but could exceed several million crowns in the event of litigation. Therefore, the risk of impact is assessed as medium. *Provision of essential services*: This is the second largest type of metering in terms of the number of points of consumption, so only a medium impact on the company in terms of unavailability of services to customers can be expected in the event of a major communication failure. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 22.

Table 22. Assets in measuring point C3 risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
High	High	Medium	Medium	Medium	>1WW	2W	BM

5.2.11. Measuring Point C4 (MPC4)

For Category C4 measurements with possible long-distance communication, the MP can be read remotely. In most cases, it will be read by a worker in the field. In the event of a communication failure for the few sites that will be remotely read, a field worker will be sent to the site. Of the Type C meters, this is one of the least represented groups of electricity meters. *Legal and contractual obligations*: For MPC44, field reading should occur once a year, and thus there would be limited violations of Decree No. 359/2020 and Decree No. 540/2005, as well as Law No. 458/2000 and Decree No. 408/2015. Therefore, the risk is set as low. *Management and operation of the organization*: The management and operation of the organization would not be significantly affected by a large-scale communication failure, as only a small percentage of consumption points would be remotely read. The only thing that could affect the management and operation at ČEZ Distribuce, a.s., is an outage of other customer sites. This could mean that the meter readings would not be completed in time. Therefore, the risk of impact is rated as medium. *Loss of credibility*: The only impact on loss of confidence could be a delay in bills due to late readings. However, this would only affect a small number of MPs; therefore, the credibility of the company would not suffer. Therefore, the risk is low. *Financial loss/disruption to operations*: In this case, only a small financial loss could occur, as this is a small group of OMs. Therefore, the risk is low. *Provision of essential services*: This is the least numerous type of metering in terms of the number of consumption points; therefore, only a low impact on society can be expected in the event of a large-scale communication failure in the form of unavailable services. A comprehensive assessment of the risks and parameters of data availability and maturity is presented in Table 23.

Table 23. Assets in measuring point C4 risk rating.

Legal and Contractual Obligations	Management and Operation of the Organization	Loss of Credibility	Financial Loss/Disruption of Activities	Provision of Essential Services	MTPD	MIDP	MTDL
Low	Medium	Low	Low	Low	1WW	1W	-

6. Discussion

The above analysis identifies the maximum impact of potential risks on an organization providing statutorily defined electricity distribution services. These risks and their associated impacts will take on defined values unless mitigation measures are properly defined and implemented to ensure the most trouble-free operation of the entire metering system and reliable of supply throughout the distribution system in the distribution territory of ČEZ Distribuce, a.s. The BIA analysis shows that the most vulnerable systems are the data center (DC), accounting system (AS), and readout and validation system (RVS), where any major outage or limitations of a few days can have a huge impact on the operation of

ČEZ Distribuce, a.s. The first measure to be addressed is the Data Centre (DC), where one of the basic measures that should be addressed is accessibility. Since hundreds of thousands of users will access the DC daily through different systems, it is necessary to define forms of access that should only take place within the internal network. Furthermore, there is a need to properly define the users who will be able to access the data in the DC in advance, as well as their access keys. Furthermore, this system should be completely independent of the others and should run a full backup of the data, which should also be completely separate from the main DC system, as described in the BIA results. In this system, the main focus must be on the backup of data, as these data are central to the company and must be restored as quickly as possible if necessary. The analysis shows that the maximum length of data loss that can be tolerated is a week, so it would be advisable to set the data backup to 24 h. The next critically vulnerable system is the Readout and Validation System (RVS). Data from the DC enter this system; therefore, the communication between these systems must be secured as best as possible using long-life encryption. The RVS should also be fully decoupled from other systems and access should be handled similarly to the DC. This system stores the basic identification data of the subscriber points, which allows it to access specific data in the DC. In the RVS system, the analysis suggests that the backup should be set for one week, which would provide sufficient time. Furthermore, it would be useful to have an entire backup system in place that could temporarily perform some important tasks until the main RVS system is made operational again. The last of the critical systems is the accounting system. This is a highly complicated system, as it will probably be accessed by most other systems, applications, and users. Therefore, it is also necessary that the system is only accessed within the company network, encrypted and, if possible, only accessed within defined user roles. Furthermore, it is extremely important that, if there is an outage, it is brought back into operation as quickly as possible. According to the analysis, a backup every 24 h should be sufficient. Here, again, it would be advisable to set up a backup system that can continue to function in the event of failure of the main system. Customer data should be stored away from the system and protected by state-of-the-art encryption for maximum security. For other systems and applications, communication should always be secure, and preferably take place on an internal network, and security packages should be updated regularly. It is also advisable to regularly adjust the security policy of the entire organization according to need, and to focus on regular audits both internally and with external vendors, to ensure the most secure and reliable operation of the company. Last but not least, it is necessary to strictly ensure the reliability of external service providers in contracts and to define the legal consequences for non-compliance with standards and contractual conditions.

In terms of the importance of datasets based on the classification of confidentiality, availability, and integrity, the most important assets for the AMM system and, consequently, for ČEZ Distribuce, a.s., itself and the services provided by it were identified as the data sets of the meter register (BW), as well as the messages used for the management of meter functions, such as the disconnection message (ODP), connection message (PRIPO), appliance blocking message (TAR) and the active power management message (BLOCK). Of these datasets, and given their packet impact, it is arguably most important that the transmission of BLOCK information is as secure as possible, as this is the tool by which the distributor ensures the stability of the entire network in real-time. There is another network management tool, namely TAR, where blocked appliances are switched on or off, in line with the very logic of AMM as a sub-solution of the Smart Grid concept. All datasets that are in any way related to meter control should be encrypted according to the current recommendations of the National Cyber and Information Security Bureau (NCISB). Subsequently, if these datasets are used for meter access, a separate set of keys should be issued for each meter, which will be encrypted in turn according to the standards and defined by the type of meter access, data reading, rate setting adjustment, disconnect or appliance lockout, or active power control. Communication of this information should be encrypted and only occur within the internal network. Where data from meters such as

PL15 and BW are involved, access should be password-protected. It should not be possible under any circumstances to overwrite the data in the meter remotely. If communication at the point of consumption is carried out by a KMZ field worker, then access to the meter should be password-protected. The KMZ worker should only work on the internal network. All communications with systems should be encrypted. The AMM datasets should be protected in a similar way to the systems in ČEZ Distribuce, a.s.; their security policies should be in line with current NUKIB and ISO 27001 recommendations and should be regularly updated.

7. Conclusions

As identified in the introductory section of this article, the issue of ensuring the cyber security of a complex AMM system is influenced by several factors. First and foremost is the fulfillment of legislative requirements, as electricity distribution is a regulated business. It is important to note that these requirements not only focus on the area of security, but also include energy legislation, both at national and international levels. This involves, among other things, the provision of a range of datasets whose inconsistencies, unavailability, or compromised integrity can have significant impacts on the entire distribution system. It is this unique perspective, which requires a combination of knowledge of security and energy legislation, process and data communication, technical principles of the AMM system, and security standards and technologies, that comes together in the presented case study dealing with the BIA of the AMM system. Why BIA? In addition to the above legislative and logical technological principles and constraints, power distribution and its management is a significant business regionally, nationally, and internationally. The responsibly developed BIA, including the classification of assets (datasets), the design and evaluation of the most significant risks, and the subsequent design of basic measures, which can be selected from corporate security baselines or security documentation from NIS or ENISA, forms a uniquely comprehensive view of the cybersecurity of the AMM system. The currently issues addressed in the cited literature deal with sub-problems and proposals from a technical or process perspective. However, these are simplified conceptual models that contain only one perspective at any given time. The necessary and unique link between the process and technology worlds, for which BIA was chosen as the basis, was, is, and always will be part of the input analysis for classification and impact analysis, based on which appropriate technological and process measures can be chosen. These should then be selected from the security baselines developed for specific environment and company processes. These insights and system then enable cost-optimization for cybersecurity and, in particular, can simplify and streamline risk management for technical assets, including vulnerability monitoring systems.

We now summarize the main contributions of the article. First of all, a technical analysis of the data in the AMM system was performed, based on which a Dataset flow diagram was created based on the principles of the BPMN model. The individual datasets were analyzed in detail, with an emphasis on their interrelationships.

The CIA criteria for evaluating the quality and significance of individual datasets in AMM were determined, and the types and classifications of risks specific to the complex AMM system were proposed according to the rules and principles of BIA. The criteria for the availability of uniform services in the form of basic availability and recovery parameters for MTPD, MIPD, and MTDL were established and justified. Subsequently, BIA evaluation metrics were established. The homogeneous datasets were then classified, and their classification was justified in detail in terms of their business impact, their interdependencies, and their relevance to the whole AMM system as part of the Smart Grid, and in their overall context as part of the Smart City type intelligence systems.

The results can be summarized concerning the above BIA outputs and the high level of requirements for data quality assurance and security in the AMM system, where it is necessary to ensure that the individual systems meet the organizational and technical

measures. These can be specified regarding the technological capabilities of the sub-meters and transmission paths for the so-called minimum cryptographic requirements, as follows:

- Confidentiality: use of the AES-256 block cipher.
- Ensuring confidentiality and integrity: use of GCM, and CCM block ciphers.
- Integrity assurance: digital signature DSA 3072, EC-DSA-25, RSA 3072
- Hashing: SHA2-256, SHA3-256
- Integrity protection mode: HMAC, CMAC
- Key Management: DH-3072, ECDH-256
- Random bit generator: for SHA2 and SHA3: HMAC DRBG, Hash DRBG.

Therefore, the resulting technical requirements must:

- Ensure safe recovery from error, fault, or failure.
- Include a reliable time synchronization.
- Include instructions for safe installation.
- Supply initialization and operation with the equipment.
- Ensure data validation before use—input protection.
- Ensure flood (DoS) protection through traffic filtering or network segmentation,
- resource management.
- Minimize the interface—disabling all unnecessary services, protocols, and physical interfaces.
- Log and report security events.

Furthermore, each device must be uniquely identifiable. Data in messages must be encrypted and messages must contain integrity protection. Systems should be implemented to confirm the execution of a command. Access to elements handling sensitive data should require the penetration of a sealed security perimeter. Cryptographic credentials should be unique to the meter and securely stored. If stolen, this should not reduce the security of another meter.

In terms of the architecture of the meter itself, the measurement and communication functions should be separated, with the remote updating of security functions and cryptographic primitives, and the remote updating of cryptographic credentials.

If these minimum cryptographic and technical requirements are met, the implemented BIA can be expected, with a high degree of probability, to ensure adequate quality and availability in AMM data, and should be usable for secure and stable smart grid operation.

Future research on the safety of AMM system implementation can be divided into technical and organizational measures. The focus of this research project was data modeling using BPMN_SC security distributions, analyzing the impacts of not guaranteeing the quality and security of AMM system data on other ICT and ICS systems involved in the Smart City concept. This is a dynamically evolving area, where the quality, security, and availability of data from the energetic networks have a profound impact on the downstream cooperating areas and systems that comprise the Smart City concept.

Funding: This work and paper were supported by the project "Application of Artificial Intelligence for Ensuring Cyber Security in Smart City", n. VJ02010016, provided by the Ministry of the Interior of the Czech Republic.

Data Availability Statement: Data sharing is not applicable.

Acknowledgments: I would like to thank my colleague R. Werner et al., from ČEZ Distribuce, a. s., for his cooperation in the analysis of data flows in the real AMM system environment.

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

References

1. Bhatia, H.; Hoang, D.; Morrical, N.; Pascucci, V.; Bremer, P.-T.; Lindstrom, P. AMM: Adaptive Multilinear Meshes. *IEEE Trans. Vis. Comput. Graph.* **2022**, *28*, 2350–2363. [CrossRef]
2. Sun, C.; Xu, H.; Wan, D.; Li, Y. Building Information Modeling Application Maturity Model (BIM-AMM) from the Viewpoint of Construction Project. *Adv. Civ. Eng.* **2021**, *2021*, 6684031. [CrossRef]

3. Miao, Y.; Stauff, N.; Bhattacharya, S.; Yacout, A.; Kim, T.K. *Advanced Moderation Module for High-Temperature Micro-Reactor Applications*; Argonne National Lab. (ANL): Argonne, IL, USA, 2020. [CrossRef]
4. Directive 2019/944 of the European Parliament and of the Council of 5 June 2019 on Common Rules for the Internal Market for Electricity. Official Journal of the European Union L 158/125. Available online: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32019L0944 (accessed on 5 February 2023).
5. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for Industrial Control Systems: A Survey. *Comput. Secur.* **2020**, *89*, 101677. [CrossRef]
6. Aldairi, A.; Tawalbeh, L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Comput. Sci.* **2017**, *109*, 1086–1091. [CrossRef]
7. Ismagilova, E.; Hughes, L.; Rana, N.P.; Dwivedi, Y.K. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Inf. Syst. Front.* **2022**, *24*, 393–414. [CrossRef]
8. Yigitcanlar, T.; Desouza, K.C.; Butler, L.; Roozkhosh, F. Contributions and Risks of Artificial Intelligence (AI) in Building Smarter Cities: Insights from a Systematic Review of the Literature. *Energies* **2020**, *13*, 1473. [CrossRef]
9. Nishant, R.; Kennedy, M.; Corbett, J. Artificial Intelligence for Sustainability: Challenges, Opportunities, and a Research Agenda. *Int. J. Inf. Manag.* **2020**, *53*, 102104. [CrossRef]
10. *ISO/IEC 27001:2023*; Information Technology—Security Techniques—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2023.
11. Antunes, M.; Maximiano, M.; Gomes, R. A Client-Centered Information Security and Cybersecurity Auditing Framework. *Appl. Sci.* **2022**, *12*, 4102. [CrossRef]
12. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. [CrossRef]
13. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the Context of Industry 4.0: A Structured Classification of Critical Assets and Business Impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
14. Oliveira, J.; Carvalho, G.; Cabral, B.; Bernardino, J. Failure Mode and Effect Analysis for Cyber-Physical Systems. *Future Internet* **2020**, *12*, 205. [CrossRef]
15. Corallo, A.; Lazoi, M.; Lezzi, M.; Pontrandolfo, P. Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. *IEEE Trans. Eng. Manag.* **2023**, *70*, 3745–3765. [CrossRef]
16. Mullet, V.; Sondi, P.; Ramat, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [CrossRef]
17. Chehri, A.; Fofana, I.; Yang, X. Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability* **2021**, *13*, 3196. [CrossRef]
18. Razikin, K.; Soewito, B. Cybersecurity Decision Support Model to Designing Information Technology Security System Based on Risk Analysis and Cybersecurity Framework. *Egypt. Inform. J.* **2022**, *23*, 383–404. [CrossRef]
19. Syed, N.F.; Shah, S.W.; Trujillo-Rasua, R.; Doss, R. Traceability in Supply Chains: A Cybersecurity Analysis. *Comput. Secur.* **2022**, *112*, 102536. [CrossRef]
20. Kitsios, F.; Chatzidimitriou, E.; Kamariotou, M. Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability* **2022**, *14*, 1269. [CrossRef]
21. Sobeslav, V.; Horalek, J.; Svoboda, T.; Svecova, H. Security Consideration of BIA Utilization in Smart Electricity Metering Systems. In *Computational Collective Intelligence: Proceedings of the 14th International Conference, ICCCI 2022, Hammamet, Tunisia, 28–30 September 2022*; Springer International Publishing: Cham, Switzerland, 2022; pp. 585–597.
22. Philips, A.; Jayakumar, J.; Lydia, M. A Review on Cyber Security in Metering Infrastructure of Smart Grids. In *Computational Methods and Data Engineering*; Singh, V., Asari, V., Kumar, S., Patel, R., Eds.; Advances in Intelligent Systems and Computing; Springer: Singapore, 2021; Volume 1227. [CrossRef]
23. Gunduz, M.Z.; Das, R. Cyber-Security on Smart Grid: Threats and Potential Solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
24. Qiu, W.; Tang, Q.; Wang, Y.; Zhan, L.; Liu, Y.; Yao, W. Multi-View Convolutional Neural Network for Data Spoofing Cyber-Attack Detection in Distribution Synchrophasors. *IEEE Trans. Smart Grid* **2020**, *11*, 3457–3468. [CrossRef]
25. Sun, C.-C.; Sebastian Cardenas, D.J.; Hahn, A.; Liu, C.-C. Intrusion Detection for Cybersecurity of Smart Meters. *IEEE Trans. Smart Grid* **2021**, *12*, 612–622. [CrossRef]
26. Kawoosa, A.I.; Prashar, D. A Review of Cyber Securities in Smart Grid Technology. In Proceedings of the 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 19–21 January 2021; pp. 151–156. [CrossRef]
27. Lee, D.; Hess, D.J. Data Privacy and Residential Smart Meters: Comparative Analysis and Harmonization Potential. *Util. Policy* **2021**, *70*, 101188. [CrossRef]
28. Singh, N.K.; Mahajan, V. End-User Privacy Protection Scheme from Cyber Intrusion in Smart Grid Advanced Metering Infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100410. [CrossRef]
29. Orlando, M.; Patti, E.; Acquaviva, A.; Macii, E.; Osello, A.; Rietto, L. A Smart Meter Infrastructure for Smart Grid IoT Applications. *IEEE Internet Things J.* **2022**, *9*, 12529–12541. [CrossRef]
30. Hasan, M.K.; Habib, A.A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, M.A. Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations. *J. Netw. Comput. Appl.* **2023**, *209*, 103540. [CrossRef]

31. Ustun, T.S.; Hussain, S.M.S.; Ulutas, A.; Onen, A.; Roomi, M.M.; Mashima, D. Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages. *Symmetry* **2021**, *13*, 826. [CrossRef]
32. Slacik, J.; Mlynek, P.; Rusz, M.; Musil, P.; Benesl, L.; Ptacek, M. Broadband Power Line Communication for Integration of Energy Sensors within a Smart City Ecosystem. *Sensors* **2021**, *21*, 3402. [CrossRef]
33. Xia, X.; Xiao, Y.; Liang, W.; Cui, J. Detection Methods in Smart Meters for Electricity Thefts: A Survey. *Proc. IEEE* **2022**, *110*, 273–319. [CrossRef]
34. Vitiello, S.; Andreadou, N.; Ardelean, M.; Fulli, G. Smart Metering Roll-Out in Europe: Where Do We Stand? Cost Benefit Analyses in the Clean Energy Package and Research Trends in the Green Deal. *Energies* **2022**, *15*, 2340. [CrossRef]
35. Ben Youssef, N.E.H. Analytical Analysis of Information-Centric Networking in Smart Grids. *Int. J. Wirel. Inf. Netw.* **2022**, *29*, 354–364. [CrossRef]
36. Kohout, D.; Lieskovan, T.; Mlynek, P. Smart Metering Cybersecurity—Requirements, Methodology, and Testing. *Sensors* **2023**, *23*, 4043. [CrossRef]
37. Kim, H.; Choi, J. Intelligent Access Control Design for Security Context Awareness in Smart Grid. *Sustainability* **2021**, *13*, 4124. [CrossRef]
38. Energy Regulatory Office ERU. *Act No. 458/2000 Coll. on the Conditions of Business and the Exercise of State Administration in the Energy Sectors and on Amendments to Certain Acts*; ERU: Prague, Czech Republic, 2000.
39. Ministry of Industry and Trade MPO. *Decree No. 359/2020 Coll. on Electricity Metering*; Ministry of Industry and Trade MPO: Prague, Czech Republic, 2020.
40. *Decree No. 82/2011 Coll. on the Conditions of Electricity Metering and the Method of Determining Compensation for Damages in the Event of Unauthorised Consumption, Unauthorised Supply, Unauthorised Transmission or Unauthorised Distribution of Electricity*; Ministry of Industry and Trade: Prague, Czech Republic, 2011.
41. ERU Energy Regulatory Office. *Decree No. 540/2005 Coll. on the Quality of Electricity Supply and Related Services in the Electricity Sector*; ERU Energy Regulatory Office: Prague, Czech Republic, 2005.
42. Energy Regulatory Office ERU. *Decree No. 408/2015 Coll. on Electricity Market Rules*; Energy Regulatory Office ERU: Prague, Czech Republic, 2015.