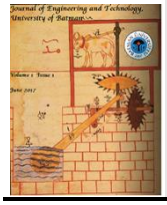
Journal of Engineering and Technology

2024 - Volume: 5 Issue: 1

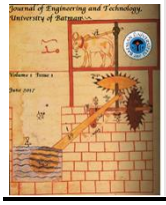
e-ISSN: 2619-9483



Journal of Engineering and Technology
DergiPark
AKADEMİK

BATMAN ÜNİVERSİTESİ 2007

Journal of Engineering and Technology 5;1 (2024)



Journal of Engineering and Technology
DergiPark
AKADEMİK

Journal of Engineering and Tecnology 5;1 (2024) 1-10

Placement of Optimum Supercapacitors Considering Cost and Loss Parameters in Reliability-based Sustainable Energy-Based Grid

[a]Merve Celik, [b]Davut Sevim

[a,b]Batman University, Faculty of Engineering, Department of Electrical and Electronics Engineering, BATMAN/TURKEY

[a] mervecelik.2197@gmail.com

ARTICLE INFO

Article history:
Received June 1, 2024
Accepted June 24, 2024
Available online June 26, 2024

Key words:
Super Capacitors
Sustainable Energy
Reliability
Cost-benefit analysis

* Corresponding author.
E-mail address:
merveclk.2197@gmail.com

ABSTRACT

This study aims to develop a method for low-cost production in power systems by analyzing key parameters such as production costs, line losses, and reliability within the contexts of production planning and load distribution processes. By taking these parameters into account, the goal is to enhance the system's sustainability and efficiency. System reliability refers to the ability of a system to perform a specified task within a given time frame. Reliability-based risk analysis is employed to assess the reliability of critical system components. Unit Commitment (UC) involves the optimal allocation of energy production units while considering production costs, line losses, and reliability factors. The amount of supercapacitors is determined by evaluating the reliability of system components, production costs, and losses. Supercapacitors are utilized in energy systems to prevent imbalances between supply and demand and are allocated to be equal to or greater than the capacity of the largest generator. Cost-benefit analysis is conducted to determine the optimal level of supercapacitors. The objective of this study is to achieve low-cost and sustainable energy production in power systems through a comprehensive analysis of production costs, line losses, and reliability parameters. The focus is on the efficient allocation of energy production units and conducting reliability-based risk analyses to achieve an optimal production balance..

1. Introduction

Meeting the connection criteria to generate and distribute sustainable and uninterrupted electricity to meet demand contributes to supply reliability. Ensuring compliance with the connection criteria of ENTSO-E (European Network of Transmission System Operators for Electricity) is essential for supply reliability. Supply reliability is also crucial for maintaining the quality of electrical energy. It is critical for ensuring that the power balance and system frequency remain within acceptable ranges, providing high-quality energy through frequency control. Common goals for the reconfiguration of distribution systems include minimizing transmission losses and/or enhancing reliability and optimal planning [1, 2]. This study presents the best combination of feeder-based units for reconfiguring storage planning in distribution systems, which is a combinatorial optimization problem that minimizes the objective function. Constraints used in this process include planning constraints for units with maximum and minimum storage capacity, line losses, and line reliability [3, 4].

The concept of reliability is generally defined as the probability that a device or system will fulfill its intended purpose under specified conditions within a certain period. This definition includes several key elements. First, reliability is a probabilistic concept, meaning it deals with the likelihood of a device or system performing its intended purpose under specific conditions at a given time [5]. Second, the concept of reliability encompasses adequate performance. For a device or system to be considered reliable, the probability of fulfilling its intended purpose must be high, indicating the importance of the device's or system's capacity to perform as expected. Third, reliability involves time. To evaluate the reliability of a device or system, the probability of it fulfilling its intended purpose over a specified period must be considered. This period is usually expressed as the lifetime of the device or a particular operational period. Finally, the concept of reliability includes operating conditions. The reliability of a device or system is assessed under specific operating conditions, which may include the characteristics of the environment in which the device is used, the frequency of use, and other factors [6]. The evaluation of these elements together determines the reliability of a device or system, playing a crucial role in its design, production, and use. Overall, reliability determines a system's ability to perform its function, aided by load changes and historical experience that help predict future performance [7]. The indices used in reliability evaluation are probabilistic and thus do not provide precise predictions. To conduct a reliability, the system's behavior in the previous period must first be known. During the analysis, various variables that can measure reliability are identified and then calculated using different methods. All these methods involve detailed examination of the future behaviors of the units [8]. The definition of reliability in electric power systems is commonly made in terms of adequacy and security [9, 10]. Adequacy refers to ensuring that all needs arising from generation, transmission, and distribution facilities are met and that demand is satisfied, taking into account planned and unplanned outages of system components. After unexpected events, the system is considered to have reached a stable point concerning transitions from one state to another without neglecting any dynamics [11]. Security refers to a system's ability to withstand failures and disruptions caused by outages of cables, transmission lines, generators, and many other components. Security analysis evaluates the system's transient response after contingency events and considers any progressive incidents arising from transient fluctuations [12].

2. Stages of Power Systems in Reliability Analysis by Function

Electric power systems are examined by dividing them into generation, transmission, and distribution regions based on functionality. These three fundamental regions contribute to the complex structure of power systems. Each region has its specific reliability indices used to evaluate the robustness and continuity of the system. The different reliability characteristics of the generation, transmission, and distribution regions necessitate a detailed approach to reliability analyses. In this context, a staged analysis should be applied to assess the reliability of the power system [13]. The first stage covers the generation process, the second stage includes both generation and transmission processes, and the third stage combines generation, transmission, and distribution processes. Each stage is designed to analyze and understand regional differences by examining specific reliability parameters in the system. This method aims to provide a comprehensive evaluation of reliability across the entire power system [14]. Staged levels in power system reliability analysis model shown as Figure 1.

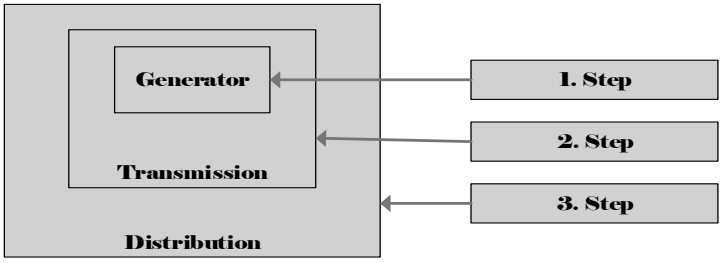


Figure 1. Staged levels in power system reliability analysis [15]

2.1. Sustainability in Power Systems

The concept of sustainability is prevalent across various disciplines, particularly in the context of energy production technologies where it is closely linked to the renewability of energy sources. The placement of optimum supercapacitors in a reliability-based sustainable energy grid must take into account not only the renewability of energy sources but also the sustainability of energy transformations. This can be effectively evaluated through Life Cycle Analysis (LCA) and exergy (usability) analyses. LCA assesses the interactions between materials, energy, emissions, solid waste, and costs involved in a production process and their impacts on the environment. In the context of a sustainable energy-based grid, sustainability is often defined as "the ability to maintain production capabilities in the future" [16]. This definition is intrinsically linked to the availability of natural resources. Another definition of sustainability is "ensuring and enhancing the integrity of life on Earth" [17]. If energy production lacks sustainability, this integrity will gradually deteriorate. In designing an optimal supercapacitor placement strategy, it is crucial to consider these sustainability principles [18]. For instance, combining LCA and exergy analyses may reveal that while biofuels can sometimes result in greater usability loss compared to gasoline, their integration into the grid with supercapacitors can mitigate such losses by balancing supply and demand. Thus, the strategic placement of supercapacitors, guided by cost-benefit and loss assessments, can significantly contribute to the sustainable and reliable operation of energy grids.

System operators (SOs) of sustainable electric power systems face technical challenges arising from the complex structures of these systems. These challenges affect the reliability and economic operation of the systems [19, 20]. In particular, the large-scale use of Renewable Energy Sources (RES) increases uncertainties during system operation, making it difficult to maintain the balance between generation and load. This situation increases the risk of load shedding, prompting system operators to plan more carefully and effectively [21]. Additionally, extra sources of uncertainty stemming from transmission systems and distribution networks add another layer to the system's reliability. The combination of these factors necessitates the development of more appropriate strategies by system operators when managing energy resources. In this context, understanding the operational challenges of sustainable energy systems and developing new strategies to address these challenges is crucial for maintaining a reliable and economical electric power system shown as Figure 2.

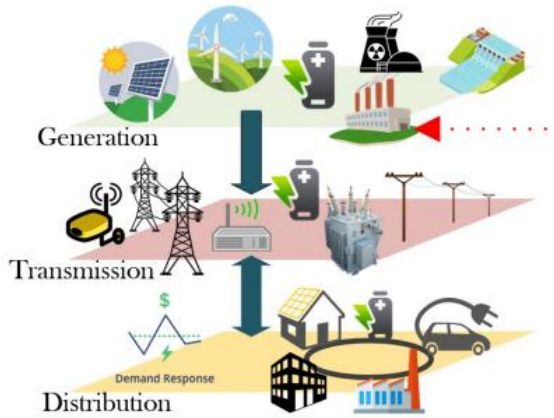


Figure 2. Sustainable Electric Energy Systems [22]

2.2. Unit Commitment in Power Systems

The Unit Commitment (UC) problem involves determining the optimal operating schedule of generation units to effectively meet load requirements on an hourly basis [23]. The aim of this optimization process is to supply energy with minimal losses and fuel consumption to maximize profit. In addition to minimizing total production cost, a generation schedule must also comply with various operational

constraints. These constraints limit decisions regarding the start-up and shutdown of generation units. Typically, these constraints include individual unit status constraints, minimum up-time, minimum down-time, capacity limits, start-up and shutdown times, limited ramp rates, group constraints, power balance constraints, and spinning reserve constraints [1, 24].

Electricity demands can vary significantly between low and high demand periods, driven by different objectives. If consumption units are monitored regularly, it may be possible to shut down certain units during periods of lower demand (for example, nighttime hours when demand is typically lower) [25]. Therefore, the primary goal of this study is to plan the operating times of different generation units to meet these constraints. UC problem can be applied to both deterministic and stochastic loads [1, 26].

A deterministic approach provides exact and unique outcomes. However, the results derived from stochastic loads might not be as definitive. Deterministic load Data Envelopment Analysis (DEA) employs the Principal Component Analysis (PCA) method [27]. Data Envelopment Analysis (DEA) is a non-parametric technique that primarily identifies input and output variables. PCA reduces the number of variables utilized in the analysis. In stochastic models, constraints are transformed into deterministic constraints, allowing the formulation to be solved using established algorithms. Various objective functions for different environments are outlined below.

2.3. Traditional Fuel-Based Approach

In Equation (1), there are three costs to be minimized. The first is the fuel cost for producing power by unit i at time t, denoted as (P(i, t)), and (M(P(i, t))) represents the fuel cost of unit i at time t. The second is the start-up cost (BM), and the third is the shutdown cost (DM) [28].

$$min \sum_{t=1}^{N_t} \sum_{i=1}^{N_0} M_i(P_{i,t}) I_{i,t} + BM + DM \quad (1)$$

The profit-based approach is applied in an environment where the primary goal is to maximize the profit of an individual generation company. UC plan has an indirect impact on price and a direct impact on average cost; thus, it is a significant part of any bidding strategy. Additionally, there is flexibility within the UC schedule. The objective function (2) can be defined as maximizing the profit (F(i,t)) of the generation company (GENCO) [29]:

$$max(F_{i,t}) \quad (2)$$

Here, (F(i, t)) represents the profit obtained from unit (i) at time (t). This function accounts for revenues from electricity sales minus the costs of production, including fuel costs, start-up costs, and shutdown costs. The aim is to achieve the highest possible profit by efficiently managing the generation schedule while adhering to operational constraints and market conditions.

3. Constraints and Cost Equations in Optimization

The Security-Constrained Unit Commitment (SCUC) solution procedure is detailed in Figure 3. This diagram illustrates the flowchart of how the optimal algorithm for unit commitment is performed [30, 31]. The initial SCUC main problem (AP1) is shown in equation (2). The SCUC main problem is defined with the iteration number "APlower," unit number (N) (1-8), period (T) (24 hours), (bmi) start-up cost, (dmi) shutdown cost, and (umi) production cost [31].

$$min\ AP1, AP_{lower} \geq \sum_{t=1}^{T}\sum_{i=1}^{N} dm_i\alpha_{it} + bm_i\ddot{u}m_{i,t} \quad (3)$$

$$(P_{i,min})I_{i,t} \leq (P_{i,t}) \leq (P_{i,max})I_{i,t} \quad (4)$$

$$\sum_{i=1}^{N} P_{i,t} + \sum_{k=1}^{N_w} W_{k,t} = Talep_t \quad (5)$$

$$(P_{i,min}) \leq \sum_{i=1}^{N} F_{i-1}P_{i,t} + \sum_{k=1}^{N_w} G_{i-k}w_{i,t} - \sum_{k=1}^{N_w} G_{i-k_{i,t}} - D_{i,t} \leq (P_{i,max}) \quad (6)$$

$$g_I(I_{i,t}) \leq 0 \quad (7)$$

$$g_r(P_{i,t}I_{i,t}) \leq 0 \quad (8)$$

$$g_r(BMI_{i,t}) \leq 0 \quad (9)$$

$$g_r(DMI_{i,t}) \leq 0 \quad (10)$$

In this equation, optimization is performed iteratively to determine which power plant will operate and to achieve the lowest cost of energy provision, represented as the (z_{lower}) value [32]. The objective is to minimize the total generation cost while meeting demand and ensuring the security and reliability of the power system. The objective function (3) includes the operating and start-up/shutdown costs of thermal generators as well as the expected wind energy curtailment. Equations (4) and (5) correspond to the system power balance constraints, while Equation (6) pertains to DC transmission constraints. The function g in Equation (7) represents constraints related to integer variables, such as minimum online/offline time limits. The g in Equation (8) signifies ramp-up and ramp-down constraints, and gc in Equations (9) and (10) indicate the constraints on the operating and start-up/shutdown costs of thermal generators.

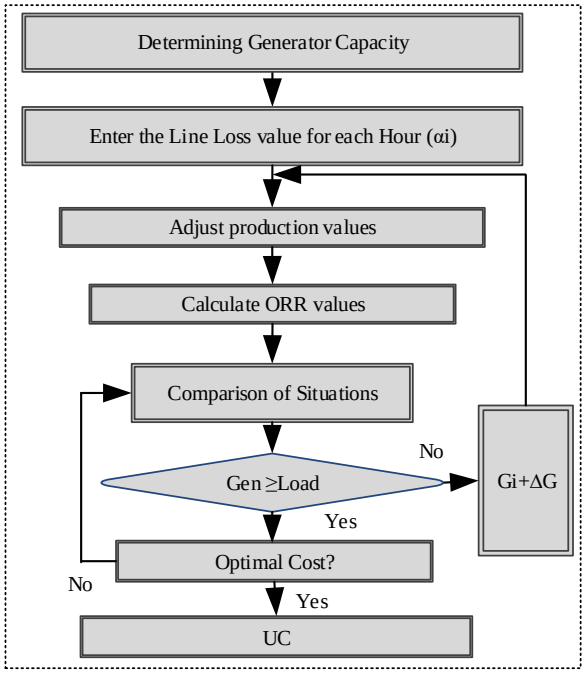


Figure 3. Foundation optimization flow chart

The following are the key components of the SCUC problem: These constraints ensure that the generation schedule adheres to the operational limits of each unit, such as minimum up and down times, ramp rate limits, and capacity limits. Power Balance Constraints ensure that the total generation meets the total demand at all times. Security Constraints include N-1 contingency criteria, ensuring that the system can withstand the failure of any single component without violating operational limits. Cost

Equations, the total cost to be minimized includes start-up costs, shutdown costs, and variable production costs.

The cost function is typically expressed as follows:

- By iterating through the SCUC problem and adjusting the unit commitments, the optimization algorithm seeks to find the most cost-effective and reliable generation schedule for the power system.
- The objective function for allocation planning is defined as follows using the Benders decomposition method to calculate the cost of replacing units in the event of outages in power systems (11):

$$AP_{lower} = 112st_{üb11} + 135st_{üb12} + 143st_{üb21} + 42st_{üb22} + \cdots + 19sd_{11} + 24sd_{12} + 31sd_{21} + 11sd_{22} + \cdots + 6595c_{üb11} + 7290c_{üb12} + 6780c_{üb21} + 1159c_{üb22} \ldots \quad (11)$$

The value "k" presented in Table 1 is a coefficient that ensures the maximum power of Gi, the strongest unit, is evenly distributed among other units. The total capacity of all units was calculated and then multiplied by the coefficient k (0.199) to determine the SKGi capacity to be maintained for each unit.

$$k = P_{max} \div \sum_{i=1}^{n=3} P_{i,max} \; and \; SK_{Gi} = k.P_{i,max} \quad (12)$$

In this analysis, a comparison between strong and weak feeders was conducted. Based on this evaluation, the use of the weak feeder will not be preferred. The SK capacity will be utilized in the most optimal and beneficial manner in conjunction with other criteria used for comparison.

Table 1. Production Capacities and Cost Functions of Generators

Unit *i* (MW)	$P_{i,min}$ (MW)	$P_{i,max}$ (MW)	P_{real} (MW)	SK_{Gi} (MW) P_{real}*0,199	Cost Functions
G_1	10	22	21	4,179	$0.022P_1^2+6.5P_1+6595$
G_2	12	24	20	3,98	$0.018P_2^2+7.5P_2+7290$
G_3	14	28	18	3,582	$0.015P_3^2+5.8P_3+6780$

To assess the reliability of the test system, calculate the overall system reliability assuming each component has a reliability of 0.9 (13). An analysis was conducted for the test system depicted in Figure 4, focusing on 3 buses.

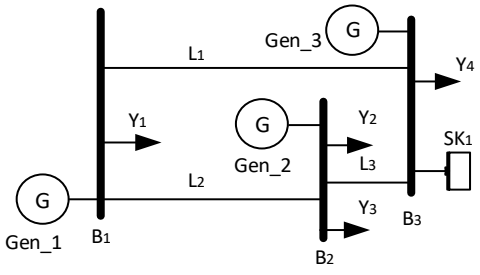


Figure 4. 3 bara, 3 Generatör, 4 Yük ve 1 Süper Kapasitör için Test Sistemi

$$Güvenirlik\ (G_s) = [\partial_s(\partial_3\partial_9)(\partial_s\partial_4) + \partial_4 - \partial_s\partial_3\partial_9\partial_4)$$
$$G_s = [0.91(0.92)(0.94) + 0.97 - 0.8719) = 0{,}8850 \quad (13)$$

If the failure rate of each component in the system is 5 f/year and the average repair time is 94.2 hours, the usability of the system is calculated as (14) and (15).

$$G_s = [\propto_s (3\ god\ value)(\propto_3)\ \propto_s (3\ bad\ value)(SKU_3) \quad (14)$$

$$System\ Unusability\ (SKU) = \frac{\lambda}{\lambda+\mu} = \frac{5}{5+95} = 0.05 \quad (15)$$

$$System\ Availability = (0.95)[0.99275] + (0.05)[0.986094] = 0.992417$$
$$System\ Unavailability = 1 - 0.99241 = 0.00759$$

In the test system, the average repair time of the supply is considered to be 0.5 f/failure per year, i.e. 2 hours. Line data are as shown in Table 2.

Table 2. Failure rate of Line

Line	**1**	**2**	**3**
Failure rate (failure/year)	3.0	4.0	5.0
Average Repair Time (hour)	4	6	8

The Decision Equation was created for the model, taking into account production cost, line losses and reliability parameters (Equation 16).

$$Decision\ Equation\ (DE)_n = \left[\left[\sum_{i=1}^{n}\frac{\propto_{i+1}}{\propto_i+\propto_{i+1}}\right]\left[\sum_{i=1}^{n}\frac{m_{i+1}}{m_i+m_{i+1}}\right]\sum_{i=1}^{n}\frac{G_i}{G_{i+1}}\right] \quad (16)$$

For the three different parameters shown in Equation (17), 23=8 cases will be analyzed as shown in Table 4. PSK is the total amount of SK and PSK1 is the amount of SK for unit 1.

$$P_{SK_n} = \sum_{i=1}^{n}\frac{KD_i}{KD_i + KD_{i+1}}P_{SK} \quad (17)$$

Following the computation of the KD values as per equation (16), the PSK value denoting Supercapacitor Power from equation (17) is determined as depicted in Table 3 for eight distinct scenarios. Taking into account the three factors of cost, loss, and reliability, a total of $2^3 = 8$ comparisons among situations will be conducted.

Table 3. Determining case study options

Cases	**Case1**	**Case2**	**Case3**	**Case4**	**Case5**	**Case6**	**Case7**	**Case8**
Reliability	-	+	-	-	+	+	-	+
Cost	-	-	+	-	+	-	+	+
Lost	-	-	-	+	-	+	+	+

In the IEEE test model used: the reliability of Line1, Line2 and Line3 are 0.95, 0.99 and 0.94 respectively, Line losses are given as α1=0.0001 and α2=0.0002 and α2=0.0004 (Table 4). According to Figure 4, by subtracting the load amount from the production total, the SK amount was obtained as 50 MW.

Table 4. Data from eight different case studies

Unit	Cost (c)	Lost (α)	Reliability (R)	SK (MW)	Total Generation Cost ($/MWh)
G1	8	0.0001	0.95	50	
G2	12	0.0002	0.99	50	
G3	10	0.0004	0.94	50	
	β1	**β2**	**PSK1**	**PSK2**	
Case1	0	0	50	50	1400
Case2	0.45	0.48	55.55	44.44	1388.88
Case3	0.43	0.66	33.33	66.66	1433.33
Case4	1.05	0.97	51.06	48.93	1397.87
Case5	0.18	0.29	38.46	61.53	1423.07
Case6	0.56	0.43	56.60	43.39	1386.79
Case7	0.34	0.65	34.28	65.71	1431.42
Case8	0.18	0.29	39.47	60.52	1421.05

Utilizing the values of C, R, and α, the acceptance matrix for the 3-bar system was constructed. This matrix is of size 3x3. The bus admission matrix is illustrated in Figure 5, highlighting the locations where non-zero elements exist. The system specifications can be found in Table 5. Figure 6 depicts the convergence plot for the P values in the program, while Table 5 presents the program results. Following the program execution, the average PSK1 power was determined to be 44.84 MW, and the PSK2 power was calculated as 55.15 MW. Consequently, the total system loss amounts to (100 - 99.99(PSK1 + PSK2)) = 0.01 MW. The system loss coefficients B were derived from the power flow analysis, and the power plants were economically loaded through the MATLAB® program. The Economic Distribution Analysis flowchart is outlined in Figure 5.

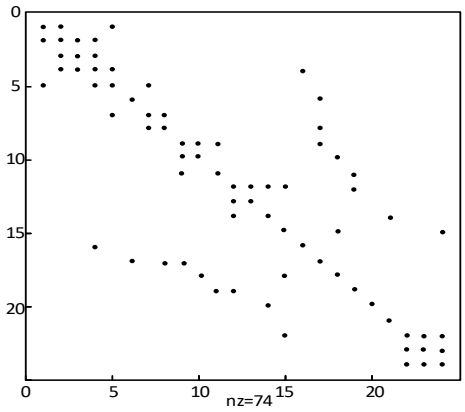


Figure 5. Non-Zero Points of the Bus Acceptance Matrix

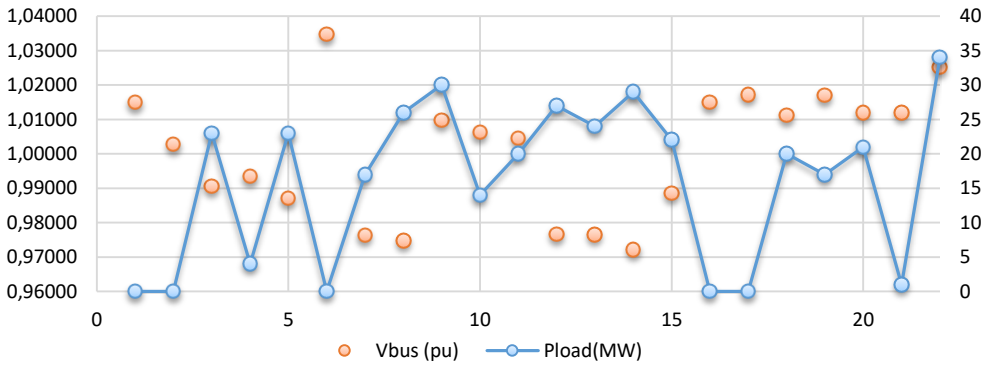


Figure 6. Program convergence chart for P and Vbus

4. Conclusion

The developed methodology entails examining production expenses, line inefficiencies, and reliability metrics to minimize production losses, optimize expenditures, and enhance system dependability. These analyses lead to improved reliability and efficiency in energy production systems. This research offers viable strategies for achieving cost-effective and sustainable energy production within power systems. Through the consideration of production costs, line inefficiencies, and reliability metrics, the methodology ensures the efficient allocation of energy production assets. It provides a comprehensive assessment of power system effectiveness and feasibility. Comparison of the results according to Table 5 reveals that the lowest cost of $8,053/MWh was attained in the sixth scenario among all cases studied. The parameters scrutinized in this scenario are production cost and reliability, indicating that the distributed production quantities are both reliable and cost-effective. Consequently, the SK allocation was achieved at a more favorable cost compared to the MATLAB result. Conversely, scenarios focusing solely on line inefficiencies or a combination of line inefficiencies and reliability appear less economical. In the case studies, a thorough examination of the scenario depicting a linear relationship between units and SK quantities reveals that the sixth scenario is the most suitable among those depicted in Figure 7. The most significant disparity in unit distribution is observed in the third case study, suggesting that only line inefficiencies were considered in the calculation.
In future studies, sophisticated modeling and simulation techniques can be employed to provide more detailed analyses of the reliability and efficiency of energy production systems. This would allow for a more realistic and comprehensive evaluation of different scenarios. Additionally, real-time data analysis and dynamic load distribution algorithms can be developed. This would contribute to a more effective allocation of energy production assets and enhance system reliability.

References

[1] Tur, M. R. (2021). Deployment of reserve requirements into the power systems considering the cost, lost, and reliability parameters based on sustainable energy. The International Journal of Electrical Engineering & Education, 58(2), 621-639.

[2] Zong, L., Zhang, X., Zhao, L., Yu, H., & Zhao, Q. (2017). Multi-view clustering via multi-manifold regularized non-negative matrix factorization. Neural Networks, 88, 74-89.

[3] Sedghi, M., Ahmadian, A., & Aliakbar-Golkar, M. (2015). Optimal storage planning in active distribution network considering uncertainty of wind power distributed generation. IEEE Transactions on Power Systems, 31(1), 304-316.

[4] Saboori, H., Hemmati, R., & Jirdehi, M. A. (2015). Reliability improvement in radial electrical distribution network by optimal planning of energy storage systems. Energy, 93, 2299-2312.

[5] Barnoy, A. (2022). An island of reliability in a sea of misinformation? Understanding PR-journalists relations in times of epistemic crisis. Journal of Public Relations Research, 34(3-4), 89-108.

[6] Arrillaga, J., Watson, N. R., & Chen, S. (2000). Power system quality assessment. John Wiley & Sons.

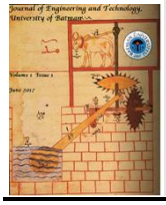
[7] Billinton, R., Allan, R. N., & Salvaderi, L. (1991). Applied reliability assessment in electric power systems.

[8] George, D., & Mallery, P. (2018). Reliability analysis. In IBM SPSS statistics 25 step by step (pp. 249-260). Routledge.

[9] Olajuyin, E. A., Olulope, P. K., & Fasina, E. T. (2022). An overview on reliability assessment in power systems using CI approaches. Archives of Electrical Engineering, 71(2).

[10] Alahmed, A., Siddiki, M. K., & Chaudhry, G. M. (2020, June). Reliability Evaluation of Microgrid Power Systems Based on Renewable Energy in Saudi Arabia. In 2020 47th IEEE Photovoltaic Specialists Conference (PVSC) (pp. 2799-2802). IEEE.

[11] Weber, E., Adler, et. Al. (1996). Reporting bulk power system delivery point reliability. IEEE Transactions on Power Systems, 11(3), 1262-1268.
[12] Tur, M. R. (2020). Reliability assessment of distribution power system when considering energy storage configuration technique. IEEE Access, 8, 77962-77971.
[13] Kucur, G., Tur, M. R., Bayindir, R., Shahinzadeh, H., & Gharehpetian, G. B. (2022, February). A review of emerging cutting-edge energy storage technologies for smart grids purposes. In 2022 9th Iranian Conference on Renewable Energy & Distributed Generation (pp. 1-11). IEEE.
[14] Ersalıcı, H. (2013). Elektrik Dağıtım Sistemlerinin Güvenilirlik Analizi (Doctoral dissertation, Fen Bilimleri Enstitüsü).
[15] Wadi, M., Baysal, M., Shobole, A., & Tur, M. R. (2018, October). Reliability evaluation in smart grids via modified Monte Carlo simulation method. In 2018 7th International Conference on Renewable Energy Research and Applications (ICRERA) (pp. 841-845). IEEE.
[16] Solow, R. (2014). Thomas Piketty is right. Everything you need to know about capital in the twenty-first century. New Republic, 22.
[17] Chan, H. Y., Riffat, S. B., & Zhu, J. (2010). Review of passive solar heating and cooling technologies. Renewable and Sustainable Energy Reviews, 14(2), 781-789.
[18] Rodríguez, M. R., De Ruyck, J., Diaz, P. R., Verma, V. K., & Bram, S. (2011). An LCA based indicator for evaluation of alternative energy routes. Applied energy, 88(3), 630-635.
[19] Moslehi, K., & Kumar, R. (2010). A reliability perspective of the smart grid. IEEE transactions on smart grid, 1(1), 57-64.
[20] Moslehi, K., & Kumar, R. (2010, January). Smart grid-a reliability perspective. In 2010 Innovative smart grid technologies (ISGT) (pp. 1-8). IEEE.
[21] North American Electric Reliability Corporation, "Task 1.6 Probabilistic Methods," NERC, Atlanta, GA, USA, July 2014
[22] Ilić, M. D., Joo, J. Y., Xie, L., Prica, M., & Rotering, N. (2010). A decision-making framework and simulator for sustainable electric energy systems. IEEE Transactions on Sust. E., 2(1), 37-49.
[23] Tur, M. R., Ay, S., Wadi, M., & Shobole, A. (2017). Obtaining optimal spinning reserve and unit commitment considering the socio-economic parameters, ECRES–5. In European Conference on Renewable Energy Systems, Herzegovina, Bosnia.
[24] Tür, M., Ay, S., Shobole, A., & Wadi, M. (2019 Güç sistemlerinde ünite tahsisi için döner rezerv gereksinimi optimal değerinin kayip parametrelerin dikkate alinarak hesaplanmasi. Journal of the Faculty of Engineering and Architecture of Gazi University, 34.
[25] Palensky, P., & Dietrich, D. (2011). Demand side management: Demand response, intelligent energy systems, and smart loads. IEEE transactions on industrial informatics, 7(3), 381-388.
[26] Strbac, G. (2008). Demand side management: Benefits and challenges. Energy policy, 36(12), 4419-4426.
[27] Haas, P. J., Naughton, J. F., Seshadri, S., & Stokes, L. (1995, September). Sampling-based estimation of the number of distinct values of an attribute. In VLDB (Vol. 95, pp. 311-322).
[28] Ding, Y., Shao, C., Yan, J., Song, Y., Zhang, C., & Guo, C. (2018). Economical flexibility options for integrating fluctuating wind energy in power systems: The case of China. Applied Energy, 228, 426-436.
[29] Azadeh, A., Ghaderi, S. F., Nokhandan, B. P., & Sheikhalishahi, M. (2012). A new genetic algorithm approach for optimizing bidding strategy viewpoint of profit maximization of a generation company. Expert Systems with Applications, 39(1), 1565-1574.
[30] Wu, L., Shahidehpour, M., & Li, T. (2007). Stochastic security-constrained unit commitment. IEEE Transactions on power systems, 22(2), 800-811.
[31] Fu, Y., & Shahidehpour, M. (2007). Fast SCUC for large-scale power systems. IEEE Transactions on power systems, 22(4), 2144-2151.
[32] Ghasemi, H., Paci, M., Tizzanini, A., & Mitsos, A. (2013). Modeling and optimization of a binary geothermal power plant. Energy, 50, 412-428.



Journal of Engineering and Technology
DergiPark
AKADEMİK

Journal of Engineering and Technology 5;1 (2024) 11-21

ISO 27001, KVKK, and GDPR: A Comparison of Information Security and Data Protection Standards

[a]Melis Böke Yazıcıoğlu

[a,c]Iskenderun Technical University, Faculty of Engineering and Natural Sciences, Department of Computer Engineering, 2017, HATAY/TURKEY

[a] bokemelis@gmail.com

ARTICLE INFO

Article history:
Received May 11, 2024
Accepted June 28, 2024
Available online June 29, 2024

Key words:
Information Security
KVKK
GDPR
Data Protection
ISO 27001

* Corresponding author.
E-mail address:
bokemelis@gmail.com

ABSTRACT

In today's digital age, safeguarding information security and data protection is crucial amid increasing cyber threats. ISO 27001:2022 focuses on establishing and executing an organization's information security management system, emphasizing risk management, and safeguarding information assets. On the other hand, GDPR and KVKK serve as legal frameworks governing the protection and processing of personal data. This article offers a detailed exploration of these standards, delineating their benefits, requirements, and the intricate landscape of compliance challenges businesses may face. By providing practical insights, it aims to furnish a vital framework for addressing information security and data protection concerns and empowering businesses to navigate these realms effectively.

1. Introduction

Information security and data protection are among the most crucial and complex issues of today's digital age. With the rapid advancement of technology and the widespread digitization, access to information increases, while cyber threats and data breaches also continue to rise. This situation poses a significant concern for both individuals and organizations. To address these concerns and ensure the security of data, international standards and local regulations have become increasingly important. In this context, standards and regulations such as ISO 27001:2022, GDPR (General Data Protection Regulation), and KVKK (Personal Data Protection Law) come into play. In this study, ISO 27001, GDPR, and KVKK standards will be examined in detail, and the benefits and requirements they provide to businesses will be thoroughly discussed. Additionally, a comparison of these standards in terms of security and compliance for businesses will be conducted, and the scope and requirements of each will be examined in detail. Finally, the process of compliance with these standards and the difficulties that businesses may encounter in this process will be addressed, such as resource constraints, enhancing technical infrastructure, and adapting to cultural shifts, along with practical recommendations. In this way, an important framework for information security and data protection will be provided, assisting businesses in operating more effectively in these areas.

2. ISO 27001: Information Security Management System

ISO 27001 is an international standard that guides an organization in establishing, implementing, monitoring, reviewing, and continuously improving its Information Security Management System (ISMS). This standard standardizes the process of managing information security by providing best practices necessary for organizations to protect their information assets. The Information Security Management System (ISMS) Standard covers all types of organizations (e.g., commercial enterprises, governmental agencies, non-profit organizations) [1]. There are main components of ISMS within the framework of ISO 27001.

2.1 Establishment and Implementation of ISMS

ISO 27001 requires an organization to establish its information security policy, define information security objectives, and establish the necessary processes and procedures to achieve these objectives. The information security policy mandated by ISO 27001 sets out an organization's information security objectives and commitments. The information security policy forms the foundation of an organization's information security culture. Effective implementation of the ISMS also involves raising awareness among all employees about information security and encouraging their active participation, thereby fostering the creation of an information security culture and ensuring that commitments are embraced by all employees. This enhances the organization's ability to protect its information assets and become more resilient against cyber threats.

Risks and Threats:

- **Information Security Breaches**: Failure to implement information security policies without necessary precautions may lead to risks such as information security breaches and data leaks.
- **Internal and External Threats**: Malicious individuals or groups from within or outside the organization may damage or gain unauthorized access to information assets. This could manifest as unauthorized access, ransomware attacks, or other cyber threats.
- **Legal and Regulatory Compliance Issues**: Non-compliance with standards like ISO 27001 can expose organizations to legal and regulatory issues, including fines, reputational damage, and other legal consequences.
- **Business Continuity and Operational Risks**: Information security breaches or cyberattacks can affect business continuity and create operational risks, such as data loss or service disruptions.

2.1.1. Risk Management

The ISO 27001 Standard enables organizations to identify, analyze, and evaluate risks that threaten the security of their information assets. Appropriate controls must be implemented to reduce these risks to an acceptable level. The Risk Management process consists of steps such as identifying risks, analyzing risks, evaluating risks, determining control measures, and assessing the acceptability of risks. Risk analysis activities are conducted within the defined scope of the ISMS. The scope of the ISMS also encompasses the scope of risk analysis [2].

2.1.2. Implementation of Controls

ISO 27001 provides a set of control measures and recommends organizations to implement these controls within the scope of their Information Security Management System (ISMS). These controls encompass the security measures necessary for organizations to protect their information assets, enhance

resilience against cyber threats, and ensure compliance with legal regulations. The control measures offered by ISO 27001 assist organizations in reducing information security risks and safeguarding their information assets. These controls can be adapted and implemented to meet the specific needs of organizations and industry requirements.

2.1.3. Information Security Policy

When organizations begin their efforts to ensure information security, they should first establish and document rules for all types of information security activities. Written rules are necessary for the planning, implementation, and continuous improvement stages of activities aimed at ensuring information security. In this regard, various guiding documents such as policies, procedures, guidelines, and instructions can be prepared. The foundation of these documents is the information security policy [3]. An organization must establish and implement an information security policy because this policy provides a framework for protecting the organization's information assets and building resilience against cyber threats. This policy defines the organization's information security objectives, responsibilities, and management approach. Establishing and implementing the organization's information security policy is a critical step in creating and maintaining an information security culture.

2.1.4. Continuous Improvement

The principle of continuous improvement in ISO 27001 is an important component for enhancing the effectiveness and efficiency of an organization's Information Security Management System (ISMS). This principle involves regularly reviewing and improving processes and controls. The continuous improvement principle of ISO 27001 enables organizations to continually enhance their information security performance.

3. Personal Data Protection Law (KVKK) and General Data Protection Regulation (GDPR)

Personal Data Protection Law (KVKK):

The Personal Data Protection Law (KVKK) is a regulation enacted in Turkey, which came into effect on April 7, 2016. It encompasses provisions regarding the processing, protection, and lawful utilization of personal data. The primary objective of the KVKK is to safeguard the privacy and security of individuals' personal data, ensure the lawful processing of such data, and protect the rights and freedoms related to personal data.

Data processing rules can be listed as follows [4]:

- Must comply with the legal system in Turkey and align with principles of fairness,
- Data should be verifiable and up-to-date when needed,
- Data processed should be limited, relevant to the purpose for which it is processed, and retained for the necessary duration.

General Data Protection Regulation (GDPR):

The General Data Protection Regulation (GDPR) is a comprehensive regulation concerning the processing and protection of personal data within the European Union (EU). It came into effect on May 25, 2018, and affects all organizations and individuals located within and outside the EU.

- Data processing must be transparent and compliant with the law.
- Data should be limited to the purpose for which it is related.

- Data quality, accuracy, and accountability should be ensured.
- Time constraints should be applied to the retention of relevant data.
- The confidentiality and integrity of the data must be maintained [5].

When these two laws are compared with each other, it is concluded that both regulations aim to protect the person to whom personal data is related, and that transparency and compliance with the law are important [4].

4. Relationship Between ISO 27001, KVKK and GDPR

ISO 27001, GDPR, and KVKK are information security and data protection standards and regulations that serve different purposes but complement each other or have similar objectives. These standards and regulations have their own purposes, scopes, and application areas. Some of them overlap, while others naturally exhibit differences.

Table 1. Standards and Regulations Comparison: ISO 27001, GDPR, and KVKK

	Purpose	Scope	Application Areas	Sanctions
ISO 27001	It provides a framework for establishing, implementing, monitoring, reviewing, and continuously improving an Information Security Management System (ISMS). Its primary aim is to protect organizations' information assets and make them resilient against cyber threats.	It covers information security management and encompasses all information assets and related processes.	It can be implemented by a wide range of organizations and industries. Any organization can implement ISO 27001 to manage information security risks and protect information assets.	ISO certification demonstrates compliance and often provides a competitive advantage in the market.
KVKK	It includes regulations concerning the processing, protection, and lawful use of personal data in Turkey. Its primary aim is to protect the privacy and security of personal data and ensure their lawful processing.	It covers the processing and protection of personal data in Turkey, affecting all organizations and individuals in Turkey.	All organizations and individuals in Turkey are obligated to comply with KVKK when processing personal data.	Non-compliant organizations with KVKK may also face significant fines. Breaches can be investigated and penalized by the Personal Data Protection Authority (KVKK).
GDPR	It encompasses comprehensive regulation concerning the processing and protection of personal data within the European Union (EU). Its primary aim is to safeguard the privacy and security of individuals' personal data and ensure the lawful processing of such data.	It encompasses the processing and protection of personal data, particularly affecting all organizations processing data of EU citizens.	All organizations, both within and outside the EU, are obligated to comply with GDPR when processing personal data of EU citizens (such as identity information, health data, address, etc.).	Non-compliant organizations with GDPR may face significant fines. Breaches can be investigated and penalized by data protection authorities. Considering the heavy administrative fines adopted by Article 83 of the GDPR, the importance of ensuring GDPR compliance, especially for companies, becomes more evident [6].

4.1 Differences

ISO 27001 regulates information security management, while GDPR and KVKK regulate the protection of personal data. GDPR affects all organizations processing data of EU citizens, while KVKK only affects organizations in Turkey. ISO 27001 is a certification standard, whereas GDPR and KVKK are legal regulations. Additionally, ISO 27001 serves as a certification standard for organizations. Companies can obtain ISO 27001 certification to demonstrate that they have implemented appropriate processes and controls and to showcase this compliance to the external world. Furthermore, GDPR differs from KVKK in several aspects. One such distinction is that under GDPR, Data Processors face much heavier legal liabilities in the event of data breaches compared to KVKK. Additionally, under GDPR, Data Controllers are obliged to oversee the compliance of Data Processors with GDPR [7].

Data controllers are required to monitor and manage data processors' compliance with the terms specified in contracts or other regulations they have signed with them. This regulation aims to ensure that both data controllers and data processors collaborate to secure the security and privacy of personal data and adhere to GDPR provisions effectively.

5. Implementation and Alignment of ISO 27001, GDPR, and KVKK

Integrating ISO 27001, GDPR, and KVKK ensures effective management of both information security and personal data protection practices within an organization. When examining the Data Security Guide published by the Personal Data Protection Board, it is evident that "data security" is directly related to ISMS, which is one of the main headings of KVKK [8]. In the Administrative Measures table in KVKK and in GDPR, the topic of Risk Assessment is present. Given that Risk Assessment is also a fundamental topic in the ISO 27001 standard, it is possible to directly associate the standard with both KVKK and GDPR. Similarly, the requirement of developing policies and procedures in ISO 27001 aligns with the transparency and accountability principles of GDPR. The alignment between the two assists organizations in identifying the necessary steps to comply with GDPR and implementing them [9]. Various approaches exist to ensure this integration in organizations. Various difficulties may be encountered in ensuring integration.In this section, relevant approaches are detailed, potential difficulties are outlined, and evaluated.

Difficulties and Tips for the Harmonization Process:

The process of achieving regulatory compliance can often be time-consuming and complex for businesses. This process consists of several steps and may vary depending on the organization's current status, size, and complexity. Generally, there can be some challenges that organizations may encounter.

Resource Insufficiency: The process of achieving regulatory compliance often requires additional resources. These resources may include time, money, manpower, and expertise. Limited resources, particularly for small and medium-sized enterprises, can make the compliance process challenging.

Complexity: Regulations are often complex and detailed. Understanding and implementing these standards can take time for businesses. Especially if compliance with multiple regulations or standards is required, the complexity can further increase.

Changing Requirements: Regulations can be updated or revised over time. This means that businesses need to continually review and update their compliance processes to meet these changing requirements. Coping with these changing requirements also poses challenges.

Cultural Change: Achieving compliance with regulations often requires changes in organizational culture. Adopting new policies and procedures and educating staff can be a challenge for some businesses, as they may encounter resistance.

Monitoring and Evaluation: The compliance process requires continuous monitoring and evaluation. It is important for businesses to constantly monitor their performance and identify improvement opportunities. However, this can be resource-intensive and time-consuming for some businesses.

External Audits and Certification: In some cases, businesses may need to undergo external audits and obtain certification to verify their compliance with regulations. This process can incur additional costs and time for businesses.

Despite these challenges, the process of regulatory compliance provides long-term benefits for businesses. Compliance with regulations can increase customer trust, provide a competitive advantage, and strengthen the organization in terms of data security. Therefore, it is important for businesses to invest in the compliance process to overcome these challenges.

There are some tips that organizations can apply to cope with these challenges. These tips can make the process of regulatory compliance more manageable and enhance the success of organizations in terms of information security and data protection.

- Starting off on the right foot
- Defining authorities and responsibilities
- Providing training and raising awareness
- Creating a compliance plan
- Embracing a culture of continuous improvement
- Utilizing external resources
- Adopting risk-based approaches
- Strengthening communication

5.1 Determining Common Principles

Taking into account the fundamental principles and requirements of ISO 27001, GDPR, and KVKK, a compliance strategy based on common principles should be established. Some of these common principles include:

- Data Protection and Privacy Principle
- Integrity Principle
- Access Control Principle
- Protection of Rights of Data Subjects
- Risk Management Principle

These common principles represent the core principles and requirements embraced by ISO 27001, GDPR, and KVKK. By adopting and implementing these principles with an integrated approach, organizations can ensure both information security and personal data protection compliance more effectively. Adopting just one principle may be insufficient; relevant standards and regulations should be approached with an integrated strategy and implemented together. This way, more effective compliance with information security and personal data protection can be ensured.

5.2 Risk Management and Checklists

The organization should adopt an integrated risk management approach considering its risk profile and compliance requirements. Risk Management is one of the requirements of these three regulations. Common risks and control lists should be established, and an integrated framework for the controls to be compliant should be developed. In terms of identifying common risks, both ISO 27001 and GDPR compliance requirements entail identifying information security vulnerabilities and taking measures against them, while KVKK and GDPR demand implementing control measures to prevent unauthorized access to personal data. An example table detailing the consolidation of control lists is elaborated in Table 1. below.

Table 2. Consolidation of Control Lists

Control Point	Description	ISO 27001 Compliance	GDPR Compliance	KVKK Compliance

Information Security Policy	Establishment and communication of the organization's information security policy.	X		
Data Access Controls	Implementation of necessary controls to prevent unauthorized access.	X	X	X
Data Breach Notification	Creation of procedures for detecting and reporting potential data breaches.	X	X	X
Employee Training and Awareness	Provision of regular training on information security and personal data protection topics.	X	X	X
Monitoring and Auditing	Regular monitoring and auditing of systems and data processing activities.	X	X	X
Determination of Data Location	Determination and recording of the locations of processed personal data.		X	X
Data Retention Limitations	Implementation of limitations on the retention of personal data for a specified period.	X	X	X

In this example, a control list is provided that includes common control points that can be used to consolidate ISO 27001, GDPR, and KVKK compliance requirements. This list combines the necessary controls for compliance under a single framework, considering the requirements of each compliance area.

5.3 Integrated Policies and Procedures

Creating integrated policies and procedures is of critical importance for ensuring compliance with ISO 27001, GDPR, and KVKK. ISO 27001 requires organizations to develop and implement information security policies and procedures [9].

These policies and procedures provide a framework that combines both information security management and personal data protection practices, encouraging a cohesive approach to compliance. Information security policies and personal data protection policies should be developed with an approach that integrates compliance requirements. Common procedures should be established, ensuring consistency across practices. These policies and procedures:

- They should encompass both information security and personal data protection principles.
- The information security policy should cover fundamental information security topics such as protection of information assets, access control, encryption, and security measures like firewalls.
- Personal data protection procedures should be created in accordance with KVKK and GDPR requirements, addressing aspects like collection, storage, use, sharing, and disposal of personal data.

5.4 Training and Awareness Programs

Training and awareness programs for employees should be integrated to cover both information security and personal data protection topics. Common training materials and awareness campaigns should be developed. Organizations should assess the training needs of employees, considering ISO 27001, GDPR, and KVKK requirements. These programs should include topics such as basic information security principles, protection of information assets, data privacy, authorization, and authentication. Additionally, personal data protection training should encompass KVKK and GDPR requirements and principles of personal data processing. Using exams and assessment tools, employees' knowledge levels can be measured, and the effectiveness of the training can be evaluated. Example training program is detailed in Table 2. Ensuring involvement and commitments from senior management in training and

awareness programs can encourage employee participation and the establishment of a culture of information security.

Table 3. Example Training Program

Training Title	Description	Target Audience	Duration
Basic Information Security Principles	An introduction to basic concepts and importance of information security.	All employees	1 hour
Protection of Information Assets	Protection and management of information assets within the organization.	All employees	2 hour
Data Privacy	Importance of data privacy and protection of personal and sensitive data.	All employees	1.5 hour
Authorization and Authentication	Access control mechanisms and methods for verifying user identities.	IT personnel, system administrators	2 hour
KVKK Fundamental Principles	Basic principles of KVKK and personal data protection topics.	All employees	1.5 hour
GDPR Practices	GDPR requirements and principles of personal data processing.	All employees	2 hour
Crisis Management and Incident Response	Effective response strategies in the event of information security breaches or crisis situations.	Executive Level Management	2.5 hour
Risk Management and Strategic Planning	Determination of organizational risk management strategies and integration of information security strategy.	Executive Level Management	2.5 hour
Legal and Regulatory Requirements	General overview of key legal regulations such as ISO 27001, GDPR, and KVKK requirements and their implementation.	Executive Level Management	2 hour

In this example, a training program is proposed targeting both senior executives and all employees. These trainings aim to assist executives in determining and implementing the organization's information security and personal data protection strategies, while also catering to the needs of all employees and aiming for participants to have varying levels of knowledge.

5.5 Monitoring and Improvement Processes

These processes enable the organization to effectively manage its compliance process, monitor its performance, and continuously improve. Integrated monitoring and internal audit processes should be established to assess the effectiveness of the compliance process. Improvement activities should be managed using common criteria and performance indicators applicable to both areas. The examples related to the processes are detailed in Table 3.

Table 4. Monitoring, Improvement, and Performance Indicator Processes

Process	Description	Performance Indicators	Common Metrics	Responsible Departments
Audit and Monitoring Plan Creation	Establishment of an annual audit and monitoring plan to ensure compliance with ISO 27001, GDPR, and KVKK. The plan involves regular monitoring, auditing, and evaluation of identified compliance requirements.	Level of implementation of the audit plan, number of completed audits, status of identified action items.	Compliance rate, implementation rate of action items	Information Security Department, Internal Audit Department
Incident and Breach Monitoring	Process established for monitoring and reporting incidents and breaches. It ensures the rapid detection of any security breach or data leakage and the implementation of appropriate measures.	Time to detect and respond to incidents, time to resolve incidents, number of breach reports.	Incident detection rate, response time	Information Security Department, Business Continuity and Risk Management Unit
Continuous Improvement Meetings	Regular meetings held to discuss identified areas for improvement. Improvement opportunities are identified based on monitoring results, improvement plans are developed, and implemented.	Rate of implementation of identified improvement activities, number of completed improvement projects, participation rate in meetings.	Effectiveness of improvement activities, success of improvement projects	Quality and Compliance Department, Internal Audit Department
Evaluation of Training Programs	Regular assessment of employee training and awareness levels. The effectiveness and participation levels of training programs are reviewed, and improvements are made as necessary.	Number of completed trainings, participation rate, employee feedback.	Training effectiveness, participation rates	Human Resources Department, Quality and Compliance Department
Performance Metrics Tracking	Regular monitoring of defined performance metrics and evaluation of performance. These metrics are used to determine the effectiveness of compliance processes, the status of achieving objectives, and the necessity of continuous improvement.	Performance metrics tracking, performance evaluation.	Compliance effectiveness, achievement status, need for continuous improvement.	Quality and Compliance Department, Business Continuity and Risk Management Unit

5.6 External Audits and Certifications

External audits and certifications are critical processes for ensuring compliance with ISO 27001, GDPR, and KVKK. These processes are used to assess the organization's level of compliance, verify its compliance through an external independent review, and demonstrate its compliance to customers or regulatory authorities. When necessary, both ISO 27001 and GDPR and KVKK compliance should be subjected to external independent audits and certification. These audits are important for verifying the effectiveness of the compliance process and promoting continuous improvement. The certification process not only demonstrates the organization's compliance to customers, suppliers, partners, and other

stakeholders but also enhances the organization's credibility and can provide a competitive advantage in business relationships.

These approaches represent different strategic steps that can be used to integrate ISO 27001, GDPR, and KVKK compliance. Organizations can adapt these approaches according to their needs and requirements, enabling them to manage the compliance process more effectively.

6. Conclusion

ISO 27001, GDPR, and KVKK underline the interconnection between information security management and personal data protection, emphasizing their relationship. While ISO 27001 aims to establish a robust information security management system, GDPR and KVKK encompass the protection of personal data and the rights of individuals. Despite the differences among these standards and regulations, they share common principles and objectives, enabling organizations to integrate their compliance efforts effectively.

Achieving compliance with ISO 27001, GDPR, and KVKK requires a strategic approach that harmonizes policies, procedures, and training programs. Identifying common principles, adopting integrated risk management practices, and establishing consistent policies and procedures allow organizations to effectively manage their compliance obligations. Thus, organizations not only strengthen their position in terms of information security but also ensure compliance with legal regulations.

However, organizations may encounter difficulties in the process of achieving regulatory compliance, such as resource constraints, complexity, changing requirements, and cultural shifts. To overcome these challenges, organizations should prioritize education, develop a compliance plan, embrace a culture of continuous improvement, and utilize external resources when necessary.

In conclusion, understanding and implementing the ISO 27001:2022 standard provides a strong foundation for both information security and personal data protection. These standards help businesses establish a secure and compliant data management culture, making them more resilient against cybersecurity threats. By proactively addressing information security and data protection concerns, organizations can effectively navigate the evolving landscape of regulatory requirements and protect sensitive information. As a result of these approaches, businesses can increase customer trust, gain a competitive advantage, enhance data security, reduce operational risks, and ensure long-term sustainability. These steps shed light on businesses successfully managing the process of regulatory compliance and gaining a competitive edge.

References

[1] Çetinkaya, M. (2008). Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması. Akademik Bilişim 2008 , 511-516.

[2] Yılmaz, H. (2014). Ts Iso/Iec 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. Denetişim, 45-59.

[3] Meral S., Bülbül H.İ. (2022). Analysis Of The Efficiency Of The Information Security Policies Of Public Institutions İn Terms Of Ensuring Corporate Information Security. Fen Bilimleri Dergisi, 314-329.

[4] Savaş, R.N., Zaim, A. H., Aydın, M. A. (2020). Kvkk Ve Gdpr Kapsamında Firmaların Mevcut Durum Analizi Üzerine Bir İnceleme. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 208-223.

[5] Kvkp (2020, Accessed On 12.05.2024). Retrieved From Https://Www.Kisiselverilerinkorunmasi.Org/Mevzuat/Avrupa-Birligi-Genel-Veri-Koruma-Tuzugu-Gdpr-Turkce-Ceviri/

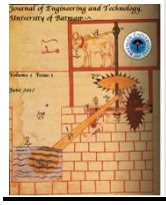
[6] Dülger, M. V. (2019). Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması. Yaşar Hukuk Dergisi C.1 S.2 , 71-174.

[7] Olca, E. A., Can, Ö. (2024). Kvkk Kavramlarının Modellenmesi İçin Ontoloji Tabanlı Bir Yaklaşım. Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen Ve Mühendislik Dergisi, 173-191.

[8] Tosunoğlu, A. (Accessed On 13.05.2024). Iso/Iec 27001 Bilgi Güvenliği Yönetim Sistemi'nin Kvkk'ya Etkisi. Retrieved From Proks Certification: Https://Proks.Co/Haberler/İso-İec-27001-Bilgi-Guvenligi-Yonetim-Sistemi-Nin-Kvkk-Ya-Etkisi

[9] Kılıç, B. (2024). Kuruluşların Başarısı İçin Iso 27001 Ve Kişisel Verilerin Korunması. 3. Nesil Hukuk Dergisi.

[10] Evren, A. G. (2023). Avrupa Birliği Ve Türkiye Kişisel Verilerin Korunması Kanunlarının Karşılaştırmalı Analizi: Temel İlkeler, Yasal Dayanaklar Ve İlgili Kişi Hakları. Kişisel Verileri Koruma Dergisi, 39-64.



Journal of Engineering and Technology
DergiPark
AKADEMİK

Journal of Engineering and Tecnology 5;1 (2024) 22-32

Providing Uninterrupted Energy with Fault Detection and Storage Method in Smart Grids

[a]Medine İzgi, [b]Mehmet Rıda Tür

[a,b]Batman University, Faculty of Engineering, Department of Electrical and Electronics Engineering, BATMAN/TURKEY

[a] yldrmedine@gmail.com

ARTICLE INFO

Article history:
Received June 15, 2024
Accepted June 26, 2024
Available online June 28, 2024

Key words:
Smart Grid
Fault Detection
Storage Systems
Electric Vehicles
Protection System
Transmission Systems

* Corresponding author.
E-mail address:
yldrmedine@gmail.com

ABSTRACT

The implementation of smart grids necessitates an upgraded protection system to enhance reliability. When a fault occurs within the electricity network, affecting either transmission or distribution systems, it often leaves a large area without power until the issue is resolved. Identifying and addressing the root cause of such malfunctions is typically a time-intensive process. Fault localization and network repair time are crucial factors for energy companies, as quicker troubleshooting can mitigate manpower demands and economic losses. This study proposes a modernized protection system designed to deliver rapid protection responses and facilitate swift repair operations during both internal and external faults, supported by energy storage solutions. Smart grid technology introduces a bidirectional power system and grid transformation, which streamlines power transmission and expedites the recovery of fault-affected areas. Frequent power outages are a significant concern for both energy companies and consumers. Faults in power systems typically result in voltage drops within the affected regions and are often caused by various disturbances in the transmission and distribution lines. Consequently, addressing failures in smart grids with the aid of storage methods and support from electric vehicles can ensure uninterrupted power supply.

1. Introduction

Smart grids (SG) are defined as an electrical power system that uses information exchange and control technologies, distributed computing, and associated sensors and actuators to provide customer-oriented power and ensure safe, reliable energy [1]. By integrating distributed energy resources, advanced sensing technologies, control methods and communication technologies into the electrical grid, PVs offer the opportunity to operate intelligently with bi-directional power flow and self-healing ability [2,3]. As shown in Figure 1, the AŞ is divided into different areas in accordance with the standard IEC 62913-1 ED2. These areas are described by the Smart Grid Architectural Model (SGAM) defined using the Architectural Approach [4] and include different sections such as mass generation, transmission, distribution, DEC, customer locations and cross-sectional area. Furthermore, the distribution field is divided into three categories: distribution network management, microgrids (MG), and smart substation automation.

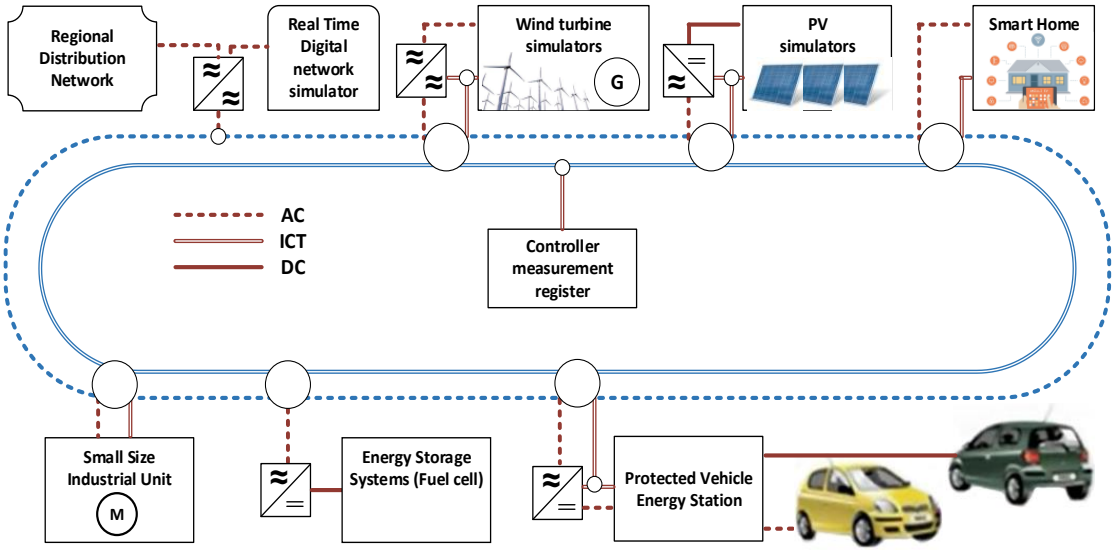


Figure 1. Main components of the smart grid system

The integration of more renewable energy sources (RES), storage systems and control devices into the distribution grid will guarantee system reliability, increase system resistance and keep current and voltage within safe ranges. However, the integration of more and more different technologies into the grid, if not handled appropriately, will lead to an increasing number of significant failure points, subsequently causing cascading failures and power outages [5]. Therefore, an appropriate fault management system [6,7] is necessary to detect, classify, localize, diagnose, isolate and repair faults to restore the system to normal function. One of the key features of PVs is the ability to self-heal by detecting and isolating outages and faults, reducing the frequency of faults, rescheduling grid resources to prevent critical situations, maintaining service continuity of the electric grid under all conditions, and shortening outage repair time [9,10]. To ensure this self-healing ability, stability, and improved system performance, fault diagnosis and positioning are important, as undesirable effects such as power outages and component failures can be reduced [11].

Detection and isolation of abnormal events are the focus of fault diagnosis [12]. The diagnostic process begins after detection. The type of existing problem and its possible causes are determined by diagnosing the severity of the problem. It can also help evaluate whether there is a fault developing that is not yet large enough to threaten the system [13]. The main considerations when developing a fault localization strategy are to locate and intervene in a power outage within the system, to improve the fault detection procedure, and to decide whether an online or offline localization approach will be used [14]. As more generation resources based on inverters, sensors, and communication systems are added to PV systems, more accurate fault location algorithms, fault predictions, and privacy-preserving schemes are needed [15,16]. More dynamic and unbalanced loads, intermittent and unbalanced generation sources, various operating modes (coupled, isolated, interconnected), different topologies (star, ring, mesh or interconnected), different fault points and various conductor sizes make fault localization a critical will make it a duty. Moreover, fast communication, significant fault current biases, and high sampling rates are required for the integration of low line impedance direct current (DC) microgrids [17].

2. Function Phasor Measurement Units to Improve the Protection System of Smart Grid

Phasor Measurement Units (PMU) use time synchronization to take real-time measurements at different remote points of an electrical grid. These devices are considered one of the most critical measuring devices of smart grids [18]. PMUs can be used as standalone devices or integrated into protective relays or other devices. PMUs detect transient waveforms created by faults, providing mathematically defined phasors. A PMU measures 50/60 Hz AC waveforms of voltage, current and phase, typically at a rate of 6-60 samples per second. Analog AC waveforms received from voltage or current signals are converted

into analog-digital signal (A/D) for each phase [19]. A GPS-powered phase lock oscillator is used as the reference source to provide high-speed synchronized sampling and operates with an accuracy of 1 microsecond. The resulting time of the phasors is transmitted to a local controller or a remote receiver at rates of 6 to 60 samples per second [20].

Transferring electrical energy from generating stations and units to system end terminals requires overhead lines and equipment at different stages [21]. This process involves increasing and decreasing voltage at subtransmission and substations within the transmission system. Electric power grid systems have been in existence for over 50 years. However, with the increasing power demand, the power system network has become more reliable in recent years and its advantages have begun to be better used. Beyond increasing power demand, several factors have caused changes in power grid systems. First, the increasing interest in distributed energy generation is notable. Secondly, the European Union has turned to renewable energy sources to significantly reduce greenhouse gas emissions in the fight against climate change. According to the Kyoto Protocol, Europe uses more renewable energy than any other region worldwide. Finally, reducing CO_2 emissions, efforts to increase energy efficiency, deregulation or competition, and diversification of energy sources are encouraging improvements in the electric power grid of the future [22].

Substations contain the major electrical equipment used in transmission and distribution systems and are used to monitor and control power fluctuations. In substations, the high voltage carried is stepped down to increase the current while maintaining the same power [23]. The main equipments are:

- Preventive maintenance and Transformers
- Lighting disconnect switches
- Electrical networks and feeders
- Circuit breakers and re-openers for protection systems
- Digital and electromechanical relays for monitoring and controlling network protection
- Fixed VAR compensators and Control building

2.1. Relays in Protection Systems

Relay applications have been used for 100 years to protect power systems. The technology used in making relays has improved significantly in terms of size, weight, cost and functionality. Relays can be classified according to technology and intended use [24]:

- It is the first type of relay used. Since it is based on a mechanical force principle, it is heavier and has lower response speeds than other technologies.
- Emerged in the early 1960s and are based on analog electronic circuits. Although static relays provide advantages over electromechanical relays, they also have some disadvantages.
- Uses analog-to-digital converters (ADC) to sample incoming analog signals and uses microprocessors to define relay logic. High accuracy and multifunctional algorithms are the main benefits of this technology.
- Works with a specific digital signal processor and performs specific digital signal processing applications.

The performance of a relay in a power system is related to the following characteristics [25]:

- It is the ability of the relay to operate correctly. Reliability has two elements: Certainty to act correctly when errors ocur and the ability to avoid unnecessary actions.
- The ability of the relay to ensure continuity of supply by disabling the minimum section required to isolate the fault.

- Ability of the relay to achieve the minimum operating time to clear a fault, thus preventing damage to equipment.
- The ability of the relay to recognize any change or abnormal operating condition exceeding a certain threshold value.

3. Improving the Protection System of Smart Grid

The future of the electric power grid is expected to evolve with the integration of new Technologies [26, 27]. One of the goals of the future smart grid is to improve the protection system to increase efficiency and reliability. In this context, the application of self-healing automation systems in medium voltage (MV) and low voltage (LV) networks is among the steps taken to improve the protection systems of the smart grid [28]. An advanced protection system using a self-healing method in the distribution systems of smart grids is introduced through the application of advanced sensors and Intelligent Electronic Devices (IED) [29]. Optimization of power grid operation is another goal involving protection automation. Reducing loss and downtime increases the reliability of supplying power to consumers with high efficiency and quality [30]. One of the aims of implementing self-healing systems in smart grids is to increase the continuity of uninterrupted power supply [31]. Distribution is the final stage of the electrical power grid and involves the transmission of electrical power to consumers. Power system automation protection includes fault localization, isolation of the area affected by the fault, and restoration of power to unaffected areas. This is the most important technique for improving power networks. When errors occur in the distribution systems of power grids, the change of voltage, current and phase signals can be detected and recorded using smart devices and PMUs (Phasor Measurement Units). These smart devices can be used to locate, update and retrieve data related to grid status in real time. Nowadays, this includes advanced scenarios using protection systems that involve fault detection and quickly isolating the affected area from the mains supply. Circuit breakers are the main cause of outage and power loss and isolate the main supply and feeder to the distribution network. This makes islanded protection systems more complex and requires the use of low-cost advanced electrical devices to integrate appropriate protection algorithms, islanded operation, and reliability [32].

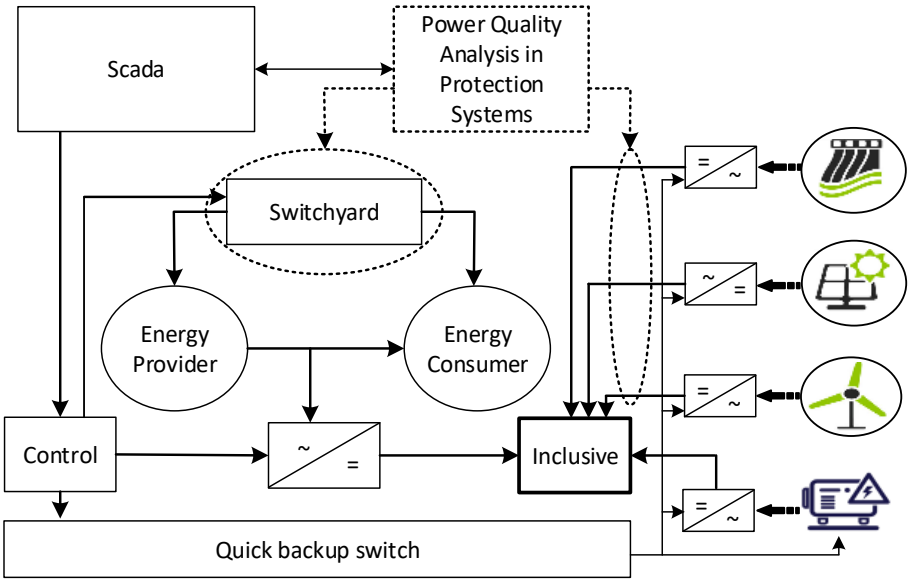


Figure 2. Distributed renewable energy and an integrated protection, monitoring and control system [32]

3.1. System Stability Maintenance and Error Detection Techniques

In order to ensure the stability of the system after the detection of a fault event, it is critical to determine the fault location geographically [33]. In the literature, various techniques are used to determine the

location of a fault in the system [34, 35]. While the frequency component and line parameters are used in the phasor-based method, the temporal components of the signals and distributed line parameters are used in the time domain-based method [36]. For example, the phasor-based method relies on traveling waves for the high-frequency components and phasor quantity for the fundamental frequency. The time domain-based method, on the other hand, determines the power outage using expert systems, neural networks or fuzzy logic [37]. Additionally, phasor angle measurements between buses in the system are used in the Gauss Markov method to determine the error [38]. The authors state that examining the lines from one or both ends can detect the fault using the impedances of the source [39, 40].

Measurements of voltage sags and swells can be used to identify faults affecting the system during short circuit events. When a large load is turned off, a large switching capacitor bank is turned on or off, and a transmission line is turned off, the RMS voltage on the faulty line decreases, a phenomenon known as voltage sag. The RMS voltage on the non-faulty line increases to determine the voltage rise [41, 42]. Another method used to find the fault in the system is State Estimation, which is a mathematical method. This method is used to determine voltages at each node in the SG and analyzes only the main grid current, ignoring other sources [43]. However, many of these methods may lack accuracy depending on the size of the power network.

3.2. Smart Grid System Examined

The proposed SG has been validated as shown in Figure 3. This represents a three-line SG supplying electricity to a town and consists of 8 MVA solar power plants, a 4.5 kVA wind turbine, 15 MWA diesel generator, a 100 kilometer transmission line and approximately 10 MVA loads and 4 MW (100*40kW) electric vehicles as storage systems. It has been stated that voltage and current changes should be within ±10% to maintain the stability of the system. In this study, power failure was detected after the current exceeded its rated values at any point. In the faulty case, the position where the current increased the most was accepted as the faulty load. The power fault must be detected within 10 ms - 50 ms and located within three cycles. The faulty load should be isolated after three cycles and the stability of the non-faulty parts of the SG should be ensured.

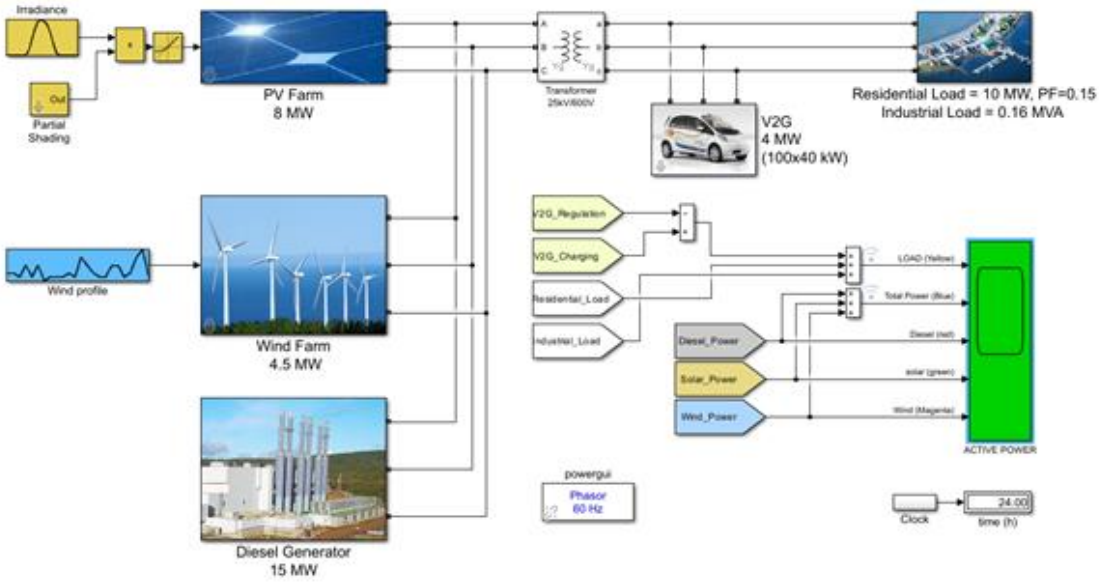


Figure 3. 24-Hour Simulation of V2G System as Storage Model

The first environment allows the user to build the system, compile it, and check for compilation errors. Once the model has been compiled without errors, the model is ready to be executed in the second environment, as a direct working model of the RSCAD software. The electric vehicle battery model used in the first model is used as storage technology to provide an uninterrupted energy system by being activated during line failure. RSCAD has a component library that allows users to control and interact with the simulated model with push buttons, control switches, gauges, and other components. If breakers are used, opening and closing operations are carried out by control switches. The hardware can be a PV or a relay. This feature allows users to connect RTDS to communicate with RSCAD and allows them to implement more complex condition expressions such as loops, conditionals, and looping expressions.

In this study, these features were used to isolate the faulty load three cycles after detecting the power fault in the system. Power failure is determined by the current exceeding its rated values. The following steps were followed to complete this study:

1. Measure the current at the "P" positions and record them in graduations.
2. Apply and save short circuit fault.
3. Detect the fault if the current exceeds its rating at any "P" position.
4. Re-measure the currents in all "P" positions and record as a fault.
5. Calculate the rate of change at all positions and record it as a fault.
6. Find the position where ΔI is maximum (max(ΔI)) and consider it as the faulty position.
7. Use the circuit breaker associated with the faulty line to disconnect the faulty load and remeasure the currents in all "P" positions.
8. Commission the storage system during the outage.
9. Compare the energy supplied to the grid with the energy stored at low prices.
10. Perform a benefit-cost analysis of the designed model.

The test model provides uninterrupted energy to the loads as long as the three-line, 8 MVA solar power plant, 4.5 kVA wind turbine and 15 MWA diesel generator produce energy. With the decrease in solar energy production and wind energy production shown in Figure 4, the supporting diesel generator comes into play. In case of long-term outages where this is insufficient, 100 electric vehicles with a capacity of 40 kW integrated into the system provide uninterrupted and low-cost energy with storage support of 4 MW capacity.

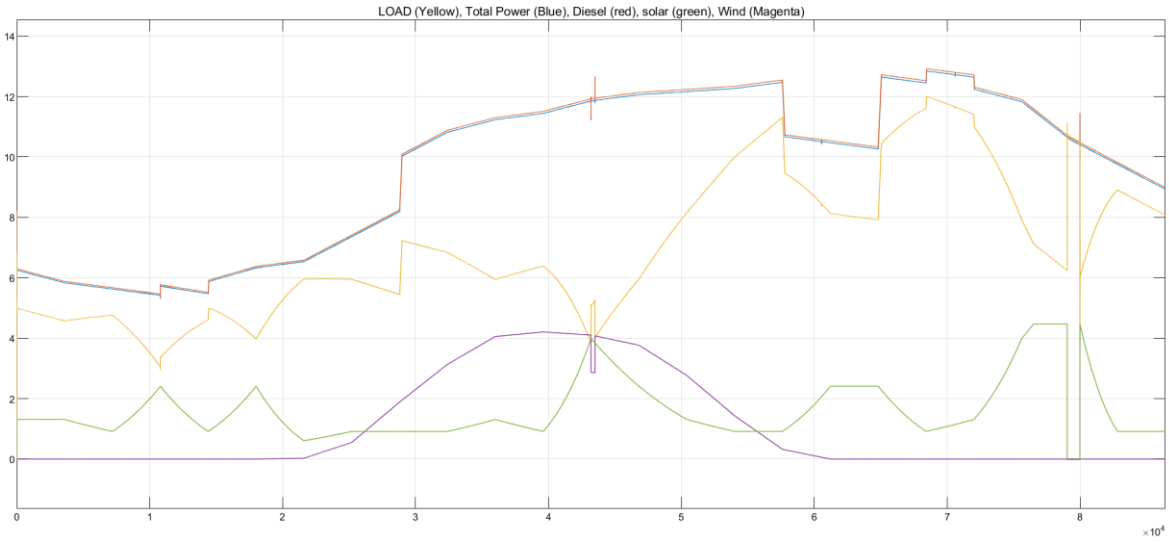


Figure 4. Solar power plant, Wind turbine, Diesel generator energy production change

Indicators P1, P2 and P3 in Figure 5 represent measurement locations defined as station solar power plants, wind turbine, diesel generator, respectively. These measuring units provide measured currents at each location during normal operation, faulty condition and after isolating the faulty load. Indicators S1,

S2 and S3 represent circuit breakers programmed in the Matlab file to isolate the faulty load. Matlab/Simulink allows the user to select the fault type and location to be applied to the system. A three-phase earth fault is considered the most severe fault type to the proposed SG and is applied at t = 1 s; The system is run for 3 s while clearing at t = 2 s. The fault location is located in the distribution line of load 4. Additionally, the system was examined in Real Time Digital Simulation (RTDS) to ensure the robustness of the proposed fault management techniques. The RTDS platform allows users to apply faults at any time during operation.

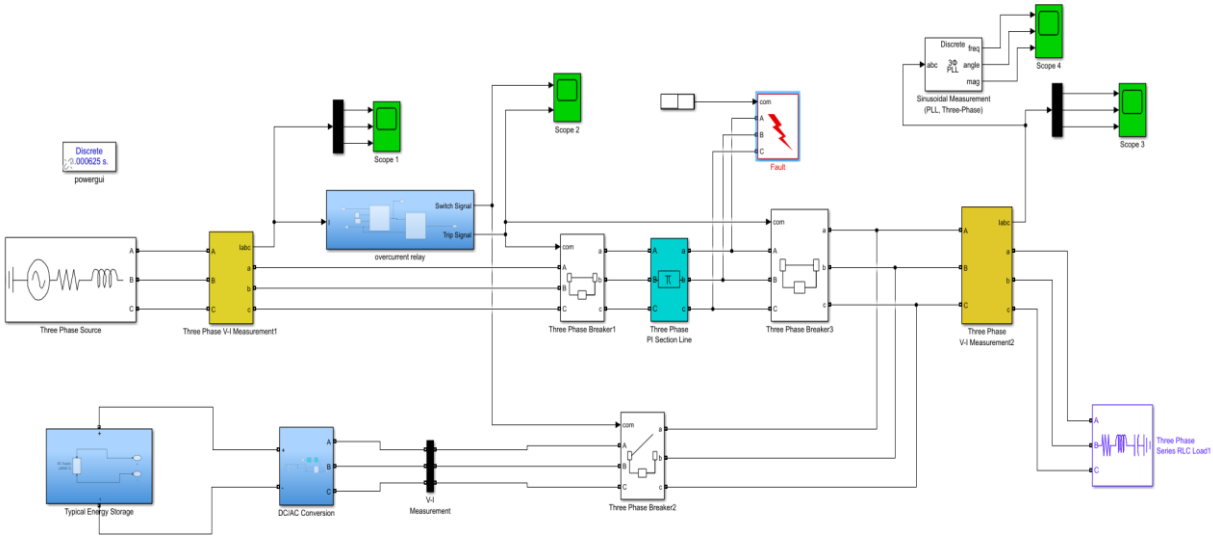


Figure 5. Integration of the Storage Model into the system as an Electric Vehicle

RTDS is a digital power system simulator consisting of advanced computer hardware and software operating in real time [52][53]. It is considered an ideal protection and control tool for the design and development of power systems and SG [53]. RTDS is characterized as a fast processor simulator thanks to its simultaneously executed procedures. RSCAD software has an extensive component library and offers the ability to simulate a large number of components. RSCAD consists of two main interconnected environments and allows users to run and execute the simulated model.

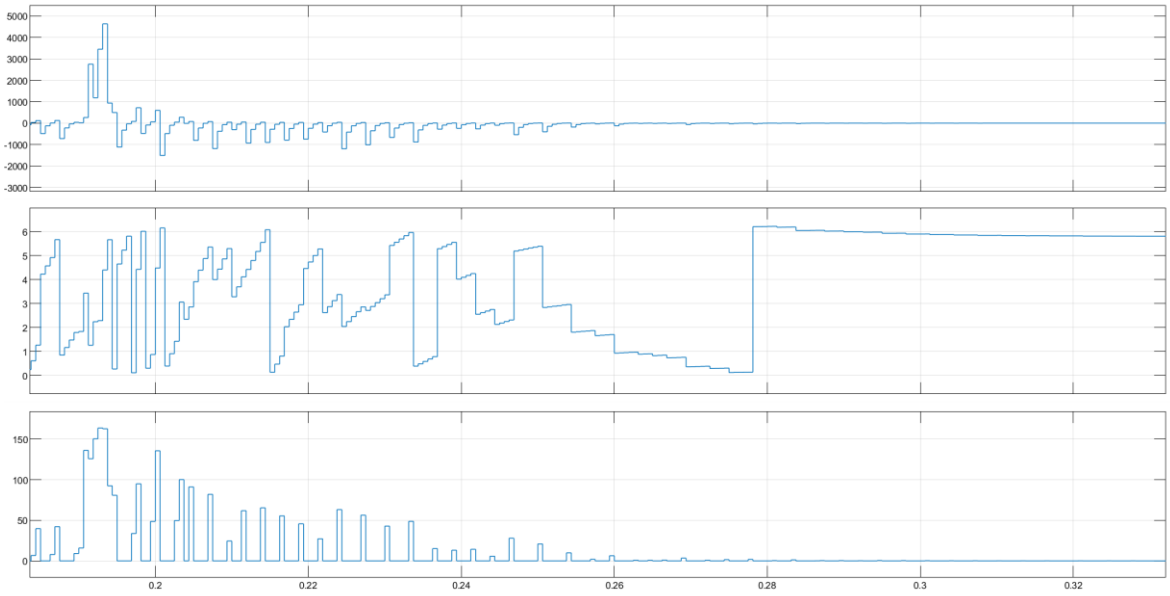


Figure 6. SG allowed error variation between 20 ms and 30 ms

Energy is provided from electric vehicles as a storage system in order to prevent the loads on the 100-kilometer transmission line from being left without energy after a fault occurs in the system between 20ms and 30ms.

The performance of the SG has been comprehensively examined by comparing it with the results of the model designed in the Matlab/Simulink environment. The user was allowed to apply errors during operation between 20 ms and 30 ms, during which time the error was implemented on the model. After the applied error, the current waveform was recorded and this waveform is presented in Figure 6.

Figure 6 shows in detail the error detection time of the designed SG and how the current changes over time. The peak value of the last normal signal was measured at 0.02 seconds, and immediately after this value the fault current exceeded the maximum rated current at 0.028 seconds. This is a sign that there is an abnormality in the system.

By taking the differences of Planned Production (MWh), Actual Production (MWh), Actual Consumption (MWh), the Actual and Planned Production (MWh) value is obtained as 2,059,021 MWh for a month on an hourly basis shown as Figure 7. When the parameter between these two values is multiplied by the system marginal price for the real power system, it is determined that 4.547.563,79 TL of energy is provided by storage. This power value, defined as a large value, will prevent customers from being left without energy.

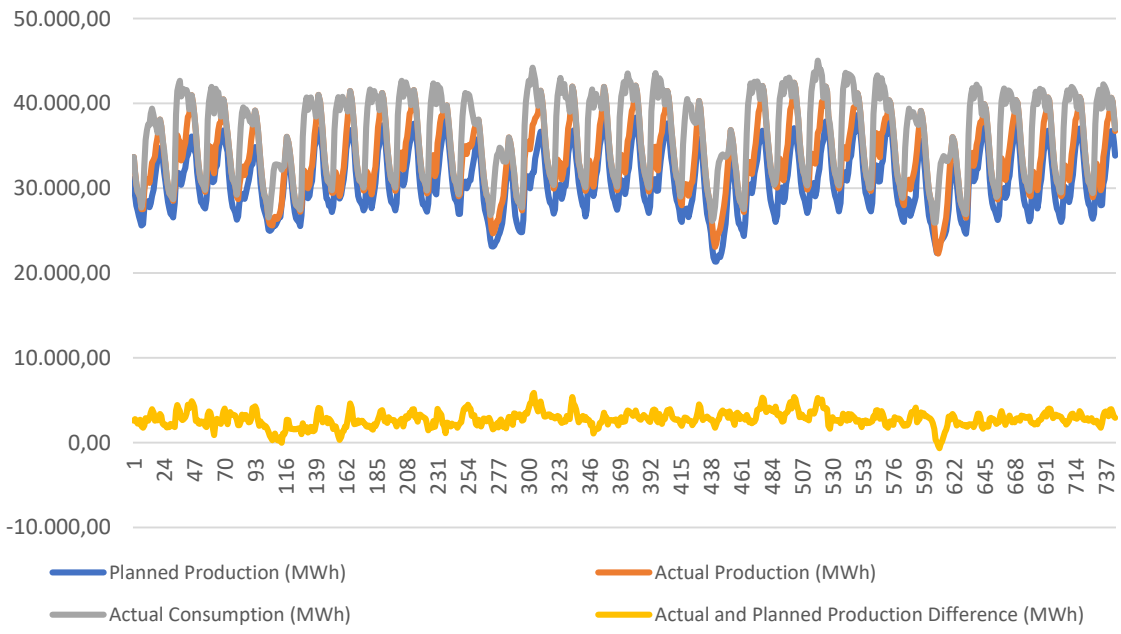


Figure 7. Planned Production (MWh), Actual Production (MWh), Actual Consumption (MWh), the Actual and Planned Production (MWh)S allowed error variation between 20 ms and 30 ms

The time it takes for the system to detect the error after the error is implemented is of critical importance. The designed SG required approximately 8 milliseconds to detect the error. This rapid detection time demonstrates the effectiveness and reliability of SG. This period ensures the system's ability to react quickly and possible malfunctions are quickly isolated and the rest of the system remains stable. These results show that the designed SG is successful in real-time error detection and isolation and is compatible with Matlab/Simulink simulations. The fast response time of the system plays an important role in increasing system reliability and performance by minimizing power outages.

3. Conclusion

This article underscores the critical importance of swift responses to power faults to protect components and prevent outages within SG. The study concentrated on detecting, locating, and isolating faulty lines using Matlab/Simulink and RTDS software. It discusses the application of phase-to-ground short circuit faults in SG and the detection of these faults within milliseconds. Upon fault detection, breakers were used to isolate the faulty line from the system. Simulation results indicate that isolating the faulty load enhances SG stability and ensures customer satisfaction. The processes of error detection, location, and isolation were elaborated using Matlab/Simulink and RTDS software. A phase-to-earth short circuit fault was implemented, and the time required for SG to detect the fault was analyzed. The faulty load was isolated within three cycles. Additionally, electric vehicle batteries were utilized as storage technology to provide uninterrupted energy. These vehicles supplied energy support during extended outages. The performance of SG was compared using Matlab/Simulink results, and the error detection time was found to be 8 milliseconds. This rapid detection time demonstrates the effectiveness and reliability of SG. In conclusion, the paper presents proposed solutions and simulation results for managing and isolating potential power faults in SG. The study's findings are significant for enhancing SG reliability and ensuring customer satisfaction.

References

[1] IEC SRD 62913-1; Generic Smart Grid Requirements—Part 1: Specific Application of the Use Case Methodology for Defining Generic Smart Grid Requirements According to the IEC Systems Approach. IEC: Geneva, Switzerland, 2022.

[2] Sarwar, M.; Asad, B. A review on future power systems; technologies and research for smart grids. In Proceedings of the 2016 International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, 18–19 October 2016; pp. 1–6.

[3] Agüero, J.R. Applying self-healing schemes to modern power distribution systems. In Proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012; pp. 1–4.

[4] Estebsari, A.; Barbierato, L.; Bahmanyar, A.; Bottaccioli, L.; Macii, E.; Patti, E. A SGAM-Based Test Platform to Develop a Scheme for Wide Area Measurement-Free Monitoring of Smart Grids under High PV Penetration. Energies 2019, 12, 1417.

[5] Haes Alhelou, H.; Hamedani-Golshan, M.E.; Njenda, T.C.; Siano, P. A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges. Energies 2019, 12, 682.

[6] Stefanidou-Voziki, P.; Sapountzoglou, N.; Raison, B.; Dominguez-Garcia, J. A review of fault location and classification methods in distribution grids. Electr. Power Syst. Res. 2022, 209, 108031.

[7] De La Cruz, J., Gómez-Luna, E., Ali, M., Vasquez, J. C., & Guerrero, J. M. (2023). Fault location for distribution smart grids: Literature overview, challenges, solutions, and future trends. Energies, 16(5), 2280.

[8] Jadidi, S.; Badihi, H.; Zhang, Y. Fault Diagnosis in Microgrids with Integration of Solar Photovoltaic Systems:A Review. IFACPapersOnLine 2020, 53, 12091–12096.

[9] Baidya, S., & Nandi, C. (2022). A comprehensive review on DC Microgrid protection schemes. Electric Power Systems Research, 210, 108051

[10] Annaswamy, A.M.; Amin, M. IEEE Smart Grid Research IEEE Vision for Smart Grid Controls: 2030 and Beyond Reference Model; IEEE Press: Piscataway, NJ, USA, 2013.

[11] Andresen, C.A.; Torsaeter, B.N.; Haugdal, H.; Uhlen, K. Fault Detection and Prediction in Smart Grids. In Proceedings of the 2018 IEEE 9th InternationalWorkshop on Applied Measurements for Power Systems (AMPS), Bologna, Italy, 26 28 September 2018; pp. 1–6.

[12] Sarathkumar, D.; Srinivasan, M.; Stonier, A.A.; Samikannu, R.; Dasari, N.R.; Raj, R.A. A Technical Review on Self-Healing Control Strategy for Smart Grid Power Systems. IOP Conf. Ser. Mater. Sci. Eng. 2021, 1055, 012153.

[13] Mousa, M.; Abdelwahed, S.; Kluss, J. Review of Fault Types, Impacts, and Management Solutions in Smart Grid Systems. Smart Grid Renew. Energy 2019, 10, 98–117.

[14] Mahmoud, M. A., Md Nasir, N. R., Gurunathan, M., Raj, P., & Mostafa, S. A. (2021). The current state of the art in research on predictive maintenance in smart grid distribution network: Fault's types, causes, and prediction methods—A systematic review. *Energies*, *14*(16), 5078.
[15] Chai, E.; Zeng, P.; Ma, S.; Xing, H.; Zhao, B. Artificial Intelligence Approaches to Fault Diagnosis in Power Grids: A Review. In Proceedings of the 2019 Chinese Control Conference (CCC), Guangzhou, China, 27–30 July 2019.
[16] Furse, C.M.; Kafal, M.; Razzaghi, R.; Shin, Y.-J. Fault Diagnosis for Electrical Systems and Power Networks: A Review. IEEE Sens. J. 2020, 21, 888–906
[17] Biswal, C., Sahu, B. K., Mishra, M., & Rout, P. K. (2023). Real-time grid monitoring and protection: A comprehensive survey on the advantages of phasor measurement units. Energies, 16(10), 4054.
[18] Al-Hammouri, A. T., Nordström, L., Chenine, M., Vanfretti, L., Honeth, N., & Leelaruji, R. (2012, July). Virtualization of synchronized phasor measurement units within real-time simulators for smart grid applications. In 2012 IEEE Power and Energy Society General Meeting (pp. 1-7). IEEE.
[19] Klein, M. E. (2010). Autonomous ultra-low power ELF/VLF receiver systems (Doctoral dissertation, Stanford University).
[20] Kiessling, F., Nefzger, P., Nolasco, J. F., & Kaintzyk, U. (2014). Overhead power lines: planning, design, construction. Springer.
[21] Cirman, A., Domadenik, P., Koman, M., & Redek, T. (2009). The Kyoto protocol in a global perspective. Economic and business review, 11(1), 3.
[22] Hussain, S., Fernandez, J. H., Al-Ali, A. K., & Shikfa, A. (2021). Vulnerabilities and countermeasures in electrical substations. International Journal of Critical Infrastructure Protection, 33, 100406.
[23] Horowitz, S. H., Phadke, A. G., & Henville, C. F. (2022). Power system relaying. John Wiley & Sons.
[24] Kiliçkiran, H. C., Şengör, İ., Akdemir, H., Kekezoğlu, B., Erdinç, O., & Paterakis, N. G. (2018). Power system protection with digital overcurrent relays: A review of non-standard characteristics. Electric Power Systems Research, 164, 89-102.
[25] Tür, M. R., Wadi, M., Shobole, A. A., & Gündüz, H. (2021). Integration problems of photovoltaic systems-wind power, solutions and effects on power quality. European Journal of Technique (EJT), 10(2), 340-353.
[26] Shobol, A., Ali, M. H., Wadi, M., & TüR, M. R. (2019, November). Overview of big data in smart grid. In 2019 8th International Conference on Renewable Energy Research and Applications (ICRERA) (pp. 1022-1025). IEEE.
[27] Shobole, A. A., & Wadi, M. (2021). Multiagent systems application for the smart grid protection. Renewable and Sustainable Energy Reviews, 149, 111352.
[28] Huynh, T. P., Sonar, P., & Haick, H. (2017). Advanced materials for use in soft self-healing devices. Advanced Materials, 29(19), 1604973.
[29] Tur, M. R. (2020). Reliability assessment of distribution power system when considering energy storage configuration technique. IEEE Access, 8, 77962-77971.
[30] Arefifar, S. A., Alam, M. S., & Hamadi, A. (2023). A review on self-healing in modern power distribution systems. Journal of Modern Power Systems and Clean Energy, 11(6), 1719-1733.
[31] Temiz, R., & Tür, M. R. (2024). Investment technique for ensuring energy supply continuity in ring grids. Turkish Journal of Engineering, 8(2), 186-195.
[32] Dashti, R., Daisy, M., Mirshekali, H., Shaker, H. R., & Aliabadi, M. H. (2021). A survey of fault prediction and location methods in electrical energy distribution networks. Measurement, 184, 109947.
[33] Chen, K., Huang, C., & He, J. (2016). Fault detection, classification and location for transmission lines and distribution systems: a review on the methods. High voltage, 1(1), 25-33.

[34] Chen, K., Huang, C., & He, J. (2016). Fault detection, classification and location for transmission lines and distribution systems: a review on the methods. High voltage, 1(1), 25-33.

[35] Theodoro, T. S., Tomim, M. A., Barbosa, P. G., Lima, A. C., & de Barros, M. T. C. (2019). A flexible co-simulation framework for penetration studies of power electronics based renewable sources: A new algorithm for phasor extraction. International Journal of Electrical Power & Energy Systems, 113, 419-435.

[36] Ramesh, M., & Laxmi, A. J. (2012, January). Fault identification in HVDC using artificial intelligence—Recent trends and perspective. In 2012 International Conference on Power, Signals, Controls and Computation (pp. 1-6). IEEE.

[37] Cao, X., Stephen, B., Abdulhadi, I. F., Booth, C. D., & Burt, G. M. (2015). Switching Markov Gaussian models for dynamic power system inertia estimation. IEEE Transactions on Power Systems, 31(5), 3394-3403.

[38] Das, S., Santoso, S., Gaikwad, A., & Patel, M. (2014). Impedance-based fault location in transmission networks: theory and application. IEEE access, 2, 537-557.

[39] Ghaderi, A., Ginn III, H. L., & Mohammadpour, H. A. (2017). High impedance fault detection: A review. Electric power systems research, 143, 376-388.

[40] Gitau, M. N., & Kala-Konga, C. L. (2010, November). Multilevel switched-capacitor DC-DC converter with reduced capacitor bank. In IECON 2010-36th Annual Conference on IEEE Industrial Electronics Society (pp. 576-581). IEEE.

[41] Ali, S. A. (2011). Capacitor banks switching transients in power systems. Energy Science and Technology, 2(2), 62-73.

[42] Mehranbod, N., Soroush, M., & Panjapornpon, C. (2005). A method of sensor fault detection and identification. Journal of Process Control, 15(3), 321-339.