International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 08, ISSN No. 2455-2143, Pages 09-21
Published Online December 2023 in IJEAST (http://www.ijeast.com)

STANDARDS AND NEW ICT TECHNOLOGIES IN THE FUNCTION OF IMPROVEMENTSAFETY AND PROTECTION OF PHOTOVOLTAIC POWER PLANTS

Prof.dr. Adis Rahmanović
University of Travnik
Faculty of Technical Studies,
Travnik & Coal mine, Banovici,
Bosnia and Herzegovina

Doc.dr. Maid Omerović
University of Travnik,
Faculty of Technical Studies,
Travnik, Bosnia and Herzegovina

MSc. Haris Berkovac
University of Travnik,
Faculty of Technical Studies,
Travnik & BH Telecom, Sarajevo,
Bosnia and Herzegovina

MSc. Marko Serdar
E.ON Zagreb, Croatia

Abstract – **Sustainable development as an imperative imposes an energy transition in which fossil fuel power plants will be replaced by renewable sources, with solar power plants having the largest share. However, the challenges that new power systems have to deal with mostly come from the domain of security and protection, a topic that we will mostly deal with through the application of new standards and ICT technologies during the preparation of this article. The aim of this article is to show the challenges but also the potential of improving safety, technical and electrical protection at Photovoltaic Power Plants by applying new standards and ICT technologies, but also to show the results and benefits of the timely application of adequate safety and protection measures. At the very beginning, we show the basic features of safety, technical and electrical protection at Photovoltaic Power Plants, then we show new standards and new ICT technologies, and through their application we show the potential of improving safety and protection, as well as the accompanying benefits from timely and adequate application of them at Photovoltaic Power Plants.**

Keywords – **Cyber security and protection, Standards and new ICT technologies, Advanced security and protection measures for Photovoltaic power plant, Benefits of adequate security and protection measure at the PV power plant.**

I. INTRODUCTION

Considering the current share of RES, with a special focus on Photovoltaic power plants in the total production of electricity, but also the trend of a multiple increase in the share, it is clear that they will be key factors for the normal functioning of the power system. Any undesirable influence on their work would represent a serious blow to the normal functioning of the power system, and indirectly to the state or a group of related states in the common power system as a whole. For this reason, electric energy is placed first on the list of 10 critical infrastructures for most advanced countries, although currently the share of uncertainty is significantly lower than some other areas, but the accompanying trend and estimates will also be drastically changed in a short period, and it is connected with the

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 08, ISSN No. 2455-2143, Pages 09-21
Published Online December 2023 in IJEAST (http://www.ijeast.com)

expansion investments in this area and a significant increase in their impact.

II. SAFETY AND PROTECTION OF PHOTOVOLTAIC POWER PLANTS

In the previous period, there was an increase in cyber attacks on critical infrastructures, and the projections indicate an increasing risk of cyber attacks on critical infrastructures, because due to new technologies such as the increasing availability of the Smart concept, IoT technology, the improvement of ICT infrastructure and appropriate Internet connections, but also artificial intelligence, ever-increasing investments in advanced technologies, but also the imperative of sustainable development, the ever-increasing number of power plants and their dispersion and dispersion. Cyber attacks on the power sector are becoming more and more intense and sophisticated, and the impact of cyber attacks in this area is becoming more and more dangerous, increasing investments, but also the need for electricity. The main reasons that increase the vulnerability of the power sector are:

- ✓ Fast pace of technological innovations applied in the domain of new Photovoltaic power plants;
- ✓ Increasing sophistication of cyber attacks, using newly developed tools and advanced technologies;
- ✓ The attractiveness of the sector as a cybernetic target, due to increasing investments, greater impact of such power plants on sustainable development and consumer dependence.

"In the EU, critical infrastructure service providers must notify their country's national authorities of cybersecurity incidents with a significant impact. At the end of each year, ENISA (European Union Agency for Cybersecurity) collects and analyzes summary reports on these incidents." ENISA [Internet] 2005-2023 by the European Union Agency for Cybersecurity [cited 2023 May. 22]. Available at: https://www.enisa.europa.eu/topics/critical-information-infrastructures-andservices. The share of attacks on the energy sector is for 2021/22. was 6, with a constant upward trend. The calculated damage done according to these data, only in the domain of decommissioning of certain power plants and lost user hours, was measured in hundreds of millions of €, while adding up other indirect damage, it produces a much larger total damage, with significant increases, as the number of such power plants increases. builds, as they have an increasing dispersion, but also a common importance for the increasing number of devices and drives that supply electricity. energy, but also by incorporating advanced technologies, with accompanying ICT infrastructure and ICT services, can have two directions of influence, positive, connected to easier management, availability, greater efficiency, effectiveness, better environmental parameters, production of economically profitable kilowatts, but also the negative one through the production of a series of risks, both in the field of security and in the field of technical and electrical protection. Based on this, we create a hypothesis: Appropriate implementation and application of standards and new ICT technologies can significantly contribute to the improvement of safety, technical and electrical protection of photovoltaic power plants, which involves a number of benefits, but also challenges, which we will try to confirm through the following content.

III. CYBER ATTACKS AS SECURITY CHALLENGES FOR PHOTOVOLTAIC POWER PLANTS

The number and types of attacks on electric power infrastructure, follows the development, significance, impact, but also the development of knowledge, the appearance of errors, automated scripts, new hacker software tools, but also new ICT infrastructure through IoT and smart technologies, but the possibilities of advanced technologies such as artificial intelligence and Fig. Hacking is a situation when a person uses the identity of another person with the intention of accessing ICT infrastructure and ICT services. This can be done through impersonation, or identity masking. Computer infrastructure protection systems should act actively in order to detect and prevent such fraud, this segment is improving more and more intensively, but it is also facing constant challenges. Physical impersonation occurs when the perpetrator uses an authorized user identity, access card, additional authentication elements, e.g. alienated smart device, etc. in order to access classified areas and gain unauthorized access to ICT infrastructure, supporting services and data. Electronic impersonation refers to the situation when the perpetrator uses legitimate user identification data, such as a username or password, but additional verification mechanisms of SIM cards, smart devices, etc., in order to log into the ICT system without authorization and illegally access data and information. .

Types of cybernetic attacks on photovoltaic power plants can be grouped into several groups described below:

- ✓ SERVER AND COMPUTER SABOTAGE

Server and computer data are increasingly valuable assets, and it often happens that their value is higher than the case of physical assets. This is especially visible in the IT sector, but in the domain of managing various systems that have increasing importance and influence, such as the power system. The value of programs, applications or source code, digital data can be greater than the value of the building in which these data are located. Constant investment in sustainable development, where due to the concept of sustainable development, the development of advanced technologies, there is a significantly greater need for electricity, which is to be replaced by renewable energy

sources where solar power plants have an increasing share, leads to increasing complexity on the one hand of such systems , with a huge increase in ICT services, ICT infrastructure, automated procedures and advanced technologies with the accompanying increasingly large and valuable digital data resource, which also in this domain confirms the importance and value of computer data in the modern business world.

✓ SABOTAGE OF SERVER, STORAGE AND COMPUTER SYSTEMS

The above-mentioned types of resources are stored on some server and data warehouses, and various computer systems, supporting applications and databases are installed on them, which it is important to ensure that they have as little disruption as possible. When it comes to disrupting the operation of the computer system, the causes can be faulty or improperly configured equipment, computer and technical support. It is important to note that work disruption does not always have to be intentional, but can result from technical or configuration problems, insufficiently defined procedures, lack of necessary knowledge, lack of awareness, excessive curiosity, etc.. Sources of disruption can be both external and internal, whereby research the cause of the disturbance may include the detection of other criminal acts, such as unauthorized access. Special tools, known as hacker tools, are often used to interfere with the operation of the computer system, but tools are also used to test the ICT infrastructure, ICT services on the computer system and accompanying digital data, as well as to determine possible defects and activities for continuous prevention, removal and minimizing them. In order to prove such actions, it is important to find the type of tool used and in what way, but also to determine possible omissions, record damage and evidence, which is what the domain of digital forensics deals with. Special attention should be paid to the domain of security of access data both in computer systems and security data related to access and management of photovoltaic power plants.

✓ SABOTAGE OF DIGITAL DATA

It is precisely the increasing value of digital data, the increasing need, the potential for influence and use, that gives greater importance to the same, and therefore produces a whole list of risks, which lead to both potential abuse and damage to digital data, but also to ICT services, systems, leading to misuse and dysfunction of systems such as power plants or the entire power system. Discovering digital data access breaches is a challenging situation that requires proactive measures to identify changes in access or in the data itself. The research is usually focused on determining whether there was an unauthorized access, a possible change, how it happened, who caused the change and with what intention, whether it caused direct or indirect damage. The key is to first determine the previous state of the data, i.e. the state before the change, because without it it is not possible to reliably conclude whether the change has taken place. Often, the causes of data changes are attributed to technical errors or system malfunctions, avoiding responsibility, therefore it is necessary to conduct research to determine that an error or malfunction is not the source of the change, which if this approach of avoiding responsibility continues, it can lead to further development and abuse of potential defects in the system, which can cause incalculable damage.

✓ DIGITAL ESPIONAGE

Research to determine the unauthorized interception of digital data is an extremely complex process, which makes it difficult to detect interception situations. Interceptions can be realized on the basis of interception activities from inside the system, such as activities, use of flaws, errors from the outside, but most often they are a combination of activities from the outside and inside, regardless of whether it is the exploitation of consciously or unconsciously created errors. In most cases, the focus is on the discovery of copies of digital data obtained through interception (the same should be encrypted with adequate encryption), and on the basis of these found data, interception actions must be proven. During the research, it is necessary to discover the tools used for such actions, as well as the perpetrator. The mere presence of these tools is not sufficient evidence because they are often used as auxiliary means for the administration of computer systems, especially wireless computer networks, so a deeper analysis of both preventive and corrective measures implemented, as well as intensive preventive action, should be carried out in order to reduce risks. to an acceptable level. These activities should be carried out, continuously, as well as the education of the staff who carry out the improvement of security, but also the education of the staff in the domain of building awareness who use ICT services, digital data, etc.

✓ DIGITAL PIRACY

Piracy of software support can be a prerequisite for various forms of attack, both in the domain of downloading data of significant value, but also in ICT services, management and automated segments of the system of electric power facilities. Thanks to the simple duplication technology, the program support enables quick and easy copying, which confronts users with a series of dilemmas that lead to abuse, regardless of the potential consequences, but also a series of potential disadvantages of using resources acquired in this way. Software piracy means the unauthorized copying and distribution of programs that are legally protected against copying. There are various ways in which software piracy can be carried out, the most common of which are: copying by the end user, hard disk cloning, downloading software from the Internet, sending via e-mail, forgery, using unauthorized software support from the server, abuse of

virtualization capabilities, abuse digital signature, abuse of automated scripts for Backup, but also copying of borrowed program support.

✓ DIGITAL FRAUD

Digital fraud includes various types of data manipulation, they were established and initially related to financial aspects, but with increasing investments and the use of ICT services, increasing importance and influence, the number, but also the probability of the risks associated with their occurrence in the domain of electronic energy systems, increases. These manipulations can occur during the input, processing, storage, distribution of data and information, as well as when exchanging data via computer networks or communication channels. Data can be located on any digital medium. Previously, a common way of manipulation was through the action of a program such as a Trojan horse, which is a computer program that, apart from its visible purpose, also has hidden functionalities that are unknown to the user, while today, an approach such as a ransomware virus, by taking control, locking data, ICT resources, control itself it leads to various forms of blackmail, extortion, which, in addition to direct damage, can produce a number of indirect harmful effects. These functionalities include changing, deleting or adding data. Such programs often contain an order to self-destruct after manipulation, and it is possible that they are activated only after a certain period of time, which makes it even more difficult to detect illegal actions. Perpetrators of this type of attack can be programmers with detailed knowledge of computer programs, employees or former employees, system programmers, computer users and computer operators or at the request of a certain specialized group.

✓ ABUSE OF ICT AND ADVANCED TOOLS

With the intensive development and application of ICT and advanced technologies, and in the domain of modern power systems, with the construction of new photovoltaic power plants and the accompanying ICT infrastructure, we are entering new stages and phases that produce new opportunities for the misuse of ICT and advanced tools, but the misuse of them can produce more and more damage, therefore, protection systems are also being developed, great efforts are being made to improve the security domain, but also legal regulations, protocols and standards are being updated. In order to commit criminal acts of computer crime, certain hardware, software or a combination of both, prior experience and professional knowledge, as well as adequate computer equipment, but also knowledge of the functioning of the system itself, automated implementation concepts that produce possible failures, etc. are needed. The aforementioned equipment and tools have global availability, predictions state that in the future there will be more and more potential tools for the execution of criminal acts of digital crime, but also tools for prevention, control and improvement of security and protection.

IV. STANDARDS AND ACTIVITIES FOR ENSURING SAFETY MEASURES APPLICABLE TO PHOTOVOLTAIC SYSTEMS

Cyber security has become extremely important in the modern world, and increasingly in the context of the security of the power sector. The development of RES technologies, including photovoltaic systems, brings numerous advantages, but at the same time opens up new challenges in terms of safety. Photovoltaic power plants are an increasingly important source of renewable energy and accordingly become a potential target of cyber attacks. Considering the complexity and sensitivity of photovoltaic systems, it is crucial to establish appropriate legislation, directives, protocols and standards that will ensure a high level of cyber security in this industry. Their application enables photovoltaic systems to identify potential threats, protect their systems from attacks, timely detect unauthorized activities, respond to incidents, and repair and rebuild after an attack, in order to minimize potential damage. Through the analysis of legal frameworks, directives, protocols and standards, it is possible to understand the main guidelines related to the cyber security of photovoltaic systems and how the industry adapts and harmonizes with them. By considering examples of the application of these regulations in photovoltaic systems, it more clearly presents their purpose and practical application. Below is an overview of the most prominent existing legislative and normative infrastructure dealing with cyber security applicable to photovoltaic systems. Through the analysis of the relevant regulations, it is possible to see the importance and impact of these measures on the protection of photovoltaic power plants from cyber threats and to understand how the power system acts in accordance with them. Cybersecurity standards for U.S. PV systems are in the development phase, and broad working groups involving industry, federal laboratories, universities, government agencies, and standards development organizations are being formed to develop cybersecurity policies that would be applicable to a large number of system, as well as a nationally accredited standard for that. Some of the established and most relevant established standards for photovoltaic systems and plants include according to NREL (National laboratory of the U.S. Department of Energy):

- ✓ DOE/DHS ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model (ESC2M2);
- ✓ DOE/NIST/NERC Risk Management Process: Electricity Subsector Cybersecurity Risk;

for Management Process

- ✓ NIST Cybersecurity Framework;

- ✓ NIST SP 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security;
- ✓ NIST Interagency/Internal Report 7628: Guidelines for Smart Grid Cybersecurity;
- ✓ IEC 62351: Power Systems Management and Associated Information Exchange - Data and;

for Communications security

- ✓ IEC 62443: Security for Industrial Automation and Control Systems;
- ✓ IEEE C37.240-2014: IEEE Standard Cybersecurity Requirements for Substation Automation;

and for Protection, and Control Systems

- ✓ IEEE 1686: Standard for Intelligent Electronic Devices Cyber Security Capabilities;
- ✓ NERC Reliability Guideline: Cyber Intrusion Guide for System Operators;
- ✓ IEEE 1547.3: IEEE Guide for Monitoring, Information Exchange, and Control of Distributed;
- ✓ Resources Interconnected with Electric Power Systems (currently under development).

The NIS Directive (The directive on Network and Information Security, NIS) in the EU represents a key framework for the protection of networks and information systems in critical infrastructure, including the power sector. This directive aims to ensure a high level of security and resistance to cyber threats and to promote cooperation between member states in the field of cyber security. The NIS Directive obliges member states to establish national strategies for cyber security and operational plans for detecting, preventing and responding to cyber incidents. Its goal is to ensure that member states are ready to face cyber threats and have mechanisms for coordinated action in emergency situations. When it comes to photovoltaic systems, the NIS Directive also plays an important role in ensuring their cyber security. The application of the NIS Directive to photovoltaic systems aims to ensure that appropriate security measures and procedures are applied to minimize the risk of cyber attacks. This includes identifying critical system components and vulnerabilities, establishing security policies and procedures, conducting regular risk assessments, and establishing mechanisms for detecting and responding to cyber incidents. Cooperation between operators, suppliers, regulatory bodies and security agencies is also encouraged to raise cyber security awareness and share information. Through the application of the NIST Directive to photovoltaic systems, the goal is to ensure their safety and reliability and to prevent or minimize potential cyber threats that could have a negative impact on electricity production and the entire electricity infrastructure. The NIS2 Directive (The directive on Network and Information Security) is an upgrade of the first NIS directive and aims to further strengthen cyber security in the EU. This directive extends the scope to new sectors, including renewable energy sources such as photovoltaic systems. The NIS2 directive also further promotes cooperation between member states and encourages the establishment of security standards and protocols for the protection of information systems in these sectors. The CER Directive (The Critical Entities Resilience Directive) or 2022 ECI Directive is a legislative instrument of the European Union aimed at ensuring a high level of security of networks and information systems, including critical infrastructure. This directive aims to protect vital services and digital infrastructure from cyber threats and ensure their resilience to incidents. The ECI Directive obliges EU member states to identify key operators of services of general interest, including those from the electricity sector, which includes photovoltaic systems. Operators of these services are required to establish appropriate measures and security practices to prevent cyberattacks, detect incidents and ensure rapid recovery in the event of a disruption. Application to photovoltaic systems includes identification of key operators in the sector, risk assessment, implementation of appropriate security measures, and establishment of a system for detecting and responding to cyber incidents. It includes establishing security policies and procedures, ensuring secure management and monitoring of systems, and regular updating and testing of security measures. ENISA (European Union Agency for Cybersecurity) is a European agency that was founded in 2004 with the aim of improving cyber security in Europe. The Agency has an important role in promoting high standards of cyber security and providing expert advice, guidance and support to the member states of the European Union. ENISA engages in a series of activities to strengthen cyber security in Europe through consulting and providing expert knowledge, developing and improving coordination and cooperation, improving technical support and services, but also developing and promoting cyber security awareness.

V. ELECTRICAL PROTECTION SYSTEMS AT PHOTOVOLTAIC POWER PLANTS

Electrical protection systems play an important role in ensuring the safety, reliability and longevity of photovoltaic power plants and associated equipment. These systems include various elements and protection measures that ensure the proper functioning of electrical components, minimizing the risk of electrical accidents, endangerment of people, damage to equipment or interruptions in the supply of electricity. Since photovoltaic systems are located outdoors, there is a possibility of overvoltage caused by atmospheric phenomena such as lightning strikes. Such an overvoltage can be caused by a direct lightning strike into the structure or by an indirect strike near the building. This overvoltage can cause damage to the equipment and cause a fire. In addition to atmospheric overvoltages, the photovoltaic power plant can also be exposed to internal

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 08, ISSN No. 2455-2143, Pages 09-21
Published Online December 2023 in IJEAST (http://www.ijeast.com)

overvoltages. Atmospheric surges are caused by lightning strikes that can directly or indirectly affect the system. A direct lightning strike occurs when lightning strikes the structure of a photovoltaic power plant, while an indirect strike occurs when lightning strikes near a structure. This includes installing surge protectors (SPDs) at the input to direct surges to ground and reduce their harmful effects on equipment. Proper grounding and proper insulation of electrical components is also applied to reduce the risk of atmospheric surges. In the case where there is a lightning protection installation, if the photovoltaic power plant does not change the external shape of the building and the distance between the power plant and the lightning protection installation exceeds the safety distance defined by the EN 62305-3 standard, additional measures for the protection of the power plant are not necessary, again it depends on the size and position of the power plant itself. Internal overvoltages in photovoltaic power plants occur for various reasons, such as the activation of switches, oscillations in the network or other electrical disturbances within the system itself. These surges can produce short-term high voltage pulses that can damage electrical equipment. Therefore, it is important to apply appropriate surge protection measures to reduce the risk of internal surges.

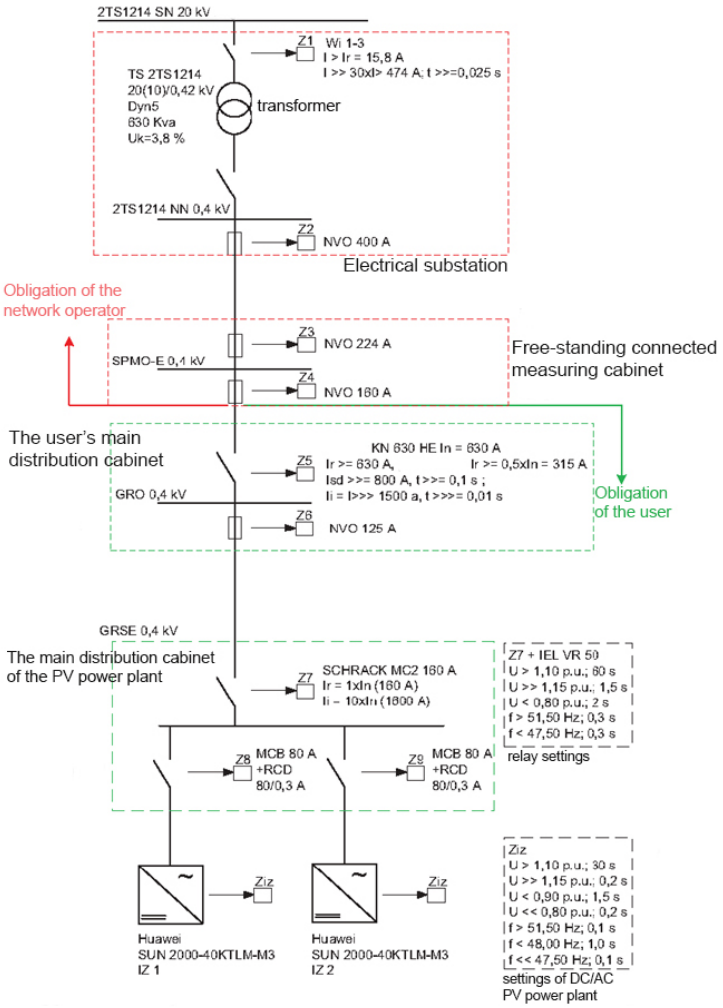


Figure no. 1. The actual setting of the existing protections of the photovoltaic power plant (own archive 2023)

This includes the use of surge protectors, proper installation and grounding of electrical components, and proper setting of protective devices. Considering the variety of overvoltage sources, photovoltaic power plants necessarily need a surge protection system that will deal with atmospheric and internal overvoltages in order to ensure the safety, reliability and durability of the power plant. Circuit breakers play a key role in overvoltage protection of photovoltaic power plants. Their role is to detect the presence of surges and quickly shut down the electrical circuit to protect people and equipment. Circuit breakers can be designed to respond to certain voltage or current values and automatically shut

down the circuit when these values are exceeded. These switches are fast and provide instant shutdown to prevent damage or injury. In PV power plants, circuit breakers are usually used at different points of the system to provide surge protection at different levels and components. Surge arresters are another important surge protection technique used in photovoltaic power plants. Their role is to absorb and redirect surges in a safe way to reduce the risk of damage to electrical equipment. Surge protectors act as a "conductor" that diverts surges toward ground, providing an alternate path for surge current instead of passing through sensitive electrical components. These protectors are designed to respond quickly to surges and absorb excess energy to protect electrical equipment from damage. Installing surge protectors at strategic locations in a PV power plant helps ensure the safety and reliability of the system. Proper grounding plays an important role in overvoltage protection of photovoltaic power plants. Grounding is used to create a safe path for the surge to earth, preventing damage to equipment and endangering personnel. In photovoltaic power plants, various components such as load-bearing substructures, photovoltaic panels, electrical cabinets and other equipment must be properly grounded. Grounding is achieved using grounding devices and grounded electrodes that are connected to the metal parts of the power plant and buried in the ground. The grounding equipment provides a safe path for the discharge of overvoltage in the event of overvoltage events, thus preventing damage and ensuring the stability of the operation of the photovoltaic power plant. For photovoltaic systems above 50 kW, it is mandatory to check the settings of the existing protection in the low-voltage (LV) distribution network, i.e. the newly installed protection in the LV network and at its interface with the LV distribution network (PMO), and based on research to propose the necessary changes in the settings (current levels operation and time delay) of the action of appropriate protection: in the transformer station (TS) high-voltage (HV)/(LV) medium voltage on the MV lines of the other MV network, then in the transformer field of the medium-voltage plant TS MV/LV (Z3), in other fields of the network which are connected to the TS MV/LV busbars to which the observed power plant is connected, at the interface of the power plant, the LV distribution network at the point for separating the power plant from the network (Z4), in the LV network of the power plant (Z5), in the exchangers (Ziz). The goal of research in the field of electrical protection (EPZ) is to determine the values of the characteristic sizes of various types of failures that can occur from the beginning to the end of the system, but also in accordance with the goal of forming optimal operating conditions, to perform the actual parameterization of the photo power plant protection settings.

VI. IMPROVING SECURITY AND PROTECTION SYSTEMS THROUGH THE APPLICATION OF ADVANCED TECHNOLOGIES

A. Advanced technologies for improving safety and technical protection at photovoltaic power plants

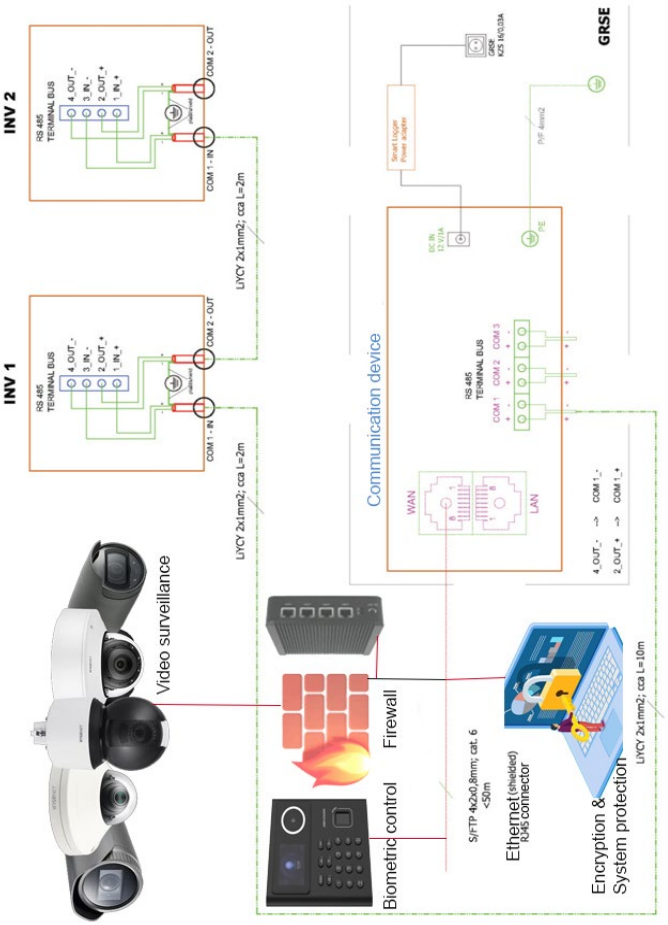
Advanced encryption methods (Advanced Encryption Standard - AES) are a key element in data protection and ensuring secure communication within the photovoltaic system. The use of advanced encryption algorithms ensures that the data transmitted within the system is encrypted in such a way that it is unreadable and unusable for unauthorized persons. Encryption methods use mathematical algorithms to convert readable data into encrypted form. Only people or devices with the appropriate key can decrypt and access that data. The application of advanced encryption methods ensures that even if an unauthorized person intercepts the data, he will not be able to understand its content. IDS (Intrusion Detection System), i.e. intrusion detection systems, are technologies that provide active protection of the photovoltaic system by identifying unauthorized access or intrusion attempts. These systems use different methods to monitor the network and detect suspicious Figure no. 2: Block diagram (detail) of the communication of the photovoltaic power plant(own archive, 2023)
activity. IDS systems can monitor the traffic within the photovoltaic system network, analyze it and identify irregularities that may indicate an attack or intrusion attempt. This includes monitoring changes in network traffic, detecting unauthorized access or data manipulation attempts. When such activity is detected, the IDS system automatically reacts and initiates appropriate countermeasures to prevent further threats. IPS (Intrusion Protection System) is a system that monitors the network and detects attempted attacks or unauthorized activities. Unlike IDS, which focuses on detecting threats, IPS has an active role in preventing and blocking attacks. It is used to identify irregular or suspicious activity, and applies appropriate security protocols to prevent further threat or intrusion. IPS uses a variety of protection techniques, including network traffic filtering, pattern analysis, heuristic analysis, and the use of security rules. When a potential attack is identified, IPS takes automatic measures to block or limit access to the threat, preventing further damage or unauthorized activity. Security certificates are digital identifiers used for authentication and trust between different parts of the PV system and external entities, such as other systems, users or service providers. These certificates are issued by trusted certificate authorities and are used to verify the authenticity and integrity of data. When a security certificate is used, each component or entity within the PV system can prove its identity through a digital signature generated with the help of a private key. This digital signature is then verified using the public key

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 08, ISSN No. 2455-2143, Pages 09-21
Published Online December 2023 in IJEAST (http://www.ijeast.com)

associated with the certificate. In this way, security certificates ensure that only trusted and authentic entities can access the photovoltaic system, preventing unauthorized access and data manipulation. The combination of advanced encryption methods, IDS and IPS systems and security certificates provides a strong system of security and protection of photovoltaic systems. These advanced technological tools enable reliable protection against cyber threats, unauthorized access and data manipulation. Biometric identification systems use an individual's unique physical characteristics, such as a fingerprint, facial recognition, or iris, to verify and confirm identity. In the context of photovoltaic power plants, biometric identification systems ensure that only authorized persons have access to the system.

The combination of advanced sensors and algorithms enables precise recognition of biometric data and prevention of unauthorized access. Biometric identification systems provide a high level of security because physical characteristics are difficult to replicate or spoof. Advanced video surveillance systems use high quality cameras with advanced features such as high resolution, night vision and analytical capabilities. These cameras are placed at strategic points within the protected area of the system in order to monitor and monitor the area in real time. Video surveillance systems enable recording of activities, detection of irregularities or suspicious situations, and timely response. Analytical capabilities include motion detection, facial or vehicle license plate recognition, which help identify potential threats. The integration of video surveillance with other security systems enables a holistic approach to technical protection. Access controls are used to regulate access to the area of the photovoltaic power plant. These systems include electronic locks, card readers, biometric readers or a combination of several methods.

Only authorized persons with valid means of identification, such as cards, keys or biometric data, can access certain parts of the system. Access control systems provide controlled access and reduce the risk of unauthorized entry or misuse. The integration of these systems with access records enables monitoring of who enters or leaves the area of the photovoltaic system... Advanced technologies in the technical protection of photovoltaic systems ensure reliable security and prevent unauthorized access. The implementation of biometric identification systems, a high-resolution video surveillance system and access controls enables comprehensive protection of the space, prevents potential threats and helps preserve the integrity of the system and equipment. In picture no. 2 shows some of the measures in the field of improving safety and technical protection at photovoltaic power plants. The applied measures depend on the size and importance of the power plant itself, but also on the assessment of the risks on it.



International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 08, ISSN No. 2455-2143, Pages 09-21
Published Online December 2023 in IJEAST (http://www.ijeast.com)

B. Improvements of electrical protection in photovoltaic power plants

High performance surge protectors are advanced electronic components used to detect and shut down surges in photovoltaic systems. They act as a quick response to overvoltages and provide equipment protection from the harmful effects of overvoltages. When the surge voltage exceeds a safe limit, the surge protector reacts quickly and ensures that the surge is diverted to ground to avoid equipment damage. High-performance surge protectors play a key role in maintaining the stable operation of photovoltaic systems in the event of atmospheric surges or other sources of surges. Isolation transformers are electrical devices used to isolate electrical circuits and provide additional protection against overvoltage. They work on the principle of electromagnetic induction and are used to convert the voltage between different parts of the photovoltaic system. Isolation transformers help reduce the risk of surges and electric shocks by providing an additional barrier between input and output circuits. Advanced automatic shutdown systems are technologies that enable the rapid shutdown of damaged parts of the photovoltaic system to prevent the spread of damage and minimize fire risks. These systems use sensors or monitoring equipment to detect surges, overloads or other critical conditions that can cause damage or fire. When such a situation is detected, the system automatically shuts down part of the system to prevent further spread. Advanced automatic shutdown systems provide quick response to critical situations and reduce potential risks of fire or equipment damage. Dynamic adaptive protection is a technology that uses advanced algorithms, neural networks for training and sensors to continuously monitor the operation of the photovoltaic system and adjust safety measures according to current conditions. This technology allows the system to dynamically adapt to changing operating conditions and optimize protective measures. For example, in case of surges or changes in grid load, dynamic adaptive protection can adjust the settings of surge protectors or activate additional safety measures to maintain the safety and stability of the PV system. Advanced technologies of electrical protection of photovoltaic systems provide comprehensive and reliable safety against overvoltage, electric shocks, fires and other risks. The combination of the mentioned technologies ensures optimal safety and reliability of photovoltaic systems. Since no smart meter is installed at the power plant, the user can only seetheproduction of the photovoltaic system.Other data such as user

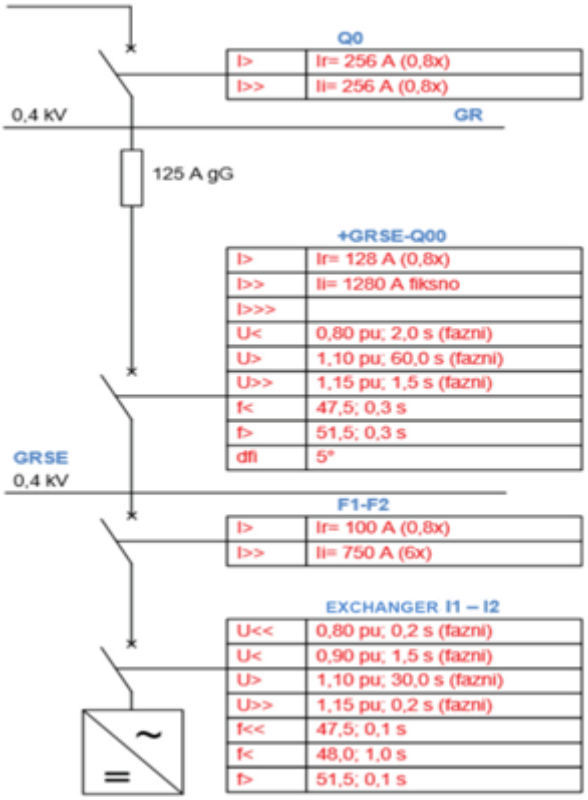


Figure no. 3: Display of parameter settings from the Elaboration of electrical protection EPZ (own archive 2023)

consumption and download/handover of electricity from/to the public power grid is not visible in such systems without a smart meter. Also, the active limitation shown in the previous case is not possible.The specificity of this system is the passive limitation that is performed on the DC/AC converters and the electrical protection in the main distribution board of the solar power plant (GRSE) in the cabinet on the protected devices. Considering that the power plant is over 50 kW according to the public electric power network, it means that it is necessary to perform the protection setting according to the electrical protection study (EPZ). In the Power Adjustment menu of the selected DC/AC converter, the maximum active power of the inverter is defined. The built-in DC/AC converters can give a maximum output of 40 kW of power, which would mean that they can give a total of 80 kW. As the electric power permit (EES) was issued for 72 kW according to the network, it was necessary to limit it passively. Therefore, the built-in DC/AC converters have a defined Max. Active power is 36 kW for each, which gives a total of 72 kW, which satisfies the condition. For the power plant in question, through the EES, the obligation to prepare an electrical protection study is defined, which elaborates and confirms the conformity of the settings (selectivity) of the protection of the power plant and the network (picture no. 3). The complete adjustment of protective elements is processed in the study. This includes all switches, switches, u/f relays and DC/AC converters. By adjusting the protective elements, the selectivity of the operation of a certain protective element is achieved depending on the nature, strength and position of the failure. This system provides the main protection in the electrical sense, which protects the power plant from breakdowns, equipment damage, accidents such as fire, and protects people from injuries and casualties. The user's main switch in the GRO cabinet represents the basic element of user protection against damage caused by overload or short circuit. This switch is existing, but due to the addition of a new energy source to the user's system, it needs to be processed and set according to the specified values through EPZ. Thus, in this case, the rated current switch In = 320 A is set to an overload current of 256 A, while the short-circuit current is set to 3200 A. The screws are visible on the devices, which can be adjusted to the desired position by turning them to the desired position. Current protection settings on the switches are carried out manually on each element individually. Also, during the operation of the possible protection, the switches turn off the circuit (open the contacts) and in this way prevent the occurrence of equipment failure or damage. Returning the switch to the operating state from the off to the on state is done manually and automation of that process is not allowed precisely for protection reasons. It is considered necessary to carry out a manual adjustment in order to be sure and aware that the fault that caused the outage has been removed and that the installation is ready for smooth operation again. As with the user's main switch in the GRO cabinet, the power plant main switch and the switch of each DC/AC converter in the GRSE cabinet are adjusted. The adjustment principle is the same as with the user's main switch, with the fact that these switches only protect the elements of the power plant. The settings are made to ensure the selectivity of the protection operation in order to separate from the electric circuit only the part where the current overload or short circuit occurred.

VII. BENEFITS OF THE APPLICATION OF NEW STANDARDS AND ICT TECHNOLOGIES IN THE FUNCTION OF IMPROVING SAFETY AND PROTECTION IN PHOTOVOLTAIC POWER PLANTS

The application of standards and new ICT technologies at photovoltaic power plants has significant potential for improving safety, technical and electrical protection, and therefore reliability, efficiency, effectiveness, and environmental parameters. Through fault detection, predictive maintenance, safety and protection, these advanced solutions can ensure the efficiency and reliability of photovoltaic power plants. Further development potentially brings further innovations and improvements that will enable even greater efficiency and integration with other renewable energy sources. Advanced information and communication technologies make it possible to improve the safety and protection of photovoltaic systems in order to ensure the protection of plant and animal life. Recycling components of photovoltaic systems contributes to reducing waste and negative impacts on the environment. Solar panels are largely recyclable. Materials such as aluminum, glass and semiconductors can mostly be recovered and thus reused.

The integration of advanced information and communication technologies enables the optimization of the operation of photovoltaic systems, the reduction of losses and the increase of overall energy efficiency.

The application of advanced telemetry systems enables precise monitoring of the performance of photovoltaic systems and quick detection of faults or problems. The use of advanced ICT technologies enables automatic diagnostics and optimization of system operation, which results in increased efficiency and reduction of energy losses. The implementation of a system for tracking the sun's path enables optimal positioning of solar panels for maximum utilization of solar energy. The application of new information and communication technologies has a wide range of advantages.

- ✓ Security:

The introduction of cryptographic techniques and multi-layered authentication methods helps protect against unauthorized access and hacking.

Systems of adaptive security measures and technical protection ensure detection of irregularities and prevention of potential damages.
Timely and adequate application of cyber security measures reduces the risk of cyber attacks and data loss.
By applying adequate safety and protection measures, we can avoid potential dangers that can lead to breakdowns or catastrophic failures at the level of the power plant, but also within the power system as a whole.

✓ Protection:
The application of advanced technologies enables the implementation of an access control system, which ensures protection against unauthorized access to the power plant's infrastructure.
The inclusion of advanced security protocols and regular software updates reduce vulnerabilities to security threats.
Adequate and timely implementation and application of measures to continuously improve safety and protection increases the reliability and security of the power supply system.

✓ Environmental parameters:
Improved safety and protection measures enable quick detection of problems and malfunctions, which reduces the negative impact on the environment. The development of systems for recycling and reuse of materials from old panels reduces the environmental footprint of the photovoltaic power plant industry.

✓ Efficiency and effectiveness:
The application of advanced technologies increases the efficiency of energy generation from photovoltaic power plants, thereby reducing production costs and increasing overall energy efficiency. The introduction of intelligent control systems enables faster detection of problems and improvement of reaction time, which leads to a reduction in losses and an increase in the effectiveness of power plant operations.

✓ Socio-economic benefits:
Increasing the use of photovoltaic power plants contributes to the reduction of emissions of harmful gases and dependence on fossil fuels, which contributes to the preservation of the environment. The development of the renewable energy industry creates new jobs and stimulates economic growth. The availability of cheap and clean energy enables the improvement of the quality of life and ultimately the reduction of costs for consumers, but it is also a prerequisite for sustainable development and survival.

✓ Advanced features:
Advanced data analytics – the development of advanced analytical tools and algorithms will enable a deeper analysis of the data collected from the photovoltaic system. This will enable a better understanding of performance, prediction of failures and optimization of work, but also a series of predictive measures in the function of improving factors that are managed in terms of optimal use of such systems.

Automated management and decision-making – advances in AI and machine learning enable PV systems to make autonomous decisions about optimal management, repairs and optimization. The systems will be able to adapt to changing conditions in order to achieve maximum efficiency, reliability, adjusting other parameters to optimal values in real time.

✓ Savings and other benefits:
Financial savings through increased reliability of equipment, greater use, better efficiency of the power plant, but also reduction of potential damage caused by triggering some of the risk factors in the domain of endangering safety and protection.
Savings in the use of other fuels for the production of electricity. we get energy by increasing the efficiency, effectiveness and reliability of the power plant's operation, because it can produce and provide planned amounts of electricity, so it is not necessary to include additional sources in order to preserve the power balance of the entire power system.
With adequate safety and protection measures both at the level of photovoltaic power plants and at the level of such power systems, we are closer to the goal of the energy transition, which, in addition to environmental acceptability, should also ensure the economic profitability of such sources, but also reduce or eliminate those comparative disadvantages, which such sources had compared to fossil fuels.
By increasingly significant exploitation of renewable energy sources such as the sun in an ecologically acceptable way, we will build an environment in which it is nicer and healthier to live for all living beings on this planet, and give all of us a new chance to apply moral principles in this area, vital for our planet and even us as the bearers of these activities...

VIII. CONCLUSION

After the research, the results undoubtedly confirm the hypothesis that the appropriate implementation and application of standards and new ICT technologies can significantly contribute to the improvement of safety, technical and electrical protection of photovoltaic power plants, which involves a number of benefits, but also challenges, which can be recognized through the presentation of safety improvement , technical and electrical protection, but also the effectiveness of the operation of photovoltaic power plants, the improvement of environmental parameters, economic indicators, but also the

accompanying social and moral factors, expressed through the imperative of sustainable development implemented by energy transition measures. Application of new standards and ICT technologies should enable adequate adjustment and detailed monitoring of key parameters and quick detection of potential problems or potential failures in photovoltaic power plants. The application of new standards and ICT technologies in photovoltaic power plants brings numerous advantages, such as increasing efficiency and reliability through the implementation of modern telemetry systems, but also the accompanying benefits of the same, which can be seen through price competitiveness, reliability of produced kW, improvement of living conditions, sustainable development and etc., but also risks that can be kept within the acceptable range only by adequate and timely measures from the domain of improving cyber security, technical and electrical protection for such systems. Continuous monitoring of technological innovations, adequate implementation and cooperation of universities and institutes with industrial partners can be key to further progress in safety and protection in photovoltaic power plants, but also in future electrical energy systems, an increasingly significant part of which is occupied by new ICT technologies. Taking into account all the above, there is an exceptional potential for the further development of photovoltaic power plants, their implementation and use, but also the improvement of safety and protection with the help of advanced information and communication technologies. Their application not only ensures efficiency and reliability, but also contributes to the safety and protection of people, equipment, and the system and stability of the power system, sustainability, reduction of fossil fuel use, and environmental protection and quality of life.

IX. REFERENCE

[1] Berkovac H.,Rahmanović A., KozićM., (2022),STANDARDIZATION OF THE SYSTEM OF TECHNICAL PROTECTION OF PREMISES FOR SERVER, DATA, NETWORK AND DR SITE, ijeast.com

[2] Blueprint Energy Solutions GmbH (“Blueprint”) at the request of the Energy Community Secretariat (“Client”) (2019) Final Report - Study on cyber security in the energy sector of the Energy Community. https://www.energycommunity.org/documents/studies.html [Accessed 26.11.2023.],

[3] Desarnaud, G. (2017) Cyber attacks and energy infrastructures: Anticipating Risks. Etudes de l'Ifri, Ifri,https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf [Accessed 22.11.2023.],

[4] ENISA [Internet] 2005-2023 by the European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/critical-information-infrastructures-andservices.[citirano nov.2023],

[5] ENISA (2020) A TRUSTED AND CYBER SECURE EUROPE: ENISA Strategy, EUROPEAN UNION AGENCY FOR CYBERSECURITY. https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secureeurope-enisa-strategy [Accessed 25.11.2023.],

[6] Majdandžić, Lj.,(2010),Solarni sustavi: teorijske osnove, projektiranje, ugradnja i primjeri izvedenih projekata, Graphis, Zagreb.

[7] Meštrović, Z., Fotonapon, (2020),Predavanja kolegija: Obnovljivi izvori energije na Tehničkom veleučilištu Zagreb.

[8] IEC 61724-1:2021,(2021), Photovoltaic system performance – Part 1: Monitoring, International Electrotechnical Commission,

[9] NIST (2023) Discussion Draft of the NIST Cybersecurity Framework 2.0 Core. Commerce Department’s National Institute of Standards and Technology:https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf [Accessed.11.2023.]

[10] Protrka, N. (2018) Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru, Doktorskadisertacija, https://repozitorij.unizd.hr/islandora/object/unizd:2333 [Accessed 22.10.2023.]

[11] Pursiainen, C., Kytomaa, E. (2022) From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, Sustainable and Resilient Infrastructure, Taylor and FrancisGroup. https://doi.org/10.1080/23789689.2022.2128562 [Accessed 25.11.2023.]

[12] Službeni list Europske unije, L 333/80; DIREKTIVA (EU) 2022/2555 EUROPSKOG PARLAMENTA I VIJEĆA od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32022L2555 [Accessed 24.10.2023.]

[13] Sviben, T. (2022) Analiza kibernetičkih napada na kritične infrastrukture, Diplomski rad, https://repozitorij.efzg.unizg.hr/islandora/object/efzg%3A9022/datastream/PDF/view[Accessed 22.11.2023.]

[14] Tošić, J. (2023) Dinamička adaptivna zaštita distributivnih mreža primjenom metoda inteligentnog pretraživanja, Doktorska disertacija, https://urn.nsk.hr/urn:nbn:hr:168:309696 [Accessed 26.11.2023.]
[15] Walker, A., Jal D., Saleem D., Gunda T. (2021) Cybersecurity in Photovoltaic Plant Operations Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-78755.https://www.nrel.gov/docs/fy21osti/78755.pdf [Accessed 20.11.2023.]
[16] https://www.dhs.gov/archive/coronavirus/cybersecurity-and-critical-infrastructure [Accessed 24.11.2023.]
[17] https://www.energy-community.org/ [Accessed 26.10.2023.]
[18] https://www.fer.unizg.hr/ [Accessed 28.10.2023.]
[19] https://www.iea.org/reports/renewables-2022/executive-summary, [Accessed 28.10.2023.]
[20] https://www.iea.org/reports/solar-pv [Accessed 03.11.2023.]
[21] https://www.nist.gov/cyberframework [Accessed 24.11.2023.]
[22] https://www.nexor.com/nis-directive/ [Accessed 04.11.2023.]