IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 7 ISSUE : 09 Print / Issue Publication Date: 09-Mar-2023

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2023.v07i09.009

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 9, ISSN No. 2455-2143, Pages 57-63
Published Online January 2023 in IJEAST (http://www.ijeast.com)

STANDARDIZATION OF THE SYSTEM OF TECHNICAL PROTECTION OF PREMISES FOR SERVER, DATA, NETWORK AND DR SITE

Prof.dr. Adis Rahmanovic
University of Travnik
Faculty of Technical Studies
Travnik, Bosnia and Herzegovina

MSc. Haris Berkovac
University of Travnik
Faculty of Technical Studies
Travnik, Bosnia and Herzegovina

Prof.dr. Muharem Kozic
University Dzemal Bijedic
Faculty of Humanities
Mostar, Bosnia and Herzegovina

Abstract-**The room protection system for Server, data, network and DR site is a great challenge for implementation, and should reflect the measure of the best available technologies in the field of protection and modern ICT technologies, as well as the optimal measure of economic investment, environmental parameters, and professional standards. Development trends in these domains with the task of complying with legal regulations and that the protection system is adequate compared to what it helps to protect.**
Through the article, we have shown the process of applying advanced measures to protect and increase the security of premises with significant ICT equipment and data, as well as effects in the field of reducing negative risks and possible damage from negative human factors, negative environmental impact, etc...
The aim is to present new technologies in this area and the justification of their implementation in the function of increasing the security of ICT equipment and data.

Keywords: **Measures to increase the security of ICT equipment, measures to increase the security of electronic data, space protection systems for server, data, network and DR site, SAR Journal.**

I. INTRODUCTION

The security of ICT infrastructure and data is becoming an increasing challenge, and it can be affected by an increasing number of factors with more intensive influence, and with the increasing implementation of new technologies and digital business transformation we have increasingly valuable ICT infrastructure and data. In this article we focus on the review of technologies in the field of protection of space, people, ICT equipment and electronic data in server rooms, data, network and security protection of software and supporting data by system recovery and activation system in remote locations in case of temporary or permanent damage ICT equipment at the base location, without major interruptions in the use of systems and data. In addition to the application of such protection systems, it is necessary to take into account the real-time monitoring of the same, as well as the possibility of reporting in the event of movements of monitored parameters outside the set limits, in order to act in a timely and preventive manner. In addition to the application of modern protection systems, it is necessary to develop appropriate procedures, so that they can minimize the number of participants, locate responsibility, minimize the negative impact of man and his unpredictable behavior. In addition, it is important to ensure that protection measures are continuously analyzed and, if necessary, improved, and for this purpose, in addition to researching the best available technologies, potential risks, legal legislation, standards, we should take into account market trends for equipment and at the economic level in the field of neutralizing or reducing potential risks to the reduction of security in this domain. In order to make the protection system more complete, it is necessary to constantly work on improving other measures of protection against the negative impact of electricity and unacceptable use of ICT equipment from the user's point of view directly, via local network or Internet, directly realized attacks or virtually using computer tools. The

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 9, ISSN No. 2455-2143, Pages 57-63
Published Online January 2023 in IJEAST (http://www.ijeast.com)

new data centers bore little resemblance to a data center of the past. It seems natural that industrial automation systems should be used to monitor and manage data centers. By using optical fiber, copper wires, wiring costs are reduced, space requirements are reduced and security increased. In addition to these technical protection measures, it is necessary to provide security measures in the field of power supply, as well as protection measures in the field of cyber security in all domains, including the computer network. As far as data is concerned, it is important to ensure that data remains confidential, that it cannot be tampered with, that it cannot be reproduced without authorization, and that lost packets can be discovered.

In the context of the above, we can ask the following question, whether the appropriate analysis and application of the best available technologies in the field of protection can provide a security system that best meets the requirements, and that is appropriate protection measures, be modern and economic investment is optimal. and in line with the value of what is being protected, as well as the potential risks that need to be reduced to an acceptable level, in terms of laws, standards and stakeholders. It is best to give answers to this question through the analysis of the application of the appropriate protection system and accompanying measures from practice, which we will discuss below.

The hypothesis is as follows: It is possible to create technical protection systems in Data/Server/Network centers according to regulations and standards adapted to the level of necessary protection.

II.DIFFERENT MEASURES OF THE TECHNICAL PROTECTION SYSTEM SHOWN THROUGH THE APPLICATION

Anti-burglary system, access control and environmental monitoring server hall Directorate Banovići:

The system of burglary, access control and environmental monitoring was presented in the case study through application in the server, data, network room of the Directorate RMU Banovići, as well as at the remote location Bešin for DR backup, and they are based on NOX Lite SET, built-in NOX modules. and different detectors and peripherals from several different manufacturers. In addition to this system, this article presents other security systems within the server room, such as electrically conductive floor and anti-burglary doors, anti-burglary and fire doors, fire protection system and video surveillance system in the above locations.

A. System capacity and capabilities –

Each system of burglary protection, access control and environmental control has its own capabilities, and some of the capabilities of this described system are presented and described below:

It has three independent busbars, each of which is protected by its own fuse (security, method of delivering system information),

Bus wire length up to 1200m, expandable with amplifier device (provides the ability to connect remote devices to connect devices remotely, such as signal lamps, audible warnings, etc.), Each device has a unique six-digit numeric address (the ability to connect multiple devices), Low energy consumption of each of the devices (energy efficiency and environmental parameters), Programmable delay time of each detector from 10ms to 20000s (possibility of fast response and setting the reaction for a longer period), Each input can be configured as quiet or working with a high level of security through support for random selection and programming of resistance values for each alarm input in values between (3-300 kΩ) (wide range and different options for setting internal device parameters), Ability to accept digital temperature and relative humidity detectors with setting and receiving alarm information about values directly via the bus with internal storage of temperature and relative humidity values within one year.

Access control support, the ability to integrate access control modules with support for readers from different manufacturers (good support features make maintenance and upgrades easier), Controlled power supply of the system with internal data storage within one year (battery voltage, output power, input voltage, temperature of the power supply module, possibility of archiving gives the possibility of subsequent analysis, planning and taking measures), Possibility of advanced testing of batteries (testing under load at a certain time) and generating technical alarms in case of anomaly detection (increases the reliability of the system in the event of a lack of electricity), Integrated RTC (Real time Clock), - possibility of time synchronization via NTP protocol, NOX data coding algorithm used to transfer data on the bus, Application of standard 4 - wire cable for power supply and data transmission on the bus (easier maintenance), Solid and sabotage-protected metal housing (additional protection of the system itself), Constant monitoring of all devices in the entire system, including the bus voltage of each device, (preventive action), Integrated Ethernet environment for system parameterization (programming), for system diagnostics and management (remote access, control, optimization and management facilitates access, saves time), Possibility of storing up to 10000 records (logs) in the headquarters with the possibility of choosing a date for a quick review of records, (saving is important for keeping evidence, subsequent analysis, taking action ...), Two-way integration with third systems using SSH (great opportunities for integration with other systems provide more information and control options), Connected to the alarm center via a standardized SIA IP alarm protocol (possibility to monitor parameters in real time), Batteries for power autonomy included (possibility of uninterrupted operation even in emergency circumstances), Included keyboard with 128x64 pixel LCD screen and backlight (basic settings and control possible on site without additional devices), Support for EN 50131 standard (adapted for

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 9, ISSN No. 2455-2143, Pages 57-63
Published Online January 2023 in IJEAST (http://www.ijeast.com)

operation according to standards).

Fig. 1. Appearance of NOX Lite Set & MIO with associated modules

B. Central component for control and management of NOX Lite SET & MIO –

The NOX Lite control panel is used for anti-burglary, access control and environmental monitoring systems. It features a massive metal housing that houses the NOX PS2 power supply unit, the NOX CPU CPU, the NOX MIO combined input-output module, and two batteries for autonomous system power in the event of a primary power outage. In addition to the listed components, the NOX Lite Set & MIO includes a NOX CPA system keyboard with LCD display. In addition to the listed NOX modules that are an integral part of the NOX Lite SET & MIO control panel, two more NOX IO4 modules, one NOX THSi module and a NOX CMO module are supplied for the needs of the project [13].

C. NOX CPU component –

The central processing unit provides an environment to the outside world, namely three NOX BUS terminal blocks P3, P4 and P6, and RJ-45 Ethernet port. The Ethernet port is used to connect to a computer that is used to configure the control panel, to diagnose and manage the system. The terminal blocks P3, P4 and P6 provide power and communicate with NOX modules. Terminal block P7 is used to power the control panel from the NOX PS2 power supply unit and to communicate the NOX PS2 power supply unit with the NOX CPU. Release communication bus NOX CPU component (central processing unit):

The central processing unit provides an environment to the outside world, namely three NOX BUS terminal blocks P3, P4 and P6, and RJ-45 Ethernet port. The Ethernet port is used to connect to a computer that is used to configure the control panel, to diagnose and manage the system. The terminal blocks P3, P4 and P6 provide power and communicate with NOX modules. Terminal block P7 is used to power the control panel from the NOX PS2 power supply unit and to communicate the NOX PS2 power supply unit with the NOX CPU. The communication bus is implemented via an RS485 BUS transceiver that allows 128 (NOX CPU + 126 NOX modules + NOX RPT) NOX devices per BUS segment. If more than 128 devices are required, the bus should be segmented using NOX RPT amplifiers. The allowed length of the bus wire is about 1200m, and if it is necessary to achieve longer lengths, it is necessary to use a NOX RPT amplifier. The connection between the NOX module and the NOX CPU is made using a daisy chain where the NOX CPU can be located at the beginning, end or somewhere in the middle of the bus.

NOX PS2 power supply unit

The power supply unit provides a nominal current of 2A at a voltage of 15VDC, and if the value of this current is exceeded, the system will send a warning message. In addition to providing power, the NOX PSU continuously monitors battery charging, output current, AC input voltage and operating temperature with internal data storage within one year. During operation, a short test is performed every 30s to confirm that the batteries are installed and ready for use. Possibility of advanced battery testing (testing under load at a certain time) and generating technical alarms in case of anomaly detection. Two 7Ah batteries each provide several hours of autonomous power at full load.

NOX MIO combined input-output module

The combined input-output module consists of eight relay outputs suitable for 30VDC voltage and 3A current of 10mA and eight monitored inputs in the range of 2 to 300kΩ, and six open-collector inputs.

NOX CPA system keyboard with LCD display

System keypad with 128 x 64pixel graphic LCD display, integrated alarm buzzer, numerickeypad with predefined "C" - clear and "E" - enter keys, and two scroll keys with variable functions is used for alarm management. The system keypad is integrated into the system, ie., connected to the NOX CPU, via the terminal block P2.

D. NOX modules –

NOX IO4 is a universal input / output (I / O) module that connects to the NOX CPU via the NOX BUS, and has 4 monitored inputs and four open-collector (OC) outputs. Under normal circumstances, the outputs are active and the GND (-potential) signal is available at the OC output of terminal P3. The technical characteristics of the NOX IO4 module and the terminal block layout are shown in the following tables. The NOX THS module allows the connection of an internal or external temperature and relative humidity sensor to the NOX CPU, via the NOX BUS. In addition, the module has a programmable relay output. NOX CMO module is a device that provides the ability to accept one or two card readers, with or without a keyboard, via OSDP protocol. The connection of

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 9, ISSN No. 2455-2143, Pages 57-63
Published Online January 2023 in IJEAST (http://www.ijeast.com)

the module to the NOX CPU is done as standard via the NOX BUS. Each card reader supports up to three LEDs with four different paints. Additionally, the module has one monitored input, relay output, open-collector output and two TTL inputs. Inputs allow you to assign an independent delay time as well as the ability to configure digital inputs. The output is basically active and is forwarded to peripherals, and the GND potential is enabled at the OC output of terminal P3. The relay output allows a short-term current of 3A in case of the need to connect inductive loads (30VDC / 3A for 10ms) [12].

Fig. 2. Security door server, data, network center

E. Detectors –

Satellite motion detector

The functionality of motion detection in the protected zone is based on dual technology, namely passive infrared (PIR) and microwave (MW) technology using a digital motion algorithm. An alarm will be issued in case the PIR and MW sensor detects movement in a time period shorter than 4s. The motion detector is equipped with anti-masking and tamper relay outputs that will be activated in case of an attempt to cover or paint the sensor lens, and remove the front sensor cover.

Satellite FD-1 flood detector

The flood detector detects the presence of water leaks or flooding in the room. The alarm will be issued approximately 4s after the water level reaches the height at which the detector electrodes are located. During the alarm, the relay output is open and the LED is active. The alarmis deactivated a few seconds after the water drops below the level at which the detector electrode is installed. In addition to detecting the presence of water, the detector is equipped with a system for monitoring the supply voltage and a tamper contact that is activated in the event of removal of the detector cover. The first state is signaled by means of a relay alarm output while the second state is signaled by means of a TMP relay output.

Indigo glass breakage detector

The glass breakage detector will issue an alarm when it detects low frequency sound (shock) followed by high frequency sound (glass breakage) in an interval shorter than 4s. The alarm is signaled via a relay output for 2 s. In addition to detecting glass breakage, the detector registers and alarms the drop in supply voltage, and has a tamper contact that will issue an alarm in the event of removal of the detector cover.

Smoke and temperature detector Satel TSD-1

This detector can detect the early stage of a fire when some of the visible smoke is present and / or in the event of a rise in temperature. The optical method was used for the section of the presence of visible smoke and in case the concentration of smoke in the optical chamber exceeds the set value, an alarm will be issued. The operating parameters of the smoke detector are modified depending on the value of the temperature registered by the temperature sensor (thermistor). The temperature sensor will sound an alarm if the temperature exceeds a certain amount (54 ° C - 65 ° C) or if the temperature rises too fast[9].

The detector automatically compensates for gradual changes in the optical chamber caused by deposition of dust.

The heat sensor operates according to the requirements of Class A1R (EN 54-5).

F. Automatic fire protection system and video surveillance–

An automatic fire protection system has been installed in the server / data / network Sali, which consists of two detectors connected to the alarm control panel, and in addition to the above detectors, the alarm control panel also contains an automatic fire extinguishing system and a communicator. The situation in this room can be monitored occasionally or as needed through the installed video surveillance system, the contents of which are recorded and available within 30 days. All sensors and information providers in the form of reports are set to send periodic emails about the state of the equipment, but also SMS messages in the state of the parameters out of the optimal range.

G. Security doors –

Anti-burglary doors consist of the components listed below, which are necessary for it to function in different circumstances, as well as to be anti-burglary not only because they are built of a physical structure that meets the standards for anti-burglary doors but also because they are designed to use different components, for control, monitoring and signaling in case of unauthorized access. Care must be taken with the door to ensure that the same installation standards are met. Anti-burglary and fire doors are Model T60 and dimensions 210x100 cm, and the door stem is made of steel profile 70x50 mm and is mounted on the wall with metal anchors, thus achieving the required strength of the stem and can only be removed by breaking the wall. The door leaf is

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 9, ISSN No. 2455-2143, Pages 57-63
Published Online January 2023 in IJEAST (http://www.ijeast.com)

made in a multi-layer sandwich construction 70 mm thick and is an obstacle that cannot be broken in a reasonable time without the use of large power tools and making significant noise in accordance with the standard BAS EN 1627: 2012 class III. In the middle of the wing is a grill made of steel profiles with a thick enough grid to prevent the passage of the face by itself. In accordance with the T-60 certificate in accordance with the standard BAS EN 1634-1: 2010, 1 mm thick steel sheet was added over the entire surface of the wing in front of the grill for the purpose of anti-burglary / fire-fighting. On the outside and inside, the panels are made of refined chipboard 10 mm thick and represent additional physical reinforcement of the wing. The space between the gratings is filled with thermal insulation stone wool 50 mm thick, which is also a sound insulation of 41 dB. The lock cylinder is manufactured by CISA. The addition of the lock is a factory-installed electric receiver, hydraulic shutter with slider, and reed contact. The lock and additional locking mechanisms are protected on the outside of the door by 4 mm thick metal plates. The wing frame is equipped with four wedges on the side of the bagla, which enter the corresponding openings in the stock. The CISA lock is stuck in the rod in the middle of the rod with four wedges, and in addition one on the upper and lower side of the rod. With such a construction and with regulating steel Q20 bags with a shaft of 12 mm, a sufficiently strong connection of the wing with the stem is achieved. The door is equipped as standard with an M-3-TPE rubber seal in the door stock, a "P" 10x5 gasket on the door leaf edges as well as an expansion gasket that blocks the passage of smoke and fire.

Security doors are highly complex systems. As movable building components they have to keep up their vital multifunctionality in tough everyday use. Combined security for example forced entry and bullet resistance – in some critical applications even have to be extended by blast resistance and/ or fire and smoke protection. Additionally, these special doors must be prepared to elegantly integrate automated fittings, access control units and escape door technology[11].

Components of security doors

- Magnetic contact Satellite

The magnetic contact consists of two elements: a magnetic sensor (reed switch) and a magnet. A reed switch positioned near the magnet establishes an electrical circuit. Each of the magnetic contact elements is encapsulated in an identical housing. The magnetic sensor is mounted on a stationary part of the protected object (window or door), while the magnet is mounted on a moving part.

- Emergency door button PIT ALARM PIT92

It is intended for installation in those places that have built-in access control in such a way that contactless ID card readers are installed on both sides of the door. In case of emergency or inability to open the door via standard authorization, pressing the button automatically unlocks the power supply in the door and allows unobstructed exit.

- Siren for indoor installation Satel SPW-220

It belongs to the group of optical-acoustic sirens. The light source consists of two LED sets, while the sound signal is generated by a piezoelectric transducer. The design of the siren by means of a tamper contact provides a high degree of protection against attempts to remove the siren cover or disassemble it. With jumper JP1 - JP5 it is possible to select one of three sounds to sound the alarm.

- Outdoor mounting siren Satel SP-4002

This siren is an optical-acoustic siren intended for outdoor installation. The acoustic signal is generated by means of a piezoelectric transducer, and the optical signal by means of LEDs. The siren has its own battery for autonomous power supply and tamper contact as protection against removing the front cover and uninstalling the siren from the wall.

- Contactless iCLASS SE HID R10 card reader

It belongs to the iCLASS SE reader family and is built on the SIA (Security Industry Association) OSDP (Open Supervised Device Protocol) standard, which ensures the transfer of data from the reader to the controller via the RS485 communication interface. The operating frequency of the reader is 13.56 MHz and for the needs of the Project MIFARE Classic contactless cards were used. The card reader includes IPM (Intelligent Power Management) which provides energy savings of up to 75% compared to standard mode.

Using the 13.56 MHz technology platform, the iCLASS R10 read only contactless smart card reader combines the longer read range of proximity with the power and heightened security of smart card technology, making it ideal for access control applications [10].

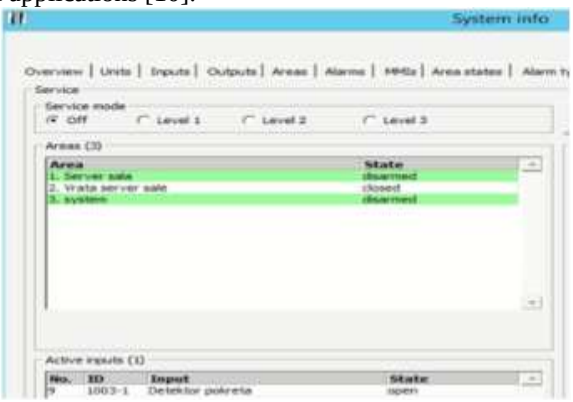

Figure 3. System info dialog box - Bešin location

- Electric door catch

The model of the electric receiver is manufactured by CISA and performed by FAIL SECURE. In the event of a final power outage (this means that in addition to the power outage, we have empty batteries that serve for autonomous operation of the technical protection system), the passage through the door

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 9, ISSN No. 2455-2143, Pages 57-63
Published Online January 2023 in IJEAST (http://www.ijeast.com)

will be blocked. In this case, staff must have a key as a last resort to enter the server room.

H. Electrostatic floor –

In very simple terms the greater the danger from a spark or electrical discharge (shock) the more conductive the floor should be. However, the lower the resistance of a floor the greater the risk there is of electrocution from a mains supply shock and that this has to be balanced against the risk of a spark or static discharge [14].

Electrostatic floor has a constant property of electrostatic conductivity and provides a safe flow of electrostatic charge to ground, and as such is used in operating rooms, laboratories, server rooms and the like. Conductive properties are achieved by the application of carbon particles that extend through the vinyl together with a pure carbon substrate. Before installing an electrostatic floor, the surface to which the floor is applied must be leveled, cleaned and must not be exposed to moisture. Earthing of the electrostatic floor is realized by applying copper tape and adhesive conductive mass in such a way that the copper strip is laid at only one end of the room perpendicular to the electrostatic floor coverings. Next, the copper strip is connected to the already existing electrical grounding of the building.

Permanently conductive adhesive based on acrylic floor adhesives is applied to the prepared substrate. Electrostatic floor coverings must be installed in such a way as to avoid differences in color and take care that the floor covering makes contact with the adhesive mass over its entire surface, and that all air is expelled. In order to better contact the electrostatic floor covering with the adhesive mass, a leveling board and a floor roller are used. The final phase of the installation of the electrostatic floor is the connection of adjacent panels, which is done by the technique of "hot welding". Daily floor cleaning involves dry or wet cleaning. The floor can be cleaned with a combined polishing and drying machine equipped with a brush of medium hardness. Treat the floor surface with neutral cleaning agents. If occasional acid treatment is required, use only agents with a pH of 3 to pH 5 with mandatory adherence to the dosage when making the solution.

Dry polishing is the most effective method of restoring the floor surface if visible minor damage has occurred. Dry polishing is best applied after machine cleaning the floor. The best results are achieved by applying 500 to 1000 rpm.

More visible damage and soiling require the application of machine cleaning. The surface is treated using a pH cleaning agent 10 - 11 dissolved in water for 5 - 10 min. Clean with a "heavy" polishing machine, remove dirty water from the floor surface and rinse with clean water, wait for the surface to dry, and then do a dry polishing according to the instructions.

III. APPLIED PROTECTION MEASURES AT A REMOTE LOCATION

The application of measures for the protection of backup and recovery of data and software is in the top five priorities of continuous action according to the source of the Enterprise Strategy Group from 2016. The access control and environmental monitoring system located at the Bešin location in the New Administration building is based on the APC NetShelter AR3104 communication cabinet, APC's NetBotz 250 access control and environmental monitoring device, and associated sensors.

I. Technical description of the access and environmental control system –

Access control to the equipment located in the 243 height AR3104 communication cabinet is controlled via the front and rear cabinet doors via contactless 13.56 MHz MIFARE Classic ID cards which control the operation of electric locks installed on the cabinet doors, while the status of the door position is realized by magnetic contacts. Electric locks and magnetic contacts are connected to the NetBotz 250 access and environment control device on the ports marked Handle # 1, Handle # 2 and Door # 1, Door # 2 located on the front of the device, via RJ45 interface, and set front door to Handle # 1 and Door # 1 ports, and rear door set to Handle # 2 and Door # 2 ports. The combined temperature and relative humidity sensor together with the wireless temperature sensor makes up a set of environmental control sensors. The temperature and relative humidity sensor is mechanically mounted on the middle part of the front door, in the area where the greatest warm air circulation is expected, and is connected to the first port of the group of ports intended for connecting sensors on NetBotz 250.The NetBotz 250 device is configured via the NetBotz 250 web UI, but network settings must be adjusted first. If there is no DHCP server on the network, it is necessary to set the static IP address via the command line interface [15]. For this purpose, it is necessary to connect a NetBotz 250 device (min USB console port) and a computer (USB port), then run one of the terminal emulators such as HyperTerminal or PuTTy, and select the serial communication parameters (baud rate: 9600bps, 8 data bits, 1 stop bit, and no flow control). For username and password is necessary to use the default account apc. Enter tcpip -i ip adress, subnet mask, gateway in the command line, and then reboot the device with the reboot command. After adjusting the network settings, the NetBotz 250 device must be connected to the local network with a network cable.

The above protection measures have been implemented in accordance with the relevant standards and regulations EN: 50600, ANSI / TIA-942-A, EN: 50131, EN: 1627 and EN: 1047 in the field of planning, design, construction, security and control of modern server rooms , anti-burglary systems and fire protection, and in addition to them implemented a system of redundant air conditioning that provides stability and

continuity of maintenance of microclimatic parameters in case of failure of the primary system, as well as security and fire protection foils on window panes that reduce burglary and broken glass, and contribute to better thermal insulation. It was taken into account that the installed components have the lowest possible power consumption due to energy efficiency and environmental parameters, but also because in the event of a power outage they can last as long as possible on the existing uninterruptible power supply structure, as well as additional batteries. Found on critical components.

IV.CONCLUSION

In this article, we have presented different protection measures that have been implemented at different locations, and which, depending on the estimated value to be protected, are incorporated as standard protection measures at locations with ICT equipment and electronic data. The above protection measures, in addition to meeting all legal regulations and standards, from the aspect of economic parameters do not represent a "high" investment, so representing the results that such measures can deliver in the protection function, so they are very acceptable to potential investors or stakeholders.

This article fully confirmed the hypothesis.

For the introduction of video surveillance measures, due to various legal solutions when it comes to recording personal data, such measures require additional permits from the competent institutions, so in some parts the same can be replaced through electronic card detection system and prescribed procedures and communication with smart technologies. forms of notification by e-mail, SMS or signal lamp in real-time monitoring centers.

Before implementing protection measures, it is necessary to analyze the value and potential values in different circumstances, the impact of ICT equipment and its functions on business, business continuity, value of ICT equipment, value of electronic data and the company's dependence on them, whether it is business secrets, personal data, projects, patents and what would be the damage in case the data is damaged, blocked or stolen, in what way and to what extent it would affect the company's business. When the required data is obtained, in accordance with laws and standards, taking into account the standardization of equipment for functionality and maintenance, as well as the possibility of upgrading it implements measures that meet all the above conditions as shown in the above two case studies.

The article shows that after the determined value and analysis, protection measures can be applied that will reduce the risks to an acceptable level in the field of economically acceptable restrictions, with the application of the best available modern ICT technologies, taking into account the autonomy and robustness of the system. and minimizing the negative impact on the environment.

V. REFERENCE

[1] Rahmanović A.(2017). Telemetry control and management using ICT. LAP, Germany, 2009.
[2] Husain B. (2020). Review Data centers. ABB, 2020.,
[3] Nemnom C. andLownds P. (2018). Microsoft System Center Data Protection Manager CookBook.Packt Publishing, UK, 2018.,
[4] Geng H. (2021). Data center Handbook: Plan, Design, Build and Operations of Smart Data Center. 2nd, Wiley, California, USA, 2021.,
[5] GasalDž. (2021).Dokumentacijasapratećimuputstvomsistematehničkezaštite. King ICT za RMU Banovići, BiH, 2019.,
[6] Group of authors (2022). Data center and server room standards. KU University of Kansas, USA, 2022.,
[7] Group of authors (2022). Protecting Data in Network Environment. Oracle Corporation, 2003 – 2022.,
[8] Snevely R. (2002). Enterprise Data Center Design and Methodology. SUN microsystems, Prentice Hall, 2002.
[9] https://www.satel.eu/en/product/538/TSD-1,Universal-smoke-and-heat-detector-for-alarm-systems
[10] https://smart-itbusiness.com/hardwarepdf/r10.pdf
[11] https://www.saelzer-security.com/images/04_Saelzer_Security-Doors.pdf
[12] https://noxsystems.com/wp-content/uploads/2022/05/220506_EN_NOX_Components.pdf
[13] https://noxsystems.com/wp-content/uploads/2017/06/ENFlyer_N193_NOX_Lite_170628.pdf
[14] https://www.flowcrete.eu/media/9888/flowcrete-uk-antistatic-flooring-explained.pdf
[15] http://cdn.cnetcontent.com/be/8b/be8b711c-9416-4a7d-aea9-1b554553956a.pdf

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143