Application and Development of Embedded Systems with IoT Components: Aspect of Safety and Reliability

Adis Rahmanović [1], Ergin Hakić [2], Muzafer Saračević [3], Enver Međedović [2]

[1] *University of Travnik, Faculty of Technical Studies, Bosnia and Herzegovina*
[2] *University of Novi Pazar, Department of law sciences, Serbia*
[3] *University of Novi Pazar, Department of computer sciences, Serbia*

Abstract **– We will present the possibilities of application and development, especially in the field of embedded systems, its interaction with other IoT components, the security aspects of individual components, as well as the domain of their interaction. In embedded systems, we will present new technologies such as fuzzy logic, application possibilities in embedded systems, and machine learning, as application possibilities through the implementation of machine learning. Then we will describe some more examples of the application of fuzzy logic, the automatic control of certain functions in cameras, as well as the defuzzification process, and the possibility of application in security cameras. In embedded systems, we will present the basic aspects of optimization and security, both in everyday applications and in interaction with other components of IoT technologies. The paper shows how security, reliability, and cost estimates affect the implementation phases and the final use of embedded systems, through examples of their application in industry. Security and data protection is shown through the construction of the mentioned devices, their application, but also different encryption methods, permissions, security devices at the network level, as well as implemented IoT technologies.**

Application examples are focused on the real segment, both in the field of transport, multimedia, design, and in the field of industrial application possibilities.

Keywords **– security, data protection, embedded systems, IoT technologies.**

DOI: 10.18421/SAR64-03
https://doi.org/10.18421/SAR64-03

Corresponding author: Ergin Hakić,
University of Novi Pazar, Department of law sciences, Serbia
Email: e.hakic@uninp.edu.rs

Received: 20 September 2023.
Revised: 16 November 2023.
Accepted: 22 November 2023.
Published: 25 December 2023.

1. Introduction

The Internet of Things (IoT) consists of devices with embedded systems that have an Internet connection, through which such devices can be controlled or managed remotely. The communication of devices with built-in systems within the IoT with other different devices is carried out via the Internet, so it is necessary to apply different methods of preparation, optimization, but also protection, both of data, instructions and the like, which is the subject of transfer, as well as the entire infrastructure, through which data transfer and performs. For such devices to work optimally and communicate with each other via the Internet, it is necessary to approach every aspect of the construction of such devices very studiously, both in the domain of system design through UML, as well as hardware and software design, all with the aim of greater robustness, optimization, security work and data processing, but also the forwarding of various instructions. Of course, the degree of reliability and safety of the operation of such devices depends on the area of application, and on that basis, different procedures for checking and determining quality are performed depending on the application and the importance of the area in which it will function.

It is important to adhere to the principles in the design of Embedded Systems, and the most commonly used principles are the 10 design principles:

1. Consideration of security (security is an important part of the specification, and is considered in the domain of users, equipment, results, and environment throughout the entire design process);
2. Refinement of the specification (it is necessary to specify and formulate precisely and correctly, including errors and their probabilities, any hypothetical specification may lead beyond the permissible limits);
3. Error containment areas (create areas in such a way that in the event of errors in the specified areas, they do not negatively affect the area where the error did not occur);
4. Consistent concept of time and state (ES should establish consistent time and state, because errors may occur due to these differences);
5. Well-defined interfaces (will enable the user to quickly understand the new design compared to previous experiences);
6. Components fail independently (it should be ensured that the failure of one component does not affect the failure of the functionality of components);
7. Accuracy of components should be considered and compared against at least several others eligible to be used;
8. ES should have mechanisms such that in the event of a failure of a component, it does not contribute to the difficulty of working with other ES components;
9. The facilitated transparency in interaction, predictability of steps, but also in case of human error, that there is a possibility of correction, or return - forgiving);
10. Keeping records - records (every anomaly has to be recorded or recorded as a log);

Embedded systems enhance efficiency through automation and real-time data processing. They enable smart homes, intelligent manufacturing, predictive maintenance, and more, leading to resource savings and improved productivity. Embedded systems can be tailored to specific applications and are highly scalable. This flexibility allows the development of specialized solutions across various domains.

2. Device Design of Embedded Systems (ES)

The essential hardware design of embedded systems depends on whether they are created in the form of a microcontroller or using a processor component,which depends on the type of purpose, area and conditions of application, but the complexity of the results they need to deliver.

The main differences between these two approaches to hardware design are as follows:

- A microcontroller contains a less complex microprocessor core, memory, peripherals, etc., while a microprocessor usually contains more cores with an ALU, a set of registers, a control unit and etc.;
- Microcontroller has small data processing capabilities, instructions, etc., while microprocessor has large data processing capabilities, instructions, etc.;
- Microcontrollers consume less electricity energy compared to microprocessors that consume a larger amount of electricity;
- A microcontroller is used in embedded systems such as cars, TVs, smart watches and IoT, whereas a microprocessor is used in personal computers and servers.

Microcontrollers have been created in various forms, and historically their development is shown below:

1. In the very beginning, microcontrollers were created as programmable read-only memory based on logic arrays;
2. The need for erasing capabilities created a new generation of so-called EPROM;
3. After that, in 1975 the Field Programmable Logic Array was developed (FPLA), and in 1980 the so-called Field Programmable Gate Array was develped as well (FPGA);
4. Microcontrollers based on integrated circuits were then developed, which had a specific application called Specific Application of Integrated Circuits (ASIC);
5. The new generation of microcontrollers are realized as a computer on a chip. They are called a microcontroller unit (MCU), and in addition to containing a microprocessor unit, they also contain the following functional components: clock or timer, memory, A/D converter, input and output ports, while some, depending on the application, they even have a segment for digital signal processing (DSP), digital filters.

The advantages of microcontrollers are lower price and implementation time, while the disadvantages are primarily focused on less computational resources such as lower speed and performance. In the following, we will list the basic characteristics of several different microcontrollers implemented in the MCU modality, computer on a chip.

ATMEL MCU is excellent for embedded systems for less resources and power, and is created as 8, 16, or 32 bit version. A programmable interface controller (PIC) is a different type of microcontroller, it is efficient for low power, resources, and represents a low-cost option, and it is created as a 16-bit version of the CPU. MSP represents an extremely low-power microcontroller that represents a very good variant for low-power operation with great possibilities of working with different signals. ARM microcontrollers are created for different applications and different companies, and have different core designs ranging from ARMv1 to ARMv9, and are created as 16, 32, or 64 bit CPUs. Due to analog components, they consume more energy, but with certain sleep mode settings, the same can be reduced. The development environment is called PSoC designer. Commercial prototype boards (PCBs) are Arduino and Raspberry Pi.

Arduino was created on the open source hardware/software concept, with great popularity and low price. Flash memory is placed on the board. There are many additional possibilities, e.g. GPS, Ethernet, LCD, Bluetooth, WiFi, as well as many ports: USB, RS232, PWM, Analog, GPIO, 12C, SPI, etc., and the development environment is Arduino Sketch. Raspberry Pi is a board created for educational purposes, and in combination with an ARM processor and a series of ports such as USB, audio/video port and VideoCore GPU graphics processor, it represents a solid platform for developing and testing various applications and capabilities. It is programmable and supports C/C++, Java, Python, Perl and Ruby. Depending on the application and availability, one or the other listed board is used, although Arduino is the more often applied choice for beginners, while in other circumstances it is necessary to consider the advantages of one over the other, so they are used accordingly. Depending on the interaction with the environment, whether it is sensors or information providers that are analog or digital, it is necessary to accept, amplify, remove noise, sample, quantize and encode the expected signals, i.e. convert from analog to digital and vice versa. Signals when measuring temperature, humidity, pressure, voltage and current if they are analog imply the concept of conversion from analog to digital signal, as well as vice versa. Commercial prototype boards (PCB) are Arduino and Raspberry Pi.

The first step in AFE design is to choose a sensor i.e. choose a sensor that has a clear physical dependence of certain quantities that can be shown mathematically through a change ratio.

With analog signals in real time, the appearance of noise is common, so it is necessary to implement analog filters in such a concept, depending on the characteristics of the noise, they are created as a high-pass filter (HPF), low-pass filter (LPF), bandpass filters (BPF), the inverse filter to BPF, whereby what is permeable previously in this case is removed (BSF), as well as filters that instead of permeability create a barrier (Notch filter - NF). In addition to noise, it is necessary to remove the negative influence of other signals, in order to have the most accurate measured signal, such as when we record an EEG signal from the brain, we can unintentionally register muscle signals originating from eye movements or heartbeats, and these are signals of a similar frequency spectrum where it cannot be removed by a filter. So, a complex statistical approach, wave decomposition or component analysis of the source itself is needed in order to get to the original signal and ensure the accuracy, safety and reliability of the results of the designed devices.

Microcontrollers use various devices for converting analog to digital signals, so-called ADC, and for converting digital to analog signals DAC. If we want to convert several analog inputs into digital output, we use AMux, i.e. analog multiplexer. In devices with embedded systems, there are a number of peripherals that can be outputs for output devices, outputs for data storage or actuators. Almost all newer generation MCUs have memory in the form of RAM and ROM, while external memory is created as a flash chip, MicroSD or even a hard disk HDD. Actuators can be analog and digital, and examples of digital ones are relays, stepper motors and buzzers, while examples of analog actuators are DC motors, speakers, where they can be combined with, e.g. with a robotic arm, an LCD or a monitor with a graphic display. Some actuators require special circuits for their needs, so certain parameters can be provided by an amplifier or relay. The output drive circuits and ports require external adjustable resistors, which always keep the parameters within acceptable limits, to protect against signals having magnitudes above the set values.

Serial communication takes place by bit-by-bit data transmission, and the standard that was used at the beginning was RS 232. This increases the bandwidth of the port, but requires more hardware, which makes it relatively expensive.

Several different ports were used because serial ports were not able to provide higher transfer speeds until the advent of the USB standard, which is used almost universally today and even for power supply and printing.

However, in some cases, parallel transmission has to be used, such as when interfacing a stepper motor with an MCU, interfacing with an LED matrix, etc.

The architecture of the microcontroller "computer on a chip" is such that the buses and peripherals are integrated, whereby the bus system is used to connect the microprocessor with the memory and input and output ports. Each I/O port contains hardware buffers, which are typically created as first input first output (FIFO). These buffers place the data in order, when sending and waiting for reception and processing from other components, and with the same it is ensured that there is no rejection or loss of data, instructions in the event of bottlenecks, when switching from internal to external buses, due to different bandwidths, etc. The polling mechanism periodically checks incoming data ports, accepting data in case new data is available. In case of the occurrence of multiple data, then the order can be established based on their priority which is created and established based on the status of the flags. Interrupts are a technique that requires deep knowledge of ES design skills to be properly implemented [8], which if properly implemented will be an effective mechanism for managing data queues, instructions, but also to provide interaction with peripherals using other mechanisms. The interrupt hardware contains input services with request flags. They produce IRQ interrupt requests.

Direct Memory Access is available in some MCU versions, and can independently read from an output port or write to an output port without the processor being involved. There are different types of DMA settings, and all have the function of freeing the processor from a function where peripherals have a request to access memory or another resource. The timer is an important piece of hardware that needs to be used well when designing the ES in order to function optimally and conserve energy. Timer hardware drives the MCU clock. The timer can be set to count forward or backward. The watchdog timer (WDT) is a special purpose timer that is off by default and can be enabled to detect software crashes. This is an important mechanism of the ES, which can provide a system restart without human intervention in case a software crash is detected.

Communications are used to manage the flow of data and signals through a medium, and the medium or means of transmitting signals (data, code, instructions) can be steam, fiber optics or air, vacuum or water.

Depending on which speeds should be provided at which distance, the appropriate medium is used with the appropriate equipment that supports the standard that describes the mode of operation and the language of communication (protocol).

Based on the needs, the performance of communications is created, and therefore the metric of communication technologies, which is measured from those with high performance, to those with medium or low performance, or those in which the removal of noise, or the removal of unwanted effects of other signals is essential (interference, etc.), based on the reliability and safety of those that have a physically tangible medium such as wire or optics, due to the possibility of greater control, better devices and configuration, and concrete connection to one physical point more reliably and safely than those that take place via air, water or vacuum.

Based on the implementation of the module for communication and Internet connection, ES devices become an integral part of the IoT network. Wired communications with ES devices have a whole spectrum of modules, standards, and ways of transmitting data, signals, instructions and code, whether in serial or parallel mode. Some of those applied standards have been previously processed, namely: UART, 12C, USB, SCI, SPI, Ethernet, Fiber Optical, and etc. Wireless communication due to ease of connection and an increasing number of devices is becoming more and more used with ES devices within IoT networks, but it brings with it greater challenges in the field of security, which we will discuss more in the rest of the chapter. We will list some of those communication standards below. A cellular data network essentially uses mobile phones, or requires the installation of a SIM card or equivalent technology in the device and requires a subscription from a service provider, and uses the infrastructure of established mobile networks, by said service provider. The standards based on which they are implemented are IEEE 802.16 and IEEE 802.16E, and examples of these technologies and their standards are: 3G (EDGE), 4G (LTE, WiMax) and 5G, and these topologies enable ES devices to access the Internet. These networks provide the possibility of establishing an Internet connection in a wide area where a signal from the service provider is provided (throughout the country, region, predefined geographical area, autonomous cars, etc). WiFi technologies allow Internet access optionally without mandatory subscription costs, they are locally limited to a narrow geographical area, and are implemented through the IEEE 802.11 standards. Each WiFi module has a MAC address (unique for each hardware) as well as an IP address (unique for each Internet identification), whereby the WiFi spectrum provides 13+1 channels for communication.

The older IPv4 (32-bit addresses) due to the increasing number of devices, is slowly being replaced by the new IPv6 standard (128-bit addresses, which gives significantly greater possibilities when connecting a larger number of devices).

WiFi works on different frequencies, but most often devices are set to work on open frequencies 2, 4 GHz with less bandwidth and bandwidth as well as 5GHz frequency with higher bandwidth and bandwidth. There are different version and security protocols, encryption and standards used to increase the security of WiFi networks. Bluetooth (BT) technology works on IEEE 802.2 standard, different versions, frequency 2.4 GHz with different channels with short distances of 10 meters in real conditions or up to 100 m in theoretical conditions with small range and for low data flow.

Sensor nodes have a focus on mesh networking and low power operations. Examples of these networks are ZigBee (a standard that defines a set of communications for low data rate, low power, low range wireless networking) or XBee and Mote. A ZigBee node can be a coordinator of a PAN network, provide full device functionality and limited device functionality. It can work through different forms of wireless networks like Star, Mesh and Cluster-tree. Mote or Sensornet is adapted to work with distributed sensor networks, and other topologies are created for low-power sensors and wearable devices and are called Ant+. Wifi networks and BT networks dominate in many applications, especially for devices that are more geographically located and have less power.

Radio frequency identification (RFID) was developed for ID smart cards, and it is created in three ways: active (supports a range greater than 10 m, but requires batteries in the sensor), semi-active (has a battery, but is only active when receive a request), as well as passive (no battery, for close operations up to 1m away), with passive RFID being the most commonly used. NFC is a similar technology often used in smart wallets. The Global Positioning System (GPS) also works on the basis of position sensors that through satellites, using the GPS sensor, locate and send the location of the position with an accuracy within a few meters. It all depends on the coverage of the given area with satellites and included coordinates. A commonly used metric is latency and throughput, where latency is expressed as the time between the start and end of a task or operation, while throughput is the number of tasks per second. The growing number of WiFi devices in the IoT, the value of data, the impact of such networks on everyday life, as well as different areas of application, are becoming an increasing lure, but also generating increasing challenges in the field of security.

Facilitations that end users are used to by WiFi networks, such as bypassing or recording authentication, automated access, etc. become the main risk factors, so more and more different authentication methods, and protocols for access control, confidentiality, and integrity are integrated into WiFi networks as mandatory, constantly improving and updating methods of cryptography, downloading certificates through private communication channels, etc. Authentication rules are created through WEP, IPSEC, SSL, EAP, etc. while encryption is performed through different algorithms such as encryption with a hash or a unique key, e.g. RSA. We will discuss more about ways to protect data through encryption in the rest of the chapter. Pulse Width Modulation (PWM) is hardware that has a wide range of applications, such as generating different blinking possibilities of LED panels by changing frequencies, filtering PWM results on the analog voltage output, controlling the speed of DC motors.

The batteries that are most often used for constant recharging of ES devices Lithium Polymer (LiPo) have a high energy density and a short charging time, and produce 3.7 volts. For LiPo batteries, an energy management chip is designed in ES. Non-rechargeable carbon-based batteries that produce 1.5 V such as AAA, AA, C, D are also used, and depending on how they are combined, in series or in parallel, they can produce different voltages. For greater autonomy, less energy consumption, optimization of operation, less heating, greater reliability and operational safety, an energy-saving mode of operation is introduced for the MCU. There are different ways of saving, e.g. by reducing the voltage from 5 to 3.3 V, we can save 56% of energy, but it is important that the components perform tasks optimally, combining different modes such as standby, sleep mode, power saver or hibernate. Depending on the functionality of ES devices, they have different modes, so it is necessary to use them as best as possible due to the effects mentioned above, depending on the need, we have Active mode, Idle mode, Mode for removing noise, and sleep mode. Managing these and new ways of working is becoming an increasing challenge and opportunity, both in the domain of energy saving, because there are billions of devices in constant operation. Furthermore, in terms of ecology, with lower energy consumption, fewer harmful particles are produced, as well as a lower level of battery replacement, both of which are positive for the environment. By consuming less energy, but also releasing fewer harmful substances, and with a lower level of battery consumption, we have better health parameters for people and living things, as well as better economic parameters.

The design of hardware ES devices is created in software adapted for these activities. In addition to modeling capabilities, the same hardware should also provide simulation, and the most common software used, depending on the complexity and field of application, is Matlab, PSpice and KiCad.

3. Importance of Application of Embedded Systems Devices

This scientific contribution explores the evolving landscape of security and data protection in embedded systems and their profound interactions with IoT (Internet of Things) technologies. As the proliferation of IoT devices continues to accelerate, ensuring the confidentiality, integrity, and availability of data in embedded systems becomes paramount. This paper highlights recent advancements and innovative approaches to fortify embedded systems against diverse cyber threats while seamlessly integrating them with IoT ecosystems. The research endeavors discussed herein encompass hardware and software security mechanisms, encryption techniques, access control strategies, and emerging paradigms that collectively enhance the security posture of embedded systems within IoT environments. Embedded systems play a pivotal role in the IoT ecosystem, powering a myriad of devices across diverse industries. However, their inherent resource constraints and connectivity requirements make them prime targets for cyberattacks. This contribution delves into the critical importance of security and data protection methods in ensuring the reliability and trustworthiness of embedded systems within the IoT framework. To mitigate vulnerabilities at the hardware level, this paper investigates the integration of secure elements, trusted platform modules (TPMs), and hardware security modules (HSMs) into embedded systems. These technologies establish a foundation of trust by safeguarding cryptographic keys and enabling secure boot processes. In the realm of software security, the research explores secure coding practices, runtime analysis, and vulnerability assessment techniques tailored to embedded systems. Additionally, the role of containerization and isolation mechanisms in reducing attack surfaces and containing breaches is discussed.

Robust encryption methods, including lightweight cryptography algorithms, are explored to protect data in transit and at rest within embedded systems. Furthermore, techniques for ensuring data integrity, such as cryptographic hashing and digital signatures, are examined to thwart tampering and unauthorized alterations.

Effective access control mechanisms are pivotal in limiting unauthorized access to embedded systems. This paper investigates multifactor authentication, role-based access control, and privilege escalation prevention methods tailored to the specific needs of IoT-connected embedded devices.

The contribution also spotlights emerging security paradigms, such as homomorphic encryption, secure enclaves, and decentralized identity solutions, which hold promise in enhancing the security and privacy of embedded systems in IoT environments. To illustrate practical applications, this contribution presents real-world case studies where advanced security measures have been successfully implemented in embedded systems interacting with IoT technologies. These case studies showcase the feasibility and effectiveness of the discussed security approaches. The scientific contribution concludes with an exploration of future research directions, including the potential integration of AI and machine learning for anomaly detection, quantum-safe cryptography, and the evolution of security standards for embedded systems in IoT.

4. Application of ES Devices as a Part of IoT in the Industry

The application of IoT in industry is developing significantly. Modern concepts of digitization and process automation include the application of artificial and business intelligence, as well as fuzzy logic wherever possible. The specifics of the industry are the working environment, which is extremely demanding in the field of exploitation itself, so the devices that are used have to comply with certain standards of protection against unwanted environmental influences, such as moisture, dust, impact, etc. Some industry segments involve high temperatures, such as the steel industry, or exposure to chemical elements that corrode the devices, but also to the conditions of the probability of fire, the occurrence of an explosion in the event of a spark in methane rooms. Accordingly, the devices should comply with the appropriate types of protection standards, both active and passive, to have reliable and safe work as long as possible, but also to make the environment as safe as possible. The domain of communication in the industrial application of IoT ES devices is such that the part related to the industrial application is created and connected through industrial buses, so after leaving the industrial conditions, it is connected to Ethernet or WiFi, and etc. [7].

Our list of industry standards for communication infrastructure includes:

- ✓ FF architecture (Foundation Fieldbus) - was created based on peer-to-peer (P2P) technology, respecting the industrial requirements of the working environment, to communicate directly with each other without the required master who initiates communication, and is used in the field of control, diagnostics, change measurement in various industrial fields;

- ✓ Profibus - primarily used in industry in construction and production processes;
- ✓ HART (Highway Addressable Remote Transducer) is designed to establish point-to-point digital communication between the ES device and the central control system;
- ✓ Interbus – fast and robust enterprise network protocol based on serial data transmission for communication between controller, system/computer, sensor/actuator;
- ✓ Bitbus is not a proprietary technology, and consists of an RS485 interface and software, and ensures low overall costs, compatibility with different operating systems, and high reliability;
- ✓ CC-Link open network for automation and data communication available for integration for different interfaces and development;
- ✓ Modbus – industrial communication protocol that is most often used for communication of PLC systems with computers via serial links;
- ✓ Batibus – developed to strengthen industrial communication in complex automated tasks, and uses a twisted pair cable system for communication between sensors and actuators;
- ✓ DigitalSTROM – transmission technology that should enable control and management of electrical systems through existing energy supply lines;
- ✓ Controller area network (CAN) – standard for serial bus communication for industrial and automated applications, with a large number of wires, and provides high speed, separate control and data messages transmitted over individual wires;
- ✓ DeviceNet – enables the communication between the PLC and other devices such as sensors, actuators, etc.;
- ✓ LonWorks – is an open network standard used for interoperable communication between devices and entities such as various control devices, sensors, actuators, etc.;
- ✓ ISA 100.11a – the standard enables wireless communication and industrial automation, and includes security measures such as AES 128 encryption [10];
- ✓ Wireless HART – similar to the previous HART standard with the possibility of Wireless communication with the rest of the HART-based devices;
- ✓ LoRa and LoRaWAN are used for communication in multiple Ghz spectrums for wireless communication over longer distances [9];
- ✓ NB-IoT – a standard that enables robust energy-efficient wireless communication for long distances, created to coexist with networks like 3G or 4G;
- ✓ IEEE 802.11AH – a newer protocol with improvements, works on free 900 MHz and consumes significantly less electricity. energy, uses OFDM modulation, significantly improving bandwidth.

The above-mentioned and described industrial communication standards are applied depending on the conditions of the working environment, distance, equipment specificity, required speeds, investor and user requirements, but also security challenges and reliability conditions of the communication links themselves [1]. In industrial conditions, such as coal mines, there are usually sensors, or information providers, which, through the certain network infrastructure, deliver data to the control system, which for industrial processes is realized through SCADA or PLC, and lately by applying fuzzy logic FLC [3], as well as in the procedure process automation, the learning process of certain procedures and automatic reactions is provided by the application of neural networks or machine learning [4].

After collecting the data, it is important to filter it according to certain criteria, then prepare and convert it into the appropriate standard, both for exchange, further processing and storage, and for the application of business intelligence, which helps managers the most in the field of business decision-making. Since it involves hundreds of sensors or information providers through a technological process, large amounts of data are collected, so it is necessary to analyze them after filtering and preparation, applying some of the same methodologies. In this domain, the Lean Manufacturing and Six Sigma (LSS) methodology is most often used, which, in addition to being widely applicable in business, is robust, and with the right approach provides waste removal, flexibility and openness to use.

Applying these analytics results in data improvement of over 30%. After this step, business process analytics (BPA) are accessed, which are integrated into some of the information systems such as SAP, Oracle, IBM, etc. The BPA framework integrates data into server storage using extract, transformation, and load (ETL). Further activities are performed through multiple servers that work as OLAP, data mining engines, or enterprise search engines, as well as reporting servers implemented in the data warehouse. After that, through the front-end application and in the domain of the visual interface, interaction, different scenarios, data and data exchange are provided.

Depending on the situation in the company, through the adequate application of IoT, ES devices, fuzzy logic, machine learning, artificial and business intelligence, through the entire process of digital transformation and the establishment of quality management, it is possible to ensure a reduction in the preparation time for maintenance from 20 to 50%, increase the working time up to 20%, reduce management costs by up to 10%, and further application of inspection and prediction measures can reduce costs by up to 25%. Data collection and automation can be used in a variety of ways to improve the reliability and safety of technological processes, employees and assets, as well as reduce costs and increase revenues in the company.

One of these ways is the application of predictive analysis for failure forecasting (PdM). To be able to use the mentioned application, it is necessary to install different information providers on the production and supporting equipment, which collect data in real-time, establish alarms, logs and information about the status of the equipment, then connect the same through industrial equipment, for example.

With industrial switches, routers, Wireless AP, wired or wireless, data is transmitted in industrial conditions while respecting industrial standards.Then, the data and server infrastructure, on which the Platform for processing large amounts of data in real-time, as well as the Platform for analyzing large amounts of data offline, is established. In interaction with the server and data infrastructure, it is necessary to provide the visual presentation and management of production and other processes in the company [2].

The framework for PdM implementation includes Project management in all seven stages, collecting and processing data related to the management domain in the function of failure prediction, and these seven steps in the function of failure prediction are:

1. Asset value ranking and feasibility study - includes the most valuable equipment and its parameters in the domain of availability, their impact on reliability, safety, as well as process costs.
2. Selection of assets for PdM - after the study, a presentation of the assets and their parameters that could influence the appropriate prediction;
3. Reliability modeling - in this step, it is important to deeply recognize the variety of failures and modes of operation, to understand the connections between sensor data, process data and external data, if necessary, and especially tools to analyze the causes and effects of failures.
4. PdM Algorithm Design – The quality of the prediction depends significantly on this step.
5. Real-time performance monitoring – After selecting and implementing the appropriate optimization algorithms through machine learning, PdM is launched in a real environment, where data is collected and visualized from various sources [5].
6. Failure prediction – Taking action based on the results delivered by the algorithm, associated with a change in mindset.
7. Prescription of preventive action - represents the highest level of intelligence of the PdM model, which, based on the knowledge acquired so far, coordinating with the algorithm and possible scenarios and procedures, establishes automatic preventive tasks in the function of preventing failure [6].

Experiences documented through studies from various mining companies tell us that the full application of technology and the development of new technologies through investment in development can preserve or save 37% of the current energy consumption in mines, which in itself means huge environmental benefits, but also financial savings.

5. Virtual Security of ES Devices Applied with IoT

Depending on the approach, virtual security with IoT and ES devices is often divided into components:

- ✓ Application security - through this type of security, the goal is to protect applications from vulnerable risks or threats using software, hardware and procedures.
- ✓ Information security - through this security, by controlling purposes, policies, and tools, it is protected against digital or non-digital threats of various data formats [11].
- ✓ Network security – a variety of policies, devices, and tools are applied to protect against unauthorized access and protect against unwanted network traffic.
- ✓ Business security - we try to look at every segment of business and upgrade in the domain of security in business cycles from initial data, revision of management processes, information policy, purpose and scope of the plan, detail and insight into procedures, flowcharts, schedules, responsibilities, to updating the final plans, with previous security analysis.
- ✓ Operational security - represents logical risk management that helps managers to recognize and protect critical data from potential attackers, using the following steps: recognition of sensitive and critical data, recognition of potential dangers, analysis of legislative deficiencies and omissions, risk assessment, and application of appropriate countermeasures threats.

- ✓ Education of end users - Education in the domain of security raises awareness, and knowledge, establishes procedures, minimizes the possibility of establishing intruders, theft of personal data, removes security risks from the domain of knowledge and application, etc.

There are several security threats in the virtual space, and below we list some of them:

- Ransomware - a type of malicious software - virus, which aims to lock or limit access to some resource such as data, using encryption techniques and requires a certain counter value to decrypt them.
- Malware - software that secretly operates on an ES device or network with the primary goal of stealing secret and important data, and important codes, interrupting normal operations, and opening up the possibility of making the device and user a victim, other threats of viruses, worms, Trojan horses.
- Social engineering – attack strategy using sensitive data, through psychological manipulation, which consists of the following steps: identification and research of information about the potential victim of the attack, engagement of the victim and his fraud, extraction of data about the victim, removal of all malware paths and possibilities. These techniques are usually used: baiting, scareware, trickery, and power feeding.
- Phishing - a very common attack, where the e-mail notification system is used to establish a connection and to establish an intruder who would collect all important information from passwords, credit card details, personal data, business secrets, payment methods, etc. There are two types most often via e-mail - where a series of e-mails are sent, and some kind of connection is expected, as well as targeted e-mails to certain persons where sensitive data is expected to exist. It is necessary to increase the security of sensitive data, both with encryption and access data (credentials).

It is necessary to carry out certain security and vulnerability tests, in all domains, and based on the above results, implement measures to increase security. This is a continuous process, and represents an increasingly demanding and responsible part of the tasks because virtual security is becoming an increasing challenge because an increasing number of companies are carrying out digital transformation, the establishment of IoT, operating through IT technologies and ES devices and Internet resources, as well as value, as the risks become greater. On the other hand, new hacking software and protection software are being developed every day, so the research and application of these areas is a continuous process.

6. Security on the Network Architecture of Embedded Systems Devices

In companies, system security solutions that include more and more broad types of protection are being applied more and more often, respecting the standards. But from one manufacturer, because by combining several manufacturers, certain comparative advantages are lost due to reduced compatibility. Such system security solutions should have security control mechanisms in the following areas:

- Access control - it should be ensured that IT resources are accessed only by authorized persons and devices, while records of the same are kept;
- Antivirus and anti-malware software - located on the firewall, as well as clients on all computer, mobile, embedded systems, as well as network infrastructure, set to perform system control and upgrade, but also signaling in case of activities where human support is required;
- Application security - includes security that should minimize risk factors at the application level, to ensure the smooth implementation of the process;
- Behavioral analytics - records and notification should be provided, but also the blocking of any unacceptable behavior or behavior that is not recommended by the user;
- Data loss prevention (DLP) – this measure is implemented through an organization, procedures, minimization of the number of access users, authorization, recording, software signaling modalities and constant improvement, and special data protection measures are implemented in companies that have very important data assets;
- Email security - blocks applications that aim to use various techniques from social engineering, spam, or similar messages to establish malicious communication, and protect sensitive data from loss;
- Firewall - serves as a fence between the intranet (secure network environment - under security measures) and the Internet (non-secure network environment), establishing access rules, monitoring and recording content. These devices are increasingly being improved by various other segments such as IPS, web security, mobile device security, Email security, application security, and data loss security, and are becoming basic security devices in an increasing number of companies that use advanced IT devices.

- Intrusion Prevention System (IPS) – investigates traffic and blocks possible traffic related to potential attacks. IPS usually comes with IDS in charge of recording this type of traffic;
- Security of mobile devices and embedded systems - unauthorized access and control of such devices is reduced, because, with the increase in the number of applications and various types of applications, security risks also increase [8], so these types of devices can access common resources by observing security rules through VPN, security certificates and the necessary encryption, as well as through the authorized access of each user and device;
- Virtual Private Networks (VPN) – a programmed environment that provides a secure and encrypted network connection between endpoints;
- A web security solution that controls web threats, user access and prohibits access to malicious threats;
- Security of the endpoint - ensuring security means control of files, and processes, checking through the organization and appropriate software of all data flows, establishing connections, active control against viruses, suspicious software, and data leaks, but also through the administration of optimizing the use of IT resources;
- Web gateway security – detection of possible DNS or IP-level attacks, such as phishing, malware and ransomware;
- Cloud Access Security Broker (CASB) – a tool that acts as a gateway between cloud infrastructure and applications, with the task of identifying malicious applications and restricting their activity by creating a security shield.

7. Security of Embedded Systems

Security is a critical aspect of embedded systems, especially in the context of their interaction with other IoT components. Ensuring the security of these systems is essential to protect against potential vulnerabilities and threats.

Here are some key aspects of security for embedded systems and their interaction with other IoT components:

Authentication and Authorization:	Embedded systems should have strong authentication mechanisms to verify their identity before interacting with other IoT components. This can involve using secure keys, certificates, or biometric authentication. Implement access control policies to determine what actions and data each embedded system can access or modify. Ensure that only authorized devices can perform specific operations.
Secure Communication:	Use strong encryption protocols to secure data in transit between embedded systems and other IoT components. This prevents eavesdropping and data tampering during communication. Choose secure communication protocols that are designed for IoT, such as MQTT or CoAP, and configure them to use encryption and authentication.
Firmware and Software Security:	Implement secure boot mechanisms to ensure that only authenticated and unaltered firmware or software can run on the embedded system. Keep firmware and software up to date to patch known vulnerabilities and improve security. Design embedded systems to resist physical tampering and unauthorized access. Use secure storage for sensitive data, such as cryptographic keys, to prevent unauthorized access or theft.
Network Security:	Employ firewalls and intrusion detection systems to monitor and control network traffic, detecting and blocking suspicious activities. Isolate IoT components into network segments to limit the potential impact of a security breach.
Secure Device Management:	Implement secure remote management capabilities to update firmware and monitor device health. Maintain a secure record of device lifecycle events, including provisioning, decommissioning, and revocation of access.
Security Monitoring and Incident Response:	Enable robust logging to track and analyze security-related events for early threat detection. Develop a comprehensive incident response plan to address security breaches promptly and effectively.
Security Standards and Compliance:	Follow industry-specific security standards and best practices, such as ISO 27001 or NIST Cybersecurity Framework. Conduct regular security audits and assessments to ensure compliance and identify weaknesses.
Supply Chain Security:	Secure Supply Chain: Ensure that components and software used in embedded systems come from trusted sources and are not compromised during manufacturing or distribution.
User Education:	Educate end-users and administrators about security best practices, including the importance of strong passwords and safe device management. In the ever-evolving landscape of IoT and embedded systems, security should be an ongoing concern. Regular updates, threat assessments, and proactive measures are essential to maintain the integrity and confidentiality of data and the reliability.

8. Conclusion

IT Security needs to be improved through software and hardware, but also through knowledge, procedures, greater commitment, greater stimulation, and punishment because the potential for damage that can be caused by a lack of security is increasing. Companies that have an information system, process automation, implemented IoT, and built-in systems, create security systemically at the level of the company itself, but also granularly by area, so it has to be coordinated. In its function, appropriate security control centers are used, which, in coordination with software, usually client-based on other devices, carry out basic security coordination in the domain of updates, and active control, but also applied security measures towards the Internet, as well as content moving from or towards the intranet platforms, intranet devices and users.

When developing a particular security mechanism, potential attacks on the mechanism have to be considered in particular, because in many cases successful attacks are designed to exploit unexpected weaknesses in the mechanism. The designer of the security mechanism has to find and eliminate all weaknesses to achieve security, while an attacker has to find only one weakness and compromise security. Cryptographic hash functions, i.e. the so-called message summaries (hash functions), represent the foundation of modern cryptography when preserving data integrity and when verifying the authenticity of a message.

Embedded systems are at the heart of the IoT revolution, enabling a wide range of devices to connect and communicate seamlessly. This connectivity is reshaping industries like healthcare, agriculture, transportation, and smart cities. While the potential is immense, security remains a paramount concern.

The interaction between embedded systems and other IoT components requires robust security measures to protect against cyber threats, data breaches, and privacy violations. Developing standards and protocols for interoperability among diverse IoT components and embedded systems is crucial for seamless communication and functionality. This ensures that devices from different manufacturers can work together effectively. The integration of AI and machine learning into embedded systems is driving innovation. These technologies enable autonomous decision-making, predictive analytics, and advanced pattern recognition, expanding the possibilities for smart applications. Embedded systems can contribute to sustainability efforts by optimizing resource utilization and reducing waste. They play a vital role in environmental monitoring, energy management, and efficient transportation systems.

As embedded systems collect and process vast amounts of data, addressing data privacy concerns and adhering to ethical principles become imperative. Transparency and responsible data handling are essential for user trust. The ecosystem of embedded systems and IoT components continues to evolve rapidly. Staying updated with emerging technologies and industry trends is essential for developers and businesses looking to capitalize on opportunities.

The future of embedded systems and their interaction with IoT components holds incredible potential for innovation and improvement across industries. However, success in this evolving landscape will depend on addressing security challenges, ensuring interoperability, and upholding ethical and privacy standards. As developers and organizations navigate this dynamic environment, they have the opportunity to shape a smarter, more connected, and sustainable future.

References:

[1]. Rahmanović, A. & Saračević, M. (2020). Analysis of Security of QoS in WiMAX and Mobile Networks. *SAR Journal*, *3*(3), 124-132.

[2]. Soofastaei, A. (2021). *Data Analytics Applied to the Mining Industry*. CRC Press.

[3]. Baradkar S.C., Ganveer A., Lokhande S., & Surender K. (2016). Fuzzy approach for examing the performance of driver. *International Journal of Advanced Research in Computer and Communication Engineering,* 5(7), 663-666.

[4]. Kasprzak, E.M., Lewis, K.E. (2001). Pareto analysis in multiobjective optimization using the colinearity theorem and scaling method. *Structural and Multidisciplinary Optimization*, *22*, 208-218.

[5]. Kopetz, H. (2011). *Real-Time Systems: Design Principles for Distributed Embedded Applications*. Springer. Doi: 10.1007/978-1-4419-8237-7

[6]. Krisciunas, K., & Carona, D. (2015). At what distance can the human eye detect a candle flame?. *arXiv preprint arXiv:1507.06270*.

[7]. Singh, M., Rajan, M.A., Shivraj, V.L., Balamuralidhar, P. (2015). Secure MQTT for Internet of things (IoT). In *2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India,* 746-751. Doi: 10.1109/CSNT.2015.16

[8]. Marwedel, P. (2021). *Embedded System Design: Embeded Systems Foundations of Cyber-Physical Systems*. Springer. Doi: 10.1007/978-3-030-60910-8.

[9]. Consul-Pacareu, S., Mahajan, R., AbuSaude, M.J., Morshed, B.I. (2017). NeuroMonitor: a low-power, wireless, wearable EEG device with DRL-less AFE. *IET Circuits Devices Syst. Journal, 11*(5), 471-477.

[10]. Misra, S., Roy, C., Murherjee, A. (2021). *Introduction to Industrial Internet of things and industry 4.0*. CRC Press.

[11]. Devi T. R. (2013). Importance of Cryptography in Network Security. In *2013 International Conference on Communication Systems and Network Technologies, Gwalior, India*, 462-467. Doi: 10.1109/CSNT.2013.102.