"COBOT" TYPE MULTIAPLICATIVE INTELLIGENT PLATFORM WITH ROBOT & HEXAPOD MICROSYSTEM AND ULTRAPRECIS PING PROBE FOR MEASURING PARTS (WITH A 3KG TABLE)

Gheorghe GHEORGHE[1]
[1]National Institute of Research and Development for Mechatronics and Measurement Technique – INCDMTM, Bucharest
Email: geocefin@yahoo.com

Abstract - The scientific paper "«Cobot» type multiaplicative intelligent platform with robot & hexapod microsystem and ultraprecise probe for measuring parts (with a mass of 3 kg)", presents an intelligent cobotic application, which provides 11 degrees of mobility for the ultra-precise probe by its positioning - in the entire general workspace - with nanometric precision [7 nm], in the vicinity of the point where the measurement is desired.

Keyword: Multi-Application Smart Platform; Hexapod Microsystem; Nanometric Accuracy.

1. Introduction

In the application depicted in the figure below, a collaborative robotic platform (1) for the intelligent measurement of functional objects with a table of 3Kg is presented, which integrates two robotic systems, in a serial-parallel display (Patent ID: A-00610), providing 11 degrees of freedom (11DOF) (6DOF universal robot (1.6), 6DOF hexapodal robot (1.12) of which 1DOF is common with that of the universal robot - respectively the final effector) and allows the positioning in space, in two stages, of the final effector, respectively an ultra-precise transducer probe (1.13), by orienting it throughout the general workspace, with the positioning accuracy of the universal robot (0.2mm) and the local orientation with nanometric precision (7nm), of the final effector probe with the hexapodal robotic system (± 7mm), in the vicinity of the point where the measurement is intended.

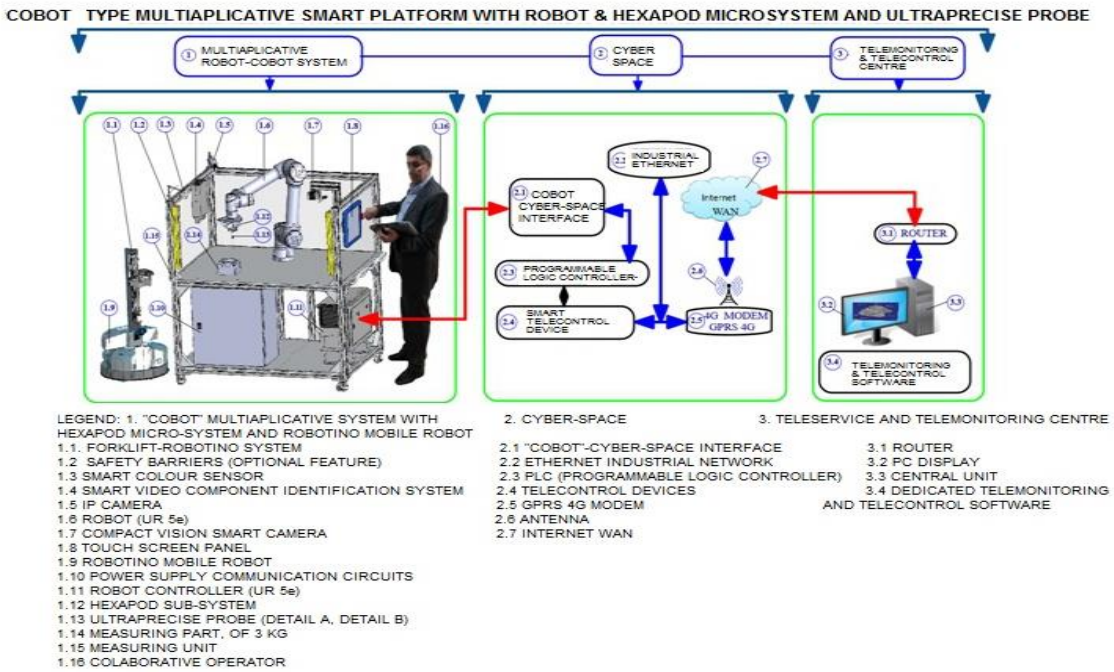

Figure 1

By using a parallel structure specific to the Stewart (hexapodal) platform that ensures a much more accurate intelligent positioning (about 28x103 times) compared to the serial structures that position the palpation transducer with the effector of a single robot.

The intelligent multi-application platform type "Cobot" realizes the remote control of mechatronic cyber-mix platforms type "Cobot multiaplicative" (1) by bidirectional data transmission and realization of remote control, telemonitoring and teleservice functions through the cyberspace (2) in the Center Remote control and Teleservice (3), using specialized programming and visualization software.

The assembly is equipped with a multisensory system consisting of: intelligent color sensor (1.3), intelligent video identification system components (1.4), IP camera (1.5), intelligent camera COMPACT VISION (1.7). The fusion of data from the multisensory system together with those from the final effector used depending on the application, allows the performance of a variety of intelligent tasks, with a high degree of adaptability and flexibility.

A mobile intelligent robotic platform (Robotino) (1.9), equipped with WiFi communication system, performs the collaborative function of supplying parts \ subassemblies subjected to the adaptive process of intelligent analysis \ measurement, by fixing them on the rigid table (1.14) using a mechatronic system Forklift-Robot (1.1). The synchronization with the cobotic platform as well as the communication with the remote control center is done via WiFi, directly in the Wan Internet network.

The system is additionally protected by infrared safety barriers (1.2) and communicates with the special equipment in the cabinet (1.11) both with the internal industrial bus (2.2) and with the WAN Internet network via the 4G GPRS modem. This communication connection connects to the remote control center (3) provided with a PC central unit (3.3) connected to the router (3.1) and on which the specialized software (3.4) runs.

The system can also be operated locally, using a pre-installed program by emulating working positions using the Touch-Screen Panel (1.8). The positioning of the final effector (3D scanner) can be done in a well-defined area of the entire workspace of the robot with 6 degrees of freedom (6DOF).

During the measurement process the position information pairs - i.e. the measured values - are transmitted in vector numerical data packages for complex processing both in real-time and for later processing.

In addition to the innovative performance of robotic platforms, operator safety is another necessary key to successful operations in the intelligent manufacturing process. To avoid risky situations, until the appearance of the cobots, industrial robots have been kept away from workers through a series of protection measures since the beginning of the history of automation. Collaborative robots have completely changed the paradigm and allowed the implementation of cobotic platforms, without a safety infrastructure that requires high costs and space. The main competitive advantages of UR cobots include easy operation, fast deployment, and the existence of an interface that allows the collaborative operator (1.16)to take on intuitive programming, which can also be performed by direct physical contact with the robotic arm or the touch-screen. Cobots are thus able to work in close proximity to humans without safety barriers, but this approach requires full control over the speed, strength, power, and momentum generated by the cobots during their operations. Even though UR cobots are at the top of safety standards, the multi-application cobot platform has also been provided with optical safety barriers, as an additional adaptive function for a wide range of applications.

The connection to the cyberspace (2) is made through a specialized interface (2.1) that allows communication with the robot controller (1.11) the data being adapted to be transferred to a Programmable Logic (PLC) (2.3) used to automatize mechatronic processes and for storing the working variables of the specific control program as well as to receive in information from the intelligent remote control equipment (2.4) in a synchronized way - this being implemented either with a microcontroller with RISC architecture or with a FPGA and which connect the PLC and the 4G telecommunication modem using a specific RS232 or USB protocol.

Various public or private networks can be used to access the 4G connection. The connection can be ensured via a wide variety of modems (2.3) that are compatible with VPN protocols. Event-driven, event-driven, or cyclic data processing is performed using special remote control protocols and allows operating personnel to efficiently manage the process as a whole or in detail.

The Remote Control Center (3) provides the WAN Internet connection (2.7) using a router (3.1) equipped with a VPN function meant to ensure data security encryption. The second level of security can be studied by using its own encryption algorithm and by specifically configuring the FIREWALL function of the operating system on the PC (based on Windows or Linux). The computer (3.3) in the Telemonitoring Center (3) runs a software specially designed to perform the functions of remote control, telemonitoring, and teleservice.

From the point of view of the integrity and security of the data flow of data from the multi-application Robot-Cobot System (1) to cyberspace (2) and the telemonitoring and remote control center (3), the issues that arise belong to two categories: hardware and software.

2. Hardware Security Issues

From a hardware point of view, the compatibility of data types and logic levels between systems and subsystems with the minimization of noise and interference levels must be considered;

The UR5e Robot Controller.

The UR5e collaborative robot (1.6) receives control signals from the Controller (1.11) which can communicate with the INDUSTRIAL ETHERNET network (2.2) via the Cobot Cyber-Space Interface (2.1) using the ETHERNET-IP protocol. In the Controller (1.11), on the bottom of the I / O interface groups, there is a rack with ports that ensure the Ethernet connections (depicted in the figure below).

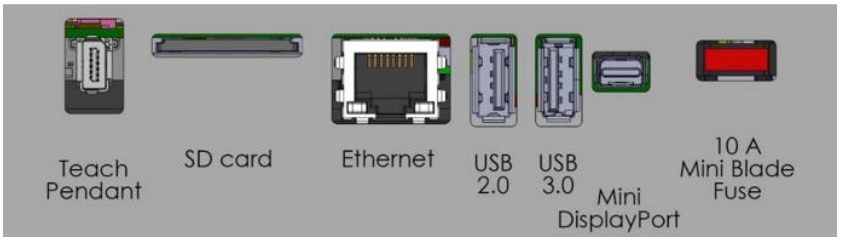

Figure 2

The robot's Ethernet interface can be used to perform the following functions:

Remote access and control.

MODBUS, EtherNet / IP and PROFINET (see PolyScope software).

The data is encapsulated in the robot controller. Encapsulation is the process of adding headers and "trailers" around the same information (data).

An example would be the transfer of data from the controller to a computer. At the Application level, as the OSI (Open Systems Interconnection) the stack is traversed, and small changes are made to the data. The data is segmented and a header is added that contains information about which process should run on the destination machine, and which should receive the message. The data package also contains information that allows the destination to reassemble the data into the original format transmitted by the source. At the Internet level, the segments are encapsulated in packages that contain the source and destination IPs of the equipment with which the transfer is made. At the Data Link level, the division into frames takes place and the physical address, the MAC (Media Access Control) address, which must be unique in the local network, is added, and in the last phase, the information is transformed into bits. Encapsulation takes place from the upper level, the Application in the lower, Physical, level, while the decapsulation is the reverse process, performed from the Physical level to the Application level. Depending on the network equipment via which data travel through the destination, the data is decapsulated at different levels. For example, a switch decapsulates in level two because it needs the MAC address in order to send the package to the destination. The router needs the destination IP address, so the packages will be decapsulated at the Network level.

The figure below integratively depicts the connection between the physical and virtual elements that make it possible to transmit the data flow between the robot and the PC Central Unit.

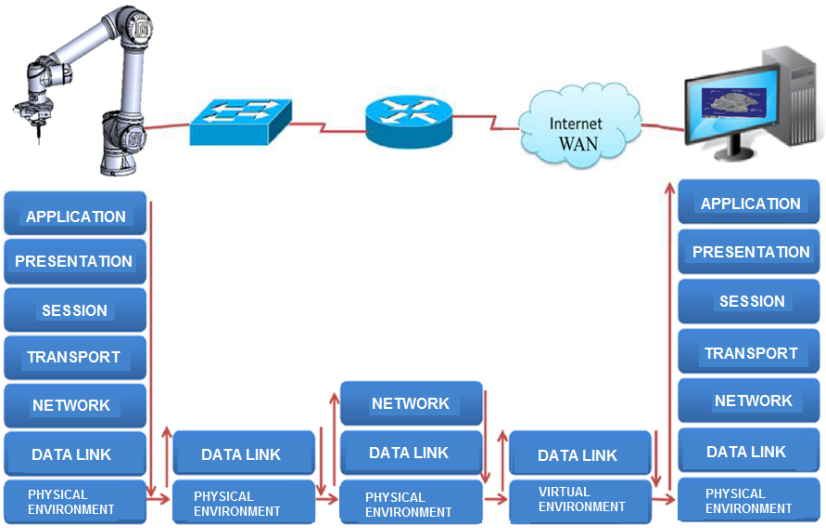

Figure 3

The smart remote control hardware firewall equipment

The smart device (2.4) is actually a hardware firewall. Firewall solutions fall into two broad categories: the first comprises professional hardware or software solutions dedicated to protecting the entire traffic between a network and the Internet, and the second category is represented by personal firewalls dedicated to monitoring traffic on your personal computer.

A hardware firewall always works with a routing program and examines each data package in the network (either local or external) that will pass through the gateway server to determine if it will be forwarded to the destination.

A hardware firewall permanently monitors and filters data transmissions made between the 4G / 5G GPRS modem (2.5) and WAN Internet (2.7), in order to protect and control the resources of the Ethernet Industrial local network (2.2) in cyberspace (2) from other users from other similar networks called firewalls.

The following figure shows an example of D-LINK DFL-800 firewall hardware, equipped with LAN: 7x 10 / 100Mbps; WAN: 2x 10 / 100Mbps.

Figure 4

A Firewall is a form of protection that can keep away cyber-attack Internet traffic, such as hackers, worms, and certain types of viruses before they cause problems to the system. The use of a firewall is especially important if the system is permanently connected to the Internet.

A firewall can perform the following functions:
- to monitor the penetration routes in the private network;
- to detect infiltration attempts;
- to select access to the private cyberspace based on the information contained in the data packages;
- to allow or prohibit access to the public network from certain specified stations;
- to isolate the private space from the public one and to realize the interface between the two domains;
- to block traffic to and from the Internet at some point.

Also, a firewall application cannot perform the following functions:
- to prohibit the import/export of harmful information transmitted as a result of the unauthorized action of some users, belonging to the private space (ex: the mailbox). This protection is to be ensured by other methods;
- to prohibit the leakage of information from other channels bypassing the firewall (access via dial-up that does not pass through the router). This protection is to be ensured by other methods;
-to protect the private network from users using mobile physical data entry systems (USB Stick, CD, etc.)
- to prevent the manifestation of design errors of applications that perform various services, as well as the drawbacks arising from the exploitation of these mistakes.

Router-like hardware equipment

A router (3.1) is a piece of hardware necessary for the connection of the PC in the Telemonitoring and Telecontrol Center (3).
A router has the following functions:
- It works in accordance with specific Internet protocols: IP, ICMP, and other protocols.
- It provides the interface between 2 or more networks. For each network that is connected to a router, it must implement the functions required by that network. These functions usually include the following: - to encapsulate and decapsulate IP datagrams - e.g. adding and removing the Ethernet header and the FCS (frame check-sum) field;
- to send and receive IP datagrams smaller than the maximum length supported by that network. This maximum length is called the Maximum Transmission Unit (MTU);
- to translate the destination IP addresses into network-level addresses suitable for the connected network (for example, an Ethernet hardware address), if necessary;
- to be familiar with the flow control network protocol and error indicators, if any;
- It receives and transmits Internet datagrams. An important feature of this process is buffer management, traffic congestion control, and prioritization, as follows:
- to recognize error conditions and generate Internet Control Message Protocol (ICMP) errors and additional information messages if applicable;
- to eliminate datagrams whose lifetime has become zero;
- to fragment datagrams where appropriate to fit into the MTU of the network on which they are to be transmitted;
- It chooses the next destination for each IP datagram, based on the information (routes) in its database;
- It supports an internal gateway protocol (IGP) needed to ensure dynamic routing and communicate with other routers that are part of the same autonomous system (AS);
- It provides network management methods and system support facilities, including upload, status reporting, exception reporting, and control.

Hardware viruses are less common and they are usually delivered with the equipment, and they are

viruses that affect flash drives, network cards and the memory.

3. Software Security Issues

The issue lies especially with the Telemonitoring and Telecontrol Center, where different application-specific programs run on the central unit (3.3). From a software point of view, the use of specific protocols at the level of cyberspace (2) and WAN (Wide Area Network) Internet communication with data encryption using the VPN (Virtual Private Network) tunnel technique must be considered, thus forming a private network between the Center of Telecontrol and Telemonitoring (3) and the "Multi-application Cobot" System (1).

3.1 Aspects regarding the connection of the Universal Collaborative Robot (UR5e) to the Industrial Cyberspace

The connection of the cobotic system (1.6) with the cybernetic space (2) is made through the Ethernet-IP type Interface (2.1).

It should be noted that here IP does not mean "*identification protocol*" but "*industrial protocol*".

The following figures show the main steps in establishing a connection with cyberspace. Thus, the figure below shows the initialization of the robot interface.

Figure 5: Initialization of the robot interface

The following figure shows how to set an IP address, and the following figure shows:

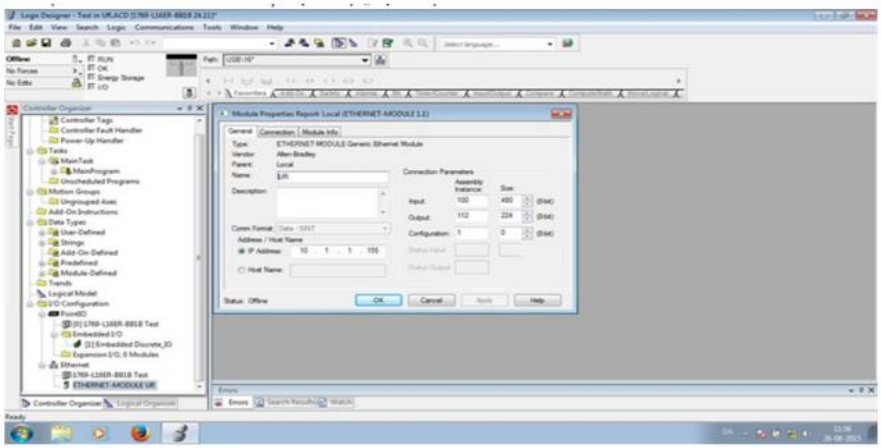

Figure 6

the window of communication to a person's own code and the setting of local variables.

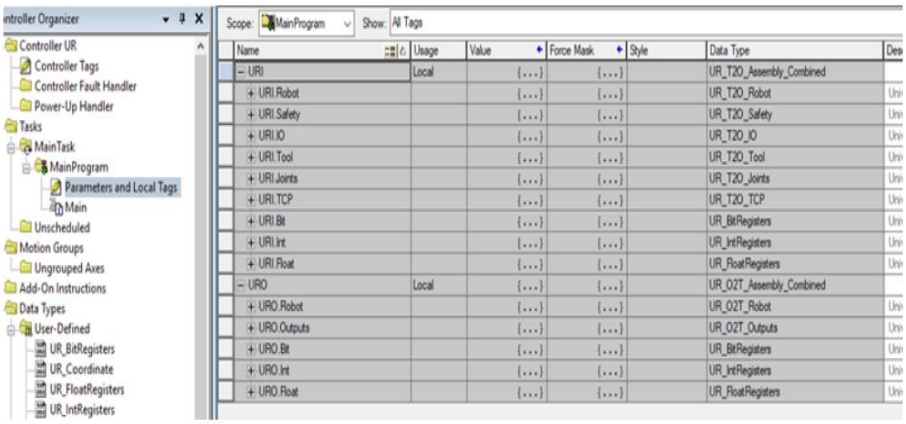

Figure 7

3.2 Software aspects regarding the Telemonitoring and Telecontrol Center

Regarding the Telemonitoring and Telecontrol Center (3) together with the application-specific programs, the Operating System (Windows, Linux, etc.) must also include the following facilities:

3.2.1 The firewall facility

The software firewall works in conjunction with a proxy server that makes packet requests on behalf of users' workstations. These protection programs are installed on computers that perform only this function and are installed in front of routers.

Thus, a firewall is used for two purposes:

- to keep malicious users (viruses, cyber worms, hackers, crackers) out of the network) away from the network

- to keep local users (operators) in the network

Firewalls can be classified according to:

- the layer in the network stack on which they operate

- the way they are implemented

Depending on the layer in the TCP / IP (Transmission Control Protocol / Internet Protocol) or OSI (Open Systems Interconnection) stack on which it operates, the firewalls are:

- Layer 2 (MAC) and 3 (datagram): packet filtering.

- Layer 4 (transport): it is also a package filtering, but one can differentiate between transport protocols and there is the option of a "stateful firewall", in which the system knows at any time what are the main features of the next expected package, thus avoiding a whole class of attacks

- Layer 5 (application): application-level firewall (there are several names). It generally acts like a proxy server for various protocols, analyzing and making decisions based on application knowledge and connection content. For example, an SMTP server with an antivirus can be considered an email application firewall.

Depending on how the firewalls are implemented, they can be either:

- dedicated, in which the device running the filtering software is dedicated to this operation and it is practically "inserted" in the network (usually right after the router). It has the advantage of increased security, or

- combined with other networking facilities. For example, the router can also serve as a firewall, and in the case of small networks, the same computer can also play the role of a firewall, a router, a file/print server, etc.

The firewall security service is package filtering. It allows or blocks the passage of certain types of packages according to a system of rules established by the security administrator. For example, IP packet filtering can be done by different fields in its header: source IP address, destination IP address, TCP or User Datagram Protocol (UDP), source port or destination port.

The filtering can be done in a variety of ways: by blocking connections to or from certain host systems or networks, by blocking certain ports, and so on.
Package filtering is usually done on routers. Many commercial routers have the ability to filter packages based on header fields.

It is recommended to block services at the firewall level:

- tftp (trivial file transfer protocol), port 69 commonly used for the boot sequence of diskless stations, terminal servers, and routers. Incorrectly configured, it can be used to read any file in the system;

- RPC (Remote Procedure Call), port 111, including Network Information System (NIS) and Network Information Frame (NIF) which can be used to obtain system information, stored files, etc .;

The following services are usually filtered and restricted only to those systems that need them:

a) Telnet, port 23, restricted only to certain systems;

b) Ftp (file Transfer Protocol), ports 20 and 21, restricted only to certain systems;

c) SMTP (Simple Mail Transfer Protocol), port 25, restricted to a central mail server only;

d) RIP (Routing Information Protocol), port 25, which can be easily deceived and determined to redirect packages;

e) DNS (Domain Name System), port 53, which can provide information about addresses, names, very pursued by attackers;

f) UUCP (Unix to Unix CoPy), port 540, which may be used for unauthorized access;

g) NNTP (Network News Transfer Protocol), port 119 for access to various network news;

h) http (Hypertext Transfer Protocol), (port 80), restricted to an application gateway running proxy services.

3.2.2 Installing Anti virus Program facility

Viruses are software programs created by computer specialists that are based primarily on how the operating system (OS) works.

Some of the effects that software viruses generate:

a) destruction of files;

b) changing the file size;

c) total deletion of information from the disk, including its formatting;

d) destruction of the file allocation table, which makes it impossible to read the information from the disk;

e) various harmless graphic / sound effects;

f) slowing down the working speed of the computer until it crashes.

g) copying data and information

Viruses can be divided into two main categories:

- **BOOT (Build-Operate-Own-Transfer) v**iruses that load into memory before the operating system, transfer BOOT contents to another sector, shuffle data, infect any logical hard disk drive and any floppy disk that is inserted into the floppy drive. This category also includes viruses that infect the hard disk partition table. Found in the partition table, they are loaded into memory before the BOOT sector.
- **File viruses** are usually attached to .exe or .com file extensions. When the infected program is run, the virus is activated, most of the time remaining in the memory to infect any program that will be launched. Unfortunately, file viruses are of many types. So far, the "classic" type has been described.

There are also viruses with the characteristics of both categories (both BOOT and file), but these come in very small numbers.

A Trojan horse - is a program that is apparently useful, but aims to destroy the host. It is a virus program whose execution produces unwanted side effects, generally not anticipated by the user. Among other things, this type of virus can give the system an appearance of normal operation. A well-known example of such a program today is the Aids Information Kit Trojan. "Trojan horse" programs also contain an important feature; unlike common computer viruses, they cannot multiply automatically. However, this is not of significant use for someone who has just lost days and months of work on a computer.

Invisible (stealth) viruses - these viruses mask their presence by hijacking DOS interrupts. Thus, the *dir* command does not allow the observation that the size of an executable file has increased because it is infected. Example: "512", "Atheus", "Brain", "Damage", "Gremlin", "Holocaust", "Telecom".

A Worm - is a program that, inserted in a computer network, becomes active in a workstation where no program is run. It does not infect other files, as real viruses do. However, it multiplies in several copies per system and, especially, in a distributed computing system. In this way it "steals" the system resources (RAM, disk, CPU, etc.).

An appending virus - is a virus that attaches its code to the existing code of the file, without destroying the original code. The first thing that happens when the infected file is launched is the fact that the virus is run. Then it multiplies, causing damage or not, after which it hands over the control to the original code and allows the program to continue running normally. This is the mode of action of a "classic virus".

A cryptographic virus (Crypto virus) - a virus that penetrates the memory of the system and allows the absolutely normal use of data entries and transmissions, having the property that, at a certain date, it self-destructs, destroying at the same time all the data in the system and making it absolutely unusable. Such an attack can simply be activated or annihilated, even by the remote cyber-criminal, by transmitting the corresponding command.

A Morphic virus - a virus that constantly changes its programming code and configuration in order to avoid a stable structure that could be easily identified and eliminated.

A non-resident virus (Runtime virus) - is the opposite of the resident virus. Non-memory viruses do not remain active after the infected program has been executed. They operate based on a simple mechanism and only infect executables when an infected program is running. The typical behavior of such a virus is to look for a suitable host file when the infected file runs, to infect it, and then to regain control of the host program.

A parasitic virus - is a computer virus which attaches to another program and is activated when the program is executed. It can be attached either at the beginning of the program or at the end of it, or it can even overwrite part of the program code. The infection usually spreads when the infected file is executed.

A resident virus - is a virus that self-installs in memory, so that even long after an infected program has been run, and it can still infect a file, based on a "trigger" routine consiting in a certain action), or to monitor the activity of the system. Almost all viruses that infect MBR are resident viruses. In general, resident viruses "hang" the code of the operating system.

Spyware - In addition to the many viruses known at this time in the computer world, there is a special category of "intruders" that have a special role: to inspect, in the computers or networks they enter, everything that spend, and send back to the owner, at a certain date and under certain conditions, a complete report on the "correspondence" on the Internet and other "actions" and send them to the spy through the infected computer.

A system is free of viruses if no virus is resident or hidden in the memory, and the programs running are clean of malicious code. In this conception, an antivirus program targets both computer memory and executable programs at the same time.

The protection programs - antivirus programs - have the role of simultaneously carrying out the following activities:

- prevention of contamination;
- virus detection;
- elimination of the virus, with the restoration of the initial context;

In general, there are two categories of antivirus programs or rather two types of activities performed by antivirus programs:

a) the file verification module used to detect inappropriate texts or recognized virus signatures; b) the module resident in the internal memory, which intercepts the special instructions or those that seem dubious.

These programs first check the internal memory and then the specific disk drive, displaying on the monitor any viruses detected and recognized in that version. After this check, the program will try to remove the detected virus through the cleaning module. It should be noted that, by using these programs, there is no certainty of cleaning the viruses, either because they somethimes cannot be recognized or because they are located in places that cannot always be detected.

3.3 Antivirus Programs Exemples

Further in the paper, I will present the main antivirus programmes on the current IT market.

3.3.1 Eset Software

Founded in 1992, Eset has focused on developing a new era in antivirus systems via NOD32. NOD32 has been developed in several years, so today it is listed as one of the best antivirus products. In fact, NOD32 has won the most awards offered by Virus Bulletin. NOD 32 Antivirus Systems provides protection against a wide range of virtual threats to PCs. it runs on various operating systems such as Microsoft Windows 95/98 / Me / NT / 2000 / XP including versions for Linux, FreeBSD, NetBSD and OpenBSD on x86 platforms. Viruses, worms and other destructive codes are kept away from valuable data. Due to the efficiency and speed of scanning the hard disk (2-50 times faster than any other similar product) and the fact that it occupies between 2-20% less system resources, several international awards have been won. NOD 32 is the world leader in Virus Bulletin medals in the 100% Awards with the most awards compared to any other antivirus product. Since the first test in which he participated, in May 1998, NOD 32 was the only product that did not lose any medal in the detection of viruses "in the Wild".

3.3.2 F-SECURE

F-Secure Corporation is one of the leading providers of centrally managed security solutions. The product portfolio includes both antivirus products and network security solutions for most platforms, from desktops to servers and from laptops to handhelds.

3.3.3 McAfee Security

A trusted name in online security, McAfee provides antivirus products (VirusScan, VirusScan Professional, anti-hacker products (Personal Firewall Plus, Internet Security), antispam products (SpamKiller, Privacy Service, Parental Controls), anti-loss products (EasyRecovery) and many others 17.

3.3.4 Grisoft

Grisoft was founded in 1991 in the Czech Republic by programmer Jan Gritzbach, and now has a headquarters in the United States.

AVG Antivirus has evolved a lot from simple-to-use utilities in the early years. To protect your computer from viruses today you need much more than just a software program. AVG, however, proves day by day that it is a comprehensive service. Prizes won:

VB100% in the November 2003 Virus Bulletin test on the Windows 2003 Server platform.

The 100% detection rate of the AVG Anti-Virus System is continuously certified by ICSA laboratories.

3.3.5 Softwin

The Romanian company SOFTWIN, through its BitDefender product suite, currently offers the most complete antivirus protection solutions both at company level and at home user level, positioning itself, at the same time, as an important integrator of security solutions. security. BitDefender products cover all possible ways for viruses to enter a company's computer network, from a small local area network to a large multi-server or multi-platform network. These include: daily product updates, non-stop technical support, installation assistance, regular system checks, on-site interventions in critical situations and, last but not least, Virus Alert services (via e-mail) and BitDefender Antidot (received within 24 hours from the appearance of a harmful virus. SOFTWIN is a company with fully Romanian capital whose main activity is the development and provision of complex

solutions and services in the field of IT&C. Established in 1990, SOFTWIN has continuously diversified its activity , adding to the core business of developing and implementing complex software applications, new solutions and services such as: ePublishing and eContent Solutions (1993), BitDefender antivirus (1997), contact center services (2000), IT helpdesk (2001) SFT (2002) With a team of over 600 employees, SOFTWIN has developed and implemented cutting-edge technologies in over 5,000 projects developed for partners across the world. world.

3.3.6 Kaspersky Labs 18

Kaspersky Antivirus first appeared in the West in 1994 under the name AVP, and from the very beginning was listed as one of the best antiviruses following credible tests: Virus Test Canter from the University of Hamburg in 1994 and 1995, and independent Virus Bulletin in 1995 and 1996.

Kaspersky Labs is an international software company that provides products for protection against viruses, hackers and spam. Founded in 1997, it has offices in Russia, France, the United Kingdom and the United States and distributes its products in more than 60 countries.

3.3.7 Norton Antivirus

Founded in 1982, Symantec Corporation, a world leader in Internet security technology, offers a wide range of security solutions for both individual users and organizations of all sizes. More than 50 million users use Symantec products, including some of the largest corporations, government agencies, and educational institutions. The company holds numerous patents and awards, which have ensured its leading position in the software market it offers.

Symantec provides solutions for virus protection, email and Internet content filtering, communications, remote management, risk management, and more.

Recent developments in computer threats, especially due to the widespread use of the Internet, have led antivirus software vendors to diversify their customer service by including new modules in their antivirus packages to respond to new threats. Thus, in addition to the main task of fighting viruses, the new antivirus programs are equipped with modules such as e-mail verification, integration in internet browsers for scanning against scripts that may come with web pages applications such as spyware and add-ware. and last but not least, the Firewall component that allows certain types of traffic to be blocked.

4. Security Instruments in the Windows Operating System

Industrial users are concerned about limiting the use of the Internet, due to the attacks that constantly threaten them. In case of performing the function of Telecontrol and Telemonitoring it is not possible to use an Industrial PC (IPC) (3.3) without a permanent connection to the Internet WAN (2.7) through a Router (3.1) and the question arises how we can secure the Operating System. Here are some basic recommendations:

- **Do not browse the Internet logged in as an administrator**

In modern Operating Systems, it is possible to strictly differentiate user accounts. This can protect data from being accessed by other users, limiting the effects of hacker attacks. Thus, authentication in the system as a user with limited rights is recommended.

In principle, it is recommended to create several accounts, one limited to daily work with the system, and another with administration rights, used only when changes and configurations of the computer need to be made. To do this, select User Accounts in the Control Panel and Create a New Accoun, as in the following figure. Now select a name for the account and click Next. The next step is to configure the rights that the new user will enjoy. There are two types of accounts available for this. Limited registration is activated and the Create Account procedure is completed. The created user has only limited rights, which do not allow changes to the system. From this account there is no possibility to install programs and access to the system configuration is not allowed. Even if a malicious program enters the system, its infection is excluded, because the virus does not have access to important system files or the Registry.

Figure 8

The newly created account must now be provided with a password.

To do this, click on *Create a Password* and enter the desired password in the field.

For security reasons, the password must be eight to ten characters long and alphanumeric.

Optionally, special characters such as $,%, § are also available. This protection only makes sense when that user's password is actually used for authentication. Therefore, the *Change the Way Users Log On an Off* option *Use the Welcome Screen* should be disabled as in the following figure.

Figure 9

• **Securing the formatted file system** NTFS/GTO (New Technology File System/ Gerber Top Overlay)

The basis for system security is the NTFS / GTO file system. It allows limited rights to be granted to users. This can remove access to system files for simple users and only the system administrator has all the rights.

If the system is still running FAT32, conversion to NTFS / GTO is possible by the convert c: / fs: NTFS / GTO command and by restarting the system. This may take up to a few minutes until the transformation is complete. To convert other partitions, repeat the procedure by changing only the letter corresponding to the desired drive as in the following figure.

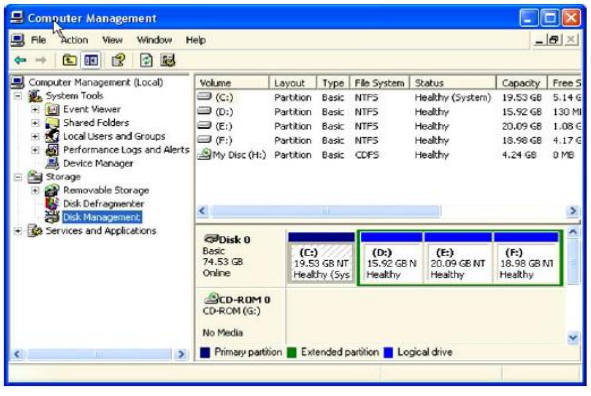

Figure 10

In addition to extended access rights, there is now the possibility to encrypt data in order to protect it from access by other users.

The base is provided by the *Encrypting File System (EFS. In Properties*, for the directory in question you can press the *Advanced and Encrypt Contents to Secure Data* buttons, as in the following figure.

From now on, the possibility to access this data belongs only to the system administrator and The user on whose behalf the encryption was made.Unlike other types of encryption, PGP (Pretty Good Privacy), for example, EFS has the advantage that no management of Registry keys is required.Windows Explorer automatically decrypts data when accessing it.

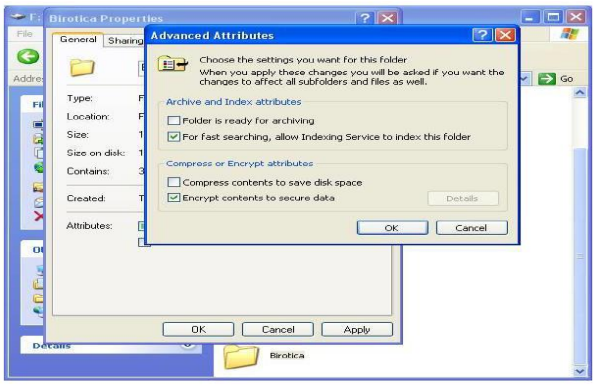

Figure 11

• Disable unnecessary services

Services are loaded processes at system startup, which provide various functions for various parts of the operating system, in the standard Windows configuration, in the background work up to eighty such services.

Additionally, there are others that are required for programs that are later installed on the system. All available services can be found via *Settings-Control Panel-Administrative Tools-Services*. If a service is permanently activated or is started only at certain requests, this is set to the *Startup Type* point. Services that are permanently needed !, receive the *Automatic* startup type, and only temporarily required services are set to *Manual*. Information about that service can be found by accessing *Properties* in the context menu of that record. In addition to the full description, it is also seen for which user it is executed, as well as if it is dependent on other services.

But users do not always need all the services. In addition, especially in network services with open ports for various functions, all sorts of problems arise. One such example is the W32.Blaster worm, which spreads through an error in the RPC service of port 135. But not only worms take advantage of these vulnerabilities, but also hackers. With the Dcom exploit, which uses the RPC service, it is possible to have total control over a computer running a Windows operating system. Therefore, network services that respond to external requests must be protected by firewalls or, if possible, completely disabled to close possible paths.

An easy way to disable services is provided by the Windows XP system setup program. It can be accessed via Start-Run and by entering the Msconfig command (see figure below) where, in the Services menu, a box in front of each service is checked for activation or deactivation, so that it is no longer executed the next time it is started.

A well-thought-out configuration of services can reduce the security risk generated by online attacks and even increase system performance.

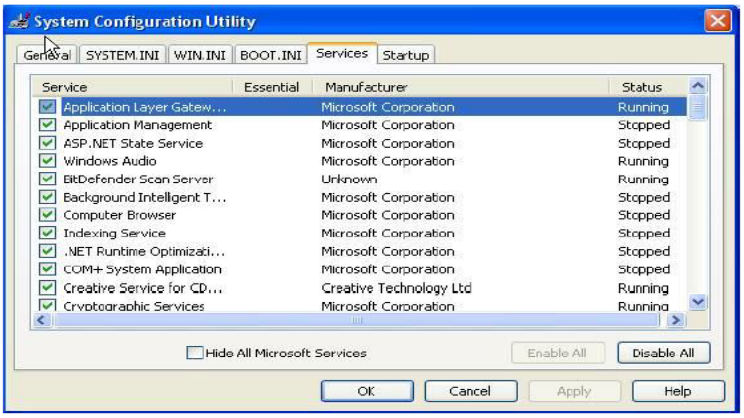

Figure 14

However, it does not disable random services, because many are necessary for the proper functioning and stability of the operating system. In the description provided by Properties, the service is explained exactly, but for the user it is not clear whether it is necessary or not. This depends more on how you use your computer, installed programs, hardware, and installed network components. When it comes to disabling a service, it is always important if the user is using the Internet, if a printer is present, or if Windows Firewall is enabled.

- Configure network shares

With the help of network sharing, individual directories or even disk drives can be used to exchange data between computers or users. This does not pose many problems if the shares are configured correctly and, implicitly, secure in terms of access by unauthorized persons. However, an incorrect configuration of the shares can lead to the reading, manipulation or even the deletion of sensitive data, with a minimum of effort.

It is also worth noting that some users offer these shares not only to the local network, but (unknowingly) to the Internet.

This means that any internet user can access these shares and the data contained in them, can manipulate them and even upload files. Viruses use such security holes in networks to infect systems and spread.

Only the Shared Documents directory is shared in the standard Windows configuration. To allow access to other directories in the system, sharing can be enabled through the *Properties and Sharing* options. By default, only read rights are enabled, and if you need write rights for that directory, they can be granted by checking the *Full Control* field in the *Permissions* chapter. For system data, such as the Windows directory, sharing is disabled for security reasons. In Windows 10, the right to write can be limited by removing the rights for the Everyone group (see figure below), after which access rights are allowed only to certain users.

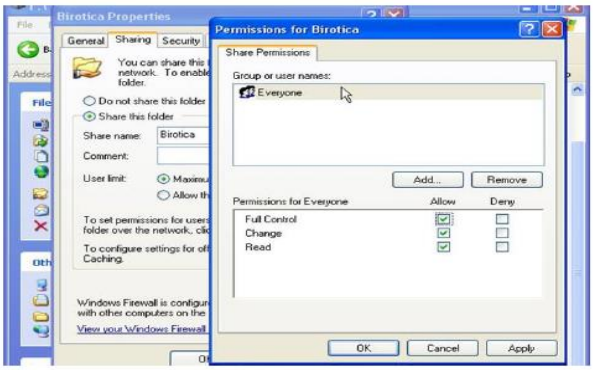

Figure 15

- Use the firewall.

The firewall component has the function of monitoring the communication of the system as well as the applications installed with the internet or network and to block unwanted connections if necessary. Firewall is activated immediately after installation and blocks most programs that communicate with the network.

If a program installed with the operating system tries to initiate an Internet or internal network connection, an information window appears.

The option to block or allow the connection is available. Depending on the selection, the firewall in automatically sets a rule. If an application must be

allowed to make connections, appropriate permanent rules can be set in the *Exceptions* register.

The Programs menu provides a list of all applications installed by the operating system, the connection settings of which can be defined according to your preferences. Individual applications are often not listed. These can be entered in the list using the *Add Program* option, then point the way to the executable by clicking *Browse.* For security reasons, you can further define, at Ports, which interfaces and which protocol - TCP or UDP - the program can use. In the same window is the *Change Scope* button, with which it is possible to enter various IP addresses of the systems with which the program is allowed to make a connection.

If this data is not yet defined, the application is able to communicate on all ports and with all systems which, depending on the application, results in various security risks.

The following diagram shows the operation of firewalls.

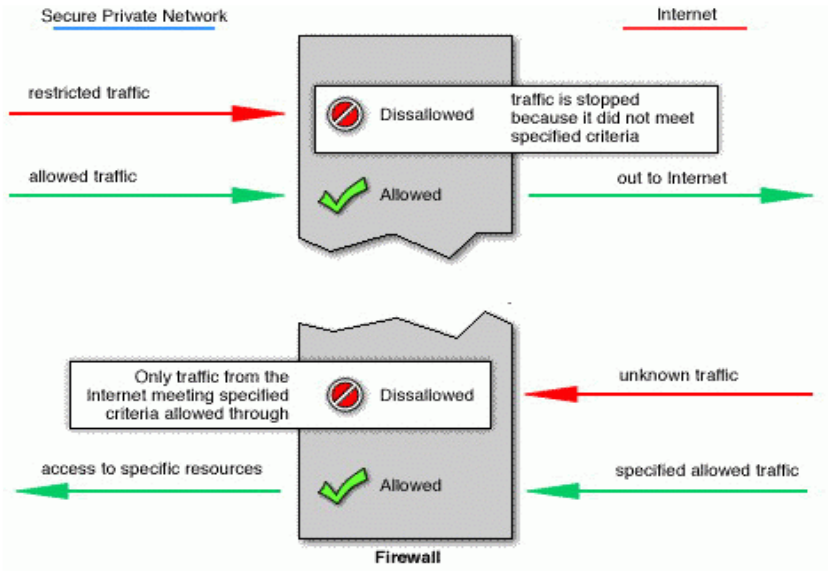

Figure 16

There are two methods of blocking traffic used by firewalls. Thus, a firewall allows any kind of traffic as long as a certain condition is not met or blocks traffic as long as a condition is not met. Firewalls can deal with the type of traffic or the addresses and ports of the source or destination. They can use a set of rules to analyze application data to determine if traffic is allowed. How a firewall determines what traffic is allowed depends on the network layer on which it operates.

4.1 Ports and services

Although a particular software service may have a port assigned by definition, there is no restriction on the application not being able to listen to other ports. A common example is the Simple Mail Transfer Protocol (SMTP). This service has assigned port 25. The ISP may block this port to avoid using a mail server on its own computer. But nothing stops us from configuring a mail server on another port. The main reason why some services have ports assigned by default is that a client can more easily find a particular service on a remote host. Some examples: FTP servers listen to port 21; HTTP servers are on port 80; client applications such as File Transfer Protocol (FTP) use randomly assigned ports usually larger than 1023.

There are just over 65,000 ports divided into well-known ports (0–1023), registered ports (1024–49151) and dynamic ports (49152–65535). Although there are hundreds of ports with the right applications, in practice less than 100 are frequently used. In Table 1 we can see the most common ports and the protocol that uses it. We must mention that these ports are the first to be targeted by a burglar on the victim's computer.

A good safety practice is to lock these ports if they are not in use. It is recommended to use the least privilege practice. This principle consists in granting the minimum access, strictly necessary for the activity of a service. Periodic testing of active ports is recommended. Applications also have different degrees of security; For example, SSH is a relatively secure application while Telnet is insecure. Adding or restricting ports with NIS is done this way - see the following figure, select the Firewall tab; in the middle of the window we can see the list of restricted ports. Also here we have the possibility to add or remove ports according to their need.

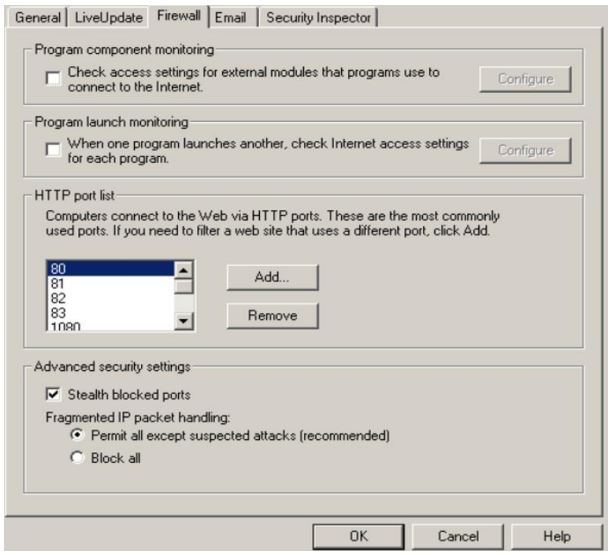

Figure 17

Table 1 Common ports and protocols

Port	Serviciu	Protocol
21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67/68	DHCP	UDP
69	TFTP	UDP
79	Finger	TCP
80	HTTP	TCP
88	Kerberos	UDP
110	POP3	TCP
111	SUNRPC	TCP/UDP
135	MS RPC	TCP/UDP
139	NB Session	TCP/UDP
161	SNMP	UDP
162	SNMP Trap	UDP
389	LDAP	TCP
443	SSL	TCP
445	SMB over IP	TCP/UDP
1433	MS-SQL	TCP

A good safety practice is to lock these ports if they are not in use. It is recommended to use the least privilege practice. This principle consists in granting the minimum access, strictly necessary for the activity of a service. Periodic testing of active ports is recommended.

Applications also have different degrees of security; For example, SSH is a relatively secure application while Telnet is insecure.

Adding or restricting ports with NIS is done as follows: select the Firewall tab; in the middle of the window we can see the list of restricted ports. Also here we have the possibility to add or remove ports according to their need.

4.2 Automatic updates protect your PC

After installation, the updates corresponding to the operating system must be loaded. Because these Updates have reached an appreciable size in the meantime, many users give up regular downloading, which results in numerous security breaches, through which viruses multiply explosively.

In Windows 10, Microsoft switched to system administration using the Automatic Updates feature. This feature keeps your computer security high because vulnerabilities found by hackers are closed by automatically installing new updates. By calling the function of automatic updates via *Start-Settings-Control Panel-System-Automatic Up-dates*, various options are available, which will allow you to choose how to proceed with the updates. Recommended is the Automatic mode, where the time and interval of downloads and installation are set through the corresponding menu. In addition, it is possible to choose the option *Notify Me But Don't Automatically Download or Install Them*, which informs about the availability of new updates and asks the user if he wants to download them immediately or later. Thus, a series of performance fluctuations of the internet connection can be avoided and any necessary restarts will be performed only after the completion of important works.

- **Ensuring optimal antivirus protection**

By using an antivirus program such as the Nod32 application described in the previous chapters

4.3 Security measures for the WiFI connection between the "Robotino" Mobile Robot and the industrial cyberspace

Unlike wired networks, wireless networks are more vulnerable to unauthorized interception. At the physical level, security is difficult to ensure because at this level a wireless network is very easy to access. To achieve an acceptable level of security in a wireless network, data must be encrypted and access control at higher levels of the network must be controlled. The security barriers (basic security) that were originally provided in the protocols of Wi-Fi networks, ensure a low level of security of these networks as in the figure below.

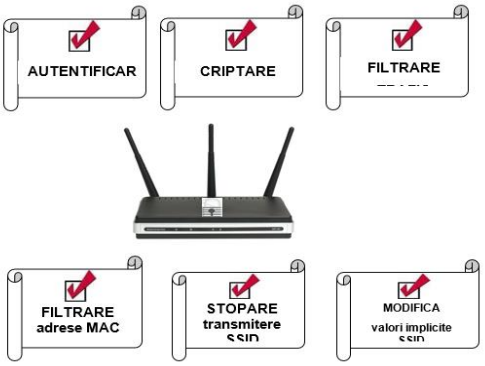

Figure 18

4.4 Basic WiFi security

It consists of controlling network access by using simple techniques, sufficient to remove some occasional intrusions. The simple techniques for controlling access to a wireless network are:

- Filtering *MAC (Media Access Control)* addresses. The MAC address is a 6-byte (48-bit) integer, which is the physical address (unique for each network access device) through which any network access device can be identified. By filtering MAC addresses, a network access point is configured with the MAC addresses of clients that are allowed to access the network. This technique is inefficient because an intruder can find out and falsify the MAC address of a station, and then connect to the network under the identity of that station.
- Stopping the public transmission of the SSID of an access point. SSID (Service Set Identifier) - is a code that defines membership in a specific wireless access point. All wireless devices that want to communicate on a network must have their own SSID, set to the same value as the SSID value of the access point to achieve connectivity. Normally an access point transmits its SSID every few seconds. Stopping the transmission of this signal hides the network presence from a surface attacker, but allows stations that know the SSID of the access point to connect to the network. Because the SSID is included in the beacon of any wireless sequence, any hacker with monitoring equipment can discover its value and connect to the network. The beacon is a small data packet transmitted continuously by an access point to ensure network management.
- Using the WEP (Wired Equivalent Privacy) algorithm. WEP enhances the continuous transmission of SSID by encrypting traffic between wireless clients and the access point.

5. Conclusions

Security in wireless networks is constantly evolving, as is the field in which they are needed. The longer an encryption algorithm is used, the more susceptible it becomes to attacks and the perpetual creation of new and high-performance algorithms. An important criterion in the development of a security technique is to ensure compatibility with existing equipment on the market, in order to ensure continuity in maintaining data confidentiality.

Even if an algorithm is efficient, but requires additional computing power than that already offered by the equipment on the market, a decisive factor in its adoption is the cost of replacement.

References

[1] Anghel Constantin, „Telementenance and Teleservice Oriented Design of Dependable Mechatronic System in Automotive Industry", Proceedings of the International Conference on Numerical Analysis and Applied Mathematics 2014 (ICNAAM-2014), AIP Conference Proceedings 1648, 620004 (2015); doi: http://dx.doi.org/10.1063/1.4912854

[2] Gheorghe, G., Bajeanru V., Ilie, I., Ingineria Mecatronică şi Cyber-MixMecatronică pentru Construcţia Intreprinderii Digitale şi Industriei Inteligente (4.0), Bucharest, CEFIN Pubishing House, (2019)

[3] Gheorghe, G., Concept and Mechatronics and Cyber-Mixmechatronics Constructions, Integrated in COBOT Type Technology Platform for Intelligent Industry (4.0), Proceedings of the International Conference of Mechatronics and Cyber-MixMechatronics, Springer Link, Publishing House (2019),

[4] Costa, D., Martins M., Martins,S., Teixeira, E., Bastos, A. Cunha, A.R., Varela, L. and Machado, J., Evaluation of Different Mechanisms of Production Activity Control in the Context of Industry 4.0, Proceedings of the International Conference of Mechatronics and Cyber-MixMechatronics, Springer Link Publishing House (2019),

[5] Gheorghe, Challenges and Research in the Innovation of Digital Enterprise and Smart Industry (4.0), Proceedings of 2019 International Conference on Hydraulics and Pneumatics – HERVEX, November 13-15, Baile Govora, Romania, ISSN 1454 – 8003 (2019).