SINGLE CARD COMPUTERS FROM THE-POINT OF VIEW OF THE SECURITY OFTHE DIGITAL SOLDIER

AZ EGYKÁRTYÁS SZÁMÍTÓGÉPEK A DIGITÁLIS KATONA BIZTONSÁGA SZEMPONTJÁBÓL

KISS Csaba[1]

Abstract

The XXI. In the 20th century, the use of artificial intelligence accelerated, including in the field of machine vision. Machine vision occupies an important place in the system of our digital life, since we acquire most of our information through vision. Writing the software necessary for the operation of machine vision is facilitated by the multitude of open source programs and single-board computers available to everyone on the Internet. With the help of these, it may be possible to develop tools that have not yet been regularized in military use. Devices created with single-card computers can even serve to increase the security of the digital soldier. The publication deals with the presentation of single-card computers and the conditions for their use from the point of view of the digital soldier performing military operations on the battlefield.

Keywords

digital soldier, single-board computer, artificial intelligence, IT security

Absztrakt

A XXI. században felgyorsult a mesterséges intelligencia felhasználása, többek között a gépi látás területén is. A gépi látás egy fontos helyet foglal el a digitális életünk rendszerében, hiszen látás útján szerezzük be az információnk nagyobb részét. A gépi látás működéséhez szükséges szoftverek megírását könnyíti az interneten mindenki részéről elérhető nyílt forráskódú programok és egykártyás számítógépek sokasága. Ezek segítségével, olyan eszközök kifejlesztésére nyílhat lehetőség, amik a katonai felhasználásban még nincsenek rendszeresítve. Az egykártyás számítógépekkel kialakított eszközök akár szolgálhatnak a digitális katona biztonságának a növelésének érdekében. A publikáció foglalkozik az egykártyás számítógépek bemutatásával, valamint azok informatikai biztonság szempontból történő elemzésével.

Kulcsszavak

digitális katona, egykártyás számítógépek, mesterséges intelligencia, IT biztonság

[1] kiss.csaba@uni-nke.hu | orcid:0000-0002-7265-8704 | PhD student, PhD hallgató |Doctoral School of Military Engineering on National University of Public Service, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola

INTRODUCTION

Accelerated military operations and increasingly powerful technologies and systems are bringing unprecedented changes to the field of military warfare today. Automated command and control technologies will appear on the battlefield as digital workstations for automated targeting systems.

Protecting the lives of soldiers on such an automated battlefield is a particularly big challenge for those involved in military technology research and development. The 'digital soldier program' can be a solution for increasing the soldiers' sense of security and for the shorter and more accurate execution of military operations. Practically, the soldier is provided with all the information he needs to fight the battle with the help of digital technologies, i.e. they provide a connection with a wifi or bluetooth application to a server computer, which can be installed even on a Lynx combat vehicle. The movements and positions of the soldiers are displayed on a screen, which is usually placed on the arm.

All elements of the individual device system of modern foot soldiers are electronic, and therefore require a source of energy. The duration of planned military tasks - when the soldier cannot charge the batteries - is a maximum of 24 hours.[1] There can be significant differences in the electrical implementation of the power supply systems, which manifests itself in the fact that custom-designed or standard batteries are used, adapted to the energy intake. This means that power supplies of different capacities and voltages are possible in digital military systems developed in different countries, so the load capacity of the batteries can also be different. As a result of the rapid technological development in this field of science, energy storage devices have a longer lifespan, an ever-increasing capacity, can be charged more easily and quickly, and are increasingly smaller in size. This is important when connecting devices made with single-board computers to the power distribution system made on the digital soldier.

Commercially available single-board computers, which are complete computers based on a single circuit board, such as Raspberry Pi, NanoPi, Banana Pi, Orange Pi, usually have power supply requirements ranging from 5V, 200mA to up to 2A, depending on the configuration.

These single-card computers can be easily programmed, even in the field of machine vision, so they can become a tool supporting the digital soldier and their power supply can even be based on the digital soldier's system. By using machine vision, we can not only correct human errors (due to fatigue or inattention, for example), but it is also possible to use it for social purposes, which can be proven in other areas.[2] [3]

In civil society, devices built with single-board computers can perform just as well in the military operational area as in the civilian area. According to the task to be performed, the same thing is done, for example: obstacle avoidance, but in terms of the result of the task, we get something different. In the civilian area, a robot may deliver medicine to an elderly person, while in the military area, the same robot brings ammunition to the trenches to the soldier from the distribution point. Obstacle avoidance (trees, ditches, etc.) can be performed by the same algorithm, therefore we can say that the various algorithms created by civil society can be suitable for increasing the defense system of the digital soldier, which can increase its combatability and chances of survival.

From the point of view of the program, it does not matter whether the algorithm is run in a civilian or military field, and from the point of view of the result, the person is the

determining factor. Such an interpretation and application of single-board computers allows the addition of military systems. The following chapter presents single-board computers.

SINGLE-BOARD COMPUTERS

One-board computers are one-board because they consist of a single printed circuit board and the circuit elements implanted on it. By connecting a keyboard, mouse and screen, we can get a complex computer workstation. Translated into English, its name in scientific literature is single-board computer, its abbreviation is SBC.

Single-board computers are popular due to their low cost and versatility, so they quickly became popular for home hobby applications, e.g. for home automation, building camera surveillance systems, controlling robots, as well as cloud services, own web server, website operation and so on. One-card computers can easily be used to learn programming languages, which is also used by schools, and its versatility is also reflected in the peripherals that can be connected to it.

The following single-board computers can be purchased commercially: Raspberry Pi, Rock Pi, Radxa Zero, Odyssey, VisionFive, Nezha, Odroid, LattePanda, Tinker Board, NVIDIA Jetson Nano, Atomic Pi, Khadas, NanoPi, Edge-V, Quartz, ROCKPro64, UDOO x86 Advanced Plus, Banana Pi, LeMaker, Orange Pi, HiKey 960. Picture 1 shows the Raspberry Pi 4B.

Picture 1.: Raspberry Pi 4B single-board computer, Christopher Barnatt: Explaining Computers.com, 2023

Picture 1 clearly shows the connection points USB, power supply and network connection interface, this is generally true for all single-board computers. Compared to the USB connector, its size is predictable: 85 mm long and 56 mm wide. They usually have a (2-8) core processor, 10/100 Mbit/s Ethernet port, WiFi, Bluetooth, RAM from 128 MB up to 8 GB, Video controllers and other additional panels (camera) depending on the type depending. Their nominal power is also possible from 200 mA (1 W) to 1.4 A (7 W). Power supply via MicroUSB or GPIO connector is DC 1.8–5.1 V. DC 3.3V and DC 1.8V are possible at the output. Their operating system usually depends on the type: Linux, Android, Ubuntu, Debian, OpenHarmony, Orange Pi OS and other operating systems. They can also have a headphone connection option and a connection option suitable for receiving audio input and output data.

Since single-card computers are suitable for the design of devices based on machine vision due to their small size, light weight and simple programmability, they can function as a complement to the digital soldier's system. Their power supply is either built on top of the digital soldier's system or has its own separate power supply, which can be a battery or a solar panel.

DIGITAL SOLDIER

Artificial intelligence has appeared in all areas of life, safety and security sciences [4] and military applications [5] are no exception.

In line with international processes, an artificial intelligence (AI) development program was launched in Hungary, during which the Artificial Intelligence Coalition (MIK) was established under the leadership of the Ministry of Innovation and Technology (ITM), whose primary goal is to improve domestic AI technologies on the international scene. their incorporation into everyday life and state activities.[6] In 2020, the Hungarian government issued Decree No. 1573/2020 to support the process. (IX. 9.) Government decision, which deals with Hungary's Artificial Intelligence Strategy and certain measures necessary for its implementation.[7]

The Hungarian Armed Forces is also not left out of the developments, since nowadays no one questions the importance of digital warfare, nor that its importance is constantly growing compared to other forms of warfare. In 2021, the National Military Strategy of Hungary (hereafter: NKS) was published, where artificial intelligence and the digital soldier program are among the development areas concerned. [8]

The development areas formulated by the NKS respond to the military challenges of the time. The most important value is human life, and the man of the age is trying to transfer this view to the military world using science. Picture 2 shows one of the construction possibilities of the digital soldier.

Picture 2.: Digital soldier, https://matasz.com/hun/a-digitalis-katona-program-a-magyar-honvedseg-teljes-gondolkodasmodjat-meg-fogja-valtoztatni/

The signal from the sensors (camera) worn on the soldier is connected to a transmitter device, the transmission of which is received by a centrally located receiver. dr. According to Lt. Gen. Gábor Böröndi: 'In the era of digital communication, it is necessary to be able to provide soldiers with all the information they need to fight.'[9] The data received by the driver through the reconnaissance system is processed and then sent to the tablet placed on the combat soldier's arm. This is how the soldiers see their own position, the position of the enemy and the military maneuver they have to carry out. By connecting them in a network, it can operate at several military levels, even at the battalion or brigade level.

It is easy to see that the soldier, with the technical devices on him, has become one of the outsourced data users and data collectors of the management's central computer. Technical devices do not work without a power supply. In the next chapter, I will examine the system created with single-board computers from the point of view of IT security.

IT SECURITY

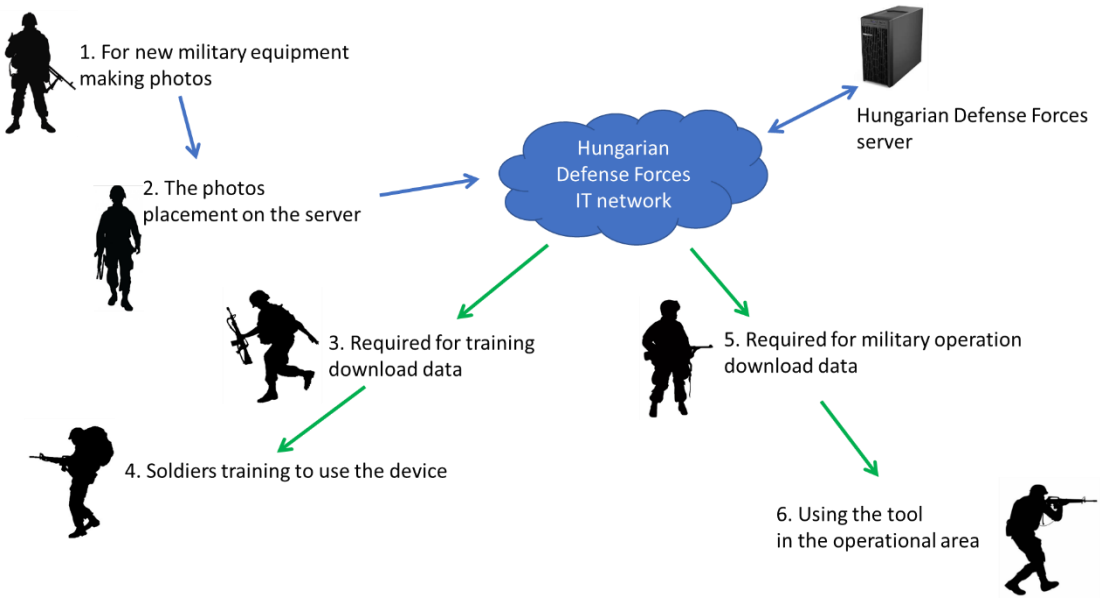
Since it is an IT device, of course a program runs on this device and the data is stored in a file system. As with all IT devices, the question may arise as to what and how the program and files running on the device ensure safe operation, i.e. how the IT protection of the program running on the device can be realized.

Soldiers could become familiar with such an IT tool during training. Military training is part of military life, which consists of theoretical and practical training, weaving through the entire military career. The training affects all types of weapons, so for each type of weapon we can examine the possibility of using a device equipped with machine vision created with a single-card computer. In general, it can help you recognize rank, military equipment, weapons, NATO symbols and other map symbols, ammunition, mines, rockets, bombs, grenades, fixed-wing and rotary-wing equipment and other special military tools. Soldiers would take the device with them and could also use it to monitor drones in the trenches, so they could also scan the sky with the help of the camera.

According to some security experts: 'IT security is a state of the protection system that is satisfactory for the defender, which is closed, comprehensive, continuous and proportionate to the risks in terms of the confidentiality, integrity and availability of the data managed in the IT system.'[10] The critical points are those activities that can be determined in the process of using single-board computers, where IT security may be compromised for various reasons.

With the spread of the use of single-card computers, the role and importance of IT security among users of single-card computers is even more appreciated. Single-card computers bring many advantages and benefits to the user, so its protection has also become critical, therefore there is an increasing need for users who are able to guarantee the safe IT use of devices equipped with a single-card computer.

Picture 3 shows the critical points arising from one of the possible conditions of use of the single-board computer from the point of view of IT security.



Picture 3.: Critical points from the point of view of IT security, own editing

In the 3rd picture, the MH IT network and the MH server can be clearly seen as the central element of the operating process of the device equipped with a single-card computer. Since the MH Informatikai network and MH server are already regulated in terms of IT security, the publication does not cover these elements. The second most important thing, which can be clearly seen in the 3rd picture, is the central role of the soldier, that is, the person who operates the process and uses the device. In the 3rd picture, you can see that there are 1 upload and 2 download directions.

I have identified a total of 6 critical points based on the 3rd image, where it is necessary to analyze IT security, these are the following:

1. The training photographs to be taken of the new military equipment. Photo files are created here, which can be files of different sizes. Up to 100 training photos can be taken from one device.
2. The files completed in point 1 are uploaded to the database located on the server, this is possible by copying the images to a folder system after logging in to a storage location.
3. Download the training photos required for military training. This is possible as described in point 2, when we log in to the storage on the server and copy the images to our device.
4. During the training, we put the device in the hands of the soldier to be trained.
5. The soldier participating in the military operation can initiate the download of the data according to the operation after logging into the database located on the server. You can copy the data to the device you want to use.
6. Use of the device loaded with training images in the military operational area.

The classification into the security class must be carried out on the basis of a risk analysis, which is defined in Art. 41/2015. (VII. 15.) BM Decree (BMr.) describes the requirements for technological security and secure information devices and products, as well as classification into security class and level.[11]

Table 1. shows the threats of the identified critical points in terms of IT security.

Critical point	Activity	Threats
1	Training photographs to be taken of the new military equipment. Photo files are created here, which can be files of different sizes. Up to 100 training photos can be taken from one device.	– industrial espionage – negligence, irresponsibility
2	The 1. the files completed in point are uploaded to the database located on the server, this is possible by copying the images to a folder system after logging in to a storage location.	– cyberterrorism – hackers, crackers
3	Download training photos required for military training. This is possible as described in point 2, when we log in to the storage on the server and copy the images to our device.	– industrial espionage – computer crimes – cyberterrorism – hackers, crackers
4	During the training, we put the device in the hands of the soldier to be trained.	– negligence, irresponsibility
5	The soldier participating in the military operation can initiate the download of the data according to the operation after logging into the database located on the server. You can copy the data to the device you want to use.	– information warfare
6	Use of the device loaded with training images in the military operational area.	– negligence, irresponsibility

Table 1. The critical points and possible threats, own editing

According to Act L. of 2013 (Ibtv.), electronic information systems must be classified into a security class in terms of confidentiality, integrity and availability. The law stipulates that the classification into the security class is approved by the head of the organization and is responsible for its compliance with legislation and risks, as well as the completeness and timeliness of the data used. The security classification must be recorded in the organization's IT security policy.[12]

According to Act L. of 2013 (Ibtv.), there are three data security requirements:

- confidentiality: only a limited number of authorized persons can know.
- integrity: that which corresponds to the original state.
- availability: access to the necessary data according to their processing where and when needed.

According to these principles, the group of authorized persons consists of trainers and IT staff, as well as an access restriction that limits the accessible files.

Since the use of the device can also take place within the IT system of a closed MH, from the point of view of IT security, the role of the soldier, i.e. the person, as a threat and risk factor increases.

Both international and domestic data show that data loss and data compromise can most often be traced back to human factors - in many cases, the incident can be prevented by paying attention to the staff and following the rules.[13] In this case, the device can be used by all soldiers, so education is what can strengthen the use of the rules of conscious IT security among soldiers.

SUMMARY

Every army strives to protect its soldiers from enemy attacks as best as possible. The probability of personal injuries and losses can be reduced with various measures and new protection techniques and tactics, but it cannot be 100% excluded. This is probably the most convincing argument regarding the need to develop a digital soldier, which can be supported even by using a single-card computer, which has already been well-proven in the civilian field.

The NATO Army Armament Group (NAAG) established Thematic Group 1 (TG/1) to coordinate the interoperability of military systems and to prevent identical developments between different military systems. This also applies to digital military systems.

Field design is important for such devices, which is not included in this publication. Due to the field design, the elements that ensure the power distribution of the digital soldier have a robust design. In practice, these connectors are elements made for special field design, so commercially available systems cannot connect to them. Due to the diversity of the power supply, which can be observed in the digital soldier, it is easiest if the single-board computers have their own power supply.

Technical progress results in a reduction in size and an increase in capabilities for all electronic devices, including single-card computers. Therefore, solutions developed at home on commercially available single-board computers and already proven in civilian life, which can be used to support the soldier on the battlefield, become applicable if IT security is observed.

The core of the device created with a single-board computer is loaded by a computer, so the IT security requirements for it are the same as the security requirements of an IT device. When using such a tool, the person is a critical point, whose training in IT security rules is a key element in achieving IT security.

The use of single-card computers is no more difficult than the usual military computers that soldiers use at work. Adherence to IT security begins with training, which the

units repeat annually at the workplace, and the soldier ensures the acceptance of the submitted material by signing it.

The best remedy for the prevention of industrial espionage and computer crimes is strengthening patriotism and the patriotism that people carry in their hearts. Patriotic education is nothing but education to protect the homeland, which can ensure that the soldier does not cause harm to his own country, i.e. protects its values. You are not only obliged to protect, but also to report if you detect an act indicating this, the same is true in the field of IT security.

REFERENCES

[1] Gácsér Z., 2008. "The possibilities of developing a modern, network-integrated individual equipment system that increases the soldier's combat ability in the Hungarian Armed Forces.", Budapest, Nemzeti Közszolgálati Egyetem.

[2] Kollár Cs. and Nagy B. "A mesterséges intelligencia felhasználási lehetőségei az objektumfelismerésben (első rész)," BIZTONSÁGTUDOMÁNYI SZEMLE, vol. 3, no. 1, pp. 123–140, 2021.

[3] Kollár Cs. and Nagy B. "A mesterséges intelligencia felhasználási lehetőségei az objektumfelismerésben (második rész)," BIZTONSÁGTUDOMÁNYI SZEMLE, vol. 3, no. 2, pp. 115–129, 2021.

[4] Kollár Cs, "A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában," in Kiberbiztonság – Cybersecurity 2., vol. 2, 2019, pp. 47–61.

[5] Kollár Cs, "A mesterséges intelligencia jelene és jövője a katonai és a polgári képzés fókuszában," in Generációspecifikus oktatásmódszertan alkalmazása a polgári és katonai oktatásban, Budapest: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft. (2023) pp. 31-44.

[7] Porkoláb I. - Négyesi I, 2019. " Researching the application possibilities of artificial intelligence in the military." Honvédségi Szemle, 2019/5. Online: https://honvedelem.hu/images/media/5f2bd1646eeb8298912683.pdf

[7] 1393/2021. (IV.24.) "Government decision on the National Military Strategy of Hungary." Magyar Közlöny 2021 (119)

[8] 1573/2020. (IX. 9.) "Government decision on Hungary's Artificial Intelligence Strategy and on certain measures necessary for its implementation" Magyar Közlöny 2020 (202)

[9] Szűcs L, 2021. " The digital soldier program - Conversation with dr. with Lieutenant General Gábor Böröndi." Online: https://matasz.com/hun/a-digitalis-katona-program-a-magyar-honvedseg-teljes-gondolkodasmodjat-meg-fogja-valtoztatni/

[10] Déri Z. at. All, 2004. "The system of requirements for the management of IT security - draft recommendation of the Information Society Coordination Interdepartmental Committee", Budapest

[11] 41/2015. (VII. 15.) "BM decree on technological security and the requirements for secure information devices and products, as well as classification into security class and security level, as defined in Act L. of 2013 on the electronic information security of state and local government bodies." Online: https://net.jogtar.hu/jogszabaly?docid=a1500041.bm

[12] Muha L.-Krasznay Cs., 2014. “Managing the security of electronic information systems.” Nemzeti Közszolgálati Egyetem, Budapest
[13] Kollár Cs, “A média mérőszámai és a digitális kommunikáció biztonságának mutatószámai,” BIZTONSÁGTUDOMÁNYI SZEMLE, vol. 1, no. 1–2, pp. 31–44, 2019.