Reconstruction and development of a wireless network in the machining hall of an industrial company

Tamás Márk Baross[1] and Attila Rónai[2]

[1] Óbuda University, Kando Kalman Faculty of Electrical Engineering, Bécsi út 96/b, H-1034 Budapest, Hungary; baross.mark@kvk.uni-obuda.hu

[2] Óbuda University, Kando Kalman Faculty of Electrical Engineering, Bécsi út 96/b, H-1034 Budapest, Hungary; raszoft@gmail.com

Abstract: When replacing and scaling the wireless network (Wi-Fi) of an industrial auto parts manufacturer, it is important to consider the demands of the present and future network infrastructure. This is due to the rapid development of information technology (IT/IOT) and INDUSTRY 4.0-5.0, as well as developments in manufacturing execution MES systems and, last but not least, the requirements of cybersecurity audits. During the survey, we assessed the status and suitability of the existing system and designed and modeled the new system in accordance with the expected requirements. During the design phase, we took into account the specific conditions and environmental characteristics of the industrial company's hall. We strived to design and install energy-efficient, modern, high-quality, reliable, and high-performance devices in terms of radio data transmission. The management of the corporate group exclusively supports CISCO product range systems, and we can only integrate this manufacturer's devices in our development. This decision significantly narrows down the options, but at the same time makes it easier to select the right devices, as we only need to look for the devices required for development in a group corresponding to one manufacturer's specialization. The physical layout of APs (access points) is essential for ensuring the performance and reliability of wireless networks. We use modern software to document and model the possible and optimal layout in order to provide adequate coverage in the hall. We place a high priority on cybersecurity and aim to minimize potential threats. To this end, we implement modern security protocols to ensure the integrity and confidentiality of company data.

Keywords: Wi-Fi, Industry 4.0, Industry 5.0, Industrial. Cisco

1. Introduction of possible solutions

When replacing and scaling the wireless network (Wi-Fi) of an industrial auto parts manufacturer, it is important to consider current and future network

infrastructure requirements, given the rapid development of information technology (IT/IOT) and the rapid development of INDUSTRY 4.0-5.0 maturity levels, developments in manufacturing and execution MES manufacturing systems, and the requirements of cybersecurity audits. An important consideration in the design process is the specific conditions and environmental characteristics of the industrial company's shop floor. Furthermore, we must strive to design and install energy-efficient, modern, high-quality, reliable, and high-performance devices in terms of radio data transmission. Ultimately, inadequate network infrastructure can directly reduce a company's effectiveness and profitability. "It is important to ensure that the data stored in the central system is protected to the maximum extent possible with the available tools, or to find a solution that does not compromise data integrity and prevent data leaks, breaches, or loss. Furthermore, we must recognize that a corporate support network and the infrastructure that serves it are exposed to significant cybersecurity threats from systems that may originate from the manufacturing network layers." [1] In the following, we would like to present the replacement of an industrial company's existing obsolete wireless network, which is no longer supported by the manufacturer, from planning to implementation. In this article, we aim to outline how we can resolve the existing issues and how we can reconstruct them using current technological tools. According to preliminary plans, we will assess the industrial company's existing and future wireless network requirements, the infrastructure of related devices and resources, the availability of the expected quality, and, with regard to the objectives, we will also examine the industrial devices of manufacturers/suppliers that can be integrated into the system and operated in the long term. The managers of the company’s group only support systems from the Cisco product range, so we can only integrate devices from this manufacturer during development. This decision significantly narrows down the options, but at the same time makes it easier to select the desired devices, because we only need to look for the devices required for development in a group that corresponds to one manufacturer's specialization.

2. Wi-Fi network assessment

Our topic specifically focuses on the development of wireless networks in manufacturing areas, which are relatively more specialized due to their complexity and, considering environmental conditions, more complex than the implementation, design and development of a system intended for office use. The total area of the hall is nearly 10,000 square meters. Previously, the wireless network was set up with a total of 26 Cisco AIR-3702e APs. To assess the Wi-Fi network, we use the high-level design (HLD), low-level design (LLD), and site survey documentation prepared for the existing network as a starting point.

Furthermore, due to information security regulations and frequent audits, the customer (company) prepares documentation resulting from system development, as well as analyses and risk assessments necessary for change management. This documentation is not part of this article, as it only covers Wi-Fi development and design, and the documentation of corporate processes is only tangentially related to our topic. As the company has several information security and automotive certificates, only protocols that are identical to or more secure than those of the existing system are acceptable, and they must also comply with Act LXIX of 2024 on cybersecurity legislation applicable in Europe and Hungary. These are based on the NIS2 Directive, which regulates cybersecurity for EU companies, stipulating that information systems must be transparent and that an appropriate information security environment must be established. With regard to radio systems, Decree 7/2024. (VI. 24.) MK defines the requirements and security classes for wireless networks [2]. In accordance with TISAX audits, the extended requirements for network management and control must be examined in accordance with information security regulations. It remains our goal that, in accordance with audit requirements, all available wireless networks should only be connected with device certificates provided by the Enterprise CA and RADIUS server-based authentication processes.

Corporate Requirements:

We would like to highlight some of the company's key expectations and requirements for wireless networks. Design and implementation may only be carried out using Cisco wireless devices and systems. A precise layout plan must be created for indoor endpoints, supported by software-based predictive analysis as well as instrumental testing. The service level such as transmission capacity and security must not fall below the current standard. The device providing the service must be suitable for industrial environments, capable of withstanding temperatures up to 50ºC, featuring at least IP67 protection, and built with industrial-grade design. Industrial-grade, low-power, small-area wireless access points may be used, and the equivalent isotropic radiated power (EIRP) of access points and antennas must not exceed Class E2 (2 watts). The solution can be connected to the IT infrastructure using existing 1 Gbps Ethernet CAT6a copper cabling, and Power over Ethernet (PoE+) or a higher-power PoE adapter may be used if the device requires increased power. The system must support 2.4/5/6 GHz Wi-Fi networks and enable the adoption of emerging technologies. During the allocation of 5 GHz frequency channels, 40 MHz channel width should be targeted in the design phase. Centralized control and configuration capabilities are required, along with WPA3 and EAP-TLS support integrated into the existing security ecosystem (e.g., Cisco ISE 3.4). From an energy-efficiency perspective, the system must be designed so that replacing the 26 access points does not exceed current energy consumption, and if possible, the number of APs should even be reduced. The manufacturer’s support period and the life cycle of the necessary devices must also be taken into account.

WLC virtualization:

Cisco C9800-CL-K9 virtual controllers (WLCs) will manage the wireless access points. Redundant operation will be implemented by two WLCs in an HA SSO (high availability stateful switchover) configuration, running on separate ESXi hypervisor hosts. The virtual controllers can be deployed in both private and public cloud environments. Multiple hypervisors are supported, and the controller itself is scalable. Only one of the controllers is active at any given time, with the other acting as a hot standby. In the event of an active failure, the secondary controller takes over the active role in such a way that users do not experience any disruption. The two wireless controllers will run within the site; off-site controllers are not involved in management. In this configuration, CAPWAP (Control and Provisioning of Wireless Access Points) channels between wireless access points and the controller are established via the local network. CAPWAP (IETF RFC 5415) between controllers and APs is a standard, interoperable protocol that allows the access controller to manage a collection of wireless endpoints [3]. The protocol channel offers the option of encrypting both data traffic and management traffic. CAPWAP is the basis of Cisco's wireless network solution, LWAPP (Lightweight Access Point Protocol - Cisco's proprietary protocol for centralized control of access points) and DTLS (Datagram Transport Layer Security - a protocol based on TLS that is capable of securing datagram transmission) and UDP. Requirements for using CAPWAP at OSI layer 3 (transport):

- IP addressing
- The CAPWAP protocol must be allowed between the WLC and AP: UDP 5246 (Control) and UDP 5247 (Data) destination ports

User traffic data is embedded in CAPWAP data frames, enabling it to be transmitted between APs and WLCs.
According to the IETF, CAPWAP supports two modes of operation:

- Shared media access control (MAC)
- Local MAC

The most important feature of CAPWAP is its split MAC architecture, where part of the 802.11 protocol family is managed by the CAPWAP AP (typically time-sensitive functions), while the rest is managed by the WLC.

WLC Redundancy and deployed EOL system configurations:

The two virtual WLCs run on the On-Premis side, and the controller outside the company's premises is not involved in management. In this design, the CAPWAP channels between the wireless access points and the controller are built over the local network. Network access for the controllers is provided by the ESXi hypervisor network layer through distribution switches.WLC controllers operate in an HA SSO redundancy model. In this configuration, one member always plays an active role, while the other waits in a standby-hot state. The controllers are dependent on each other, their configurations and databases are synchronized, and

they share a common IP address. Due to the active/standby configuration, AP and client load balancing between the two controllers is not applicable. In the event of a role change, the secondary member becomes active and the APs automatically connect to this member without restarting. There are several conditions for properly configured SSO redundancy, but the most important of all is that both members can see each other on the redundancy interface (Gi 3 / vNIC 3) via an L2 connection. To install WLC controllers, we use the OVA format installer available for download from the manufacturer's website. We will not detail the entire installation process, as most settings contain basic information. The company aims to use low-power, low-consumption indoor units with a maximum transmit power of 30 dBm, i.e. ~1W, for the desired frequencies. The expected frequency band is 2.4-5Ghz, but the new system must also provide the option of using the 6 GHz frequency band in the future. The wireless performance of the network is greatly influenced by the type of 802.11-based WLAN topology mode we provide. The system operated the centralized system in infrastructure topology mode. The company previously installed Cisco Aironet 3702e indoor APs with 802.11a/g/n/ac dual-band 2.4-5 GHz internal antennas [4], for which official manufacturer support ended on April 30, 2024. These devices were primarily designed for office use, given that their casing and other components are not fully compatible with industrial environmental conditions. In recent years, we have taken temperature measurements in the hall on several occasions and found that on a day with a temperature of 38-40º Celsius, temperatures of up to 50º Celsius were recorded at a height of nearly 5-6 meters. This temperature had such an effect on the APs that their operation became unstable, and in many cases they lose connection with central service. In some cases, 9-10 of the 26 APs were no longer providing Wi-Fi coverage and were unable to load their embedded system when restarted. Due to the problems outlined above, the company was forced to rebuild its wireless network.

3. Preparing and designing a new system

During the planning of each AP location, a predictive simulation survey (Pre-deploy Apos) and documentation were prepared in advance. During the planning phase, coverage and heat maps were created using the Ekahau [5] system and instrumentation for the frequency bands required at the time. The company provided the necessary hall map and area for the survey. In the Wireless Controller (WLC), i.e., the controller that monitors our Wi-Fi system, DSSS modulation technology was disabled at 802.11b 2.4 GHz, thus avoiding unnecessary and different modulation problems, low speeds, and additional loads on the Wi-Fi network. Furthermore, with 802.11k enabled, clients receive information from nearby APs, allowing them to make quick and optimal decisions regarding roaming.WPA and WPA2 (Wi-Fi® Protected Access) data encryption

protocols have been implemented for wireless local area networks (SSIDs) announced at the company's premises. Taking security requirements into account, Wi-Fi communication for all company devices is authenticated using certificate-based, encrypted communication in accordance with the EAP-TLS 802.1x IETF RFC 5216 standard. This was accompanied by Cisco ISE 3.1 [6], Radius-based AAA (Authentication, Authorization, Accounting) back-end authentication server, which ensures mutual EAP-TLS certificate-based authentication of clients to the network and the establishment of an encrypted communication channel. The system or device initiating EAP-TLS authentication must be capable of supporting the TLS v1.2 and TLS v1.3 encryption protocols specified in the IETF RFC 8446 [7] standard. The EAP-TLS access protocol is one of the most secure authentication methods, as it is resistant to man-in-the-middle attacks and other forms of network intrusion. At the 2024 Cisco Techtorial conference in Budapest, following the presentations and professional discussions held there, we briefly outlined our experiences and problems to the experts presenting at the event. The manufacturer's representatives suggested that we try out a new, heavy-duty device that is suitable for stable operation in an industrial environment and to which high-gain and directional antennas can be connected. They promised to send us a test device for a few weeks so that we could learn and experience the possibilities offered by the new AP, as well as perform measurements according to environmental conditions. Types of test equipment provided by Cisco:

- 1 Cisco IW9167E Heavy Duty Access Point [8]
- 2 Cisco AIR-ANT2513P4M-N dual-band polarization directional antennas

The testing project was implemented after the necessary internal approvals were obtained, and we installed the testing equipment on a temporary basis in a location and substructure that we considered ideal, thereby minimizing the downtime of the productive system. The physical installation and mounting on the ceiling was carried out by the company's internal maintenance department's building operations team, as only our employees with the appropriate permits and licenses were able to install the equipment at a height of nearly 5 meters using a self-propelled aerial work platform. Cisco provided the necessary installation materials and connection cables. We solved the Cat6a copper RJ-45 Ethernet network connection by suspending a nearby AP and temporarily rerouting its network cable. I determined the layout instructions for the physical installation of the antennas and the test AP, as well as the orientation of the antennas. I set the orientation of the antennas, i.e., the angle enclosed by the ceiling, at 15º. We did this so that the signal dispersion shown in the simulation would be comparable to the performance of the old AP, and so that the signal dispersions of the antennas would overlap only to a very small extent. We connected the four-port polarization antennas according to Cisco's official installation guide. We connected the AP's red connection ports to the left antenna and the blue ones to the right antenna. We solved the AP's power supply with a factory power supply for the Cisco IW9167, as we did not have a switch port providing 802.3bt/UPOE

voltage. We connected the RJ-45 Ethernet interface to the IT network via a factory block connector using a Cat6a flexible patch cable. The problem was that officially, AIR-3702e APs could only be operated on WLC version 17.4.x, and the new devices received for testing were only supported by WLC versions 17.9.4 and above [8]. As a result, we installed a stable version 17.9.6 for testing purposes in a separate data center test VLANs suitable for the purpose. The WLC installation was the same as the previous installation procedure, with the only difference being that the management IP address was different and no redundant installation was required for the test operation. The configurations, policies, WLAN SSIDs, RADIUS, and FLEX were identical to the settings in the production system without exception. We reprogrammed the switch port configuration and management VLANs connected to the test AP to the new WLC network segment, and after successfully downloading the new software version (in about 15 minutes), the test AP was available within a few minutes.

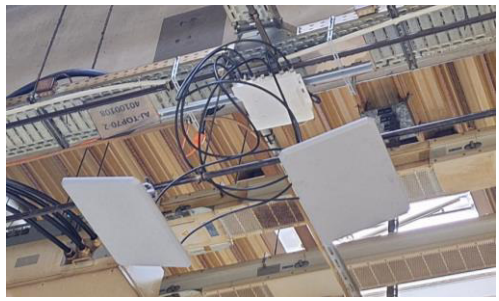

Figure 1. Test device equipped: Cisco IW9167E and two AIR-ANT2513P4M-N dual-band antennas

4. Planning phase

We performed our measurements using Ekahau (version: 10.4) software, provided by our company's network solutions partner, as we did not have a software license (this would have required a significant financial investment on the part of our company, so this was the only way to perform the measurements). The measurements were performed at 2.4 GHz - 5 GHz frequencies by physically walking through the existing map. On the WLC, we set the parameters for our first scan to 5 GHz 100.104 channels with a channel bandwidth of 40 MHz and the maximum available signal strength (which in this case was 27dBm). The following shows how the measurement heat map developed and how much coverage the tested AP provided at 5 GHz. One test AP was able to cover approximately 50% of the entire hall with a signal of sufficient quality at maximum signal strength. We also obtained good results among the manufacturer's equipment located in the hall. At the same time, the 2.4 GHz 20 MHz band was also measured, which also covered nearly 50% of the hall. The

maximum performance measurements showed very important and useful results for us, as well as the reference values of the test AP in a given case and how we can use these properties in line with our plans. We then scaled back the performance to nearly 50% because it provides a useful reference value for our placement concept. I did not change any other existing parameters in the 5 GHz settings, only the maximum transmit power of the AP. In summary, with the AP properly oriented, even at a lower power than the maximum, it is capable of covering one-third of the hall at an adequate level. The Cisco Catalyst IW9167E high-performance access point AP recommended by Cisco's representative met our requirements, taking into account the following parameters [8]: The Catalyst IW9167 series is specifically designed for heavy-duty industrial use, featuring a construction that is resistant to shock, vibration, and extreme temperatures. With support for industrial protocols, the device provides modern, secure, and highly available wireless connectivity, including compatibility with Wi-Fi 6 and the 6 GHz frequency band. Its dual Multigigabit Ethernet ports enable speeds of up to 5 Gbps, while the eight N-type antenna ports allow the connection of Cisco factory external antennas. The device operates effectively within a wide temperature range, from −40°C to +70°C, and can withstand +85°C for up to 16 hours. It is certified to IP66 and IP67 standards (EN/IEC 60529), ensuring protection against dust and water. Wireless performance is enhanced by 4×4 downlink MU-MIMO technology with four spatial streams on both 5 GHz radios, as well as maximum ratio combining (MRC) and 802.11ac beamforming. It supports 20, 40, 80, and 160 MHz channels, achieving a physical data rate of up to 3.4 Gbps (with dual 4×4:4SS at 80 MHz). Packet aggregation methods A-MPDU and A-MSDU for both transmit and receive ensure efficient data handling. The device complies with 802.11 DFS requirements, supports CSD functionality, and includes WPA3, the latest Wi-Fi security standard. The advantages of the Wi-Fi 6 standard include higher and more reliable data transfer speeds, more channels, energy efficiency, and, last but not least, more effective protection and data traffic encryption in terms of security. In addition, the AP supports MESH technology, where clients and active Wi-Fi systems can communicate with each other on a shared radio frequency network. The advantage is that network data traffic can be handled without loss in a given area, even with multiple APs and/or through APs. Using the company's existing infrastructure and the parameters of the device received for testing purposes, we used the Ekahau 10.4 Wi-Fi planning system to create a predictive heat map. It was important for us to create a physical topology that would cover the entire area of the hall and ensure fault-tolerant availability in case an AP was forced to shut down due to hardware failure. Last but not least, we had to take the company's budget into account, strive for the absolutely necessary coverage, and consider the power consumption of the APs to be installed. For reasons of economy, we should use the existing Cat6a copper-based Ethernet RJ-45 free endpoints, and if necessary, we can also use the network connections of the existing old APs. The question arose as to how suitable the POE+ switches on the existing Ethernet Access side would be for powering the new system. The

current RJ-45 network topology does not allow for the power supply of UPOE devices, so depending on the number of wireless network access points (APs), we need to purchase UPOE adapters or UPOE switches. We were able to replace the power supply by purchasing temporary UPOE (Power over Ethernet, 802.3bt, 60 watts) adapters, as the available switches are capable of providing POE+ (Power over Ethernet, 802.3at, 30 watts) power. In the following predictive plans, we focused on 5 GHz frequencies because this is expected in the long term and in terms of the current equipment pool. During the initial planning phase, a significant number of APs were planned, and macrocell coverage is not complete; there are also places where structures taller than 5 meters limit coverage signal levels. In our opinion, the plan below needs to be supplemented with two more APs, as coverage within the hall is uncertain and the bands between tall buildings are unusable. In the case of tall buildings, it is important that the handheld barcode readers used by employees working their function properly. Based on the above, we concluded that the hall should be divided into six cells, resulting in a total of seven coverage areas. We paid particular attention to the coverage to be established in the area of tall buildings and possible solutions. We considered the internal building within the hall as a separate (macro)cell. After the division, we concluded that the cells should be supplied from two directions, thus optimally reducing the number of APs and setting the coverage signal levels to approximately 60-70% of the transmitter power. We place the APs on the horizontal axis of the entire hall, and with antennas directed at approximately 40-45º, we can cover the cells with an adequate signal, creating a redundant pair for that area. The advantage is that each cell is served by two APs with one antenna each, and in the event of an AP failure, we can continue to ensure macrocell coverage manually or automatically. In our opinion, a total of nine APs fully cover the service area, thereby reducing energy consumption and increasing security and high availability. As planned, we put together a sample of the purchased devices with the company's building operations department. We took into account Cisco's recommendation that the two directional antennas should be at least 1.5 m apart horizontally and rotated at a minimum of 90º relative to each other [9]. We connected the coaxial cables of the antennas to the AP with appropriate bends and fasteners. We connected the antennas in the same order as we did with the test AP. The vertical tilt angle of the antennas was gradually changed between 15º and 85º, and I finalized it based on the reference data obtained during the measurement. The RJ-45 patch cable was connected through an airtight block connector so that the AP's internal electrical system would not be exposed to environmental stress.

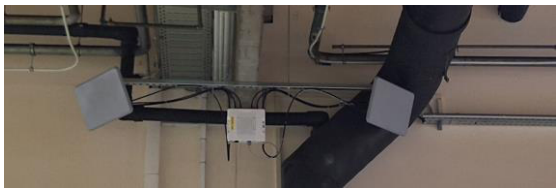

Figure 2. Installing and commissioning the first AP

The next AP setup was different in that the distribution and connection points of the opposing antennas were reversed, i.e., the opposite of the first one. This was good for us because it allowed us to apply different settings per antenna/slot when distributing Wi-Fi channels.

Figure 3. Installing and commissioning the second AP

I created a new radio frequency profile (RF profile) for the APs installed in the new hall for the 5 GHz frequency band, called Production_5 GHz. This was not necessary for the 2.4 GHz band, because I derived the previous settings and they will not change in the future. By default, the new AP is installed in outdoor mode, and we would like to keep it that way because the goal is for it to operate in the 5 GHz UNII-2C and UNII-2-Ext (Unlicensed National Information Infrastructure) bands between 100 and 144. For the APs installed in the new hall, we created a new radio frequency profile (RF profile) for the 5 GHz frequency band called Production_5 GHz. This was not necessary for the 2.4 GHz band because we derived the previous settings, and these will not change in the future. By default, the new AP is installed in outdoor mode, and we would like to keep it that way because the goal is for it to operate in the 5 GHz UNII-2C and UNII-2-Ext (Unlicensed National Information Infrastructure) bands between 100 and 144. We couldn't do the setup because the WLC rejected it with an error message and automatically changed the APs' Slot2 40 MHz channels to 20 MHz.

AP neve	Slot1	Slot2
1. AP	100-104	108-112
2. AP	100-104	108-112
3. AP	132-136	100-104
4. AP	132-136	100-104
5. AP	100-104	108-112
6. AP	100-104	108-112

Figure 4. Manual channel allocation on 5Ghz 40Mhz band overlapping cells

The manufacturer acknowledged that, according to point 4.2.3.2.2 and Table 2 of an old ETSI regulation [10], the power of the second antenna at 5 GHz must not exceed the power of UNII-2a, but this is no longer included in the newer regulation. Following further consultations and negotiations, we agreed that Cisco's programming team would treat this as a bug, i.e. a system error, in the following registry list, and that they would be willing to fix this problem to our satisfaction:
A Cisco Bug availability:
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo41248

Therefore, we chose the following temporary solution. The UNII-2a channels consist of 40 MHz channels 52-56 and 60-64, and the maximum available transmit power is 19 dBm. We did not plan to maximize the power of the UNII-2c channels anyway, so I set the maximum power of all Slot1 and Slot2 5 GHz antennas to between 19 and 21 dBm. This allowed me to achieve nearly identical coverage and transmitter power on both antennas of the APs in every cell.

AP neve	Slot1	Slot2
1. AP	100-104	52-56
2. AP	108-112	60-64
3. AP	60-64	108-112
4. AP	52-56	132-136
5. AP	100-104	52-56
6. AP	108-112	60-64

Figure 5. Temporary channel allocation on 5Ghz 40Mhz band overlapping cells

We tested the wireless network after installation using the following procedures. First, we turned off all old AP radio transmissions in the cell where we performed the tests. Using WLC, we checked whether any interfering devices were affecting the performance of the cell. We selected at least four critical locations in the cell we chose. For example, we performed software and speed tests with laptops among extensive manufacturing equipment. We continuously monitored changes in signal levels, network availability, and speed. In terms of software, we used Iperf and Speedtest applications to test speeds, and I used NetSpot and Wi-Fi Analyzer software to analyze the network. We used the following company devices for testing: laptop, industrial PC, barcode scanner, mobile phone. We also plan to perform Ekahau thermal mapping measurements, but only if Cisco system errors can be completely repaired. Finally, we disconnected all AIR-3702e AP radio traffic and put the new APs into live service. We visited several areas in the hall and asked for the opinions of employees who regularly use Wi-Fi devices in manufacturing processes. Their experiences and feedback on the new system were extremely positive, with no significant problems reported. The introduction of Wi-Fi 6 technology provides visibly higher data transfer rates and lower latency. Thanks to high-gain antennas, coverage of the area allows for more efficient use, reducing dead spots and improving radio signal quality. Better signal strength and stability enhance the user experience, especially in critical areas where it is challenging to build an adequate wireless network. The newly built wireless network can be easily upgraded if the physical dimensions and layout of the hall change. The locations of antennas and APs can be changed, positioned, and relocated as needed. Based on existing plans and experience, they can be planned in advance, and the capacities required for the investment can also be predicted. The device has a life cycle of at least 8-10 years, which allows for security improvements and the introduction of new protocols. The company does not currently have 6GHz devices, but the current system allows for conversion and frequency access. If higher bandwidth is required, the AP can also be connected to an optical network, as it has an SFP+ interface, so theoretically, data transfer

speeds of nearly 10Gbits can be achieved. If the company purchases IoT and automated equipment, the AP also supports high-availability MESH technology. To ensure network security, we integrate additional security systems to detect newly discovered vulnerabilities and intrusion attempts in a timely manner. Last but not least, we are exploring the possibility of integrating artificial intelligence-based systems to enhance the security of the new system.

Conclusions

In this article, we have presented how to prepare for the reconstruction of an industrial company's wireless network and implement it in accordance with expectations and plans. We have described and researched the possible methods and related professional experiences. We have modeled and tested the new system using state-of-the-art testing equipment. We have performed numerous measurements in the industrial area and used them to design the optimal layout of the devices. During the physical implementation of the wireless network, we specified the technical parameters required for the equipment and supervised the processes throughout. We designed the performance of the new network, which we adjusted and documented according to the circumstances. We sought a solution to a system error from Cisco so that the system could be put into live operation as soon as possible. We made the transition smoothly: users did not notice any network or service outages. The network is stable, reliable, provides full coverage of the hall and is redundant where necessary, and we have also managed to reduce energy consumption by reducing the number of APs. We have met both current and future expectations by introducing new technologies and security protocols.

References:

[1] M. T. Baross and A. Rónai, *Current methods of remote access to automotive manufacturing systems and security risks for the IT Data Center*. [Online]. Available: https://tinyurl.com/4vmb8an5.

[2] Nemzeti Jogszabálytár, *7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről*. [Online]. Available: https://njt.hu/jogszabaly/2024-7-20-7G.3.

[3] P. Calhoun, M. Montemurro and D. Stanley, *Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5415.

[4] Cisco, *Cisco Aironet 3700 Series Access Points*. [Online]. Available: https://www.cisco.com/c/en/us/support/wireless/aironet-3700-series/series.html.

[5] Ekahau, *Introducing Survey 2.0 and Pro 10.4*. [Online]. Available: https://www.ekahau.com/blog/introducing-survey-2-0-and-pro-10-4/.

[6] Cisco, *Supported Protocol Standards, RFCs, and IETF Drafts*. [Online]. Available: https://tinyurl.com/ykxkvbn2.

[7] Internet Engineering Task Force (IETF), *The Transport Layer Security (TLS) Protocol Version 1.3*. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8446.

[8] Cisco, *Cisco Catalyst IW9167 Heavy Duty Series Data Sheet*. [Online]. Available: https://tinyurl.com/mrxf5szz.

[9] Cisco, *Cisco Catalyst IW9167E Heavy Duty Access Point Hardware Installation Guide*. [Online]. Available: https://tinyurl.com/5nvmrvnv.

[10] ETSI, *ETSI EN 301 893 V2.2.0 (2023-11)*. [Online]. Available: https://tinyurl.com/yc2czmh6.