Design of Functional Networking Components as Elements of an Industrial Ecosystems

Valery A. Kokovin, member IEEE
Department of Automation of Technological Processes
State University "Dubna", branch "Protvino"
Protvino, Moscow reg., Russia
kokovin@uni-protvino.ru

Alexander A. Evsikov
Department of Automation of Technological Processes
State University "Dubna", branch "Protvino"
Protvino, Moscow reg., Russia
eaa@uni-protvino.ru

Vladimir I. Diagilev
Department of Automation of Technological Processes
State University "Dubna", branch "Protvino"
Protvino, Moscow reg., Russia
dvi@mail.ru

Victor V. Skvortsov
Department of Experimental Physics
Institute for High Energy Physics of the National Research Centre 'Kurchatov Institute'
Protvino, Moscow reg., Russia
skvv@rambler.ru

Saygid U. Uvaysov
Department of Design and Production of Radio-Electronic Means
MIREA – Russian Technological University
Moscow, Russia
uvaysov@yandex.ru

Aida S. Uvaysova
Department of Design and Production of Radio-Electronic Means
MIREA – Russian Technological University
Moscow, Russia
uvayaida@gmail.com

***Abstract*—The article analyzes industrial networking ecosystems that have added intelligence to manufacturing equipment, processes, and control. The features of the development of Functional Networking Components (FNC) are presented. FNC have the ability to receive and process information (the presence of a computer with network ports), have a physical nature (including hardware and software resources) and can affect the environment,. The structure of the FNC, which determines the function of these devices, and its main elements are considered. The article analyzes cybersecurity problems and ways to solve it. The use of digital matrices (FPGA) as part of the FNC hybrid calculator makes it possible to solve some security problems successfully. An example of the development and simulation of the FNC functional module, a combined generator of powerful ultrasonic vibrations, is considered. The network capabilities of FNC for switching and routing information packets are noted. FNC can be used as an element of a telecommunications network.**

Keywords— Functional Networking Components, IIoT, cybersecurity, FPGA, telecommunication net

I. INTRODUCTION

The digital revolution, based on the rapid development of such areas as microelectronics, information and communication technologies, nano-, bioengineering and additive technologies, leads to a change in technological structures. The expansion of the above technologies is proceeding at a high rate. As a result, industrial network ecosystems are rapidly developing, targeting various industries and technologies.

The competitive development of modern production of electronic devices and related technologies requires an increase in the efficiency of this production. All of these aspects are presented by the developed concept of Industry 4.0 [1]. This concept has given impetus to the development of industrial networking ecosystems, which is based on the well-established networking solutions of the *IoT (Internet of Things)* paradigm. The concept of *Industrial IoT (IIoT)* is successfully implemented in production. *IoT* has added intelligence to manufacturing equipment, processes and control [2]. Intelligent manufacturing solutions use connected sensors and devices to improve machine and human performance in real time and transfer data to the cloud for deeper analysis. The increased intellectualization of production components allows the functionality of technological systems to be expanded. The intelligence of the equipment is provided by the increased computing power of controllers, additional ability for video processing in real time and high touch sensitivity. But most importantly, it became possible to collectively solve production problems through the network interaction of individual production structures. Many algorithmic problems that were previously solved with the involvement of a centralized computer can now be solved at the level of the intelligent equipment itself or a cluster of such devices.

By analogy with IIoT, other networked ecosystems have emerged. For example, the Internet of Robotic Things (IoRT) aims to implement robotic technologies by extending the functionality of IoT devices. The work [3] presents the concept of IoRT, which emphasizes the tremendous flexibility in the development and implementation of new applications for networked robotics while achieving the goal of providing distributed computing resources. The emergence of network capabilities in mechatronic devices made it possible to interact and cooperate to solve the assigned tasks.

Telecommunication systems or their mechanisms are usually built into these devices to ensure cooperation in solving a distributed technological problem.

In distributed technological systems, among the participants in network ecosystems, there may be not only mechatronic components. In such systems can be also self-sufficient electrical devices with built-in intelligence. These devices don't include precise mechanics (which is a sign of mechatronic devices). "Self-sufficiency" is the ability of devices to solve independently a part of a distributed technological problem. At the same time, it is necessary to exchange information with other participants to solve the entire problem. Conventionally, such devices are called Functional Networking Components (FNC). This class of devices will include devices that have the ability to receive and process information (the presence of a computer with network ports), which have a physical nature (and not just a software resource) and are capable of affecting the surrounding physical environment [4]. The last condition in

978-1-6654-3941-1 @2021 IEEE

relation to FNC can be decisive, since it highlights the properties of these devices in relation to the environment of their use. In addition, FNCs of different "nature" (mechatronic, electrical, etc.) can affect the physical environment in different ways, which is reflected in the peculiarities of their organization as network devices. IoRT ecosystem devices are a special case of FNC.

The article is organized as follows. Section 2 gives the structure of the FNC, and the specifics of the organization. Section 3 discusses an example implementation of FNC, modeling and exploring individual nodes. The network capabilities of FNC's as elements of a telecommunication system are discussed. An algorithm for their interaction is considered. The properties of the FNC as elements of industrial ecosystems are discussed in Section 4. The conclusion is presented in Section 5.

II. Fanctional Networking Components

The development of microelectronics, information and communication technologies allows intellectualization of the network ecosystems devices. These devices increase the efficiency and functionality of microelectronics. As a result, their autonomy is also increasing, when making technological decisions. At a same time, certain problems related to the safety of use and cybersecurity may appear.

The history of the technics and technology development knows many cases of borrowing ideas and technologies from wildlife. There are lot of examples: sonars from whales, ultrasound scanners from bats, android robots that emphasize human resemblance, and so on. There is a science called biomimetics, which deals with the imitation of models, systems and elements of nature in order to solve complex human problems [5]. The famous Soviet physiologist, academician Anokhin P.K., the creator of the Theory of Functional Systems, wrote in his work [6]: *"Functional systems are dynamic, self-organizing, self-regulating structures, all the constituent elements of which interact and mutually contribute to the achievement of useful for the system and the integral organizations they build higher level of results"*. And further: *"The meaning of the systems approach is precisely that an element or component of functioning should not be understood as an independent and independent entity. It is understood as an element whose remaining degrees of freedom are subordinate to the general plan for the functioning of the system, directed by obtaining a useful result. The component should be an organic link in very extensive cooperation with other components of the system."* Taking into account these statements onto the network functional devices of technological systems, it is possible to outline the structure and specific goals for the creation and development of Functional Networking Components.

A. Structure of FNC

The structure of FNC should contain modules and be subject to the performance of the task (or tasks) that is determined by the function of the given device. Fig. 1 shows the FNC structure, which consists of individual modules interacting with each other. The composition of these modules may vary depending on the functionality of the FNC. But each FNC has a set of required modules:

- FNC is a network device, so there must be a network controller with a set of network interfaces. In addition to traditional wired interfaces (Ethernet, RS-485) and wireless (WiFi), there can be specialized ones, for example, an interface defined by the standard *IEEE*-1355 [7].
- Each FNC handles communication requests from other network devices and information from process sensors, implements cloud technologies and performs part of the distributed algorithm of the overall task. All of these are solved by a computing device. In the paper [8] hybrid configuration, using of the devices type FNC is presented. Such devices may include several heterogeneous computers built based on different computation models.
- Solving more and more complex problems requires increased intellectualization at the FNC level. The creation and development of FNC is closely related to the use of Artificial Intelligence (AI) elements. The main purpose of using AI in FNC is to solve evaluative and expert problems caused by sifting through a large amount of data. A separate challenge for AI is the need to ensure cybersecurity.

B. Cybersecurity and Engineering Safety problems of network devices based on platform IoT

The penetration of network ecosystems into industrial processes and infrastructure solutions requires increased cybersecurity of individual network devices. Considering that the *Internet of Things* is the expansion of Internet connectivity to physical devices and everyday objects, the USA in 2020 passed the IoT Cybersecurity Enhancement Act [9]. The law includes a requirement for the *National Institute of Standards and Technology* (NIST) [10] to ensure that standards are developed and published to improve IoT cybersecurity. In the future, digital certificates may appear for cryptographically binding devices on the IoT platform and, for example, websites. This will increase the protection of devices from unauthorized access.

The second important aspect of the network devices safe operation is Engineering Safety. It is related to the functioning of the FNC, which largely derives from cybersecurity. The work [11] analyzes the safety of IoRT robotic devices. The authors formulate the reasons for the emergence of abnormal situations when working with robots: problems with authentication and remote hacking of robots, performing cloud operations, lack of proper encryption on the side of suppliers, which can reveal confidential data, etc.

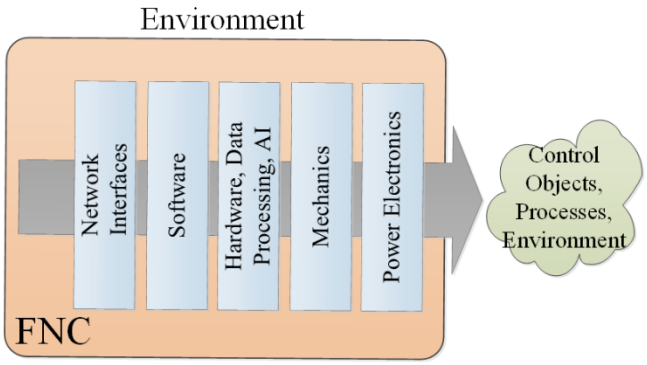

Fig. 1. Structure of Fanction Networking Components

Cybersecurity of network devices is primarily associated with the transmission and processing of data using communication protocols, so such messages must be encrypted, although in most cases this does not happen [12].

Safe operation of any type FNC devices (IoRT, network electrical devices, controlled drones, etc.) is largely associated with solutions to the same problems that are given in [11, 12]. As mentioned above, the FNC structure can contain a hybrid type-computing device (for example, on the ARM platform and FPGA). The use of FPGA can completely solve the cryptographic problem without compromising the manageability of the FNC, i.e. communication encryption, authentication, digital certificate support, etc.

III. Design and Simulation of FNC Nodes

An important part of the FNC is the node that defines the function of the device. This node, in fact, determines the functional purpose of the network device. An example of such a unit (a combined generator of powerful ultrasonic vibrations) is presented below.

In technological processes of mechanical engineering, ultrasonic treatment and cleaning of various parts are widely used. Also, methods of acoustic control are widely used for non-destructive testing of mechanical engineering products. As a rule, powerful generators are used as part of ultrasonic installations, which generate sinusoidal signals with low distortion. Such generators must be able to change the frequency and amplitude of the output signal to effectively use the ultrasonic transducer (UT), which is used as piezoelectric transducers. In technological processes the main technological parameter is the vibration amplitude.

On the other hand, generators can be used in the automation of technological processes. These processes are associated with the production of electronic devices, as part of actuators based on electric motors.

The use of a two-link oscillatory circuit with serial and parallel capacitors as part of a generator allows obtaining an undistorted sinusoidal voltage at the output with amplitude and frequency control. Digital control of the key elements of the converter makes it possible to formalize the task of monitoring and diagnosing an electric drive, including remote control. Simplified circuit of a combined generator (Fig. 2), which consists of two parts that perform different functions, is presented. The first part is a generator that generates an amplitude-modulated harmonic signal. The second part of the generator is responsible for the formation of powerful rectangular pulses with adjustable amplitude.

The first part of the generator includes a power supply 1, key power transistors T1-T4, a first control unit for 2 transistors T1, T3 and a second control unit for 3 transistors T2, T4; source of modulating voltage (low frequency signal) 4, oscillatory system (resonant LC1 circuit) and load R1.

The control unit of the left arm of transistors 1 and 3 (block 2) is the leading one in relation to block 3, which is synchronized from it.

To obtain a modulated sinusoid in the load, it is necessary to introduce block 4 into the circuit. Block 4 with control unit 3 enables transistors 2 and 4. The carrier frequency is many times greater than the frequency of the modulating voltage source 4. Thus, on the pulses of the carrier frequency control signals superimposed the signal slowly changing modulating

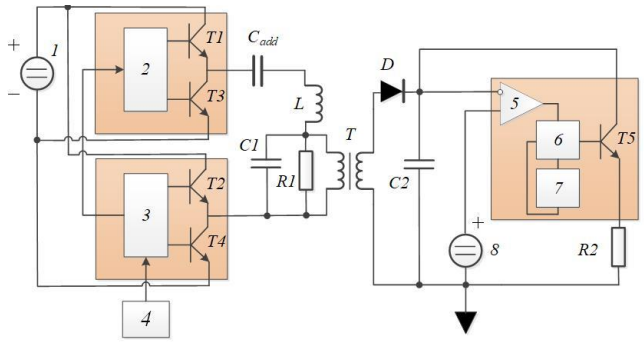

Fig. 2. Circuit of combined generator

voltage. With an increase in this voltage, the duration of the current flow in transistors 2 and 4 decreases, which leads to a decrease in the sinusoidal voltage in the load. This ensures non-simultaneous unlocking of transistors 2 and 4 in relation to transistors 1 and 3.

To regulate the output voltage (at the load R1) at a given level, it is necessary to add an additional capacitor C_{add} to the circuit. C_{add} is connected in series with the choke. In this case, voltage regulation is performed by changing the capacitance C_{add}.

The second part of the circuit makes it possible to implement a generator of rectangular voltage pulses. The generator with specified parameters in a wide range in amplitude (from zero to the maximum amplitude of the supply voltage) and a specified pulse duration. The input of the pulse generator receives an alternating voltage from the secondary winding of the transformer T. Then, through the diode D, the rectified signal is fed to the capacitor C2 and the inverse input of the comparator 5. Its second input is supplied with the setpoint voltage from the reference voltage source 8. When these voltages are equal, the comparator 5 is triggered, those. generates a signal that sets the trigger 6 in the active state.

The signal from the trigger output starts timer 7 for a specified time and opens the transistor switch T5. After a specified time, equal to the pulse duration, timer 7 resets trigger 6 and locks T5. The amplitude value of the output voltage across the load resistor R2 is set by the operator by setting the voltage value at the output of the reference voltage source 8. Then a timer determines the duration of the output pulse. As an input signal of the pulse generator, both an industrial network and any alternating periodically increasing voltage can be used.

Fig. 3 shows the equivalent generator circuit of powerful rectangular pulses and the timing diagram of its operation. The circuit works as follows: the comparator compares the reference signal Ref1 and the feedback signal from the voltage divider formed by resistors R5 and R6. According to the difference between the signal levels, the VT2 transistor is turned on or off. The switching frequency of the transistor and the hysteresis of the circuit are regulated by a divider of resistors R1, R8 and an integrating circuit R4, C2.

When transistor VT1 is saturated, the divider decreases the amplitude of the reference signal and increases the delay time for turning on the transistor VT2. The power amplifier of the rectangular pulses generator is assembled on the VT3 transistor. The timing diagram (Fig. 3) shows the sequence of the rectangular pulses formation.

From the block diagram Fig. 2 it can be seen that in order to set and change the parameters of a sinusoidal signal at the output of the first generator and square-wave pulses of the second generator, digital nodes (as part of the FNC) are required. In addition, the FNC is a network device, so resources are needed to remotely configure and interact with other network members.

IV. FNC'S AS ELEMENTS OF AN INDUSTRIAL ECOSYSTEM

FNCs, as part of an industrial ecosystem, must meet specific hardware, software and communication requirements. An analysis of works on the selected topic shows that the main trends in the organization of FNC boil down to the unification of control and communication subsystems, an increase in the computing power of each component and the presence of both wired and wireless communication facilities on board.

An important task in the FNC creation and operation as part of a distributed technological system is the development of software control applications.

The most optimal solution for the creation of software (SW) for industrial systems is to use generally accepted industrial standards. Until recently, most software developments were based on the languages and specifications of the *International Electrotechnical Commission (IEC) IEC* 61131-3 [13].

In 2005, *IEC* adopted a new standard IEC 61499 [14], which defines the way to build control systems for distributed technological processes. Software platforms based on the *IEC* 61499 standard used to develop distributed application projects meet most of the requirements set forth above for FNC. Additional solutions are required for process control where fast response and strict determinism of control signals are required. One of such solutions can be the use of hybrid computers on different hardware platforms [15].

Modern trends in the development of hardware for network ecosystems are associated with the active use of wireless technologies. However, there is no one-size-fits-all solution for IoT networks. Solutions must be tailored for individual industries, taking into account the requirements for bandwidth, reliability, transmission distance and safety. For example, in the automotive industry, automotive software is updated over Wi-Fi, while in the energy and construction industries, IoT is used to implement failure prediction and maintenance (O&M). [16].

FNCs can be used as elements of enterprise level telecommunications network. A model of a scanning information and navigation network (SINS) for interaction and navigation of AGV devices is proposed. SINS is defined by a set of distributed scanning cells that perform information and communication interaction. AGVs can exchange messages with each other on the basis of optical wireless technologies, broadcast through the SINS to the central computer of the received and processed data over the communication network. In this case, each AGV acts as a switch and router for the transmitted message packets.

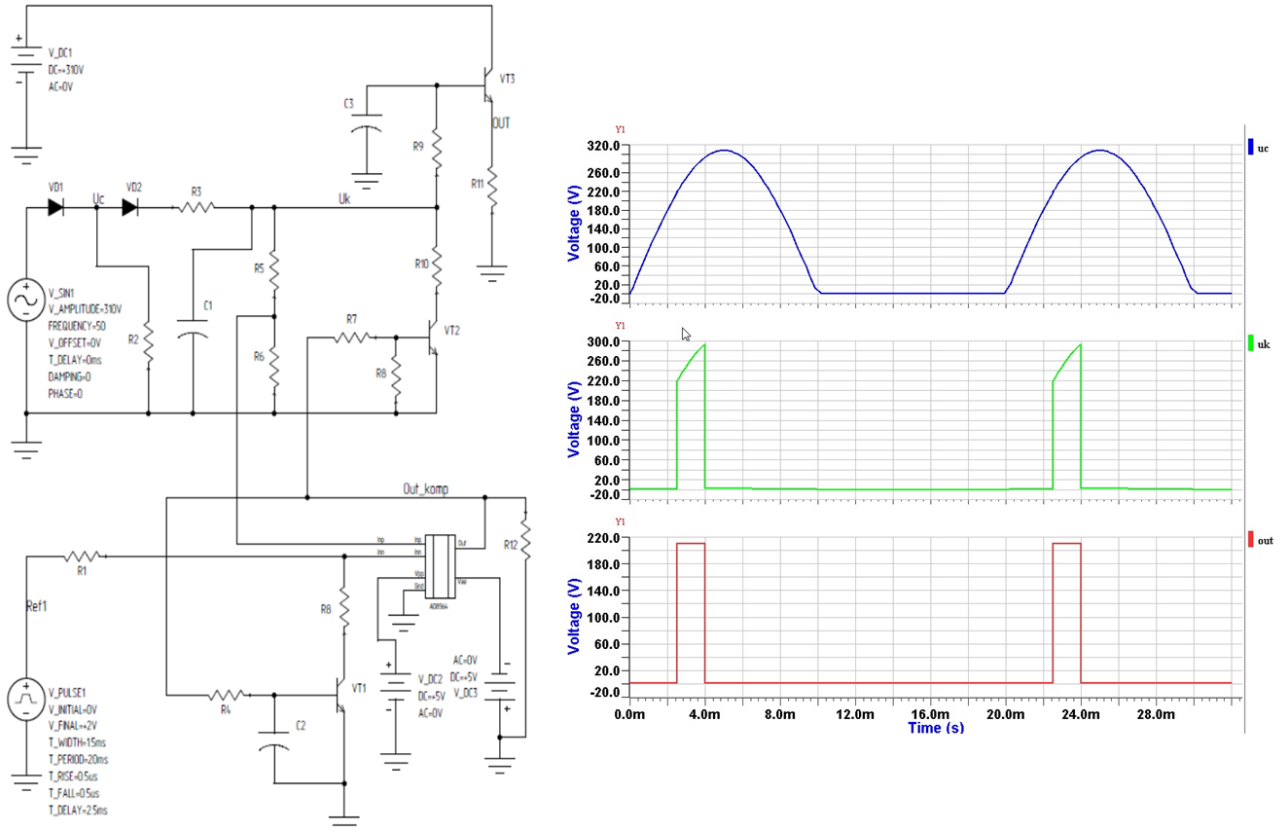

Fig. 3. Pulse generator equivalent circuit (left) and time diagram (right)

V. Discussion and Conclusions

The proposed solutions to the problem of FNC interaction within a distributed production ecosystem requires an analysis of the technological processes nature, an analysis of FNC algorithms dependence on data or control, etc. This analysis allows to identify the characteristics of the FNC organization in terms of the management and communication requirements for solving the tasks.

The article analyzes the development trends of industrial network ecosystems, hardware and software tools for the implementation of network associations. In particular, the considered capabilities of the software platform based on the *IEC* 61499 standard for the development of FNC control programs meet the requirements for network components. Possible non-determinism of interaction (as noted in [15]) is compensated by using FPGAs as part of FNC controllers when creating additional fast communication links for implementing deterministic network applications. The proposed additional computing platform based on FPGA, together with the ARM controller, forms a hybrid computing device as part of the FNC. It allows to control fast technological processes. In addition, the use of FPGA can help solve the cybersecurity problem by performing a cryptographic task without compromising the manageability of the FNC, i.e. communication encryption, authentication, and digital certificate support. The possibility of parallel data processing on FPGA allows fast switching of received information packets and their routing. As a result, it allows using FNC's as elements of a telecommunication network.

References

[1] F. Shrouf, J. Ordieres, G. Miragliotta, "Smart factories in Industry 4. 0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm", *2014 IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 697-701, 2014.

[2] B. Javed, M. W. Iqbal and H. Abbas, "Internet of things (IoT) design considerations for developers and manufacturers," *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, Paris, 2017, pp. 834-839, doi: 10.1109/ICCW.2017.7962762.

[3] P. P. Ray, "Internet of robotic things: Concept technologies and challenges", *IEEE Access*, vol. 4, pp. 9489-9500, Jan. 2017.

[4] V. A. Kokovin, A. A. Evsikov, S. U. Uvaysov and S. S. Uvaysova, "Event-based Cooperation of Functional Networking Components in Distributed Technological Systems," *2020 Moscow Workshop on Electronic and Networking Technologies (MWENT)*, Moscow, Russia, 2020, pp. 1-5, doi: 10.1109/MWENT47943.2020.9067384.

[5] Vincent, Julian F. V.; et al. "Biomimetics: its practice and theory", in *Journal of the Royal Society Interface*. **3** (9), pp. 471–482, August 2006.

[6] P. K. Anokhin, “Fundamental questions of the general theory of functional systems,” in: Principles of System Organization of Functions, Nauka, Moscow (1973), pp. 5–61.

[7] IEEE Standard for Heterogeneous Interconnect (HIC) (Low-Cost, Low-Latency Scalable Serial Interconnect for Parallel System Construction)”, IEEE Standard 1355 - 1995, IEEE, June 1996

[8] V. Kokovin, V. Diagilev, S Uvaysov and S. Uvaysova, “Intelligent power electronic converter for wired and wireless distributed applications”, In Proc. of the IEEE International Conference SED-2019, 2019, pp. 1-5, doi: 10.1109/SED.2019.8798455

[9] Internet of Things Cybersecurity Improvement Act of 2020. (Online) Available: https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf

[10] National Institute of Standards and Technology. (Online) Available: https://www.nist.gov/

[11] I. Afanasyev *et al*., "Towards the Internet of Robotic Things: Analysis, Architecture, Components and Challenges," *2019 12th International Conference on Developments in eSystems Engineering (DeSE)*, Kazan, Russia, 2019, pp. 3-8, doi: 10.1109/DeSE.2019.00011

[12] G. Hu, W. P. Tay and Y. Wen, "Cloud robotics: architecture, challenges and applications," in *IEEE Network*, vol. 26, no. 3, pp. 21-28, May-June 2012, doi: 10.1109/MNET.2012.6201212

[13] International Standard IEC 61131-3 (edition 2.0): Programmable Controllers / International Electrotechnical Commission. – Geneva, 2003. – 230 p.

[14] International Standard IEC 61499. Function blocks for industrial-process measurement and control systems. Part 1: Architecture / International Electrotechnical Commission. – Geneva, 2005. – 245 p

[15] H. Pearce and P. Roop, "Synthesizing IEC 61499 Function Blocks to hardware," *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, Auckland, New Zealand, 2019, pp. 1-6, doi: 10.23919/ELINFOCOM.2019.8706345.

[16] (Online) Available: https://e.huawei.com/ru/eblog/enterprise-networking/wifi6/iot-wifi-networking