CYBER RESILIENT PLATFORM FOR INTERNET OF THINGS (IIOT/IOT)ED SYSTEMS: SURVEY OF ARCHITECTURE PATTERNS

Petrenko S.A.[1]

Abstract.

Purpose of the article*: development of tools for building the cyber resilient platform for Internet of things (IIoT/IoT). The urgency of development the cyber resilient platform for Internet of things (IIoT/IoT) is to provide the required security and resilience of critical information infrastructure of the Russian Federation in the face of rising security threats, and imperfection of the known models, methods and means for data collection and processing in IIoT/IoT networks, based on the wireless technology Sigfox, LoRaWaN, "Strij/"Vaviot" (XNB/Nb-Fi), NBIoT.*

Research methods*: It uses the author's models and methods of similarity and dimensions theory of the distributed computing, as well as the domestic technology of wireless communication Logic Inter Node Connection (LINC) (http://aura360.ru/), as well as the domestic FenixOS operating system (https://fenix.link/kontakty/), designed for collecting and processing the telemetry data.*

Results: *Developed tools for building the cyber resilient platform for Internet of things (IIoT/IoT).* The article presents the main scientific and technical results of solving this problem. The research was carried out within the framework of the Federal project "Information security" of the national program "Digital economy of the Russian Federation". It is important to note that the results allowed designing a prototype of the domestic Internet of things (IIoT/IoT) platform with self-healing data reception and transmission paths between smart devices.

Keywords: *Digital transformation, Digital economy, Critical information infrastructure, Cyber resilience, Self-organization, Domestic Internet of things (IIoT/IoT) platform.*

DOI: 10.21681/2311-3456-2021-2-81-91

Critical analysis of well-known IIoT/IoT platforms

According to *IHS Markit's IOT Trends to Watch* analytical review[2] by 2021, the number of connected IIoT/IoT devices in the world will exceed 51 billion units. First of all, the increase in the number of mentioned devices will occur due to the need for remote control of equipment. According to available forecasts, the commercial and industrial sector, which uses solutions for building automation, industrial automation and smart lighting, in the period from 2020 to 2030, will account for about half of all connected devices. At the same time, the so-called hyperconvergence of the modern digital transformation technologies comes to the fore: the Internet of things *(IIoT/IoT*), Artificial intelligence (*AI*), *Cloud and Fog computing* and, of course, the Big data collection and processing (*Big Data*). Today, the number of *IIoT/IoT* devices and related microelectronic components is increasing rapidly. The complexity of Internet of things platforms – a variety of finite elements (sensors, sensors, base stations, etc.), as well as the complexity of the behavior of these systems – algorithms and methods of interaction between them – is also constantly growing (see figures 1-2). First of all, this applies to IIoT/IoT platforms for smart cyber systems: smart energy, smart cities and transport, smart homes, etc. The mentioned *IIOT/IOT* platforms and end devices also support various formats of inter-network interaction, including formats of low-power wide – area network *(LPWAN): LoRa, Narrow Band IoT (NB-IoT), XBN, ZiNa, NB-Fi, Sigfox, ZigBee, PLC (PLC), Strij, Vaviot, LINC*, etc. [1-3, 7]. In the mentioned review of *IoT Trends to Watch*, IHS Markit analysts identify the following key trends that will affect the development of *IIoT/IoT* in the nearest future:

1. Attractive features of the Internet of things (*IIoT/IoT*) contributed to the emergence of a large number of duplicate and similar solutions based on *Bluetooth, Wi-Fi, 5G, NB-IoT, LoRa, Sigfox* and other wireless communication technologies. Consolidation of communication and data processing standards is still ahead, but fragmentation and competition of *IIoT/IoT* solutions will prevail in the nearest future.

2. Hybrid approach, based on local *Data storage and processing centers and private clouds* is gaining strength, since such placement and appropriate data processing are a competitive advantage for digital economy enterprises. More and more digital businesses are expected to use local Data storage and processing centers and on-premises cloud services to manage their IT infrastructure.

3. Development of requirements for the functionality of *low-power Internet of things (IIoT/IoT)* devices, the

1 Sergei Petrenko [0000-0003-0644-1731], Innopolis University, Universitetskaya 1, Innopolis, 420500, Russia. E-mail: s.petrenko@innopolis.ru

2 https://cdn.ihs.com/www/pdf/IoT-Trend-Watch-eBook.pdf

ability to work in the licensed and unlicensed spectrum, as well as providing better coverage significantly reduce the costs of enterprises using *LPWAN* solutions.

4. *Cellular IIoT/IoT gateways* for connecting to the global Internet are used for organizing and performing the so-called boundary or edge computation. At the same time, the cybersecurity of cellular *IIoT/IoT gateways* will require more attention.

5. Cybersecurity problem is becoming one of the main ones for the formation and development of the well-known Internet of things *(IIoT/IoT) platforms*. The risks for them will increase significantly. Despite the popularization of blockchain technology, it is not a panacea for building secure and trusted solutions. At the initial stages of *IIoT/IoT platform* development, *blockchain technology* will be used in asset management and *Smart contracts*.

6. Most *IIoT/IoT platforms* are becoming more integrated. Today, more than 400 developers and suppliers of such solutions are known. However, significant innovations and corresponding results will appear when developers *of IIoT/IoT applications* will get into all the rich functionality of *Big data* collection and processing technology.

For example, *IIoT/IoT solutions* from Modern Radio Technologies[3] - "*Strizh*" – based on a proprietary data transfer technology *LPWAN XNB (previously-Marcato[2])*, which is a modification of the *French Sigfox LPWAN technology*. *XNB* has a narrow focus and is characterized by a number of features, in particular, low data transfer rate, limited amount of data transmitted, low level of cryptographic protection of communication channels and data. This technology works in an Internet environment, characterized by a low energy efficiency and data transfer speed (the data packet transfer time is approximately 6 seconds) [4-6].

Decisions of the "*Waviot*" company[4] (came from the "*Modern Radio Technology*") based on the *NB-Fi* wireless data transmission technology, which received the status of the first national communication standard for *IIoT/IoT* in Russia in 2019. At the same time, it is also characterized by a narrow focus and significant limitations, including a low data transfer rate (similar to the technology described above), a small amount of useful data, a large amount of overhead data, and an insufficient level of cryptographic protection of communication channels and data. This technology lacks a symmetric return channel for operating modes and devices, as well as the ability to build local systems without the Internet [6-12].

Solutions of companies from *LoRa Alliance-Lartech*[5], "*Smartiko*"[6], *Network 868*"[7], *ER-Telecom*[8] and others - based on the *American LoRaWan technology (Long Range Wide Area Networks)* [8-11], developed on the basis of the LoRa modulation method of the *California company Semtech, USA*[9]. In addition to *Semtech, the Alliance includes IBM* (founder), a number of well – known electronics manufacturers - *Cisco, Kerlink, IMST, Microchip Technology* - and leading Telecom operators-Bouygues Telecom, Inmarsat, Singtel, Proximus, Swisscom and others. Today, *LoRaWAN networks* are operated in more than 15 countries (tested in more than 60 countries), the largest are deployed in the *United States, Australia and several European* countries. *LoRaWan technology* and related solutions belong to the broadband class and provide high performance of the communication channel budget (up to *168 dB*). However, these solutions do not work without Internet access. The operation results indicate an irrational use of the allocated frequency band and a significant amount of service information in the package (overhead). For these reasons, the number of end devices is limited. The packet duration is long, which leads to a lower energy efficiency and less frequent data transmission. A full-fledged feedback channel for Autonomous devices is not possible, and there are no retransmitting modes. Finally, *LoRaWan*-based solutions are characterized by a low jamming immunity.

"*Energomera*" solution[10] - automated data collection system of the Utility metering system – based on *ZigBee communication technology*. However, its distribution is limited to the electricity market. In addition, *ZigBee* is based on automatic signal retransmission and routing, characterized by a relatively short range of the radio signal, the complexity of signal routing and network configuration. And due to the implementation of its Protocol, it is not possible to use Autonomous devices.

RIA-Group solution[11] - "*Aura 360*" (Figure 3) - based on the original technology and the eponymous *LINC (Logic Inter Node Connection)* wireless communication Protocol. The data collection system uses the well-known *OSI model* (it operates over the LINC Protocol, combining OSI layers from 2 to 6). "*Aura 360*" uses an accessible data transmission environment, including *Ethernet, RS-485, GSM (GPRS, LTE, NB-IoT, etc.), and even LoRa*. However, the "last mile" physical environment uses a narrow-band *LPWAN* radio channel from the non-licensed bands, which allows the implementation of the last mile to be attributed to *UNB systems*. Here, the ultra narrow band (*UNB*) is characterized by higher bandwidth and provides the most efficient use of the frequency band. For example, in the upper license - free range for Russia (*868.7-869.2*), up to 60 communication channels are supported, unlike *LoRaWAN* with three channels and a width of *125 kHz*. It is important that *LINC* can work over the existing data transmission channels and in it exceeds the characteristics of well-known foreign (and based on them) communication technologies – *LoRaWAN, XNB ("Strizh"), NB-Fi ("Vaviot"), ZiNa (Fenix), Sigfox, ZigBee* and others. The *LINC Protocol* is characterized by a high level of a cryptographic protection, greater versatility, and can work in different physical communication environments.

3 www.strij.tech
4 https://waviot.ru/
5 https://lar.tech/
6 https://smartiko.ru/
7 https://net868.ru/
8 https://iot-ertelecom.ru
9 https://www.semtech.com/lora
10 http://www.energomera.ru/
11 http://aura360.ru/

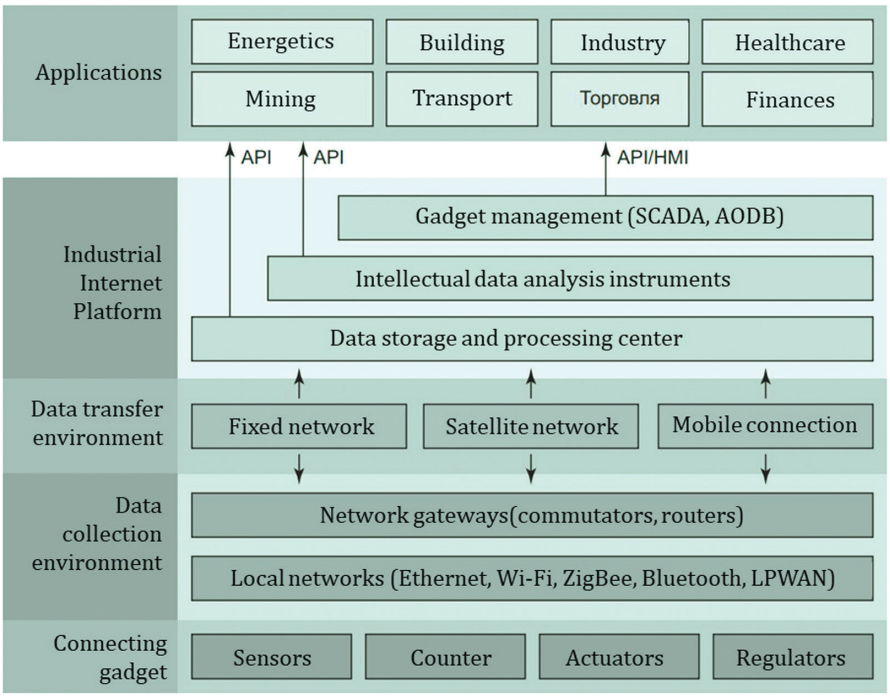

Figure 1. Current model of the most well-known Internet of things (IIoT/IoT) platforms

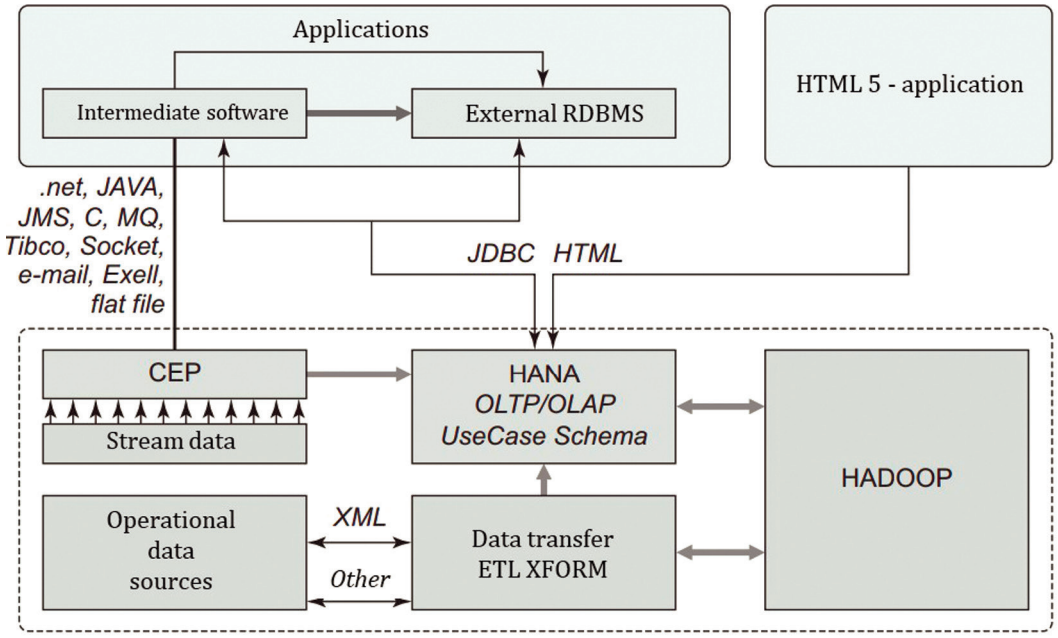

Figure 2. Possible core diagram of the Internet of things (IIoT/IoT) platform

DOI: 10.21681/2311-3456-2021-2-81-91

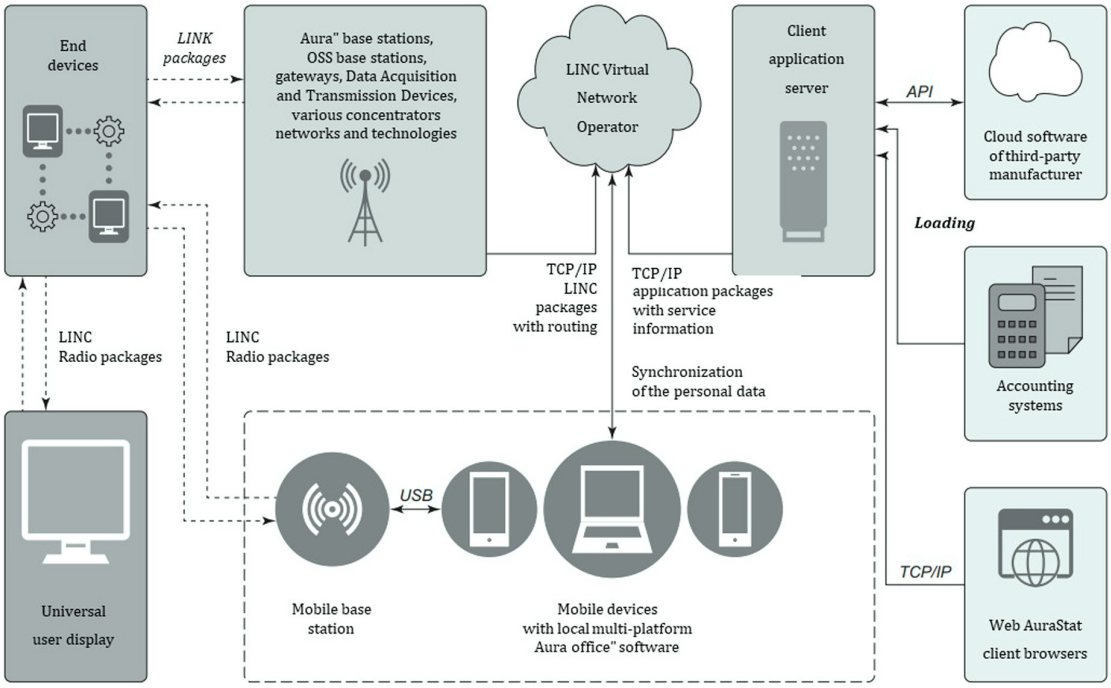

Figure 3. Possible core diagram of the Internet of things (IIoT/IoT) platform on the example of "Aura 360"

The main advantages of "*Aura 360*" (Figure 4) include:

- high communication parameters: range up to 15 km point-to-point (25 mW) or up to 100 km (using directional retransmitting);
- permanent two-way communication (half-duplex) even with Autonomous devices;
- full management of end devices, including Autonomous ones;
- efficient use of the frequency range (UNB);
- point-to-point and point-to-multipoint relation;
- implementation of relay and broadcast command modes;
- support for devices with small computing resources;
- no limit on the data transfer rate (meets the specifications of transceivers);
- no restrictions on the amount of data transmitted;
- amount of data in a packet is up to 256 bytes;
- supports up to 48,000 devices per base station channel, up to 60 channels in the upper 868 MHz band;
- support for working without the Internet and cloud technologies (on-premises systems);
- support for most known devices and components;
- protection of communication channels based on the TLS 1.3 specification;
- ability to work in a wide temperature range: from -60 to +80C.
- independence from the sanctions policy of foreign states, etc.

In the given example (see figure 4), the optimal base rate of the uplink channel of *1200 bps* provides a short data packet transmission time *of 0.3-1.7 seconds*, if the packet volume does not exceed *256 bytes* (and at the same range as in *LoRaWAN systems on SF12 at 300 bps*). Accordingly, the "*Aura 360*" device is in transmitting mode (with the same packet size) for six times less time than the *LoRaWAN* device and *12 times* less than the *NbFi/XNB device ("Vaviot"/"Strij")*, which indicates greater energy efficiency of the "*Aura 360*"devices.

2. Operating systems for IIoT/IoT platforms

A number of the well-known companies are developing operating systems for the Internet of things (IIoT/IoT): *Amazon Web Services (Amazon IoT), Arm Holdings with technology partners (mbed OS), "Contiki" (Contiki OS for microcontroller), "Fenix link" (FenixOS)* and others. Also, most of the diversified large IT companies, including *IBM, Microsoft, SAP, Oracle, Apple, Google*, and others are conducting similar developments. At the same time, it should be noted that the system and application software (software) and computing devices of the Internet of things (IIoT) are fragmented and diverse [9-15]. Let us comment on a number of well-known solutions.

Amazon Web Services (AWS)[12] - Internet of things platform with the same OS. The American company of the same name is developing its own Amazon IoT platform (from end devices to cloud systems): a number of solutions have been developed for the industrial and user segments of the Internet of things. Their features include binding to the Amazon server infrastructure, integration with Amazon Web Services, and support for a limited list of hardware platforms (microcontrollers).

ARM platform of the Internet of things based on the open-source OS Mbed is being developed by the British

12 https://aws.amazon.com/iot

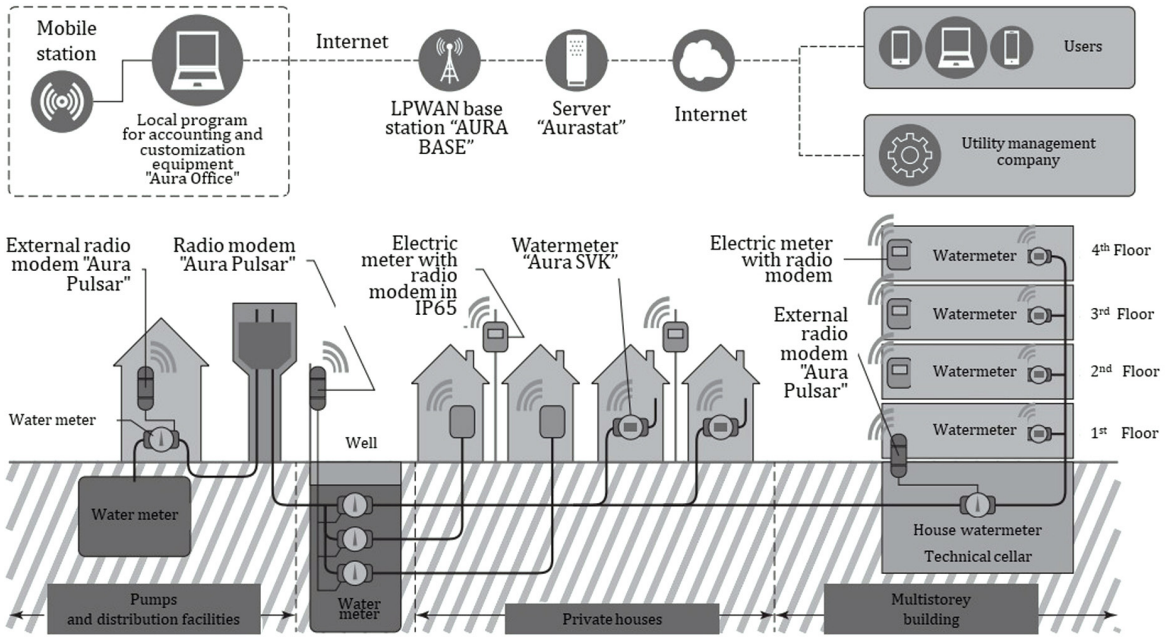

Figure 4. Possible implementation of the Internet of things (IIoT/IoT) platform on the example of "Aura 360"

holding ARM Holdings[13] for the corresponding microcontroller-based devices. Mbed code[14] is distributed under the Apache 2.0 license. The development of this OS is carried out in the direction of supporting IIOT/IoT communication channels and adding server tools, as well as APIs for integrating the solution platform on the Internet.

Contiki: The Open Source OS for the Internet of Things[15] is a non-commercial open source operating system. Designed for managing various IIOT/IoT devices with limited resources. The OS was named after the team of the famous Norwegian Explorer-traveler *Thor Heyerdahl (1914 - 2002*). In 1947, to prove the hypothesis of the migration of the Polynesian ancestors from South America to the Islands of the Eastern Pacific Ocean, scientists repeated their route on an exact copy of the balsa raft of the fifth C.E. *"Con-Tiki" (the Sun God - Tiki).* The Contiki OS project was initiated by the *Swedish Institute of Computer Science (SICS)* in 2006. It continues today. Contiki OS is written in *C* and runs on a variety of computing platforms and architectures, from *TI MSP430* (with 2 KB of RAM and 60 KB of permanent flash) and *Atmel AVR* to earlier architectures. In terms of source code and memory utilization, this operating system is relatively small. For example, *Contiki OS* requires no more than *30 to 40 KB* of *RAM* to run and work with the graphical interface. In addition, the amount of memory can be configured for the tasks to be solved.

Let's look at this OS in more detail and list its features.

- *Event-driven (ED) system core* that allocates processor time, but not memory (designed for hardware without - a memory management unit, MMU). For this reason, all processes are executed in the same address space.
- A *compact scheduler* that sends events to running processes. There are two types of events: asynchronous and synchronous. The first are similar to deferred procedure calls: they are queued by the kernel and passed to processes after some time. The second trigger immediate process planning. Control is returned to the initiator process after the target finishes processing the event.
- A *polling mechanism* is a high-priority event, triggered between asynchronous events. It is usually used by processes that operate hardware, for example, to check device status updates. When a survey is scheduled, all processes where it is applied are called in priority order.
- The *preemptive multitasking mechanism* is implemented as a library and, if necessary, can be linked to applications that require such a functioning model.
- *Protothreads* – threads that work with a single shared stack. It is written in the C programming language without using machine-oriented Assembly code and requires only two bytes of memory to store states. This made it possible to significantly reduce the complexity of programs developed using the finite state machine paradigm, radically reduce the number of States and transitions, and reduce the amount of code.
- A dynamic runtime linker that binds, transfers, and loads applications and services as ELF object files, which is standard in many operating systems for

13 https://www.arm.com
14 https://os.mbed.com
15 http://www.contiki-os.org/)

personal computers and workstations, and is suitable even for WSN nodes.

- *The CTK (Contiki Tool-Kit*), which provides graphical user interface primitives, is designed to be highly modular to allow the same program to function on a wide range of monitors, from graphical terminals and virtual displays like VNC to text displays (in a terminal window from Telnet).
- *Lightweight implementation* of the *TCP/IP stack* and IP for Internet connectivity for resource-constrained systems. Supports TCP, IP, ARP, SLIP, ICMP (ping), and Unicast UDP protocols. However, the number of TCP connections is unlimited. The uIP code takes up several kilobytes of permanent memory and several hundred bytes of RAM. The stack package also includes a Web server and client, an SMTP client, and Telnet and DNS servers. PPP support has been worked out
- Contiki VNC is a server that provides remote access to the system desktop from almost any operating system via the Internet. It is a u VNC port that connects to the CTK as a driver.

Fenix Link[16] - a domestic IIOT/IoT platform based on the original FenixOS (Figure 5), optimized for telemetry data collecting and processing. In this development, the main principles are:

- priority of efficiency in providing basic telematics processes and resources over functionality (functionality that is not directly related to telematics) and the variety of tasks to be solved;
- limiting the number (variety) of processes;
- simplification of existing processes, including those necessary for solving telematics problems;
- microkernel as a type of operating system kernel;
- threads as a software model;
- minimizing the need for middleware;
- algorithms for fast transition to the sleep mode;
- proprietary process control algorithms.

Thus, *FenixOS* is an operating system based on a microkernel, as opposed to operating systems based on a monolithic kernel. At the same time, the *FenixOS core* contains only the key components necessary for telematics systems of the Internet of things *(IIoT/IoT*). It uses algorithms for managing operating system processes that minimize power consumption and hardware requirements, including algorithms:

- process execution;
- prioritizing the order of process execution;
- process planning and dispatching;
- allocating resources (available) to a process and distributing them between processes.

Note that *FenixOS* does not implement a preemptive multitasking mechanism. Here it is achieved by switching between processes-cooperative multitasking ("simulating" multitasking and multiprocessing), without real parallelization and multitasking, unlike other well-known operating systems. The *FenixOS* core is written in the C programming language, which allows accurately managing the processes at a low level. The operating system's libraries and drivers support various communication standards, including *LPWAN (Low-power Wide-area Network*). Devices which microcontroller operates on the basis of *FenixOS* work with common communication formats, such as *LoRa (Long Range), Narrow Band IoT of the 3GPP consortium (NB-IoT), XBN and NB-Fi (Russian developments), Sigfox, ZigBee, ZiNa (Zigzag Narrow-band), Fenix Link, PLC (PLC), LINC,* and others. An *API* has also been developed for working with a variety of Internet of things *(IIoT/IoT)* applications and devices.

Justification of the approach to building cyber-resilient IIOT/IoT platforms

Today, the *TCP/IP Protocol stack* (Figure 6) is the standard for interaction between typical digital platforms of the Digital economy of the Russian Federation. The *IP Protocol* (versions v.4 and v.6) performs network communication functions in the stack. Representatives of transport layer protocols are UDP, TCP, and the modern *SCTP standard* [12-15]. Almost all known standards can be used as lower-level *IP protocols. Most often, Ethernet, Frame Relay, ATM, PPP, MPLS,* and others are used as channel-level protocols. Due to the special position occupied by the *TCP/IP stack*, almost all modern application-level protocols are oriented towards using *TCP or UDP* as a transport Protocol. These include, for example, email (*SMTP and POP*), domain name service (*DNS), WWW – world wide web (HTTP), file transfer protocol) (FTP), network news transfer protocol (NNTP), Microsoft basic network service (NetBIOS), distributed database interaction (SQL*Net),* and others.

A characteristic feature of the current Protocol system is, first, the tendency to implement the functions of the session level of the OSI model by a Protocol that was originally designed as a transport Protocol (for example, TCP or SCTP), or an application-level Protocol. In some cases, session information storage functions are shared between these protocols. Second, in the vast majority of cases, the functions of the OSI model level 6-data representation – are inextricably integrated with the application layer Protocol. This is due to the fact that at the development stage of most of these protocols, the format for processing the data representation level was rigidly fixed. Third, a similar situation is observed with the combination of approximately equal functional load of the physical and channel levels [12-15].

Thus, the most common network Protocol stack that a message passes through consists of four protocols: the application-level Protocol, the transport level Protocol (TCP or UDP), the IP Protocol, and one or more physical and link level protocols. Therefore, first of all, the work was performed in terms of converting the data transceiving model into a dimensionless form for organizing semantic dynamic control of the digital platforms.

Let's look at the main ideas of the author's approach using an example.

Example of checking application semantics

Operator of the form:

16 https://fenix.link/kontakty

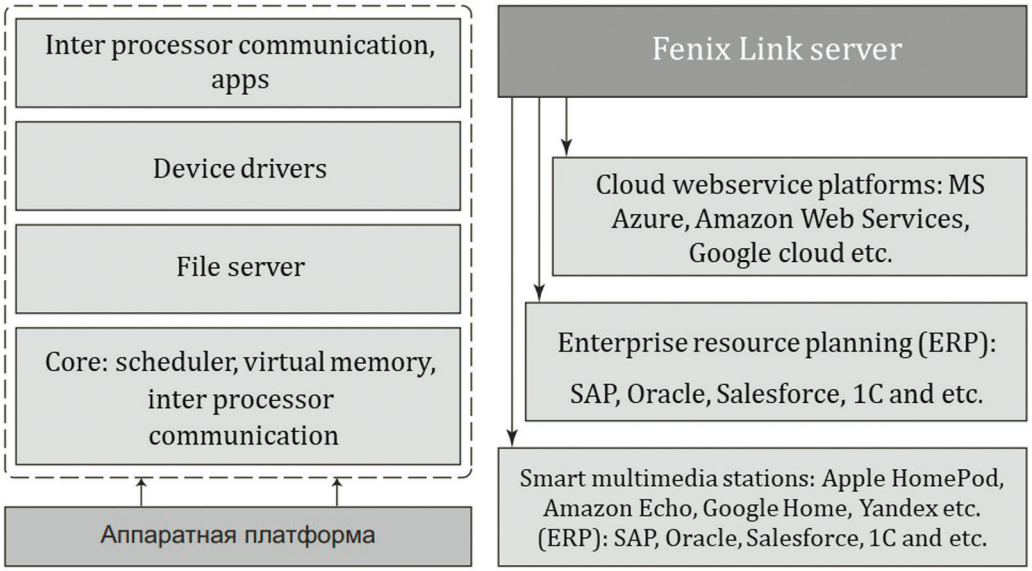

Figure 5. Fenixos OS block diagram

$$A = B \cdot C + \frac{D}{E} + 1 \quad (1)$$

In terms of dimensions, we obtain three corresponding equations of dimensions (2 - 4):

$$(1)\cdot\ln[A]+(-1)\cdot\ln[B]+(-1)\cdot\ln[C]=0, \quad (2)$$

$$(1)\cdot\ln[A]+(-1)\cdot\ln[D]+(1)\cdot\ln[E]=0, \quad (3)$$

$$(1)\cdot\ln[A]^1=0. \quad (4)$$

If in (4) we consider a numeric constant as a variable (for example, named CONST_1) of a certain dimension, then the operator (4) will add six variables to the constraint system (A, B, C, D, E, CONST_1). The equation (5) will also change to look like this:

$$(1)\cdot\ln[A]^1+(-1)\cdot\ln[CONST\_1]^1=0. \quad (5)$$

As a result, the variable A will remain in the system with a non-trivial value until the end of calculations [23-32, 35].

Validation of correctness

Such change of status of numerical constants allows defining the criteria of semantic correctness of technological platform of some digital enterprise in the following form [12-15]:

Statement 1. For semantic correctness of the technological platform of a digital enterprise, it is necessary that the system of dimensionality equations constructed for it, taking into account numerical constants, has at least one of the sets of solution vectors consisting of all non-zero components.

Proof of the statement (from the opposite). The appearance of one that is identically equal to zero for any values of other variables corresponding to dimensions means that it is dimensionless. However, this contradicts the condition of constructing a system of constraints, namely, the introduction of dimensions to all variables and constants of the process.

The statement is proved.

For numerical verification of the criterion, we construct a system of equations of dimension of the matrix R based on the matrix S of coefficients, which has a special form:

$$R = \begin{Vmatrix} 1 & 0 & \dots & 0 & c_{1,1} & \dots & c_{1,n-k} \\ 0 & 1 & \dots & 0 & c_{2,1} & \dots & c_{2,n-k} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & c_{k,1} & \dots & c_{k,n-k} \end{Vmatrix}. \quad (6)$$

The matrix R in this form can be represented by the formula:

$$R_{k\times n} = E_{k\times k} \mid C_{k\times(n-k)}, \quad (7)$$

where:

E – the identity matrix,

k and n are the number of rows and columns of the original S matrix , respectively.

To construct the R matrix, it is sufficient to use three types of operations:

- adding an arbitrary row of a matrix to a linear combination of other rows;
- permutation of rows;
- permutation of columns.

The main course of the process of achieving the form is similar to the Jordan-Gauss method (see, for example, [12-15]). The difference is:

- double pass of the algorithm: first in the forward (top-down) direction, and then in the reverse (bottom-up) direction;
- when a non-zero value in a cell within the first k columns, which is not the first non-zero value in the row, cannot be converted to zero due to the absence of other non-zero members in this column.

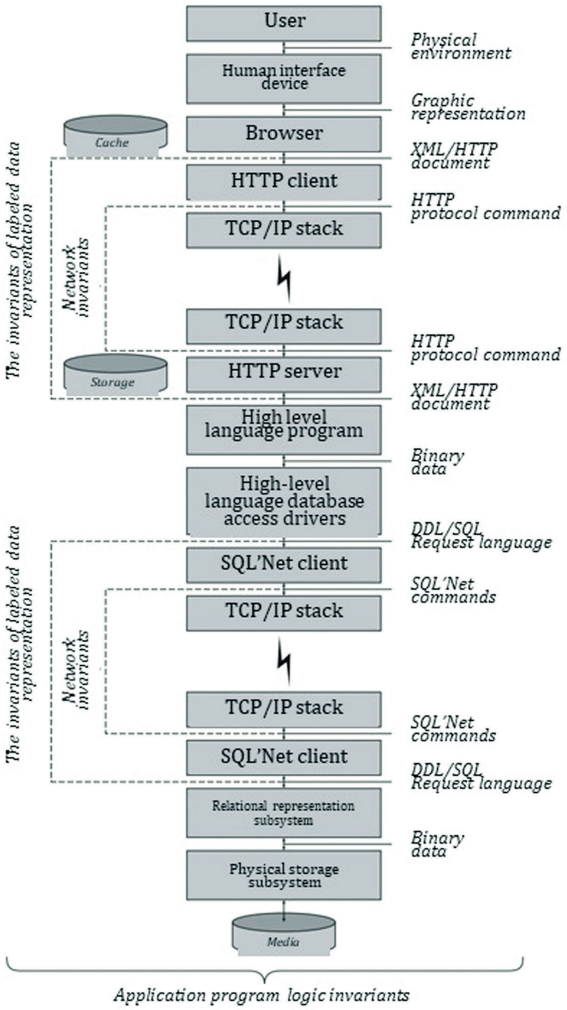

Figure 6. Typical scheme of data transceiving

Applied to the solution of a system of dimensional constraints matrix R is identical to the matrix S, except for possible column permutations. That is, there is an equivalent:

$$(S \cdot X = 0) \Leftrightarrow (R \cdot T \cdot X = 0), \quad (8)$$

where:

T is a square permutation matrix of dimension n×n corresponding to the permutations of columns in S performed at the construction stage R.

This result is due to the nature of the transformations performed on the matrix S in the process of constructing the matrix R.

Correctness conditions

Formula (8) allows using the R matrix instead of the S matrix when checking semantic correctness. Let's formulate the following statement for this purpose:

Statement 2. To have among the first k values of the vector-solution of the restriction system of the i-th component dimension, which is identically equal to zero, it is necessary and sufficient that in the i-th row of the matrix C in the formula all elements are equal to zero.

Let us prove the necessity of the condition (from the opposite). Let in the i-th row of the matrix C (for example, in position j) be at least one non-zero element . Then, setting all (n-k) last variables equal to zero, with the exception of (k+j)-th, we get the following equality:

$$\sum_{p=1, p\neq i}^{k} 0 \cdot x_p + x_i + \sum_{q=1, q\neq j}^{n-k} c_{i,q} \cdot 0 + c_{i,j} \cdot x_{k+j} = 0 \quad (9)$$

$$x_i = -c_{i,j} \cdot x_{k+j}, \quad (10)$$

which means that in this case, the variable xi is not zero.

This is a contradiction.

The necessity of the condition is proved.

Let us prove the sufficiency of the condition. If all elements of the I-th row of the matrix C are equal to zero, we get the following equality:

$$\sum_{p=1, p\neq i}^{k} 0 \cdot x_p + x_i + \sum_{q=1}^{n-k} 0 \cdot x_{k+q} = 0, \quad (11)$$

from which the desired identity is obtained directly:

$$x_i \equiv 0. \quad (12)$$

The statement is proved.

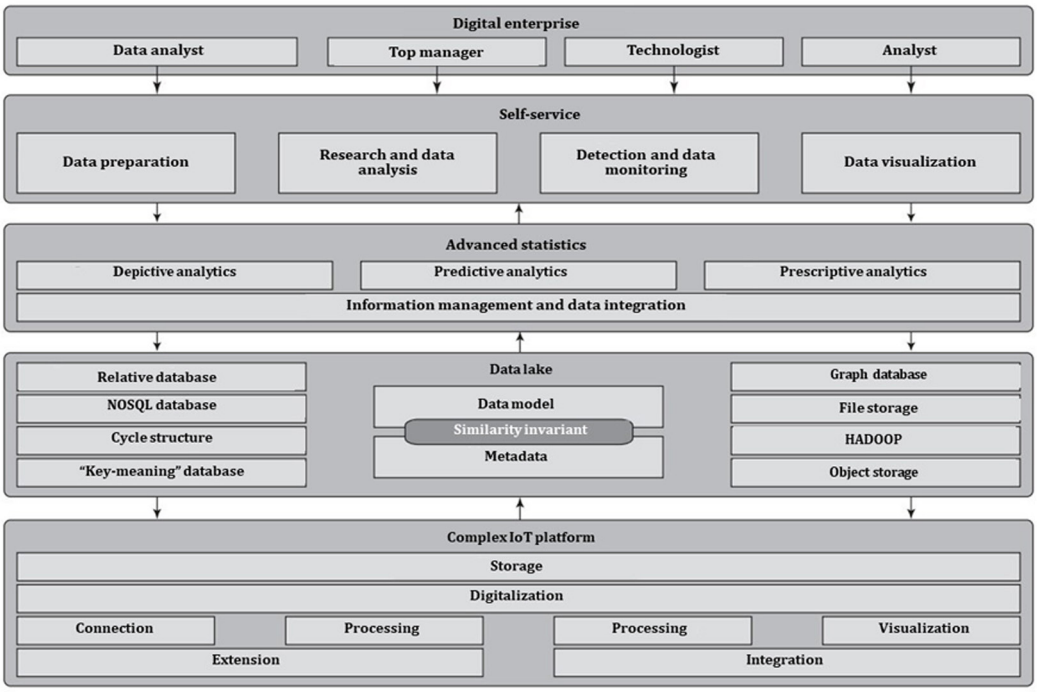

Figure 7. Target model for a cyber-resilient Internet of Things platform (IIoT/IoT)

- The variables corresponding to the first *k* columns of matrix *R* are basic (independent) in this system of dimensional invariants. The variables corresponding to the other columns of matrix *R* are dependent. Thus, the above statement defines the connection between the incident of abnormal functioning of the technological platform of the digital enterprise and the situation when one of the basic variables has the dimension "*0*". The reason for this relationship is that the situation of dimension "*0*" is impossible according to the method of building a system of dimensional invariants. This method (with complete construction of matrix *R*) is the basic one for construction of optimized algorithms of criterion checking. As input data, the algorithm uses the k×n completely exclude the computational costs associated with the late (within the pass of the *Jordan-Gauss* algorithm) rearrangement of the matrix columns;
- reduce the number of computational operations during the selection of a single matrix in the left part of R.

The algorithm requires an additional storage of permutation matrix *T* throughout the analysis phase of the digital enterprise technology platform and slightly slows down an access to matrix elements. However, the use of efficient data structures reduces the additional costs to a negligible low value. Matrix R construction allows detecting an incident of abnormal functioning of the mentioned technological platform before the end of construction (however, the criterion of semantic correctness will not necessarily be broken at the moment of adding information about a semantically wrong operator). This fact is an advantage of the modified technique in case of a large number of erroneous packages (intentionally or unintentionally generated). In this case, the receiving station L, without yet decoding the message completely, may decide to ignore it, thus freeing up its computing resources. This feature of the method can be used when including it into an echelonized system of protection against cyber-attacks of "*denial of service*" class. Under normal operating conditions, the possibility of early packet rejection does not affect the average computational effort. This is due to the fact that under such conditions the share of abnormal implementations of network protocol stack processes should tend to zero [11-15].

Thus, the following method is proposed for building an initial set of equations (2) for each model of data processing network or system *IIoT/IoT*:

- Let us take an arbitrary sampling of implementations of the process described by the model;
- Let us check the representativeness of the sample by covering all the vertices of the model control graph;
- Let us perform the model control graph conversion in order to select the computational operators from the operators of checking the conditions and organization of cycles;
- Select from the sample all unique operators that meet the above-described limitations on the type of functional relationship;
- Select variables and constants involved in the operators, supposing that they are used:

a) elements inside the array with equal size values;

b) numerical constants in pairs with different sizes (their belonging to certain classes is determined automatically at the stage of matching the size matrix).

DOI: 10.21681/2311-3456-2021-2-81-91

The transitions of the control graph, connected with calculation of complex functional dependences and corresponding to the subroutine call operators, supplement the system (4) with sets of formal parameters assignment operations. Such additional restrictions play a binding role between the values of the main body of the algorithm and the values of the subprograms. This step must be performed when building a unified model of the Internet of Things platform (IIoT/IoT) functioning (Figure 4).

4. Conclusion

The proposed passportization of data reception and transmission schemes in standard Internet of Things (IIoT/IoT) platforms on the basis of classical three-part architecture and control systems of invariants and dimensions has many advantages. These include, first of all, high selectivity and the highest quality of detection of abnormal functioning and unauthorized actions. Being developed in accordance with the principles of the system approach, such a system ensures maximum convergence of the necessary criterion of semantic correctness with the notion of semantic correctness proper.

Building a through system of identification of data processed in a computer system at various levels of the scheme of receiving and transmitting data in networks and systems IIoT/IoT, can provide a high-quality and reliable system of reverse tracing error or unauthorized action. In this case, it is possible to clearly specify the level of initial impact and the object that was the point of its application. A single variable space or mapping schemes between variables at different levels can unambiguously identify the minimum set of data potentially damaged by a security incident. Moreover, if certain combinations of controlled invariants are used, it is possible to restore damaged data in real time with a predefined corrective capacity of the system.

The integration of several different levels of systems for the detection of abnormal functions with the possibility of rejection or correction of data also has additional advantages when processing data using transactions. As early as possible (low-level) detection of data corruption in this case allows moving to an emergency branch of a transaction of a high degree of nesting, in many cases, correctly process the exceptional situation and thus successfully complete the main transaction.

The purpose of searching for an optimal set of similarity and dimensional invariants for controlled patterns of data reception and transmission in IIoT/IoT networks and systems may be to maximize the corrective capacity of similarity and dimensional invariants. The initial parameter of optimization can be the volume of additionally transmitted information or the probability of successful self-recovery of data under growing security threats.

References

1. Markov, A. Barabanov and V. Tsirlov (2018). Periodic Monitoring and Recovery of Resources in Information Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A. Kostogryzov. IntechOpen, pp. 213–231.
2. A. Barabanov and A. Markov (2015). Modern Trends in the Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08–10, 2015). SIN '15. ACM New York, NY, USA, pp. 30–33.
3. Dorofeev A.V., Markov A.S., Tsirlov V.L. APPLICATION OF OPEN DATA IN ACCORDANCE WITH INFORMATION SECURITY REQUIREMENTS: CEUR Workshop Proceedings. ISTMC 2019 - Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation "Information Systems and Technologies in Modeling and Control". 2019. C. 36-46.
4. P. Goodwin and S. Pike (2018). Five Key Technologies for Enabling a Cyber-Resilience Framework. [Electronic resource] – Access mode: https://cdn2.hubspot.net/hubfs/4366404/QRadar/QRadar%20Content/ Five%20Key%20Technologies%20for%20Enabling%20a%20Cyber% 20Resilience%20Framework.pdf?t=1535932423907.
5. A. Kott and I. Linkov (2019). Cyber Resilience of Systems and Networks, Risk, Systems and Decisions, Springer Nature Switzerland AG, [Electronic resource] – Access mode: https://doi.org/10.1007/978-3- 319-77492-3. References 411
6. A. Kott, J. Ludwig and M. Lange (2017). Assessing mission impact of cyberattacks: Toward a model-driven paradigm. IEEE Security and Privacy, 15(5), pp. 65–74. DOI: 10.1109/MSP.2017.3681068
7. O. Logan Mailloux (2018). Engineering Secure and Resilient CyberPhysical Systems, Systems Engineering Cyber Center for Research, US Air Force. [Electronic resource] – Access mode: https:// www.caecommunity.org/sites/default/files/symposium_presentations/Engineering_Secure_and_Resilient_Cyber-Physical_Systems.pdf.Bodeau D., Graubart R., Heinbockel W. and Laderman E.:Cyber Resiliency Engineering Aid-The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques (MTR140499R1PR 15-1334) (May 2015).
8. Bodeau D., Brtis J., Graubart R. and Salwen J.:Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain (MTR 130515, PR 13-3513), (September 2013).
9. Ronald S. Ross: Risk Management Framework for Information Systems and Organiza-tions: A System Life Cycle Approach for Security and Privacy (December 20, 2018).
10. Markov A., Markov G., Tsirlov V. SIMULATION OF SOFTWARE SECURITY TESTS BY SOFT COMPUTATIONAL METHODS: CRITICAL INFRASTRUCTURES: CONTINGENCY MANAGEMENT, INTELLIGENT, AGENT-BASED, CLOUD COMPUTING AND CYBER SECURITY (IWCI 2019). Proceedings of the VIth International Workshop. Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences. 2019. C. 257-261. 1
11. Petrenko Sergei (2018). Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation, ISBN 978-3-319-79035-0 and ISBN 978-3-319-79036-7 (eBook), https://doi.org/10.1007/978-3-319-79036-7 ©2018 Springer Nature Switzerland AG, part of Springer Nature, 1st ed. XXVII, 249 p. 93 illus.

12. Petrenko Sergei (2018). Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation, ISBN: 978- 87-7022-022-4 (Hardback) and 978-87-7022-021-7 (eBook) ©2018 River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 490 p. 198 illus.
13. Petrenko, S. A. and Stupin, D. D. (2018). National Early Warning System on Cyber-attack: a scientific monograph [under the general editorship of SF Boev] ©2018 "Publishing House" Athena", University of Innopolis; Innopolis, Russia, 2 ed. 440 p. 162 illus.
14. Petrenko Sergei (2019). Cyber Resilience, ISBN: 978-87-7022- 116-0 (Hardback) and 877-022-116-2 (Ebook) ©2019 River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2019, 492 p. 207 illus.
15. Petrenko Sergei and Khismatullina Elvira (2019). Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats. Software Technology: Methods and Tools 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.), eBook ISBN 978-3-030-29852-4, DOI: 10.1007/978-3-030-29852-4, Softcover ISBN 978-3-030-29851-7, 420 p. (https://www.springer.c om/gp/book/9783030298517).

Acknowledgement

The publication was carried out with the financial support of *Russian Foundation for Basic Research (RFBR)* in the framework of the scientific project *No. 20-04-60080*.