Internet of Things
for Industry and Human Applications

Internet of Things for Industrial Systems

Internet of Things
for Industry and Human Applications

Internet of Things for Industrial Systems

TRAININGS

Funded by the
Erasmus+ Programme
of the European Union

Ministry of Education and Science of Ukraine
Petro Mohyla Black Sea National University
Zaporizhzhia National Technical University
National Aerospace University "Kharkiv aviation institute"

Yu.P. Kondratenko, G.V. Kondratenko, O.V. Kozlov, A.M. Topalov,
O.S. Gerasin, S.O. Subbotin, A.O. Oliinyk, D.V. Pavlenko,
S.D. Leoshchenko, R.M. Babakov, V.S. Kharchenko, O.O. Illiashenko

Internet of Things for Industry and Human Applications

Internet of Things for Industrial Systems

Trainings

Edited by Yu.P. Kondratenko and V.S. Kharchenko

Project
ERASMUS+ ALIOT "Internet of Things: Emerging Curriculum for Industry and Human Applications"
(573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)

2019

UDC 004.415/.416::338.45](076.5)=111

I-74

Reviewers: Dr. Giuseppe Lami, ISTI-CNR, Pisa, Italy
Prof., DrS. Volodymyr Opanasenko, V.M. Glushkov Institute of Cybernetics of NAS, Kyiv, Ukraine

I-74 Yu.P. Kondratenko, G.V. Kondratenko, O.V. Kozlov, A.M. Topalov, O.S. Gerasin, S.O. Subbotin, A.O. Oliinyk, D.V. Pavlenko, S.D. Leoshchenko, R.M. Babakov, V.S. Kharchenko, O.O. Illiashenko. **Internet of Things for Industrial Systems**: **Trainings** / Yu.P. Kondratenko and V.S. Kharchenko (Eds.) – Ministry of Education and Science of Ukraine, Petro Mohyla Black Sea National University, Zaporizhzhia National Technical University, National Aerospace University "KhAI", 2019. – 143 p.

ISBN 978-617-7361-85-4

The materials of the training part of the study course ITM6 "IoT for industrial systems", developed in the framework of the ERASMUS+ ALIOT project "Internet of Things: Emerging Curriculum for Industry and Human Applications" (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

The structure of work on verification of residual knowledge in the discipline, the corresponding training material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical aspects of IoT for industrial systems are presented. The structures, models and technologies for development of industrial IoT-based systems, advanced techniques and means for design, modernization and implementation of industrial IoT-based systems, application of IoT technologies in engineering, and development and hardware optimization of control units for IoT devices in industry systems are examined.

It is intended for engineers, developers and scientists engaged in the IoT for industrial systems, for postgraduate students of universities studying in area of IoT-based systems, as well as for lecturers of relevant courses.

Ref. – 117 items, figures – 106, tables – 7.

Approved by Academic Council of National Aerospace University "Kharkiv Aviation Institute" (record No 4, December 19, 2018).

ISBN 978-617-7361-85-4

Міністерство освіти і науки України
Чорноморський національний університет ім. Петра Могили
Запорізький національний технічний університет
Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський авіаційний інститут”

Кондратенко Ю.П., Кондратенко Г.В., Козлов О.В., Топалов А.М.,
Герасін О.С., Субботін С.О., Олійник А.О., Павленко Д.В.,
Леощенко С.Д., Бабаков Р.М., Харченко В.С., Ілляшенко О.О.

Інтернет речей для
індустріальних і гуманітарних застосунків

Інтернет речей для промислових систем

Тренінги

Редактори Кондратенко Ю.П. та Харченко В.С.

Проект ERASMUS+ ALIOT
“Інтернет речей: нова освітня програма для потреб
промисловості та суспільства”
(573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)

2019

УДК 004.415/.416::338.45](076.5)=111
І-74

Рецензенти: Др. Джузеппе Ламі, ISTI-CNR, Піза, Італія

Д.т.н., проф. Володимир Опанасенко, Лауреат Державної премії України, Інститут кібернетики ім. В.М.Глушкова НАН України

Кондратенко Ю.П., Кондратенко Г.В., Козлов О.В., Топалов А.М., Герасін О.С., Субботін С.О., Олійник А.О., Павленко Д.В., Леощенко С.Д., Бабаков Р.М., Харченко В.С., Ілляшенко О.О.

І-74 Інтернет речей для промислових систем: Тренінги / За ред. Ю.П. Кондратенка та В.С. Харченка. – МОН України, Чорноморський національний університет ім. Петра Могили, Запорізький національний технічний університет, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ». – 143 с.

ISBN 978-617-7361-85-4

Викладено матеріали тренінгової частини курсу ITM6 “IoT для промислових систем”, підготовленого в рамках проекту ERASMUS+ ALIOT “ Internet of Things: Emerging Curriculum for Industry and Human Applications” (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

Наведена структура робіт з перевірки знань з курсу, відповідний тренінговий матеріал, приклади виконання завдань та критерії оцінювання. В процесі навчання наводяться теоретичні аспекти IoT для промислових систем. Вивчаються структури, моделі та технології розробки промислових IoT систем, сучасні методики і засоби проектування, модернізації та впровадження промислових IoT систем, застосування IoT технологій в інженерії, а також розробка та апаратна оптимізація блоків управління для IoT пристроїв в промислових системах.

Призначено для інженерів, розробників та науковців, які займаються розробкою та впровадженням IoT для промислових систем, для аспірантів університетів, які навчаються за напрямом IoT систем, а також для викладачів відповідних курсів.

Бібл. – 117, рисунків – 106, таблиць – 7.

Затверджено Вченою радою Національного аерокосмічного університету «Харківський авіаційний інститут» (запис № 4, грудень 19, 2018).

УДК 004.415/.416::338.45](076.5)=111

ISBN 978-617-7361-85-4

ABBREVIATIONS

CBM – Condition Based Maintenance
CoAP – Constrained Application Protocol
DM – Diagnostic Model
DT – Datapath of Transitions
FSM – Finite State Machine
GSA – Graph Scheme of the Algorithm
HTTP – HyperText Transfer Protocol
IEC – International Electrotechnical Commission
IIoT – Industrial Internet of Things
IoT – Internet of Things
ISO – International Organization for Standardization
LSTM – Long Short-Term Memory
MQTT – Message Queuing Telemetry Transport
NGFW – New Generation Firewall
PDA – Personal Digital Assistant
RNN – Recurrent Neural Network
RTM – Real-Time Monitor
SCADA – Supervisory Control And Data Acquisition
SDP – Specification of Developed Project
STD – System of Technical Diagnostics
VPN – Virtual Private Network

INTRODUCTION

The materials of the training part of the study course ITM6 “IoT for industrial systems”, developed in the framework of the ERASMUS+ ALIOT project “Internet of Things: Emerging Curriculum for Industry and Human Applications” (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)[1].

The structure of work on verification of residual knowledge in the discipline, the corresponding training material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical aspects of IoT for industrial systems are presented. The structures, models and technologies for development of industrial IoT-based systems, advanced techniques and means for design, modernization and implementation of industrial IoT-based systems, application of IoT technologies in engineering, development and hardware optimization of control units for IoT devices in industry systems are examined.

Theoretical issues for “IoT for Industrial Systems” are described in Part XIV (sections 52-55) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

The module ITMM6.1 “Structures, models and technologies for development of industrial IoT-based systems” contains two trainings and one seminar. The first training provides a technique of step-by-step development of an industrial IoT-based system, in particular, designing of the SCADA system and its integration with the cloud service IBM Bluemix. The second training covers techniques for protecting information from cyber-attacks by setting up a brand-name and using VPN technology. The seminar discusses the development of structures and models of IoT-systems in the industrial sectors. The recommendations for the preparing essays and presentations are given.

The module ITMM6.2 “Advanced techniques and means for design, modernization and implementation of industrial IoT-based systems” contains two trainings and one seminar.

---

[1] *The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*

The first training provides a method for the step-by-step development of specialized computerized system for technical diagnostics of the level sensors of the floating dock ballast complex capable of providing results of technical diagnostics to the cloud services ThingSpeak.

In the second training the method of modernization of the computerized system of the specialized pyrolysis complex is considered at the expense of the merging of the SCADA system TRACE MODE with the web-server TRACE MODE Data Center.

The seminar discusses the use of modern hardware and software of IoT-systems in the industrial sectors. The recommendations for the formation of essays and presentations are given.

The module ITMM6.3 “Application of IoT technologies in engineering” contains two trainings.

The first training provides development of specialized computerized system for technical diagnostics of the level damage to elements of aircraft of providing results of technical diagnostics to the cloud services ThingSpeak.

The second training provides development of specialized computerized system for technical diagnostics and prediction the state of the process of cutting thin-walled parts with end mills.

The module ITMM6.4 “Development and hardware optimization of control units for IoT devices in industry systems” contains one seminar and one practicum.

The first seminar is focused on industrial Internet of Things and trends of technologies in industry 4.0/5.0.

The first practicum is aimed at improving the understanding of the process of algebraic synthesis of microprogrammed finite state machine with datapath of transitions (FSM with DT).

The course is intended for engineers, developers and scientists engaged in the IoT for industrial systems, for postgraduate students of universities studying in area of industrial IoT-based systems, as well as for teachers of relevant course.

Training prepared by Professor, DrS. Yu.P. Kondratenko, Assoc. Professor, Dr. G.V. Kondratenko, Assoc. Professor, Dr. O.V. Kozlov, Ph.D. Student A.M. Topalov, Ph.D. Student O.S. Gerasin (Petro Mohyla Black Sea National University), Professor, DrS. S.O. Subbotin, Assoc. Professor, Dr. A.O. Oliinyk, Assoc. Professor, Dr. D.V. Pavlenko, Ph.D. Student S.D. Leoshchenko (Zaporizhzhia National Technical

University), Professor, DrS. V.S. Kharchenko, Dr O.O. Illiashenko (National Aerospace University "KhAI"), Assoc. Professor, Dr. R.M. Babakov (Vasyl' Stus Donetsk National University). General editing was performed by Head of Intelligent Information Systems Department of Petro Mohyla Black Sea National University, Professor, DrS. Yu.P. Kondratenko and Head of Computer Systems, Networks and Cyber Security Department of National Aerospace University "KhAI", Professor, DrS. V.S. Kharchenko.

The authors are grateful to the reviewers, project colleagues, staff of the departments of academic universities, industrial partners for valuable information, methodological assistance and constructive suggestions that were made during the course program discussion and assistance materials.

ITMM6.1. Structures, models and technologies for development of industrial IoT-based systems

Prof., DrS. Yu.P. Kondratenko, Assoc. Prof., Dr. G.V. Kondratenko, Assoc. Prof., Dr. O.V. Kozlov, PhD Student A.M. Topalov, PhD Student O.S. Gerasin (PMBSNU)

Training 1

MAIN STAGES OF INDUSTRIAL IOT-BASED SYSTEM DEVELOPMENT

The aim of the training: to study the technique of step-by-step development of an industrial IoT-based system, in particular, designing of the SCADA system and its integration with the cloud service IBM Bluemix.

Training participants: lecturers, scientists, technical staff, students and post-graduate students of the department (faculty, institute) of the university; developers, engineers, trainees of industrial objects.

To complete the training, it is necessary to carefully read the theoretical foundations given below. For a deeper acquaintance with the material, it is necessary to use the technical literature, to which references are given in the instructions. If during the study of the discipline there will be questions that are not answered in this training or technical literature, it is necessary to consult a leading lecturer.

Theoretical information

The emergence of cloud computing in industrial automation has allowed to expand the capacity of existing SCADA systems, to increase the capacity of processing of incoming information, to solve the problem of a small amount of memory as well as to improve visualization. Automating the control system based on IIoT also gives the opportunity to create various documents, reports on the state of the technological process and remotely control the process [1-3].

To study the problems of designing and researching of automated industrial systems using IIoT, let us consider a two-tier system of

interaction between SCADA and the IoT cloud. In this case, a two-tier system has a lower level, which is designed to implement a local control system based on SCADA TRACE MODE 6. In turn, the upper level of this system is implemented on the Watson IoT Platform on IBM Bluemix [4-7].

The main task of this system is to process the conditional signal at the lower level and transmit it for further processing to the upper level.

The input value of the signal varies in the range: [0-100]. It is necessary to ensure the range of the signal as [0-5]. The signal is processed according to the equation [8]:

$$Y = K \cdot X + Z,$$

where Y is the result of converting; X is the input value of the signal; K is the multiplier; Z is the displacement.

The structure of the system under study is presented in Fig. 1. The implementation of this structure can be based on various software and hardware automation tools. In this case, training stand consists of: the first computer with an installed SCADA TRACE MODE; interface converter - ICP DAS I-7520 module; analog output module - ICP DAS I-7021; analog input module - ICP DAS I-7017; IoT controller - WISE 5231, connected to the Internet; IoT cloud - Watson IoT Platform on IBM Bluemix; second computer, connected to the internet [9-12].

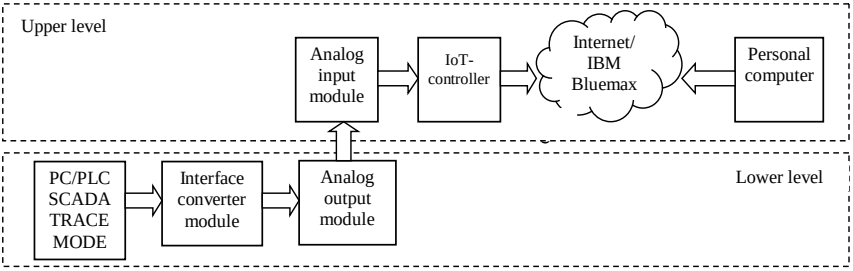

Fig. 1.1 – Two-tier structure of an automated control system based on IIoT

SCADA-TRACE MODE system of AdAstraResearch Group, Ltd (Russia) is a high-tech software system for automating technological processes, remote control, telemechanics, dispatching, resource

accounting and building automation. It is an integrated information system for industrial production management, combining in a single whole products of the class SOFTLOGIC-SCADA and economic modules T-Factory HMI-MESEAM [4].

The TRACE MODE 6 software package can be divided into 3 parts:

– integrated project development environment (IE) - a single software shell containing all the necessary tools for project development. The result of the development of the project in the IE is the creation of files containing the necessary information about the algorithms of the ACS. These files are then placed on hardware (computers and controllers) and executed under the control of the TRACE MODE execution modules [4, 6, 10];

– executive modules (real-time monitors, RTMs) - software modules for various purposes, which performed the real-time control of the components of the project on individual computers or in controllers;

– exchange drivers - drivers used by TRACE MODE monitors to communicate with devices, which exchange protocols are not built into the monitors.

The main connecting elements in project development in the TRACE MODE system are “channels”. Channel is the basic concept of a system. Data from external devices is recorded in the channels. Data from the channels are sent to external devices and displayed in various forms on the monitor screen. The operator enters control data into the channels. Values from channels are recorded in archives, operational reports and in all generated documents., The data conversion is performed in the channels. The control of the information displayed on the screen, sound effects, archives, etc., and the entire system can be performed by means of changing the values on the system channels [3].

To transmit data through the Internet of Things technology to the Watson IoT Platform on IBM Bluemix cloud, the Wise 5231 controller is used, that is a new generation intelligent Web controller with the Internet of Things (IoT) function and a built-in data logger, designed for remote control and monitoring of devices and sensors in industrial applications. Programming of this controller does not require installation of special software. Settings changing and programming is performed through a common WEB browser. To control and monitor I/O channels in the real time mode, the controller is compatible with a variety of communication protocols. Support for the Modbus TCP/RTU protocol ensures the interaction of the module and its associated devices with the

SCADA system. In addition, SNMP and MQTT protocols are supported for quick integration with MES (Manufacturing Execution System) and others [4].

As the IoT technology the IBM Bluemax is used, which supports several programming languages and development environments, as well as DevOps-style tools for building, running, deploying and managing applications in the cloud. IBM Bluemax is based on Pivotal's Cloud Foundry technology and operates on the basis of the SoftLayer infrastructure [7].

Watson IoT Platform on IBM Bluemix provides [8]:

– connecting and managing of devices, networks and gateways;

– information management, storage and archiving, metadata management, reporting, data streaming, analysis and transformation, unstructured data management;

– analytics, extraction of new knowledge, discoveries from available information using real-time analytics, predictive and cognitive analytics;

– risk management, security analytics, data protection, audit/ logging, firmware updates, certificates management.

Training implementation

In accordance with the described structure and composition of the elements of the project, let’s consider the sequential implementation of the task.

Run the TRACE MODE 6 program (tmdevenv.exe file). To create a new project, click on the “New” line in the “File” menu. The created project will become as shown in Fig. 1.2. Save the created project using “Save” or “Save As” in the “File” menu.

Then, depending on the operating system and the type of PLC/PC in which the project files will be installed, one of the following types of nodes is selected: RTM, MicroRTM, Logger, EmbeddedRTM, NanoRTM, Console, EmbeddedConsole. Let's create an RTM node for work within the MS Windows OS at the automated workplace (AWP) of the operator. To do this, call the context menu from the string “System” in the project navigator. In the context menu, select the line “Create Node”. Then, select RTM among the proposed types of nodes. The project navigator in the “System” section will display the created node. An example of the created node with the name “RTM_1” is shown in Fig. 1.3.

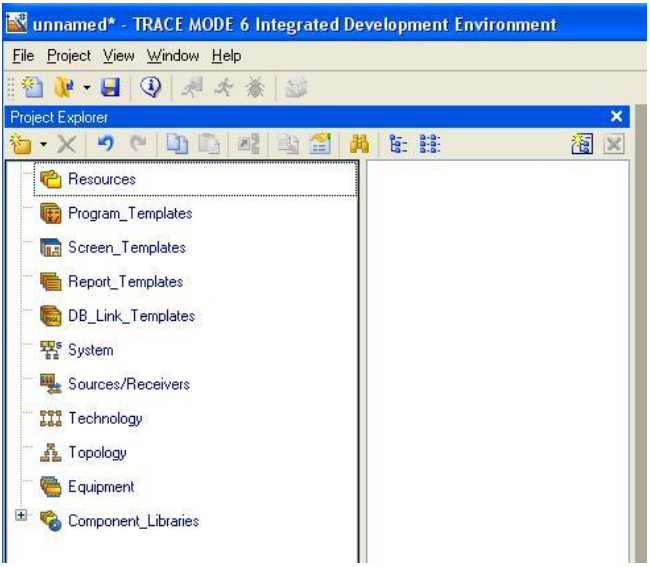

Fig. 1.2 – TRACE MODE new project

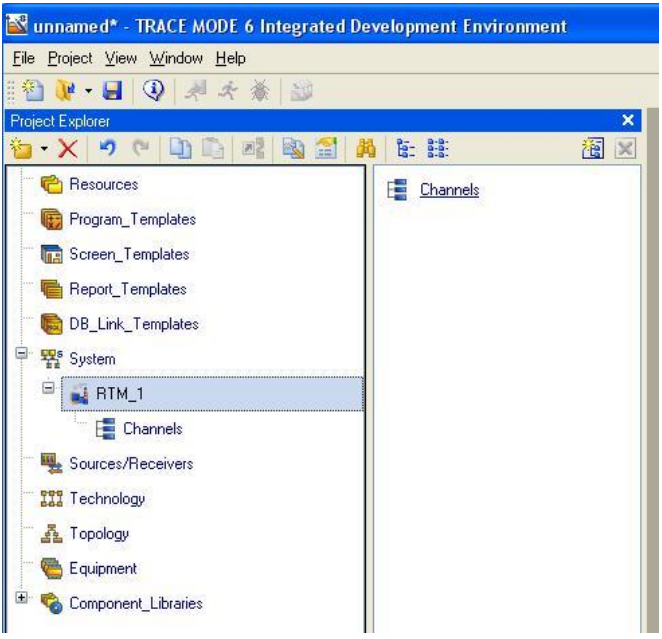

Fig. 1.3 – Created “RTM_1” node

Next, it is necessary to create channels to implement the movement of information in this project. Create two channels: the first for the original signal, the second for the signal after program processing.

Select the “Channels” group of the “RTM_1” node. Call the context menu. In the context menu that appears, select the line “Create Component”. Among the suggested components, select “FLOAT_channel”. Thus, two channels will be created, which are shown in Fig. 1.4.

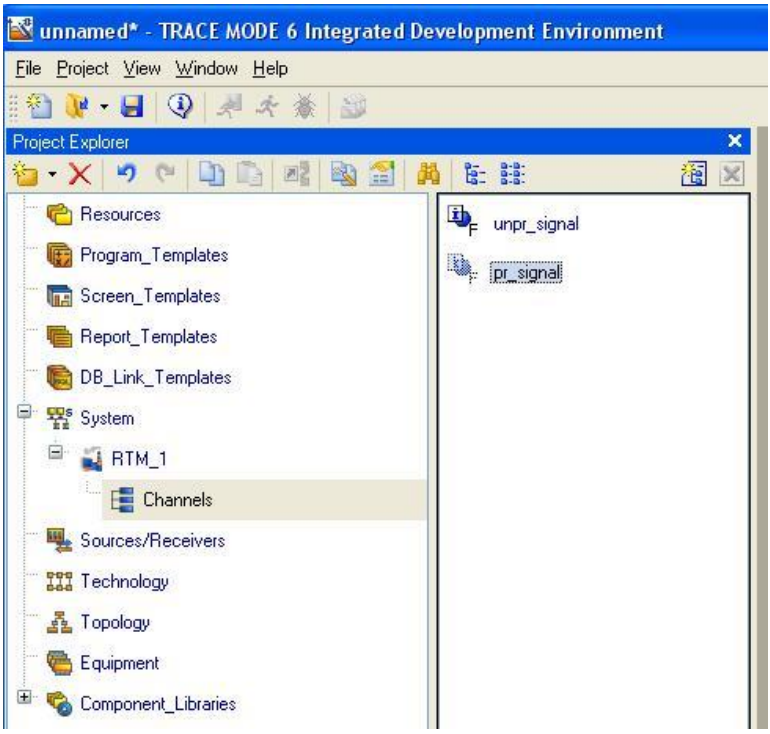

Fig. 1.4 – Creating project channels

Next, it is necessary to create the “Screen” component used to form the human-machine interface of the operator.

In the “RTM_1” node, call the context menu. In the context menu, select the line “Create Component”. Among the proposed components, select the “Screen”. At the end, a blue screen will be created (the color is set to the default of the program) (Fig. 1.5).

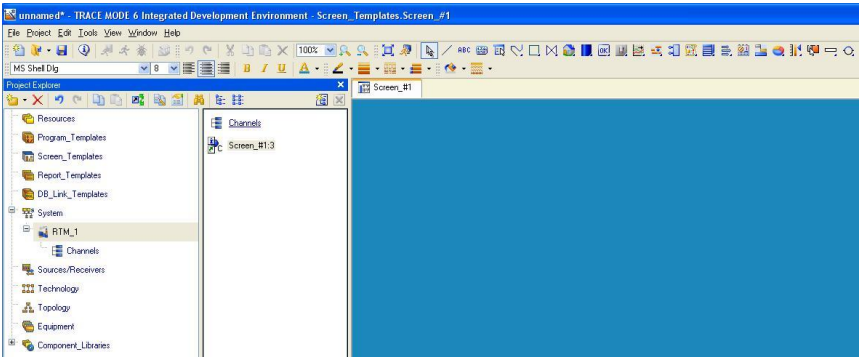

Fig. 1.5 – Created screen

Let's display the processed signal data flowing in real time on the screen in this project. For these purposes create a trend.

To create a trend, click on the icon with the inscription "Trend" (first find it on the graphic panel). To place a trend on the screen, left-click where one of the corners of the trend should be located. Move the cursor to the position where the opposite corner of the trend should be located and click the left mouse button. Select the created trend, the trend property window will open. Initially, the "Object Properties" tab will be opened. In the "Caption" field, enter the text you want to display as the title. Click on the "Curves" tab. Select the line "Curves" and call the context menu. In the context menu that appears, select "Curve". In the "Title" field that appears, enter the name of the curve created. In the "Max value" enter the value of the upper limit of the range, in the field "Min value"- the lower limit of the range. The trend will take the form shown in Fig. 1.6.

To create a curve argument in trend properties, click the "Binding" field. This opens the window shown in Fig. 1.7. Next, click the "Create Argument" icon. In the name column an arbitrary name for this argument can be specified. It is advisable to avoid spaces in argument names. In the type column indicate the type of the argument: "IN", and in the data type column indicate: "Real".

Theoretical issues for "IoT for Industrial Systems" are described in Part XIV (sections 52-55) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

Fig. 1.6 – Created trend

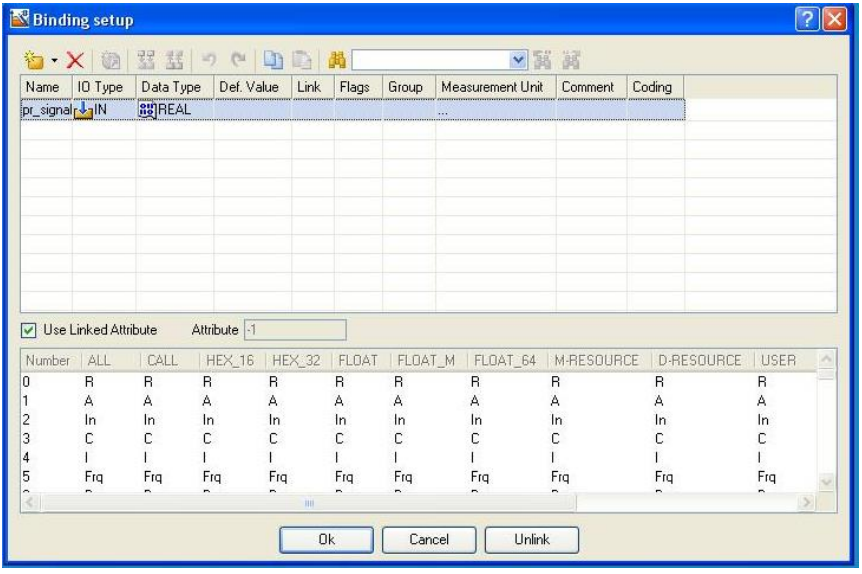

Fig. 1.7 – Created trend argument

Let's bind the trend argument to the "pr_signal" channel as follows. Open the properties of the screen and go to the category of "Arguments". In the "Link" column, a binding is made to a specific value of the channel (Fig. 1.8), where the required channel and its values (attribute) are selected.

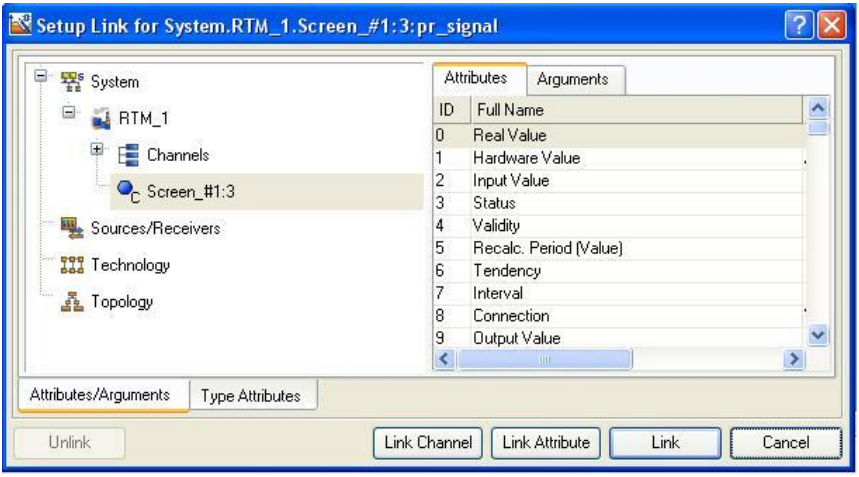

Fig. 1.8 – Binding the argument to the channel

Imitation of the original signal will be done by generating signals.

Create a group "Generators". To do this, select the line "Sources/Receivers" of the project navigator and call the context menu. In the menu that appears, select the line "Create Group". Among the proposed groups, select "Generators". Call the context menu from the created group. In the context menu, select the line to create a component. Among the proposed generators, select the required type of generator (Fig. 1.9). With the help of the drag-and-drop mechanism, transfer the created signal source to the "unpr_signal" channel in the "Channels" group.

The signal processing ($Y = K \cdot X + Z$) will be performed using the program in the ST language. In this case, the source signal has a range [0 - 100], respectively, to receive a signal with a range [0 - 5], $K = 0.04$, $Z = 1$.

In the "RTM_1" node, create the "Program" component. Open it and go to the tab "Arguments" and "Local Variables". Then, create the necessary arguments for the work (Fig. 1.10) and local variables

(Fig. 1.11) and assign the arguments to the channels of the "RTM_1" node using the program properties.

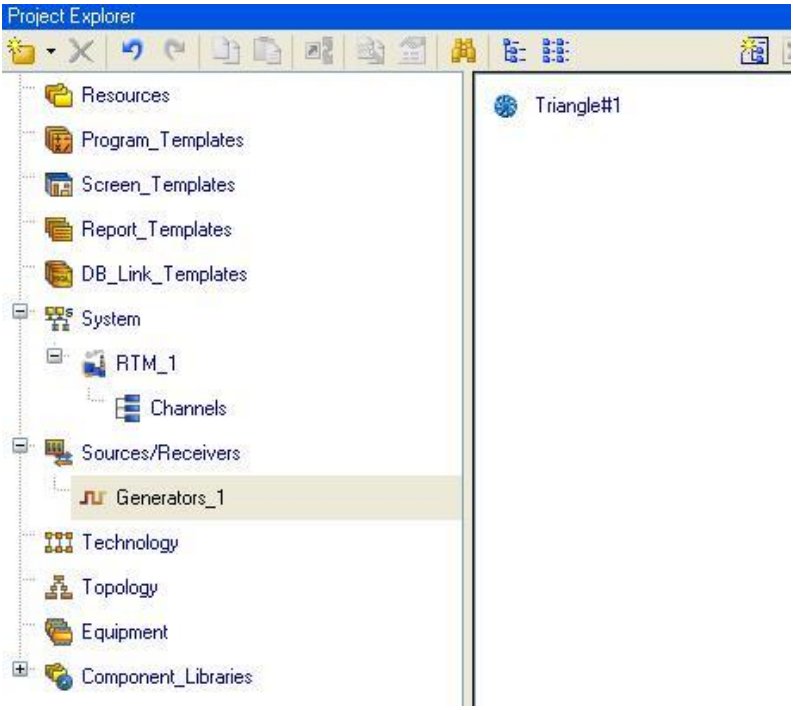

Fig. 1.9 – Created generator of the tested signal

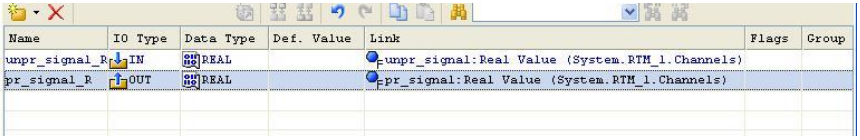

Fig. 1.10 – Creation of arguments of the program

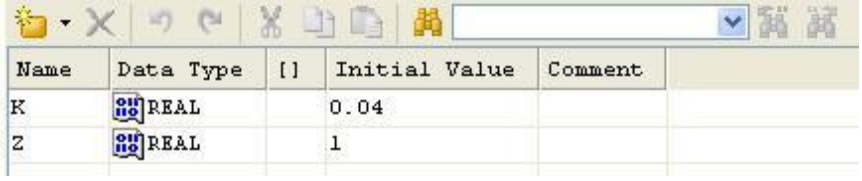

Fig. 1.11 – Creation of local variables of the program

Next, activate the line “Program” and a window appears with a choice of programming language. Select ST and write the next program (Fig. 1.12).

```
PROGRAM
    VAR_INPUT unpr_signal_R : REAL; END_VAR
    VAR_OUTPUT pr_signal_R : REAL; END_VAR
    VAR K : REAL := 0.04; END_VAR
    VAR Z : REAL := 1; END_VAR

    pr_signal_R=((unpr_signal_R*K)+Z);

END_PROGRAM
```

Fig. 1.12 – Program listing

To output the processed signal, we use the analog output module ICP DAS I-7021.

Let’s introduce in the created project module I-7021. Preconfigure the module using the configuration utility supplied with the module, set the output format, assign it a number in the RS-485 network equal to 1 and set the data exchange format to 57600,n,8,1 without checksum. Connect the module to the computer COM1 port through the I-7520 automatic interface converter.

Next, it is necessary to open the “Sources/Receivers” layer and create the “Distributed_DCO_(DCS)” group in it through a PC. In the “Distributed_DCO_(DCS)” group, create the “I-7000_#1” group (Fig. 1.13).

Open the created group “I7000_#1” and create the group “I-7021#1” in it. Select component “AO#1” and go into edit mode of its attributes. All the main attributes that set the module settings are left by default: Port number 0 corresponds to the COM1 of the computer, the module address in this case is 1, the “Channel” and “Slot” attributes are not specified for the selected module, Checksum is absent, Signal type is Output.

To create a channel in the “RTM_1” node associated with the ICP DAS I-7021 module, it is necessary to select the “AO#1” component in the group “I7021#1” and drag it to the group “Channels” to the “pr_signal” channel using the drag-and-drop mechanism.

Fig. 1.13 – Created group of I-7000 modules

Creating and configuring a COM port. Open the context menu of the “RTM_1” node and select the line “Create Group”, then click “COM_ports” (Fig. 1.14).

Edit the newly created “COM_Port#1” as follows: leave all attributes set to default, changing only the speed to 57600.

Save the project and execute the save procedure for the real-time monitor. Start the real-time monitor (rtc.exe), open the project with the .dbb extension and launch it (Fig. 1.15).

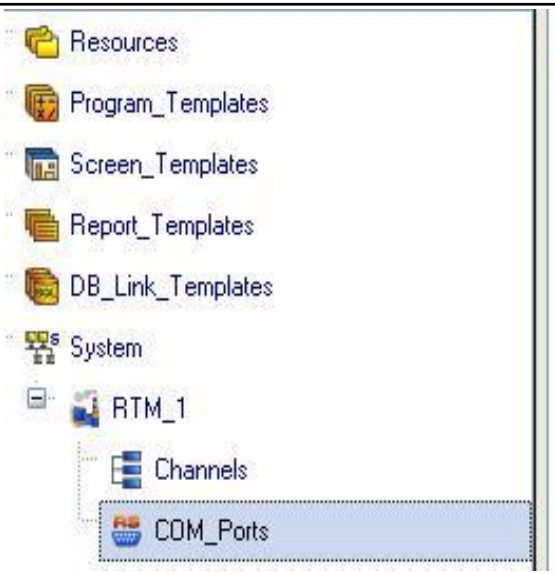

Fig. 1.14 – Created COM port

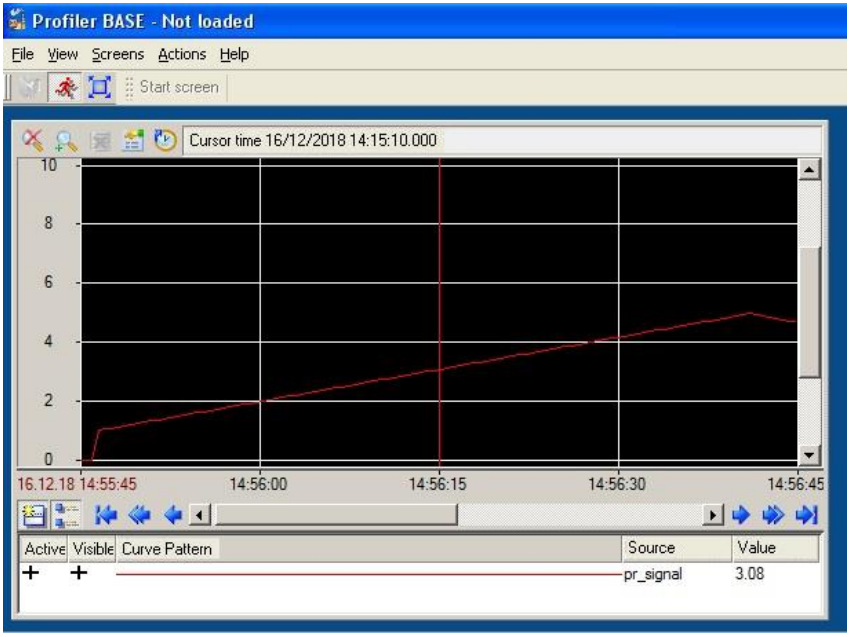

Fig. 1.15 – Launched SCADA project

Let’s turn to the settings that are required to work with the Watson IoT Platform on IBM Bluemix.

First it is necessary to configure the IoT controller.

Open the WEB-browser and enter the controller's IP in the address bar. In the authorization window enter the password “admin” (Fig. 1.16).

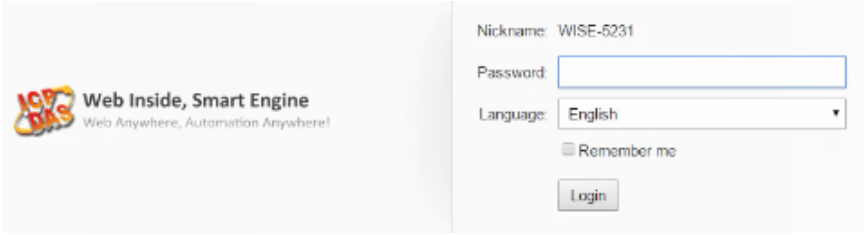

Fig. 1.16 – WISE-5231 registration

After authorization opens the main page. In the “Com Port Interface Setting” it is necessary to configure the parameters of ports and communication protocols. An analog I-7017 communication module is connected to COM3, respectively, let's set the DCON Master operation mode. After making changes, save them using the “Save” button (Fig. 1.17).

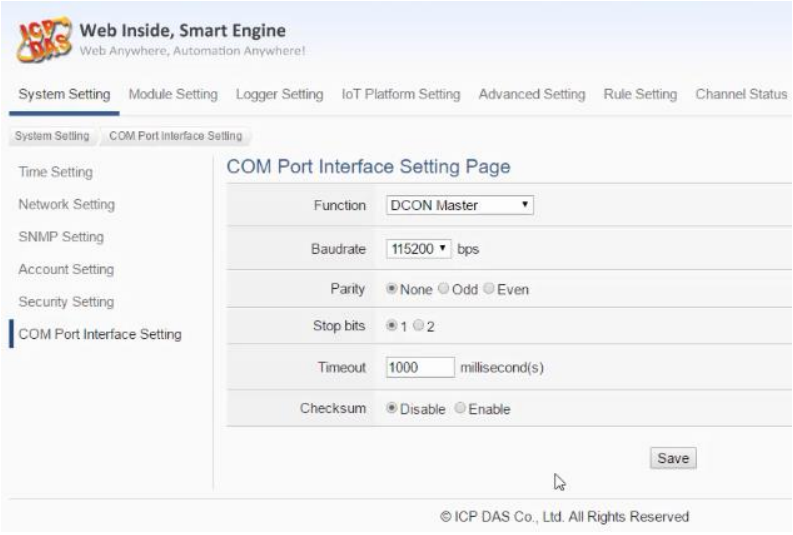

Fig. 1.17 – Configured Serial Port

COM port settings are configured. Now go to the “Moduls Setting” page to configure the I-7017 input module. In the “Remote I/O Module Setting” window go to the previously configured COM port. In the configuration table of the module, connected to the COM port, click on the icon in the form of a magnifying glass. In the window that appears, click Scan (Fig. 1.18).

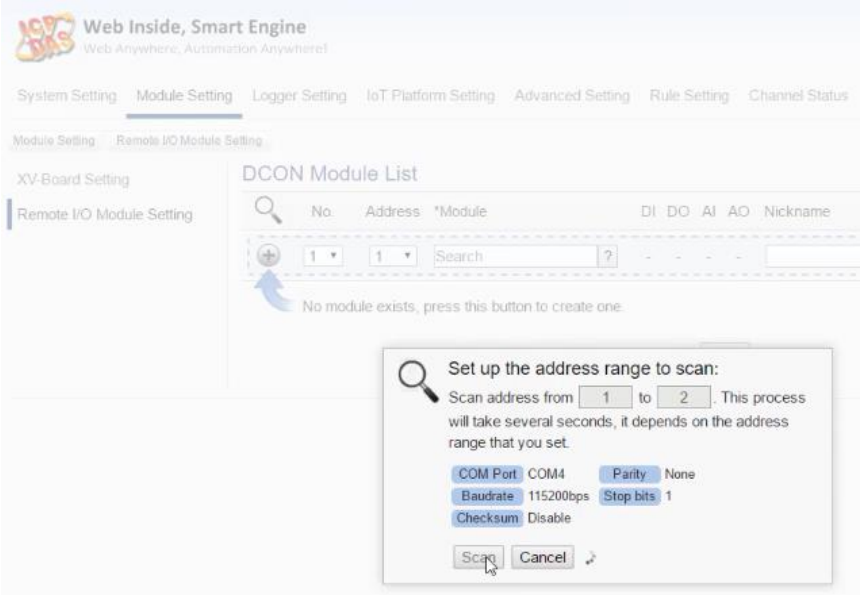

Fig. 1.18 – The address range setting window for scanning

After the scan operation is completed, the “Setting” button will appear, after clicking of which, the I-7017 module settings window will open. Let's call the 4th channel “Input Signal”, set the measurement range from -5V to 5V. In the “Remote I/O Module Setting” window save the changes using the “Save” button.

Set up the connection to the IBM cloud. Go to the “IoT Platform Setting” submenu and select “IBM Bluemix Platform Setting”. To activate it, put a tick in the “Enable” field (Fig. 1.19).

Let’s configure directly the Watson IoT Platform on IBM Bluemix.

It is necessary to open a new browser tab and go to the IBM Watson IoT Platform page (Fig. 1.20).

Fig. 1.19 – IBM Bluemix Platform Setting window

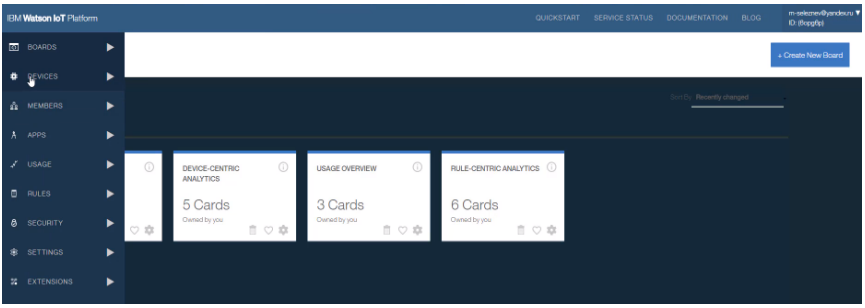

Fig. 1.20 – IBM Watson IoT Platform page

Go to the “Devices” tab and click “Add Device”, in the “Choose Device Type” window select “controller”, click “Next”. In the “Device ID” window select “WISE-5231”, click “Next” three times and then click “Add”. Then, transfer the information opposite the lines “Organization ID”, “Device Type”, “Device ID”, “Authentication Token” into the corresponding fields of the tab “IoT Platform Setting” (website “WISE ICP DAS” → “IoT Platform Setting” → “IoT Platform Setting”). Click “Add new Publish Message” (Fig. 1.21).

In the next window in the section “Channel Data” opposite “Ch” change to “4”, select “Periodical Publish”, change the name to the “Signal”, in the “Event ID” also enter the “Signal”, click “OK” Press “Save” and save the general settings in this tab.

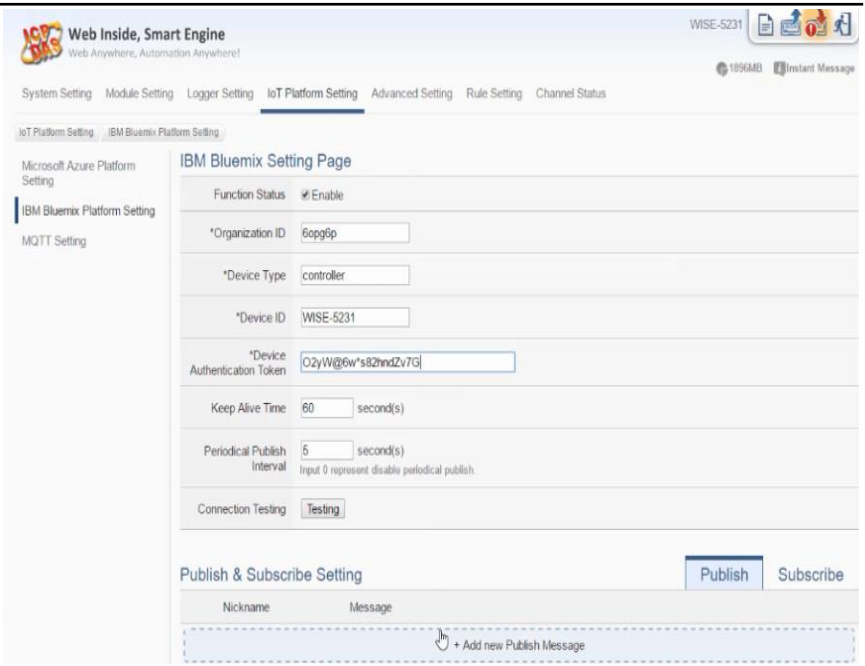

Fig. 1.21 – WISE-5231 pairing with IBM Watson IoT Platform

Return to the “IBM Watson IoT Platform” website, on the left in the panel select the “Boards” tab and click “Create New Board”. In the “Board Name” field enter “WISE-5231”, click “Next” and then click “Submit”.

Go to the settings “WISE-5231” in the cloud “IBM Watson IoT Platform”. Click on the appropriate device “WISE-5231”. Click “Add New Card”, in the window that appears select “Line Chart” (Fig. 1.22). Then, select “WISE-5231” and click “Next”.

Then click “Connect New Data Set” and a window appears in the “Event” tab. Then, select “Signal”, select “Value” in “Property”, change the name to “Signal”, select “V” in the “Unit” tab and click “Next”. Select the size of the chart “L” and click “Next”. Choose the color of the frame of the graph, enter the header and click the “Submit” button to place it in the module menu (Fig. 1.23).

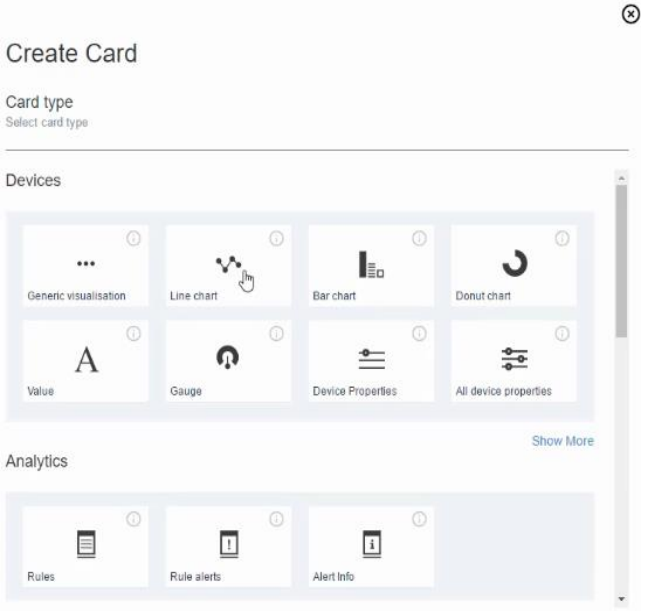

Fig. 1.22 – Choice of information visualization

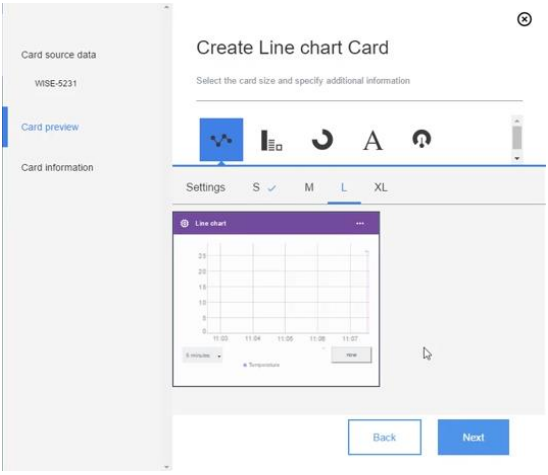

Fig. 1.23 – Line graph of information output

On the created chart, the processed signal will be displayed according to the training task.

Tasks for extracurricular work

Process the conditional signal in the SCADA system and transfer it for further processing to the IBM Watson IoT Platform. Variants of signal ranges and types are presented in Table 1.1.

Table 1.1 – Tasks for the variants for extracurricular work

Variant number	Signal form	Input signal range	Output signal range
1	sawtooth	[0 - 100]	[0 - 5]
2	triangular	[0 - 100]	[0 - 5]
3	sine wave	[0 - 100]	[0 - 4]
4	sine wave	[0 - 100]	[0 - 5]
5	triangular	[0 - 100]	[0 - 5]
6	sine wave	[0 - 100]	[0 - 5]
7	triangular	[0 - 100]	[0 - 3]
8	sawtooth	[0 - 100]	[0 - 5]
9	sawtooth	[0 - 100]	[0 - 5]
10	sawtooth	[0 - 100]	[0 - 3]

Report

The report should contain:

- title page with the name of the training work and the contractor;
- aim of the work;
- problem statement according to the variant;
- the progress and results of the study in graphical form;
- analysis of the results and conclusions.

All materials of the report should be printed, billed, the pages should be numbered.

Test questions

1. What is the IBM Watson IoT Platform?
2. SCADA TRACE MODE and its components?
3. What is the most important connecting element in the development of SCADA TRACE MODE projects?
4. What means for information displaying in the IBM Watson IoT Platform do you know?
5. What types of signals are used in this work?

Recommended literature

1. S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things*. Switzerland: Springer International Publishing, 2017.

2. R. H. Weber and R. Weber, *Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2010.

3. "The use of an integrated platform for creating TRACE MODE SCADA and Production Management: Theory and Practice," 5th int. conf., 2005.

4. A. Kor, C. Pattinson, M. Yanovsky, and V. Kharchenko, "IoT-Enabled Smart Living," in *Technology for Smart Futures*, M. Dastbaz, H. Arabnia, and B. Akhgar, Eds., 2017, pp. 3-28.

5. F. Paternò and C. Santoro, "A design space for end user development in the time of the internet of things," in *New Perspectives in End-User Development*, F. Paternò and V. Wulf, Eds., 2017, pp. 43-59.

6. B. Ahlgren, M. Hidell, and E. Ngai, "Internet of Things for Smart Cities: Interoperability and Open Data," in *IEEE Internet Computing*, vol. 20, no. 6, 2016, pp. 52-56.

7. Y. Kondratenko, O. Kozlov, O. Korobko, and A. Topalov, "Internet of Things Approach for Automation of the Complex Industrial Systems," *13th International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI'2017, CEUR-WS*, pp. 3-18, May 2017.

8. D. Uckelmann, M. Harrison, and F. Michahelles, *Architecting the Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2011.

9. D. Giusto, A. Lera, G. Morabito, and L. Atzori, *The Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2010.

10. B. Payam, W. Wang, C. Henson, and K. Taylor, "Semantics for the Internet of Things: early progress and back to the future," in *International Journal on Semantic Web and Information Systems*, vol. 8, no. 1, 2012, pp. 1-21.

11. E. Delgado, *The Internet of Things: Emergence, Perspectives, Privacy and Security Issues*. New York: Nova Science Publishers, 2015.

12. M. Bottone, F. Palumbo, G. Primiero, F. Raimondi, and R. Stocker, "Implementing virtual pheromones in BDI robots using MQTT and Jason," *5th IEEE International Conference on Cloud Networking*, pp. 196-199, October 2016.

Training 2

FIREWALL AND VPN TECHNIQUES IN IOT-BASED INDUSTRIAL SYSTEMS

The aim of the training: to study technics of information protection from cyber-attacks by setting up a Firewall and using VPN technology.

Training participants: lecturers, scientists, technical staff, students and post-graduate students of the department (faculty, institute) of the university; developers, engineers, trainees of industrial objects.

To complete the training, it is necessary to carefully read the theoretical foundations given below. For a deeper acquaintance with the material, it is necessary to use the technical literature, to which references are given in the instructions. If during the study of the discipline there will be questions that are not answered in this training or technical literature, it is necessary to consult a leading lecturer.

Theoretical information

The amount of data for transmission and storage has been multiplied with the advent of the "Internet of Things". At the same time, there is a risk of information loss and hacking of the system, which entails the possibility of identity theft (when one device connects to another to receive or transmit data each time). Fortunately, there are already ways to solve this problem. To get started, just configure a network of devices and routers using a VPN and firewall [1-3].

Firewall is a network security appliance that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a set of security rules [4, 5].

Firewalls have been used as a first line of defense for networks for more than 25 years. They put a barrier between secure, controlled internal networks, that can be trusted and unreliable external networks connected to the Internet [1, 6, 7].

Firewall can be hardware, software or mixed type [1].

There are several types of firewall applications, the most common types are: proxy server; firewall with session state monitoring; UTM firewall; new generation firewall (NGFW); NGFW with active threat protection [8-10].

VPN technology is also used to protect transmitted data. VPN is a virtual private network that uses several different protocols, including upper layer encryption, to provide a continuously secure point-to-point connection. It also masks the user's IP address by redirecting traffic through a network of dedicated servers, so that the user can hide his location, ensure the confidentiality of data and protect against attack [1].

VPNs cannot solve all security problems, but they offer a reliable solution to several basic problems in networks. Virtual private networks can create a private network on the Internet through which your IoT devices can communicate securely with each other, as well as safely connect to the Internet. This is especially important for the security of the Internet of things due to the low computing power of many devices. Typically, an IoT device does not need much computational power because it needs to perform only its small task. This means that it is impractical for each device to use serious encryption software, however, without encryption, devices become vulnerable to hacking when they are connected to the Internet. When devices are connected via VPN, all connections are encrypted and forwarded through a secure tunnel directly to the destination [2-4, 8].

Thus, one of the many benefits of using VPN is encryption. Encryption is a standard part of a VPN service and ensures that even if the connection is broken and/or information is stolen, data recognition will become impossible. Another significant advantage that is important for IoT networks is changing the IP address and the user’s location. VPN hides the IP address and, thus, misinforms the attackers about the actual location of the user [6, 10].

There are several types of VPNs: The most common types are PPTP VPN, Site-to-Site VPN, L2TP VPN, IPsec, SSL, MPLS VPN, and Hybrid VPN. Let’s consider them in more detail [4].

Firewalls and virtual private networks are often used together. Many firewall products provide encrypted firewall tunnels. In particular, application gateways hide an IP address by encapsulating one IP packet in another. This is tunneling related to VPN [7].

Firewalls control access to corporate network resources and establish trust between the user and the network. An example of such a network is presented in Fig. 2.1 [2].

A firewall on each network controls access to resources in the network. However, the data transmitted between the two sites are still vulnerable to attack when they cross the Internet [5].

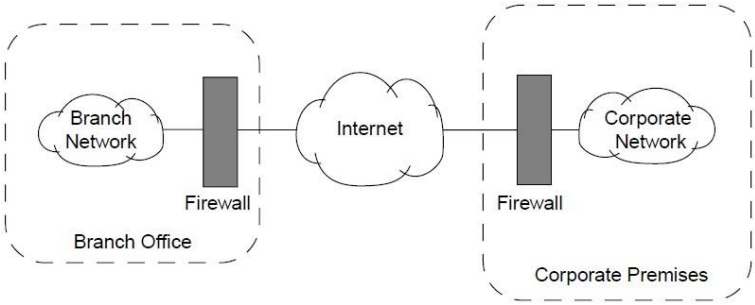

Fig. 2.1 – Network configuration with Firewall

On the other hand, a VPN is created to ensure confidentiality between two networks. The combination of firewall and VPN establishes trust and ensures confidentiality between the two networks. This approach provides greater security than the use of firewalls in both sites or VPN between two networks. Fig. 2.2 shows an example of using a VPN tunnel between two firewalls [3].

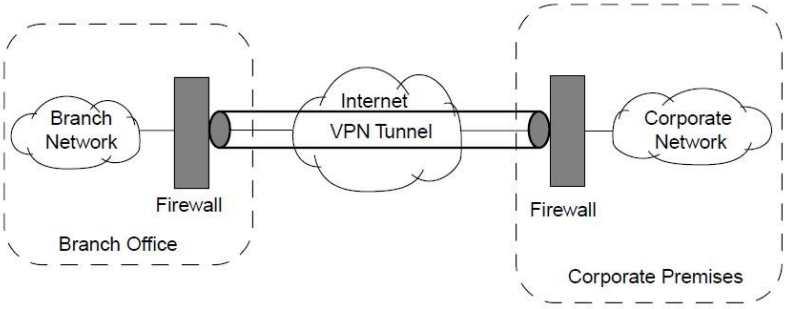

Fig. 2.2 – Network's configuration using VPN and Firewall technologies

Firewall products provided only firewall security services in the past. However, many new firewall products support VPN features now. As stated earlier, firewall and VPN functionality is required to ensure effective security controls in IoT systems [2, 7].

Theoretical issues for "IoT for Industrial Systems" are described in Part XIV (sections 52-55) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

Training implementation

All actions will be carried out on a computer with the Windows 7 operating system in this training. First, let's look at how to configure Windows Firewall settings, and then proceed to create a virtual private network.

Windows Firewall configuration

To configure Windows Firewall settings, follow the next steps.

Go to the firewall settings "Windows Firewall" (bottom "Start"→ item "Control Panel" → "Windows Firewall"). As a result, the main menu to configure the firewall will be available (Fig. 2.3).

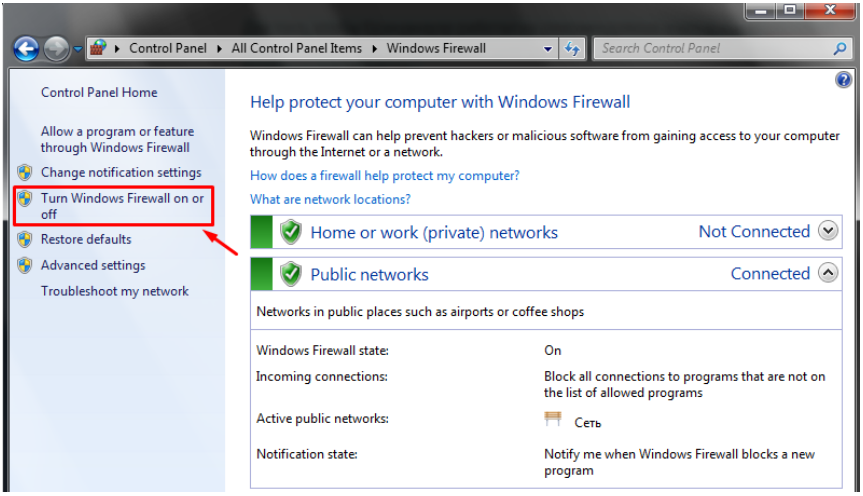

Fig. 2.3 – The main menu to configure the firewall settings

Click on the "Turn Windows Firewall on or off" menu item in order for the firewall to work on the settings recommended by Microsoft. Mark the items highlighted in the screenshot and click "OK" (Fig. 2.4.).

Some programs or applications can be blocked after activating the firewall. Users will add some programs to blocking exceptions for this purpose. Go back one step to the main firewall settings menu and go through the tab "Allow a program or feature through Windows Firewall". Put here checkmarks in front of each program that will be added to the exceptions (Fig. 2.5).

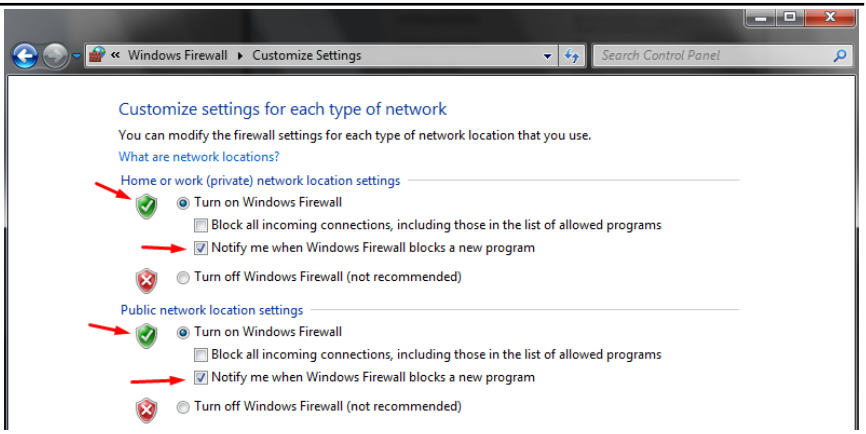

Fig. 2.4 – “Customize Settings” menu for each type of network

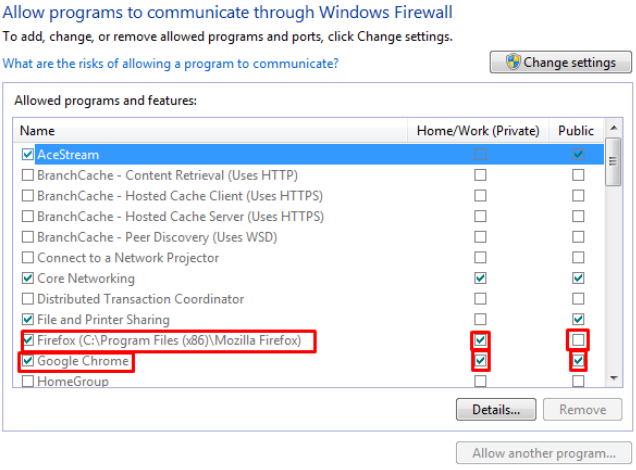

Fig. 2.5 – The procedure for adding programs to blocking exceptions

The firewall needs to further configure for working in the Windows 7 system in a heightened security environment. Go back one step to the main firewall settings menu and go to the “Advanced settings” tab. Additional parameters are configured, such as connection rules (may be created own) and a domain profile in the opened window. Select “Inbound Rules” in the list on the left. Click on the “New Rule” panel in the right panel to add a traffic processing rule (Fig. 2.6).

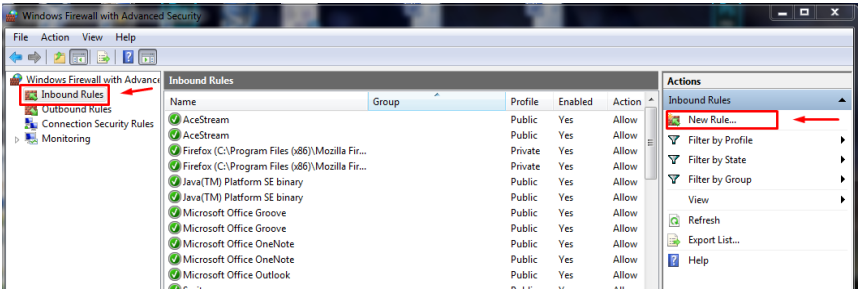

Fig. 2.6 – Window with all connection rules

The “New Inbound Rule Wizard” window opens. It is necessary to specify the type of the rule – “Custom” and go to the next step on the “Next” button (Fig. 2.7).

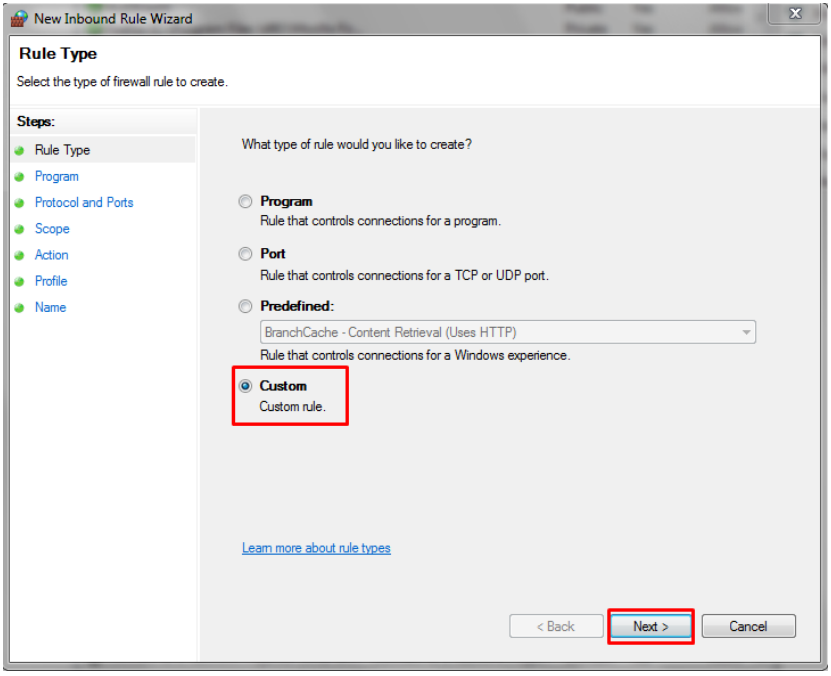

Fig. 2.7 – Connection Rule Settings Window

There is no need to change the settings in the “Program” and “Protocol and Ports” points, so leave them by default.

In the “Scope” point, set the “Any IP address” switch to “These IP addresses” and click on the “Add” button. In the opened window specify “This IP address or subnet” and click “OK”. After that, click “Next” after entering the required values. Then leave the preset value “Allow the connection” in the item “Action” and click “Next”.

Further select a profile to which the configured rule will belong in the “Profile” item. Since the setting is performed for a computer connected to the home network of the Internet center, it is enough to leave a tick in front of the “Private” profile (apply when the computer is connected to a private network).

So, specify the name of the rule and add an explanatory “Description” in the item “Name”. Finish creating the rule by clicking the “Finish” button.

Now the created rule is displayed in the “Inbound Rules” view window (Fig. 2.8). There is no additional actions are required to apply the setting in the latest versions of Windows. The configuration of the firewall can be considered as completed.

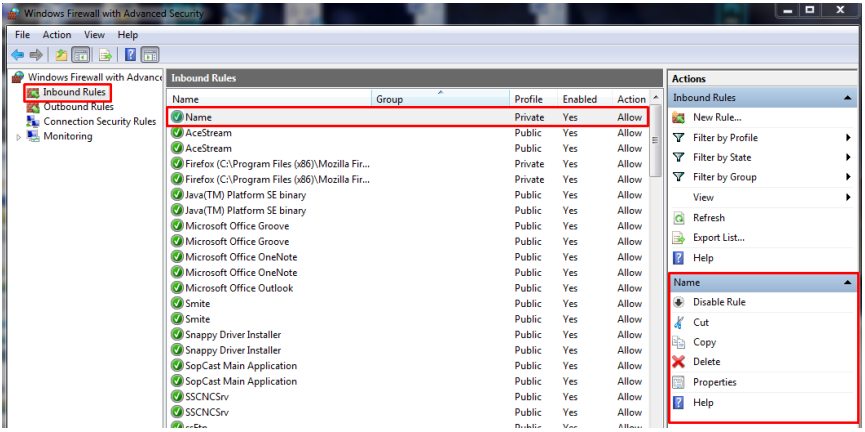

Fig. 2.8 – All connection rules window with new rule added

VPN connection configuration

To configure VPN connection settings, follow the next steps.

Go to the “Network and Sharing Center” VPN connection settings: “Start” → “Control Panel” → “Network and Internet” → “Network and Sharing Center”. As a result, the main menu for setting up networks opens (Fig. 2.9).

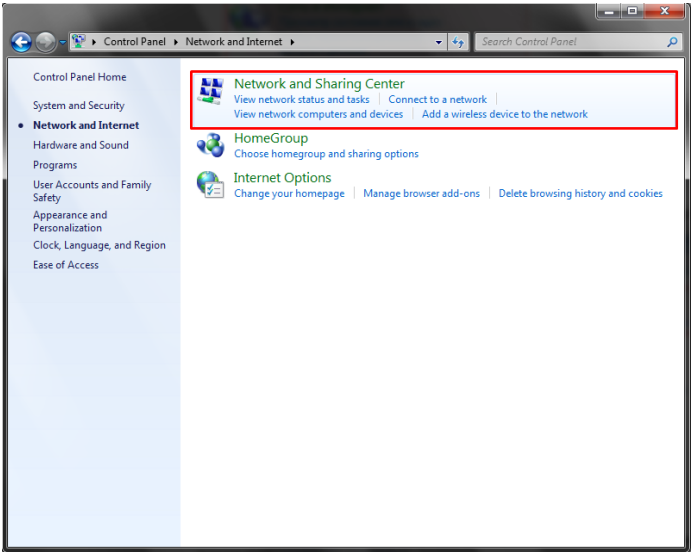

Fig. 2.9 – Network settings window

Let's go to the "Set up a new connection or network" link in the "Network and Sharing Center" window and then the "Set Up a Connection or Network" window will appear on the screen, select the "Connect to a workplace" option and click on the "Next" button. On the "Connect to a workplace" page, select the "Use my Internet connection (VPN)" option (Fig. 2.10).

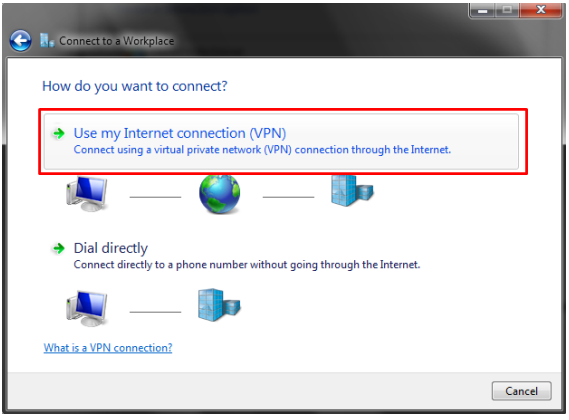

Fig. 2.10 – Window of connection type selection

Further, the address of the VPN server and the name of the connection should be entered on the next page in the “Internet address” field. Let’s enter the address “inter.net” in the “Destination name” field, enter “VPN Connection”, check the box “Don’t connect now; just set it up so I can connect later” and click on the “Next” button (Fig. 2.11).

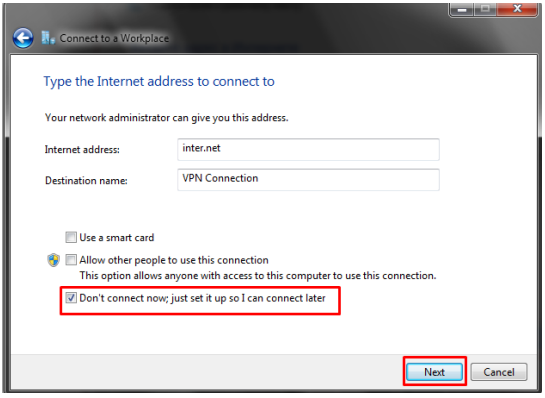

Fig. 2.11 – VPN server settings window

On the next page, enter the “User name” and “Password” given to you when concluding an agreement with the supplier of the VPN technology, check the box “Remember this password” and click on the “Create” button (Fig. 12). Further, click on the “Close” button.

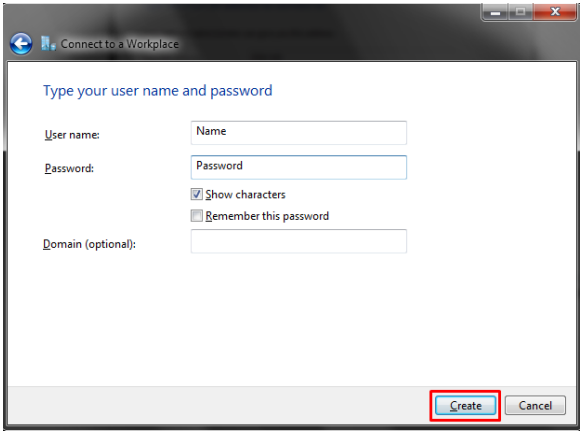

Fig. 2.12 – Window of user’s authentication in the network

Click on “Change adapter settings” in the left panel of the “Network and Sharing Center” window (Fig. 2.13).

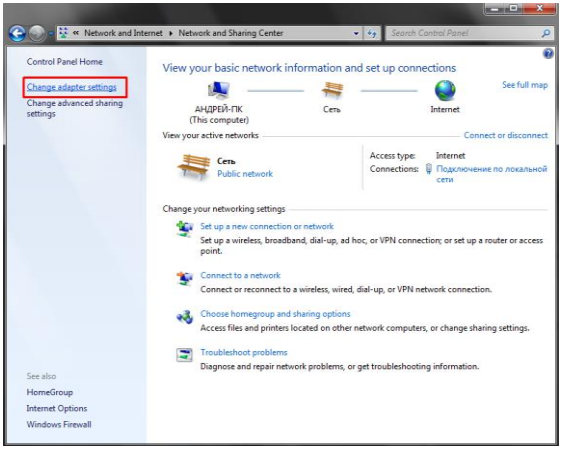

Fig. 2.13 – Network and Sharing Center Window

So, on the created VPN connection open the context menu (in the opened “Network connection” window) and select the “Properties” item in the context menu. On the “General” tab, the address of the VPN server should correspond to the address “inter.net” (Fig. 2.14).

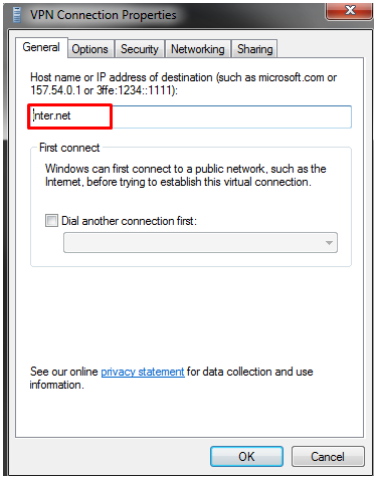

Fig. 2.14 – Window of VPN connection settings

Then, click the “Options” tab and uncheck the “Include Windows logon domain”. Let’s go to the “Security” tab and in the “Type of VPN” drop-down list, select “Protocol L2TP with IPsec (L2TP/IPsec)”, then in the “Data encryption” drop-down list, select “Optional encryption (connect even if no encryption)” and click on the “OK” button. Go to the “Network connection” window and bring up the context menu from the “VPN Connection”, then select the “Create Shortcut” item in the context menu (Fig. 2.15).

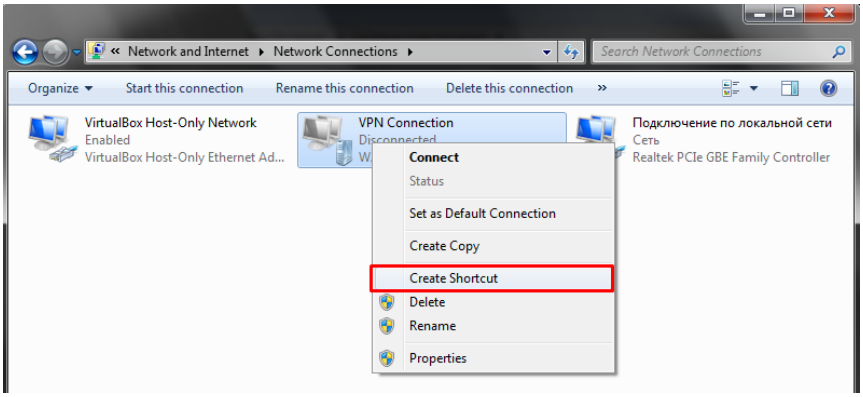

Fig. 2.15 – “Network connection” window

When the message “Windows can`t create a shortcut here. Do you want to click on the desktop instead?” Click on the “Yes” button. Creating a VPN connection to the Internet can be considered successful.

To connect a VPN connection, go to the desktop and launch the shortcut (Fig. 2.16). In the window that opens, click on the “Connect” button.

Fig. 2.16 – Shortcut activate VPN connection

Tasks for extracurricular work

Configure the firewall and create a connection to the Internet through a VPN on an individual computer by each training participant.

Report

The report should contain:

- title page with the name of the training work;
- aim of the work;
- problem statement according to the task;
- the progress and results of the study in graphical form;
- analysis of the results and conclusions.

All materials of the report should be printed, billed, the pages should be numbered.

Test questions

1. What types of attacks in the Internet do you know?
2. What is a firewall and what types of firewall exists?
3. What is VPN technology and what types of VPNs exists?
4. What data transfer protocols are used in the Internet?
5. What are the advantages of a common using firewall and VPN?

Recommended literature

1. Z. Schreuders, E. Butterfield, and P. Staniforth, "An open cloud-based virtual lab environment for computer security education: A pilot study evaluation of oVirt," *The first UK Workshop on Cybersecurity Training & Education (Vibrant Workshop 2015)*, pp. 5-6, June 2015.

2. A. Alfeo, P. Barsocchi, M. Cimino, D. La Rosa, F. Palumbo, and G. Vaglini, "Sleep behavior assessment via smartwatch and stigmergic receptive fields," in *Personal and Ubiquitous Computing*, vol. 22, no. 2, 2017, pp. 227-243.

3. V. Miori and D. Russo, "Home automation devices belong to the IoT world," in *ERCIM news*, vol. 101, 2015, pp. 22-23.

4. C. Pattinson, A. Cor, and R. Braddock, "Community Wide Area Network and Mobile ISP," in *Green Information Technology: A Sustainable Approach*, M. Dastbaz, C. Pattinson, and B. Akhgar, Eds., 2015, pp. 3-28.

5. S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things*. Switzerland: Springer International Publishing, 2017.

6. O. Vermesan and P. Friess, *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*. NY: River Publishers, 2016.

7. Y. Kondratenko, O. Korobko, and O. Kozlov, "PLC-Based Systems for Data Acquisition and Supervisory Control of Environment-Friendly Energy-Saving Technologies," in *Green IT Engineering: Concepts, Models, Complex Systems Architectures, Studies in Systems, Decision and Control*, vol. 74, V. Kharchenko, Y. Kondratenko, and J. Kacprzyk, Eds., 2016, pp. 247-267.

8. A. Pullin, C. Pattinson, and A. Kor, "Building Realistic Mobility Models for Mobile Ad Hoc Networks," in *Informatics*, vol. 5, no. 22, 2018, pp. 1-52.

9. D. Puthal, R. Ranjan, S. Nepal, and J. Chen, "IoT and Big Data: an architecture with data flow and security issues," in *Cloud Infrastructures, Services, and IoT Systems for Smart Cities. IISSC 2017, CN4IoT 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 189, A. Longo et al., Eds., 2018, pp. 243-252.

10. A. Iqbal, C. Pattinson, and A. Kor, "Introducing controlling features in cloud environment by using SNMP," in *Green IT Engineering: Concepts, Models, Complex Systems Architectures. Studies in Systems, Decision and Control*, vol. 74, V. Kharchenko, Y. Kondratenko, and J. Kacprzyk, Eds., 2018, pp. 147-160.

Seminar 1

IOT SYSTEMS' STRUCTURES AND MODELS IN INDUSTRY APPLICATIONS

The aim of the seminar: acquisition of theoretical knowledge and practical skills at the preparation of the project (essay, analytical review) on issues of modern development of prospective structures and models in the field of designing of highly effective IIoT systems.

Learning tasks:

– analysis of industrial standardization and fundamentals of automation systems building in production;

– studying the principles and levels of IIoT;

– analysis of modern approaches and principles of designing structures and models of IIoT systems.

Practical tasks:

– conducting of an analytical review of automation systems building in production using IoT;

– rational selection of basic information according to the topic of the seminar;

– the acquisition of individual skills at preparing the essay.

Preparation for the seminar

Preparation for the seminar includes the following steps.

1) Receiving (determining) the topic of the essay (analytical review) and clarifying the tasks of individual work.

Topics of essays can be formed by students independently based on the general structure of the work of IIoT systems (Fig. 3.1). Industrial systems based on the Internet of Things combine, as a rule, four stages: the presence of the technological process; data collection from sensors; data analysis on the local level and at the cloud; taking steps to improve the quality of the process.

Topics of the essays can also be formed by students on their own based on the following chain of keywords that are somehow related to IIoT:

– standards (international, national, industrial), requirements (general, specific), guideline (general, specific), ISO (International Organization for Standardization), IEC (International Electrotechnical Commission)…;

– principles, methods, techniques, tools, technologies…;

– technological process, automated control system, assembly production line …;

– data processing, system analysis, databases, cloud computing;

– human machine interfaces, user interfaces, graphic interfaces, human factors, usability, quality in use….;

– hierarchical control systems, multi-level systems with decentralized data processing.

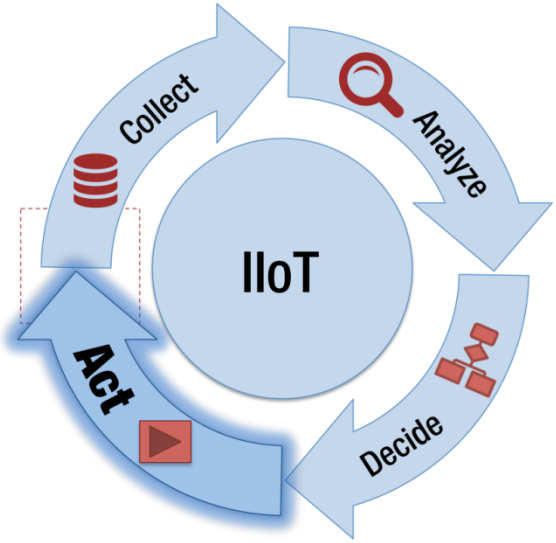

Fig. 3.1 – General structure of the IIoT system

Examples of essays topics:

– IoT technology as means of industrial modernization;

– basic principles and levels of IIoT systems;

– standardization of IIoT systems and problems of implementation in production;

– four generations of industrial automation;

– IoT technology and its place in the industry 4.0;
– concepts of IoT (communication at any time, communication of any devices, communication anywhere) in the industry;
– the main parts of the structure of IIoT systems. Components, structural blocks, system of systems;
– interaction model of the IIoT system. Connection from device to device;
– interaction model of the IIoT system. Connection from device to the cloud;
– interaction model of the IIoT system. Connection from device to gateway;
– sharing data on the server;
– intersectoral IIoT Concepts. Intellectual energy systems;
– intersectoral IIoT Concepts. Logistics;
– methods for assessing (ensuring) the security of IIoT systems;
– problems of IIoT systems designing for energy facilities;
– security problems in industrial IoT-based systems;
– security policy of industrial systems based on IoT;
– cloud computing capabilities for automation tasks;
– multilevel IoT systems with cloud computing.

Topics of the essays should be coordinated with the lecturer and fully comply with the subject area of the course. In preparing for the seminar should use literary sources.

Theoretical issues for "IoT for Industrial Systems" are described in Part XIV (sections 52-55) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

2) Development of a plan of the work on the essay.

The work is carried out individually. Typical work involves the preparation by each student the essay and presentation on issues of modern and prospective development of structures and models in the field of designing of highly efficient IIoT systems.

3) Development of the essay plan.

Before to start writing an essay, it is necessary to clearly formulate the task of finding information according to the required essay plan.

The essay plan includes:

– introduction (relevance, brief analysis of the state of the question). In the introduction of the essay, it is necessary to justify the choice of the topic;

– systematic presentation of the main parts of the essay (structures, models, methods, tools, comparative analysis);

– conclusions (ascertaining the achievement of the goal, the main theoretical and practical results, their significance, directions for further work);

– references (paper and digital sources);

– appendix (presentation slides).

4) Writing an essay.

Writing and design of the essay (including the title page, references) should be literate. Use only the material that reflects the essence of the topic.

The essay has a volume of 15-20 pages of A4 format (font 14, 1.5 interval, 2cm margins), including the title page, content, main text, references, appendix.

At the preparation of the essay, it is necessary to use materials of modern publications not older than 5 years. The presentation of the essay should be consistent. Ambiguous language, speech and spelling errors are not allowed. Particular attention should be paid to the conclusion. In the conclusion, the answers to the tasks set in the introduction should be presented. The general conclusion should be formulated and the goal achievement of the essay should be given. The conclusion should be concise, clear and should follow from the content of the main part.

A mandatory attachment to the abstract is the presentation slides and the electronic version of all materials.

5) Preparation of the presentation.

The presentation is developed in PowerPoint and corresponds to the plan of the essay (10-15 slides) based on the time for the report – 10 min.

The presentation should include the following slides:

– title slide (indicating organization, department, discipline, topic of the report, author, date of presentation);

– content (structure) of the report;

– the relevance of the issues under consideration, the purpose and objectives of the report;
– slides with the disclosure of the content of the objectives;
– report conclusions;
– list of references.

Each of the slides should contain the footer with the title and author of the report.

The content of the slides should not contain parts of the text from the essay, but include keywords, pictures, formulas.

Submission of information can be dynamic.

6) Presentation.

The presentation (report) is carried out at the seminar, takes 15 minutes and includes the report itself (10 minutes) and discussion (5 minutes). Presentation and essay Language is English.

7) Evaluation.

Evaluation for this work takes into account:

a) quality of the essay text (form and content);

b) presentation quality (content and design);

c) report quality (content, logical structure, division of time, conclusions);

d) completeness and correctness of answers to questions.

The grade for the essay and presentation is set for each participant of the seminar individually in accordance with the results.

8) References for seminar preparation.

1. S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems and security and privacy implications," in *Cryptographic Hardware and Embedded Systems-CHES 2002*. *Lecture Notes in Computer Science*, vol. 2523, 2003, pp. 454-469.

2. V. Ovidiu, P. Friess, P. Guillemin, et al., "Internet of things strategic research roadmap," in *Internet of Things-Global Technological and Societal Trends*, 2011, pp. 9-52.

3. S. Sulthana, G. Thatiparthi, and R.S.Gunturi, "Cloud and Intelligent Based SCADA Technology," in *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, vol. 2, iss. 3, 2013, pp. 293-296.

4. R. H. Weber and R. Weber, *Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2010.

5. U. Egham, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", *Gartner.com*, 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. [Accessed: 30- Aug- 2018].

6. A. Kor, C. Pattinson, M. Yanovsky, and V. Kharchenko, "IoT-Enabled Smart Living," in *Technology for Smart Futures*, M. Dastbaz, H. Arabnia, and B. Akhgar, Eds., 2017, pp. 3-28.

7. A. Alfeo, P. Barsocchi, M. Cimino, D. La Rosa, F. Palumbo, and G. Vaglini, "Sleep behavior assessment via smartwatch and stigmergic receptive fields," in *Personal and Ubiquitous Computing*, vol. 22, no. 2, 2017, pp. 227-243.

8. V. Miori and D. Russo, "Home automation devices belong to the IoT world," in *ERCIM news*, vol. 101, 2015, pp. 22-23.

9. S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things*. Switzerland: Springer International Publishing, 2017.

10. Y. Kondratenko, O. Kozlov, O. Korobko, and A. Topalov, "Internet of Things Approach for Automation of the Complex Industrial Systems," *13th International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI'2017, CEUR-WS*, pp. 3-18, May 2017.

11. C. Pattinson and K. Hajdarevic, "Timing considerations in detecting resource starvation attacks using statistical profiles," in *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 2, 2007, pp. 194-205.

12. G. Barbon, M. Margolis, F. Palumbo, F. Raimondi, and N. Weldin, "Taking Arduino to the Internet of Things: The ASIP programming model," in *Computer Communications*, vol. 89-90, 2016, pp. 128-140.

13. R. Minerva, A. Biru, and D. Rotondi, *Towards a definition of the Internet of Things (IoT)*. Telecom Italia S.p.A., 2015.

14. H. J. Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," in *International Journal of Distributed Sensor Networks*, vol. 8, iss. 11, 2012, pp. 29-37.

ITMM6.2. Advanced techniques and means for design, modernization and implementation of industrial IoT-based systems

Prof., DrS. Yu.P. Kondratenko, Assoc. Prof., Dr. G.V. Kondratenko, Assoc. Prof., Dr. O.V. Kozlov, PhD Student A.M. Topalov, PhD Student O.S. Gerasin (PMBSNU)

Training 1

IOT-BASED SYSTEM FOR REMOTE DIAGNOSTICS OF LEVEL SENSORS IN THE FLOATING DOCK BALLAST COMPLEXES

The aim of the training: development of specialized computerized system for technical diagnostics of the level sensors of the floating dock ballast complex capable of providing results of technical diagnostics to the cloud services ThingSpeak.

Training participants: lecturers, scientists, technical staff, students and post-graduate students of the department (faculty, institute) of the university; developers, engineers, trainees of industrial objects.

To complete the training, it is necessary to carefully read the theoretical foundations given below. For a deeper acquaintance with the material, it is necessary to use the technical literature, to which references are given in the instructions. If during the study of the discipline there will be questions that are not answered in this training or technical literature, it is necessary to consult a leading lecturer.

Theoretical information

The complex automation of the floating dock and the presence of a large number of sensors are related to the need of reducing the likelihood of a violation of the normal mode of operation of the computerized system of monitoring and control of the floating dock in different operating modes. An effective way to increase the reliability of such a computerized system is to periodically or continuously carry out diagnostic procedures of the most important elements of the system, in particular sensors for determining the water level in the respective ballast tanks. Consequently, the general problem of ensuring the effective

functioning of the floating dock arises in the field of accurate and reliable measurements, and therefore, along with the automation of the floating dock, considerable attention is paid to solving the problems of selection and technical diagnostics of sensors [1-4].

In the case of simplified technical diagnostics of sensors, one can restrict the standard capabilities of common industrial computerized monitoring and control systems. The standard features of diagnostic testing primarily include work with events as well as analog and discrete alarms. To implement more sophisticated technical diagnostics, IoT technology is used and additional hardware and specialized diagnostic equipment is needed [2, 5-7].

The functional diagram of the proposed remote system of level measurement and control is shown in Fig. 1.1, where the following abbreviations are accepted: SBC – single-board computer; R – router; M – modem; PC – personal computer; DB – device with browser (smartphone, computer); IC – interface converter; TDAM – temperature data acquisition modules; CIM – current input modules; DIM – discrete signals input modules; DOM – discrete output modules; TS, PS – the sensors of temperature and pressure respectively; HPS – hydrostatic pressure sensor; FLS – float level switch; L, T, P – the values of liquid level, temperature and pressure in the relevant tanks; V – drain valves; Q – the value of liquid flow at the opening drain valve.

The TRACE MODE is used in this computerized system for remote level control as a software platform. The TRACE MODE software has its own integrated development environment with more than 10 editors arranged in it. Moreover, it includes the built-in drivers for more than 2572 PLCs and I/O devices (including the products of the ICP DAS company) and has its own industrial real time database management system [1, 6, 8-10].

Level sensors and actuators include the following sensors and actuators: Dwyer Instruments 673-type pressure sensor, thermocouples of the L-type, discrete float level sensors and normally closed Jaksa D224 valves. Level of monitoring and management consists of programmable logic controllers and the peripheral input/output (I/O) modules: IC interface converter; TDAM ICP DAS I-7018P modules are used as the data acquisition modules for the thermocouples readings; CIM ICP DAS I7017C modules with current input signal are used for data acquisition from the pressure sensors; DIM ICP DAS I-7053D

modules for the discrete input signals; in addition, DOM ICP DAS I-7067D is used for the discrete output signals. The level of visualization, dispatching (monitoring) and data acquisition include the computer is equipped with a TRACE MODE 6 for successfully launching of liquid level control system with discrete self-testing [11, 12].

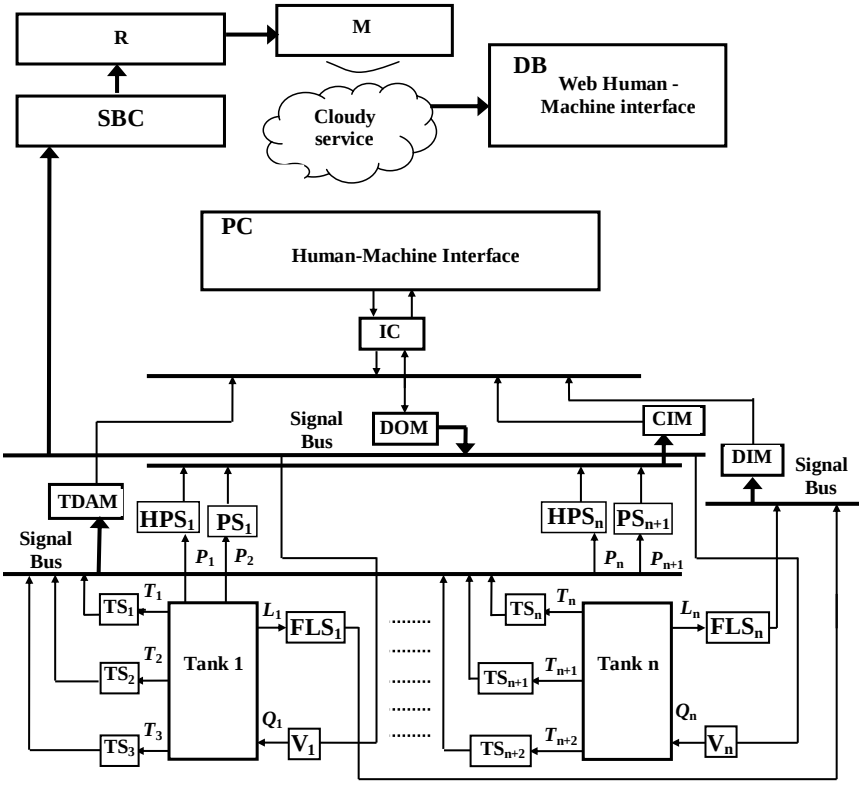

Fig. 1.1 – The functional diagram of the system of remote level measurement and control

The computerized intelligent system for remote diagnostics of HPS sensors in the ballast complex consists of diagnostic equipment. The equipment should include the FLS diagnostic sensor (float sensor), SBC (Raspberry Pi), R (Wi-Fi router), M (modem 4G), and cloud service ThingSpeak [4].

The diagnostics includes monitoring of the HPS state in order to detect and prevent its failures. The technical state of the HPS is characterized by factors that can include the effects of climatic conditions, aging with time, operation of regulation of mechanical and electronic components, adjustment during maintenance or repair, replacement of faulty elements, etc [4, 6].

The diagnostics is carried out using diagnostic tools that can be embedded or external [5]. The embedded tools allow continuously controlling the corresponding parameters. By means of the external tools, periodic monitoring is carried out. To implement the proposed method of technical diagnostics, let's consider one ballast tank. In a ballast tank FLS, a higher HPS is set at a fixed height and a specialized approach is used in which the state of the HPS is verified at discrete time intervals by comparing the current level of liquid L to the diagnostic level of L_F.

Consequently, the HPS, which is the pressure measuring device, is used to obtain information about the current level in the ballast tank, that is sent to the ICP DAS I7017C. To monitor the diagnostic value of the L_F level, FLS is used, which can be performed as a float sensor. According to the design, the signal from the FLS is sent to the ICP DAS I-7067D. The data from HPS and FLS sensors are processed using the program TRACE MODE in the control computer where the state of the hydrostatic sensor is determined (1 - working, 0 - not working). The diagnostic information, in the form of a logical signal, is transmitted from the PC through the DOM to the SBC, which transmits data over the Internet to the cloud service ThingSpeak. The Internet is provided by a 4G modem using 4G global wireless mobile technology (data transfer speeds up to 1 Gbit/s) and is distributed through a Wi-Fi router [10].

Diagnostics of other HPS sensors is performed in the same way [7].

The general results of the remote diagnostics system for level sensors are displayed graphically in real time on any computer or mobile device that has access to the Internet [2].

The work with the data of technical diagnostics in ThingSpeak channels is carried out using periodic POST and GET queries, indicating the API key and value for the corresponding channel field. And the channels supported formats XML, JSON and CSV [8].

Also, data downloading to the channels can be implemented by using URL-addresses. For example, if the key is API-

XXXXXXXXXXXXXXX, the URL-addresses for updating fields 1 and 2 with the values 1 and 0 has the following form:

"Http://api.thingspeak.com/update?key=ABC1234L6789STIV&field1=1&field2=0".

Each used input channel is stored along with the date and time label, as well as a signed unique entry identifier (entry_id). Accordingly, the stored data can be obtained by time or by the identifier [9, 11].

Theoretical issues for "IoT for Industrial Systems" are described in Part XIV (sections 52-55) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

Training implementation

To build a technical diagnostic system, let's use the integration of the cloud service ThingSpeak with the SCADA system TRACE MODE 6. Let's consider the case of diagnosing of a single HPS sensor by means of another FLS sensor.

Launch TRACE MODE 6 (tmdevenv.exe file) and create a project with a RTM type node for work under MS Windows operating system on the automated operator workstation (AOW). Details of how to work with the system TRACE MODE 6 are discussed in the specialized literature and training "Main stages of industrial IoT-based system development" of the given course.

Next, it is necessary to create channels for implementing the transfer of information within the framework of this project. Let's create three channels: the first and the second for signals from HPS sensors and FLS; the third for the resultant signal after the software diagnostics.

Select the "Channels" group of the "RTM_1" node. Call the context menu. In the context menu, select the "Create Component" line. According to the proposed variants, create one channel "Float_Channel" for moving the information of the sensor HPS, as well as two channels "HEX16_Channel": one for moving the information of the sensor FLS, and the second for the result of the diagnostics. Accordingly, three channels will be received: "HPS_Channel", "FLS_Channel", "Result_Diagnostics" (Fig. 1.2). And it is also necessary to edit the channel "HPS_Channel". Open the channel for editing and add the zoom

according to the Dwyer Instruments 673-type sensor, so the channel will convert the current value (mA) to the equivalent pressure value (PA).

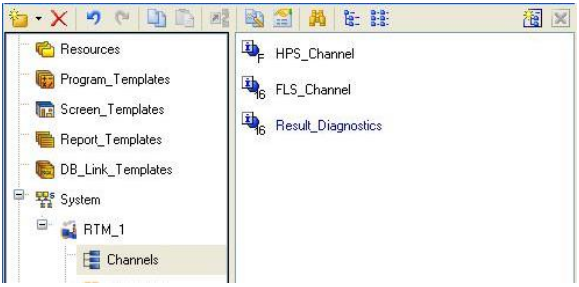

Fig. 1.2 – Created project channels

Let's describe the diagnostic procedure using TRACE MODE 6 programming tools. In the "RTM_1" node, create the "Program" component. Open it and go to the "Arguments" tab and the "Local Variables" tab. Create the necessary arguments (Fig. 1.3) and local variables (Fig. 1.4), and bind the arguments to the "RTM_1" node's channels through the properties of the program. Also, set the diagnostics values to the local variables: "Coefficient_for_level" is the coefficient of the product of the liquid density and the acceleration of the free fall; "Value_of_a_given_level" is the control level of the HPS check (location of the FLS installation); "Maximum_limit" is the value of the tolerable drop in HPS values at the control level.

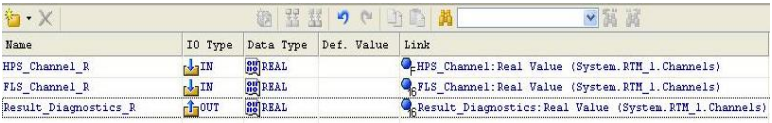

Fig. 1.3 – Creation of arguments of the program

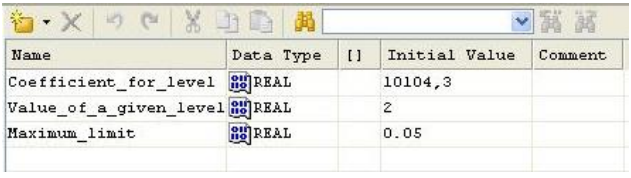

Fig. 1.4 – Creation of local variables of the program

Next, activate the line “Program” and a window appears with a choice of programming language. Select FBD and write the next program (Fig. 1.5).

Let's consider the settings of software and hardware modules of this diagnostics system. The ICP DAS I-7017C with a current input signal is used for data acquisition from HPS; The ICP DAS I-7053D module is used for data acquisition from FLS; The ICP DAS I-7067D module with relay output is used to output diagnostics information.

All modules are pre-configured using the configuration utility supplied with the modules, namely numbered on the RS-485 network, configured to exchange data at 57600 without a checksum. Let’s connect the modules to the COM1 PC port via the automatic I-7520 interface converter.

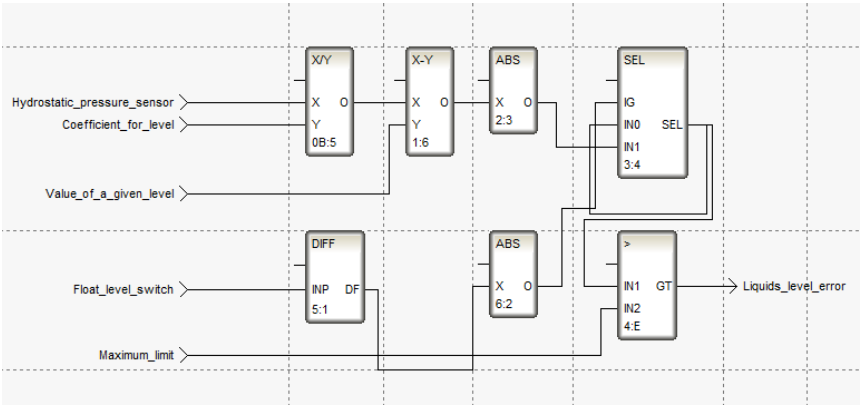

Fig. 1.5 – Program listing

Let’s introduce the necessary modules for the task into the created project. It is necessary to open the “Sources/Receivers” layer and create a “Distributed_Modules_(DCS)” group via the PC, then open the “Distributed_Modules_(DCS)” group and create a group “I-7000_#1” through the PC (Fig. 1.6).

Open the created group “I7000_#1” and create subgroups “I7017C#1”, “I-7053D#2”, “I-7067D#3” in it.

Open the group “I7017C#1” and edit the component “AIn#1” as follows: port number 0 corresponds to COM1, module address in this case is 1, checksum - absent, signal type - in.

Open the “I7053D#2” group and edit the component “DI#1” as follows: port number 0 corresponds to COM1, module address in this case is 2, checksum - absent, signal type - in.

Open the “I7067D#3” group and edit the component “DO#1” as follows: port number 0 corresponds to the COM1, the module address in this case is 3, the checksum - absent, the signal type - the output.

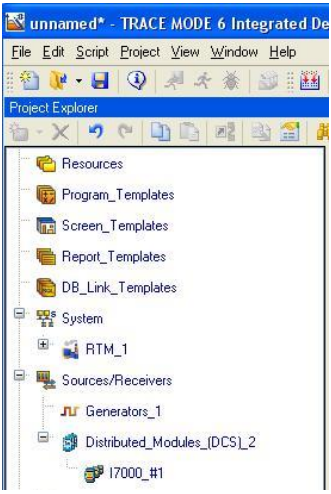

Fig. 1.6 – Creation of a group for modules I-7000

To create in the RTM_1 node a channel associated with the ICP DAS I-7017C module, it is necessary to select the “AIn#1” component in the “I7017C#1” sub-group and use the drag-and-drop mechanism to transfer it to the “Channels” group to the “HPS_Channel” channel.

To create in the “RTM_1” node a channel associated with the ICP DAS I-7053D module, it is necessary to select the “DI#1” component in the subgroup “I7053D#2” and use the drag-and-drop mechanism to transfer it to the “Channels” group to the “FLS_Channel” channel.

To create in the “RTM_1” node a channel associated with the ICP DAS I-7067D module, it is necessary to select the “DO#1” component in the “I7067D#3” sub-group and use the drag-and-drop mechanism to transfer it to the “Channels” group to the “Result_Diagnostics” channel.

Creating and configuring a COM port. Open the context menu of the “RTM_1” node and select the line “Create Group”, then click

"COM_Ports" (Fig. 1.7).

Fig. 1.7 – Created COM port

Edit the newly created "COM_Port#1" as follows: leave all attributes set to default, changing only the Speed to 57600 (Fig. 1.8).

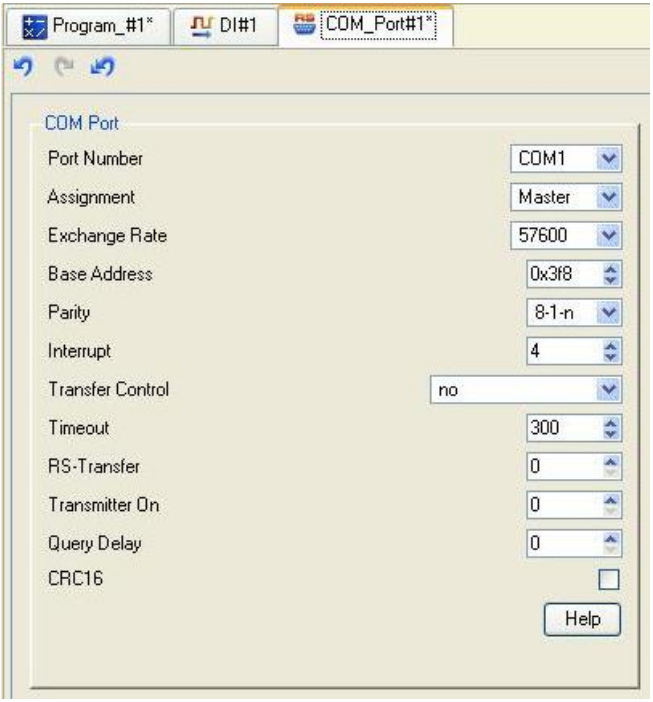

Fig. 1.8 – COM Port configuration window

Save the project and execute the save procedure for the real-time monitor.

Let's go to the settings that are required to work with the ThingSpeak cloud server.

For this work it is necessary to use: a single-board computer Raspberri Pi Model B+ with installed operating system through Matlab 2015b and configured SSH protocol; Wi-Fi adapter for Raspberri Pi connection with Internet; a personal computer with the installed Matlab 2015b program and connection to the internet. Also, the Internet source for the single-board computer and a personal computer should be the same.

Open Matlab 2015b and put the following in the command line: “mypi = raspi ('169.254.0.2', 'pi', 'raspberry')”. Then, press “Enter” on keyboard. The ip address also should be specified according to the ip address of the Wi-Fi adapter. As a result, the connection of raspberry B+ with Matlab 2015b is set (Fig. 1.9).

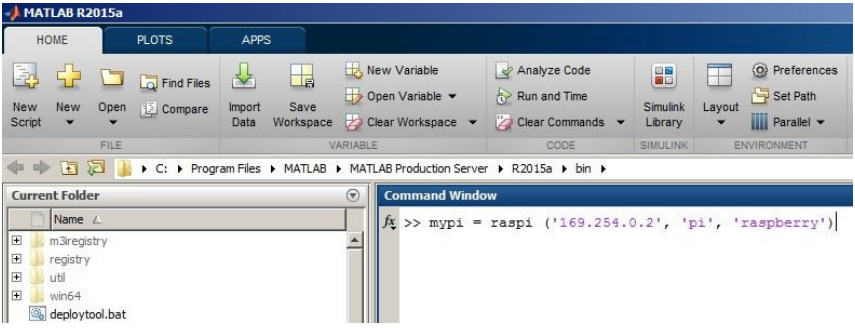

Fig. 1.9 – Matlab's 2015b main window

Then it is necessary to build connection of the Raspberri Pi B+ pinouts with the cloud-based ThingSpeak service in the Simulink environment. Press “New” and choose “Simulink model”.

Let’s complete the simulation settings in the “Simulink model”. To do this, click on “Model Configuration Parameters”.

In the “Solver” tab set the settings for “Solver options” and, respectively, Type – “Fixed-step”, Solver – “discrete (no continuos state)” (Fig. 1.10).

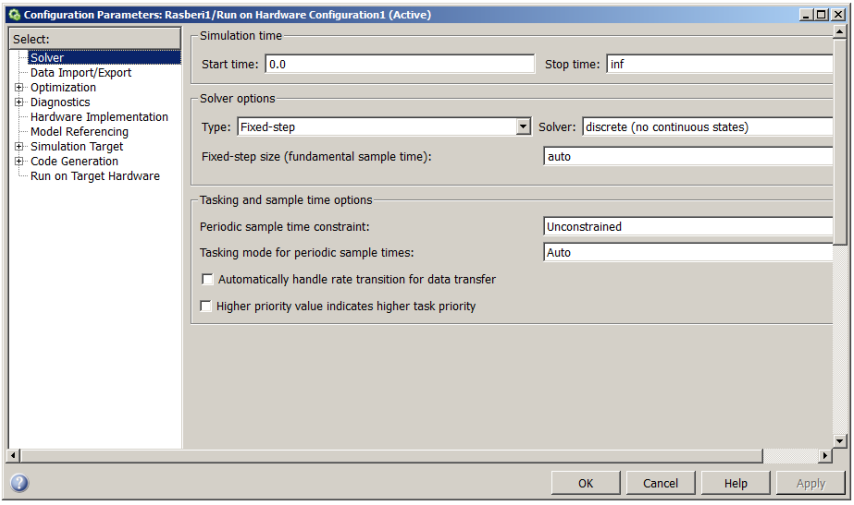

Fig. 1.10 – Simulation setting window

In the “Run on Target Hardware” tab set the settings for “Target hardware selection” according to Target hardware: “Raspberry PI”. Press “OK” and close the simulation setting.

Then, let’s build the scheme of transferring the diagnostic information of one HPS sensor to the cloud service ThingSpeak.

Open the Simulink library of blocks “Library Browser” and write “raspberry” in the search (Fig. 1.11). Drag the blocks “GPIO Read” and “ThingSpeak Write” into the Simulink workspace. Then write in the search “Data Type Conversion” and drag the same name block into the Simulink model workspace.

Edit each of the blocks. Open “GPIO” Read block setting and specify GPIO number 20 and then press “OK”. Open the “Data Type Conversion” block setting and specify Output data type – “single” and press “OK”.

Connect the blocks sequentially as shown in Fig. 1.12.

To get started with the service ThingSpeak, it is necessary to register at the ThingSpeak website. Then create a channel in which the data from the sensors will be stored.

To create a channel, click on the “New Channel” button and click “Save Channel” (Fig. 1.13).

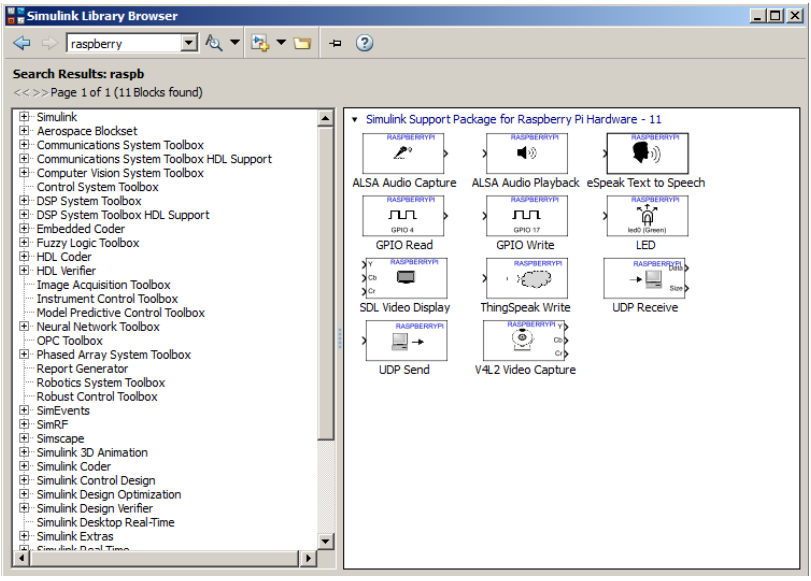

Fig. 1.11 – The Simulink library of blocks

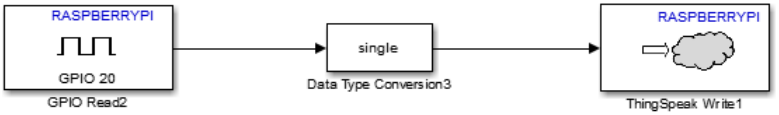

Fig. 1.12 – Scheme of data transfer to the cloud service ThingSpeak

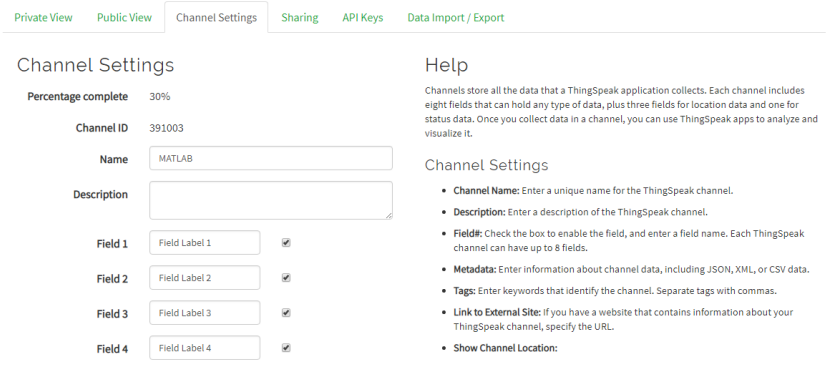

Fig. 1.13 – ThingSpeak channel window

Visualization of the state of the HPS diagnostics will be performed in the graphical form.

In the “Private View” tab of the main ThingSpeak window click on “Add Visualizations” and select “Field 5 Chart”. Then, receive an element of visual display (Fig. 1.14).

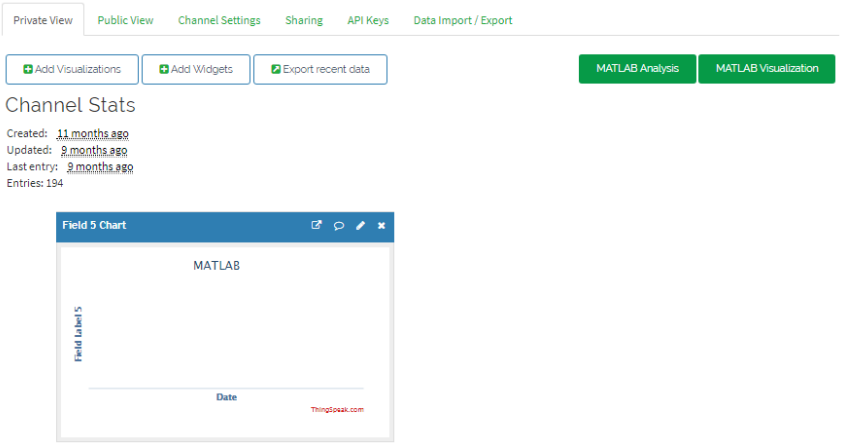

Fig. 1.14 – Graph of display

Then, go to the “API Keys” tab and in the window copy a unique key for writing data to the ThingSpeak cloud (Fig. 1.15).

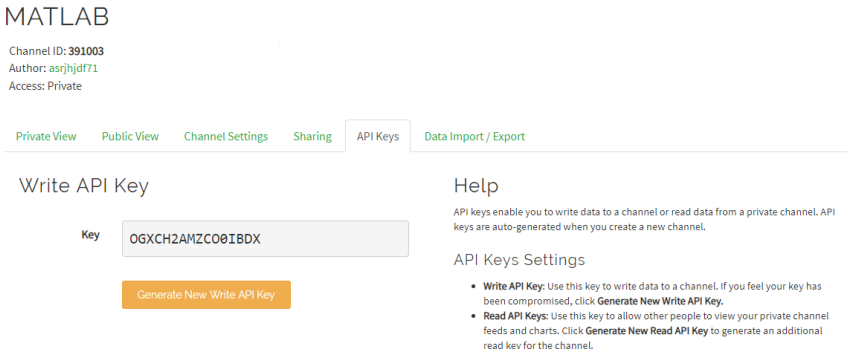

Fig. 1.15 – The window of generating a unique key

Return to the Simulink model and set up the “ThingSpeak Write” block, open its configuration, and specify: in the field “Updata URL” – “https://api.thingspeak.com/update”, in the field “Write API key” – “OGXCH2AMZCO0IBDX” (insert the copied key with ThingSpeak), in the field “Number of variables to send” – “1”, in the field “Update interval” – “60”. The settings can be considered complete, press “OK” (Fig. 1.16).

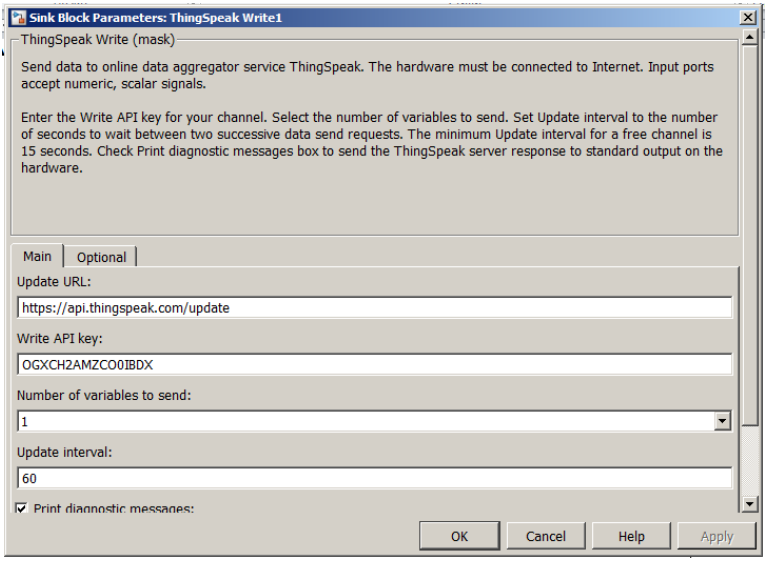

Fig. 1.16 – Setting window for “ThingSpeak Write” block

For Raspberi pi B+ board to work offline, without using the Matlab environment, generate code from the Simulink model and write it to Raspberi pi B+. To do this, click on the “Deploy to Hardware” button and wait for some time to write the code in Raspberi pi B+. After that the Raspberi pi B+ is ready for offline work.

Let's check the work of ThingSpeak with the SCADA TRACE MODE system.

Connect all components of the system and provide power. Start the real-time monitor (rtc.exe), open the project with the .dbb extension and launch it. Open ThingSpeak and observe the visual display of the operation of the HPS sensor (Fig. 1.17).

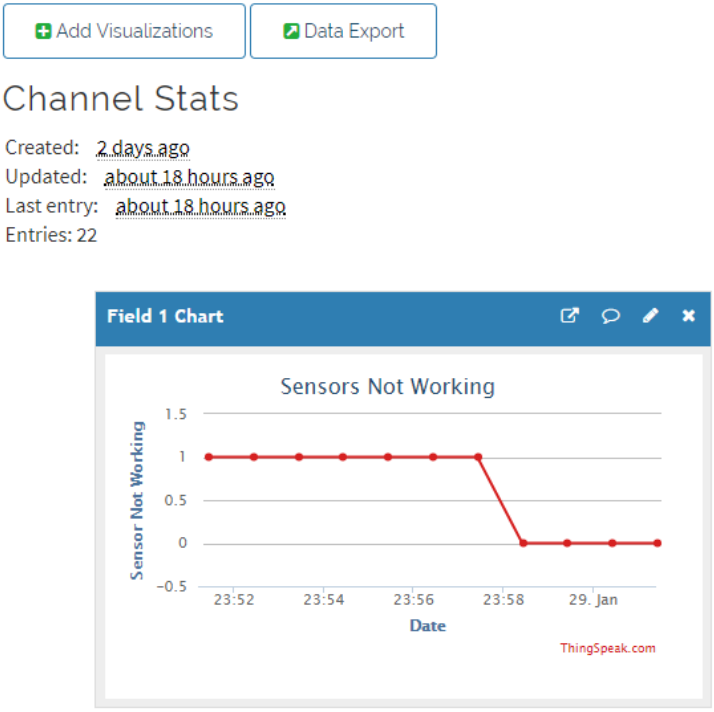

Fig. 1.17 – Modeling of sensor operation

Moreover, the TRACE MODE project can be changed and stored for the real time monitor. Thus, restarting the .dbb file in the real-time monitor can affect the state of the sensor's operation, respectively, and in the ThingSpeak, two positions of the sensor operation (1 - working, 0 - not working) are obtained.

Tasks for extracurricular work

Perform the diagnostics of the HPS sensor using TRACE MODE with the appropriate diagnostic error and diagnostic control level as well as pass the diagnostic result to the cloud service ThingSpeak to visualize the status of the sensor operation.

Variations of permissible error and control levels of diagnostics are presented in Table 1.1.

Table 1.1 – Tasks for the variants for extracurricular work

Variant number	Control level for diagnostics	Permissible diagnostic error
1	1.5	0.05
2	1	0.07
3	2	0.07
4	1	0.1
5	2	0.1
6	1	0.08
7	1.5	0.09
8	1	0.05
9	2	0.1
10	2	0.07

Report

The report should contain:

- title page with the name of the training work;
- aim of the work;
- problem statement according to the variant;
- the progress and results of the study in graphical form;
- analysis of the results and conclusions.

All materials of the report should be printed, billed, the pages should be numbered.

Test questions

1. What is a ThingSpeak cloud service?
2. SCADA TRACE MODE and its programming languages?
3. Information security system in ThingSpeak service?
4. What types of signals are used in this work?
5. What is a real time monitor SCADA TRACE MODE?

Recommended literature

1. A. Topalov, O. Kozlov, and Y. Kondratenko, "Control Processes of Floating Docks Based on SCADA Systems with Wireless Data Transmission," *Perspective Technologies and Methods in MEMS Design (MEMSTECH 2016)*, pp. 57-61, April 2016.

2. R. H. Weber and R. Weber, *Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2010.

3. G. Yang, H. Liang, and C. Wu, "Deflection and inclination measuring system for floating dock based on wireless networks," in *Ocean Engineering*, vol. 69, 2013, pp. 1-8.

4. I. Efimov and D. Soluyanov, *SCADA-system Trace Mode*. Ulyanovsk: UlGTU, 2010. (in Russian).

5. V. Bukreeva and A. Tskhe, *Fundamentals of Tool-System Development of SCADA Trace Mode*, Tomsk: TPU, 2004 (in Russian).

6. A. Kor, C. Pattinson, M. Yanovsky, and V. Kharchenko, "IoT-Enabled Smart Living," in *Technology for Smart Futures*, M. Dastbaz, H. Arabnia, and B. Akhgar, Eds., 2018, pp. 3-28.

7. Y. Kondratenko, O. Kozlov, O. Korobko, and A. Topalov, "Internet of Things Approach for Automation of the Complex Industrial Systems," *13th International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI'2017, CEUR-WS*, pp. 3-18, May 2017.

8. B. Payam, W. Wang, C. Henson, and K. Taylor, "Semantics for the Internet of Things: early progress and back to the future," in *International Journal on Semantic Web and Information Systems*, vol. 8, no. 1, 2012, pp. 1-21.

9. E. Delgado, *The Internet of Things: Emergence, Perspectives, Privacy and Security Issues*. New York: Nova Science Publishers, 2015.

10. P. Simoens, M. Dragone, and A. Saffiotti, "The Internet of Robotic Things: A review of concept, added value and applications," in *International Journal of Advanced Robotic Systems*, vol. 15, no. 1, 2018, pp. 1-11.

11. G. Barbon, M. Margolis, F. Palumbo, F. Raimondi, and N. Weldin, "Taking Arduino to the Internet of Things: The ASIP programming model," in *Computer Communications*, vol. 89-90, 2016, pp. 128-140.

12. B. Ahlgren, M. Hidell, and E. Ngai, "Internet of Things for Smart Cities: Interoperability and Open Data," in *IEEE Internet Computing*, vol. 20, no. 6, 2016, pp. 52-56.

Training 2

IOT-BASED SYSTEM FOR SPECIALIZED PYROLYSIS COMPLEX

The aim of the training: designing of a computerized system for monitoring the operating parameters of a specialized pyrolysis complex using the Web server of TRACE MODE Data Center.

Training participants: lecturers, scientists, technical staff, students and post-graduate students of the department (faculty, institute) of the university; developers, engineers, trainees of industrial objects.

To complete the training, it is necessary to carefully read the theoretical foundations given below. For a deeper acquaintance with the material, it is necessary to use the technical literature, to which references are given in the instructions. If during the study of the discipline there will be questions that are not answered in this training or technical literature, it is necessary to consult a leading lecturer.

Theoretical information

The control of technological processes is provided by the SCADA system, which is designed for the development and operation of distributed automated control systems in industry. The SCADA system is used for supervisory control and data acquisition. However, its appointment has been expanded significantly in recent versions. New advanced features are regularly added [1, 2].

Often SCADA-system is understood as the specialized software that implements the interface between man and control system, communications with the outside world via the Internet. The following SCADA systems were widely distributed: Genesis, TRACE MODE, InTouch and others. SCADA-systems of the local level of automation in production are recently modernized and supplemented by computing means of cloud technologies of the Internet [3-5].

Consequently, the introduction of IIoT technologies in SCADA enables the creation of a highly effective system for monitoring and managing technological processes that will work through the Internet. For the processing and storage of data, given from the technical object, it is advisable to use embedded software and hardware means in the form

of small-sized computers (for example, Raspberry Pi, Intel Edison) with access to the Internet. For the processing of measurement data today are available for free in the test mode such cloud services as: Azure, Freeboard, Grovestreams, Developer.ibm, Thingspeak, Thingworx and other [2, 6].

Also today, IIoT is considered by global manufacturers of SCADA systems as the implementation of monitoring and management systems in a cloud server with the display of real-time imitator based on web technologies. In this case, SCADA monitoring and control are implemented through a usual browser acting as a thin client. Similar systems include IIoT server and client terminals: personal computers (PC), personal digital assistants (PDA) or smartphones. Customers can connect to the IIoT server by Internet/Intranet and interact with applied automation tasks through Web or WAP pages [7-9].

In particular, SIEMENS developed the WebNavigator package for the WinCC SCADA system, another example is the Adastra company that developed the TRACE MODE Data Center web server for the SCADA system Trace node 6. All of these solutions provide access to the project for remote clients. Thin client technology allows you to view and make adjustments to operational and archival information from any remote workplace through any browser [8].

The functional structure of the highly effective computerized system for the specialized pyrolysis complex is shown in Fig. 2.1 [1].

The proposed structure (Fig. 2.1) of the computerized system based on IoT is built taking into account the necessity of the simultaneous measurement of various physical quantities, functioning in real-time mode and also the need to build a modular system that has the ability of integration into existing large-scaled IIoT systems. In turn, the designed structure allows to measure and control the main technological parameters of the municipal polymeric waste utilization process, such as: temperature, pressure and load level values in the reactor, fuel liquid fractions level in the fuel tank and a set of temperature values in key points of specialized pyrolysis complex [1].

For hardware implementation of the mentioned above system for monitoring and automatic control of specialized pyrolysis complex main process parameters used hardware means company ICP DAS (shown in Fig. 2.1).

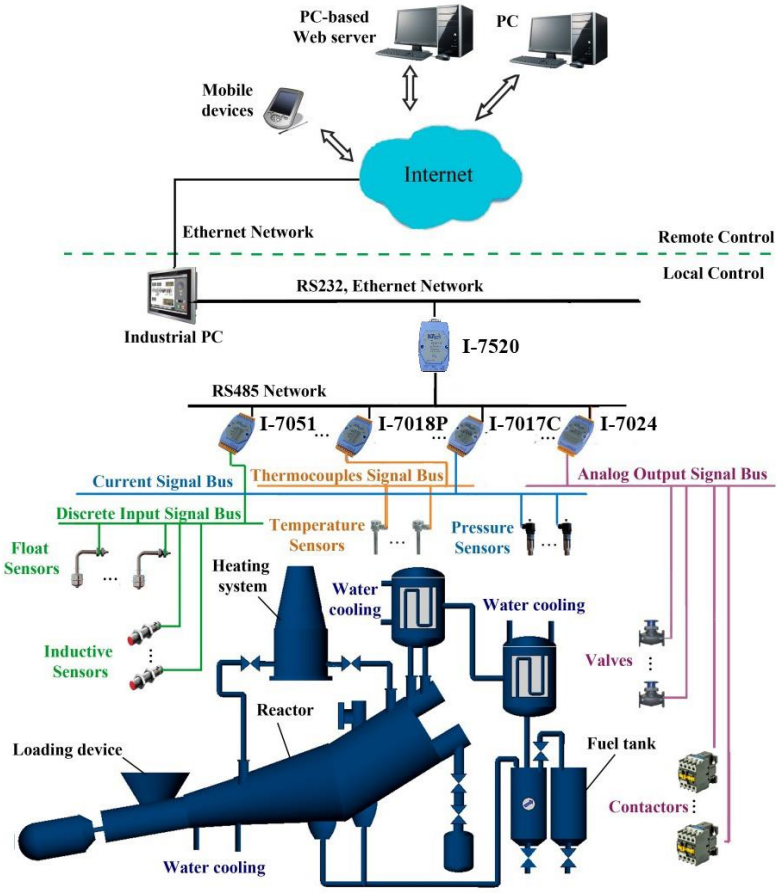

Fig. 2.1 – Functional structure of computerized system for the specialized pyrolysis complex

As the software facilities of the developed computerized system of the specialized pyrolysis complexes for the municipal polymeric waste thermal processing the TRACE MODE 6 is also used. It belongs to the class of integrated systems that provide maximum comfort to designers and users [5].

A special web server TRACE MODE Data Center is used for remote control of specialized pyrolysis complexes. The main objective of

this software product is to provide users with the ability to control the process through a web browser using Internet / Intranet networks or wirelessly (GPRS, Wi-Fi, Bluetooth, etc.). This new web server enables you to access real time data from any computer using different operating systems (Windows, Linux, Mac OS, etc.). With the help of TRACE MODE Data Center, you can not only monitor the process, but also manage it online - changing the task control to the temperature and pressure regulators on the screen. It is also possible to generate reports on the technological process [8, 9].

TRACE MODE Data Center has a security system integrated into the TRACE MODE 6 security system. Therefore, only authorized users can access the web server data. The rights of various users are flexibly configured and administered in real time. To insure more safety TRACE MODE Data Center supports reliable encrypted VPN connection from external PCs connected to Internet [6].

TRACE MODE Data Center licensing is based on concurrent connections of the client devices (PCs, pocket PCs, mobile phones, etc.). The program is available in versions for 4, 8, 16, 32, 64 and unlimited workplaces. When using TRACE MODE, the data center does not require the installation of Web servers from other manufacturers (such as Microsoft IIS), which distinguishes this system from the solutions used by some competing SCADA developers. Moreover, TRACE MODE Data Center requires a separate PC [3].

In the SPC based on the IIoT Systems, the TRACE MODE Data Center serves the local SPC management system. The TRACE MODE Data Center receives real-time data from local system on the base TRACE MODE 6 over TCP / IP and provides access to data via the Internet for computers and mobile devices (smartphones). To control the pyrolysis process, the operator logs on to the Web browser page that supports the virtual Java machine, opens the SPC based on IIoT project. Moreover, the graphical capabilities of the real-time monitor on the web page almost coincide with the real-time monitor of the local system [9].

Theoretical issues for “IoT for Industrial Systems” are described in Part XIV (sections 52-55) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

Training implementation

The web-server TRACE MODE Data Center is used to build a computerized control system of a specialized pyrolysis complex on the basis of IoT technologies. Moreover, the project of control system for the specialized pyrolysis complex will be launched on one computer, and the web-server TRACE MODE Data Center – on the other.

Firstly, run TRACE MODE 6 and open the finished project for control of specialized pyrolysis complex (Fig. 2.2). Main principles how to operate in TRACE MODE 6 is detail discussed in the specialized literature and training "Main stages of industrial IoT-based system development" of the given course.

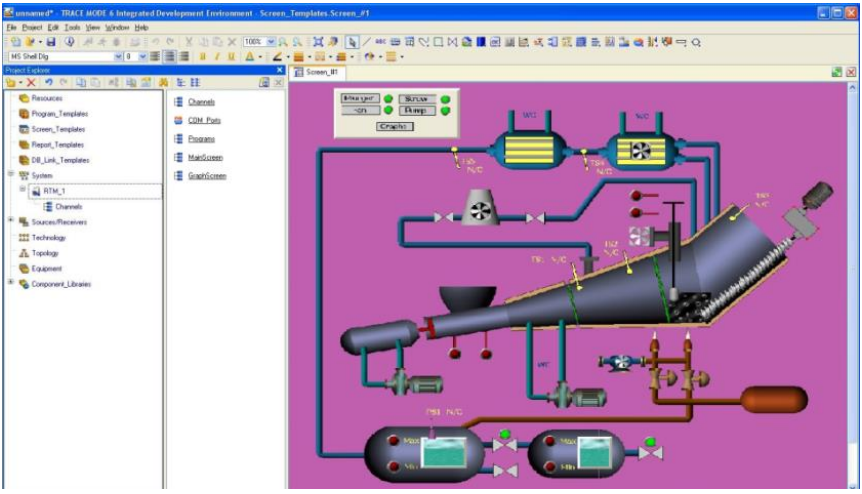

Fig. 2.2 – TRACE MODE project for control of specialized pyrolysis complex

Let's open the node "RTM_1" for editing and set up the first network adapter for reception and sending (put a confirmation in front of "Reception" and "Sending"). Also, indicate the IP address of the control computer, in our case "192.168.86.130" (Fig. 2.3).

Create the "EmbeddedConsole_2" node and open it for editing (Fig. 2.4). Adjust the system adapter for reception and sending (provide confirmation in front of "Reception" and "Sending").

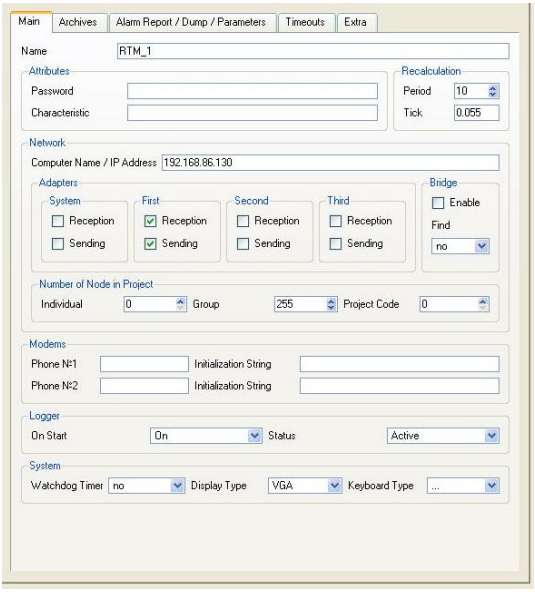

Fig. 2.3 – Node “RTM_1” editing window

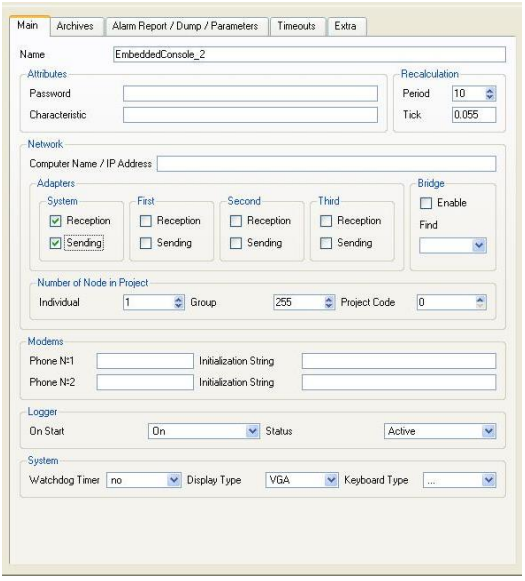

Fig. 2.4 – Node “EmbeddedConsole_2” editing window

Next, open the “channels” group of the node “EmbeddedConsole_2” and create a graphic panel. Make a functional copy of the human-machine interface of the home screen of the “RTM_1” node in this graphic panel (Fig. 2.5). The pyrolysis plant can be made as a background for the convenience, and then dynamic elements of automation can be anew built. All the arguments of the graphic panel should be tied to the channels of the “RTM_1” node.

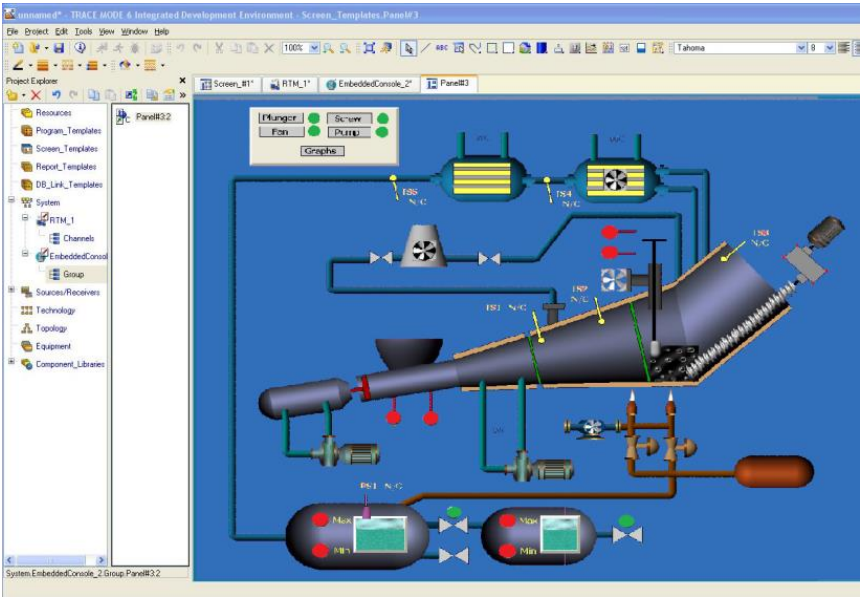

Fig. 2.5 – Graphic panel of the “EmbeddedConsole_2” node

Save the project and execute the save procedure for the real-time monitor. Start the real-time monitor (rtc.exe), open the project with the .dbb file from the folder “RTM_1” extension and launch it. Copy the folder with this TRACE MODE project to the external storage and copy it to the computer where the TRACE MODE Data Center is installed. Next, open the TRACE MODE Data Center application on a web server computer (Fig. 2.6).

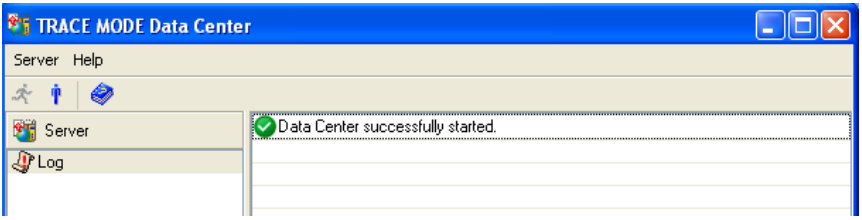

Fig. 2.6 – TRACE MODE Data Center main window

Let's stop it (click on the appropriate label of the standing person) and click on “Server”, where open the “Change Settings”.

Put “81” in the “Web Server Port” and substitute “Overwrite if Names are the same” in the “Publisher” tab (Fig. 2.7).

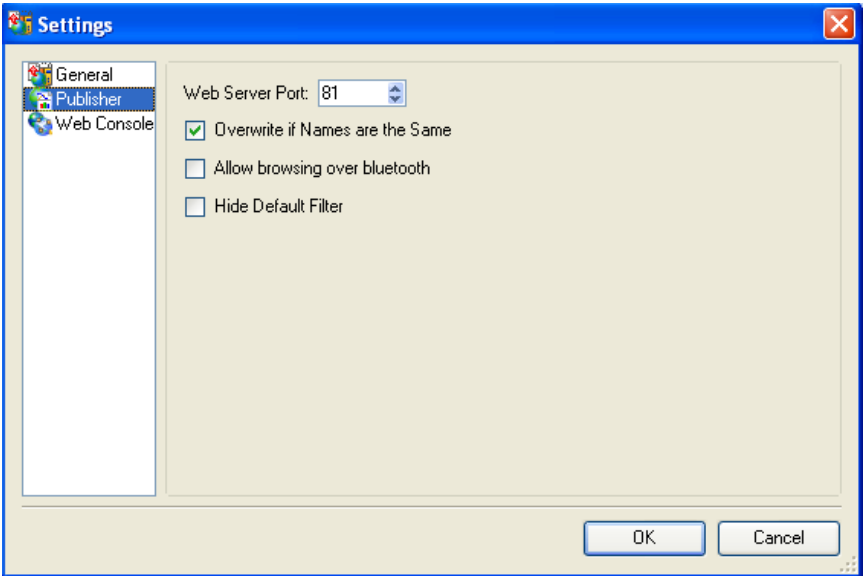

Fig. 2.7 – “Publisher” editing window

Install “82” in the “Web Server Port”, “8080” – in the “Proxy Server Network Port” and “Infinity” – in “Proxy Server Keep Alive Timeout” in the “Web Console” tab (Fig. 2.8). Click “OK” when the setup is complete.

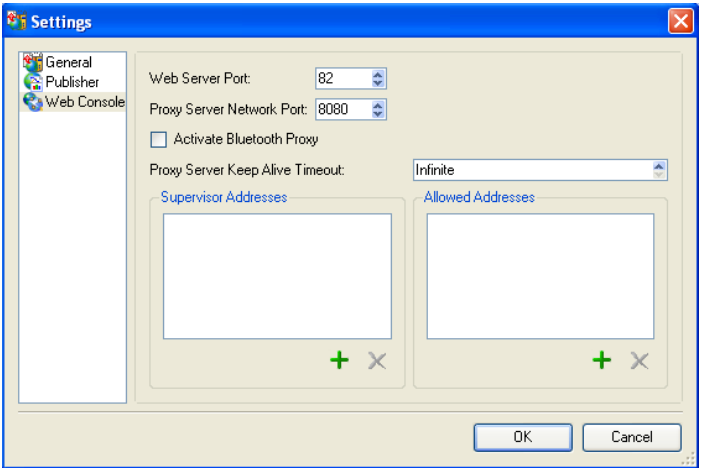

Fig. 2.8 – "Web Console" editing window

Let's launch the Web server (click on the corresponding shortcut with the running person). Open the "Web Console" tab from the main menu and insert the "EmbededConsole_2" node from the TRACE MODE project folder. To do this, firstly, indicate the name and path to the .dbb file from the "EmbededConsole_2" folder of the TRACE MODE project for control of the pyrolysis installation (Fig. 2.9).

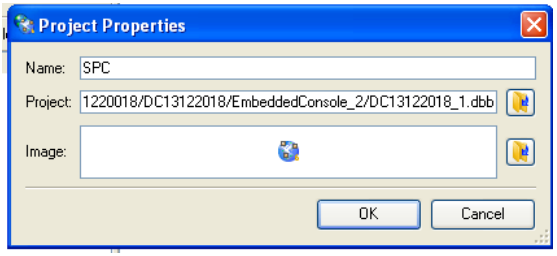

Fig. 2.9 – Window of "Embedded Console" node connection

Open Internet Explorer with the installed JAVA virtual machine. In the address line place the IP addresses of the computer with the installed web-server TRACE MODE Data Center and add at the end: "82", so "http://192.168.86.131:82" is obtained. Then press "SPC" and go to the web-human-machine interface (Fig. 2.10).

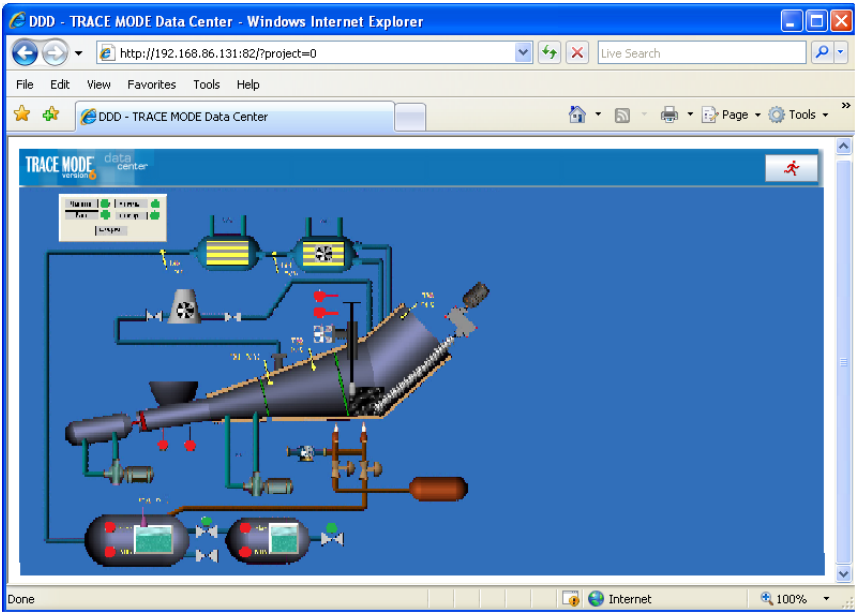

Fig. 2.10 – Web-human-machine interface for the control system of the specialized pyrolysis complex

An operator should click “Start server” (a shortcut with a running person) to work with the web-man-machine interface and click “Stop server” (a shortcut with a person standing) to stop working.

Tasks for extracurricular work

Perform connection of the local SCADA system of the specialized pyrolysis complex to the TRACE MODE Data Center web server by each participant of the training.

Report

The report should contain:

- title page with the name of the training work;
- aim of the work;
- problem statement according to the task;
- the progress and results of the study in graphical form;
- analysis of the results and conclusions.

All materials of the report should be printed, billed, the pages should be numbered.

Test questions

1. How to create a human-machine interface in the TRACE MODE system?
2. What data transfer protocols are used in this training?
3. What web-servers are usually used for industrial automation?
4. What is the TRACE MODE Data Center web server and how to configure it?
5. Why the web server TRACE MODE Data Center should be placed on a separate computer?

Recommended literature

1. Y. Kondratenko, O. Kozlov, O. Gerasin, A. Topalov, and O. Korobko, "Automation of Control Processes in Specialized Pyrolysis Complexes Based on Web SCADA Systems," *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 107-112, September 2017.

2. I. Efimov and D. Soluyanov, *SCADA-system Trace Mode*. Ulyanovsk: UlGTU, 2010. (in Russian).

3. V. Bukreeva and A. Tskhe, *Fundamentals of Tool-System Development of SCADA Trace Mode*, Tomsk: TPU, 2004 (in Russian).

4. A. Alfeo, P. Barsocchi, M. Cimino, D. La Rosa, F. Palumbo, and G. Vaglini, "Sleep behavior assessment via smartwatch and stigmergic receptive fields," in *Personal and Ubiquitous Computing*, vol. 22, no. 2, 2017, pp. 227-243.

5. A. Iqbal, C. Pattinson, and A. Kor, "Introducing controlling features in cloud environment by using SNMP," in *Green IT Engineering: Concepts, Models, Complex Systems Architectures. Studies in Systems, Decision and Control*, vol. 74, V. Kharchenko, Y. Kondratenko, and J. Kacprzyk, Eds., 2018, pp. 147-160.

6. V. Denisenko, *Computer control of technological process, experiment, equipment*. Moscow: Goryachaya liniya - Telekom, 2009. (in Russian).

7. P. Markopoulos, J. Nichols, F. Paternò, and V. Pipek, "Editorial: End-user development for the internet of things," in *ACM Transactions on Computer-Human Interaction*, vol. 24, no. 2, 2017, pp. 1-3.

8. O. Vermesan and P. Friess, *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*. NY: River Publishers, 2016.

9. D. Puthal, R. Ranjan, S. Nepal, and J. Chen, "IoT and Big Data: an architecture with data flow and security issues," in *Cloud Infrastructures, Services, and IoT Systems for Smart Cities. IISSC 2017, CN4IoT 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 189, A. Longo et al., Eds., 2018, pp. 243-252.

Seminar 1

HARDWARE AND SOFTWARE MEANS FOR MONITORING AND CONTROL IN IOT-BASED INDUSTRIAL SYSTEMS

The aim of the seminar: collective acquisition of knowledge and practical skills in the preparation of an essay and the presentation on the development of IIoT monitoring and control systems based on modern hardware and software.

Topic of the seminar. The course structure includes a seminar on the topic: "Hardware and software means for monitoring and control in IoT-based industrial systems". During the seminar, an analysis of current and prospective developments in the field of creating mobile and embedded IIoT systems is performed.

Preparation for the seminar

Preparation for the seminar includes the following steps.

1) Receiving (determining) the topic of the essay (analytical review) and clarifying the tasks of individual work.

Topics of essays can be formed by students independently based on the general structure of IIoT systems building. The IoT-based industrial systems use various networking technologies. Usually, the IIoT monitoring and process control systems consist of three levels (the first level of sensors and actuators, the second level of control, the third level of operators). The first and second levels use industrial networks (Fieldbus), which include Profibus, CANbus, Modbus and many others. At the third level, Ethernet and TCP / IP are most widely used. Wireless technologies are increasingly being used in measurement and control systems at various levels of the hierarchy. The most common technologies for wireless transmission of information in production are: Bluetooth, Wi-Fi, WiMAX, GPRS.

Topics of the essays can also be formed by students on their own based on the following chain of keywords that are somehow related to IIoT:

– automation hardware, programmable logic controllers, input / output modules, single board computers, …;

– automation software, data exchange protocols, human-machine interfaces, programming languages, software development environments, …;

– communications, wired connections, wireless connections, …;

– data processing, system analysis, databases, cloud computing;

– hierarchical control systems, multi-level systems with decentralized data processing.

Examples of essays topics:

– basic concepts and principles of industrial sensor networks;

– methods for data transmission in wired networks of IIoT systems;

– industrial data bus, Modbus, Profibus, CAN;

– serial interfaces RS-232, RS-422, RS-485;

– USB (Universal Serial Bus);

– wireless data transmission technologies, WI-FI, Bluetooth, Zigbee;

– wireless data transmission technologies, GSM, GPRS, 3G, 4G;

– SCADA systems in the concept of IIoT systems;

– real-time monitoring and control technologies;

– advantages and disadvantages of wired and wireless monitoring and control systems in IIoT systems;

– connecting devices to the Internet via CoAP, HTTP, MQTT data transfer protocols;

– overview of hardware of IIoT systems. I/O modules;

– overview of hardware of IIoT systems. Programmable logic controllers;

– overview of hardware of IIoT systems. Gateways;

– OSI network model in modern IIoT systems;

– cloud services: Azure, Thingspeak, Bluemix;

– web SCADA systems and their servers;

– programming languages iec 61131-3 in the concept of IIoT systems;

– work with Big DATA in Cloud Computing;

– information security issues in hardware and software of IoT systems.

Topics of the essays should be coordinated with the lecturer and fully comply with the subject area of the course. In preparing for the seminar should use literary sources.

Theoretical issues for "IoT for Industrial Systems" are described in Part XIV (sections 52-55) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

2) Development of a plan of the work on the essay.

The work is performed collectively, tasks are distributed among teams. Each team consists of 3 people. Time resource is 9x3 = 27 hours (+15 min for presentation). The distribution of responsibility is determined by the team members.

Typical work provides for each team to prepare 3 essays and a general presentation on the development of IIoT monitoring and control systems based on modern hardware and software.

3) Development of the essay plan.

Before to start writing an essay, it is necessary to clearly formulate the task of finding information according to the required essay plan.

The essay plan includes:

– introduction (relevance, brief analysis of the state of the question). In the introduction of the essay, it is necessary to justify the choice of the topic;

– systematic presentation of the main parts of the essay (structures, models, methods, tools, comparative analysis);

– conclusions (ascertaining the achievement of the goal, the main theoretical and practical results, their significance, directions for further work);

– references (paper and digital sources).

– appendix (presentation slides).

4) Writing an essay.

Writing and design of the essay (including the title page, references) should be literate. Use only the material that reflects the essence of the topic.

The essay has a volume of 15-20 pages of A4 format (font 14, 1.5 interval, 2cm margins), including the title page, content, main text, references, appendix.

At the preparation of the essay, it is necessary to use materials of modern publications not older than 5 years. The presentation of the essay should be consistent. Ambiguous language, speech and spelling errors are not allowed. Particular attention should be paid to the conclusion. In the conclusion, the answers to the tasks set in the introduction should be presented. The general conclusion should be formulated and the goal achievement of the essay should be given. The conclusion should be concise, clear and should follow from the content of the main part.

A mandatory attachment to the abstract is the presentation slides and the electronic version of all materials.

5) Preparation of the presentation.

The presentation is developed in PowerPoint and corresponds to a common team work on essays (20-25 slides) based on the time for the presentation – 30 min.

The presentation should include the following slides:

– title slide (indicating organization, department, discipline, topic of the report, author, date of presentation);

– content (structure) of the report;

– the relevance of the issues under consideration, the purpose and objectives of the report;

– slides with the disclosure of the content of the objectives;

– report conclusions;

– list of references.

Each of the slides should contain the footer with the title and author of the report.

The content of the slides should not contain parts of the text from the essay, but include keywords, pictures, formulas.

Submission of information can be dynamic.

6) Presentation.

The presentation (report) is carried out at the seminar, takes 30 minutes and includes the report itself (25 minutes) and discussion (5 minutes). Presentation and essay Language is English.

7) Evaluation.

Evaluation for this work is given to each student from the group of authors of the report individually and takes into account: the quality of the text of the essays (form and content); quality of presentation (content and design); report quality (content, logical structure, division of time, conclusions); completeness and correctness of answers to questions.

The evaluation for the essay and presentation is set for each student from the group of authors of the report individually in accordance with the results and distribution of responsibility.

8) References for seminar preparation.

1. U. Egham, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", *Gartner.com*, 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. [Accessed: 30- Aug- 2018].

2. S. Sulthana, G. Thatiparthi, and R.S.Gunturi, "Cloud and Intelligent Based SCADA Technology," in *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, vol. 2, iss. 3, 2013, pp. 293-296.

3. I. Efimov and D. Soluyanov, *SCADA-system Trace Mode*. Ulyanovsk: UlGTU, 2010. (in Russian).

4. V. Bukreeva and A. Tskhe, *Fundamentals of Tool-System Development of SCADA Trace Mode*, Tomsk: TPU, 2004 (in Russian).

5. R. H. Weber and R. Weber, *Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2010.

6. Z. Aydogmus and O. Aydogmus, "A Web-Based Remote Access Laboratory Using SCADA," in *IEEE Transactions on education*, vol. 52, no. 1, 2009, pp. 126-132.

7. A. Alfeo, P. Barsocchi, M. Cimino, D. La Rosa, F. Palumbo, and G. Vaglini, "Sleep behavior assessment via smartwatch and stigmergic receptive fields," in *Personal and Ubiquitous Computing*, vol. 22, no. 2, 2017, pp. 227-243.

8. V. Miori and D. Russo, "Home automation devices belong to the IoT world," in *ERCIM news*, vol. 101, 2015, pp. 22-23.

9. O. Vermesan and P. Friess, *Internet of Things: Global Technological and Societal Trends from Smart Environments and Spaces to Green ICT*. NY: River Publishers, 2011.

10. Y. Kondratenko, O. Kozlov, O. Korobko, and A. Topalov, "Internet of Things Approach for Automation of the Complex Industrial Systems," *13th International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI'2017, CEUR-WS*, pp. 3-18, May 2017.

11. C. Pattinson and K. Hajdarevic, "Timing considerations in detecting resource starvation attacks using statistical profiles," in *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 2, 2007, pp. 194-205.

12. G. Barbon, M. Margolis, F. Palumbo, F. Raimondi, and N. Weldin, "Taking Arduino to the Internet of Things: The ASIP programming model," in *Computer Communications*, vol. 89-90, 2016, pp. 128-140.

13. R. Minerva, A. Biru, and D. Rotondi, *Towards a definition of the Internet of Things (IoT)*. Telecom Italia S.p.A., 2015.

14. Z. Schreuders, C. Payne, and T. McGill, "The functionality-based application confinement model," in *International Journal of Information Security*, vol. 12, no. 5, 2013, pp. 393-422.

15. H. J. Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," in *International Journal of Distributed Sensor Networks*, vol. 8, iss. 11, 2012, pp. 29-37.

16. A. Kor, C. Pattinson, M. Yanovsky, and V. Kharchenko, "IoT-Enabled Smart Living," in *Technology for Smart Futures*, M. Dastbaz, H. Arabnia, and B. Akhgar, Eds., 2017, pp. 3-28.

17. S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things*. Switzerland: Springer International Publishing, 2017.

18. A. Topalov, O. Kozlov, and Y. Kondratenko, "Control Processes of Floating Docks Based on SCADA Systems with Wireless Data Transmission," *Perspective Technologies and Methods in MEMS Design (MEMSTECH 2016)*, pp. 57-61, April 2016.

19. Y. Kondratenko, O. Gerasin, and A. Topalov, "A simulation model for robot's slip displacement sensors," in *International Journal of Computing*, vol. 15, no. 4, 2016, pp. 224-236.

20. D. Russo, "Domotics and Robotics," in *Dolentium hominum*, vol. 84, 2014, pp. 137-144.