Internet of Things for Ecology,
Safety and Security Monitoring Systems

Internet of Things
for Industry and Human Applications

ALIoT

Internet of Things for Industry and Human Applications

Internet of Things for Ecology, Safety and Security Monitoring Systems

TRAININGS

Funded by the
Erasmus+ Programme
of the European Union

Ministry of Education and Science of Ukraine
National Aerospace University "Kharkiv Aviation Institute"

S.V. Morshchavka, R.K. Kudermetov, I.S. Skarga-Bandurova,
T.O. Biloborodova, A.Y. Velykzhanin, Y.O. Krytska,
V.S. Kharchenko, H.V. Fesenko, D.D. Uzun, O.O. Illiashenko,
O.O. Solovyov, Al-Khafaji Ahmed Waleed

Internet of Things for Industry and Human Applications

Internet of Things for Ecology, Safety and Security Monitoring Systems

Trainings

Edited by V. S. Kharchenko and H.V. Fesenko

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/.416:502.17](076.5)=111
I-73
Reviewers: Dr. Mario Fusani, ISTI-CNR, Pisa, Italy
Dr. Olga Kordas, KTH University, Stockholm, Sweden

I- 73 Internet of Things for Ecology, Safety and Security Monitoring Systems: Trainings /V.S . Kharchenko and H.V. Fesenko (eds.) - Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", 2019. – 119 p.

ISBN 978-617-7361-90-8.

The structure of work on verification of residual knowledge in the course, the corresponding training material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical and practical aspects of IoT application for ecology monitoring systems are presented. The structures, models and technologies for development of IoT-based systems for ecology, safety and security monitoring, advanced techniques and means for design, modernization and implementation of IoT-based systems for ecology, safety and security monitoring, application of IoT technologies in engineering are examined.

The book is intended for MSc and PhD students studying IoT technologies, software and computer engineering and science. It could be useful for lecturers of universities and training centers, researchers and developers of IoT systems.

Fig.: 52. Ref.: 57. Tables: 7.
Approved by Academic Council of National Aerospace University "Kharkiv Aviation Institute" (record № 4, December 19, 2018).

ISBN 978-617-7361-90-8.

Міністерство освіти і науки України
Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський Авіаційний Інститут”

С.В. Морщавка, Р.К. Кудерметов, І.С. Скарга- Бандурова,
Т.О. Білобородова, Я.О. Критська, А.Ю. Великжанін,
Г.В. Фесенко, В.С. Харченко, Д.Д. Узун, О.О. Ілляшенко,
О.О. Соловйов, Ахмед Валід Аль-Хафаджі

**Інтернет речей
для
індустріальних і гуманітарних застосунків**

Інтернет речей для систем моніторингу екології та безпеки

Тренінги

Редактори: Харченко В.С. та Фесенко Г.В.

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

2019

УДК004.415/.416:502.17](076.5)=111
I-73
Рецензенти: Др. Маріо Фузані, ISTI-CNR, Піза, Італія
Др. Ольга Кордас, KTH University, Стокгольм, Швеція

I-73 **Інтернет речей для систем моніторингу екології та безпеки /** За ред. В. С. Харченка та Г.В. Фесенка. - Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. - 119 с.

ISBN 978-617-7361-90-8.

Наведена стр уктур а робіт з перевірки знань з кур су, відповідний тренінговий матеріал, приклади виконання завдань та критерії оцінювання. В процесі навчання аналізуються теоретичні і практичні аспекти використання IoT для систем екологічного моніторингу Вивчаються структури, моделі та технології розробки IoT для систем моніторингу екології та безпеки, сучасні методики і засоби проектування, модернізації та впровадження таких систем, застосування IoT технологій в інженерії інформаційної, функціональної та фізичної безпеки.

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

Книга підготовлена українськими університетськими командами за підтримки колег з академічних закладів країн ЄС, що входять до консорціуму проекту ALIOT.

Книга призначена для магістрантів і аспірантів, які вивчають технології IoT, програмну і комп'ютерну інженерію, комп'ютерні науки. Може бути корисною для викладачів університетів і навчальних центрів, дослідників і розробників систем IoT.

Рис.: 52. Посилань: 57. Таблиць: 7.

Рекомендовано до видання вченою радою Національного аерокосмічного університету імені М.Є. Жуковського «Харківський авіаційний інститут» (протокол № 4 від 19 грудня 2018 г.).

ISBN 978-617-7361-90-8.

INTRODUCTION

The materials of the training part of the study course ITM5 “IoT for ecology, safety and security monitoring 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 ecology, safety and security monitoring systems are presented. The structures, models and technologies, advanced techniques and means for design, modernization and implementation of IoT-based systems for ecology, safety and security monitoring, application of IoT technologies in engineering, development control units for IoT devices for ecology, safety and security monitoring systems are examined.

Theoretical issues for “IoT for Ecology, Safety and Security Monitoring Systems” are described in Part XIV (sections 48-51) 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, 915 p.].

The module ITMM5.1 “IoT systems for controlling small artificial ecological systems” contains two trainings and one seminar. The first training provides a technique of step-by-step calibration and using UAV based IoT system for estimating the parameters of fields and other ecological systems. The second training provides information for development IoT system for controlling greenhouses. The seminar discusses the development of structures.

The module ITMM5.2 “IoT-based water quality monitoring system” contains three trainings.

[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 covers the network operating system, water quality system setup, water sensors setting.

The second training is devoted to the work of AT-commands esp8266.

The third training presents the developed IoT water quality device.

The module ITMM5.3 “IoT-based systems for monitoring of severe accidents” contains two trainings.

The first training provides a set of reliability drone fleets assessment attributes and the main steps of evaluating reliability of a multi-fleet with a reserve drone fleet.

The second training presens reliability models for a multi-fleet of drones with one- and two level system of control stations and formulates recommendations for choice of a structure of system of control stations.

The module ITMM5.4 “IoT based physical security systems of buildings and campuses” contains one training.

The training is devoted to exploration of the known techniques and tools used in physical security systems assessment and presents principles for selection of the correct structural hierarchical scheme for physical security systems.

The course is intended for engineers, developers and scientists engaged in the IoT for ecology, safety and security monitoring systems, for postgraduate students of universities studying in area of ecology, safety and security monitoring systems, as well as for teachers of relevant course.

Training prepared by Assoc. Professor, Dr. S.V. Morshchavka, Assoc. Professor, Dr. R.K. Kudermetov (Zaporizhzhia National Technical University), Professor, DrS. I.S. Skarga-Bandurova, Assoc. Professor, Dr. T.O. Biloborodova, Ph.D. Student A.Y. Velykzhanin, Ph.D. Student Y.O. Krytska (Volodymyr Dahl East Ukrainian National University), Professor, DrS. V.S. Kharchenko, Assoc. Professor, Dr. H.V. Fesenko, Assoc. Professor, Dr. D.D. Uzun, Dr. O.Illiashenko, PhD student O.O. Solovyov, PhD student Al-Khafaji Ahmed Waleed (National Aerospace University “KhAI”). General editing was performed by Head of Computer Systems, Networks and Cyber Security Department of National Aerospace University “KhAI”, Professor, DrS. V.S. Kharchenko and Associate Professor of Computer Systems, Networks and Cyber Security Department of

National Aerospace University “KhAI” H.V. Fesenko.

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.

ITMM5.1. IoT systems for controlling small artificial ecological systems

**Assoc. Prof., Dr. S.V. Morshchavka, Assoc. Prof.,
Dr. R.K. Kudermetov (ZNTU)**

Training 1

USING UAV BASED IOT SYSTEMS

In recent decades, a number of technological changes have taken place in agriculture. Thanks to various “smart” agricultural gadgets, farmers have gained complete control over the process of growing livestock and producing crops.

Appropriate training will enable future specialists to acquire skills in the field of development of agriculture IoT systems. The name and the material of the trainings are closely linked with the scientific, technological, practical and organizational research and development that are carried out by the authors in the framework of the project: Erasmus+ ALIOT project “Internet of Things: Emerging Curriculum for Industry and Human Applications”, 2016-2019 (reference number 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

This module block contains two training and one seminar.

The first training provides a technique of step-by-step calibration and using UAV based IoT system for estimating the parameters of fields and other ecological systems.

The second training provides information for development IoT system for controlling greenhouses.

The seminar discusses the development of structures and models of IoT-systems in the agricultural sector on examples of implementations.

Trainings and seminar goals:

– to familiarize the business user with the short description and basic concepts of the IoT systems and indicate advantages of their using in agriculture applications;

– to master the technique of creating a local IoT system for estimation of fields yields or (and) controlling parameters of artificial ecological systems;

Training and seminar participants: lecturers, scientists, students and post-graduate students, business owners and technical staff of agriculture firms.

This practical module is prepared by author Sergii Morshchavka, Assoc. Prof. or Radioengineering and Telecommunication dept. of National University “Zaporizka Politecnica”.

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

NDVI (Normalized Difference Vegetation Index) – the normalized relative vegetation index is a simple quantitative measure of the amount of photosynthetically active biomass (usually called the vegetation index). One of the most common and used indices for solving problems using quantitative estimates of vegetation cover.

The NVDI can be calculated by formula:

$$NDVI = \frac{NIR - RED}{NIR + RED} \tag{1.1}$$

where: NIR – reflectivity in near-infrared area of spectra;
RED – reflectivity in red area of spectra.

The calculation of NDVI is based on the two most stable parts of the spectral reflection curve of plants. In the red region of the spectrum (0.6–0.7 µm) lies the maximum absorption of solar radiation by chlorophyll of higher vascular plants, and in the infrared region (0.7–1.0 µm) is the region of maximum reflection of leaf cell structures. That is, high photosynthetic activity, that usually associated with the density of vegetation, leads to less reflection in the red region of the spectrum and more in the infrared. The ratio of these indicators to each other allows you to clearly separate and analyze plant from other natural objects. Using not a simple ratio, but a normalized difference between the minimum and maximum reflections increases the accuracy of the measurement, reduces the effect of such phenomena as differences in the illumination of the image, cloudiness, haze, absorption of radiation by the atmosphere, etc.

There is a strong correlation between NDVI and productivity for different types of ecosystems. This property is rather actively used for regional mapping and analysis of various types of landscapes, and for assessing the resources and areas of biosystems at the scale of countries and continents. Being an artificial dimensionless indicator, NDVI is designed to measure the ecological and climatic characteristics of vegetation, but at the same time it can show a significant correlation with some parameters, in a completely different area:

- productivity (temporary changes);
- biomass;
- humidity and mineral (organic) soil saturation;
- evaporation (evapotranspiration);
- the amount of precipitation;
- power and snow cover applications.

Due to all these features, NDVI maps are often used as one of the intermediate additional layers for more complex types of analysis. The results of which can be maps of forest and agricultural land productivity, maps of landscape types, vegetation and natural zones, soil, arid, phyto-hydrological and other ecological-climatic maps. Also, based on it, it is possible to obtain numerical data for use in calculating the estimation and forecasting of productivity and productivity, biological diversity, the degree of disturbance and damage from various natural and man-made disasters, accidents, etc. In general, the main advantage of NDVI is the ease of obtaining it: to calculate the index, no additional data and methods are required, except for the satellite imagery itself and knowledge of its parameters.

Training implementation

Calibrating Camera Multi-spectral (RGN, OCN, NDVI) Images

The first step for obtaining NVDI map is calibrating images used for measuring the reflectance of materials such as vegetation in a crop field.

The Sun emits a large spectrum of light which is reflected by objects on the Earth's surface. A camera can be used to capture this reflected light in the wavelengths that the camera's sensor is sensitive to. The sensors that we supply are based on Silicon which is sensitive in the Visible and Near Infrared spectrum from about 400-1200nm. Using band-pass filters that only allow a narrow spectrum of light to reach the sensor we can capture the amount of reflectance of objects to that particular band of light.

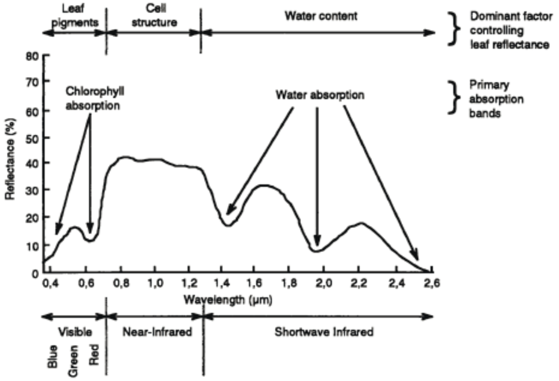


Fig. 1.1 – The spectra obtained by sensors

For instance if the camera's filter selects two 25nm wide bands with peak wavelengths of 660nm and 850nm (see Fig. 1.2) it will only capture the reflected "red" and "near infrared" light emitted by the sun around those wavelength peaks.

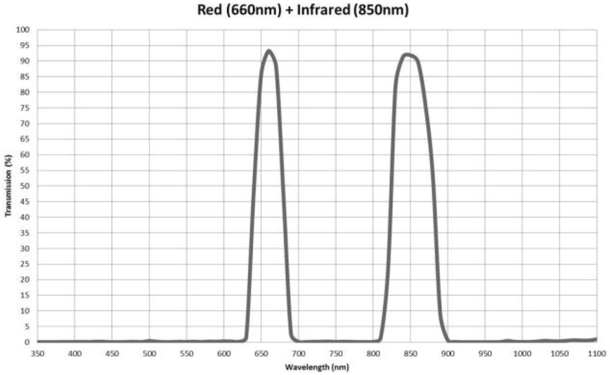


Fig. 1.2 – Two band spectra

These are the peaks in the NDVI (Red+NIR) filter we sell cemented to the bottom of the 3.97mm (recommended), 4.35mm, and 5.4mm lenses. Each pixel in the image's RGB channels is thus a percentage of the reflected light allowed to pass through the filter.

Always set the camera to RAW (DNG) mode for the best results, as calibrating the JPGs will further compress them and it may make it difficult to stitch. If you need JPGs as the final result (such as for online services like Drone Deploy) you can save the TIFFs as JPGs during calibration.

It is important to also make sure the camera settings (shutter speed, ISO, EV, White Balance) are adjusted so that no pixels reach the maximum pixel value. If a pixel would normally be higher than the max value the information will be lost. Here are the recommended settings to use (required if not using our reflectance calibration target):

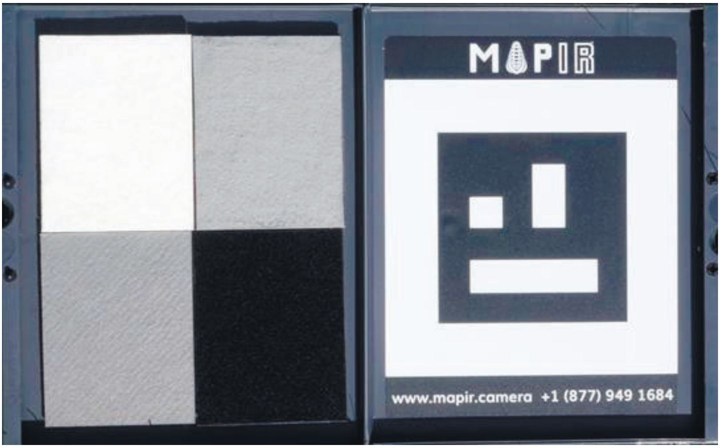
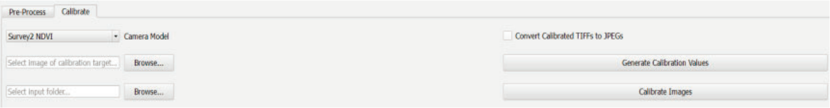


Fig. 1.3 – The calibration pattern

The cameras are not "calibrated" from the factory for reflectance calibration. We need something then to calibrate each pixel using a known reflectance value. It will need to do this by capturing a photo of our MAPIR Camera Reflectance Calibration Ground Target Package just before each survey, which contains 3 targets that have been measured at incremental wavelengths by a spectrometer (a calibrated lab instrument). The pixel values of the captured target image are then compared with the known reflectance values of the targets. Using this information in our MAPIR QGIS plugin we then transform the pixel values and thus calibrate the survey images.

Once the images are calibrated you can stitch them together into a single image called an ortho-mosaic, or "ortho" for short. The resulting ortho images can then have some indice calculations performed on the pixels to produce different types of analysis.

After you have pre-processed your images you have the option of stitching them into the final orthomosaic or calibrating each photo before stitching. Typically it's better to stitch the non-calibrated images and then calibrate the orthomosaic due to possible issues with stitching the calibrated images. This is especially important with point-cloud software like Pix4D and Photoscan to calibrate after ortho generation. To begin calibration, open the QGIS MAPIR plugin and click on the Calibrate tab (Fig. 1.4):



Survey2 NDVI Camera Model

□ Convert Calibrated TIFFs to JPEGs

Fig. 1.4 – The calibration settings

Select camera model from the drop-down menu. If the MAPIR Camera Reflectance Calibration Ground Target Package taken before the survey (recommended) then it needs to click the first Browse button and select the QR target image. When the software has detected the QR target the dialogue box on the right will let you know if it was successful. If none of the images is able to be used to detect the QR code the program will use hard-coded values which were obtained during a clear sunny day. There may be a slight inaccuracy if the hard-coded values are used so make sure to capture a few good images of the target shortly before your survey for the best results.

After the plugin has obtained the necessary calibration values click the lower Browse button to select the input image directory. A Calibrated folder will be automatically created in the input folder for the calibrated images. If you would like the calibrated TIFFs to be converted to JPGs please select the "Convert Calibrated TIFFs to JPGs" box. To begin calibration please selects the "Calibrate Images" button.

Further Processing Calibrated Images

Each pixel in the images now represents a percentage of reflectance for the photographed area. They may be dark (not bright), but don't worry this is normal. Remember, you are capturing reflectance information, not a 'pretty picture".

You will now want to upload the images to the software you are choosing to generate the ortho-mosaic image.

Drone Deploy supports NDVI (Red+NIR) filter setup and it's an easy way to get calibrated NDVI results. Once processed simply choose the Plant Health feature, choose the RGN filter and the the NDVI index. If you are not processing your images in Drone Deploy, you will need to stitch the ortho-mosaic using your own software (ie Pix4D) and then process the NDVI index yourself. The reflected red light will be in the image's red channel and the reflected NIR light will be in the blue channel. Using the NDVI formula (1.1) the next image can be created:

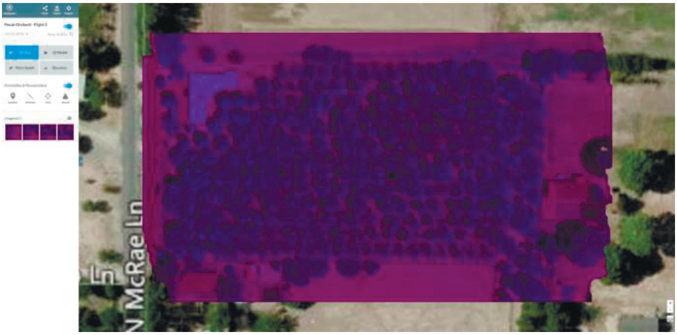


Fig. 1.5 – Camera DJI Phantom 3-3.97mm NDVI

Pix4D is software that takes images and finds thousands of common points, or matched keypoints, between the images. These matched keypoints, where 2 keypoints on 2 separate images are the same, are used to create one 3D point. If there is a lot of overlap between the images then more keypoints can be matched, as shown in Fig. 1.6. Recommended overlap in general is at least 75% frontal, and 60% side overlap. Images should be collected in a grid-like manner, with a constant height. Pix4D can process multiple flights, but much like a single flight, the pilot should undertake it with enough overlap between the images, and in the same conditions (height, sun light, weather, etc.).

This is a general recommendation. Requirements change depending on what kind of terrain is being anazlyed. If it is snow and sand, then high overlap is needed, as the snow and sand blends together more and common points are harder to find, with at least 85% frontal and at least 70% side overlap and high contrast. The same is true with uniform fields. When terrain is so similar it is difficult to find common keypoints. For uniform fields (like agriculture fields), over lap should be the same as snow and sand, at 85% frontal and 70% side. The more overlap the better the resulting 3D image. Frontal overlap follows the flight path, where as side is at a right angle to the path.

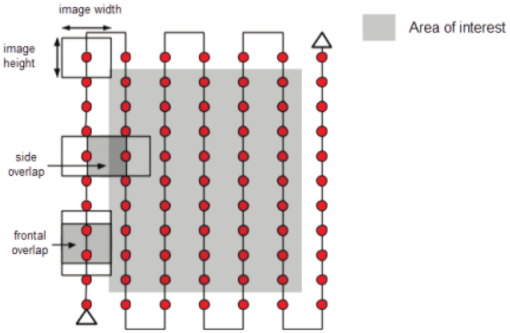


Fig. 1.6 – The overlap of keypoints in the area of interest

Using Pix4D, it possible to create 3D images of terrain. This allows the use of DSMs, or Digital Surface Models. A DSM gives a better idea of elevation of the surface, including things other than the terrain, such as buildings and trees.

Because many pictures with high resolution are taken, processing can take a long time. In the case of this lab, initial processing took around 10 minutes, but for larger projects processing can take days. Rapid check can be used to speed the process up, however, the image scale is set lower than full and thus resolution and accuracy is not as high. This is okay to use in the field, as it can give a good indicator on the quality of the data set.

Pix4D can process oblique imagery, or images taken at an angle instead of straight down, as shown in Fig. 1.7. To do so, there must be enough overlap between datasets and GCPs (ground control points) or manual tie points should be used so that the images can be adjusted properly.

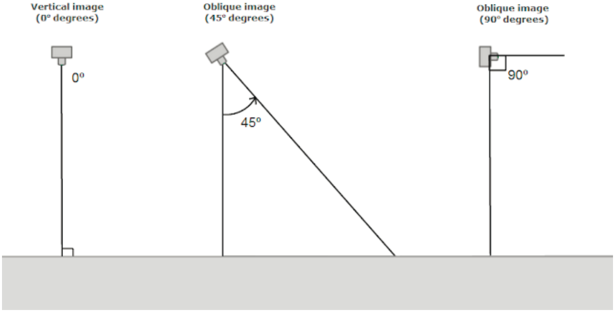


Figure 1.7 – The angles fir capturing images

GCPs are not required, but very highly recommended with processing an image that has no geolocation information attached to it. GCPs are points within the area of interest where the coordinates are known, having been measured with traditional survey methods or through other sources. If there is no geolocation information, and no GCPs, then the final results will have no orientation, scale, or absolute position information. These results cannot be used for overlay, measurements, or comparison with other results. The reconstruction in 3D might not preserve the shape of the area of interest as well. GCPs should be placed evenly within the area of interest as shown in Fig. 1.8, and a minimum of 3 is required, while 5 is recommended.

Methods - Using Pix4D

In this lab the imagery being processed is geotagged, or has geographic location information attached, but there are no ground control points. The steps used in Pix4D Mapper to process the images are below.

First a new project was created. The project name should include the date, site the photos were taken, the platform used, and the altitude, as shown in Fig. 1.9.

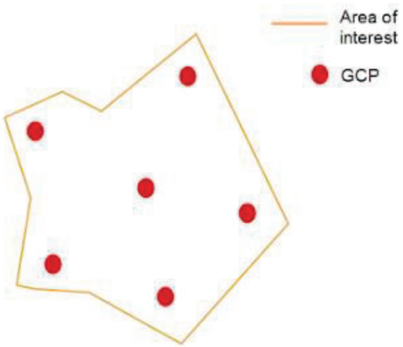


Fig. 1.8 – The spaced out Ground Control Points

20160621_litch_rs_phantom3_60m.p4d 3/8/2017 4:52 PM P4D File

Fig. 1.9 – The date, site, username, platform, and altitude are used to name the P4D file

After this the images for processing must be added. If they are in a file directory it possible add them that way, otherwise they can be manually added. These images have .exif data attached to them; the .exif data is the metadata of the image. This notes the geographic coordinate system, and if the images are geotagged. The camera model and information is also there, but can be inaccurate. This information should be double checked before the processing is done. In the case of this particular data set, the only thing that needed to be changed was the shutter model, which was changed from global shutter to linear rolling shutter. Processing templates are available that have preset processing information and outputs. The 3D Maps template was used for this project. Once the preliminary settings are selected processing can begin.

A maps screen will pop up when clicked the final finish. Before complete processing is done, initial processing should be completed. This gives a good idea of the quality of the data. This initial processing is shorter than total processing, and can provide quick feedback to the user if more data is needed.

Once initial processing is completed, a quality report is produced. This report contains valuable information regarding the data set, such as a quality check, initial image positions, overlap, camera parameters, geolocation details, and various statistics. It includes how many images were included, and how many were rejected.

Any problems that come up with the data set will be in the initial report and are suggested to be addressed before a final processing is completed. Final processing will take longer than initial processing. What the program looks like when running this processing is show in Fig. 1.10.

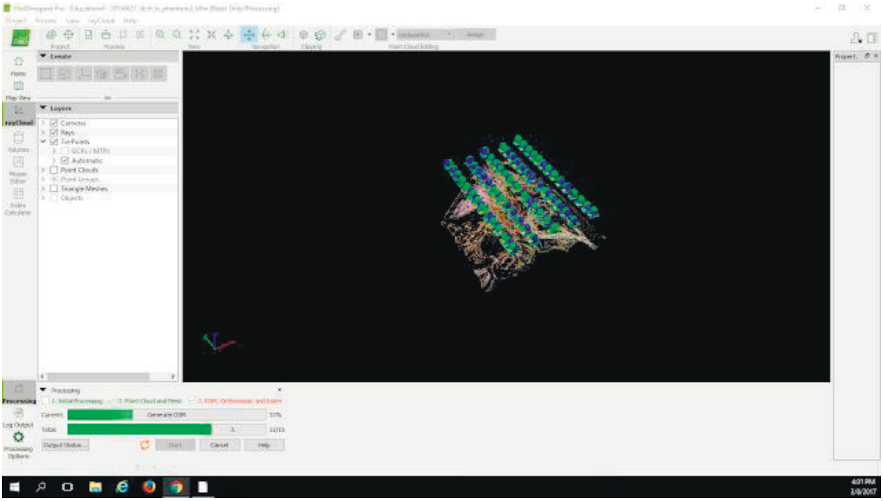


Fig. 1.10 - The visualization of keypoints and where the photographs were taken

Once final processing is done, a DSM is created, as shown in Fig. 1.11, which can be added into ArcMap to manipulate for different needs.

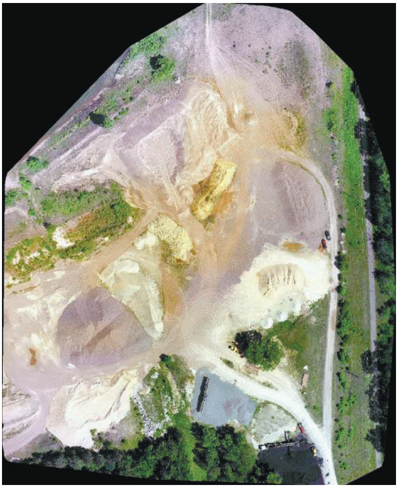


Fig. 1.11 – Overlay of the DSM produced by Pix4D from the images taken by the Phantom drone

Pix4D also provides the ability to create a video of the drove flyover. The resulting DSM can be added into ArcMap and a map can then be created, as shown in Fig. 1.11.

Conclusion

Pix4D appears to be a very useful tool in the geographer's toolbox. It is user friendly and creates easy to work with models that can be used in ArcMap to be further analyzed. Only the surface of Pix4D was touched in this lab, as the majority of the features it possesses were not utilized, especially since GCPs were not used in the imagery. As a result, this review of the software is only basic and not to be seen as an exhaustive review.

Tasks for extracurricular work

Process the proposed by teacher image set with calibration and making NVDI and DSM images.

Report

The report should contain:

- title page with the name of the training work and the contractor;
- aim of the work;

- 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 NVDI?
2. How NVDI map can be used?
3. Why is needed the calibration?
4. What are possibilities of Pix4D software?
5. What are keypoints and Ground Control Points?

Recommended literature

1. Muneza et al. (2015). A Photogrammetry Approach for Map Updating using UAV in Rwanda. GeoTechRwanda, 1-8.

2. Agisoft (2013). Agisoft PhotoScan User Manual: Professional Edition, Version 1.3. Retrieved from http://www.agisoft.com/pdf/photoscan_python_api_1_3_0.pdf

3. Pérez M., Agüera F., Carvajal F. Low cost surveying using an unmanned aerial vehicle. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. XL1/W2, UAV-g, Rostock, Germany, 2013.

4. Yun M., Kim J., Seo D., Lee J., Choi C. Application possibility of smartphone as payload for photogrammetric UAV system. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. 39, Issue B4, 2012, p. 349-352.

Training 2

USING LIBELLIUM WASPMOTE AGRICULTURE SET

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

Considering the steps of data sensing, data acquisition, data communication and data processing for smart farming applications, here the whitepaper discusses how Libelium technologies provide all the elements for smart agriculture implementations. Libelium's Waspmote provides everything that is needed to collect, forward and store data collected from remote sensors.

Data Collection.

The data collection phase consists of sensors, devices and gateways. Sensors differ in type and amount of data they are collecting, intervals of collection, and power source – e.g. battery or solar. Libelium's Waspmote Agriculture 2.0 Board (see Fig. 2.1) collects multiple environmental parameters for "Libelium's Waspmote provides everything that is needed to collect, forward and store data collected from remote sensors" a range of agricultural applications, from analysing plant growth to weather observation.

For this reason, sensors are configured to collect data for various applications. Types of data collected include air and soil temperature and humidity, luminosity, solar visible radiation, wind speed and direction, rainfall, atmospheric pressure, leaf wetness and fruit or trunk diameter measurement (dendrometer).

The main applications for Waspmote Plug & Sense! Smart Agriculture are precision agriculture, irrigation systems and greenhouses. Fig. 2.2 shows a Waspmote mounted on a post, measuring airborne parameters. Libelium Waspmote Plug & Sense! allows to control the amount of sugar in grapes to enhance wine quality, as well as to control micro-climate conditions to maximize the production in greenhouses.

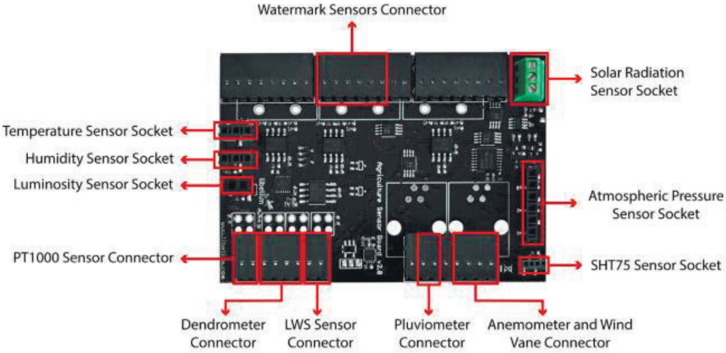


Fig. 2.1 - Libelium main PCB

Source: Libelium

Fig. 2.2 - Waspmote Powered by Solar Panel

The three levels of depth of the soil moisture sensor are helpful to reduce waste of water by selective irrigation in dry zones. On the other hand, controlling humidity and temperature levels in hay or straw can prevent fungus and other microbial contaminants.

Libelium has also developed a Plug & Sense! application model for Smart Water which is suitable for potable water monitoring, chemical leakage detection in rivers, fish tank and aquaculture monitoring, remote measurement of swimming pools and spas and levels of seawater pollution. In Precision Farming is applied specially to control and monitor irrigation systems.

Sensor probes can be easily attached by screwing them into the bottom sockets of the platform. Developers can add new sensing capabilities to existing networks, to cater for changes in requirements; likewise sensor probes may be easily replaced in order to ensure the lowest maintenance cost overall of the sensor network. Libelium's preconfigured sensor devices make deployment easier, so as to also ensure minimum maintenance costs.

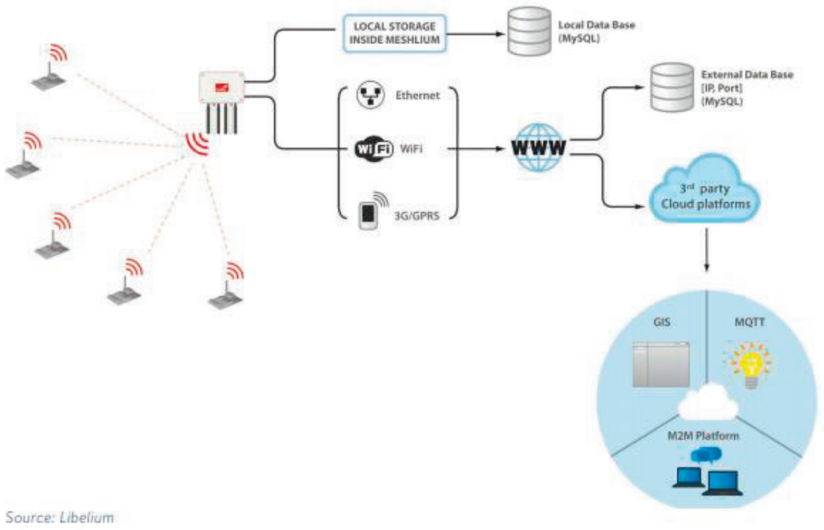
Data Communications, storage and processing

The Libelium architecture is network agnostic. In fact, Waspmote supports the following radio interfaces: XBee-ZigBee, LoRaWAN, Sigfox, WiFi, Bluetooth Low Energy, GPRS and all cellular connectivity from 2G to 4G. Therefore, the distances supported range from 100 metres (Bluetooth) to 100 km (cellular connectivity). Fig. 2.3 shows a schematic of the total Libelium connectivity architecture, from data collection to forwarding to storage to the Cloud and M2M analytical platform.

Meshlium is a multi-protocol router which works as the Gateway of the Waspmote Sensor Networks. It can contain 6 different radio interfaces: WiFi 2.4GHz, WiFi 5GHz, 3G/GPRS, Bluetooth, XBee and LoRaWAN. As well as this Meshlium can also integrate a GPS module for mobile and vehicular applications and be solar and battery powered.

A ready-to-be-deployed Smart Agriculture Solution Libelium launched on March 2016 The IoT Marketplace [1], a one-stop click-and-buy-store, offering complete Internet of Things solutions ready to deploy smart applications including hardware, software and cloud connection. Libelium has partnered with several cloud software solution providers to offer ready interoperability with systems such as AWS, Microsoft Azure, ESRI, IBM Bluemix, Indra, ThingWorx and others. The kits includs a number of components, but also the necessary documentation and Libelium technical support in order to enable companies to develop their own applications.

One of the aims of the company is to facilitate the access to develop new IoT solutions for Agriculture market with an out-of-the-box kit that enables to monitor environmental parameters in farming, vineyards, greenhouses or golf courses. Developers and System Integrators use this kit to make Proof of Concepts to test business cases before going for massive deployments. Libelium Smart Agriculture Vertical Kit allows controlling different parameters such as soil moisture, temperature, humidity, leaf wetness or atmospheric pressure



Source: Libelium

Fig. 2.3 - Libelium Meshlium Connectivity Option

Training implementation

Waspmote Plug & Sense! can be reprogrammed in two ways. First, the basic programming is done from the USB port.

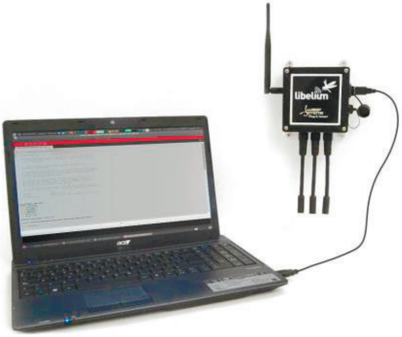


Fig. 2.4 – Programming the node

Just connect the USB to the specific external socket and then to the computer to upload the new firmware. Over the Air Programming (OTAP) is also possible once the node has been installed (via WiFi or

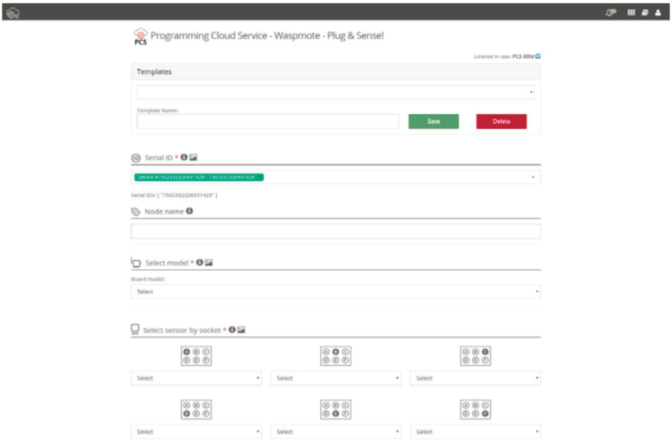
4G radios). With this technique you can reprogram, wireless, one or more Waspmote sensor nodes at the same time by using a laptop and Meshlium.

The second way - the Programming Cloud Service is an intuitive graphic interface which creates code automatically. The user just needs to to fill a web form to obtain binaries for Plug & Sense!. Advanced programming options are available, depending on the license selected. Check how easy it is to handle the Programming Cloud Service at: https://cloud.libelium.com/

The installing required software:

a) Installing Waspmote. The next step is to unzip the downloaded file to the chosen folder. This folder includes the drivers needed in the next step to install the USB and FTDI converter.

b) Connecting a Waspmote board. When connecting a Waspmote board using the mini-USB connector, the message "New device found" will appear. A window will open for the installation of this device. Select the option "Not right now" and press the 'Next' button.



Programming Cloud Service - Waspmote - Plug & Sense!

License in use: PCS Elite

Serial IDs: ["75023323269331429"]

Board model: Select

Fig. 2.5 – Programming cloud service

Next select the path where the drivers for the FTDI converter are. These drivers are in the folder where Waspmote was unzipped. Then proceed to the installation of the FTDI converter drivers, which shows the following message when finished.

Once installation is finished, the message 'New device found' will appear, referring to the USB. The same process carried out for the FTDI converter must now be followed, choosing the same options in all the windows. The path for the drivers is the same as that previously specified.

Once this installation is finished, a message will appear indicating the correct installation of the USB. Once both devices are correctly installed, the port on which the Waspmote board has been installed will appear in the “Device Administrator”.

Installing gateway.

Waspmote comes preconfigured from factory with a program which lets you check the right operation of the device. This program sends standard frames to the Gateway. It is called wasp_pro_test_code.pde and available inside the IDE and on this link: www.libelium.com/development/waspmote/examples/waspmote-pro-test-code

This program sends wireless frames for the following radio modules:

- XBee 802.15.4
- XBee 868MHz
- XBee 900MHz
- XBee Digimesh
- XBee ZigBee
- LoRa

For other modules, the program works, but connectivity is limited to send frames via USB.

Steps:

1. Install the drivers and the serial monitor software on the computer.

2. Connect the antennas and the rest of the desired components to Waspmote and Waspmote Gateway.

3. Plug Waspmote Gateway to the USB port on the computer.

4. Launch the serial monitor application and set the next parameters:

- USB port: 115200bps
- 8 bits
- 1 bit stop
- no parity setting

5. Connect the batteries to the Waspmotes.

6. Switch Waspmotes to the ON position.

When the program starts, it executes sequentially these actions:

- State 1 – Leds ON for 5 seconds
- State 2 – Leds blinking for 3 seconds
- State 3 – Sending messages

State 1 and 2 are only executed once (when program starts) whereas state 3 will loop indefinitely every second (if we reset Waspmote, the program starts again).

Every packet contains a message with sensor data formatted as Waspmote Data Frame. The sensor fields added to the frame are: Accelerometer values, RTC internal temperature value, and battery level. In the case the XBee is not using DigiMesh protocol, then the MAC address is added (because of length constraints). For further information, please check the Waspmote Data Frame Guide: http://www.libelium.com/development/waspmote/documentation/programming

Receiving Frames from Waspmote

Example:

~\0x00I\0x90\0x00}3\0xa2\0x00@z\0xcb\0x92\0xd8\0xd3\0x02<=>\0x80\0x03#35689722##7#ACC:80;10;987#IN_TEMP:22.50#BAT:93#\0xb4

Initially there are some hexadecimal characters, which belong to the frame header, followed by the message. In the above example the message is:

<=>\0x80\0x03#35689722##7#ACC:80;10;987#IN_TEMP:22.50#BAT:93#

To use the Waspmote-IDE compiler we must run the executable script called ‘Waspmote’, which is in the folder where the compiler has been installed.

Compiling a New Program

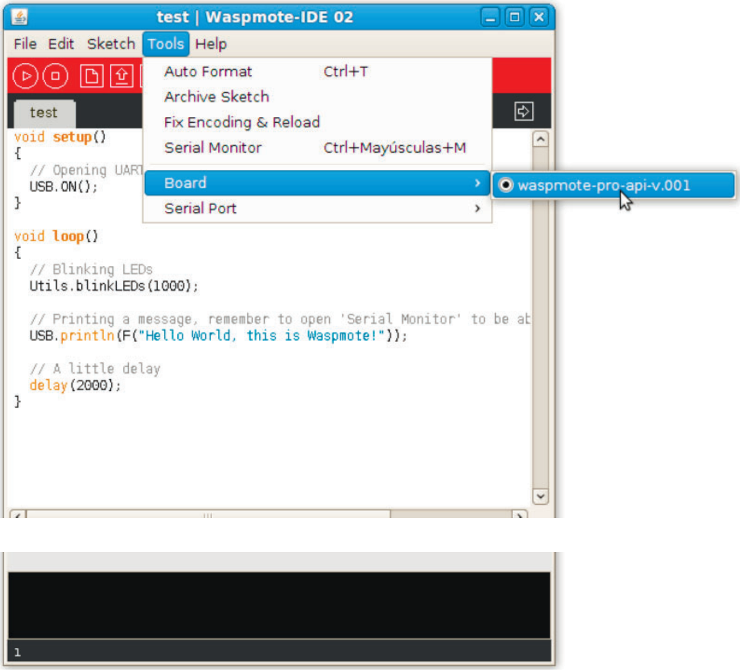
Once the program has been opened correctly some configuration changes must be made so that the programs load correctly in Waspmote.

In the ‘Tools/Board’ tab the Waspmote board must be selected. This refers to the API selected.

Once these 2 parameters have been configured we can load a program onto Waspmote. The process will be explained using a very simple example. A series of examples for learning and familiarizing yourself with the Waspmote environment have been included in the downloaded file that contains the compiler.

The simplest example is the file called ‘test.pde’. In this example the text string “Hello World!” appears on the screen. The example shows how to load a program onto Waspmote and how to show information on the screen.

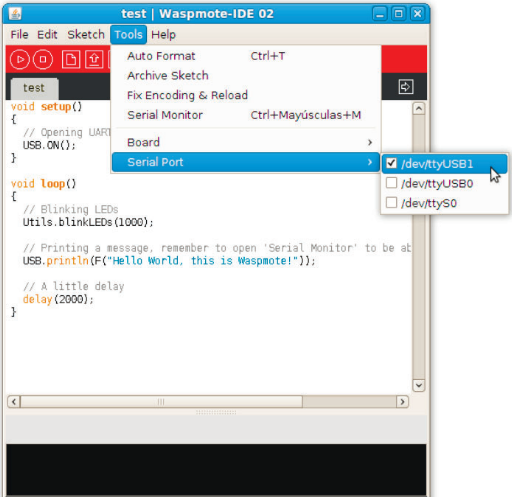
The next step is to configure the folder where the created programs are going to be saved. In the Waspmote-IDE this folder is called ‘sketchbook’ and can be configured by accessing the ‘File/Preferences’ tab. Clicking on this tab will open a new window where the location of the sketchbook can be indicated. Once the sketchbook folder path is indicated, the downloaded test program must be saved in this folder.



```
void setup()
{
  // Opening UART
  USB.ON();
}

void loop()
{
  // Blinking LEDs
  Utils.blinkLEDs(1000);

  // Printing a message, remember to open 'Serial Monitor' to be ab
  USB.println(F("Hello World, this is Waspmote!"));

  // A little delay
  delay(2000);
}
```

Fig. 2.6 – Select API

In the ‘Tools/Serial Port’ tab, the USB to which Waspmote has been connected to the computer must be selected.



```
void setup()
{
  // Opening UART
  USB.ON();
}

void loop()
{
  // Blinking LEDs
  Utils.blinkLEDs(1000);

  // Printing a message, remember to open 'Serial Monitor' to be at
  USB.println(F("Hello World, this is Waspmote!"));

  // A little delay
  delay(2000);
}
```

Fig. 2.7 – Select USB port

Waspmote-IDE must be closed so that the changes and the newly saved program in the sketchbook folder are reflected. Run Waspmote again and open the downloaded test program by clicking on ‘Open’. Select the ‘test.pde’ file in the path where it has been unzipped and open it. As can be seen, it is a very simple code which lights up a LED every 3 seconds and writes “Hello World!” on the screen. The next step is to load the program onto Waspmote. To do this Waspmote must be connected to the computer through the USB and the button ‘upload’ must be clicked. Then, it will start compiling the program. When the program has been compiled correctly, a message will appear on the lower part of the window indicating this event. Conversely, if a fault occurs, red messages will appear indicating the bugs in the code. When compiling is over, the code will be loaded onto Waspmote. When the program has been loaded correctly, a message appears in the Waspmote window indicating ‘Done Uploading’. Conversely, if some problem occurs during loading, red messages will appear indicating the failures.Once this program is loaded onto the board, the loaded code will run as was explained in the Architecture and System chapter

Uploading a New Program to Waspmote

The following steps must be done each time we must upload code, always:Step 1: Switch Waspmote ON (in the image, move the switch to the left).

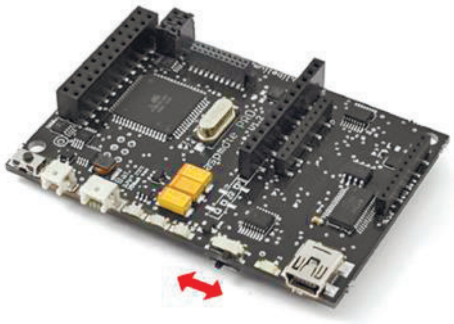
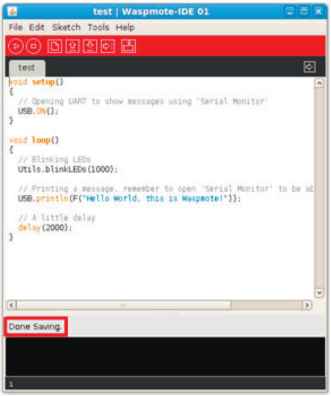


Fig. 2.8 – Switch Waspmote ON



```
void setup()
{
  // Opening UART to show messages using 'Serial Monitor'
  USB.ON();
}

void loop()
{
  // Blinking LEDs
  Utils.blinkLEDs(1000);

  // Printing a message, remember to open 'Serial Monitor' to be ab
  USB.println(F("Hello World, this is Waspmote!"));

  // A little delay
  delay(2000);
}
```

Done Saving.

Figure 2.9 – Save program

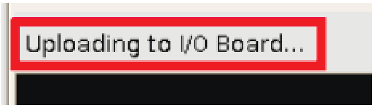
Step 2: Connect Waspmote to your PC through the USB cable. Open the Waspmote's IDE and select the proper Board and Serial Port with in the "Tools" menu.

Step 3: Prepare your code for Waspmote. In our case, go to the template of the "hello_world" or copy and paste the text in the sketch.

Step 4: Save the sketch (the IDE has a button for that), for example with the name "hello_world", and check the IDE states "Done Saving".

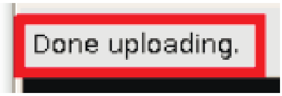
Step 5: Compile the code (the IDE has a button for that), and check there are no errors or warnings. The IDE should say "Done Compiling".

Step 6: Upload the code to Waspmote: click the "Upload" button and wait a few seconds until the process ends; check there are no error messages, just "Done uploading".



Uploading to I/O Board...

Fig. 2.9 – Upload your program



Done uploading.

Fig. 2.10 – Program uploading done

The next steps depend on what kind of project you want to develop. Normally, a program for Waspmote is composed of 4 parts:

1. configuration (RTC, sensors, communications module)

2. read sensor(s)
3. communications (XBee, LoRa, WiFi, GPRS, ...)
4. enter sleep mode

This steps are Hardware Depended and reading Waspmote Technical Guide gives all needed information on them.

Tasks for extracurricular work

Configure the Libelium Smart Agriculture Kit and create a connection to the Internet for a given combination of sensors.

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 sensors provided in Waspmote Plug & Sense! Smart Agriculture?
2. What are interfaces can be used in Waspmote Sensor Networks?
3. What iare main applications for the Waspmote Plug & Sense! Smart Agriculture?
4. Where is data from sensors collected?
5. What are the advantages of using Libellium Kits for implementations the IoT projects in agriculture?

Recommended literature

1. The IoT Marketplace of Libelium. https://www.the-iot-marketplace.com/

2. Karimov, Akmal, et al. "A water accounting procedure to determine the water savings potential of the Fergana Valley." Agricultural water management 108 (2012): 61-72.

3. Savic T., Radonjic M., "Proposal of Solution for Automated Irrigation System", Proc. of 24th Telecommunication Forum TELFOR 2016, Belgrade, Serbia, November 2016.

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

Seminar 1

IOT SYSTEMS’ STRUCTURES AND MODELS IN INDUSTRY APPLICATIONS

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 directions of the development agricultural IoT systems

Examples of essays topics:

- Forest Fire Detection: Monitoring of combustion gases and preemptive fire conditions to define alert zones;
- Air Pollution: Control of CO2 emissions of factories, pollution emitted by cars and toxic gases generated in farms;
- Snow Level Monitoring: Snow level measurement to know in real time the quality of ski tracks and allow security corps avalanche prevention;
- Landslide and Avalanche Prevention: Monitoring of soil moisture, vibrations and earth density to detect dangerous patterns in land conditions;
- Earthquake Early Detection: Distributed control in specific places of tremors. IoT technology as means of industrial modernization;
- Wine Quality Enhancing: Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health;
- Green Houses: Control micro-climate conditions to maximize the production of fruits and vegetables and its quality;
- Golf Courses: Selective irrigation in dry zones to reduce the water resources required in the green;
- Meteorological Station Network: Study of weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes;
- Compost: Control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants;
- Hydroponics: Control the exact conditions of plants grown in water to get the highest efficiency crops.
- Offspring Care: Control of growing conditions of the offspring in animal farms to ensure its survival and health.

- Animal Tracking: Location and identification of animals grazing in open pastures or location in big stables.

- Toxic Gas Levels: Study of ventilation and air quality in farms and detection of harmful gases from excrements.

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.

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 5-10 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.

The example of such a shortened essay with some plan demonstration is given below.

WASTEWATER IRRIGATION MONITORING

Background

Pacific Environment is an environmental technology and consulting company based in Australia, with a client base world-wide. The company is composed of staff with expertise in a number of areas, including economists and scientists. The client, AJ Bush (Manufactures) Pty, a meat rendering company based in Australia sought the assistance of Pacific Environment to undertake a series of modeling and monitoring studies, in response to an Environmental Protection Order issued by the Queensland Department of Environment and Heritage Protection.

Organic wastes from such facilities pose significant environmental management challenges. The management of soil moisture in wastewater irrigation is essential for the protection of groundwater from nitrate contamination.

Initiation of development of the project

The project area covers approximately 500 hectares, of which about 160 hectares will be irrigated with treated wastewater from cattle farming. The team became aware that a real-time monitoring platform would enable AJ Bush to effectively manage their wastewater irrigation, without impacting the receiving environments of soils, groundwater and nearby creeks.

The solution only took a few weeks to develop, given that Pacific Environment knew what sensors were needed, the best location for the sensors to collect the necessary data, and had its decision support system to transform raw data into environmental and operational intelligence.

Development of the solution

The decision support part of the solution was based on Pacific

Environment's EnviroSuite, a proactive environmental management system that combines real-time monitoring and predictive modelling with high resolution weather forecasting and automated data analysis. The sensors network was sourced from Libelium's Plug & Sense. The client purchased all the components of the solution from Pacific

Environment

Libelium's Plug & Sense! Smart Water sensor network was installed in the wastewater irrigation area. This comprises sensors that measure electrical conductivity, temperature and dissolved oxygen.

Through the real-time monitoring of water quality, the sensor network provides an early warning system for potential surface water contamination. The plan is to install additional sensors for the measurement of nitrate, pH and flow in real-time.

Installation details

Starting in early 2016, Pacific Environment's field scientists installed the sensors and related communications equipment, with some assistance from AJ Bush personnel. To date, the team have installed equipment, initially to assess any site specific teething problems (e.g. curious cows), and to verify the stability and reliability of the data and communications. They envisage that to install the entire 160 hectare site would require two people one calendar month to install.

Customer benefits

The system has the potential to significantly reduce the cost of environmental reporting and compliance, in the broad range of human activities that affect both surface and ground water.

The projected payback for investment in the hardware is approximately 18 months. From then on, AJ Bush estimates it will be making significant savings in reduced lab fees and related sampling costs, as well as being able to maximise the amount of wastewater that they irrigate on their land. The other notable benefit is mitigating their environmental risk by not polluting groundwater and surface water resources with nitrate, in accordance with the Queensland government's environmental protection mandate.

Pacific Environment benefits

For the company, this was a pioneering project in its use of a real-time monitoring intelligence platform as an operational and environmental management tool for wastewater irrigation.

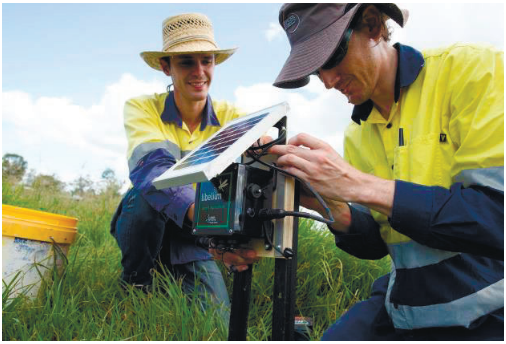


Fig. 3.1 - Libelium sensors and EnviroSuite Agriculture Model being installed at AJ

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.

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.

Recommended literature

5. Y. Liu, C. Zhang, P. Zhu, "The temperature humidity monitoring system of soil based on wireless sensor networks", 2011 International Conference on Electric Information and Control Engineering, pp. 1850-1853, 2011.

P. Kumar, S. R. N. Reddy, "Design and development of M3SS: A Soil Sensor Node for precision agriculture", 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-10, 2016

6. J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay, M. A. Porta-Gandara, "Automated Irrigation System Using a Wireless Sensor Network and GPRS Module", IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 1, pp. 166-176, Jan. 2014.

A. Khattab, A. Abdelgawad, K. Yelmarthi, "Design and implementation of a cloud-based IoT scheme for precision agriculture", 28th International Conference on Microelectronics (ICM), pp. 201-204, 2016.

ITM 5.2 IoT-based water quality monitoring system

Prof., DrS. I.S. Skarga-Bandurova, Assoc. Prof., Dr. T.O. Biloborodova, Ph.D. Student A.Y. Velykzhanin, Ph.D. Student Y.O. Krytska

Training 1

WATER QUALITY SENSORS: CONFIGURATION AND SETTING

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

Goal and objectives: This training includes the study of the network operating system, water quality system setup, water sensors setting.

Learning objectives:

- to study family of water quality electrodes, their functionality, potential for use in IoT system;
- to study operating principle of water quality electrodes relating to IoT based water quality monitoring system.

Practical tasks:

- acquire practical skills in working with series of electrodes;
- perform experiments with different calibration solutions.

Exploring tasks:

- explore the communication tools of the OS to exchange of messages in the network.

Recommended hardware and software:

Name	Link
Arduino UNO R3	https://store.arduino.cc/arduino-uno-rev3
Gravity IO Expansion Shield for Arduino V7.1	https://www.dfrobot.com/product-1009.html
Analog Sensor Kit	https://www.dfrobot.com/product-1797.html
EC, ORP, pH	https://www.dfrobot.com/product-1071.html https://www.dfrobot.com/product-1782.html

USB 2.0 cable type A/B	https://store.arduino.cc/usb-2-0-cable-type-a-b
Jumpers	*Optional*
Breadboard	*Optional*

Theoretical information

Remote monitoring and automatic water quality monitoring process includes the following components:

(1) Wireless acquisition nodes installed in local ponds, and directly connected with the water quality sensors including temperature, water level, PH, DO (dissolved oxygen) sensors to implement the water quality data collection, storage and distribution.

(2) Routing nodes installed between the ponds and monitoring system.

(3) The monitoring system receives the data including water quality data and the node voltage data.

(4) Through the water quality data, monitoring system can manage the water quality environment and decision-making. Send control commands to the control device, and send messages to the user PDA to notify the user, the user can remote control valve by SMS.

In this training, we will focus mostly on the first component, namely water quality sensors.

Training preparation

In preparation for this practical training it is necessary:

- to clarify the goals and mission of the research;
- to study theoretical material contained in this manual, and in [1]-[4]);
- to familiarize oneself with the main procedures and specify the program according to defined task.

Before using the sensors, remove protective cap, then connect the wire as shown below. After completing the measurement, clean the sensor and insert it into the protective cap.

Training implementation

1.Install Arduino IDE. To do this, join the shield to the Arduino.

2.Connect the electrode to the shield in accordance with Fig. 1 and connect the device to the computer.

Arduino GND → EC Board Black Wire

Arduino GND → EC Board Red Wire
Arduino A1 → EC Board Signal Wire

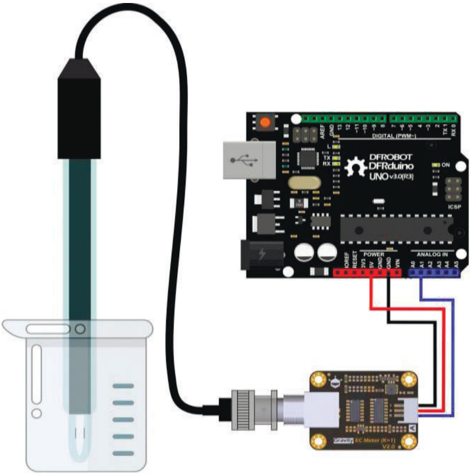
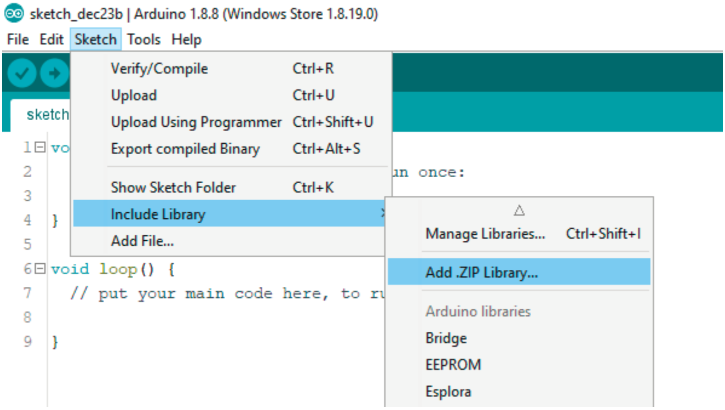


Fig. 1.1 – Electrical Conductivity Electrode connection diagram (Image source: [3])

3. Connect shield to Arduino UNO. Connect electrode to shield.
4. Connect the library (see Fig. 1.1–1.5).


sketch_dec23b | Arduino 1.8.8 (Windows Store 1.8.19.0)
File Edit Sketch Tools Help
sketch
Verify/Compile Ctrl+R
Upload Ctrl+U
Upload Using Programmer Ctrl+Shift+U
Export compiled Binary Ctrl+Alt+S
Show Sketch Folder Ctrl+K
Include Library
Add File...
Manage Libraries... Ctrl+Shift+I
Add .ZIP Library...
Arduino libraries
Bridge
EEPROM
Esplora

```
vo                                  un once:


}

void loop() {
  // put your main code here, to ru

}
```

Fig. 1.2 – Open Add.ZIP Library option

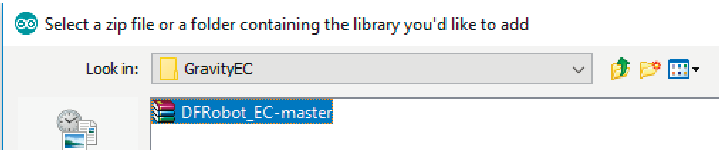

Select a zip file or a folder containing the library you'd like to add
Look in:
GravityEC
DFRobot_EC-master

Fig. 1.3 – Select a zip file or a folder containing the necessary library

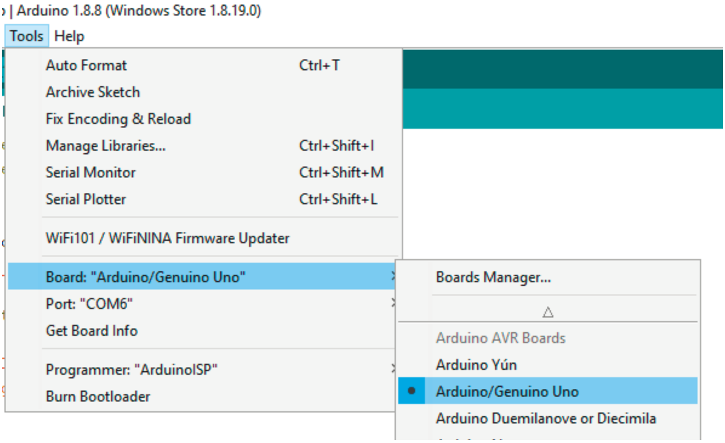

| Arduino 1.8.8 (Windows Store 1.8.19.0)
Tools
Help
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Manage Libraries... Ctrl+Shift+I
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
WiFi101 / WiFiNINA Firmware Updater
Board: "Arduino/Genuino Uno"
Port: "COM6"
Get Board Info
Programmer: "ArduinoISP"
Burn Bootloader
Boards Manager...
Arduino AVR Boards
Arduino Yún
● Arduino/Genuino Uno
Arduino Duemilanove or Diecimila

Fig. 1.4 – Choose the board for your project (Arduino/Genuino Uno)

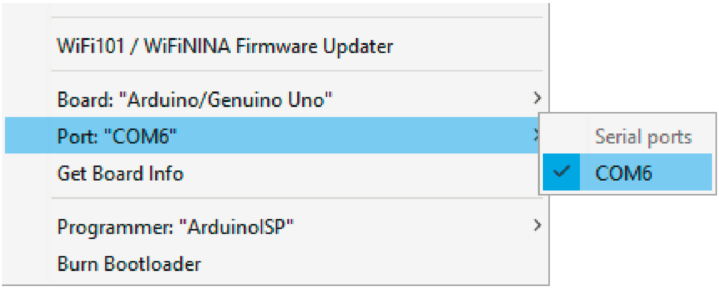


Fig. 1.5 – Select a serial port (COM6)

5.Upload a sketch from Appendix B and select Serial Monitor option (see Fig. 1.6).

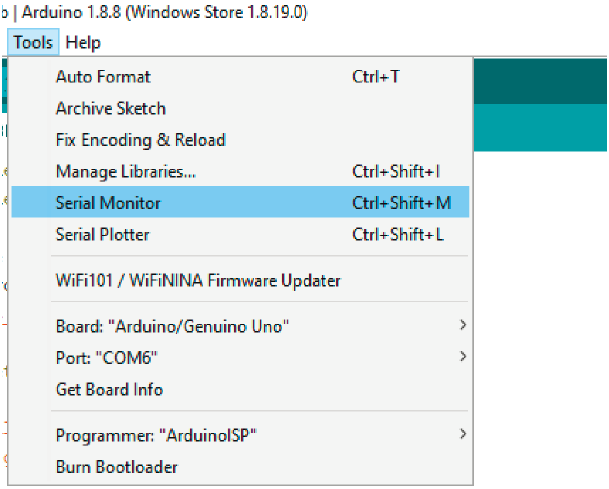
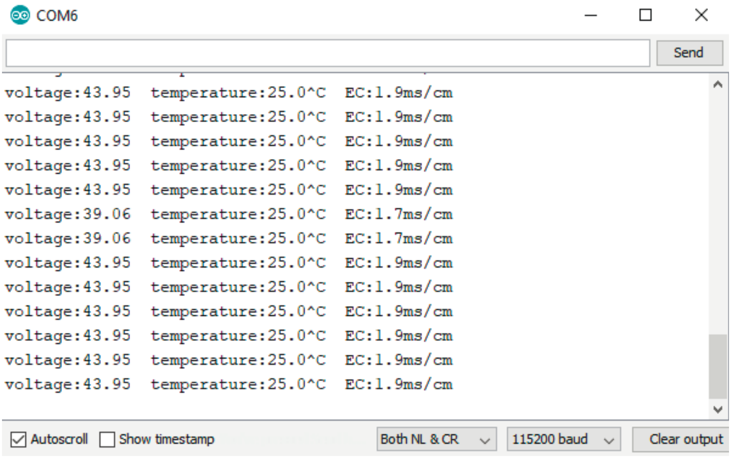

b | Arduino 1.8.8 (Windows Store 1.8.19.0)
Tools
Help
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Manage Libraries... Ctrl+Shift+I
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
WiFi101 / WiFiNINA Firmware Updater
Board: "Arduino/Genuino Uno"
Port: "COM6"
Get Board Info
Programmer: "ArduinoISP"
Burn Bootloader

Fig. 1.6 – Select a Serial Monitor

6. Put the probe to a water container.
7. Measured parameter will appear on your screen (see Fig. 1.7).



```
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:39.06  temperature:25.0^C  EC:1.7ms/cm
voltage:39.06  temperature:25.0^C  EC:1.7ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
voltage:43.95  temperature:25.0^C  EC:1.9ms/cm
```

☑ Autoscroll □ Show timestamp Both NL & CR 115200 baud

Fig. 1.7 – The data of measured parameter

8. Perform calibration

To ensure accuracy, the sensor used for the first time or for a certain period of time must be calibrated. We suggest to use point-to-point calibration and therefore standard 4.0 and 7.0 buffer solutions. The following steps show you how to work with two-point calibration [2].

Upload the sample code to the Arduino board, then open the serial port monitor, you can see the temperature and pH. If you have added a temperature sensor, be sure to write the corresponding function and call it.

Rinse the probe with distilled water, then absorb the remaining drops of water with paper. Insert the pH sensor into the standard buffer solution 7.0, stirring gently until the values are stable.

Once the values are stabilized, the first point can be calibrated. The specific steps are as follows:

– Input ENTER command in the serial monitor to enter the calibration mode.

– Input CAL commands in the serial monitor to start the calibration. The program will automatically identify two kinds of standard buffer solutions: 4.0 and 7.0. In this step, the standard buffer solution of 7.0 will be identified.

– After the calibration, input EXIT command in the serial monitor to save the relevant parameters and exit the calibration mode. Note: Only after input EXIT command in the serial monitor can the relevant parameters be saved.

– After the above steps, the first point calibration is completed. The second point calibration will be performed below.

Wash the probe with distilled water, then absorb the residual water-drops with paper. Insert the pH probe into the standard buffer solution of 4.0, stir gently, until the values are stable.

After the values are stable, the second point can be calibrated. As same with the first calibration step, the specific steps are as follows:

– Input ENTER command in the serial monitor to enter the calibration mode.

– Input CAL commands in the serial monitor to start the calibration. The program will automatically identify two kinds of standard buffer solutions: 4.0 and 7.0. In this step, the standard buffer solution of 4.0 will be identified.

– After the calibration, input EXIT command in the serial monitor to save the relevant parameters and exit the calibration mode. Note: Only after input EXIT command in the serial monitor can the relevant parameters be saved.

After completing the above steps, the two-point calibration is completed, and then it can be used for actual measurement. The relevant parameters in the calibration process have been saved to the EEPROM of the main control board.

Tasks for individual work

Analyze the work of the system for monitoring and forecasting results of IoT-based devices on various sensors. Add 2 own sensors. Produce sensor forecasting using exponential smoothing method and production rules. For each electrode (except ORP) there is a library that needs to be connected. It is located on the links to the manuals [3, 4]. Perform an experiment with the calibration solutions that provided with the kit.

Report

The report should contain:

- title page with the title 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 are the main purposes to add cellular connectivity to IoT projects?
2. Why we need sensors calibration?
3. What the main stages of sensors calibration?

Recommended literature

1. R. Ranjan, O. Rana, S. Nepal, M. Yousif, P. James, Z. Wen, S. Barr, P. Watson, P. Jayaraman, D. Georgakopoulos, M. Villari, M. Fazio, S. Garg, R. Buyya, L. Wang, A. Zomaya and S. Dustdar, "The Next Grand Challenges: Integrating the Internet of Things and Data Science", *IEEE Cloud Computing*, vol. 5, no. 3, pp. 12-26, 2018.

2. K. Singh and D. Kapoor, "Create Your Own Internet of Things: A survey of IoT platforms", *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 57-68, 2017. Available: 10.1109/mce.2016.2640718.

3. "Gravity Analog Electrical Conductivity Sensor Meter V2 K=1 SKU DFR0300", *Wiki.dfrobot.com,* 2018. [Online]. Available: https://www.dfrobot.com/wiki/index.php/Gravity:_Analog_Electrical_Conductivity_Sensor_/_Meter_V2_(K%3D1)_SKU:DFR0300 [Accessed: 22 December 2018].

4. "Analog ORP Meter SKU SEN0165", *Wiki.dfrobot.com,* 2018. [Online]. Available: https://www.dfrobot.com/wiki/index.php/Analog_ORP_Meter [Accessed: 22 December 2018].

Training 2

COMMUNICATING WITH IOT DEVICES: AT-COMMANDS ESP8266

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

Goal and objectives: This training includes the study of the work of AT-commands esp8266.

Learning objectives:

- to study basic AT commands;
- to study hardware and software configuration for communication between IoT devices and cloud storage.

Practical tasks:

- acquire practical skills in working with AT-commands;
- update firmware by using AT-commands;
- running simple server by using AT-commands.

Exploring tasks:

- explore of communication between devices by using AT-commands.

Recommended hardware and software:

Name	Link
Esp8266-07	https://goo.gl/MDsHNF
USB-TTL converter	https://goo.gl/LF2Jbz
Wi-Fi router	*Internet connection required*
Flash Download Tools (ESP8266 & ESP32)	https://www.espressif.com/en/support/download/other-tools
ESP8266 NONOS SDK V2.0.0 20160810	https://www.espressif.com/en/support/download/sdks-demos

Theoretical information

IoT is a network of physical devices that can connect to the network and exchange data. Each "thing" or "smart device" is a gadget with built-in electronics and software that can act as a sensor or actuator.

The connectivity between IoT things and the cloud part provides by a gateway, which transmits control commands going from the cloud to things.

In simple terms, things equipped with sensors to gather data and actuators to perform commands received from the cloud, and control applications to send commands to actuators.

AT commands are commands which are used to control the modems where AT stands for Attention. These commands were derived from Hayes commands which were used by the Hayes smart modems. Every wireless, as well as the dial-up modems, require an AT command to interact with a computer machine. These AT commands along with other extended commands also require Hayes command set as a subset.

The Hayes command set [1] consists of a series of short text strings which can be combined to produce commands for operations such as dialing, hanging up, and changing the parameters of the connection. The vast majority of dial-up modems use the Hayes command set in numerous variations.

ESP8266 (see Fig. 2.1), in its default configuration, boots up into the serial modem mode. In this mode, you can communicate with it using a set of AT commands.

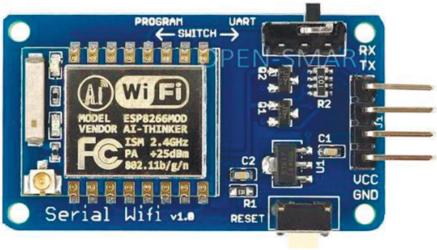


Fig. 2.1 – Esp 8266-07 (8Mbps flash)

Training preparation

In preparation for this practical training it is necessary:

- to clarify the goals and mission of the research;

- to study theoretical material contained in this manual, and in [1]-[4]);
- to familiarize oneself with the main procedures and specify the program according to defined task.

Training preparation and execution order

1. Download all files.
2. Connect Converter to esp8266.

2.1 Connect usb-ttl to esp8266.

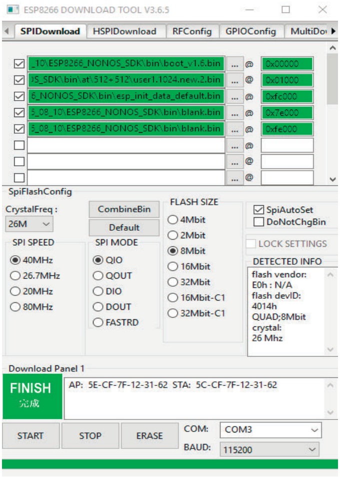
esp8266 RX → Converter TX
esp8266 TX → Converter RX
esp8266 5V → Converter 5V
esp8266 GND → Converter GND

2.2 Change switch position on board to program.

2.3 Connect to computer.

3. Run Flash Downloads Tool.
4. Set paths and addresses in the program

4.1 Set settings, paths and addresses in the window as it shown in Fig. 2.2.



☑	_10\ESP8266_NONOS_SDK\bin\boot_v1.6.bin	@	0x00000
☑	)S_SDK\bin\at\512+512\user1.1024.new.2.bin	@	0x01000
☑	6_NONOS_SDK\bin\esp_init_data_default.bin	@	0xfc000
☑	5_08_10\ESP8266_NONOS_SDK\bin\blank.bin	@	0x7e000
☑	5_08_10\ESP8266_NONOS_SDK\bin\blank.bin	@	0xfe000
□		@	
□		@	
□		@	

SpiFlashConfig

CrystalFreq : 26M

SPI SPEED: ● 40MHz ○ 26.7MHz ○ 20MHz ○ 80MHz

SPI MODE: ● QIO ○ QOUT ○ DIO ○ DOUT ○ FASTRD

FLASH SIZE: ○ 4Mbit ○ 2Mbit ● 8Mbit ○ 16Mbit ○ 32Mbit ○ 16Mbit-C1 ○ 32Mbit-C1

☑ SpiAutoSet
□ DoNotChgBin
□ LOCK SETTINGS

DETECTED INFO
flash vendor:
E0h : N/A
flash devID:
4014h
QUAD;8Mbit
crystal:
26 Mhz

Download Panel 1

FINISH
完成

AP: 5E-CF-7F-12-31-62 STA: 5C-CF-7F-12-31-62

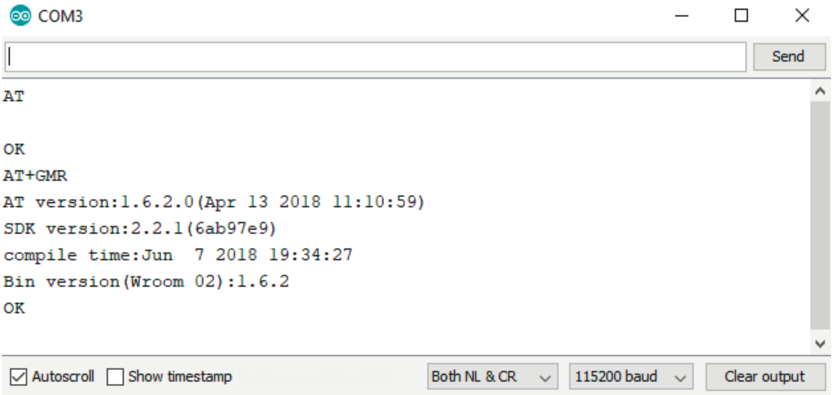
COM: COM3
BAUD: 115200

Fig. 2.2 – Set settings, paths and addresses

Select port and baud rate. Click Start.

4.2 Select port. Wait for the firmware to load.

4.3 Open a Serial Monitor on Arduino IDE with settings as shown in Fig. 2.3.



```
AT

OK
AT+GMR
AT version:1.6.2.0(Apr 13 2018 11:10:59)
SDK version:2.2.1(6ab97e9)
compile time:Jun  7 2018 19:34:27
Bin version(Wroom 02):1.6.2
OK
```

☑ Autoscroll □ Show timestamp Both NL & CR 115200 baud

Fig. 2.3 – Setting of Serial Monitor on Arduino IDE

4.4 Enter “AT”. Click “Send”. If everything is ok, you will see the answer “Ok”.

5. Update the firmware to the latest version.

5.1 AT+GMR — you can check the version of firmware.

5.2 In terminal entering following commands:

```
AT+CWMODE=3
OK
```

5.3 Replace to your Wi-Fi SSID name and Wi-Fi password

```
AT+CWJAP="ssid","12345678"
OK
AT+CIFSR
192.168.1.134
```

5.4 Check last version firmware.

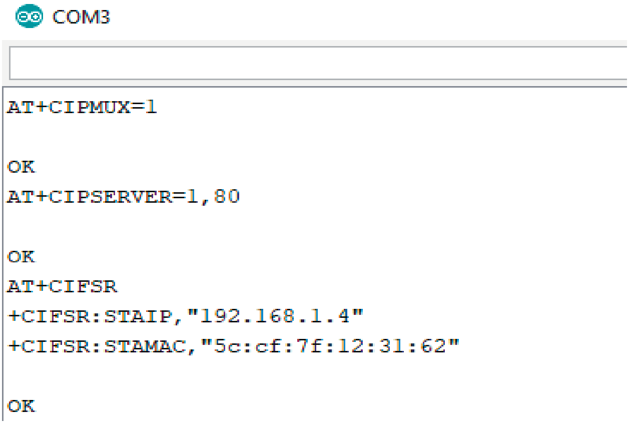
```
AT+CIUPDATE
+CIPUPDATE:1    found server
+CIPUPDATE:2    connect server
+CIPUPDATE:3    got edition
+CIPUPDATE:4    start start
OK
```

5.5 Wait firmware updated.

5.6 When in terminal you will see “OK”, check firmware version be using command “AT+GMR”

6. Running a webserver. Do not close the terminal window (see Fig. 4).

```
AT+CIPMUX=1
OK

AT+CIPSERVER=1,80
OK
```



```
AT+CIPMUX=1

OK
AT+CIPSERVER=1,80

OK
AT+CIFSR
+CIFSR:STAIP,"192.168.1.4"
+CIFSR:STAMAC,"5c:cf:7f:12:31:62"

OK
```

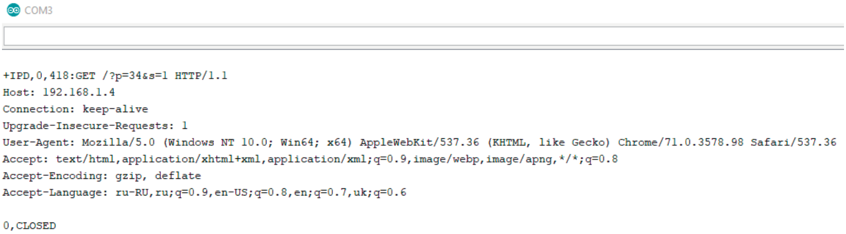
Fig. 2.4 – Running a webserver

6.1 Command for IP check:

```
AT+CIFSR
```

6.2 Open browser and go to addresses (Change IP, to esp8266 IP)

http://IP_address_you_esp8266 /?p=34&s=1. On terminal window, you will see follow (see Fig. 2.5)



```
+IPD,0,418:GET /?p=34&s=1 HTTP/1.1
Host: 192.168.1.4
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6

0,CLOSED
```

Fig. 2.5 – Terminal window

6.3 Try other AT-commands (see Appendix C).

Test questions:

1. What is AT commands?

2. How could be AT commands use in IoT systems? What function its do?

Recommended literature

1. R. Ranjan, O. Rana, S. Nepal, M. Yousif, P. James, Z. Wen, S. Barr, P. Watson, P. Jayaraman, D. Georgakopoulos, M. Villari, M. Fazio, S. Garg, R. Buyya, L. Wang, A. Zomaya and S. Dustdar, "The Next Grand Challenges: Integrating the Internet of Things and Data Science", *IEEE Cloud Computing*, vol. 5, no. 3, pp. 12-26, 2018.

2. K. Singh and D. Kapoor, "Create Your Own Internet of Things: A survey of IoT platforms", *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 57-68, 2017. Available: 10.1109/mce.2016.2640718.

3. "ESP8266 AT Instruction Set", *Espressif.com,* 2019. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/4a-esp8266_at_instruction_set_en.pdf [Accessed: 2 August 2019].

4. "Building Wireless Sensor Networks", *Oreilly.com,* 2018. [Online]. Available: https://www.oreilly.com/library/view/building-wireless-sensor/780596807757/ [Accessed: 22 December 2018].

Training 3

SIMPLE CLOUD WATER QUALITY MONITORING SYSTEM

Goal and objectives: In this training we create out first IoT water quality device.

Learning objectives:

- to study the abilities of the ThingSpeak service;
- to study sensor data transmission technique.

Practical tasks:

- create firmware for a monitoring device according to an example.

Exploring tasks:

- explore of configuration by devices and cloud storage.

Recommended hardware and software:

Name	Link
Arduino UNO R3	https://store.arduino.cc/arduino-uno-rev3
Gravity IO Expansion Shield for Arduino V7.1	https://www.dfrobot.com/product-1009.html
Analog Sensor Kit	https://www.dfrobot.com/product-1797.html
EC, ORP, pH	https://www.dfrobot.com/product-1071.html https://www.dfrobot.com/product-1782.html
USB 2.0 cable type A/B	https://store.arduino.cc/usb-2-0-cable-type-a-b
Jumpers	*Optional*
Breadboard	*Optional*
Esp8266-07 (with AT-commands firmware)	https://goo.gl/MDsHNF
Wi-Fi router	with internet connection

Theoretical information

Several things are needed in the hardware and software to connect a device and cloud on IoT-based system. The ThingSpeak cloud used the sensor data visualization when several physical devices can be connected and used in a union but appear to the user as one machine (despite that at the physical level, the machines function independently) [1]. This method of computing thus allows changes to be made to the 'virtual' server much easier than before. In this case, an object will connect to the cloud through an Internet connection to upload or receive data. Device to be connected are typically augmented with either sensors or actuators.

For the purpose of connecting an object to the IoT, we focus on the ThingSpeak API. The interface provides simple communication capabilities to objects within the IoT environment, as well as interesting additional applications. Moreover, ThingSpeak allows you to build applications around data collected by sensors. It offers near real-time data collection, data processing, and also simple visualizations for its users. All incoming data is time and date stamped and receives a sequential ID. Once a channel has been created, data can be published by accessing the ThingSpeak API with a 'write key', a randomly created unique alphanumeric string used for authentication. Essentially, things are objects that are given sensors to collect data. The data is then uploaded to the cloud and from there can be used for a variety of purposes. In turn, data (such as commands or choosing certain options) can be gathered and communicated to the cloud, which in turn sends these messages to the object.

Training preparation

In preparation for this practical training it is necessary:

- to clarify the goals and mission of the research;
- to study theoretical material contained in this manual, and in [1]-[3]);
- to familiarize oneself with the main procedures and specify the program according to defined task.

Before using the sensors, remove protective cap, then connect the wire as shown below. After completing the measurement, clean the sensor and insert it into the protective cap.

Execution order

1. Connect Shield to Arduino UNO (see Fig. 3.1).
2. Connect sensor to shield (see Fig. 3.1).

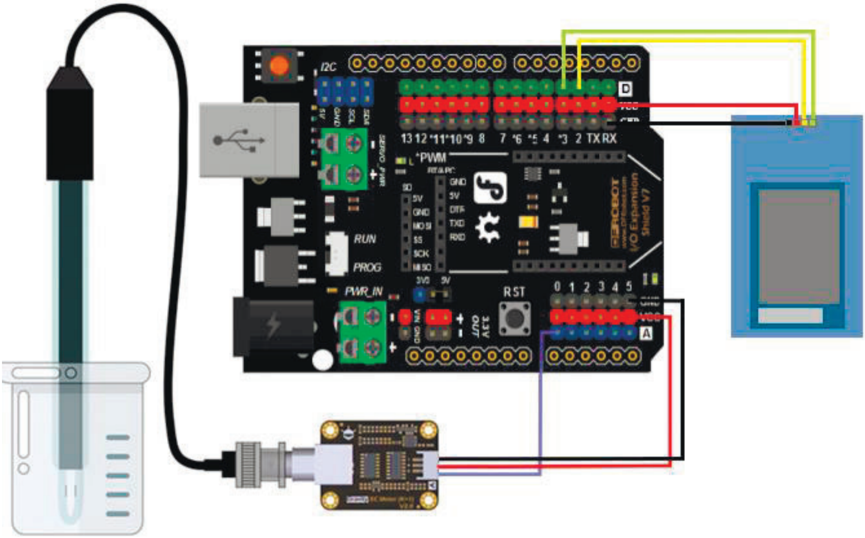
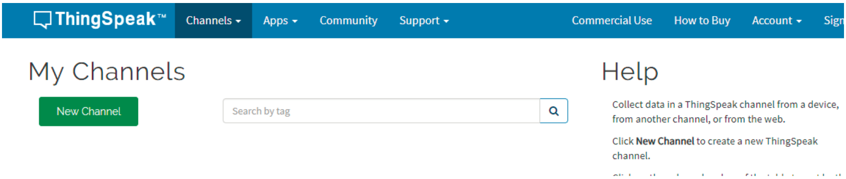


Fig. 3.1 – Connection of Shield, Arduino UNO and sensor

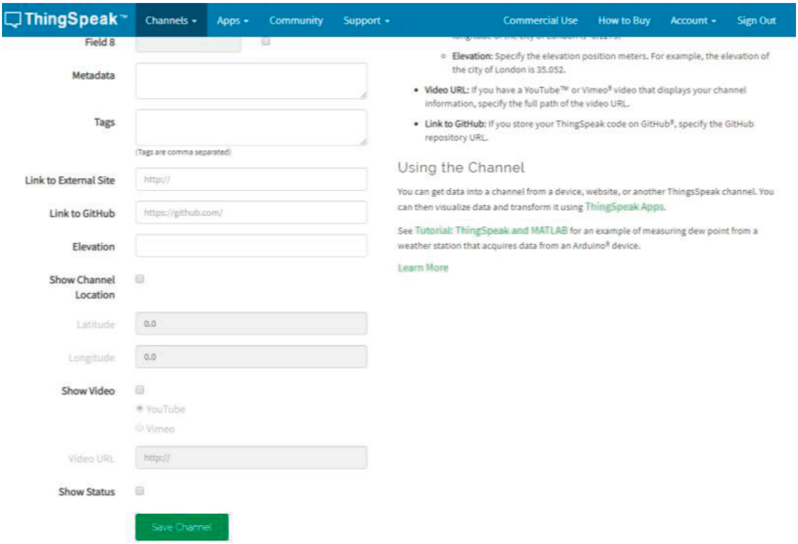
3. Use sketch from Appendix B to Arduino.
4. Register on the service ThingSpeak.
5. Create a new channel (see Figs. 3.2, 3.3)



Collect data in a ThingSpeak channel from a device, from another channel, or from the web.

Click **New Channel** to create a new ThingSpeak channel.

Fig. 3.2 – The new channel creating – step 1



Field 8 □

Metadata

Tags

(Tags are comma separated)

Link to External Site: http://

Link to GitHub: https://github.com/

Elevation

Show Channel Location □

Latitude: 0.0

Longitude: 0.0

Show Video □

● YouTube

○ Vimeo

Video URL: http://

Show Status □

Save Channel

- ◦ **Elevation:** Specify the elevation position meters. For example, the elevation of the city of London is 35.052.
- **Video URL:** If you have a YouTube™ or Vimeo® video that displays your channel information, specify the full path of the video URL.
- **Link to GitHub:** If you store your ThingSpeak code on GitHub®, specify the GitHub repository URL.

Using the Channel

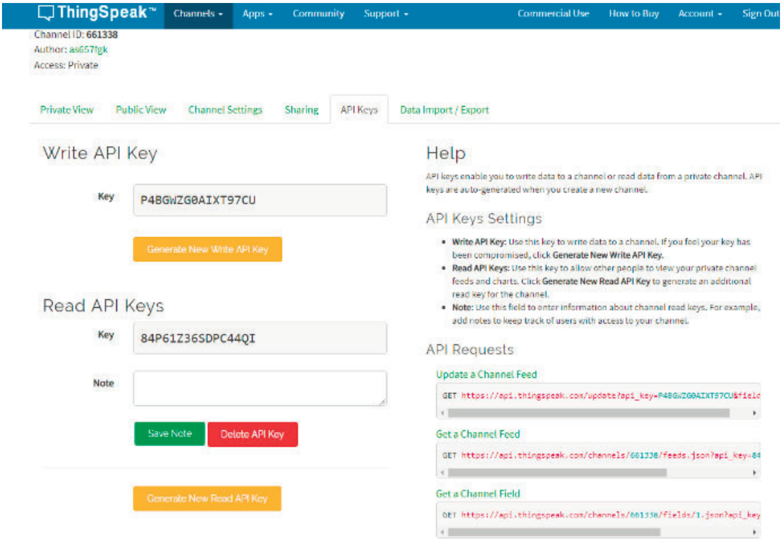
You can get data into a channel from a device, website, or another ThingsSpeak channel. You can then visualize data and transform it using ThingSpeak Apps.

See Tutorial: ThingSpeak and MATLAB for an example of measuring dew point from a weather station that acquires data from an Arduino® device.

Learn More

Fig. 3.3 – The new channel creating – step 2

6. Get Write API key (see Fig. 3.4).



Channel ID: 661338
Author: as657fgk
Access: Private

Write API Key

Key: P4BGWZG0AIXT97CU

Generate New Write API Key

Read API Keys

Key: 84P61Z36SDPC44QI

Note

Save Note | Delete API Key

Generate New Read API Key

Help

API keys enable you to write data to a channel or read data from a private channel. API keys are auto-generated when you create a new channel.

API Keys Settings

- **Write API Key:** Use this key to write data to a channel. If you feel your key has been compromised, click **Generate New Write API Key.**
- **Read API Keys:** Use this key to allow other people to view your private channel feeds and charts. Click **Generate New Read API Key** to generate an additional read key for the channel.
- **Note:** Use this field to enter information about channel read keys. For example, add notes to keep track of users with access to your channel.

API Requests

Update a Channel Feed

```
GET https://api.thingspeak.com/update?api_key=P4BGWZG0AIXT97CU&field
```

Get a Channel Feed

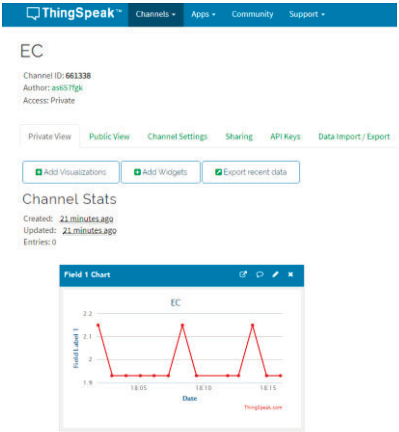
```
GET https://api.thingspeak.com/channels/661338/feeds.json?api_key=84
```

Get a Channel Field

```
GET https://api.thingspeak.com/channels/661338/fields/1.json?api_key
```

Fig. 3.4 – The API key writing

7. Create a firmware using Appendix D (use Write API key from 6), Training 1 and Example from Appendix E.
8. Connect Arduino UNO to your computer.
9. Update firmware.
10. If everything is ok, you will see every 65 sec new dots in the plot.



EC

Channel ID: 661338
Author: as657fgk
Access: Private

Channel Stats

Created: 21 minutes ago
Updated: 21 minutes ago
Entries: 0

Fig. 3.5 – Sensor data visualization

Test questions

1. What is IoT cloud?
2. What the feature of the ThingSpeak cloud.
3. What is API write key?

Recommended literature

1. M.A.G. Maureira, D. Oldenhof, L. Teernstra, "ThingSpeak–an API and Web Service for the Internet of Things". World Wide Web, 2011.

2. R. Ranjan, O. Rana, S. Nepal, M. Yousif, P. James, Z. Wen, S. Barr, P. Watson, P. Jayaraman, D. Georgakopoulos, M. Villari, M. Fazio, S. Garg, R. Buyya, L. Wang, A. Zomaya and S. Dustdar, "The Next Grand Challenges: Integrating the Internet of Things and Data Science", *IEEE Cloud Computing*, vol. 5, no. 3, pp. 12-26, 2018.

3. K. Singh and D. Kapoor, "Create Your Own Internet of Things: A survey of IoT platforms", *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 57-68, 2017. Available: 10.1109/mce.2016.2640718.

ITM 5.3 IoT-based systems for monitoring of severe accidents

Prof., DrS. V.S. Kyarchenko, Assoc. Prof., Dr. H.V. Fesenko

Training 1

EVALUATING RELIABILITY OF A MULTI-FLEET WITH A RESERVE DRONE FLEET

Aim: to study the approach to evaluating reliability of a multi-fleet with a reserve drone fleet.

Learning Objectives:

1. To study a set of reliability drone fleets assessment attributes.
2. To study the main steps of evaluating reliability of a multi-fleet with a reserve drone fleet.

Practical task:

to acquire practical skills in working with the approach.

Preparation for the training needs:

1. To get the theoretical information.
2. To develop a work plan in accordance with the achieved variant.

Training implementation during the training needs:

1. Read the theoretical information.

2. Prepare the initial data according to your variant presented in Table 2.

3. Following the recommendations presented in 1.2, you should obtain the first dependency from 1.3 for your variant.

4. Write a report which should include:

4.1. The aim and tasks.

4.2. The brief theoretical information.

4.3. The obtained results.

4.4. Conclusions on the obtained results.

4.5 Answers the test questions.

5. Prepare a presentation.

Defending the training results

1. Present a presentation and defending the report of the task results.
2. Evaluation of work.

Theoretical information

Since the Fukushima accident, to minimize the risk and impact of radiation to a nuclear power plant accident response team, drones (also known as unmanned aerial vehicles are actively used to map and monitor radioactive sites. From the utilization of drones, we can get a wireless radiation monitoring system that capable of detecting beta radiation (electrons), gamma radiation (photons) and X-rays from a safe distance.

In addition to radiation mapping, drone fleets can be used for creating an internet-of-drone-based multi-version post-severe accident monitoring system to maintain the following functions [1]:

1) to monitor and collect all data from sensor modules that are equipped with wireless connections;

2) to form a reliable mesh network for optimal data streaming between point-to-point transmissions;

3) to provide surveillance imaging for damage control, and search and rescue;

4) to summarize areas of contamination;

5) to provide an unmanned observation platform for exploratory surveillance.

Maintaining a high reliability level of a drone fleet is of great significance considering the presence of its drone failures. It is vital note that in many real-life NPP monitoring missions via a drone fleet, binary-state assumption when developing drone fleet reliability models may not be adequate.

In multi-state reliability modeling, the drone fleet/multi-fleet may rather have more than two levels of performance varying from perfect functioning to complete failure. This means that the drone fleet/multi-fleet can be considered as a multi-state system that may occupy different intermediate states between working perfectly and total failure.

Describing the proposed approach

Introduce the following abbreviation and notations.

DDL	the different distribution law for drones
DFT	redundant drones have different flight time (FT) from a starting position to a failed drone/drone fleet. FT = Switching-on time of redundant drone(s) + Time of flight to change failed drone(s)
MG	the main group of drones (main drone fleet)
N	No
RG	the redundant group of drones (reserve drone fleet)
RBD	reliability block diagram
PFFO	probability of failure-free operation
SDL	the same distribution law for drones
SFT	redundant drones have the same flight time from a starting position to a failed drone/drone fleet
Y	Yes
DF1, DF2, … , DFn	main drone fleets
CU	the control unit of a main drone fleet
CU_M	the control unit of the multi-fleet
d_1, d_2, … , d_k	drones under redundancy of a main drone fleet
d_{k+1}, d_{k+2}, … , d_ω	redundant drones of a main drone fleet
d_1, d_2, … , d_r	drones of the reserve drone fleet

The approach is based on a matrix of a drone fleet and reliability assessment attributes (Table 1.1).

The following attributes of drones and drone fleets are considered:

1. Type: single drone, fleet of drones, multi-fleet of drones.

2. Parameters describing the number of performed functions (one or more than one function; for example, functions of video, measurement, control), state levels (“Y” is used to show that a fleet/multi-fleet is an MSS, “N” is used to show that a fleet/multi-fleet is not an MSS, i.e. a fleet/multi-fleet has two states only: up state and down state), heterogeneousness (“Y” is used to show that heterogeneous fleets are considered, “N” is used to show that heterogeneous fleets are not considered).

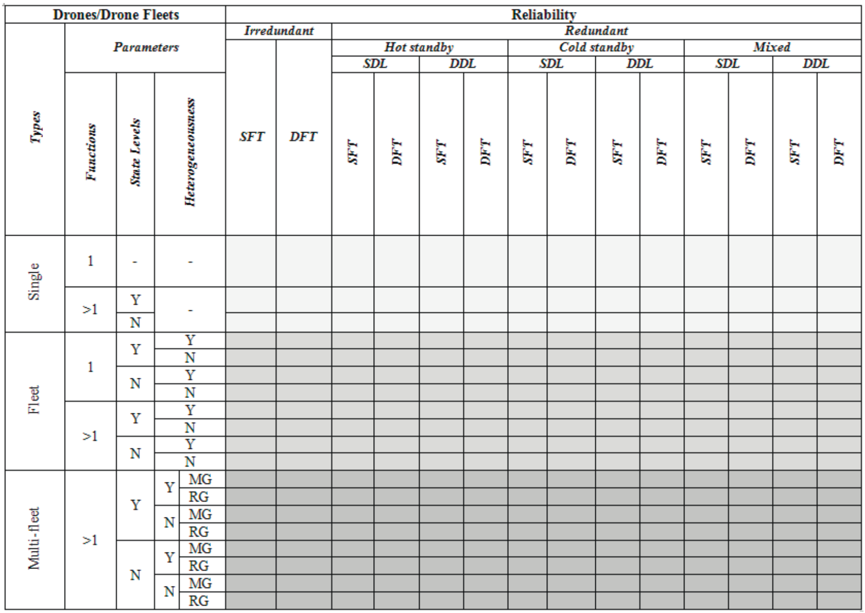
The following attributes of drone fleet reliability are considered:

1. Irredundant.
2. Redundant.

The following redundancy techniques (attribute “Redundant”) are considered:

1. Hot standby.
2. Cold standby.
3. Mixed standby.

Table 1.1 – Matrix of drone fleet reliability assessment attributes



Drones/Drone Fleets					Reliability													
Types	Parameters				*Irredundant*		*Redundant*											
							Hot standby				*Cold standby*				*Mixed*			
							SDL		*DDL*		*SDL*		*DDL*		*SDL*		*DDL*	
	Functions	*State Levels*	*Heterogeneousness*		*SFT*	*DFT*	*SFT*	*DFT*	*SFT*	*DFT*	*SFT*	*DFT*	*SFT*	*DFT*	*SFT*	*DFT*	*SFT*	*DFT*
Single	1	-	-															
	>1	Y	-															
		N																
Fleet	1	Y	Y															
			N															
		N	Y															
			N															
	>1	Y	Y															
			N															
		N	Y															
			N															
Multi-fleet	>1	Y	Y	MG														
				RG														
			N	MG														
				RG														
		N	Y	MG														
				RG														
			N	MG														
				RG														

Note that in order to assess reliability of drone fleets, the following recovery policies can be analyzed:

1. No recovery, no delays for changing failed drones by redundant ones (FT = 0).
2. No recovery of failed drone(s). Unavailability is caused by delays of changing failed drones by redundant ones (if FT > 0).

Recovery of failed drones is carrying out at the starting position. In this case possibility/probability of returning failed/partially failed/maintained drones can be considered.

For subcases when FT = 0 or FT > 0, assessment of availability can be done.

Consider a multi-fleet that is used for NPP monitoring missions. The multi-fleet comprises *n* main drone fleets and one reserve drone fleet. Each main drone fleet, consisting *ω* drones, has *k* drones under redundancy and *ω-k* redundant drones. The reserve drone fleet consists of *r* drones. A drone of the reserve drone fleet can be used to replace a failed drone of a main drone fleet. Using our Matrix (Table I), we can describe the multi-fleet in the following way: Type of Drone Fleets: Multi-fleet, Functions: >1, State Levels: N, Heterogeneousness: N, Reliability: Redundant, Redundant: Hot standby, Hot standby: SDL, SDL: SFT (FT=0).

In Fig. 1.1, we construct and illustrate the RBD for the multi-fleet described above, from which a formula for the PFFO of the multi-fleet can be obtained.

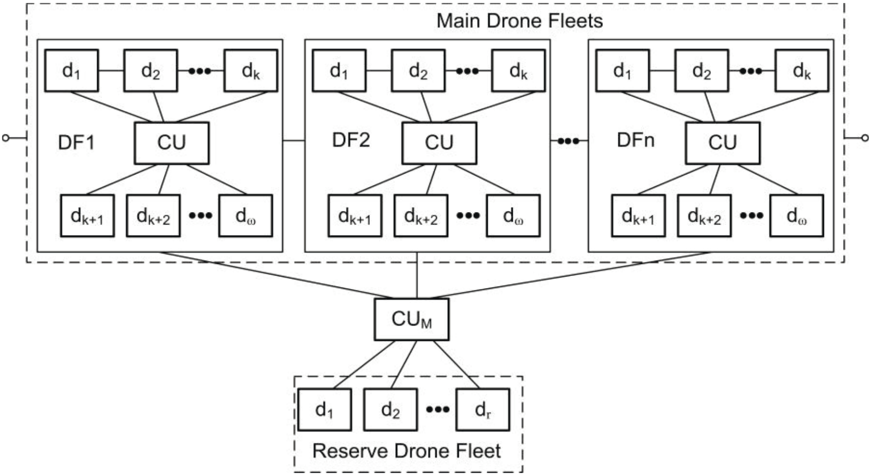


Fig. 1.1 – Reliability block diagram for the multi-fleet

The construction of the RBD is based on the following assumptions:

1. Drone fleets are unrecoverable.
2. Each of the drones has two states: up state and down state.
3. Drones’ failures are independent.
4. Both a main drone fleet and the multi-fleet have a structure of type “k-out-of-n”.

5. Drones of the reserve drone fleet are used as redundant drones for a main drone fleet.

6. A switching process fulfilled by means of a control unit is ideal.

7. All drones of the multi-fleet are identical.

Two strategies of redundancy application can be used:

Strategy 1: Replacement of failed drones of a main drone fleet is fulfilled by drones of the reserve drone fleet after failure of a main drone fleet only.

Strategy 2: Replacement of failed drones of a main drone fleet is fulfilled by drones of the reserve drone fleet immediately.

Two cases are possible considering a value of *r*:

Case a): $r \leq n$.

Case b): $r > n$.

Let's consider Strategy 1, Case a). The PFFO for a main drone fleet can be calculated in the following way:

$$F(k,\omega) = \sum_{i=0}^{\omega-k} C_{\omega}^{i} p_d^{\omega-i} (1-p_d)^i p_c \tag{1.1}$$

where p_d is the PFFO for a drone of the multi-fleet,

p_c is the PFFO for the control unit of a main drone fleet.

If the reserve drone fleet has no drones (r=0), an equation for obtaining the PFFO for the multi-fleet can be written as follows:

$$P(n,k,\omega,0) = F^n(k,\omega). \tag{1.2}$$

The PFFO for the multi-fleet with 1 drone, 2 drones, and r drones in the reserve drone fleet can be calculated by means of (1.3), (1.5) and (1.6), respectively:

$$P(n,k,\omega,1) = P(n,k,\omega,0) + R(n,k,\omega) \tag{1.3}$$

where

$$R(n,k,\omega) = n\left[1 - F(k,\omega)\right] p_d F^{n-1}(k,\omega) p_{cm} \tag{1.4}$$

where p_{cm} is the PFFO for the control unit of the multi-fleet.

$$P(n,k,\omega,2)=P(n,k,\omega,1)+\left[1-P(n,k,\omega,1)\right]R(n,k,\omega)\,. \tag{1.5}$$

$$P(n,k,\omega,r)=P(n,k,\omega,r-1)+\left[1-P(n,k,\omega,r-1)\right]R(n,k,\omega). \tag{1.6}$$

In some cases, calculation of the probability of the multi-fleet failure is preferable to calculation of the PFFO for the multi-fleet. The PFFO for the probability of the multi-fleet failure with 1 drone, 2 drones, and *r* drones in the reserve drone fleet can be obtained by means of (1.7), (1.8) and (1.9), respectively:

$$Q(n,k,\omega,1)=1-P(n,k,\omega,1)\,. \tag{1.7}$$

$$Q(n,k,\omega,2)=1-P(n,k,\omega,2)\,. \tag{1.8}$$

$$Q(n,k,\omega,r)=1-P(n,k,\omega,r)\,. \tag{1.9}$$

An example of the proposed approach application

Let's analyze reliability of redundant multi-fleet with reserve drone fleet using (1)-(9). The following dependencies have been obtained:

1. A per cent increase in the PFFO for the multi-fleet by using 3 drones of the reserve drone fleet on the number of the main drone fleets (p_c = 0.997, p_{cm} = 0.999, k = 6, ω = 9) (Fig. 1.2).
2. A per cent decrease in probability of the multi-fleet failure by using 3 drones of the reserve drone fleet instead of 1 drone/2 drones on the number of the main drone fleets (p_d = 0.95, p_c = 0.997, p_{cm} = 0.999, k = 6, ω = 9) (Fig. 1.3).

We can make the following conclusions based on the analysis of the dependencies shown in Fig. 1.2 and Fig. 1.3:

1. The maximum per cent increase in the PFFO for the multi-fleet by using 3 drones (7.4 per cent) is achieved when PFFO for a drone p_d = 0.92 and the number of the main drone fleets n = 15 (Fig. 1.2), whereas the minimum per cent increase in the PFFO for the multi-fleet by using 3

drones (1.5 per cent) is achieved when PFFO for a drone p_d = 0.99 and the number of the main drone fleets n = 2.

2. When 3 drones of the reserve drone fleet are used as redundant drones for the main drone fleets, growth in the number of the main drone fleets from 5 to 15 (Fig. 1.3) leads to a per cent increase in the PFFO for the multi-fleet by 2.8, 3.4, and 4.7 per cent for p_d = 0.99, p_d = 0.95, and p_d = 0.92, respectively.

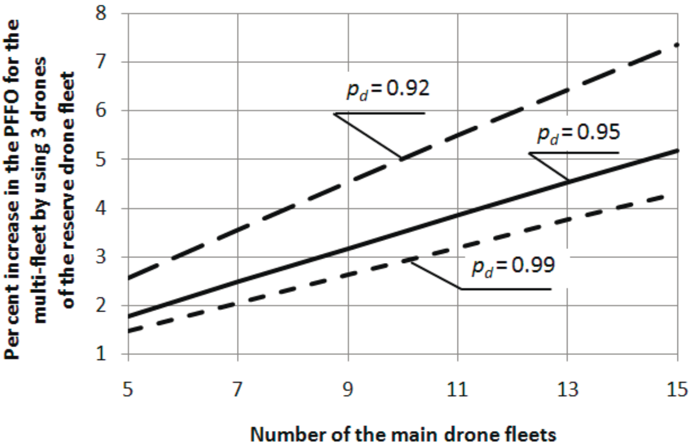


Fig. 1.2 – Per cent increase in the PFFO for the multi-fleet by using 3 drones of the reserve drone fleet on the number of the main drone fleets

A rise of 2 drones (3 drones instead of 1 drone) in the reserve drone fleet drones number (Fig. 1.3) causes a decrease of between 3.7 per cent (the number of the main drone fleets n = 5) and 11,2 per cent (the number of the main drone fleets n = 15) in probability of the multi-fleet failure.

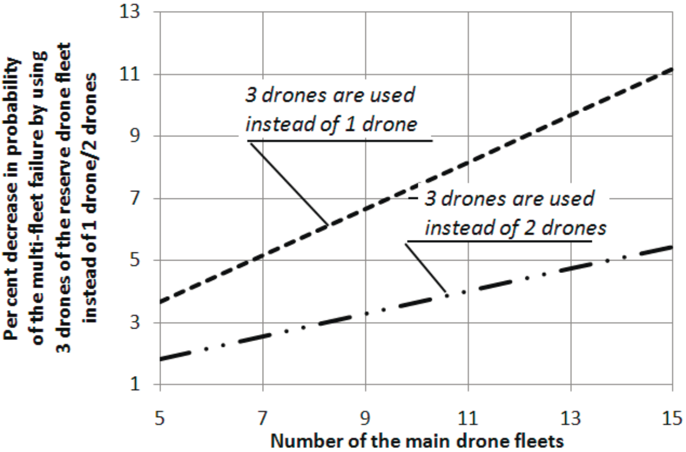


Fig. 1.3 – Per cent decrease in probability of the multi-fleet failure by using 3 drones of the reserve drone fleet instead of 1 drone/2 drones on the number of the main drone fleets

Test questions

1. What attributes of drone fleet reliability are considered?

2. What the main strategies of redundancy application can be used for the multi-fleet?

3. What assumptions is the construction of the RBD based on?

4. What parameters should be given to evaluating reliability of a multi-fleet with the reserve drone fleet?

Recommended literature

1. H. Fesenko, V. Kharchenko, A. Sachenko, R. Hiromoto, and V. Kochan, "An Internet of Drone-based Multi-version Post-severe Accident Monitoring System: Structures and Reliability," in *Dependable IoT for Human and Industry Modeling, Architecting, Implementation*, V. Kharchenko, A. Kor, A. Rucinski, Eds. Denmark, The Netherlands: River Publishers, 2018, pp. 197-217.

Variants

Table 1.2 – The variants

Variants	p_c	p_{cm}	k	ω
1	0.996	0.998	6	10
2	0.995	0.999	7	9
3	0.997	0.998	6	9
4	0.996	0.997	5	10
5	0.995	0.997	6	10
6	0.996	0.998	7	10
7	0.996	0.998	6	9
8	0.995	0.999	5	10
9	0.997	0.998	6	10
10	0.996	0.997	7	10
11	0.995	0.997	6	10
12	0.996	0.998	7	9
13	0.996	0.998	6	9
14	0.995	0.999	5	10
15	0.997	0.998	6	10
16	0.996	0.997	6	10
17	0.995	0.997	7	9
18	0.996	0.998	6	9
19	0.996	0.998	5	10
20	0.995	0.999	6	10
21	0.997	0.998	7	10
22	0.996	0.997	6	10
23	0.995	0.997	7	9
24	0.996	0.998	5	10
25	0.996	0.998	6	10
26	0.995	0.999	6	10
27	0.997	0.998	5	10
28	0.996	0.997	6	10
29	0.995	0.997	7	10
30	0.996	0.998	7	9

Training 2

EVALUATING RELIABILITY OF A MULTI-FLEET OF DRONES WITH TWO-LEVEL HOT STANDBY REDUNDANCY CONSIDERING A CONTROL SYSTEM STRUCTURE

Aim: to study an approach to evaluating reliability of a multi-fleet of drones with two-level hot standby redundancy considering a control system structure features.

Learning Objectives:

1. To study structures of control systems for the multi-fleet of drones.
2. To study reliability models for the multi-fleet of drones with one- and two level system of control stations.
3. To study recommendations for choice of a structure of system of control stations.

Practical task:

to acquire practical skills in working with the models.

Preparation for the training needs:

1. To get the theoretical information.
2. To develop a work plan in accordance with the achieved variant.

Training implementation during the training needs:

1. Read the theoretical information.
2. Prepare the initial data according to your variant presented in Table 3.
3. Following the recommendations presented in 1.2, you should obtain all the dependency from 1.3 for your variant.
4. Write a report which should include:

4.1. The aim and tasks.

4.2. The brief theoretical information.

4.3. The obtained results.

4.4. Conclusions on the obtained results.

4.5 Answers the test questions.

5. Prepare a presentation.

Defending the training results

1. Present a presentation and defending the report of the task results.
2. Evaluation of work.

Theoretical information

Over the last few years, drones have become a popular tool for a variety of applications at nuclear facilities, including both indoor and outdoor inspections and mapping.

The possibility of using drones when creating new NPP accident monitoring system is generating a lot of interest [1].

It is vital to note, that a drone fleet involved in performing NPP monitoring missions should maintain a high reliability level considering the presence of its drone failures. One of the widely used techniques for implementing dependable systems with high reliability and fault tolerance is standby redundancy, in which one or several elements are online and working with some redundant elements serving as standby spares. When an online element experiences a failure, a standby element is activated to replace it and take over the work. The k-out-of-n system structure is a very popular type of redundancy in fault-tolerant systems.

In a fault-tolerant drone fleet, one part of drones should be under redundancy and other one should be used as redundant drones. A switching process allowing the drone fleet to activate a redundant drone can be carried out via a control system (control station).

Hence, there are a few challenges related to application of drone fleets to assure reliable monitoring of severe accidents in the aggressive environment and to optimize a schedule of fleet application and control stations structure.

Describing the proposed approach

Introduce the following abbreviation and notations.

MFD	multi-fleet of drones
NPP	nuclear power plant
RBD	reliability block diagram
RDF	reserve drone fleet
SCS	system of control stations
PFFO	probability of failure-free operation

DF1, DF2, … , DFn	main drone fleets
CS1	the control station of the multi-fleet of drones
CS2	the control station of a main drone fleet
d_1, d_2, … , d_k	drones under redundancy of a main drone fleet
d_{k+1}, d_{k+2}, … , d_ω	redundant drones of a main drone fleet
d_1, d_2, … , d_r	drones of the reserve drone fleet
$F(k,\omega)$	probability of failure-free operation of a main drone fleet
$P(n,k,\omega,0)$	the probability of failure-free operation of the multi-fleet of drones with no drones in the reserve drone fleet
$P(n,k,\omega,1)$	the probability of failure-free operation of the multi-fleet of drones with 1 drone in the reserve drone fleet
$P(n,k,\omega,2)$	the probability of failure-free operation of the multi-fleet of drones with 2 drones in the reserve drone fleet
$P(n,k,\omega,r)$	the probability of failure-free operation of the multi-fleet of drones with *r* drones in the reserve drone fleet
$R(n,k,\omega)$	the probability of the state when 1 drones of the reserve drone fleet is used to change a failed drone of a main drone fleet
p_d	the probability of failure-free operation of a drone of the multi-fleet of drones
p_{CS1}	the probability of failure-free operation of a main fleet control station
p_{CS2}	the probability of failure-free operation of a control station of the multi-fleet of drones

Consider a multi-fleet that is used for NPP monitoring missions. The multi-fleet comprises *n* main drone fleets and one reserve drone fleet (RDF). Each main drone fleet, consisting *ω* drones, has *k* drones under redundancy and *ω-k* redundant drones.

The RDF consists of *r* drones. A drone of the RDF can be used to replace a failed drone of a main drone fleet. Using the matrix from Training 1, we can describe the MFD by the following way: Type of Drone Fleets: Multi-fleet, Functions: >1, State Levels: No, Heterogeneousness: No, Reliability: Redundant, Redundant: Hot standby, Hot standby: the same distribution law for drones.

The construction of the RBD is based on the following assumptions:

1. Drone fleets are unrecoverable.
2. Each of the drones has two states: up state and down state.
3. Drones' failures are independent.
4. Both a main drone fleet and the MFD have a structure of type "k-out-of-n".
5. Replacement of failed drones of a main drone fleet is fulfilled by drones of the RDF after failure of a main drone fleet only.
6. No delays for changing failed drones by redundant ones.
7. All drones of the MFD are identical.

Depending on the number of control levels, SCS can have one of the following structures:

1. Centralized (irredundant) SCS.
2. Centralized (redundant) SCS.
3. Decentralized SCS.
4. Partially decentralized SCS (with z control stations for n groups of fleets, z < n, n = az, a – integer).

Reliability block diagrams for the described SCS structures are shown in Figs. 2.1-2.4.

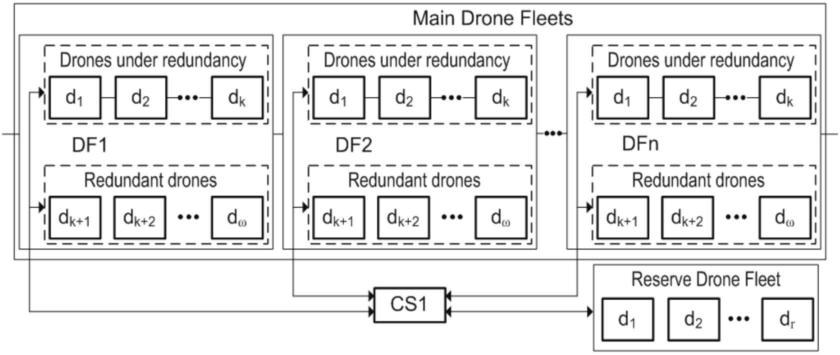


Fig. 2.1 – RBD for the MFD with the centralized (irredundant) SCS

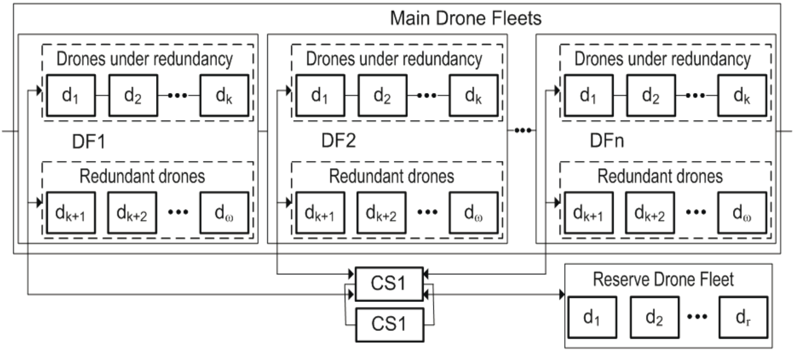


Fig. 2.2 – RBD for the MFD with the centralized (redundant) SCS

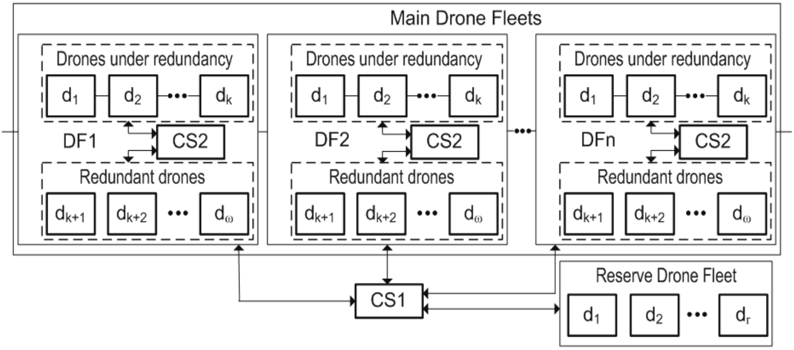


Fig. 2.3 – RBD for the MFD with the decentralized (redundant) SCS

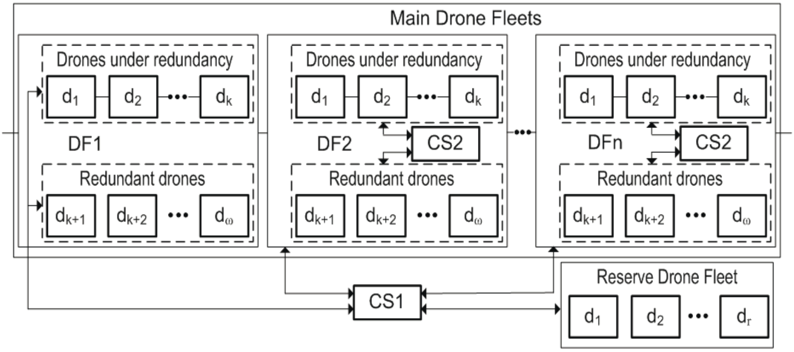


Fig. 2.4 – RBD for the MFD with the decentralized (redundant) SCS

Based on the developed RBDs, formulae for the PFFO for all of the considered MFD, except for the MFD with the partially decentralized SCS (Fig. 2.4), have been obtained (Table 2.1, 2.2). These formulae generalize the analytical model presented in Training 1 for different SCS structures and allow making decisions and choice one of them in accordance with the reliability criteria and cost.

Table 2.1 – Formulae for the PFFO of the MFD with the centralized (redundant/irredundant) SCS structures

Parameter	**Formula**	
	MFD with the centralized (irredundant) SCS	***MFD with the centralized (redundant) SCS***
$F(k,\omega)$	$\sum_{i=0}^{\omega-k} C_\omega^i p_d^{\omega-i}(1-p_d)^i$	$\sum_{i=0}^{\omega-k} C_\omega^i p_d^{\omega-i}(1-p_d)^i$
$P(n,k,\omega,0)$	$F^n(k,\omega)p_{CS1}$	$F^n(k,\omega)\left[1-(1-p_{CS1})^2\right]$
$R(n,k,\omega)$	$n\left[1-F(k,\omega)\right]p_d\times$ $\times F^{n-1}(k,\omega)p_{CS1}$	$n\left[1-F(k,\omega)\right]p_d F^{n-1}(k,\omega)\times$ $\times\left[1-(1-p_{CS1})^2\right]$
$P(n,k,\omega,1)$	$P(n,k,\omega,0)+R(n,k,\omega)$	$P(n,k,\omega,0)+R(n,k,\omega)$
$P(n,k,\omega,2)$	$P(n,k,\omega,1)+$ $+\left[1-P(n,k,\omega,1)\right]R(n,k,\omega)$	$(n,k,\omega,1)+$ $+\left[1-P(n,k,\omega,1)]R(n,k,\omega)\right]$
$P(n,k,\omega,r)$	$P(n,k,\omega,r-1)+$ $+\left[1-P(n,k,\omega,r-1)\right]\times$ $\times R(n,k,\omega).$	$P(n,k,\omega,r-1)+$ $+\left[1-P(n,k,\omega,r-1)\right]\times$ $\times R(n,k,\omega).$

Table 2.2 – Formulae for the PFFO of the MFD with the decentralized SCS structures

Parameter	**Formula**
	MFD with decentralized SCS
$F(k,\omega)$	$\sum_{i=0}^{\omega-k} C_{\omega}^{i} p_d^{\omega-i}(1-p_d)^i p_{CS2}$
$P(n,k,\omega,0)$	$F^n(k,\omega)$
$R(n,k,\omega)$	$n\left[1-F(k,\omega)\right]p_d F^{n-1}(k,\omega)p_{CS1}$
$P(n,k,\omega,1)$	$P(n,k,\omega,0)+R(n,k,\omega)$
$P(n,k,\omega,2)$	$P(n,k,\omega,1)+\left[1-P(n,k,\omega,1)\right]\times R(n,k,\omega)$
$P(n,k,\omega,r)$	$P(n,k,\omega,r-1)+\left[1-P(n,k,\omega,r-1)\right]R(n,k,\omega).$

An example of the proposed approach application

Using formulae from Tables 2.1 and 2.2, the dependency of the PFFO for the MFD with 3 drones in the RDF on the number of the main drone fleets have been obtained (Fig. 2.5) ($p_{CS1} = p_{CS2} =$ 0.99, $p_d =$ 0.92, k = 6, ω = 9).

We can make the following conclusions based on the analysis of the dependency shown in Fig. 2.5:

- When 3 drones of the RDF are used as redundant for the main drone fleets, growth in the number fleets from 5 to 15 leads to decrease in the PFFO for the MFD by 0.0008, 0.0014, and 0.0012 for the MFD with the centralized (irredundant), the centralized (redundant), and the decentralized SCSs, respectively.
- The MFD with the centralized (redundant) SCS has the best PFFO value among other structures.
- When the number of the main drone fleets is less than 12, the use of the MFD with the decentralized SCS is preferable to the MFD with the centralized (irredundant) SCS.

Based on the presented results the following tasks on choice of the SCS structure can be formulated: (1) to obtain the maximum complexity for the centralized (irredundant) MFD SCS allowing the MFD to be as reliable as the MFD with the decentralized SCS; (2) to obtain the maximum complexity for the centralized (redundant) MFD SCS allowing the MFD to be as reliable as the MFD with the decentralized SCS.

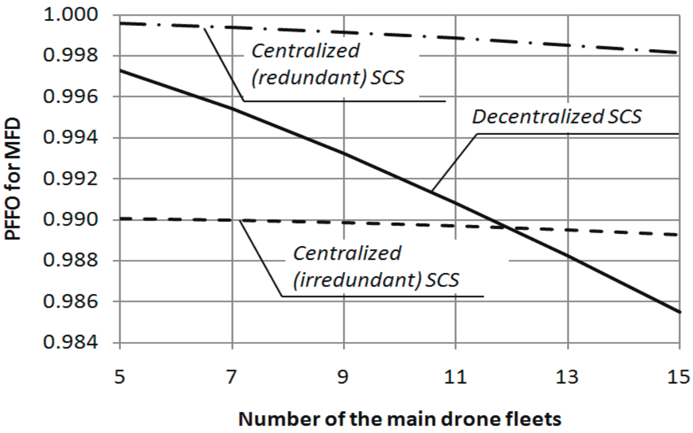


Fig. 2.5 – Dependency of the PFFO for the MFD with 3 drones in the RDF on the number of the main drone fleets

Test questions

1. What is the k-out-of-n system structure?
2. What structures can SCS have depending on the number of control levels?
3. What parameters should be given for the approach use?
4. What tasks on choice of the SCS structure can be formulated?

Recommended literature

1. H. Fesenko, V. Kharchenko, A. Sachenko, R. Hiromoto, and V. Kochan, “An Internet of Drone-based Multi-version Post-severe Accident Monitoring System: Structures and Reliability,” in *Dependable IoT for Human and Industry Modeling, Architecting, Implementation*, V. Kharchenko, A. Kor, A. Rucinski, Eds. Denmark, The Netherlands: River Publishers, 2018, pp. 197-217.

Variants

Table 2.3 – The variants

Variant	p_{CS1}	p_{CS2}	p_d	k	ω
1	0.998	0.996	0.92	6	10
2	0.999	0.995	0.93	7	9
3	0.998	0.997	0.94	6	9
4	0.997	0.996	0.95	5	10
5	0.997	0.995	0.93	6	10
6	0.998	0.996	0.94	7	10
7	0.998	0.996	0.92	6	9
8	0.999	0.995	0.93	5	10
9	0.998	0.997	0.94	6	10
10	0.997	0.996	0.95	7	10
11	0.997	0.995	0.93	6	10
12	0.998	0.996	0.94	7	9
13	0.998	0.996	0.92	6	9
14	0.999	0.995	0.93	5	10
15	0.998	0.997	0.94	6	10
16	0.997	0.996	0.95	6	10
17	0.997	0.995	0.93	7	9
18	0.998	0.996	0.94	6	9
19	0.998	0.996	0.92	5	10
20	0.999	0.995	0.93	6	10
21	0.998	0.997	0.94	7	10
22	0.997	0.996	0.95	6	10
23	0.997	0.995	0.93	7	9
24	0.998	0.996	0.94	5	10
25	0.998	0.996	0.92	6	10
26	0.999	0.995	0.93	6	10
27	0.998	0.997	0.94	5	10
28	0.997	0.996	0.95	6	10
29	0.997	0.995	0.93	7	10
30	0.998	0.996	0.94	7	9

ITM 5.4 IoT based physical security systems of buildings and campuses

Assoc. Prof., Dr. D.D. Uzun, Dr. O. Illiashenko, PhD student O.O. Solovyov, PhD student Al-Khafaji Ahmed Waleed (KhAI)

Training 1

DEVELOPMENT OF SUMMARY PROJECT FOR IOT BASED PHYSICAL SECURITY SYSTEMS OF BUILDINGS AND CAMPUSES

Objectives and tasks

Objectives: to study the known techniques and tools used in physical security systems assessment and development tasks.

Learning tasks:

- to study the principles of physical security systems techniques;
- to study the possibilities security systems;
- to select the correct structural hierarchical scheme for physical security systems.

Practical tasks:

- to gain experience with understanding and application physical security systems techniques;
- to develop the summary project using and make the PSMECA analysis for that project.

Exploring tasks:

- to understand principles of IoT based physical security systems development and design.

Setting up

- to study the theoretical basics can be used materials contained in the according chapter, as well as a list of references.

Synopsis

For successfully development of this summary project, students should go through the process of models of physical security systems functions and components and according IoT tasks and problems.

A brief introduction to IOT based physical security systems

The modern qualitative and quantitative growth of the achievements of science and technology has served as the driving force for creating a multitude of scientific and practical developments. The importance of such developments is difficult to overestimate, because the average person is the carrier and / or implementer of many different ideas and technical solutions. In addition, it is necessary to take into account such aspects of socialization as culture and traditions, politics, religion, which often are catalysts to the acceleration of the diffusion of scientific and technical solutions and modern society.

Given that the objective existence of a set of positive scenarios for the application of science and technology achievements is undeniable, it is also necessary to take into account potential destructive actions and / or their scenarios. One of the systems, on which such destructive actions can be directed, is the physical security systems (PSS) of the sophisticated objects related to state buildings, buildings of infrastructure objects, buildings of educational units (universities, schools, etc.), buildings cultural fund buildings and so on.

Analysis of information from the world-known, generally accepted open sources [1-5] allows drawing a conclusion about a large number of terrorist acts on state, infrastructure facilities, objects of cult of cultural heritage in such countries as Iraq. The reasons for such attacks are obvious - inadequate security of objects of social significance.

The main points in the security of physical security of this kind of objects include 4 types of events: physical security (guards), frames - metal detectors, Closed-Circuit Television (CCTV), electronic access cards. However, the real problem is that the operators of the control room are exposed to the type of blackmail, intimidation, etc., as a result, they often become involuntary accomplices in crimes. Therefore, the problem arises of automating the functions of operators. On the other hand, there are multi-vector attacks, such as malicious disconnection of electricity, which disables video surveillance and access control systems or provocations to distract attention with the aim of enabling the penetration of intruders into the protected territory.

Another aspect that should be underlined is that the global physical security market size was valued at USD 133.94 billion in 2016, registering a compound annual growth rate of 9.1% over the forecast period [6].

Taking into account all of the above, the need of physical security to an environment aimed to mitigate or reduce terrorists acts, crime or vandalism through theft, burglaries and fire are anticipated to be the key trends driving the market and society.

Analysis shown that authors do not provide a holistic approach of analysis of intrusion modes, their effects and further risk-assessment by ranging of its criticality. Threat assessment and response for intrusions applied to power substations is presented in [7]. The same researchers describe physical security monitoring system with the use of multi-agent system [8] authors which can be applied for CCTV. The process of designing, analysing, and selecting an exterior physical security system is studied in 9]. The importance of system vulnerability assessment as an outcome of analysis and evaluation is underlined in [10]. The importance of determination of vulnerabilities and threats is considered as one of the most critical considerations for physical systems in [11]. Although the assessment guide of physical security systems, developed by US Department of Energy [12] describes assessment methods and outlines their use, it contains only the overall picture without addressing the technologies for been used for providing security systems on the market.

There are various definitions and approaches to ensure dependability and resilience of complex systems. Some of them are reviewed in [13-15]. In the context of the research interest, the PSS of the RI object is, on the one hand, a subsystem of the RI, and on the other hand, it includes a deterministic (finite) set of subsystems (or components), which it consists of. Each subsystem (or component) can be represented structurally in the form of separate elements and connections among them.

The formulation of the task directly includes the research of the functioning of PSS. There are various formulations for the definition of PSS and approaches to ensure it [16-18]. In general, PSS can be represented by an appropriate subsystem within the boundaries of the enterprise's integrated security system (facility or region).

The object of research and analysis is the PSS of the facility belonging to the Ministry of Education and Science of Iraq (as an infrastructure object of the region), and the territory of compact residence of students and employees.

In addition it is necessary to gather the following information:

- the types of failures which can occur in the system;
- the ways of distribution of the possible failures over the subsystems (components) and its elements;

- the likelihood of failures' occurrence;
- estimation of the risk of a successful attack on the protected object;
- the time needed to restore the normal functioning mode of the corrupted subsystem (or its component);
- the criticality of each specific type of attack, which can be a set (vector) of one and / or more failures (failure scenarios) provided their natural or artificial occurrence;
- determination of both sufficient and cost-effective countermeasures in order either to eliminate identified (or even possible in future) attacks, vulnerabilities and threats or make them difficult (or even impossible) to exploit by an attacker [19].

The actual decomposition of the real PSS of a specific infrastructure facility of the region can be described by the filling of the components and elements in accordance with the specifics of the technical implementation (see Figure 1). In the figure, for each element (subsystem), the proposed method of security analysis, which will be discussed in more detail later, is indicated.

After the designing of the structural-hierarchical scheme, it is necessary to research and analyse the behavior of the system and the individual elements and the interactions between them during the time.

Thus, the objectives of the section are the following:

- analysis IoT-based PSS;
- development of the scheme of research and development of models and methods of risk analysis of PSS, model of functions and components of PSS, fault models of PSS;
- discussion of analysis results and of the occurrence of failures in PSS.

Principles of IoT based physical security systems development

An example of the practical implementation of the structural hierarchical scheme for the PSS of the RI can be represented by a set of subsystems, e.g.: motion/intrusion detection subsystem and access control subsystem; 24/7 monitoring and signalling/alerting subsystems; CCTV subsystem; lighting subsystem; subsystem of communications and others.

The general view of the structural and hierarchical scheme of the PSS of the RI must be filled by the above subsystems (shown on Figure 2.1). Based on the example of the practical implementation of the structural hierarchical system for physical security of the RI facility, shown in Figure 2.1, we will consider modelling a prototype system using Raspberry Pi [20, 21] as the main module.

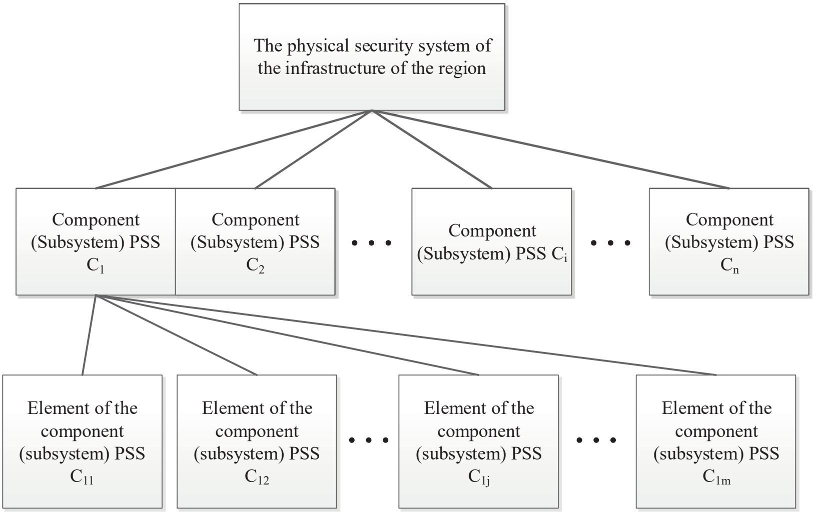

The physical security system of the infrastructure of the region
Component (Subsystem) PSS C_1
Component (Subsystem) PSS C_2
Component (Subsystem) PSS C_i
Component (Subsystem) PSS C_n
Element of the component (subsystem) PSS C_{11}
Element of the component (subsystem) PSS C_{12}
Element of the component (subsystem) PSS C_{1j}
Element of the component (subsystem) PSS C_{1m}

Fig. 1.1 - General view of the structural and hierarchical scheme of the physical security system

The Raspberry Pi microcomputer was chosen as the main control module due to the advantages in low power consumption, which allow creating an autonomous workstation for performing the tasks of automation. Due to the functional deployment using remote access and full-fledged graphic interfaces, this system is completely "friendly" for the operator and end user, which is not unimportant in the processing of information data [22].

Technical capabilities allow simulating the behavior of devices as connected directly through analog interfaces, and remotely via wireless systems. As the analogues of the microcomputer Raspberry Pi, the less expensive version which was studied is Banana Pi [23].

This is a hardware-software complex that allows performing operations like Raspberry Pi, but with some hardware deviations and reduced processing power.

More expensive analogue existed on the market which was reviewed during the research is CubieBoard4 [24].

Based on the device behavior pattern in the context of the common system, the purpose of the final product imposes a certain format of interaction between the modules.

For the description of attack scenarios (intrusion) or cascade failure of subsystems / elements, CASE-tool with the ability to describe the processes occurring in the system can be applied. To provide clarity, the scenario of power outage (accidental or intentional) in the interconnection of lighting and video surveillance subsystems, described in IDEF0 notation, is presented in Figure 1.3.

The next stage is to conduct the Failure, Modes, Effects, and Criticality Analysis for PSS (PSMECA) [26] which allows effectively solving the following problems:

- determination of possible types of failures of components (subsystems) of the system;
- analysis of the impact of these failures on the functioning of the system;
- establishing the countermeasures aka the possibilities (methods) of preventing failures and / or eliminating the effect of failures on the functioning of the system.

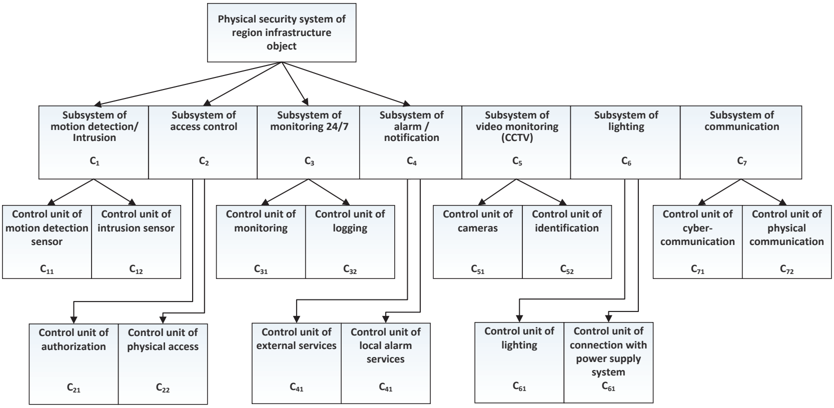

Physical security system of region infrastructure object
Subsystem of motion detection/ Intrusion C_1
Subsystem of access control C_2
Subsystem of monitoring 24/7 C_3
Subsystem of alarm / notification C_4
Subsystem of video monitoring (CCTV) C_5
Subsystem of lighting C_6
Subsystem of communication C_7
Control unit of motion detection sensor C_{11}
Control unit of intrusion sensor C_{12}
Control unit of monitoring C_{31}
Control unit of logging C_{32}
Control unit of cameras C_{51}
Control unit of identification C_{52}
Control unit of cyber-communication C_{71}
Control unit of physical communication C_{72}
Control unit of authorization C_{21}
Control unit of physical access C_{22}
Control unit of external services C_{41}
Control unit of local alarm services C_{41}
Control unit of lighting C_{61}
Control unit of connection with power supply system C_{61}

Fig. 1.2 - An example of practical implementation of the structural hierarchical scheme for the PSS of the RI facility

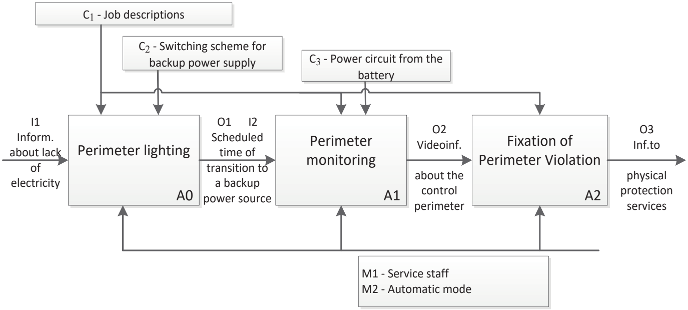

C1 - Job descriptions
C2 - Switching scheme for backup power supply
C3 - Power circuit from the battery
I1 Inform. about lack of electricity
Perimeter lighting
A0
O1 I2 Scheduled time of transition to a backup power source
Perimeter monitoring
A1
O2 Videoinf. about the control perimeter
Fixation of Perimeter Violation
A2
O3 Inf.to physical protection services
M1 - Service staff
M2 - Automatic mode

Fig. 1.3 - IDEF0 diagram of PSS functioning

Models of physical security systems risk analysis

The process of research and development of models and methods for the risk analysis of physical security systems has been carrying out in the corresponding scheme shown in Figure 3, where HW – hardware, SW – software, HF – human factor, PIMECA – Physical Intrusion Modes, Effects and Criticality Analysis, IIMECA – Information Intrusion Modes, and Criticality Analysis.

PIMECA and IIMECA are both modifications of FMECA. More information about variations of FMECA-family analysis methods, which specifically concentrates on corruption of information security and cybersecurity in a form of intrusions in complex systems could be found in [19; 27-29]. The problem of choice of FMECA-family techniques and tools for safety analysis of critical systems is described in [30].

Objects under study represent as follows: components of the system, their interrelations and functions as well as environment, which also plays a significant role during evaluation as well as its defects and faults. Environment state include both normal state (when single and multiple fault can occur, but their criticality and the related risk can be easily mitigated and so doesn’t harm the security properties) and aggressive environment state (with indication of single and multiple attacks, which can harm the security properties of the object), assessment of risk and consequences includes the appropriate method of risk assessment and its practical issues.

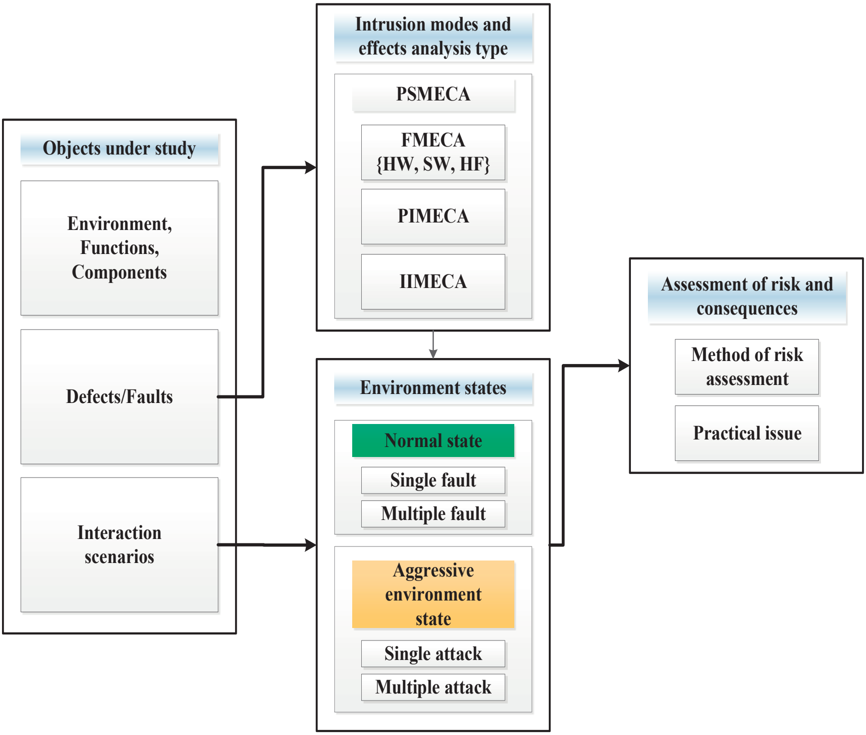


Fig. 1.4 - Scheme of research and development of models and methods of risk analysis of PSS

Models of physical security systems functions and components

This subsection contains formal description of the functions and components of PSS. *PSS* is a system of physical security, which is a part of the metasystem (*MS*), which in its turn includes the environment of the system (*ES*):

$$MS = \{PSS, ES\} \tag{1.1}$$

PSS is designed to perform the following functions:

$$SFPSS = \{FVis, FVDet, F\inf\}, \tag{1.2}$$

where *FVis*, *FVDet* , *Finf* are substes of visualization, detection and information processing correspondingly.

PSS consists of a set of disjoint components:

$$SCPSS = CHF \cup CHW \cup CSW, \tag{1.3}$$

where *CHF* – multiple components (operators) which are difficult to formalize, *CHW* – multiple hardware components, and *CSW* – multiple software components. In order to reveal prime reasons of failure occurrence the intersection of hardware components and software components, human factor and hardware components, human factor and software components are defined as null:

$$CHF \cap CHW = \varnothing, CSW \cap CHF = \varnothing, \mathrm{CHW} \cap \mathrm{CSW} = \varnothing. \tag{1.4}$$

In its turn

$$CHW = CHWS \cup CHWH, CHWS \cap CHWH = \varnothing, \tag{1.5}$$

where *CHWS* – a subset of hardware (primary) components - media of software (storage devices, data stores), *CHWH* - a subset of hardware (secondary) components – video cameras, motion sensors, presence, etc.

In its turn, the dependency between system software and applications could be written as:

$$CSW = CSWS \cup CSWA, CSWS \cap CHWA = \varnothing, \tag{1.6}$$

where *CSWS* – a subset of system software (operating systems), *CSWA* is a subset of application software (specialized software).

The environment includes physical components (*EPS)* and information components or subsystems (*EIS*). *EPS* and *EIS* subsystems are divided into natural (passive) subsystems (*EPNS* and *EINS*) and artificial (active or aggressive with respect to the system) – *EPAS* and *EIAS*.

From one side, systems environment consists of its physical and information components

$$ES = \{EPS, EIS\} \tag{1.7}$$

From other side it could be represented in a form of its environment states – normal (*ENS*) or aggressive (*EAS*)

$$ES = \{ENS, EAS\} \tag{1.8}$$

In other words, the medium can described by the Cartesian product

$$ES = \{EPS, EIS\} \times \{ENS, EAS\} = \{EPNS, EINS, EPAS, EINS\}. \tag{1.9}$$

There is a mapping ΩEC of sets of subsystems of the environment of functions

$$SFPSS = \{FVis, FDet, FInf\} \tag{1.10}$$

on sets of components

$$SCPSS = CHF \cup CHW \cup CSW \tag{1.11}$$

which could be represented as

$$\Omega EC : SFPSS \to SCPSS\ , \tag{1.12}$$

which is described by a Boolean matrix BFC , such that 0, if there is no influence (dependence); 1, if there is some influence; *Ø*, if the nature of the indicators is different.

There is a mapping ΩEF of sets of subsystems of the environment of functions

$$SFPSS = \{FVis, FDet, FInf\} \tag{1.13}$$

on sets of components

$$SCPSS = CHF \cup CHW \cup CSW \tag{1.14}$$

which could be represented as

$$\Omega FC : SFPSS \to SCPSS\ \ , \tag{1.15}$$

which is described by a Boolean matrix BFC with the following values:

- 0 – in case if there is no influence (dependence);
- 1 – in case if there is influence;
- Ø – in case if the nature of the indicators is different.

Fault models of physical security system

In accordance with [1, 3] the faults are divided into four types:

- physical (*pf*),
- project (*df*),
- operator (*hf*),
- interaction (*if*).

Respectively, a number of faults of the *SDPSS* of the *PSS* system consist of disjoint sub-spaces.

$$SDPSS = SDpf \cup SDdf \cup SDhf \cup SDif, \tag{1.16}$$

and

$$SDpf \cap SDdf = \varnothing,\ SDdf \cap\ SDif = \varnothing,\ SDpf \cap\ SDif = \varnothing, \ldots \tag{1.17}$$

The non-intersection of subsets of faults means that they concern different causes of their occurrence, but not consequences.

Given that

$$ES = \{EPS, EIS\},\quad SDPSS = SDpf \cup SDdf \cup SDhf \cup SDif \cup SDiif. \tag{1.18}$$

Errors associated with the actions of the operator can also be divided into those that cause physical defects (*hpf*) or information violations (*hif*).

In this case

$$SDPSS = SDpf \cup SDdf \cup SDhpf \cup SDhif \cup SDipf \cup SDiif. \tag{1.19}$$

There is a mapping ΩDC of set of system faults *SDPSS* on the set of components *SCPSS*:

$$\Omega DC : SDPSS \rightarrow SCPSS, \tag{1.20}$$

which is described by a Boolean matrix BDC, such that 0, if there is no influence (dependence); 1, if there is some influence; $\varnothing$, if the nature of the indicators is different.

Models of physical security systems functions and components

At this stage, it is necessary to determine the uniqueness of the correspondence of the failures arising in the physical security system (in fact – violations in the implementation of the functions specified in the system design) and the components of this system (necessary to perform the functions).

Thus, taking into account the occurrence of failures of different nature (hardware, software, human factor ones), the sought-for match is represented as a projection of the hierarchical structure on the table of the basic structural elements of the physical security system.

The construction of the table is caused by the need of justification of formal confirmation (proof) of the reason for including different types of components in the generated fault matrixes. PSMECA tables implies information from both FMECA and IMECA. This construction grounds on formulas 1.1-1.20 and allow us to formalize different nature of failure occurrence. The implementation is presented below in Fig 1.5.

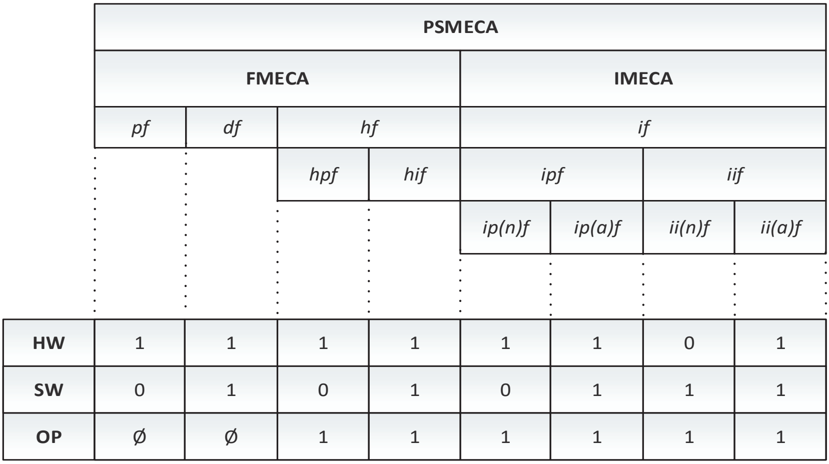
Considering the dynamical nature of failures in the system of physical security the necessity of defining set of scenarios is existed. Set of scenarios (*SScen*) consists of different consequence of events, which drive to failure. So, taking into account the scenarios of dynamical occurrence of failures in the system of physical security under investigation:

In this case

$$SScen = \sum SSceni,\ i = 1, \ldots, n \tag{1.21}$$

taking into account the factor of time (*t*).

Thus, the developed formalization of the hierarchical structure of failures in connection with failure source nature will allow creating PSMECA tables based on set-theoretical model of the PSS components.



	PSMECA							
	FMECA				IMECA			
	pf	*df*	*hf*		*if*			
			hpf	*hif*	*ipf*		*iif*	
					ip(n)f	*ip(a)f*	*ii(n)f*	*ii(a)f*
HW	1	1	1	1	1	1	0	1
SW	0	1	0	1	0	1	1	1
OP	Ø	Ø	1	1	1	1	1	1

Fig. 1.5 - The projection of the hierarchical structure of failures on the table of the main structural elements in the physical security system

Example

An example of PSMECA tables for the case of CCTV subsystem functioning in normal operation mode. The process of creating PSMECA tables begins from developing the similar (basic or source) FMECA tables, which are modified according to developed set-theoretical model of the PSS components. Main goal of such modification is to go deep into structure of analysed system failure sources to provide more strictly formalized approach, based on additional structure elements and levels of hierarchy, as shown in Figure 1.5.

Thus, for this example, first step will be developing the FMECA table of video surveillance subsystem. Table 1.1 depicts results of FMECA analysis, where: P – probability, S – severity, M – maintainability, C – Criticality. Probability, severity and maintainability are ranged from low (L) through medium (M) to high (H) and the assessment is expert-based.

The resulted level of criticality (C) is indicated by the maximum range of probability, severity, and maintainability for the corresponding mode of failure. Iuch fuzzy values (Low, Medium, High) are chosen just to demonstrate the opportunity of implementation of developed approach without unnecessary complication of calculations. FMECA table for the case of CCTV subsystem functioning in normal operation mode should be modified into similar PSMECA table according to the developed set-theoretical model of the PSS components.

The assessment of probability, severity and maintainability is also based on expert judgement. The probability for PSMECA is established as low (L), low to medium (L/M), which depends on aggressive environment conditions (e.g. in case of intensification of terrorist activities), medium (M) and high (H). For severity and maintainability the same range (low, medium, high) as in in previous case is used.Developed PSMECA table can be used for setting the more detailed causal relationship between subsystems, their failure types and PSS security risks.

Table 1.1 - FMECA table of CCTV subsystem functioning in normal operation mode

Subsystem	**Failure type**	**Failure mode**	**Failure cause**	**Failure effect**	**P**	**S**	**M**	**C**
Motion/ intrusion detection subsystem	HW	Does not start	Installation error or emergency stop (interrupt)	Movement monitoring within the controlled perimeter is disabled	L	H	L	H
		Improper functioning			M	M	M	M
	SW	Does not work	Staff error or design error		L	H	M	H
		No feedback			L	M	M	M
Access control subsystem	HW	Does not start	Installation error or emergency stop (interrupt)	Unauthorized access to the secured area can be granted	L	H	L	H
		Improper functioning			M	M	M	M
	SW	Improper functioning	Staff error or design error		L	M	M	M

Table 1.2 - PSMECA table of CCTV subsystem functioning in normal operation mode

Sub system	**Failure type**				**Failure mode**	**Failure cause**	**Failure effect**	**P**	**S**	**M**	**C**
Motion/ intrusion detection subsystem	HW	pf			Does not start	Installation error or emergency stop (interrupt)	Movement monitoring within the controlled perimeter is disabled	L	H	L	H
		df						L	H	L	H
		hf	hpf		Improper functioning			M	H	L	H
			hif					M	M	M	M
		if	ipf	ip(n)f				L	L	L	L
				ip(a)f				L/M	L	M	M
			iif	ii(a)f				L/M	H	H	H
	SW	df			Does not work	Staff error or design error		L	H	M	H
		hf	hif		No feedback			L	M	M	M
		if	ipf	ip(a)f				L/M	H	M	H
			iif	ii(n)f				L	L	M	M
				ii(a)f				L/M	H	H	H
Access control subsystem	HW	pf			Does not start	Installation error or emergency stop (interrupt)	Unauthorized access to the secured area can be granted	L	H	L	H
		df						L	H	L	H
		hf	hpf		Improper functioning			M	H	L	H
			hif					M	M	M	M
		if	ipf	ip(n)f				L	L	L	L
				ip(a)f				L/M	L	M	M
			iif	ii(a)f				L/M	H	H	H
	SW	df			Improper functioning	Staff error or design error		L	H	M	H
		hf	hif					L	M	M	M
		if	ipf	ip(a)f				L/M	H	M	H
			iif	ii(n)f				L	L	M	M
				ii(a)f				L/M	H	H	H

Thus, based on the results of Table 1.2, obtained from Table 1.1, it is possible to determine the cause of the failure occurrence in the physical security system and the value of failure criticality more accurately.

Execution order

In order to successfully development of summary project are needed:

1. Create a prototype of the final project, it may be simple, because it is not the aim of this course to make a complex fully functional project, also you can get really project from your environment;
2. Make the PSMECA analysis for that project;
3. Prepare the presentation for all previous steps;
4. Formulate outcomes;
5. Explain an understanding of the results.

Requirements to the content of the report

The report should include:

- title page;
- project name, goal and tasks;
- structural and functional decomposition of the physical security system of the RI was developed;
- engineering solutions for the implementation of the standard functions of the subsystems in the research object;
- the set-theoretical models of the physical security system components, environment and faults, and general issues of PSMECA-based assessment;
- presentation for all previous steps;
- conclusions.

Testing questions

1. What are basic tasks of physical security systems?
2. Which are objectives of physical security systems assessment?
3. What information need to gather for the research of the functioning of PSS?
4. What are the principles for developing IoT-based physical security systems?

5. What are steps of IDEF0 diagram of PSS functioning?
6. What are tasks solving by PSMECA?
7. What are elements/stages of the risk analysis of PSS?
8. What is difference between PIMECA and IIMECA?
9. What are the main features of the PSME(C)A technique?
10. How many types of PSS faults should be analysed?
11. Describe the hierarchical structure of failures.
12. What elements does consist the PSMECA platform of?

Recommended literature

1. 2010 Baghdad church massacre https://en.m.wikipedia.org/wiki/2010_Baghdad_church_massacre

2. CNN, Deadly bombings worst Iraq attack in two years, http://edition.cnn.com/2009/WORLD/meast/10/25/iraq.violence/index.html

3. BBC news, Gunmen attack Iraqi central bank, http://www.bbc.com/news/10304652

4. The Guardian, Six bombs, 95 dead – carnage and despair return to Iraq, https://www.theguardian.com/world/2009/aug/19/iraq-baghdad-bombings

5. The New York Times, Suicide Bomber Kills Dozens in Attack on Iraqi Army Recruits, https://mobile.nytimes.com/2010/08/18/world/middleeast/18iraq.html

6. Grand View Research, 'Physical Security Market Size, Share, & Trends Analysis Report By Component, By Hardware, By Services, By End-use (Energy, Utility, Retail, Commercial), And Segment Forecasts, 2018 – 2025', 51 p. https://www.grandviewresearch.com/industry-analysis/physical-security-market

7. Jing Xie, Chen-Ching Liu, Marino Sforna, Martin Bilek, Radek Hamza, "Threat assessment and response for physical security of power substations", Proceedings of Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES, 2014, October 12-15, Istanbul, pp. 1-6, DOI: 10.1109/ISGTEurope.2014.7028837

8. Jing Xie, Chen-Ching Liu, Marino Sforna, Martin Bilek, Radek Hamza, "Intelligent physical security monitoring system for power substations", Proceedings of Intelligent System Application to Power Systems (ISAP), 2015 18th International Conference on, Porto DOI: 10.1109/ISAP.2015.7325524

9. Han Lin, David Burnett, Don Sheaffer, Eric Arnold, "Applying decision analysis process to exterior physical security system technology design and selection", Proceedings of Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on, 5-8 Oct. 2009, Zurich, IEEE, pp. 312-312, DOI: 10.1109/CCST.2009.5335519

10. Siva RP, How to design effective physical security system, April 20, 2017, https://www.linkedin.com/pulse/how-design-effective-physical-security-system-siva-rp-cpp-psp/

11. Kline Technical Consulting, 'The 7 Most Critical Considerations for Physical Security Systems' Whitepaper http://www.klinenm.com/uploads/common/The_7_Most_Critical_Considerations_for_Physical_Security_Systems.pdf

12. Physical security systems. The assessment guide. US Department of Energy. Dec.2016 https://www.energy.gov/sites/prod/files/2017/02/f34/PhysicalSecuritySystemsAssessmentGuide_Dec2016.pdf

13. A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", IEEE Transactions on Dependable and Secure Computing, 1(1):11-33, Jan-March 2004.

14. M. Yastrebenetsky, V. Kharchenko (editors and authors), "Nuclear Power Plants Instrumentation and Control Systems for Safety and Security". Hershey PA, USA: IGI Global, 2014, 470 p.

15. Qahtan, M. A.-S. Abdulmunem, and Kharchenko, V., (2016). "Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models" in Proceedings of Third International Conference on Mathematics and Computers in Sciences and in Industry, China, Greece, 302-307. DOI: 10.1109/MCSI.2016.062.

16. F. Charlie and M. Brayon, "Physical Protection Principles", Nuclear Installation Dept. AELB. www.aelb.gov.my.

17. S. Harris, "Physical and Environmental Security. In CISSP Exam Guide", USA McGraw-Hill, 6th ed., pp.427-502 2013.

18. J. Conrath, "Structural Design for Physical Security: State of the Practice [et al.]", Task Committee, Structural Engineering Institute, ASCE Reston, 1999, 264 p.

19. Kharchenko, V. S, Illiashenko, O. A, et.al. (2014) "Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique", International Conference on Nuclear Engineering, Volume 3:

Next Generation Reactors and Advanced Reactors; Nuclear Safety and Security, ASME, 22nd International Conference on Nuclear Engineering ICONE

20. S. Monk, "Programming the Raspberry Pi: Getting Started with Python", McGraw Hill Professional, 2015, 192p.

21. J. Blum, "Exploring Arduino: Tools and Techniques for Engineering Wizardry", Jonh Willey & Sons, 2013, 384p.

22. Raspberry Pi Official page, https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

23. Banana Pi Official page, http://www.banana-pi.org/

24. Cubieboard Forum page, http://cubieboard.org/model/cb4/

25. Poschmann, A., Leander, G., Schramm, K., Paar, C., (2007) "New Light-Weight Crypto Algorithms for RFID', 2007 IEEE International Symposium on Circuits and Systems, New Orleans, LA, pp. 1843-1846.

26. Waleed, A. K. A., Kharchenko, V., Uzun, D., Solovyov, O., (2017) "IoT-based physical security systems: Structures and PSMECA analysis," 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, 2017, pp. 870-873.

27. Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A. (2006) "F(I)MEA-technique of Web Services Analysis and Dependability Ensuring", Lecture Notes in Computer Science, vol. 4157, 2006, pp. 153-167.

28. Babeshko, E., Kharchenko, V., Gorbenko. A. (2008) "Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assess-ment and Ensuring". Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX, 2008, pp. 309-315

29. Kharchenko,V., Illiashenko, O., Kovalenko, A., Sklyar, V., Boyarchuk, A., (2014) "Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique", Proceedings of the 22nd International Conference on Nuclear Engineering ICONE, Prague, Czech Republic.

30. Illiashenko, O., Babeshko, E. (2012) "Choosing FMECA-based techniques and tools for safety analysis of critical systems" Information & Security: An International Journal, 2012, no. 28(2), pp. 275-285

31. Tempus SEREIN project official website http://serein.eu.org/

32. Erasmus+ ALIOT project official website http://aliot.eu.org/

APPENDIX A

TEACHING PROGRAMME OF THE COURSE ITM5 "IOT FOR INDUSTRIAL SYSTEMS"

DESCRIPTION OF THE COURSE

TITLE OF THE COURSE	Code
IoT for Industrial Systems	**ITM6**

Teacher(s)	Department
Coordinating: Prof., DrS. V.S. Kharchenko	Computer Systems Networks and Cyber Security (KhAI)
Others: Modules ITMM5.1: Assoc. Prof., Dr. S.V. Morshchavka, Assoc. Prof., Dr. R.K. Kudermetov	Software Tools (ZNTU)
ITMM5.2: Prof., DrS. I.S. Skarga-Bandurova, Assoc. Prof., Dr. T.O. Biloborodova, Ph.D. Student A.Y. Velykzhanin, Ph.D. Student Y.O. Krytska	Computer Engineering (EUNU)
ITMM5.3: Prof., DrS. V.S. Kharchenko, Assoc. Prof., Dr. H.V. Fesenko ITMM5.4: Assoc. Prof., Dr. D. D. Uzun, PhD student O.O. Solovyov, PhD student Al-Khafaji Ahmed Waleed	Computer Systems Networks and Cyber Security (KhAI)

Study cycle	Level of the course	Type of the course
Trainings	A	Bounden

Form of delivery	Duration	Language(s)
Full-time tuition	One semester	English

Prerequisites	
Prerequisites: Software Control Systems in Industry; Internet-of-Drone-based systems; Information-Networking Technologies in Industry; Foundations of Modeling; Computer Systems and System Analysis; Theory of Automatic Control; Programming, Telecommunications Foundations;	**Co-requisites (if necessary):** IoT for Smart Energy Grid; IoT for Smart Building and City; IoT for Intelligent Transport Systems; IoT for Health Systems; IoT for Industrial Systems.

Probability Theory and Foundations of Mathematical Statistics; Foundation of Modeling; Intelligent Systems; Computer Systems and System Analysis.			
Credits of the course	**Total student workload**	**Contact hours**	**Individual work hours**
4	120	56	64

Aim of the course: competences foreseen by the study programme
The aim of the course is to create a knowledge base for multidisciplinary research in the field of the building and further use of IoT-based systems for, to give students practical skills in designing and implementation of modern systems based on IoT as well modernization of existing ecology, safety and security monitoring systems using IoT technology. The IoT technologies considered to implement the monitoring and control tasks of industrial facilities, as well as the issues of industrial networks security are considered. The study expands theoretical background of IoT-based ecology, safety and security monitoring systems, also considers intelligent approaches to efficiency improving of IoT-based ecology, safety and security monitoring systems. In addition, the local aim of course is to create a knowledge base for multidisciplinary research on intelligence technologies of IoT for ecology, safety and security monitoring systems and to provide a prerequisites for practical use of intelligence methods for application of IoT technologies in engineering. The study also expands the current research on IoT for ecology, safety and security monitoring by combining intelligence technologies and theory of ecology, safety and security monitoring systems in the context of the study of IoT technologies in engineering.

Learning outcomes of course	**Teaching/learning methods**	**Assessment methods**
At the end of course, the successful student will be able to:		
1. Learn the physical principles and basics of work of sensors for monitoring artificial ecosystems	Interactive lectures, Just-in-Time Teaching	Course Evaluation Questionnaire
2. Learn the basic concepts and architecture of IoT water monitoring systems (WMS)	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Course Evaluation Questionnaire

3. Create own IoT WMS for industrial and (or) municipal water data	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Course Evaluation Questionnaire
4. Learn the basic concepts and architecture of Multi-version drone-based systems for monitoring of NPP severe accidents	Interactive lectures, Just-in-Time Teaching	Course Evaluation Questionnaire
5. Learn the development of summary project for IOT based physical security systems of buildings and campuses	Interactive lectures, Just-in-Time Teaching	Course Evaluation Questionnaire

Themes	**Contact work hours**							**Time and tasks for individual work**	
	Lectures	Consultations	Seminars	Practiacl work (training)	Laboratory work	Placements	**Total contact work**	**Individual work**	**Tasks**
1. IOT systems for controlling small artificial ecological systems 1.1. Sensors for monitoring artificial ecosystems, the basics of work and physical principles 1.2. Features of the collection and analysis of information about the state of ecosystems by using IoT devices 1.3. Examples of control systems for small artificial ecosystems	6		2	6			**14**	**16**	1.4. Estimating parameters of fields and other ecological systems via UAV 1.5. IoT systems for agriculture

2. IoT technologies for monitoring and control tasks implementation in industry 2.1. IoT Water Monitoring System (WMS) 2.2. Parameters and data management in IoT WQMS 2.3. IoT WQMS evolution: from collecting data and data visualization to real-time predictive analytics	6			8			**14**	**16**	2.4. Collation of the available features and components of IoT WMS to implement water monitoring, selection of specified components 2.5. Determination of the completeness and objectivity of water quality characteristics that were investigated (critical assessment algorithms forecasting)
3. IoT-based systems for monitoring of severe accidents 3.1. General information on systems for monitoring of critical industry objects/NPP accidents 3.2. Multi-version drone-based systems for monitoring of NPP severe accidents 3.3. Reliability of IoD-based systems for monitoring of NPP severe accidents	6			8			**14**	**16**	3.4. Survivability of drone-based systems for monitoring of NPP severe accidents 3.5. Using the travelling safety problem with drones approaches for NPP monitoring mission planning
4. IoT based physical security systems of buildings and campuses 4.1. Physical security systems assessment and	6			8			**14**	**16**	4.4. Ehe main features of the PSME(C)A technique 4.5. PSMECA

development tasks 4.2. IoT based physical security systems development 4.3. Models of physical security systems risk analysis									based assessment of physical security systems
On the whole	**24**		**2**	**30**			**56**	**64**	

Assessment strategy	Weight in %	Deadlines	Assessment criteria
Lecture activity, including fulfilling special self-tasks	10	7,14	85% – 100% Outstanding work, showing a full grasp of all the questions answered. 70% – 84% Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material. 60% – 69% A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics. 50% – 59% There should be a good grasp of several important topics, but with only a limited understanding or ability in places. There may be significant omissions. 45% – 49% Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others will be either omitted or incorrect. 40% – 44% There should be some work of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range. 20% – 39% There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little

			relevant and correct material in places. 0% – 19% Very little or nothing that is correct and relevant.
Learning in laboratories	30	7,14	85% – 100% An outstanding piece of work, superbly organized and presented, excellent achievement of the objectives, evidence of original thought. 70% – 84% Students will show a thorough understanding and appreciation of the material, producing work without significant error or omission. Objectives achieved well. Excellent organization and presentation. 60% – 69% Students will show a clear understanding of the issues involved and the work should be well written and well organized. Good work towards the objectives. The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments. 50% – 59% The work should show evidence that the student has a reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organization should be reasonably clear, and the objectives should at least be partially achieved. 45% – 49% Students will show some appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives. 40% – 44% There should be some work towards the laboratory work objectives, but significant issues are likely to be

			neglected, and there will be little or no appreciation of the complexity of the problem. 20% – 39% The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements. 0% – 19% Very little or nothing that is correct and relevant and no real appreciation of the laboratory work requirements.
Course Evaluation Quest	60	8,16	The score corresponds to the percentage of correct answers to the test questions

Author	Year of issue	Title	No of periodical or volume	Place of printing. Printing house or internet link
Compulsory literature				
R. H. Weber, R. Weber	2010	Internet of Things.		Berlin, Heidelberg: Springer-Verlag
D. Giusto, A. Lera, G. Morabito, L. Atzori	2010	The Internet of Things		Berlin, Heidelberg: Springer-Verlag
D. Uckelmann, M. Harrison, F. Michahelles	2011	Architecting the Internet of Things		Berlin, Heidelberg: Springer-Verlag
D. Pimentel, B. Berger, D. Filiberto, M. Newton, B. Wolfe, E. Karabinakis, S. Clark, E. Poon, E. Abbett, S. Nandagopal	2004	Water resources: agricultural and environmental issues	Vol. 54, No. 10	BioScience
J. Zhao, J. Zhang, Y. Feng, J. Guo	2010	The study and application of the IOT technology		3rd International Conference on Computer Science

		in agriculture		and Information Technology
A. Elsts, R. Balass, J. Judvaitis, R. Zviedris, G. Strazdins, A. Mednis, L. Selavo	2012	SADmote: A Robust and Cost-Effective Device for Environmental Monitoring	Vol. 7179	ARCS LNCS
S. Ivanov, K. Bhargava, W. Donnelly	2015	Precision Farming: Sensor Analytics	Vol. 30, No. 4	IEEE intelligent Systems
P. Lottes, R. Khanna, J. Pfeifer, R. Siegwart, C. Stachniss	2017	UAV-based crop and weed classification for smart farming		IEEE International Conference on Robotics and Automation (ICRA)
K. O. Flores, I. M. Butaslac, J. E. M. Gonzales, S. M. G. Dumlao, R. S. J. Reyes	2016	Precision agriculture monitoring system using wireless sensor network and Raspberry Pi local server		IEEE Region 10 Conference (TENCON)
J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao	2017	A survey on internet of things: Architecture enabling technologies security and privacy and applications	Vol. 4, No. 5	IEEE Internet of Things Journal
V. Radhakrishnan and W. Wu	2018	IoT technology for Smart water system		IEEE 20th Intern. Conf. on High Performance Computing and Communications; IEEE 16th Intern. Conf. on Smart City; IEEE 4th Intl. Conf. on Data

				Science and Systems
T. P. Lambrou, C. C. Anastasiou, C. G. Panayiotou and M. M. Polycarpou	2014	A Low-Cost Sensor Network for Real-Time Monitoring and Contamination Detection in Drinking Water Distribution Systems		IEEE Sensors Journal
S.K. Alshattnawi	2018	Smart Water Distribution Management System Architecture Based on Internet of Things and Cloud Computing		Proc. IEEE Intern. Conf. on New Trends in Computing Sciences
International Atomic Energy Agency	2015	Accident monitoring systems for nuclear power plants	No. NP-T-3.16	IAEA, Vienna
R. Hiromoto, A. Sachenko, V. Kochan, V. Koval, V. Turchenko, O. Roshchupkin, and K. Kovalok	2014	Mobile Ad Hoc wireless network for pre- and post-emergency situations in nuclear power plant		Proc. 2nd IEEE Int. Symp. on Wireless Systems within the Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)
V. Kharchenko	2016	Diversity for safety and security of embedded and cyber physical systems: fundamentals review and		Proc. of the 15th Biennial Baltic Electronics Conf. (BEC)

		industrial cases		
A. Sachenko, V. Kochan, V. Kharchenko, M. Yastrebenetsky, H. Fesenko, and M. Yanovsky	2017	NPP post-accident monitoring system based on unmanned aircraft vehicle: Concept, design principles	Vol. 73, No. 1	
V. Kharchenko, H. Fesenko, A. Sachenko, R. Hiromoto, and V. Kochan	2017	Reliability issues for a multi-version post-severe NPP accident monitoring system	Vol. 2	Proc. 9th IEEE Int. Conf. Intell. Data Acquisition and Advanced Computing Syst.: Technology and Applicat. (IDAACS)
H. Fesenko, V. Kharchenko, A. Sachenko, R. Hiromoto, and V. Kochan	2018	An Internet of Drone-based Multi-version Post-severe Accident Monitoring System: Structures and Reliability		Dependable IoT for Human and Industry Modeling, Architecting, Implementation, The Netherlands, River Publishers
Iinternational electrotechnical commission	2011	Nuclear Power Plants – Control Rooms – Design	Standard 60964	IEC, Geneva
S. Monk	2015	Programming the Raspberry Pi: Getting Started with Python		McGraw Hill Professional
J. Blum	2013	Exploring Arduino: Tools and Techniques for Engineering Wizardry		Jonh Willey & Sons

Additional literature				
H.A Lee, N. Lee	2016	Compressive Sensing-based		Proc. IEEE Conference ICTC

		Data Processing Method for Massive IoT Environments		
Y. Ji, C. Bockelmann, A. Dekorsy	2015	Compressed sensing based multi-user detection with modified sphere detection in machine-to machine communications		Proc. Intern. ITG Conf. on Systems, Communications and Coding
International Atomic Energy Agency	2012	Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series	No. SSR-2/1	IAEA, Vienna

APPENDIX B

SKETCHES FOR TRAINING 1 (ITM 5.4)

SKETCH FOR ELECTRICAL CONDUCTIVITY ELECTRODE

```
#include "DFRobot_EC.h"
#include <EEPROM.h>

#define EC_PIN A1
float voltage,ecValue,temperature = 25;
DFRobot_EC ec;

void setup()
{
  Serial.begin(115200);
  ec.begin();
}

void loop()
{
    static unsigned long timepoint = millis();
    if(millis()-timepoint>1000U)  //time interval: 1s
    {
      timepoint = millis();
      // read the voltage
      voltage = analogRead(EC_PIN)/1024.0*5000;

      // read your temperature sensor to execute
      //temperature compensation
      //temperature = readTemperature();

      // convert voltage to EC with temperature
compensation
      ecValue =  ec.readEC(voltage,temperature);
      Serial.print("temperature:");
      Serial.print(temperature,1);
      Serial.print("^C  EC:");
      Serial.print(ecValue,2);
      Serial.println("ms/cm");
    }
    // calibration process by Serail CMD
    ec.calibration(voltage,temperature);
}

float readTemperature()
{
```

```
//add your code here to get temperature from your
temperature sensor
}
```

Sketch for pH Meter

```
#include "DFRobot_PH.h"
#include <EEPROM.h>

#define PH_PIN A1
float voltage,phValue,temperature = 25;
DFRobot_PH ph;

void setup()
{
    Serial.begin(115200);
    ph.begin();
}

void loop()
{
    static unsigned long timepoint = millis();
    //time interval: 1s
    if(millis()-timepoint>1000U){
        timepoint = millis();

        // read your temperature sensor
        //to execute temperature compensation
        //temperature = readTemperature();

        // read the voltage
        voltage = analogRead(PH_PIN)/1024.0*5000;
        // convert voltage to pH with temperature
compensation
        phValue = ph.readPH(voltage,temperature);
        Serial.print("temperature:");
        Serial.print(temperature,1);
        Serial.print("^C  pH:");
        Serial.println(phValue,2);
    }
    // calibration process by Serail CMD
    ph.calibration(voltage,temperature);
}

float readTemperature()
{
  /*add your code here to get the
    temperature from your temperature sensor*/
}
```

Sketch for ORP Meter

```
#define VOLTAGE 5.00    //system voltage
#define OFFSET 0        //zero drift voltage
#define LED 13         //operating instructions

double orpValue;

#define ArrayLenth  40    //times of collection
//orp meter output,connect to Arduino controller ADC pin
#define orpPin 1[redacted]

int orpArray[ArrayLenth];
int orpArrayIndex=0;

double avergearray(int* arr, int number){
  int i;
  int max,min;
  double avg;
  long amount=0;
  if(number<=0){
    printf("Error number for the array to avraging!/n");
    return 0;
  }
  if(number<5){ //less than 5, calculated directly 
statistics
    for(i=0;i<number;i++){
      amount+=arr[i];
    }
    avg = amount/number;
    return avg;
  }else{
    if(arr[0]<arr[1]){
      min = arr[0];max=arr[1];
    }
    else{
      min=arr[1];max=arr[0];
    }
    for(i=2;i<number;i++){
      if(arr[i]<min){
        amount+=min;        //arr<min
        min=arr[i];
      }else {
        if(arr[i]>max){
          amount+=max;    //arr>max
          max=arr[i];
        }else{
          amount+=arr[i]; //min<=arr<=max
        }
      }//if
    }//for
    avg = (double)amount/(number-2);
  }//if
  return avg;
}


void setup(void) {
  Serial.begin(9600);
  pinMode(LED,OUTPUT);
}

void loop(void) {
  //analog sampling interval
  static unsigned long orpTimer=millis();
  static unsigned long printTime=millis();
  if(millis() >= orpTimer)
  {
    orpTimer=millis()+20;
    //read an analog value every 20ms
    orpArray[orpArrayIndex++]=analogRead(orpPin);
    if (orpArrayIndex==ArrayLenth) {
      orpArrayIndex=0;
    }
    orpValue=((30*(double)VOLTAGE*1000)
      - (75*avergearray(orpArray, ArrayLenth)
      * VOLTAGE*1000/1024))/75-OFFSET;

    //convert the analog value to orp according the circuit
  }
  //Every 800 milliseconds, print a numerical,
  //convert the state of the LED indicator
  if(millis() >= printTime)
  {
  printTime=millis()+800;
  Serial.print("ORP: ");
  Serial.print((int)orpValue);
        Serial.println("mV");
        digitalWrite(LED,1-digitalRead(LED));}}
```

APPENDIX C

AT COMMANDS FOR TRAINING 2 (ITM 5.4)

Commands	Description	Set/Execute	Parameters
AT+RST	restart the module	–	–
AT+CWMODE	wifi mode	AT+CWMODE=<mode>	1= Sta, 2= AP, 3=both
AT+CWJAP	join the AP	AT+ CWJAP =<ssid>,< pwd >	ssid = ssid, pwd = wifi password
AT+CWLAP	list the AP	AT+CWLAP	
AT+CWQAP	quit the AP	AT+CWQAP	
AT+ CWSAP	set the parameters of AP	AT+ CWSAP= <ssid>,<pwd>,<chl>, <ecn>	ssid, pwd, chl = channel, ecn = encryption
AT+ CIPSTATUS	get the connection status	AT+ CIPSTATUS	
AT+CIPSTART	set up TCP or UDP connection	1)single connection (+CIPMUX=0) AT+CIPSTART= <type>,<addr>,<port>; 2) multiple connection (+CIPMUX=1) AT+CIPSTART= <id><type>,<addr>, <port>	id = 0-4, type = TCP/UDP, addr = IP address, port= port
AT+CIPSEND	send data	1)single connection(+CIPMUX=0) AT+CIPSEND=<length>; 2) multiple connection (+CIPMUX=1) AT+CIPSEND= <id>,<length>	
AT+CIPCLOSE	close TCP or UDP connection	AT+CIPCLOSE=<id> or AT+CIPCLOSE	
AT+CIFSR	Get IP address	AT+CIFSR	
AT+	set mutiple	AT+	0 for single

CIPMUX	connection	CIPMUX=<mode>	connection 1 for mutiple connection
AT+ CIPSERVER	set as server	AT+ CIPSERVER= <mode>[,<port>]	mode 0 to close server mode, mode 1 to open; port = port
+IPD	received data		

APPENDIX D

AT COMMANDS FOR TRAINING 3 (ITM 5.4)

```
#include <SoftwareSerial.h>
#define RX 2
#define TX 3
String AP = "YOU_SSID_NAME";       // CHANGE ME
String PASS = "YOU_PASSWORD"; // CHANGE ME
String API = "YOU_API_WRITE_KEY";   // CHANGE ME
String HOST = "184.106.153.149";
String PORT = "80";
String field = "field1";
int countTrueCommand;
int countTimeCommand;
boolean found = false;
int valSensor = 1;
SoftwareSerial esp8266(RX,TX);

void setup() {
  Serial.begin(9600);
  esp8266.begin(115200);
  delay(7000);
  sendCommand("AT",5,"OK");
  sendCommand("AT+CWMODE=1",5,"OK");
  sendCommand("AT+CWJAP=\""+ AP +"\",\""+ PASS +"\"",20,"OK");
}
void loop() {
 valSensor = getSensorData();
 String getData = "GET /update?api_key="+ API +"&"+ field
+"="+String(valSensor);
 sendCommand("AT+CIPMUX=1",5,"OK");
 sendCommand("AT+CIPSTART=0,\"TCP\",\""+ HOST +"\","+
PORT,15,"OK");
 sendCommand("AT+CIPSEND=0,"
+String(getData.length()+4),4,">");
 esp8266.println(getData);delay(1500);countTrueCommand++;
 sendCommand("AT+CIPCLOSE=0",5,"OK");
}
int getSensorData(){
  return random(1000); // Replace with
}
void sendCommand(String command, int maxTime, char
readReplay[]) {
  Serial.print(countTrueCommand);
  Serial.print(". at command => ");
  Serial.print(command);
  Serial.print(" ");
  while(countTimeCommand < (maxTime*1))
  {
    esp8266.println(command);//at+cipsend
    if(esp8266.find(readReplay))//ok
    {
      found = true;
      break;
    }

    countTimeCommand++;
  }

  if(found == true)
  {
    countTrueCommand++;
    countTimeCommand = 0;
  }

  if(found == false)
  {
    countTrueCommand = 0;
    countTimeCommand = 0;
  }

  found = false;}
```

APPENDIX E

CODE FOR TRAINING 3 (ITM 5.4)

```
#include "DFRobot_EC10.h"
#include <EEPROM.h>
#include <SoftwareSerial.h>

#define RX 2
#define TX 3
#define EC_PIN A1

String AP = "YOU_SSID_NAME";            // CHANGE ME
String PASS = "YOU_PASSWORD"; // CHANGE ME
String API = "YOU_WRITE_API_KEY";        // CHANGE ME
String HOST = "184.106.153.149";
String PORT = "80";
String field = "field1";
int countTrueCommand;
int countTimeCommand;
boolean found = false;
String valSensor;
float voltage,ecValue,temperature = 25;

SoftwareSerial esp8266(RX,TX);
DFRobot_EC10 ec;

void setup()
{
  Serial.begin(115200);
  ec.begin();
  esp8266.begin(115200);
  delay(7000);
  sendCommand("AT",5,"OK");
  sendCommand("AT+CWMODE=1",5,"OK");
  sendCommand("AT+CWJAP=\""+ AP +"\",\""+ PASS
+"\"",20,"OK");
}

void loop()
{
    static unsigned long timepoint = millis();
    if(millis()-timepoint>65000U)  //time interval: 65s
    {
      timepoint = millis();
      voltage = analogRead(EC_PIN)/1024.0*5000;  // read
the voltage
      ecValue =  ec.readEC(voltage,temperature);  //
```

```
convert voltage
      //to EC with temperature compensation
      sendData(ecValue);
    }
}

//Don't change
void sendData(float vol){
 valSensor = String(vol);
 String getData = "GET /update?api_key="+ API +"&"+
field +"="+String(valSensor);
 sendCommand("AT+CIPMUX=1",5,"OK");
 sendCommand("AT+CIPSTART=0,\"TCP\",\""+ HOST +"\","+
PORT,15,"OK");
 sendCommand("AT+CIPSEND=0,"
+String(getData.length()+4),4,">");

esp8266.println(getData);delay(1500);countTrueCommand++;
 sendCommand("AT+CIPCLOSE=0",5,"OK");
}

void sendCommand(String command, int maxTime, char
readReplay[]) {
  Serial.print(countTrueCommand);
  Serial.print(". at command => ");
  Serial.print(command);
  Serial.print(" ");
  while(countTimeCommand < (maxTime*1))
  {
    esp8266.println(command);//at+cipsend
    if(esp8266.find(readReplay))//ok
    {
      found = true;
      break;
    }

    countTimeCommand++;
  }

  if(found == true)
  {
    Serial.println("OYI");
    countTrueCommand++;
    countTimeCommand = 0;
  }

  if(found == false)
  {
    Serial.println("Fail");
    countTrueCommand = 0;
    countTimeCommand = 0;
  }

  found = false;
}
```

АНОТАЦІЯ

УДК 004.415/.416:502.17](076.5)=111

Морщавка С.В., Кудерметов Р.К., Скарга-Бандурова І.С., Білобородова Т.О., Критська Я.О., Великжанін А.Ю., Фесенко Г.В., Харченко В.С., Узун Д.Д., Ілляшенко О.О., Соловйов О.О., Аль-Хафаджі Ахмед Валід. **Інтернет речей для систем моніторингу екології та безпеки: Тренінги** / За ред. В.С. Харченка та Г.В. Фесенка. – МОН України, Запорізький національний технічний університет, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ». – 119 с.

Викладено матеріали тренінгової частини курсу ITM5 “IoT для систем моніторингу екології та безпеки ”, 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 систем моніторингу екології та безпеки. Вивчаються структури, моделі та технології розробки IoT для систем моніторингу екології та безпеки, сучасні методики і засоби проектування, модернізації та впровадження таких систем, застосування IoT технологій в інженерії безпеки.

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

Бібл. – 52, рисунків – 57, таблиць – 7.

ЗМІСТ

CONTENTS

Сергій Володимирович Морщавка
Равіль Камілович Кудерметов
Інна Сергіївна Скарга-Бандурова
Тетяна Олександрівна Білобородова
Яна Олександрівна Критська
Артем Юрійович Великжанін
Герман Вікторович Фесенко
Вячеслав Сергійович Харченко
Дмитро Дмитрович Узун
Олег Олександрович Ілляшенко
Олександр Олександрович Соловйов
Ахмед Валід Аль-Хафаджі

Інтернет речей для систем моніторингу екології та безпеки: Тренінги

(англійською мовою)

Редактори: Харченко В.С. та Г.В. Фесенко

Комп'ютерна верстка
Г.В. Фесенко
О.О.Ілляшенко

Зв. план, 2019
Підписаний до друку 27.08.2019
Формат 60х84 1/16. Папір офс. No2. Офс. друк.
Умов. друк. арк. 7,09. Уч.-вид. л. 7,62. Наклад 150 прим.
Замовлення 270819-6

Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут"
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu

Випускаючий редактор: ФОП Голембовська О.О.
03049, Київ, Повітрофлотський пр-кт, б. 3, к. 32.
Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців,
виготовлювачів і розповсюджувачів видавничої продукції
серія ДК No 5120 від 08.06.2016 р.

Видавець: ТОВ «Видавництво «Юстон»
01034, м. Київ, вул. О. Гончара, 36-а, тел.: +38 044 360 22 66
www.yuston.com.ua
Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців,
виготовлювачів і розповсюджувачів видавничої продукції
серія ДК No 497 від 09.09.2015 р.