ALIoT

Internet of Things for Industry and Human Applications

Internet of Things for Smart Energy Grid

TRAININGS

Funded by the
Erasmus+ Programme
of the European Union

Internet of Things for Industry and Human Applications

Internet of Things for Smart Energy Grid

Ministry of Education and Science of Ukraine
Ternopil National Economic University
Petro Mohyla Black Sea National University
National Aerospace University "Kharkiv Aviation Institute"

Z.I. Dombrovskyi, A.O. Sachenko, I.M. Zhuravska,
M.Z. Dombrovskyi, G.M. Hladiy, M.P. Musiyenko,
Y.M. Krainyk, E.V. Brezhniev, M.O. Kolisnyk

Internet of Things for Industry and Human Applications

Internet of Things for Smart Energy Grid

Trainings

Edited by E.V. Brezhniev

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/.416:621.31](076.5)=111
I-73

Reviewers:
Dr. Ah-Lian Kor, Leeds Beckett University, UK
DrS, Prof. Volodymyr Mokhor, director of Pukhov Institute for Modelling in Energy Engineering, corresponding member of NAS of Ukraine

I-73 Z.I. Dombrovskyi, A.O. Sachenko, I.M. Zhuravska, M.Z. Dombrovskyi, G.M. Hladiy, M.P. Musiyenko, Y.M. Krainyk, E.V. Brezhniev, M.O. Kolisnyk. **Internet of Things for Smart Energy Grid**: Trainings / Brezhinev E.V. (Ed.) – Ministry of Education and Science of Ukraine, Ternopil National Economic University, Petro Mohyla Black Sea National University, National Aerospace University "KhAI", 2019. – 141 p.

ISBN 978-617-7361-91-5.

The materials of the training part of the study course ITM1 "IoT for Smart Energy Grid", developed in the framework of the ERASMUS+ ALIOT project "Internet of Things: Emerging Curriculum for Industry and Human Applications" (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

The structure of work on verification of residual knowledge in the discipline, the corresponding practical material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical aspects of IoT for smart energy grid are presented. IoT infrastructure for smart energy grid based on embedded systems devices, its safety, reliability and security are examined.

It is intended for engineers, developers and scientists engaged in IoT for smart energy grid, for postgraduate students of universities studying in areas of IoT-based systems, smart energy grid, embedded systems, as well as for teachers of relevant course.

Ref. – 49 items, figures – 62, tables – 9.

Approved by Academic Council of National Aerospace University "Kharkiv Aviation Institute" (record No 6, February 22, 2017).

ISBN 978-617-7361-91-5.

Міністерство освіти і науки України
Тернопільський національний економічний універиситет
Чорноморський національний університет ім. Петра Могили
Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський Авіаційний Інститут”

Домбровський З.І., Саченко А.О., Журавська І.М.,
Домбровський М.З., Гладій Г.М., Мусієнко М.П.,
Крайник Я.М., Брежнєв Є.В., Колісник М. О.

Інтернет речей для індустріальних і гуманітарних застосунків

ІНТЕРНЕТ РЕЧЕЙ ДЛЯ РОЗУМНОЇ ЕНЕРГЕТИЧНОЇ МЕРЕЖІ

Тренінги

Редактор Брежнєв Є.В.

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

2019

УДК 0 04.415/.416:621.31](076.5)=111
І-73
Рецензенти: Др. А-Ліан Кор, Leeds Beckett University, Велика Британія

Д.т.н., проф. Володимир Мохор, директор інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, член-кореспондент НАН України

І-73 Домбровський З.І., Саченко А.О., Журавська І.М., Домбровський М.З., Гладій Г.М., Мусієнко М.П., Крайник Я.М., Брежнєв Є.В., Колісник М.О. **Інтернет Речей для розумної енергетичної мережі. Тренінги** / За ред. Є.В. Брежнєва – МОН України, Тернопільський національний економічний університет, Чорноморський національний університет ім. Петра Могили, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», 2019. – 141 с.

ISBN 978-617-7361-91-5.

Викладено матеріали тренінгової частини курсу ITM1 “IoT для розумної енергетичної мережі”, 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 практичний матеріал, приклади виконання завдань та критерії оцінювання. В процесі навчання наводяться теоретичні аспекти IoT для розумної енергетичної мережі. Вивчаються IoT-інфраструктура для інтелектуальної енергетичної мережі на основі пристроїв вбудованих систем.

Призначено для інженерів, розробників та науковців, які займаються розробкою та впровадженням IoT для розумної енергетичної мережі, для аспірантів університетів, які навчаються за напрямами IoT систем, розумних енергетичних мереж, вбудованих систем, а також для викладачів відповідних курсів.

Бібл. – 49, рисунків – 62, таблиць – 9.

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

ISBN 978-617-7361-91-5.

ABBREVIATIONS

AC – availability function

AMI – Advanced Metering Infrastructure;

AP – Access Point;

API – Application Programming Interface;

CDR – Cloud-Based Demand Response;

CLI – Command-Line Interfaces;

DoS – Denial-of-Service attack

DDoS – Distributed Denial-of-Service attack

D^2R – Dynamic Demand Response Optimization;

DR – Demand Response;

EQI – Electricity Quality Indicators;

GUI – Graphical User Interfaces;

HAN – Home Area Network;

IaaS – Infrastructure-as-a-Service;

ICT – Informatively-Communication Technologies;

IoT – Internet of Things

LAN – Local Area Network ()

LCD – Liquid Crystal Display

M2M – Machine-to-Machine;

NAN – Neighborhood Area Network;

NICT – New Information and Communication Technologies;

NTE – New Power Technologies;

PaaS – Platform-as-a-Service;

PLC – Power Line Communications

PS – Power System;

PSG – Power Smart Grid;

QoS – Quality of Service;

SEG – Smart Energy Grid

SEM – Smart Energy Meters

SG – Smart Grid

WAN – Wide Area Network;

WSN – Wireless Sensor Networks.

UART – Universal Asynchronous Receiver-Transmitter

INTRODUCTION

The materials of the training part of the study course ITM1 “IoT for Smart Energy Grid”, developed in the framework of the ERASMUS+ ALIOT project “Internet of Things: Emerging Curriculum for Industry and Human Applications” (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)*.

The structure of work on verification of residual knowledge in the discipline, the corresponding practical material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical aspects of IoT for smart energy grid are presented. IoT infrastructure for smart energy grid based on embedded systems devices, its safety, reliability and security are examined.

The module ITM1.1 “Integration of IoT and Smart Grid components” contains of 3 training packages.

First training package includes studying the problem of existing grid as well as a conceptual model of Smart Grid (SG). Its aim is to learn the implementation of the smart grid in the existing grid.

Second training package includes the studying the problems of SG implementation and applying the IoT in SG projects. Its aim is to learn the structure of integrated Smart Grid system in IOT environment.

Third training package includes studying a conceptual model of Cloud computing and integrating the Cloud computing and Big Data into the Smart Grid environment. Its aim is to learn for implementing the Cloud computing and Big Data in the smart grid.

The module ITM1.2 “IoT infrastructure for smart energy grid based on embedded systems devices” contains 1 seminar and 3 trainings.

The first seminar is intended to provide understanding of the fundamental concepts of the SEG and its local area and IoT appliances specifically.

The first training is concerned with smart meter connection and PLC-equipment configuration to obtain data from smart meter to the network.

The second training is oriented on the topic of IoT-devices programming. Students are to program development board with STM32 microcontroller and WiFi-module ESP8266 which are contemporary hardware components for sensor networks.

The third training is supposed to provide basic knowledge about modern software infrastructures and particularly on cloud-based development environment mbed.

The module ITM1.3 “Availability assessment of IoT based IT infrastructure of Power Grids” includes 1 training and 1 laboratory work. The training is intended to provide the theory and practice of the Bayesian (BBN) and Fault Tree Analysis (FTA) application for safety and reliability assessment of IoT based smart grid and systems. Laboratory work is focused on usage of the Markov models for dependability assessment for SG systems and practical exercises on how transition rates values of Markov model of SG system functioning change availability function of SG system.

The module ITM1.4 “IoT for smart grid safety and security management” includes two trainings. Training 1 is focused on obtaining the basic skills of applying STAMP models for analyzing of safety/security accidents related to IoT based smart grid and systems. The second training is focused on training of skills of root cause analysis of smart grid security accidents with application of 5Why method.

The course is intended for engineers, developers and scientists engaged in IoT for smart energy grid, for postgraduate students of universities studying in areas of IoT-based systems, smart energy grid, embedded systems, as well as for teachers of relevant course.

Practicum prepared by D. Dombrovskyi, A. Sachenko, I. Zhuravska, M. Dombrovskyi, G. Hladiy, M. Musiyenko, Y. Krainyk, D. Hladiy, E. Brezhniev, M. Kolisnyk. General editing was performed by Professor of National Aerospace University “KhAI”, DrS. Brezhniev E.V.

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.

[*] 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.

ITM1.1. Integration of IoT and Smart Grid components

Ph.D. Z.I. Dombrovskyi, Prof., DrS. A.O. Sachenko,
M.Z. Dombrovskyi, Ph.D. G.M. Hladiy (TNEU)

Training 1

THE INTEGRATED SMART GRID SYSTEM IN IOT ENVIRONMENT

The aim of the training: to learn the implementation of the smart grid in the existing grid.

Learning objectives:

1. Studying the problem of existing grid.
2. Studying a conceptual model of Smart Grid
3. Studying the methods used in trainings and their implementation;

Practical tasks:

Criteria for selecting the Investment Projects to implement the smart grid in the existing grid.

Preparation for the training needs:

1. Get the topic of the analytical review and clarify conditions of the task.
2. To develop a work plan and distribute roles between group members (Students arrange among themselves parts of the work for which they will report)

Training implementation during the training needs:

1. Search information of the training topic and the received task.
2. Perform the necessary actions to complete the received task.
3. Get the results needs to complete the task.
4. Develop a frame for both report and presentation, which illustrate the implementation of the received task.
5. Write a report.
6. Prepare a presentation.

Defending the training results

1. Presenting and defending a work and the report.
2. Evaluation of work.

Theoretical information

Existing grid problem and its solution

In the global market environment, the development of business entities, including the energy company, is ongoing throughout the world.

Existing electricity networks cannot provide a constant increase in electric power consumption due to low efficiency associated with transmission losses. Stakeholders often do not have the needed knowledge to set goals for the development of the network and implementation of PSG (Power Smart Grid) to make strategic decisions aimed at introducing PSG innovative technologies using IoT.

In the conditions of the dynamic change of market priorities of energy, tasks and solutions, the imperfection of the existing supply system, the organizational structure of supply and management companies, does not allow us to increase their competitiveness and the quality of products and services in line with the growing demands of consumers.

In this case, it is important to identify the possibility of forming "super-objective" ways of working, which include the system approach, modeling, forecasting and design.

The development of society is accompanied by increasing consumption of electric energy.

The restructuring of energy, the creation of an energy market, and the implementation of energy saving technologies have led to new relationships between the staff of power plants, electrical networks and consumers. Losses from the power supply breakdown, the reasons for the output of parameters for the quality of electricity at normalized values and the associated losses are not abstract. Consumers are not always satisfied with the quality and value of services they use.

All this requires an integrated approach to the quality of energy supply. Every consumer of electrical energy must have uninterrupted supply of high-quality electrical energy. To ensure uninterrupted supply of electrical energy, reliable electrical systems must be provided. That is, you need to have power lines (transmission lines) that meet the necessary operating conditions. However, one uninterrupted supply of electric energy does not end, because the electricity released to consumers should be of appropriate quality: by frequency and voltage. We can almost measure frequency fluctuations, but we cannot influence it. Fluctuations and deviations of voltage, we have the ability to adjust to some extent. In this case, the main subject of demand is the power consumption of electric energy. This means that the object of marketing is the mode of consumption of electric energy in general: in the daily, weekly and seasonal (annual) aspects.

Therefore, it's necessary to propose an innovative project to reorganize the organizational structure of the energy supply company based on the experience of partner teams and world achievements by moving to a virtual enterprise in the field of electricity supply using smart grids, IoT technology and cloud computing.

Organization of hardware control of electricity quality indicators (EQI), organizational and economic mechanism of influence on the cause of deterioration of the electricity quality, development of methods and technical ways for elimination of distortions is important for the normalization of the electric power quality. Due to the mutual influence of consumers, it is necessary to formulate conditions for joining the network of new consumers.

Since virtually all technical means for increasing the quality of electricity have in their composition reactive elements and it is necessary therefore to maintain a balance of reactive power in the network.

Problems in Power Grid and a Smart Grid conceptual model. Several basic decencies in the traditional electric grid increase its vulnerability to failure as power use continues to rise.

Because electricity cannot be stored, whatever amount of power is needed at a given moment must be generated and transported to the end users at that moment.

This means that the traditional electric grid must always be capable of generating at peak load capacity even though that peak load may only be required for a few hours a day. In fact, the grid must have some excess generating capacity above any anticipated peak because if demand rises at any time above the system's ability to respond with adequate power, the result will be some type of power failure in the system.

Peak demand in one part of the grid may be met by transporting power into the high - demand area from another part of the grid where demand is lower, but this is an incident and potentially dangerous method of meeting peak-demand needs. The further electric power is transported over high-voltage transmission lines, the more power is lost due to resistance in the wires.

The old technology of power grid turns into a factor of restricting a final consumption. Therefore, to protect, control and optimize the energy consumption of all consumers needs innovative technology upgrading power system (PS).

The purpose of this part is to establish requirements for building smart (intelligent) business processes of the integrated power grid system and to develop a conceptual model of a prospective vision of the smart energy system based on cyber physical methods (table 1).

Table 1 - Characteristics of Existing Grid and Smart Grid

Existing Grid	**Smart Grid**
Electromechanically	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors thousand
Manual monitoring	Self-monitoring
Manual restoring	Self-healing
Failures and blackout	Adaptive and islanding
Limited control	Pervasive control
Few customer choices	Many customer choices

The term “Grid” referees to the electrical grid that provides energy to the end consumer. The “grid” amounts to the networks that carry electricity from the plants where it is generated to consumers. Smart grid is an approach in which user safety should be ensured while monitoring, updating and continuously reliably distributing electricity grid by adding smart meters and monitoring systems to the power grid in order to ensure electronic communication between suppliers and consumers. A smart grid is an electrical grid that uses information and communications technology to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity.

Smart grids include electricity networks (transmission and distribution systems) and interfaces with generation, storage and end-users. While many countries have already begun to “smarten” their electricity system, all countries will require significant additional investment and planning to achieve a smarter grid. Smart grids are an evolving set of technologies that will be deployed at different rates in a variety of settings around the world, depending on local commercial attractiveness, compatibility with existing technologies, regulatory developments and investment frameworks.

The smart grid topology needs to adapt and shift from a centralized source to a distributed topology that can absorb different energy sources in a dynamic way. There is a need to track real-time energy consumption and demand to the energy supply: this goes with the deployment of more remote sensing equipment capable of measuring, monitoring and communicating.

A smart grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users. Smart grids co-ordinate the needs and capabilities of all generators, grid operators, end-users and electricity market stakeholders to operate all parts of the system as efficiently as possible, minimizing costs and environmental impacts while maximizing system reliability, resilience and stability.

The concept of SG (fig.1) is quite comprehensive, although there is no unique definition. According to the IEEE P2030 Project “the Smart Electric Grid or Smart Power (Smart Grid) is a complex end to end system that is composed of multiple sub-power systems interconnected and interrelated to each other through multiple protocols that contain multiple layers of technologies (energy, ICT and control/automation) ”.

Nowadays it is possible to point the row of priority directions, where we observe the most of the progress.

The first direction is modernization of main and distributive networks, introduction of technological components of Smart Grid.

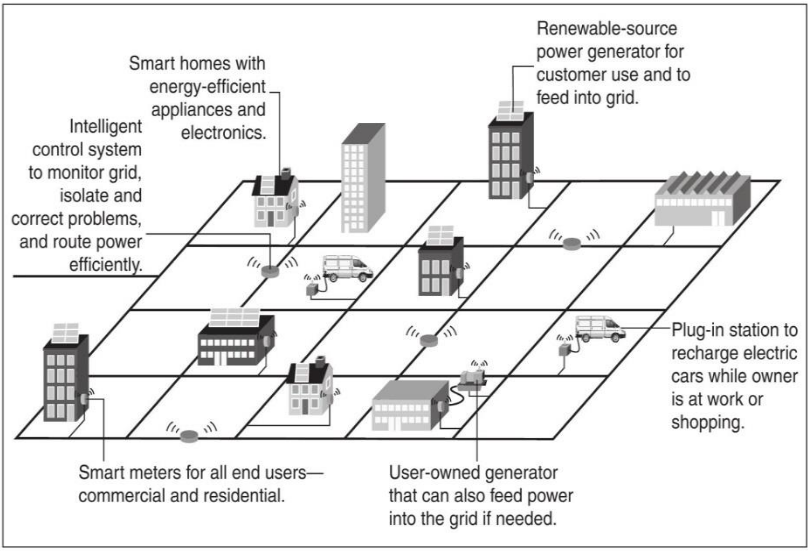

Renewable-source power generator for customer use and to feed into grid.
Smart homes with energy-efficient appliances and electronics.
Intelligent control system to monitor grid, isolate and correct problems, and route power efficiently.
Plug-in station to recharge electric cars while owner is at work or shopping.
Smart meters for all end users—commercial and residential.
User-owned generator that can also feed power into the grid if needed.

Fig.1 - Smart Grid conceptual model

The second direction is integration of the dispersed generation and renewable energy sources in the power system.

The third direction is introduction of «intelligent» account and of communication infrastructure for consumers.

The European Union’s Smart Grid vision of the European Technology Platform SG is shown in fig. 2.

Example of applying the basic principles of Smart Grid

The growth of cities and significant increasing the cost of electricity and developing generation increases the risk of threats and leads to changing the strategy and improving the management of energy supply.

The main prerequisites for improving the management of energy supply are:

– separation of local markets;

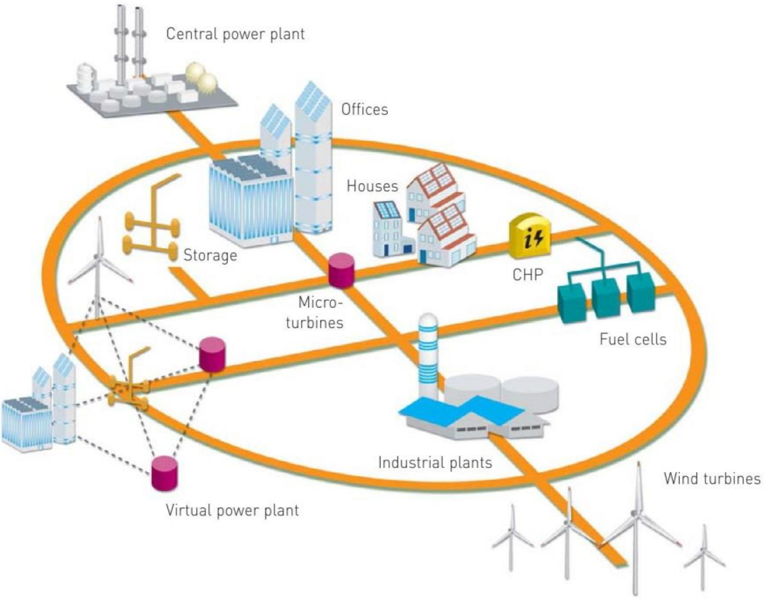


Fig. 2 - European Union’s Smart Grid vision of the European Technology Platform SG

– the emergence of active consumers;
– increasing competition from local energy trading platforms;
– global strategy to reduce energy consumption;
– improving the quality of energy consumers cities.

Thereby, the emphasis is made on the three generations of Smart Grid which enables to move coherently in the direction of the goal model. (See table 2).

Table 2 – Tree generations of Smart Grid

Development stages	Key Characteristics
Current state	Analog devises (meters). Digital meters. Control system for local decisions
SG 1	Response on demand. Specialized devises. Distributed automatization
SG 2	Network interconnection (IP)

	protocols. Power storage
SG 3	Power rooming. Power trade. Peer to peer
SG 4 of IoT	Internet of Things in power smart grid

Smart Grid 1.0 – state of power generation infrastructure

In which individual devices and system objects can connect to the network without using general digital standards;

Smart Grid 2.0 – state of power infrastructure, by which the connection of any system nodes is only possible under condition of switching to a unified IP protocol and interconnection of the nodes into unified integrated IP network;

Smart Grid 3.0 – flexible power system that is based on the principles of decentralized control and equality of the consumer and the supplier

Internet of Things (IoT): A network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

From a technical view, the SG can be divided into the three major systems: smart infrastructure, smart management and smart protection systems.

The smart infrastructure system is the energy, information, and communication infrastructure underlying the SG. It supports two-way flow of electricity and information.

The Smart grid architecture (Fig. 3) increases the capacity and flexibility of network and provides both advanced sensing and control through modern communications technologies.

New Grid Paradigms - Micro grid: Distributed generation promotes the development of a new grid paradigm, called micro grid, which is seen as one of the cornerstones of the future SG. It is expected the organic evolution of the SG comes through the plug-and-play integration of micro grids (Fig. 4).

A micro grid is a localized grouping of electricity generations, energy storages, and loads. In the normal operation, it is connected to a traditional power grid (macro grid).

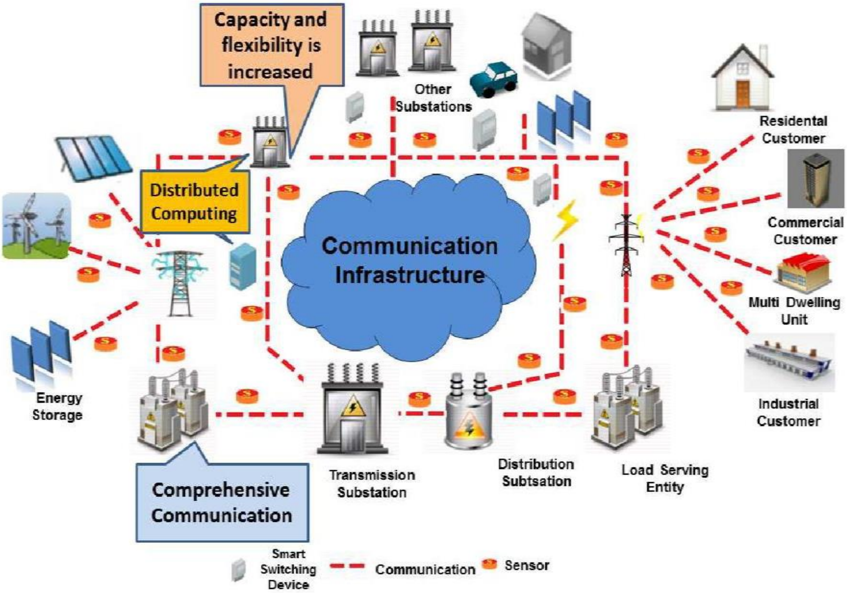


Fig. 3 - Smart grid architecture

The users in a micro grid can generate low voltage electricity using distributed generation, such as solar panels, wind turbines, and fuel cells. The single point of common coupling with the macro grid can be disconnected, with the micro grid functioning autonomously.

This operation will result in an islanded micro grid, in which distributed generators continue to power the users without obtaining power from the electric utility located in the macro grid (fig. 5). Thus, the multiple distributed generators and the ability to isolate the micro grid from a larger network in disturbance will provide highly reliable electricity supply. Note that although these users do not obtain the power from outside in the islanding mode, they may still exchange some information with the macro grid.

The lower layer shows a physical structure of this micro grid, including four buildings, two wind generators, two solar panel generators, and one wireless access point (AP). These buildings and generators exchange power using powerlines.

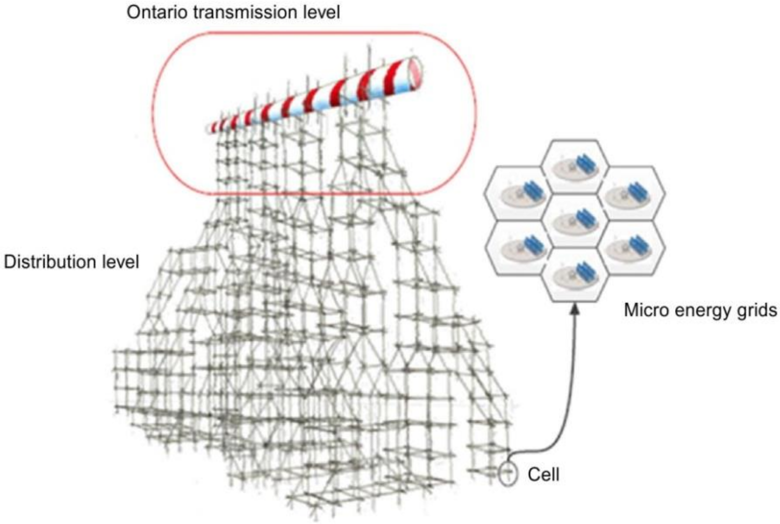


Fig. 4 - Micro grid as a localized grouping of electricity generations, energy storages, and loads

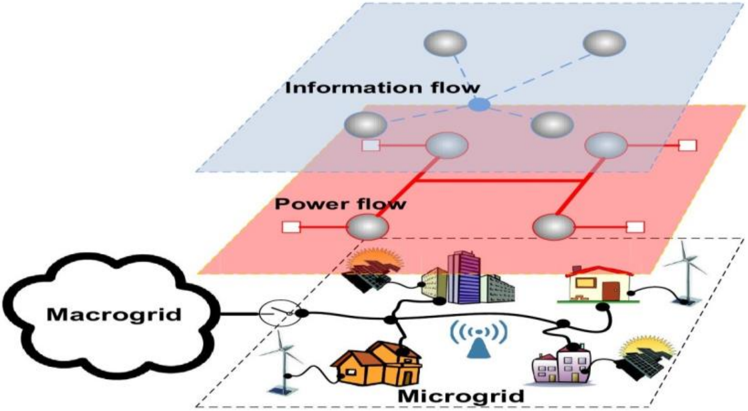


Fig. 5 - Example of Micro grid

Holistic viewpoint of an overall architecture named Smart Grid Architecture Model European Commission’s Standardization Mandate

M/490 is shown in fig. 1.6, and the Step-by-step implementation of this European model Smart Grid is shown in fig. 7.

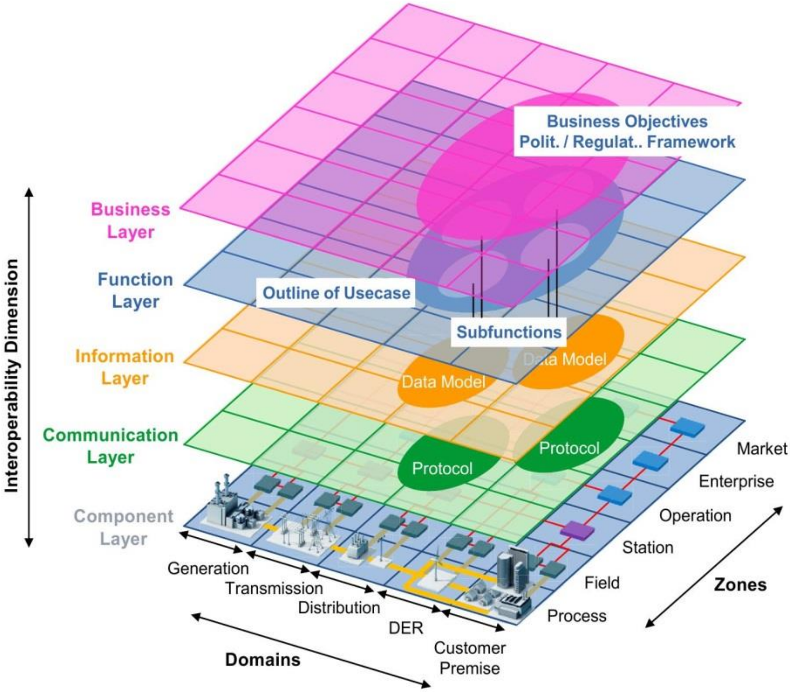


Fig. 6 - Integrated model architecture named as Smart Grid (Architecture Model European Commission’s Standardization Mandate M/490)

The computational efficiency in grid operations is low, and that can lead to the inability of grid operations of real-time (fig. 8).

Test questions

The material above describes the basic tasks of Smart Grid system in IoT environment. For a better study of the educational material, we suggested a list of test questions below:

1. What is the smart grid? Give a definition of smart grid.
2. What differences are between the smart grid and existing grid?
3. Why do we need a smart grid?
4. What is the micro grid

5. What are the smart grid costs and benefits?
6. What types of smart grid are used in power engineering?
7. How does Internet technology affect the smart grid?

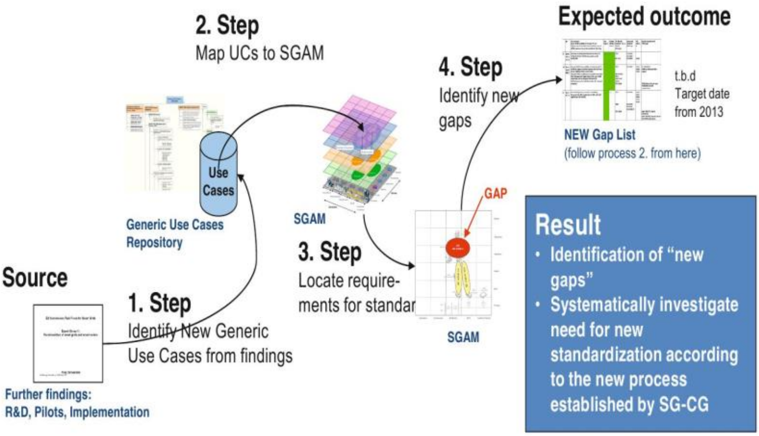

2. Step
Map UCs to SGAM
Use Cases
Generic Use Cases Repository
SGAM
Source
1. Step
Identify New Generic Use Cases from findings
Further findings: R&D, Pilots, Implementation
3. Step
Locate require-ments for standar
4. Step
Identify new gaps
GAP
SGAM
Expected outcome
t.b.d
Target date from 2013
NEW Gap List
(follow process 2. from here)
Result
• Identification of "new gaps"
• Systematically investigate need for new standardization according to the new process established by SG-CG

Fig. 7 - Implementation of SG model step-by-step

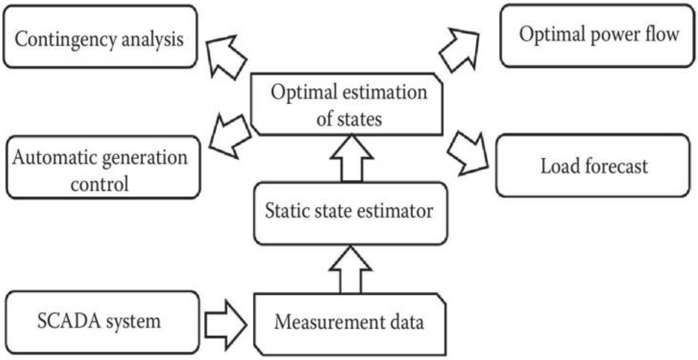


Fig. 8 - Functional structure of real-time power grid operations

Recommended literature

1. International Energy Agency Smart Grid Roadmap. – https://www.iea.org/publications/free publications/publication/ smartgrids_roadmap.pdf.

2. Fitzpatrick, G.J. and Wollman, D.A. (2010) NIST Interoperability Framework and Action Plans. IEEE Power and Energy Society General Meeting, Minneapolis, 25-29 July 2010, 1-4. http://dx.doi.org/10.1109/pes.2010.5589699.

3. T. Basso, J. Hambrick, D. DeBlasio (2012) Update and review of IEEE P2030 Smart Grid Interoperability and IEEE 1547 interconnection standards. 2012 IEEE PES Innovative Smart Grid Technologies (ISGT).

4. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. NIST Special Publication 1108r3. – September 2014.

5. Faheem M.S., Shah B.H., Butt R.A., Raza B., Anwar M., Ashraf M.W., Ngadi M.A., Gungor V.C. (2018) Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. Computer Science Review. August 2018. – pp.1-30.

9. X. Jin, Z. He, Z. Liu, (2011) Multi-agent-based cloud architecture of smart grid, Energy Procedia, 2011, 12, pp. 60–66.

10. Kuzlu M., Pipattanasomporn M., Rahman S. (2014) Communication network requirements for major smart grid applications in HAN, NAN and WAN. Computer Networks, 67, 2014, pp. 74-88.

11. Garner, G. (2010) Designing Last Mile Communications Infrastructures for Intelligent Utility Networks (Smart Grids). IBM Australia Limited.

12. Al-Omar, B., Al-Ali, A.R., Ahmed, R. and Landolsi, T. (2012) Role of Information and Communication Technologies in the Smart Grid. Journal of Emerging Trends in Computing and Information Sciences, 3, 707-716.

13. Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C. and Hancke, G.P. (2013) A Survey on Smart Grid Potential Applications and Communication Requirements. IEEE Transactions on Industrial Informatics, 9, pp. 28-42. http://dx.doi.org/10.1109/TII.2012.2218253

14. Hatziargyriou, N., "Microgrids-The future of small grids," Key note speech, Future Power Systems, FPS 2005, Amsterdam, 16-18 November 2005.

TRAINING 2
APPLYING THE IOT IN SMART GRID PROJECTS

The aim of the training: to learn the structure of integrated Smart Grid system in IoT environment.

Learning Objectives:

1. Studying the problem implementation of the smart grid.
2. Study of applying the IoT in Smart grid projects.
3. Studying the methods used in trainings and their implementation.
4. Studying the methods of image base creation.

Practical tasks: a conceptual model applying the IoT in Smart grid projects.

Preparation for the training needs:

1. Get the topic of the analytical review and clarify the conditions of the task.
2. To develop a work plan and distribute responsibility between group members (students arrange among themselves parts of the work for which they will report)

Training implementation

During the training needs:

1. Search information of the training topic and the received task.
2. Perform the necessary actions to complete the received task.
3. Get the results needs to complete the task.
4. Develop a plan of the report and presentation, which illustrate the implementation of the received task.
5. Write a report.
6. Prepare a presentation.

Defend training results

1. Presenting and defending a work and the report.
2. Evaluation of the work.

Theoretical information

Applying the IoT in Smart grid projects

In fact, the new technology will be successful in the case where it is combined with that of the management. So important is the desires of researchers to identify such dependencies, fundamental foundations in the realization of the potential scientific and technological factors, which have followed specific management strategies, improve the management and their consequences. In today's globally competitive economy, business survival factor is the ability and flexibility to respond to dynamic market changes and provide the individual needs of consumers at market price. Thus is the introduction of innovations in technology and management. The need for the introduction of innovative technologies in management due to the time factor.

Management of the PS on decision-making time is divided into long and short term (Fig. 9).

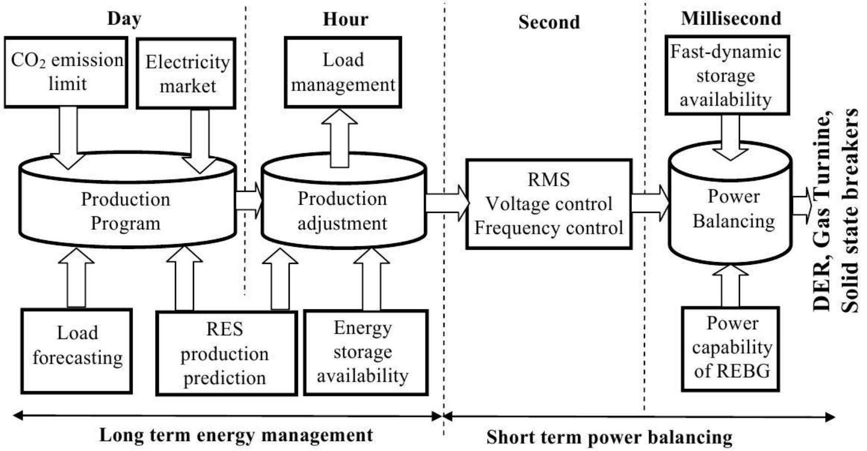

Day
Hour
Second
Millisecond
CO₂ emission limit
Electricity market
Load management
Fast-dynamic storage availability
Production Program
Production adjustment
RMS Voltage control Frequency control
Power Balancing
DER, Gas Turnine, Solid state breakers
Load forecasting
RES production prediction
Energy storage availability
Power capability of REBG
Long term energy management
Short term power balancing

Fig. 9 - Timing classification of control functions for PS management

In the long run, there a number of contentious interactions between the components of the following management activities:

- a lack of functional approaches in their bureaucracy and benefits system in their consideration of the external environment. Therefore, to succeed in global competition, instead of using the system functions;

- a technology is becoming "smarter" and faster, which requires a new definition of the role of managers;

- a standardization helps to reduce costs and increase profitability, flexibility and ensures the survival of companies in the face of a changing environment;

- contrary to market values are measured activity of less money terms, and becoming increasingly important criterion for activity.

In the short run briefly (seconds, milli sec) is a critical time and information to make decisions, because power management in real time requires the introduction of a cybernetic system.

The above formulation can include relationship to a new paradigm of scientific and technological factors, and the efficiency of such provisions. First, the technology becomes a limiting factor. Second, performance indicators are increasingly becoming consumer ratings, foundation management activities should be perceived consumer value and consumer decisions regarding their consumption. So based on this idea we should start today on transformation of management strategy from system- oriented approach to client- oriented in IoT environment.

Development of intelligent power grids directions. One of directions is the distributed generation. The transition from hard supervisory planning and regulation to organize coordinated work of all network facilities. Distribution management features throughout its architecture. The introduction of new technologies and security devices that provide maneuverability and controllability PS and its facilities. Creation of intelligent measurement, calculation, diagnostics and management, covering distributed generation, transmission, distribution and consumption.

Formation of highly integrated information and computer structures as PS core consists of autonomous energy sources (solar, wind).

Forming the strategic vision redistribution. Electricity requirements and basic functional properties of all elements of the power system: generation, transmission and distribution, sales, consumption and dispatch. New solutions and technologies for active - adaptive features, including a new system status monitoring, self-healing, relay protection and emergency automation, energy metering systems

Major characteristics of a smart substation shall include digitalization, autonomization, coordination, and self-healing.

The single point of common coupling with the macro grid can be disconnected, with the micro grid functioning autonomously (Fig. 10).

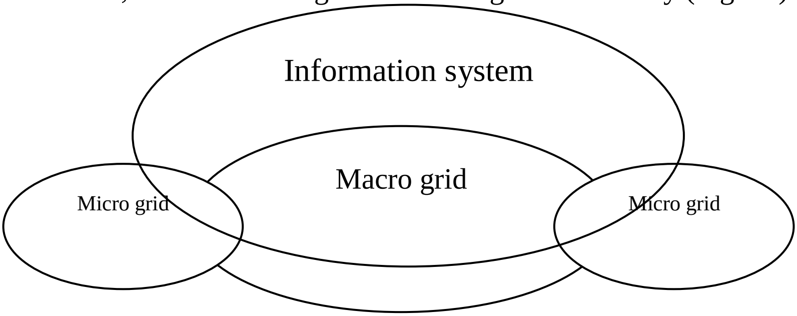


Fig. 10 - Example of a power grids and information system combination

Implementation of the strategy carried out based on the concept of Smart - Self-Monitoring, Analysis and Reporting Technology management principles Grid - self monitoring, analysis, reporting and technology. Smart grid - set of organizational changes, new models of processes and decisions in the field of information technology and solutions in the field of automated process control systems and supervisory control in the electricity.

A key feature of smart grids is the interconnection of a potentially large number of disparate energy distribution networks, power generating sources and energy consumers.

The components of each of these entities will need a way of communicating that will be independent of the physical medium used and also independent of manufacturers and the type of devices.

Appearance of new technologies on the joint of NTE (new power technologies) and NICT (new information and of communication technologies) requires introduction in an action of standards that als must be set in a collaboration with the organs of standardization and divided by two areas: electric networks and of informatively-communication technologies (ICT). Separate components of Smart Grid are an equipment of distributive networks, intelligent meters, objects of individual generation. Model of SG operating is shown in fig. 11.

As a result, multiple communication technologies and standards could coexist in different parts of the system.

Wireless sensor networks (WSN) application should be extended to smart grid and metering. WSN has been an active research topic for nearly ten years and has found many applications.

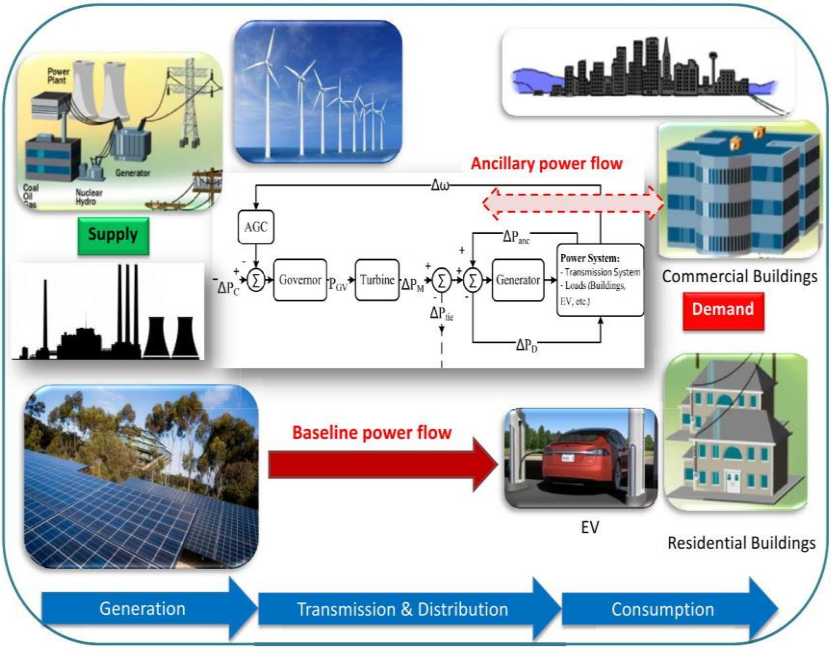


Fig. 11 - Model of SG operating

Smart grid/metering appear to be a major application for WSN, especially related to Internet of Things and machine-to-machine (M2M) communications. Existing industry efforts include IETF 6LoWPAN and ROLL. Internetworking between cellular networks and local area networks (e.g. WLAN) has received a lot of attention because of the need for seamless mobility and quality of service (QoS) requirements.

Because of the scale and deployment complexity of smart grids, telecommunication network systems supporting smart grids are likely to rely on the existing public networks such as cellular and fixed wired access technologies, as well as private and dedicated networks belonging to different administrative domains.

A logical model in Fig. 12 illustrates a conceptual diagram for SG Information Network, showing the interconnections of networks between various domains.

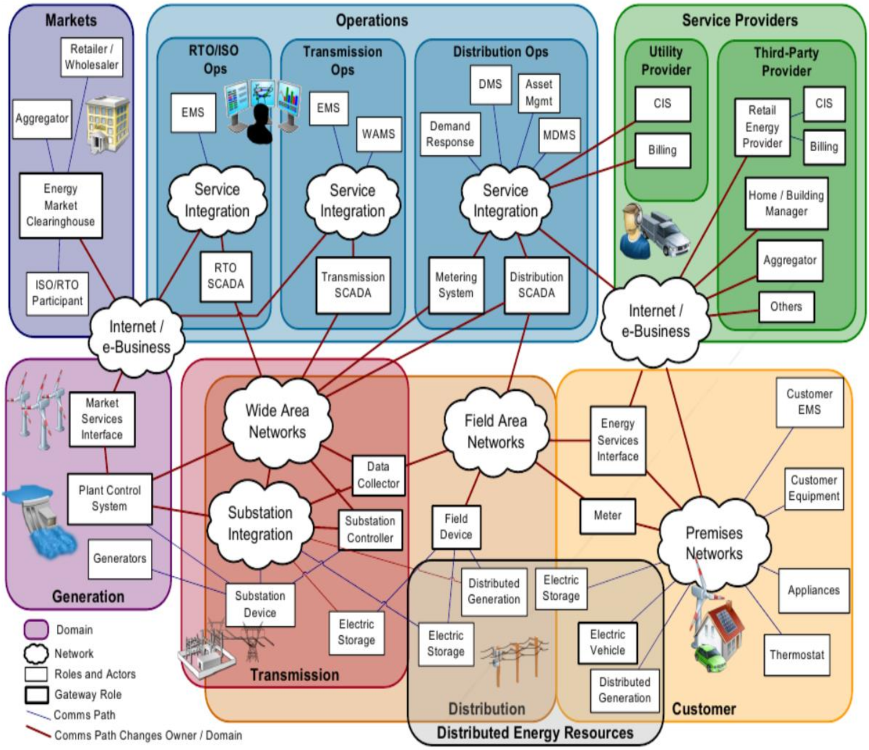
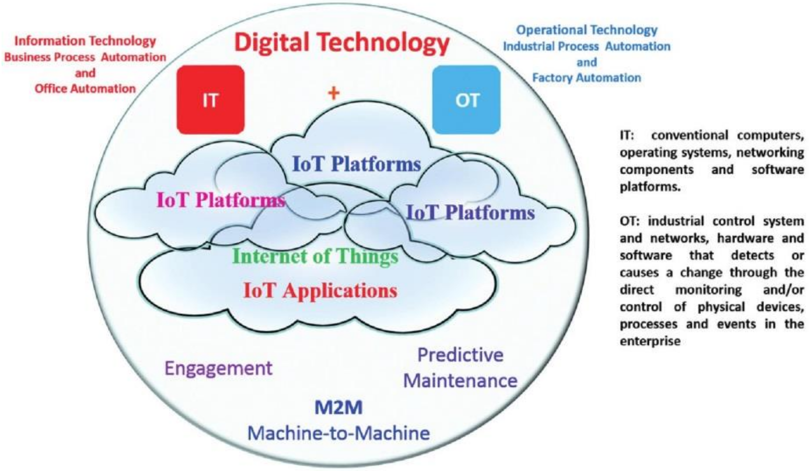


Fig. 12 - Logical model with conceptual domains for smart grid information networks

Internet of Things - a concept of integrated IT and OT (Fig. 13), automated control system for bilateral flows of electric power and data between power plants and all consumers in real time. Smart Grid using new technologies cyber – physical, forms and methods of "knowledge" energy systems to dramatically improve the efficiency of its operation.



IT: conventional computers, operating systems, networking components and software platforms.

OT: industrial control system and networks, hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise

Fig. 13 - Concept of integrated IT and OT in the Internet of Things

Power and information flow under smart grid are used for management and cyber physical flow (Fig. 14).

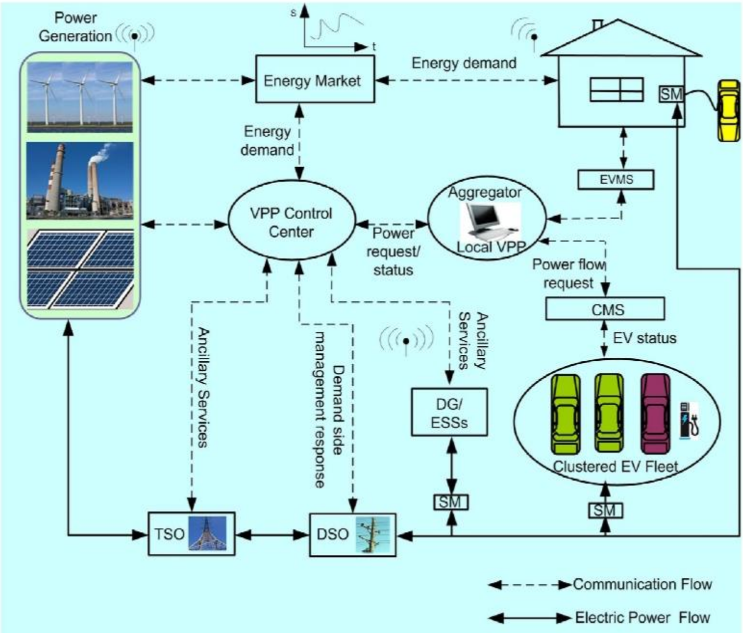


Fig. 14 - Management by the flows in under smart grid

All flows in the smart grid are shown in detail in Fig. 15.

Paradigm the Internet of Things. The Internet of Things (IoT) is a paradigm that is included in the Internet of the Future. Internet of Thing can be viewed simultaneously both as an environment in which smart grids are integrated, and as a key component of the same smart grid.

The determinations of Internet Things - a network from physical objects, to that it is possible to get access for help the Internet and that contains built-in technologies that are cooperating with their internal state or environment.

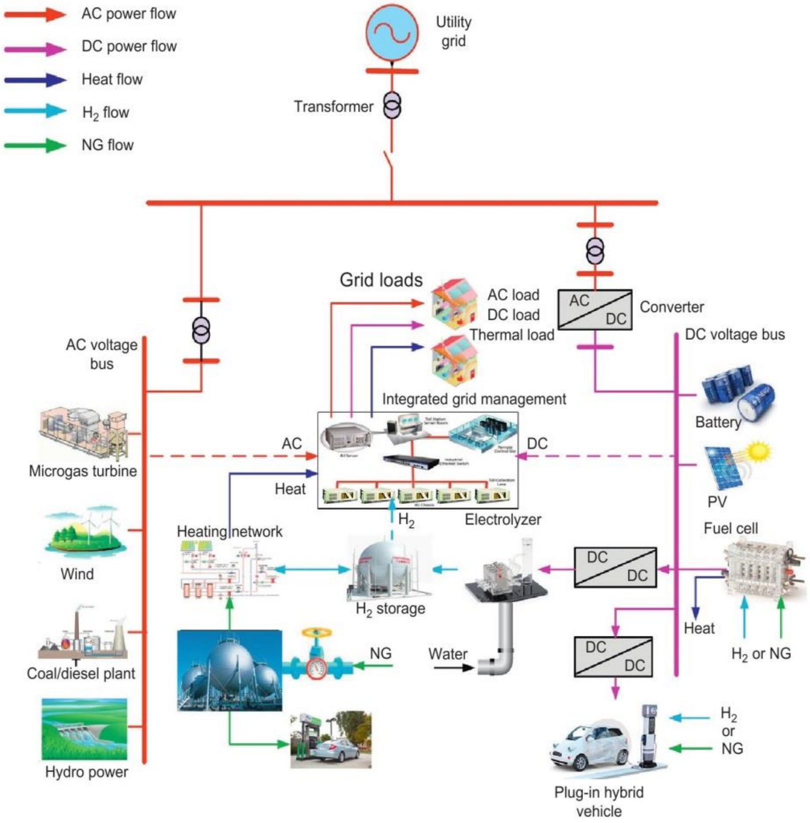


Fig. 15 - Flows in smart grid

In SG, the IoT has several potential benefits in various applications, such as smart homes, smart cities, smart security etc.

2. An example to use of IoT in Smart Grid

The fundamental principle of IoT is to offer users seamless interoperability, advanced connectivity between machines, humans, services, disparate networks, and in particular control systems for enabling real-time transfers of knowledge among organizations and inside organizations. Thus, the use of IoT in SG enables making intelligent systems, management decision support systems, and predictive diagnostic systems in order to increase the power generation capacity and thus result in significant financial benefits. In SG, the numerous components of IoT architecture comprise of radio frequency identification, sensors, actuators, context-aware computing, cloud technologies and various wired and wireless communication technologies for intensive interconnectivity. These objects through a uniquely assigned address scheme can interact and cooperate autonomously with other traditional devices like tablets, smartphones, personal computers, etc., using web services over the internet for the purpose of collecting and exchanging data in the digital world (Fig. 16).

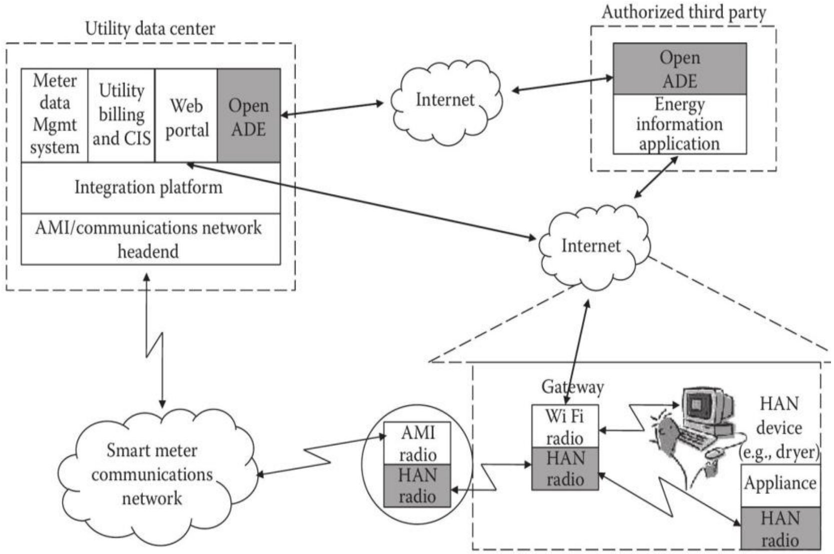


Fig. 16 - Internets of Things in the Smart Grid

The first step of integration in this direction is applying the intelligent measuring equipment (Smart Meters) which are growing tremendously. According to the norms of EU 2020, the intelligent meters must serve an 80 % energy consumption in Europe.

Smart meters. Smart meters and micro-grid are the most important components that have been incorporated in the smart grid architecture. Smart metering is one of the most emerging technologies used in smart grid to obtain information about customers' real-time energy consumption. It is also capable of controlling the advanced metering infrastructure (AMI) systems. AMI is supported with bidirectional communication mechanism to obtain real-time energy consumption at the customers' ends remotely. A smart meter is a device deployed at the distribution-end, and capable of recording the energy consumption by the customers. Customers and utilities are benefited with smart metering infrastructure. For example, a customer can estimate his energy consumption during the whole day for cost-optimization, and utility is able to maintain real-time monitoring for the supply-demand curve.

A smart metering communication system consists of the following components:

– **smart meter** which is a two-way communicating device that measures energy consuming at the appliances (electricity, gas, water or heat);

– **home Area Network (HAN)** which is an information and communication network formed by appliances and devices within a home to support different distributed applications (e.g. smart metering and energy management in the consumer premises);

– **neighborhood Area Network (NAN)** that collects data from multiple HANs and deliver the data to a data concentrator;

– **wide Area Network (WAN)** which is the data transport network that carries metering data to central control centers;

– **gateway** which is the device that collects or measures energy usage information from the HAN members (and of the home as a whole) and transmits this data to interested parties.

A Table 3 indicates the typical communication requirements and the potential technologies that could be employed to implement the different types of network mentioned above.

Table 3 - Communication requirements and capabilities of the different types of networks

Type of Network	Range	Data Rate Requirements	Potential Technologies
HAN	Tens of meters	Application dependent but generally low bit rate control information	ZigBee, Wi-Fi, Ethernet, PLC
NAN	Hundreds of meters	Depends on node density in the network (e.g. 2Kbps in the case of 500 meters sending 60 byte metering data every 2 minutes per NAN)	ZigBee, Wi-Fi, PLC, cellular
WAN	Tens of kilometers	High capability device such as a high speed router/switch (a few hundred Mbps to a few Gbps)	Ethernet, microwave, WiMax, 3G/LTE, fibre optic links

Fig. 17 shows a typical smart metering architecture, considered, just an example, in the European standards development process. At the most basic level, the home will be equipped with a series of smart meters, one each for electricity, gas, water and heat (if applicable), according to the facilities available at each home. These will be connected to a metering gateway in the home, which may or may not be part of an existing home gateway device. The HAN through which they communicate with the metering gateway may be multi-standard. This is mainly due to differing meter locations and power availability; for example, gas and water meters may have to use only battery power. Multiple HANs are further connected into a NAN via a wireless mesh network.

Smart meters are solid-state programmable devices that perform main functions:

– time-based pricing;

– consumption data for consumer and utility;

– net metering;

– loss of power (and restoration) notification;

– remote turn on / turn off operations;

– load limiting for “bad pay” or demand response purposes;

– energy prepayment;

– power quality monitoring;
– tamper and energy theft detection.
– communications with other intelligent devices in the home.

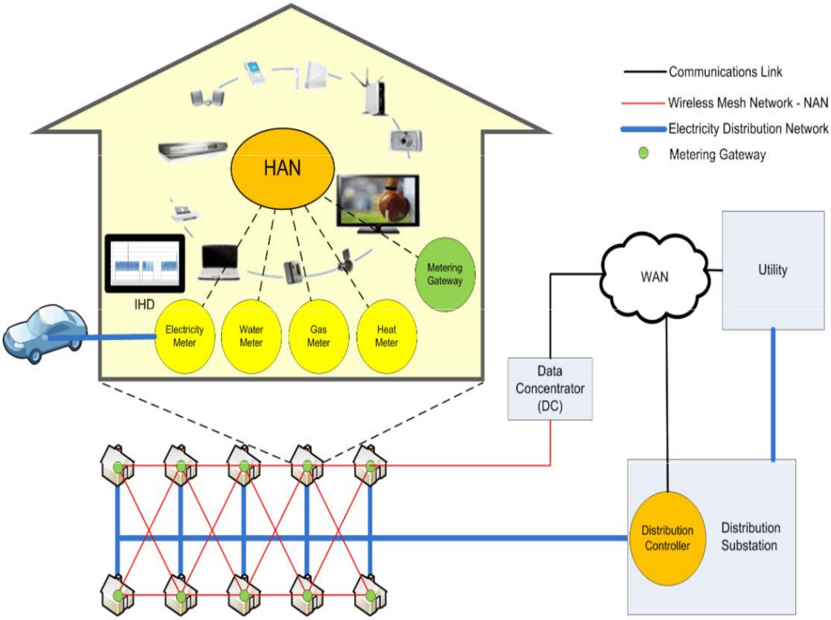


Fig. 17 - Typical smart metering architecture

Additionally, they can control and distribute electricity to the end-users (micro-grids). In the presence of an intrusion in the entire system, a micro-grid acts in the islanding mode. In such a situation, a micro-grid is able to control the power flow autonomously (Fig. 18).

Strengthening of integration of Smart Grid and systems of domestic automation (smart house) is show in fig. 19.

Model of the smart grid within the IoT context, smart home appliances, renewable energy resources, substation devices and workforce tools will be assigned IPV6 address have Smart home appliances.

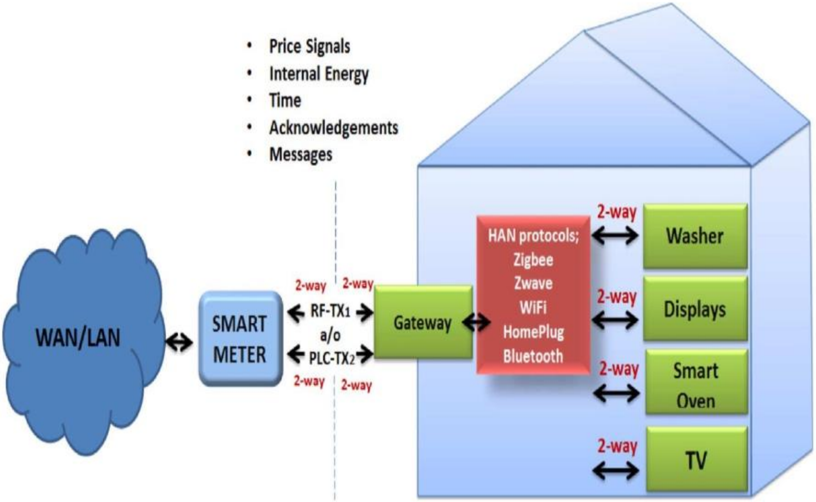


Fig. 18 - Communications smart meters with intelligent devices at home

Recent smart homes are equipped with smart appliances and each appliance is considered as a thing (object).

These things can be an air-conditioner, water-heater, dishwasher, refrigerator, smart energy/gas/water meters, in-home-display, automated lights, solar energy cell, wind mill, electrical rechargeable vehicle, and storage battery.

Monitoring of SG indicators is shown in fig. 20.

Test questions

In order to better understand and assimilate the educational material that is presented in this training, we invite readers to answer the following questions:

1. What is the long and short term of managing the PS on decision-making time?
2. Please give a definition of a Model for SG operating
3. What is a concept of IoT?
4. Please determine a paradigm of the Internet of Things (IoT)
5. What does mean an integration of IoT and the Smart Grid?
6. Please give a definition of Smart Meter

7. How do smart meters communicate with intelligent devices at smart home?

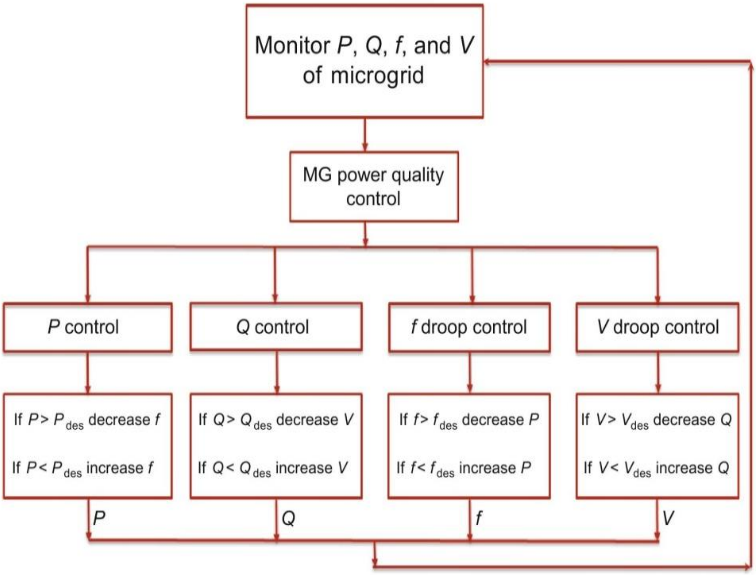

Monitor P, Q, f, and V of microgrid
MG power quality control
P control
Q control
f droop control
V droop control
If $P > P_{des}$ decrease f
If $P < P_{des}$ increase f
If $Q > Q_{des}$ decrease V
If $Q < Q_{des}$ increase V
If $f > f_{des}$ decrease P
If $f < f_{des}$ increase P
If $V > V_{des}$ decrease Q
If $V < V_{des}$ increase Q
P
Q
f
V

Fig. 19 - Monitoring of SG indicators

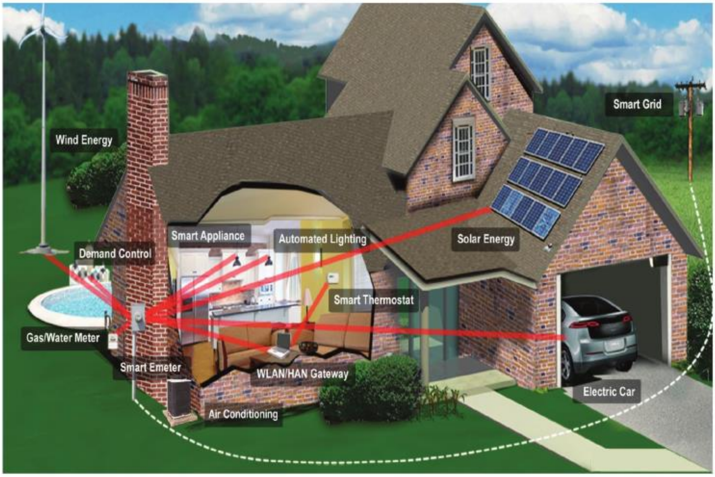


Fig. 20 - Smart grid connectivity enabling smart home services

Recommended literature

1. Kuzlu M., Pipattanasomporn M., Rahman S. (2014) Communication network requirements for major smart grid applications in HAN, NAN and WAN. Computer Networks, 67, 2014, pp. 74-88.

2. International Energy Agency. Distributed generation in liberalized electricity markets 2002.

3. A. Bose. Smart transmission grid applications and their supporting infrastructure. IEEE Trans. Smart Grid, 1 (1), pp.11–19, 2010.

4. European Smart Grids Technology Platform. Vision and strategy for Europe's electricity networks of the future, http://www.smartgrids.eu/documents/vision.pdf. 2006.

5. Al-Ali, A.R. and Aburukba, R. (2015) Role of Internet of Things in the Smart Grid Technology Journal of Computer and Communications, 3, 229-233. http://dx.doi.org/10.4236/jcc.2015.35029.

6. D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.) (2010). The Internet of Things, Springer, 2010.

TRAINING 3.
CLOUD COMPUTING AND BIG DATA AS A PART OF THE IOT SMART GRID

The aim of the training: to learn for implementing the Cloud computing and Big Data in the smart grid.

Learning Objectives:

1. Studying a conceptual model of Cloud computing.
2. Study for integrating the Cloud computing and Big Data into the Smart Grid environment.
3. Studying the methods used in trainings and their implementation.

Practical tasks: explore the possibilities of using the different types of Cloud computing and Big Data in smart grid.

Preparation for the training needs:

1. Get the topic of the analytical review and clarify the conditions of the task.
2. To develop a work plan and distribute a responsibility between group members (students arrange among themselves parts of the work for which they will report).

Training implementation

During the training needs:

1. Search information of the training topic and the received task.
2. Perform the necessary actions to complete the received task.
3. Get the results needs to complete the task.
4. Develop a plan of the report and presentation, which illustrate the implementation of the received task.
5. Write a report.
6. Prepare a presentation.

Defend training results

1. Presenting and defending the report of the task results.
2. Evaluation of work.

Theoretical information

Processes in the integrated smart grid system on cloud

The heterogeneous architecture of smart grids, demand response (DR), and micro-grids are the main building blocks in the smart grid architecture. The grid topology needs to adapt and shift from a centralized source to a distributed topology that can absorb different energy sources in a dynamic way.

The purpose of this part is to establish requirements for building intelligent (smart) processes of the integrated smart grid system and to develop a conceptual model of a prospective vision of the intelligent energy system based on cloud computing and big data.

Complex of system resources and services that provide support of organization of control system and realized as a platform. Setting of standard architecture provide the implementation of the most progressive methods IoT and cloud computing.

The smart grid infrastructure needs to be deployed globally. Scalable platform is needed in order to rapidly integrate and analyze information streaming from multiple smart meters simultaneously, in order to balance the real-time demand and supply curves.

Advocated that cloud platforms are well suited to support such huge data and computationally-intensive, always-on applications. In such applications, cloud offers advantages of scalable and elastic resources to build a software infrastructure to support such dynamic and always-on applications. In these environments, the cloud platform is running as intrinsic components due to the following diverse benefits:

1) Cloud acts elastically to avoid costly capital investment by the utility during the peak hours.

2) Real-time energy usage and pricing information can be shared, so that the customers can get benefited from the real-time information.

3) Some data can be shared with a third party by using cloud services, after meeting the data privacy policies for developing intelligent applications to customize consumer needs.

Cloud-based software platform for smart grids

The cloud “promises high reliability, scalability and autonomy” for the next framework can be considered as “cloud based”. The Cloud platform is used in the multi-level smart grid (Fig. 21).

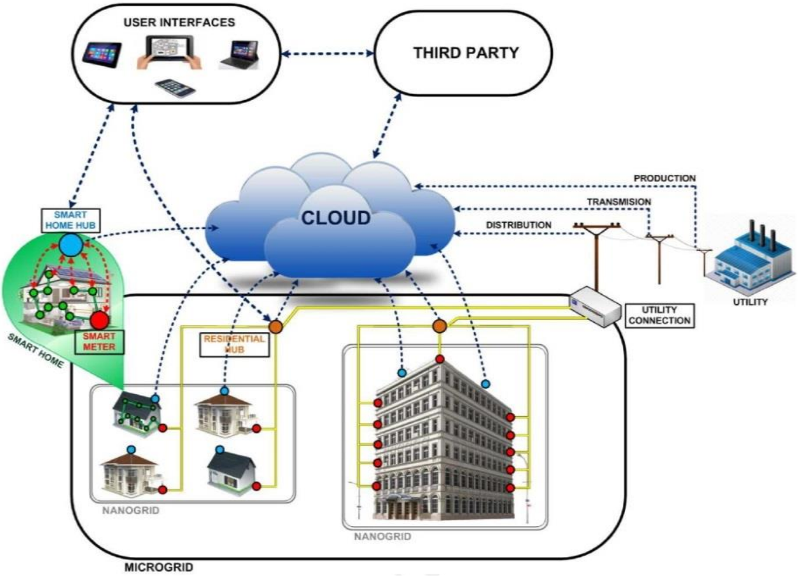


Fig. 21 - Cloud in the multi-level smart grid

Demand Response (DR) – a mechanism by which the customers can actively participate in balancing the supply and demand curves. In the presence of demand response mechanism, customers can schedule their appliances during off-peak hours to minimize the energy consumption cost, which in turn minimizes the load on the micro-grids during on-peak hours. Customers can take adequate decision while they have grid, storage, and self-generated energy as well to minimize the energy cost with the help of demand response mechanism. On the other hand, virtual energy storage is also one of the useful techniques for reliable energy supply. In the presence of virtual energy storage platform, the micro-grids can store their excess energy, while other micro-grids can consume the storage energy to fulfill their customers' demand.

Peak loads may be caused by a drop in the supply from renewable generation or an increase in the demand due to, say, a heat-wave in a region. Current grid technology limits DR to static strategies, such as time-of-use pricing and day-ahead notification based on historical averages. However, SG infrastructure offers instantaneous communication capability between the utility and the customer, and automated controls at residences and buildings that enables using the dynamic demand response optimization (D^2R) for near real-time detection, notification and response.

D^2R software platform on Clouds

The two key ingredients for successful and agile D^2R operations are demand forecasting and curtailment strategy selection. In a data-rich Smart Grid, these decisions are guided by data analytics and mining that must scale with the number of buildings and customers, and the temporal granularity of decision-making. Further, the research aspects of our project requires that we learn more from the operational impact of D^2R and offer techniques for diverse conditions.

Fig. 22 shows the lifecycle of D^2R operations within micro-grid and components of software platform that support it. Most of these components, shown with a blue cloud backdrop, are hosted on Clouds. We also can use different flavors of Clouds, including public and private Clouds, as also Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). The choice of the Cloud flavor for each component is based on their specific needs, which include elastic resource acquisition, platform manageability, data reliability, and scalable programming abstractions.

The software platform can be seamlessly layered on top the hybrid Cloud infrastructure and cluster. Next, we will review the architecture of the platform and life cycle D^2R.

First, data has to be acquired from thousands of equipment sensors and smart meters in buildings through the energy control system. These include instantaneous data sampled and streamed periodically, as well as historical data aggregated over several years that need to be bulk-loaded. Behavioral research and end-use analysis require not just sensor data but also the context for energy use.

Automated data cause using the pipeline which has to support dynamic data acquisition at variables rates and volumes, and be adaptive to current data sources and operational needs.

Data acquired by the pipeline has to be stored and shared with different D^2R applications. These applications vary from operational analytics for initiating D^2R curtailment strategies, to researchers mining and exploring data for correlations, to consumers visualizing and gaining knowledge on their energy profile.

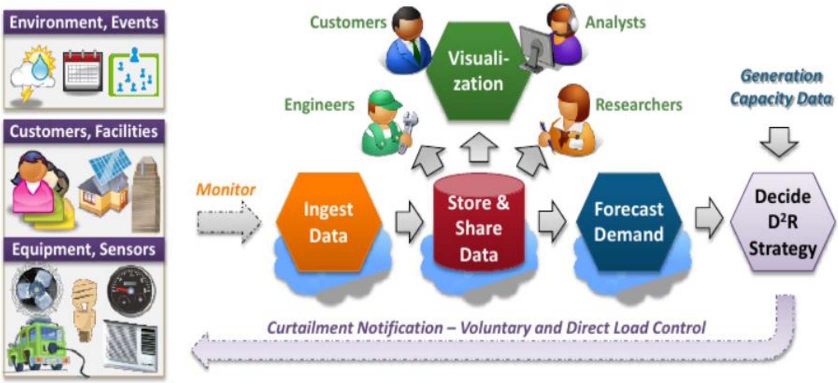


Fig. 22 - D^{2}R lifecycle in micro-grid on a base of Cloud-based software platform

Data-driven forecasting models are essential for D^{2}R, and there are two key classes of these. Demand forecasting models predict the energy consumed (in KWh) at different spatial and temporal granularities. Curtailment forecasting models offer predictions on potential energy reduction (negative KWh).

2. Example of using the Cloud computing as operation platform for IoT in smart grid systems

The operation platforms for IoT in SG systems include cloud computing, fog computing and big data. Cloud computing – a model that enables convenient, ubiquitous, on-demand access to a pool of computing resources (e.g. servers, networks, applications, storage, and services) that are configurable. Using a cloud infrastructure, a customer can gain an access to their applications anytime, from anywhere, through a connected device to the network. Let us consider integrating cloud computing applications in smart grids, in aspect of energy management. Communications networks of the smart meters in the Cloud computing is shown in Fig. 23.

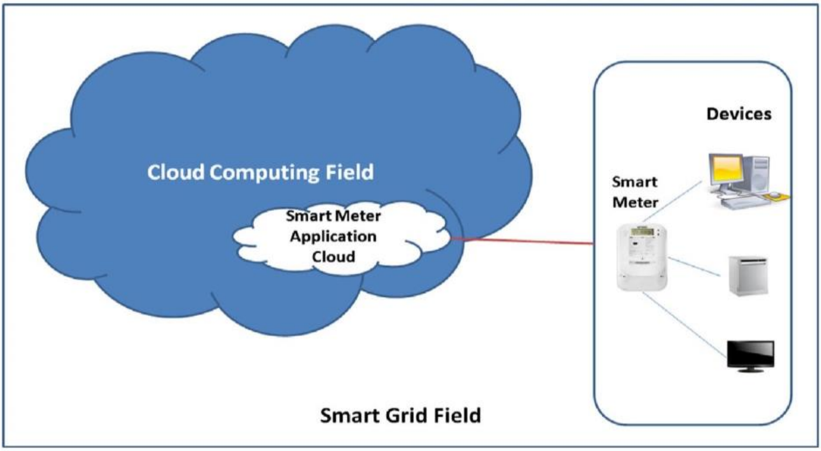


Fig. 23 - Communications networks of smart meters in Cloud computing

It delivers infrastructure, platform, and software to customers as subscription-based services in a pay-as-you-go model. The advantages of using the cloud computing model are as follows:

– **On-demand self-service**: A consumer can individually provision computing capabilities as needed automatically without requiring human interaction with each service provider.

– **Broad network access**: Capabilities are available over the network. It can be accessed through standard mechanisms, to be used by heterogeneous thin or thick client platforms.

– **Resource pooling**: A multi-tenant model is used to serve multiple consumers from a pool of computing resources. The customer has no control over the exact location of the provided resources.

– **Rapid elasticity**: Cloud computing supports elastic nature of storage and memory devices. It can expand and reduce itself according to the demand from the users, as needed.

– **Measured service**: Cloud computing offers metering infrastructure to customers. Cost optimization mechanisms are offered to users, enabling them to provision and pay for their consumed resources only.

– **Infrastructure-as a Service**: IaaS provides scalable infrastructure e.g. servers, network devices, and storage disks to consumers as services on demand. The access to the cloud is provided through various user interfaces, such as web service application programming interface (API), command-line interfaces (CLI) and graphical user interfaces (GUI) which provide different level of abstraction..

– **Platform as a Service**: PaaS provides a platform where users or customers can create and run their applications or programs. The users can build and deliver Web-applications without downloading and installing required software, as PaaS service completes the requirements. The most important customers for this layer are the developers

– **Software-as a Service**: SaaS is responsible for delivering various kinds of applications plus the interfaces for the end users The SaaS provides the modeling of software deployment where users can run their applications without installing software on his/her own computer.

According to the deployment model, a cloud can be classified as public cloud, private cloud, community cloud, and hybrid cloud.

The advantages of using the cloud computing model are following (Fig. 24):

– Elastic Nature: Cloud computing supports elastic nature of storage and memory devices. It can expand and reduce itself according to the demand from the users, as needed.

– Shared Architecture: Cloud computing also supports shared architecture. Information can be shared among the users after meeting the privacy issues, and, thereby, reducing service costs.

– Metering architecture: Cloud computing offers metering infrastructure to customers. In the metering system, cost optimization mechanisms are offered to users, enabling them to provision and pay for their consumed resources only.

In fig. 25 (a), a conceptual view of the conventional smart grid (without cloud) is shown, where customers are serviced by micro-grids. A micro-grid has some self-generation unit such as solar, and wind generation.

All the different components (substations, micro-grids, and customers) can communicate with utility providers over the communication network. The integration of cloud applications in the smart grid architecture is shown in Figure 25 (b). The cloud applications can be served as the virtual energy storage and data storage devices. In such a scenario, smart grid components communicate with the cloud instead of doing so with one another directly, and taking necessary decisions for energy management.

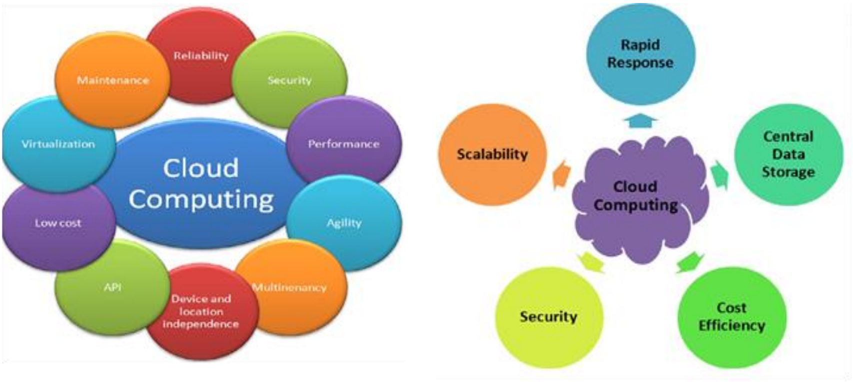


Fig. 24 - Advantages of using a cloud computing model for smart grid

Big Data in smart grid systems - the integration of IoT technology with SG comes with a cost of managing the huge volumes of data, with a frequent processing and storage. Such data includes consumers load demand, energy consumption, network components status, power lines faults, advanced metering records, outage management records and forecast conditions. This means that the utility companies must have hardware and software capabilities to store, manage and process the collected data from IoT devices efficiently and effectively.

Big Data is defined as data with huge volume, variety and velocity (three V’s). The high frequency of data collection by IoT devices in SG makes the data size as very large one. The variety is represented by the different sensors that produce different data. The data velocity represents the required speed for the data collection and processing. Hence, IoT-aided SG systems can apply the techniques of big data management and processing.

In SG, the SCADA system is the main element of decision-making. It collects data from IoT devices that are distributed over the grid and provides real-time online monitoring and controlling. Additionally, it helps to manage the power flow throughout the network in order to achieve consumption efficiency and power supply reliability.

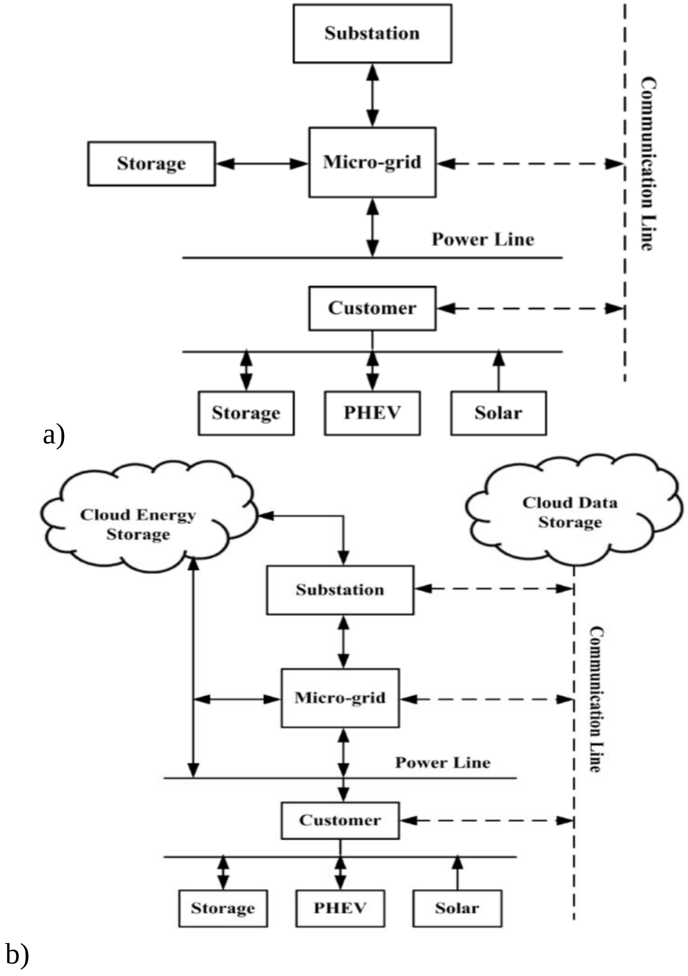


Fig. 25 - A smart grid without (a) and with (b) cloud application

IoT- aided SG systems involve processing data that requires Big Data techniques (Fig. 26). The techniques for big data processing include Map Reduce and stream processing. Map Reduce is suitable for static and non-real time applications and it analyzes large historical data. It splits big data sets into smaller data sets and processes these smaller data sets concurrently on multiple machines. Stream processing is suitable for both real and non-real time applications and is ideal for sensors and big data streams. It is fault tolerant, and it has a great potential for big data management in IoT-aided SG systems.

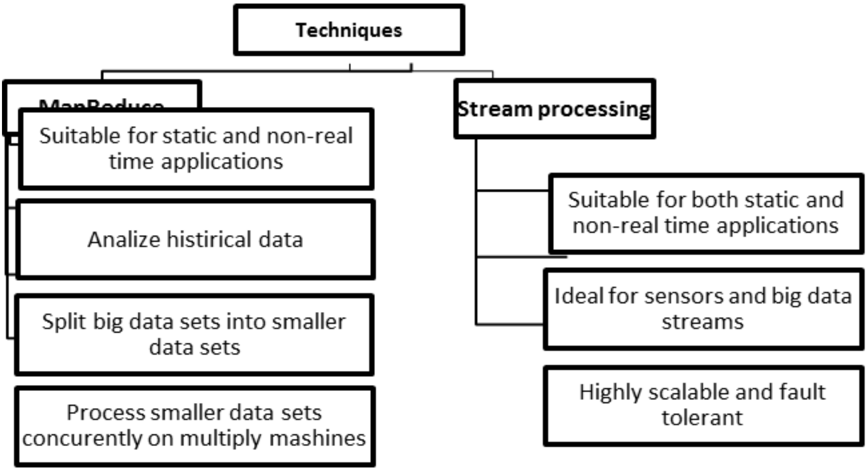

Techniques
MapReduce
Suitable for static and non-real time applications
Analize histirical data
Split big data sets into smaller data sets
Process smaller data sets concurently on multiply mashines
Stream processing
Suitable for both static and non-real time applications
Ideal for sensors and big data streams
Highly scalable and fault tolerant

Fig. 26 - Big Data techniques for SG

Concept of Cloud-Based Demand Response (CDR) proposed for fast response times in large scale deployment. In this architecture, the master/slave demand response model is proposed, in which the smart meters and the home EMS act as slaves, and the utility acts as the master. In such a scenario, the CDR leverages data-centric communication, publisher/subscriber and topic-based group management, instead of IP-centric communication.

Solution Concept with Cloud Applications. For several years, researchers proposed several solution concepts for demand response and micro-grid management

Two cloud-based demand response models are proposed as follows: (a) data-centric communication and (b) topic-based group communication. Secure, scalable and reliable demand response can be achieved by using the CDR approach. However, the demand-response model discussed in has an overhead problem with the implementation of private cloud for a small-sized network. Some of the overhead problems are the implementation cost, and the selection of appropriate strategy. Even for a small-sized network, all the features of cloud computing platform should be supported in order to have reliable, and secure electricity distribution in a smart grid, and, thus, implementation cost of cloud applications is higher than the existing methods for a small-sized network.

Therefore, there is a need for developing such a demand-response model using cloud-based applications that will facilitate both the large and small-scale network.

Energy management can also be addressed with the implementation of dynamic pricing have two smart grid related issues: (a) peak demand and (b) dynamic pricing. With the integration of cloud, the incoming jobs are scheduled to be executed according to the available resources, job priority, and other applicable constraints. During peak hours, the messages from smart meters are more than those in the non-peak hours. However, in such a scenario, incoming jobs from users are scheduled according to their priority, available resources, and applicable constraints. With the integration of dynamic bandwidth allotment mechanism using cloud application, these issues can be addressed conveniently. During the peak-hour, the allotted bandwidth is higher than that in the non-peak hour, to serve all the incoming jobs simultaneously.

Cloud computing can be implemented in the form of different strategies of the micro-grids.

These are then run on local workstations or remote cyber-infrastructure using workflow engines that orchestrate the task execution and data exchanges between them. Despite their growing popularity and ease of use, existing workflow engines have limited support for processing continuous data streams with the same flexibility and efficiency as processing files. Support for both bulk data files and dynamic streaming data, which scales to thousands of sensor streams with low latency processing, is essential for composing data acquisition pipelines for the SG CPS. Further, these pipelines when running in an operational setting are in an “always on” mode. Hence any change to the pipeline’s composition has to done in-place, without loss of in-flight data. This form of application dynamism is, again, not considered by contemporary workflow systems.

Smart grid data management based on cloud computing

The smart grid consists of bidirectional electrical as well as communication flows, primarily enabled with the help of advanced sensor network technology. The smart meters are also deployed at the customers’ end to communicate with the service provider. Due to this architecture, massive data are generated from both the utility and end-users sides. The management of vast amount of such data is challenging using the traditional data management approaches due to the different constraints (such as processing unit storage, and memory). Consequently, cloud computing applications are one of the best methods to control such vast data in order to have a reliable, robust, and efficient smart grid environment.

In a typical city environment, millions of smart meters are deployed at the distribution side. To successfully handle such massive data, a useful technique is required.

Cloud computing is such a useful technology for smart grid information management due to the following reasons:

– The requirements of information processing in smart grid fit well with the computing and storage mechanisms available for cloud applications.

– In a smart grid, information sharing is one of the most important issues.

– Shared information is accessible to the micro-grids, end-users, and utilities, though they function in the islanded mode.

– Management of massive data is complex, costly, and may be beyond the capacity of existing data management systems in the smart grid.

For data management in smart grid can be used a cloud data warehouse application (fig. 27). This cloud data warehouse architecture provides different services for smart grid information management such as multi-dimensional data analysis, and data mining.

Test questions

1. What operation platforms are used in cloud computing for IoT?
2. What does the D2R software platform mean applying to SG?
3. What cloud services are used in smart grids?
4. What are the prospects of using a cloud computing in the area of IoT smart grid?
5. Please, give a definition of Big Data.
6. Please, give an example and explain some Big Data technique for SG.

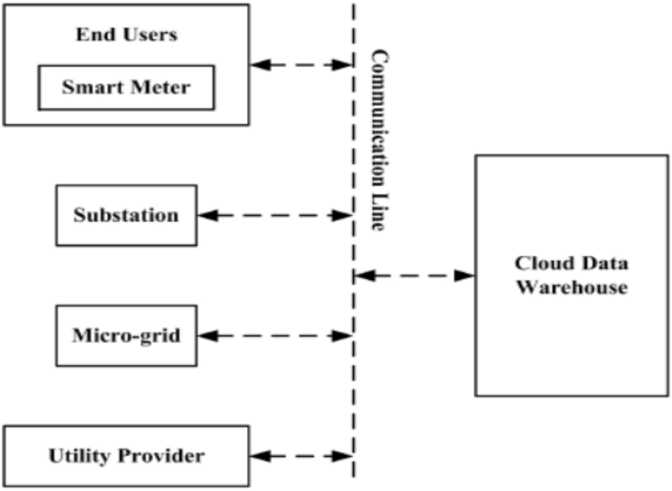


Fig. 27 - A smart grid communication with cloud data-warehouse

Recommended literature

1. Naveen P., Ing W.K., Danquah M.K., Sidhu A., Abu-Siada, A. (2016) Cloud computing for energy management in smart grid – an application survey. CUTSE2015. IOP Conf. Series: Materials Science and Engineering 121.

2. Al-Ali, A.R. and Aburukba, R. (2015) Role of Internet of Things in the Smart Grid Technology. Journal of Computer and Communications, issue 3, pp.229-233.

3. Bera S., Misra S., Rodrigues J. P. C. (2013) Cloud Computing Applications for Smart Grid: A Survey. DOI 10.1109/TPDS.2014.2321378.

4. H. Kim, Y. Kim, K. Yang, and M. Thottan, (2011) Cloud-based demand response for smart grid: Architecture and distributed algorithm," in Second IEEE International Conference on Smart Grid Communications.

ITM1.2. IoT infrastructure for smart energy grid based on embedded systems devices

**Prof., DrS. M. P. Musiyenko, Ass. Prof.,
Dr. I. M. Zhuravska, Dr. Y. M. Krainyk (PMBSNU)**

Seminar 1

I&C, AND HARVESTING SYSTEMS: ARCHITECTURE AND DEVISING METHODS

The aim of the seminar: to receive knowledge and practical skills in local Smart Energy Grid (SEG) based on Internet of Things (IoT) infrastructure field and particularly topics concerned with I&C, and harvesting systems, their architectures and devising methods for this purpose.

Preparation to seminar:

1. Receiving research topic.
2. Negotiation of the plan.
3. Information search.
4. Presentation preparation.

Questionnaire for seminar:

1. Three-layer architecture of SEG.
2. Details on perception layer in SEG.
3. Prosumers and their influence on SEG architecture.
4. IoT-components for local SEG segment.
5. Communication protocols for components of IoT-enhanced SEG.
6. Notion of smart energy metering.
7. Communication technologies for smart energy meters.
8. IEEE 1901 standard and its application for energy metering.
9. Five-layer architecture of SEG.
10. Wireless communication technologies for IoT in local SEG.
11. Single-board computers as control device for local SEG.
12. Wireless modules ESP8266 for local SEG.
13. Software platforms for ESP8266.
14. Advantages of NodeMCU software for ESP8266.
15. Smart devices in local SEG.

16. Role of microcontrollers in sensor measurements.
17. Interaction between microcontroller and Wi-Fi-module for sensor processing and measurements accumulations.
18. Consumption of IoT-components for local SEG.
19. Brief overview of security topics for local SEG.
20. PLC-technology for local SEG.
21. Equipment that supports PLC-communications.
22. Models of energy harvesting systems for local SEG.
23. Information flow in local SEG environment.
24. Control actions for local SEG.
25. Methods for energy harvesting in local SEG.
26. Minimal function set for control device in local SEG.
27. Network topology for local SEG.
28. Communications based on different network technologies in local SEG.
29. Peculiarities of sensor measurements gathering in local SEG.
30. Additional smart equipment for local SEG.

Theoretical issues for “IoT for Smart Energy Grid” are described in Part IX (sections 32-35) of the book [Internet of Things for Industry and Human Application, vol. 3. Assessment and Implementation, V. S. Kharchenko, Ed. Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

Work defense.

Work defense takes place during the seminar and should be 10 minutes long with 7 minutes for presentation (oral presentation with slides) and 3 minutes for question and answer session.

Assessment.

During the assessment process, the following factors are taken into consideration:

– quality of material;
– compliance with research topic;
– number of reviewed scientific sources;
– originality of compiled materials;
– presentation quality.

Each work is assessed individually according to the specified criteria. Special emphasis should be made on peculiarities of local SEG part and implications that it causes for models, architectures, devices, etc. The report materials should reference at least 20 external sources (scientific papers, web-documents, official reports, etc.).

Report requirements.

The report have to comply with traditional structure:

1. Topic
2. Relevance of the topic in context of current technology state.
3. Main tasks of investigation.
4. Brief overview of cited sources.
5. Main part with detailed presentation of synthesized materials.
6. Outlooks and future implementations.
7. Conclusions.
8. Cited sources.

Test questions:

1. List necessary components of local SEG architecture.
2. What are the security issues concerned with smart meters?
3. List communication technologies used in local SEG.
4. Explain connection approaches for sensor nodes in local SEG.

References for seminar preparation.

1. S. Salinas, M. Li, P. Li, and Y. Fu, "Dynamic Energy Management for the Smart Grid With Distributed Energy Resources," in IEEE Transactions on Smart Grid, vol. 4, no. 4, 2013, pp. 2139-2151. DOI: 10.1109/tsg.2013.2265556.

2. M. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 3, no. 1, 2016, pp. 70-95.

3. F. Hussain, Internet of Things: Building Blocks and Business Models. Cham: Springer, 2017.

4. R. Moghaddass and J. Wang, "A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data," in IEEE Transactions on Smart Grid, vol. 9, no. 6, 2018, pp. 5820-5830. DOI: 10.1109/tsg.2017.2697440.

5. B. P. Roberts and C. Sandberg, "The Role of Energy Storage in Development of Smart Grids," in Proceedings of the IEEE, vol. 99, iss. 6, 2011, pp. 1139-1144. DOI: 10.1109/JPROC.2011.2116752.

Training 1

ENERGY MEASUREMENT SYSTEMS USING PLC-TECHNOLOGY (IEEE 1901)

The aim of the training: investigation of PLC-technology, its general features and peculiarities in context of local Smart Grid based on IoT solutions. Data transmission mechanisms and practical usage for organization of local Smart Grid infrastructure are considered in this practical part.

Learning tasks:

– understanding of PLC technology and its role in IoT-applications;

– knowledge of IEEE 1901 standard that allows transmitting measurement data over existing electrical infrastructure.

Practical tasks:

– organization of PLC-network;

– integration existing WiFi-network with PLC-enabled equipment;

– receiving data from smart meters using existing electrical infrastructure;

– monitoring of energy consumption with smart meters.

Theoretical information

Set of PLC-adapters with PLC-gateway are used in the process of this practicum. WiFi-network must be deployed to provide transmission from the gateway into WLAN domain. Appropriate quantity of RJ-45 cables is an obligatory to execute tasks. Electricity meter (e.g. NIK2104 or similar with support of PLC technology) with support of PLC technology is also an obligatory. It is recommended to follow severe precautions for installation of electricity meter. It should be performed only by qualified specialist. It is also recommended that all equipment for the work should be organized as fully connected testbed. Students are responsible for organization of logical communications among installed devices. Additional devices used as a load for the electrical network with included metering device (e.g. laptops) might be brought by students or laboratory equipment can be used for the purpose. Dedicated electrical sockets must be available on the testbed.

Survey on Smart Energy Metering and Power Line Communications.

Smart Energy Meters (SEM) have become ubiquitous equipment for Smart Energy Grid [1-3]. In comparison with their predecessors, SEM provide novel functions to grid participants. From the customer's point of view, it provides information about consumption and using that information customer can optimize consumption plan and pay less for energy resources. From the point of view of distributors' side, SEM allow retrieving information about consumption from all customers in the dynamic mode and adjust generation of energy for balancing resources in the network. They also can be used effectively for learning customers' behavior and prediction for resource generation and consumption, complex dynamic payment plans composition, etc. These advanced or "smart" features would be impossible to implement without smart meters.

Peak period of SEM installation starts from 2010. More than 100 million devices was to be installed in European region by 2016 [2]. But the pace of installation is even higher now and statistics states about 200 million SEM installed in European Union [4]. However, the process of substitution previous generation of meters by smart meters is still going on. It is expected that SEM will be used in every building and it is going to be one of the important steps for SEG implementation roadmap.

Considering functionality of SEM, it can be stated that the main difference from previous generation of meters is that they can send short messages to the energy providers and customers. Therefore, changes are relatively small. However, these small changes has a huge outcome as they allow reducing payments for customer and make energy consumption more frugal. You can distinguish SEM by presence of Liquid Crystal Display (LCD) as illustrated in Fig. 28 [2]. Meters without smart functions have other means for informing users (mechanical in most cases).

Although, customer always can check current measurements personally on the meter's display, there are also solutions that allow receive these data and show them on separate device. It typically has color display and responsible for visualization of measurement data.

SEM in most cases support different tariffs. The most common is presence of day and night tariffs. However, they can be more complicated and provide more possibilities of configuration and regulation of power consumption.

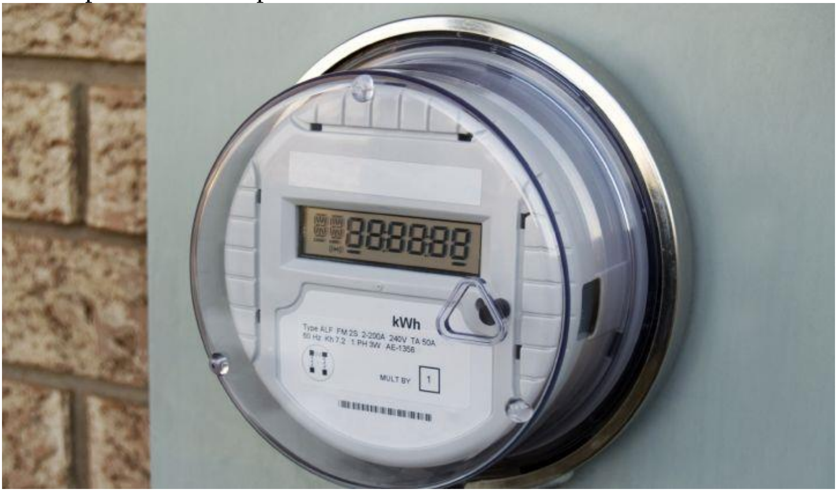


Fig. 28 – Design of modern smart meters

Smart meter is designed to send information to participants of SEG. However, this functionality should not be implemented at the expense of higher power consumption from the meter itself. It can erase advantages from this feature if power consumption rises notably. This is the reason why SEM transfers small chunks of data in relatively large interval window.

Great concerns [5-7] rise because SEM send information to the supplier automatically and customers have to deal with it. The main concerns are connected with security and privacy questions. Critics of SEM allege that based on information sent from meters hackers can indirectly extract information about customer’s behavior patterns, presence or absence inside premises, etc. This information might be further used for malicious purposes. Thus, data accumulated from customers should be strongly protected against hackers. Another reason of negative smart meters treatment is health-related problems. Some materials claims that radiation from smart meters affects customer’s health. However, as amount of information that SEM generate is relatively small in comparison to other technologies that are typically present in customer environment, contribution of SEM in this issue should be quite small.

At the customer side, SEM can transfer data over wired and wireless channel. ZigBee is a typical choice for wireless data transmission while PLC is an option for wired connection.

Combination of SEM and PLC technologies looks like essential solution for local part of SEG [8, 9]. Meters with support of PLC-transmission can send data to corresponding devices connected via PLC. In fact, any device connected to PLC-adapter can receive the data. PLC supposes usage of existing electrical wiring infrastructure for data transmission. PLC-enabled meter works with this same medium. Thus, no additional communication channels need to be installed and customer can just plug appropriate adapter into the socket and connect device that monitors data.

End devices connect to the network using PLC-adapters [10]. They can be considered as a gateway from electrical wire data communication to traditional digital interfaces. Most common solution is Ethernet connection. Adapter contains socket for connection of Ethernet cable as demonstrated in Fig. 29 [10]. As PLC throughput depends on many factors (device producer, device series, electrical equipment used in the moment, etc.), it is preferable to use cable that support maximum data rate for the present socket. For instance, if device can handle throughput up to 500 Mbit/s, there is no sense in usage CAT5 cable that provides only 100 Mbit/s. Use CAT5e cable instead.

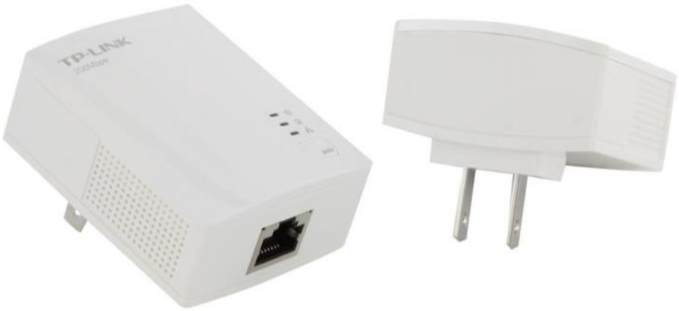


Fig. 29 – PLC-adapters

Two adapters plugged into electrical sockets automatically recognize each other and provide low-level layer for communication. Configuration of higher level depends on customer.

More advanced device type is PLC-adapter with embedded Wi-Fi [11]. The purpose of such devices is to extend WiFi-network in the local area network (LAN) and provide better network coverage. Devices of this type are recommended for practical task.

Sample workflow.

Students receive equipment and organize connection based on PLC-modules. Established connection and communications should be demonstrated to the lecturer. Next, network connectivity based on PLC-gateway should be provided. All connections must be verified by explicit data transmission among devices in the network. Additionally, check transmission speed over PLC by sending large amount of data from one network node to another. Make conclusion about relevance of measured speed and speed achieved during this testing procedure. It is obligatory during the work to use all the proposed components types to demonstrate understanding of how different technologies can be combined with each other. Additionally, it is also necessary to show data transmission from network part based on one technology to the part that is based on another technology. To observe changes in meter's measurements, some load equipment should be connected to the testbed.

Theoretical issues for "IoT for Smart Energy Grid" are described in Part IX (sections 32-35) of the book [Internet of Things for Industry and Human Application, vol. 3. Assessment and Implementation, V. S. Kharchenko, Ed. Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

Assessment.

During the assessment process, the following factors will be taken into consideration:

- successful deployment of PLC-equipment;
- ability to communicate between WiFi-part and PLC-part;
- usage of all provided parts during practicum task;
- complexity of the deployed network topology;
- general correctness of the topology;
- total time spent on task execution;
- information reception from smart meter;
- team work and cooperation among students;
- theoretical knowledge of smart metering;

– theoretical knowledge of the data transmission process in PLC-networks.

Report requirements.

Report must contain:

– scheme of the PLC-equipment connection;

– screenshots that demonstrates connection configuration at the notebook or workstation;

– screenshots that demonstrates reception of the data from smart meter (Wireshark software is the recommended environment to capture network traffic).

Test questions:

1. What does PLC stands for?
2. List equipment that is necessary to capture data from PLC-enabled smart-meter.
3. How much traffic does smart meter transmit?
4. Explain peculiarities of connection of smart meter and PLC-equipment.

Recommended literature.

1. "UK smart meters explained: The good, the bad and why you should wait" [Online]. Available: https://www.the-ambient.com/guides/smart-meters-uk-guide-418.

2. "100 Million Smart Meters to Be Installed in Europe by 2016, but Are End-Users Engaged?" [Online]. Available: https://www.greentechmedia.com/articles/read/100-million-smart-meters-to-be-installed-in-europe-by-2016-but-are-end-user#gs.2NrJpLXX.

3. "Stay on track with a smart meter" [Online]. Available: https://www.eonenergy.com/smart-meters.html.

4. "Smart Metering deployment in the European Union" [Online]. Available: https://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union.

5. "Six reasons to say no to a smart meter" [Online]. Available: https://www.telegraph.co.uk/money/consumer-affairs/six-reasons-say-no-smart-meter/.

6. S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," 2011 IEEE International Conference on Smart Grid Communications

(SmartGridComm), pp. 190-195, October 2011. DOI: 10.1109/SmartGridComm.2011.6102315.

7. M. Jawurek, M. Johns, and F. Kerschbaum, "Plug-In Privacy for Smart Metering Billing," in Privacy Enhancing Technologies Lecture Notes in Computer Science, 2011, pp. 192-210. DOI: 10.1007/978-3-642-22263-4_11.

8. S. Galli, A. Scaglione, and Z. Wang, "For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid," in Proceedings of the IEEE, vol. 99, no. 6, 2011, pp. 998–1027. DOI: 10.1109/JPROC.2011.2109670.

9. G. Artale, A. Cataliotti, V. Cosentino, D. D. Cara, R. Fiorelli, S. Guaiana, N. Panzavecchia, and G. Tinè, "A new PLC-based smart metering architecture for medium/low voltage grids: Feasibility and experimental characterization," in Measurement, vol. 129, 2018, pp. 479-488. DOI: 10.1016/j.measurement.2018.07.070.

10. "TP-LINK TL-PA2010KIT AV200 Nano Powerline Adapter Starter Kit, up to 200Mbps" [Online]. Available: https://www.newegg.com/Product/Product.aspx?Item=N82E16833704164.

11. "300 Mbps Wi-Fi HomePlug® AV500 Powerline Adapter Kit" [Online]. Available: https://www.asus.com/Networking/PL-N12-Kit/.

Training 2

IOT-CONTROL SOLUTIONS BASED ON STM32-BOARDS, ESP8266

The aim of the training: investigation of combined IoT-node comprised of microcontroller (STM32 board) and wireless module (ESP8266). The node connects to the user network. The components of the node can communicate with each other.

Learning tasks:

– introduction to development for STM32 microcontrollers using STM32CubeMX software;

– understanding networking capabilities of the complex IoT-node.

Practical tasks:

– programming microcontroller STM32;

– programming ESP8266 with NodeMCU firmware;

– estimate power consumption and measure real consumption values;

– analyze expected and received results;

– organizing intercommunications between microcontroller and wireless module.

Preliminaries.

The following software must be installed:

– STM32CubeMX [3];

– SystemWorkbench for STM32;

– ESPlorer [1, 2];

– NODEMCU Flasher;

– drivers for USB-UART-adapter (depends on the version of ESP8266 module).

All mentioned software is freeware and requires no additional fee.

STM32 development board (STM32 Nucleo 64 is assumed to be used in the example) is used during the work alongside with ESP8266 module (NodeMCU). Firmware for ESP8266 and STM32CubeMX project for STM32 board are provided. It is recommended to deploy wireless network during the work so ESP8266 can connect to it. Multimeter usage is recommended during measurement stage of the work. Acquaintance with NodeMCU platform and knowledge of Lua programming language would be an advantage. Only small subset of the language is used.

Execution of the work.

ESP8266 is supposed to have NodeMCU firmware onboard (provided).

Connect to ESP8266 via virtual COM-port that matches device. 115200 or 9600 baud rate are usual values for communication parameter.

Configure ESP8266 to connect to access point using following script.

```
station_cfg={}
station_cfg.ssid="station_name"
station_cfg.pwd="password"
station_cfg.save=true
station_cfg.auto=true
wifi.sta.config(station_cfg)
```

Substitute SSID and password values with ones for your network. Additionally, you may need to send one more instruction to connect to the network

```
wifi.setmode(wifi.STATION)
```

which initiates connections with applied parameters. “save” option is set to value `true` to store configuration in memory so you do not have to execute this code every time. When device is powered up next time, connection will be established automatically.

To organize the workflow for ESP8266 we offer the following model represented in Fig. 30.

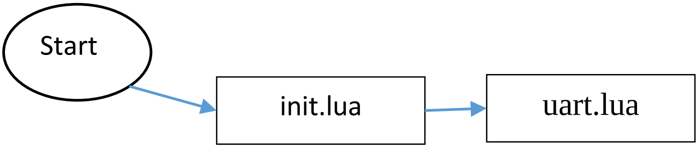


Fig. 30 – Diagram of control transaction in ESP8266

As the module is powered up, it executes init.lua script. In the script availability of the network is checked. When the connection is provided, the control is passed to the main script that is uart.lua in this case. Establish the proposed file structure by clicking on upload button and then selecting files to upload into device memory.

The content of the init.lua file is shown in the next view:

```
     function start()
         print("Starting")
         dofile("uart.lua")
     end

     tmr.create():alarm(5000, tmr.ALARM_AUTO,
     function(timer)
         if wifi.sta.getip() == nil then
             print("Not connected")
         else
             timer:unregister()
             print("WiFi connection established")
             tmr.create():alarm(1000,
tmr.ALARM_SINGLE, start)
         end
     end)
```

This sample code actively uses callback functions (in this case callback for timer event). As connection is established and module is successfully connected to the network, it calls another script that actually contains application logic.

File uart.lua is responsible for transmission of the received data to the network. Here goes sample implementation for uart.lua code.

```
sk = net.createConnection(net.TCP, 0)
sk:connect(3333, “192.168.1.25”)

uart.on("data",
  function(data)
    print("receive from uart:", data)
    sk:send(data)
end, 0)
```

Actually it just forwards received data from UART into the network. IP-address and port may be adjusted to match your particular network. Network communications can be tested using mobile applications like Simple TCP Socket Tester for Android [5] or any other similar application for mobile or desktop devices.

The connection between ESP8266 and STM32 device is organized using Universal Asynchronous Receiver-Transmitter (UART) interface (Fig. 31).

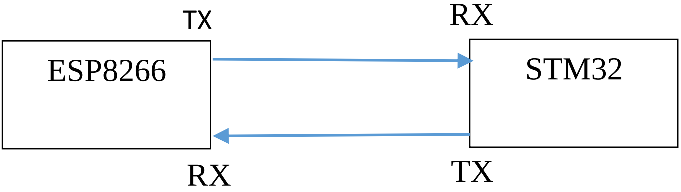


Fig. 31 – Interconnection between ESP8266 and STM32

ESP8266 receives data from STM32 via UART and then transmits into the network.

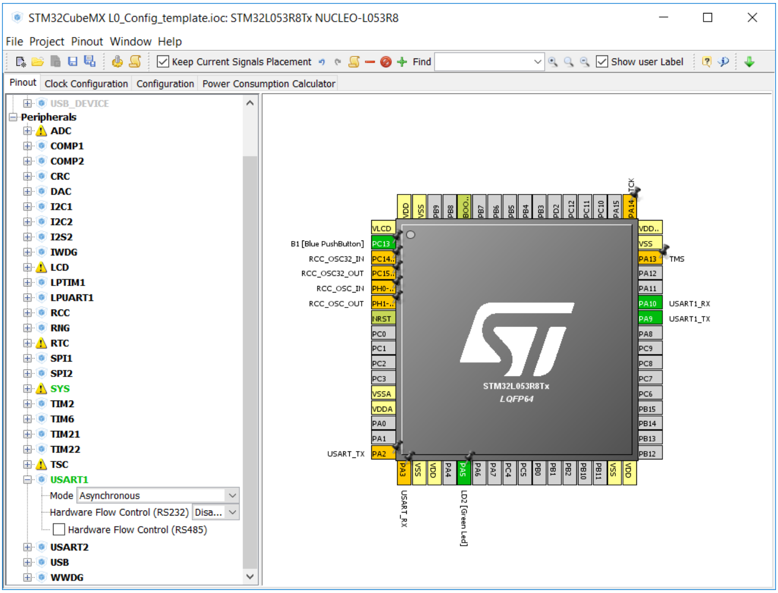
Configuration of STM32 is performed using STM32CubeMX with further generation of bootstrap project for SystemWorkbench and loading firmware to development kit. Assure that specific bundle for L0 microcontroller series is installed (menu item Help/Install New Libraries) for code generation.

Activate USART1 and select Asynchronous mode from the combo box. Two pins (PA9 and PA10) on the diagram now are activated to work in UART mode (Fig. 32).

Go to Configuration tab and select USART1 button. In the dialog window select NVIC Settings and activate interrupts connected with USART (Fig. 33).

The described communication model supposes transmission of the data from microcontroller to WiFi-module over the fixed periods of time. Thus, we need to activate timer functionality (Fig. 34) to measure time in microcontroller.

Theoretical issues for “IoT for Smart Energy Grid” are described in Part IX (sections 32-35) of the book [Internet of Things for Industry and Human Application, vol. 3. Assessment and Implementation, V. S. Kharchenko, Ed. Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].



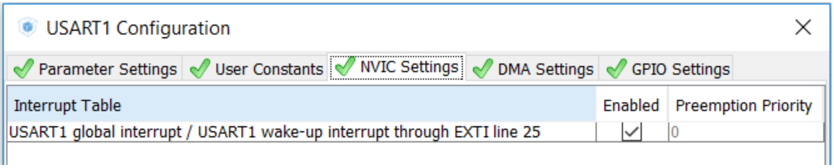
USART1

Mode: Asynchronous

Hardware Flow Control (RS232): Disa...

□ Hardware Flow Control (RS485)

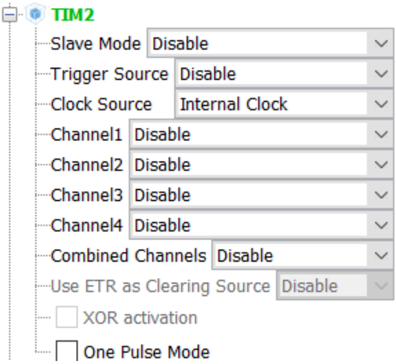
Fig. 32 – Pinout diagram



USART1 Configuration

Interrupt Table	Enabled	Preemption Priority
USART1 global interrupt / USART1 wake-up interrupt through EXTI line 25	☑	0

Fig. 33 – Interrupt settings for UART



TIM2

Slave Mode: Disable

Trigger Source: Disable

Clock Source: Internal Clock

Channel1: Disable

Channel2: Disable

Channel3: Disable

Channel4: Disable

Combined Channels: Disable

Use ETR as Clearing Source: Disable

□ XOR activation

□ One Pulse Mode

Fig. 34 – Basic settings of timer

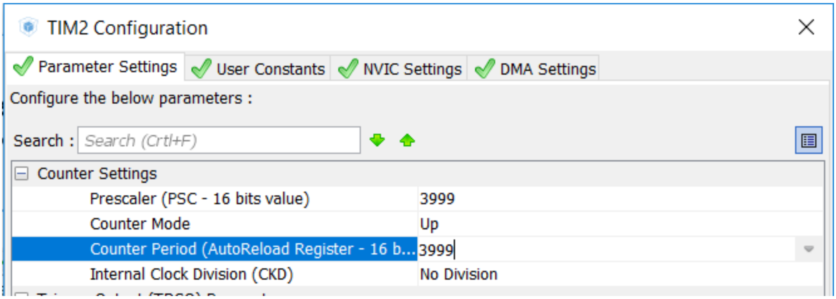
In addition, it is required to enable timer interrupts in the configuration tab in timer settings.

Timer as internal module depends on clock frequency that device works on. This parameter can be set in Clock configuration tab by selecting internal clock source HSI 16 (16 MHz). Being aware of clock frequency, it is easy to adjust timer parameters to receive interrupt approximately each second. It can be devised from the equation

$$\text{Period}(\text{s}) = \frac{\text{Frequency(Hz)}}{(\text{prescaler\_val}+1)\cdot(\text{counter\_period}+1)}, \qquad (3.1)$$

where prescaler_val - prescaler value; counter_period - counter period; Frequency - work frequency, Hz; Period - period of interrupts, s.

Value 1 is subtracted from prescaler and period value due to the fact that they start from 0. One of the possible valid options for these parameters are shown in Fig. 35.



Configure the below parameters :

Counter Settings	
Prescaler (PSC - 16 bits value)	3999
Counter Mode	Up
Counter Period (AutoReload Register - 16 b...	3999
Internal Clock Division (CKD)	No Division

Fig. 35 – Counter settings for timer

According to the values in Fig. 3.4, we can verify results for timer period calculation from (3.1) as

$$\text{Period} = \frac{16000000}{(3999+1)\cdot(3999+1)} = 1(\text{s}).$$

Actually, there are many options how to set up necessary period by adjustment counter period and prescaler and there is no strong recommendations about values of these parameters except it is preferred that they should be selected so the values explain its gist and can be easily tuned in the future.

Regarding clock source configuration, we could not leave unmentioned configuration of the input frequency for the device. The Clock configuration tab (Fig. 36) provides full control on the clocking device and each its specific part. It is easy to notice that clock system of the device is quite complex and can be tuned to achieve optimal performance in terms of computational resources and power consumption for concrete application.

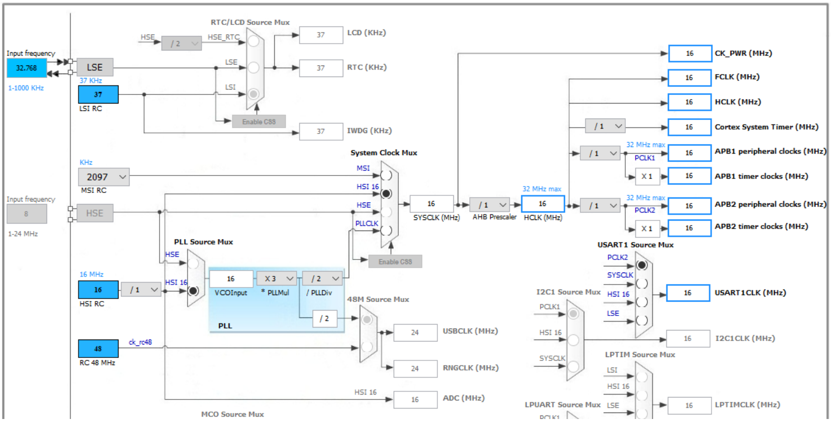


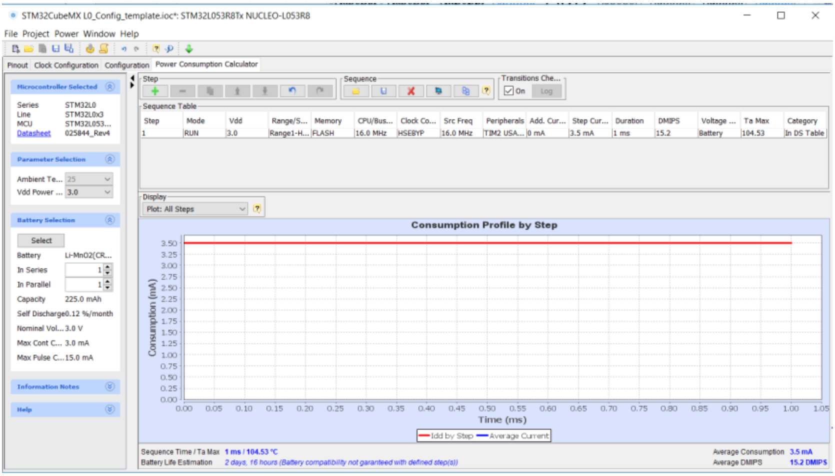
Fig. 36 – Clock configuration view

Various clock sources are available for clocking microcontroller. In this example, we use internal clock source with 16 MHz frequency. By the means of Phase-Locked Loop (Loop) it can be downgraded to lower values. The big advantage of this automation tool is that all configurations are automatically checked so you are not allowed to end up with incorrect clock settings.

Tune the parameters in the Clock configuration tab to achieve maximum clock frequency for the selected device (32 MHz). Try to set frequency higher than maximum allowed one and observe actions of the environment. Activate peripherals that work on Low-Speed frequency (e.g. Real-Time Clock, RTC) and select clocking source for them.

As all configuration parameters are set you can generate project using menu item Project/Generate Code. However, before that check that in Project/Settings value of IDE is set to SW4STM32. Also, provide project name in the same settings window. Run generation of the code and then you can open project in SystemWorkbench for STM32.

Take additional step to check estimated power consumption in the selected mode with the specified peripheral devices. Go to Power Consumption Calculator and set up all the values applied on the previous stages. You should observe the following results (Fig. 37).



Series STM32L0
Line STM32L0x3
MCU STM32L053...
Datasheet 025844_Rev4

Ambient Te... 25
Vdd Power ... 3.0

Battery Li-MnO2(CR...
In Series 1
In Parallel 1
Capacity 225.0 mAh
Self Discharge0.12 %/month
Nominal Vol... 3.0 V
Max Cont C... 3.0 mA
Max Pulse C... 15.0 mA

☑ On

Sequence Table

Step	Mode	Vdd	Range/S...	Memory	CPU/Bus...	Clock Co...	Src Freq	Peripherals	Add. Cur...	Step Cur...	Duration	DMIPS	Voltage ...	Ta Max	Category
1	RUN	3.0	Range1-H...	FLASH	16.0 MHz	HSEBYP	16.0 MHz	TIM2 USA...	0 mA	3.5 mA	1 ms	15.2	Battery	104.53	In DS Table

Plot: All Steps

Sequence Time / Ta Max 1 ms / 104.53 °C
Battery Life Estimation 2 days, 16 hours (Battery compatibility not garanteed with defined step(s))
Average Consumption 3.5 mA
Average DMIPS 15.2 DMIPS

Fig. 37 – Consumptions expectations

Tune the parameters and add additional steps to achieve better longevity for the power source (e.g. 1 month without exchange power supply).

To develop firmware for STM32 board use SystemWorkbench for STM32. Open created on the previous step project template and edit source code to organize communication between devices. Hardware Abstract Library (HAL) is recommended for microcontroller software development [4].

Note that the most part of the code has been already generated for you and only small chunks of code need to be added to the file. The following code sample shows how you can implement transmission over UART using timer interrupts.

```
…
#include <string.h>
#include <stdlib.h>
```

```
    …

    char message[20];

    void
HAL_TIM_PeriodElapsedCallback(TIM_HandleTypeDef    *
timHandle) {
      sprintf(message, "%f", status_message);
      HAL_UART_Transmit(&uart,    (uint8_t*)message,
20, 1000);
      //HAL_UART_Transmit_IT(&uart,
(uint8_t*)message, 20);
    }

    void
HAL_UART_TxCpltCallback(UART_HandleTypeDef * huart)
{
      // UART code goes here
    }
```

The first function callback is responsible for processing timer update interrupts. It sends diagnosis message that is floating-point number in this case. Transmission can be executed in synchronous mode or asynchronous mode. For the second case it is necessary to implement transmission callback to process this event.

Report requirements.

Report must contain:

– source code of the program;

– demonstration of communications between ESP8266 module and STM32 board;

– demonstrations of data transmitted over the network from ESP8266.

Test questions

1. What programming languages are recommended for STM32 and ESP parts?
2. What mechanism is established in NodeMCU firmware to react on external events?
3. How to connect two devices via UART interface?
4. Explain file organization and control flow for NodeMCU.

Recommended literature.

1. "NodeMCU Documentation", 2018. [Online]. Available: https://nodemcu.readthedocs.io/en/master/.

2. "Integrated Development Environment (IDE) for ESP8266 developers", Github, 2018. [Online]. Available: https://github.com/4refr0nt/ESPlorer.

3. "STM32CubeMX", 2018. [Online]. Available: https://www.st.com/en/development-tools/stm32cubemx.html.

4. Description of STM32F4 HAL and LL drivers, 5th ed. STMicroelectronics, 2017 [Online]. Available: https://www.st.com/content/ccc/resource/technical/document/user_manual/2f/71/ba/b8/75/54/47/cf/DM00105879.pdf/files/DM00105879.pdf/jcr:content/translations/en.DM00105879.pdf.

5. A. Parra, "Simple TCP Socket Tester", Google Play, 2018. [Online]. Available: https://play.google.com/store/apps/details?id=com.simplesockettester&hl=en_US.

Training 3

CLOUD SOFTWARE DEVELOPMENT PLATFORM "MBED" FOR LOCAL INFRASTRUCTURE IOT-SOLUTIONS

The aim of the training: to get acquainted with mbed development platform and its infrastructure to understand its advantages for further usage.

Learning task:

–introduction to the work with mbed development platform and classes to measure external signals using ADC.

Practical tasks:

–firmware development for measurement of external signal and evaluation of the IoT-node consumption represented by STM32 board;

–work with documentation system of mbed;

–work with repository system of mbed.

Theoretical information

Student should be registered at https://os.mbed.com as developer to access on-line software. USB-cable with mini-USB jack is required to program the device. Any STM32 development board with "mbed" mark on the package can be used during this work. It is recommended to use STM32 Nucleo 64 board.

Execution of the work.

First, you need to register at https://os.mbed.com [1, 2] to access programming features of the platform. It requires setting credentials and additional information about the user. Just as you registered and logged into the system you can access compiler by clicking Compiler button in the top right corner of the site (Fig. 38).

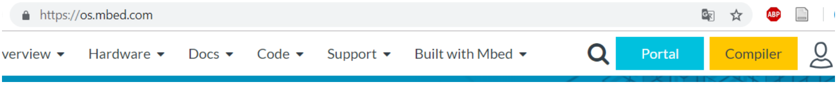
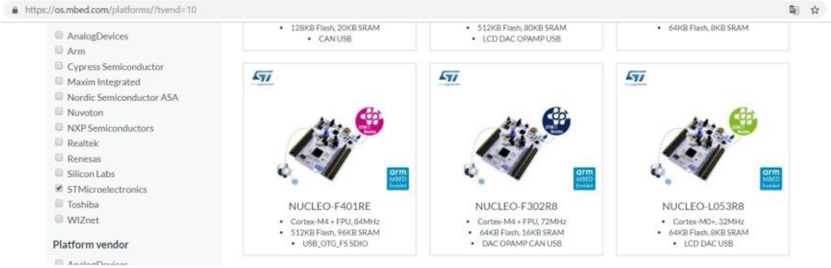


Fig. 38 – Compiler button in the main site menu

To develop in mbed environment it is necessary to specify target device that is chosen from the list of hardware added to account. To add board use menu item Hardware/Boards from the main page (os.mbed.com) and find your target device. For this practice task, you should find NUCLEO-L053R8 board (Fig. 39).



https://os.mbed.com/platforms/?tvend=10

- □ AnalogDevices
- □ Arm
- □ Cypress Semiconductor
- □ Maxim Integrated
- □ Nordic Semiconductor ASA
- □ Nuvoton
- □ NXP Semiconductors
- □ Realtek
- □ Renesas
- □ Silicon Labs
- ☑ STMicroelectronics
- □ Toshiba
- □ WIZnet

Platform vendor

- 128KB Flash, 20KB SRAM
- CAN USB

- 512KB Flash, 80KB SRAM
- LCD DAC OPAMP USB

- 64KB Flash, 8KB SRAM

NUCLEO-F401RE

- Cortex-M4 + FPU, 84MHz
- 512KB Flash, 96KB SRAM
- USB_OTG_FS SDIO

NUCLEO-F302R8

- Cortex-M4 + FPU, 72MHz
- 64KB Flash, 16KB SRAM
- DAC OPAMP CAN USB

NUCLEO-L053R8

- Cortex-M0+, 32MHz
- 64KB Flash, 8KB SRAM
- LCD DAC USB

Fig. 39 – Nucleo board on the hardware page

Click on the tile with selected board and at the redirected page you can add board to your compiler environment. Click on Add to your Mbed Compiler button (Fig. 40) to finish the process. The button is usually located on the right side of the page near Overview section.

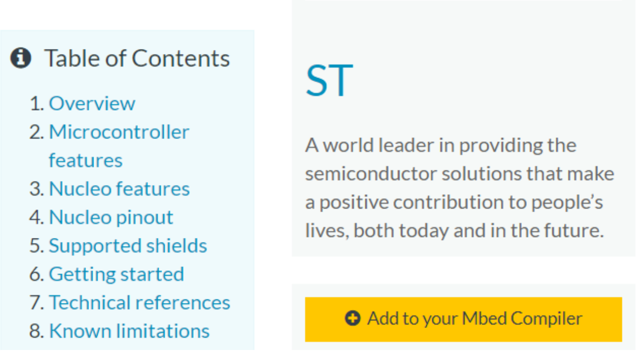


Table of Contents

1. Overview
2. Microcontroller features
3. Nucleo features
4. Nucleo pinout
5. Supported shields
6. Getting started
7. Technical references
8. Known limitations

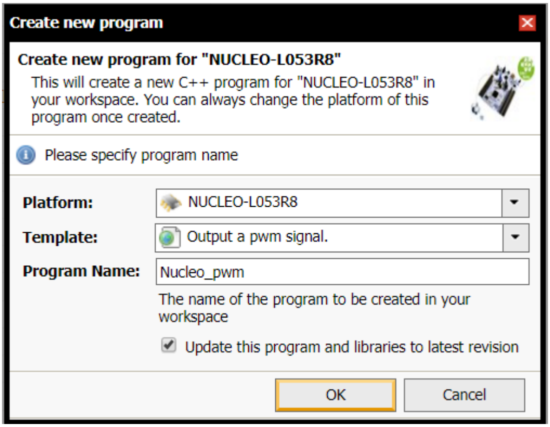
ST

A world leader in providing the semiconductor solutions that make a positive contribution to people's lives, both today and in the future.

Fig. 40 – Button to add board into Compiler

Now selected board is available in the Compiler and you can develop firmware for the board.

Create new program by clicking New/New Program menu item to get started. In the dialog window enter name of the program and select template for the created program. The sample configuration is shown if Fig. 41.



Create new program for "NUCLEO-L053R8"

This will create a new C++ program for "NUCLEO-L053R8" in your workspace. You can always change the platform of this program once created.

Please specify program name

Platform: NUCLEO-L053R8

Template: Output a pwm signal.

Program Name: Nucleo_pwm

The name of the program to be created in your workspace

☑ Update this program and libraries to latest revision

Fig. 41 – Dialog window for new program

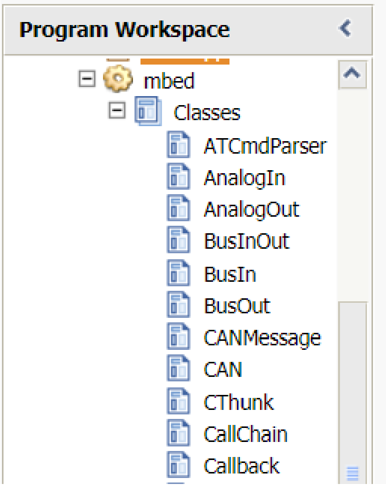
Make sure that in the Platform combo-box you have selected correct target. With one board added to the compiler it will be correct automatically but when several platforms are available it just sets last selected board in the field. It may be an issue because program expect presence of resources that are available on the different board.

Another option is to import existing project from repository. Use import menu item and Programs tab to search for available programs.

Among the other advantages, mbed provides exhaustive documentation for built-in classes. To access documentation for concrete class in Program Workspace select mbed node and expand it. Then expand Classes node (Fig. 42). List of available classes drops down. Selection of the item from the list causes opening documentation tab in the main panel.

Classes are developed in Arduino-like style and guarantee minimum amount of code to get started with device. In this practicum we are interested in measurement of power supply signal. AnalogIn class is the class (Fig. 43) that represents Analog-Digital Converter (ADC) to monitor voltage.

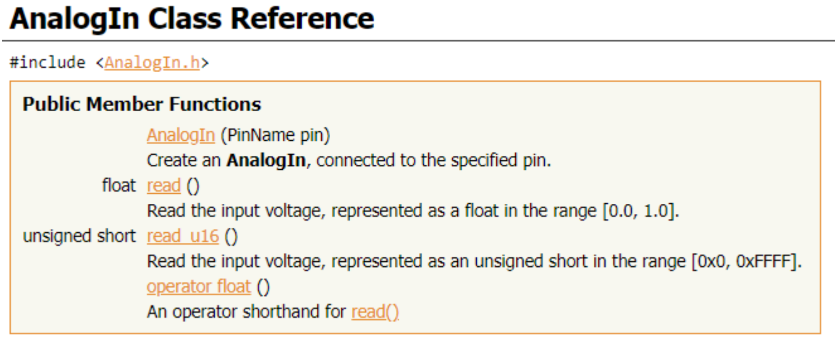
According to documentation, it contains only four class members. One of them is constructor that requires valid pin name. `read()` function allows to retrieve data in float format with normalized value that goes between [0.0, 1.0]. In case you need raw integer data, use `read_u16()` function instead.



Program Workspace

- mbed
  - Classes
    - ATCmdParser
    - AnalogIn
    - AnalogOut
    - BusInOut
    - BusIn
    - BusOut
    - CANMessage
    - CAN
    - CThunk
    - CallChain
    - Callback

Fig. 42 – List of built-in classes in mbed



AnalogIn Class Reference

`#include <AnalogIn.h>`

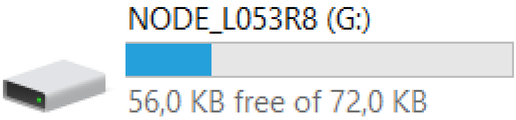
Public Member Functions

	AnalogIn (PinName pin) Create an **AnalogIn**, connected to the specified pin.
float	read () Read the input voltage, represented as a float in the range [0.0, 1.0].
unsigned short	read_u16 () Read the input voltage, represented as an unsigned short in the range [0x0, 0xFFFF].
	operator float () An operator shorthand for read()

Fig. 43 – Documentation for AnalogIn class

Despite the huge advantages of the platform, the main drawback is a lack of debugging support in web-environment. Thus, it is responsibility of programmer to provide debugging marks to verify correctness of the program.

Let us briefly explain process of programming device supported by mbed platform. The device contains special type of firmware in the second microcontroller on the board. This firmware describes connected board as mass storage device. Thus, you can go to Computer folder and check that new storage device has appeared. Device’s name should start from STM or NODE. Typically, series part also appears in the name (e.g. L053). Total volume of mass storage should be 72 kbytes that matches volume of flash memory in the microcontroller as it is shown in Fig. 44.

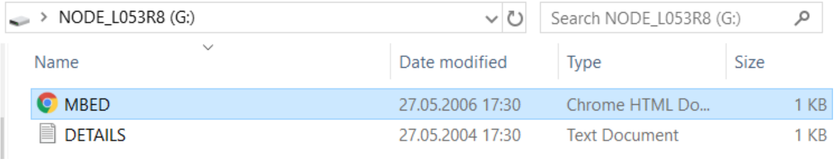


NODE_L053R8 (G:)

56,0 KB free of 72,0 KB

Fig. 44 – Board icon in Computer window

If you open this drive, you can notice two files in HTML and text format (Fig. 45). Those are information files and do not affect work of the system.

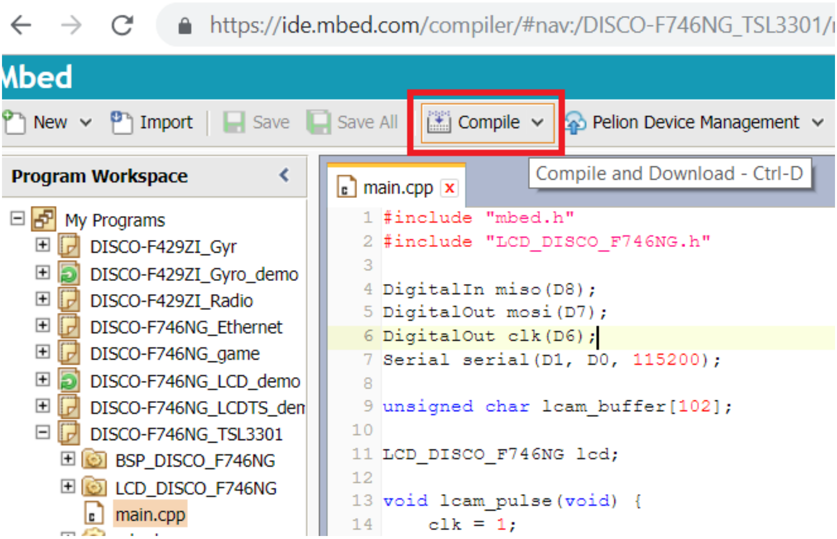


Name	Date modified	Type	Size
MBED	27.05.2006 17:30	Chrome HTML Do...	1 KB
DETAILS	27.05.2004 17:30	Text Document	1 KB

Fig. 45 – Content of the storage device

To program device you need to obtain a compiled binary file from compiler environment. Compile item on the menu panel provides function to run compilation what is shown in Fig. 46. By default, if compilation is successful, you can download binary file. Either download starts automatically or you have to approve download in the dialog window. This behavior depends on browser.

Download starts only if there are no compilation errors in the project. Sometimes, environment helps you to solve issues automatically. In this case, Fix it button appears near error message. In most cases, it supposes import of libraries. When multiple projects present in the workspace and have open files in the editing area, you should check that necessary file and project are active so you get binary from your current project. In case you do not need to download binary file and just want to check if any errors exist in your code you can select Build Only option from the list.



```
#include "mbed.h"
#include "LCD_DISCO_F746NG.h"

DigitalIn miso(D8);
DigitalOut mosi(D7);
DigitalOut clk(D6);
Serial serial(D1, D0, 115200);

unsigned char lcam_buffer[102];

LCD_DISCO_F746NG lcd;

void lcam_pulse(void) {
    clk = 1;
```

Fig. 46 – Compile item in the main menu

As you have downloaded binary file, you can program the device. To do this copy binary file to the mass storage device that matches development board. During flashing firmware into device you can observe that LED on the board is blinking and changing its color. Typically, reset happens automatically after firmware has been flashed into memory. Otherwise, press the RESET button on the board. Repeating programming of the device with new firmware might require refresh folder view of the disk because of not enough disk space issue. Operating system might precalculate that available space on the disk is not enough to write new file and prevent file from writing. You should refresh folder (F5 button) so last copied file will disappear from the folder. If this recommendation does not help to solve problem, try reconnecting device.

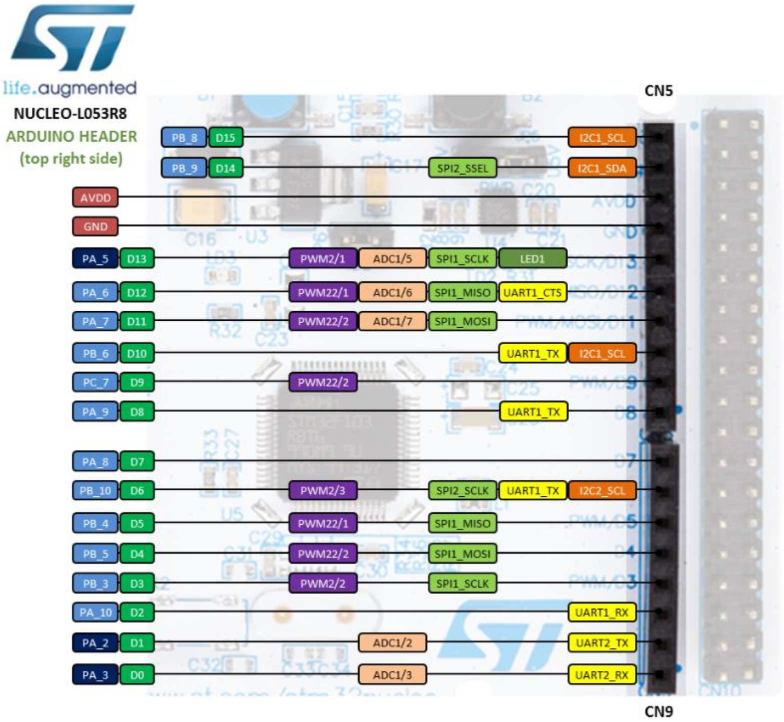
Let us consider basic example to get started with mbed environment.

```
#include "mbed.h"

DigitalOut myled(PC13);

int main() {
    while(1) {
        myled = 1; // LED is ON
        wait(0.2); // 200 ms
        myled = 0; // LED is OFF
        wait(1.0); // 1 sec
    }
}
```

In the example, we create an instance of DigitalOut class that is assigned to work with pin PC13. The main function contains infinite while loop. In the loop, state of the output pin is changed in different intervals of time. Notice that syntax of mbed library allows you to perform assignment of value directly via numerical value. mbed library overrides implementation of assignment operator (=) and makes it easier for developer to control pins and provides better understanding with such syntax construction. Another important feature is that you initialize pin with just one line of code. Most part of the initialization process is hidden from developer. It results in more concise code. It is also worth mentioning that you need to include just one header file – mbed.h. All the other necessary headers will be included from this file. The last one option to discuss in the example is that mbed provides unified delay function wait. It accept both integer and floating point values and organizes delay in seconds. E.g., 0.2 passed as parameter to this function means that delay will take 0.2 s.

Although, many actions mbed performs automatically, developer should follow several rules to get correct firmware. First, you should carefully check if pin supports function you select for it. Integrated circuit production process fixes that function can be used only on several pins and will not be available on the others. Limited number of functions can be multiplexed to the pin. To check if function is available to the pin or group of pins (interfaces usually use several pins for their work), developer should go to the page dedicated to the board (menu item Hardware/Boards on the main page of mbed). This page contains information about functions of pins in graphical form. Part of this information is shown in Fig. 47. Pins on the development board are routed to two types of connectors. They are Arduino connectors (female) and Morpho connectros (male). Arduino connectors are organized and placed the same way as it is done in original Arduino board. Thus, the board is Arduino compatible and various shields may be used with Nucleo board. However, microcontroller in the board is more powerful.

It also have more outputs and more peripheral modules. To make all outputs from microcontroller available to the developer, Morpho connectors are placed on the board. They provide access to all pins in microcontroller and allow user to harness all potential of the microcontroller. Functional purpose of pins (or alternate functions) grouped by peripheral. You can also observe that user free to choose among multiple pin options for peripheral, e.g. SPI1. Keep in mind that Morpho duplicates Arduino connections so it will be the same pin accessed.



life.augmented
NUCLEO-L053R8
ARDUINO HEADER
(top right side)
CN5
PB_8 D15 I2C1_SCL
PB_9 D14 SPI2_SSEL I2C1_SDA
AVDD
GND
PA_5 D13 PWM2/1 ADC1/5 SPI1_SCLK LED1
PA_6 D12 PWM22/1 ADC1/6 SPI1_MISO UART1_CTS
PA_7 D11 PWM22/2 ADC1/7 SPI1_MOSI
PB_6 D10 UART1_TX I2C1_SCL
PC_7 D9 PWM22/2
PA_9 D8 UART1_TX
PA_8 D7
PB_10 D6 PWM2/3 SPI2_SCLK UART1_TX I2C2_SCL
PB_4 D5 PWM22/1 SPI1_MISO
PB_5 D4 PWM22/2 SPI1_MOSI
PB_3 D3 PWM2/2 SPI1_SCLK
PA_10 D2 UART1_RX
PA_2 D1 ADC1/2 UART2_TX
PA_3 D0 ADC1/3 UART2_RX
CN9

Fig. 47 – Diagram of pin functions

One important thing that should be mentioned about pin configuration in mbed is support of two naming schemes for pins. Blue and green labels at the left side of the image are interchangeable. E.g. PA_8 and D7 denote the same pin. Main advice for using pin names in program code is to select one style and follow it through the whole program, do not mix different naming conventions (e.g. PB_10 and D7 in the same program).

From Fig. 47 you can notice that several pins supports functionality of ADC. ADC in microcontroller has multiple channels and can obtain data from all of them. Number after slash in ADC label means number of ADC channel that corresponds to pin. Those ones should be used in the next task. Select one of them to measure input signal.

Monitoring state of the power supply (battery) can be performed in the following way. Output voltage of the source have to be measured. Then, we can apply retrieved value in our program to monitor supply. As the device works it should receive lower and lower values from analog input and signal about it to the user. It can be done using LED available on the board (connected to PC13). When the voltage goes beyond selected margin from the start level (e.g. 90-95%), visual signal is activated to inform about it.

Implement functionality described above using AnalogIn class. You may need DigitalOut class to write values to signal about changes in the voltage level.

Theoretical issues for “IoT for Smart Energy Grid” are described in Part IX (sections 32-35) of the book [Internet of Things for Industry and Human Application, vol. 3. Assessment and Implementation, V. S. Kharchenko, Ed. Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

Report requirements.

Report must contain:

– source code of the program;

– measurements of the start voltage level end signal voltage level for power source;

– demonstrations of the visual signals during different stages of device work.

Test questions:

1. Explain the workflow offered by mbed environment.
2. Compare mbed library organization with the organization of HAL from Practicum 2. What library does provide a higher level of abstraction?
3. How is the board recognized at the PC-side?
4. How to manipulate digital pins of the board?

Recommended literature.

1. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies Protocols and Applications," in IEEE Commun. Surv. Tutorials, vol. 17, iss. 4, 2015, pp. 2347-2376. DOI: 10.1109/COMST.2015.2444095.

2. "Mbed OS 5", Mbed, 2018. [Online]. Available: https://os.mbed.com/.

ITM1.3. Availability assessment of IoT based IT infrastructure of Power Grids

DrS, Prof. Brezhniev E.V. (KhAI)

Training 1

INTEGRATION OF RELIABILLITY METHODS INTO SAFETY ASSESSMENT PROCESSES FOR IT INFRASTRACTURE OF POWER GRID

The aim of the training: to obtain the basic skills of integration of reliability models into safety assessment of IT infrastructure of power grid.

Learning tasks:

– study of basic theoretical information about the Bayesian (BBN) and Fault Tree Analysis (FTA) which are used for safety and reliability assessment of IoT based smart grid and systems;

– getting the knowledge on approaches and principle of integration of reliability and safety assessment methods.

Practical tasks:

– gaining skills in the practical application of software tools which are used to support for BBN (Netica 512) and FTA (Cafta 6.0) calculations;

– development of soft skills for public presentation of work results.

Theoretical information

The principle of integrating safety and reliability analysis methods shall be applied for analyzing the safety of a smart grid. The idea is to integrate the results of assessment of smart grid (SG) systems' reliability parameters into safety assessment modelling as inputs to improve the credibility of results of calculations.

Method of safety assessment taking into account the reliability of systems (subsystems) is considered in this subsection. For SG power plant (NPPs for example), the safety key factor is the reliability of the transformer substation equipment, through which external power supply is provided, as well as the reliability of power lines, etc. The SG consists of generating stations and an electrical system (see Fig. 48).

Digital substation is one of the important assets of the SG, which provides reception, conversion and distribution of electrical energy. In fact, it is the interface between the power plant and the electrical system located in close proximity to the plant.

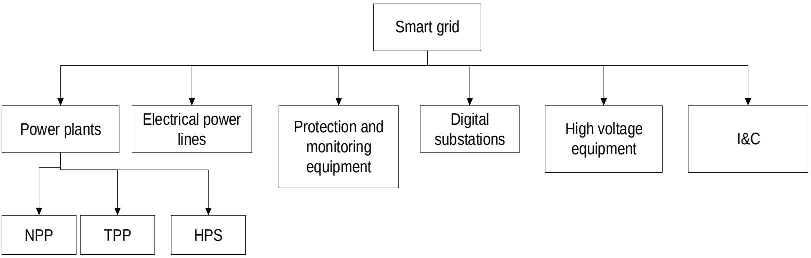


Fig. 48 - The general representation (“high level”) of SG

Within this approach, it is proposed to use the operational readiness ratio as an indicator of the SG substation reliability. The operational availability ratio is probability that the SG substation will be operational (provide electricity for the plant) at an arbitrary point in time and from this point on it will work flawlessly within a specified period of time.

To assess the impact of reliability indicators of a substation on the SG safety, it is proposed to use the method based on the combined use of BBN and the failure tree analysis method (FTA). When constructing BNN, it is very important to set priori probabilities of the parent nodes states correctly. It is proposed to use the method of the fault tree analysis for this.

The proposed method involves the following stages: definition and structuring of all substation assets; risk analysis of substation assets, considering the severity of failures for the substation; substation risk asset ranking, taking into account the impact on performance of the digital substation. At this stage, the most critical assets are identified, the failures of which lead to a loss of readiness of the digital substation; the construction of BBN, including the node(s), taking into account the digital substation reliability in the form of availability factor, namely, the probability of finding the substation in working condition.

The probabilities of finding the substation assets in working condition are determined using FTA.

The steps of the method are shown in Fig. 49.

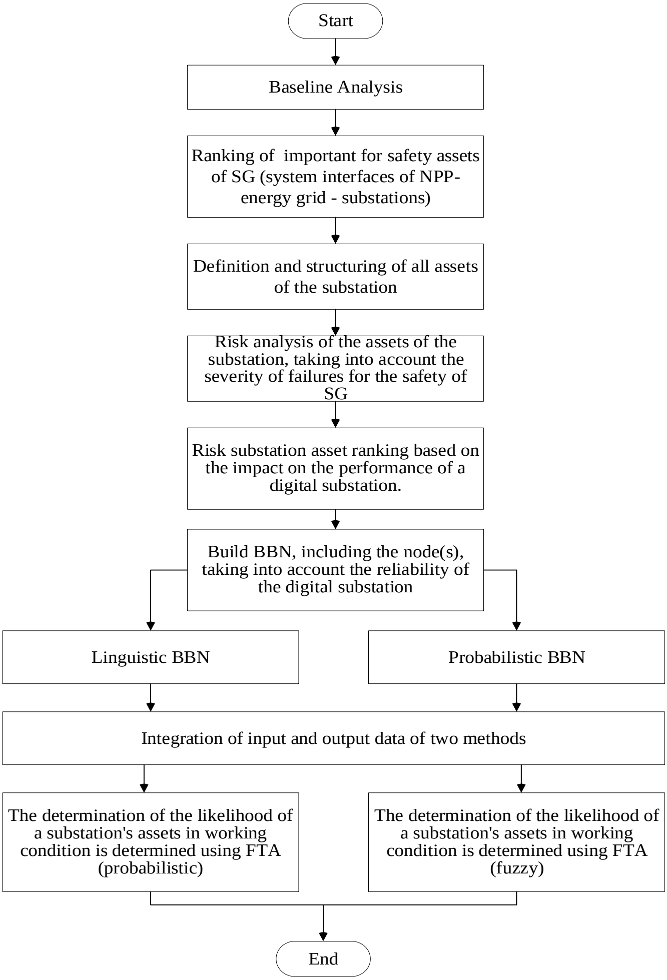

Start
Baseline Analysis
Ranking of important for safety assets of SG (system interfaces of NPP-energy grid - substations)
Definition and structuring of all assets of the substation
Risk analysis of the assets of the substation, taking into account the severity of failures for the safety of SG
Risk substation asset ranking based on the impact on the performance of a digital substation.
Build BBN, including the node(s), taking into account the reliability of the digital substation
Linguistic BBN
Probabilistic BBN
Integration of input and output data of two methods
The determination of the likelihood of a substation's assets in working condition is determined using FTA (probabilistic)
The determination of the likelihood of a substation's assets in working condition is determined using FTA (fuzzy)
End

Fig. 49 - Stages of the SG safety assessment taking into account the reliability of subsystems

As an example of the method application, the BBN fragment is given to assess the safety of a nuclear reactor, taking into account the state of sources of external and internal energy supply (Fig. 50).

The main nodes are: a state node of the reactor (reactor state unit), metering nodes of the state of two safety systems (RCIC, RPS), metering nodes of external and internal power supply (Off_site_power_state, On_site_power_state), state nodes of three digital substations (smart_substation_ (1 3)), nodes for diesel generator (DG) and battery (DC_batteries).

This BBN was built using the Netica 512 tool.

For example, after ranking, RTU is set to be the most critical asset. RTU is a remote terminal device that performs important functions in ensuring the operability of a digital substation. Its failures can lead to the loss of load (operability) of a digital substation. In turn, this event leads to the loss of one of the lines ensuring the supply of all NPP safety systems.

The main reasons for the loss of RTU performance can be: I / O terminal failures, software failures, power supplies.

The FTA for the event is the loss of operational readiness of the substation, constructed within a given illustrative example, is shown in Fig. 51. The operational readiness ratio of the substation is determined on the basis of FTA. Calculations of the substation reliability indicators were carried out using the Cafta 6.0 a tool.

The construction of BBN and its integration with the method of analysis of failure trees is shown in Fig.52.

It should also be noted that when BBN and FTA are used together, two cases may arise:

– for the safety assessment, a combination of linguistic BBN and classical (probabilistic) FTA is used. In the linguistic BBN, all network parameters, including conditional probabilities, are represented as linguistic values (LV);

– for the safety assessment, a combination of probabilistic BBN and FTA is used, in which the probabilities of basic events can be partially or completely represented as LV. Fuzzy FTA extension is used in case of insufficient failure statistics, which allows determining the reliability parameters of a complex system.

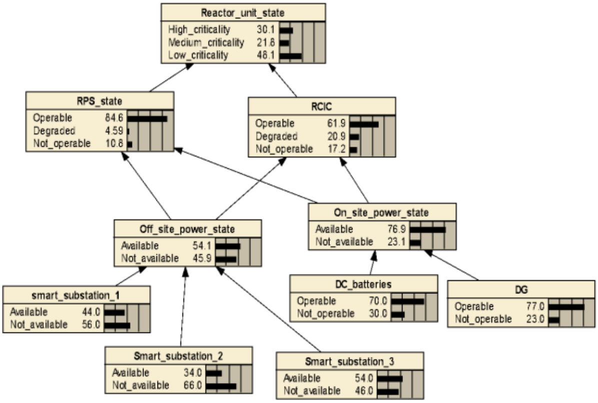


Fig. 50 - BBN for nuclear power plants safety assessing, taking into account the performance of digital substations and internal power supply

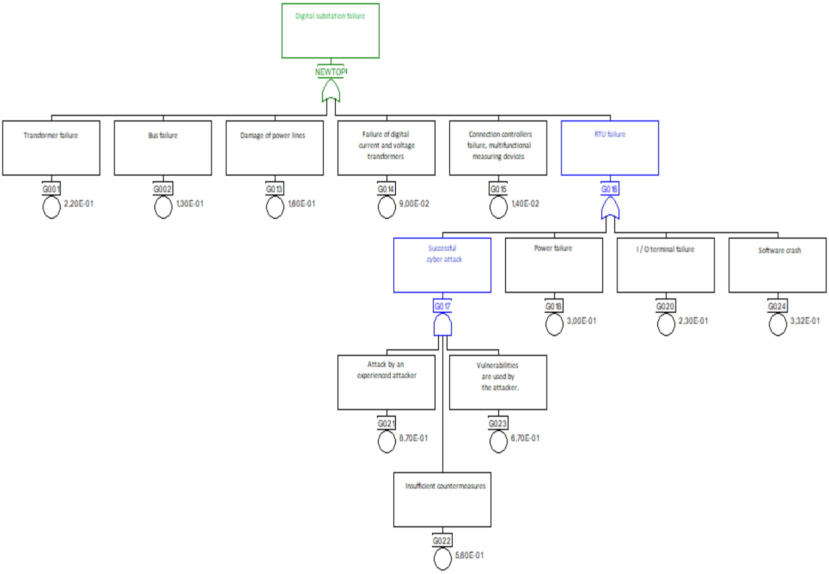


Fig. 51 - Failure tree for RTU, built in the context of an illustrative example

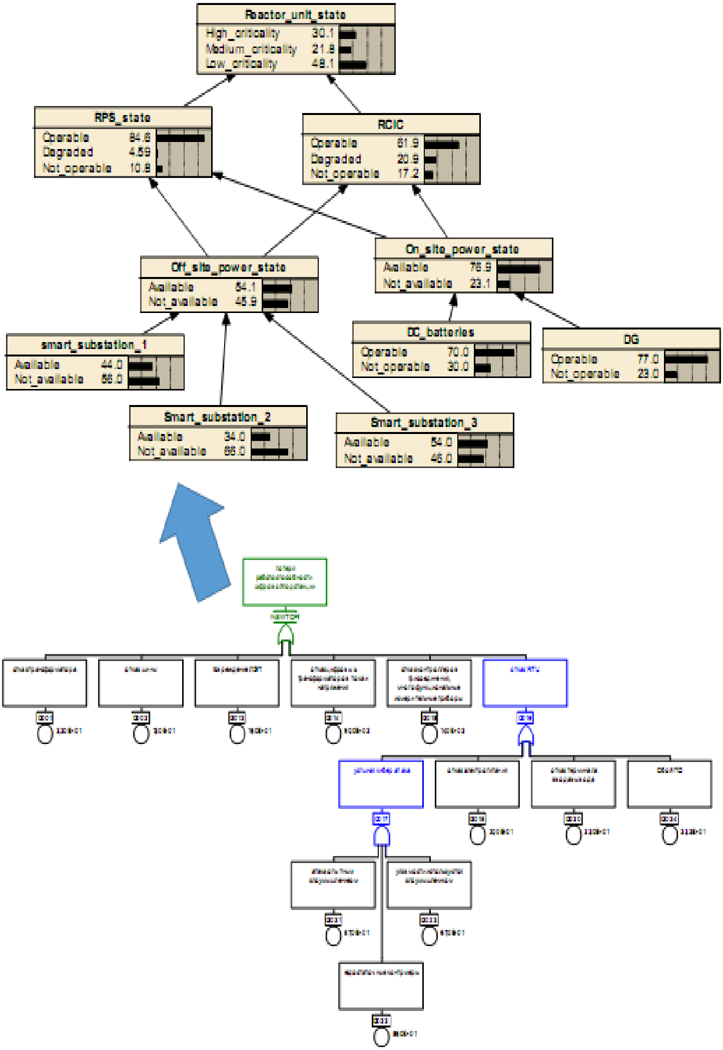


Fig. 52 - Integration of failure tree and BBN methods

For both cases, the question of the integration of input and output data arises. As a solution, it is proposed to use fuzzification and defuzzification methods. Fuzzification allows to integrate probabilities into linguistic BBN. It is theoretically possible to defuse linguistic BBN. However, this task may require resource costs. For the second case, it is possible to use the fuzzification of the classical BBN, which is also a costly process.

In this case, the most convenient approach is to defuse the output values obtained using the fuzzy method of analyzing failure trees.

Training implementation during the training needs:

1. Read the theoretical information.

2. Install on your PC the trial versions of Cafta 6.0 and Netica 512.

3. Build FTA as shown on Fig. 51. Calculate the failure of substation considering your variants (see Table 4).

4. Build BBN as shown on Figure 50 and taking the results of failure probability calculation (from bullet 3).

4. Calculate the criticality of Reactor Unit.

5. Write a report. See report requirements below.

6. Answers the test questions.

5. Prepare a presentation.

Report requirements.

1. Report language is English.

2. The report should include:

- a title page with information about the author, the name of the discipline, analysis topics, option, teacher, university and department logos;
- content;
- Section 1 – a short description of BBN method;
- Section 2 - a short description of FTA;
- Section 3 – results: screenshots of BBN, FTA, BBN&FTA (integrated), probabilities of reactor unit' criticality states with input from FTA calculation.

3. The report shall be presented in two formats (doc and pdf) and sent to the teacher's e-mail.

A presentation shall be prepared to defend the results. The presentation should include:

1. The title page.

2. The content of the presentation.

3. Description of the BBN and FTA.

4. Screenshots of FTA, BBN, BBN&FTA.
5. Results.
6. Conclusions.

The training is considered to be completed after the defense of the presentation by each student individually.

Presentation time is up to 10 minutes. English language.

Table 4 – Students’ task variants

	FT Probability of failures									
	T	B	PL	DCT	C	RTU	CA	PF	I/O	S
1	1E-3	1,1E-4	2,9E-5	4,7E-6	1,6E-3	1,4E-6	2,2E-5	1,7E-4	4,9E-7	1,8E-2
2	1E-4	1,2E-4	3,9E-4	5,9E-4	1,9E-6	1,8E-4	3,9E-6	1,9E-8	5,9E-4	1,3E-3
3	1E-5	1,5E-4	4,9E-5	2,9E-3	8,9E-4	1,9E-5	2,9E-4	1,6E-4	1,9E-7	1,2E-4
4	1E-6	1,7E-4	5,9E-4	1,9E-4	1,8E-5	1,6E-4	7,9E-6	1,5E-3	7,9E-3	1,8E-4
5	1E-7	1,66E-2	5,8E-3	3,9E-5	2,9E-4	1,7E-5	2,9E-6	1,6E-4	3,9E-5	2,9E-7
6	1,1E-4	1,21E-4	4,2E-4	6,9E-4	1,9E-4	5,9E-4	4,9E-8	1,7E-5	2,9E-4	3,9E-6
8	1,2E-5	1,31E-4	5,2E-7	2,9E-3	3,9E-6	4,9E-4	1,9E-3	1,5E-4	6,9E-5	4,9E-6
9	1,5E-3	1,23E-6	5,5E-4	5,9E-7	1,9E-4	2,9E-3	1,8E-4	1,4E-6	2,9E-3	3,9E-5
10	1,6E-3	1,88E-5	6,9E-3	1,9E-3	4,9E-3	3,9E-6	1,7E-5	1,3E-4	2,9E-4	1,8E-4
11	1,8E-2	1,9E-3	8,8E-4	3,9E-5	2,9E-5	5,9E-4	1,9E-6	1,2E-7	1,9E-5	1,9E-3

Note.
T - Transformer
B – bus
PL – power Line
DCT – direct current transformer
C - Connections
RTU – remote terminal unit
CA - Cyber Attack
PF – power failure
I/O – input /output failure

Recommended literature.

1. Risk management: a tool for improving Nuclear Power Plant performance, IAEA VIENNA, 2001, IAEA-TECDOC-1209, ISSN 1011-4289, April 2001, 88.

3. Mosleh A., et al "Procedures for treating Common Cause Failures in Safety and Reliability Studies. Analytical Background and Techniques (NUREG/CR-4780 ERPI NP-5613 Vol.2)", 2000, 88.

4. International Electrotechnical Commission (IEC), IEC 61511, "Functional Safety: Safety Instrumented Systems for the Process Sector", Geneva, Switzerland (2003).

5. Schellhorn G., Thums A. "Formal fault tree semantics" (paper presented at the Sixth World Conference on Integrated Design & Process Technology, Pasadena, CA, 2002).

6. Rausand M. System analysis. Event tree Analysis. System reliability Theory (2nd edition), Wiley, 2004-26/28.

7. Bowles JB. "An assessment of PRN prioritization in a failure modes effects and criticality analysis", Journa1 of the IEST, 2004:47:51-6.

8. Mohammed J. Wadi Reliability Evaluation in Smart Grids via Modified Monte Carlo Simulation Method/ 7th International Conference on Renewable Energy Research and Applications (ICRERA), 2018

9. Ashwani M., Rakesh G. Calculating Grid Reliability in Bayesian Networks International Journal of Computer Science and technology Issue 4, 2012, 854-857 pp.

Laboratory work 1

Dr., Assoc. Prof. M. O. Kolisnyk (KhAI)

DEPENDABILITY ASSESSMENT OF SMART GRID SYSTEMS

Objectives: to study and apply the Markov models method for the Smart Grid (SG) systems assessment of dependability.

The aim of the training: Research of the availability function of the Smart Grid systems using the mathematical apparatus of Markov models.

Learning tasks:

– to research the Markov models method for dependability assessment for SG systems;

– to research, how transition rates values of Markov model of SG system functioning change availability function of SG system.

Practical tasks:

- to assess the availability function of SG system for different variants;
- to build graphical dependences of availability function on change the transition rate and to make an analysis of values of availability function and give practical recommendations for reach high value of availability function of SG.

Theoretical information

When organizing SG system, it is necessary to take into account the security, reliability of software and hardware of SG components and their energy consumption modes [1,2]. Availability is one of the impotent properties of dependability. The Markov model in fig. 5.7 describes the states of SG taking into account the attack on the system and the various power modes of the server and the router. The Markov availability model reflects the considering faults and failures of the hardware and software components of the server and router, as the SG subsystems. Also, the model takes into account the impact of cyber-attacks (special attacks and denial-of-service attacks), the transition of the server and the router in several modes of energy consumption.

Assumptions taken to construct and research the SG availability model:

- assume a Poisson flow of failure distribution of hardware and software of the SG components. This assumption allows to use the apparatus of Markov random processes for estimate availability;

- the means of control and diagnostics, as well as the means of switching to backup units, are considered ideal (they correctly identify the failed units and perform the switching to serviceable ones).

- the process, which occurs in the system, it is a process without aftereffect, every time in the future behavior of the system depends only on the state of the system at this time and does not depend on how the system arrived at that state. Therefore, the process has the Markov property.

The availability function is defined as the sum of the probabilities of a system in a good working state.

Then, according to the graph, a system of linear differential equations is compiled and initial conditions and normalization conditions are specified.

Initial conditions to resolve the system of Kolmogorov-Chapman differential linear equations for the Markov model (fig. 5.7):

$$\sum_{i=1}^{22} Pi(t) = 1; P1(0) = 1. \tag{1}$$

To assess the SG availability with the conditions of external factors, such as various attacks on the router, the availability factor AC was chosen, the value of which for SG systems is defined as the sum of the probabilities of such systems being in good working states:

$$AC=P\,1(t)+P\,2(t)+P\,3(t)+P\,4(t)+P\,5(t)+P\,12(t)+P\,13(t)+ P15(t)+P\,16(t)+P\,21(t).$$

Theoretical material for SG systems are described in Part 34 of the book [3].

Execution order

The transition rates are shown in the graph (Fig. 5.7): λij, μij - the transition rates, αij - the attack rates, γij - the transition rates in different modes of power consumption of the router and the server, where i = 1 ... 22, j = 1 ... 22), which depend on the time of occurrence of events.

A Markov model of SG subsystems functioning, represented in fig. 53, considering DDoS attacks and energy modes of server and router, which has the following states: Good-working state (1); State when the server is fully used with high power consumption S0 (2); State when the server is fully used, the hardware, that are not used, can enter the low-power mode S1 (3); State of the server sleep mode with low power consumption, a computer can wake up from a keyboard input, a local access network or universal serial bus device S2 (4); State when power consumption of server is reduced to the lowest level S3 (5); State of server failure (6); State of switching to the backup server device after the server failure (7); State of restarting the server software after the software fault (8); Successful DDoS-attack on the server after the firewall failure (9); State of firewall software or hardware failure (10); Attack on the power supply system after the firewall failure, that lead the failure of general power system of IoT system (11); State of switching from the general power system after its failure on the alternative energy sources (solar, diesel generator, wind turbine) (12); Router Status Active - sending packages with high power consumption (13); successful DDoS-attack on the router (14); Good-working state of the router without transmitting packets - Normal Idle (15); Good-working state of the router without packet transmission Low-Power Idle (16); Router software or hardware failure (17); State of server software or hardware fault (18); State when router hardware or software fault (20); State of switching to the backup router device after the router failure (21); State of restarting the router software after its fault (22).

For the proposed model, we compose a system of Kolmogorov-Chapman differential linear equations.

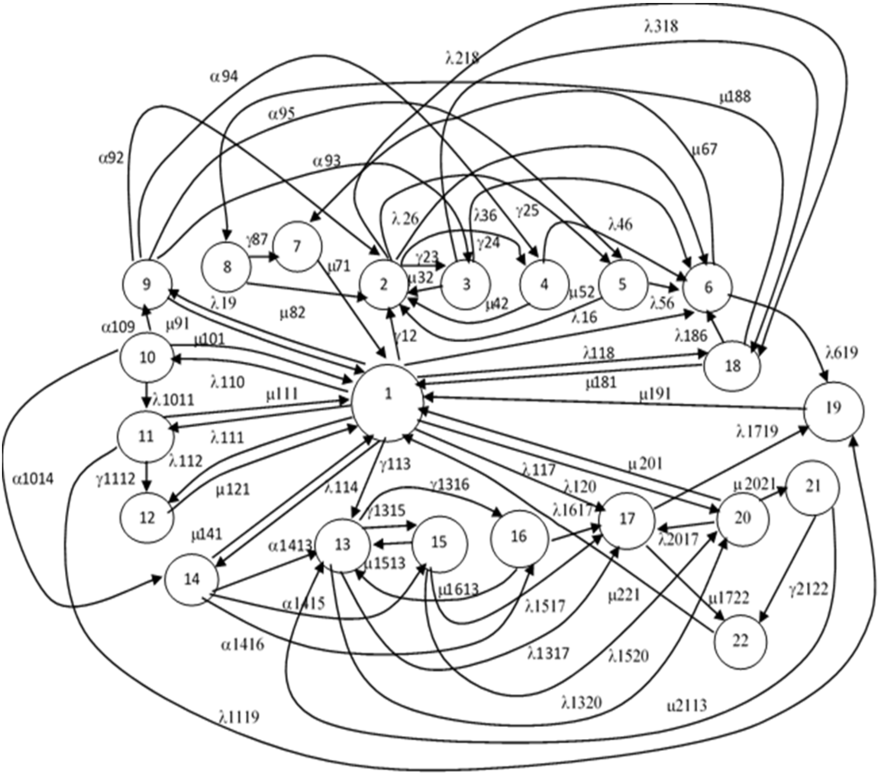


Fig. 53 – State graph of Markov model of SG functioning

$$\frac{dP1(t)}{dt} = \mu 71 \cdot P7(t) + \mu 91 \cdot P9(t) + \mu 101 \cdot P10(t) +$$
$$+\mu 111 \cdot P11(t) + \mu 121 \cdot P12(t) + \mu 141 \cdot P14(t) + \mu 181 \cdot P18(t) + \mu 191 \cdot P19(t) + \mu 201 \cdot P20(t) + \mu 221 \cdot P22(t) - P1(t) \cdot (\lambda 16 + \gamma 12 + \lambda 118 + \lambda 19 + \lambda 110 + \lambda 111 + \lambda 112 + \lambda 113 + \lambda 114 + \lambda 117 + \lambda 120)$$

$$\frac{dP2(t)}{dt} = \gamma 12 \cdot P1(t) + \mu 82 \cdot P8(t) + \alpha 92 \cdot P9(t) + \mu 32 \cdot P3(t) + \mu 42 \cdot P4(t) + \mu 52 \cdot P5(t) - P2(t) \cdot (\lambda 26 + \gamma 23 + \lambda 218 + \gamma 25 + \gamma 24);$$

$$\frac{dP3(t)}{dt} = \gamma 12 \cdot P1(t) + \alpha 93 \cdot P9(t) - P3(t) \cdot (\lambda 36 + \mu 32 + \lambda 318);$$

$$\frac{dP4(t)}{dt} = \gamma 24 \cdot P2(t) + \alpha 94 \cdot P9(t) - P4(t) \cdot (\lambda 46 + \mu 42);$$

$$\frac{dP5(t)}{dt} = \gamma 25 \cdot P2(t) + \alpha 95 \cdot P9(t) - P5(t) \cdot (\lambda 56 + \mu 52);$$

$$\begin{aligned}\frac{dP6(t)}{dt} = {} & \lambda 56 \cdot P5(t) + \lambda 46 \cdot P4(t) + \lambda 26 \cdot P2(t) + \lambda 16 \cdot P1(t) \\ & + \lambda 186 \cdot P18(t) + \lambda 36 \cdot P3(t) \\ & - P6(t) \cdot (\lambda 619 + \mu 67);\end{aligned}$$

$$\frac{dP7(t)}{dt} = \gamma 87 \cdot P8(t) + \mu 67 \cdot P6(t) - \mu 71 \cdot P7(t);$$

$$\frac{dP8(t)}{dt} = \mu 188 \cdot P18(t) - P8(t) \cdot (\gamma 87 + \mu 82);$$

$$\begin{aligned}\frac{dP9(t)}{dt} = {} & \alpha 109 \cdot P10(t) + \lambda 19 \cdot P1(t) \\ & - P9(t) \cdot (\alpha 92 + \alpha 93 + \mu 91 + \alpha 94 + \alpha 95);\end{aligned}$$

$$\begin{aligned}\frac{dP10(t)}{dt} = {} & \lambda 110 \cdot P1(t) \\ & - P10(t) \cdot (\alpha 109 + \alpha 1014 + \mu 101 + \lambda 1011);\end{aligned}$$

$$\begin{aligned}\frac{dP11(t)}{dt} = {} & \lambda 111 \cdot P1(t) + \lambda 1011 \cdot P10(t) \\ & - P11(t) \cdot (\gamma 1112 + \mu 111 + \lambda 1119);\end{aligned}$$

$$\frac{dP12(t)}{dt} = \gamma 1112 \cdot P11(t) + \lambda 112 \cdot P1(t) - \mu 121 \cdot P12(t);$$

$$\begin{aligned}\frac{dP13(t)}{dt} = {} & \gamma 113 \cdot P1(t) + \mu 1513 \cdot P15(t) + \alpha 1413 \cdot P14(t) \\ & + \alpha 2113 \cdot P21(t) + \mu 1613 \cdot P16(t) \\ & - P13(t) \cdot (\lambda 1320 + \lambda 1317 + \gamma 1315 + \gamma 1316);\end{aligned}$$

$$\begin{aligned}\frac{dP14(t)}{dt} = {} & \alpha 1014 \cdot P10(t) + \lambda 114 \cdot P1(t) \\ & - P14(t) \cdot (\alpha 1415 + \alpha 1416 + \mu 141 + \alpha 1413);\end{aligned}$$

$$\begin{aligned}\frac{dP15(t)}{dt} = {} & \alpha 1415 \cdot P14(t) + \gamma 1315 \cdot P13(t) \\ & - P15(t) \cdot (\lambda 1520 + \mu 1513 + \lambda 1517);\end{aligned}$$

$$\begin{aligned}\frac{dP16(t)}{dt} = {} & \alpha 1416 \cdot P14(t) + \gamma 1316 \cdot P13(t) \\ & - P16(t) \cdot (\mu 1613 + \lambda 1617);\end{aligned}$$

$$\frac{dP17(t)}{dt} = \lambda117 \cdot P1(t) + \lambda1617 \cdot P16(t) + \lambda1517 \cdot P15(t) + \lambda2017 \cdot P20(t) - P17(t) \cdot (\lambda1719 + \mu1722);$$

$$\frac{dP18(t)}{dt} = \lambda118 \cdot P1(t) + \lambda218 \cdot P2(t) + \lambda318 \cdot P3(t) - P18(t) \cdot (\lambda186 + \mu188 + \mu181);$$

$$\frac{dP19(t)}{dt} = \lambda1719 \cdot P17(t) + \lambda619 \cdot P6(t) + \lambda1119 \cdot P11(t) - \mu191 \cdot P19(t);$$

$$\frac{dP20(t)}{dt} = \lambda120 \cdot P1(t) + \lambda1520 \cdot P15(t) + \lambda1320 \cdot P13(t) - P20(t) \cdot (\lambda2017 + \mu2021 + \mu201);$$

$$\frac{dP21(t)}{dt} = \mu2021 \cdot P20(t) - P21(t) \cdot (\gamma2122 + \alpha2113);$$

$$\frac{dP22(t)}{dt} = \mu1722 \cdot P17(t) + \gamma2122 \cdot P21(t) - \mu221 \cdot P22(t).$$

$$\sum_{i=1}^{22} Pi(t) = 1; P1(0) = 1.$$

An example of a graphical dependence that students should receive and analyze is shown in the figure 54. Initial data for calculation the AC presented in the table 5.

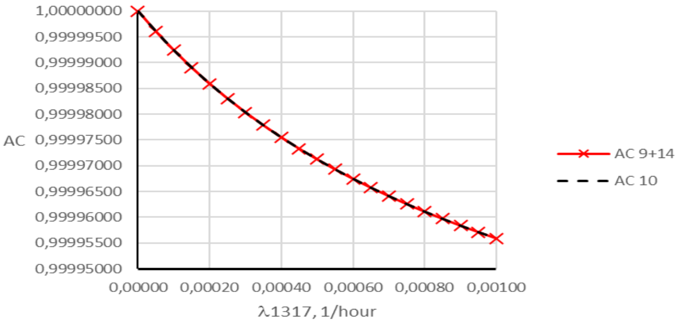


Fig. 54 - Graph of dependence of SBC AC on the transition rate λ1317 from active-power state of the router 13 to a state of the router failure 17 for the model if λ1317 change values in range 0...10^{-3} 1/h

Table 5 – Initial data for calculation the AC

Transition rate	Value	Transition rate	Value
γ12	10000000,000000000000	λ1317	0,000570776256
γ113	10000000,000000000000	λ1517	0,000010000000
γ23	0,208000000000	λ1617	0,000001000000
γ24	0,230000000000	λ218	0,000010000000
γ25	0,130000000000	λ318	0,000010000000
γ1315	0,420000000000	λ1320	0,000001000000
γ1316	0,210000000000	λ1520	0,000001000000
γ1112	0,200000000000	λ2017	0,001141552511
γ87	2,000000000000	λ120	0,000001000000
γ2122	2,000000000000	μ67	60,000000000000
α1014	0,002283105023	μ141	0,125000000000
α109	0,009740000000	μ111	0,500000000000
α92	0,002435000000	μ32	40,000000000000
α93	0,002435000000	μ42	30,000000000000
α94	0,002435000000	μ52	30,000000000000
α95	0,002435000000	μ1513	50,000000000000
α1413	0,000761035008	μ1613	60,000000000000
α1415	0,000761035008	μ71	0,020830000000
α1416	0,000761035008	μ87	2,000000000000

λ114	0,000001000000	μ81	30,000000000000
λ110	0,000114000000	μ101	1,000000000000
λ112	0,000022831050	μ121	5,000000000000
λ19	0,000001000000	μ181	1,000000000000
λ118	0,000000100000	μ191	0,020833333333
λ1011	0,000570776256	μ91	1,000000000000
λ16	0,000001000000	μ171	1,000000000000
λ196	0,002430000000	μ188	60,000000000000
λ1719	0,000230000000	μ61	0,020833333333
λ619	0,000010000000	μ2021	60,000000000000
λ111	0,000076103501	μ221	20,000000000000
λ1119	0,000228310502	μ211	30,000000000000
λ117	0,000000100000	μ1722	60,000000000000
λ186	0,001141552511	μ201	40,000000000000
λ26	0,002283105023	μ2113	20,000000000000
λ36	0,000100000000	λ56	0,000010000000
λ46	0,000010000000		

1. In laboratory work, students must for the model proposed in Fig. 1 to find the value of the AC using either a program written for this in one of the programming languages or one of the mathematical programs MS Excel, Mathcad, Matlab, SMathSudio.

2. For the values of the transition rate, specified in the Table 6 for the variants, construct graphical dependences of the AC on the change in the value of the transition rate.

AC = f(λ_{ij}).

3. Students should receive 5 graphical dependencies in a query and analyze which transition rates and at what values most strongly affect the value of the availability function.

4. Results of research and conclusions.

5. Students must to give practical recommendations.

Table 6 – Variants of transition rates of the Markov model

№	Transition rates values

1	λ114 = 0...0.01; μ101 = 0...15; λ218 = 0...0.01;
	λ619 = 0...0.001; μ61 = 0...5

2	λ19 = 0...0.01; μ1513 = 0...15; λ112 = 0...0.01; λ56 = 0...0.001; μ101 = 0...5
3	λ1011 = 0...0.01; μ91 = 0...15; λ318 = 0...0.01; λ171= 0...0.001; μ61 = 0...5

4	λ1719 = 0...0.01; μ191 = 0...15; λ1520 = 0...0.01;
	λ1317 = 0...0.001; μ211 = 0...5

5	λ117 = 0...0.01; μ201 = 0...50; λ56 = 0...0.01; λ112 = 0...0.001; μ188 = 0...5
6	λ114 = 0...0.01; μ101 = 0...20; λ218 = 0...0.01; λ619 = 0...0.001 ; μ2113 = 0...5
7	λ186 = 0...0.01; μ101 = 0...15; λ36 = 0...0.01; λ114 = 0...0.001; μ61 = 0...5
8	λ114 = 0...0.01; μ221 = 0...50; λ118 = 0...0.01; λ23 = 0...0.001; μ87 = 0...5

9	λ112 = 0...0.01; μ2021 = 0...70; λ218 = 0...0.01;
	λ1119 = 0...0.001; μ91 = 0...5

10	λ1517 = 0...0.01; μ71 = 0...15; λ111 = 0...0.01; λ46 = 0...0.001; μ121 = 0...5

Requirements to the content of the report

The report should include:

- title page;
- research purpose and program;
- graph of the Markov model;
- results of AC assessment;

- analysis of assessment results and conclusions;
- practical recommendations.

Testing questions

1. Please explain how you can calculate the availability function for the Smart Grid system using the mathematical apparatus of Markov models?

2. What are the main methods of SG reliability assessment do you know?

3. What are the main indicators of the reliability of Smart Grid systems, which can be determined using the mathematical apparatus of Markov models?

4. What components have the SG network and how consider their reliability in the Markov model?

5. What mathematical apparatus for SG systems reliability assessment do you know?

6. What assumptions must to have failures stream for use the Markov models apparatus for reliability assessment?

References

1. Maryna Kolisnyk, Vyacheslav Kharchenko, Iryna Piskachova, Nikolaos Bardis. A Markov model of IoT system availability considering DDoS attacks and energy modes of server and router. ICTERI 2017. 14 p. [http://ceur-ws.org/Vol-1844/10000699.pdf].

2. Kharchenko Vyacheslav, Kolisnyk Maryna, Piskachova Iryna. Reliability and Security Issues for IoT-Based Smart Business Center: Architecture and Markov Model. IEEE; Computer of science, MCSI 2016, Greece, Chania, 2016. Paper ID: 4564699.

3. 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. – 740 p.

ITM1.4. IoT for smart grid safety and security management

DrS, Prof. Brezhniev E.V. (KhAI)

Training 1

APPLICATION OF STAMP METHOD FOR SMART GRID SAFETY/SECURITY ACCIDENT ANALYSIS

The aim of the training: The purpose of the training is to obtain the basic skills of applying models for analyzing of safety/security accidents related to IoT based smart grid and systems.

Learning tasks:

– study of basic theoretical information about the methods and approaches used in the analysis of safety/security accidents of complex IoT based smart grid and systems;

– analysis of the causes of accidents and incidents, the formation of proposals for their prevention and risk reduction.

Practical tasks:

– gaining skills in the practical analysis of safety/security accidents using System-Theoretic Accident Model and Processes (STAMP) method;

– development of soft skills for public presentation of work results.

Theoretical information

Traditional system safety approaches are being challenged by the introduction of new technology and the increasing complexity of the systems we are attempting to build. STAMP is a new system thinking approach to engineering safer systems described in [1, 2]. While relatively new, it is already being used in space, aviation, medical, defense, nuclear, automotive, and other sectors.

STAMP is an accident causality model based on systems theory and systems thinking and was originally developed by Prof. Dr. Nancy Leveson at MIT. STAMP integrates into engineering analysis causal factors such as software, human decision-making and human factors, new technology, social and organizational design, and safety culture, which are becoming ever more threatening in our increasingly complex systems. It expands traditional models [3, 4] that focus on individual component failures or chains of directly-related failure events to include more complex processes and unsafe interactions among system components. Safety is treated as a dynamic control problem rather than a «prevent failure» problem. The STAMP model includes traditional component failures but also considers design flaws, incomplete or inadequate requirements, dysfunctional interactions among subsystems or components (all of which may be operating exactly as specified), human interactions, and other causes of accidents and incidents. With STAMP, the emphasis changes from simply preventing failures to enforcing constraints on system behavior and interactions.

Traditional system safety approaches [5 - 7], which started in the missile defense systems of the 1950s, are being challenged by the introduction of new technology and the increasing complexity of the systems we are attempting to build. Software is changing the causes of accidents and the humans operating these systems have a much more difficult job than simply following predefined procedures. We can no longer effectively separate engineering design from human factors and from the social and organizational system in which our systems are designed and operated.

Some advantages of using STAMP are that:

– It works on very complex systems because it works top-down rather than bottom up.

– It works extremely well for software-intensive systems (like autonomous self-driving cars and UAS) and human interactions

– It also applies to management, organizations, safety culture, etc. without having to treat them differently or separately.

– It allows creating more powerful tools, such as STPA (hazard analysis), safety-guided design, CAST (analyzing previous accidents), identification and management of leading indicators of increasing risk, organizational risk analysis, etc.

STAMP and STAMP-based methods have become incredibly popular and the demand for qualified experts and training has become overwhelming. STAMP Safety and Security Consulting (S3C) was created in response to the increasing demand to provide industry support, guidance, training, and facilitation for organizations who are adopting or exploring STAMP.

Popular Services:

– Training in STAMP, CAST (accident analysis), STPA (hazard analysis), and other STAMP-based techniques.

– Hands-on workshops.

– Ongoing support for STAMP-based techniques applied to real projects.

– Expert facilitation and guidance.

– Preliminary exploration and evaluation of STAMP-based techniques in your domain.

– Support for pilot-studies and comparisons to existing processes.

– Integration of STAMP-based techniques into overall engineering processes, operations, and policies.

– Webinars.

Industries where STAMP-based approaches are being used:

– Automotive (autonomous self-driving cars, driver assistance systems, etc.);

– Aircraft systems and equipment (military, commercial, UAVs, etc.);

– Airline operations;

– Manufacturing;

– Oil & Gas;

– Chemical;

– Nuclear power;

– Space systems;

– Military and Defense;

– Healthcare;

– Medical devices;

– Robotics;

– Mining;

– Healthcare and patient safety;

– Workplace safety;

– Cyber Security.

STAMP uses three fundamental concepts from system theory: Emergence and hierarchy, Communication and control, and Process models. Detailed instruction for them is described below. The following table 7 lists the foundations of STAMP, which are called new assumptions. For comparison, it also lists the corresponding assumptions of traditional hazard analysis methods, which are called old assumptions.

Table 7 - Foundations of STAMP

Old Assumption	New Assumption
Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur.	High reliability is neither necessary nor enough for safety.
Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chains of events leading to the loss.	Accidents are complex processes involving the entire socio-technical system. Traditional event-chain models cannot describe this process adequately.
Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.	Safety may be best understood and communicated in ways other than probabilistic risk analysis.
Most accidents are caused by operator error. Rewarding safe behavior and punishing unsafe behavior will eliminate or reduce accidents significantly.	Operator error is a product of the environment in which it occurs. To reduce operator error, we must change the environment in which the operator works.
Highly reliable software is safe.	Highly reliable software is not necessarily safe. Increasing software reliability will have only minimal impact on safety.
Major accidents occur from the chance simultaneous occurrence of random events.	Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk.
Assigning blame is necessary to learn from and prevent accidents or incidents.	Blame is the enemy of safety. Focus should be on understanding how the system behavior contributed to the loss and not on who or what to blame for it.

Emergence and Hierarchy

The concept of emergence means that at a given level of complexity, some properties of that level (emergent at that level) are irreducible. Safety is clearly an emergent property of systems because safety can only be determined in the context of the whole. Statements about safety without the context information are meaningless. Hierarchy theory describes the relationships between different levels, including what generates the levels, what separates them, and what links them. In STAMP, safety is treated as an emergent property at each of these hierarchy levels that arise when the system components interact within an environment. It depends on the enforcement of constraints on the behavior of the components in the system, including constraints on their potential interactions.

Communication and Control

Control processes mostly operate at the interfaces between two hierarchy levels and always are related with the imposition of constraints. STAMP uses the concept of imposing constraints in system behavior to avoid unsafe events or conditions rather than focusing on avoiding individual component failures. Between the hierarchical levels of each safety control structure, effective communication channels are needed during the control processes. There are two kinds of communication channels as shown in Fig. 55. A downward reference channel provides the information necessary to impose safety constraints on the level below. An upward measuring channel provides feedback about how effectively the constraints are being satisfied. Communication also determines whether the control processes could be established or achieve the expected goals. Typical control processes often use feedback loops to keep interrelated components in a state of dynamic equilibrium. A standard control loop is shown in Fig. 65. According to Fig. 56, four conditions are required to establish control processes:

– Goal Condition: The controller must have a goal or goals (for example, to maintain the set point).

– Action Condition: The controller must be able to affect the state of the system. In engineering, control actions are implemented by actuators.

– Model Condition: The controller must be (or contain) a model of the system. It will be discussed in the following part of process model.

– Observability Condition: The controller must be able to ascertain the state of the system. In engineering terminology, observation of the state of the system is provided by sensors. In STAMP, goal condition is the safety constraints that must be enforced by each controller in the hierarchical safety control structure. The action condition is implemented in the downward control channels and the observability condition is embodied in the upward feedback or measuring channels.

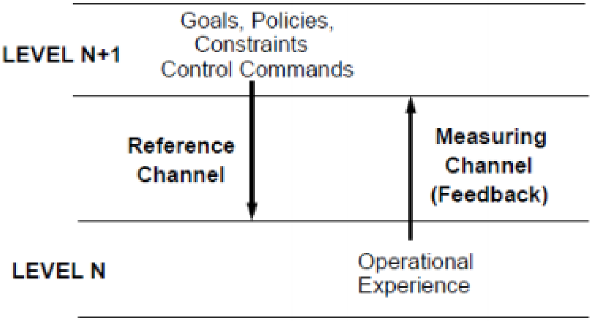


Fig. 55 - Communication Channels between Control Levels

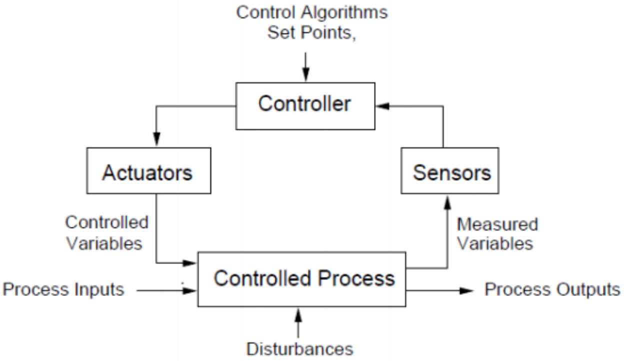


Fig. 56 - A standard control loop

Process Model

Process model is a concept in control theory. The reason why it is discussed individually here is just because it is an essential concept of STAMP. The four conditions required to control a process are already provided above. The most important condition is the model condition. It means that any controller, no matter human or automated, needs a model of the process being controlled to control it effectively. The purpose of using process model is to determine what control actions are needed based on knowing the current state of the controlled process and to estimate the effect of various control actions on that state. For software controller, process model refers to software logic, which can be called logic model. A simple general process model is shown in Figure 57.

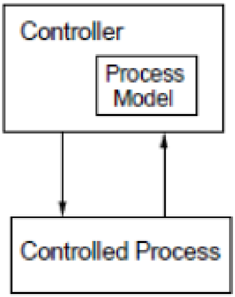


Fig. 57 - A general process model

The process model could be very simple with only a few variables or very complex with many state variables. If the process model does not match the process, that could result in four different kinds of problems, each of which could lead to an accident. This is especially true for component interaction accidents. In summary, this systemic approach considers accidents not only arising from component failures, but also from the interactions among system components. It usually does not specify single causal variables for factors. Emergent properties like safety are controlled or enforced by a set of constraints (control laws) related to the behavior of the system components. Safety then can be viewed as a control problem.

When control processes provide inadequate control and the safety constraints are violated in the behavior of the lower level processes, accidents occur. In other words, accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled by the control system.

During its lifecycle any systems might have accidents. There are four STAMP-based Analysis Processes which are used during a system lifecycle (see Table 8).

Table 8 - STAMP-based Processes to perform Model-based Analysis Processes

STPA	Systems theoretic process analysis	Hazard-analysis
CAST	Casual analysis based on STPA	Accident / Event analysis
STPA-Sec.	Systems theoretic process analysis - Security	“Hazard” Analysis-Security focused
STECA	Systems theoretic early concept analysis	Safety-Guided Design / Hazard Identification

Each of these models/processes might be used during particular cycles to decrease a probability of accident (see Fig. 58).

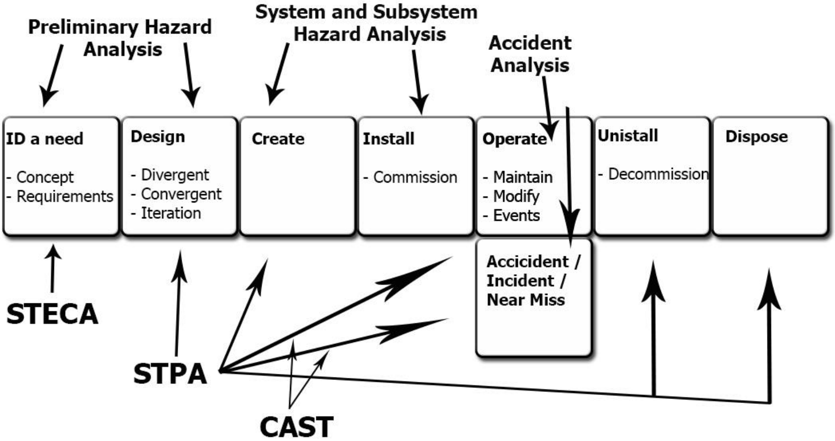


Fig. 58 - System Lifecycle and Processes to be used

The main stages of STAMP-based Analysis of the accident

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur because:

a. A control action required for safety is not provided or not followed.

b. An unsafe control action is provided.

c. A potentially safe control action is provided too early or too late; that is, at the wrong time or in the wrong sequence.

d. A control action required for safety is stopped too soon or applied too long.

2. Determine how each potentially hazardous control action identified in step 1 could occur.

a. For each unsafe control action, examine the parts of the control loop to see if they could cause it. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.

b. Consider how the designed controls could degrade over time and build in protection, including:

i. Management of change procedures to ensure safety constraints are enforced in planned changes.

ii. Performance audits where the assumptions underlying the hazard analysis are the preconditions for the operational audits and controls so that unplanned changes that violate the safety constraints can be detected.

iii. Accident and incident analysis to trace anomalies to the hazards and to the system design.

STAMP is designed to determine ways in which the human controller, in addition to the automated controller, may have a flawed process model. If humans tasked with supervising an automated process receive active indication of a system failure or otherwise suspect that a failure has occurred, they may resort to responding with experimentation in the absence of adequate training and procedural guidance. Additionally, process models embedded in automated controllers are typically static in nature. It is most often up to the human controller to manage any environmental cues that are unknown to the automated controller’s process model and adjust the controlled process as necessary [8 – 10]. Without proper understanding of the automated controller’s process model and associated algorithms, the human supervisor may take insufficient or incorrect action when intervening to direct the previously automated process. Fig. 59 depicts the importance of including human controllers within the bounds of a STAMP.

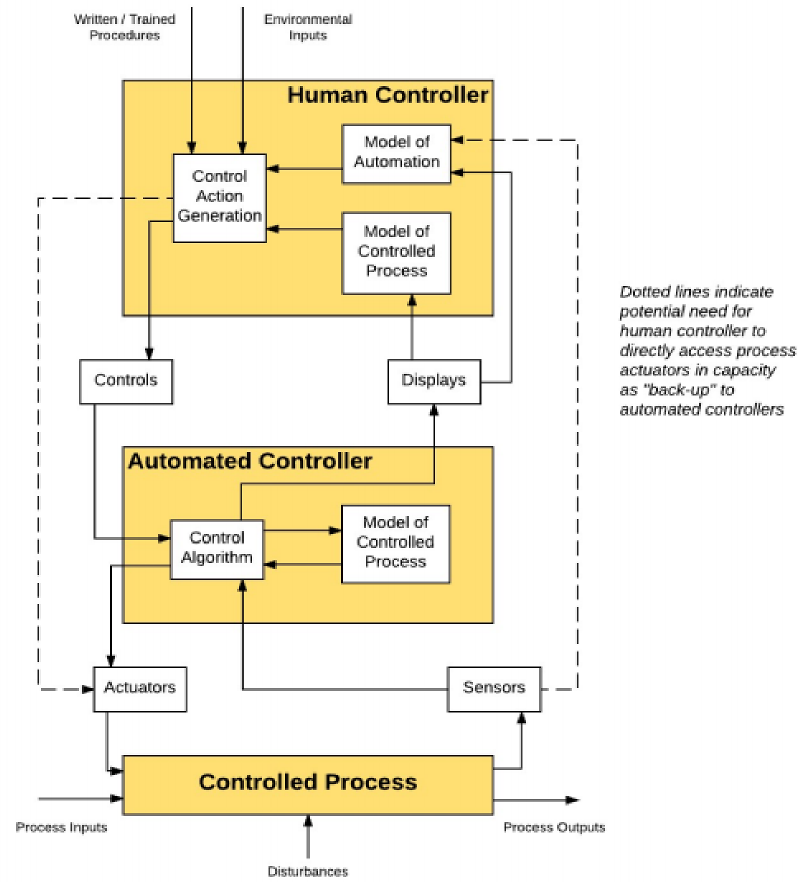

Written / Trained Procedures
Environmental Inputs
Human Controller
Model of Automation
Control Action Generation
Model of Controlled Process
Controls
Displays
Dotted lines indicate potential need for human controller to directly access process actuators in capacity as "back-up" to automated controllers
Automated Controller
Control Algorithm
Model of Controlled Process
Actuators
Sensors
Controlled Process
Process Inputs
Process Outputs
Disturbances

Fig. 59 - General Form of a Model of Socio-Technical Control

Report requirements.

1. Report language is English.
2. The report should include:

- a title page with information about the author, the name of the discipline, analysis topics, option, teacher, university and department logos;

- content;

- Section 1 - a related and understandable description of the STAMP method used. Pictures and diagrams detailing this description, are welcomed;

- Section 2 - a brief description of the accident, analysis of the accident using the method used (for the variant see Table 9);

- Section 3 - recommendations on how the accident could be avoided.

3. The report is sent in two formats (doc and pdf) to the teacher's e-mail.

A presentation shall be prepared to defend the results. The presentation should include:

1. The title page.
2. The content of the presentation.
3. Description of the accident.
4. Analysis of the accident (incident) using STAMP method.
5. Proposals to reduce the risks of such accidents in the future.
6. Conclusions.

The training is considered to be completed after the defense of the presentation by each student individually.

Presentation time is up to 7 minutes. English language. Language of presentation is one out of English, Ukrainian, Russian. Use of English is encouraged.

Table 9 – Students' tasks

№	Accident	Reference of accidents
1.	Cyber attack on Ukrainian power grid 2015	https://ru.tsn.ua/ukrayina/pravitelstvo-ssha-oficialno-priznalo-chto-ataki-na-ukrainskie-oblenergo-sovershili-hakery-587599.html
2.	Saudi Aramco	https://www.risidata.com/Database/P30
3.	Wanna Cry	

№	Accident	Reference of accidents
4.	Petya	https://www.risidata.com/Database/P30
5.	London August 2003 Power Blackout	https://www.risidata.com/Database/P30
6.	Russian-Based Dragonfly Group Attacks Energy Industry	https://www.risidata.com/Database/P30
7.	SCADA Workstation Infected by W32/Korgo Worm	https://www.risidata.com/Database/P30
8.	Trojan Backdoor on Water SCADA System	https://www.risidata.com/Database/P30
9.	Worm attack on Drilling Control system	https://www.risidata.com/Database/P30
10.	Slammer Impact on Ohio Nuclear Plant	https://www.risidata.com/Database/P30
11.	Shamoon virus knocks out computers at Qatari gas firm RasGas	https://www.risidata.com/Database/P30

Test questions:

1. Why is the systematic approach to safety important?
2. What are the main differences between STAMP and other traditional methods for safety analysis?
3. Name the advantages of using STAMP?
4. Name the industries where STAMP-based approaches are being used?
5. What are the STAMP three basic concepts?
6. What are the STAMP stages?

Recommended literatures.

1. Leveson, Nancy G. (1995) Safeware: System Safety and Computers, Addison-Wesley.

2. Leveson, Nancy G. (2003) A New Accident Model for Engineering Safer Systems, to appear in Safety Science, Elsevier Science Ltd.

3. Dien, Y., Dechy, N. and Guillaume, E., 2012. Accident investigation: From searching direct causes to finding in-depth causes – problem of analysis or/and of analyst? Safety Science, 50(6), pp. 1398-1407.

4. Dutch Transport Safety Board, 2012. Experiences and challenges in using STAMP for accident analysis, First STAMP/STPA Workshop at MIT, April 2012, Massachusetts Institute of Technology.

5. Ferjencik, M., 2011. An integrated approach to the analysis of incident causes. Safety Science, 49(6), pp. 886-905.

6. Harris, D. and Li, W.-C., 2011. An extension of the human factors analysis and classification system for use in open systems. Theoretical Issues in Ergonomics Science, 12(2), pp. 108-128.

7. Hollnagel, E., 2004. Barriers and accident prevention. Aldershot: Ashgate Publishing Limited.

8. Hollnagel, E. and Goteman, Ö., 2004. The Functional Resonance Accident Model, Cognitive System Engineering in Process Control 2004, 4 - 5 Nov 2004, CSEPC, pp. 155-161.

9. Hollnagel, E., Pruchnicki, S., Woltjer, R. and Etcher, S., 2008. Analysis of Comair flight 5191 with the Functional Resonance Accident Model, Proceedings of 8th International Symposium of the Australian Aviation Psychology Association, 2008, Australian Aviation Psychology Association.

10. Hollnagel, E. and Speziali, J., 2008. Study on developments in accident investigation methods: A survey of the'state-of-the-art. SKI Report 2008:50. Sophia Antipolis, France: Ecole des Mines de Paris.

Training 2

ACCIDENT ROOT CAUSE ANALYSIS OF IOT BASED SMART GRID WITH FIVE WHYS METHOD

The aim of the training: The purpose of the training is to obtain the basic skills for root cause analysis of smart grid security accidents with application of 5Why method.

Learning tasks:

– study of basic theoretical information about the 5Why method which is used in the root cause analysis of security accidents of complex IoT based smart grid and systems;

– root cause analysis of the accidents and incidents, the formation of suggestions for prevention of accident and risk reduction.

Practical tasks:

– gaining the practical skills in the root cause analysis of security accidents using 5Why method;

– development of soft skills for public presentation of work results.

Theoretical information

Safety management is a function that enhances company performance by predicting operational, procedural or environmental risks and threats before they occur [1 – 3]. Safety management is a strategic process that identifies and addresses safety issues for employees and the company. Aside from being a pre-emptive and preventative process, safety management also corrects deficiencies and performance errors.

Incident investigation is a part of safety management [4]. The Incident investigation can be simple or complex depending upon the severity of the event. In principle, investigators would be trained to discover the facts, collect evidence, ascertain the root cause(s), and make recommendations in a written report. However, many investigators often seize on the first set of ‘symptoms’ as the Root Cause, rather than the Root Cause(s) themselves. This is why the same type(s) of incidents are often repeated.

Root Cause Analyses [5] helps you get to the 'bottom' of events to prevent recurrence. A Root Cause is the most basic cause (s) identified as contributing to an incident, and that is within peoples control to fix. A number of tried and tested methods are available to help identify these most' basic' causes. These include 'Influence & Causal Factor' Charting, the '5 Why's', 'Fishbone' or 'Ishikawa' Cause & Effect Diagrams and Applied Behavioral Analysis (ABA). Each of these methods is in widespread use throughout industry with their pedigrees going back to the early 1970's. BSMS trains investigators how to use each of these methods in various combinations to ensure all the angles have been covered.

Five Whys Method

Five Whys [6] is an iterative interrogative technique used to explore the cause-and-effect relationships underlying a particular problem. The primary goal of the technique is to determine the root cause of a defect or problem by repeating the question "Why?". Each answer forms the basis of the next question. The "5" in the name derives from an anecdotal observation on the number of iterations needed to resolve the problem (fig. 60).

Not all problems have a single root cause. If one wishes to uncover multiple root causes, the method must be repeated asking a different sequence of questions each time.

The method provides no hard and fast rules about what lines of questions to explore, or how long to continue the search for additional root causes. Thus, even when the method is closely followed, the outcome still depends upon the knowledge and persistence of the people involved.

The questioning could be taken further to a sixth, seventh, or higher level, but five iterations of asking why is generally sufficient to get to a root cause. The key is to encourage the trouble-shooter to avoid assumptions and logic traps and instead trace the chain of causality in direct increments from the effect through any layers of abstraction to a root cause that still has some connection to the original problem.

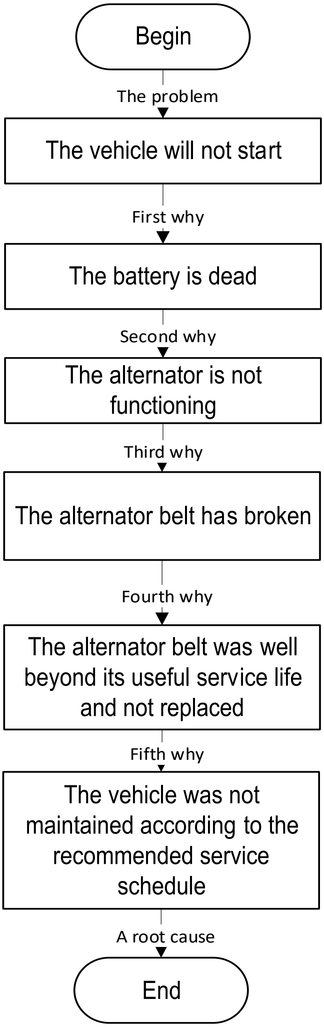

Begin
The problem
The vehicle will not start
First why
The battery is dead
Second why
The alternator is not functioning
Third why
The alternator belt has broken
Fourth why
The alternator belt was well beyond its useful service life and not replaced
Fifth why
The vehicle was not maintained according to the recommended service schedule
A root cause
End

Fig. 60 - An example of method Five Whys

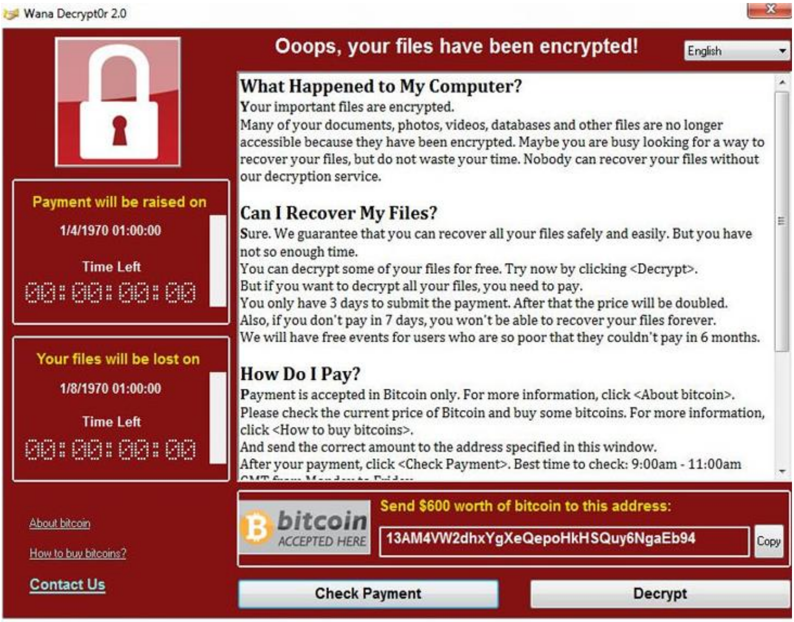
The last answer points to a process. This is one of the most important aspects in the 5 Why approach - the real root cause should point toward a process that is not working well or does not exist. Untrained facilitators will often observe that answers seem to point towards classical answers such as not enough time, not enough investments, or not enough manpower. These answers may be true, but they are out of our control. Therefore, instead of asking the question why? ask why did the process fail? A key phrase to keep in mind in any 5 Why exercise is "people do not fail, processes do".

Let’s consider the example of application of 5Why method for the WannaCry ransomware attack.

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.

Organizations that had not installed Microsoft's security update from April 2017 were affected by the attack. Those still running unsupported versions of Microsoft Windows, such as Windows XP and Windows Server 2003 were at particularly high risk because no security patches had been released since April 2014 (with the exception of one emergency patch released in May 2014). A Kaspersky Lab study reported however, that less than 0.1 percent of the affected computers were running Windows XP, and that 98 percent of the affected computers were running Windows 7. In a controlled testing environment, the cybersecurity firm Kryptos Logic found that they were unable to infect a Windows XP system with WannaCry using just the exploits, as the payload failed to load, or caused the operating system to crash rather than actually execute and encrypt files. However, when executed manually, WannaCry could still operate on Windows XP.



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Fig. 61 - Window Wanna Decrypt0r 2.0

As mentioned above, to obtain the root cause of a problem, it is necessary to correctly formulate both the problem itself and the five “why” questions.

Look into Loss of personal data problem.

1. Why? The computer infected with WannaCry.
2. Why? The exploit Eternal Blue implemented using a backdoor Double Pulsar.
3. Why? Port 445 opened to use the vulnerable SMB protocol.
4. Why? A vulnerable version of Windows installed on the computer.
5. Why? The user did not update the OS or used an unsupported version of Windows.

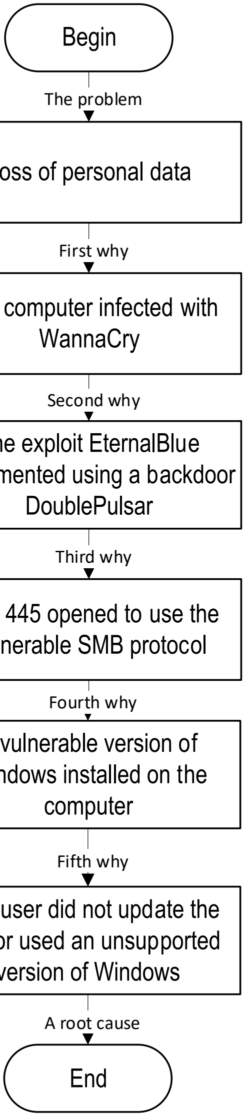

Begin
The problem
Loss of personal data
First why
The computer infected with WannaCry
Second why
The exploit EternalBlue implemented using a backdoor DoublePulsar
Third why
Port 445 opened to use the vulnerable SMB protocol
Fourth why
A vulnerable version of Windows installed on the computer
Fifth why
The user did not update the OS or used an unsupported version of Windows
A root cause
End

Fig. 62 - Using method Five Whys for analysis WannaCry

As a result of the analysis, it was found that the root cause was the use of the majority of affected users of the vulnerable version of Windows.

Report requirement.

1. Report language is English.

2. The report should include:

- a title page with information about the author, the name of the discipline, analysis topics, option, teacher, university and department logos;
- content;
- Section 1 – an algorithm of the 5 Why method.
- Section 2 - a brief description of the accident, analysis of the accident as per students' variants (for the variant see Table 10);
- conclusion and recommendations.

3. The report is sent in two formats (dock and pdf) to the teacher's e-mail.

A presentation shall be prepared to defend the results. The presentation should include:

1. The title page.
2. The content of the presentation.
3. Description of the accident.
4. Analysis of the accident.
5. Proposals to reduce the risks of such accidents in the future.
6. Conclusions.

The training is considered to be completed after the defense of the presentation by each student individually.

Presentation time is up to 10 minutes. Language of presentation is one out of English, Ukrainian, Russian.

Table 10 – Students' tasks

№	Name of accident	Year	Reference
1.	Wolf Creek Nuclear Plant Cyberattack	017	https://www.theenergytimes.com/cybersecurity/wolf-creek-nuclear-plant-hit-cyberattack
2.	Ukraine power grid cyber attack	015	https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/
3.	Russian-Based Dragonfly Group Attacks Energy Industry	2014	http://www.itbusinessedge.com/blogs/data-security/russian-based-dragonfly-group-attacks-energy-industry.html
4.	German Steel Mill Cyber Attack	2014	http://www.risidata.com/Database
5.	Public utility compromised after brute-force hack attack, says Homeland Security	2014	http://www.navigo.su/index.php?option=com_content&view=article&id=100:2009-10-26-08-37-21&catid=51:2009-09-27-11-41-45&Itemid=86
6.	U-2 spy plane caused widespread shutdown of U.S. flights	2014	http://www.reuters.com/article/us-usa-airport-losangeles-idUSBREA420AF20140503
7.	Iranian Oil Terminal offline after malware attack	2012	http://www.bbc.com/news/technology-17811565
8.	Hackers Attack NZ & Aust for Joining Gulf Taskforce	1998	http://www.risidata.com/Database

9.	Slammer Infected LaptopShutsDownDCS	2003	http://www.risidata.com/Database/Detail/slammer-infected-laptop-shuts-down-dcs
10.	Reverse Osmosis System PLC Attacked	2002	http://www.risidata.com/Database/Detail/reverse-osmosis-system-plc-attacked

Test questions:

1. What is meant by Root Cause Analysis?
2. Why is it important in Safety Management?
3. Name the main stages of Five Why Methods?
4. What are main benefits and disadvantages of 5 Why method?
5. Does 5 Why take into account a dynamical nature of problem? Give an example.

References.

1. Safety Management Manual, International Civil Aviation Organization Third Edition, 2013, University Street, Montréal, Quebec, Canada H3C 5H7, 251 p.

2. Floyde A., Lawson G., Shalloe S., Eastgate R., D'Cruz, M. The design and implementation of knowledge management systems and e-learning for improved occupational health and safety in SMEs, Safety Science, # 60, 2013, pp. 69–76.

3. Gerbec, M., Balfe, N., Leva M.C. Prast S. Risk assessment and optimization for rare, new or complex processes: Combining task analysis, 4D process simulation, hazard analysis and optimization. Special Issue of Safety Science, 2016, pp. 34 – 43.

4. Leva, M.C., Kontogiannis, T., Balfe, N., etc. Human factors at the core of total safety management: The need to establish a common operational picture. In: S. Sharples, S. Shorrock, P. Waterson (Eds.) Contemporary Ergonomics, 2015, pp. 163-170.

5. B. Andersen, T. Fagerhaug Root Cause Analysis: Simplified Tools and Techniques, Second Edition Paperback, 2006, ASQ quality press, Milwaukee, Wisconsin, 219 p.

6. Root Cause Analysis: The Core of Problem Solving and Corrective Action, 2009, ASQ Quality Press, 200 p.

APPENDIX A

TEACHING PROGRAMME OF THE COURSE ITM1 "IOT FOR SMART ENERGY GRID"

DESCRIPTION OF THE COURSE

TITLE OF THE COURSE	Code
IoT for Smart Energy Grid	**ITM1**

Teacher(s)	Department
Coordinating: Prof., DrS. E. V. Brezhnev **Others:** Module ITM1.1: Assoc. Prof., Ph.D. Z. Dombrovskyi, Prof., DrS. A. Sachenko, Ph.D. Student M. Dombrovskyi, Assoc. Prof., Ph.D. G. Hladiy. Module ITM1.2: Prof., DrS. M. P. Musiyenko, Ass. Prof., Dr. I. M. Zhuravska, Dr. Y. M. Krainyk. Modules ITM1.3: DrS. E. Brezhniev, Ph.D. M. Kolisnyk , ITM1.4: DrS. E. Brezhniev	Department of Computer systems, Networks and Cyber Security (KhAI); Department of Information and Computing Systems and Control (TNEU); Intelligent Information Systems (PMBSNU)

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: Foundation of Modeling; Computer Networks; Computer Systems and Embedded System; Computer electronics.	**Co-requisites (if necessary):** Foundations of Dependability and Information Security; System and Network Security.

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 on IoT infrastructure for smart energy grid (SEG) and to provide

<table>
<tr><td colspan="3">prerequisites for practical use of such embedded system. The study also expands the current research on SEG by combining system approach in the context of the study the monitoring and control function of IoT embedded system.</td></tr>
<tr><th>Learning outcomes of course</th><th>Teaching/learning methods</th><th>Assessment methods</th></tr>
<tr><td>At the end of course, the successful student will be able to:
1. to understand the model of SG and, and implementing the Cloud computing and Big Data in SG.</td><td>Interactive lectures, Learning in laboratories, Just-in-Time Teaching</td><td>Course Evaluation Questionnaire</td></tr>
<tr><td>2. to understand the structure of integrated Smart Grid system in IOT environment</td><td>Seminars, project work</td><td>Module Evaluation Questionnaire</td></tr>
<tr><td>3. To obtain the basic skills of integration of reliability models into safety assessment of IT infrastructure of power grid and to apply the Markov models method for the SEG assessment of dependability</td><td>Interactive lectures, Learning in laboratories, Just-in-Time Teaching</td><td>Course Evaluation Questionnaire</td></tr>
<tr><td>4. to implement the Cloud computing and Big Data in Smart Grids</td><td>Seminars, individual work</td><td>Module Evaluation Questionnaire</td></tr>
<tr><td>5. Employ the models and methods for structural organization of local SEG infrastructure</td><td>Interactive lectures, Learning in laboratories, Just-in-Time Teaching</td><td>Course Evaluation Questionnaire</td></tr>
<tr><td>6. Select appropriate hardware for control and harvesting energy flow in local SEG</td><td>Interactive lectures, Learning in laboratories</td><td>Course Evaluation Questionnaire</td></tr>
<tr><td>7. Analyze most common architecture solutions for local SEG and their main pros and cons and propose the most appropriate hardware/software set for their organization</td><td>Interactive lectures, Learning in laboratories</td><td>Course Evaluation Questionnaire</td></tr>
<tr><td>8. Leverage advantages of hardware and software components for local SEG according to its peculiarities</td><td>Interactive lectures, Learning in laboratories</td><td>Course Evaluation Questionnaire</td></tr>
</table>

Themes	**Contact work hours**							**Time and tasks for individual work**	
	Lectures	Consultations	Seminars	Practical work (training)	Laboratory work	Placements	**Total contact work**	**Individual work**	**Tasks**
1. Existing grid problem and its solution using the integrated Smart Grid system in IoT environment. 1.1. Existing grid problem and its solution 1.2. Problems in Power Grid and a Smart Grid conceptual model 1.3. European Smart Grid Architecture Model and New Grid Paradigms - Micro grid	6		4	4			**14**	**16**	1.1. Studying the problem of existing grid. 1.2 A conceptual model of Smart Grid 1.3. Criteria for selecting the Investment Projects to implement the Smart Grid in the existing grid
2. Applying the IoT in Smart Grid projects 2.1. Development of intelligent power grids directions. 2.2. Forming the strategic vision redistribution 2.3. Paradigm the Internet of Things	6		4	4			**14**	**16**	2.1. Studying the problem implementation of the Smart Grid 2.5. Applying the IoT in Smart Grid projects 2.3. A conceptual

									model applying the IoT in Smart Grid projects
3. Cloud computing and big data as a part of the IoT Smart Grid 3.1. Processes in the integrated smart grid system on cloud 3.2. Cloud-based software platform for smart grids 3.3. D2R software platform on Clouds	6		4	4			**14**	**16**	3.1. A conceptual model of Cloud computing 3.2. Integrating the Cloud computing and Big Data into the Smart Grid environment 3.3. Explore the possibilities of using the different types of Cloud computing and Big Data in smart grid
4. Availability assessment of IoT based IT infrastructure of Power Grids 4.1 Integration of reliability methods into safety assessment processes for it infrastructure of power grid 4.2 Dependability assessment of Smart Grid	6			4	4		**14**	**16**	4.1 Predictive analytics, diagnostics and maintenance of SEG ***4.2***

systems 4.3 Application of STAMP method for smart grid safety/security accident analysis 4.4 Accident root cause analysis of IoT based smart grid with Five Whys Method									
5. Development of I&C and harvesting systems for local SEG 5.1. Complex interdependencies that characterize local SEG 5.2. Architecture of I&C and harvesting systems 5.3. Devising methods of I&C and harvesting systems	6			4	2		**12**	**18**	5.1. Local SEG organization 5.2. Architecture of SEG
6. Hardware components for local SEG (sensors, measurement units, control units – Raspberry Pi, STM32 boards, ESP8266, PLC, Phoenix, etc.) 6.1. Sensors, measurement units. Energy measurement systems using PLC technology (IEEE 1901) 6.2. IoT control solutions based on STM32 boards, ESP8266 6.3. PLC in SEG architecture. Mini-computers for local SEG	6			4	4		**14**	**16**	6.1. Wireless solutions architecture using ESP8266 6.2. The main types and characteristics of COM-ports in counters that record the consumption of various types of energy
7. Software components of SEG 7.1 Protocols for device	6			4	4		**14**	**16**	7.1. Software platform

communication 7.2. Cloud infrastructure used by local SEG 7.3. Local software for SEG. Software platform named “mbed” for local infrastructure IoT solution									named “mbed” means and methodologies 7.2 Device communication protocols usage
On the whole	**42**		**12**	**28**	**14**		**96**	**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				
1	D. Uckelmann, M. Harrison, F. Michahelles	2011	Architecting the Internet of Things		Berlin, Heidelberg: Springer-Verlag
2	S. Galli, T. Lys	2015	SMART GRID COMMUNICATIONS: Next Generation Narrowband (Under 500 kHz) Power Line Communications (PLC) Standards		China Communications

3	S. Galli, A. Scaglione, Z. Wang	2011	For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid	Vol. 99, No. 6	Proceedings of the IEEE
4	S. Monton	2008	Improving Flow Measurement Using PLC Based Flow Computing		ProSoft Technology
5	H. Makita, Yu. Shida, N. Nozue	2012	Factory Energy Management System Using Production Information		Mitsubishi Electric ADVANCE. Technical reports
6	P. Li, S. Guo, Z. Cheng	2013	Joint Optimization of Electricity and Communication Cost for Meter Data Collection in Smart Grid		http://ieeexplore.ieee.org/document/6563124/
7	International Energy Agency		Smart Grid Roadmap		https://www.iea.org/publications/ free publications/publication/smartgrids_roadmap.pdf
8	Fitzpatrick, G.J. and Wollman, D.A.	2010	NIST Interoperability Framework and Action		IEEE Power and Energy Society General

			Plans		Meeting, Minneapolis, 25-29 July 2010
9	T. Basso, J. Hambrick, D. DeBlasio	2012	Update and review of IEEE P2030 Smart Grid Interoperability and IEEE 1547 interconnection standards		2012 IEEE PES Innovative Smart Grid Technologies (ISGT)
10		2014	NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0.		NIST Special Publication 1108r3
11	Faheem M.S., Shah B.H., Butt R.A., Raza B., Anwar M., Ashraf M.W., Ngadi M.A., Gungor V.C.	2018	Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges.	August 2018	Computer Science Review.
12	X. Jin, Z. He, Z. Liu,	2011	Multi-agent-based cloud architecture of smart grid,	12	Energy Procedia
13	Kuzlu M., Pipattanasomporn M., Rahman S.	2014	Communication network requirements for major smart grid applications	67	Computer Networks

			in HAN, NAN and WAN		
14	Garner, G.	2010	Designing Last Mile Communications Infrastructures for Intelligent Utility Networks (Smart Grids)		IBM Australia Limited
15	Al-Omar, B., Al-Ali, A.R., Ahmed, R. and Landolsi, T.	2012	Role of Information and Communication Technologies in the Smart Grid.	3	Journal of Emerging Trends in Computing and Information Sciences
16	Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C. and Hancke, G.P.	2013	A Survey on Smart Grid Potential Applications and Communication Requirements.	9	IEEE Transactions on Industrial Informatics
17	Hatziargyriou, N.	2005	Key note speech "Microgrids-The future of small grids"		Future Power Systems, FPS 2005, Amsterdam, 16-18 November 2005
18	A. Bose	2010	Smart transmission grid applications and their	1 (1)	IEEE Trans. Smart Grid

			supporting infrastructure		
19	European Smart Grids Technology Platform	2006	Vision and strategy for Europe's electricity networks of the future,		http://www.smartgrids.eu/documents/vision.pdf
20	Al-Ali, A.R. and Aburukba, R.	2015	Role of Internet of Things in the Smart Grid	3	Technology Journal of Computer and Communications
21	D. Giusto, A. Iera, G. Morabito, L. Atzori	2010	The Internet of Things		Springer
22	Naveen P., Ing W.K., Danquah M.K., Sidhu A., Abu-Siada, A.	2016	Cloud computing for energy management in smart grid – an application survey		CUTSE2015. IOP Conf. Series: Materials Science and Engineering 121
23	Al-Ali, A.R. and Aburukba, R.	2015	Role of Internet of Things in the Smart Grid Technology	issue 3	Journal of Computer and Communications
24	Bera S., Misra S., Rodrigues J. P. C.	2013	Cloud Computing Applications for Smart Grid: A Survey.		DOI 10.1109/TPDS.2014.2321378
25	H. Kim, Y. Kim, K. Yang, and M. Thottan	2011	Cloud-based demand response for smart grid: Architecture and distributed		Second IEEE International Conference on Smart Grid Communications

			algorithm		
26	Maryna Kolisnyk, Vyacheslav Kharchenko, Iryna Piskachova, Nikolaos Bardis..	2017	A Markov model of IoT system availability considering DDoS attacks and energy modes of server and router	1844	Proceeding IEEE, ICTERI Conference, 14 p. [http://ceur-ws.org/Vol-1844/10000699.pdf].
27	Kharchenko Vyacheslav, Kolisnyk Maryna, Piskachova Iryna.. 2016,	2016	Reliability and Security Issues for IoT-Based Smart Business Center: Architecture and Markov Model		IEEE. Computer of science, MCSI Greece, Chania. Paper ID: 4564699.
28	Leva, M.C., Kontogiannis, T., Balfe, N., etc. In: S. Sharples, S. Shorrock, P.	2015	Human factors at the core of total safety managemen: The need to establish a common operational picture.		Waterson (Eds.) Contemporary Ergonomics, pp. 163-170.
29	Gerbec, M., Balfe, N., Leva M.C., Prast S.	2016	Risk assessment and optimization for rare, new or complex		Special Issue of Safety Science, pp. 34 – 43.

			processes: Combining task analysis, 4D process simulation, hazard analysis and optimization		
30	Floyde A., Lawson G., Shalloe S., Eastgate R., D’Cruz, M.,	2013	The design and implementation of knowledge management systems and e-learning for improved occupational health and safety in SMEs		Safety Science, # 60, pp. 69–76.
31	Bregnev E.V.	2001	Risk management : a tool for improving Nuclear Power Plant performance	88	IAEA, VIENNA, 2001, IAEA-TECDOC-1209, ISSN 1011-4289
32	Ashwani M., Rakesh G.	2012	Calculating Grid Reliability in Bayesian Networks	Issue 4	International Journal of Computer Science and technology, 854-857 pp.
33	Rausand M.	2004	System analysis.		System reliability

			Event tree Analysis		Theory (2nd edition), Wiley, 26/28
34	Mosleh A.	2000	Procedures for treating Common Cause Failures in Safety and Reliability Studies	2	Analytical Background and Techniques (NUREG/CR-4780 ERPI NP-5613), 88.
35	Bowles J.B.	2004	An assessment of PRN prioritization in a failure modes effects and criticality analysis		Journal of the IEST,:47:51-6.
36	Mohammed J. Wadi	2018	Reliability Evaluation in Smart Grids via Modified Monte Carlo Simulation Method		7th International Conference on Renewable Energy Research and Applications (ICRERA)
37		2003	Functional Safety: Safety Instrumented Systems for the Process Sector		International Electrotechnical Commission (IEC), IEC 61511, Geneva, Switzerland
38	Schellhorn G.,	2002	Formal fault		Paper

	Thums A.		tree semantics		presented at the Sixth World Conference on Integrated Design & Process Technology, Pasadena, CA
	Additional literature				
39	S. Hadim, N. Mohamed	2006	Middleware: middleware challenges and approaches for wireless sensor networks		http://ieeexplore.ieee.org/document/1621014/
40	M. Rana	2017	Architecture of the Internet of Energy Network: An Application to Smart Grid Communications		http://ieeexplore.ieee.org/document/7891908/
41	Yu Wang, S. Mao, R. M. Nelms	2013	Online Algorithm for Optimal Real-Time Energy Distribution in the Smart Grid		http://ieeexplore.ieee.org/document/6558479/
42	M. Simonov, G. Chicco, G. Zanetto	2017	Event-Driven Energy Metering: Principles		http://ieeexplore.ieee.org/document/7875140/

			and Applications		
43	S. Salinas, M. Li, P. Li, Y. Fu,	2011	Dynamic Energy Management for the Smart Grid With Distributed Energy	vol. 9, no. 6	IEEE Transactions on Smart Grid, 8, pp. 5820-5830. DOI: 10.1109/tsg. 2017.2697440
44	B. P. Roberts, C. Sandberg	2011	The Role of Energy Storage in Development of Smart Grids	99, iss. 6	Proceedings of the IEEE, pp. 1139-1144. DOI: 10.1109/JPROC.2011.2116752.
45	M. Razzaque, M. Milojevic-Jevric, A. Palade, S. Clarke	2016	Middleware for Internet of Things: A Survey	vol. 3, no. 1	IEEE Internet of Things Journal, pp. 70-95.
46	F. Hussain	2017	Internet of Things: Building Blocks and Business Models.		Cham: Springer
47	R. Moghaddass, J. Wang	2013	A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale	vol. 4, no. 4	Resources IEEE Transactions on Smart Grid, pp. 2139-2151. DOI: 10.1109/tsg. 2013.226555

			Smart Meter Data		6.
48		2013	Safety Management Manual		International Civil Aviation Organization Third Edition, University Street, Montréal, Quebec, Canada H3C 5H7, 251 p.
49	B. Andersen, T. Fagerhaug.,	2006	Root Cause Analysis: Simplified Tools and Techniques		Second Edition Paperback, ASQ quality press, Milwaukee, Wisconsin, 219 p.

ABSTRACT

UDC 004.415/.416:621.31](076.5)=111

Z.I. Dombrovskyi, A.O. Sachenko, I.M. Zhuravska, M.Z. Dombrovskyi, G.M. Hladiy, M.P. Musiyenko, Y.M. Krainyk, E.V. Brezhniev, M.O. Kolisnyk. **I**oT for Smart Energy Grid. Trainings / Edited by E.V. Brezhnev – Ministry of Education and Science of Ukraine, Ternopil National Economic University, Petro Mohyla Black Sea National University, National Aerospace University “KhAI”, 2019. – 141 p.

The materials of the training part of the study course ITM1 “IoT for Smart Energy Grid”, developed in the framework of the ERASMUS+ ALIOT project “Internet of Things: Emerging Curriculum for Industry and Human Applications” (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

The structure of work on verification of residual knowledge in the discipline, the corresponding practical material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical aspects of IoT for smart energy grid are presented. IoT infrastructure for smart energy grid based on embedded systems devices, its safety, reliability and security are examined.

It is intended for engineers, developers and scientists engaged in IoT for smart energy grid, for postgraduate students of universities studying in areas of IoT-based systems, smart energy grid, embedded systems, as well as for teachers of relevant course.

Ref. – 49 items, figures – 62, tables – 9.

CONTENTS

АНОТАЦІЯ

УДК 004.415/.416:621.31](076.5)=111

З.І. Домбровський, А.О. Саченко, І.М. Журавська, М.З. Домбровський, Г.М. Гладій, М.П. Мусієнко, Я.М. Крайник, Д.М. Гладій, Є.В. Брежнєв, М.О. Колісник. Інтернет Речей для розумної енергетичної мережі. Тренінги / За ред. Є.В. Брежнєва – МОН України, Тернопільський національний економічний університет, Чорноморський національний університет ім. Петра Могили, Національний аерокосмічний університет ім. М.Є.Жуковського «ХАІ», 2019. – 141 с.

Викладено матеріали тренінгової частини курсу ІТМ1 “IoT для розумної енергетичної мережі”, 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 практичний матеріал, приклади виконання завдань та критерії оцінювання. В процесі навчання наводяться теоретичні аспекти IoT для розумної енергетичної мережі. Вивчаються IoT-інфраструктура для інтелектуальної енергетичної мережі на основі пристроїв вбудованих систем.

Призначено для інженерів, розробників та науковців, які займаються розробкою та впровадженням IoT для розумної енергетичної мережі, для аспірантів університетів, які навчаються за напрямами IoT систем, розумних енергетичних мереж, вбудованих систем, а також для викладачів відповідних курсів.

Бібл. – 49, рисунків – 62, таблиць – 9.

ЗМІСТ

Домбровський Збишек Іванович
Саченко Анатолій Олексійович
Журавська Ірина Миколаївна
Домбровський Михайло Збишекович
Гладій Григорій Михайлович
Мусієнко Максим Павлович
Крайник Ярослав Михайлович
Брежнєв Євген Віталійович
Марина Олександрівна Колісник

ІНТЕРНЕТ РЕЧЕЙ ДЛЯ РОЗУМНОЇ ЕНЕРГЕТИЧНОЇ МЕРЕЖІ

Тренінги
(англійською мовою)

Редактор Брежнєв Є.В.

Комп'ютерна верстка
В.С. Харченко,
О.О. Ілляшенко

Зв. план, 2019
Підписаний до друку 27.08.2019
Формат 60x84 1/16. Папір офс. No2. Офс. друк.
Умов. друк. арк. 8,19. Уч.-вид. л. 8,81. Наклад 150 прим.
Замовлення 270819-3

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.