ACTA TECHNICA CORVINIENSIS
– Bulletin of Engineering
Tome X [2017]
Fascicule 2 [April – June]
ISSN: 2067 – 3809

[1] Davor ZORC

INTERNET OF THINGS (IoT) IN INDUSTRIAL ENGINEERING EDUCATION

[1] University of Zagreb, Faculty of Mechanical Engineering and Naval Architecture, Ivana Lucica 5, Zagreb, CROATIA

Abstract: This paper presents an overview of current state of affairs in the Internet of Things (IoT) domain and briefly discusses its industrial applications. This has provided a motivation for the development of educational IoT laboratory setup based on legacy (mature) microcontroller-based control hardware, which should be easily upgraded by expanding it with a serial connection-equipped embedded network controller board such as ESP8266 module. The laboratory setup upgrade process is briefly outlined and Industrial IoT educational aspects implementable on such a platform are briefly discussed.

Keywords: Internet of Things, industrial computer control, education

INTRODUCTION

Internet of Things (IoT) is one of the latest "buzzwords" in the information and communication technology (ICT) sector, likely to exceed the impact of already well-known Cloud Computing paradigm [1]. Integration of sensors with microprocessor and wireless network adapters is hardly a new concept, but widespread availability, low prices and possibility of miniaturization lead to widespread use of such small-scale and ubiquitous systems. The goal of IoT movement is to network everything, from home appliances [2] and cars [3], to healthcare [4, 5], and smart cities and smart energy systems [3, 6, 7]. IoT prophets declare that it will be the next great industrial revolution, and that it will change everything within our lifetimes.

Similar statements have also been heard when microprocessors were first introduced. Many people did not believe that such small thing can have such profound impact. But 45 years later we can see that it was true – we have at least one microprocessor core in our pocket phone and many household appliances. So it really seems possible that IoT will change many things in our lives that we have taken for granted. Current state of the art is that IoT devices are getting increasingly smaller (possibly 1 cubic cm or less) and also cheaper. Perhaps in the future, people will have it implanted in their bodies as well [4]?

IoT may use standard Internet protocols but there are many other things to standardize (like data formats) so as to enable interoperability. Currently there is a kind of a "Standards War" with still uncertain final outcome which should establish who will be able to control this huge system. Industry consortiums are formed in order to protect their market shares, while at the same time various interest groups are also involved, such as those supporting an open system approach, which should be available to anyone. The main challenges facing the future of IoT are [2, 8, 9]:

- Privacy and security problems;
- Notable increase in electro-magnetic noise due to enormous number of such devices;
- Substantial increase in the amount of generated/stored data (so-called "data deluge").

Naturally the bulk of research efforts are aimed at solving the above problems, so that IoT devices may find their place in the future ICT infrastructure in spite of those challenges.

For more than 25 years we at the Faculty of Mechanical Engineering and Naval Architecture at the University of Zagreb teach mechanical engineering students how to control machines by means of microprocessors-based systems. In doing so we want them to have a first-hand experience using dedicated laboratory setups even at entry-level and basic courses such as "Electrical engineering basics" and with more details in specialized courses such as “Microprocessor-based control”. In our current scheme, device networking is typically based on industrial protocols and computers are mostly in the form of Programmable Logic Controllers (PLCs) in the role of typical industrial hardware, which may also be equipped with Internet protocols too [10], even if those protocols would not be the best suited ones for low-level industrial control due to possible issues with the demand for simultaneous real-time operation of control algorithms.

Assuming that this new IoT paradigm is here to stay, there is no way of avoiding the introduction of those systems into the ever changing subject curriculum, for which a dedicated laboratory setup is currently being built. As a first step towards achieving this goal we have initiated the upgrade of current setups for analog, digital and PLC-based control, which has been emulated by a microcontroller system commanded via a PC terminal. The proposed upgrade consists of a wireless system on a module being able to communicate with user’s smartphone, tablet or notebook computer. By using IoT technology this control could be carried out over Internet from any place worldwide, thus extending the laboratory work into the virtual domain [11]. To this end this paper presents our implementation of the aforementioned IoT system using ESP8266 chip, a System on chip with processor, network adapter and Wi-Fi link [12].

The paper is organized as follows. In chapter 2 industrial IoT is discussed in general terms in order to illustrate its applicability to industrial system supervision and control, while in chapter 3 the target ESP8266 embedded IoT system suitable for such purposes is presented. Chapter 4 is dedicated to the laboratory setups built for educational purposes, which may be suitable for the implementation of IoT concepts in automation and control. Concluding remarks are given in Chapter 5.

INDUSTRIAL IoT (IIoT)

The rise of computer-based control systems in the form of easy-to-use universal controllers started in late sixties by the advent of first PLCs (programmable logic controllers), whereas today these control platforms predominate in industrial applications, representing a well-established, standardized, reliable, easy-to-use and affordable control system solution. The main advantage of such systems is that PLC programming languages are oriented towards control-specific tasks, and are much easier to use and learn then standard higher-level computer programming languages (see e.g. [10], [18] and [19]). On the other hand, computer networks for industrial use have also progressed recently, thus resulting in several solutions that are now industry standards, while in the meantime there was also a rise of Internet use and Internet/Ethernet protocols. This technology became widely known to programmers and general public. So this notable change in the way how people exchange information and communicate had also an impact in industrial systems [20].

Moreover, today’s industry along with PLC’s also fields a growing number of industrial PC’s and their corresponding communication protocols. Although Ethernet protocols are neither designed nor well suited for low-level control in industry (because of stringent requirements on real-time communication), the advances in microprocessor processing speed seem to compensate for that disadvantage. Finally, a range of modifications to Ethernet protocols has been introduced over the years, so now there are Ethernet variants that are able to handle real-time problems as well. This represents a fertile field for the introduction of Internet of Things (IoT) into the industrial communication environment as well. In particular, in the survey paper [15], IoT is defined as: “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual ‘Things’ have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network”.

The Industrial Internet of Things (IIoT) [15] technology is apparently aimed towards bringing automation and control systems to new levels, so the trend of using IoT [14] technology in the industry seems to be on the rise. The term IIoT (Industrial Internet of Things) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT.

IIoT in manufacturing would probably generate so much business value that it will eventually lead to the fourth industrial revolution, the so-called Industry 4.0. In particular, IoT represents the final cornerstone in the Industry 4.0 concept, the others being: (i) machine-to-machine (M2M) interfacing which enables large-scale flexible production, (ii) mobile Internet which allows for flexible data collection, (iii) Big Data and Cloud Computing which may enable the innovative concepts of industrial intelligence, and (iv) social media to promote the Industry 4.0 as a new product [21]. However, it is likely that the main beneficiaries of this new “revolution” will likely be the countries in the developed world, whose existing information infrastructure is significantly better equipped for the uptake of these propulsive technologies compared to developing countries.

So the scope of IIoT is broader then only technical aspect of it, as it includes global business plans and the way things will be manufactured in the future [17]. One of basic technologies for IoT integration within the existing infrastructure is radio-frequency identification (RFID) technology. Using RFID tags objects can be identified, tracked and monitored, and they have been used since 1980s in logistics, pharmaceutical production, retailing, and supply chain management. Another foundational technology for IoT is the wireless sensor networks (WSNs), which mainly use interconnected intelligent sensors for sensing and monitoring. With the advances in wireless communication, smartphones, and sensor network technologies, an increasing number of networked “things” or smart objects are being involved in IoT [15]. As mentioned above, so far, IoT has been gaining attraction in specific industries such as logistics/transportation, intelligent manufacturing, retailing, and pharmaceutics/healthcare. The key to the IoT success appears to be its standardization, which should provide interoperability, compatibility, reliability, and effective IoT system operation on a global scale.

In particular, IoT can be considered as a world-wide physical inter-connected network, within which “things” or smart devices can be accessed and controlled remotely. The decentralized and heterogeneous nature of IoT requires that the architecture provides efficient event-driven capability.

Thus, service-oriented architecture (SOA) is considered a suitable approach to achieve interoperability between heterogeneous devices in a multitude of ways. In order to do that a four-layered architecture is elaborated for IoT in [15], comprising the following components (i) sensor layer, (ii) network layer, (iii) service layer, and (iv) interface layer. From the viewpoint of the information network, the IoT is a complex heterogeneous network, which includes the connection between various types of smart devices through various communication technologies.

It is broadly accepted that the IoT technologies and applications are still in their infancy. There are still many research challenges for industrial use such as: technology issues, standardization requirements, security protocols, and privacy concerns. Nevertheless, IoT approach will significantly augment network traffic and data storage needs so it can be presumed that IoT will gradually be developed as those technologies evolve.

MODULE nodeMCU

Node MCU (Figure 1) is one of many solutions suitable for small-scale IoT applications [13]. It is a small and inexpensive module based on ESP8266 chip technology [12], which is basically a microcontroller connected to a Wi-Fi transmitter/receiver unit. The target microcontroller can be programmed in a familiar way, for example using Arduino’s software tools and its C-like higher-level programming language [16], or by using a LUA interpreter.

The microcontroller module is connected to the PC by using the embedded USB interface which is then used for transferring the user program to the module. Besides running the user program, this embedded system runs the whole stack of Internet protocols. So, if its Internet part is configured properly, one can easily connect to the local wireless network. In this way this small-scale embedded microcontroller system can be visible to all Internet users and it can also be controlled by virtually anybody from any location (of course, password-restricted access is possible). On the user side of the communication only a suitable Internet browser is needed running on user smart device.

The embedded system can also be configured to become a Wi-Fi hotspot and can be accessed from smart phones or laptops in its vicinity. This system can but need not be connected to the global Internet.

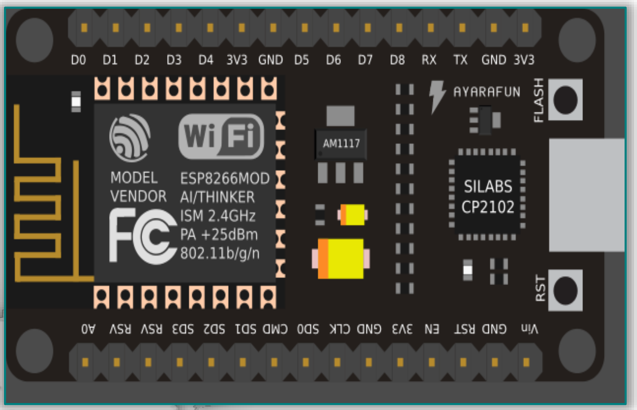

D0 D1 D2 D3 D4 3V3 GND D5 D6 D7 D8 RX TX GND 3V3
AYARAFUN
FLASH
Wi Fi
MODEL ESP8266MOD
VENDOR AI/THINKER
ISM 2.4GHz
PA +25dBm
802.11b/g/n
AM1117
SILABS CP2102
RST
A0 RSV RSV SD3 SD2 SD1 CMD SD0 CLK GND 3V3 EN RST GND Vin

Figure 1 – Module nodeMCU printed circuit board with component layout.

LABORATORY SETUPS

The Robotics and Manufacturing Systems Automation Department at the Faculty of Mechanical and Naval Engineering, University of Zagreb, Croatia has a long standing tradition of teaching electrical and electronics engineering, automatic control, computer control, robotics and other related fields.

In particular, within the introductory electrical/ electronics engineering courses there was a need to enable undergraduate students to get first-hand experience in computer control of engineering systems in order to grasp its basic concepts. For that reason, several variants of computer-based control systems laboratory setups have been developed over the last 25 years.

Laboratory setup - version 1

First computer control laboratory setup was developed in 1993 (Figure 2), comprising of three physical systems (processes) intended to be controlled by the dedicated microcontroller:

- A model of street traffic lights (semaphores), which represents a case study in sequential control;
- A model of temperature controlled chamber, which is used to demonstrate the concepts of closed-loop control by using a simple relay feedback controller;

- A PLC application for universal digital control, which is primarily used to demonstrate the effectiveness of logic control-oriented programming languages, such as Instruction Set language.

The communication with the target controller is implemented using a serial PC interface, wherein the PC user communicates with the microcontroller by using a serial terminal program (Hyper-terminal).

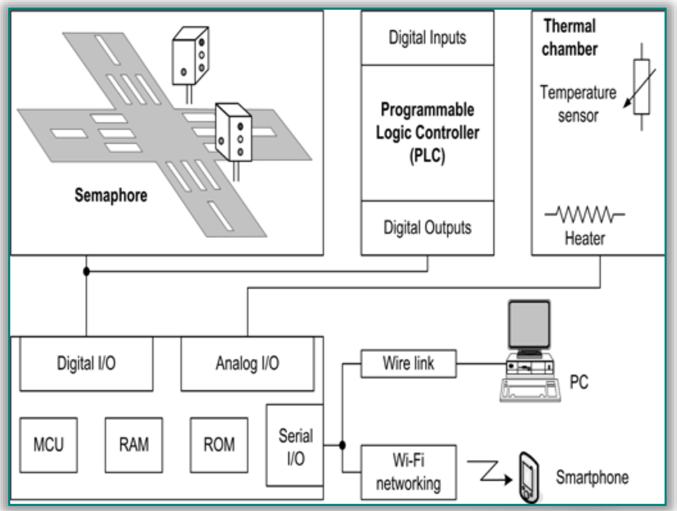
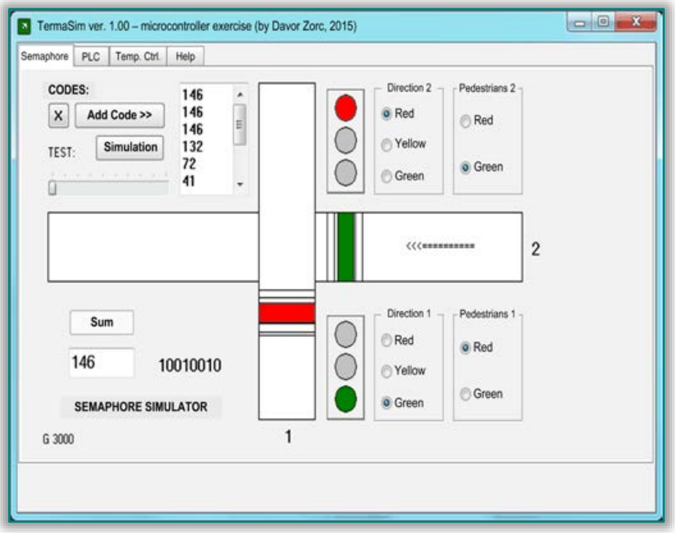


Figure 2 – Laboratory setup
for computer control education purposes.

Laboratory setup - version 2

Second version of the aforementioned laboratory exercises has been developed in 2013, and it includes a PC application for animated simulation, programming or configuration of aforementioned physical objects intended for control system testing.

The simulation and process data visualization system interfaces for the traffic lights (semaphores), PLC system emulation and thermal chamber control are shown in Figures 3 – 5, respectively.



```
146
146
146
132
72
41
```

146 10010010

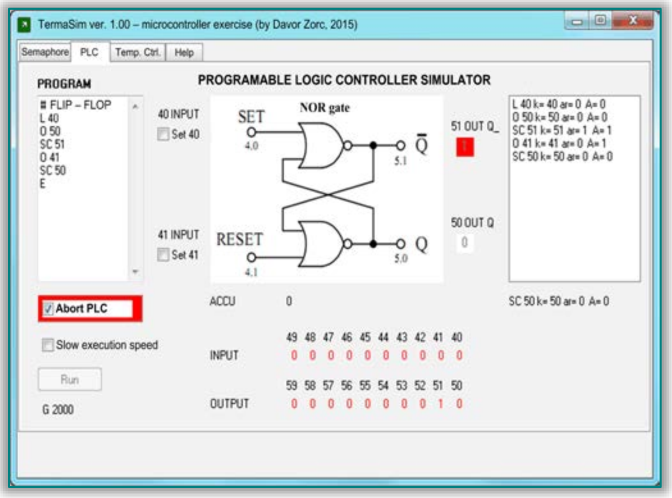
Direction 2: ● Red ○ Yellow ○ Green

Pedestrians 2: ○ Red ● Green

Direction 1: ○ Red ○ Yellow ● Green

Pedestrians 1: ● Red ○ Green

Figure 3 – Simulation of traffic lights (semaphore) system for simple crossroads.



```
# FLIP – FLOP
L 40
O 50
SC 51
O 41
SC 50
E
```

```
L 40 k= 40 ar= 0 A= 0
O 50 k= 50 ar= 0 A= 0
SC 51 k= 51 ar= 1 A= 1
O 41 k= 41 ar= 0 A= 1
SC 50 k= 50 ar= 0 A= 0
```

□ Set 40

□ Set 41

☑ Abort PLC

□ Slow execution speed

ACCU 0

SC 50 k= 50 ar= 0 A= 0

	49	48	47	46	45	44	43	42	41	40
INPUT	0	0	0	0	0	0	0	0	0	0

	59	58	57	56	55	54	53	52	51	50
OUTPUT	0	0	0	0	0	0	0	0	1	0

Figure 4 – Simulation of Flip-Flop operation using PLC Instruction Set language.

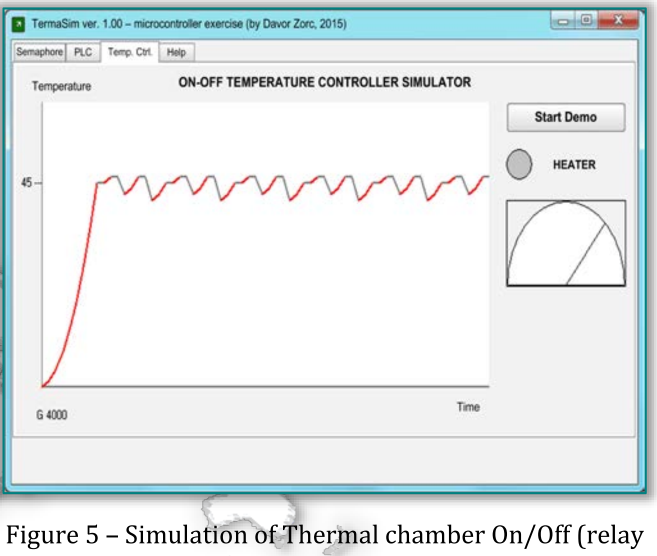

TermaSim ver. 1.00 – microcontroller exercise (by Davor Zorc, 2015)
Semaphore
PLC
Temp. Ctrl.
Help
ON-OFF TEMPERATURE CONTROLLER SIMULATOR
Temperature
45
Time
G 4000
Start Demo
HEATER

Figure 5 – Simulation of Thermal chamber On/Off (relay feedback) control.

After the functionality of the control code has been thoroughly checked within the simulation environment, the control program may then be downloaded through the serial interface onto the target microcontroller system and then run for the purpose of final control code verification.

Laboratory setup - version 3

Third version of the laboratory setup is a work in progress, which includes porting the same functionality of the version 2 setup to the Arduino/ESP8266 platform. This version does not need a PC as terminal device; on the contrary, students may program/configure different objects of control system using tablet PCs or even their own smartphones.

A tablet PC or smartphone is connected to the ESP8266 module by choosing it from the instantaneously generated list of available Wi-Fi hotspots. When connected, Internet browser can be used to monitor and manipulate control program objects.

Alternatively, ESP8266 can be configured as Telnet protocol server. In this way user interface is of the console type, but Telnet app needs to be downloaded beforehand. As this exercise is for students physically present in the laboratory, ESP8266 can be configured/programmed as intranet device, i.e. for local use only.

CONCLUSIONS

The paper has first presented an overview of Internet of Things (IoT) technologies state-of-development and potentials for its application in industrial applications in the form of Industrial Internet of Things (IIoT). This has provided an additional motivation for the inclusion of such topics in the teaching programs (curricula) dealing with electrical engineering, automation and industrial systems control-related subjects currently being taught at the University undergraduate level.

Using current embedded microcontroller technology it should be relatively straightforward to develop small-scale hardware and software applications including basic IoT functionalities, which can be easily integrated with the existing legacy hardware and control-oriented software via simple serial interface. Hence, these augmented teaching aids should be able to provide an additional benefit in the overall teaching process through the inclusion of straightforward interfacing between the user (student) and the legacy control hardware.

Since the IoT technology is still under development, it is reasonable to expect that it would gradually find its place in various industries. However, based on the current state-of-affairs in the IoT field, increased efforts are required in terms of development and implementation of suitable standards. Since reliability is crucial in industrial applications, and particularly attention needs to be devoted to communication system security, many problems already present in general Internet use may also be expected with increased uptake of IoT in industrial applications. Since security issues can be overcome, as proven by the reliability of today's Internet commerce and banking, notable attention needs to be devoted to this particular aspect of IoT, in order to facilitate successful implementation of IoT in the industry in the near future.

Acknowledgements

Technical support related to the functionality testing and initial development of Arduino/ESP8266 embedded system provided by Professor Mario Essert and Mr. Zvonko Grgec is highly appreciated, as well as the initial efforts made by Igor Ratković, mag. ing. during the development of second-generation laboratory exercises on Arduino platform.

Finally, useful discussions and technical support provided by Professor Danijel Pavković in the preparation of the final manuscript are also greatly appreciated.

Note

This paper is based on the paper presented at The International Conference Management of Technology – Step to Sustainable Production (MOTSP 2016), organized by the Faculty of Mechanical Engineering and Naval Architecture, Croatian Association for PLM and the University of North, in Porec/Parenzo, Istria, CROATIA, June 01–03, 2016.

References

[1] Want, R., Schilit, B. N., Jenson, S.: Enabling the Internet of Things, IEEE Computer Magazine, 48(2015)1, 28-35.

[2] Grau, A.: Can You Trust Your Fridge, IEEE Spectrum, 52(2015)3, 50-56.

[3] Jin, J., Gubbi, J., Marusic, S., Palaniswami, M.: An Information Framework for Creating a Smart City Through Internet of Things, IEEE Internet of Things Journal, 1(2014)2, 112-121.

[4] Jiang, Z., Abbas, H., Jang, K. J., Mangharam, R.: The Challenges of High-Confidence Medical Device Software, IEEE Computer Magazine, 49(2016)1, 34-42.

[5] Catarinucci, L., de Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., Tarricone, L.: An IoT-Aware Architecture for Smart Healthcare Systems, IEEE Internet of Things Journal, 2(2005)6, 515-526.

[6] Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of Things for Smart Cities, IEEE Internet of Things Journal, 1(2014)1, 22-32.

[7] Spanò, E. Niccolini, L., Di Pascoli, S., Iannacconeluca, G.: Last-Meter Smart Grid Embedded in an Internet-of-Things Platform, IEEE Transactions on Smart Grid, 6(2015)1, 468-476.

[8] Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things, IEEE Computer Magazine, 44(2011)9, 51-58.

[9] Stankovic, J. A.: Research Directions for the Internet of Things, IEEE Internet of Things Journal, 1(2014)1, 3-9.

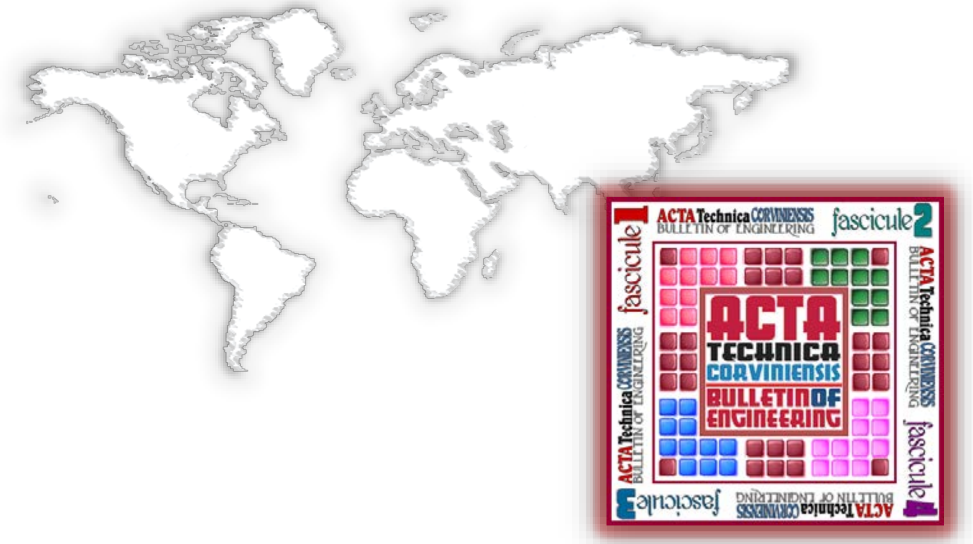
[10] Creating and using user-defined web pages on S7-1200, Siemens AG, support.industry.siemens.com/cs/document/58862931/creating-and-using-user-defined-web-pages-on-s7-1200?dti=0&lc=en-WW, 2016-02-26.

[11] Ruiz, E. S., Martin, A. P., Orduna, P., Martin, S., Gil, R, Ruiz Larrocha, E., Albert, M. J., Diaz, G., Meier, R., Castro, M.: Virtual and Remote Industrial Laboratory: Integration in Learning Management Systems, IEEE Industrial Electronics Magazine, 8(2014)4, 45-58.

[12] ESP8266EX Datasheet – version 4.3, Espressif Systems IOT Team bbs.espressif.com/, 2016-02-26.

[13] NodeMCU, en.wikipedia.org/wiki/NodeMCU, 2016-02-26.

[14] Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey, Computer Networks, 54(2010)15, 2787-2805.
[15] Xu, L. D., He, W., Li, S.: Internet of Things in Industries: A Survey, IEEE Transactions on Industrial Informatics, 10(2014)4, 2233-2243.
[16] Arduino Website, www.arduino.cc/, 2016-05-03.
[17] Internet of Things, en.wikipedia.org/wiki/Internet_of_Things#Manufacturing, 2016-05-03.
[18] Berger, H.: Automating with SIMATIC, Publicis MCD Verlag, Munich, Germany, 2000.
[19] Bolton, W.: Instrumentation and Control Systems, Newness (imprint of Elsevier), Oxford, UK, 2004.
[20] Reynders, D., Mackay, S., Wright, E.: Practical Industrial Data Communications, Newness (imprint of Elsevier), Oxford, UK, 2005.
[21] Chen, C., Xu, L.: SAP: Enabler of Industry 4.0, Huawei Technologies Co. Ltd, 2015.


ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING
fascicule 1
fascicule 2
fascicule 3
fascicule 4
ACTA TECHNICA CORVINIENSIS BULLETIN OF ENGINEERING

ISSN:2067-3809