Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 19 (2018) 103–110

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

6th International Conference on Through-life Engineering Services, TESConf 2017, 7-8 November 2017, Bremen, Germany

A cost estimation approach for IoT modular architectures implementation in legacy systems

Stefano Tedeschi[a*], Duarte Rodrigues[a], Christos Emmanouilidis[a], John Erkoyuncu[a],Rajkumar Roy[a], Andrew Starr[a]

[a]*EPSRC Centre for Innovative Manufacturing in Through-life Engineering Services Manufactturing Department, Cranfield University, MK43 0AL, UK*

Abstract

Industry 4.0 has encouraged manufacturing organisations to update their systems and processes by implementing Internet of Things (IoT) technology in legacy systems to provide new services such as autonomous condition monitoring and remote maintenance. However, there is still no literature that guides in realizing the advantages and disadvantages of the fourth industry revolution in terms of complexity, data security, and cost. This paper lays the foundation for the creation of an innovative conceptual model to estimate the cost for implementation of new architectures for legacy systems. The proposed approach considers aspects that impact the cost of different IoT architectures such as: complexity, data gathering and sharing protocols, and cyber security. The authors suggest a further implementation of the cost model, in order to guide the organisations in the most cost-effective architecture for modernisation of their legacy systems.

Peer-review under responsibility of the scientific committee of the 6th International Conference on Through-life Engineering Services.

Keywords: IoT, Modular Architectures, Legacy Systems, Cost Estimation, Smart Manufacturing

1. Introduction

The digitalization revolution called Industry 4.0 engages consumer and benefits business in a new and innovative way where products, processes, persons and places are involved through data trial that can be captured, tracked, shared,

* Corresponding author. Tel.: + 44 7474903481
E-mail address: s.tedeschi@cranfield.ac.uk

2351-9789
Peer-review under responsibility of the scientific committee of the 6th International Conference on Through-life Engineering Services.
10.1016/j.promfg.2018.01.015

combined, mined, and analysed. Internet of Things (IoT) is an important and innovative technology in this new revolution. It is used to defining internet protocols to allow communication between machines, devices, objects and sensors anywhere on the network [1]. Along with its recognised benefits, Industry 4.0 also creates new challenges for industries in the development of technologies and processes. In this context, special attention is given to legacy systems that are not equipped with monitoring technology to know more about the machine status and performance. As legacy machine tools that are often isolated, not well-equipped with modern communication technologies, and with lack of open Application Programming Interfaces (API), it is difficult to monitor and control the entire production process [2]. Monitoring is the capability of the object to behave as a sensor or to be able to produce information about itself or the encompassing environment; control refers to the capability of remotely controlled objects with internet technology. Mainly, the IoT applications are used for monitoring and controlling. A new concept of intelligent systems, processes and machines is rising, which also brings new challenges associated to Information Technology (IT). This aspect is of high impact for factories that will be increasingly intelligent with the ability to collect, analyse and distribute data, converted into important information for monitoring and maintenance services. At the same time these new intelligent systems based on IoT architectures expose the industries at the cyber-security risks often linked to the work environment, the workers, and the IT technology adopted for sharing information and data. Many IoT kits are available in the market, which are able to manage information and data, but they still not focus on the security aspects for quick adoption into the industry. Moreover, industries are still relatively not familiar with different IoT solutions, and in particular they do not know the cost associated to the implementation of these architectures as well as the cost to make it secure. This paper aims to mitigate this challenge by presenting a conceptual model for estimating the cost for implementation of an IoT modular architecture for smart manufacturing environments, while focusing on legacy machine tools. The paper is structured as follows: Section 2 describes the research problem. Section 3 outlines related work. Section 4 explains the methodology adopted to carry out the study. Section 5 presents the cost model to mitigate the research problem. Section 6 describes a case study that was applied to validate the model. Section 7 makes a discussion of the results. Section 8 presents the conclusions and future work suggestions.

2. Research Problem

Manufacturing organisations typically aim at producing high-quality products to avoid defects as well as to make sure the machines run for a long-time span without compromising the company's profit with prolonged break-downs. However, most of the manufacturers are equipped with legacy systems that are usually not effective in terms of life-cycle duration and operational performance. Legacy systems are typically a piece of manufacturing equipment natively lacking external communication capabilities and API that could provide real-time machining data [2]. This fact makes it difficult to easily monitor the systems, which can introduce inefficiency and generate higher cost of sensor integration [12]. IoT technology emerged as a solution to improve legacy systems in order to achieve higher productivity and reduce machines breakdowns. This technology covers for example the installation of smart sensors able to analyse the machine performance in terms of machine status, energy usage and others machining parameters using power signals analysis [2], which allow optimising the machine usage and maintenance actions. However, to use these new smart applications (e.g. smart sensors, IoT technology, etc.) the manufacturers need to reconfigure the IT level to create the new generation of "smart legacy machines". In this context, it is challenging for the companies to identify a standard IoT architecture for all machines because they are all very different. Moreover, there is limited insight from literature about the advantages and disadvantages of the different IoT architectures in terms of cost, considering relevant parameters that impact on cost such as security and complexity. For example, monitoring systems for legacy machine tools raise security aspects related to data sharing and data protection that are associated to both hardware and software threats. These threats can cause machines breakdowns and data compromise that may represent drop in productivity and competitiveness, which in turn represent higher costs to the organisation and loss of profitability. On the other hand, mitigation strategies for these threats have associated costs that need to be assessed by the companies at the type of deciding to implement a smart manufacturing system. This paper provides guidance to the manufacturing organisations through a cost estimation model aiming at assessing different IoT architectures assembly, considering important parameters associated to smart manufacturing implementation such as complexity of the solution, level of vulnerability of the machines, and data loss caused by new cyber threats, and estimating their cost for implementation.

3. Related Work

The connection of millions of devices in both commercial and industrial applications is growing up [3]. Solution based on IoT technology can upgrade the data capabilities of manufacturing systems, pushing the integration of cloud computing and big data into smart manufacturing environments in order to realize connection from M2M which include the connections man-to-man, man-to-machine, and machine-to-machine [4]. In this way, this technology generates the common issues target for various attacks [5, 6, 7]. Many research projects have been proposed to develop remote monitoring and maintenance systems through IoT devices such as: [8], where the authors developed a wall-mounted boiler remote monitoring and control systems based on cloud platform. In other related project; [9], where the authors developed an IoT application for fault diagnosis and prediction; [10], where a system called IoT for university has been developed, and [11], where the authors developed a security architecture for SOA-based IoT middleware based on data protection. These and many more publications present different remote monitoring and maintenance systems strategies to evaluate the performance of industrial machines. Also, a collection of the IoT papers focused on home, academic and industrial applications is available in literature. However, these examples do not cover issues related to cost assessment and estimation for the configuration and implementation of IoT architectures in the manufacturing environment. This paper introduces a cost estimation model for IoT architectures implementation.

4. Research Methodology

The methodology of this paper fits within the description of Soft Systems Methodology (SSM) [13]. This methodology proved to be effective in dealing with issues in socio-technical systems comprising technology, processes, and human involvement to function in the whole system in meeting a desired objective [14]. In the research, the objective consisted of assessing the cost for implementation of an IoT system in legacy systems. To achieve the aim of this research, the typical seven steps of the SSM methodology have been simplified and applied in four iterative steps as follows:

1. Understanding the state of practice of smart manufacturing implementation in legacy machines, and identifying the current challenges;
2. Reviewing the literature to analyse the state of art of IoT systems implementation within the context of smart manufacturing;
3. Identification of a suitable technique for developing of a solution to the research problem;
4. Identifying an IoT system for applying and validating the developed solution, identify the key elements of that system that impact its cost for development and studying the interrelationships between those elements towards application of the proposed solution. This flexible approach was taken in mind of the real world industrial context of IoT systems implementation in legacy machine tools (e.g. Industry 4.0), and to improve its practices through an iterative analysis, design and development of a solution for estimating the cost for implementation of an IoT system. An essential part of the study was the collaboration among researchers and practitioners. Within this process, there was an in-depth interaction with industrial practitioners, through semi-structured interviews, to understand the state of practice and to identify the current challenges experienced. In parallel with the industrial interaction, literature reviewed was carried out to identify related research results and to confirm a gap of research in this field. Also, modeling approaches were identified in literature and assessed in terms of their suitability to be applied to develop a solution to the research problem. The adopted technique was selected in agreement with all the researchers and based on their experience. A case study was also identified from literature where the proposed solution could be applied and validated. This case study consisted of an IoT architecture proposed in [18], and a number of assumptions were built based on empirical knowledge and literature results in order to allow the application of the proposed solution to this IoT architecture. The validation of the proposed solution through the case study analysis has been assessed by the researchers and it is believed to be innovative and a valuable conceptual solution for implementation that will aid for the organisations that plan to move towards the fourth industry generation.

5. Cost Assessment Model for Smart Manufacturing Implementation in Legacy Systems (CAM-SMILS)

This section presents a conceptual model called Cost Assessment Model for Smart Manufacturing Implementation in Legacy Systems (CAM-SMILS). As discussed before, the innovation of the legacy systems and the creation of smart manufacturing environments is a relatively new concept that brings challenges to companies in terms of assessing the benefits and drawbacks of the concept. This assessment covers aspects such as complexity, security, usability, and perhaps more important, cost. The importance of these elements in the smart manufacturing environment is widely discussed in literature. The cost is associated to various aspects such as: implementation cost, maintenance cost, security costs etc. The CAM-SMILS model aims at assessing the cost for implementation of an IoT system in legacy machine tools, considering the complex environment of smart manufacturing. The model is targeted to support decision-making at the management level, guiding the organisations in the best strategy for innovating their legacy systems by comparing the cost of different IoT architectures. The CAM-SMILS is based on a Rule Based Fuzzy Cognitive Maps (RBFCM) technique that allows a representation and interpretation of the dynamics and complexity of an IoT system. The technique is an advanced modeling approach that mitigates limitations of other well-known techniques such as neural networks and system dynamics [15]. The representation of the IoT elements is made by fuzzy directed graphs with feedback, which are composed nodes (concepts) and fuzzy links (relations). The concepts are fuzzy variables described by linguistic terms, and relations are defined with fuzzy rules [16]. The variables can be: causal, if they have causal influence on another variable (node); effect, if they are subject to that influence; and causal-effect if they verify both cases. Each variable is assessed in terms of defined attributes that will map the cause/effect of the rules.

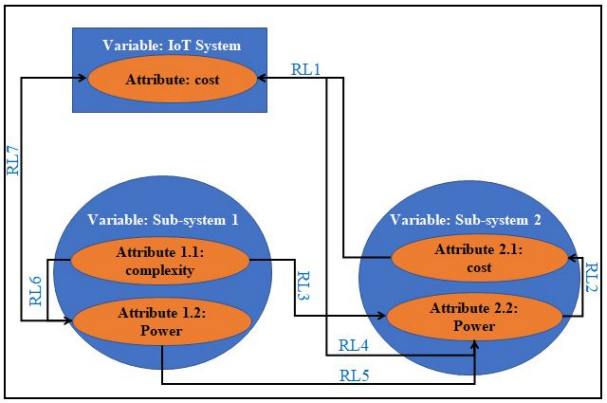

Figure 1: CAM-SMILS Model Description

Along these lines, the proposed model works as follows:

- Each element of the system (e.g. IoT system) is a variable. Each variable can also be broken-down in to sub-variables and so on;
- Each variable has associated one of more attributes, that will be used to define causal-effect relationships with other attributes through rules;
- Each attribute has a qualitative scale associated (e.g. low, medium, high). Different attributes can have different scales and they can have different levels of granularity;
- IF-THEN rules are used to build the causal-effect relationships, as adapted from [17];
- The overall system (e.g. IoT system) is itself a variable that has associated a cost attribute. This system is directly or indirectly subject to the influence of all the other variables of the model. A possible configuration of the model is illustrated in Figure 1. The figure considers three variables, which includes the IoT system and two elements of that system such as: sub-system 1 and sub-system 2. Each variable has also associated some attributes that indicate the characteristics of those variables that impact other variables. Possible links between the variables and respective attributes are labeled as RLx, where x is the ID of the link. Each link has associated a number of rules that establish the relationship between attributes. For example, let's consider the links RL1, RL2 and RL3, and let's assume that attributes 1.1, 2.2, 2.1 are all measured in the same scale which is defined as: low, medium, high. Let's also consider

that the cost attribute from the IoT system is measured in a scale defined as: very low, low, moderate, high, very high. Under these conditions, rules can be defined for each link that will impact in the overall IoT system' cost. These rules can be defined, for example, based on the opinion and experience of subject matter experts. Examples of possible rules are:

- **For link RL3**: low complexity of sub-system 1 cause high power in sub-system 2;
- **For link RL2**: high power in sub-system 2 causes high cost in sub-system 2;
- **For link RL1**: high cost in sub-system 2 causes medium cost of IoT system.

Other links and rules can be defined, and different configurations can be tested for each attribute in each variable, to assess the overall impact in the cost for implementation of the IoT system. There are also two other important aspects to refer about the model: the influence relation of multiple concepts, and the accumulation of impacts. When a rule involves two or more conditions to be verified (involving two or more different attributes) in order to define the impact in an attribute, Boolean operators AND or/and OR are used. Also, when two different rules impact the same attribute, that impact can be defined as cumulative using a pre-defined cumulative logic (e.g. medium + medium = high). The cumulative logic has to consider the different scales used to assess the different attributes.

6. Case Study of Application: A modular IoT architecture approach

Industry 4.0 requires legacy systems to upgrade their IT capabilities and create new services such as remote monitoring and remote maintenance [18, 19], using different standard communication protocols.

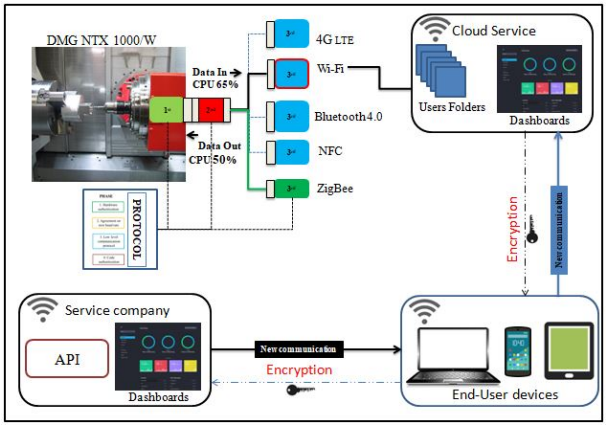

Figure2: The Modular IoT Architecture

Along with these lines, a new modular IoT architecture has been proposed in [18], to create a smart manufacturing environment upon legacy machine tools, as illustrated in Figure 2. That architecture is used in this work as a case study for validating the applicability of the CAM-SMILS model. A brief description of this IoT architecture is presented in Section 6.1. Then in Section 6.2, the important elements of this architecture are identified as well as their key attributes that impact the overall cost for implementation of the IoT system.
An application of the CAM-SMILS model to the presented IoT architecture is then outlined based on a set of rules that have been built from literature review results and empirical knowledge.

6.1. Case Study Description

The IoT architecture presented in Figure 2 fits into any legacy machine [18]. It is a new remote monitoring architecture, and consists of three modules managed with an authenticated protocol. The first module (green box) is the static part fixed on the machine as sensors, actuators, and transceivers. Depending on the operating environment, it is possible to find different scenarios. The second module (red box) is the transmitter consisting of the activation protocol to start the data collection. The third module (blue box/dark green box) is the transceiver able to share the data using different communication technologies. The modular architecture presented was designed to ensure a sealed

and secure IoT Unit. Between the modules there is a standardised communication interface using a hardware and software authentication protocol allowing access to the data only for authorised users. This architecture communicates at the Machine-to-Machine (M2M) level as well as into the cloud or end-user's device. The approach is designed to be auditable so that any misuse can be identified. The modular IoT Unit uses only a single sensor or actuator and a single communication component at a time. Limiting the size, the power supply and memory to process data is paramount. In terms of cost, cheap sensors can be applied with good resolution, good microcontrollers for monitoring and processing data as well as the different communication protocols for data sharing. This IoT architecture can be implemented with different kind of legacy systems and it is completely automatic as it only needs to plug the modules to each other. This architecture presents high flexibility to different working environments and a mitigation strategy to reduce its vulnerability to cyber-attacks.

6.2. CAM-SMILS model application

In the IoT architecture described, which will be denoted as IoT system, four sub-systems have been considered as shown in Figure 3(a). These sub-systems consist of:

Sub-system 1 - "Legacy system" - is characterized by the attribute cost of the machine tool and complexity of devices' implementation (e.g. the difficulty to equip the machine with external devices). This sub-system also includes sub-system 1.1 - "Smart sensors" – which regards the machine capability in terms of quality of the signals transmitted, signals speed and battery life-time. Sub-system 1.1.1 includes sub-system 1.1.1 - "Cyber-security" – which includes attributes as complexity of user authentication, vulnerability and the ability to avoid physical tampering on the device.

Sub-system 2 - "Cloud" - is characterized by the attributes: capacity of network storage and client platform in terms of compatibility level. It includes sub-system 2.1 - "Support service" – which concerns the level of autonomous service and software complexity that includes: technology used, bandwidth and connectivity. It also includes hardware complexity considering the networking equipment. Sub-system 2.1 includes sub-system 2.1.1 - "Cyber-security" – which involves attributes such as complexity of the authentication and security of the communication protocols.

Sub-system 3 - "Service company" - the attributes are: cost of hardware (e.g. application program interface (API), hard disks, etc.), and speed data monitoring. It includes sub-system 3.1 - "Cyber-security" – which involves attributes such as: complexity of user authentication and security of the communication protocols and avoid tampering attack to the hard disks.

(a) (b)

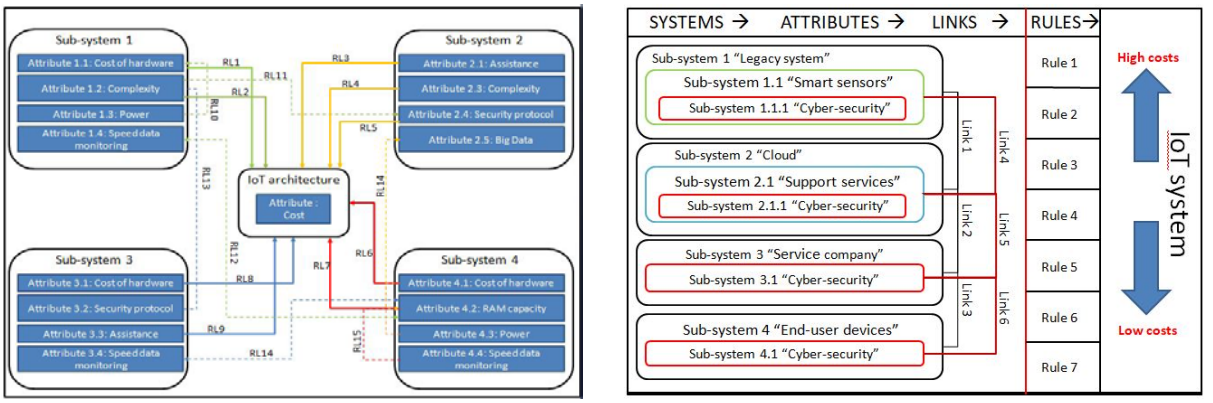

Figure 3: (a) IoT System Cost Model Application; (b) IoT Systems: Attributes, Links and Rules

Sub-system 4 - "End-user devices" - involves attributes such as: complexity, compatibility and quality of software and hardware parts (e.g. type of devices, category of devices, type of vendor, type of operative system (OS) version). It includes sub-system 4.1 - "Cyber-security" – which concerns about the attributes: support manufacturer, accessibility, and authentication protocols (e.g. to avoid physical access by unauthorized users). The links between the sub-systems described and that were considered for the case study analysis are described in Figure 3(b).

This figure is a representation of the system presented in Figure 2 in the form of a system of systems. For the purpose of analysis, all the attributes considered for each system will be measured in the same scale which is defined as: low, medium, and high, including the cost attribute of the IoT system. The sub-systems are connected to each other through the links RLx, x ∈ [1, 17], where each link has an association between two attributes from two sub-systems. To facilitate the interpretation of the links identified, they were divided in two categories where the first category (RLx, x ∈ [1,9]) have a direct link to the the IoT architecture cost, while the second category (RLx, x ∈ [10, 17]) involves direct links between sub-systems of the IoT system (e.g. indirect links to the IoT architecture cost).

Thus, for the first category of links the following rules were considered:

RL1: if the cost of hardware equipment for sub-system 1 is low, the cost of the IoT architecture is medium;
RL2: if the complexity of sub-system 1 is medium, the cost of the IoT architecture is medium;
RL3: if the assistance cost of sub-system 2 is low, the cost of the IoT architecture is medium;
RL4: if the complexity of sub-system 2 is high, the cost of the IoT architecture is high;
RL5: if the cost of the security protocol of sub-system 2 is low, the cost of the IoT architecture is medium;
RL6: if the cost of the hardware equipment of sub-system 4 is medium, the cost of the IoT architecture is high;
RL7: if the RAM capacity of sub-system 4 is medium, the cost of the IoT architecture is medium;
RL8: if the cost of the hardware of sub-system 3 is high, the cost of the IoT architecture is high;
RL9: if the assistance cost of sub-system 3 is low, the cost of the IoT architecture is medium;

For the second category of links, the following rules were established:

RL10: if the power of sub-system 1 is high, the cost of hardware for sub-system 1 is high;
RL11: if the complexity of sub-system 1 is low, the cost of security protocols of sub-system 2 is medium;
RL12: if the RAM capacity of sub-system 4 is low, the speed of data monitoring for sub-system 1 is low;
RL13: if the complexity of sub-system 1 is medium, the security protocol of sub-system 3 is low;
RL14: if the speed of data monitoring of sub-system 3 is high, the RAM capacity if sub-system 4 is high;
RL15: if the speed of data monitoring of sub-system 4 is high, the RAM capacity of sub-system 4 is high;

With these established links and rules, and using the logic of the CAM-SMILS model presented in Section 5 (after further implementation of the model in a simulation platform), the companies can see the impact on cost to implement the IoT architecture presented in Figure 2, and establish a cost-effective move to the Industry 4.0.

7. Discussion

The main challenge identified in this work is related to the cost estimation of the implementation of IoT technology in legacy systems. After an interaction with industry practitioners, as described in Section 4, it was possible to identify a lack of understanding in this field, which raises their uncertainty about the advantages and disadvantages of these new approaches, and in terms of cost. Moreover, literature also gives limited insight about this topic and no research has been identified that quantifies the cost for implementation of different IoT architectures. In this paper, the authors present the CAM-SMILS model that aims at being a conceptual solution to assess the cost for implementation of different IoT architectures. One important characteristic of the CAM-SMILS is the ability to perform the cost assessment based on qualitative input data. This is very important and in particular at the management level, as decisions can be made based on a quick and relatively easy assessment over the concept of IoT and smart manufacturing, considering subjective and hardly quantifiable aspects such as complexity, speed, and security. The CAM-SMILS is based on a RBFCM technique, which the authors believe to be an appropriate approach to assess the benefits and drawbacks of the legacy machines innovation, giving a high-level perception of the most effective IoT configuration according to cost expectations and targets.

8. Conclusion and Future Work

The outcomes of this research benefit organisations through the conceptual solution proposed to estimate and compare between the cost of different IoT architectures for their legacy systems. This study is also a lever to the research in this area, motivating further work in the field. Along these lines, the authors suggest a further implementation of the CAM-SMILS model in a simulation platform so that it could be applied in a practical industry scenario and assessed and validated with more confidence. It can also be applied to different IoT architectures in order

to allow a comparison between the cost of implementation of each one and identify the most suitable for a particular scenario.

Acknowledgements

This work is being undertaken with the EPSRC, grant number EP/I033246/1 and collaboration with the group Kennametal and was conducted in the EPSRC Centre for Innovative Manufacturing in Through-life Engineering Services. Many thanks also to DMG Mori who made the CNC turn-mill centre NT1000/W available for this research.

References

[1] Del Giudice, M., 2016 "Discovering the Internet of Things (IoT): technology and business process management, inside and outside the innovative firms" Business Process Management Journal, 22 (2). doi.org/10.1108/BPMJ-02-2016-0029

2] Deshpande, A.; Pieper, R. Legacy Machine Monitoring using power signal analysis. ASME 2011 International Manufacturing Science and Enginnering Conference MSEC2011, Corvallis, OR, United States 13-17 June 2011; pp. 207-214

[3] Vermesan, O., Friess, P.: Internet of Things - From Research and Innova-tion to Market Deployment. River Publishers, 2014.

[4] Tao, F., Cheng, Y., Xu, L.D. CCIoT-CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System. IEEE Transactions on industrial informatics, vol. 10, N.2, May 2014.

[5] Mehnen J., He H. , Tedeschi S., Tapoglou N. (2017).Practical Security As-pects of the Internet of Things. Cybersecurity for Industry 4.0, pp.225-242, doi:10.1007/978-3-319-50660-9_9

[6] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T.: Comprehensive exper-imental analyses of automotive attack surfaces. In USENIX Conference on Security. USENIX Association, 2011

[7] Cui, A., Stolfo, S.J.: A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan. In Annual Computer Security Applications Conference (ACSAC). ACM, 2010.

[8] Yonggang Gong, Aide Zhou, Yanan Xiao, (2014) "Design of wall-mounted Boiler Remote Monitoring and Control System based on the Ayla IOT Cloud Platform" Applied Mechanics & Materials, Issue 571-572: 1047.

[9] Chen Wang, Hoang Tam Vo, Peng Ni, (2015) "An IoT Application for Fault Diagnosis and Prediction" IEEE International Conference on Data Science and Data Intensive Systems: 726-731.

[10] Kamlesh Sharma ,T. Suryakanthi, (2015) "Smart System: IoT for University" International Conference on Green Computing and Internet of Things (ICGCloT): 1586-1593.

[11] Ramão Tiago Tiburski, Leonardo Albernaz Amaral, Everton De Matos, Fabiano Hessel, (2015) "The importance of a standard security architecture for SOA-based IoT middleware" IEEE Communications Magazine, 53(12):20-26.

[12] Janak, L., Stetina, J., Fiala, Z., Hadas, Z. (2016) "Quantities and sensors for machine tool spindle condition monitoring". MM science journal: 1648-1653.

[13] Delbridge, R., Fisher, S. (2007) "The use of soft systems methodology (SSM) in the management of library and information services: a review". Library Management, Vol. 28 Issue: 6/7, pp.306-322, https://doi.org/10.1108/01435120710774459.

[14] Md Saad Hasliza, N., Kasimin, H., Alias, A, R., Rahman, A, A. (2012) "Soft Systems Methodology: A Conceptual Model of Knowledge Management System Initiatives". International Joint Conference on Knowledge Discovery, Knowledge Engineering, and Knowledge Management. Vol. 415, pp. 377-392.

[15] Carvalho, J. P., & Tome, J. A. B. (2001). Rule based fuzzy cognitive maps - expressing time in qualitative system dynamics. 10th IEEE International Conference on Fuzzy Systems. (Cat. No.01CH37297). https://doi.org/10.1109/FUZZ.2001.1007303

[16] Seising, R., & Gonzalez, V. S. (2012). Soft Computing in Humanities and Social Sciences (1st ed.). Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-642-24672-2

[17] Petrovic Colinç Zdanowicz, Pawel, D. I. (2013). Modelling and Analysis of Defense Lines of Development Using Fuzzy Causal Maps with a Practical Example. In Proceedings of the 30th International Symposium on Military OR.

[18] S.H. Yang, Ch. Dai, and R.P. Knott (2007) "Remote Maintenance of Control System Performance over the Internet" Control Engineering Practice, 15(5): 533-544.[17] K. Feldmann, J. Gohringer (2001) "Internet based Diagnosis of Assembly Systems" Annals of the CIRP, 50 (1):5–8

[19] Tedeschi, S., Mehnen, J.,Tapoglou, N., Roy, R. 2017 "Secure IoT Devices for the Maintenance of Machine Tools". Procedia CIRP, Vol. 59, pp: 150-155