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.