Abstract

Currently Information and Communication Technologies (ICT) support most of the industrial manufacturing processes. The IT revolution has brought an important transformation in organizations with high impacts, which are comparable to the mechanization and electricity brought in the first and second industrial revolution. This evolvement has promoted the emergence of cloud-based systems, the Internet of Things (IoT), Big Data, Industry 4.0, BYOD (Bring Your Own Device) and CYOD (Choose Your Own Device) trends. However, new technological solutions always carry security vulnerabilities, which most of time reveal unexpected risks. In fact, with increasing reliance on technology to gain competitive advantage, security issues have been one of the most critical and challenging requirements for conducting successful business. In this paper, it is highlighted some reflections regarding the challenges of Industry 4.0 emphasizing the security issues, towards raising awareness for security good practices within Industry 4.0.

© 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the Manufacturing Engineering Society International Conference 2017.

Keywords: Industry 4.0; Information and Communication Technologies (ICT); Security Challenges; Security Incidents.

T. Pereira b,∗ L. Barreto a, c, A. Amaral a, b

∗Corresponding author. Tel.: +351 258 809 679; fax: +351 251 800 841.
E-mail address: tpereira@esce.ipvc.pt
1. Introduction

The first three industrial revolutions evolved through proper management of the mechanization, electricity and IT phenomenon. The recent trend of the Internet of Things (IoT) has heavily influenced the manufacturing environment and thus promoted the fourth industrial revolution – Industry 4.0. The forthcoming businesses will certainly establish global networks and incorporate their machinery, warehousing systems and production facilities as internet-enabled cyber physical systems. In the manufacturing context, these cyber physical systems comprise smart machines, storage systems and production facilities capable of exchanging information, triggering actions and controlling each other independently. In general, this brings significant improvements to the industrial processes involved in manufacturing, engineering, supply chain and life cycle management. In practice, products are uniquely identified, may be located at all times and it is possible to know their own history, current status and alternative routes for achieving their target state. It is deeply recognized and emphasized the huge potential of the Industry 4.0 among successful industrial companies, which will become true digital enterprises, with physical products at the core of its action, augmented by the digital interfaces and the development of innovative data-based services. For example, in Industry 4.0 dynamic business and engineering processes enable last minute changes to production and deliver the ability to respond with flexibility to the disruptions and failures on behalf of suppliers. End-to-end transparency is provided over the manufacturing process, facilitating optimized decision-making. Industry 4.0 paradigm will certainly also promote the development of new ways of creating value and innovative business models, in particular, it will provide startups and small businesses with opportunity to develop and provide downstream services [1]. It is undoubtedly that smart factories have already begin to appear, and introduce a completely new approach to production and supply chain management. But whenever there is a widespread change, new inherent challenges arise, particularly regarding information and communications security issues. The integration of new systems and their increased hypothetical potential third-party access mean that a whole new range of security issues arise in this context. Security is critical to the success of smart manufacturing systems. It is important to ensure the protection of the enterprise infrastructures as well as the data and information contained in their systems against misuse and unauthorized access.

In this paper, it is highlighted some reflections regarding the challenges of Industry 4.0 emphasizing the security issues, in order to raise awareness required in Industry 4.0. This paper is structured as follows: in section 2, it is introduced the current challenges of manufacturing industry processes, in the advent of Industry 4.0; in section 3, it is presented an overview of the security challenges organizations should be aware, including an overview of the major security threats; conclusions and further developments are presented in section 4.

2. Challenges in Industry 4.0

The term Industry 4.0 is recent and is related with the Information and Communication Technologies (ICT) evolution, particularly the integration of information technology, into the production processes. Industry 4.0 refers to the fourth in a series of technological revolutions: the first Industrial Revolution brought through the invention of the steam engine and the increase use of water and steam power, resulting into the mechanization of the industry at the end of the 18th century; The second industry revolution labeled as the “Mass Production” was promoted by the introduction of electricity and the assembly line at the start of the 20th century; Finally, the third era of revolution came with the advent of computers and the beginning of automation, when robots and machines began to replace human workers on those assembly lines. This third revolution era was known as “Information Age”, evolving to “knowledge-based economy”. The recognition of knowledge as “human capital” together with IT technology brought important impacts in economic growth, and consequently promotes the emergence of the fourth Industrial Revolution through the use of cyber technologies [2, 3]. The value proposition of the industry concept 4.0 is closely associated with the end-to-end digitization of all physical assets and with the integration into digital ecosystems of all value chain partners [4].

These cyber-technologies are leading to the creation of a “smart” and highly versatile cyber-physical production environment. It involves various smart sensors, connected self-configuring robots, cloud computing, 3D printing, device to device (D2D) communications, big data analytics and communication channels sending and receiving massive amounts of data. The integration of cyber-technologies turns products and services as internet-enabled, which facilitates the integration of processes and systems across sectors and technologies and thus contributes to a better...
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات