Computers in Industry 103 (2018) 97–110

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Cybersecurity for Industry 4.0 in the current literature: A reference framework

Marianna Lezzi*, Mariangela Lazoi, Angelo Corallo

Università del Salento, Dipartimento di Ingegneria dell'Innovazione, Campus Ecotekne, Via per Monteroni, s.n. 73100 Lecce Italy

ARTICLE INFO

Article history:
Received 2 July 2018
Received in revised form 7 September 2018
Accepted 10 September 2018
Available online xxx

Key words:
Cybersecurity
Industry 4.0
Industrial Internet of Things
Review

ABSTRACT

The cybersecurity issues represent a complex challenge for all companies committing to Industry 4.0 paradigm. On the other hand, the characterization of cybersecurity concept within Industry 4.0 contexts proved to be an emerging and relevant topic in the recent literature.

The paper proposes to analyse, through a systematic literature review approach, the way in which the existing state of art deals with the cybersecurity issues in Industry 4.0 contexts. In particular, the focus will be on the investigation of the main elements associated with cybersecurity theme (i.e. asset involved into cyber-attacks, system vulnerabilities, cyber threats, risks and countermeasures) within those industrial contexts where physical systems (machines, shop floors, plants) are connected each other via the Internet. Four areas of analysis are defined: definitions of cybersecurity and Industry 4.0 concepts, the industrial focus of the analysed studies, the cybersecurity characterization and the management attempts of cybersecurity issues. Through the literature review analysis, a framework of the main features characterizing each area is discussed, providing interesting evidences for future research and applications.

Contents

* Corresponding author.
E-mail address: marianna.lezzi@unisalento.it (M. Lezzi).

https://doi.org/10.1016/j.compind.2018.09.004
0166-3615/

1. Introduction

An ever-increasing number of companies are approaching to Industry 4.0 paradigm (even known as Industrial Internet of Things or Industrial Internet), by connecting the factories and plants to the Internet with the aim to improve their efficiency and effectiveness. In these Internet-connected industrial contexts, the cybersecurity issues represent one of the most relevant challenges to be dealt with.

According to the management-consulting firm, McKinsey & Company, Industry 4.0 transformations are potentially able to create value equivalent to efficiency improvements of 15 to 20 percent [1]. This means a reduction of total machine downtime thanks to predictive maintenance or remote monitoring, as well as an increase of labour productivity due to the automation of manual work. Moreover, a certain number of benefits result from the possibility to analyse the huge amount of data coming from industrial processes (for instance, from sensors and actuators which connect machines and products to computing systems). These benefits include the reduction of inventories and the improvement of service levels (in terms of shorter time-to-market, delivery time and freight costs) and of the product quality (more compliant to the customer expectations).

Within Industry 4.0 contexts, cybersecurity plays a leading role in preventing the loss of companies' competitiveness. In fact, critical industrial equipment is today vulnerable to a number of cyber-attacks, which are able to affect the entire business model. According to Cisco 2018 Annual Cybersecurity Reports [2], 31% of organizations have experienced cyber-attacks on Operational Technology (OT); while, 38% expect attacks to extend form Information Technology to Operational Technology. Although cybersecurity is perceived as a priority by 75% of experts, only 16% say their company is well prepared to face cybersecurity challenges [3]. This is mainly due to the lack of accurate standards to which companies can refer to, as well as the lack of managerial and technical skills necessary to implement them.

European and international organizations are moving in this direction. For instance, in 2017, European Cyber Security Organization (ESCO) collected in a document all existing standards and specifications related to Cybersecurity in reference to the European Digital Single Market [4]. This document helps to understand which schemes (if existing) can be used by companies to address the cybersecurity challenges. In addition, International Electrotechnical Commission (IEC) has published a guide on information security and data privacy [5], which provides guidelines to be covered in IEC publications, and explains how to implement them. IEC Publications are recommendations (accepted by IEC National Committees) for international use.

In the current fast-moving scenario, it is expected that cybersecurity will become an integral part of the strategy, design, and operations of companies that embrace Industry 4.0 paradigm.

Through a systematic literature review approach, the purpose of the paper is to investigate cybersecurity within Industry 4.0 contexts. A reference framework as basis of future research and applications in the field of cybersecurity management in such Internet-connected industrial contexts will be defined.

The next section of the paper describes the research method, and, in particular, the search process (which includes searching criteria definition, papers selection and their assessment). In Sections 3– 6, definitions of industry 4.0 and cybersecurity, the target industrial focus, cybersecurity characterization and managing of cybersecurity issues, based on the literature review, are respectively explored. The final sections, concerning findings and conclusions, end the paper.

2. Research method

This study adopts the systematic literature review approach [6] with the aim to characterize the cybersecurity concept within Industry 4.0 contexts. This was achieved by investigating: the target industries to which cybersecurity refers to and the industrial assets damaged; the typology of cyber-threats and the resulting risks for the industrial contexts; the countermeasures to be taken to deal with the cyber-attack events; the guidelines and solutions to manage cybersecurity issues.

According to the systematic approach, the literature review process was based on keywords and search terms with a replicable and defined search strategy. Although the literature review cannot be considered exhaustive, this provides a significant overview of the current role played by cybersecurity within Industries 4.0, revealing as an emerging research field at international level.

2.1. Search process

The search process consists of three main steps: (i) definition of searching criteria, (ii) papers selection, and (iii) papers assessment. The papers search was carried out through three important indexed electronic scientific databases: Scopus (www.scopus.com), Web of Science (www.webofknowledge.com) and Scholar (scholar.google.it). The research took place until March 2018. Chapters of books, as well as the non-scientific material coming from Google Scholar were not considered.

2.1.1. Searching criteria definition

The criteria for searching are based on the terms "cybersecurity" and "Industry 4.0". In order to strengthen the research, some of the most significant related words to the cybersecurity concept, as well as the most accredited variants of Industry 4.0 are taken into consideration.

In particular, concerning *cybersecurity*, the following definitions were considered to create a properly taxonomy:

- "The ability to protect or defend the use of cyberspace from cyber attacks" [7];
- "Preservation of confidentiality, integrity and availability of information in the cyberspace" [8];
- "All activities necessary to protect cyberspace, its users and impacted persons from cyber threats" [9];

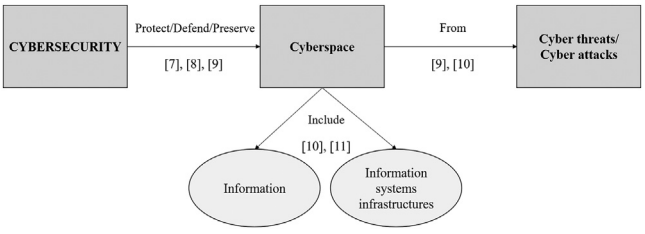

Fig. 1. Cyber security definition.