Proceedings of the 2019 International Conference on Industrial Engineering,
Quito, Ecuador
February 20-22, 2019

Challenges and Opportunities of Security in Industry 4.0

Nancy Velásquez[1], Elsa Estevez[2,3], and Patricia Pesado[1,4]

[1]Facultad de Informática, Universidad Nacional de La Plata (UNLP), Argentina

[2]Departamento de Ciencias e Ingeniería de la Computación, Universidad Nacional del Sur (UNS), Argentina

[3]Instituto de Ciencias e Ingeniería de la Computación, UNS-CONICET, Argentina

[4]Instituto de Investigaciones en Informática-LIDI, Facultad de Informática, UNLP, Argentina

Corresponding author's Email: nanve87@gmail.com, ece@cs.uns.edu.ar, ppesado@lidi.info.unlp.edu.ar

Abstract: Technological advances, disruptive technologies, behavior change and consumer habits are transforming productive systems. The industries have the need to manufacture customized products with flexibility, quality and efficiency. Industry 4.0 allows the change of the hierarchical model of traditional production, by a totally interconnected model, related to the smart factory, smart products and connected world to meet current demands.

Industry 4.0 incorporates the benefits of information technology and communications to the production chain, allowing to represent virtually the real production system, the digital management of the product life cycle and obtaining data of the entire operation in real time for decision making at different levels of the organization. In Industry 4.0, robots work collaboratively with people, creating an interconnected environment where security is an essential enabler, which guarantees the safety of people, fulfills market demands and the current legislation.

The aim of this study is to present the results of the comprehensive and holistic review of the Reference Architecture Management Industrial 4.0 (RAMI 4.0) of the Platform Industrie 4.0 of Germany, now converted into the German standard DIN SPEC 91345, the Industrial Internet Reference Architecture (IIRA) which is US sponsored by the Industrial Internet Consortium (IIC), industry standards such as IEC 62443 and information security and cybersecurity standards such as: ISO/IEC 27000, ISO/IEC 27032, security certifications sponsored by prestigious organizations in the environment of industrial control and information technology such as ISA, ISC2 to determine the challenges and opportunities for research and safety development in Industry 4.0, field in which there are tools and standards that can be applied directly, however others must be adapted and in most cases they must be created.

Keywords: Cybersecurity, information security, Industry 4.0

ISBN: 97819384961-5-8