Chapter 10
Industrial Cyber-Physical Systems Ensuring Safe Automation in Smart Manufacturing

P. William
https://orcid.org/0000-0002-0610-0390
Sanjivani College of Engineering, Kopargaon, India

Saiprasad Potharaju
Symbiosis Institute of Technology, Symbiosis International University, Pune, India

Ved Prakash Mishra
Amity University, Dubai, UAE

Ritesh Agwan
Sanjivani College of Engineering, Kopargaon, India

Pramod Kumar
Swami Rama Himalayan University, Dehradun, India

Gurpreet Singh Chhabra
https://orcid.org/0000-0002-3905-7974
GITAM School of Technology, GITAM University, Visakhapatnam, India

A. Sharmila
https://orcid.org/0000-0002-9871-3871
Raj Kumar Goel Institute of Technology, Ghaziabad, India

ABSTRACT

The adoption of Industry 4.0 technologies like cyber-physical systems, the internet of things, and connected services has radically changed manufacturing in a brief time. Smart production has evolved swiftly. Nevertheless, securely maintaining dependability, adaptability, and protection from cyber risks remains an important struggle. This work aims to enhance decision-making that considers people, optimize operations, and strengthen flexibility by merging socio-technical systems and

DOI: 10.4018/979-8-3373-1832-5.ch010

analyzing the progress from intelligent making to prudent production. By centering choices around human concerns and needs, competence and resilience can be increased for a changing world. The association of infrastructure, information, and services offers prospects to rethink creating things for betterment. The in-depth analysis explored how artificial intelligence has been utilized across various sectors, and investigated the impacts on key performance signs.

1. INTRODUCTION

The industrial sector has seen tremendous change as a consequence of the integration of Industrial Cyber-Physical Systems (ICPS) into Industry 4.0, leading to increased levels of automation, efficiency, and productivity. Through the combination of real-time data processing and computational intelligence, these technologies enable seamless communication between people and machines. However, in the realm of smart manufacturing, guaranteeing the security and safety of ICPS components remains a major obstacle (Alaya, Dafflon, Moalla, & Ouzrout, 2017). Cloud platforms, actuators, sensors, and networked industrial control systems are some of the components that make up the Industrial Control Programming System (ICPS). It has the ability to enhance industrial processes on its own. Despite the fact that contemporary technology offers many advantages, it also increases the danger of cyberattacks, data breaches, and system malfunctions. A security breach might result in financial losses for the business, disruptions to operations, and even harm to employees and equipment. The goal of this study is to examine the main issues related to the usage of ICPS in order to achieve safe automation in smart manufacturing. This article explores the risks associated with cybersecurity, potential solutions to reduce those risks, and how artificial intelligence (AI) might protect industrial automation. Furthermore, it emphasizes the creation of best practices, legal frameworks, and technological advancements to provide a safe manufacturing and production environment (Keating et al., 2003).

Safety concerns must be addressed if firms are to fully realize the potential of automation while lowering risks and guaranteeing adherence to industry standards. Cyber-physical systems must maintain strong security and safety features even when the industrial environment changes in order to guarantee dependable and sustainable smart production. Over the course of multiple time periods, two technologies that are helping to expand Industry 4.0 are the Internet of Things (IoT) and the Internet of Services (IoS). Cyber-physical systems, the internet of things, the internet of services, and the smart factory have been proposed as the four core elements that comprise Industry 4.0. As a result, the previously discussed concepts get confused, as seen in Figure 1. “Smart manufacturing” (SM), which includes “smart factories,”