ISSN Number: 2454-2024(Online)

International Journal of Technical Research & Science

CYBER SECURITY FOR DIGITAL MANUFACTURING

Abeera Jan, Arti Vaish
E-Mail Id: abeerajan.mhs20@sushantuniversity.edu.in, artivaish@sushantuniversity.edu.in
Sushant University, Gurugram, Haryana, India

Abstract-Digital production objectives to create rather customizable merchandise with higher nice and decrease costs with the aid of integrating Industrial Internet of Things, massive statistics analytics, cloud computing, and advanced robots into manufacturing vegetation. As manufacturing machines are more and more retrofitted with sensors as well as related through WIFI networks or stressed out Ethernet, digital manufacturing systems are getting more accessible than ever. While advancement in sensing, synthetic intelligence, and wireless technology permits a paradigm shift in production, cyber-assaults pose sizeable threats to the producing region. This paper provides a assessment of cybersecurity in digital production systems from system characterization, threat and vulnerability identification, manipulate, and hazard dedication components in addition to identifies demanding situations and future paintings.
Keywords: Digital manufacturing, cyber physical systems, security indicators, system sustainability, homeostasis, information security, self-similarity.

1. INTRODUCTION

Digitalization of manufacturing aided by using advances in sensors, artificial intelligence, robotics, and networking era is revolutionizing the traditional manufacturing enterprise by rethinking production as a service (1). Concurrently, there may be a shift in call for from high-volume production to batches-of-one, custom production of merchandise. The contemporary stage of improvement of technological know-how and technology is characterized by an lively transition from automated to virtual manufacturing. This transition involves the transformation of the present technological infrastructure, the combination of technology and current traits right into a international multi-degree and multi-thing machine that could absolutely change the existing technological structure and bring all sectors of the united states of America's activity to a new competitiveness stage (2) . As one of the key permitting technologies for virtual manufacturing, cloud-primarily based production refers to a carrier-oriented production paradigm wherein carrier clients perform layout and manufacturing obligations the use of cloud-based totally digital design, engineering analysis, manufacturing programs.

2. SYSTEM CHARACTERIZATION

To determine dangers for a manufacturing machine, step one is to discover the additives, sources, and facts that constitute the device (4). A production system includes five layers, which includes agency useful resource making plans (ERP) systems, manufacturing execution structures (MES), SCADA and PLCs, sensors and actuators, and commercial protocols (3). A production execution system is a manipulate gadget that improves productivity and decreases cycle time by way of tracking and controlling production machines in actual time. A SCADA gadget consists of supervisory computer systems, remote terminal gadgets, PLCs, communique infrastructure, and a human-gadget interface. A SCADA device gathers records on manufacturing strategies from PLCs, sensors, and actuators as well ascends control instructions to the sector related gadgets (11_15). PLCs according to form sequential relay manipulate, movement manipulate, and method control. Virtual production system model consisting of records era (IT) and operational technology (OT) systems (5). The IT systems use computer systems to save, retrieve, transmit, and method layout- and production-associated facts including CAD models and CNC packages. The OT systems use hardware (e.g., sensors and PLC) and software program (e.g., SCADA) to reveal and manipulate manufacturing device (e.g., valves and pumps) and manufacturing techniques (e.g., milling and turning). With the emergence of the Eliot technologies, IT systems used for data-intensive computing has been incorporated with OT systems used to reveal and manage occasions, methods, and gadgets.

3. VULNERABILITY AND THREAT

After characterizing a production device, the following step is to pick out threats and vulnerabilities. According to the NIST's risk management manual for facts era systems, a chance refers to "the capacity for a specific chance-source to successfully exercising a particular vulnerability" (6). A risk supply refers to "any condition or event with the potential to cause harm to an IT system." A vulnerability refers to "a flaw or weakness in system protection tactics, layout, implementation, or inner controls that could result in a safety breach or a contravention of systems' safety policy." An attack refers to "a try to advantage unauthorized access to system offerings, sources, or information, or a try to compromise device integrity." Cyber-enablement and interconnectivity of DSNs introduce threats along with financial robbery and theft of IP (7_10). Some of the threats are specific to DM which includes digitally printing dangerous or unlawful additives, stealing competitor IP (e.g., the layout documents), editing them, and production

counterfeits or substandard additives, and deny service via taking production flora or important components of the manufacturing vegetation (e.g., printers) offline. The attackers may additionally have exclusive motivations, consisting of: 1) country nation actors; 2) prepared criminals; 3) politically, socially, or ideologically influenced hacktivists; 4) hackers with monetary benefit or sabotage rationale; 5) competition; and 6) malicious insiders (8). The motivation of the attacker, sources to be had, and the damage caused in each category may be special and should be part of the danger evaluation.

4. CONTROL METHODS

After identifying threats and vulnerabilities, the following step is to analyse the controls that could be applied to do away with a listing of get admission to manipulate strategies or minimize the opportunity that the vulnerabilities may be exercised (9). Security controls are a fixed of moves that locate, counteract, or limit safety dangers. Some methods are here access control, encryption, authentication, and intrusion detection.

4.1 Access Control

Access Control is the selective limit of get admission to infrastructures and assets. Access manage strategies can be categorised into four classes, which includes position-primarily based, characteristic-based totally, context-based totally and consider-primarily based get right of entry to control.

4.2 Encryption

In cryptography, encryption refers back to the procedure of encoding a message in a way that best legal parties can get admission to it. Encryption is often carried out in steady communique protocols together with Internet Protocol Security (IPsec), Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), and Wi-Fi Protected Access (WPA). These stable conversation protocols assist diverse encryption algorithms.

4.3 Authentication

Authentication is a manner in which the credentials provided are in comparison to the ones on file in a database. A user may be authenticated through three factors: what the consumer is aware of (memo metrics), what the person acknowledges (cognometrics), and who the user is (biometrics).

4.4 Intrusion Detection

Intrusion detection is a technique wherein activities in a network or laptop machine are monitored for possible safety problems. Intrusion detection includes tracking of device activities, auditing of system vulnerabilities, statistical analysis of activity patterns, and unusual hobby analysis.

5. RISK DETERMINATION

Risk determination entails assessing the extent of threat to a production system. Mathematical modelling methods based totally on probability principle, fuzzy setts, neural networks are normally used to evaluate risk degrees. Cherdantseva et al. performed an overview of cybersecurity risk assessment methods for SCADA structures (11). An overview of twenty-four hazard assessment strategies for SCADA structures become provided. Henry et al. [83] developed a technique to quantify the chance of cyber-assaults on SCADA structures using Petri Nets (16). This method permits a proper assessment of candidate regulations to manage risks by way of the diminishing elements of the community vulnerability to intrusion. A new algorithm became developed to robotically generate the Petri internet version that represents a SCADA gadget. Experimental effects have proven that the method is able to evaluating the protection of a risky liquid loading manner correctly (12). Roy et al. introduced an attack-countermeasure tree-based technique for modelling and analysing cyber-attacks. The attack-countermeasure tree allows qualitative and probabilistic evaluation of cyber-assaults in addition to the optimization of defence strategies.

CONCLUSION

This paper offers a review of the maximum critical aspects of cybersecurity in virtual production with a particular recognition on machine characterization, identity of threats and vulnerabilities, attack scenarios, manage techniques, and threat determination strategies (13). As superior sensing, excessive performance computing, synthetic intelligence, and facts analytics technology are increasingly exploited in cutting-edge digital factories, cyber safety is turning into a number one concern for producers. Not all members in a production deliver chain may additionally have the identical level of assets to implement the maximum superior defences. The weakest links in a deliver chain, besides compromising their own property, might also compromise the belongings of all contributors within the supply chain. This is mainly proper for the MSEs, with restricted assets, who despite the fact that have to embody the adoption of digitalization and DM.

REFERENCES

[1] http://refhub.elsevier.com/S0278-6125(18)30039-6/sbref0005

[2] V. Woollaston. (2017). Wannacry is Back! Virus Hits Australian Traffic Cameras and Shuts Down a Honda Plant in Japan. Accessed: May 2020.
[3] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," Proc. IEEE, vol. 105, no. 2, pp. 219–240, Feb. 2017.
[4] R. K. Behera, S. Sivaprakasam, L. N. Jagannathan, and N. Gupta, "System and method for security and management of computer-aided designs," U.S. Patent 16 657 048, Oct. 18, 2019.
[5] K. Yanamandra, G. L. Chen, X. Xu, G. Mac, and N. Gupta, "Reverse engineering of additive manufactured composite part by toolpath reconstruction using imaging and machine learning," Composites Sci. Technol., vol. 198, Sep. 2020, Art. no. 108318.
[6] Y. Gao, B. Li, W. Wang, W. Xu, C. Zhou, and Z. Jin, "Watching and safeguarding your 3D printer: Online process monitoring against cyber-physical attacks," in Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol., vol. 2, no. 3, pp. 1–27, 2018
[7] A. Slaughter, M. Yampolskiy, M. Matthews, W. E. King, G. Guss, and Y. Elovici, "How to ensure bad quality in metal additive manufacturing: In-situ infrared thermography from the security perspective," in Proc. 12th Int. Conf. Availability, Rel. Secur., 2017, pp. 1–10
[8] A. E. Elhabashy, L. J. Wells, J. A. Camelio, and W. H. Woodall, "A cyber-physical attack taxonomy for production systems: A quality control perspective," J. Intell. Manuf., vol. 30, no. 6, pp. 2489–2504, Aug. 2019.
[9] M. Wu et al., "Establishment of intrusion detection testbed for CyberManufacturing systems," Procedia Manuf., vol. 26, pp. 1053–1064, 2018
[10] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, "Intelligent manufacturing in the context of industry 4.0: A review," Engineering, vol. 3, no. 5, pp. 616–630, Oct. 2017.
[11] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," J. Manuf. Syst., vol. 47, pp. 93–106, Apr. 2018.
[12] Retière, N., et al., Fractal grid—towards the future smart grid, CIRED 2017—24th International Conference on Electricity Distribution, 2017, p. 1236