Information Security and Adoptable Solutions in the Implementation of Industry 4.0 Strategy for the Fourth-generation Industrial Revolution

Xiaolei Cheng¹,²*, Pinghua Zhang³
¹ Science and Engineering Department, Wanbo Institute of Science and Technology, Hefei, Anhui, 230031, China
² Hefei University of Technology, Hefei, Anhui, 230009, China
³ Hefei Technology College, Hefei Anhui 230000, China;
*yangpeizhou@hfut.edu.cn
*Corresponding author’s e-mail: chengxiaolei1982@163.com; 87328113@qq.com

Abstract. Industry 4.0 is recognized as the fourth-generation industrial revolution, which can drive the development of the world's smart manufacturing industry. The information security in the implementation of Industry 4.0 strategy was analyzed in this article. The specific measures to ensure the information security of Industry 4.0 were proposed from the perspectives of industrial control system security strategy, security measures, security awareness, data security protection, data security responsibility, and encryption technology. Furthermore, the distributed control system and IT network security communication platform construction are applied to solve the information security problem of Industry 4.0. The adoptable solutions will provide an important reference to maintain the information security of Industry 4.0.

1. Industry 4.0 Strategy
In order to seize the opportunity in the latest round of the industrial revolution, under the strong promotion of the German Academy of Engineering, Siemens, Fraunhofer Association and other top German academics, the German government officially launched the "Industry 4.0" strategy at Hannover Messe in April, 2013. Industry 4.0 is to enhance the global competitiveness of the German manufacturing industry, protect the domestic manufacturing industry, and support the development and innovation of revolutionary technologies in the industrial field based on a comprehensive analysis of the advantages and disadvantages of the industrial development of the United States, China, Russia, India and other countries. To make Germany a leader in providing solutions to global challenges, the “High-Tech 2020 Strategy” focuses on five priority areas for Germany’s future development including climate/energy, health/food, mobility, security and communications. Industry 4.0 is one of the top ten strategies of the German government to clarify the future [1].

The implementation of Industry 4.0 is recognized as the fourth industrial revolution. Different from the previous three industrial revolutions, Industry 4.0 deals with real-time management of power and information technology, so that efficiency gains and resource productivity run through the entire value network. Intelligent assistance systems help workers free themselves from performing specific tasks, allowing workers to focus on innovative value-added activities. In response to the worldwide problem of the shortage of skilled workers, Industry 4.0 can help extend the working life of workers,
improve their productivity and improve their career development opportunities. The key areas involved in Industry 4.0 include: (1) standardization and reference architecture; (2) management of complex systems; (3) comprehensive broadband infrastructure; (4) safety and security; (5) organization and design; (6) training and continuous professional development; (7) rules and regulations; and (8) resource utilization efficiency[2].

2. Security issues of Industry 4.0

In the past, people did not know much about IT threats, and did not pay enough attention to the security of equipment and machines. As malware Duqu, Stuxnet, and flame seriously threatened the security of industrial control information systems, industrial IT security was gradually affected by equipment manufacturers and operators. In particular, the “Stuxnet virus” attack on Iran’s nuclear power plant in 2010 caused many countries to worry about the information security of industrial control systems. Subsequently, major industrial powers raised the security of industrial control to a strategic level. The security of the Industry 4.0 strategy is an important guarantee for the smooth implementation of the fourth industrial revolution. The security of manufacturing equipment and its products is extremely important. The areas of security mainly include: (1) safety for people and the environment; (2) the safe equipment and its products, especially to protect the key production data and its operation mode, to avoid mis-operation and unauthorized access. The former considers factors related to production equipment and manufactured products, while the latter involves production safety that is constrained by the overall mechanism. Regulations and standards should be formulated to ensure the normal operation of the system.

From the Industry 3.0 era (information technology and electromechanical integration), the manufacturing industry’s requirements for production and information security have increased dramatically. At present, many of the operational safety and information security solutions that appeared in Industry 3.0 have not been completely completed, especially in the field of security assurance. The solutions provided are not comprehensive. With the advent of the Industry 4.0 era, information security requires higher quality security standards. In addition, Industry 4.0 imposes many additional safety requirements. The intelligent manufacturing system of Industry 4.0 integrates a large number of workers, computer systems, automation components, and machine equipment into an organic system with a highly networked system structure. A highly temporal data and information exchange occurs between system components. In addition, the self-conscious workers (workers and managers) in the system are involved in the value chain of the system. Industry 4.0 based on cyber-physical systems (CPS, Cyber-Physical Systems) is facing extremely severe security threats. In addition to operational security, the network security and unpredictable third-party access are new security issues encountered by Industry 4.0 [3].

Compared with the traditional industrial model, the operation of the Industry 4.0 strategy requires a more active security assurance program. In addition, the problem-solving program is constantly changing and needs to be revised and improved in practice. Therefore, the security of Industry 4.0 cannot be mechanically divided into functional components, but should be adjusted and developed in time according to the actual situation. In the response process of the plan, it is very important to support comprehensive information exchanges across departments to achieve rapid response time. In addition, measures such as risk assessment indicator monitoring will help prevent the rapid spread of software viruses and network attacks.

3. Adoptable solutions

In order to actively respond to the security threats of intelligent manufacturing Industry 4.0, the technical support needs to be strengthened from the following perspectives.

3.1. Ensure safety from the design

In traditional industrial information security maintenance, the physical measures are mainly used to protect against external attack threats. For example, access restrictions and other central control
security measures are used to isolate the external environment and maintain its own operation. In a cyber-physical system-based Industry 4.0 strategy production system, it is far from enough to simply add measures related to security functions to the entire system. In the field of information security, the security measures must be added from the equipment production design stage. In the system, this security measure also needs to be able to dynamically adjust[4].

3.2. Safety measures
The implementation of security policies and architecture standards can give the system a high degree of confidentiality, availability and integrity, and can promote the interaction between networked and heterogeneous components. The maintenance of intellectual property rights and data in the process of industrial digitization requires manufacturers and operators to provide a reliable solution in advance. In Industry 4.0, it is very necessary to take global security measures and necessary to consider the impact of encryption procedures and authentication procedures on time-critical functions and resource availability. In addition, a dual strategy (dual insurance) is adopted to ensure the safety of Industry 4.0. Firstly, upgrading the internal security measures of the factory, strengthening the protection of the maintenance and update of the machinery and equipment, and proposing an operational emergency plan; secondly, the new factory and new machinery develop a solution plan. In the transition phase from the third to the fourth industrial revolution, to achieve as seamless and smooth transition as possible, both equipment providers and operators need to deeply understand the differences between the two generations of industrial revolutions, especially the fourth generation of industries. The entire value chain in the revolutionary Industry 4.0 strategy involves the safety and architecture of all actors.

3.3. Safety awareness
Industry 4.0 faces many security challenges. In addition to technical factors, the security solutions also include business, psychological and educational issues. Due to the lack of standardized security operation platform, it is difficult to provide high-quality and safe solutions. The existing infrastructure can’t be expanded or upgraded, many security solutions are fixed, and the space for adjustment is very small, which affects the synchronous upgrade and security measures. The long industrial chain of Industry 4.0 requires the mutual trust of the owners in each industry chain. The network connection, psychology and education level of partners in each value chain directly determine the safe implementation of Industry 4.0 to a certain extent[5].

3.4. Data security protection
Big data is produced with the maturity of Internet technology and its wide application in intelligent factories. In the industrial chain of Industry 4.0, thousands of companies and research institutions are involved. Not only are the affiliated institutions dynamic, but also the dynamic changes of the company network may occur, forming a new value chain. Under the background of intelligent manufacturing, a large number of new data can be generated independently, and can be transmitted to the outside according to the needs. Most of these huge databases are harmless data, but there are also some important sensitive data. In the process of intelligent machine outward transmission, inevitably beyond the controllable range, some external data may be used by competitors or third parties. If enterprises want to protect their own competitive advantages and avoid the negative impact of information leakage, they can balance the interests of enterprises in the industrial chain by sharing fees, so as to ensure the fair sharing of information resources among enterprises. In the way of information sharing and exchange fees, the dynamic pricing mode or fixed pricing mode can be adopted. At the same time, the corresponding cooperation agreements to protect the interests of all parties need to be signed.

3.5. Enterprise data security
Enterprise data can be generally divided into trade secret data and trade secret data. At present, the data protection regulation of most enterprises only deals with the sensitive areas involving their own
direct interests and the future of the enterprise, and those that can protect and investigate the responsibility of the other party are only applicable to the premise of illegal disclosure. In the context of big data generated in the process of intelligent manufacturing, a large number of data are legally obtained, and even some confidential information is also legally obtained by the adversary, and then the key information may be used for other purposes. In the Industry 4.0 system, the self-restraint of each value chain can better block the loopholes in the law, such as signing confidentiality agreements, controlling a large number of data within a certain range, limiting a large number of new data generated within the industrial chain, thus blocking the channels of data leakage and protecting the interests of all parties[6].

3.6. Responsibility for data security
Under the Industry 4.0 strategy, the data of companies in the value chain need to exchange and share resources including some sensitive data. These data will inevitably produce certain risks. These data may be illegally occupied and used, or leaked to the third party through illegal channels. There are also some parties that can accept the information lack of security measures, which are attacked by third-party hackers, leading to critical numbers according to the leakage and its legal protection is also very difficult. To solve the data security under the condition of big data, we can define the technical standards and determine additional measures to punish the behavior of violating the agreement. The intelligent manufacturing equipment of Industry 4.0 receives intelligent control, and the data generated involves all fields of the product, including shape, performance, material, etc. Once the information is leaked, serious consequences will inevitably occur. The person responsible for information leakage should not only bear the legal responsibility for product loss, but also the responsibility for the intelligent network fault. Therefore, the method of responsibility identification is very important. Due to the lack of structural transparency in the network of autonomous system deployment and the whole value chain, it is impossible to clearly determine who performs a specific action, and the generated data is difficult to determine which specific intelligent machine is sent out, which has uncertainty in legal liability. In order to clarify the responsibility, the enterprise assembly line is equipped with an independent data processing system, which is responsible for the safety of production facilities and products. If the partners want to avoid joint and several liability in law and have the right of recourse to other partners, then before the implementation of the project, all parties need to clarify their system legal liability through agreements, contracts and other forms[7].

3.7. Encryption technology
In the complex system of Industry 4.0 chain, some components may be restricted by domestic and international trade. Encryption technology can ensure the integrity and confidentiality of information physical system. In the field of software protection technology, the main measures are serial number protection, time limit, key file protection, cd-check, softdog, floppy disk encryption, combination of software and hardware information. In the international market, countries have special requirements on encryption technology. For example, China is only allowed to export and use encryption products within the scope set by the license, while EU only allows encryption technology to be applied to Europe and some specific countries, including the United States, Japan and Canada. Some companies hope to achieve the market monopoly of their products through encryption technology, which is easy to cause technical and trade barriers.

Based on the strategy of industrial control system security, the security of industrial control system not only directly affects the production of enterprises, the safety of employees’ life and property, but also may involve the safety of industry or national level. The power failure in Shenzhen on April 10, 2012 caused a power outage of more than two hours in Futian resulting in a direct economic loss of nearly 1 billion yuan. On November 22, 2013, the oil pipeline of Sinopec Weifang branch company was broken, and the direct economic loss was more than 750 million yuan. In addition, a large number of innocent people were killed and injured. In June 2013, Edward Joseph Snowden, a former U.S. intelligence officer, disclosed the documents of the US National Security Agency monitoring program
to the Washington Post. On June 21, 2013, Snowden again exposed the secret surveillance project of "temporal watch" in the UK. Snowden's "prism door" reflects the hidden worries of China's information security. There are countless cases of enterprise theft all over the world, which seriously affect the normal operation of industrial manufacturing and trade[8].

4. Industry 4.0 strategy application

The Industry 4.0 strategy will connect resources, materials, things, people, information and services, innovate and transform the existing manufacturing industry, and integrate intelligent machines, production facilities and storage systems into information/physical systems. Purdue University has proposed a classic five-layer control model for integrating automation and informatization, which are: L1 layer/field equipment layer; L2 layer/process control layer; L3 layer/production execution layer; L4 layer/operation management layer; L5 layer/strategic decision layer. External Internet and internal malicious attacks may cause information leakage of the whole network and even system crash. The biggest threat comes from the third party's on-site operation, remote dial-up attack and field network attack. The international security manual "industrial control system security guide" (NIST sp800-82) describes the network threats of industrial control in detail, and describes the information security risks of the system and the vulnerability of the network. The emphasis of security in different fields is quite different. Military system emphasizes information confidentiality, power system emphasizes uninterrupted dispatching system, petrochemical emphasizes production continuity, Industry 4.0 not only emphasizes the stability of the whole system operation, but also attaches importance to information confidentiality. At present, the industrial enterprise information integration system (GT/T) is commonly used by enterprises (26335-2010) can't adapt to Industry 4.0, especially industrial control information security needs to be adjusted properly[9].

Any enterprise attaches great importance to the safety of production. Protocol and network detection and protection are used in industrial network to ensure information security. At present, the internationally popular communication protocol names and their suppliers are Modbus/Modicon, PROFIBUS/Siemens, OPC/OPC foundation, foundation fieldbus/Fisher Rosemount, Ethernet/IP/ODVA, ControlNet/Rockwell, DeviceNet/Allen Bradley, CC link/Mitsubishi Electric Co., Ltd. of Japan, EtherCAT/befell of Germany, p-net/Danish process data company, WorldFIP/Alston of France, INTERBUS/Phoenix Contact of Germany, and can/Rober Bosch Company of Germany.

5. Conclusions

With the development of intelligent equipment and networked control system, software has an obvious value-added effect on mechanical equipment manufacturing products, and the number of embedded software components in the equipment is increasing rapidly. Industry 4.0 involves voice signal, high-speed image rate and big data transmission. The maturity of Ethernet and control network technology promotes the combination of them. Multi standard industrial control network interconnection technology, wireless technology, embedded technology and other technologies accelerate the integration under the promotion of network tide, which expands the development space of industrial control, brings new opportunities, and also puts forward higher information security requirement. In Industry 4.0, network system security is paid special attention to. It is the key to implement Industry 4.0 to take active strategies to ensure network security and prevent the infringement caused by hackers and network spies. The big data generated by the interaction between a large number of components related to Industry 4.0 and the management platform related to equipment data exchange are also new automatic control concepts. The distributed control system and the construction of IT network security and efficient communication platform are helpful to solve the information security problem of Industry 4.0.

Acknowledgments

The research is supported by the provincial quality project of Anhui Province for the major online teaching reform research project (grant No. 2020zdxsjsjg381) and academic funding project for top-
notch discipline (specialty) talents in colleges and universities of Anhui Province in 2020 (grant No. gxbjZD2020116).

References
[1] Sabine Pfeiffer. (2017) The vision of “Industrie 4.0” in the making-a case of future told, tamed, and traded. NanoEthics, 11:107-121.
[2] Andreas Huber, Astrid Weiss. (2017) Developing human-robot interaction for an Industry 4.0 robot: how industry workers helped to improve remote-HRI to physical-HRI. Conference: Companion of the 2017 ACM/IEEE International Conference, 137-138.
[3] Haihui Gao, Yong Peng, Kebin Jia, Zhe Wen, Hanjing Li. (2015) Cyber-physical systems testbed based on cloud computing and software defined network. Conference: 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 337-340.
[4] Yude, Shuilan, (2018) Optimal prevention and control strategy against preconceive faults in electric cyber-physical system. 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), 1-9.
[5] Jan Stodt, Christoph Reich. (2020) Data confidentiality in P2P communication and smart contracts of blockchain in Industry. Conference: 10th International Conference on Computer Science, Engineering and Applications (CCSEA 2020), 4.0:1-10.
[6] Da Xu, Lian Duan. (2019) Big data for cyber physical systems in Industry 4.0: a survey, Enterprise Information Systems, 13(2): 148-169.
[7] Gunasekaran Manogaran, Chandu Thota, Daphne Lopez, Revathi Sundarasekar. (2017) Big data security intelligence for healthcare Industry 4.0. Cybersecurity for Industry 4.0, 103-126.
[8] Md Mehedi Hassan Onik, Dr Miraz, Chul-Soo Kim. (2018) A recruitment and human resource management technique using blockchain technology for industry 4.0. Conference: IET Smart Cities Symposium 2018 (SCS ’18) at: University of Bahrain, Bahrain, 1-40.
[9] Jaione Ganzarain, Nekane Errasti. (2016) Three stage maturity model in SME’s toward Industry 4.0. Journal of Industrial Engineering and Management, 9:1-8.