THE SAFETY ANALYSES FOR CYBER-PHYSICAL SYSTEMS IN INDUSTRY 4.0

Major: **Automotive engineering**

Name: **Li angwei**

Student number: **S243267**

Professor: **Micaela.demichela**

Date: **2018/8/22**

ABSTRACT

This paper introduces the background of Industrial 4.0 and through a comparison with the previous three industrial revolutions, emphasizing on the core idea which is put forward as the deep fusion of information systems and physical systems. Through the introduction of physical information fusion systems, we begin to analyze the interaction between the open interconnected network, its associated information along with the physical components, which makes the cyber-physics system face great security challenges. This paper presents research on Cyber Physics Department Security targets and the attack model of the unified system, giving an in-depth description about the security structure of layered information physical systems. The security of cyber physical system primarily exists to solve encryption technology in the case of malicious attacks, access control strategies, elastic mechanisms and so on. After introducing research relating to the cyber physical system security, key technologies such as the access control strategies and the privacy data protection mechanisms in the security layout of the cyber physical system are studied deeply. Finally, from the point of view of intelligent manufacturing, this paper analyzes the security problem of CPS, which has the characteristics of data-driven, software definition, ubiquitous

connection, virtual reality mapping, heterogeneous integration and system autonomy, and should adopt the combination of "autonomy" and "common governance" to establish its security framework from the aspects of perception, transmission, computation, control and service. Also introduce the focus and direction of CPS research, such as blockchain.

Keyword: industry 4.0, cyber-physical system, safety, encryption technology, access control, privacy data protection, blockchain.

INTRODUCTION

Cyber-physical System, CPS is the further extension and development of the Internet. Small to medical device systems, large to industrial-grade smart grid systems, CPS has a broad application prospects. Similar to the Internet changes the way that people interact, the advent of CPS will profoundly change the way that people interact with the physical world, and it is another information revolution. In recent years, with the development and maturity of embedded technology, wireless sensor technology and cloud computing technology, CPS has become the research hotspot of information technology. CPS realizes the integrated design of computing, communication and physical system, makes the system more reliable, efficient, real-time synergy, has an important and extensive application prospects, Especially in Industry 4.0, CPS has a wide range of applications, but because this technology is not very mature, so there are many security problems, so in this paper, we will focus on the analysis of CPS safety and security applications.

CHAPTER 1 INDUSTRY 4.0

1.1 Introduction

1.1.1 The birth of Industrial 4.0

In the 2011 Germany Hannover Industrial Exposition, a German Association began introducing the initial concept of Industry 4.0. After subsequent efforts made by other associations such as the German machinery association and the equipment Manufacturers Association led by experts from enterprises, governments and research institutions established the "Industry 4.0 Working Group" to further strengthen the Industrial 4.0 research and promote better reporting to the German government. In 2013, the Industrial 4.0 Standardization Road map was published and the Industrial 4.0 platform was set up with widespread participation of associations and enterprises. The German government also incorporated industrial 4.0 into its “High-tech Strategy 2020”, turning industrial 4.0 into a successful national strategy. At present, Germany is planning to promote industrial 4.0 in the context of relevant laws, whereby the industrial 4.0 will take industrial policies up to the level of national law. The uptake of industry 4.0 in Germany occurred in a very short period of time by the parties, Governments, enterprises, associations, institutions and quickly became widely recognized. It

reached a consensus owing to its focal point aligning with the concept of rapid evolution of civil society and strategic national industry, going from an industrial policy to the level of national law. Industry 4.0 has been widely recognized in Germany in relatively short time and thus there is contingency and inevitability, which comes from Germany's long-standing cornerstone of industry as a national economy. This comes from the revolutionary impact of information and communication technology on industry, as well as the fear surrounding Germany's industrial status in the modern-day state of technological revolution in the world.

1.1.2 Content of Industry 4.0

Industry 4.0 depicts a personalized and digitized vision of an intelligent manufacturing model with effective universal communications for personal, equipment and product use. From the point of industrial technology development, Industrial 4.0 highlights the historical trend of the development of the manufacturing industry across its entire timeline. Human society has experienced three industrial revolutions. In the 18th century, manufacture of machinery equipment served as the first symbol of industry 1.0. The early 20th century saw electrification as the symbol of Industrial 2.0, and in the 1970s large-scale quantities of standardized

simplified production modes became the symbol of the industrial 3.0. Unlike the primary argument from the international community on the subject of the third industrial revolution, German academics and industry members believed that the first three industrial revolutions were due to advances in mechanization, power and information technology. They introduced the 18th century machinery manufacturing equipment as Industrial 1.0, electrification at the beginning of 20th century as 2.0, and automation of the production process in the1970s as 3.0. More recently, the introduction of the Internet of things and novel manufacturing services have ushered in the fourth industrial Revolution, or revolutionary production methods, that have led to intelligent manufacturing, or namely "industrial 4.0”. The German "Industry 4.0" strategy aims to promote the transformation of the manufacturing industry towards intellectualization by making full use of a combination of information and communications technologies alongside the cyber Physics system. Industry 4.0, in a simple phrase to sum it all up, is based on intelligent manufacturing-led production methods across the present-day cyber physical environment which aims to build a standardized intelligent factory using dynamic configurations to achieve innovative production.

Industry 4.0 projects are mainly divided into three major themes:

1) "Intelligent Factory" - focusing on production system intelligence and processes, as well as the realization of networked distributed production facilities.

2) "Intelligent production" – which mainly relates to the entire enterprise production logistics management, human-computer interaction and 3D technology in the applications forming out of the industrial production process. The strategy focusses in particular on attracting small and medium sized enterprises into a participation agreement. This marks a clear effort to aid SMEs in becoming the users and beneficiaries of the next generation of intelligent production technologies, as well as the creators and suppliers of advanced industrial production technologies.

3) "Intelligent Logistics" - operating mainly through technologies including the Internet, networking systems, logistics networks, integration of logistics resources and these capabilities give full play to the existing logistics resources of the efficiency of the supply side. In terms of demand, intelligent logistics can quickly obtain service matching and logistics support.

CHAPTER 2 CYBER PHYSICAL SYSTEM

2.1 Introduction

Serving as the point of unity between computational processes and physical processes, cyber physical systems (CPS) are the next generation of intelligent systems that have the potential to integrate computing, communication and control. The cyber physical system interacts with a physical process through a man-machine interaction interface. It then uses the network space to manipulate a physical entity in real-time in a remote, reliable, secure and cooperative way.

The cyber physics system ubiquitously makes use of systems engineering to optimize its operation. Such instances include environmental perception, embedded computing, network communication and network control, which makes the physical system possess elements of computing, communication, precise control, remote collaboration and autonomous functionality. The system targets key computing resources and physical resources associated with close integration and coordination. This is mainly used in particular intelligent sub-system frameworks such as equipment interconnection, object-linked sensing, intelligent households, robotics, intelligent navigation and so on.

Based on environmental perception, CPS is a trusted, controllable and scalable networked physical device that integrates computing, communication and control capabilities in remarkable depth. This enables deep fusion and real-time interaction to increase or extend new functionalities by employing computational processes and feedback loops that interact with physical processes. The result of these points is a much more secure, reliable, efficient and instantaneous method of detecting or controlling a physical entity.

The central importance of CPS is to connect physical devices to the Internet, so that physical devices have five primary functions: computing, communication, precise control, remote coordination and autonomy. While CPS is essentially a network with control attributes, it does differ from existing control system characteristics. CPS puts communications on an equal footing with computing and control. It achieves this because physical devices are coordinated in the distributed application system which, by way of CPS, is inseparable from communication. In regards to internal network equipment, remote coordination capabilities and autonomous capacity, the number and type of control objects far exceed the scale of the network compared to the existing industrial control network.

CHAPTER 3 ANALYSIS OF THE SECURITY OF CYBER PHYSICAL SYSTEMS AND RELATED MEASURES

3.1 Introduction

Cyber Physics Systems (CPS) are a complex multi-dimensional array of comprehensive computing, communications and physical environments. They are a next-generation intelligent system which realizes the close combination and coordination of computational resources and physical resources. Security is the leading priority of large complex systems. CPS emphasizes the interaction between information and physics, thereby adding weight to the importance of the security of information transmission between physical components and information systems. The scale and complexity of CPS systems are also put heightened due to greater requirements for information system security. For physical information systems, a comparatively perfect security service includes: data confidentiality, information integrity, identity authentication, access control, usability, robustness, scalability, timeliness, adaptive and privacy protection.

3.2 Security objectives for Cyber Physical Systems

Network security and CPS security are very different subjects of network security. The update mechanism is often used to repair previous security software, but this approach to CPS system security does not apply. This is because it will take a lot of time to arrange for the system to run offline, and if the industrial server is stopped or the computer installs new security patches on a regular basis there is a significant loss of economic benefits before upgrading the system. Security issues in the cyber physics system need to be upgraded to existing technical security levels, some of which require new security technologies. The security objectives of CPS are based on traditional security objectives and can be divided into three main categories: integrity, validity and confidentiality. Integrity refers to the trustworthiness of data or resources, validity refers to the accessibility and usability of the system, and confidentiality refers to the inaccessibility of information to an unauthorized user. The needs of CPS system security can be divided into the following categories: sense of security, communication security, information storage security, behavior control security and feedback security. The system architecture of cyber physics system can be divided into three layers, namely: the perceptual layer①, the data transmission layer② and the application control layer③ as shown in Figure 1:

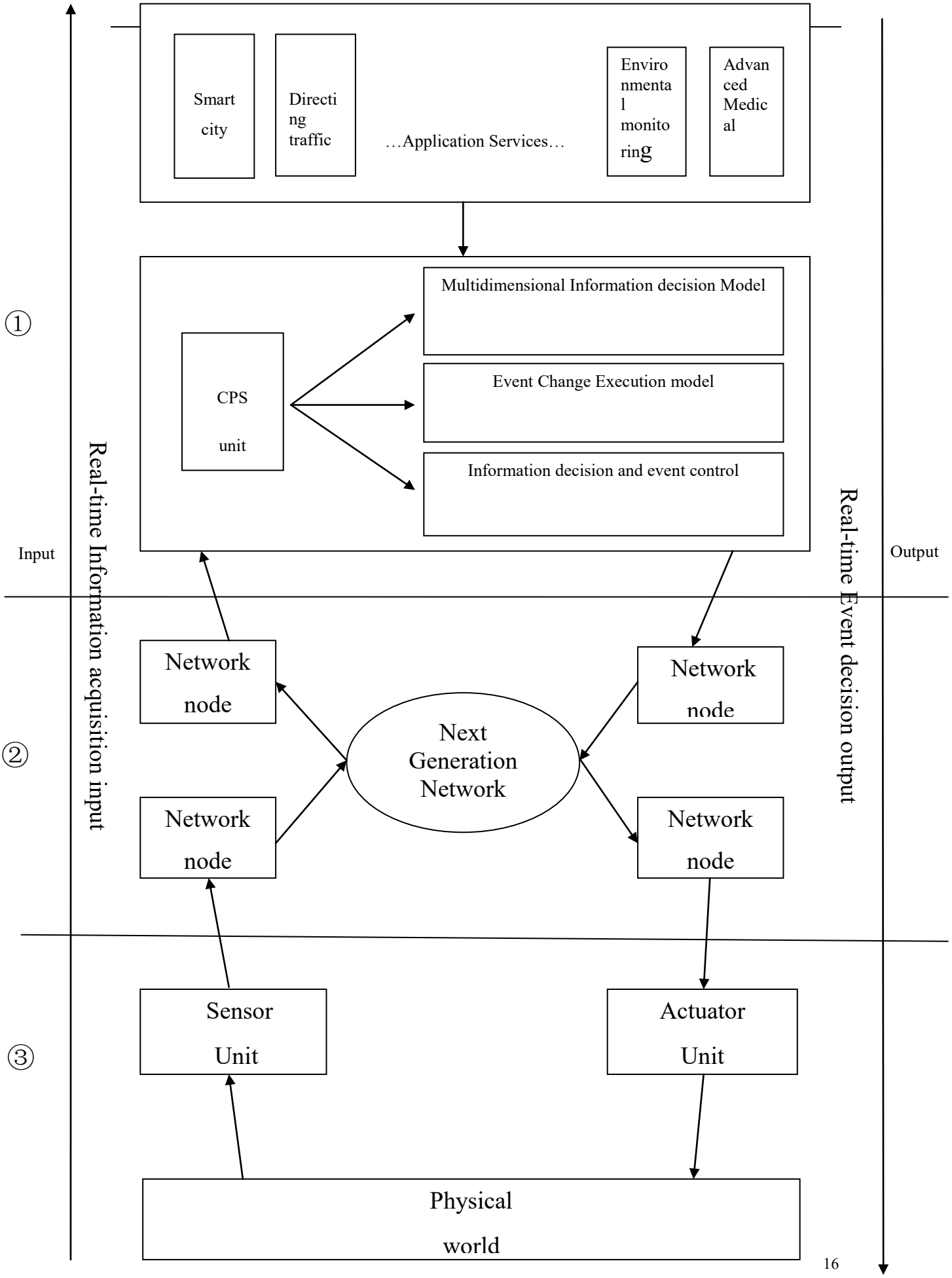

Fig. 1 Architecture of cyber Physics system

3.3 Information Physical system attack model

In Figure 1, the CPS architecture is displayed where real-time information acquisition is first input, real-time event decisions are subsequently output. The inputs are represented by inputs from sensor data and feed into the application of the control layer CPS unit, whereas the outputs indicate CPS Unit commands that are sent to the actuator. In the application control layer, CPS unit algorithms are usually divided into two categories. The first is an estimation algorithm for tracking the physical world in a real-time state, and the second is the control algorithm which bases on the estimation algorithm to select the appropriate control command return.

Displayed in the attack model in Figure 2, A and B represent spoofing attacks. In A, the process of sending input information from the physical world to the CPS control unit is illustrated. Here, the attacker converts input to input’. Whereas in B, the changes to output', the error message may contain data errors, collection errors, time errors, ID errors, and so on are shown. C and D represent the in which a service attack is denied. In C, the example is for an attacker who blocks or interrupts the information entry process, while in D an attacker blocks or interrupts the command transfer process. In both C and D, attacks on a network node continue until it stops working resulting in a blocked network. The

remaining mode is a sleep attack on the perceptual layer which forces the perceived node to fail prematurely.

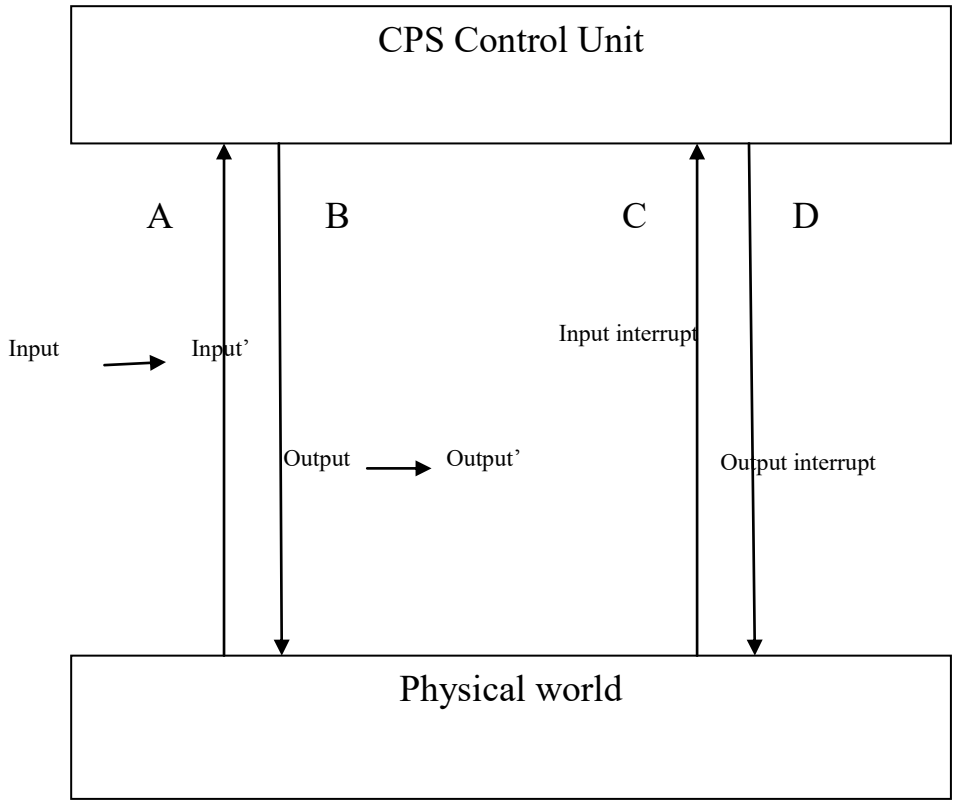

Fig.2 CPS Attack mode

3.4 Cyber Physical system security framework

The application control layer operates on the decision-making level of CPS. It therefore needs to make decisions on resource allocation, task scheduling within the CPS system along with consideration of the restriction of economic factors. The application control layer provides a variety of CPS platforms including integration of data management, business management, middleware and other technologies. In addition, application platform software involves a large amount of user data. Thus there may be other factors coming into play such as unauthorized access, data mining in the Privacy Disclosure, control command forgery attacks, database attacks and other security threats. The privacy information of the application control layer must be protected for these reasons. Technical security countermeasures for these security threats include computer forensics, privacy protection, identity authentication and data encryption and access control among others.

The cyber physical system has unique physical characteristics in which the system computation and communication behavior all need to satisfy the same real-time constraint. In a dynamic scene where resource allocation is limited, the cyber physical system also needs to satisfy adaptive characteristics, potentially avoiding excessive resource invocation and insufficient utilization constraints. The influence of the

network system on the cyber physical system is enormous because it determines both the cognition precision of the CPS system to the physical world along with the degree of control execution by the CPS system to the physical world. There are many security threats in data transmission layers, not limited to authentication attacks, denial of service attacks, routing attacks, cross-network node attacks, route tampering, network join attacks and so on. The technical security countermeasures include intrusion detection, traffic detection, identity authentication, routing security, redundant routing, encryption and hop-and-jump authentication mechanisms before key distribution mechanism are carried out.

The perceptual layer is closely linked to the physical world and contains two parts: perception and control. Typical physical hardware comprising this include an RFID devices, actuator units, image capture devices, GPS devices and other sensors such as infrared and temperature. The security threats of the perceived layer include equipment damage, equipment failure, electromagnetic interference, clock synchronization attacks, resonant attacks and so on. The technical security countermeasures include physical device protection, backup and redundancy of physical equipment, electromagnetic shielding, global clock control, wireless resource monitoring and so on.

3.5 Cyber Physical systems security technology

Research into Cyber Physical systems is in its very early stages and the related research is limited. From the perspective of security, it is of foremost importance to solve the problem of encryption technology, access control strategies and elasticity mechanisms under malicious attacks. The paper [2] provides a certificate-free signature mechanism in wireless mobile CPS networks which solves the problem of complexity between encryption cost and key management. In reference [3], the author proposes use of a time characteristic for achieving private decision-making. The author also uses a formal information flow model for describing the information disclosure in the CPS model and gives a simulation result from a cyber physical system. This is done because the information interaction between the information component and the physical component may lead to some degree of unexpected information flow. The cyber physical system contains a large number of feedback control loops. If these control loops are attacked, it will have great disastrous consequences for the entire system. The greater the size of the control system and the more dispersed the location, the more vulnerable it is to be attacked. In reference [4], Hamza Fawzi et al first estimated the elastic strain capacity of a system under attack, and then conceptualized

an algorithm to estimate the state of the system under attack and provide a performance description of that system.

3.5.1 Access control policies

In the cyber physical system, applications on the control layer are convoluted by complexities due to changed access entities, changed entities accessing resources and environmental constraints for specific resources. Access control policies should therefore also include environment-context security. In addition, the external environmental factors may cause a change in the access control configuration. The security of the physical environment that accesses control strategies thus needs to be considered. Early access control models mainly appear in the literature as DAC (discretionary access controls), MAC (mandatory access Controller), RBAC (role. Based access Control) [5], ABAC (attribute-based access control) [6,7] and UCON (Usage control) [8].

In 1992, David Ferraiolo and Rick Kuhn proposed an RBAC (Role Based Access Contro1) model. In this model, the concept of role is introduced for the first time. It defines the user and authority in a way that separates them logically by role. The model also suggests that most access control models are extended on the basis of RBAC model, which allows for an

increase in the temporal and spatial constraints and enhances the expressive ability of the RBAC model. However, the RBAC model Series does not consider contextual information, causing restricted application of RBAC model in cyber physical systems. In reference [9], Garcia-morchon et al extends the RBAC model, allowing context perception to be included in the access control system. The system is setup with three states including a normal state, a state of emergency and a serious state. The access control strategies in each of the three different cases are given respectively.

Busch et al use uniform rules to describe the security policies of different models in reference [10], and they propose a security strategy that can be combined with multiple access control models. The UCON model is a next-generation access control model proceeding the RBAC model. In reference [11], the authors realize access control to the sensor node data through a multi-hop mode in wireless sensor networks. The fuzzy set theory is an interval-valued method of access control that was established by Wang Xiaoming et al. and it proposes an interval-valued fuzzy inference authorization algorithm [12]. Dou Wenyang et al. also put forward a fuzzy access control model for pervasive computing (Fuzzy Role Based Access Control, FRBAC) [13]. By reasoning the fuzzy context, the model can be used to activate the user's role in the current state, and

the user gains access to the resource through the active role. In reference [14], the author proposes a fuzzy active access control model (Fuzzy Active Access Control, FAAC) for pervasive computing. Additionally, based on the ECA (Event Condition Action) Rule form, the initiative and ambiguity of access control for pervasive computing are described.

In reference [15], the author presents an access control model (FEAACS) of the cyber physical system which can adaptively assign a crisis role in the crisis state. FEAACS can assign the access control authority to a specific entity and select the optimal response path using the action generation model based on the priority and dependence on the crisis state. A fault-tolerant access control strategy can be used to eliminate the crisis state after a crisis management failure.

Comparing the above access control strategies, we can see that the research progress of access control in recent years is mainly in the following perspectives:

①Research on the extension of traditional access control mechanisms.

② Access control research for dynamic change of environment and resource context.

③Fuzzy access control.

④Trust-based access control [16-19].

CPS systems not only comprise information systems, but also physical systems. To find an access control model which fully adapts to CPS systems application and meets more in-depth research, the environment and internal entities of security and stability need higher requirements. CPS systems access control strategies also have the following several problems:

1. In a crisis situation where the authorization is required to be verified quickly, the reliable authorization efficiency of the access control policy is low, which directly affects the handling of crisis events.

2. Active access control mechanisms are not flexible, autonomous or adaptive. Such examples cannot meet the characteristics of an adaptive CPS system.

3. Insufficient utilization in an environmental context which makes systems poorly adaptable to the network environment of wireless sensor networks.

3.5.2 Privacy Data Protection

In a specific application, privacy is sensitive or proprietary information that the data owner, such as an individual or an organization, is unwilling or unable to disclose. Privacy protection is a kind of information security issue, where information security concerns the confidentiality, integrity and usability of data. The main concern of privacy protection is whether the system provides anonymity of privacy information. With the rapid development of WLEB2.0 technology, a variety of network applications have recently become available and are expected to expand in the near future. A large number of personal data and information transmission in the network ensures that the information in the network holds a sufficient level of security.

User privacy on the internet can be broadly divided into three categories: identity information, secret information and user addresses. Identity information includes name, sex, cell phone number, ID number, among others. The secret information category includes personal logs, internal information within an organization and so on. User addresses includes the network environment of user IP information which contains the actual MAC address information.

Radio frequency identification (RFID) is the coupled use of RF signals to achieve contactless information transmission across different systems in close range. While uses for the transmitted information is typically used to achieve the purpose of identification, radio frequency identification systems usually consist of three primary parts: RFID tags, RFID readers and a back-end database. The security threats in RFID systems mainly include signal jamming, malicious intrusion and communication security. Means of privacy within the RFID system includes location privacy and information privacy. There are two techniques to resolve privacy protection of RFID systems. One method is to adopt the physical protection method of RFID tag itself and another is to adopt cryptography based technology.

Privacy protection in data mining is centered on making accurate and efficient data mining on the basis of protecting user's privacy. The method of hiding sensitive data in the process of data mining is done by using encryption technology, and is widely used in the Distributed application environment. For example, Secure Multiparty Computation (SMC) is a major user of privacy protection using encryption. In reference [20], the authors provides two computing methods: user anonymity and secure multi-party computation. The term ‘user anonymity’ is defined as the hiding of user data by means of random data

allocation. The research of data anonymity mainly revolves around two aspects. The first is to study the principle of better anonymity, in pursuit if better publishing data and protecting privacy. On the other hand, in the context of specific applications, the principle of anonymity for specific data designs more “Efficient” anonymous algorithms. This makes the algorithm achieve a better balance between data precision and computation cost. In reference [21], the author proposes a classical K-anonymous algorithm which can ensure that the privacy information of any user is indistinguishable when the data contains more than ‘K’ number of user's privacy information. Taking it a step further, in reference [22] the authors give a multidimensional K-anonymous algorithm. This rendition of the algorithm is able to publish data with high precision and map the original data to a multidimensional space, before making an optimal partition of multidimensional data in the space. All points mentioned above are anonymous data algorithms for static data, reference [23] further proposes an anonymous principle m-invariance to protect privacy in a dynamic environment.

Existing technology	Main advantages	Main disadvantages
Radio Frequency Identification Privacy protection	Automatic identification, wide application	An attacker can steal entity information via RF tags, tracking entity identities and acquiring entity privacy
User Anonymous Privacy protection	Good degree of privacy protection	The design of anonymity principle, the computation cost of anonymity algorithm is big, the data precision is not high
Data Mining Privacy Protection	Clear Data analysis	The potential correlation between data exposes personal privacy, and a certain degree of data loss affects the accuracy of the data
Wireless sensor network Location privacy protection	Suitable for wireless sensor networks	Communication module has high energy consumption, high communication cost, long communication delay and low privacy protection.
LBS (Location-based Service) Location Privacy Protection	Quick and accurate access to your location makes it easy to use a variety of advanced applications	Attackers can infer other privacy information using location information

Table 1 Classification analysis of privacy protection methods

However, the existing privacy protection technology still has the following deficiencies:

1) The simple superposition of privacy protection technology can not meet the new privacy protection requirements.

2) The existing privacy protection technology has different emphases in different fields and different network forms. There is also no connection between technologies and the heterogeneity of technology cannot be shielded.

3.6 Future trends

In light of existing security issues and security technologies, future research on CPS security will be in the following areas:

1) In the future, the research direction of access control is likely to include the following focal points. The research of security and access control for nodes with limited computing, communication and storage capability and mobility in wireless sensor network environment are all areas of prospective research. This is also needed in situations where a

quick authentication and authorization is required. It is also a meaningful research direction to study the secure, reliable, fast, verifiable and active access control mechanisms.

2) In the environment of physical information systems, the context information of computable resources is usually fuzzy, uncertain and incomplete. These types of computing resources are updating dynamically and therefore the theory and techniques of fuzzy access control will become an important research direction.

3) For privacy data protection, further research on privacy protection in wireless sensor networks and data mining is needed. Anonymity technology in privacy protection needs to deal with the balance between privacy protection and the resultant accuracy. To study methods of hiding data the heterogeneous data fusion of CPS is a necessary research direction in the field of CPS security.

4) Traditional security multi-party computation requires that the computational resources involved can be computed and communicated. The efficiency associated with this is low, and it is an important problem to search for the ideal secure multi-party computation algorithm for CPS security research.

5) Non-technical factors of information security, including public awareness of data security, is not strong. Enterprise weight-data collection, light data mining, intelligent processing, lacking social information for security related laws are other future security research areas which must consider at least one of these factors.

From the perspective of induction, transmission and service, the architecture of physical information systems can be divided into the perceptual layer, data transmission layer and application control layer. It is necessary to provide different preventive strategies for different security threats because the security threat of physical information systems is very different in physical entities, network space and application services. Some security issues have not changed in new physical information systems, resulting in upgrades only to existing security levels. Some security issues require the study of new security technologies. The next major goal to be studied is to improve the existing security services and build a secure service model of physical information systems.

CHAPTER 4 SECURITY OF CYBER PHYSICS SYSTEMS IN THE INTELLIGENT MANUFACTURING

4.1 Security Challenge of CPS in the intelligent manufacturing

4.1.1 Characteristics and security requirements of CPS in the intelligent manufacturing.

The core of Industry 4.0 is intelligent manufacturing, so in order to analyze the security of cyber Physics system in Industry 4.0, we should start from the realization level of intelligent manufacturing analysis, CPS for the whole process of manufacturing, the whole industry chain, product life cycle, can from the unit level, system level to System on system (SOS) level deepening, Realize the reconstruction of manufacturing production paradigm. Multiple minimum units (unit level) through industrial networks (such as industrial field bus, industrial Ethernet, etc.), to achieve a wider range of data flow in a wider area, the realization of multiple cell-level CPS interconnection, interoperability and interoperability, and further improve the manufacturing resources to optimize the allocation of breadth, depth and precision, The system-level CPS realizes the self-organization, self-configuration, self-decision and self-optimization of local manufacturing resources based on State awareness, information

interaction and real-time analysis of multiple cell-level CPS. Multiple system-level CPS forms the SOS-class CPS. Such as multiple production lines or collaboration between multiple plants to achieve the entire product life cycle and enterprise system-wide integration. The intelligent manufacturing CPS features data-driven, software-defined, ubiquitous connectivity, virtual-reality mapping, heterogeneous integration, and system autonomy. Unlike the Internet of Things (IOT), CPS is able to perform feedback operations through computing, communication, and control systems after sensing physical environment information. CPS not only has the ability to perceive and transmit information, but also has the ability of intelligent processing, and with the industrial Internet, CPS emphasizes human, machine and object fusion, emphasizing the control of physical entities. Intelligent manufacturing CPS Security should ensure the continuity and reliability of intelligent production, ensure the safety of intelligent equipment, industrial control equipment and systems, and focus on the availability, integrity and confidentiality of equipment and systems.

1) Intelligent manufacturing CPS Software defined characteristics means not only intelligent manufacturing equipment, all intelligent products itself is CPS, software can not only control equipment and product operation, but also the equipment and products in real-time display,

through analysis, optimization, the role of equipment, product operation, and even design links. Therefore, the overall safety design for the whole process of intelligent manufacturing is needed.

2) Intelligent Manufacturing CPS Virtual reality mapping is based on the static model produced by physical entity modeling, through real-time data collection, data integration and monitoring, dynamic tracking physical entity's working status and work progress, the physical entity in the physical space in the information space to reconstruct all elements, forming a sense, analysis, decision-making, The digital twins of the ability to execute. Traditional information security focuses on the impact of the attack on the confidentiality, completeness and availability of the information, while CPS security must take into account the impact of malicious attacks on the performance and system services of the closed-loop system in both information space and physical space.

3) The autonomous characteristics of the CPS system of intelligent manufacturing indicates that CPS is able to handle and analyze the information space based on perceived environmental changes, adapt the external changes effectively, and realize the self-organization between CPS in the higher-level CPS. The system can constantly evolve and learn to improve itself. CPS security also needs to evolve independently as the system structure and functions evolve dynamically.

4) The Intelligent manufacturing CPS Heterogeneous integration feature indicates that CPS units and systems need to be shared online, and can be called through standardized interfaces to realize efficient self-organizing intelligent manufacturing of manufacturing resources. CPS security technology needs to efficiently implement both identity authentication and trusted transactions.

5) Intelligent Manufacturing CPS must ensure long-term operation of the system safe and reliable, industrial control process continuous drinking high availability. Equipment and system maintenance need to implement planning and scheduling, and CPS contains a large number of real-time dynamic processes, should solve unpredictable interruptions and people in the loop of uncertainty, to ensure the flexibility of CPS system, that is, at any time to ensure the safe and reliable operation of the system, and provide acceptable service capabilities.

4.1.2 Security challenges for smart manufacturing CPS

CPS security runs through the architecture sense, transmission, computing, control, and service 5 Layers . The following is an analysis of the intelligent Manufacturing CPS Security Challenge from CPS tiers.

1) Sensing Safety. The challenges of perceived security are mainly embodied in the following aspects: limited computing capacity of perceptual nodes, instability and uncontrolled deployment environment; Because of the complexity of the interaction between intelligent devices and physical processes, it is difficult to guarantee the authenticity of perceptual data; physical nodes are distributed and independent, infrequently replaced, difficult to physically access and repair and upgrade, Devices need to be authorized to search their own software upgrades, confirm the credibility of each other, and pay for resources and services; Tens of billions of to hundreds of millions of millions of smart devices make the node authentication problem more complex.

2) Transport Security. The Intelligent manufacturing CPS Network covers industrial Fieldbus, industrial Ethernet, industrial wireless network, wireless sensor network, mobile Internet, Internet, etc., with heterogeneous fusion, independent autonomy, open interconnection and other characteristics, which will make the traditional industrial control system to break the previous sealing, will face viruses, trojans, hackers, Traditional information security threats such as denial of service. At the same time, there are many mobile nodes in the intelligent manufacturing CPS, these mobile nodes need more stringent access authentication and roaming mechanism, unified authentication and roaming switching will

increase the burden of central server and network communication, and how to realize efficient authentication and roaming switching is an urgent problem to be solved. In addition, the open Environment Sharing awareness and control network leads to more serious privacy and conflict issues.

3) Control safety. Proprietary industrial Control communication protocol or protocols are usually designed to emphasize the real-time and availability of communication, which is generally insufficient for security, and its information security vulnerabilities include control protocol vulnerabilities (such as authentication defects, plaintext transmission, etc.), control software vulnerabilities (such as configuration software buffer overflow), etc. The large-scale, dynamic and hierarchical SOS features of the intelligent manufacturing CPS make the mechanism of the influence mechanism, trust and control of the information security to physical security very complicated; In addition, the system uncertainty is increased in the loop, and the real-time control system is difficult to guarantee.

4) Application Security. The intelligent manufacturing CPS is a comprehensive complex system, its application has the features of service interoperability, heterogeneous integration, application migration and so on, the security loopholes in the application system compiled by different

manufacturers and different development platforms make the whole CPS system more vulnerable to attack; the whole life cycle management of large-scale CPS units and systems, The security and trust management of heterogeneous CPS, autonomy and self-owned CPS, CPS Emergency Behavior and CPS collaboration have also made the application security problem more complex.

5) Data Security. Data-driven is an important feature of the intelligent manufacturing CPS, and CPS generates a large amount of data in the process of sensing, computing and service, which has the risk of eavesdropping, alteration, deletion, injection and replay of the data in the process of transmission and storage. The large number of intelligent devices, heterogeneous multi-domain networks, a wide variety of private industrial control system protocols, CPS system, "people in the Loop" and other features increase the risk of data security.

In general, the security challenges of the intelligent manufacturing CPS system are as follows: 1). The system security boundary is gradually blurred; 2) The number of entities and the scale of the network are greatly doubled; 3) various safety problems throughout the CPS unit and system life cycle; 4) The Attack of intelligent manufacturing CPS is automated, intelligent, Collaborative, group, organized, Characteristics of large-scale, high concealment and strong persistence. At the same time, the intelligent

manufacturing CPS Business system need to ensure continuous, automatic, real-time response, and storage space, memory usage, processor use, network connectivity and power consumption and other issues related to the availability of the system is not the highest priority of security mechanism issues, traditional IDS, IPS and other security technology can not effectively integrate with CPS, compatibility, composability, scalability is not strong, is the CPS lack of effective resistance to network intrusion, therefore, in the intelligent manufacturing CPS system, only rely on the traditional containment passive defense system has been unable to effectively deal with, need in offensive and defensive status is seriously asymmetric, There is a large number of compromised real-world environments that are protected from the unknown threats that span the physical-information space.

4.2 Security framework for intelligent manufacturing CPS

4.2.1 The security countermeasures of intelligent manufacturing CPS

The CPS PWG Working Group, which was set up in NIST in 2015, released the CPS framework (Framcwork for cyber physical systems), and proposed the construction of CPS Information security assurance System, including: 1) to build more adaptable and The more expanded

intelligent information security protection system, the system can deal with all kinds of information security threats, select the priority protection target, adjust the information security protection resources, delay the occurrence of information security threats, and mitigate the impact of information security events. 2) to form a more granular and accurate information security protection strategy. By analyzing the raw data, the system can link the operational target with other potential targets such as stability, safety and efficiency, reduce the conflict between information security policies, improve the overall consistency of the information security protection system, and focus on information security, privacy, physical and functional safety (safety), reliability Elastic. According to NIST CPS information security ideas, combined with intelligent manufacturing CPS hierarchical architecture features, intelligent manufacturing CPS Security Strategy analysis is as follows.

1) CPS security "divide-and-conquer" strategy. The "divide-and-conquer" strategy extends the traditional information security to all the key subsystems of CPS, and gradually expands the scope of information security to solve the information security problem in the whole CPS. At present, this kind of thought has the successful practice in the electric power, the nuclear facility and so on, and forms the IEC 62443,nist sp800-82 and so on a series of standard specification. In the intelligent

manufacturing CPS hierarchy, we can identify key CPS units and systems, ensure the security of these key units and systems, and divide and conquer the system to provide complete protection for the most important systems, and ensure the security of these important systems. The disadvantage is that the technical ideas tend to be "closed" and "blocked", which are inconsistent with the opening of CPS. The protection means of traditional information security need to be further modified to adapt to the business continuity requirements of the intelligent manufacturing CPS.

2) CPS Security "autonomous" strategy. The "autonomous" strategy guarantees the security of the whole CPS by guaranteeing the security of each CPS subsystem, and each CPS first defines its functions, organization, user, credibility, time, data, boundary, composition, life cycle and other elements, each of which is regulated by concept, implementation, and guarantee. In recent years, the main modeling methods include statistical machines and artificial neural networks, and these methods have achieved better safety protection in the business systems of specific industries. The "autonomous" strategy makes the self-organization and dynamic structure of the units and systems in the intelligent manufacturing CPS have a certain degree of security protection in the predictable range, the disadvantage is that these measures are difficult to validate effectively.

3) CPS Security "common governance" strategy. The "Co-governance" strategy includes centralized co-governance and decentralized co-governance, which refers to the mutual support of each subsystem in security, which is coordinated and assigned by the Security Control center, such as cooperative linkage defense, while decentralized co-governance is a security strategy for each subsystem to share the protection resources, to center or to intermediary, such as blockchain technology. The "Co-governance" strategy is a new hotspot in the research of CPS information security technology, the blockchain technology to center, transparent contract implementation automation, traceability and other characteristics in line with intelligent manufacturing resources autonomy and online self-organization application needs.

4.2.2 Security framework for intelligent manufacturing CPS

Based on the proposed intelligent manufacturing CPS architecture, CPS security features components include: environmental security, physical security, perceived security, network security, control security, application security, and data security, as shown in Figure 3 below:

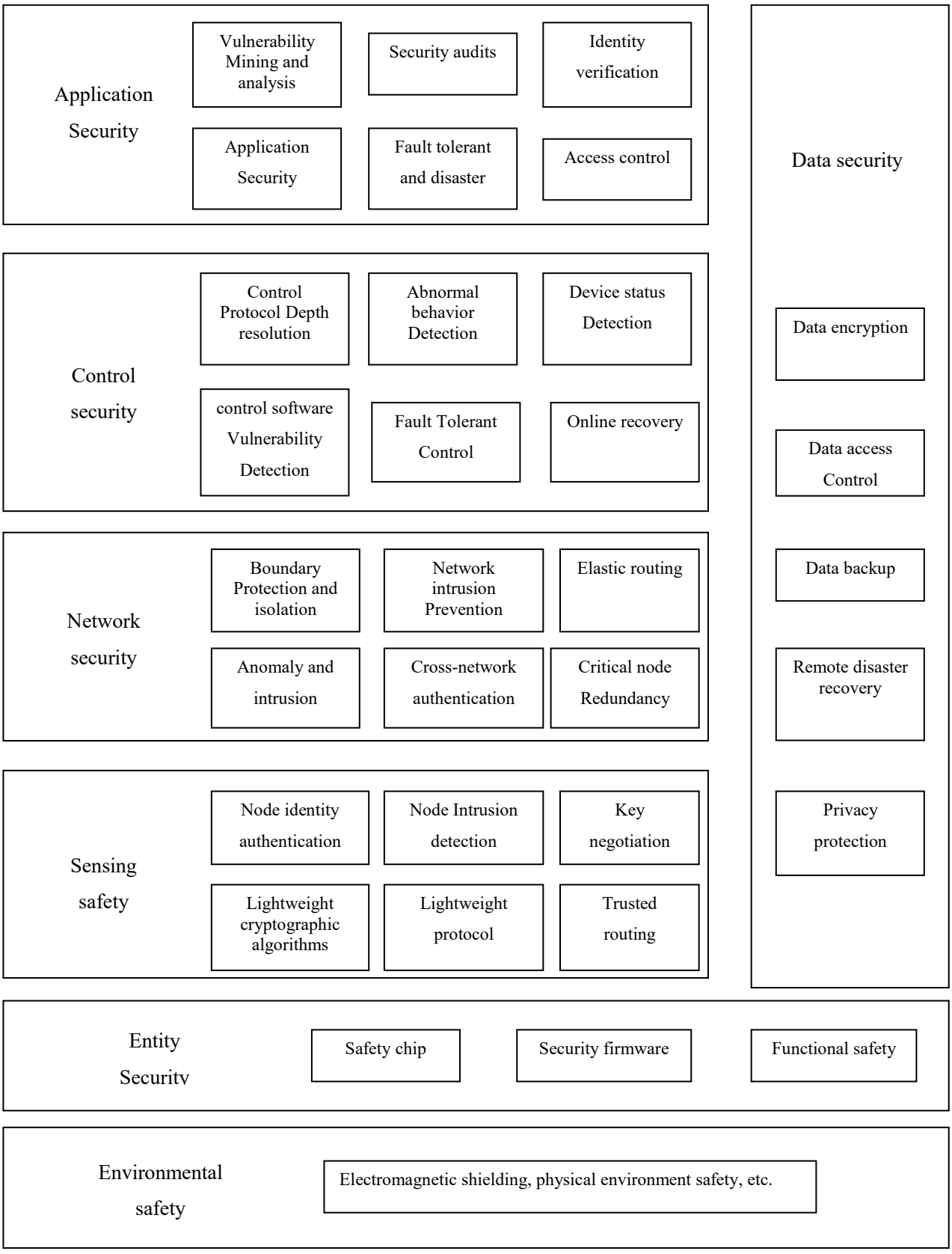

Figure 3 Intelligent Manufacturing CPS Security function framework

1) Physical Security. The number of physical entities (sensors, actuators, etc.) involved in the CPS is large, diverse, widely distributed and rapidly growing, greatly increasing the risk of the system being attacked. Physical security, the need to follow functional safety requirements, even if the entity fails, you need to reliably enter and maintain a safe state, to avoid harm to people or the environment.

2) Sensing Safety. In the CPS network environment, the two-way authentication between the external network and the Peripheral network node has two problems, the authentication process must fully consider the limitation of the Peripheral network resources, the computation of authentication mechanism and the communication cost must be as small as possible, and the number of peripheral networks connected to the external network is huge and the structure is different. An efficient identification device must be established to differentiate these networks and their internal nodes, and to give unique identities. For the general sensor network sense Security research, the key technologies involved in intelligent manufacturing of CPS include node identity authentication, lightweight encryption, such as AES encryption algorithm, DESL encryption algorithm, XXTEA encryption algorithm, key negotiation and trusted routing.

3) Network Safety. Network security focus from the point of view of network boundary security protection, according to the principle of layered sub-domain deployment, undertake the network attack detection and Security Assurance task for CPS, and take account of the efficiency, specificity and compatibility. Research on the Safety of Industrial control network, the key technologies of intelligent manufacturing CPS heterogeneous multi-domain network security are as follows: Network security with active protection ability layer-by-step isolation deployment system, including security gateway intrusion Prevention, boundary detection, protection and isolation of network boundary ; Heterogeneous multi-domain network structure Security vulnerability Mining and analysis, distributed intrusion detection and protection, network access violation operation, unauthorized access behavior supervision, network intrusion forensics, heterogeneous network encryption secure transmission and cross-network authentication; elastic routing, multipath routing, reconfigurable Overlay network technology to enhance network affordability, Absorptive capacity and resilience, heterogeneous multi-domain network security test verification and evaluation.

4) Control Safety. Control security mainly solves the problem of distributed security control under the structure of open interconnection and loosely coupled networked system. As far as possible, industrial

control system should adopt the High security industrial control software and communication protocol with authentication, encryption and authorization mechanism to ensure the safe transmission of control commands and production data. The research on control security has found that the control security needs to provide the protocol anomaly detection capability, including the Industrial Control Protocol flow depth analysis and anomaly detection, as well as encryption control protocol flow Statistical Characteristics Analysis, protocol process modeling and abnormal behavior detection, detection control protocol flow tampering, forgery, deception and other attacks. In addition, it is necessary to ensure the safety of control methods, mainly refers to the control method to ensure that the control system in the sensor, actuator or component failure is still able to maintain a stable theoretical method, the key technologies include fault tolerant and intrusion control methods, fault-tolerant control methods such as robust control, intelligent control, etc. Intrusion control methods such as dynamic light-weight and self-encrypting control, etc.

5) Application Safety. Application security specifically covers the operational security and physical security of the application system two aspects, wherein the application system operating security refers to the use of vulnerability detection and repair technology, to prevent the application system in the design, development, deployment and

maintenance of security vulnerabilities in the system to be hacked to cause the crash; application system entity security refers to the security protocol technology, Protection applications are not hijacked, forged, tampered with or impersonator during use. Therefore, the key technologies involved in application security include: Application System vulnerability Mining, vulnerability analysis technology, application system security evaluation technology and security testing technology.

6) Data Security. Data security specifically covers the data itself security and data protection security two aspects, wherein the data self-security refers to the data encryption means, to prevent data theft, to ensure data concealment; Data protection security refers to the prevention of data leakage, tampering and loss, to ensure the confidentiality, integrity and availability of data, The key technologies involved in data security include: Data encryption technology, data access control technology, data backup technology, remote disaster recovery technology and digital watermarking technology.

4.3 Security Research direction and focus of intelligent manufacturing CPS.

4.3.1 Security Research direction of intelligent manufacturing CPS

1) Intelligent manufacturing CPS security protection architecture. The intelligent manufacturing CPS contains many components, such as CPS unit, System and intelligent service platform, and the interaction between information and physical processes is complex, and it is necessary to study how to construct a new system security architecture with endogenous security dynamic defense capability, and form a multi-level defense system for the intelligent manufacturing CPS hierarchical system.

2) Intelligent manufacturing hierarchical CPS Trust and control interaction mechanism and controller design method. It is necessary to reveal the mechanism of trust and control interaction of intelligent manufacturing hierarchical CPS system in dynamic environment, based on dynamic Evolution control mechanism of security state estimation, intrusion and anomaly detection, state estimation and control algorithm joint design method, research new controller design theory, improve the robustness, robustness, security of control unit, and overcome the key issues of multiple heterogeneous fault tolerance, cooperative perception

and security linkage, adaptive integrity detection, dynamic isolation and online recovery.

3) Active Defense technology. It including dynamic platform technology, dynamic operating environment technology, dynamic software and data technology, by increasing the randomness of the system or reduce the predictability of the system to combat unknown attacks, the attackers can not detect and predict the situation, the network, host and application dynamic adjustment and configuration, thereby preventing, Delays or blocks network attacks.

4) Abnormal behavior detection and threat warning in whole process. The intelligent manufacturing CPS security problem runs through the whole process of manufacturing, and it is necessary to study how to construct the formal analysis framework of information space and physical space synthesis based on the multi-dimensional engineering features such as real-time data, operation behavior, historical data and time record parameters of the intelligent manufacturing CPS system. The paper constructs a vulnerability analysis and threat perception theory and model with deep defense capability.

5) Intrusion Tolerant Defense. There are many threats to the intelligent manufacturing CPS network space, which are unpredictable, irresistible

and impossible to prevent, and the traditional reliability theory and fault-tolerant computing technology can't avoid the failure or even the collapse of the system completely. Intrusion tolerant defenses recognize the existence of vulnerabilities and assume that some of these vulnerabilities may be exploited by attackers to attack the system. The Intrusion Tolerance technology studies how to reduce the loss, recover as soon as possible, and complete the healing and regeneration of the target system in the case of the system has been destroyed. The cost, cost and benefit of intrusion tolerance will be the next research direction.

6) Co-linkage defense. The current security equipment and defense technology is mostly "fighting each other", the data between network protection node is difficult to share, protection technology is not related, resulting in the current defense system is isolated and static, can not meet the increasingly complex network security situation needs, Through the cooperative linkage mechanism, the relatively independent security equipment and technology in the network are organically combined, learn from each other, cooperate with each other and resist all kinds of attacks, which has become the inevitable choice for the future development of cyber space security defense.

4.3.2 Block chain application technology of intelligent manufacturing CPS

Blockchain technology is a kind of distributed peer-network mutual-trust Intelligent ledger technology based on cryptography principle, the "Chinese blockchain technology and application white paper" Prepared in China's blockchain technology and Industry Development Forum defines the blockchain as: Distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other computer technology new application mode. It is generally believed that the blockchain technology integrates the following key technologies: Peer-network technology, distributed ledger technology, asymmetric encryption technology, consensus mechanism technology, intelligent contract technology, and so on, to make the blockchain a new generation of information technology with open and just, safe, reliable and high-efficiency intelligence, which is the focus of safety and reliability. Blockchain technology realizes the fault tolerance of blockchain network and the integrality, consistency, authenticity, non-repudiation and privacy of data stored and transmitted in the block chain.

A number of projects have begun to attempt to use blockchain technology for the Internet of things and smart devices, such as January 2015, when IBM announced a project-adept project, hoping to bring in a device that

automatically detects problems, automates updates, and does not require any human action; filament company put forward their sensor devices , which allows for rapid deployment of a secure, full-scale wireless network in seconds, blockchain technology enables filament devices to process payments independently and allows smart contracts to ensure the trustworthiness of transactions; ePlug provides optional Meshnet, distributed computing, end-to-end data encryption, The blockchain platform is used for login authentication; Tilepay uses bitcoin-based blockchain technology to accept payments, providing a human-to-machine or machine-to-machine payment solution; Power Ledger uses blockchain technology to enable residents to generate electricity and sell them on the Internet. Therefore, the transaction has the unique network signature, the future data transmission between the robots, can use the blockchain technology to carry on the user's identification and authentication, but also may carry on the robot's title registration based on the blockchain technology. The research on various projects has been applied in the aspects of identity authentication and transaction security, and has not yet become a systematic application.

Blockchain technology is applied to intelligent manufacturing, which can be expanded from various layers, such as blockchain data layer, network layer, consensus layer, contract layer and application layer, and applied to

intelligent manufacturing of large-scale entity identity and authentication, de-Centralized industrial field network, industrial big Data security, intelligent contract Support self-organization manufacturing, Intelligent manufacturing process abnormal behavior detection and threat warning. At present, blockchain technology has shortcomings in the aspects of interoperability, security standards, throughput and development tools, high cost in processing, storage and replication technology, and there are many problems in the application of intelligent manufacturing CPS, such as cell-level CPS processing and storage capacity is limited; All devices need to perform cryptographic algorithms, Many devices use only simple processors and operating systems, may not support complex security methods, blockchain ledgers are stored on nodes, and over time, the size of the ledger will increase, which will exceed the capabilities of the smart device, and the overall lifecycle maintenance and management of the device, as well as privacy issues, are complex. Applying blockchain to intelligent manufacturing CPS still needs to combine "autonomy" and "common governance" strategy to study new computing and storage architectures and lightweight security methods.

CHAPTER 5 ANALYSIS ABOUT CHINA INDUSTRY 4.0 AND THE CYBER-PHYSICAL SECURITY

5.1 The background of industry 4.0 in China

Industry 4.0 (also known as the Fourth Industrial Revolution) is an opportunity to improve the digital level of manufacturing.

Rooted in breakthrough technologies such as the Internet of things, cloud computing, artificial intelligence, virtual reality, value-added manufacturing, and robotics, Industry 4.0 fully integrates and optimizes the virtual and real-world's resources, talent, and information, and also is committed to creating "smart factories" with high flexibility and resource utilization to achieve product development, procurement, manufacturing, distribution, retail, Continuous, real-time information flow to end customers. This "digital thread", which runs through the entire business value chain, greatly improves information transparency, significantly reduces operating costs, and highly personalized products, and flexible and efficient manufacturing and product development processes, and promotes innovation in business models.

Industry 4.0 is an important opportunity to break through the bottleneck of the existing productivity growth in the world. Although China has written the legend of manufacturing in the past 30 years, productivity still lags behind that of developed countries: even after 15 years of rapid development, productivity levels are still only 1/5 of the dominant developed countries. The rapid growth of Chinese manufacturing in the past has relied mainly on cheap labor, capital and imitation of innovation, but these competitive advantages are now gradually being lost. The Chinese government has unveiled "Made in China 2025", striving to draw on the wave of Industry 4.0, from the world's largest manufacturing power among the major developed manufacturing countries. But for Chinese manufacturers to succeed in digital transformation, they must seek the path of digital transformation suitable for China based on their own status quo.

To get a comprehensive picture of the digital operations of Chinese companies, McKinsey visited 130 business representatives from various industries. According to the survey, Chinese manufacturers have great enthusiasm and expectation for industry 4.0, and companies in the United States, Japan and Germany are more optimistic: 76% of Chinese respondents believe that the technological revolution will enhance their competitiveness, far higher than the US, Germany and Japan (the United

States 57%, Germany 50%, Day 54%). Moreover, China's private companies are the most optimistic, with 86% per cent believing that the technological revolution is conducive to improving competitiveness, while national companies and multinationals are relatively conservative, at 68% and 73%.

Therefore, industry 4.0 is a very important role for China's manufacturing industry, from China's national conditions to analyze, although the start is a little later, industry is backward, but the first rise of 5G network, China's Industrial 4.0 development is provided superior conditions, so the analysis of Industrial 4.0 in China and cybersecurity is crucial.

5.2 Cybersecurity strategy in China

From the document “The future of Cybersecurity in Italy: Strategic focus areas”, it has one chapter considers the international scenario described by Italian colleagues who have been working in foreign universities or research institutions for some time. It shows the cybersecurity strategy of China.

China’s cybersecurity strategy is deeply rooted in the government’s attention to information management. Throughout the millennia of Chinese history, the role of information in both civilian and military

affairs has been of primary importance. The current Chinese cybersecurity strategy and the new law and regulations on cybersecurity are both firmly grounded in this tradition.

The Cyberspace Administration of China (CAC) is the central internet regulator. The CAC is responsible for policy formulation and implementation, domain name registration and content supervision.

The CAC white paper guidelines that are at the core of the Chinese government's cyber governance strategy revolve around four main objectives: (i) Guarantee cyberspace sovereignty and national security; (ii) Protect critical information infrastructures; (iii) Act against cyber terror and cyber crimes; (iv) Expand international cooperation.

On November 1st, 2016, the Standing Committee of the National People's Congress promulgated the first comprehensive Cyber Security Law (CSL). More than 700 million people in China use the internet. The CSL, which came in to effect on June 1st, 2017, is intended to protect the critical information infrastructure, to regulate Chinese user data, to augment internet security, and to monitor and certify foreign technologies that enter the Chinese market.

Under the new CSL, the mainland network operators (a notion that includes a wide array of actors) must adopt stringent internal and

operational procedures as well as strong and updated technical protocols in order to prevent computer viruses and cyber attacks. In addition, telecommunication hardware and software, which is under intense scrutiny, requires proper certifications before it can be used in the domestic market. The law applies to both Chinese companies as well as to international companies that operate in China.

The Chinese cybersecurity information architecture also includes many other actors, including the following:

Ministry of Industry and Information Technology (MIIT). The MIIT closely monitors the cybersecurity aspects related to the development of the information highway and cooperation in the communication technology sector in China and abroad.

Ministry of State Security (MSS). The MSS, which is in charge of the security services, also closely monitors the cyber aspect of information and communication technologies (ICT).

Ministry of Public Security (MPS). The MPS is focused on the cyber crimes committed at the national level as well as cyber terrorist attacks. The Ministry is responsible for the oversight and enforcement of the CSL.

China Information Technology Security Certification Center (CNITSEC) The CNITSEC is responsible for security reviews and approvals of

network products, services and the related supply chain in accordance with the CSL.

China National Vulnerability Database of Information Security (CNNVD) The CNNVD provides a public database of confirmed software vulnerabilities. CNNVD's early warning capabilities support efforts in both the public and private sectors to address any cyber vulnerabilities.

5.3 The China's 5G technology and application to industry 4.0

5.3.1 The 5G technology

The concept of China's fifth generation mobile communication system (5G) was first proposed at the China International Communication Conference in August 2012, and compared with 4G, the characteristics and advantages of 5G include the following aspects:

(1) The network peak transmission rate is more than 10 times higher than 4G, that is, to reach 10Gb/s, under special circumstances, the user's single-link rate can reach 10Gb/s.

(2) The average user acquisition rate of more than 10Mb/s, for special industries, such as telemedicine and other data flow requirements of high business, need to be improved to 100Mb/s.

(3) The data throughput capacity is 1000 times higher than the 4G, and the throughput per unit area is at least 100GB/s/km.

(4) The system capacity is 100 times greater than the 4G. By 2020, the number of networked terminals will reach 500-1000 trillion units, the unit area terminal density may exceed 1 million per square kilometer, the system capacity needs to be improved rapidly.

(5) Energy consumption utilization rate increased by 1000 times. With the popularization and application of D2D technology, the energy consumption of equipment will be greatly reduced on the basis of 4G.

(6) Spectrum utilization rate increased by 5-10 times. 5G actively adopts high frequency spectrum transmission medium, expands bandwidth and improves spectrum utilization.

(7) Network delay is reduced by 5-10 times, the average delay is controlled within 5-10MS,in ideal state it can be less than 1ms.

5.3.2 Impact of 5G on Industry 4.0 and safety

As mentioned earlier, industry 4.0 is through advanced Internet technology to build the ecology of emerging industries, the implementation of comprehensive innovation for the industry. Traditional

industrial development has some limitations in the application of computer technology and communication technology, and it is mentioned in the CPS security analysis above that CPS emphasizes the interaction between information and physics, so the transfer of security information between physical components and information systems becomes more important. The scale and complexity of CPS system also put forward higher requirements for information system security. Among them, in CPS security, there is a very important factor is the timeliness, integrity and effectiveness of information transmission, so through the application of 5G technology can further optimize the application quality of industrial Internet, promote the performance of industrial Internet improvement.

5.3.2.1 Theory of Industrial Internet application

The application performance of industrial Internet technology in 5G technology environment can be greatly improved, in order to get a better understanding of the industrial Internet, it is necessary to further understand its related theory. The industrial Internet was initially connected mainly through the Internet system and industrial manufacturing systems, and through a number of systems, such as industrial sensors and controllers, to form a centralized feedback system,

which would facilitate the management of industry and promote the quality and efficiency of products. The application of the digital nervous system in the embryonic form of the industrial Internet is more prominent, which combines the gateway with the sensor and the industrial software. With the development of technology, the level of industrial Internet technology should also be further improved, the intelligent level of industrial Internet has been further improved, intelligent industrial Internet technology is mainly in big data and cloud computing and other related technology applications, the industrial Internet has been optimized, changing the form of industrial control, Added embedded industrial control, which can greatly improve the level of application of industrial Internet technology quality. The sensors involved in the industrial Internet industry, as well as the related software such as industrial control systems, are important software systems for the application of industrial Internet technology, and the core technology is standard packaging and super-large integrated chip technology.

5.3.2.2 Key Technologies of 5G technology

The development and research of 5G technology has just entered a new situation, and has been applied in some fields, in the future development,

the application of 5G technology has become inevitable, 5G technology involves more key technologies, among which the non-orthogonal multi-address access technology is a more important technology, The application of this technology can satisfy the multi-address access of multi-user communication between base station and terminal, and can effectively meet the requirements of data reuse when users communicate, and plays an important role in the scientific application of resources. Under the application of non-orthogonal and multi-access technology, the quality of information transmission can be greatly improved, and the use of a variety of information resources to carry information, as a key technology in 5G technology, the optimization of the application performance of the industrial Internet plays a positive role.

Millimeter wave communication technology in 5G technology also makes the more critical application technology, which is high quality as well as the value setting parameters and the technology is more mature wireless transmission technology, and optical communication properties are basically the same. Has the high resolution and the power density, also has the relatively strong anti-jamming ability. The application of 5G technology in the process of many communication needs and network realization vision and millimeter wave communication characteristics and ability comparison crystallization, this technology application in the

industrial Internet can help improve the performance of network applications, improve the network's anti-jamming ability.

The application of network function virtual technology in 5G technology plays a key role, which is a comprehensive technology of traditional router, firewall and intrusion detection technology, and network function virtualization technology is to divest the network function from the special hardware equipment under the decoupling of software and hardware, and then realize the independence of software and hardware coupling. Network hardware resources can be standardized and shared, so as to ensure the high performance of network functions, energy conservation has a positive role.

5.3.2.3 Main technical advantages of industrial Internet

After the concept of industrial Internet was put forward, the speed of development in a short period of time is relatively fast, the application of industrial Internet technology involves a lot of technology, in which software definition machine is widely used, which is the application of high-performance standard hardware equipment based on software application technology, Other related applications wind energy is through the machine download software definition, the main feature is the APP

and analysis results embedded in the machine, but also embedded in the cloud, can effectively achieve machine intelligence and self-awareness, which to improve the intelligent level of equipment play a positive role. And can be organically connected with the Internet, can be the platform application to make efficient and effective improvement, so that the function is more comprehensive.

The Super Mobile computer terminal in the industrial Internet technology is also more critical, the main characteristic of these devices is that the processing computing power is relatively powerful, the memory storage capacity is strong, has a relatively powerful operating system and management software, in the cost is also relatively cheap. With the support of the application of 5G technology, it can provide users with convenient operation service, can grasp the dynamic information timeliness of the equipment, and also provides a great convenience for the implementation of the management work.

The security advantage in the technical advantage of industrial Internet is more prominent, in the practical application of industrial Internet system, security is more important, if it can not guarantee the security of network applications, it will inevitably cause great economic losses. The application information of industrial Internet is not only distributed in the network, but also all over the location of Supercomputing terminal and

mobile terminal, so as to effectively guarantee the security of the Internet interface, the security of network information transmission can also be effectively guaranteed. The application of network security monitoring technology ensures the safe and reliable application of the system.

5.3.2.4 The influence of 5G technology on industry 4.0

The application of 5G technology in the industrial Internet has a profound impact, first of all, in the application of 5G Mobile Terminal, on the application of the industrial Internet has a great impact, can effectively promote the industrial Internet derivative more and update applications, in the application of super-large integrated technology will be widely used 7nm line width, Chip integration is also relatively high, computing power is also relatively high, functional aspects are also more, can be directly connected to the network services smartphone. With the application of 5G technology, the user and the connected function terminal in the system will become the theme of information generation and interaction, which can guarantee the attribute of Intelligent terminal Platform more prominent, and can effectively improve the application quality level of industrial Internet system.

The application of NFV technology in 5G technology has a great impact on it, which plays a positive role in promoting the software definition and the driving force of technology development, the technical standard Server software can effectively realize the traditional network equipment function, so as to ensure the virtualization and programming of network equipment, It lays a technical foundation for the goal realization of intelligent network maintenance, which enables the whole architecture to scale automatically in combination with the change of business volume, thus saving the cost of network hardware. In the application of NFV technology in industrial Internet applications, we should pay full attention to the classification of equipment, and then subdivide the functions of no class equipment, with standard hardware, different software virtual, different machine functions, which has a great impact on software-defined machines.

5G technology applied in the industrial Internet, the impact for open and unified integrated platform is also more prominent, this new proprietary technology combines current technology and applications, on the basis of mature technology to add a number of innovative integrated technologies, this open and unified multi-standard platform technology has greatly improved the application level of industrial Internet, it also played a positive role in the application and development of different industry

standard Internet technology, it has been effectively reduced in the industrial chain link, it can achieve the goal of unified interchange between the pipeline and the workshop, thus facilitating the improvement of industrial management level.

In the application of 5G technology in industrial Internet, SDN technology has a more prominent impact on it, which can promote the interconnection of heterogeneous networks in the Internet is relatively simple and convenient, this design idea under the goal of software and centralization, the openness of the network and high efficiency to produce effective promotion, so that the control plane for the user standard programming interface , through the implementation of the standard protocol interface receiving strategy, can ensure the sharing of the entire industry, the overall level of industrial manufacturing has played a positive role in the improvement. In addition, this technology from the bottom can ensure that the industry professional subnet connection is more simplistic, and generally reduce the cost of network management.

The high speed, high broadband and high quality of 5G networks can help the industrial Internet integrate into the mobile internet sector. The highly networked and intelligent of industrial manufacturing system requires the network system to have high broadband, high speed and high reliability, to ensure the accuracy of operation in the connection and

automatic control of all links in industrial production, especially in the mobile Internet environment, the interconnection of users with the machines located in each factory, the reliability is highly dependent on the high quality of mobile network. As a 5G system of mobile internet in the future, most of the new technologies focus on wireless channel high broadband, high speed and high reliability, such as non-orthogonal multi-access, large-scale MIMO antennas, millimeter wave communication and simultaneous frequency full duplex, respectively, the use of time, frequency, space, code and other channel resources to expand bandwidth, increase the rate, The diversity technology is used to improve the reliability of transmission. Therefore, the impact of 5G network on the integration of the industrial Internet into the mobile environment is enormous.

5.4 Analysis of cybersecurity’s threat in China's industry 4.0

With the development of China's industry 4.0, manufacturing industry has ushered in a huge opportunity to develop, but at the same time it also brought a new network information security threat, only a thorough study about the network information security threat’s new characteristics,

according to these characteristics to propose new preventive measures and solutions, in order to fully maintain the information security.

5.4.1 Network Information Threat characteristics

With the development of Industry 4.0, Chinese manufacturing began to strengthen, industrial production more and more information, intelligence, network and data become an indispensable part. These developments are premised on the assurance that information security can be guaranteed. In the development of Industry 4.0, production began to integrate, and this poses a growing threat to network information security, mainly manifested in the following aspects:

(1) Alienation affecting the morphology and characteristics of matter.

With the development of the Internet, many commercial industries began to use the Internet development, has become the most potential emerging markets, but this will not affect the changes in material form and characteristics. However, with the integration of the Internet into intelligent manufacturing, many products to achieve data and remote operation, real-time sensing. These established platforms can achieve their own data exchange and product monitoring and decision-making, the overall implementation of autonomous operation. We can find that

only manufacturing in the network security can not only achieve the intrusion of all aspects of the product, but also can affect and change the physical and physical form of the product itself, and gradually alienate it, thus creating a new network information security threat.

(2) Cyber-Physics system becomes the core target of cybersecurity threat.

Because the information stored in the information Physics system is not very hidden, it is vulnerable to attack. This involves privacy issues and security issues. In an open environment, network information can be easily stolen, but also affect the efficiency of use. Many control tasks are changed without authorization and there is no guarantee of effective control. This has become the influence of intelligent manufacturing on the new characteristics of network information security threats.

(3) There is a risk that intelligent manufacturing is under attack.

Today's technology makes it easy for many information threats to be realized in open spaces. For example, through electromagnetic interference, thus destroying the operating environment, and then can achieve large-scale data attacks. The consequences of this data attack are more serious. This threat exists in countries around the world, so we need to take malicious attacks seriously, which is also a new challenge.

(4) Lack of intelligent manufacturing safety standards.

In the want to achieve a highly intelligent operation of the integrity, it is necessary to a unified, perfect intelligent manufacturing security standards. Only by using the perfect intelligent manufacturing safety standard as the foundation, can the optimal configuration of various systems be truly realized. The threat in this regard is also a threat that we are most concerned about. Most countries in the world already have their own relevant standards.

5.4.2 New challenge of network information security

The use of a wide range of intelligent systems in industry would have been an independent system that would not be disturbed by the outside world, but with the development of the Times, it was gradually invaded and destroyed by many hackers. Information security in industrial systems is threatened and shows an increasing trend. This is very detrimental to the economic development of the country, especially the self-replication of the virus, remote monitoring and direct attack. Many of China's high-tech industry core products are from abroad, the probability of data being monitored will also increase, so faced with the danger of starting late, only the weak security protection function to pay attention to, in order to minimize the network information security threat coefficient.

5.4.3 Improvements of intelligent manufacturing cloud security and big data security

Cloud security and big data security is an indispensable part of intelligent manufacturing in the future, which is also the trend of information development. Data preservation will rely heavily on cloud services. The security of personal information can only be ensured by minimizing the risks that exist in the cloud computing environment. Currently, many data breaches are related to intentional attacks, accidental leaks and losses.

Only by realizing the security protection at the technical level can we reduce the risk on the basis.

To ensure cloud security and data security, you need to start with 2:

(1) To improve the technical level. Only with a high level of technology, can we achieve a higher level of information security protection. One of the important characteristics of intelligent manufacturing is the huge amount of information. This is also an easy cause of information disclosure, but it is also a key point in improving the technical level. By combining prevention of real-time data and business data, we can strengthen the management of illegal network behavior, reduce hacker

intrusion and network fraud, use big Data technology to integrate information, and find the source of attackers.

(2) The development of intelligent manufacturing can not be separated from legal supervision. Only legal constraints, can be reasonable development, only the use of rules and order to achieve constraints, play the role of network supervision, in order to solve the network complete problem.

5.5 The 5G Technology to protect cybersecurity.

As described above, the cybersecurity is the base of cyber-physical security, it plays the key role in the CPS, and now the 5G technology is a new technology and quickly development, as we introduce above, it also play an important role in the industry 4.0, so use the 5G to protect the cybersecurity can ensure the safety of cyber-physical system.

As the reference of “The future of Cybersecurity in Italy: Strategic focus areas ”describes, the wireless and mobile nature of communications in cellular systems has historically implied the need to protect data in transit. This activity has been duly tackled over the course of previous generations of cellular systems, with solutions that, though gradually and through various evolutions, have now reached a level of protection

considered satisfactory (it is not a coincidence that over the last ten years there have been no significant developments in this field).

However, the 5G network includes not just the mobile network, but also landlines, supplying services arranged end-to-end and with performance parameters that are by far better than the actual solutions. Moreover, it has a wider ecosystem that involves many players and more complex relationships and business opportunities; it sets new requirements (e.g., relative to the IoT environment and to highly reliable and low-latency applications); it is characterised by increased heterogeneity and dynamism, radically new technical solutions, among which the "softwarisation" of network functions and the splitting of the network into "slices".

Such functions are today at least partially implemented in hardware, also by virtualising current physical devices. A network implemented in a software can be split into slices, each of which supplies, end-to-end, a virtual autonomous network to a subgroup of users, able to meet specific needs of a specific scenario/case of use, in a comprehensive framework, in which different organisations coexist within a network (multi-tenancy).This set of features deeply changes network security issues.

In view of the considerable progress made in recent generations, with regard to the security of cellular networks, it is legitimate to wonder if security should also play an important role in 5G networks, or if the bulk of the work has already been done. The answer is that, despite the significant improvements made to cellular networks over previous generations, the new emerging requirements in 5G systems and, above all, the radical change of perspective that characterises the 5G network (which includes not only the cellular network but also the fixed network), bring about new problems that must be faced. While the previous 2/3/4G systems were well defined a priori and their requirements clearly listed, homogeneous and relatively stable, as well as the related security and data protection solutions, the emerging 5G systems are strongly focused on the integration between heterogeneous technologies, partitioning (slicing) and virtualisation of network infrastructures, and on the support of extremely diversified services. They are also no longer exclusively dedicated to human users.

We therefore believe that the security architecture of 5G systems should be extended to cover (at least) the following aspects:

• IoT and heterogeneous Terminals — One of the most significant differences between traditional cellular systems and the new generation 5G consists in the availability of services no longer necessarily reserved

for terminals managed by humans, but extended also to Machine-TypeCommunication (MTC). This will lead to the spread of terminals with extremely disparate characteristics (in terms of cost, energy consumption and complexity of implementation) so that a "one-size-fits-all" security model, which had characterised security solutions in previous generations, may no longer be adequate. For example, security mechanisms designed for mission-critical services may not be applicable at all in a context of IoT devices, where network sensors have very few computational and energy resources and where data transmission is sporadic. 5G systems will therefore not only be called upon to support cryptographic techniques (for authentication or encryption of data) that are extremely variable in terms of robustness and level of protection, but, above all, it will be necessary to develop both new models for the management of such heterogeneous security solutions and new trust models.

• Signalling Traffic — In addition to the need to identify differentiated security solutions for the services offered, that are also more flexible than the 'unique" solution currently offered by 4G systems, another important aspect related to MTC services is that signalling traffic could even be more dominant than data traffic. This is followed, for example, by the need to develop solutions capable of recognising (and defending oneself

from) attacks aimed at saturating the network resources dedicated to signalling traffic; a well-known bottleneck in the case of MTC services is the access to the RACH (Random Access Channel) which could become critical in case of simultaneous and malicious activation by a botnet IoT.

• “Flexible” security — The 5G network will be characterised by the need to have extremely flexible security solutions and to be adaptable to the specific (different) scenarios considered. For example, services with very low latency characteristics will require security solutions which in turn require very low latency and therefore (ultimately) flexibility in the ability of the network to activate the most suitable security solutions for a given scenario. In addition, the problem of flexibility in security management must go hand in hand with tools to simplify the management of network security, allowing rapid adaptation to new services and needs, not only regarding network operation, but also the security solutions proposed.

CONCLUSION

CPS is another big change after the internet, which has broad application prospect and great social influence in agriculture, industry, transportation, daily life and so on. But the deep fusion of information systems and physical systems makes CPS far more complex than the previous single system and hides more security flaws. Security is always a important factor in the development process of CPS, and will ultimately determine the use of CPS degree. Because of the particularity of CPS network, it will face great security challenge. This paper analyzes the security threats faced by CPS, gives the corresponding countermeasures, and finally emphatically analyzes the authentication technology, access control technology and privacy protection technology. The safety technology of CPS in guarding against attacks outside the system and protecting users ' privacy has yet to be further researched in order to make it more perfect.

In the future, the research direction of access control is likely to include the following focal points. The research of security and access control for nodes with limited computing, communication and storage capability and mobility in wireless sensor network environment are all areas of prospective research. This is also needed in situations where a quick authentication and authorization is required. It is also a meaningful

research direction to study the secure, reliable, fast, verifiable and active access control mechanisms. In the environment of physical information systems, the context information of computable resources is usually fuzzy, uncertain and incomplete. These types of computing resources are updating dynamically and therefore the theory and techniques of fuzzy access control will become an important research direction.For privacy data protection, further research on privacy protection in wireless sensor networks and data mining is needed. Anonymity technology in privacy protection needs to deal with the balance between privacy protection and the resultant accuracy. To study methods of hiding data the heterogeneous data fusion of CPS is a necessary research direction in the field of CPS security. Traditional security multi-party computation requires that the computational resources involved can be computed and communicated. The efficiency associated with this is low, and it is an important problem to search for the ideal secure multi-party computation algorithm for CPS security research. Non-technical factors of information security, including public awareness of data security, is not strong. Enterprise weight-data collection, light data mining, intelligent processing, lacking social information for security related laws are other future security research areas which must consider at least one of these factors. From the perspective of induction, transmission and service, the

architecture of physical information systems can be divided into the perceptual layer, data transmission layer and application control layer. It is necessary to provide different preventive strategies for different security threats because the security threat of physical information systems is very different in physical entities, network space and application services. Some security issues have not changed in new physical information systems, resulting in upgrades only to existing security levels. Some security issues require the study of new security technologies. The next major goal to be studied is to improve the existing security services and build a secure service model of physical information systems.

Also the industry 4.0 process and it's CPS still has a long way have to go, but with the quickly development of some technology, such as 5G technology , is a very good factor to push the advance of industry 4.0, as well as a good measure to ensure the CPS, So we believe that the future of industry 4.0 should strongly have the aid of 5G technology.

REFERENCE DOCUMENTS

1. Akella R，McMillin BM ．Model—checking BNDC properties in cyber-physical systems. Proc.of International mputer software and Application Conference．Seattle，WA．2009．660-663．

2. Xu Z，Liu X，Zhang GQ，He WB，Dai GZ，Shu WH．A certificate less signature scheme for mobile wireless cyber-physical systems． Proc．of the 28th International Conference on Distributed Computing Systems Workshops．

3. Tang H，McM illin BM．Security property violation in CPS through Timing． Proc． of the 28th International Conference on Distributed Computing Systems Workshops ． Beijing ． 2008 ． 5 19-524．Beijing．2008．489-524．

4. Fawzi H，Tabuada Digga~ S．Secure estimation and control for cyber-physical systems under adversarial tacks．http：// arxiv．Org//abs/1205．5073． [2013—8—8]

5. Ferraiolo D, Kuhn R．Role—based Access Controls．Proc．of l 5th NIST-NCSC National Computer Security Conference ． USA Baltimore．1992．554-563．

6. Bonatti P, Samarati A uniform framework for regulating service access an d information release on the web．Journal of Computer Security,2002，10(3)：24l_271．

7. Wang XM, Fu H, Zhang LC. Research progress of attribute-based access control. Electronic Journal. 2010，38(7)：1660-1667

8. Park J, Sandhu R. The usage control mode1. ACM Transactions on Information and System Security,2004，7(1)：128—174．

9. Garcia—Morchon O, Wehrle K． Modular context—aware access control for medical sensor networks． Proc． of the 1 5th ACM Symposium on Access Control Models an d Technologies．New York，NY,USA．2010．129—138．

10. Busch S, Muschall B，Pernul G Priebe Authmle. A generic rule—based authorization module．Lecture Notes in ComputerScienee，2006，4127：267—281．

11. Wu J，Shimamoto S．Usage control based security access scheme for wireless sensor networks． Proc． Of the IEEE International Conference on the Communications(ICC’2010)． Cape Town,South Africa．2010．1-5．

12. Wang Xiaoming. Interval-valued fuzzy access control for pervasive computing. Computer Science and exploration, 2010，4(10)：865—880．

13. Dou WY, Wang XM, Zhang LC. Research on dynamic fuzzy access control model in pervasive environment. Computer science, 2010，37(9)：63—67．

14. Zhang Lichen. Research on active access control model oriented to pervasive computing, 2011.

15. Lu Dongze. Security access control mechanism of information physical system, 2010.

16. Guo YJ, Wang L, Hong F, Han LS. Dynamic authorization model of pervasive computing based on trust. Journal of Hust (Natural Science Edition), 2007,35 (8): 70-73.

17. Liao JG, Hong F, Zhu GM, Yang QW. Authorization delegation model based on trust degree. Journal of Computer Science, 2006,29 (8): 1265-1270.

18. Campbell R，AI·Muhtadi J，Naldurg P，Sampemane G Mickunas MD．Towards security and Privacy for pervasive computing．Lecture Notes in Computer Science．2003．2609．77-82．

19. Hourdin Tigli J，Lavirotte S，Rey G Riveill M．Context—sensitive authorization in interaction patern s．Proc．of the 6th International Conference on Mobile Technology, Application & Systems. Nice. France．2009．1-8．

20. Oleshchuk V. Internet of Things and Privacy Preserving Technologies．Proc．of the 1 st International Conference on Wireless Communication， Vehicular Technology, Inform action Theory and Aerospace& Electronic Systems Technology, Wireless VITAE'09． Aalborg Denmark．2009．336-340．

21. Sweeney L． K-anonymity： A model for protecting privacy． International Journal of Uncertainty, Fuzziness and Knowledge—based Systems，2002，1 O(5)：557-570．

22. LeFevre K， DeWitt DJ， Ramakrishnan R． Mondrian multi-dimensional k-anonymity Proc. of the 22nd International Conference on Data Engineering(ICDE)．Atlanta，Georgia，USA．2006．25-35．

23. Xiao X． Tao Y m-Invariance： Towards privacy preservingre． publication of dynamic datasets． Proc． of the ACM SIGMOD Conference on Management of (SIGMOD)．Beijing．2007．689-700．

24. Roberto Baldoni, Sapienza Università di Roma Rocco De Nicola, IMT School for Advanced Studies, Lucca Paolo Prinetto, Politecnico di Torino： The Future of Cybersecurity in italy: Strategy project areas 2018