# Establishment of Industrial Internet Security Management System

## Wang Dahai

Changchun Humanities and Sciences College, Changchun, Jilin, China

**Keywords:** Industrial Internet, Security management system, Establishment strategy

**Abstract:** With the continuous construction of "new infrastructure", the field of industrial Internet has attracted much attention. Industrial Internet platform is closely related to industrial production and enterprise management. Once the platform is invaded or attacked, it may cause industrial production to stagnate, affecting not only a single enterprise, but also the entire industrial ecosystem. Therefore, doing a good job in platform security is an important guarantee to ensure the safety of industrial Internet application ecology, industrial data, industrial system equipment, etc. Based on this, the article explores the establishment of industrial Internet security management system.

## 1. Introduction

The rapid development and application of industrial Internet has promoted the intelligent development of manufacturing industry, which not only helps to reduce labor costs, but also promotes the improvement of production quality through automatic and intelligent control, decision-making, adjustment, perception, etc. The biggest risk facing the development of industrial Internet is security. Therefore, we should strengthen the research on security development and do a good job in security protection.

## 2. Overview of Industrial Internet

Industrial competition is very fierce. In the past, there was a big gap between China's industrial development and developed countries. Industrial Internet provides an opportunity for China to catch up with developed countries. Although the current industrial development plans of various countries are different, they are fundamentally committed to promoting industrial innovation and change, in which the industrialized Internet plays a major role in promoting and driving. Industrial Internet is actually the integration of modern technologies, such as information technology and Internet technology, with industrial manufacturing and production to form a new industrial ecological model. Compared with traditional industrial production, the industrial Internet ecological model is highly intelligent, and all kinds of information can be obtained in the comprehensive and in-depth combination of the two. Connect all parts by using network information technology. In addition to industrial production equipment and machines, people and products involved in production will also be introduced into the interconnected system. Finally, in automatic control and information acquisition, master the situation of industrial production, and then rely on relevant modules to process data, on this basis, carry out intelligent adjustment and control, and be able to make intelligent decisions. Under the industrial Internet mode, production synergy is stronger, and it promotes the development of personalized production and automated production. The biggest risk of industrial Internet is security, so it is necessary to strengthen security prevention and control.
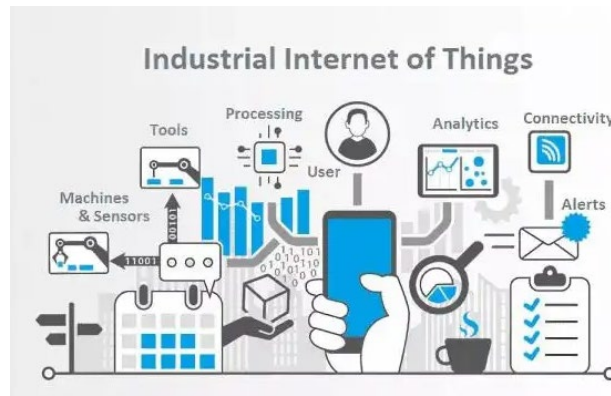
Figure 1 Mode of industrial Internet

## 3. The Security Risks of Industrial Internet

### 3.1. Network security issues

In the past, bus technology was mainly used in the network part of industrial production. Now there are great changes in this aspect, and it will gradually form a combination of three networks and flexible networking under the continuous development, which will have a certain impact on the safety of industrial production network. The new network form and network form of industrial production have prominent security problems, which are mainly reflected in the vulnerability to external attacks. The network needs to use switches in supporting industrial production, which has poor security performance and insufficient ability to resist and resist attacks. In addition, there are still serious static security problems in the industrial Internet ecological model. Compared with the past, the networking form is more free and has obvious dynamic characteristics. If the static security prevention and control mode is still adopted, the network security risk will inevitably increase. The application of wireless technology in industrial production meets the requirements of network related performance to a certain extent, such as real-time transmission, but it also brings a great risk of information leakage and faces severe potential intrusion.

### 3.2. Equipment Risk

After the shift from manual production to mechanized production, safety risk prevention and control mainly focus on two parts. One is personal safety, the other is physical safety. In the industrial Internet Ecosystem, when production equipment changes, the software that needs to be used or the system that needs to be used in production will be embedded into the equipment system, and then control and decision-making tasks will be completed in production. Industrial production is more intelligent. Although it helps to improve productivity, it also makes the equipment have greater security risks and the probability of network attack increases. Once the equipment is infected by the virus, because the whole production is interconnected, the virus will quickly spread and spread among the equipment, which will not only lead to equipment operation failure, but also a very large information security risk.

### 3.3. Data Risk

With the combination of industrial production and network information technology, the level of automation and intelligence of production will be improved, and massive data will be generated. These data have the characteristics of many structures and types, and show a trend of two-way flow. The data risk rises all at once, which is mainly reflected in the complex industrial production, strong liquidity after data generation, and the transmission path is not fixed, resulting in difficulties in management and control, which makes it difficult to play a good protective effect, and increases the safety risk of production data. Information can generate value, which is the most important feature of the era of big data. At present, the value of mining data and information has been generalized. Driven by interests, there are many data collection behaviors, which are easy to cause data to be

stolen or illegally used. Although some of the data analysis master low value data, they can master relevance in analysis and sensitive data information in prediction and inference. In addition, the industrial Internet has expanded the production service space and promoted personalized customization. The generated data information is related to privacy, and once it is leaked, it will cause serious trouble to customers.

## 3.4. Targeted Attack Threat

The development of industrial Internet can promote the improvement of industrial control level and ability, but there are also hidden dangers, which are mainly reflected in the frequent targeted attack threats. Among the industrial Internet security threats, targeted attacks organized by hackers are the main part, which is difficult to prevent. Critical industrial systems are currently the main targets of hacker attacks, and the incidence is still rising, which must be paid attention to. Hackers often carry out targeted attacks on industrial Internet systems through malicious code because of interests or other reasons. It is found from the targeted attack data of industrial Internet published by various countries that this situation is relatively serious, and the resulting security incidents are harmful, which seriously affects the security of industrial systems. China's industrial Internet is facing great challenges. It is found in relevant monitoring and tracking that important industrial fields (such as military industry, energy, etc.) are the primary targets of attacks. There are two kinds of attacks: puddle attack and harpoon attack. The ultimate goal is to steal important and confidential industrial data.

## 4. The Establishment Strategy of Industrial Internet Security Management System

### 4.1. Improving the Safety Management Mechanism

Under the research of industrial safety guarantee, developed countries set up an overall planning organization for safety protection. The development of industrial safety in China can be used for reference. In improving the safety management mechanism, we can also set up a special safety planning organization, and clarify the responsibilities of management and protection responsible persons and relevant positions. The development of industrial Internet security is within the management responsibility of the security planning organization, and we should do a good job in the division of labor for this aspect of security assurance. Governments at all levels should be involved in the management organization, clarify the management responsibility and authority, and do a good job in coordination. Network security management forms a common force, the management effect will be better, and the security of industrial Internet will be more guaranteed.

### 4.2. Improving the Safety Standard System

The development of industrial Internet security needs to establish security standards and establish a sound standard system, so as to effectively reduce the risks of equipment security, data security and network security. This requires the linkage of relevant departments to jointly develop industrial Internet security. Industrial Internet security involves a wide range, and it is difficult to achieve the purpose of control by relying on simple forces. Therefore, it is necessary to coordinate the relevant parts together to achieve the expected control effect under the cooperation of various forces. Government Internet Security Supervision and management departments, Internet security research institutions, industrial equipment and software manufacturers, industrial production enterprises, etc. cooperate and enhance exchanges, and jointly study and discuss to determine safety technical standards, safety management standards and safety evaluation standards. Under the development of industrial Internet Ecology, these standards should be strictly implemented to promote the standardization and standardization of Internet security control. The development of industrial Internet security should have international awareness and vision, actively participate in the formulation of relevant standards in the world, and participate in the formulation of rules to enhance China's voice and influence in this field.

## 4.3. Improving the Level of Safety Assurance Technology

The development of industrial Internet is unstoppable, and security is the main factor affecting the development. Therefore, we should improve the level of security technology to achieve the purpose of eliminating all kinds of security risks. The industrial Internet should be well constructed in combination with the characteristics of development and the actual situation of the system architecture. Under the background of industrial Internet, it can develop towards discrete industry and create discrete industry in line with the development characteristics. These belong to the national level, and then from the perspective of risk prevention and control, relevant staff can use simulation or security testing to combine relevant technologies, grasp the basic characteristics of industrial Internet security issues, and formulate targeted security strategies on this basis.

## 4.4. Attaching Equal Importance to Functional Security and Information Security

With the development of industrial Internet, industrial systems have been greatly improved, but there are also great information security risks. Once it is leaked, especially important and confidential, it will cause major problems in industrial development and great losses. Therefore, in the era of industrial Internet, we should not only enhance security from the perspective of function, but also ensure security through effective means from the perspective of information security. For targeted attacks, we should do a good job in security compliance construction, improve standards, improve functional security and information security protection benefits, and maximize the control of security incidents. In practice, for hacker attacks or other attack uncertainties, we must change from the original response and protection to the establishment of a new security operation mode to prevent attacks.

## 4.5. Establishing a Collaborative Protection System

The security problem of industrial Internet is prominent and serious, and has strong complexity, so the security protection should establish a collaborative mechanism. In view of the security risks and problems existing in the industrial Internet, we should establish a protection alliance, do a good job in the security system architecture, and work together to enhance the effect of security protection. Comprehensively strengthen safety operation, carry out closed-loop operation while monitoring risks, and dynamically monitor and deal with security threats at the same time, so as to make security protection more in-depth, and maximize the comprehensive security protection ability and effectiveness on this basis.

## 5. Conclusion

In short, major changes have taken place in industry with the support of the Internet, which will promote productivity to the greatest extent. At the same time, the Internet also brings great challenges to industrial development, that is, industry needs to face certain security risks. Industrial Internet is the general trend, and the integration will be closer in the future. Therefore, at present, relevant staff should strengthen the research on security issues, find effective methods and paths to prevent and eliminate network security risks in industrial production, help the industrial Internet economy take off, enhance information security and functional security in industrial development, and promote better development.

## References

[1] Tianlikun. It is urgent to build a security management system for industrial Internet platforms[J]. China Science and technology industry, 2022 (03): 28-29.

[2] Zhaoyue. Analysis and Research on security protection system of industrial Internet platform[J]. Changjiang information and communication, 2021,34 (06): 132-134.

[3] Majuan, Yuguangchen, Kehaoren, Yangdongmei. Research on network security management and protection of industrial Internet equipment[J]. China Engineering Science, 2021,23 (02): 81-87.