ISSN: 2664-9640

Research on the Challenges and Countermeasures Facing the Application of IOT for Equipment Security

Yue Liu[1,a] , Tielin Liu[1,b], Rongzeng Li [2,c] , Yongfeng Wang [2,d], Yanhui Liu [2,e]

[1]Shijiazhuang campus of Army Engineering University of PLA, Shijiazhuang, China

[2]Unite 93786 of PLA, Zhangjiakou, China

[a]224455864@qq.com, [b]sfep2001@sina.com, [c]sishuiliunian3@163.com, [d]sishuiliunian3@163.com, [e]sishuiliunian3@163.com

Abstract

The application of Internet of things technology in the field of equipment security, accelerate the development of equipment security intelligence, is an important way to develop military intelligence. In this paper, based on the analysis of the factors that restrict the development of the application of the Internet of things in equipment security, the countermeasures to accelerate the development of the Internet of things in equipment security are proposed, which have a reference to the application of the Internet of things in equipment security.

Keywords

Equipment security; Internet of things; radio frequency identification.

1. Introduction

The 19th Party Congress pointed out the need to speed up the development of military intelligence and improve the ability to conduct joint operations based on the network information system and the ability to conduct all-area operations. As an important part of the development of military intelligence, the Internet of Things for equipment security, by fully integrating the traditional thinking of the physical space of the battlefield and the cyberspace of equipment security needs, open the channel of direct communication between the virtual network world and the real physical world, so as to be able to obtain comprehensive, accurate, real-time equipment information flow and security information flow in all aspects of the battlefield, to obtain the state of things, people, and the environment in equipment security activities Information and characteristics, strengthen the ubiquitous interconnection between people and things, things and things, people and the environment, and ultimately achieve information interoperability, integration and sharing, and improve equipment security capabilities. Therefore, the rapid development of equipment security Internet of things has been an important way for each military power to seize the strategic high ground.

2. The difficulties and challenges facing the application of equipment security IOT

Internet of things in the field of equipment security as a strategic emerging industries, broad application prospects, rapid development, but its related technology development and application are in the initial stage. In terms of the current application status, equipment security Internet of Things application also faces multiple difficulties and challenges.

a. Lack of talent is the soft resistance that restricts the application of equipment to protect the Internet of Things

ISSN: 2664-9640

At present, the comprehensive quality of security personnel and traditional equipment security thinking has seriously restricted the use of the Internet of Things in the field of equipment security. The U.S. Army believes that "training and absorbing all kinds of talents with strong information capability is the key to improve the overall information capability". In recent years, the U.S. military has taken various measures to train a large number of high-quality personnel, thus laying a solid foundation for the U.S. military information technology construction. However, our military equipment security Internet of things in the initial stage, technical talent reserves lagging behind, the level of technical personnel is relatively low, the learning of Internet of things technology, skills mastery, operational applications can not meet the needs of the troops. Secondly, the equipment security personnel traditional mechanized equipment security mode of thinking hinders the application of the Internet of things in the field of equipment security. Internet of things as a new technology, the application in the field of equipment security is in its infancy, security personnel do not know enough about the Internet of things, can not correctly understand the advantages of equipment security Internet of things and the importance of the application, distrust and skepticism of the Internet of things, restricting the development of the Internet of things in the field of equipment security.

b. High cost is a hard resistance to the application of equipment security IOT

The Internet of things applied to the field of equipment security can undoubtedly improve equipment security benefits, but the higher cost of intelligent induction equipment has become a constraint factor for the Internet of things to be widely used. Will the Internet of things applied to equipment security, the most important is the RFID system set up, with its related equipment, such as electronic tags, antennas, read-write expensive, at the same time for the implementation of radio frequency identification equipment to be used in the infrastructure, such as the acquisition of readers, etc., the employment and training of related technical personnel, the establishment of related communication equipment, data processing platform, integrated comprehensive system are required a lot of capital investment. In addition, the superiority of the equipment security Internet of things need network scale to a certain extent to show, from the overall point of view, the current stage of equipment security Internet of things construction range is small, narrow application areas, the development is still very unbalanced, has not formed a large-scale network chain. Only continuously improve the construction of equipment security network of things road, its advantages can be given full play. It can be seen that to achieve the scale of equipment security Internet of things still need to invest a lot of human, material and financial resources.

c. Information security is a potential threat to the application of equipment security IOT

In the underlying structure of the equipment security IOT, the battlefield environment is complex and harsh, and the position of each terminal node changes dynamically, which has a certain degree of influence on the safe and stable operation of the equipment security IOT and poses a great threat to the battlefield survivability of the equipment IOT.

In the application process of IOT technology, security and reliability is the basis of equipment security IOT application. The information transmitted in the equipment security IOT involves troop secrets and carries a large number of complex equipment security operations such as status monitoring, fault diagnosis, security force command, equipment supply security, etc. However, the equipment security IOT as a platform for information interaction and sharing, in addition to having a variety of threats such as information leakage, information tampering, denial of service, etc. faced by general wireless networks, also faces sensing nodes that are vulnerable to attackers Physical manipulation and theft of all information stored in the sensing node security risks. In particular, RFID tags are mainly through sensing technology to obtain information without direct contact with the transceiver, the user will be unknowingly read the information stored in the tag by others, posing a serious threat to information security.

ISSN: 2664-9640

At this stage, the equipment to ensure that the sensor connection technology used in the Internet of Things is more restricted by the influence of distance. As the sensor itself is a precision device, the external environment requirements are high, it is easy to be subject to interference from the external environment, therefore, to ensure the safe and stable operation of the Internet of Things, the equipment and subsystems within the system must have superb reliability and resistance to destruction. In particular, the complex electromagnetic environment under the full range of high mobility operations, the RFID system read and write distance, the sensitivity of the induction has a great impact; furthermore, RFID UHF tags due to electromagnetic backscatter characteristics, the metal and liquid and other environments are more sensitive, can lead to this working frequency passive tags difficult to work in objects with metal surfaces or liquid environment.

The energy consumption and transmission efficiency of wireless sensor network nodes are also important factors that affect the survivability of equipment to safeguard the IOT battlefield. First, the many wireless sensing network nodes, in the long working process consume a lot of energy, and the network node energy device replacement will consume a lot of human, material and financial resources, the design can be charged quickly, less energy-consuming sensing system, is an important issue to be resolved. The second is the efficiency of wireless sensing network transmission data problem. The sensing layer of the IOT system can acquire a huge amount of data at the same time, which makes the IOT system have large limitations in data transmission, storage and processing.

d. Architecture is the fundamental obstacle that restricts the application of IOT for equipment security

Our military equipment security Internet of things construction has not yet formed a more complete planning program, framework structure and standard system, the lack of overall planning guidance, and has not formed a mature mode of operation and application system, which to a certain extent hindered the integration of equipment security Internet of things development.

IOT information chain involves a wide range, many departments, in the construction process of equipment security IOT, the existing information system has not formed interoperability, mutually compatible system structure, the lack of standardized information classification and processing, data format and business process inconsistent, data exchange is not standardized and interconnection interface is not compatible, it is difficult to achieve data exchange and integration, networked information resources synthesis and information Sharing, resulting in the division of the "silo", the formation of "things and things connected, network and network isolated" status quo, how to integrate information systems, to achieve equipment security networking hardware matching, software compatibility, unified standards, plug and play, has become the equipment The main problem facing the construction of the Internet of things to protect.

At present, the Internet of things is not a widely recognized architecture, the most representative IOT architecture is the European and American support of the EPC Global IOT architecture and Japan's Ubiquitous (UID) IOT system. China is also actively involved in the above-mentioned IOT system, is actively developing IOT standards and architecture in line with the development of our country, is committed to completing the construction of independent technical standards system framework, promote the development of common and key technical standards, the development of equipment to ensure the construction of IOT standard system. Only unified technical standards, improve the management mechanism, the use of a unified platform, standard mode of operation, in order to play a leading role of the Internet of things in the field of equipment security.

ISSN: 2664-9640

3. Analysis of countermeasures for the construction of the Internet of Things for equipment security

a. Unify the construction ideas and do the overall planning layout

Equipment security Internet of things is a new thing, both no theoretical results reference, and lack of construction experience to follow. Therefore, it is necessary to closely follow the foundation of equipment security information construction and the current situation, combined with the current needs of the development of equipment security and the current situation, the scientific establishment of equipment security Internet of things construction ideas.

Top-level design, task traction. Our army equipment security Internet of things construction must be incorporated into the overall framework of information technology construction of the army, from the security needs and objective reality, the Internet of things construction and development of integrated planning. Combined with the latest development trends inside and outside the military, objective analysis of construction conditions, scientific and reasonable to establish the equipment security networking technology system and mode of operation. At the same time, equipment security networking construction must be combined with the new era of military struggle preparation, carefully study the basic requirements of information warfare on equipment security, from the actual forces, reasonable planning equipment security networking construction.

Divided into phases, highlight the focus. According to the technical characteristics of the equipment security network of things, on the basis of a full demonstration, divide the stages, highlight the focus, that is, according to different needs, highlight the key links and key systems, in stages, step by step construction. First, adhere to the end first, that is, first in a single suit and below the battalion combat and security detachment for end construction, and then to the high level by level expansion, through the end of the construction of key technologies, the implementation of demonstration projects, to explore the application model. Second, adhere to the pilot first. Carry out the innovation of application mode, establish pilot operation mechanism, and carry out the demonstration of the application of equipment security Internet of Things in the fields of condition monitoring, battlefield perception, and fault diagnosis. In the country and the army system selected relevant representative units as a pilot, in accordance with the strategy - battle - tactical three levels to build level by level, and at each level to promote the Internet of things and cloud computing information processing platform construction, as appropriate, gradually and fully promoted. Third, adhere to the side of the construction of the use, the combination of construction and use. In the application of deepening demand, repeated practice, and constantly improve the update, promote the development, especially in infrastructure, technology applications, organizational systems, regulations and systems, personnel training and other elements of the construction has not been perfect, involving many factors, complex systems, its construction is by no means a quick fix, need to constantly explore the verification and a lot of technical, financial and human investment, relying on the reality of national conditions and military conditions for Long-term planning, deal with the relationship between long-term development and current needs, step by step implementation, focus on accumulation, steady progress, so that the construction of equipment security Internet of things become a spiral development process.

b. Increase scientific research to break through the bottleneck of technological development

Accelerate the construction of equipment security Internet of things, must focus on multiple resources, collaborate to carry out major technical research and application of integrated innovation, as soon as possible to break through the core key technologies.

ISSN: 2664-9640

Research and development of decision support systems, improve decision-making capabilities. To real-time perception, intelligent control as the goal, the development of the Internet of things on the analysis and optimization of massive data, intelligent processing technology and scientific analysis of battlefield information algorithms, the establishment of intelligent decision support system; promote parallel computer technology, vigorously strengthen the research and development of intelligent information networks as the central nerve of the Internet of things, give full play to cloud computing and "supercomputer " powerful processing capabilities, efficient use of RFID tags and sensors to obtain a large amount of equipment security information, fast, intuitive, flexible for the equipment security commander to provide different target perspective of the decision program recommendations.

Strengthen technical prevention and improve system security. In wartime and peacetime emergency security tasks require data network transmission and navigation and positioning platform, etc. to achieve equipment security sensitive, fast, the whole visual and controllable functions. In the process of construction of equipment security Internet of things, increase the network, communication, navigation and positioning and radio frequency identification system security protection, such as wartime network platform may be subject to enemy virus implantation, information bombs and other forms of attack threats, network security issues are very prominent, in order to improve the confidentiality of network information availability, must be used to establish firewalls and related security protocols and other ways to improve network security level, build The comprehensive network security protection system of "security protects the win"; the radio frequency recognition system should adopt the relevant anti-jamming technology, examine and screen the interference signal, and encrypt the transmission data, and use the encryption algorithm to verify the authority when the radio frequency recognition reader and the electronic label communicate, so as to fully realize the security and confidentiality of the communication data, etc. . Through the realization of network communication and real-time data transmission and other systems of safe operation, for the equipment to protect the extensive use of the Internet of things "escort".

c. Deepen the civil-military cooperation and promote the rapid development of integration

Military intelligent construction can not be separated from the development of civil-military integration, equipment security IOT construction needs to make full use of local IOT technology resources, talent resources, to do military technology sharing, resource sharing, so that equipment security IOT in the rapid development of civil-military integration.

Military and civilian Internet of things technology integration, resource sharing. Internet of things technology is widely used, whether it is IOT network terminals, or network information technology, can be through the way of civil-military integration development, to achieve infrastructure sharing, sharing of key technologies, to reach the military hardware matching, software compatibility, improve the quality of construction of equipment security Internet of things. Based on the sharing of security resources of IOT technology, realize the sharing of information of military and local resources, incorporate the information of local security resources into the information base of equipment security resources, and realize the accurate docking between equipment security needs and local security resources.

Deepen military-civilian integration, adhere to the level of war coordination. Establish equipment security Internet of things, first of all, we should make full use of modern information technology such as national logistics network and cloud computing platform, strengthen the network terminal construction of equipment security system, integrate equipment resource information, establish efficient and smooth contact channels and operational communication mechanism between military and national warfare departments, unify the deployment of logistics equipment facilities and develop technical standards for equipment logistics, realize equipment security based on information sharing The military-civilian integration type development of real-time perception of needs and controlled security

ISSN: 2664-9640

activities, and effectively promote the change of military equipment security capacity generation mode. Secondly, we should adhere to the principle of level-war coordination, one is to build a dual development model to achieve peacetime service "market" and wartime security "battlefield"; the second is to attach great importance to the use of logistics network technology and cloud computing platform technology in equipment security training, and Establish "big data security concept", pay attention to the collection and accumulation of information data, for wartime accurate and "intelligent" prediction of security needs, the allocation of security resources to provide experience data and technical support, and comprehensively improve the equipment security level battle conversion capabilities.

4. Ending

With the development of military intelligence, equipment security Internet of things has become an important part of the field of equipment security intelligence, is a solid foundation for the realization of intelligent equipment security. Accelerate the construction of equipment security Internet of things, can constantly improve the overall equipment security capacity of the troops, to provide a strong equipment support for combat victory.

References

[1] Peng Pei,Xing Jian-liang. Application of Internet of things technology in equipment security[J]. Naval Equipment Maintenance,2019.02.
[2] Ma Liang-li,Wu Qing-yi. Internet of things machine military applications [M]. Beijing:National Defense Industry Press,2016.05.
[3] Lan Shi-bin,Xia Wen-xiang. Reflections on countermeasures to promote the construction of military Internet of things system[N],Journal of Internet of Things,2018.02
[4] Liu Tie-lin. Research on equipment security innovation based on the nature of activities [M]. Beijing:PLA Press,2016.04.
[5] Liu Tie-lin. Equipment security force generation model under the conditions of informationization [M]. Beijing:PLA Publishing House,2017.