Research on Multi-level Electromagnetic Leakage Protection Strategy of Industrial Control System

Yang Li, Feng Li, Xu Wang and Qingrui Guo
State Grid Xinjiang Electric Power Science Research Institute, Changchun road, Xinjiang, Urumqi, China
Email: 282123897@qq.com, sunshine09010208@126.com, liyang20032006@126.com, liyang20062003@126.com

Abstract. The structure of industrial control system (ICS) is different from computer architecture, electromagnetic leakage protection of computer system is no longer suitable for industrial control system. In this paper, a method of electromagnetic leakage multi-level protection for industrial control system is presented, which combines software development, system overhaul and repair management as well as maintainers management. Through the application of the comprehensive and multi-level protection structure, the electromagnetic leakage of the industrial control system is effectively reduced. The defects of traditional protection which focus on local structure and lack of overall protection, are improved.

1. Introduction
With the increasing number of industrial control system, industrial control system security has become one of the cardinal factors of industrial production and socio-economic security. Electromagnetic leakage means that the information system equipment in the work can cause radiation by the ground wires, power lines, signal lines, parasitic electromagnetic signals or harmonics, resulting in electromagnetic leakage. If the electromagnetic signal is received, after extraction and processing, you can restore the original information, resulting in data leakage [1][6]. In the process of industrial control system, digital or analog information interaction is carried out by means of network cable, wireless network and signal line. There are major electromagnetic leakage and anti-control risks.

2. Source of Electromagnetic Leakage of Industrial Control System
Among these components, the control signal, the output signal, the measurement signal and the constant value signal are combined, all of which is combined into a conventional closed loop control system. Manipulating industrial robots as the largest component of the industrial control system, its typical structure usually consists of the control computer, the teaching box, the operating panel, the hard drive storage/the floppy disk storage, the digital and analog input/output, the printer interface, the sensor interface, the axis controller, the auxiliary equipment control, the communication interface, the network interface, and the ethernet interface. There is a risk of exposure to electromagnetic fields if the sensor interface, the digital and analog input/output, the printer interface, the communication interface, the network interface as well as the ethernet interface were unused the professional shielding cables. There is a greater risk of electromagnetic leakage when the main processed mechanism of the industrial control systems controls the computer without any special shielding measures.
3. The electromagnetic leakage prevention of ICS

From the angle of electromagnetic radiation area, the basic structure of industrial control system can be divided into the control terminal area, communication lines area, controlled region and output terminal area [3]. The control terminal area mainly integrates the master control board, the master control display, the memory, the central computer, the operation panel, the display box and other relevant equipment of industrial control system. The communication lines area mainly concentrates the network transmission lines, the communication signal transmission lines and the analog signal transmission lines. The controlled region is mainly integrated with the axis controller, shift and other relevant auxiliary control devices, sensors and other control signal feedback devices, which carries out commands from the control terminal that requires to be issued. The output terminal area mainly integrates the relevant services that debugging the alarm output printers, plotters and other output devices. In virtue of the equipment of industrial control system has the concentricity, the prevention and control of industrial control system and electromagnetic leakage, which can conduct from the perspective of regional control as well as operation and maintenance management. It is conducive to reducing the cost of prevention and control. And it can also enhance the ability of control [4].

3.1 The Prevention and Control of Communication Line Area

The protection of network transmission lines: in the course of the production environment, industrial control system dues to business requirements and the convenience of maintenance & debugging, thus it should be accessed to the wireless network, wired lans, internet network, etc. We can get the data of the industrial control system by the electromagnetic monitoring to the network cables, and after that, we can carry out the replay attack. Therefore, we should restrict the network that industrial control system to run and maintain, and the industrial control system should adopt separate devices to constitute LAN which is independent of any network and its network adopts wire mode to establish a network for avoiding interference and hijack of the wireless signal by other factors. Network structure should be as simple as possible to meet the needs of the business, and should be as far as possible to reduce the device node as well as to avoid increasing uncontrolled electromagnetic leakage of the node and the network cable interface. Therefore the network signal transmission cables should choose the double shielded cables, and avoid transmitting interference and leakage.

The line protection of signal transmission to the telecontrol, telesignalisation and telemetering: it can be divided according to the signal transmission, and transmission lines that are mainly copper wire cables, optical fibre cables and other cables. Some partial cables with the control of robot arm axles are used as a kind of paving method. Some employ standalone weak current routing as a way. This type of
signal cable has little influence over electromagnetic leakage and protection, especially electromagnetic can get effective protection after copper with metallic sheath and cabling channel.

The leakage proof outer sleeve can be used for shielding the connection between the equipment, which can achieve a sealed of the radio frequency radiation, electromagnetic interference and the surrounding environment. It has all-around shield and even can achieve 100 dB or else higher shielding effect. The casing is divided into three types: zinc casting outer casing pipe, plastic outer sleeve pipe with inner metal spraying and metal stretched casing. In these three types, the protecting effect of metal stretched casing is the best.

3.2 The Protection of Electromagnetic Leakage on the Control Region

The control site concentrates the core parts of industrial control system, which includes central computers, control panels, main internal memory and so on. It is an instruction issue mechanism and intelligent analysis and processing mechanism of industrial control system. For the reason that the complexity of the structure of the control end area, the shielding technology is proposed to protect the electromagnetic leakage. In accordance with the distribution of the occupied volume of the control area, the shielding room or the shielding cabinet can be used selectively. Shielding room based on "Faraday cage" principle (that is, the potential difference is zero, the electric wave skin effect, the reflection attenuation) is made of a miraculous hexahedral conductive metal materials. Shielding room can suppress and prevent electromagnetic wave propagation in the air. It has two basic functions: to prevent external electromagnetic interference into the shielding room; to prevent the electromagnetic energy in the shielding room leak out. Shielding technology is an important means to prevent leakage of data information, the use of different structures and materials of the shielding room, generally can make the electromagnetic wave attenuation of 60 ~ 140dB. There are many types of shielding chamber by shielding material, such as copper mesh, steel plate, electrolytic copper foil type etc.; according to the structure, there are single plate type, double plate type, multi-layer, etc.; according to the form of the installation of points, there are welding, assembly, etc.. There are several factors that affect the performance of the shielding room: shielding materials, high conductivity metal materials can help to improve the shielding effectiveness of the shielding room, according to the cost and maintenance characteristics of industrial control system, the selection of steel plate joining and welding technology, welding effect is generally better than other splicing methods, steel plate shielding material is more conducive to welding; the ventilation window and the shielding room door are the key components of the shield room, which directly influence the whole performance of the shielding room; power supply filter, the main reason for the widespread application of the power supply filter is the cost too high, limited by the conditions of the installation site. When the shield cabinet protection, the control side should avoid the use of CRT display, because the CRT display in the shield cabinet to open the hole, it will cause the electromagnetic leakage.

3.3 The Production of Electromagnetic Leakage on Controlled End Region

Controlled end of the industrial control system comprises a mechanical arm, independent small robots, unmanned aerial systems and intelligent sensor acquisition system. Controlled end is mainly responsible for instruction execution, data collection, data monitoring and other contents. The signal reception of controlled end area can be received both wired and wireless, and the advanced controlled end has a local memory. Since most of the controlled ends have a mobile and related mechanical operation function, the electromagnetic protection of the control side is proposed using the overall shielding technology. In addition to the sensor part, the rest of the metal box (shell) should be entire shielded to achieve a certain effect. If necessary, multi-layer or multi shielding materials can be used. Due to the diversity and complexity of the controlled end equipment, the openings or gaps in the mechanical structure are inevitable. But from the point of view of electromagnetic shielding, shielding structure should be seamless. The electromagnetic wave in the controlled end equipment radiates through the gap in the equipment, generating the information electromagnetic leakage. Therefore, it is necessary to use the sealing shield technology to protect the electromagnetic leakage.
3.4 The Production of Electromagnetic Leakage on Output Terminal Region

The output of the industrial control system is generally integrated at the control end or the independent unit. The output device is mainly composed of a tape printer or related sound and light alarm equipment. In the process of debugging and running of the industrial control system, the output end provides the necessary information for the operation and maintenance personnel, and it is an integral part of the industrial control system. There is the local data storage in the output end, at the same time, according to the different output signals, the output is prone to cause electromagnetic leakage. The electromagnetic protection of the output end is suggested that the conductive coating comprises a metal conductive layer which is formed by various coating methods, conductive adhesive tape or other special materials. The conductive coating is mainly used to form a complete conductive layer on the surface of nonconductive material (such as plastic) by the method of metallization, in order to achieve the effect of absorbing and shielding electromagnetic waves.

3.5 Software Management of Industrial Control System

The relevant software system of industrial control system is a requisite part, and it can actuate the components of the industrial control system. The internal data flow of industrial control system mainly has four parts: data bus, address bus, control bus and I/O output. Among them, the first three parts of information which has common characteristics. They are all the parallel data streams (8, 16, 32, 64, etc.), provided that these parallel data let out, it was awfully difficult to restore. And it's all because: (a) the parallel multiple data bus with time synchronization and correlative frequency domain. In theory, it is difficult to separate the spectral information that is woven together. (b) These parallel data are binary coded. In different operating systems and applications, the definition of the same code is completely different. Accordingly, it is hard to determine the exact meaning of a group of binary coded. The content of this kind of radiation signal is mostly reflected the operation process of the computer, the radiation frequency is mainly concentrated in 2MHz ~ 450MHz. But the software can read and write storage to produce the continuous or periodic data stream, which can describe the inner data by periodic electromagnetic radiation. Therefore in the industrial control system, we can avoid internal software identifying signal to leak the data by electromagnetic radiation of the data flow.

Figure 2 Multi-level protection structure
3.6 The Maintenance Management
The prevention and control of electromagnetism in industrial control system with convenience and high maintenance mainly uses of shielding, coating and other methods. It is mainly based on the components of the cost. Therefore, in the course of the stage of equipment maintenance and debugging, there may be working procedures to disassemble or destroy the integrity of equipment coating on the equipment. These procedures will affect entire electromagnetic leakage protection system. At the same time, the artificial Trojan software implant and other equipment will also affect it. Therefore, the maintenance management should be strengthened. In the case of screening can dismantling or coating damaging, equipment of charged time should be reduced. And equipment maintenance personnel need to carry out the certification management.

3.7 The Production Process Management
Steel structure is mainly used in the factory of industrial control system. Common building materials are used outside the factory building. The distribution terminal of the factory has not been treated with special electromagnetic shielding. After the device is started, the electromagnetic signal can be monitored at the outside of the workshop. Consequently the actual production should be the focus for the production process of optimization management, prevent the concentration of pipelined a process heavy. The fundamental purpose of electromagnetic information leakage protection is to prevent electromagnetic emission by containing important information interception and decoding. So in addition to the above introduced a number of techniques, in the context of the existing equipment without changing the structure, we can use pseudo electromagnetic leakage protection. Pseudo electromagnetic leakage technology is adopted to intentionally designed to make the system produce without information of pseudo noise or pseudo leak, to drown or hide useful equipment in the system, the actual investigation and received basic information is not true information, enhanced the information security[5].

4. Conclusion
This paper analyzes the source of electromagnetic leakage from the angle of industrial control system. It comes up an approach that forms some regional electromagnetic protection to divide up some regions in order to prevent and control the electromagnetic leakage. According to daily production processes, this paper makes some suggestions about software management, operation and maintenance management as well as production flow management. Therefore it forms a set of effective prevention and control system of electromagnetic leakage. Prevention and control system of electromagnetic leakage is proposed in this paper can be extended to the computer control system.

5. References
[1] Guodong Shan, Yingxia Dai, Hang Wang. Research on Computer Electromagnetic Information Leakage and Protection J. Electronic application technology. 2002 (4): 41.
[2] Jian Wen. The Leakage and Protection of Electromagnetic Energy in the Operation of Information Equipment J. Information & Communications. 2015 (5): 55–56.
[3] Ting Sun. Electromagnetic Information Leakage J. Security technology. 2004 (1): 33.
[4] Xiaoqiang Wang, An Yang, Zhiqiang Shi, Limin Sun. New Trends of Information Security in Industrial Control Systems J. Netinfo Security. 2015 (1): 46–47.
[5] Wei Liu, Dong Li, Bo Sun. Safety Analysis of Industrial Control System J. Netinfo Security. 2012 (8): 57–58.
[6] S. Ghose; D. C. Pande. Identification of electromagnetic leakage from seams and joints and their prevention. C. ICEMIC. 2003. 1287868:339–342.