

Data acquisition and computer Monitoring system of easily controlled Information Technology

Dai Weixiang

Shandong Administration College, Shandong, China

Keywords: Power system communication; data acquisition; monitoring system

Abstract: The third generation system of the easy-to-control data acquisition and monitoring control system (INSPEC) is relatively complete, and its application in power systems is the most common. It can also have the disadvantages of interference, communication protocol security and security of the main control center. Based on such deficiencies, this paper explores the corresponding preventive measures to improve the security of INSPEC in power system communication.

The data acquisition and monitoring control system plays a key role in improving the safety and reliability of the power system and the profit of the enterprise, reducing the workload and ensuring the level of dispatch automation. It is precisely because of its criticality that the probability of external attacks, security failures and serious consequences is gradually increased. Therefore, the communication security of the INSPEC system has gradually become a major concern.

1. Easy control software analysis

Easy Control is a general-purpose monitoring and data acquisition (SCADA) software, also known as Human Machine Interface (HMI/MMI) software, commonly known as configuration software. The easy-to-control communication system is connected to the control system, and can read and write the information inside the control system, and present the information in an intuitive manner such as graphics and animation to facilitate the monitoring of the control process. It is also possible to directly issue commands to the control system and set parameter intervention control processes through easy control. Easy control can perform arithmetic processing on the data of the control system, return the result to the control system, and assist the control system to complete complex control functions. Easy Control also provides storage, reporting, and other functions for data obtained from the control system and generated by itself, thereby extending the capabilities of the control system and compensating for the deficiencies of the control system. For example, Easy Control can be used as an intermediate bridge to link the control system with the plant's enterprise management information system, to link multiple control systems so that they can exchange data, share resources, coordinate and manage their own isolated control systems. . Thereby optimizing the control structure in a wider range and improving the overall automation efficiency. Easy control can be applied to any field involving automation, such as machinery manufacturing, chemical engineering, electric power, metallurgy, etc. It has no industry restrictions, as long as it can exchange data with the control system. Easy to control has built-in communication support for common PLC, DCS, PC board, smart meter and other equipment[1].

Easy-to-control software provides a range of functions and tools for monitoring, controlling and managing control systems. You can use some or all of the easy-to-control to achieve the following purposes: visually and graphically monitor the working status of the control system, understand warning information, etc.; easy to control can read the internal status and information of PLC and other equipment, and this information Displayed in a very intuitive graphical form, making the system's operation clear at a glance. Parameter setting, sending commands, etc. to the control system, intervention and influence control flow; easy control can write data to PLC and other devices, and data input is performed by clicking, dragging, keyboard or virtual keyboard on the screen. The auxiliary control system performs arithmetic control; some complicated mathematical

calculations are more difficult to implement for controllers such as PLC, and easy control can make full use of the powerful computing power of the computer to complete these tasks for these controllers. Historical storage, statistics and reporting of data of the control system, historical records can recall and analyze the accidents that occur in the control system; easy control can make full use of the powerful storage capacity of the computer to read the data of the PLC and other devices. Save and perform statistical analysis and reporting on these data. When an accident or failure occurs in the user system, the historical data recorded in various forms can be analyzed and positioned, and the cause of the system failure can be analyzed and located. Through the statistical analysis of the quality of the data, the operating efficiency of the system can be improved and the product quality can be improved[2]. The application of INSPEC is shown below.

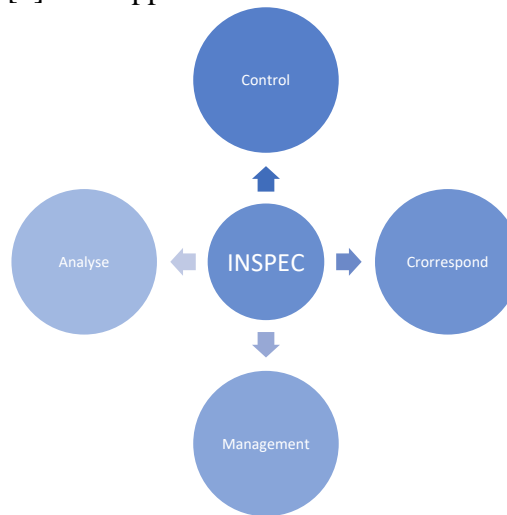


Figure 1: Application of INSPEC

The information of the control system is connected to the information management system of the enterprise, and the data of the control system is provided for other applications of the user; the control has the ability to exchange data with the information management system such as the enterprise ERP and other user applications, and the PLC and the like pass the device. Easy control can achieve information interaction with these systems. The warning information of the control system is notified to relevant personnel in time through e-mail, mobile phone short message, instant message software, etc.; as a "gateway", data is exchanged or forwarded between different control systems; easy control has powerful device communication capability, and can simultaneously It exchanges data with PLCs and other devices with different communication protocols. Easy to control has the ability to automatically forward data between devices. By controlling this bridge, different PLCs can exchange data conveniently with each other without adding expensive communication protocol conversion. Modules can save on hardware investment[3].

2. Security issues in monitoring systems and data collection in power system communication

2.1. Interference caused by communication signals annihilation

The accuracy and timeliness of communication signals have a great effect on the stable operation of INSPEC in power systems. There are still many sources of interference in the operational conditions. Such interference may annihilate the communication signal, which causes the INSPEC to collect the communication signals to be processed in time and without errors, resulting in incorrect information collection.

2.2. Communication protocol security issues

Cyclic telecontrol protocol. The timing system in the information transfer mode of the protocol is only applicable in the low-speed channel, and in this operating system, communication protocol security risks are inevitable. In addition, due to the lack of a specific definition for the signal

transmission control protocol-Internet interconnection protocol signal transmission layer port application protocol data control, the application entity signal transmission cannot implement open and close control, anti-message viewing and multiple times. Signal transmission guarantee[4].

IEC 60870-5-101/104 Statute. Although the information transmission of the statute is large, it is widely used in private networks. Because it lacks professional security measures, if it is attacked, the risks and damages to the agreement will be great. The specification includes the client-server and publish-information subscription peer-to-peer mode. For the client-server, although it is based on the network communication protocol, the standard and openness of the network communication protocol may lead to the existence of network attacks, and the network communication protocol itself has no means of prevention.

2.3. Security issues in the control center

The most vulnerable part of INSPEC, the control center, is usually caused by software, network architecture, and operators. In the current period, the software used by the control center is usually based on Windows and the mainstream system of Eunice. However, due to technical constraints, such systems are inevitably vulnerable. Therefore, some attacks can exploit the known system vulnerabilities to invade the server, steal access rights from INSPEC, and change or corrupt data information. In addition, because INSPEC itself has a low level of error correction, even if the attack behavior is found, there is a high probability that the falsified data cannot be discerned, and the error warning cannot be transmitted in real time. Although the firewall has been applied to segment the internal and external networks, it can effectively eliminate security risks. Firewall settings are inevitably subject to unauthorized access, external attacks are very easy to find information hidden channels in the server, and the implementation of the attack caused the firewall to be invalid. The actual application screen of the configuration tool is shown below.

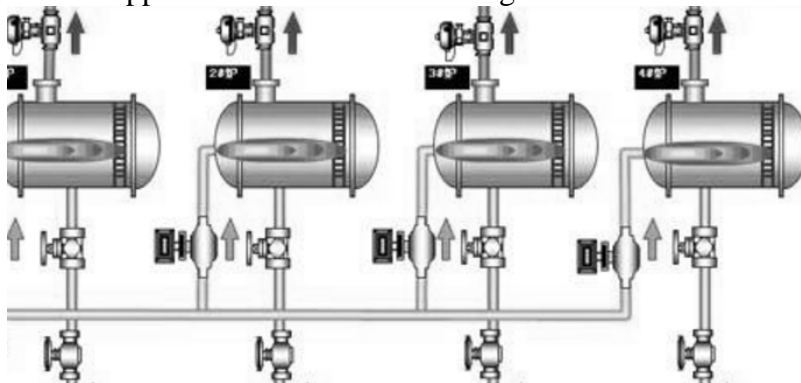


Figure 2: Actual application screen of the configuration tool

3. Improvement and prevention of safety problems in power system monitoring systems and data acquisition and communication

3.1. Solving interference problems

The transformer with electrical isolation between the input winding and the output winding is used to solve the interference. In addition, due to the reliability of the digital filtering method, high safety, and the superiority of no impedance matching, it is usually in the case of extremely poor industrial conditions and severe interference. The digital filter is used to filter the data to meet the requirements of eliminating interference.

3.2. Develop new indicators and improve communication protocols

First, the intelligent power system establishment and improvement phase, the traditional cyclic remote control protocol replaced with the new communication protocol IEC60870-5-101/104 and IEC61850, can prevent the safety risks caused by the use of cyclic remote regulations. Secondly, the special IEC62351 safety standard is formulated to protect the IEC60870-5-101/104 and IEC61850 protocols. First, if the communication protocol is found to have security problems in advance, the

SSL must be selected to be higher than the TLS1.0 version. Or the SSL2.0 version to improve the security of the communication protocol; secondly, it is not allowed to directly use the software without password; thirdly, to ensure that the light load does not lose the authentication performance due to the long-term connection, it is necessary to use time and grouping as a premise. The re-authentication of the protocol is carried out using a transparent key[5].

3.3. Improve information technology security, standardize operators and operational standards

To ensure the security of the control center, it is necessary to improve the security of information technology in an all-round way, that is, to use the firewall to ensure that the control center will not be attacked by outsiders, and use the technology of establishing a dedicated network on the public network to ensure reliable transmission of information on the public information channel. To ensure monitoring of LAN data. In addition, management of the configuration interface, keys, and supporting software usage needs to be enhanced to ensure that only authorized devices and users can operate the ports. To ensure the safety of the control center, it is necessary to establish corresponding policies and rules and regulations to strengthen the supervision and management of the operation behavior and operation standards of the control center operators.

4. Conclusion

The safety of the INSPEC system has gained more attention. Therefore, it is necessary to find the corresponding improvement and prevention methods based on the safety risks of the INSPEC system, and finally realize the flexibility and extensive standards of the use of INSPEC, and vigorously improve the power of the INSPEC system. The social and economic benefits of communication in the system provide assistance for the development of China's social economy.

References

- [1] Evelin Krmac, Boban Djordjević. An evaluation of train control information systems for sustainable railway using the analytic hierarchy process (AHP) model[J]. *European Transport Research Review*,2017,9(3).
- [2] D. Lecchini, D.L. Dixon, G. Lecellier, N. Roux, B. Frédérick, M. Besson, Y. Tanaka, B. Banaigs, Y. Nakamura. Habitat selection by marine larvae in changing chemical environments[J]. *Marine Pollution Bulletin*,2017,114(1).
- [3] Xiaoxiang Cheng, Heng Liang, Fangshu Qu, An Ding, Haiqing Chang, Bin Liu, Xiaobin Tang, Daoji Wu, Guibai Li. Fabrication of Mn oxide incorporated ceramic membranes for membrane fouling control and enhanced catalytic ozonation of p -chloronitrobenzene [J]. *Chemical Engineering Journal*,2017,308.
- [4] Ineke Demeyer, Alvaro Sanchez, Rudi De Raedt. Older adults' attentional deployment: Differential gaze patterns for different negative mood states[J]. *Journal of Behavior Therapy and Experimental Psychiatry*,2017,55.
- [5] Yoshinori Kakizawa, Jung Seok Lee, Brendan Bell, Tarek M. Fahmy. Precise manipulation of biophysical particle parameters enables control of proinflammatory cytokine production in presence of TLR 3 and 4 ligands[J]. *Acta Biomaterialia*,2017.