Industrial Network Isolation Technology and Products

Based on the Photo Data Transfer Principle

Jian Wang

OptimiPro Control Technology Co., Ltd.

Keywords: industrial network security, network isolation, photo data transfer, WannaCry virus, DCS security, database, data acquisition network.

Abstract: This article introduces an industrial network isolation technology based on the photo data transfer principle. By utilizing a non-networked data transmission system, it effectively blocks and isolates existing and future network-based viruses and hacker attacks. After decades of research and development, this technology has evolved into multiple product lines and dozens of products, which have been deployed in large-scale industrial networks for a long time, demonstrating stable and reliable operation. During the recent "WannaCry" virus attack, this technology successfully blocked the attack, maintaining the DCS and production equipment within the isolated protection zone intact.

1. Overview

Currently, computers (DCS, distributed control systems) are widely used to control production processes in industry. In most factories, these DCS systems are connected to the factory's real-time database and office network, as shown in Figure 1.1. Hundreds or even thousands of computers are connected to the network link to the DCS. If a virus is infected on one of these computers, it could potentially be transmitted to the DCS through the computer network.

Preventing viruses and hackers from attacking industrial control computer systems through data acquisition networks is a typical perimeter protection issue. Traditionally, this is achieved through the use of antivirus software, industrial gateways, and network gatekeepers.

Some current network attack techniques can already circumvent these protective measures.

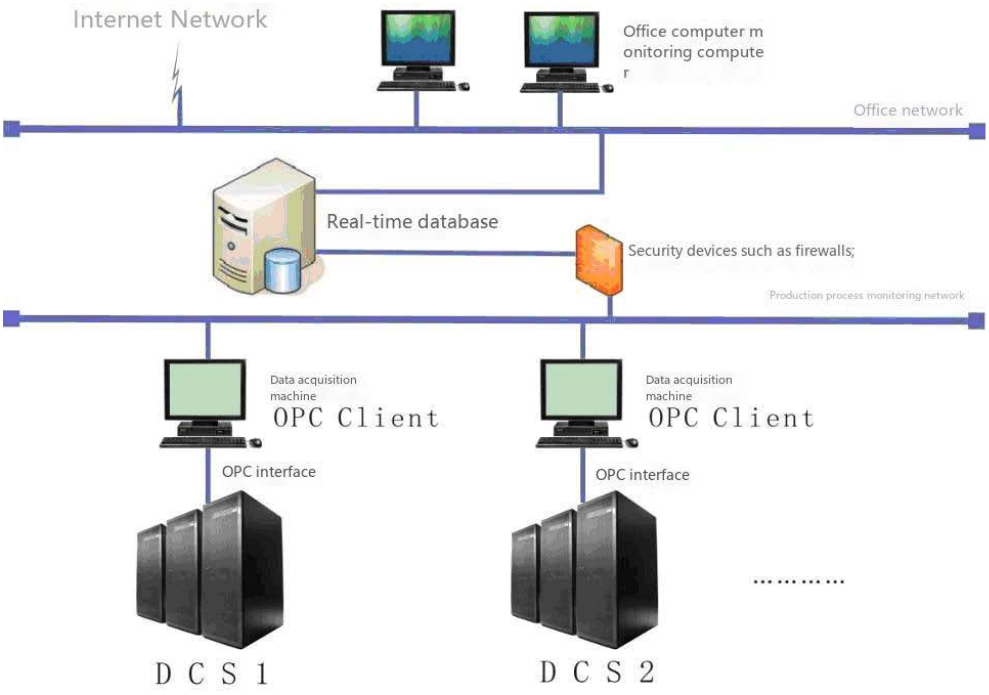

Figure 1.1 Conventional Data Acquisition System

This conventional data acquisition system presents the following network security issues:

1. A significant issue with this data acquisition and monitoring system is the physical connection between the process control computer and the local area network.
2. This data acquisition and monitoring system exposes the process control computer to viruses or hacker attacks from the office management network.
3. Despite the availability of both hardware and software antivirus software and firewalls, absolute security for the process control computer cannot be guaranteed and can lead to unpredictable consequences.

2. Photo Data Transfer

The reason a DCS can be infected with viruses is that it maintains a physical network connection with the real-time database and office system, which transmits data from production equipment. If this network is disconnected, the DCS will not be infected by viruses. However, this also prevents the real-time database from accessing production data. Is there a way to transmit DCS production data to the real-time database without using a computer digital network? If this were possible, it would completely eliminate the transmission pathways for computer viruses and hackers, essentially ensuring the security of the DCS.

After more than a decade of research and development, and with significant investment in both manpower and resources, OptimiPro Control Technology Co., Ltd. ultimately developed "photo data transfer technology," enabling the transmission of DCS data to a real-time database without a digital network connection. This technology has also been commercialized. In 2009, this technology was granted a People's Republic of China invention patent (patent number: ZL200610064971.8). Due to its novelty, patent applications are currently underway in over 40 countries, with some already granted, as shown in Table 2.11.

In 2015, this technology also won the "2015 China Industrial Control Network Security Best Solution Award" and the "2015 China Industrial Control Network Security Innovation Enterprise Award" from the China Academy of Information and Communications Technology Development of the Ministry of Industry and Information Technology.

Table 2.1: Domestic and International Patents for photo data transfer Technology

	Patent Number

People's Republic of China	ZL 2006 1 0064971.8
People's Republic of China	ZL 2007 8 0018261.4
United States	US 8,341,741 B2
Canada	2,645,722
Europe	2003815
Russia	2426248
South Korea	10-1146184
Japan	4971420

2.1 Principle of Photo Data Transfer

So, how can data be transmitted without a digital network? Figures 2.1 and 2.2 show the basic principles of photo data transfer.

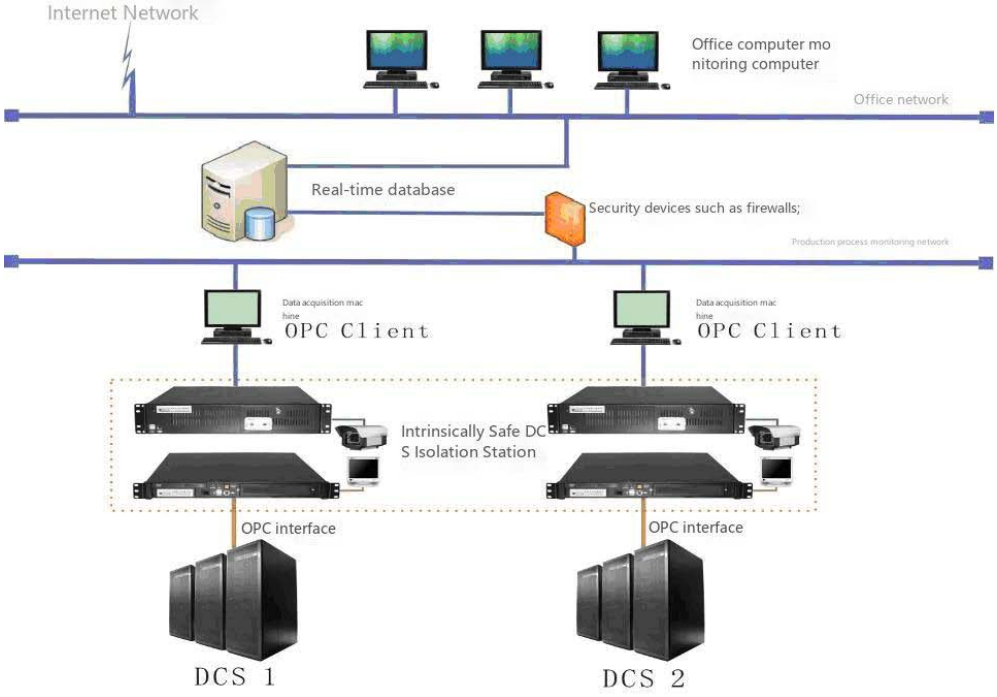

Figure 2.1 Intrinsically Safe DCS Isolation Station Network Structure Diagram

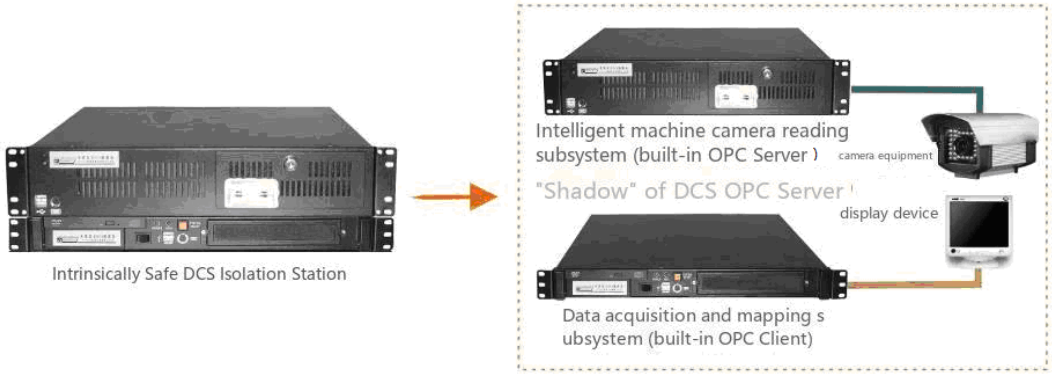

Figure 2.2 Intrinsically Safe DCS Isolation Station Network Structure Diagram

As shown in the diagram, the data to be uploaded by the DCS is collected by a dedicated data acquisition computer and displayed on the computer screen. A camera system also automatically captures the real-time data displayed on the screen at regular intervals. The captured data in graphic format is automatically interpreted by an intelligent machine reading system to obtain the data to be uploaded, which is then sent to the real-time database and office network via the local area network. This eliminates any physical connection between the local area network and the DCS, making it impossible for viruses and hackers to infiltrate the DCS through the network. This inherently ensures the security of the DCS, regardless of how the virus evolves.

Currently, OptimiPro Control Technology Co., Ltd. applies this principle to integrate a data acquisition computer, display, photographic system, and intelligent machine reading system, resulting in a commercially available intrinsically safe DCS isolation station. This station has been operating stably for a long time in multiple DCS systems, as shown in Figure 2.3.

Figure 2.3 Intrinsically Safe DCS Isolation Station Group

3. Product Series Based on Photo Data Transfer Technology

Based on the patented photo data transfer technology, we have developed a series of commercial products. See Figure 3.1 for an overview. The figure shows the specific products and their locations within the network.

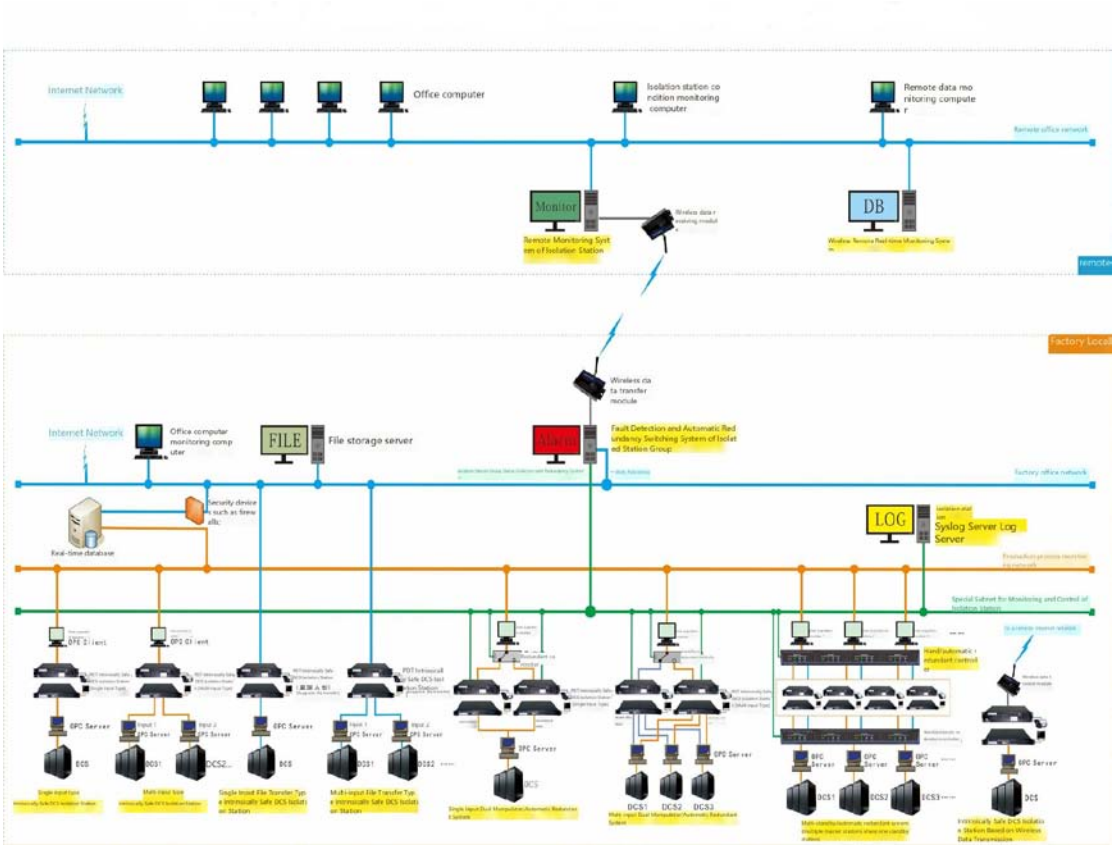

Figure 3.1 Overview of Industrial Network Security Products Based on Patented Data Photography Technology (Yellow Label)

3.1 Intrinsically Safe DCS Isolation Station Series

1. PDT Single-Input Intrinsically Safe DCS Isolation Station
This product provides an input interface and an output interface. The input interface can connect to an OPC server on the DCS side to upload data. After passing through the photo data transfer, this data enters the isolation station's built-in OPC server. External OPC clients connect to the built-in OPC server through the isolation station's output interface to retrieve data.

2. PDT Multiple-Input Intrinsically Safe DCS Isolation Station
This product provides multiple input and output interfaces, each of which can connect to the corresponding DCS OPC server. This allows a multi-input isolation station to connect to multiple DCS OPC servers to collect and upload data. After one-way graphic transmission of data, it enters the isolation station's built-in OPC servers and is output via multiple output interfaces in an OPC format.

3. PDT Single-Input File Transfer Intrinsically Safe DCS Isolation Station
This product has one input and one output. The input allows for the input of files to be transferred. Files are then transferred unidirectionally using a photographic systme, and then pushed out through the output. This isolation station can be used not only for unidirectional file transfer from the DCS to the outside, but can also be used in any application requiring unidirectional file push.

4. PDT Multiple-Input File Transfer Intrinsically Safe DCS Isolation Station
This product has multiple inputs and multiple outputs. Each input port can receive its own file for transmission. After one-way transmission using a photographic system, it is then sent out through one or more output ports. This isolation station can be used not only for one-way file transmission from the DCS end, but also for any application requiring one-way file push.

5. Isolation Station Group Fault Detection, Alarm, and Automatic Redundancy Switchover System
The system can automatically detect the working status and health status of each DCS isolation station. If any problem is found, it will automatically sound and light alarms and send short messages to designated

mobile phones. The automatic redundancy switching system will send instructions to the manual/automatic redundancy controller to cut out the faulty DCS isolation station and switch the isolation system to the preset backup plan.

6. Manual-Automatic Redundancy Controller
This manual-automatic controller receives instructions from the isolation station group fault detection, alarm, and automatic redundancy switchover system to switch the always-on master station to the backup station, or vice versa. It can also manually force a master-backup switchover. Additionally, it can implement manual-automatic switching for isolation solutions.

7. Single-Input Dual-Machine Manual-Automatic Redundancy System
This system consists of a always-on master isolation station, a backup isolation station, and a redundant controller. When a master station fails, the redundant controller automatically switches to the backup station. If the master station returns to normal operation, it automatically switches from standby to master. The master-standby station can also be manually forced to switch.

8. Multiple-Standby Automatic Redundancy System
This system consists of multiple master isolation stations and one backup isolation station. Multiple master stations share one backup isolation station. When one of the master stations fails, it automatically switches to the backup station. Since multiple master stations share one backup station, the reliability of the isolation system is greatly improved and redundancy costs are significantly reduced.

9. Isolation Station Log Server
The behavior of each isolation station in the isolation station group can be logged for security audits.

10. Remote Monitoring System for Isolation Station Operation Status. This system uses wireless data transmission components for remote information transmission, centrally displaying and monitoring the operating status of isolation stations located in various branches across the country. It is particularly suitable for the isolation management of large, geographically dispersed industrial networks.

11. PDT Wireless Transmission Intrinsically Safe DCS Isolation Station
After the station collects the uploaded data, it uses a photographic method to transmit the data in a one-way isolated manner. The data is then transmitted to a remote wireless real-time monitoring system via a mobile phone network. The station is equipped with a local intelligent diagnosis and repair system, which has high reliability and can be operated unmanned.

12. Wireless remote real-time monitoring system
The system has a built-in real-time database that receives real-time DCS data from the wireless transmission system's intrinsically safe DCS isolation stations and performs health status monitoring, data management, and analysis for multiple remote stations located in different locations.

4. Application Samples

Intrinsically safe DCS isolation stations have been used in many large enterprises since 2007. Currently, over 100 units are in operation on-site, with the longest-standing service life exceeding 10 years, demonstrating their proven long-term performance. We will use two large industrial enterprises of Sinopec as examples to illustrate their application in these enterprises.

4.1 Whole-Plant DCS Safety Isolation System of a Sinopec’s refinery

Sample 1 is a large-scale refinery with an annual processing capacity of 10 million tons. It has 19 old units and a newly built large refinery complex unit. After optimizing the design, only ten intrinsically safe DCS isolation stations are needed to provide the most thorough network security protection for the entire plant's production process control network, as shown in Figure 5.1.

1. The newly built large-scale refinery-related equipment has approximately 20,000 tags. The maximum processing capacity of a single intrinsically safe DCS isolation station is 6,000 tags. Considering the possibility of adding tags in the future, providing them with five isolation stations will meet the demand.

2. The 19 existing equipment sets have a total of approximately 24,000 tags. Considering that some equipment sets have only dozens or hundreds of tags, a comprehensive analysis from the perspectives of feasibility, safety, and economy has determined that providing them with four multi-input and two single-input intrinsically safe DCS isolation stations will meet the actual needs.

3. The new and existing equipment in the entire plant has a total of approximately 44,000 tags. A total of ten intrinsically safe DCS isolation stations are required to complete the isolation. The project will be carried out in two phases: seven isolation stations in the first phase and three isolation stations in the second phase.

4. Equipped with a DCS isolation station monitoring system, it can detect the various working conditions and health status of the isolation stations in real time.

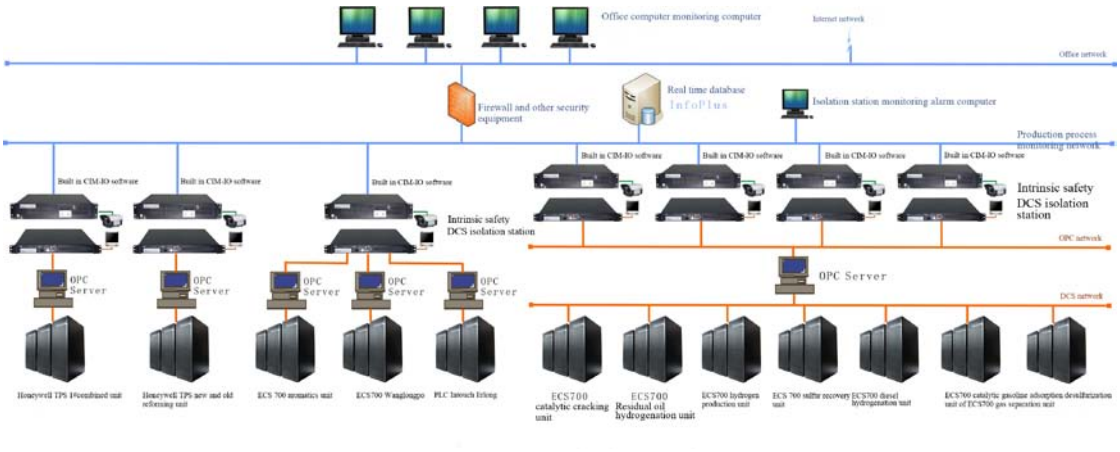

Figure 4.1 Configuration structure diagram of the intrinsically safe DCS isolation station of a Sinopec refinery (partial)

Since its commissioning in August 2012, the DCS safety isolation system has been operating smoothly and stably, earning high praise from all applicable departments.

(1) The safety isolation systems of each real-time database operate normally;

(2) The collected and isolated data are complete and accurate;

(3) Equipped with a specially designed DCS isolation station monitoring system. Users can view the health status of the system operation of each isolation station, record various events that occur in the isolation station, and publish important events through text messages;

(4) The system responds quickly, the system recovery time is short, and the impact on system application is small.

The system passed the test acceptance of Sinopec in October 2013.

4.2 Application Sample 2 of the Intrinsically Safe Isolation Station in a Chemical Plant

The intrinsically safe DCS isolation project of a chemical plant was contracted in January 2015 and put into operation in September 2015.

In this project, the plant adopted OptimiPro Control Technology Co., Ltd.'s patented photo data transfer technology and used 8 sets of PDT4000 intrinsically safe DCS isolation stations to isolate 8 key units: synthetic ammonia unit, oxygen and acetylene production unit, power, new and old VAE units, east-west circulation, PVA, power generation 124# and soft water. After using the isolation stations, the DCS data of these units can only be transmitted one-way to the plant-wide implementation database, and viruses and hackers on the external network cannot launch attacks on the DCS through the data acquisition network system, thereby ensuring production safety.

Innovations of the plant's intrinsically safe DCS isolation system project:

1. The latest PDT4000 series products were used in the project.

The PDT4000 series is the fourth generation of intrinsically safe DCS isolation stations. Compared to the third generation, it offers the following technological advancements:

- The tag list can be added and edited online. In the past, when adding or deleting the uploaded tag, the isolation station needed to be offline for a period of time, which would cause data transmission to be interrupted. Now, the tag of the uploaded data can be modified without interrupting data transmission.
- Volume reduced by 1/3.
- Energy consumption reduced by 2/3.
- Hardware redesigned and developed for higher reliability.

2. Adoption of new fully automatic redundancy technology with multiple backups greatly improves system reliability.

This project utilizes an innovative 1-for-8 automatic redundancy solution. If the system detects a problem of one isolation station, it automatically switches the isolation task to the backup station. Furthermore, if another primary station subsequently experiences a problem, as long as the faulty primary isolation station's transmission tag count does not exceed the backup station's maximum capacity, the isolation transmission task will automatically switch to the backup station. In other words, even if multiple primary stations experience problems simultaneously, they can still be switched to the backup station simultaneously.

This shows that the application of one-for-multiple backup system technology can achieve fully automatic redundancy across multiple systems with minimal additional investment in backup redundancy, significantly improving system reliability and ensuring the transmission of production data.

5. Successful Blocking of the "WannaCry" Virus by Intrinsically Safe DCS Isolation Station

The WannaCry virus, which broke out in May 2017, infected the production monitoring platform of an industrial enterprise's oil depot. The virus spread along the database's data acquisition network to the DCS and production equipment. Thanks to the pre-installed intrinsically safe DCS isolation station on the database's data acquisition channel, it provided timely protection, blocking the spread of the virus to the DCS system, protecting the industrial control system, and ensuring normal production.

Figure 5.1 is a topology diagram of the oil depot's production monitoring platform:

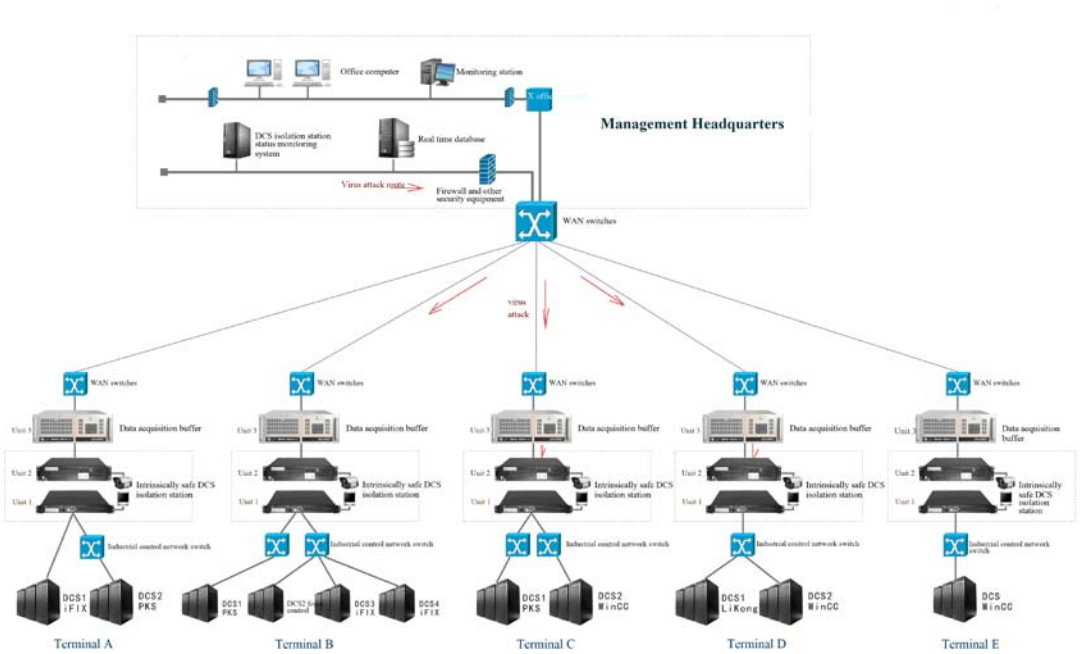

Figure 5.1 Topology diagram of a certain enterprise's oil depot production monitoring platform

In the topology diagram above, the device connecting the data acquisition buffer (unit 3) and the industrial control network switch is an intrinsically safe DCS isolation station. It consists of two devices: the data acquisition and mapping subsystem (unit 1) and the automatic photographic and intelligent reading subsystem (unit 2). Unit 2 is connected to unit 3, and unit 1 is connected to the industrial control network switch. The isolation device's mission is to protect the DCS system from viruses and hacker attacks on the upper network while ensuring real-time transmission of production data from the DCS system to the upper database.

After the WannaCry worm outbreak, the monitoring platform was attacked by the virus. The process was as follows:

1. A virus infected the real-time database server at the management headquarters.
2. The virus spread to oil depots in various places through the dedicated network, and was transmitted to the data acquisition computer through the switch, causing the data acquisition buffer computer (No. 3) at the oil depots B, C, and D to be infected.
3. The virus from the three locations mentioned above continued to penetrate downward through the network, reaching the intrinsically safe DCS isolation stations and infecting Unit 2 of the isolation stations at locations C and D.
4. Due to the one-way transmission feature of photographic data in the intrinsically safe DCS isolation station, the virus on machine 2 cannot continue to spread to machine 1, blocking the downward spread of the virus and thus protecting the DCS system below.

This shows that in this virus attack, it was blocked by the intrinsically safe DCS isolation station, protecting the industrial production equipment within the protected area.

6. Conclusion

The intrinsically safe DCS isolation station based on photo data transfer technology has the following features:

- Completely one-way data transmission cuts off the attack channel from the external network to the DCS, which can prevent existing and future network-based viruses and hacker attacks.
- Forward data transmission adopts a non-network method and has no digital network transmission channel, which can prevent network spyware in the DCS intranet from transmitting intelligence to the outside and resist network viruses or hackers from launching attacks from the intranet to the database end;
- It has an industrial standard OPC interface, which is convenient for users.
- It can be used with multiple DCS systems, reducing user isolation costs.
- Having an isolation station group fault detection and alarm system can greatly simplify management for large enterprises.
- Multiple primary isolation stations can share a single backup isolation station, enabling fully automatic switching, significantly improving the reliability of the isolation system and reducing redundancy costs.
- After long-term (more than ten years) use in large petrochemical enterprises, the system has proven stable and reliable operation.