MOXA®

CONNECT THE DOTS

BY MASTERING FOUR OT DATA CAPABILITIES

2

www.moxa.com

Starting Your Digital Journey - From Zero to One Is Hard

Industrial digital transformation (Industrial DX) first emerged as a business strategy during a discussion about Industry 4.0 in Germany in 2013. Since then, it has become an important indicator of industrial development for countries across Europe, the Asia-Pacific region, and the U.S. However, the German National Academy of Science and Engineering, Acatech, recently classified the more than 90% of companies that have declared themselves as adoptees of this trend only as “Beginners” in its 2020 Industry 4.0 Maturity Survey[(1)]. This classification clearly indicates that most companies are still stuck in the preliminary stage of simply digitally recording the status of their equipment, systems, and personnel information, and passing the data between a variety of systems. So there is still a long way to go to reach the expected goals of Industrial DX. These goals include reduced costs, increased efficiency, and finding innovative business models through the collection and analysis of big data.

Then, why is there a discrepancy between these expectations and the actual reality? As often mentioned, big data analysis, artificial intelligence, and other disruptive innovations pertain mostly to what is to come in the latter stages of Industrial DX, instead of the early stages. What is mostly needed for such high-caliber analysis to work is a large amount of diversified and high-quality data. In other words, data is the crucial foundation to ensure that artificial intelligence (AI) or machine learning (ML) technology can exert its expected value. Thus, to start your Industrial DX journey, you first need to connect your operational data (OT data).

[(1)] Using the Industrie 4.0 Maturity Index in Industry, Acatech, 2020.

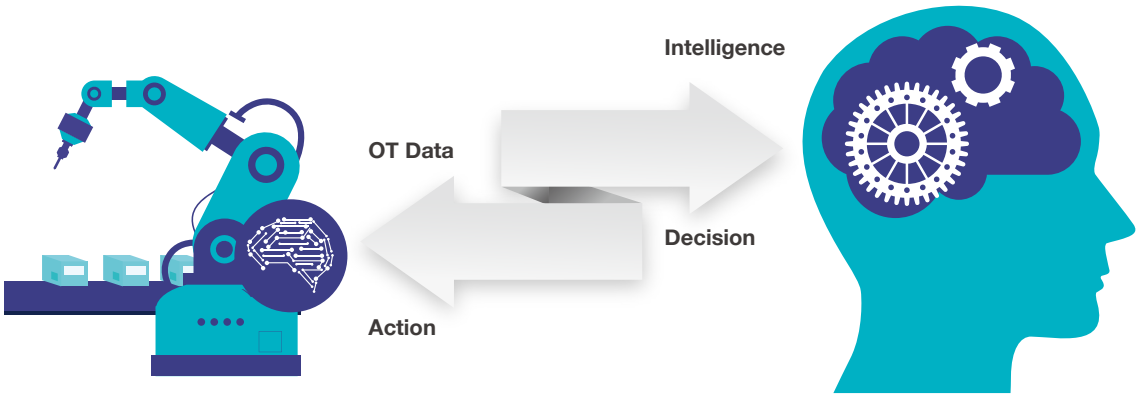
The OT Data Revolution: Qualitative and Quantitative Changes

OT data has long played a significant part in industrial automation. Since it basically represents the operative status or results of equipment in systems, and subsequently the key to the smooth operation of machines. However, industrial DX has introduced a whole new world where the competitive edge no longer lies with the amount of automated equipment owned, but with the amount of quality data mastered, as well the identification of the key problems from the aforesaid data. This major paradigm shift has prompted "qualitative" and "quantitative" changes to OT data and brought to light new challenges.

The Qualitative Changes of OT Data

Shifting Purpose: Moving from Monitoring to Optimizing

As demanded by the Industrial DX, the purpose of obtaining OT data has changed from "monitoring and control" to "optimization. By analyzing OT data in-depth, its short-term impact or long-term changes can be explored. Such analysis can lead to more comprehensive knowledge of the key factors involved in system operation efficiency. Furthermore, the analysis can ultimately be used to create an optimized, long-term implementation strategy.



OT data's reach has expanded from controlling end devices to business decision

More Impactful: Reaching Beyond the Device to the Executive Branch

Industrial DX regards OT data as an important business asset. Moving beyond the simple status report, today's OT data carries more weight than that of the past. Through continuous analysis, the original raw data can now be elevated to greater values, thus, increasing its influence. Effectively, it extends OT data's influence beyond the device on the floor to executive decisions in the boardroom.

All in all, Industrial DX has altered the expectations for OT data. Simply receiving raw data in a always stable flow is no longer good enough, as we expect more from extracted data nowadays. So, what is considered as high-quality OT data? This is where the four quantitative changes of OT data (the 4 Vs) come in.

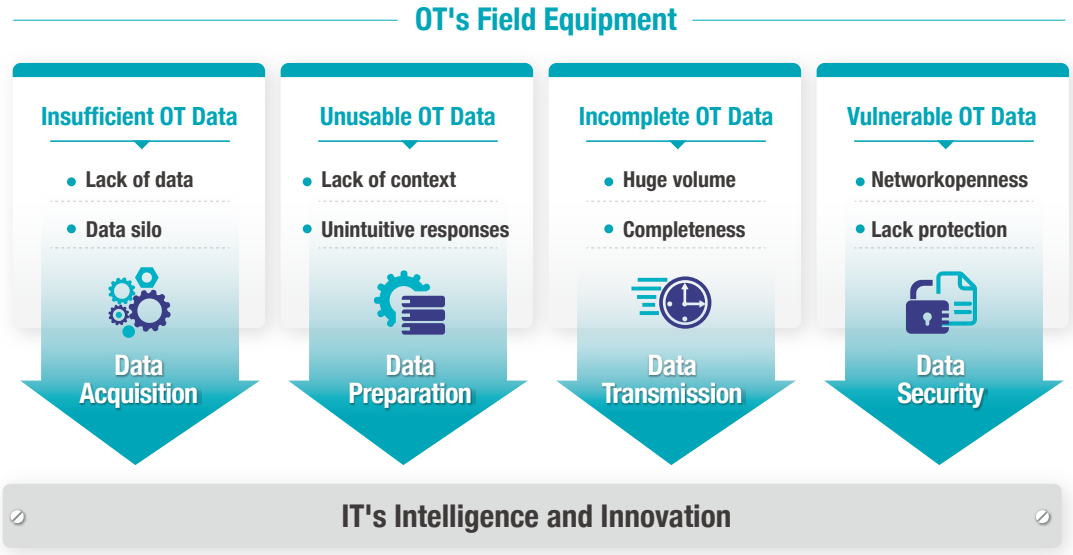
Quantitative Changes of OT Data

The qualitative changes also brought forth four quantitative changes to OT data (4 Vs), each with its own new challenges:

OT Quantitative Changes	New Challenges
Variety Requires "deeper" and "wider" data	**Insufficient Data** To address the need for diverse data, sensors and meters are added onto the original systems to collect the OT data. However, the various manufacturers of OT equipment use different protocols. Furthermore, the existence of data silos adds to the complexity of data connectivity. Thus, breaking down the barriers between data silos and completing the missing data are the main challenges.
Velocity Requires circular feedback of data for real-time display, analysis, and feedback	**Unusable Data** Raw data extracted directly from OT equipment cannot be analyzed by IT because of the lack of important context. Also, to analyze and make sense of the large amount of OT data often takes time, which goes against the real-time demands of control and feedback on OT's end. The velocity issue requires a new collaboration method between OT and IT to meet the immediacy requirement.
Volume Requires reliable network to stream large volumes of diverse data	**Incomplete Data** Transmitting diverse data in bulk and in real-time while maintaining its integrity is the main challenge when trying to integrate OT and IT networks and data. Other challenges include avoiding interference with the operation of equipment while transmitting large media files and overcoming environmental disturbances, such as electromagnetic waves, extreme temperatures, vibrations, etc.
Veracity Requires the security of data and networks	**Vulnerable Data** Cybersecurity is a matter of concern nowadays because OT data is now digitized and online. The IIoT has opened the floodgates to cyberattacks as everything is online. Hence, cybersecurity needs to be prioritized when investing in Industrial DX

The 4 Pillars of Connecting OT Data:
Jump-starting Your Industrial DX

The pace of the Industrial DX hinges on the level of mastery of the OT data. With the qualitative and quantitative changes to OT data, four new challenges have surfaced: insufficient data, unusable data, incomplete data, and vulnerable data. Moxa proposes the following data connectivity capabilities to combat these challenges:



See how each capability can help enterprises initiate industrial data transformation.

Expert Advice:
4 Self Evaluation Questions to See If You Are OT Data-ready

- Am I capable of getting the necessary OT data?
- Can my OT data be effortlessly connected to the IT system for display and analysis?
- Is my network ready to stably transmit large amounts of OT data?
- Is my OT data and network protected enough to minimize the risk of cyberattacks?

OT Data Acquisition

A lack of physical form has made digital data more unobtainable than imagined. Over the past 30 years, while assisting clients to acquire data on-site, Moxa has found that clients usually face the following three categories of difficulties.

OT Field Equipment Lacks the Ability to Provide the Right Data

Automation system provide raw OT data related to the system's output results, such as how many products are produced, the amount of power generated, the amount of water, etc. However, this is not nearly enough data under the new industrial digital transformation premise. So, this is the first obstacle many clients face. For example, product equipment can provide how many hours it's running, but it may not provide the power usage data for further analysis. This is a common occurrence in the initial phase of Industrial DX. As it is impossible to make the original equipment spew out data outside its original production scope, acquiring the necessary data for analysis becomes an issue.

Additional external sensors

Consider adding sensors such as vibration sensors to detect the vibration of a motor or fan, or a power meter to get the energy consumption data.

Irretrievable OT Data

Another problem related to data acquisition is that even existing data can be irretrievable. Many automation systems or equipment includes sensors, which transmit a continuous wave of "analog signals", such as voltage, current, light, temperature, pressure, and others, to back-end controllers, such as PLC, DCS , or SCADA, to monitor or control the equipment. Although these signals have been converted into digital format in the controller, acquiring it for analysis is still a challenge. Since controllers are not designed to constantly provide large amounts of data, frequently requesting them to provide or transmit additional data to other systems may affect the original purpose. Potentially, this could diminish the efficiency of the original operation, which is why obtaining OT data without disturbing original functions is critical.

Additional analog-to-digital conversion devices

Convert signals into digital data by incorporating an analog-to-digital device with the detectors. By incorporating a remote I/O, one can convert the analog signal to digital signal and upload it to the cloud or an upper server.

Complex Communication: Multitude of Disunited Interfaces and Languages

One of the signature characteristics of trying to control OT applications is the absence of a shared language. Different manufacturers often prefer to use their own unique hardware designs on equipment, which results in specialized communication interfaces and dedicated protocols. On the one hand, this allows each system to operate stably and provide the best performances when working independently. However, the downside sets in when equipment from different manufacturers is linked together. When data is collected from different systems for collaboration, finding a common ground for everyone becomes a major issue. For example, different production lines in a factory may use PLC controllers from different manufacturers, each with its own language, for instance, Modbus protocol in electric meters and IEC 61850 in power control systems. Attempting to collect the operating status and power consumption of different equipment on different production lines in a factory would be extremely time and effort consuming. The number of resources required to be proficient in all of the languages and protocols is colossal.

Make use of protocol translation tools or adopt a common protocol for the entire system

- A large number of protocol converters that can translate unfamiliar protocols into ones that users are familiar with are available, such as Modbus to BACnet, and vice versa.
- Use protocol converters to convert devices with different settings into a single common data exchange protocol for the upper system. For example, OPC UA/DA protocol, which is supported by most major industrial equipment manufacturers, or the MQTT protocol for cloud servers.

OT Data Preparation

Industrial DX creates a data processing loop that enables data to flow between OT and IT. Therefore, companies can receive data, analysis, and feedback to make real-time adjustments. However, the data processing cycle on the OT side differs from the one on the IT side:

- OT's data processing is for immediate monitoring and control; IT's data processing is for building a behavior model or filtering abnormalities through large amount data.
- OT works with scattered, individualized data; IT works with centralized collections of big data
- The OT side does not require a database; the IT side requires a database, and the data structure needs to conform to the database's format.
- OT processes data close to the edge; IT processes data on the remote/cloud end.

These differences exacerbate the difficulties encountered when attempting to integrate the data from both ends. Overall, four frequently seen challenges arise:

OT Data Cannot Be Used Directly by IT

OT data straight from equipment is referred to as raw data or value. In industrial automation, data is basically used to control, warn, monitor, etc. Hence, the value in its original form is sufficient for automatic operation. However, with Industrial DX, data is required to perform more than just direct control. To meet the new goals, value must be added to transform raw data into meaningful data. For example, raw data from a 16-bit temperature sensor shows 10,000. This raw data must be converted into meaningful data, for example, 45.60 degree, to show that it represents temperature. Adding context to the data, such as a unit, time, where the data comes from, etc., is an important preparatory task for data to be analyzed and further used.

Data preprocessing

Consider adding an IIoT gateway to bridge the systemic data between OT and IT. The advantages includes:

- Lowering the impact on the original functions of the equipment
- Converting raw data into meaningful data on the OT end
- Receiving detailed background description of the data
- Delivering data in accordance to the IT's database's requirements

OT Edge Real-Time Control vs. Cloud Analysis

Many applications on the OT end, such as system emergency stop or personnel safety management applications, require real-time responses. Since it cannot wait for the data to be first processed in the cloud by AI or ML, sending out the execution order, balancing on-site real-time requirements, and the optimization predicated on cloud intelligence will be a challenge.

Edge-cloud-integration

To achieve the preferred results and allow for feedback to be fed to the field site for real-time optimization, as well as other varying degrees of intelligent computing activities, integrated analysis of data and a suitable AI model on a cloud computer with significant computing power are important. These AI models are then deployed on edge computers to assist them to make better on-site decisions, for example, with regard to image recognition on railroad tracks, the safety of unmanned vehicles, and so on. The cloud will continuously collect the latest data, and then update the edge AI so that the optimization is continuous.

Balancing Challenge Between Data Upload and Cost

For many, the initial approach to achieve Industrial DX is to send all data collected on the OT end directly to the IT database or the cloud. Much of the data is considered useless. Sending it to the cloud not only lowers process efficiency but also increases the transmission and storage cost.

Data publishing

As data transmission is made easier by cloud services and the IIoT, the calculation of costs is now based on the data volume, storage space, and computing power. Therefore, data transmission between OT and IT must also be taken into consideration when trying to reduce costs.

- Only send meaningful data, such as sending the mean value for a specific timeframe
- Only send abnormal data, such as values that deviate from the normal range
- The data release frequency can be adjusted according to changes in data volume or special conditions

The Challenge of Data Loss

Since the OT environment is often subjected to uncontrollable disturbances, such as electromagnetic waves, extreme temperatures, vibration, etc., data is often lost during transmission. Thus, transmitting data without any interruption is very important on the OT side. Furthermore, receiving intermittent data can lead to poor or even wrong data analysis results on the IT side. Subsequently, the feedback to OT would be incomplete and incapable of execution. In a worst-case scenario, if the transmitted data is an update program for a device, this type of data loss could lead to the receiving device failing to reboot all together.

Data redundancy

To avoid data loss due to various on-site factors, keep a certain number of backups at the sender for a rainy day. In addition, at the data receiving end, include the ability to resume transmission after disconnection. The most common scenario occurs when IoT devices need to do over-the-air updates (OTA) and get disconnected due to a poor signal.

OT Data Transmission

Diversification and immediacy are required of OT data in Industrial DX. The combination of the two has greatly increased OT data's transmission volume. Coupled with the fact that high-definition images have gradually become an important source of OT data, the total transmission volume has surged significantly. Furthermore, Industrial DX requires long-term data streams for analytic purposes. All of which make transmitting data more complex than before. To build an OT network that can establish a stable and uninterrupted mass data transmission system involves several challenges:

Harsh Environments Affect Data Transmission, Resulting in Incomplete Data

Different industrial applications have varying environmental factors that could affect data transmission. From natural elements, such as extreme temperatures, humidity, etc., or manmade disturbances, such as electromagnetic interferences, vibrations caused by the equipment being onboard a moving machine or vehicle, all can cause data transmission interruptions and data loss. Wireless data transmission technology may seem convenient in the short term, but the interference problems and the complexity of long-term maintenance make the adoption of this technology hard.

Elevate the resilience of a data transmission system:

A number of incidents can occur during OT data transmissions. Consider these actions:

- If the wired network is disconnected or the wireless network is disturbed, switch automatically and quickly to a backup network to ensure that data will not be lost
- Network equipment should have a backup power system, or use an uninterrupted power system
- In response to the unique environmental requirements of different industrial applications (such as extreme temperatures, moisture, electromagnetic interference, explosion-proof, etc.), industrial-grade, certified or tested network equipment, specifically designed for these environments, should be selected

Control Network and OT Data Network Interfering With Each Other

Originally, OT networks were used to transmit device control commands and data, but with Industrial DX an influx of unfamiliar data, including device statuses, images, and sound, was added to the network. This additional data can potentially overload the network, resulting in the loss of systemic control in applications. For example, when multiple mechanical arms work coordinated on an automobile production line, resulting in unstable control. Therefore, one of the new challenges would be to construct a stable data network without control and data interfering with each other.

When constructing an industrial network, it is important to correctly calculate the bandwidth necessary for data transmissions. Also, take future transmissions into consideration. In addition, to ensure that the real-time OT control signals are prioritized above others, consider separating the OT data pathway from the control network to avoid competition between the various types of data. Another solution to avoid interference in one network is time-sensitive network (TSN) technology. TSN can also be adapted as the infrastructure of industrial communication network to ensure the transmission of important control signals while maintaining the real-time, low-latency, and security demands of OT data transmissions.

OT Network Management Becomes Complicated

Traditional automation uses direct connections, which connect devices directly to each other independently. As the number of devices that needs to be connected multiplies, so does the physical connections. Industrial Ethernet was able to resolve this issue by connecting hundreds of devices within the same system to each other via one network line. However, Industrial DX requires connections across different systems in the same network, making their management a major challenge.

As OT networks become more complex, the management methods need to keep up with the following:

- **Deploying OT-side network management tools:**
The intangible nature of data requires an easy-to-use industrial network management tool to convert data into tangible information. This could speed up on-site or remote personnel's judgment calls and shorten the period spent on resolving problems.
- **Establish an OT and IT network collaboration mechanism:**
Since industrial digital transformation is an application scenario requiring IT and OT collaboration, an intercommunication and collaboration method between the two network management teams should also be established. From the exchange of network management messages, to further discussions on how to build, maintain, and finally anomaly management, an integrated communication system will be able to respond efficiently when problems arise.

OT Data Security

Cybersecurity is a relatively unfamiliar territory to OT, since its systems aren't traditionally connected to the Internet. In the past, physical access control was the best and most efficient way to protect OT systems. Nonetheless, as the era of Industrial DX draws near, connecting to the Internet and opening the system to the outside world have become inevitable. The weaknesses of enterprises are exposed, and company secrets are now vulnerable to hackers. In recent years, frequent cybersecurity incidents occurred in key manufacturing and infrastructure industries due to the rising exposure and lack of subsequent protection. The COVID-19 pandemic has further accelerated the integration of OT and IT systems and, by extension, the need for remote maintenance. OT systems' cybersecurity capabilities have gradually become the primary indicator for evaluating the reliability of an Industrial DX system. Enterprises face the following challenges as they invest in the strengthening of their OT network security:

OT Lacks Both Expertise and Experience to Deal With Security

Without enough cybersecurity expertise and experience, it can be daunting to come up with a suitable defense against cyberattacks from various fronts. Often, OT staff are scratching their heads trying to figure out where to start. Furthermore, the return-on-investment (ROI) for cybersecurity isn't immediate in most cases, which makes it a hard sell to managers. Therefore, most of the time, cybersecurity vendors are brought onboard in a rush due to a pending cyberattack, which by then has already wreak havoc on the system.

Cybersecurity as risk management:
The investment in cybersecurity should not be evaluated from a ROI standpoint, but rather from a cost of inaction (COI) standpoint. Evaluating the losses of tangible money and personnel, as well as the threat to the intangible brand image, in case of a cyberattack is necessary.
Establish a dedicated OT and IT integrated cybersecurity team:
Only a dedicated cybersecurity team that understands the needs of IT and OT can quickly assess the potential risks and formulate a defense strategy that meets the overall needs, while sidestepping a minefield of unclear responsibilities. So, in the event of an attack, it can be dealt with effectively and quickly to reduce corporate risks.

IT Cybersecurity Tools Don't Work in OT Environments

One common scenario occurs when OT maintenance departments place the burden of building a cybersecurity system solely on IT's shoulders. While traditionally the IT department has more experience in the aforesaid field, its methods often don't work in an OT environment:

- Anti-virus software cannot be installed on OT equipment: Most OT automation equipment runs on special operating systems, which prevent packaged anti-virus software from being installed.
- Computers in an OT environment cannot undergo regular cybersecurity repairs to avoid vulnerabilities:

OT equipment usually operates 24/7, which means it doesn't have a 'down time' to fit in scheduled cybersecurity updates to patch up vulnerabilities. Beyond the need to stay powered on continuously, a potential interference of the equipment's operational efficiency is also a major concern that prevents routine cybersecurity updates.

- OT communication protocols lack authentication and encryption mechanisms: Most OT communication protocols do not have security measures such as authentication or encryption. The IT management tools cannot separate the communication protocols from the malware as they cannot recognize the protocols, creating a major security vulnerability. In other words, anyone who has access to the OT network can issue

Provide cybersecurity protection measures from an OT operational POV:

Most cybersecurity protocols can be divided into three parts, terminal equipment protection, network security, and security management. However, implementing security protocols in an OT environment is vastly different from that of IT:

- **The continuous operation of OT equipment as the primary goal:**

Often when IT detects cybersecurity vulnerabilities, the priority is placed upon the immediate elimination of these risks at all costs. However, OT's priorities are to keep the equipment operational, which makes for a decidedly different approach when dealing with cyberthreats. OT would favor deploying mitigating measures to reduce the risk while keeping the automated equipment running instead of shutting down all system to install fixes or upgrades. To resolve this, an intrusion prevention system (IPS) can be installed to create virtual patches to eliminate security vulnerabilities, without forcing the device to shut down and upgrade.

- **Hierarchical management to control the scope of the damage:**

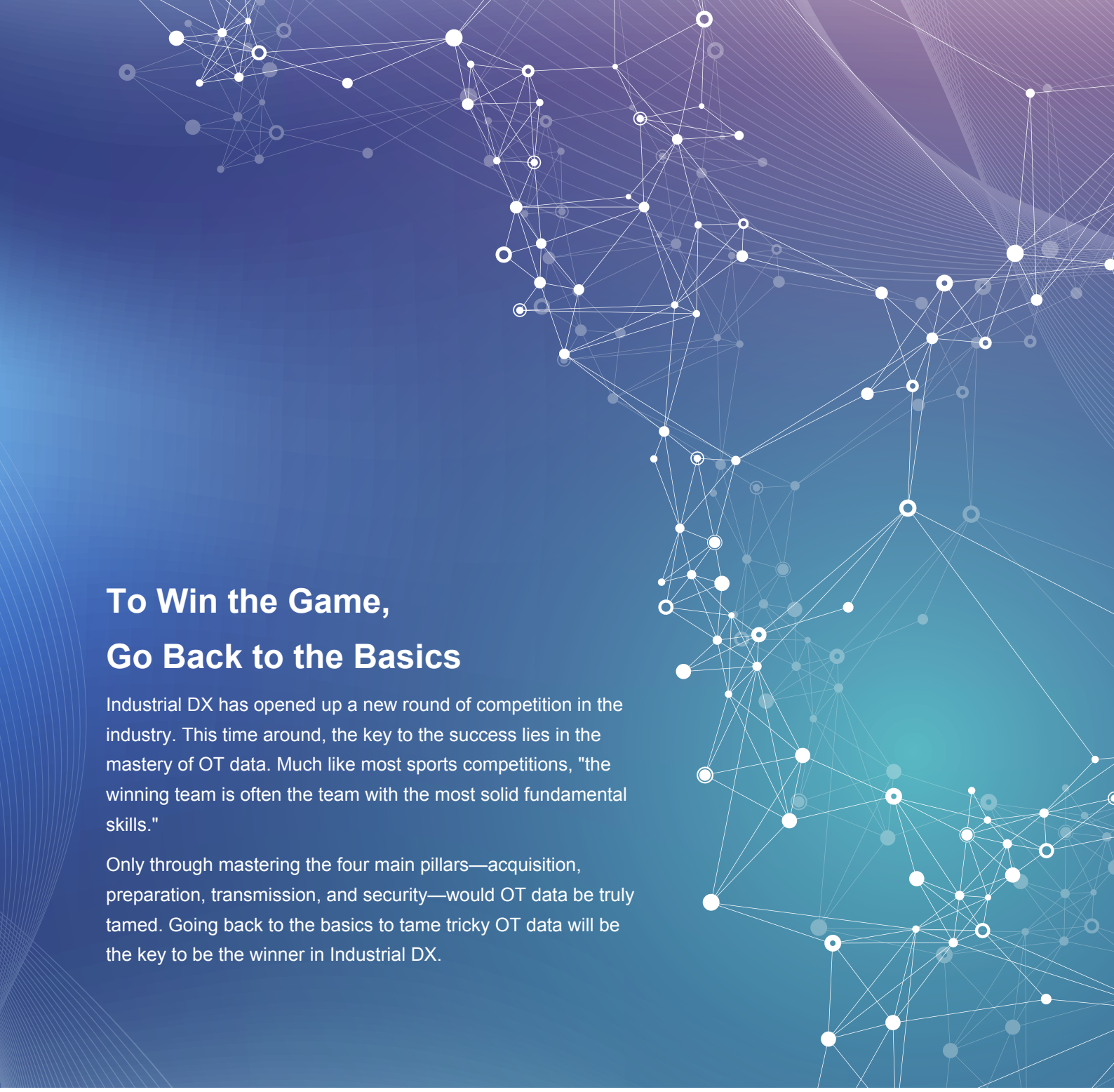
As OT networks are becoming increasingly complex, it is also necessary to introduce the "in-depth defense" concept, which manages network packets via a hierarchy through firewalls and managed switches. This type of divide-and-conquer strategy is used by IT management to prevent confidential information from leaking. Whereas for OT, this strategy can help isolate an attack and prevent it from wreaking havoc on the entire network.

- **Focus on OT communication anomaly management:**

Since most of the OT communication protocols are not authenticated and/or encrypted, it is necessary to consider monitoring and managing abnormal OT commands. For example: if a controller normally only sends out commands to read the status of the gate on weekdays, and it suddenly issues a command to control to open the gate, then an alarm should be raised.

- **Eliminate potential security breaches in remote maintenance:**

Post-COVID, remote maintenance has become one of the fastest and most effective ways to solve customers' problems. While its remote nature allows third-party vendors the convenience to privately install a free remote desktop software to install, update, or check remote equipment through the Internet, it also opens the door to cyberattacks. By ignoring the viruses contained in the software, or forgetting to terminate the connection after repairing, could place the entire network in jeopardy. Companies should plan to provide safe solutions to OT personnel to eliminate these common security breaches.



To Win the Game, Go Back to the Basics

Industrial DX has opened up a new round of competition in the industry. This time around, the key to the success lies in the mastery of OT data. Much like most sports competitions, "the winning team is often the team with the most solid fundamental skills."

Only through mastering the four main pillars—acquisition, preparation, transmission, and security—would OT data be truly tamed. Going back to the basics to tame tricky OT data will be the key to be the winner in Industrial DX.