Autonomous and Controllable: The Safety Valve for Industrial Internet (Postprint)

Authors:

Date: 2023-10-08T00:00:00+00:00

Abstract

The industrial internet, as a product of the deep integration of new-generation information technology and manufacturing, has shown vigorous development momentum in recent years. However, as increasing numbers of industrial control systems and devices connect to the internet, the open and interconnected environment has made industrial internet security issues increasingly prominent. According to statistics, in the past year alone, the National Information Security Vulnerability Sharing Platform …

Full Text

Preamble

Special Feature: Media Watchtower
ChinaXiv Partner Journal
Autonomous Controllability: The Safety Valve of Industrial Internet

The industrial internet, as a product of the deep integration of new-generation information technology and manufacturing, has shown vigorous development momentum in recent years. However, as increasing numbers of industrial control systems and devices connect to the internet, the open and interconnected environment has made industrial internet security issues increasingly prominent. According to statistics, in the past year alone, the National Information Security Vulnerability Sharing Platform has cataloged over 100 software security vulnerabilities in industrial control systems that have widespread impact on China. The development and research of industrial control security represent one of the key focuses of industrial internet security. At the 2018 Annual Conference of the Information Security Professional Committee of China Information Industry Association and the 8th High-End Forum on Cybersecurity Innovation Development, Zhang Ni, Deputy Director of the Sixth Research Institute of China Electronics Corporation and Executive Deputy Director of the

National Engineering Laboratory for Industrial Control System Information Security Technology, emphasized the importance of autonomous controllability for industrial internet security. This issue presents selected excerpts for our readers.

Industrial control systems are divided into three categories: discrete control, process control, and motion control. These systems are widely used in energy generation and distribution, as well as in transportation, logistics, and other industries that rely heavily on such control systems. In the pre-Industry 4.0 era, security considerations were minimal, based primarily on two assumptions: physical isolation and relatively simple protocols and business logic. The Industry 4.0 era, however, brings intelligent and information-based development with more software connectivity, terminal-to-cloud connections, and various networked terminals, making security issues critical. How do we protect our critical infrastructure?

First, autonomous controllability is not merely a cybersecurity concept but a broader security concept—an extension of security. While everyone supports the idea of autonomous controllability, implementation remains difficult in practice. It does not require that everything be autonomous and controllable; global industrial development constitutes an entire ecosystem that allows for industry integration, but we must maintain autonomous controllability over core components.

Second, the key to autonomous controllability lies in freedom from maintenance and upgrade constraints—we must escape the predicament of being "choked by the neck" or "led by the nose." For instance, at the device level, small intelligent devices that play critical roles in the field should be replaced with autonomous and controllable alternatives whenever possible. PLCs, switches, routers, and servers are all critical network devices that require autonomous controllability.

Third, autonomous controllability does not equal security. Preemptive situational awareness is an integral part of security protection. Industrial security devices involve substantial professional experience and knowledge, and security protection must be integrated with the business operations of each industry. This involves both information security and autonomous controllability security. After several years of convergence, these two approaches will reach a balance that enables development while ensuring security. Current security assurance is not about preventing all faults but about ensuring we are not targeted by hostile forces.

Overall, the key to autonomous controllability lies in application. Large-scale application requires genuine users. Security equipment proves its feasibility through extensive deployment—only through widespread use can it be truly implemented. Information security must match on-site security pain points, with security planning and construction proceeding synchronously.

The security of industrial control systems currently faces numerous threats and challenges. First and foremost, industrial control systems have become primary targets for national-level hackers. What attacks these systems are not viruses but cyber weapons. Second is the autonomous mastery of core technologies. Third, industrial terminals are transitioning from closed-loop to open-loop systems, presenting a new challenge. As new technologies continuously evolve and upgrade, we inevitably face growing security pains. Fourth is the security simulation environment for the industrial internet—industrial environments have high barriers and testing platforms are costly to build. Fifth is industrial big data. Big data platforms are internet-based, involving a series of processes including storage, collection, mining, analysis, publishing, and sharing. For industrial control systems, this open and interconnected environment poses challenges to industrial internet security.

Cloud computing, big data, and the Internet of Things have increased the openness and uncertainty of industrial processing workflows, further concentrating security risks. The security of industrial control systems is not a minor security concept but requires a deep security defense system. From the top level, the nation is increasingly prioritizing cybersecurity issues. Both regulations, guidelines, and plans have elevated public security to a national strategic level. For two consecutive years, the Ministry of Science and Technology has designated industrial control system security as an important direction for cyberspace security.

Facing these many challenges, how should we respond?

Note: Figure translations are in progress. See original paper for figures.