

AI Is Transforming Manufacturing, Increasing the Role of Data Security

As artificial intelligence becomes increasingly integrated into manufacturing, data is becoming more valuable to businesses, while data security is emerging as a critical element of digital transformation. The latest version of GENESIS, developed by Mitsubishi Electric Iconics Digital Solutions, combines advanced security features with AI-ready APIs and integration capabilities.

Manufacturing facilities are generating rapidly growing volumes of data across every layer of their operations, from sensors and machines to control systems and enterprise applications. As AI and advanced analytics become more deeply integrated into manufacturing processes, collecting and analyzing this data is no longer enough. Ensuring that data is accurate, reliable and accessible in a controlled manner is becoming equally important. As a result, securely managing the data used by AI applications is becoming just as important as the quality of the data itself.

This shift is also changing how industrial organizations approach data security. As manufacturing environments become increasingly connected and data exchange grows, security is moving beyond its traditional role as a layer of protection against external threats. It is becoming a fundamental part of supporting sustainable digitalization.

AI Starts with a Reliable Data Infrastructure

GENESIS, Mitsubishi Electric Iconics Digital Solutions' next-generation HMI/SCADA and digitalization platform, enables organizations to collect, visualize and analyze data across a wide range of applications, including building automation, energy management, manufacturing operations and data center infrastructure management. The platform also supports centralized system monitoring and control.

The latest GENESIS architecture features an AI-ready API infrastructure designed to enable new use cases between automation and AI applications. Secure machine-to-machine authentication capabilities also help ensure that data is exchanged between systems in a controlled manner. This allows businesses to take advantage of AI and automation technologies while keeping security at the core of their digital infrastructure.

As connections between systems and data sources increase within manufacturing environments, the attack surface that organizations need to manage can also expand. To help address these risks, Mitsubishi Electric Iconics Digital Solutions recommends avoiding direct exposure of industrial

systems to the internet, securely separating production systems from other enterprise networks, and using protective measures such as firewalls and VPNs.

The company also highlights the importance of disabling unused services, controlling network access and keeping systems up to date as measures that can help reduce the attack surface. This approach is designed to maintain the flow of data across connected manufacturing environments while addressing security in a comprehensive manner.

Cybersecurity Approach Backed by International Standards

Mitsubishi Electric Iconics Digital Solutions integrates security throughout the software development process. Supported by technologies including encryption, certificate-based authentication and access controls, this approach is also backed by international standards.

In addition to ISO/IEC 27001:2022 certification for its Information Security Management System, the company holds IEC 62443-4-1 certification covering secure product development processes for industrial automation systems. These standards demonstrate that security is addressed systematically across different stages of product development, starting from the earliest phases of the process.

The GOT3000 Series HMI provides a recent example of Mitsubishi Electric's approach to cybersecurity. The series has been certified by TÜV Rheinland in accordance with IEC 62443-4-2:2019, which defines technical cybersecurity requirements for devices used in industrial automation systems. This certification further supports Mitsubishi Electric's approach to cybersecurity as a fundamental element of its industrial automation solutions. From product development processes to device-level security requirements, this multi-layered approach enables cybersecurity to be addressed across different levels of industrial automation.