Thinking Outside the Black Box: Scalable Use-Case Solutions for Factory IT Management

A properly designed security system – no matter whether it involves cryptography, locksmithing or cybersecurity – should remain secure even if everything but the key itself is public knowledge. No secret can remain safe forever, and the moment these black boxes are opened, they inevitably become worthless for securing data.

INTRODUCTION

The Industrial Internet of Things (IIoT), once just a buzzword, has now become a vital part of the manufacturing ecosystem as companies strive to collect and analyze data to track Overall Equipment Effectiveness (OEE) and create fully optimized processes. However, the increasing digitization of manufacturing brings new risks, and with cybercrime on the rise, manufacturing information technology (IT) professionals have a vested interest in preventing criminals from accessing networks, particularly as increasingly large amounts of data are moving across factory floors and between machines.

In some cases, manufacturers have turned to cybersecurity solutions that involve so-called "black boxes," or systems that remain completely opaque to the user. This approach can be criticized as a form of "security through obscurity," a concept that has been widely known among security experts since the late 1800s, when cryptographer Auguste Kerckhoffs developed what became known as Kerckhoffs' principle: A properly designed security system – no matter whether it involves cryptography, locksmithing or cybersecurity – should remain secure even if everything but the key itself is public knowledge. No secret can remain safe forever, and the moment these black boxes are opened, they inevitably become worthless for securing data.

In addition to the security flaws created with black-box systems, this approach also closes systems to any improvements after deployment. Not only does a black box hides the mechanism by which it outputs data, it prevents the user from changing or improving the mechanism. After all, if one opens the box to change anything inside, the box loses its ability to provide security. Given that manufacturers frequently discover new use cases for their data – such as new methods for machine monitoring or preventive maintenance – this level of inflexibility severely hampers efforts to further improve and optimize processes.

Mazak

To overcome these challenges and deliver a truly robust cybersecurity launch platform, Mazak Corporation designed its Mazak SmartBox to operate with open-source software and protocols at the same time it offers virtually limitless scalability. A digitally integrated platform that ensures manufacturers can achieve fully secure plantwide networks, including legacy machines, the SmartBox's internal Linux PC allows for the adoption of new use cases without compromising cybersecurity.

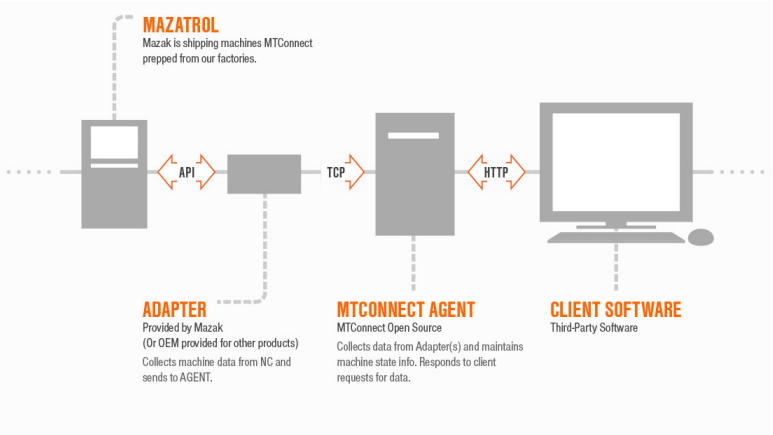
TECHNICAL BACKGROUND

Removing black boxes and empowering IT professionals to solve a wide variety of use cases in manufacturing requires two key technologies. The first, the Mazak SmartBox and its Cisco® Industrial Ethernet 4000 Series Switch, ensures robust, safe networking to bridge the gap at the edge of machine tool networks. The second is Mazak's full-featured implementations of the MTConnect® standard communications protocol on its machines, which provides a common language for devices in the manufacturing environment.

To overcome these challenges and deliver a truly robust cybersecurity launch platform, Mazak Corporation designed its Mazak SmartBox to operate with open-source software and protocols at the same time it offers virtually limitless scalability.

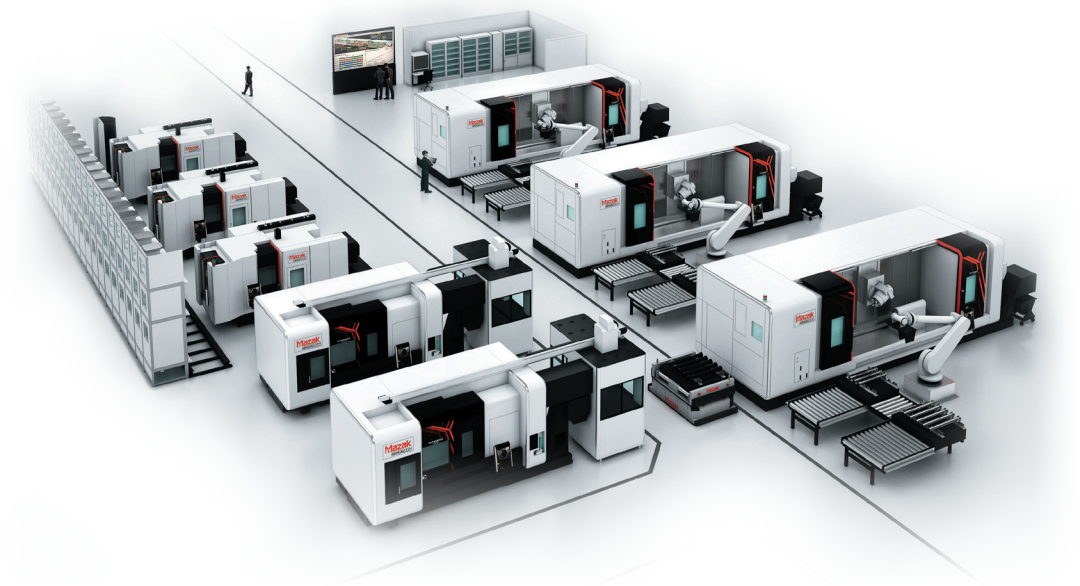
MTCONNECT

MTConnect, an open, royalty-free manufacturing communications protocol, fosters greater interoperability between manufacturing devices and software. By connecting diverse equipment with a single method of communication, MTConnect makes it possible to monitor and harvest data from the entire production floor, including machines, cells, devices and processes. The standard is implemented with XML and HTTP technology, widely used internet technologies for real-time data sharing.



INDUSTRIAL ETHERNET 4000 SERIES SWITCH

As an industrial machine connectivity solution, Cisco Industrial Ethernet 4000 Series Switches offer a secure, scalable way to connect machines to platforms capable of tracking OEE or other software solutions for analyzing manufacturing technology. The all-in-one nature of the 4000 also provides security and computing capabilities, solving the problems typically associated with access, management and scalability. This empowers both IT departments and their colleagues on the factory floor, encouraging them to work together to drive machine efficiency and visibility.



A core component of the Mazak iSMART Factory™ paradigm, the SmartBox enables the complete digital integration of Mazak's advanced manufacturing cells and systems to achieve free-flow data sharing in terms of process control and analytics.

SMARTBOX

Combining MTConnect and the 4000 Switch, the Mazak SmartBox provides connectivity for machines and devices, which enhances monitoring and analytical capabilities as it provides a far greater level of cybersecurity. With several standard input ports and connection ports, SmartBox quickly and easily connects any standard off-the-shelf sensors to the system for machine-data gathering and condition monitoring. One SmartBox, installed on a nearby I-beam or a Mazak-supplied stand, can serve several machine tools, along with other associated manufacturing equipment, depending on the application and cybersecurity needs.

The Mazak SmartBox offers network isolation, which prevents unauthorized access from both directions – to and from the machines and equipment on a network – through a virtual local area network (VLAN). With this, as well as its implementation of MTConnect, the SmartBox satisfies the critical security concerns of IT departments when connecting new and legacy equipment alike to a plant's main network for the purpose of gathering manufacturing data. A core component of the Mazak iSMART Factory™ paradigm, the SmartBox enables the complete digital integration of Mazak's advanced manufacturing cells and systems to achieve free-flow data sharing in terms of process control and analytics. As a result, Mazak has increased utilization for monitored machines by double-digit percentages, a capacity windfall that has reduced operator overtime by 100 hours per month and brought 400 hours per month of previously outsourced work back in house.

COMPUTING AT THE EDGE

The drive toward full digital factory integration has increasingly focused on an area or region known in the IoT community as the "edge" – the boundary between the physical piece of equipment's data stream and a wider network. In the case of the Mazak SmartBox, the interface between the machine network's VLAN and the facility's network acts as this edge. As machine tools create more and more data, IT professionals have focused on performing more computing at the edge to reduce the impact large amounts of high-frequency data have on overall factory network traffic.

In addition to managing network traffic, performing computing tasks at the edge also improves overall cybersecurity. Rather than pushing data outside the network for analysis on external hardware or cloud-based solutions, manufacturers' IT departments maintain complete control over their data, most of which can remain safely within the confines of VLANs that link individual groups of machines

BEYOND BLACK BOXES

As the world economy increasingly centers itself on the big data that underpins all industries, protecting that data becomes vital. This is especially true for manufacturers, many of whom do sensitive work that requires security clearances, Department of Defense (DOD) oversight or, in some cases, Host Intrusion Prevention System (HIPS) certification from the National Security Agency (NSA). However, this level of trust requires complete transparency from manufacturers – including their security systems. Mazak, in seeking to help manufacturers meet these stringent security requirements, removed any black boxes from the SmartBox's system architecture. Not only does this qualify the device for the most demanding security applications, but it gives manufacturers and their IT departments complete ownership of their data, a commodity in and of itself.

Much like the personal information bought and sold by business-to-consumer companies, manufacturing data have intrinsic value. The natural result of this is that whether it involves cloud computing, remote data storage, online customer service or machine monitoring, most IT solutions for manufacturers include black boxes in which the owners lose control of the data. And if the manufacturer does not control the data, they can safely assume the builder of the black box does instead.

As IT professionals increasingly demand to own and control their data, the Mazak SmartBox is a vital tool. With a SmartBox-powered network, IT professionals collect and store the data themselves. If the data must be shared, IT departments can now audit it and send only what a partner or vendor needs to accomplish their task. This is a massive paradigm shift, one that empowers manufacturers to realize the advantages of data stewardship.

AN IT SOLUTION FOR OT

The Mazak SmartBox is much more than a security solution, however. It can best be described as an IT solution for operational technology (OT), a newer term that refers to the equipment used to manipulate or control physical systems, such as manufacturing equipment and machine tools. These two disciplines have traditionally been separated by numerous factors, but the Industrial Internet of Things serves as the intersection between IT and OT, a fact that has disrupted the entire industry.

Because IT and OT departments have not historically overlapped to any significant degree, the Mazak SmartBox has brought together professionals who now must work together to establish use cases and deploy software solutions. Two of these

Because IT and OT departments have not historically overlapped to any significant degree, the Mazak SmartBox has brought together professionals who now must work together to establish use cases and deploy software solutions.

use cases – the machine connectivity itself and the secure file transfer via HTTPS that it enables – are solved by the SmartBox upon installation. IT departments can now further protect their networks against intrusion, including eliminating the need to deploy machining programs via USB or other physical media. This prevents numerous vectors for cyberattacks.

With the help of their OT colleagues, IT professionals can use these tools to expand upon the SmartBox's existing feature set. As an IT solution, the SmartBox requires active management by IT professionals, who can interact with SmartBoxes on an individual basis or use software like the Cisco Fog Detector to manage an installation with numerous SmartBoxes. Because each SmartBox is built around a Linux PC, the microapplication possibilities are virtually endless; if a sensor exists to measure data in a machine, it can be incorporated into the SmartBox data collection routine.

SUMMARY

The Mazak SmartBox represents a major step forward for manufacturers in terms of balancing cybersecurity needs with the utilization of data leveraged toward improving OEE. By eschewing security through obscurity and empowering IT professionals to collaborate with their OT colleagues with computing at the edge, Mazak has ensured that real-time manufacturing data continues to play a vital role in manufacturers' efforts to improve productivity, efficiency and responsiveness to customers and market changes.

About Mazak

Mazak Corporation is a leader in the design and manufacture of productive machine tool solutions. Committed to being a partner to customers with innovative technology, its world-class facility in Florence, Kentucky, produces over 100 models of turning centers, Multi-Tasking machines and vertical machining centers, including 5-axis models. Continuously investing in manufacturing technology allows the Kentucky iSMART Factory to be the most advanced and efficient in the industry, providing high-quality and reliable products. Mazak maintains eight Technology Centers across North America to provide local hands-on applications, service and sales support to customers.