KASPERSKY INDUSTRIAL CYBERSECURITY PROTECTS AGC

KASPERSKY lab

AS A SUPPLIER TO THE AUTOMOTIVE INDUSTRY, BUSINESS PROCESS CONTINUITY IS CRITICAL FOR AGC. WHICH IS WHY ITS PRODUCTION LINES ARE PROTECTED WITH KASPERSKY INDUSTRIAL CYBERSECURITY.

Automotive

- *Founded: 2003*
- *Market share: approx. 23%*
- *Using Kaspersky Industrial CyberSecurity since 2016*

AGC Glass Germany GmbH has been producing automotive glass for leading manufacturers such as BMW, Volkswagen, Mercedes, Volvo and Opel since 2003. It employs 150 staff at its site in Wegberg near Mönchengladbach, Germany, and is part of the Asahi Glass Company, a world-leading Japanese glass manufacturing group that employs more than 50,000 people in 20 countries around the world.

AGC Glass Germany GmbH processes automotive glass panels produced elsewhere in the group to tailor them to its customers' specific needs. This can include adding heating or rain sensors to the glass panels, or surrounding them with seals. The glass elements are then taken on to production lines across the automotive industry.

Process stability is a top priority

When it comes to standardized, large-batch manufacturing like at AGC Glass Germany, process stability is absolutely critical. A delay in production or worse, a complete breakdown of the production lines, can not only incur cancellation fees, but in many cases expensive contractual penalty charges, too. To combat this, AGC uses the Industry 4.0 platform Tomorrow Connect and its eApps to gather real-time information about process stability and deviations from its set values.

"We decided to partner with Kaspersky Lab as Kaspersky Industrial CyberSecurity could be implemented whilst our operations were still running, and because the solution is compatible with both the control systems we use and Tomorrow Connect."

Jan Houben, Plant Manager at AGC Glass Germany GmbH

The solution was developed by the Kaspersky Lab partner Tomorrow Labs in collaboration with the Fraunhofer IPA and machine manufacturers. It collects, links and visualizes machine and ERP data from different manufacturers and so allows information from across departments and the company to be brought together to facilitate transparent, autonomous production.

IT security for industrial control systems

However, having such a large amount of networked production equipment also exponentially increases the number of weak points for cyberattacks. These can in turn cause considerable financial losses and long-lasting damage to a company's image.

Where in the past individual computers in offices would be the target of such attacks, they can now take down entire production systems or even cause subtle reductions in quality that, in a worst-case scenario, will not be noticed until the product reaches the end customer. To reduce these risks, AGC has chosen to secure its production equipment with Kaspersky Industrial CyberSecurity (KICS).

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity was developed specifically for critical infrastructures and industrial equipment.

The solution combines a range of conventional security technologies such as malware protection, whitelisting and vulnerability management. It also includes device access control which enables the customer to monitor connections to portable data storage media and peripheral devices.

SECURITY

Combines conventional cybersecurity technologies with technologies developed specifically for industrial environments

RISK MANAGEMENT

Protects against contractual penalties

CONTROL

Detects unauthorized devices, providing maximum control over industrial networks

agc-automotive.com
tomorrow-connect.com

150
Employees

10
protected production lines

"The Kaspersky Lab solution recognizes when an employee connects a USB stick to our network", explains Jan Houben. "It then searches its list of authorized USB sticks to determine whether the user should be permitted to use the device or not."

These more standard functionalities are further supplemented by technologies specifically designed for industrial environments, such as integrity checks and semantic monitoring of process control commands. Kaspersky Industrial CyberSecurity also features a special monitoring mode developed to detect cyberattacks, employees' operational errors and anomalies within industrial networks.

Ten production lines protected

At AGC, each individual production line is protected with Kaspersky Industrial CyberSecurity. The solution monitors all network levels and scans all kinds of activities. Kaspersky Industrial CyberSecurity alerts the company immediately to any anomalies in production.

"Kaspersky Industrial CyberSecurity is based on a modular system, so it can be adapted to our individual requirements and specific infrastructures", continues Jan Houben. "The solution gives us cybersecurity across all network levels without affecting the operational continuity of our technological processes."

Kaspersky® Industrial CyberSecurity

KASPERSKY lab

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212
info@kaspersky.com
www.kaspersky.com

For more information about Kaspersky Industrial CyberSecurity and other solutions contact your account rep or visit www.kaspersky.com/ics