

SIEMENS



Site-wide digitalized  
**security systems for  
smart factories**

According to McKinsey, digitalization and Internet of Things (IoT) trends have fueled the widespread distribution of low-cost smart sensors, increased connectivity, and new-generation data analysis tools and software across industries. In fact, Forbes predicts that \$267+ billion USD will be invested globally in IoT technology over the next five years.

This digitalization movement is already in full swing. A recent PwC survey of manufacturers reveals that 66% have a digital transformation roadmap in place for some or all departments, while 72% of organizations categorize themselves as quick to adopt new technologies.

Although core production applications have received the bulk of the digitalization attention, other important areas, such as industrial security, have quietly evolved to enhance the protection of workers, products, trade secrets, and important data.

The evolution in industrial security among workers and the changing nature of threats to human and asset safety have made protection of employees, products, and data more complex over time. Fortunately, there are new, integrated digital solutions that enable real-time monitoring across multiple sites, helping plant managers and security support teams to act quickly when threats appear.

**These solutions offer a holistic approach** – helping factories achieve higher levels of prevention and resilience, while eliminating downtime and enhancing situational awareness. Below are examples of these digital solutions:



### Access management

Access control, including perimeter protection, is the first line of defense. Products like Siemens SiPass integrated Access Control and Siveillance Control serve as security management station components that integrate access control, intrusion detection, and video surveillance into a single security platform. The open security architecture interface ensures that new components integrate easily and enhances situational awareness across the plant. These solutions can be customized based on what needs to be protected and who requires access to particular assets.

### Video surveillance

The most common threats to industrial plants include violence, theft, vandalism, and trespassing. An investment in security cameras is a good way to boost security. Besides being used to monitor perimeters and suspicious activity, cloud-based video systems centered on intelligent video analytics and sensor inputs offer the ease and benefit of off-premise video hosting, reduced capital expense, and lower maintenance costs. Products like Siveillance Video offer analytics and alarming through the use of video for unattended object detection, loitering, flow of traffic, and aggressive behavior incidences.





## Suspect tracking

New security tools now make it easier than ever to follow a target of interest through the entire network of surveillance cameras. For example, Suspect Follower, a new plugin for the Siveillance Video system, allows security officers to generate a storyboard of the suspect's path by manually tracking a suspect's movement using live stream or recorded video footage. Multiple operators can also work within the system, managing major live incidents with multiple targets.



## Cybersecurity

While enhanced connectivity is valuable for facility performance, it also increases cyber-attack threats. According to a recent Kaspersky report, almost half of industrial systems bore evidence of attempted break-ins in 2018. The most common form of attack, according to the report, was Trojan malware, which it detected on 27% of industrial control system computers. To help combat these threats, Siemens, as a Charter of Trust founding member, is dedicated to providing operation technology (OT) cybersecurity solutions and services to customers across a wide range of different industries.



## Mass notification

In the event of a security incident, factory owners want to be equipped with the latest technology to help protect employees, assets and buildings. Centralized, customizable mass notification solutions are now available that can integrate and streamline multiple disciplines – from fire safety and security to building automation. For example, by integrating Siemens Siveillance Video with Shooter Detection System LLC's Active Shooter Detection, building alarms and security systems can be alerted to active shooter incidents. When properly deployed, emergency communications processes are automated at the first moment gunshots are detected and systems identify, track, and potentially respond to active shooter situations. Building security and law enforcement gain instant access to critical information, which reduces response times and accelerates the engagement of automated security protocols.



# Siemens Unified Security Approach



No manufacturing facility is secure using only one product, technology, or methodology. A holistic approach should be applied when protecting manufacturing assets. Siemens security experts help clients build integrated security platforms that enable efficient monitoring, faster response times, and fewer false alarms. Learn more about Siemens holistic approach by visiting us on the web.

**For the U.S. published by  
Siemens Industry, Inc.**

Smart Infrastructure  
1000 Deerfield Parkway Buffalo Grove,  
IL60089 Tel: (847)215-1000

All rights reserved.

Printed in the USA

© 2022 Siemens Industry, Inc.

Order no.: 153-SBT-1507

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

© Siemens 2022