WHITEPAPER

BIOMETRICS IN THE MANUFACTURING SECTOR

Automating Identity Management with Biometrics

INTRODUCTION

WITH JUST A GLANCE AT A FACE OR IRIS READER, WORKERS CAN UNLOCK DOORS OR MACHINERY WITHOUT USING THEIR HANDS, WHILE WEARING GLOVES, MASKS, AND GOGGLES.

The drugs we take, the cars we drive, the electronics we use, and much of the food we eat pass through a manufacturing plant. So do all the cleaners, cosmetics, and other household supplies in our homes. We assume these products are safe to use or consume because we trust the manufacturing process.

When lapses occur, they impact companies' profits, reputations, and consumer safety. Preventing unauthorized or untrained personnel from having access to manufacturing equipment, materials, and processes is crucial for maintaining quality control.

The manufacturing process must also be safe for workers. A single violation of OSHA regulations costs an offending company $15,625 per day. Protecting intellectual assets is equally important. Management must prevent competitors from gaining access to unique designs, formulas, ingredients, and assembly processes.

Biometric identity solutions can support the manufacturing environment in addressing all these challenges. Beyond safety and security, they create operational efficiencies and encourage greater employee productivity. Following is an introduction to how and where the implementation of biometric technology offers these benefits.

WORKPLACE SAFETY

Manufacturing environments must have physical access control in place to comply with a wide range of regulations, many of which exist to ensure worker safety. Employees should only have access to the parts of the facilities that are essential to their jobs. They must wear appropriate protective gear. Anyone operating heavy machinery must be trained and authorized. Shift workers who don't belong on the floor at a given time shouldn't be there – they can be distracting to those working.

Biometrics tied to access control offers superior convenience and security. With just a glance at a face or iris reader, workers can unlock doors or machinery without using their hands, while wearing gloves, masks, and goggles. Such solutions create a seamless verification process for access to areas and equipment with incomparable accuracy. As biometrics are intrinsically linked to the individual, nobody can successfully pose as an imposter by borrowing someone else's credentials.

QUALITY CONTROL

Quality control requires consistency and precision. Manufacturing Execution Systems (MES) optimize the manufacturing process by monitoring, tracking, documenting, and controlling the entire production lifecycle. Much is automated, but humans play a critical role. Their intuition and experience augment the software's capabilities and contribute to creative problem solving.

Access to a plant's MES must be tightly controlled. Unauthorized users may inadvertently or intentionally alter production parameters, schedules, inventory levels, or other sensitive data leading to costly issues. They may also infect the software with ransomware. Renault Nissan is just one of countless manufacturers that have suffered a cyberattack. In 2017, it was forced to temporarily halt production at five plants, incurring losses estimated to be as high as $4 billion.[1]

The Zero Trust model is growing in popularity as a means to secure networks supporting MES platforms. It requires authorization and authentication of all users each time they interact with software. However, requiring operators to repeatedly enter passwords or scan credentials while doing their jobs is inconvenient and may interfere with performance continuity.

Biometric identity solutions are ideal in this scenario. Using a computer's embedded camera or attaching an encrypted biometric reader to verify the user's face or iris can continually validate that only authenticated users are accessing the network. If a worker temporarily steps away from their post, an unauthorized worker cannot continue in their place.

Quality control requires that materials, supplies, and finished goods be kept secure throughout the production cycle. Physical access control reduces the potential for theft or product tampering. Biometric credentials, used alone or as part of multi-modal authentication, raise the level of security to a higher level.

Companies that manufacture pharmaceuticals, biotech, semiconductors, and microchips must maintain clean-room environments in which access control is critical. With biometric readers, suited-up workers can verify their identities with just their eyes, leaving badges or other IDs outside the controlled space.

[1] Manufacturing Cybersecurity Statistics 2022 [Recent Cyber Attacks, Threats, Risks in Manufacturing Industry] (ecsoffice.com)

INTELLECTUAL PROPERTY

In today's digital age, intellectual property theft most likely occurs through a cyber breach. The risk isn't just from hackers. With unfettered network access, employees can locate documentation of their companies' manufacturing secrets: product plans, designs, recipes, schematics – whatever elements make their offerings unique. One such breach occurred at DuPont in 2007. An employee downloaded over 20,000 abstracts from the company's data library, including information on the company's primary technologies and products under development. He ultimately served an 18-month prison sentence and was fined $44,500 – a token compared to the estimated $400 million+ market value of the technology he illegally accessed.[2]

The same security precautions applied to a manufacturer's MES platform should protect the company's entire network. As previously explained, Zero Trust enforces strict identity authentication and authorization of every user on every device, whether inside or outside the organization's network. For office workers with the luxury of hybrid attendance policies, biometrics can ensure their use of applications and files from home is as secure as at the plant. A camera or reader attached to their laptop repeatedly verifies their identity as they access network resources.

Some intellectual property breaches still occur the old-fashioned way. Someone snaps a photo of a prototype or sneaks it out of the facility. For these reasons, physical access control is also essential. Biometric credentials harden access to highly secure areas where valuable intellectual assets reside.

[2] Biggest Manufacturing Industry Cyber Attacks | Arctic Wolf

OPERATIONAL EFFICIENCIES

Biometric solutions can save manufacturers money and streamline the administration of employee identity programs. They can also create a more convenient environment for workers.

Many plants are continuous process operations, with workers reporting for one of three eight-hour shifts. Biometric time and attendance solutions can dramatically reduce the time needed for employees to "punch in and out" while eliminating time clock fraud and buddy punching.

For HR teams, biometrics provide an easy and economical way to credential a large workforce. Some solutions allow for self-enrollment, allowing new hires to begin onboarding from home using the camera on their phone. When they arrive on site for their first day of work, HR has less work to do getting them set up.

With biometrics, administrators are freed from the hassle of issuing replacement credentials for employees who lose theirs. They can stop stocking large quantities of fobs or key cards. Plus, less plastic ends up in landfills.

Linking biometrics to point-of-sale systems can speed up cafeterias and vending machine lines. For workers on 15-minute breaks, this convenience translates to coveted time to eat or relax.

Efficiencies extend to visitor management, which can be a time-consuming responsibility for security and operations teams. Integrating biometrics within a visitor management platform can automate registering first-time and one-time visitors and make their movement throughout the facility more convenient and secure. The same technology also speeds entry for repeat visitors who have been preauthorized with limited access at designated times.

SUMMARY

Advances in robotics and artificial intelligence have led to great advancements in manufacturing processes, but have also opened the door to a new range of security threats. Identity verification of anyone involved in the manufacturing process, regardless of role, is fundamental to maintaining the safety of workers, protecting the supply chain, securing intellectual property, and ensuring quality control. Biometrics are the most convenient and most secure way to verify the identities of employees and visitors at manufacturing facilities, and anyone who accesses the company's network or computer systems onsite or remotely.

As automation continues to drive advancements in the manufacturing sector, biometrics will help automate the processes that allow humans to work seamlessly and securely side-by-side with the industrial technology transforming the economy.