Schneider Electric White Paper:

The Value of Biometric Technology in Protecting the Security of Your Plant and Workforce

By Selin Yilmaz, Product Manager, Schneider Electric

We've all seen movies that show FBI agents scanning their fingerprints to gain access to highly classified situation rooms. Did you realize, though, how widespread that technology is becoming throughout society, and how it can help your plant not just reduce risks but save money?

Industrial factories face a range of threats. In extreme cases, they include terrorist attacks at chemical or food plants that could harm millions of people. But all plants also face the possibility of revenge attacks or random acts of vandalism that could halt production, disrupt your supply chain and harm your bottom line. It's critical for plants to limit access to sensitive equipment to only authorized workers, yet while we quickly list security as a top priority, it's rarely considered throughout the day.

So how effective is your security system? How difficult would it really be for someone to gain access to sensitive areas, machine functions or even just one piece of equipment where they could cause significant harm, if only through inexperience or lack of training?

Passwords, swipe cards and pin numbers have been the standard security approaches, but they can easily be lost, stolen, borrowed, guessed or forgotten. And each time a password needs to be reset, or a card needs to be reissued, it takes time and money. For instance, according to industry experts:

- Up to 40 percent of all calls to IT help desks stem from password problems.
- The average cost of each password-related call ranges from $10 to $31, and each year, companies can expect an average of two calls per worker.
- Companies each year spend $80 to $100 per worker trying to maintain secure passwords.

Unauthorized use of a machine can be even more costly when it results in worker injuries or even deaths. That's why the most effective approach to security – and long-term, the cheapest solution – may be biometrics.

From airports to the Olympics

Biometrics identify people based on their unique set of traits, such as fingerprints, voices, retinas, irises, facial features or the shape of their hands and palms. Throughout history, for example, no two pairs of fingerprints – not even those of identical twins – have ever been found to be alike. And even as people get older, the relationship between the ridges of their fingerprints does not change, just like a picture on a balloon remains recognizable both before and after it's inflated.

While some employees may be initially concerned about sharing such personal information, the public has grown increasingly comfortable with the technology. A Unisys survey in December 2008, for example, found that more than 70 percent of respondents would trust banks and government to use biometrics to confirm someone's identity, thanks largely to its frequent use by law enforcement. Seventy-two percent said they would prefer using fingerprints as the primary authentication method, nearly as many as the 73 percent who preferred passwords.

In 2009, biometrics is a $3.42 billion industry, according to the International Biometric Group, a New York-based consulting firm. That's nearly three times as much as it was worth in 2007, according to some estimates, and by 2014, it's expected to surge to $9.37 billion. It's easy to see why. Consider:

- The airports in Charlotte, N.C., as well as JFK in New York and Logan in Boston, have used iris-recognition technology to verify the identity of airport and airline workers. Travelers have used similar systems at other U.S. and European airports, and at the Sydney airport in Australia, passengers can confirm their identity through face-recognition technology.
- Students in England scan their fingerprints to borrow books, buy lunch and sign up for classes.
- At recent Olympic competitions, Germany required visitors to scan their fingerprints and provide other biometric data in order to access the central meeting place for its athletes, families and guests.
- Banks in Japan require ATM customers to have their palms scanned. The process verifies identities based on the patterns of the blood vessel in a person's hand.
- To implement the new system of electronic health records in the U.S., many medical clinics and doctors are requiring patients to have their palms or fingerprints scanned.
- Iraqis must provide an iris image and fingerprints to access U.S. facilities.
- Israelis have been debating a switch to a biometric database that would use fingerprints on passports, identification cards and other documents.

To be sure, no security system – not even biometrics – is perfect. In isolated instances, hackers have forged fingerprints or even the appearance of their eyes. But there's little debate that biometrics are more effective than either swipe cards than can be lost or borrowed, or passwords that people often jot down near their desks, share with others, or choose based on something that's easy enough to figure out.

In one high-profile case in 2004, for example, an FBI computer consultant used software commonly found on the Internet to learn the secret passwords of the agency's director. The consultant navigated his way into the deepest reaches of the FBI's internal network.

Need for industrial biometrics

So why use this gee-whiz technology in an industrial plant? Think about the areas of your plant where you'd most want to restrict access. Areas with specific or dangerous processes, or where machines are serviced or set up. Areas where you keep equipment that switches machines to maintenance mode or resets emergency stops. Access to certain buildings, rooms and equipment, such as garage doors, or to control changes to parameters in PLC programs or limit who can download data. And what about the areas with key-operated switches, badges, codes and passwords and other costly security methods?

Think of what could go wrong if your plant had a security breach. Think about the risks for the people who work with the machinery, the downtime it would cause at your plant, the damage that could be caused to products being manufactured and the headaches for your business that would surely ensue.

Schneider Electric, a world leader in push buttons, sensors and other control technologies, was the first manufacturer to introduce a biometric switch specifically for the harsh conditions of industrial environments. Activated by a fingerprint- reader, it's designed to provide a simple, proven and efficient way to restrict access to sensitive zones and machine functions, such as starting, adjustment and maintenance. Biometric devices can increase security for your employees, machines and systems, and lower operating and administrative costs. The Schneider Electric switch is also the only biometric device designed to protect against unauthorized use of industrial equipment.

That's important, because while the technology is similar to those FBI movies, this isn't a system designed to protect a data center or a room with top-secret documents. In an industrial environment, you experience extreme temperature variations, exposure to dirt, oil, water and corrosive chemicals, potential damage from lift trucks and other machines banging into equipment, not to mention operators who either don't know or don't care about security procedures. In this kind of environment, biometric devices must be "industrially hardened" so they can handle whatever happens all around them.

For companies and their plant engineers, maintenance workers and operators, biometrics provides an additional level of security that really delivers peace of mind.

To learn more about biometric switches and other innovative control solutions from Schneider Electric, please visit www.us.schneider-electric.com

Document 0100DB1014