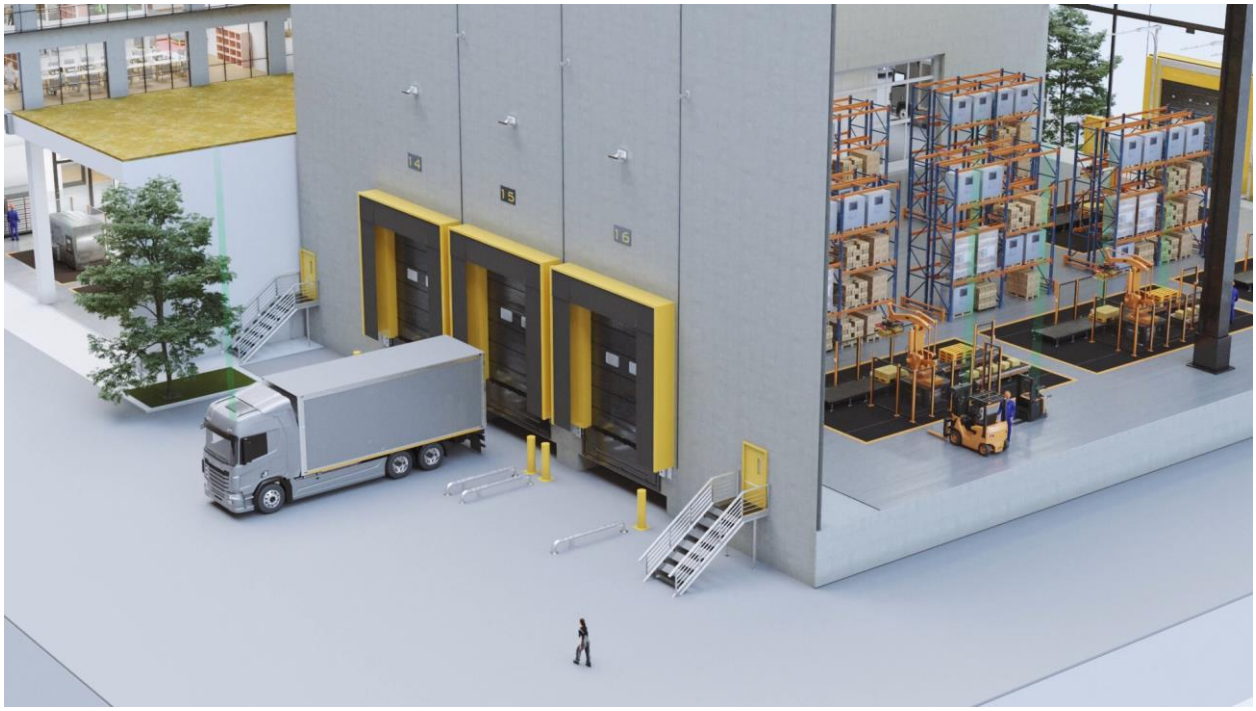
ELATEC
RFID Systems

AUTHENTICATION IN THE NETWORKED FACTORY

Protecting people, infrastructure and data in modern production environments



In modern factories, increasing networking and automation are opening up a wide range of opportunities to increase efficiency and productivity. However, digitalization also brings new challenges in terms of safety. After all, any disruption can have serious consequences in such a complex environment. An intelligent authentication solution makes an important contribution to protecting people, infrastructure and data.

Today's highly automated production facilities use advanced technologies such as the Internet of Things (IoT), artificial intelligence and data analytics to connect manufacturing processes and equipment, enabling seamless communication and data transfer. Through the use of sensors and IoT devices, huge amounts of data are generated and analyzed to maximize efficiency and quality. Current data from the International Federation of Robotics (IFR) is the best evidence that this development is finding its way into more and more factories: Around 72,000 new robots were put into operation in EU countries in 2022, an increase of 6% on the previous year.

Safety challenges in the modern factory

Despite all the benefits, intelligent production environments also bring with them new security risks. Cyberattacks are one threat. The networking of machines and systems offers attackers numerous entry points to penetrate the factory network. If security precautions are inadequate, hackers can not only disrupt production processes, but also steal valuable business data and intellectual property. There is also a potential risk from within the company: if, for example, untrained employees gain access to the systems, a human error can have serious consequences, including security risks and production downtime. However, security is not the only consideration when it comes to transparency into who has accessed devices or systems, at what times, and for how long. Plant managers also need this information to increase operational efficiency and optimize plant processes.

The employee ID card is generally used as an identification medium in production -but smartphones can also be used.

All-in-one authentication

Reliable security measures are crucial in order to manage the aforementioned risks and create transparency. An indispensable part of a comprehensive security strategy is a powerful authentication solution that regulates access and entry and reliably restricts it to authorized persons. In reality, however, there are often a large number of different authentication systems in a production environment. Employees juggle multiple passwords and PINs, physical keys and authentication systems. This leads to password fatigue, inefficiency and, ultimately, an increased risk of security breaches. In addition, IT staff are faced with managing multiple systems. This increases the workload, which means security risks can be more easily overlooked.

An all-in-one authentication solution based on Radio Frequency Authentication (RFID) and the mobile technologies Near Field Communication (NFC) and Bluetooth Low Energy (BLE) offers an innovative approach to the protection of industrial facilities. It can cover a wide range of applications with one system. The spectrum ranges from machine authentication and logging into the company network to access to sensitive areas or payment in the cafeteria. A standardized system can cover all access and entry requirements in a factory. In production, the existing robust employee ID card is usually used as the identification medium. However, smartphones can also be used as an authorization badge if required.

A powerful authentication solution that regulates access and entry and reliably restricts it to authorized persons is essential for a security strategy.

Success factors

The selection of a flexible and scalable system that is tailored to the individual needs of the company is crucial for the long-term success of such an authentication solution.

The following aspects must be taken into account.

1. **Needs analysis**: Determination of the company-specific requirements for the authentication and access control system.
2. **Future-proof:** Only a scalable system with regular updates and upgrades is the right solution in the long term.
3. **Integration into existing infrastructure:** Seamless integration of the selected solution into the existing IT landscape.
4. **Flexibility**: Multi-frequency readers enable companies to use identification media with different transponder technologies.
5. **Training of employees**: Imparting the necessary know-how in dealing with the new systems and raising awareness of security aspects.
6. **Compliance and data protection guidelines**: Consideration of the legal regulations and compliance guidelines applicable in the respective country as well as the relevant labor laws that regulate the use of quality assurance and time recording systems.
7. **Continuous monitoring and optimization:** Regular review of the implemented solution for effectiveness and possible adjustments, if necessary.

A standardized authentication solution is essential for modern, networked factories as it reduces complexity and increases security. This not only increases productivity, but also minimizes the risk of plant downtime. At the same time, it creates a robust and future-proof basis for protecting infrastructure in the age of Industry 4.0 and IoT applications.

Author

ELATEC GmbH
Zeppelinstr. 1
82178 Puchheim, Germany,
Phone: +49 89 552 9961 0
E-mail: info-rfid@elatec.com

In cooperation with