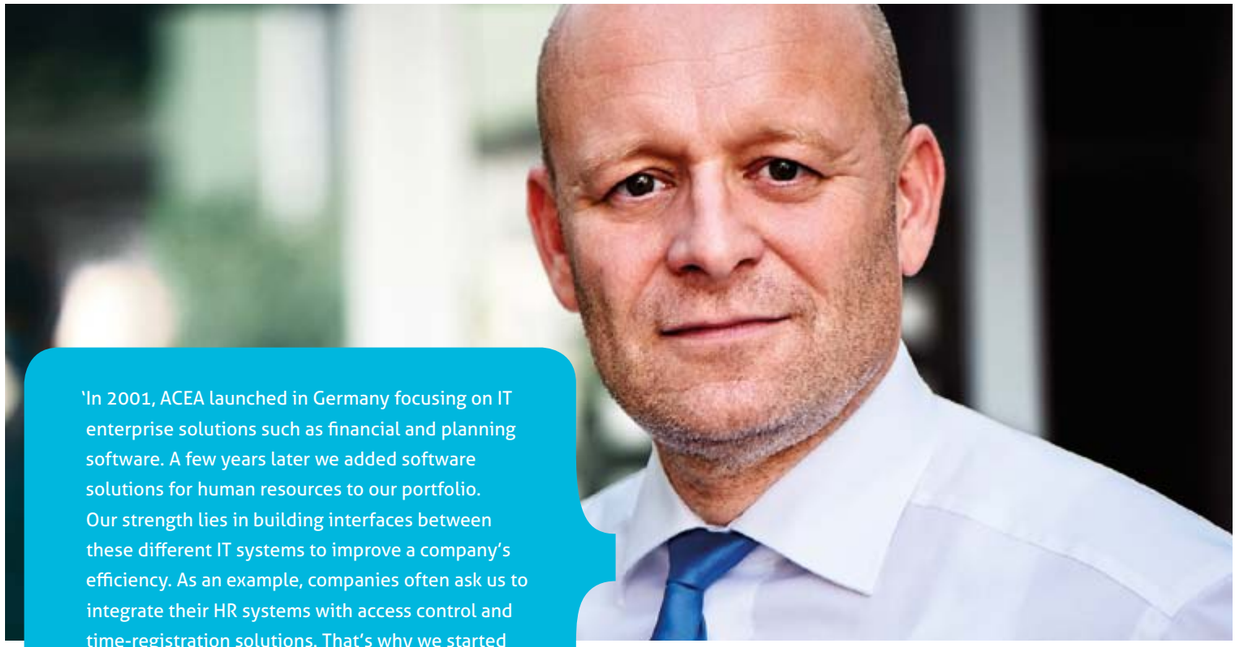

'In 2001, ACEA launched in Germany focusing on IT enterprise solutions such as financial and planning software. A few years later we added software solutions for human resources to our portfolio. Our strength lies in building interfaces between these different IT systems to improve a company's efficiency. As an example, companies often ask us to integrate their HR systems with access control and time-registration solutions. That's why we started searching for a suitable security system that could integrate with IT architectures easily. Nowadays, fifty percent of our annual turnover is derived from security solutions.'

ACEA
Dirk Kappert
Owner/CEO/IT specialist

The relevance of upgrade assurance

In the IT world, innovation moves quickly. New versions of software are launched every day to keep business processes running smoothly. So frequent upgrading isn't even a choice anymore – it's a must to avoid losing valuable time and data. Nedap sat down with Dirk Kappert, IT specialist and CEO of the German company ACEA, to ask him about the relevance of upgrade assurance. And how it applies to physical security as well.

by Maureen Hallers

Why do companies view it as a necessity to upgrade their IT systems but not their physical security systems?

In the IT business, upgrade assurance is very common. Because new software versions are developed every day, you need to upgrade frequently to ensure your systems keep communicating with one other. There's a clear difference between the worlds of IT and physical security in this respect. For instance, in the world of IT, hardware is less important. This is because software is developed to run on every kind of device. In the world of physical security, hardware still plays a leading role when selecting a system. Although practically all security controllers nowadays are IP-based, they're still pretty much always dedicated to perform one single functionality, such as access control. This makes many physical security systems inflexible and hard to integrate with IT systems.

Why is it relevant for a physical security system to integrate with IT systems?

In practice, customers often require smart integrations between IT systems and physical security systems. For example between an access control system and an HR system and intranet. The benefit of this is that you only have to enter a new employee's personal data, for example, into the HR system and you can automatically import it into your access control system to create a card for them. You don't have to enter their personal data twice in different systems, so the chance of making mistakes is lowered.

What difference does upgrade assurance make?

Ninety percent of our customers have a service agreement with us to provide upgrade assurance. We visit them once a year to upgrade all of their software and, very often, we link their access control system to their IT systems. Because if we don't upgrade their access control along with the rest of their IT systems, it can easily cause miscommunication between systems, meaning their security is compromised. Regular upgrading not only ensures all systems communicate correctly, it means our customers always have the latest new features, so their security is always up-to-date.

And what about the ten percent that don't choose to include upgrade assurance in their service contract?

Some customers don't opt for it at first because they don't think they need it. But the complexity of today's IT world has greatly increased. To obtain exchange of data between a physical access control system and other systems such as SQL Server and interfaces, updating an access control system is mandatory. That's why upgrade assurance in physical security is just as relevant as in the world of IT.

What characteristics should a physical security system have to ensure it integrates easily with IT systems?

When selecting a physical security system to add to our portfolio of IT solutions, we looked at database structures and the role of software and hardware. When we checked Nedap's AEOS system, we found its principles are very similar to those in the IT world. For example, the system is based on generic IP-controllers in combination with behavioral software components. This makes it possible to build a system according to a customer's specific requirements – a bit like Lego. Some time ago, a customer asked us if we could add Airlock functionality to a complex entrance situation. He'd already asked his access control supplier for the cost to develop this and they quoted 40,000 euros.

With a system like AEOS, which is based on software components, we could have just configured a software solution that he could adapt himself. This would have cost less than 10 percent of the price. So AEOS is as beneficial to customers as it is to us; maintaining it is easy and cost-effective. We're truly happy being a certified Nedap Business Partner.