

Security Magazine

1st edition - 2008

TMF: The challenge of a worldwide project

The world wide implementation of the AEOS Security System
for the financial management firm TMF

Security Management at Geneva Airport

Airport secured with AEOS solution from Nedap

nedap®

Table of Contents

1st edition - 2008

Trends

The future of integration	3
---------------------------	---

Case Studies

TMF: The challenge of a worldwide project	5
Saertex: High-tech security for high-tech companies	8
Geneva Airport: Security Management at Geneva Airport, Switzerland	10
Erkert: a new access control system for a high-tech automotive supplier	12

Solutions & Products

Product Preview

AP6003 IP Reader	13
------------------	----

Product Indepth

AEOS faces - tutorial	14
Convexs reader series	17

Solutions

New AEOS features	16
User Style Sheets	17
Security at your fingertips	18

Reader Service

Nedap N.V. Security Management
Marketing & Communications
Phone +31 544 471 743
Fax +31 544 46 42 55
E-mail info@nedap-aeos.com

Reproduction is subject to permission
from Nedap Security Management.

Nedap®, AEOS®, AEOS faces®, etc.
are registered trademarks of Nedap N.V.

The future of integration

The Security Management market was created when the first products were introduced that automated certain tasks that were previously done by human security guards. The first automated intrusion detection systems were aimed at reducing the number of guards needed to protect a facility. Automated access control systems replaced guards by automatically checking credentials against a list of authorizations. The advent of these types of systems has led to significant savings on man guarding.

But this trend has also led to the disintegration of the different security functions that used to be combined in the security guard. Everybody expects a guard to visually inspect a building when he has heard the sound of broken glass. And to switch on the lights if he suspects that someone has entered the building. If he smells smoke he has to switch off the ventilation and open up the doors so that everyone can leave the building quickly. This way of working has always been very scalable and robust. Just by adding more guards more facilities can be covered without one single point of failure.

The latest trend in the Security Management market is back towards a fully integrated system. In fact, the good old human security guard is now often seen as the ultimate level of integration. Of course, this time the security integration is achieved by applying the latest technology. In this article we discuss what steps need to be taken to get back to this high level of integration.

Three levels of integration

In the current Security Management market three levels of integration can be distinguished:

- Server Level integration
- Controller Level integration
- Sensor Level integration

Server level integration

The most common form of integration is what we call Server Level Integration. Each security function like access control or intrusion detection is in fact handled by a fully standalone application with its own server, controllers and sensors. Using a software interface at the server, information regarding events and status can be sent to an overlying Security Management System. Also, commands can be sent to the underlying system eg. for opening up a door or for arming an intrusion zone.

The big advantage of this approach is that for almost all access control systems, intrusion detection systems or CCTV systems, such software interfaces are available or can be created. However, these software interfaces can be very complex and need to be maintained. Also, by integrating at server level a single point of failure has been created. If the software interface fails everything fails. Also, in case



of a large scale emergency those interfaces can easily be swamped with thousands of events. And a timely reaction on an event or command cannot be guaranteed.

Controller level integration

In recent years some manufacturers have developed a new form of integration. This is what is called Controller Level Integration. Two different controllers (for example one for access control and one for intrusion detection) are connected over a serial or TCP/IP interface and can exchange events and commands. Thanks to the distributed character, this type of integration is very scalable and robust. Also, the amount of data send on the connection is limited. Therefore the complexity of the integration is far less compared to server level integration and significantly less maintenance-prone. However, since these controllers are still equipped with processors with limited performance the integration will not be very sophisticated nor flexible. Also, Controller Level integration is usually done between different products of the same manufacturer making vendor lock-in a real issue.

Sensor Level Integration

With the latest generation of very powerful controllers a completely new approach to integration emerges. Taking a page out of the playbook of the PC-industry these new generic security controllers can be loaded with different software modules. Just like you install spreadsheet program and word processing program on one PC, both access control and intrusion detection software can be installed on such a security controller.

So, instead of using a separate controller for each security function one single powerful security controller does it all, significantly reducing the investment in hardware. All relevant sensors and actuators like readers, door monitors, door strikes, Passive Infra Red detectors and light switches can be connected directly to this controller. With a user-friendly graphical configuration tool the links between this sensors and actuators and the software modules can be made. The most sophisticated integrations like automatically disarming and re-arming intrusion zones during a guard tour become feasible. Using the PIR-detector to detect whether the lights can be switched automatically off when no-one is there is another.



Sensor Level Integration has many advantages. It is inherently scalable, very reliable, easy to understand very flexible and powerful. In our opinion this level of integration will be eventually the preferred way of integrating the required security functions. However, currently not many of these powerful controllers have been installed. So, any successful approach to security integration needs to be capable of handling all three levels of security integration in one single system.



The challenge of a worldwide project

A powerful personality and experience are necessary to execute a world wide implementation of a security system. To draw up a corporate security policy and implement it as well. To handle cultural differences without making concessions. Dick Kuizenga, director of European VIP services in Amsterdam is working on the worldwide implementation of the AEOS security system together with Nedap Business Partners for the financial management firm, TMF.

TMF is a genuinely global management and accounting outsourcing firm, with over 2.000 professionals working from 77 offices in 60 countries around the world. All offices are

company-owned to ensure the highest quality world-wide. 25 of the offices are already equipped with the security management system from Nedap AEOS, and the implementation continues to be successful.

Dick Kuizenga started his carrier with the military police and worked at the National Airport, Schiphol. The royal family was also secured under his responsibility.

In 1978 Dick Kuizenga started his own company in the hotel security branch. European VIP Services now has become a company with expertise in different areas, such as hotel security, event security and risk management. Furthermore European VIP makes business continuity plans for companies and also provides courses for document recognition. A varied product line with one purpose: making sure that people can be safe.

Implementation of a corporate security policy

According to Dick Kuizenga the reason that a company would want to have a single security system world-wide, is quite simple. "When a company expands fast and the customers' confidential information needs to be guaranteed, it is very important to be able to minimize risks, and to keep the risks involved under control. A single global security system enables you to be more efficient in arranging these necessities. If employees travel regularly between different offices in different countries, it is of absolute importance to arrange in advance who has access to which buildings and, even more important, to which information. With



multiple systems this is impossible. For example: has the fired employee really been deleted from the access control system and can we therefore be sure that he no longer has access to the offices? Also, evaluating the implemented security policy becomes easier with one single system."

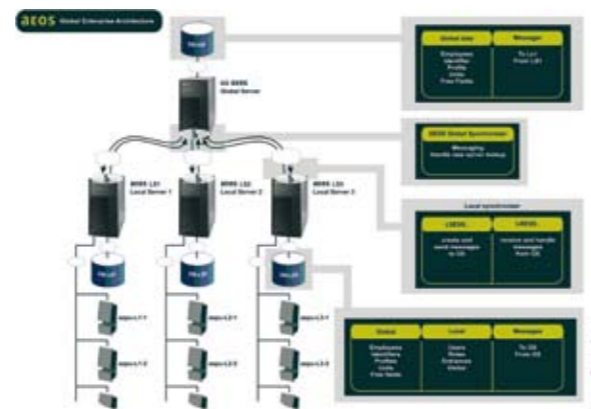
One may think that implementation of a world-wide security system is a lot of work. In fact, the contrary is true, continues Dick Kuizenga. "AEOS offers the possibility to divide authorizations by location or region, meaning that visitors and employees can be registered locally. The final check can still be done centrally and issued badges are verified from one central point. The AEOS users operate the web application via a standard web-browser. If the software needs to be updated, it is much more complicated if this has to be done for different systems in different countries. With a single system, it can be done in one go."

The corporate Safety & Security policy for TMF can be implemented in all the TMF offices in the world by using AEOS. Nevertheless, there are some aspects of any security policy that can not easily be implemented in a security system. For instance, searching for locations for new offices involves a detailed environment investigation to exclude external risks, such as dangerous companies in the neighbourhood, as much as possible. Furthermore the security system at TMF is extensively supported through reliable locking, fire detection and smoke detection. Important and vulnerable spaces or rooms, like a server room, are protected via additional measures.

Risks

Dick Kuizenga suggests that their single global security system, AEOS, controls and minimises these risks. "The central server of TMF in Amsterdam fulfills a very important role. The AEOS controllers in the different time zones are connected with this server through network connections. However, if one of these connections is interrupted, this

does not have any consequences for individual offices. Locally, one can always unbolt doors or activate alarm systems via the AEOS system. AEOS also makes sure that the different locations function properly. Possible defects at UPS or electronic locks are reported and locations can be called upon to recover these."



The global Enterprise Edition for AEOS is especially designed for a global business environment with, amongst others, multiple sites in different countries, local administrators and shared information between different sites and servers.

The number of servers for TMF will be further extended, according to Dick Kuizenga. "We want to put in an extra server per continent to keep the risk of interrupted network connections to a minimum. This means that if the network breaks down, local users can continue with their work. The locally imported data is distributed via global servers, meaning that the servers in the different continents always have the necessary data."

Multiple Time Zones

Another important issue that is involved when executing a world wide project is multiple time zones.

Normally, the time zone where the central server is situated is the time zone which is reflected. AEOS is the first system that makes it possible to configure access templates in the local time zone. 7 O'clock in the morning in Hong Kong, really is 7 O'clock in the morning, whilst in São Paulo also the local time is reflected. This feature really improves and simplifies administering access templates. By event monitoring both the server and the local time can be showed and therefore prevents for mistakes.

Document Control

Refinement of the required information is really important in a worldwide security system. Because AEOS is able to connect intrusion, fire and video data locally, this information can also be centralised. For example, if an employee gives his/her authorised badge to another person, AEOS can check by means of a video camera if the person matches with the photo in the AEOS database.

Personalised and intelligent access badges and accurate document control are of great importance for a perfectly working security system. In 75 percent of the cases, the judgment of documents is not difficult if employees have had a good education in document control. Nevertheless, in 25 percent the documents are false, falsely acquired or look-a-likes. In the 27 countries of the European Union, where citizens have the right to move and reside freely within the territory of the Member States, there are 27 official passports. Accordingly, all employers in Europe should be able to verify at least 27 passports authenticity.

At the moment it is being investigated if the registration of visitor information can be improved for TMF. By connecting a document scanner in AEOS, information can automatically be taken from a document. Visitor Management becomes easier for receptionists and the risk of making mistakes can be reduced.

This is another step ahead to keep risks under control as efficiently as possible.

It is important that the impact on the organization should be minimized. With this as a priority, the organization and its employees can give as much attention to their customers as possible. The clientele from TMF may trust that everything possible will be done to guarantee that confidential informa-

tion will be treated as such; access control for employees and visitors of the office is an important link in this process.



Installation and support of a global security system

How can one support and install a global system in so many different locations in different countries in an efficient way? Dick Kuizenga suggests that:

"Nedap makes it possible, with its extended Business Partner network, to deliver both quality and an unambiguous solution. To make this possible, a blue print has been designed together with Nedap. This blueprint enables all the partners to reach the same quality. In practice, the partners differ from each other, for instance they are inspired by different cultures."

Nedap employs a Global Project Manager to level out these differences and to guarantee the quality and progress of the projects. In the countries where Nedap does not have business partners, these will be identified with TMF. Nedap then educates the business partners. Obviously, besides installation and configuration, the service is very important. Without a local partner, good service cannot be provided.'



Facts TMF

- Headquartered in Amsterdam
- 77 offices worldwide
- Active in 60 countries
- 2000 employees
- AEOS Security System in 25 offices

High-tech security for high-tech companies

A pure idyllic place in Saerbeck, Westfalia. There is little to point to the fact that a leading German high-tech company has its headquarters here.

Well secured behind gates and fences, **Saertex GmbH & Co. KG** develops and manufactures, amongst others, the most modern reinforcing materials for the aircraft industry.

Over 33,500 square metres, technical fabrics made of glass, aramide and carbon fibres are manufactured here. As well as being used in the Airbus, these materials are also manufactured for the aircraft, boat and shipping industries and for wind power installations. With its 350 highly-qualified employees, the company's achievements were recently marked by receiving the JEC Innovations Award in the Energy & Industry category in Paris. This know-how, of course, needs to be protected. Last year Saertex' managers therefore decided to re-structure the entire access control system.



Convincing presentation

For this purpose the HR department, the security service and system house GED (Gesellschaft für Elektronik und Datentechnik mbH – Electronics and data technology company) developed a concept involving various security rings. The outer ring around the company's site consists of barriers, fencing and a roller gate. High security areas – for example the development and data processing department, laboratories, the server room and store – form the innermost circle. "Reliable access control is the basic prerequisite for all other

security measures", explained Stephan Stappers, the Saertex HR Manager. "After contacting several potential suppliers, we ultimately decided for the Nedap AEOS® security management system." There were numerous reasons for choosing this system. Stappers said: "For one thing it is user-friendly. We can also expand it if necessary, without having to invest again in basic components. But in the end, personal service and the live demonstration at the Nedap headquarters in Groenlo in Holland convinced us." Of course technical performance data also played a part: the wide pick-up bands of the aerials, for instance, which means that one badge can operate the doors as well as the barriers, and the remote control/maintenance via TCP/IP. Since identification of the badges takes place in the protected area, technical defects, vandalism and manipulation of the readers are minimised. Being "well-connected" creates security – and this does not only apply to the inclusion of readers and the evaluation unit, but also the co-operation of the firms involved.

The identification process of AEOS® is based on its 120 Kilo-hertz technology. The multifunctional badge activates access control and time recording at the same time. It is used as an employee badge and the barcode printed on it is used for machine data records, production planning and goods information systems. The variety and individuality of the aerials used is impressive. This ranges from type DC 130 detection aerials with a reading distance of ten centimetres for sliding doors and security areas up to T-bar aerials DCI500 with a range of 150 centimetres on both sides of the barriers in the approach area. In the main entrance to the administrative block, disc aerials (DCI005) with a range of 50 to 80 centimetres are used. A reader which "swallows" or retains visitors' badges is used by freight companies and external firms, and guarantees that the duration of their visit can be determined precisely and the sliding gate is controlled. When it is inserted, the badge is read and then invalidated. A total of 35 readers and twelve controllers are in use; the headquarters are connected with two companies and the subsidiary in Stade.

Strict visitor administration

The new access control system has also enabled Saertex to implement strict visitor administration. Suppliers, installers or service personnel receive visitor badges with varying authorisation levels. This means that for every person who has entered the company's site, information is available: when and where they requested access and how long they stayed on the company's site.

The card design was created with the Card Designer integrated in AEOS®. Using the AEOS® Import Tool, 350 images can be allocated to employees within a minimal of time. It only took a few minutes per employee for the full process of printing cards using the Card Designer, including taking the photo, personalising the card and printing it on a Retransfer XID 570 ID card printer.

Linux based

The Saertex HR department is responsible for the administration of the system; visitor administration is done at the central reception. There are ten different access templates in total with subordinate access groups, for instance production, management, general access to senior management and visitors.

The intelligent controller in the AEOS® access control system is based on the Linux operating system. The AEOS® management server, the configuration module and the MS-SQL database are installed on an MS Windows 2003 Server. The user front-end is fully web-based. The AEOS® server is operated together with six other virtual Windows servers in a VM Product 3-environment. The basic operating system for the VM Product Server is thus based on Linux. "This reduces IT energy consumption by using less hardware and requires less cooling, which in turn means less energy is consumed," explains Heiko Stahnke, system administrator with Saertex.

Moreover, the concept was implemented in only a few months. The first contact between Saertex and GED took

place in August 2006. After acceptance of the bid in December, only three months were required for full installation, configuration and training. "Such a project is a living thing. But as the system can be flexibly adapted to new requirements, no problems occurred," said GED Managing Director Martin Sindermann. The system has been up and running since April 2007. At the start of the changeover, there was a certain reluctance on the part of employees in relation to the access control implementation. Co-operating with the plants' Council and a poster campaign providing continual information to employees ultimately promoted understanding about the necessity for the measures. "However, you can lose the acceptance won in this way within a day if you cannot deliver what is promised." Mr Stappers acknowledges.

He was all the more pleased that the changeover of time-recording terminals to Nedap XS readers carried out during a shift change and commissioning of the access controls went completely smoothly – not a single "stamp" was lost. Employees themselves were only aware of the change because of the change in ID passes organised in advance.

Nedap N.V.,
www.nedap-aeos.com.

Saertex GmbH & CoKG
www.saertex.com

GED mbH, Emsdetten,
www.ged-mbh.de

Published in Protector 09/2007
Editor: Hagen Zumpe

Security Management at Geneva Airport, Switzerland

Airport secured with AEOS solution from Nedap.



Aéroport International de Genève, the second largest airport in Switzerland

AIG, Aéroport International de Genève, is one of the most dynamic airports in Europe. In 2006 alone it handled almost 10 million passengers and 170.000 flights to 100 destinations, serviced by 150 different companies. Obviously, with these figures, security is an important issue and needs to be up to standard at all times.

The implemented AEOS system controls the access of a workforce of 13,500, manages 37,500 badges, 60 shops and 150 organizations working at the airport's facilities. Securing and controlling such a dynamic environment requires a flexible access control system, based on state of the art technology which is able to meet present demands as well as future security requirements.

AEOS

One of the main reasons for AIG to choose Nedap AEOS as its security management system was its structural different architecture based on behaviour components. AEOS behaviour components allow the system to support and enhance the airport's security policy and procedures. Furthermore, changing requirements can be put into effect much more easily.

Another reason to choose AEOS is its capability of simulta-

neously handling multiple reader and credential technologies in a single system. The implementation took place through the Swiss certified business partner of Nedap: Tyco Fire & Integrated Solutions.

Different card and reader technologies in a single system

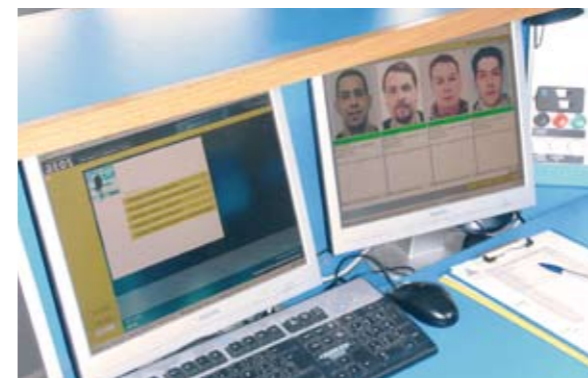
Four different identification technologies are used simultaneously in the AEOS access control system at Geneva Airport: Nedap, Mifare, Legic and Magnetic stripe, each technology serving a different purpose. The Nedap Combi card has been put into place, which combines all the required technologies, therefore increasing convenience for the users, as they do not have to carry four different cards.

Nedap technology is used for convenient hands-free access (up to 1m) for people, and long-range reading distances for vehicles. Vehicle identification at the premises is achieved via the Nedap TRANSIT long-range reader and compact tag, which detects vehicles up to 10m away. Mifare technology is used, amongst others, for data transaction purposes, e.g. secured storage of biometric templates in the Mifare chip. Legic technology is applied to preserve previous investments in the field of access control. For vending purposes, a magnetic stripe has been added to the Combi card.

Contractor, Vendor & Permit Management

The majority of AIG's workforce is employed by the 150 companies operating at the airport. A considerable amount of time is required to manage the flow of people and access rights of the people (contractors) working for these companies (vendors). The contractors are to be managed and separated from AIG employees. For the airport, it is important to separate the access rights and events/alerts generated for each category of persons in the access control system. Furthermore, the access rights for contractors should be blocked automatically once they have finished their job and/or once the vendor's permit has expired. The AEOS software features contractor and vendor & permit management provide a good solution. Contractor ma-

agement distinguishes contractors from employees and visitors. The contractors' person data are linked to the applicable vendor information and a contact person, usually an employee. Vendor management registers the applicable vendor data and links the vendor to a permit. A permit determines how many and which contractors are allowed to work on this permit, the type of work it is issued for, and the validity period. Once the permit's validity has expired, all the contractor's access rights are automatically blocked.



Visitors at Geneva Airport

A strict security policy is in place with regards to visitors, as they are not allowed to walk around freely. They must be accompanied by an authorised employee at all times and will only receive access to certain areas in the employee's presence. Only a certain, selected group of employees are allowed to accompany a visitor. This security policy is enforced via the "two men rule", which means that a visitor badge should only be accepted when an employee badge is presented at the same reader within a certain time frame. Thanks to the AEOS behaviour components, this specific security policy is easily put into effect. AEOS verifies the authorisation that is granted to the visitor and determines whether the employee is authorised to guide a visitor. When these conditions are fulfilled, both visitor and employee will have access.

Extensive monitoring

At AIG, different security levels apply depending on the facilities zone or area. Certain areas have a high security level and are equipped with a 24/7 manned security desk. Whenever a person wishes to enter such an area, he or she must present his/her badge at the applicable reader at the security desk. Once AEOS has verified the authorisation's validity, a display above the desk indicates whether the person is granted or denied access. At the same time, the security guard monitors via AEOS the person's data, photo and authorisation validity: checking that the person is really the rightful badge owner. The AEOS photo event feature instantly provides the security guard with other relevant information: persons name, department, personnel number, reasons for not being authorized, etc.

As a matter of policy, employees, contractors and visitors have to wear their badge visibly at all times. For visual identification and authorization purposes, badges have different colors which tell the security guards which areas of the airport these people have access to. With the Nedap GPRS hand-held scanner, patrolling security guards can read a person's badge, verify its validity and find out the persons last movements.

Facts and Figures Aéroport International de Genève

- 10 million passengers annually
- 170 000 flight movements
- 150 organisations and 60 stores
- 13.500 employees (Incl. contractors)
- 37.500 badges
- 200 Nedap readers
(to be extended to 400 in the near future)

A high-tech automotive supplier gets a new access control system

The Swabian automotive supplier Erkert specialises in processing steel and aluminium to make customer-specific precision parts and components. The company's structure, which has grown over the time, has led to the company's property being scattered around different sites at Sulzbach an der Murr. A new access control system had to bring these different locations together and reflect the customer's shift patterns. The AEOS® System from Nedap N.V. is being used.



Access control & existing time recording

The company's continual expansion has led to the production shops being spread around the town. "On top of this, the real challenge, according to Dirk Kappert, Managing Director of the Ober-schleißheim company ACEA GmbH, in the "access control" project, lies in the fact that individual production units in Erkert have varying shift patterns which the access management system has to reflect both simultaneously and flexibly."

The new system therefore had to be able to connect various different sites and had to be integrated into the customer's own shift planning tool to maintain the existing reader infrastructure. ACEA GmbH has already installed a time-recording system at Erkert and the existing Legic transponders were now also to be used for access control. With the access control system used up to now, this could not be done.

Flexible and easy to maintain



The concept proposed by ACEA GmbH, explained Dirk Kappert, consisted of a flexible access control management system with low maintenance costs in a single place, with which external systems could be easily integrated. It was implemented using a security management solution from Nedap; AEOS® Enterprise. It is a web-based access control and security management system which can be accessed with any normal web browser independent of site and place and therefore ideal when the company's sites are scattered. AEOS works on the principle of "decentralised intelligence" and therefore functions securely independent of the availability of the network or the server. AEOS® is not only an access control management product, but also offers visitor management, vehicle identification and EMA functions, so that almost all the areas of a modern facility control software package are covered. One of the particular advantages of the Nedap solution is

the open strategy made possible by the database-supported system with which other systems can be integrated seamlessly, regardless of circumstances – such as time recording or staff resource planning. Erkert, for instance, has a complex shift planning tool for its various production shops which manages various shift patterns for different groups of workers and the various different plants – and with which

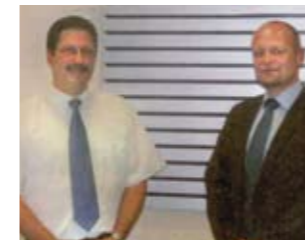
CNC automatic lathes, honing machines and multi-spindle machines stand in the plants of one of the largest supplier of turned parts in Germany, the company Hermann Erkert. These are special machines developed by the company, with which it can make capacity available for serial production, even at short notice. They are used to produce highly sensitive and complex precision parts, mostly to supply the car industry.

Customers such as Daimler-Chrysler, Bosch, FAG, Hilti, LuK, Siemens Automotive and ZF use these high-tech products which are supplied ready to fit and pre-assembled as parts for steering, brakes, pumps and injection systems in vehicles.

This highly modern machinery is located in the Swabian-Franken Forest national park – in the nationally acclaimed spa town of Sulzbach an der Murr, about 40 km north east of Stuttgart. Erkert is 50, somewhat like an exemplary solid middle-class resident of Baden-Württemberg. The firm employs a highly qualified workforce of over 850 men and women, and has a consistent commitment to training: every year 30 industrial technicians are trained in the areas of precision tools and light engineering.

access had to be linked. It poses no problem, for instance, if an employee's working hours have to be moved to the following day, in Plant 3, perhaps, instead of in Plant 1 – and to the late shift instead of the early shift, explains Dirk Kappert.

Implemented at lightning speed



Jürgen Frank, IT Manager at Erkert (left) and Dirk Kappert, Managing Director of ACEA GmbH, Oberschleißheim

For Kappert, what was particularly convincing about the Nedap system was the speed with which the project was carried out: within only one and a half day the existing Legic readers and the Nedap access control management system were linked together. The fact that the existing cabling infrastructure could be re-used was very helpful – not a single meter of new cable had to be laid. The customer benefits from this minimal project time, as the service component of overall investment costs thereby remains particularly low. The fact that external readers and aerials can be connected and the modular structure of hardware and software mean that the customer's earlier investments can truly be protected. Plus, the licences relate solely to the functions actually used – the customer therefore pays only for what he really needs and uses.

Complex system – user-friendly

Ultimately one of the main decisive factors in favour of the Nedap system for Mr Herr Jürgen Frank, Project and IT

Manager at Erkert, was the fact that it is particularly user-friendly and can be easily extended: the user interface "AEOS-faces" can be set up precisely according to the wishes and tasks of the relevant employee and his own operating processes. Security guards, receptionists and employees in the telephone exchange can all operate the system immediately without training. Overall a very flexible and functional access system was created - there is already a plan to expand it (by for instance including IP cameras to monitor the entrance).

Kester Peter Brands

Nedap Deutschland GmbH
www.nedap-aeos.com

Mr Dirk Kappert

ACEA GmbH, Oberschleißheim
www.acea.de

Published in GIT 07/2007
http://www.gitverlag.com
Editor : Matthias Erle

Solutions & Products

Create your own AEOS Interface



The new feature "User style sheets" in AEOS enables users to give AEOS their own personal look and feel.

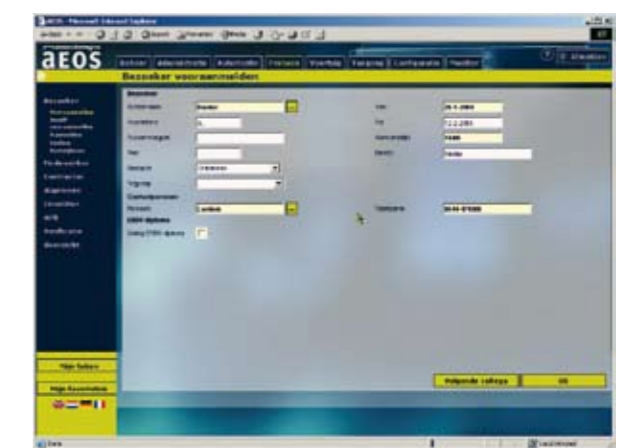


Where standard security systems have a standard interface with only limited possibilities to adjust it to personal preferences, AEOS now offers its users the possibility to create a customized interface to match, for example, their corporate style.



The look and feel of AEOS can be adjusted to the preferences of the user by changing the Cascading Style Sheets (CSS). CSS is a language that is used to describe the presentation of a document written in a mark up language. Its most common application is to style web pages which are written in HTML. With a little knowledge

of html-coding one can adjust the AEOS Interface to accommodate a companies' corporate style. Companies' logos can be added to the interface and the background can be tuned to the companies' corporate colors.





AEOS faces step-by-step easy configuration

The central focus of AEOS faces is the end user and the specific tasks to be performed by the individual end user. User friendliness and usability are the keys. Complex systems become easier to work with, and user errors are reduced significantly. This benefits productivity and security.

aeos | faces

New ways of looking at security management

AEOS faces supports each role within your organization with its own interface, designed for the specific tasks of the employees and to support the work process in a logical manner. For example, a receptionist has different demands of the system compared to those of your security officer or logistics manager. This system will adapt itself to the wishes and tasks of your employees, rather than the other way round.



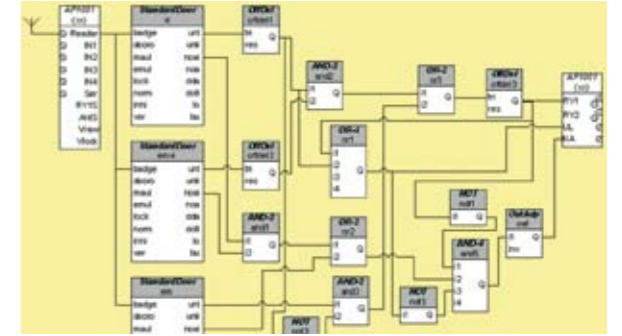
AEOS faces is designed to improve the operation for individual end users. But not only the end-users benefit, it is also simple to configure in a few steps.

In this tutorial is explained what a Face exists and what the possibilities are.



Step 1: design task based user-interface lay-out

Analyse the daily tasks of the user. Based on this you determine their ideal user-interface, with consisting of only the most essential elements.



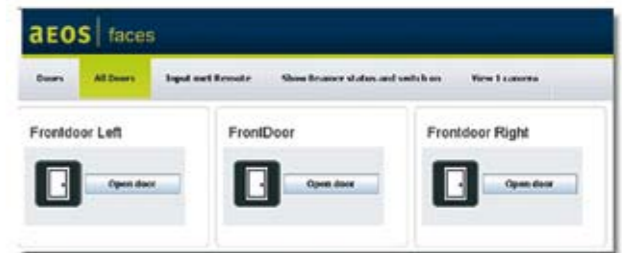
Step 2: Define needed components (e.g. camera, access point, etc)

Check from which systems you need information. Is it just the Access Control system, or would you also like messages or images from the database. Would you like to combine live images from camera's that are available?



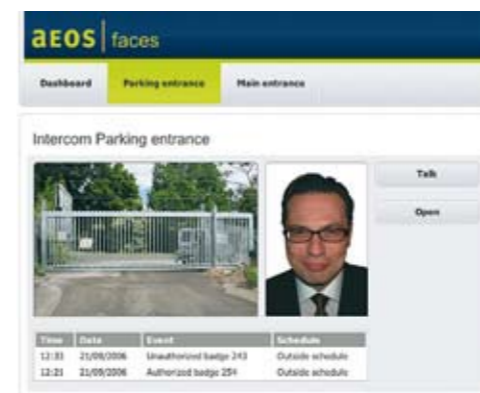
Step 3: Activate needed components

Of course you would like the buttons to reflect the actual status of the defined components. To do this you need to address them in AEOS and connect them to the status images in the graphical user interface.



Step 4: Combine multiple components

Now it's time to get back to your original design. Based on your drawing in step 1, you combine all the needed active components into one interface.



Step 5: Make a multidashboard

Of course one performs different tasks during different times of the day. During office hours one might have a Face that combines Access Control and CCTV to check visitors. After office hours one might like a face to check if all the doors are closed. Or a Face to check if all the lights are of. Therefore you can group different task based interfaces into one screen: a multidashboard.



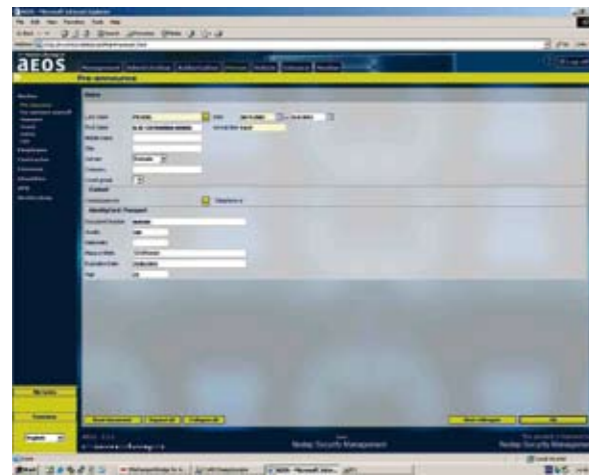
Step 6: Enjoy your coffee!

You're ready!

Features in AEOS 2.2

Keep your photos up to date in AEOS! With AEOS you can now give a limited validity to the photos in your security system.

For receptionists and guards it is often difficult to determine whether the person who is carrying a badge, really is the owner of that badge. Photos, printed on the badge and saved in the system can help to recognize the carriers. The problem with these photos is their transience, people change in the course of time and photos become outdated. Therefore the photos need to be updated every few years.



To solve this problem, AEOS 2.2 has been equipped with a new feature that allows users to set a limited validity to the photos attached to persons in their security management system. In the system properties a validity period can be set as a number of days. When this period is exceeded the user will

receive a message if he opens the persons' data screen in AEOS. The system will then ask for an updated photo. If the Data Card package and a photo camera are connected to AEOS, it only takes a single click on the button "take photo" to make a new picture. With these new features it becomes much easier for users to keep their security databases updated. It will definitely improve the recognition of badge carriers, which is an important aspect of a good functioning security policy.

Visitor enrollment within 30 seconds!!

With AEOS a fast and secure visitor enrollment is guaranteed. Enrolling employees and visitors into your security management system, can be a time consuming and cumbersome task. Especially if you take into account that

everytime you enroll a person, you should also establish the authenticity of his identity. Integration with a document reader (picture 1) has a lot of advantages and makes the enrollment procedure (not only for visitors but also for employees and contractors) fast and accurate. It basically works as follows:

- if an employee or visitor requires new access rights, his or her ID are asked for
- A document scanner checks whether the ID is valid or not. (picture 2)
- AEOS automatically fills the appropriate datafields. (picture 3)
- AEOS verifies the Violations & Blacklist for this person.
- AEOS Issues a badge.

Within approximately 30 seconds you can hand out new access rights, based on a thorough though fast enrolment process.

Extended Visitor Management

In AEOS 2.2 the Visitor Management procedure can be extended with even more options to secure your visitor management procedures.

In large offices there can be a lot of people going in and out of the building. Guards and receptionists somehow need to keep track of all these people.

For employees it's not that difficult to establish a day and time frame in which they are allowed to access certain areas. For visitors such as service mechanics or suppliers, however, it's a bit more difficult to narrow the timeframe in which they can use their access rights. Simply because you don't know exactly at what time during the day they will come.

To solve this problem, some new options are added in AEOS 2.2 that allow you to limit the access rights of people or vehicles without knowing the exact date or time of their visit. These new options are called Maximum Movement control and Maximum Time control. They allow the user to set a limit to the maximum number of movements in and out of a zone a carrier (e.g. visitor, contractor) is allowed to make or the maximum presence time. The system automatically checks if the maximum is reached. If the maximum is reached AEOS automatically generates an event.

This maximum number of movements can for instance be set in a situation when suppliers need to deliver goods at several places in your building. The supplier receives an access badge for the day but you do not want him to be able to walk in and out of the building the entire day. If you set a maximum number of movements according to the number of deliveries he has to make AEOS will generate an event if this maximum number is reached and, if necessary, the guard can check upon the supplier.

New: The Convexs Series

New reader series characterized by exceptional slim design and extensive reading options.



The new Convexs reader series are a fine example of Nedap's effort to combine the latest technological options into a smart and slim design. That design has been a prime driver in the development of the new reader series. The name, Convexs,

has been derived of the Latin word "convexus" and refers to the arched shape of the design.

Technology wise, the Convexs® readers incorporate the latest in reading technology. All models are equipped with three different configurable interfaces: Wiegand, RS485 and RF. Through the Wiegand output, the reader can be integrated into third party systems, which makes it extremely versatile.

There four different models with different reading capabilities or different mounting characteristics. The most complete model, the Convexs® MN80 is equipped with a dual reading technology print, suitable for both Mifare and Nedap credentials. There's also a more basic model, the Convexs® M80 that reads only Mifare credentials. Both the MN80 and the M80 read the Mifare CSN, Sector data, and support the MAD. All Convexs® readers are available in a surface mount and flush mount version. The

flush mount version has especially been developed to fit in a junction box. As an add-on special vandal proof protectors are available for the different versions of the Convexs® readers.

Besides its compact size and smart design of the Convexs readers, which are relevant to new installations, the Convexs reader can also be a great asset to existing systems. The Convexs® MN80, for example, enables smooth migration to Mifare card technology in both existing Nedap XS and Nedap AEOS Enterprise systems. Card populations can be migrated gradually since the Convexs® reader allows for simultaneous usage of both Nedap and Mifare credentials. Thus allowing the card population to exist of a mix of both Nedap and Mifare cards. This way Mifare cards can be issued, e.g. for temporary use by visitors or contractors.

Another major benefit of using the Convexs® reader in existing systems is that it leaves much of the existing installation in place. There's no need to replace existing controllers or antenna cabling does not have to be replaced.

With the Convexs® reader series Nedap provides a solution that perfectly fits in projects where smart design or ease of installation, secure Mifare or smart migration trajectories are key requirements.

NEW: AP6003 IP Access Controller



With TCP/IP technology getting less expensive and Power over Ethernet technology getting more advanced, the benefits of IP security devices become more and more apparent. To address the growing customer demand for a fully one tier Ethernet security solution, Nedap adds a new category of hardware to its range of IP based security solutions: IP Access Controllers.

The first unit in this range is the new IP Reader Interface: the AP6003. The AP6003 is a fully transparent IP reader that communicates via Ethernet instead of the CANbus. The power for the unit can be supplied via a traditional power supply or via Power over Ethernet. The AP6003 Reader Interface is developed to control two doors and has a reduced mode which, if the network fails, guarantees basic access control at all times.

With this new product Nedap offers its clients more flexibility. On the one hand there is the option to use the highly reliable CANbus communication for the communication between the controllers and the reader modules. And on the other hand, there is the option to choose a full Ethernet network solution in which also the communication from the controllers to the reader modules is over IP.

The advantages of this last option are the most obvious in places where clients like to use their existing IP infrastructure. The cost of security systems is for a large part determined by the installation and maintenance costs of the infrastructure. Research has indicated that cost reductions of up to 30% can be achieved.

The new AP6003 enables clients to fully optimize their investments.

Hands free identification up to 4 meters



Nedap introduces the TRANSIT Entry reader, the latest in technology for secure handsfree access and other RFID applications. The TRANSIT Entry reader offers handsfree person and vehicle identification up to 4 meters.

The TRANSIT Entry combines the convenience of traditional door automation with the security of restricted access. The TRANSIT Entry has great benefits, especially in situations where people cannot use their hands to present their ID badge to open the door, but where high security needs to be maintained.

Some applications are;

- Emergency rooms
- Disabled access
- Secure warehouse facilities
- Building access
- Gated vehicle access.

The TRANSIT Entry reader can be installed next to a door without the need for any additional mounting accessories or wiring. The reader can be integrated seamlessly in existing access control systems via Wiegand communication.

The TRANSIT Entry reader can be featured with an optional proximity and ISO compliant smartcard interface, which enables the reader to read standard proximity cards and smartcard CSN at short distances. The interface eliminates the need for multiple readers nearby a door or boom gates.



Security at your fingertips



Even in its most basic form, the AEOS Security Management system provides high-security access control unrivalled in the industry. And in an emergency you can manually override the system settings. But in today's world that may no longer be good enough. Nowadays, anticipation is key. You need to be prepared to respond appropriately to different crises and possible threats, without giving up control. This is where the new AEOS Security Level Management option plays a crucial role: pre-define emergency scenarios and activate them at the touch of a button.

Under normal circumstances our versatile, IP-based, AEOS Security Management software allows you to regulate employee and visitor traffic and keep close tabs on people's movements. But in case of an emergency, your only options are to lock or unlock all access points in the system. Either no-one can

get in or out, or everyone can; you relinquish all your carefully constructed control in one fell swoop.

But with our new Security Level Management option you retain control of access to your premises, even in a crisis. By pre-defining any number of scenarios you can switch to a different access mode in a matter of seconds. Security Level Management is ideal for large companies

operating in various locations, regions or countries; organisations with large and complex employee and visitor flows; and businesses that require extra security because of the hazardous or valuable commodities they deal with.

Security Level Management allows you to define your own crisis or threat levels and conditions. Imagine that there is a strike. Under normal conditions a facility might leave its inner perimeter doors unlocked. During business hours they only require presenting an access card at the outside doors. Now there's a risk of unauthorised people, such as the media, walking along with some of the employees. However, with pre-set security level scenarios you can quickly activate verification and check all 'direction in' on crucial access points. You could also specify that at some locations directors and technical staff can still enter presenting only their cards, while production


personel has to go through a more thorough check, such as verification. Scenarios like this one have a great advantage: they are entirely software-based and easily adjusted. They can also be activated with a few clicks of your computer mouse.

Another example is burglary or theft. Within seconds, security can activate a pre-set 'theft scenario'. This blocks all exits and turnstiles to anyone except police, who can only enter the building.

The AEOS Security Level Management option is based on freely definable scenarios. You can devise any number of scenarios to temporarily change the system's response to pre-defined groups of people. And best of all, these scenarios are literally at your fingertips: click on a few buttons and the scenario you need is active.

Security Level Management offers precision access in a crisis. And it is only a click away.





Can you account for all active badges that have gone missing?

Research has shown that from every hundred provided access badges 1 to 5% goes missing without being de-activated.

That is no surprise: people lose their badge, employee replacement badges aren't removed from the database or visitors simply forget to hand in their visitor badge. These irregularities are often unnoticed. With Nedap's security management system AEOS the access rights of any person can automatically be blocked once the assigned cards haven't been used for some time. **Take no chances. Nedap AEOS.**

nedap
aeos