INFORMATION

Essen, September 17, 2024

From perimeter to AI:

Trends in the security industry in 2024

Numerous exhibitors at Security Essen show their innovations

Innovations play a key role in the security industry. Artificial intelligence (AI) is one of the most important drivers of new technological advances, but digitalization is also advancing in other areas. Some of the most important trends are:

1) Artificial intelligence

With **ChatGPT**, developments in the field of AI have taken a big step forward. Machine learning is an integral part of many security applications, from video analysis to building automation. The networking of IoT (Internet of Things) networks, the analysis of large amounts of data and the detection and prevention of cyberattacks are no longer conceivable without the integration of AI.

Deep learning can be used to create non-linear, complex correlations within data sets, which requires large amounts of data for training purposes. Analysis tools that are integrated into the cameras themselves (edge computing) save data bandwidth during processing and increase process speed.

Dahua (Hall 5, Stand 5C14) uses **AI** in video surveillance with its WizSense series to precisely distinguish between people and vehicles, for example. Eagle Eye Networks (Hall 5, Stand 5C22) uses advanced artificial intelligence to increase the accuracy of video analysis applications. This is possible because the video management system is cloud-based and offers greater computing power than decentralized solutions.

Dallmeier (Hall 5, Stand 5B19 and Hall 8, Stand 8A15) is also using AI-based edge analysis in its Domera camera range to ensure that **AI object classification can be used for accurate results**. AI is also used in Reconeyez's **perimeter** protection solutions (hall 5, stand 5B24). Machine learning algorithms evaluate the data and only solve an alarm in case of a real, previously defined threat.

2) Cybersecurity

Virtually every digital development or technology today must be thought of cybersecurity. **Whether government, business or private use: cybercriminals pose a serious threat to everyone equally.** Ransomware attacks have increased in particular, which means that data is encrypted and decrypted for ransom. In the context of the Ukrainian war, sabotage and espionage efforts against military and economic targets also come to the fore and threaten critical infrastructures.

Here, too, **AI has long since found its way into the cybercriminal business**; it's never been easier to create malicious code with AI. Many activities can now be automated, such as sending, evaluating and optimizing phishing emails. **Cybercrime-as-a-service** is also booming, so the cyber attack on demand. The new possibilities of AI in terms of image and audio manipulation require more than ever that security service providers and their own IT security keep up with the pace. Fault gates represent all digitally networked components and trades, which is why manufacturers and fitters must pay equal attention to the safety of the produced and installed hardware and software.

TAS (Hall 7, Stand 7D31) enables a certified cyber-secure solution for remote access to all types of alarm systems with its TAS Secure platform. Rohde & Schwarz (Hall 6, Stand 6C39) develops and produces high-speed, highly secure network encryption and zero trust endpoint security.

3) The danger of drones is increasing

Drones are becoming more powerful year by year, both in terms of their flight characteristics and payload. **AI also plays a role here, because it can autonomously control individual or entire swarms or help in the detection and defense of non-cooperative drones.** The use of commercial drones in the Ukraine war shows the many uses and the difficult defense against the often small and very agile flying objects.

As the **UEFA Euro 2024** takes place, security authorities see drones as a potential threat and have their detection and defense on the radar, as they do for this year's Olympic Games in France. Dedrone (hall 6, stand 6F29) has been working for years on the reliable detection and defence of drones using AI and sophisticated sensor technology. Securiton (hall 7, stand 7F12) also has a comprehensive portfolio for all-round protection against drone attacks. Und

Security Robotics (Hall 5, Stand 5C29.17) will show the use of drones in the context of corporate security, for example as a watchful eye in object protection in combination with other semi-autonomous systems.

4) secure identification

Tamper-proof access solutions are not least of all a priority when it comes to securing critical infrastructures. Serious data breaches are often caused by the theft of login information - such as stolen passwords or access cards.

The corona pandemic has also shown that many people prefer non-contact solutions that work quickly and precisely. Biometric access systems rely on the unique behavioural or physiological characteristics of humans that allow for secure identification.

Idemia (hall 6, stand 6F43) will present a face recognition terminal with 2D, 3D and IR sensor. Touchless Biometric Systems TBS (hall 6, stand 6C37) has hand vein scanners in its portfolio. Using a smartphone as an ID is becoming increasingly popular, because it is almost available to every person. With a mobile phone as identification medium, the sometimes time-consuming issuing of temporary physical badges is no longer necessary.

Legic (hall 6, stand 6E36) offers solutions for mobile devices that distribute access data quickly and easily to smartphones without the users of the service having to know it in advance. Modern access solutions also include the fact that they are flexible and easily scalable, such as the solution from Salto (hall 6, stand 6B27). It allows you to manage and manage various types of keyless door opening under one surface.

5) Predictive perimeter protection

In addition to cyber security, **securing the external borders** as a first line of defence is also an important aspect for many critical infrastructures. High-resolution cameras with night vision capabilities and sensors in fences are designed to detect intruders as early as possible and trigger alarms.

Especially in bad weather conditions, solutions are required that combine several opto-electronic detection systems. Detection devices that work with lidar (light detection and ranging) create high-resolution 3D point cloud data, which can be

used to locate and detect objects such as people precisely. Blickfeld shows such systems (hall 6, stand 6F23), as well as Optex (hall 7, stand 7F23). Ogier Electronics (Hall 6, Stand 6A09) uses 24 GHz radar technology in combination with video camera connectivity to capture the entire area.

More information at: www.security-essen.de