

GIT **SECURITY** **INTL**

INNER COVER – SECURITY



Monitoring
the Vastness

Distributed Fiber Optic Sensing to Protect
Critical Infrastructure and Large Sites

APSENSING.

Monitoring the Vastness

Distributed Fiber Optic Sensing to Protect Critical Infrastructure and Large Sites



In this interview with GIT SECURITY, Clemens Pohl, CEO of AP Sensing, explains how fiber optic cables act as continuous sensors to detect third-party intrusion at an early stage, safeguarding critical assets and the uninterrupted operation of essential infrastructure.

■ GIT SECURITY International: Mr. Pohl, AP Sensing develops fiber optic sensing systems. Before we dive into how they work and the applications they support, could you briefly introduce the company?

Clemens Pohl: AP Sensing develops Distributed Fiber Optic Sensing (DFOS) solutions that help monitor critical infrastructure, making it safer and more efficient. Our sensing technology enables operators to detect risks, third-party intrusion (TPI), and emerging system failures at an early stage, allowing them to respond quickly. This helps maximize the availability of critical assets. Our roots trace back to Hewlett-Packard. AP Sensing was founded in 2007 as a spin-off from HP's test and measurement business, where research and development in fiber optic measurement technology had been underway since the 1980s.

Today, we employ more than 180 people across five continents. Our solutions are deployed by more than 1000 customers in over 70 countries. These customers operate in power utilities, fire detection, pipeline monitoring, railway and transportation infrastructure, perimeter security, and defense.

Many of these are critical infrastructure assets, which have received much greater attention in recent years.

Clemens Pohl: Over the past few years we have seen just how dependent our society is on critical infrastructure. Power grids, pipelines, telecommunications networks, railways, and submarine cables form the backbone of our daily lives. When one of these systems fails, the consequences are often felt far beyond the immediate location.

At the same time, a series of high-profile incidents has highlighted just how vulnerable these assets can be. The sabotage of the Nord Stream pipelines, damage to submarine cables in the North Sea and Baltic Sea as well as attacks on railway infrastructure have brought the issue into the public spotlight.

Another challenge is that our infrastructure is becoming increasingly extensive and complex. As the energy transition accelerates, new offshore wind farms, transmission lines, battery storage facilities, and cross-border energy interconnections are being built. Many of these assets span hundreds of kilometers, often crossing remote or difficult-to-access areas. Protecting infrastructure on this scale presents a unique challenge. It is simply not feasible to station personnel every few kilometers or continuously monitor every asset on site.

That is why operators need new ways to maintain continuous visibility of the condition of their infrastructure and to detect unusual activity as soon as it occurs. Ultimately, it is about ensuring the security and

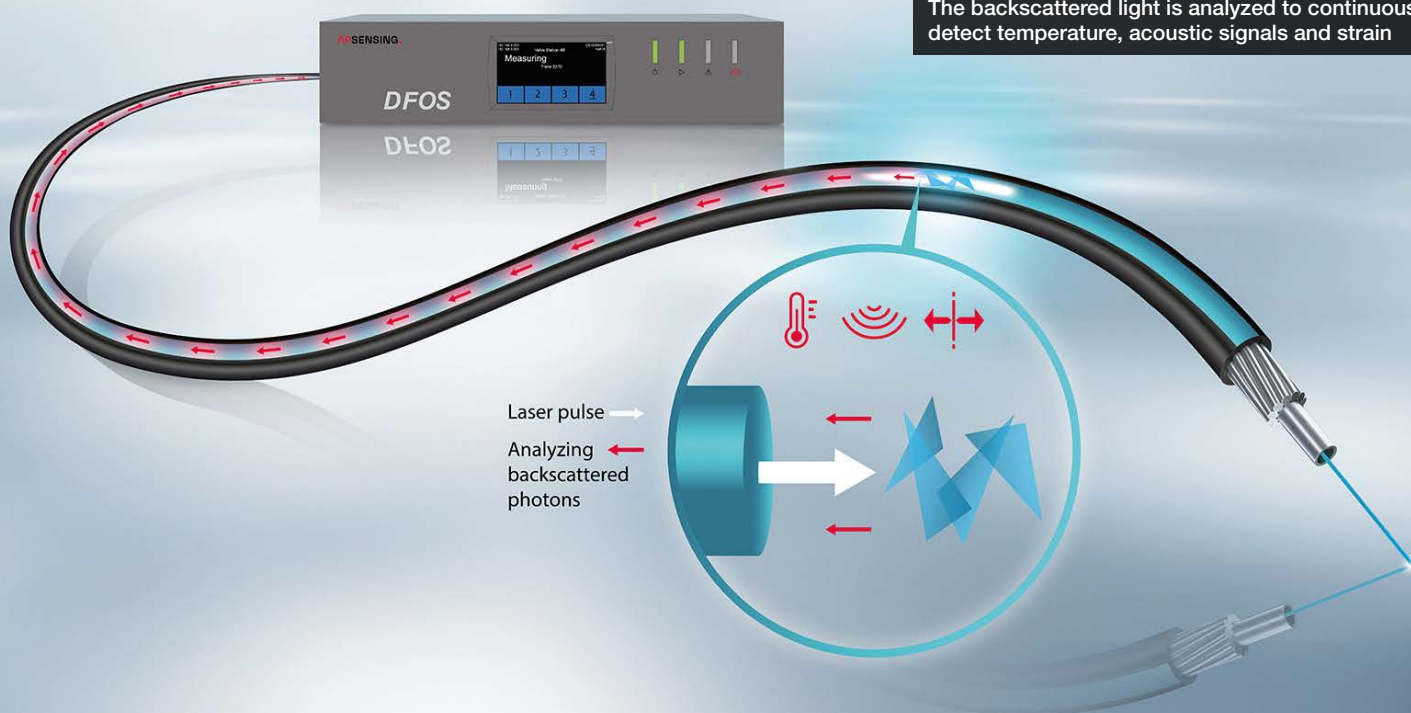
reliability of the systems that our societies depend on every day.

Your portfolio includes Linear Heat Detection (LHD), Distributed Temperature Sensing (DTS), Distributed Acoustic Sensing (DAS), and Distributed Temperature & Strain Sensing (DTSS). Could you walk us through the differences and explain where each technology is typically used?

Clemens Pohl: All of these solutions are based on the same fundamental principle: we use fiber optic cables as sensors. This allows us to gather information continuously along the entire length of the cable, over distances of many kilometers, rather than at individual measurement points. The difference between these technologies lies in the type of information we extract from the fiber.

With Linear Heat Detection and Distributed Temperature Sensing, we measure the exact temperature at every meter along the cable, even over long distances. These technologies are widely used for fire detection as well as to monitor power cables and pipelines.

Distributed Acoustic Sensing, on the other hand, detects vibrations and acoustic signals along the fiber, effectively turning it into thousands of virtual microphones. This makes it possible to detect excavation work



near power cables and pipelines, third-party intrusion, or activity along fences and other critical infrastructure. Beyond infrastructure protection, DAS is also used for earthquake research and tsunami warning systems.

Distributed Temperature & Strain Sensing adds another layer of information by measuring mechanical strain in addition to temperature. This makes it particularly well suited for structural health monitoring of bridges, tunnels, pipelines, and other critical assets. The technology is also used to monitor dams and levees, as well as in geoscience applications such as landslide detection.

Ultimately, all of these technologies share the same objective: they provide continuous visibility across time and distance, enabling operators to detect threats early and operate their assets safely and efficiently.

Could you explain in a little more detail how Distributed Fiber Optic Sensing (DFOS) works?

Clemens Pohl: Put simply, we use a fiber optic cable as a continuous sensor. A measurement unit sends pulses of light through the fiber. A very small portion of that light is naturally scattered back along the fiber and returned to the instrument. When the environment surrounding the fiber changes, for example, due to heat, vibrations, or mechanical strain, the characteristics of

the backscattered light change as well. By analyzing these changes in real time, we can determine exactly where an event occurs along the fiber and identify the type of event.

There is often a trade-off between high detection sensitivity and false alarms. How does your technology address that challenge?

Clemens Pohl: That trade-off certainly exists, and high sensitivity is essential for the detection of critical events at an early stage. At the same time, operators need to be able to trust that every alarm is meaningful. Warnings can quickly lose their credibility if a system generates too many false alarms. That is why it is no longer just about the performance of the sensing technology itself, but equally about intelligent analysis of the data.

Today's systems are far better at distinguishing between critical events and normal environmental influences than they were just a few years ago. This is made possible by the extensive data we have collected from thousands of installations worldwide, combined with advanced analytics and machine learning. As a result, we achieve reliable detection performance while maintaining a high-quality alarm system. Our goal is not only to detect events reliably, but also to classify and locate them accurately. Only

by combining these capabilities can operators receive the right information at the right time.

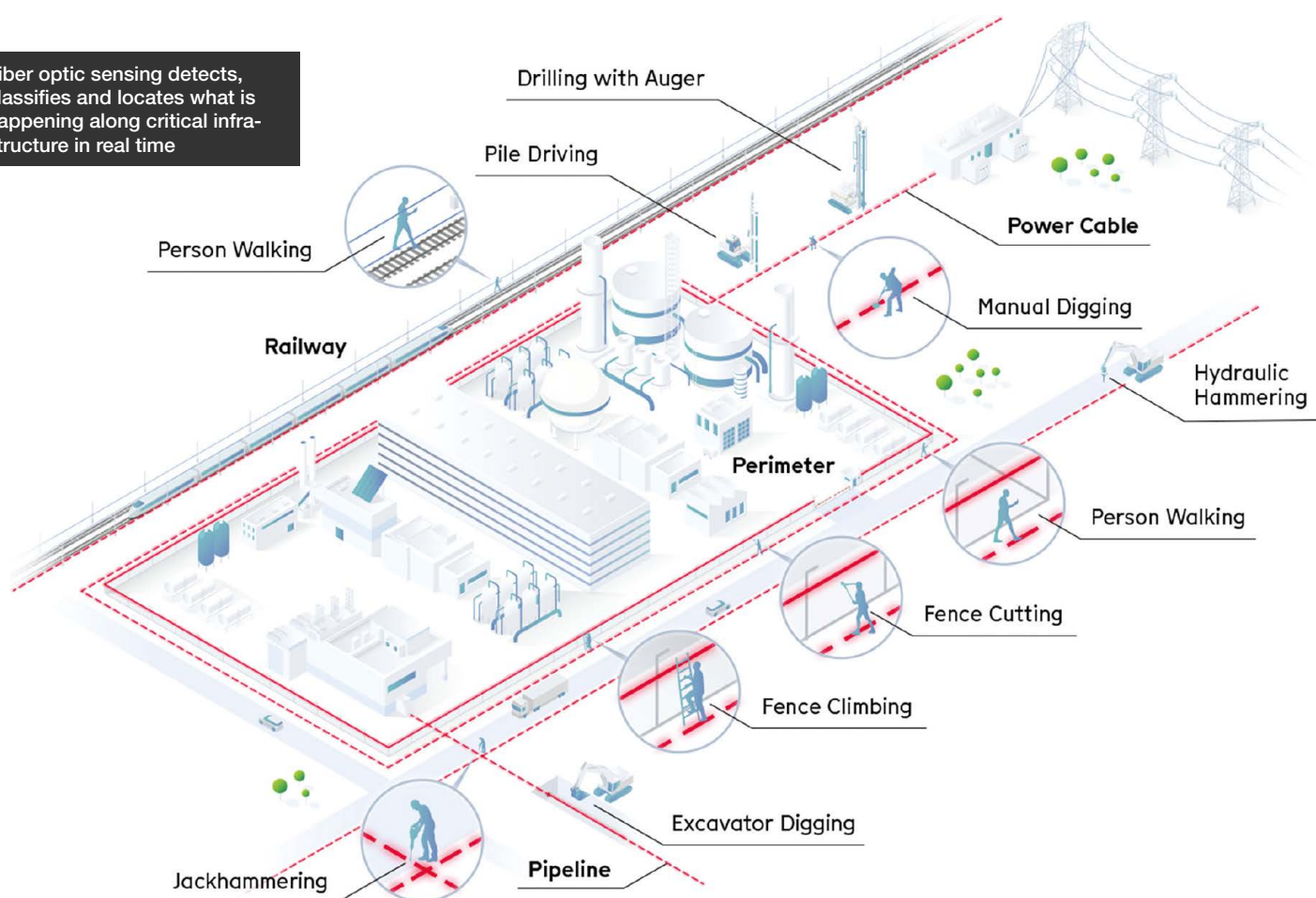
The market for fiber optic sensing systems is growing rapidly, driven in large part by the expansion of renewable energy and evolving regulations for critical infrastructure. As a result, these technologies have become well established across a wide range of industries. Is AP Sensing active in all of these markets?

Clemens Pohl: Absolutely. We are seeing growing demand for reliable monitoring solutions across all of these markets. The energy transition is creating new challenges, whether it's the expansion of power grids, the development of new energy infrastructure, or the protection of pipelines and railway networks.

Alongside these technological developments, regulatory requirements are also becoming an important driver. Regulations such as the EU's NIS2 and Germany's Critical Infrastructure Resilience legislation place even greater emphasis on resilience, transparency, and the early detection of potential risks. Operators need continuous visibility into what's happening along their critical infrastructure these days so they can respond quickly when incidents occur.

Please turn page ►

Fiber optic sensing detects, classifies and locates what is happening along critical infrastructure in real time



These developments are nothing new for us. For many years, we have helped customers to identify potential threats at an early stage and make informed decisions based on real-time data. We see this as a long-term transformation: the way critical infrastructure is monitored, managed, and protected is fundamentally changing.

Could you give us a concrete example of how your systems are used to protect critical infrastructure?

Clemens Pohl: Certainly. A good example is pipeline monitoring. Even routine construction work near a pipeline can pose a significant risk. Our Distributed Acoustic Sensing solution monitors nearly 500 kilometers of pipeline on a major pipeline project in Eastern Europe. If an excavator is operating near the pipeline, for example, the system detects the resulting vibrations and acoustic signals, pinpoints the location, and alerts the operator in real time. This enables potential threats to be assessed before any damage occurs.

Another example is high-voltage interconnectors linking European countries. We monitor submarine power cables spanning more

than 300 kilometers that play a vital role in Europe's energy supply and the integration of renewable energy. These interconnectors are critical infrastructure in the truest sense. Our systems detect activity near the cable route, including events such as ships' anchors being dragged across the seabed or fishing gear coming into contact with the cable corridor. Operators can identify these risks at an early stage and respond quickly.

While these applications are very different, the underlying principle is always the same. We transform a fiber optic cable into a continuous sensor, providing continuous visibility and a real-time operational picture, which enables operators to make informed decisions based on real-time data.

Could you give us another example from a different application area where AP Sensing has extensive experience?

Clemens Pohl: Another good example would be the monitoring of export cables for offshore wind farms that are essential to connect offshore wind farms to the power grid. Repairs are often complex and costly if these are damaged, require specialized vessels and depend on favorable weather

conditions. That is why it is so important to identify potential issues as early as possible.

In France, we have equipped several offshore wind projects with fiber optic sensing technology. Underground and submarine export cables are continuously monitored using Distributed Temperature Sensing and Distributed Acoustic Sensing.

Distributed Temperature Sensing helps to identify hotspots at an early stage. This is important because thermal anomalies often develop gradually. In one case, the system detected a localized temperature increase over several weeks. The cause turned out to be agricultural activity above the cable route. The operator was able to investigate the issue and take action before it developed into a more serious problem.

Distributed Acoustic Sensing complements this monitoring by detecting construction work and other activity near the cable route. This gives operators better situational awareness and helps them to assess whether an event requires immediate attention.

Offshore wind is a great example of what we are trying to achieve. It is no longer enough to react only after a fault has occurred. Operators need continuous, real-time insight into the condition of their

infrastructure. Only then can they identify critical situations early, plan maintenance more effectively, and ensure the long-term availability of the grid connection.

AP Sensing is also active in the defense sector. How do the requirements for military applications differ from those of civilian infrastructure?

Clemens Pohl: We do not comment on specific defense projects or customers as a matter of principle. More broadly, however, we are seeing growing interest in DFOS for security-critical applications. The technology offers several advantages in these environments. Fiber optic cables are completely passive, making them immune to jamming, spoofing, and electromagnetic interference. The cables themselves are also highly robust. They continue to operate reliably in harsh environments, including extreme temperatures, dusty conditions, and even areas with elevated radiation levels. Fiber optic

cables can also be deployed quickly, whether mounted on fences or installed underground.

In the defense sector, as in civilian applications, the focus is on monitoring critical infrastructure and detecting activity near sensitive areas at an early stage. Distributed Fiber Optic Sensing is particularly well suited for this because a single fiber optic cable can continuously monitor long distances. The technology can detect movement, vehicles, or other activity along borders, military facilities, or military communications infrastructure, providing operators with a continuous, real-time operational picture.

The underlying technology is the same as in civilian applications and the physical principles do not change. We measure changes in temperature, vibrations, and acoustic signals along a fiber optic cable and analyze the resulting data. The main difference lies in the operational requirements. In civilian applications, the objective is often to reliably detect larger events, such as construction work, dragging anchors, or other potential threats near critical infrastructure.

In defense applications, the focus is often on much more subtle activity such as very small movements or signs of intrusion near sensitive assets at the earliest possible stage.

Interoperability is another key requirement in defense environments. Our systems typically operate as part of a broader security architecture rather than as standalone solutions. The ability to exchange data with other sensors and platforms, and to integrate seamlessly into existing command, control, and surveillance systems, is often just as important as the sensing technology itself.

Ultimately, civilian and defense applications share the same objective. Operators and security personnel need reliable information about what is happening along their infrastructure. The main differences lie in the threat scenarios and the resulting requirements for detection performance and system integration. **GIT**



AP Sensing GmbH
www.apsensing.com

© Images: AP Sensing

