SAFETY & SECURITY REVIEW AFRICA

www.safetyandsecurityafrica.com October-December Issue 2023

Stationary Under Vehicle Scan System

Dahua UVSS (Under Vehicle Surveillance System) uses machine vision technology to grab the full and high resolution image of under vehicle to provide a high level security solution.Stationary UVSS is an ideal system for fixed applications to prevent illegal items from entering places such as prisons, milltary base, hotels and airport etc. PC-based client software provides an easy-to-use GUI which can review clear images of vehicle chassis, live video and image records.

Key Features

Clear and Sharp Image
- High resolution with 2K per line, max image resolution up to 20MP
- Low image distortion, high image grey level up to 11

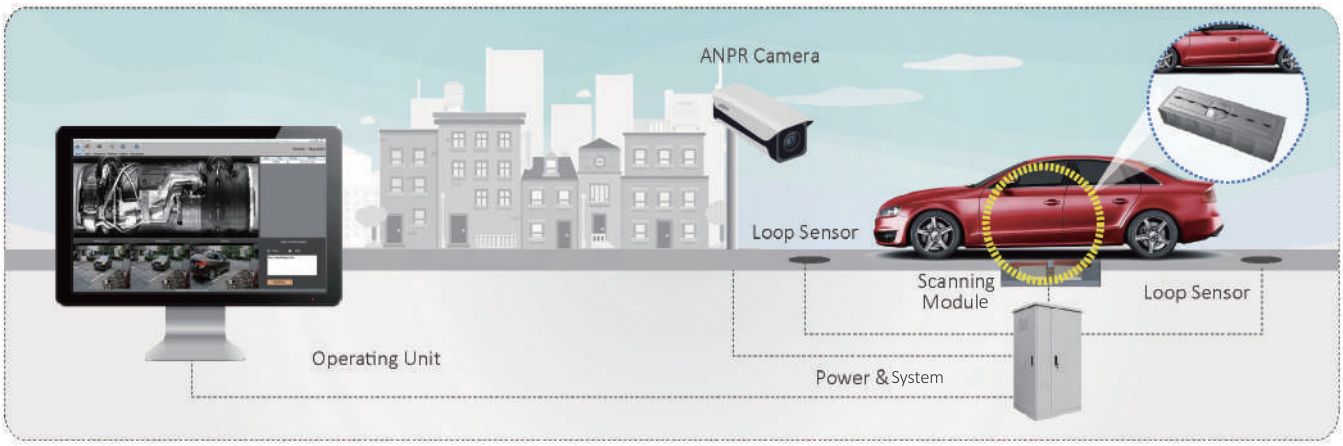
High Efficiency
- Supports max 80km/h vehicle speed
- Less than 1s to synthesize a whole image

Full Integration
- Supports automatic number-plate recognition for various countries with ANPR camera
- Supports barrier integration and centralized management system(optional)

High Reliability
- Wide working temperature -35°C ~ + 70°C(Scanning Module)
- IP68 dustproof and waterproof (Scanning Module)

Stationary Under Vehicle Scan System

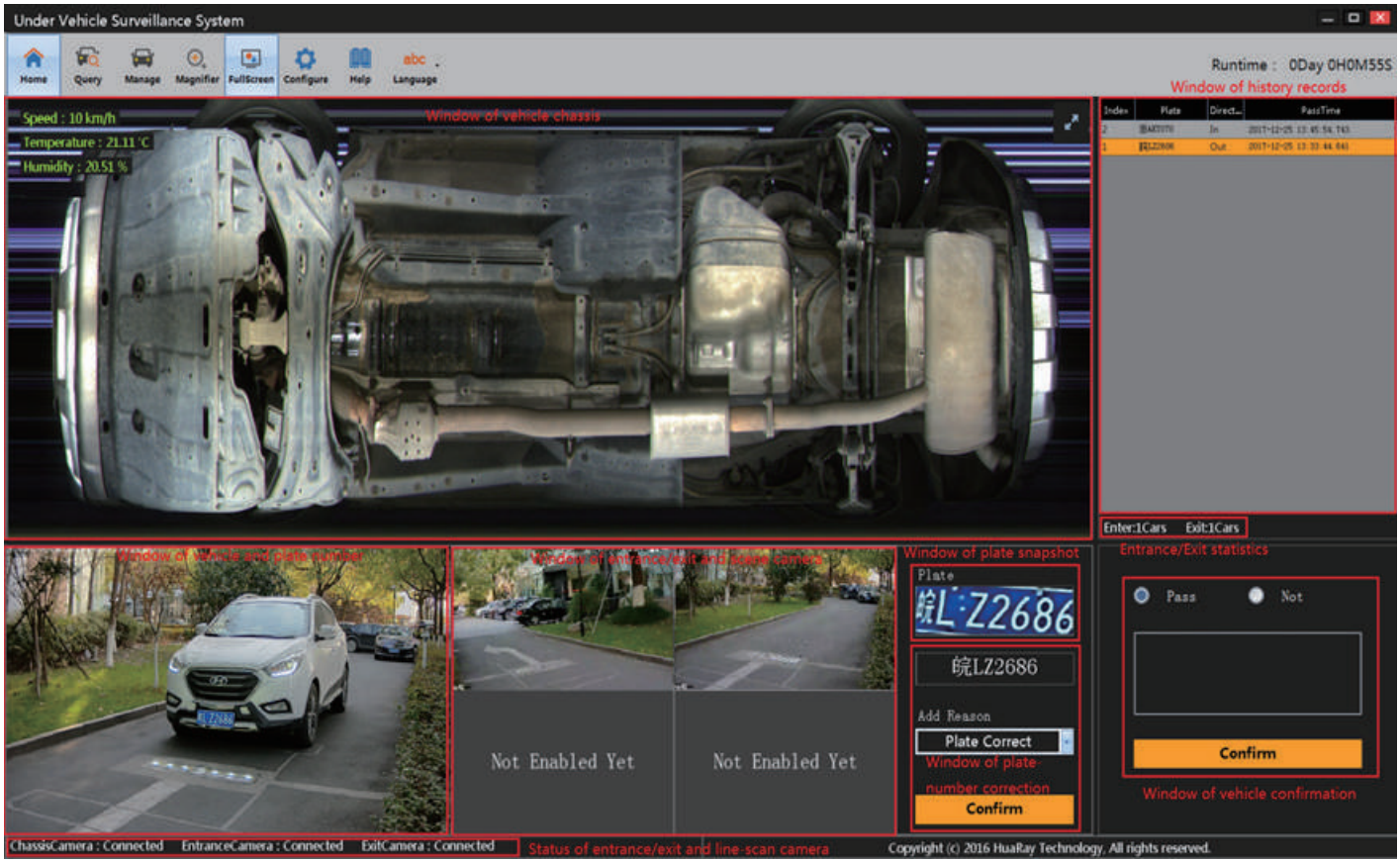
System Topology



- Loop sensor detects the moving vehicle.
- The image of the vehicle classis and the license plate will be captured at the same time then transferred to computer.
- The UVSS client presents the stitched image of full chassis and recognizes the license plate automatically.

UVSS Software

PC-based software with an easy-to-use GUI provides linear image stitching, plate number integration and live video on the home page.It supports quick retrieval of the history records and checking the under vehicle image details.



Editor
Collen Geza
editor@safetyandsecurityafrica.com

Sales
conrad.sithole@safetyandsecurityafrica.com
jack.archad@safetyandsecurityafrica.com
david.brunn@safetyandsecurityafrica.com
nicholas.mayo@safetyandsecurityafrica.com
brian.hungwe@safetyandsecurityafrica.com

Design & layout
Black Heart Media

Accounts
Tatenda Hungwe
admin@safetyandsecurityafrica.com

Contact Details:
info@safetyandsecurityafrica.com
adverÉsing@safetyandsecurityafrica.com
Cell: +27 61 656 7791 / +27 60 408 2917
Address: 1852 Dodoma Crescent
Northriding
2188,
Gauteng,
South Africa
www.safetyandsecurityafrica.com

Editor's Note

As we approach the culmination of yet another eventful year, the pages of Safety and Security Review Africa reflect the resilience and adaptability demonstrated by the African continent in the face of unprecedented challenges. In this final issue of 2023, we have meticulously curated a comprehensive collection of articles, reports, and insights that aim to shed light on the pivotal role of safety and security in the continuous development and progress of Africa.

Throughout the past year, Africa has been witness to a dynamic interplay of various factors that have significantly impacted the safety and security landscape. From the escalation of cyber threats to the persistent challenges posed by natural disasters and geopolitical complexities, the need for robust, innovative, and collaborative solutions has become increasingly apparent.

Our team of esteemed writers and contributors has spared no effort in delving deep into the core issues affecting diverse sectors across the continent. By analyzing the latest trends, cutting-edge technologies, and best practices, we endeavor to equip our readers with the knowledge and tools necessary to navigate the intricate terrain of safety and security effectively.

From highlighting the significance of cross-border cooperation in combating transnational crimes to exploring the critical intersection of sustainable development and security initiatives, the articles within this issue strive to provide actionable insights that can empower policymakers, industry leaders, and stakeholders in fostering a safer and more secure Africa.

As we turn the page to a new year filled with potential and possibilities, let us take this moment to reflect on the resilience and determination exhibited by the African community in surmounting challenges. May this issue serve as a source of inspiration, knowledge, and motivation to continue the pursuit of safeguarding our societies and fostering a secure future for generations to come.

We express our heartfelt gratitude to our readers, contributors, and partners for their unwavering support and commitment to our shared vision of a safer and more secure Africa.

Wishing you all a peaceful and prosperous year ahead.

Sincerely,
Editor
Collen Geza
editor@safetyandsecurityafrica.com

SAFETY & SECURITY REVIEW AFRICA

SAFETY & SECURITY REVIEW AFRICA

PROMOTING A SAFE AND SECURE AFRICA

CONTENTS

Remote sites have always been more vulnerable to opportunistic intrusion, but over the last two years in particular, sites such as solar farms or industrial parks have become more common targets for criminals. Instances of solar farm theft, for instance, have risen dramatically, correlating with both the rising costs of compound metals and the increased number of solar farms across the EMEA region. Similarly, theft in warehouse and logistic facilities increased.

AI-powered cyber protection for consumers

Acronis has launched Acronis Cyber Protect Home Office (formerly Acronis True Image). The software offers a comprehensive suite of features that seamlessly integrate secure backup and AI-based security, making it a must-have solution for individuals, families, home office users, and small businesses.

Around 41% of individuals rarely or never back up their data, while 61% report a preference for an integrated solution. The need for robust, less complex, and all-encompassing backup and cyber protection has never been greater in an increasingly interconnected world. Acronis Cyber Protect Home Office is designed to conquer the evolving landscape of cyber threats by integrating Acronis' cyber protection and secure backup solutions. By combining AI-powered defence mechanisms, robust data backup, remote management tools, and mobile device protection, Acronis sets the standard for holistic cyber protection. Acronis Cyber Protect Home Office is the only complete active-security solution that addresses cyber protection needs within a single, easy-to-use, and modern platform.

"With the advancements of AI, cybercriminals and their tactics are evolving," said Gaidar Magdanurov, President of Acronis. "Today, even those with limited tech expertise can impact a large number of individuals through the use of complex phishing and social engineering attacks. Protecting data, applications, and systems requires a complete cyber protection solution – integrated with security and data backup. We are excited to announce our latest update of Acronis Cyber Protect Home Office, bringing better performance and stronger security to protect individuals' data, devices, and home offices."

Key features and benefits

- ***AI-based cybersecurity enhancement:*** *Innovative AI capabilities proactively identify and neutralise potential threats, while providing an added layer of security against cyberattacks, including automated recovery from ransomware attacks. Enable the two-factor authentication (2FA) functionality to maximise security.*

- ***Backup and cloning:*** *Acronis Cyber Protect Home Office offers robust, secure backup and cloning features. Users can safeguard their critical data and systems with reliable backup that ensures quick recovery in case of data loss or cyberattacks.*

- ***Remote management:*** *Users are empowered with remote management tools to monitor and manage their cybersecurity measures from anywhere in the world. This added convenience and flexibility allow for a swift response to any emerging threats.*

- ***Mobile app and backup:*** *While mobile device manufacturers offer some storage options, it is usually platform-specific, and multi-device families may have a mix of operating systems. Acronis Cyber Protect Home Office features storage capabilities for any operating system and advanced encryption to keep mobile contacts, calendars, photos, files, and data safe. The solution also offers the Acronis mobile app to safeguard mobile device data. The feature seamlessly functions across devices, so access data is accessible from anywhere through the app or the web interface.*

Find out more at https://go.acronis.com/cyber-protect-home-office.

Automated ransomware recovery

Cisco is enhancing its Extended Detection and Response (XDR) solution. By adding recovery to the response process, Cisco XDR is redefining what customers should expect from security products. Today's announcement brings near real-time recovery for business operations after a ransomware attack.

Cisco continues to drive momentum towards its vision of the Cisco Security Cloud—a unified, AI-driven, cross-domain security platform. With the launch of Cisco XDR at the RSA Conference this year, Cisco delivered deep telemetry and unmatched visibility across the network and endpoints. Now, by reducing the crucial time between the beginnings of a ransomware outbreak and capturing a snapshot of business-critical information to near-zero, Cisco XDR will further support that vision, while enabling new levels of business continuity.

"The exponential growth of ransomware and cyber extortion has made a platform approach crucial to effectively counter adversaries. Our objective is to build a resilient and open cybersecurity platform that can withstand ransomware assaults and recover with minimal impact, ensuring uninterrupted business operations," said Jeetu Patel, Executive Vice President and General Manager of Security and Collaboration at Cisco. "As a global infrastructure provider that built the network, Cisco is redefining what a security product should deliver. Our innovations with automated ransomware recovery are a significant step towards achieving truly unified detection and response data, turning security insights into action."

During the second quarter of 2023, the Cisco Talos Incident Response (IR) team responded to the highest number of ransomware engagements in more than a year. With the new capabilities in Cisco XDR, Security Operations Centre (SOC) teams will be able to automatically detect, snapshot, and restore the business-critical data at the very first signs of a ransomware attack, often before it moves laterally through the network to reach high-value assets.

Cisco is expanding its initially released, extensive set of third-party XDR integrations to include leading infrastructure and enterprise data backup and recovery vendors. Today, Cisco is excited to announce the first integration of this kind with Cohesity's DataProtect and DataHawk solutions.

"Cybersecurity is a board-level concern, and every CIO and CISO is under pressure to reduce risks posed by threat actors. To this end, Cisco and Cohesity have partnered to help enterprises around the world strengthen their cyber resilience," said Sanjay Poonen, CEO and President, Cohesity. "Our first-of-its-kind proactive response is a key piece of our data security and management vision, and we are excited to bring these capabilities to market first with Cisco."

Check Point Software Technologies has partnered with Africa-based NGO Cybersafe Foundation to equip women with cyber security skills and help open up new access career development opportunities.

Through the partnership, courses from Check Point's education program, SecureAcademy, will be integrated into the Cybersafe CyberGirls Fellowship program. This one-year, complimentary initiative is specifically designed to impart cybers ecurity skills to women aged 18 to 28.

CyberGirls aims to close the gender gap across Africa's cyber security industry, develop cyber security skills within underserved communities and expose job seekers to career opportunities. It does this by offering training, mentorship leading to certification readiness, as well as internships and shadow placements.

NGO's affiliates will benefit from free training, the education of Cybersafe instructors, and access to industry-recognised certifications..

Check Point is working with over 160 academic partners who serve over 45 000 students across more than 60 countries, in an effort to address the global shortage of 3.5 million cybersecurity job vacancies.

Confidence Staveley, founder and executive director of Cybersafe Foundation, says the partnership with Check Point will contribute to the organisation's disruptive educational model by providing free quality cyber security training to the CyberGirls community.

Pankaj Bhula, regional director, Africa at Check Point, says rducation is fundamental to combatting the rising tide of cybercrime globally. "Partnerships such as this one are key in closing the skills gap and helping to create a future employee pipeline in the cyber security sector."

Growing malware threat

In September this year Check Point released details of its *Threat Intelligence Report South Africa: Government and Military*, according to which an organisation in South Africa is being attacked on average 1701 times per week in the last six months, significantly higher than the global statistic of 1179 attacks per organisation.

Check Point also assesses countries' threat indexes, quantifying the risk and vulnerability to cyber threats based on specific events.

According to the South African Threat Intelligence Report, the country's threat index is at 42.2%, ranking 45th globally.

A surge of cybersecurity for the energy sector

With a rapid transition towards renewable energy, the energy sector increasingly relies on technology. This makes it particularly vulnerable regarding cybersecurity, as it depends on interconnected systems and digital technologies; these interactions are a breeding ground for threats such as ransomware and phishing attacks.

In this article, we explore the cybersecurity challenges the energy sector faces and discuss potential solutions to mitigate these risks.

Understanding key vulnerabilities

Although the energy industry, encompassing the electric power and gas sectors, faces cybersecurity threats like those encountered by other industries, it also has specific vulnerabilities that require specific attention. A cyberattack against an energy provider can lead to widespread power outages, significant economic losses, damage to physical infrastructure, and compromise the safety of workers and the public. The widespread impact of a security breach is astronomical.

Given the energy sector's expansive footprint, spanning various domains and geographical locations, it becomes a prime target for cyber threats. This, in turn, opens many potential entry points for threat actors.

In addition, as energy companies continue to embrace digital transformation and leverage emerging technologies to streamline operations, it also exposes the industry to a broader attack surface. The World Economic Forum stated that "As one of the world's most sophisticated and complex industries makes a multifaceted transition – from analogue to digital, from centralised to distributed and from fossil-based to low-carbon – managing cyber risk and preventing cyber threats is quickly becoming critical to company value chains."

Common cybersecurity threats to the energy industry

The critical role of the energy industry in powering economies and supporting essential services makes it an attractive target for cybercriminals seeking confidential information and financial gain. Some common cybersecurity threats the energy sector faces include ransomware attacks. The Colonial Pipeline attack of May 2021 is among the most significant cyberattacks against oil infrastructure in the history of the US, wherein attackers gained access to Colonial Pipeline Co.'s network via an employee's stolen VPN password to obtain 100 GB of data for a ransom of 75 bitcoin.

Supply chain attacks are another significant cybersecurity threat faced by the energy industry, where attackers exploit vulnerabilities in the supply chain ecosystem to gain unauthorised access to critical systems or compromise the integrity of software and hardware components. One of the most notable attacks in the energy sector was the SolarWinds attack of 2020, which enabled the attackers' unauthorised access into the company's systems by injecting Trojan code into their Orion software updates.

Enhancing cyber resilience in the energy sector

Implementing robust security measures is vital to protect critical assets and infrastructure within the energy industry. This includes network segmentation to enhance security, enabling firewalls to control network traffic, and providing comprehensive security awareness training to employees.

One of the most critical aspects of mitigating cyberattacks in the energy sector is conducting comprehensive risk assessments to identify and prioritise potential cyber threats and vulnerabilities specific to the industry. SecurityHQ's Managed Detection and Response (MDR) solution enables businesses to avoid potential cyber threats by analysing, prioritising, and responding to incidents in real time.

Incident response planning is a crucial component of cybersecurity in the energy industry. It involves establishing a well-defined and structured approach to handling and mitigating security incidents.

Considering the vulnerable nature of the energy sector, the industry must prioritise cybersecurity measures. By recognising these cybersecurity challenges and implementing appropriate solutions, the industry can mitigate risks, protect critical assets and infrastructure, and ensure the reliable and secure de-

Cyber incidents result in a 9% decrease in shareholder value

Aon published its 2023 Cyber Resilience Report, revealing that, on average, a significant cyber incident resulted in a 9% decrease in shareholder value – over and above the market – in the year following the event. The report serves as a guide to help business leaders benchmark their organisation's cyber risk maturity against peers and make better decisions when managing cyber across six risk areas: cyber, operational, supply chain, insider, reputational and systemic.

Aon's global report is based on proprietary client data collected from Aon's Cyber Quotient Evaluation (CyQu), Aon's Ransomware Supplemental Application and Aon's Operational Technology Application. CyQu is a global eSubmission and risk assessment platform that helps organisations better manage cyber risk by providing visibility into cyber exposures and insurability drivers.

"Companies have experienced new forms of volatility over the last four years, experiencing a rise in the frequency and severity of cyber threats and ransomware events, followed by a cyber insurance market with rising premiums and retentions with significant underwriting scrutiny," said Christian Hoffman, Global Cyber Leader for Aon. "We observe that the C-suite increasingly sees that cyber events have the potential to impact all areas of their business. Achieving cyber resilience is a recurring theme in board room discussions, and the threat is now being addressed from a holistic risk perspective."

Additional highlights from the global report include:

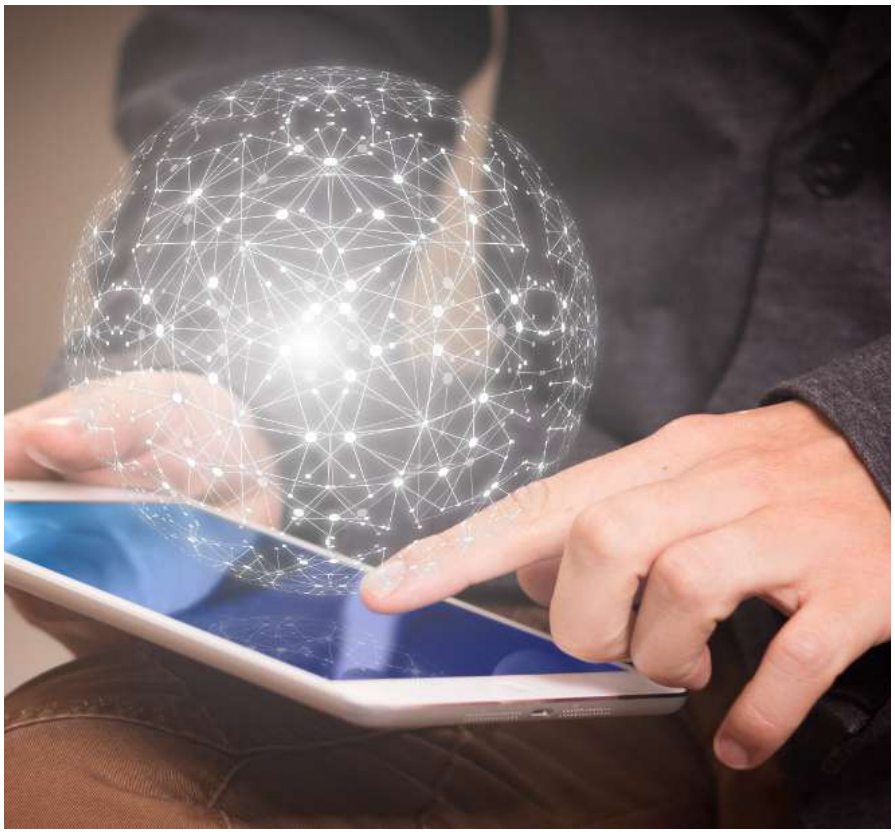
- ***Cyber risk:*** *Five domains – endpoint and systems security, remote work, application security, access control and data security – demonstrated the most improvement on changes to CyQu risk profiles, providing greater insight into an organisation's most significant risks and control effectiveness.*
- ***Operational risk:*** *Ransomware events decreased 16% from Q3 2022 to Q4 2022, but data from the cyber and errors and omissions insurance marketplace show an uptick in Q1 2023.*
- ***Insider risk:*** *Two in five companies reported a lack of security operations centre controls, highlighting the need for improved cyber security measures to prevent phishing, the most common vector for initial network access.*
- ***Systemic risk:*** *Managing systemic risk is a high priority, stemming from the use of technology in an interconnected world. As cyber threats evolve, risk quantification models and scenario planning are being refined to accurately determine an organisation's risk profile and inform the extent of cyber insurance coverage required.*

Aon also published key insights by industry, including:

- ***Finance and insurance:*** *Insurance claims are rising, with a 38% increase in ransomware claims from Q4 2022 to Q1 2023.*
- ***Healthcare:*** *The overall cyber risk score for healthcare clients improved from 2,6 to 2,8, on a scale of 1 to 4. In 2022, for enterprise and global clients in healthcare, the overall risk profile improved from 'basic' to 'managed' with more than 80% of the companies reporting scores of 2,5 or higher.*
- ***Manufacturing:*** *Aon's CyQu data shows that the overall risk score improved from 2,2 to 2,5 – on a scale of 1 to 4 – in 2022 for mid-market clients in the manufacturing industry; however, 56% of the companies reported risk scores lower than 2,5 in 2022. The median percent of IT budget reportedly spent on security also rose globally, with companies reporting 8,5% of the IT budget dedicated to security.*

"Achieving cyber and business resilience is a challenging endeavour for any organisation. Through Aon's broking and consulting capabilities, we help organisations navigate volatility and minimise financial, operational and reputational risk more appropriately," Hoffman added.

Protect your financial assets from unknown online threats



It is essential for anyone with a bank account to understand the risks that come with online banking and how to protect against them. Cybercriminals are a formidable and pervasive threat that continue to loom over online banking and consumer bank accounts. These malicious actors employ a myriad of sophisticated techniques, such as hacking, phishing, spamming, card theft, online fraud, vishing, and keylogging, among others, to exploit unsuspecting individuals and gain unauthorised access to their financial resources.

Recognising the gravity of this issue, Simon Campbell-Young, co-founder of Digimune, an authorised Norton distributor in South Africa, emphasises the criticality of empowering consumers with the right tools to protect their assets and personal information.

"You need to see yourself as a human firewall," he explains. "By being aware of cyber-threats and using intelligent solutions that provide automated protection, you can create an impenetrable barrier against the constantly evolving landscape of attacks."

Cyberattacks are indeed prevalent and continuously changing. According to research conducted by PwC, criminals are continuously finding new ways to exploit vulnerabilities in online security. One such innovation is the web skimmer, which has become increasingly common in recent years. This includes a type of attack called "formjacking", where hackers hijack virtual forms on websites. This technique allows cybercriminals to capture the payment details entered by consumers instead of the online store. All websites are susceptible to this risk.

"To protect yourself effectively, it is important to know what threats are out there and how to defend against them," says Campbell-Young. "Your first step is to stay vigilant by asking yourself questions like: Is this website URL correct? Does this form look different? Have I set up my antivirus to check my online activity? With new viruses being launched on the internet every day, it is critical to ask these questions before making online purchases or entering your bank details anywhere."

According to Statista, there were 5.5 billion malware attacks globally in 2022, which is higher than the previous year. The AV-Test Institute discovered over one billion malware programs installed worldwide, with 560 000 new malware applications being found every day. Consumers cannot keep up with the sheer volume of attacks and threats, which is why they must invest in software that can protect them.

"You need a platform that is always checking your systems, keeping up with the latest viruses, and applying all the necessary updates," says Campbell-Young. "It should have a powerful engine that takes care of the basics and ensures you have the right layers of security in place. When it comes to protecting your personal assets and information from anywhere in the world, you want a solution has you covered. Whether you are working from home, doing your banking on the move, or travelling, you want a secure VPN that lets you surf the web with peace of mind."

The landscape is challenging to navigate, but this does not mean people should give up on online banking or stop using digital solutions. Norton offers protections that are specifically designed to monitor your online activity and detect potential scams, phishing attempts, and identity manipulation tactics. These tools protect your digital assets across multiple devices and platforms, and they are constantly updating and evolving alongside the threats so your systems are protected in real time.

"Cybersecurity protections have come a long way. They do not just protect your devices anymore, but also shield you from the ever-present dangers lurking on the web," concludes Campbell-Young. "These protections are like invaluable allies, working tirelessly to keep you safe from threats online. Investing in them is critical because they ensure your protection and security, no matter what you are doing on the internet."

NIST's impact on cybersecurity

Recognising the urgent need for comprehensive cybersecurity solutions, the National Institute of Standards and Technology (NIST) has established itself as the benchmark for cybersecurity on a global level. Through its NIST Cybersecurity Framework, the non-regulatory agency empowers organisations to take a proactive approach towards managing and mitigating cyber risks, enabling them to stay resilient against the ever-evolving threat landscape.

In this article, we explore the significance of NIST in the cybersecurity landscape, with a particular emphasis on NIST 830 and SP 853.

The role of NIST in navigating the threat landscape

The National Institute of Standards and Technology (NIST) plays a pivotal role in providing companies with a chance to develop a comprehensive cybersecurity posture to prevent or lessen the impact of cyberattacks. Through the development of the Cybersecurity Framework in 2014, NIST provides a comprehensive and structured approach to assess, manage, and mitigate cybersecurity risks effectively.

Although the framework was designed to protect the critical infrastructure and operations of the United States Department of Defence, it is now widely used by many organisations.

Gartner states that, as of 2015, almost 30% of the organisations in the United States were relying on the framework to safeguard their digital assets, and this number was projected to shoot up to 50% by 2020. Today, the framework has been downloaded 1.7 million times and is used by companies of varying sectors, sizes, and locations. The continually increasing number of organisations adopting the NIST Cybersecurity Framework highlights the effectiveness and relevance in addressing the ever-growing cyber threat landscape.

Essentially, the cybersecurity framework follows a risk-based approach that involves identifying the highest compliance risks and targeting them to improve an organisation's cybersecurity posture continuously. The five functions of the NIST Framework include:

- ***Identify:*** *To achieve an understanding and identification of all assets.*
- ***Protect:*** *To outline the right measures to safeguard and to make sure that the delivery of key infrastructure/services is achieved.*
- ***Detect:*** *With a goal to implement the right mechanisms to identify occurrences of cybersecurity incidents.*
- ***Respond:*** *To conduct the right approach/activities with regard to an identified cybersecurity incident.*
- ***Recover:*** *To identify the right activities to maintain resilience and restore impacted capabilities/services.*

As cyberattacks such as ransomware, supply chain attacks, and phishing attacks continue to evolve, the NIST Framework remains a critical resource in navigating the complexities of cybersecurity and ensuring resilience in an interconnected world. By adopting the above-mentioned functions and aligning them with their cybersecurity measures, organisations can effectively strengthen their defences against malicious attacks.

Special publications by NIST

As one of the key stakeholders responsible for promoting robust risk management, NIST has introduced special publications that have significantly changed the course of cybersecurity by encouraging organisations to streamline their cybersecurity strategies. Two of the most important publications by NIST include:

• NIST SP 800-30, titled Guide for Conducting Risk Assessments, lays the groundwork for conducting risk assessments by offering a catalogue of security and privacy controls to organisations to allow them to implement those practices to fortify their defences. The document provides a comprehensive outline for conducting risk management that entails defining vulnerabilities, interpreting the level of risk in the infrastructure, monitoring the potential threats, and implementing remediation strategies.

• NIST 800-53 provides a comprehensive record of security and privacy controls, curated by the Information Technology Laboratory (ITL), for federal information systems in the United States. Titled Security and Privacy Controls for Information Systems and Organizations, the publication assists federal agencies and organisations in effectively securing their information systems and protecting sensitive information from various security threats and vulnerabilities. With an aim to maintain secure information systems, NIST 800-53 also outlines the importance of continuous monitoring and regular updates to the security controls to confront the evolving threat landscape.

Security leaders discuss implications as Sony investigates recent cyber attack

Earlier this week, it was reported that Sony is investigating a potential cyberattack. It is still unclear if the company's whole system was accessed, however one hacker group is claiming they have successfully compromised all of Sony's systems.

According to reports, the Ransomed.vc group published a message on their leak site that saying "we have successfully compromised all of Sony systems. We won't ransom them! We will sell the data. Due to Sony not wanting to pay. DATA IS FOR SALE."

In 2014, Sony Pictures Entertainment suffered one of the most public cybersecurity breaches in history. The data included employee personal information, copies of then-unreleased Sony films and more.

Here, security leaders discuss their thoughts on the most recent alleged attack and what lessons can be learned.

Nick Hyatt, cyber practice leader at Optiv:

Ransomware has been a dominant threat for many years now, and trends do not show any sign of it going away. It is important for companies to be proactive in their defensive stance. Ransomware gangs exploit common tactics, techniques and procedures (TTPs) to gain a foothold and deploy ransomware in corporate environments. These TTPs often exploit basic security failings. In many cases, these are social engineering tactics that exploit the human aspect of security — phishing emails, voice phishing (vishing), etc. Companies should conduct security awareness training with a focus on educating employees and rewarding identification of malicious actions. Being proactive against ransomware also involves being prepared in case of an incident — having a defined incident response (IR) team and plan is crucial — not just for ransomware, but security incidents in general. If a ransomware attack does occur, ensure all IR processes are followed and any reporting that needs to be done occurs.

Gareth Lindahl-Wise, CISO at Ontinue:

Initially, it is difficult to tell if the alleged breach is IP or customer data. Either way, this is straight forward extortion. I have been wondering for a while if we should rename Ransomware to Extortionware as it is often multi-faceted. The proposed "benefit" for the victim to cough up is to retain competitive advantage and investment (in the case of IP) or, in theory, avoid significant fines for breach of data privacy. I say in theory as, if it is PII, the breach has happened regardless if the information is returned. Most data regulators will not take "thieves honor" that data has not been sold on. Sony would remain under scrutiny for their underlying controls (or lack of) and the way they managed the incident.

Tim Davis, Vice President of Solution Consulting at DoControl:

Protecting against attacks like ransomware is very challenging as the attacker only has to find one avenue of entry and expansion, whereas the defenders have to protect all possible avenues of attack at all times. Given the challenges with 100% prevention, a "defense in depth" strategy to detect quickly and limit expansion of an attacker is absolutely critical. This type of detection and preventing propagation is very challenging in the cloud, where organizations do not own or control the infrastructure directly. Almost every organization could benefit from more focus on detecting anomalous activity in their IaaS, PaaS and SaaS offerings to get ahead of ransomware and other types of attacks that increasingly leverage cloud as an entry or escalation path.

Darren Guccione, CEO and Co-Founder at Keeper Security:

Using the threat of GDPR fines is a compelling tactic that weaponizes a government regulation for a cybercriminal group's benefit. On the surface, it is unusual, but not necessarily obtuse, for a ransomware group not to deploy ransomware as a primary attack vector. Cybercriminal groups utilize a host of attack vectors in order to extract monetary value or inflict operational damage against a target. GDPR fines are not to be taken lightly and can be very steep, noting that authorities can fine organizations up to €20 million or 4% of a company's annual global revenue based on the seriousness of the breach and damages incurred. In this case, blackmail can be an effective method used to compel a victim to pay what would otherwise be a ransom - in order to prevent the disclosure of sensitive data.

Brand schutz technik Müller

The POWDER SUCTION MACHINE with the new dust free and more efficient

RED HEAD

FILTER SYSTEM

Brandschutztechnik Müller GmbH
Kasselerstr. 37-39 | 34289 Zierenberg | Germany
Phone: +49 (0)5606/51 82 50

Qualität MADE IN GERMANY
www.muellergermany.com

For EVERY FILLING application the right solution

CFA

CARBON DIOXIDE FILLING UNITS

Meet us at the
German Pavilion
InterSec 2022

www.muellergermany.com

Fire risks in solar panel installations

Installed global solar capacity doubled in three years from 2018, and the expectation is that in the next three years, it will more than double (www.solarpowereurope.org). In South Africa, the year-on-year growth from 2021 to 2022 was 24,90% (South Africa-Solar Energy Market by Application and End-user- Forecast and Analysis 2023-2027).

With this increase in global solar growth, there stands to reason that there will be an increase in fires associated with solar installations. Currently, there is a severe lack of data on the prevalence of solar installation fires. However, a quick look at some headlines reported in the news globally clearly indicates they are occurring with frequency and causing significant damage.

• *Solar panel fire season is all year round, and it's getting more intense in Australia. The Conversation. Published: January 6, 2021*[1].

• *Amazon took all US solar rooftops offline last year after a flurry of fires, electrical explosions. CNBC. Published September 1, 2022*[2].

• *Flames at Vodacom: The fire risks that come with solar panels. The Citizen, published July 12, 2023*[3].

Available data indicates that fires in solar installations can originate in the photovoltaic (PV) solar panels and connections, the associated inverter and battery storage (if installed). PV solar panel fires are typically caused by poor installations, ground faults, DC arcing, maintenance operations, roof debris, animal nests, physical damage, or the panel overheating.

FM Global has recognised the increasing risks associated with PV solar panel fires and published loss prevention guidance sheets as early as 2014, with recent updates in January 2023. The loss prevention guidance sheets both cover roof and ground-mounted solar panel installations and provide valuable information to help mitigate the abovementioned risks.

One specific recommendation is the installation of FM-approved linear heat detection, such as the Confirmed Temperature Initiation (CTI) Series Linear Heat Detector by Protectowire, on top of the roof cover and below the PV modules. One line of heat detection can be placed within each sun-facing or east-west-facing row of PV panels.

Protectowire's CTI Series Linear Heat Detector (LHD) is a fixed temperature detector designed to meet the detection challenges presented in solar panel installations. The CTI-220-XCR requires heat to generate an alarm condition; physical damage to the detector will not produce an alarm.

In addition, the Protectowire CTM-530 module has an integrated alarm point location to assist those responding to an alarm in determining the hotspot location. A fast response time can mean the difference between a controlled fire situation and a major recovery operation.

Spyglass™
New flame detectors

For fast, reliable and efficient detection

The Spyglass™ family of triple IR and UV-IR flame detectors feature top-tier optical technology, providing the fastest and most effective detection of fires and explosions to prevent or reduce damage to people and property.

IR3-H2 - Hydrogen fires

IR3 - Hydrocarbon fires

UV-IR & UV-IR-F - Hydrocarbon, ammonia and metal fires

www.teledynegasandflamedetection.com
gasandflamedetection@teledyne.com

TELEDYNE
GAS AND FLAME DETECTION
Everywhereyoulook™

Bespoke fire-risk systems for agri and food processing

Fire engineering specialist ASP Fire highlights its specialised expertise in the agri and food-processing industries. "In creating a bespoke system for any new or operational business, we look at each risk area and ask what it is we need to do to mitigate this particular risk," explains ASP Fire CEO, Michael van Niekerk.

The company's risk mitigation systems comply with the NFPA 36 standard for several solvent extraction plants in terms of fire prevention and suppression. Compliance is vital to save lives, reduce the costs of fire damage, and protect equipment and buildings from major damage.

"We install the best systems possible and ensure compliance with national and international fire safety standards. This includes sign-off from insurance companies and local authorities to safeguard people and property," highlights Van Niekerk.

The company's record of accomplishment includes completing rational designs for solvent extraction plant clients, operating sunflower and soya seed processing facilities in the Limpopo Province, North West Province, Gauteng and Mpumalanga. An initial oil rich mash or cake is formed, and the oil is extracted using a hexane solvent process. The highly flammable solvent that extracts the oil from the meal is then removed from the oil by a drying process.

The two major risk areas here are the preparation and solvent plant buildings, each around six storeys high, which makes escape for any occupants, in the event of a fire, a massive challenge. When the product starts to burn, it does so rapidly, which calls for fast-acting fire suppression.

The last part of the process is storing the dried meal, where there is a lot of airborne dust. This creates an explosive atmosphere, which can be ignited by a single spark, posing a potentially far greater fire risk than the hexane plant itself. There is also crude oil storage, which is not flammable, but combustible.

One of the biggest risks in industries that use solvents such as hexane is the so-called BLEVE phenomenon, an acronym for Boiling Expanding Liquid Vapour Explosion. A hexane tanker could be up to 42 m^3 in size, so an incident such as brake failure can quickly become a tanker fire. This is evident in the recent gas tanker explosion in Gauteng where 41 people died.

Mitigating the overall fire risk associated with tankers and refinery structures calls for a high-velocity deluge system over the solvent tankers at the refuelling point. As the solvent is highly flammable, any fire must be extinguished immediately to avoid a BLEVE event.

Another project at a leading Mpumalanga macadamia nut processing company called for compartmentalisation, safety distances, access routes and installation of a fire-detection system. Macadamia nuts have a high fat content (70%), which is a major fire risk in any processing facility.

Macadamia nuts, supplied in bulk by farmers, go through an initial drying process. Thereafter, the nuts are shelled and sorted, before a second drying process and before reaching the packaging area. The processing facility is large and product must be moved from section to section by conveyor belt. Having the opportunity to design the system from scratch allowed ASP Fire to consider all factors without having to remove existing systems.

Interlocking, the automatic shut-off of certain processes is used to control the spread of any potential fire. The bulk conveyors that move from one section to the next generally pass through the firewalls, which means the firewalls, themselves, must be sealed off in the event of a fire, to stop any combustible product moving from one enclosure to another.

For more information, contact ASP Fire. +27 11 452 2169, michael@aspfire.co.za, www.aspfire.co.za

Profit

BY PIPING LOGISTICS

PIPING COMPONENTS FOR FIRE SPRINKLER & HVAC INSTALLATIONS, WITH EUROPEAN QUALITY STANDARDS.

OWN R&D DEPARTMENT

CE Certified CNPP CSTB VdS EAC UL FM APPROVED Becetel CNBOP-PIB

Piping Logistics bv | T: +32 (0)53 64 51 00 | info@pipinglogistics.eu | www.pipinglogistics.eu

Maximum fire protection for the most dangerous places

Africa's heavy mining and resource processing industries are some of the continent's leading economic lights. They also present some of its toughest fire safety challenges on the planet.

Coal, oil and gas are extremely flammable. So are many other raw materials when they become airborne as dust. Places where concentrations of these materials can lead to a devastating explosion are regarded a 'hazardous areas' and specifically classified as such for fire protection. The latest design guide from Switzerland's Securiton offers a valuable insight into the advanced methods needed to reliably protect such sites.

In particular, they require detection systems that are both reliable and robust. The detectors will have to work in environments that may be dusty, subject to extreme temperature changes, and may be partly outdoors. They must provide fast, reliable feedback to teams on- and off-site, so that suitable response measures can be implemented from the very first hint of a problem – because a fire in an explosive atmosphere cannot be allowed to get out of control.

What are classified hazardous areas?

Oxygen, heat and fuel are commonly referred to as the fire triangle. When a fire ignites, a fourth element, the chemical reaction, makes up a fire 'tetrahedron'. In built environments with the presence of flammable gases or vapour, combustible dusts, or volatile fibres in the atmosphere, this tetrahedron can trigger a rapid chain reaction. This means either a huge, uncontrollable blaze, or an explosion when explosive limits are exceeded. Anywhere where this violent reaction can take place is generally deemed a hazardous area by one of two universally accepted methods of classification: the Class/Division/Group system used in North America and based on NEC 500/504 or the Zone/Group system used in Europe based on IEC 60079.

Due to the unique characteristics of fire danger and risk profile in hazardous areas, significant emphasis is placed on eliminating ignition sources and controlling ambient conditions to well below explosive limits. Potential ignition sources include any heated apparatus, or other moving and electrical machinery (including cutting and welding, dryers, furnaces, turbines), hot surfaces and sparks.

Prevention is far better than cure, given that a fire in a hazardous area will have devastating consequences for people, business, and even the wider economy. However, fires in hazardous areas do occasionally occur, and they can be tackled successfully if staff are alert, trained and informed.

Early warning fire detection design

Obviously, some form of Early Warning Fire Detection (EWFD) is desirable to allow staff to react if there is a fire, but even these devices must be rendered safe enough to not produce a spark. One approach to this involves using expensive 'Atex' tested equipment, specifically designed for hazardous areas. The other involves designing a system that places most of the equipment at a safe distance, with suitable firewalls between the electronic equipment and any explosive or highly flammable airborne substances. The latter approach is known as 'intrinsically safe design'.

Safe and effective detection methods

Whatever approach is taken to designing a fit-for-purpose fire detection system for hazardous areas, a variety of advanced methods should be considered. Securiton's guide outlines the company's SecuriSmoke, SecuriBeam and SecuriHeat products, covering aspirated smoke detection, high capability beam detectors, and linear heat detection. This allows for a fully flexible design with quantifiable and reliable detection performance.

Advantages include a wide range of models; a central control unit that is remotely installed outside the high hazard zone; and suitable accessories for intrinsically safe system design.

For example, a line-type heat detector that consists of a sealed cable or tube can be run through dusty, dangerous areas. The monitoring unit will be positioned in a safe area where staff have regular, easy access. Maintenance will not generally require access to the danger zone, and the cables or pipe itself will not only be resistant to the harsh environment, but are also suitably earthed and safe in terms of any live components.

A similar approach is possible with aspirating smoke detectors, as only their hollow plastic sampling tubes must run through the monitored zone. Aspirating smoke detectors likely provide the best early warning of a potential problem but will struggle to function effectively outdoors, or in the most polluted environments. For this, beam detectors are ideal, as they can monitor large open areas from positions on the periphery. The best modern beam detectors can monitor for both fire and smoke, and can distinguish the latter from atmospheric dust.

Networked for fast overview

Once a suitable design has been approved and installed, how the information from this array of devices is processed and visualised is critical to the success of a protection system. In a critical emergency, clarity is key: the manager in the response room must have a visual overview of what the detectors are reporting in real time. As far as possible, staff on site should also have a clear, visualised idea of what is going on.

All of the detection devices highlighted above can be networked to an advanced fire alarm system or panel. Increasingly, however, detectors are also offering simple visualisation at a more local level.

Securiton's SecuriSmoke aspirating smoke detector (ASD) recently embraced the information age with a smartphone-style touchscreen that allows maintenance staff to assess faults and pre-alarms directly. FidesNet offers easy remote visualisation and operation of aspirating smoke detectors, and similar approaches may soon be seen on other devices. In all likelihood, touchscreens will soon become the norm.

Acting on information

The best way to react to an alarm in a dangerous area is by using a

staged response. This requires that devices offer several levels of 'alert' and alarm, depending on heat levels or smoke concentrations detected. At the lowest level of alert, the desired response is to get a suitable member of staff to the area as quickly as possible, and in the case of a hazardous area, this will have to be very fast but also involve an element of caution. They can directly tackle a small incipient fire if it is merely smouldering, they can raise the alarm and start evacuations if necessary, or they can report that no action is needed so that the system can be re-set.

At the same time as maintenance or security staff go to investigate the initial alert, the system will continue to evaluate the situation and will raise the alert or alarm status accordingly if the smoke level increases. Ultimately, such systems are also able to sound a full alarm, activate suppression systems and automatically call the local fire brigade – but the aim of the staged response is to prevent the need for such drastic measures with successful early intervention.

When it comes to safeguarding critical but dangerous infrastructure and ensuring that heavy, valuable industry is also safe to the local population, fire safety professionals need to use every resource at their disposal. That means sensitive detection, staged alert and alarm levels, clear visualisation, fast information relays and a suitable response should the worst happen.

For more information, contact Securiton +41 58 910 50 50, info@securiton.com, www.securiton.com

New FireClass Essential Panel

Johnson Controls has announced the new FireClass Essential conventional fire alarm control panel. The cost-effective panel is simple to use, install and maintain right out of the box, with little to no training required for setup and operation. The Essential Panel makes reliable and compliant fire detection easily accessible for small commercial facilities like schools, shops, restaurants and medical offices.

"We designed the new Essential Panel with simplicity, functionality and affordability in mind. It's the perfect product to round out our complete portfolio of conventional detection panels and devices," said Tony Gryscavage, Director, Product Management, Fire Detection Products at Johnson Controls. "With this new Essential Panel offering, FireClass can offer customers the latest conventional technology at a competitive price, providing compliant fire detection that's simple to use and fits any budget."

The panel's compact, plastic construction features durable covers and a straightforward, easy-to-understand interface that is simple to configure and operate. It offers a delayed option to minimise false alarms and walk testing to confirm reliable operation. Additional features include disable capability for sounders and conventional zones as well as buttons for silence, resound and reset.

The FireClass Essential Panel is available in two- and four-zone models. Each zone can support up to 32 devices, with a maximum of 64 devices for the two-zone model and 128 devices for the four-zone model. The panel supports all FireClass 600 and 700 series conventional detectors, sounders and devices. It meets EN54-2, EN54-4 approvals and is listed as part of the EN 54-13 system certificate, the latter of which goes beyond the basic standards that most conventional panels must meet.

The products in the FireClass conventional portfolio, including the Essential Panel, are compatible with other available products in the market and can act as a drop-in replacement in installed systems. The Essential Panel is ideal for both new construction and retrofit applications.

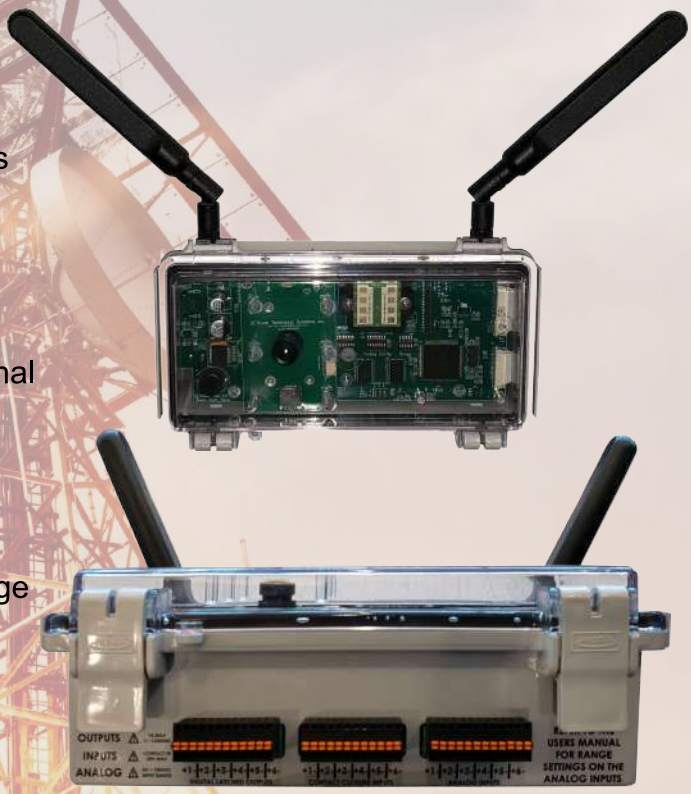
TOWER-TECH

Keep an eye on your critical infrastructure locations from miles away...

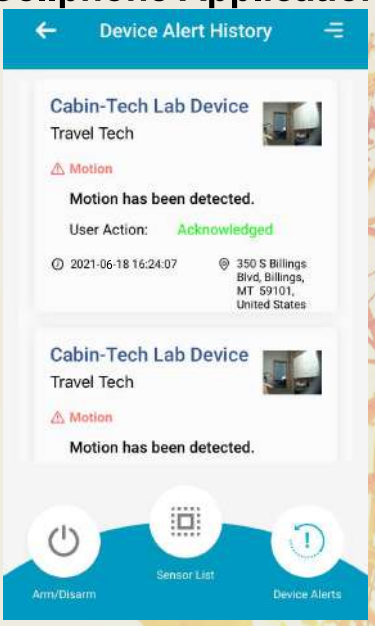
FEATURES:

- ► Motion/Single Image Capture When someone enters the site
- ► Cellular notifications of detection events
- ► Power is lost/restored
- ► Set High/Low alarm points
- ► Temperature probe for internal or external monitoring
- ► Critical cabling is cut/stolen
- ► Critical equipment falls outside the user set ‘safe range’ of current or voltage

Additional monitoring/control points:
- 6 Opto-Isolated Inputs
- 6 Analog Inputs
- 6 Digitally Latched Outputs



Cellphone Application



Web Management Portal

TRACER®
TECHNOLOGY SYSTEMS
TECHNOLOGY THAT SAVES LIVES

+1 (406) 203.1955
www.cabin-tech.net

MADE IN THE USA

Smart firefighting

By Winter Leng, ICT Specialist and Senior Technical Manager at Hytera.

Winter Leng.

Firefighting is a dangerous and challenging task where every decision matters. To safeguard lives and property from fire, the adoption of modern technologies is crucial. Smart firefighting, powered by a wide range of technological advancements, such as broadband communications, IoT, and AI, creates a proactive and efficient approach to fire prevention and responds to emergencies effectively.

Advanced wireless communications and smart sensors play vital roles in this transformation in obtaining and transmitting real-time awareness and facilitating incident command and control. Integration of technologies, like modern smart radios, ad-hoc repeaters and MESH, cellular LTE/5G, ensure seamless communications and real-time information sharing among firefighters, commanders, and dispatchers throughout all firefighting stages.

This article delves into these technological advancements empowering firefighters with 'knowledge is power' and explores how fusion tactical networks and modern radios transform firefighting operations and enhance health and safety.

1. Reliable two-way radios

For decades, two-way radios, powered by push-to-talk (PTT) voice technology, have been the go-to communication tools for firefighters. Their efficiency and reliability make them indispensable in critical situations, allowing swift status updates and commands by simply pressing the dedicated PTT button and speaking.

The shift from analogue to digital technology has further improved voice clarity, data service (SDS), and spectrum utilisation, resulting in more efficient and effective communication. In addition, global standardisation efforts for interoperability among vendors, the establishment of public-safety-grade (PSG) systems with high availability and the use of ruggedised devices for harsh environments have played crucial roles in the success of PMR (private mobile radio) worldwide.

Notably, public safety two-way radios are purpose-built to excel in touch environments, featuring rugged designs to withstand vibration, impact, extreme temperatures, and exposure to dirt and water. These reliable radios ensure that first responders can carry out their operations effectively. Additionally, they support hands-free operations for firefighters wearing bulky gear and provide man-down emergency alerting.

With necessary intrinsically safe (IS) certification for use in explosive environments, these radios are crucial for ensuring the safety of firefighters. In contrast, commercial off-the-shelf (COTS) devices lack the required reliability and durability for emergency responders, making them unsuitable for demanding firefighting conditions.

2. The emergence of multimedia and IoT

In the future, firefighting demands a shift from relying solely on voice communication to embracing data and video for enhanced situational awareness and decision-making, known as Smart firefighting.

Multimedia services like PTToC and 3GPP MCX will play a crucial role in converging voice, data, and video services, enabling smart fighting applications like video streaming, sensor data sharing, and location tracking. Smart devices like hybrid PMR/LTE radios will ensure reliable communication and high-data transmission, seamlessly connecting to various networks for efficient emergency response.

Safeguarding firefighters' health and safety is paramount, and mission critical IoT technologies play a vital role. Incorporating biometric, environmental and location sensors enables real-time monitoring of critical information like temperature, vital signs, hazardous materials and positioning, ensuring safety and transforming firefighting operations.

While voice communication remains essential, video-as-a-sensor (VaaS) offers an invaluable addition, enhancing situational awareness. Smart radios with push-to-video features access video feeds from body cameras, carry-on cameras, CCTV, UAVs and more, providing real-time visual information and valuable perspectives of the scene. Specialised video applications, like helmet-mounted cameras with thermal imaging, help firefighters quickly detect victims and assess interior conditions, contributing to comprehensive situational awareness.

3. Building a robust sensor data network on the scene

To ensure effective communications and sensor data transmission, a reliable field network, known as Personal-Area Network (PAN) and Local-Area Network (LAN), is essential, especially in areas with limited network coverage. Integrating various communications systems, such as DMO, repeater, MESH, LTE/5G, satellite and airborne replays, allows IC to establish a robust tactical network on the scene. This mesh network enables seamless information sharing among firefighters and commanders, avoiding a single point of failure.

Notably, ad-hoc networking and cognitive radio technologies, such as ad-hoc repeater and advanced mesh have gained popularity due to their flexibility and robustness. With their multi-hops relays and self-organisation capabilities, these technologies can be deployed effortlessly and penetrate dense construction materials and thick smoke, making them practical and reliable in firefighting scenarios.

In addition, video applications rely on high-data transmission, where advanced mesh technologies play a crucial role in reliably maintaining a high-performance data link, also complementing two-way radios through their higher audio fidelity. Moreover, technological convergence in devices has resulted in the development of hybrid radio, a single device that combines multiple wireless and networking technologies.

These smart devices can easily access and switch across different networks, eliminating the need to carry separate radios. Serving as a hub, they connect wearable sensors and communication systems, transmitting critical data about firefighters' health and safety. By embracing the apps ecosystem of the commercial world, these versatile radios have become powerful tools for firefighters.

4. Harness fusion wireless solution to enable robust, seamless connectivity

The fusion wireless solution is transforming firefighting with advanced tactical communications. It combines lightweight wireless units, including ad-hoc repeater, advanced mesh, Wi-Fi and LTE, with hybrid-mode smart radios, creating a flexible and robust ad-hoc network without infrastructure. The solution enables seamless communications across different networks without disrupting critical operations while delivering voice, data and video services. Additionally, it includes a command post with built-in LTE and satellite backhaul for central dispatch and monitoring by IC at the scene. With these features, the solution extends dependable network coverage to remote areas or inside structures, enhancing situational awareness, decision-making and firefighter safety.

Key components of the solution are:

a. Manpack ad-hoc repeater: Going beyond the traditional repeater, it provides long-distance separate voice and low-data communications with its powerful 10 W RF and multi-hops and aerial relay capabilities, ideal for complex terrains and conditions.

b. Cognitive manpack mesh: This advanced technology offers a high-performance data link for video and voice data through intelligent routing, MIMI, resistance to interference, multi-hops and aerial reply, adapting to challenging RF environments and scenarios.

c. Command post: An all-in-one centralised platform for ICs that integrates voice dispatch, video monitoring and GIS mapping for unified on-scene coordination and real-time decision-making during firefighting operations.

d. A fleet of hybrid-mode rugged smart radios: Specially designed for modern firefighters and emergency responders, these radios combine multiple wireless technologies and come with features like one-button switch and call, making them powerful tools. With these radios, firefighters can communicate quickly, access apps, monitor vital signs and share real-time information across various networks through firefighting stages.

Fusion solution and the fleet of hybrid-mode radios

With the fusion of these advanced technologies, firefighters gain improved communication reliability, enhanced situation awareness, access to critical apps, and real-time health monitoring, resulting in smarter firefighting operations and enhancing their capabilities during life-saving missions.

Furthermore, the integration of the Public Safety Answering Point (PSAP), control room, PMR and LTE networks, and the field fusion wireless network empowers firefighters with hybrid-mode device fleets. These devices serve as powerful tools throughout the entire response stage, enabling quick response to assignments, staying connected with dispatchers via multimedia service while en route, and facilitating robust voice and data communications in challenging fireground conditions. Additionally, the devices and platforms record invaluable data for post-event analysis, contributing to improvement in fire response strategy and techniques.

In conclusion, as firefighting continues to face ever-evolving challenges and dangers, leveraging new technologies and innovative solutions is crucial for improving firefighting effectiveness and safety. By integrating smart radios, innovative wireless technologies, fusion field networks, and IoT sensors, firefighters can respond faster and coordinate better during emergencies, protecting lives, property, and their own safety.

Find local Hytera suppliers at www.hsbd.co.za/brand-suppliers.aspx?agacc=5711

Fidelity SecureFire steps into critical fire response space

With the majority of fire stations around the country being crippled by a lack of resources to offer effective responses, Fidelity Fire Solutions, a division of the Fidelity Services Group, is stepping into the forefront of fire safety with a unique own 'first responder' model, Fidelity SecureFire.

The service is already available in Johannesburg and Tshwane as of 1 August and includes a fire chief and 55 fully trained firefighters on standby 24/7.

Wahl Bartmann, CEO of Fidelity Services Group says just this month the group has had to respond to 35 fires, 78% of which were in the Tshwane area and 21,6% in the Johannesburg area.

Fidelity ADT armed response officers will also be 'first responders' as part of this critical new service. These first responder vehicles are certified for Level one and two firefighting and are equipped with fire-fighting packs called the Roto Pack Lithium Gel and FFG Gel, which provide a reach of nine to 12 metres.

The three-pronged model will fully equip these firefighters to manage Class A and B fires involving ordinary combustible materials, flammable liquids, or gasses like gasoline and oil. These fires can be particularly dangerous due to their potential for rapid flame spread. "We will also be able to attend to Class D fires with our Lithium extinguishers for fires caused by electronic devices like smartphones, laptops and tablets and, of course, electric vehicles. These fires are unfortunately becoming more common with our ongoing loadshedding schedule impacting appliances."

The community will now have access to 350 first responders and 10-second responders comprising Mahindra and Land Cruiser RIVs. The service is reinforced by rapid intervention units comprising six-plus fire engines, water tankers and pumps to supply water.

With one large 18 000 litre tank on site already, the plan is to get another large tanker as well as two smaller ones with a 9 000 litre capacity. "One of the key challenges experienced in our existing municipal structures is the lack of water in the fire hydrants, so even if the response is on time, they may be hamstrung with no water."

"Fidelity SecureFire will be able to respond effectively to large fires, all domestic household fires, small to medium commercial fires and fires at shopping centres, schools or churches. "Basically, wherever the danger is and where our customers and/or their property are in harm's way due to a fire, they can rely on us being their first line of defence," says Bartmann.

Bartmann emphasised that the service would in no ways be competing with the existing fire service. In fact, it would complement and support their efforts and the teams will work very closely with the existing fire departments. "Our target is to reach any fire within five minutes," he says.

Roll-out will commence in KwaZulu-Natal in December 2023 and then in Cape Town between April – June 2024, followed by the balance of areas where Fidelity operate.

For more information, contact Fidelity Services Group, charnelh@fidelity-services.com, www.fidelity-services.com

Fire prevention for energy systems

With the significant push towards renewable energy, such as wind and solar, the demand for battery energy storage systems (BESS) has grown exponentially.

Most BESS utilise lithium-ion (Li-ion) batteries, bringing particular fire risks. There are many stories of laptop and cell phone lithium-ion batteries catching fire, and on a larger scale, there were 23 BESS fires in South Korea alone between 2017 and 2019, resulting in losses valued at $32 million.

As a result, there is a rapidly evolving regulatory environment to address these risks. One of the leading regulatory authorities in the USA, Underwriter Laboratory (UL), developed UL 9540A to address 'Thermal Runaway Fire Propagation in Battery Energy Storage Systems'. Already there have been four iterations of the standard since 2014.

Most authorities will agree that there are two main windows of opportunity to implement fire protection measures for BESS. The first and most critical is the detection of off gas (battery electrolyte vapours), which typically occurs 11-12 minutes before smoke is generated. Li-ion Tamer GEN 3 from Xtralis is designed to monitor Lithium-ion batteries of all chemistries and to detect any off-gases to provide an early warning to BESS system providers. When the Li-ion Tamer GEN 3 alerts to the presence of an off gas, it can activate several mitigating actions. Perhaps the most important is shutting down power to the affected cell(s). Additionally, the gas detection equipment can:

- *Activate a ventilation system within the BESS enclosure to remove flammable gases and heat.*
- *Activate local and remote alarms.*
- *Provide an early warning for operators to take additional measures.*

If preventative measures are unsuccessful and a damaged lithium-ion battery ignites, fire suppression measures must be implemented to contain the resulting fire and minimise the potential for propagation to other battery cells within the BESS.

Stat-X condensed aerosol fire suppression is the fire suppression system of choice of several lithium-ion battery OEMs and leading global BESS integrators, having undergone rigorous private and commercial testing in line with UL and NFPA standards. The tests concluded that the Stat-X agent successfully extinguished single and double-cell battery fires and prevented a re-flash of the fire due to its residual nature.

It is also important to note that condensed aerosol fire suppression agents have no global warming or ozone depletion properties. They do not harm sensitive equipment and require limited clean up after discharge. The agents are rated for normally occupied areas.

Technoswitch believes the combination of Li-ion Tamer and Stat-X offers an ideal detection and containment solution for BESS fires.

Paxton opens first experience centre in South Africa

The new Paxton Experience Centre in Johannesburg is now open and welcoming security installers and end users who want to see Paxton's products in action.

Werner Geldenhuys, Paxton's Regional Sales Manager in South Africa, said, "Providing opportunities for our customers to get hands-on with our products is what we strive for at Paxton. The Experience Centre is a dedicated venue for security professionals and end users to get to know our easy-to-install and use access control solutions."

"We see increasing demand for our products in South Africa, so we built our own product hub. Thank you to all customers who have supported us and enabled us to grow continually in the market."

The Paxton Experience Centre is the manufacturer's first product showroom in South Africa. It showcases its core product range, including access control systems Net2 and Paxton10, door entry solution Entry, and energy efficient wireless door handles, PaxLock Pro.

Paxton's expert trainers will be onsite to conduct product demonstrations and are available to discuss customers' specific installation projects.

Geldenhuys continues, "Installers are welcome to invite their customers to the Experience Centre. Also, security system users interested in learning more about our products can visit us and experience the systems first-hand."

Email experience@paxtonaccess.co.za and book a time slot to see how Paxton's smart access control solutions can help secure your site.

Kentec
Electronics Ltd

Safe in our hands

Life Safety solutions with leading installation support and training services

From early warning through to **FIRE** detection and suppression, Kentec Electronics is a world-leading manufacturer of life safety solutions, with the international standards to match. We offer unrivalled technical support to installers – ensuring that every installation realises the full benefit of our panels' highly-sophisticated, SMART features. Everything we do is designed and manufactured to make the lives of our installers and end users easier. It's a philosophy that's embedded in our culture and one we call Manufacturing Expertise.

We protect you, always.

+44 (0)1322 222121
www.kentec.co.uk

Modern retail requires modern AI and surveillance

Marcel Bruyns.

By Marcel Bruyns, Sales Manager for Africa at Axis Communications.

If there is any sector that has been subject to dramatic digital transformation, for both consumers and businesses, it's retail. Whether you're shopping for daily groceries, investment appliances, or your next big furniture purchase, the experience is not the same as it was 10 years ago. For operators, shifting consumer trends and fluctuating business environments demand flexibility, innovation, and an ability to scale operations accordingly.

That's a lot for retailers, both big and small, to consider. Fortunately, advancements in new technologies like AI and smart analytics have given way to new tools and resources. In this case, offering data and data analytics to learn more about business activities and unlock new insights.

South Africa's retail sector faces intense economic challenges, such as decreasing trade sales and continuing inflation[1]. This is in addition to always-on challenges such as crime; reports suggest increases in property related crimes and burglaries at non-residential premises[2]. The pressure is on operators to attract customers with a shopping experience characterised by convenience and quality of service. At the same time, they need to leverage the power of technology to cement that experience, secure their premises, and extract maximum value from cutting-edge smart solutions.

Accessing the future

Retailers have a lot to gain by introducing intelligent, IP-based surveillance and access control measures to their operations. The result of that integration is an interconnected technological ecosystem that keeps operators ahead of the competition and up to date with customer expectations.

Picture the typical retail premise, complete with customer and staff entrances, aisles, and cashier points. Operators can use advanced scheduled door access with additional authentication measures needed outside of business hours[3]. Network intercoms allow for authorised access with the help of QR codes, complemented by IP audio that can make announcements or play in-store messages. Applying these technologies, operators can enhance cashier points with fast lane checkouts; customers scanning a QR code on their receipt or mobile device via an integrated smart camera at a terminal.

Access control becomes part of centralised store management, which itself can be done remotely or in a hybrid manner. Scalability is also covered. Regardless of the size of the store or how many stores you operate, edge-based access control with multi-site capabilities allow operators' security measures to grow as their business does.

These use cases represent major changes for the retail employee experience, but not to their detriment. According to IDC research, many retail associates believe technology will enable them to do their jobs more effectively and lead to them being more engaged with their organisation[4]. All of this forms a working scenario, where retailers can secure and survey more effectively, while learning more about themselves thanks to actionable data insights.

The power of AI

In today's business world, data is a valuable commodity and data insight is a way for enterprises to stay a step ahead of their competitors, but innovations in AI have yielded new ways for enterprises to leverage and respond to that data in meaningful ways.

One of those innovations is 'computer vision', which is set to transform the retail sector[5]. A subcategory of AI, computer vision entails devices scanning and analysing their surroundings the same way a human would, providing operators with insight into customer behaviour as well as product quantity and availability. If there's a product that's flying off the shelves or being ignored by customers, operators can identify the trend in real time. The same technology can be applied for customer and premise monitoring; identifying anomalous behaviour or incidents that require immediate action.

This use of AI feeds into the greater adoption of cloud-based and networking technologies by retailers. Using network cameras, high resolution video is processed at the edge and transmitted to the cloud. Actionable insights are packaged as notifications and sent to onsite or offsite personnel, or other business management software solutions, like inventory management, that then trigger human or automated responses.

Shopping for intelligence

Network and surveillance solutions stand to benefit from the increased capabilities of applied AI and data analytics. As an important sector of South Africa's economy, the retail industry can benefit from a holistic and AI-enabled approach to security and site management, culminating in an upgraded customer experience and comprehensive insight into business operations.

"Empowering Security Solutions: Identbase GmbH, Europe's Leading ID Card Company"

Identbase GmbH are the Europe's leading ID card company specialising in ID card printers, card printer ribbons, blank plastic cards, contactless cards, card readers, lanyards, ID card holders , ID card reels, card design software and much more. Our key company milestones are listed below:

✓ 30+ years industry experience

✓ Over 25,000 customers

✓ Sold to 100+ countries worldwide

✓ Price match promise on any product

Identbase GmbH delivers both, nationally and internationally to hubs, branches, regional offices and headquarters daily. We provide unique opportunity to combine your domestic and/or global purchasing power to maximize your profitability.

For more information call a member of our International expert team on +49 5931 9989 1355.

Key Contact Person: Nick Markoski
Title: International Sales Manager
Contact Email: nick@identbase.de
Contact Phone: +49 5931 9989 1355

Our Products portfolio:

Card Printers	Cleaning materials	RFID Keyfobs	Magnetic stripe readers	Card holders
ID Ribbons	Software	RFID Cards	Barcode Scanners	Lanyards
Laminates	Blank cards	RFID Wristbands	Badge Reel's/Yo-Yo's	Access Control Systems
Printer Spare Parts	RFID Disc Tags	RFID Labels	ID Clips	Mailing Services
Hybrid Cards	RFID Readers	Smart Card Readers	Custom Printed Lanyards	Time & Attendance Systems

Stadium security with Panomera

The Alsancak Mustafa Denizli Stadium in Izmir – named after former Turkish football player and current football coach Mustafa Denizli – is a multipurpose stadium that mainly hosts football matches. With over 15 000 seats, it is one of the medium sized stadiums in Turkey. Originally built in 1929, it was demolished in 2015 and reopened after reconstruction in November 2021.

Up to 15 % fewer spectators due to riots

In Turkey, stadiums are usually owned by the Ministry of Sport, which then grants the rights of use to an operator. In the case of the Alsancak stadium, the operator is Altay Izmir, an Izmir-based football club that currently plays in Turkey's top professional league. The club, like so many other football stadiums, has had its fair share of repeated incidents and threats to spectators and players. These have included verbal abuse and even the throwing of objects onto the pitch. In addition to the intangible damage to the image, the consequences have been painful, ranging from traditional fines to the closure of an entire block of spectators – a loss of 1000 to 2000 spectators per home game, and that on a regular basis.

Recognising perpetrators?

Under these conditions, the operators were looking for a solution that would allow them to detect and track potential offenders reliably. The tender specified a minimum resolution density of 144 pixels per metre (px/m), which is also required by law. This means that there must be at least 144 pixels in the camera image to represent every metre of reality in the stands. This value is between the recognition (125 px/m) and identification (250 px/m) qualities specified in the IEC EN 62676-4 standard for video surveillance systems.

Only ten cameras to monitor the stands

To find the most suitable solution for the Alsancak Stadium, the Ministry of Sports decided to invite various manufacturers to a comparative test. After receiving the proofs of concept (PoC) of several companies, the owner chose a solution from the German manufacturer Dallmeier Electronic. In addition to around 140 single-sensor cameras for corridors, outdoor areas and entrances, only ten Panomera multifocal sensor systems are required for the particularly critical grandstand surveillance.

39% more resolution than required

The low number of camera systems required for grandstand surveillance is due to the patented multifocal sensor technology; Panomera cameras combine the images from up to seven detail sensors and one overview sensor in a single camera system. This provides the user with a high resolution overview of the entire area to be monitored, which acts as a single image of a vast environment.

Within this overall picture, system operators can now open any number of detail views at the same time, while the overall scene is always available in high resolution – even during recording, which is essential for possible prosecution. This provides an optimal overview of the situation and ensures that all events can be followed in real time, in high resolution and in detail. Thanks to this technology, a minimum of 200 px/m is now available throughout the Alsancak stadium instead of the required 144 px/m – 39% more than originally required.

Remote FAT and training

Due to the COVID-19 pandemic, the stadium's technicians were unable to travel to Dallmeier's headquarters in Regensburg, Germany, to commission the system and attend classroom training. For this reason, the Dallmeier Factory Acceptance Test (FAT) took place online. The entire system was set up, configured and remotely accepted in the FAT centre in Regensburg. The training of the technicians and operators was carried out by Dallmeier Turkey experts on site.

Serkan Atalar, CEO of RESA Construction Electromechanical Inc. CO, the installer company that implemented the project, is very pleased, "Dallmeier's collaborative approach, as well as the high-tech products and after-sale support they offered, were very impressive. We thank Dallmeier Turkey for the great cooperation."

Serkan Atalar summarises. "Alsancak Stadium only needs three system operators with one monitor each. They also have two workstations for the police and management. The solution always gives them 100% control of the security situation in the stadium, allowing them to react immediately and reliably track down perpetrators. All this is at a low total cost of ownership and with minimal manpower thanks to the unique multifocal sensor technology."

unv

New & Exciting Releases from Uniview!

State-of-the-art IP Surveillance solutions to fit every need!

The safety of your home, business and assets is top priority. Invest in an effective security system. Uniview offers a wide range of exciting surveillance products that deliver high-quality recording and smart intrusion prevention features at an unbeatable price!
At MiRO we have the entire range in stock. Shop today!

SCAN ME
For more info

MiRO

IP Convergence Solutions

CALL or WHATSAPP **012 657 0960**
OR VISIT **www.miro.co.za**

Turkish university installs IDIS surveillance

IDIS Solution Suite VMS has streamlined operations and transformed security for the Social Sciences University of Ankara (ASBU), Türkiye.

ASBU's historic city centre location, with its night-time economy, makes it the study destination of choice for around 5500 students annually. But with such a busy site, the university also has to deal with an increased risk of incidents, including crime and anti-social behaviour.

A 350-camera surveillance system, monitored 24/7 from ASBU's dedicated control room, had been expanded several times over the years, however, the resulting mix of six different vendor brands had left the VMS struggling with frozen live images, a hard-to-manage data burden, and difficult-to-use controls.

The IDIS integration partner was asked to devise the best upgrade route. In an onsite proof of concept demonstration, the company showed how IDIS's VMS, IDIS Solution Suite, (ISS Expert) could quickly register all the mix-and-match cameras and devices, including recorders and a 3 x 3 video wall.

With the project now completed, the result is eliminated complexity, allowing seamless control, full functionality of all cameras regardless of the brand, and transformed ease of use for operators. They can now control the system from their workstations as well as from the video wall, with browser features allowing the university's fire system to display on the same screen. IDIS MapVue is also being added, with a schematic showing the locations of the cameras, to improve domain awareness and make navigational playback easier.

The IDIS solution is easy to maintain and expand, and a further 100 cameras will be added in the next phase of the project when two renovated accommodation buildings will also benefit from upgraded surveillance. The new cameras will include IDIS 12 MP Fisheyes and domes, which are ideal for the historic setting where ceiling heights are up to 9 m, and where full coverage with HD image capture is needed, with minimal structural modifications.

To save bandwidth and reduce the storage burden, cameras in corridors, the basement, and other key areas have been set to record only when motion is detected, using a combination of IDIS Motion Adaptive Transmission and ONVIF motion detection on the other brands.

ASBU's security team can now easily comply with requests from law enforcement agencies for video evidence. Bookmarked event recording makes it easy for ASBU operators to skip from scene to scene when reviewing recordings.

In the next project phase, IDIS Deep Learning Analytics (IDLA) tools will be added for even faster, automated footage review. The IDIS solution also makes it easy and affordable to expand the system, for example, with IDIS 310D servers that will allow more cameras to be added and increase storage capacity to ensure longer retention periods without increasing storage costs, thanks to IDIS Intelligent Codec.

"IDIS Solution Suite solved all the problems we had with our complex and ageing system, with an easy upgrade that extends the life and performance of all our cameras," says Zafer Buldu, Manager of Hardware & Technical Services, ASBU.

Koray Ozyildirim, IDIS Turkey Country Manager, said, "IDIS Solution Suite has turned ASBU's cluttered and failing system into a powerful, integrated surveillance solution that is easy to use, adapt, and upgrade, with the assurance of an extended lifespan backed by industry-best warranties."

For more information, go to www.idisglobal.com

DualCurtain Outdoor

Wireless outdoor bidirectional curtain motion detector

Smart motion detection

Two independent detectors in one

30m

30 m detection range

IP54

Weatherproof design

Free apps for installers and end-users

ajax.systems

macOS

Windows

iOS

Android

Watch the video

No missed alarms and reduced false alarms

Remote sites have always been more vulnerable to opportunistic intrusion, but over the last two years in particular, sites such as solar farms or industrial parks have become more common targets for criminals. Instances of solar farm theft, for instance, have risen dramatically, correlating with both the rising costs of compound metals and the increased number of solar farms across the EMEA region. Similarly, theft in warehouse and logistic facilities increased.

The challenges of protecting remote sites

The fact that a large number of these sites are located in isolated areas typically means that security is monitored and managed remotely, and the use of video surveillance is essential to confirm if an alert is real. Beyond visual verification, the biggest challenge faced by remote security teams is to reliably detect any intrusions as early as possible in order to take the appropriate response and deter theft or damage to the premises.

Commonly, remote sites can be prone to environmental conditions such as uneven terrain, lack of lighting, vegetation, changing weather and temperatures. To add to the complexity, typically the perimeter of these facilities is large and has many different zones to protect, each with its own characteristics. All of these elements can be challenging for some technologies and can increase the chances of nuisance alarms or even worse – missed alarms. Nuisance alarms can be extremely costly, dispatching response teams to remote sites for verification of non-genuine intrusions.

Equally important is the eroded trust in the system, which is a natural outcome when guards are repeatedly attending false alarms. However, there is no question missed alarms can be significantly more costly; the loss of assets or damage to facilities is not only costly in itself, it also impacts operational continuity, leaving businesses facing the challenge of lost revenues or even periods of being non-operational.

What are volumetric thermal detectors?

Volumetric thermal detectors, also known as thermal motion detectors or passive infrared (PIR) volumetric sensors, are used to detect motion and changes in temperature within a defined area. They work by capturing the infrared radiation emitted by objects and analyse the temperature variations to identify movement and human presence. This allows them to accurately differentiate between a human presence and environmental factors that can trigger false alarms, such as moving foliage or changes in weather and ambient temperature.

As they rely on detecting heat signatures rather than visible light, volumetric thermal detectors, such as OPTEX's REDWALL SIP series, function effectively in low light or even complete darkness. This makes them a perfect solution for areas which don't have thorough illumination or which are subject to challenging environmental conditions, including fog, smoke or harsh weather, where other technologies might be limited. The main benefit of this reliable detection capability is to provide the surveillance system with the intelligence to filter out the main causes of false alarms and, more importantly, to avoid any missed genuine alarms.

OPTEX REDWALL SIP sensors have been deployed across thousands of remote sites in Europe where they contribute to creating a more reliable and efficient surveillance system. REDWALL SIP integrates with IP video, LED security lighting, audio and other security equipment and contributes with its reliable detection to ensure there are no missed alarms.

Highly reliable and accurate detection

One of the key challenges when protecting remote sites is maintenance; the fact that REDWALL SIP sensors can automatically adjust to the environment and the unevenness of the terrain is a huge support to the security team and means they do not have to physically attend the site to change the settings of the sensor. It is also a robust and durable device which ensures a long product life and cost effective solution.

Volumetric thermal detectors also provide a wide coverage area, typically covering a longer range compared to traditional short-range PIR sensors. OPTEX REDWALL series includes a wide range of sensors offering wide areas up to 30 x 50 m or corridor detection areas up to 100 m.

It provides a uniform detection in the whole protection area, which is achieved thanks to different sensors housed in the same device – for far zone, near zone and creep zone. The different zones allow PTZ cameras to track intruders across zones and also provides the possibility of having independent alarm outputs, as well as the implementation of detection logic.The logical configuration of detection means that you can combine two zones to know in which direction the intruder is moving and whether it should trigger the alarm or not. In addition, the creep zone below the sensor allows self-protection in case of vandalism against the equipment.

For more information, contact Optex, sales-sa@optex-europe.com, www.optex-europe.com

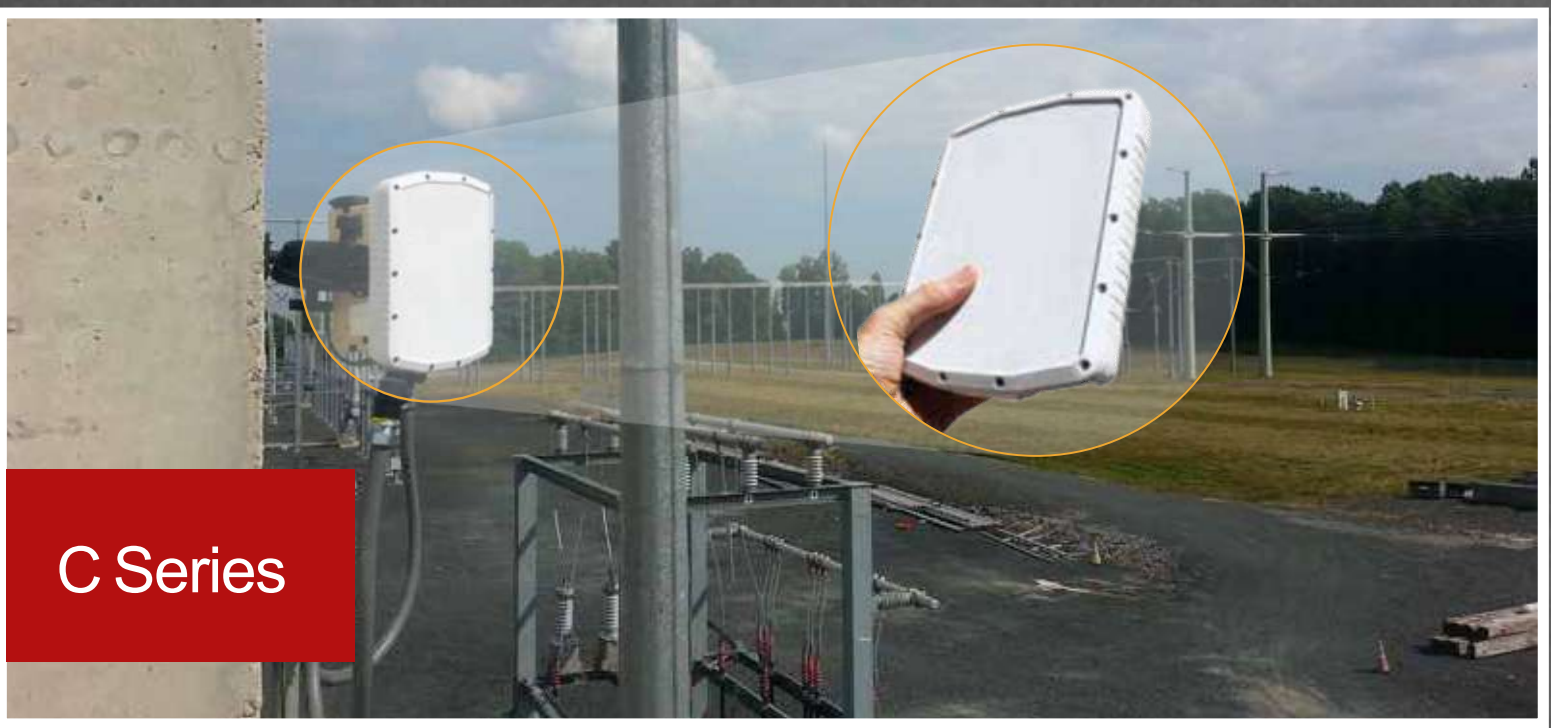
ASTROPHYSICS®

THE ULTIMATE
In X-Ray Imaging

www.astrophysicsinc.com sales@astrophysicsinc.com

TOMORROW'S TECHNOLOGY FOR TODAY'S SECURITY™

Ground & Over-Water Radar



C Series

GROUND RADAR COVERAGE COMPARISON

Contact: Scott Wilson
0829094566
031 942 3853
Scott.wilson@a1fenceproducts.co.za
www.a1fenceproducts.co.za
www.a-1fenceproducts.co.za/Radar.php

Protection Beyond Fences

SpotterRF

Protecting Assets,
Protecting Borders,

A-1 FENCE
Fence & Fence-abilty

COMPACT RADAR SECURITY?

PROTECTION BEYOND FENCES ™

Existing security systems are all about protecting the fence line. SpotterRF Radars offers a pre alert about possible intrusions that may occur over the fence line and even internally. SpotterRF radars are powered with a superior target tracking algorithm capable of detecting human, vehicle, drone or animal intrusions via land, sea or air thus offering a complete package of security on all fronts.

The radars also seamlessly integrate with PTZ cameras and other video surveillance systems making it very compatible and the early warning layer that was always missing.

SO WHY RADAR?

WIDE COVERAGE AREA

Whether you are required to protect an area big or small, our radars come with a coverage range of 15 - 380 acres so it can fit into different applications. This significantly reduces the need for extra cameras and radar gives you a superb early warning security advantage.

PORTABLE

SpotterRF Ground Surveillance Radars can come with a well-designed case which makes it easy to transport and very quick to deploy in different areas. It can be mounted on trailers for easy deployment or preset masts can be set up for the radar to be moved around.

VERY LONG LIFE

SpotterRF radar has a Mean Time Before Failure of 90,000 hours which makes it rugged & ensures longevity. It has no moving parts so low maintenance and because of its design material it cannot rust.

CONTROL NUISANCE ALARM

Animals, vegetation, and weather are the most likely causes of nuisance alerts. SpotterRF Technology has the capability to adapt to its environment, to maintain high detection, and eliminate nuisance alarms. It will only cue the cameras to real threats thus eliminating nuisance alarms.

SpotterRF

DETECTS IN ANY CONDITIONS

No issues with direct sunlight, reflections, rain, hail, snow, mist, Sea spray, or dust. So where other Detection and monitoring systems have weaknesses, radar will keep on tracking, giving you ultimate security.

Coupled with a good PTZ your security protection now covers a larger area, tracking, recording, and seeing where the intruders came from and are hiding.

With quick installation, very little maintenance, and no down time, SpotterRF is becoming a much-needed defense tool in your security layers.

With the superb AI any new nuisance alarms that appear can easily be removed with training the system. With multiple tracking of 20 targets you will not miss anyone, and your camera can be set to monitor the nearest, newest, fastest threat or particular zones whichever way you choose to set it up.

For a site demo we can set up mock radars on a Google map to show the coverage and positioning to best suit the client. These can show exclusion zones and alarm zones giving the client a good idea of the power of the system.

Contact: Scott Wilson
0829094566
031 942 3853
Scott.wilson@a1fenceproducts.co.za
www.a1fenceproducts.co.za
www.a-1fenceproducts.co.za/Radar.php

About A-1 Fence
We are an international fence manufacturing company with global representation. Our strength is our ability to offer internationally accredited fencing products from borders to domestic applications. **NB:** We do not install, we are suppliers only,

The importance of CCTV for internal perimeter protection

By Dr Craig Donald.
For years, history has reflected the importance of perimeter defence. Whether a primitive palisade, high walls, castles and fortresses for defence, or barbed wire and electric fences, and patrolling guards; mostly the focus is of keeping dangers out.

The Trojan horse and gaining access to Troy was one of the earliest and widely popularised breach events, deployed to gain access to the interior of a defended area. It seems this technique is still popular given accounts I heard this week of criminals using a modern truck loaded with pallets (rather than a wooden horse), which they hid behind to gain access to airside in a major airport, showing the technique still has wide application. However, the focus on keeping things and people from getting out has not shown nearly the same dedication, unless you are working in places like prisons, high-risk biological labs, or sites working with precious minerals.

Yet one of the central themes associated with theft from any kind of site or operation involves the penetration of protection barriers outwards. Whether a casino, logistics facility, production enterprise, a precious minerals operation, or a shop where you buy your regular groceries, protection from internal leakage to stop stolen items becoming a torrential flow of material and affecting the organisation's financial well-being is becoming increasingly important.

The main strategy to prevent internal loss has been the use of physical barriers and access control to prevent leakage. Much of the technology associated with keeping things out, is also used to keep things in, including metal detectors, goods x-ray, full body human x-ray equipment, and searching protocols. However, we know that the penetration of perimeter barriers to facilitate the removal of product is a key tactical element of criminal strategies.

It surprises me how often there are a lack of cameras or specified operator focus on infrastructure and vulnerable points within the perimeter. Using cameras provides a great chance to use crime behaviour detection to identify the signs that criminals are compromising your perimeter protection measures. I see three main points to such camera use:

- *To preserve the integrity of your protection infrastructure.*

- *To audit that processes and procedures are in line with expected standards.*

- *To ensure that people do not have the freedom of behaviour that would enable them to compromise security precautions and facilitate theft.*

Safeguarding high-risk areas

One of the key internal security strategies is to define high-risk areas and safeguard the perimeters around them. Additional perimeters for lower risk areas may be set, or naturally delimited by the infrastructure or environment around these high-risk areas. High-risk areas define themselves by the likelihood of theft, usually because of a high value or portability of product. At a casino roulette table, the area of high value chips in the float are a focus of attention, as well as the perimeter of the layout where chips move in and out.

Security then extends to the perimeter of the gaming table where positioned people may behave in ways to cheat or steal, then to the perimeter of the gaming floor through which people may move or within which syndicates may operate, to the perimeter of the casino building and finally to the perimeter of the whole casino property. In this way, effective detection of early threat conditions on the furthest perimeters can lead to a lockdown or enhanced protection and control over high-risk areas, before they can be affected.

For example, in the case of a casino robbery, the detection of suspicious vehicles or vehicle movement outside the entrance can indicate preparation for a potential robbery, and can be proactively addressed. Entry of a known or targeted suspect into a store can result in increased surveillance, especially when moving through the perimeters of areas of high value products or commonly stolen items. Inversely, compromising of a high-risk area that may involve theft of chips off the layout or float, can lead to a quick recognition of behaviour around the table and sealing off the gaming area or exits to the casino.

Similarly, storage of cellular phones, or other high value electronic items in a vault, secure room, safe or handling area should be monitored and audited with cameras. This ensures that people do not move items through to an area with a less secure facility, without adherence to procedure. If detected it should be possible to track the suspect through the various areas, with the last resort held at the store or production facility exit.

Detecting suspicious activity at the perimeters

Shifting things through perimeters from one area to another using concealment, disguise or packaging, to areas where protection is not as much of a priority is a common theft technique. Ideally, the crime behaviour or violations of procedure associated with unauthorised movement of goods should be identified at the core area, although with each perimeter crossing it still means there is some chance of detecting the theft.

Crime behaviours that assist in detection of theft would include unusual positioning around high value items, introducing or using blind spots, looking around, loss of natural body flow due to tension, and increased levels of anxiety. Where electronic tagging systems are used to protect perimeters – operators need to be able to recognise the signs that people are using equipment to compromise tags, including specific foil bags used in the industry, or packaging containing foil, or other methods used to move tagged items beyond detection points.

Perimeters are not only around the sides of a site, but they also exist to separate higher and lower areas. Especially in some environments where there are multiple working levels and where items or material can be dropped, spilled, poured, or cascaded down to less protected working areas or places where material can be accessed or even concentrated for greater value

more easily. Use of drones has also been reported as a way of moving material up out of otherwise restricted areas.

Operators would need to look for people in areas they do not expect them to be. Excessive loitering in a particular area, unusual carrying of containers or tools, leaving boxes open or not replacing them back in position correctly, carrying unusual packages or parcels, time spent around trollies or materials due to be moved to another area or through airlocks, and behaviour such as crouching or bending over can all indicate potential issues.

Waste material is often used as a facilitator to get things out of an area, with the items often concealed underneath material that may be unpleasant or difficult to get to such as kitchen waste, or in cleaning trollies and dustbins which may legitimately pass through perimeters. Where a company in retail or logistics deals with returns, packaging can be used to hide or substitute items, or lack of control can lead to theft of items before reintegration into the inventory. Waste bins near despatch points represent potential risk areas and may easily be used to hide or store items for later collection.

Two sides to a perimeter

Movement and positioning around perimeters are key considerations when viewing cameras for possible theft activity. This may be complicated somewhat by the volume of movement of people who are in that area for conventional purposes, whether it be people outside the perimeter using a thoroughfare, people taking a route home, and logistics or production activities that occur as part of the normal day's routine. However, the fewer people normally in that area, the more we can use cameras to identify people of interest for further viewing.

Even when there are numerous people, the patterns of movement will often make theft type of activity noticeable if one is looking out for it, especially if these happen around vehicles, doors, passageways, gullies, piles of debris or materials, overhangs, tree clusters, rock outcrops, riverbeds and deliberately introduced blind spots. I am still amazed when I see unsecured and unmonitored emergency exists, or doors to a warehouse, supposedly locked, but have people moving in and out from time to time.

Suspicious movement around the outside perimeter may not reflect intent to get into the operation, but collection of items or material that have been moved to the perimeter by being deliberately thrown, left, or channelled to a location outside of the infrastructure or property perimeter by inside theft activity and removal of product. That means we have to use cameras to monitor and review behaviour on the inside perimeter of these areas to see if there is behaviour linked to what we are seeing outside.

Conventional areas such as dispatch, collection and access control are key areas to look at to protect against loss, and monitoring transactions at these interfaces are important; activities such as validation of correct people, processes, volumes and waybills may be done remotely.

I have come across numerous cases of holes pierced in metal or brick walls and used for smuggling material through the sides of infrastructure. Pipes inserted through walls. Material being diverted using valves in existing pipes to waste or disposal areas, or even transport vehicles. Unmonitored use of emergency exits to move goods out. Use of smoking areas that allow access to balconies outside, to throw or drop goods on the outside of the facility. Toilet windows interfacing with the outside, ventilation pipes and facilities, and drainage systems, and even a case with a front-end loader tipping gold bearing material across an outside fence.

Movement and behaviours on the inside of the perimeter should therefore be monitored, particularly when there is little reason to be there as part of normal operations. In such cases, just being there without any kind of justification can mean the person becomes a target of interest and the focus of the CCTV operator. Together with coordinated behaviour of someone outside the perimeter that may strongly suggest collection rather than trying to get into the premises.

Internal dynamics and behaviour

Management therefore needs to pay careful attention to internal dynamics and behaviour around perimeters, as well as outside threats. In one case, I watched a thermal video of a suspect trying, for ten minutes, to get out of a residential estate. Not detected by operators or video analytics on a camera at the time, because all analytics were exclusively set to outside the perimeter fence. In another instance, a missing package had finally been detected, almost at the outside perimeter disposal. Shown to be an accident, rather than theft, purely because cameras placed in a position that allowed one to audit how the package got through the various perimeters, and the behaviour and intentions of those who happened to handle it through sections of the workspace.

Camera audits can establish both guilt and innocence. As I indicated, criminals will attempt to pierce walls or surrounds in order to move things out and both physical inspections as well as camera monitoring of behaviour in these areas can prove invaluable in maintaining infrastructure integrity. The process of moving high value items internally needs auditing, and behaviour around vulnerable locations needs to be checked and explained.

Audit of movement of high-risk product, in particular, needs to be done on a regular basis, as well as checks of goods or items around possible access areas that could be easily collected and passed through. Constant violations of procedures governing access, unusual handling of goods, empty boxes or containers of product lying around or hidden behind other goods, unauthorised use of exit areas around the site, and movement to unexpected perimeter areas can demonstrate that the organisation has a major issue with potential loss and a likely impact on bottom line profitability.

Dr Craig Donald.

Dr Craig Donald is a human factors specialist in security and CCTV. He is a director of Leaderware which provides instruments for the selection of CCTV operators, X-ray screeners and other security personnel in major operations around the world. He also runs CCTV Surveillance Skills and Body Language, and Advanced Surveillance Body Language courses for CCTV operators, supervisors and managers internationally, and consults on CCTV management. He can be contacted on +27 11 787 7811 or craig.donald@leaderware.com

New distributed acoustic sensors in EMEA

Fiber Sensys, part of the OPTEX group, has launched EchoPoint Distributed Acoustic Sensors (DAS) for advanced intrusion detection across the highest security sites.

The latest evolution in fibre optic sensing technology, the new EchoPoint series uses intelligent detection algorithms to provide point detection of +/- 6 m in a range of up to 100 km. This accurate and reliable detection make the sensors ideal for large perimeters and high security sites, such as airports, logistic centres, railways, critical infrastructure and to protect data conduits and pipelines, where being able to locate and identify the precise point of intrusion is critical.

Thanks to its advanced pattern-recognition classification algorithm, the sensors are able to distinguish between common causes of false and nuisance alarms, such as wildlife and environmental conditions, and genuine intrusion attempts. The system is also immune to electromagnetic interference (EMI), radio frequency interference (RFI) and lightning, providing a reliable and safe solution.

The flexibility and versatility of the EchoPoint series is such that they can be operated across multiple applications – installed on fences, buried or in a hybrid layout. When mounted on a fence, the sensors can identify someone cutting the fence or attempting to climb it. When buried, the system can differentiate between footsteps, manual and machine digging, and vehicle movements.

To meet the individual needs of every site, the EchoPoint series features intelligent software zoning. This means different detection zones can be configured, with the ability to independently adjust the sensitivity and output within each zone, helping to provide maximum capture rates and minimise nuisance alarms.

Masaya Kida, Managing Director of OPTEX EMEA, says that the new EchoPoint series has been developed to provide advanced intrusion detection. "By utilising the latest fibre optic sensing technology and highly intelligent classification algorithms, the new EchoPoint series is ideally suited to protect large sites where pinpoint intrusion location and detection is required to protect people, assets and infrastructure, and to maintain business operations."

When installed in a loop configuration, the sensors provide cut tolerance, so even if a sensor is cut or disconnected, the system will continue to operate. It can also feature dual redundancy, so that in the unlikely event of a processor failure, the second processor will automatically take over to ensure the wider security system is maintained and remains operational. With an average lifespan of 20 years, EchoPoint DAS provide a cost effective and futureproof sensing solution.

For more information, contact Optex, sales-sa@optex-europe.com, www.optex-europe.com

Hover Ark H3

Remote-Controlled Lifesaving Buoy

Professional Water Rescue

Toughness in Operation

Adaptability in Different Waters

Built to save more lives

- Can Work When Flipped Over
- Auto Return Upon Loss of Contact
- One Click Auto Return
- GPS Positioning
- Auto Course Correction
- Withstand Rolling Waves

HW-3

ELECTROMAGNETIC LINE THROWER

- Long distance throw
- Safe Power Source
- Wide Range of Applications

HOVERSTAR FLIGHT TECHNOLOGY CO.,LIMITED.

Contact us for more product info

+86-755-33138076 | info@hoverstar.com | www.havospark.com

Search **Hoverstar** at

Integrated and innovative smart security solutions

Olarm provides innovative integrated smart security solutions that enhance and expand existing security systems in South Africa and selected International countries. It has become a popular choice in the market owing to their comprehensive and feature-rich approach to enhancing security, providing additional digital convenience for asset protection, and improving monitoring and response capabilities.

Its flagship product, Olarm PRO 4G, is a multi-channel dual SIM 4G/2G and Wi-Fi communicator that empowers users to monitor and control a broad range of security peripherals, including individual integration with over 25 alarm panels and electric fence energisers, through the Olarm APP (for end-users) and Olarm Command Centre (for monitoring and response partners).

One of the key benefits of Olarm is its ability to integrate easily with existing security systems, making them smarter and more effective. Rather than replacing your current setup, Olarm allows users to enhance it via app-enabling and expanding it, creating a more comprehensive and advanced smart security solution you can monitor and control from your smartphone with the app.

The Olarm APP is a feature-rich solution, offering users more customisation, in-depth and on-the-go features than traditional keypads. As the Olarm PRO 4G is versatile on many peripherals, users can also monitor various devices and properties in one app, allowing for scalability in affordable smart security.

With Olarm's remote control capabilities, users have the convenience and peace of mind to access their security system using their smartphone anytime, anywhere (the Olarm PRO 4G and Olarm APP require a mobile and/or Wi-Fi connection and subscription for remote control capabilities). This real-time control and notification functionality allows users to easily arm, disarm, and bypass the system remotely, check zones and activity for added reassurance, and receive instant alerts, providing a layer of security and control for their property.

Olarm enables partnered service providers to offer beneficial upgrades and manage multiple clients' security systems from the Olarm Command Centre. This can help increase efficiency and reduce costs, as security personnel can quickly and efficiently respond to alerts and remotely configured client systems when required. Olarm's auto-configuration feature, furthermore, reduces installation times.

Overall, Olarm represents the future of integrated smart security solutions. Its advanced features, flexible integration capabilities, and scalable design make it the perfect choice for anyone looking to take their security to the next level. With the added benefits of cost-effectiveness and increased convenience, Olarm has become a top choice for those seeking peace of mind and upgraded smart protection.

8 Ways to Secure a Facility's Perimeter

Facilities managers are tasked with collaborating closely with security professionals to craft comprehensive security strategies aimed at fortifying the perimeters of their respective properties. Recognizing the individual nature of each location, it becomes imperative to tailor security plans accordingly, catering to the diverse needs of highly secure environments, such as military installations, and open-access areas, like shopping centers.

To effectively regulate vehicular access, highly secure premises should consider the installation of perimeter fences to deter unauthorized vehicle entry. The International City/County Management Association (ICMA) outlines several vehicle access control systems that can be employed, including personnel-operated gates, keypad access, license plate recognition, RFID cards, and smartphone applications.

Enhancing the security of interior spaces involves careful consideration of appropriate locking systems. These may range from traditional locks and keycard systems to advanced biometric authentication methods, providing an additional layer of security for high-risk areas.

Strategic deployment of surveillance cameras plays a crucial role in maintaining a vigilant security posture. Proper placement, camera type selection, and efficient video retention methods are essential factors to consider when implementing an effective surveillance system.

Proper lighting plays a critical role in deterring criminal activities, especially in areas that may seem unoccupied. Incorporating floodlights, spotlights, wall lights, ceiling lights, and lamp posts can effectively illuminate the surroundings, reducing the risk of security breaches.

Regular property maintenance protocols are vital to identifying potential security breaches and vulnerabilities. Prompt identification and resolution of issues such as breaches in perimeter barriers, weaknesses in access control points, and any signs of vandalism are crucial in maintaining a secure environment.

For larger properties, the integration of security canines can significantly enhance security measures. They can be employed for mobile patrols, as alarm-based deterrents, and even as sentries, providing an additional layer of security against potential threats.

Effective patrolling strategies are instrumental in maintaining a secure environment. Foot patrols, desk duties, and vehicle patrols, including the use of bicycles, golf carts, or motor vehicles, can help in effectively monitoring and safeguarding the property.

In the modern context, the incorporation of robotic and drone surveillance can further bolster security measures. Robotic systems can handle tasks that are hazardous or monotonous, while drones can be instrumental in conducting scheduled patrols and monitoring critical events, ensuring comprehensive security coverage.

Establishing comprehensive emergency response teams and protocols is imperative for ensuring the safety and security of all individuals within the facility. Collaboration with law enforcement, fire services, emergency medical services, hazardous materials experts, emergency management specialists, and public works authorities is essential in handling various emergency situations effectively.

In conclusion, by integrating these comprehensive security measures and fostering a collaborative approach among personnel, businesses and organizations can ensure maximum perimeter security, prioritizing the safety of both the property and its occupants.

Elvey Group has partnered with HALO to provide Africa's first truly cost.

Elvey Group, the exclusive HALO distributor to Africa, offers a range of body-worn cameras and DAMS software that has been designed for the needs of tomorrow. Whether you need an IP68-certified body camera or a 4G connected device HALO has the body cam solution for you.

Horizon Series Body Camera

Designed for the future of public safety, the HALO fully customisable Horizon Body Camera allows you to tailor the solution to suit your requirements. With a three-year product warranty, the Body Camera has a full-shift battery life, enabling you to capture footage back-to-back.

Key Features include:

- 16-hour continuous recording
- Super-fast charge
- Fixed cost data usage and storage
- Starlight lens technology
- Free setup & support

HALO Vault: Digital Asset Management Software (DAMS)

HALO Vault is Halo's bespoke digital asset management software for storing, viewing, and streaming multi-media types all in one secure cloud-based environment.

Build One Case in One Place

Ingest all digital media types
Reduce paperwork
Fixed data usage and storage costs

Key Features:

- Cloud or hybrid based
- One case in one place
- Redaction engine
- Tiered access
- Mark footage
- GDPR complaint
- Secure storage
- Share evidence
- No hidden charges

HALO Nanocam

The HALO NanoCam is revolutionising retail loss prevention and providing enhanced security measures for retail clients. Bodycams have become business critical for capturing first-hand evidence, recording in-store footage, and protecting customer facing staff.

Features include:

- 12 hours continuous recording.
- AES256 encryption.
- Compact and lightweight.
- 1080P full HD resolution.
- Livestream capable via Wi-Fi.
- Crystal clear evidence.

HALO Aware Geofence technology

Using a holster sensor, HALO Aware has been specifically designed to automatically switch-on any HALO Body Cameras into active recording mode within a 9.1 m radius, once a police officer draws their firearm, baton or taser. HALO's geofencing technology triggers supporting officers' Body Cameras as they arrive on the scene to capture a chained series of BodyCam footage, providing complete situational awareness.

The long-lasting battery and one-month standby time allow for back-to-back shifts as the HALO recharges in 1.5 hours via the USB Type-C fast-charge port, allowing officers to focus on what really matters, getting back to serving communities in less time.

HALO

ELVEY Group

FIXED PRICE BODY-WORN SOLUTION

CUTTING-EDGE TECH IN YOUR HANDS.

- WIDE ANGLE STARLIGHT LENS THAT RECORDS IN 1440P & 1080P
- WATERPROOF WITH IP68 CERTIFICATION THAT IS SUPER FAST CHARGING
- GPS ENABLED WITH ON-BOARD SYNC

SIGN UP TODAY!

Email:halosales@elveygroup.com

SCAN TO DOWNLOAD BROCHURE

3 MONTHS RISK-FREE

Terms & Conditions Apply

ADVERTISER'S INDEX

www.prevent-a-fire.eu

CUSTOM MADE
HEAT- AND FIRE DETECTOR UNITS
FOR INDUSTRIAL AND HAZARDOUS AREAS

We just want to warn you. In time.

ENGINE ROOMS | SAUNAS | INDUSTRIAL KITCHENS | POWER AND NUCLEAR PLANTS | MARINE OPERATIONS

Certificated, easy-to-install aluminium and stainless steel heat- and fire detector units with DAF sensor for commercial and industrial usage both for low- and high temperature operation, fit for any requirements.

EN54-5 ATEX

LICO Mechatronic Kft - LICO Electronics GmbH

certified Heat- and Fire Detector units manufactured in the European Union.

For more information: www.prevent-a-fire.eu | sales@lico.hu +36 23 520 138
sales@lico.at +43 1 706 43 000

LICO

YOU DESERVE BETTER

Altronix secures and connects critical infrastructure to make every environment safer and more efficient, providing the foundation for any physical security system. Our comprehensive range of solutions is designed and manufactured to the highest standards – backed by Altronix lifetime warranty with the best support in the industry.

Altronix

altronix.com