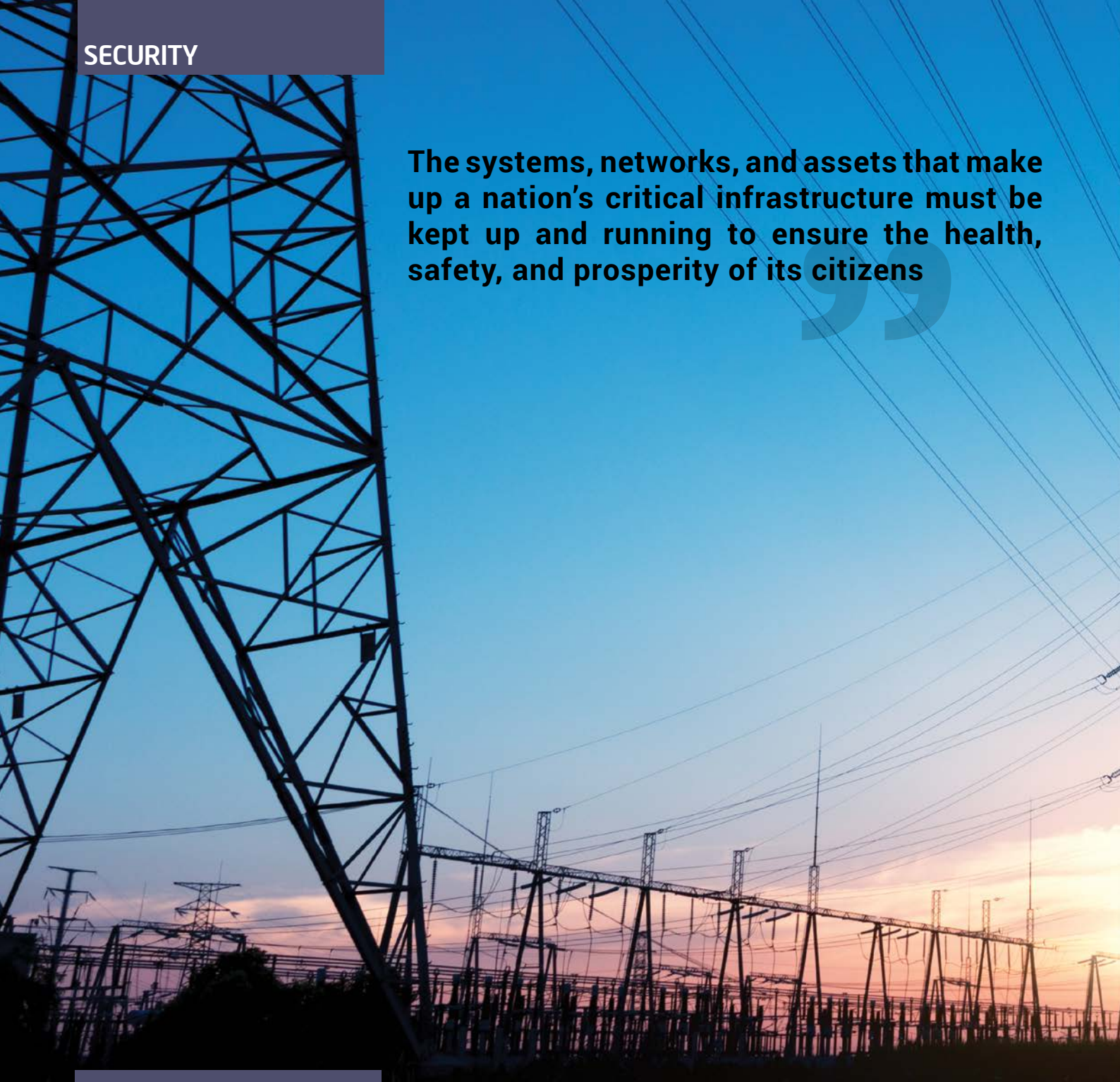


The systems, networks, and assets that make up a nation's critical infrastructure must be kept up and running to ensure the health, safety, and prosperity of its citizens

ABSTRACT

Due to its unique position within critical infrastructure, the energy sector is very vulnerable. Cyber security threats targeting critical infrastructure are a growing concern as they can even threaten national security. There is an urgent need to define unified cybersecurity solutions for the energy sector to keep it safe and reliable.

KEYWORDS:

security, cyber-security, energy sector, infrastructure

The importance of unifying physical security within the energy sector

Steve GREEN

The systems, networks, and assets that make up a nation's critical infrastructure must be kept up and running to ensure the health, safety, and prosperity of its citizens. Countries all around the world recognise the importance of protecting their critical infrastructure and invest heavily to secure its continued operation.

In the UK, the National Cyber Security Council (NCSC) identifies 13 critical national infrastructure sectors whose loss or compromise would have a debilitating effect on the country. These sectors include food, water, health, nuclear, transport, and energy [1].

The energy sector, however, is the enabling infrastructure for all the other sectors.

It supplies energy, including fuel, to the transportation industry and electricity to businesses and households. When it fails, the impact is felt across the entire economy and wider society. It has become the foundation of so many of our day-to-day activities.

As a uniquely critical sector, energy requires special consideration with regards to physical security, especially as the unique make-up of a national power distribution and transmission network throws up some unusual and challenging situations. Not only do you have to consider a mix of geographically remote and fragile locations such as pylons and towers, but also vulnerable sites like sub-stations and generation plants. The move to decarbonise the sector through the introduction of renewable technology has also added an additional layer of complexity in regard to security.

The move towards renewable energy

It is not surprising that the demand for renewable energy is having a significant impact on the energy sector. According

What energy organisations need is a unified security platform that is designed with critical infrastructure owners in mind

to an EY Report in 2019, clean energy deals made up over 60 % of overall deal value amongst mergers and acquisitions (M&A) as governments around the world continued to set clean energy targets for the future [2].

Cross-border investments in renewable energy, combined with a convergence of oil, gas, and power utilities, mean that M&A are happening on a global scale. At the same time, the sector is also moving from an analogue, scale-driven, centralised energy model to a digital and distributed model.

One of the unintended results of this transformation has been a rise in security-related challenges. Leaders in the industry have to consider how they can standardise and centralise their solutions as they inherit legacy systems that were intended to perform in isolation. They are asking themselves how they can secure a growing number of assets across a dispersed and expanding territory.

To keep pace, energy organisations must modernise their security technology. That means developing a strategy that will meet their current and future needs and also go beyond securing people and assets. Deploying a unified security system is an important step towards achieving this goal. A portfolio of unified security solutions will help address evolving security needs while also improving operations, simplifying compliance, and increasing cybersecurity.

Securing critical infrastructure and improving operations

A comprehensive physical security strategy is key to ensuring operational efficiency. Breaches in security often result in downtime that can cost organisations millions of dollars. But, more than that, when it comes to the energy sector, breaches can have a far-reaching and potentially catastrophic impact on other critical infrastructure.

What energy organisations need is a unified security platform that is designed with critical infrastructure owners in mind. By blending IP (Internet Protocol) security systems within a single platform and unifying video monitoring, access control, automatic number plate recognition (ANPR), and intrusion, a unified

solution can help organisations improve their physical security and, as a result, increase their operational efficiency.

Deploying a unified system can help organisations extend their security beyond the perimeter. It can allow them to use radar, LiDAR, fence intrusion detection, and video analytics to detect potential intruders or drones beyond the fence line and then take action to protect facilities before a breach occurs. This can be especially important for isolated facilities like transmission stations or storage depots.

Within the perimeter, ANPR can provide a real-time inventory of vehicles on-site that would allow security personnel to manage access to restricted areas based on number plates. This can also reduce downtime associated with people attempting to access restricted areas without authorisation.

An IP video management system (VMS) can give security personnel a clear picture of events and enable them to quickly respond to threats and incidents. Organisations can further improve security with an IP access control system (ACS). For example, by using built-in people counting together with access control events, security personnel can monitor where employees, contractors, and visitors are at all times. This includes routine operations as well as incidents and evacuations. In addition to tracking movements over a geographical map or through visual reports and dashboards, the system can also be set up to automatically send reports to key personnel within the organisation as well as to first responders.

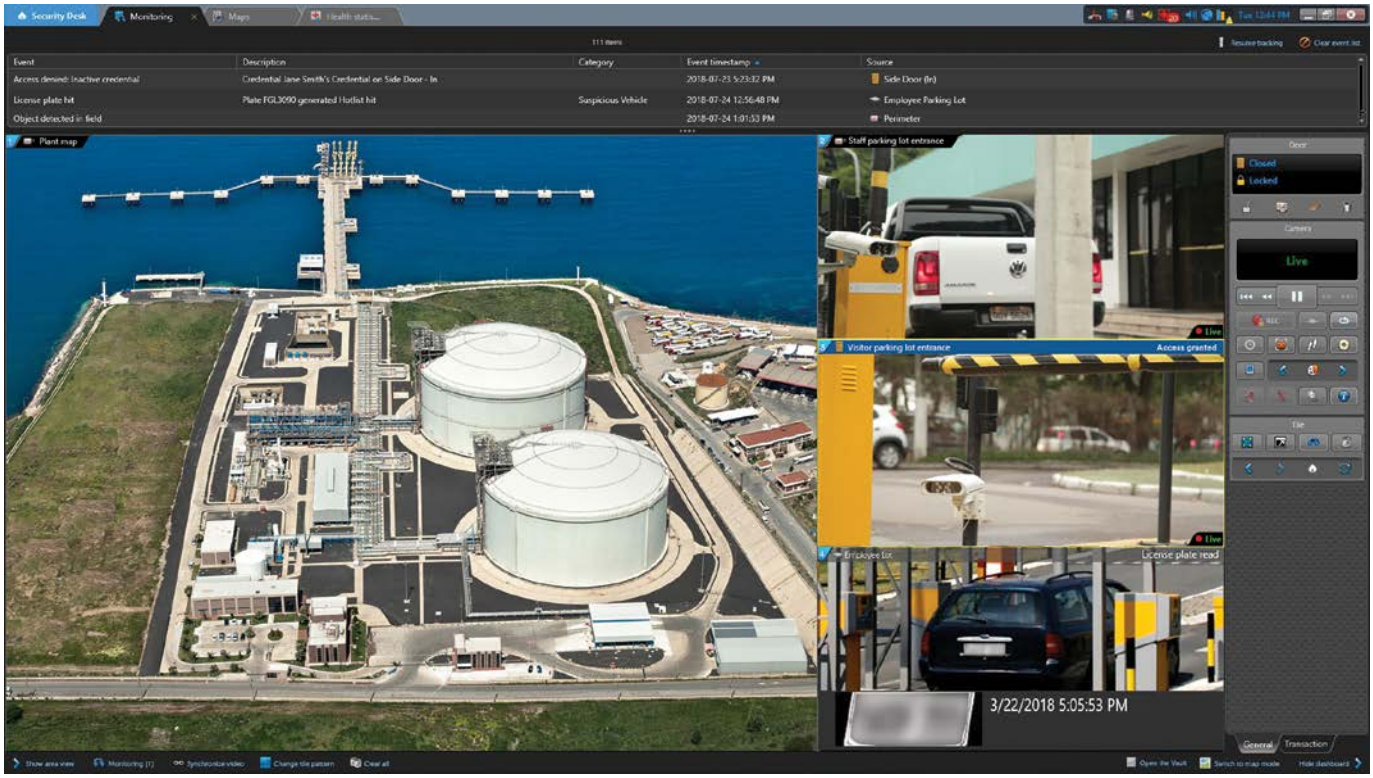
A unified security system that optimises evidence reporting and the digitisation of standard operating procedures can help energy organisations comply with these regulations

Simplifying the compliance process

Regulatory agencies around the world are tasked with ensuring the security and reliability of bulk power systems in different countries. Whether it be water, communications, energy or oil and gas, industry players are responsible for demonstrating compliance with a wide range of industry-specific standards, including those for physical security, for protecting the integrity of supply.

The most common physical security requirements are to record all access control activities, maintain logs for authorised access, and monitor critical facilities for unauthorised access 24/7. In the event of an access breach, organisations must investigate and categorise the alarm incident and implement the appropriate response plan within strict timeframes. Verification of the alarm details as well as the response must be doc-

For governments around the world, cyber security threats targeting critical infrastructure are a growing concern as they can threaten national security



A poorly protected camera, unencrypted communication between a server and client application, or out-of-date firmware all have the potential to be exploited by cybercriminals

umented and are subject to an audit and review with severe penalties enforced for violations.

A unified security system that optimises evidence reporting and the digitisation of standard operating procedures (SOPs) can help energy organisations comply with these regulations. Being able to securely collect, manage, and share digital evidence from multiple sites makes it easy to meet different audit requirements.

Organisations can also use a unified security system to predefine a wide variety of criteria and create digitised SOPs to guide personnel in their responses to events. This ensures compliance across a distributed organisation since all security teams, regardless of shift or location, are always operating according to the same SOPs. This is especially important when exporting and sharing workflow diagrams and incident reports with auditors.

Cybersecurity risks and new regulations

In recent years we have seen a rise in cyberattacks from sophisticated hacker attacks. For governments around the world, cyber security threats targeting critical infrastructure are a growing concern as they can threaten national security. As the UK Minister for the Cabinet Office makes clear in his foreword to the National Cyber Strategy 2022; "we should strengthen our hands in technologies that are critical to cyber [and] we should limit our reliance on individual suppliers or technologies which are developed under regimes that do not share our values" [4].

Because of its unique position within critical infrastructure, the energy sector is especially vulnerable. In fact, according to the insurance company Hiscox's Cyber Readiness Report 2021, the UK's energy sector is at the greatest threat, despite a higher percentage of firms than in other sectors having upped their cyber security budgets. This higher risk level is attributed to a lack of adequate preparation [4].

Organisations must now contend with managing and mitigating the impact of these attacks. In particular, they have to align their physical and cybersecurity networks to protect their businesses from current and future threats.

Strong cybersecurity is key

Modern physical security devices and systems are increasingly interconnected, which is helping security personnel keep people and organisations secure. At the same time, this growing connectivity is increasing the risks associated with the criminal cyber activity.

Greater connectivity of systems over the internet means that a vulnerable device can become a gateway to an organisation's data and sensitive information. For example, a poorly protected camera, unencrypted communication between a server and client application, or out-of-date firmware all have the potential to be exploited by cybercriminals.

This means that security systems can no longer focus solely on physical threats. Organisations must choose hardened solutions that also work to protect all other systems and information connected to the network against the criminal cyber activity. Companies like Genetec can provide solutions that help organisations protect their data and operations, help them comply with regulations and meet audit requirements without compromising physical security functions.

Conclusion

The energy sector is changing and facing new and evolving challenges in regard to the security of the physical assets of the network. Building stronger, more unified solutions and working with partners with a proven track record and expertise in the area will help to protect what is one of the most important parts of every nation's critical infrastructure.

Bibliography

[1] National Cyber Security Centre UK, CNI Hub; Access: https://www.ncsc.gov.uk/section/private-sector-cni/cni

[2] *National Cyber Security Strategy 2022*

[3] *Clean energy drives power and utility M&A activity amid overall decline in deal value,* EY, Press Release, 9 May 2019; Access: https://www.ey.com/en_ro/news/2019/05/clean-energy-drives-power-and-utility-m-a-activity-amid-overall-decline-in-deal-value

[4] UK Government, 7 February 2022; Access: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[5] *Hiscox Cyber Readiness Report 2021,* Hiscox; Access: https://www.hiscox.co.uk/cyberreadiness

Author

Steve Green is a Business Development Manager at Genetec. Mr. Green brings over 20 years of experience in the IT and Physical Security sectors and, in that time, has worked for some of the industry-leading software manufacturers and solutions providers. Since joining the company in 2015, his focus has been on working closely with customers in the oil, gas, energy and transports industries to develop their use of Genetec solutions.