A Synectics Guide To

Surveillance Upgrades for Oil & Gas Operators

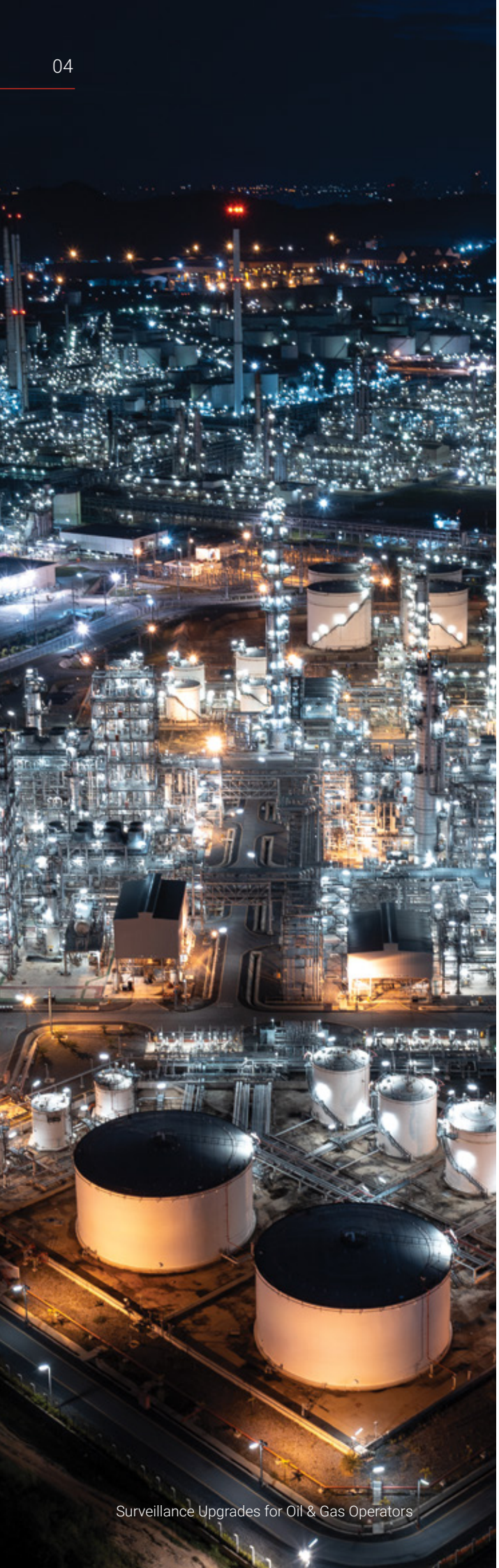
Enhancing Security, Reducing Costs, and Maximising Efficiency

SYNECTICS

Contents

This guide looks at why upgrading security and surveillance has become a critical issue for many oil and gas operators. In it, we examine common concerns and outline practical, cost-effective solutions and approaches that minimise disruption while modernising legacy infrastructure – improving security and safety for operators and assets alike.


9.3t
22
22
22



Factors Influencing Upgrade Decisions

Before looking more closely at specific upgrades and approaches, it's important to understand why these might be needed. To do that, let's first examine what's impacting the oil and gas, marine and other related industries such as petrochemicals.

Brownfield asset life extension

Investment in greenfield oil and gas facilities to meet the rebound in global demand is significant, especially in offshore, where over $200 billion[1] is estimated to have been spent on new projects in the last two years alone. What's interesting is the impact this is having on brownfield developments. More than ever, operators of midlife and maturing sites are under pressure to extend the economic life of facilities and vessels, and enhance process efficiencies to stay competitive.

Safety remains a key issue

Enhanced regulations and stricter compliance measures have played a critical role in improving safety standards in oil and gas, but further improvement is necessary. And not simply to protect and attract workers. A strong safety record is also critical for cost control, especially with the sector seeing some of the highest insurance premiums to date. Technologies that support automation in hazardous areas and help enforce protocols are becoming operationally critical.

Fewer workers are the new norm

While protecting workers on site is essential, many facilities now have fewer or are unmanned. Factors such as automation, technological advancements, and industry consolidation mean employment in the sector is down, while production is up. It's also increasingly common for sites, especially in remote locations, to operate skeleton teams where possible as part of energy and resource-saving initiatives.

Cyber is a key part of the 'security risk' mix

Protecting oil and gas plants, platforms and vessels from theft, vandalism, unauthorised breaches, production disruption, and safety risks has always been essential. Equally essential today is protecting data. 94% of the world's top 400 oil and gas companies have suffered at least one data breach to date[2] making cyber protections a crucial component of security.

Minimising environmental impact matters

From reducing energy consumption to identifying and tracking leaks of various pollutants like methane, volatile organic compounds (VOCs), and other greenhouse gases, oil and gas operators are under increased regulatory and ethical pressure to demonstrate more sustainable operations.

All of these factors impact surveillance requirements for oil, gas and fleet operators, but the implications are twofold for brownfield operators.

1. Extending life – addressing the basics

Ageing assets have ageing CCTV systems. This threatens long-term operations from a basic functionality perspective. Hardware becomes more challenging to maintain and replace, and outdated software becomes more vulnerable to faults and cyber risk.

2. Boosting performance – achieve more with less

To address many of these challenges, a security and surveillance solution that supports integration and unified systems monitoring is crucial. It should also be able to incorporate the adoption of newer digital technologies, from more powerful cameras to AI.

This guide explores how these can be achieved with minimal disruption while controlling costs.

1 https://www.rystadenergy.com/news/offshore-is-back-more-than-200-billion-of-greenfield-investments-expected-by-2025

2 https://www.worldpipelines.com/equipment-and-safety/20052025/report-over-50-of-top-oil-and-gas-firms-hit-by-data-breaches-in-last-30-days/#:~:text=94%25%20of%20the%20largest%20oil,lowest%20average%20score%20at%2065.

Transitioning to IP-Based Cameras

Transitioning to IP-based cameras isn't just about avoiding the maintenance and security risks of older, analogue-based equipment. It's also a crucial step towards improving performance in line with evolving threats and sector challenges.

Top Tip: Consider ONVIF

Check for ONVIF compliance. ONVIF is a global and open industry forum focused on standardising communication between IP-based physical security products to achieve interoperability between equipment. This will be important for future-proofing your system and ensuring compatibility with new systems you may introduce.

Analogue vs IP Cameras

IP cameras, especially those with 4K resolutions, provide clearer and more detailed images than their analogue counterparts.

Achieving this clarity is essential for effective security, safety, process monitoring, and leveraging video analytics.

Other advantages include:

- **Install and access flexibility**
  IP cameras can be easily connected to a network and accessed remotely, offering more flexibility in camera placement, monitoring and remote maintenance and configuration.

- **Advanced features**
  IP cameras increasingly feature built-in or 'edge-based' recording and video analytics, such as the ability to detect and classify objects and movements for improved risk detection.

- **Minimise environmental risk**
  Thermal cameras with advanced radiometric capabilities are becoming essential for operators aiming to ensure flare compliance. By providing accurate, real-time monitoring, they help reduce environmental risk and demonstrate regulatory adherence.[3]

	Analogue	IP
Image quality	Analogue cameras only offer standard definition, typically up to 960H or 1080p with HD analogue.	HD and megapixel IP cameras, including 4K models, offer far superior resolution levels for detailed image capture.
Scalability	Video is transmitted to a DVR using a coax cable, where data is converted into a format that can be stored and reviewed. Each DVR has a finite capacity regarding the number of cameras it can accommodate.	Any number of cameras can be added to the network, in line with asset requirements, without requiring cameras to be physically cabled.
Accessibility	Analogue systems require additional physical infrastructure to enable remote viewing.	IP-based solutions offer flexibility in where footage is viewed, because information can be transmitted over a WAN or a secure VPN.
Adaptability	Data is often siloed and difficult to standardise and interrogate.	IP-based solutions enable sophisticated data integrations and analytics at the edge (IP cameras) or via centralised software.
Maintenance	Maintenance requires on-site access, a significant time and trained resource.	Centralised monitoring and management make troubleshooting easier. Firmware upgrades can also be carried out remotely.

3 From January 2025, Minimum fines for flaring and venting breaches increased to £500,000 in he UK.

Upgrading Hardware and Software

Legacy CCTV systems – especially those reliant on analogue technology and in situ for over eight years with minimal upgrades – present distinct risks for operators and fleet companies.

Upgrading your hardware

Hardware issues with legacy tech can lead to downtime. The industry's shift towards digital IP-based solutions makes it difficult to source spare parts, obtain technical support, and guarantee ongoing maintenance for ageing analogue cameras, servers, and other critical hardware assets. Ageing tech also requires more frequent repairs and troubleshooting, which can be a significant problem, especially for offshore sites, vessels and projects located in remote locations.

Servers, storage, and control devices should run the latest operating systems, optimised for 4K video, analytics, and AI. Modern hardware also includes built-in cybersecurity, long-term OS support, and health alerts to help ensure uptime.

To prevent hardware obsolescence and cybersecurity risks always:

- Replace at-risk hardware and cameras with the latest models
- Consider critical assets first, ensuring they're equipped with modern cyber security and encryption standards
- Schedule regular firmware upgrades to maintain security, consistently enhance performance and ensure ongoing compatibility

Choosing software

Upgrade to an open-architecture security and surveillance platform to future-proof your operations and enhance flexibility. When selecting the right software, consider a solution that offers:

Third-party integration – for seamless connection with other systems and devices for unified monitoring and control.

Feature-rich tools – such as dynamic mapping with CAD support and advanced alarm management for better situational awareness.

Automation – look for solutions that support automation and allow you to tailor the interface, reports, workflows and accessibility to the requirements of your assets, protocols and data sources.

Built-in cyber security – to protect against evolving threats with robust security measures at the core of the system.

Remote and centralised multi-site management – to allow users to monitor and control systems from anywhere, improving responsiveness and efficiency.

System health dashboards – for real-time insights into performance and alerts to support planned maintenance and avoid potential issues.

Bulk camera configuration – essential for efficiently managing large estates with high camera counts.

Choosing a platform with these capabilities ensures greater scalability, resilience, and ease of use across your operations.

Top Tips: Making sure your software is cyber-secure

- ☑ **Safeguard Your Network Perimeter**
  Implement multi-layered protection by deploying firewalls, intrusion detection systems (IDS), and up-to-date virus scanners.

- ☑ **Ensure Compliance with Standards**
  Ensure full compliance with modern cyber security protocols and data privacy regulations. These may include IEC 62443, ISO/IEC 27001, NIS2 (EU), NERC CIP (US), UK NIS Regulations, GDPR/UK GDPR, and relevant national or sector-specific frameworks that govern the protection of surveillance data and network-connected systems.

- ☑ **Run Automated Configuration Audits**
  Use built-in tools to flag risks like default passwords, missing updates, or inactive workstation lockdowns.

- ☑ **Encrypt Data End-to-End**
  All data, whether at rest or in transit, should be encrypted. For evidence transfer, include hashing to verify data integrity.

- ☑ **Enforce Multi-Factor Authentication**
  This will validate all users and connected devices using robust MFA protocols.

Using Existing Cabling Cost Effectively

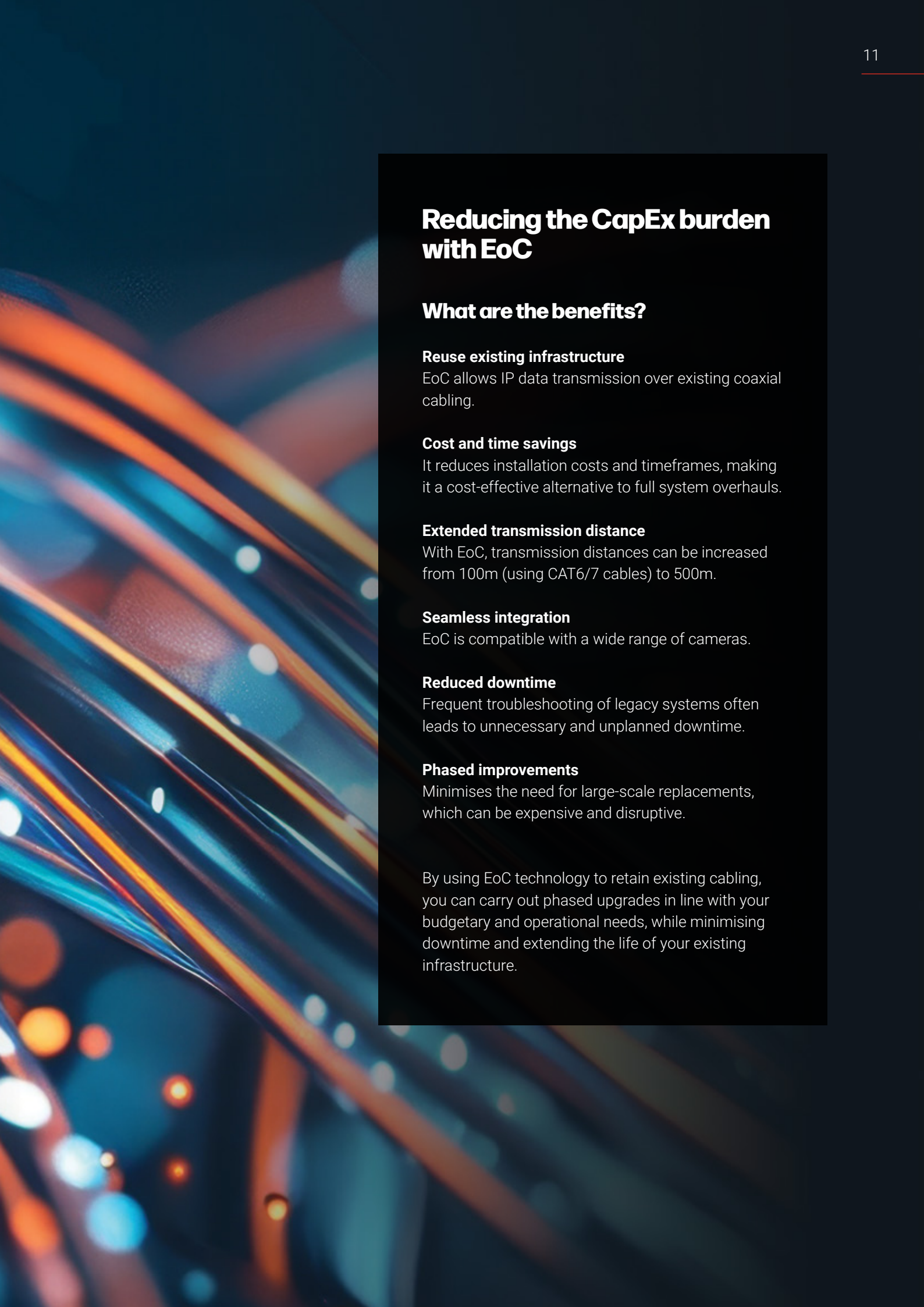
With modernisation that maximises cost efficiency

If the benefits of modernisation and migrating to IP appeal, but there isn't an existing cabling infrastructure to make it a reality, there is a cost-effective solution.

Make more of what you have

Ethernet over Coaxial (EoC) provides an alternative upgrade path by allowing IP data transmission over existing coaxial cables. This method minimises cost and mitigates the risk of installation disruption and associated system downtime.

Offering the benefits of IP, without the need for extensive cabling replacements, EoC future-proofs installations for the asset lifespan and delivers flexibility according to your specific upgrade strategy.



Reducing the CapEx burden with EoC

What are the benefits?

Reuse existing infrastructure
EoC allows IP data transmission over existing coaxial cabling.

Cost and time savings
It reduces installation costs and timeframes, making it a cost-effective alternative to full system overhauls.

Extended transmission distance
With EoC, transmission distances can be increased from 100m (using CAT6/7 cables) to 500m.

Seamless integration
EoC is compatible with a wide range of cameras.

Reduced downtime
Frequent troubleshooting of legacy systems often leads to unnecessary and unplanned downtime.

Phased improvements
Minimises the need for large-scale replacements, which can be expensive and disruptive.

By using EoC technology to retain existing cabling, you can carry out phased upgrades in line with your budgetary and operational needs, while minimising downtime and extending the life of your existing infrastructure.

The Benefits of a Unified Solution

Here's some of the performance-enhancing benefits available with a unified security and surveillance solution.

1. Complete situational awareness

A unified security and surveillance solution provides centralised oversight and control of multiple site systems – including surveillance, process, emergency, and safety. It also delivers a 360° view of incidents that is not be possible when monitoring systems separately. This saves busy, resource-tight teams considerable time, improving efficiency and productivity.

Unmanned or low-manned locations, such as platforms and rigs, can be monitored and managed remotely, where it's not always efficient, economical, or safe for staff to be deployed on site.

2. Proactive asset protection

Advanced features are common with unified security and surveillance solutions to ensure efficient asset protection. These include capabilities such as:

- Advanced alarm management
- Flare monitoring
- Radiometric analysis to monitor heat variations in critical processes and storage facilities
- AI-powered risk detection
- Facial recognition
- Radar integration
- Mobile app task management and surveillance

3. Cost-effective scalability

Upgrading to a latest solution makes it easier to add or change cameras, integrate new technologies, and to encompass monitoring of new zones or additional sites, all with minimal disruption or additional infrastructure cost.

Multi-site management provides complete control and enables you to:

- Centralise process, security, and safety monitoring from a corporate HQ.
- Remote monitoring and troubleshooting. This removes the need to have personnel permanently located on site and ensures uncrewed facilities are effectively monitored 24/7.

4. Meet compliance standards

It can help meet compliance standards by using AI to help identify hazards. Proximity to dangerous equipment, correct use of PPE for specific zones, appropriate team protocols (where specific tasks require a particular number of people for safety), and slips, trips, and falls (onboard and overboard) can all be automatically detected.

Future-Proofing Your Investment

With over 40 years' experience in safeguarding assets, from onshore refineries, plants, and pipelines to offshore rigs, platforms and vessels, Synectics can help you make the changes you need, in a way that ensures cost savings, minimal downtime, and long-term system performance.

Our COEX™ cameras and Synergy software are used globally to detect threats, ensure uninterrupted operations and comply with strict regulations.

Why Choose Synectics

1. Reliable cameras designed for longevity

Compatible with any control software to give you maximum flexibility, our COEX IP safe-area, hazardous-area and thermal cameras are built to last and perform even in the most extreme weather, temperature and lighting conditions.

2. Smart, scalable software

Synergy software seamlessly integrates with legacy infrastructure while giving you access to advanced capabilities such as alarm management, AI-powered risk detection, flare and radiometric monitoring, remote access and integration with radar and other specialist systems.

3. Future tech ready

As new technologies emerge or operational needs evolve, additional tools and integrations can be easily layered on, without overhauling your core investment. In other words, your platform grows with you, enabling future-ready transformation without disruption.

We can help you:

- **Transition to IP-based CCTV systems, ensuring future readiness.**
- **Leverage EoC technology to cut upgrade costs and simplify the process.**
- **Extend the life of critical assets and reduce system downtime.**
- **Boost the efficiency and effectiveness of your security and surveillance capabilities**.

Protecting what matters, where it matters most

Synectics is a leader in advanced security and surveillance solutions that help protect people, property and assets around the world.

We transform customer operations by seamlessly integrating systems, technologies, and data into a unified solution-enhancing safety, improving efficiency, and enabling smarter, faster decision-making and response capabilities.

With our technical expertise, decades of experience, and strong partnerships, we set ourselves apart by delivering innovation and service that drive real value and long-term success.

To learn more about how we can help keep your people and assets safe, visit **synecticsglobal.com**

Specifications subject to change. E & OE.

Literature Reference: EUOG/EB Iss 1

SYNECTICS

synecticsglobal.com