A Synectics Guide To

Effective Security and Operations for Utilities

Best Practices That Keep Assets, Networks and People Safe

SYNECTICS

Contents

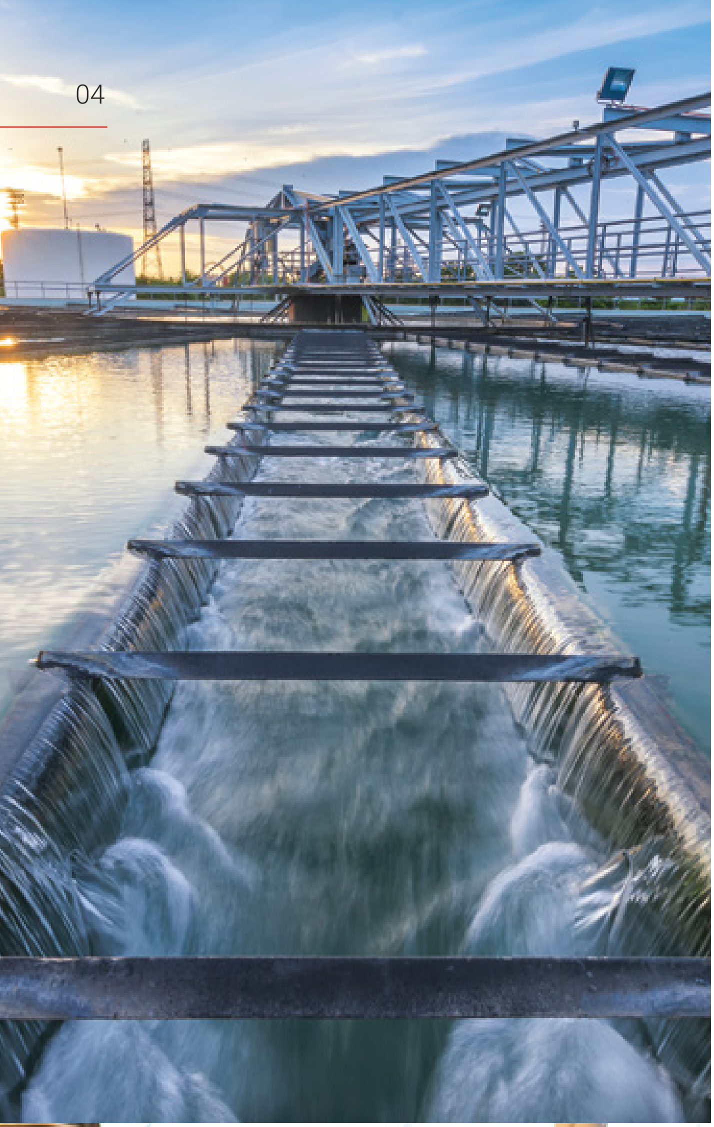
About This Guide

How can utility providers keep their infrastructure, personnel, and operations secure, while maintaining efficiency and regulatory compliance?

This guide explores how a modern security and surveillance solution can be deployed across power generation facilities, electrical substations, water treatment plants, and renewable energy sites to achieve exactly that.

It focuses on the real-world challenges operators face, such as distributed sites, hazardous environments, and critical service continuity, and how unified security and surveillance platforms can help mitigate them.

Whether you're managing a single facility or an entire network, this guide will give you practical guidance on selecting and deploying surveillance solutions that meet operational needs, environmental conditions, and evolving threat landscapes.



Current Trends and Challenges

Before diving into how integrated security and surveillance solutions can support the sector, it's useful to understand the landscape of risk and operational pressure that utilities face today.

1 Rise in theft, sabotage and intrusion

Utility providers face growing physical threats, from organised copper theft to direct attacks on operational sites. In the UK, at least 12 large windfarm sites were stripped of copper cabling in just three months in early 2025[1]. This is just a recent example of what has become a major issue for the UK utilities sector[2]. In the US, the Department of Energy logged 95 human-caused incidents targeting the electricity sector in the first half of 2023, the highest on record[3].

2 Distributed sites, limited resources

Power networks and water systems span large geographic areas, with many critical assets, like uncrewed substations, solar farms, or booster stations, located in isolated or rural areas. Maintaining security coverage across all these points while keeping costs and headcount manageable is a growing concern.

Mobile patrols are resource-intensive and often delayed, meaning threats like intruders, leaks, or fires can go undetected without a responsive surveillance infrastructure in place.

3 Compliance and regulatory burden

From the US NERC CIP standards to the UK's CAPSS guidance and the EU's NIS2 Directive, utilities face stringent physical and cyber security obligations. Security and surveillance platforms must not only protect operations but also withstand formal assessment against these national and regional frameworks.

4 Pressure to modernise

In an age of digital transformation, integrating video surveillance into broader operational systems, like SCADA, BMS, access control, and analytics, is crucial. Operators want actionable insights, not just video footage.

The shift toward AI-enabled monitoring, remote access for distributed teams, and cloud-based incident response tools reflects the need to do more with less, while still upholding safety, security, and resilience standards.

5 Insider and contractor risk

Many breaches originate from authorised personnel misusing access, whether unintentionally or maliciously. With large numbers of third-party contractors and rotating field teams, verifying identities, logging activity, and responding to unauthorised behaviour is a security challenge. Integrated security and surveillance platforms with access control, credential validation, and location tracking ensure greater accountability and visibility into who is where, and when.

It's clear that keeping utility infrastructure secure and operational is an increasingly critical task.

[1] https://www.theguardian.com/business/2025/jun/23/windfarms-in-england-hit-by-wave-of-copper-cabling-thefts

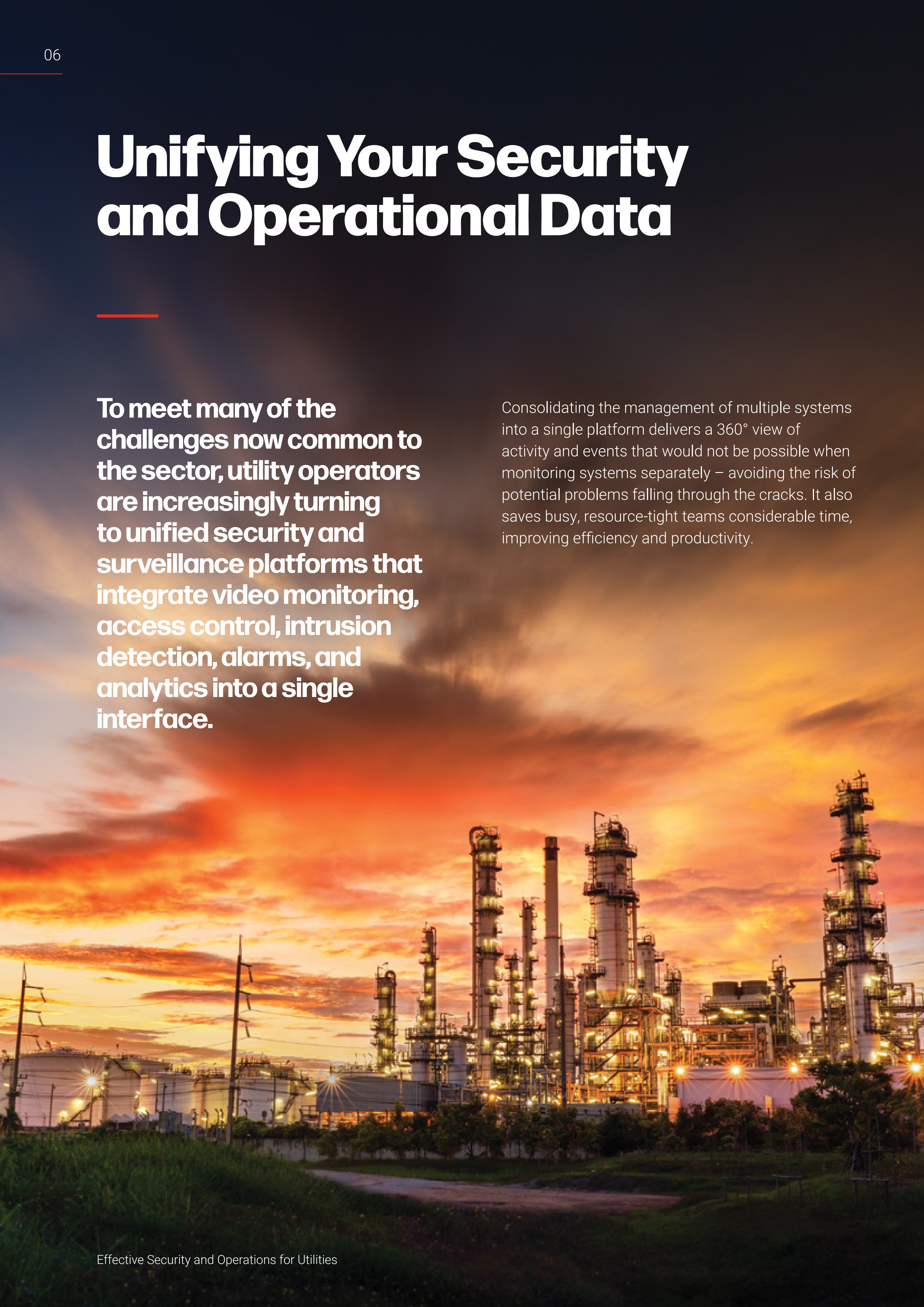
[2] https://www.energynetworks.org/work/metal-theft

[3] https://www.reuters.com/business/energy/north-american-grid-regulator-tests-physical-cyber-security-preparedness-2023-11-16/#:~:text=Data%20on%20electric%20disturbances%20reported,records%20dating%20back%20to%202000

Unifying Your Security and Operational Data

To meet many of the challenges now common to the sector, utility operators are increasingly turning to unified security and surveillance platforms that integrate video monitoring, access control, intrusion detection, alarms, and analytics into a single interface.

Consolidating the management of multiple systems into a single platform delivers a 360° view of activity and events that would not be possible when monitoring systems separately – avoiding the risk of potential problems falling through the cracks. It also saves busy, resource-tight teams considerable time, improving efficiency and productivity.

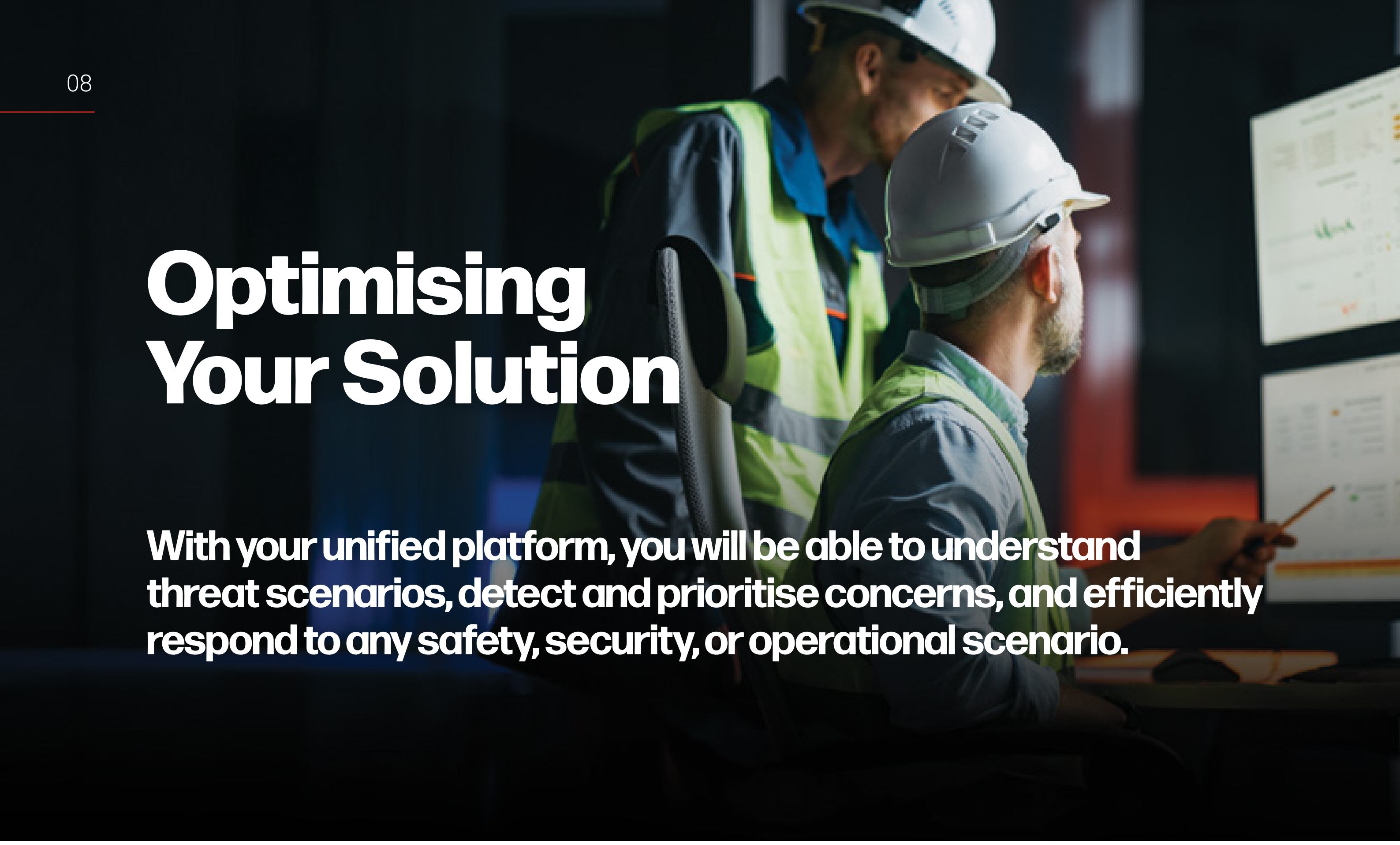


Here are some examples of third-party data sources that can be integrated:

Security	Operational	Safety	Environmental
CCTV cameras (fixed/ PTZ, thermal)	SCADA data feeds	Lone worker alarms	Weather and flood alerts
License plate recognition (ANPR)	Asset tracking (e.g. substation tools)	Panic and emergency buttons	Air quality monitors
Facial recognition	Contractor check-in/out logs	Fire and smoke detection systems	Water quality sensors
AI and video analytics (e.g. loitering, breach)	Drones (e.g. monitoring and maintenance checks)	Public Address systems	Gas and leak detection sensors
Access control and badge readers	Inspection and maintenance schedules	Communication and Dispatch	Temperature and humidity sensors
Perimeter intrusion detection (fence, radar)	Power flow or outage data	Safety compliance monitoring	Reservoir and tank level sensors

Spotlight On: Integrating process monitoring

Real-time process data, such as pressure levels, chemical dosing rates, and flow measurements, can be visualised within the security and surveillance platform. By integrating with SCADA, PLCs, or industrial IoT sensors, control room teams can be alerted and correlate physical events (e.g. a door opened) with process anomalies, helping detect tampering, failure, or unsafe conditions faster.



Optimising Your Solution

With your unified platform, you will be able to understand threat scenarios, detect and prioritise concerns, and efficiently respond to any safety, security, or operational scenario.

For this to be as effective as possible, four specific technology features are recommended. Ask your provider about:

1. Mapping made for complex layouts

Power stations, substations, water treatment plants, and renewable energy sites are often spread across large areas and connected to vital public infrastructure. To detect and coordinate responses effectively, advanced mapping capabilities are essential.

Choose a solution that supports the integration of geo-spatial mapping such as OpenStreetMap, as well as locally hosted maps like CAD renderings of site and facility schematics. Your platform should display camera locations and integrated device data as glanceable, interactive icons or clusters. This enables your teams to zoom out for a network-wide view or drill down to monitor and coordinate incidents at specific assets, with location data adding crucial context.

2. Analytics-driven intelligence

By integrating AI-based video analytics tools into your platform, you will be able to create customised rules and thresholds which can then be applied to all data captured to raise real-time alerts whenever specific criteria are met. This supports proactive risk detection (risks that operators might otherwise miss) and enables much faster footage review for real time and post-event investigation.

3. Workflows and automation

When risks are identified (including those from analytics), workflows are triggered to ensure the correct response steps, delivering on-screen instructions to guide operators through standard operating procedures (SOPs). For example, this could include automatically locking down access gates or notifying field teams of equipment tampering. Workflows can also automate day-to-day processes for greater speed, consistency, and reduced operator workload.

4. Remote access to information

Utility networks often require multiple teams – control room staff, maintenance engineers, contractors, and emergency responders – to share time-sensitive information. Remote access allows authorised personnel outside the control room to securely view live footage, alarms, and reports relevant to their duties, helping them make informed decisions in real time.

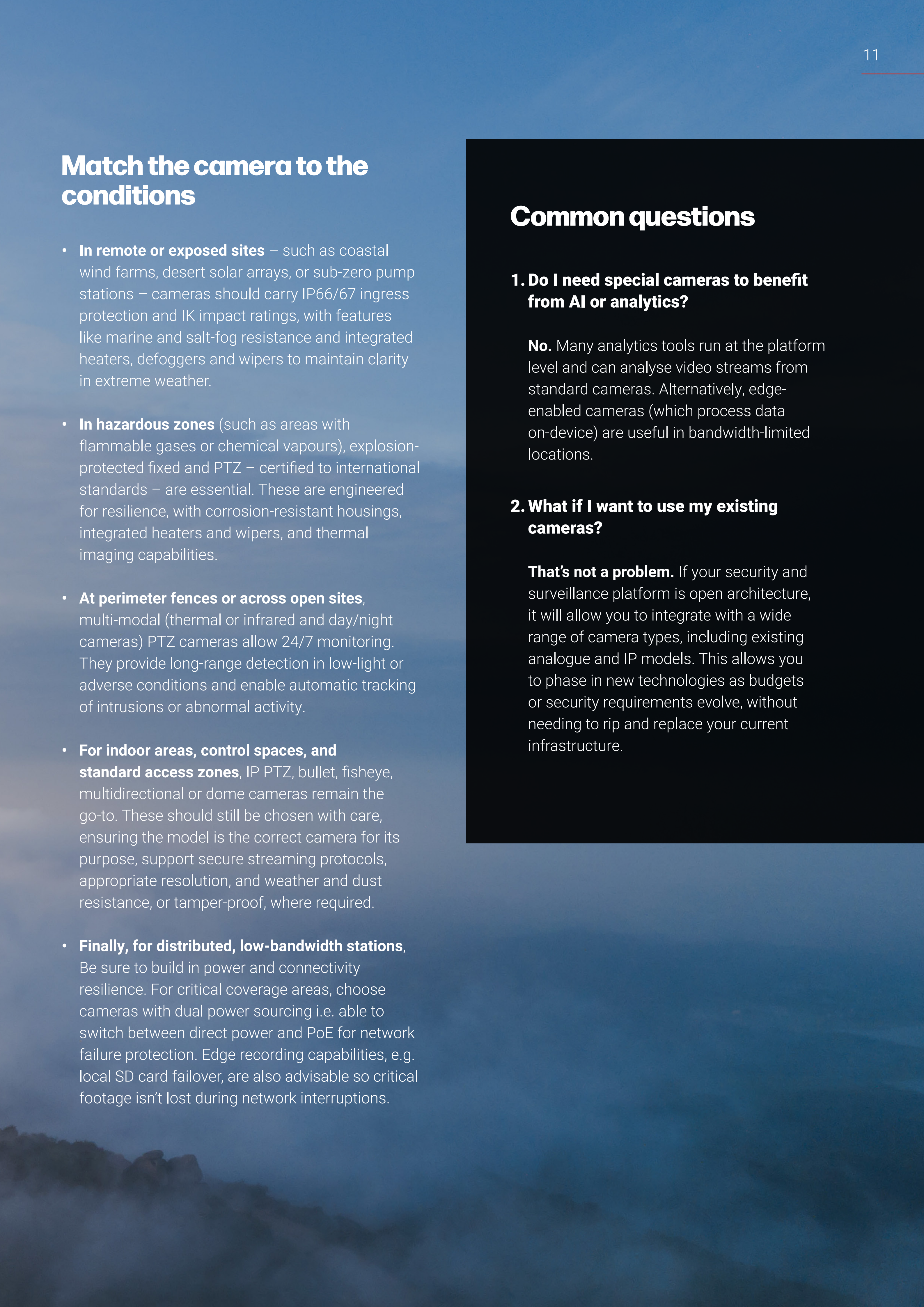
There are two main types of remote access to be aware of:

What	How it Works	Perfect For:
Secure web access	Uses WebRTC (Web Real-Time Communications) to enable authorised users to securely access live video streams, playback, alarms, and reports from authenticated mobile devices connected to the web.	Internal information sharing between distributed teams, maintenance staff, or on-call security managers.
	ASK: your provider if a dedicated mobile app is available to support task assignment and reporting	
Cloud-based sharing	Digital evidence lockers and incident-sharing tools in the cloud allow critical video or operational data to be sent to authorised parties quickly and securely.	External collaboration, such as sharing incident footage with law enforcement, regulators, or emergency services.

Because utility networks face dispersed sites, strict regulations, and time-critical threats, optimising your security and surveillance platform with mapping, analytics, workflows, and remote access ensures both stronger protection and faster incident resolution.

Selecting the Right Cameras

Choosing the right camera for each location is critical to long-term reliability and evidential quality. For utility environments, this often means balancing image performance with resilience against harsh conditions.



Match the camera to the conditions

- **In remote or exposed sites** – such as coastal wind farms, desert solar arrays, or sub-zero pump stations – cameras should carry IP66/67 ingress protection and IK impact ratings, with features like marine and salt-fog resistance and integrated heaters, defoggers and wipers to maintain clarity in extreme weather.

- **In hazardous zones** (such as areas with flammable gases or chemical vapours), explosion-protected fixed and PTZ – certified to international standards – are essential. These are engineered for resilience, with corrosion-resistant housings, integrated heaters and wipers, and thermal imaging capabilities.

- **At perimeter fences or across open sites**, multi-modal (thermal or infrared and day/night cameras) PTZ cameras allow 24/7 monitoring. They provide long-range detection in low-light or adverse conditions and enable automatic tracking of intrusions or abnormal activity.

- **For indoor areas, control spaces, and standard access zones**, IP PTZ, bullet, fisheye, multidirectional or dome cameras remain the go-to. These should still be chosen with care, ensuring the model is the correct camera for its purpose, support secure streaming protocols, appropriate resolution, and weather and dust resistance, or tamper-proof, where required.

- **Finally, for distributed, low-bandwidth stations**, Be sure to build in power and connectivity resilience. For critical coverage areas, choose cameras with dual power sourcing i.e. able to switch between direct power and PoE for network failure protection. Edge recording capabilities, e.g. local SD card failover, are also advisable so critical footage isn't lost during network interruptions.

Common questions

1. **Do I need special cameras to benefit from AI or analytics?**

   No. Many analytics tools run at the platform level and can analyse video streams from standard cameras. Alternatively, edge-enabled cameras (which process data on-device) are useful in bandwidth-limited locations.

2. **What if I want to use my existing cameras?**

   That's not a problem. If your security and surveillance platform is open architecture, it will allow you to integrate with a wide range of camera types, including existing analogue and IP models. This allows you to phase in new technologies as budgets or security requirements evolve, without needing to rip and replace your current infrastructure.

Securing Perimeters, Sites, and Substations

Security starts at the boundary. For utility providers, particularly those responsible for high-voltage substations, remote energy assets, and water treatment facilities, perimeter protection is a critical line of defence against threats ranging from trespass and theft to sabotage, terrorism, and environmental hazard.

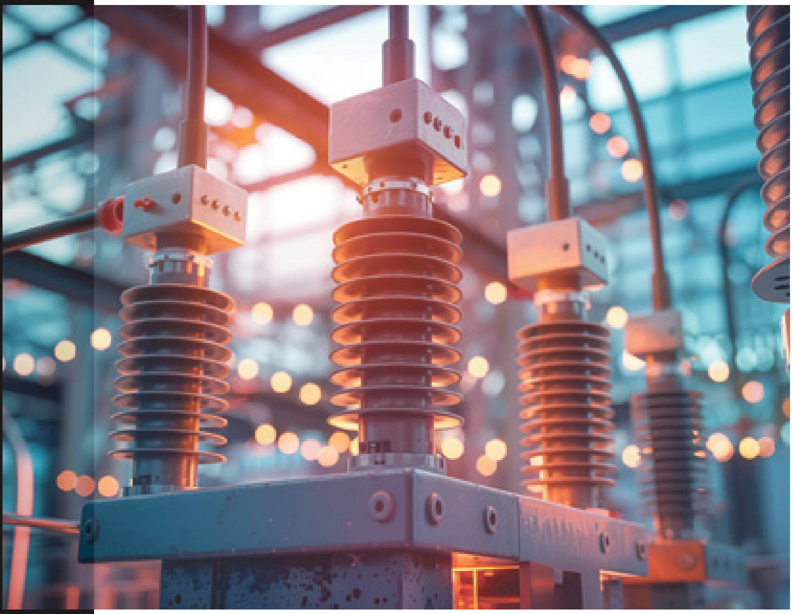
Many utility sites are large, exposed, and often uncrewed. Effective surveillance in these areas requires a combination of area-suited cameras, intelligent video analytics, and integration with systems that support rapid, coordinated incident response.

Copper theft alone causes over $1 billion in damages annually in the US[4], with tens of thousands of incidents also reported across UK and EU energy networks. Coordinated attacks, such as those on US substations in 2022, have left tens of thousands without power, reinforcing utilities' vulnerability to both opportunistic and targeted threats[5].

Detect, respond, resolve

Strategically placed thermal or infrared PTZ and fixed cameras allow 24/7 monitoring of perimeter fences, gates, service yards, and vulnerable outdoor infrastructure. When paired with AI-driven analytics, they detect:

- **Loitering or suspicious behaviour near critical assets**
  Triggering an alert with live camera feed sent to control room and patrol units or security teams.
- **Tailgating or forced entry at vehicle and pedestrian gates**
  Activating an automated workflow: visual verification prompt, access denial, and emergency escalation if needed.
- **Movement in restricted/no-access zones**
  Launching auto-tracking with PTZ and issuing mobile notification to designated responders.
- **Environmental indicators (e.g. smoke, flooding, debris)**
  Triggering incident reporting tools and alerting maintenance teams for rapid intervention.



Scenario: Coordinated copper theft

After-hours motion is detected near cable drums at a remote substation. PTZ cameras auto-track the movement while access control keeps gates locked. The security and surveillance platform alerts police, and a complete evidence pack is compiled, including licence plate recognition (LPR) data and a timeline of the incident.

What if there's no physical fence?

Not all assets have physical boundaries. Sites like reservoirs, pumping stations, or long-distance pipelines often sit in public or open-access environments, making traditional perimeter control difficult or impossible.

In these cases, virtual perimeters created using long range cameras and intelligent video analytics can detect:

- Movement or unauthorised presence (land or air e.g. drones)
- Suspicious lingering or gathering
- Suspicious scene changes
- Potential false alarms can be easily ruled out e.g. animal intrusion or debris movement caused by bad weather.

Solutions can also be configured to vary alert levels based on specific parameters and conditions, for instance time of day, movement rules, or access permissions, allowing site operators to monitor vast, unfenced landscapes without the need for physical barriers.

Where aerial threats are concerned, the risk is growing. In late 2024, reported drone flyovers of US nuclear facilities doubled in just one week[6]. By combining drone detection technologies, such as radio frequency and radar sensors, with cameras that automatically focus on the target, operators can see exactly where a drone is, follow its movement, and take immediate action. This can include alerting the control room, adjusting site operations, and sharing live footage with authorities.

[4] https://www.copperweld.com/blog/copper-theft-crisis?

[5] https://www.climatesolutionslaw.com/2023/04/physical-security-of-substations/

[6] https://www.twz.com/news-features/massive-uptick-in-official-drone-sightings-by-nuclear-power-plants

Verifying Site Access and Activity

For utility operators, controlling who enters a site, and ensuring that person is who they claim to be, is a core part of physical security.

Whether it's a lone maintenance engineer arriving on-shift, a delivery vehicle at a treatment plant, or a contractor working on a high-voltage transformer, every access event carries risk.

Security and surveillance solutions integrated with access control and analytics, provide the visibility and assurance needed to manage that risk effectively. Here's an overview of how:

- At many sites, access control begins with credentials: ID cards, fobs, mobile badges, or biometric verification. But on their own, these methods only confirm that a credential is valid, not that it's being used by the right person. Integrating access control with a security and surveillance solution allows operators to visually verify access events in real time.
- When someone presents a badge at a gate or door, the system can automatically display the relevant camera feed for that access point, providing a clear image of the individual or vehicle. Operators can check that the person matches the ID on file, that they're entering during authorised hours, and that no one is attempting to tailgate behind them. Facial recognition solutions can also be used to automate this process.
- License Plate Recognition (LPR) systems extend this principle to vehicle access. Registered vehicles can be granted entry automatically, while unknown or blocklisted plates can trigger an alert and require manual review. This is especially useful at uncrewed or low-staffed locations, where on-site verification isn't always possible.

Two-factor at the gate

For added assurance, especially where contractors or temporary staff are involved, entry can be granted only when a valid ID badge matches the registered licence plate of the arriving vehicle. The system automatically presents the live video feed for operator confirmation before access is approved.

- Every access attempt, successful or denied, is logged and can be linked with recorded footage. This creates a robust audit trail for security reviews, compliance reporting, and investigations.
- In high-risk environments, these tools help prevent unauthorised access, insider threat, and procedural breaches. They also support safety, ensuring that only trained personnel enter zones with specific operational or hazard risks.

Importantly, this comprehensive access verification process aligns with the requirements of both NERC CIP and CAPSS, where the ability to monitor, control, and audit access to critical infrastructure is essential.

Carry out virtual patrols

For dispersed or low-staffed locations, virtual patrols offer an efficient way to maintain visibility. Pre-set camera tours combined with AI analytics can simulate on-site patrols and detect:

- Unauthorised persons in restricted zones
- Environmental changes (e.g. debris blocking access, vegetation growth obscuring signage or camera views)
- Abnormal vehicle presence (e.g. parked too long, parked near restricted access points)
- When an anomaly is detected, workflows can dispatch mobile responders or escalate to emergency services as appropriate.

Protecting Personnel and the Public

Utility workers often operate in hazardous, high-risk environments, from isolated substations and chemical dosing zones to wind turbine plants and confined tunnels. Many of these locations are remote, physically demanding, or inherently dangerous.

Security and surveillance solutions, when integrated effectively, play a critical role in protecting field staff and lone workers. They support real-time visibility, enable rapid escalation, and help enforce adherence to essential safety protocols.

Supporting lone workers in isolated environments

Lone working is a reality for many maintenance and engineering teams. Whether responding to faults or conducting scheduled inspections, individuals may be required to access facilities alone, sometimes for hours at a time day or night, often without mobile signal or easy road access.

A unified security and surveillance platform can help mitigate this risk by:

- Logging access events (e.g. badge scans, gate unlocks) to monitor presence and duration.
- Using AI analytics to detect motion absence or prolonged inactivity, and trigger alerts if expected activity isn't detected.
- Employing time-at-risk timers to monitor how long an individual remains in a confined space, chemical zone, or other high-hazard area without checking in – alerting a supervisor if thresholds are exceeded.
- Enabling remote visual check-ins via PTZ cameras or wearable cameras.
- Integrating with AI detection, panic buttons or fall sensors, so alerts can be raised if a worker becomes incapacitated or distressed.

Remote teams or control rooms can then view live camera feeds and provide direct assistance accordingly, reducing discovery time and improving response outcomes.

Spotlight: Enforcing safety protocols

Security and surveillance solutions can be used to monitor and enforce critical safety procedures including the use of mandatory protective equipment and team-based working protocols.

For example:

- AI-based PPE detection can be used to verify and enforce equipment compliance for specific zones.
- Integrated analytics can alert operators if a lone worker enters a zone requiring a two-person team.
- Access logs can be cross-referenced with video to confirm procedural adherence after an incident, or during audits.

This supports a culture of accountability and offers clear evidence in the event of safety investigations or regulatory review.

Protecting the public in shared-use environments

Not all utility infrastructure is isolated. Assets like reservoirs or inspection shafts are often located in, or near, public areas – often without fences or active barriers.

In these cases, surveillance plays a dual role: detecting unauthorised access and helping to prevent accidental harm.

Examples include:

- Detecting members of the public approaching dangerous drop zones, such as open reservoir banks or outlet channels.
- Monitoring for people near unsafe or restricted structures.
- Using PA systems to issue audio warnings or alerts, triggered by motion or loitering detection.
- Alerting response teams to attend and escort individuals from high-risk zones.

Protecting public safety in these contexts is not only an ethical duty, it can also protect the operator from liability and reputational damage.

Legal duty... even to trespassers

Under the Occupiers' Liability Act 1984, UK utility operators can be liable for injury or death, even if the person was trespassing. An operator has a legal duty of care if they:

- Know (or should know) about a danger on site,
- Foresee the risk of trespass near it, and
- Could reasonably act to prevent harm.

Failing to act, for example by not using deterrents like surveillance or PA warnings, can result in civil liability. In other words, warning signs alone may not be enough – especially in areas accessible to children.

Reducing risk through remote technology

Advanced surveillance isn't just for detection, it can also reduce the need for humans to be exposed to risk in the first place.

Increasingly, utility operators are using technologies such as:

- Drones to inspect towers, rooftops, solar arrays, or remote pipelines
- Fixed-position or PTZ cameras in confined or hard-to-access spaces
- Thermal and infrared imaging to identify leaks, overheating equipment, or electrical faults without requiring physical proximity

Rapid Incident Investigation and Reporting

In the utilities sector, incidents must be addressed swiftly, not just to prevent recurrence, but to meet regulatory obligations, provide transparency, and minimise disruption.

Whether it's unauthorised access, a safety breach, or an equipment fault, having clear, time-stamped evidence is essential for internal reviews, compliance reporting, and, in some cases, legal defence.

A unified security and surveillance platform with built-in investigation tools can dramatically reduce the time and effort required to understand what happened, when, and why.

Accelerating footage review with AI

Traditional CCTV review can be time-consuming, especially when multiple cameras are involved across a large or multi-site operation.

AI-powered analytics transform this process by enabling operators to:

- Search by object (e.g. person, vehicle, bag).
- Filter footage based on clothing, facial features, colour, or movement patterns.
- Apply time and location constraints to rapidly narrow the field.
- Automatically extract relevant scenes where specific actions or objects appear.

Some security and surveillance platforms now support natural language query, allowing users to search video libraries with descriptive commands such as ‘Show all footage of a white van arriving after 18:00 near the chemical storage area.’

This makes it easier for non-technical personnel, such as operations managers or safety officers, to locate relevant footage without needing to master complex filtering systems.

Event linking across systems

Modern security and surveillance platforms don't just show video, they correlate it with data from other systems, including:

- Access control logs
- Alarm triggers
- Sensor alerts
- Maintenance schedules

This allows operators to build a full picture of how an incident unfolded. A badged entry, followed by a failure alarm and captured footage, can be reviewed in one unified timeline, reducing manual cross-referencing and improving response accuracy.

Scenario: Security breach

A remote electrical substation triggers a motion alert at 02:16. The security and surveillance platform automatically flags the event, queues the nearest PTZ camera, and sends the footage to the control team's mobile devices. A person wearing civilian clothing is seen climbing the fence, approaching cable storage units.

Using AI tools, the operator quickly filters the previous two hours of footage to track the individual's movements, confirming the point of entry and duration on-site. Access logs confirm no authorised personnel were scheduled. Within minutes, the footage is packaged and securely shared with local law enforcement, with system logs showing all actions taken.

Supporting regulatory and legal requirements

Footage and incident data often need to be shared with HSE teams, regulatory bodies, legal teams, or insurers. A well-configured system allows:

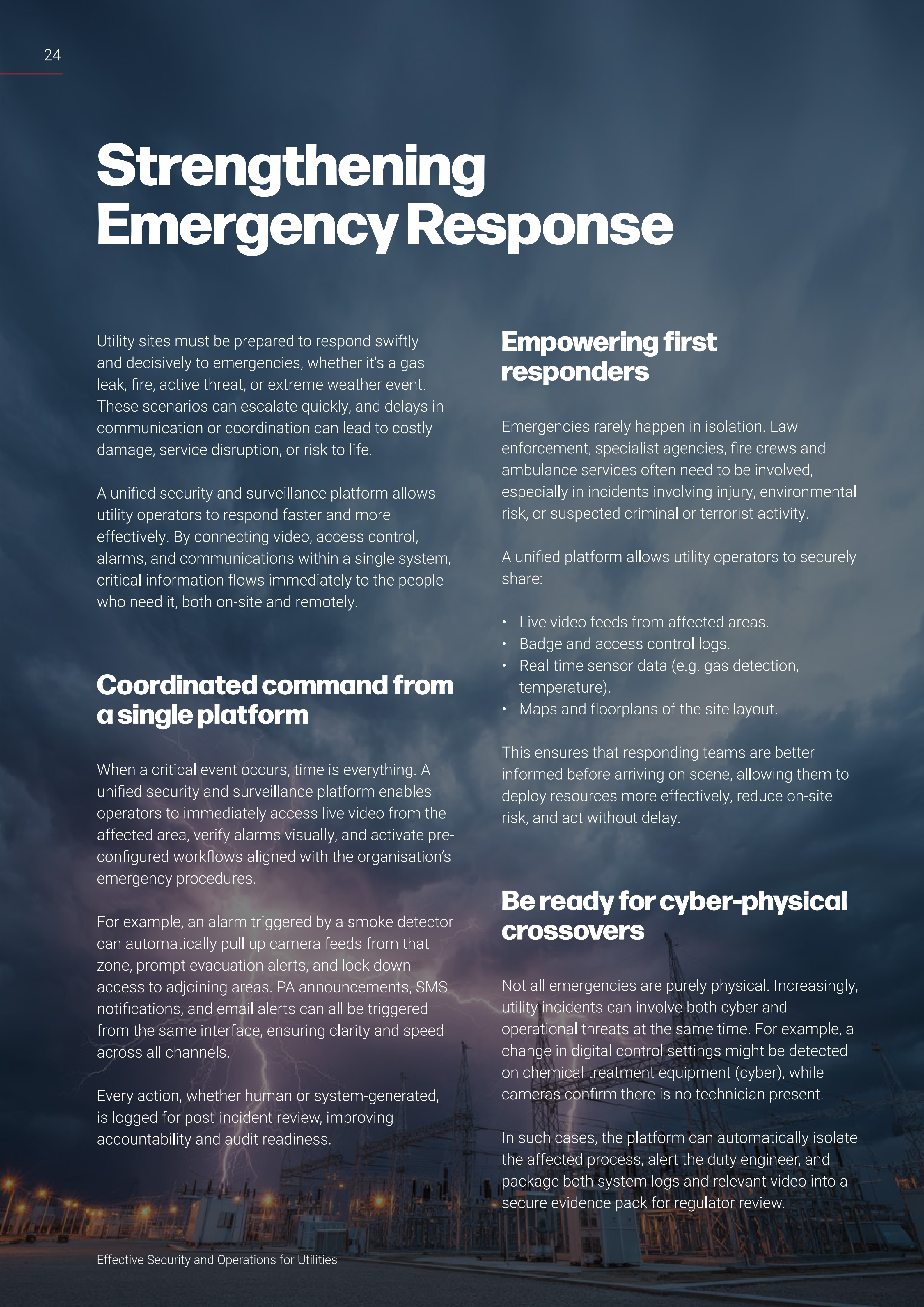
- **Secure evidence export** with audit trails and encryption
- **Redaction tools** to blur faces or licence plates for privacy compliance
- **Custom retention policies**, ensuring footage is stored in accordance with legal or operational requirements

In the US, for example, utilities governed by NERC CIP must retain and secure access logs and event data to support audits. In the UK and EU, GDPR requires careful handling of surveillance data, particularly when individuals can be identified.

Scenario: Contractor injury

A contractor reports a fall near a treatment tank. The security and surveillance platform has retrieved video footage from the relevant zone at the reported time. AI-based posture analytics detect and timestamp a slip event at 14:47. Footage reveals the contractor was wearing PPE, but the walkway was wet due to a leak.

Further review shows another worker walked past the same spot 15 minutes earlier and radioed a fault, helping confirm procedural compliance. Video, access records, and incident response data are compiled and shared with HSE investigators and the contractor's employer, demonstrating both transparency and a timely response.



Strengthening Emergency Response

Utility sites must be prepared to respond swiftly and decisively to emergencies, whether it's a gas leak, fire, active threat, or extreme weather event. These scenarios can escalate quickly, and delays in communication or coordination can lead to costly damage, service disruption, or risk to life.

A unified security and surveillance platform allows utility operators to respond faster and more effectively. By connecting video, access control, alarms, and communications within a single system, critical information flows immediately to the people who need it, both on-site and remotely.

Coordinated command from a single platform

When a critical event occurs, time is everything. A unified security and surveillance platform enables operators to immediately access live video from the affected area, verify alarms visually, and activate pre-configured workflows aligned with the organisation's emergency procedures.

For example, an alarm triggered by a smoke detector can automatically pull up camera feeds from that zone, prompt evacuation alerts, and lock down access to adjoining areas. PA announcements, SMS notifications, and email alerts can all be triggered from the same interface, ensuring clarity and speed across all channels.

Every action, whether human or system-generated, is logged for post-incident review, improving accountability and audit readiness.

Empowering first responders

Emergencies rarely happen in isolation. Law enforcement, specialist agencies, fire crews and ambulance services often need to be involved, especially in incidents involving injury, environmental risk, or suspected criminal or terrorist activity.

A unified platform allows utility operators to securely share:

- Live video feeds from affected areas.
- Badge and access control logs.
- Real-time sensor data (e.g. gas detection, temperature).
- Maps and floorplans of the site layout.

This ensures that responding teams are better informed before arriving on scene, allowing them to deploy resources more effectively, reduce on-site risk, and act without delay.

Be ready for cyber-physical crossovers

Not all emergencies are purely physical. Increasingly, utility incidents can involve both cyber and operational threats at the same time. For example, a change in digital control settings might be detected on chemical treatment equipment (cyber), while cameras confirm there is no technician present.

In such cases, the platform can automatically isolate the affected process, alert the duty engineer, and package both system logs and relevant video into a secure evidence pack for regulator review.

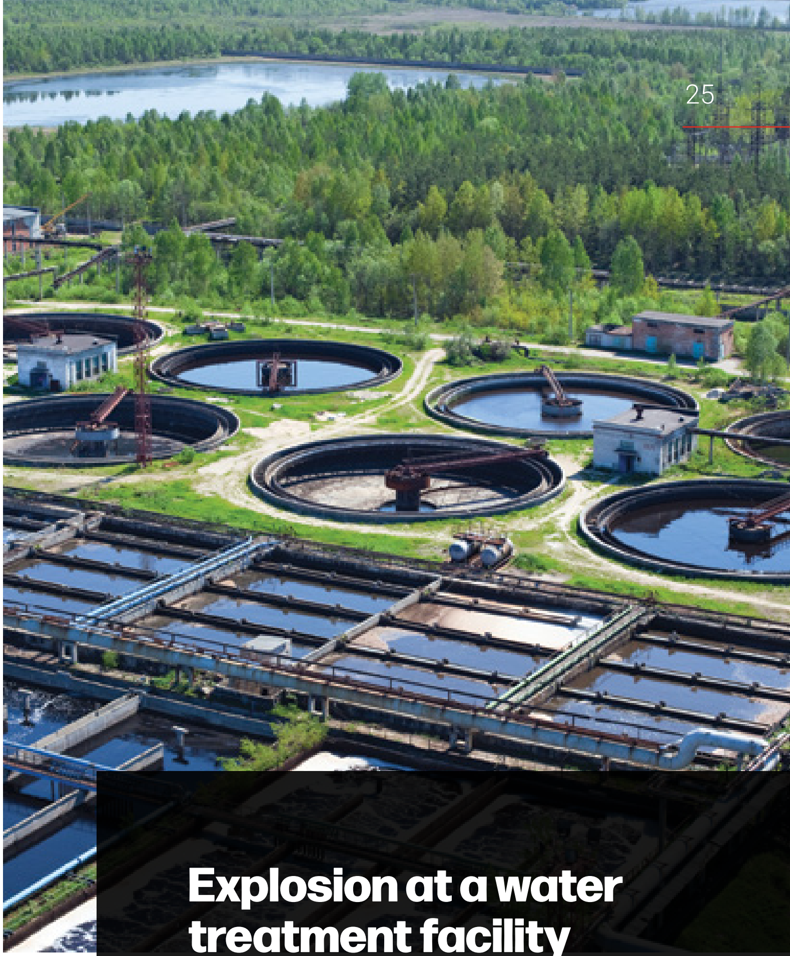
The US Environmental Protection Agency reported that over 70%[7] of inspected water systems since September 2023 have failed to meet required cyber standards.

Common scenarios

From a power station fire to a missing worker, the types of emergencies faced by utility providers are varied but many can be managed more effectively when systems are integrated.

A fire or gas leak can trigger a targeted evacuation protocol, illuminating safe routes and preventing re-entry. A physical threat can initiate a site lockdown, alert security teams, and enable real-time tracking of the threat via PTZ cameras.

Even medical emergencies can benefit from the system's data. Badge scans and video feeds can help locate an injured technician and guide paramedics to their exact location, especially in large or multi-level sites.



Explosion at a water treatment facility

An explosion occurs at a regional water treatment site, activating fire and impact sensors within the control building. Within seconds, the unified platform:

- Presents live footage of the impacted zone to the central control room.
- Locks all non-essential access points while keeping exit routes clear.
- Sends evacuation instructions via SMS and PA system.
- Shares camera feeds, maps, and hazardous zone data with emergency responders en route.
- Flags access logs to identify who was on site at the time of the incident.
- Tracks remaining personnel via badge data and AI-based location tools.
- Records all actions and responses for regulatory and insurance reporting.

This system-driven level of coordination can significantly reduce chaos, improve response times, and potentially save lives.

[7] https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities

Managing Multiple Sites and Remote Operations

Utility providers are rarely responsible for just one site. Whether operating a regional water network, a national energy grid, or a fleet of renewable assets, most providers manage dispersed and varied infrastructure, some of which is staffed, much of which is not.

Coordinating security and surveillance across these locations can be an operational challenge. A unified security and surveillance platform can provide secure, centralised visibility and control, making it easier to monitor activity, respond to incidents, and maintain consistent security standards across all facilities.

Central command for a distributed network

A unified system allows operators to view and manage surveillance feeds, alarms, access events, and system health from a single, central interface, accessible via secure desktop or mobile application.

Whether it's a local substation or a reservoir hundreds of miles away, incidents can be seen and addressed in real time, even without a physical presence on site.

Live dashboards display alerts across locations, while maps and camera groupings provide visual context for multi-site coordination. System status tools can notify teams of camera faults, connectivity issues, or unusual access behaviour, allowing problems to be addressed before they escalate.

Standardising access and permissions

Managing who has access to what, and when, is particularly challenging when contractors, maintenance crews, or vendors are moving between locations.

A unified system supports:

- Centralised credential management
- Role-based access profiles
- Time-limited or site-specific permissions
- Remote revocation of access in case of risk

This reduces the administrative burden and ensures policies are enforced consistently across every location, minimising human error and insider risk.

Monitoring mobile services and field operations

For operators managing mobile units such as maintenance crews, field-based water testing teams, or emergency repair vehicles, surveillance and tracking doesn't stop at the site perimeter.

Modern systems can integrate with GPS and onboard camera feeds to monitor:

- Live vehicle location and route history
- Driver identification and behaviour
- Boarding and departure logs (e.g. using ID badges or facial recognition)
- Incident alerts (e.g. harsh braking, unauthorised stops, or lone worker timeouts)

This provides full situational awareness of not only your infrastructure, but also the personnel and resources operating across it.

Responding remotely

With mobile-enabled response tools, operators can assess and act on incidents without being physically present. For example, if a fire alarm is triggered at a small rural substation:

- A remote operator can instantly view camera feeds from the location
- Cross-reference with temperature sensor data
- Check access logs to determine who last entered the area
- Notify emergency services, while activating automated lockdown or alert workflows all from a central control centre or secure mobile device

This reduces response time, eliminates unnecessary travel, and ensures coverage even in low-resource or out-of-hours scenarios.

Maintaining Compliance and Data Integrity

With the growing use of surveillance, analytics, and remote monitoring, utility providers must ensure that security doesn't come at the expense of privacy or introduce cyber vulnerabilities.

From GDPR obligations to NERC CIP compliance, data protection is not just about best practice, it's usually a regulatory requirement.

A well-configured security and surveillance platform should provide both physical security and data assurance, protecting the identities of individuals, securing sensitive operational footage, and reducing exposure to cyberattack.

Role-based access and user control

Not everyone needs access to every camera feed or system feature. To maintain accountability and reduce the risk of misuse, your platform should support:

- Role-based permissions that limit access based on job function
- Tiered clearance levels for sensitive footage or critical control features
- Full user audit trails showing who accessed what, when, and why

These controls not only protect privacy but also support transparency in the event of an internal inquiry or regulatory audit.

Privacy safeguards for individuals

Surveillance footage often captures images of employees, contractors, and members of the public. To ensure this data is handled ethically and legally, your system should offer:

- **Automated redaction tools** to blur faces or licence plates - either in real time or during footage export.
- **Privacy zones**, where specific areas (e.g. break rooms, public footpaths near sites) are masked or excluded from monitoring.
- **Audit-logged footage sharing**, so any external disclosure is tracked and documented.

These features will help you comply with data protection rules while helping to maintain trust with your workforce and local communities.

Video governance essentials

In the UK and EU, the Information Commissioner's Office (ICO) advises organisations to follow clear privacy-by-design principles when deploying or upgrading surveillance. Similar principles are reflected in US state privacy laws (such as CCPA/CPRA in California or BIPA in Illinois) and in industry-specific requirements like NERC CIP for utilities. Good practice includes:

- Complete a Data Protection Impact Assessment (DPIA), or equivalent risk assessment, before introducing new analytics, such as facial recognition.
- Use clear signage to inform people they are being recorded and the purpose of the monitoring.
- Apply purpose limitation i.e. only collect and process footage necessary for the stated purpose.
- Set retention periods to the shortest necessary for operational or legal needs
- Maintain audited logs for all footage sharing or disclosure.
- Enforce role-based viewing controls so only authorised users can access sensitive material.
- Use automatic redaction on export to protect identifiable individuals.

Ensure cyber resilience

Security and surveillance systems are increasingly part of the broader operational technology (OT) network, which means they can become a target for cyberattacks if not properly secured. Key security features to look for include:

- End-to-end encryption (AES-256 for data at rest; HTTPS/TLS for data in transit)
- System configuration encryption, to prevent reverse-engineering or tampering
- Multi-factor authentication for all admin and remote access points
- Automated configuration audits, to flag default passwords or outdated firmware
- Network segmentation to separate surveillance from critical control systems

These capabilities help ensure your surveillance system isn't a weak link in your organisation's broader cyber defence strategy.

Data retention done right

There's no one-size-fits-all rule for how long to store video footage, but in most regions, retention must be proportionate to purpose and legally justifiable.

Your platform should allow customisable retention schedules, based on camera, zone, or event type. For example:

- Keep standard footage for 30–90 days
- Retain incident-related footage indefinitely or until investigations conclude
- Lock footage for regulatory or legal purposes as required

This flexibility helps reduce storage burden while ensuring you're covered for compliance and incident review.

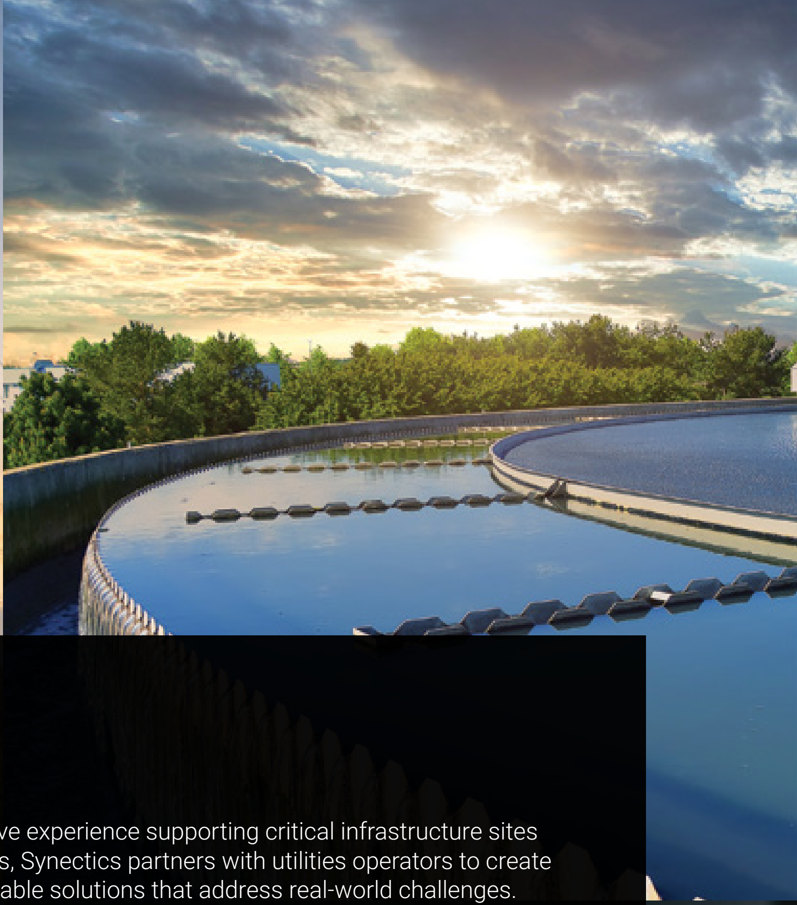
A Platform for the Future

The right security and surveillance solution doesn’t just protect, it strengthens resilience.

By streamlining critical security operations and improving situational awareness, it helps your teams detect, respond to, and minimise threats in real time, safeguarding infrastructure, field personnel, and essential services.

Built for adaptability, these platforms integrate seamlessly with emerging technologies and operational systems, allowing you to expand capabilities without replacing your core investment. The result is long-term value, future-proof flexibility, and minimal operational disruption.

s Month
Abduction
D.O.C
ASB
Assault (SEH)
Footage Requested
idents Today
Footage Requested
Map Display
Video
Lecture Hall
hion
t New Map
unctions
Snapshots Bar
Poi Bar
Help Point 5
Health emergency
✓ Call emergency services
✓ Mobilise nearest officer
✓ Ambulance on scene
× Incident resolved
ious Package
ation and item verified



Let’s Talk.

With extensive experience supporting critical infrastructure sites and networks, Synectics partners with utilities operators to create tailored, scalable solutions that address real-world challenges.

To discover how we can support your organisation, visit **synecticsglobal.com**.

Specifications subject to change. E & OE.

Literature Reference: UTIL/EB Iss 1

SYNECTICS

synecticsglobal.com