Offshore Threat Detection
Oil and Gas Surveillance at Sea

SYNECTICS

Introduction

Oil and gas provide the world's seven billion people with 60 percent of their daily energy needs. The offshore market plays an essential role in facilitating this supply. It is a sector of global importance.

Harsh, changeable weather conditions, industrial hazardous areas (often in close proximity to living quarters), and sheer distance from land-based response teams make offshore platforms and vessels extremely challenging in terms of both safety and security.

Operational malfunction, environmental impact, and external attack are all areas of significant potential threat that need

to be addressed with a precise, efficient, and effective approach – a task increasingly fulfilled using an integrated approach to surveillance.

This white paper examines these themes in detail and looks at how existing and emerging technologies are being used to protect and defend our global offshore industry.

An Unavoidable Truth

The importance of offshore assets to our economic and energy infrastructure inevitably makes them high-value targets. Given current international security concerns, this is a fact that cannot be ignored, and the threat is ever present.

While there have been few successful terrorist attacks targeting offshore

platforms to date, emphasis on prevention and response has never been stronger.

Offshore assets – fixed or floating – may not be able to prevent physical incursions, but the technology now available ensures crew or dedicated security teams are better equipped to monitor waters and identify potential

threats at significant distance. This enables response protocols to be activated much earlier including requests for response or support teams to be deployed.

But first, threats must be detected.

Potential threats need to be addressed with a precise and effective approach.

Anti-Piracy Detection, Monitoring, and Tracking Solutions

Establishing an Anti-Piracy, Monitoring, and Tracking solution is now widely regarded as industry best practice. It involves the integration of an asset's security and operational systems to identify and track potential threats.

This can be achieved using a database-agnostic surveillance command and control platform to merge data from multiple technologies and sub-systems, enabling users to identify threats and control the response from within a single unified environment.

What Type of Technologies Can Be Integrated into Such a Solution?

This will depend on the type of asset (platform or vessel, fixed or floating), however, the most common are:

- Primary detection sensor systems including marine pulse radar and Frequency Modulation Continuous Wave (FMCW) radar.
- Cameras – fixed, PTZ, Analog or IP, thermal and multi-spectral (color, mono, thermal). Most camera stations in an offshore setting will be certified for use in hazardous areas.
- Automatic Identification Systems (AIS).
- Electronic Chart Display and Information Systems (ECDIS).

What Does a Solution Like This Involve?

- Creation of a virtual perimeter (boundary) around the asset.
- Detection of any intrusions that cross, or are within, that boundary.
- Identification and classification of threat e.g. known hostile vessel.
- Threat tracking using visual and data positioning information.
- Automated response protocols e.g. emergency authority SOS notification.

What Happens When a Threat Is Detected?

The following example outlines a potential threat detection and response scenario:

An operator in the control room receives an alert on-screen informing of movement within a set perimeter has been detected.

The system 'knows' to tag the object for tracking once it crosses a pre-set virtual perimeter and satisfies the closest point of approach criteria of the asset. At this point an image is streamed live to the operator's monitor for visual tracking. The system is able to select the most appropriate camera sensor for the clearest footage e.g. mono, color or thermal, and then automatically track the target using precise Absolute Positioning.

Because the surveillance command and control platform is integrating other ship systems, the visual data is immediately cross-referenced with AIS information, which flags the approaching object as a risk requiring further investigation.

This risk alert initiates an on-screen workflow prompting the operator to lock down specific areas of the offshore asset, alert onshore response teams, and relocate all personnel to dedicated safe zones.

All actions and footage are automatically logged on the system for review and possible evidentiary use.
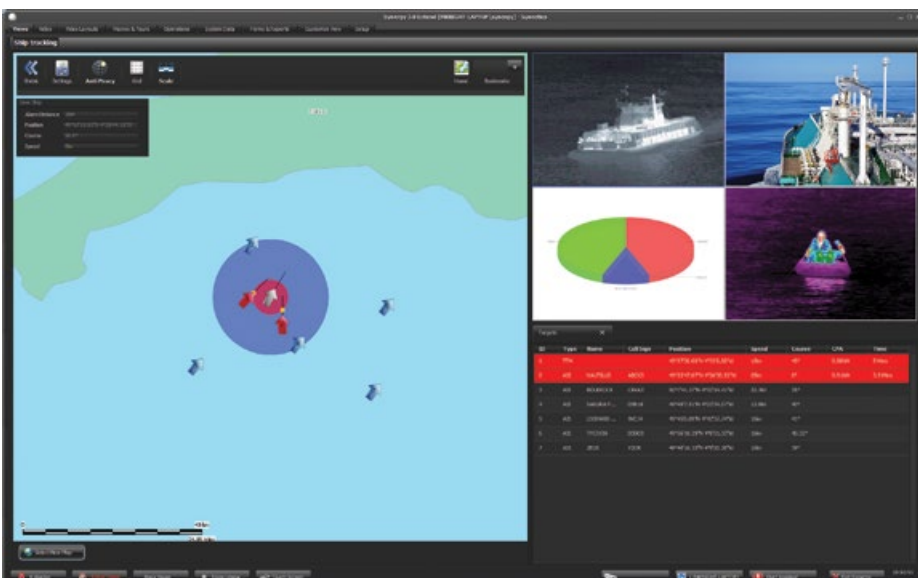
Ensuring Staff Safety

As well as ensuring adequate threat detection mechanisms are implemented, operators of offshore assets need to establish that the correct procedures are in place to protect their workers.

As referenced earlier, one element will include establishing dedicated safe zones including muster points and citadels. A safe muster point is a designated area chosen to provide maximum physical protection to the platform staff or vessel crew. It is intended to be a short-term haven.

Should the asset be boarded by hostile intruders, personnel would be relocated to a citadel (a secure area) equipped with its own access to the surveillance command and control platform where continuous situational awareness can be fed through to a central land-based monitoring center.

In some cases it may also be possible for teams taking refuge in the citadel to transmit footage or communicate via VSAT to 'friendly forces' such as the police or coastguard, providing real-time updates of the situation as it unfolds.

Not All Threats Are From Intruders

While guarding against physical security breaches is a key area of offshore threat detection, not all risks involve external hostile forces. Offshore asset operators also need to mitigate risks posed by operating conditions, as well as threats the asset itself may pose to its immediate environment.
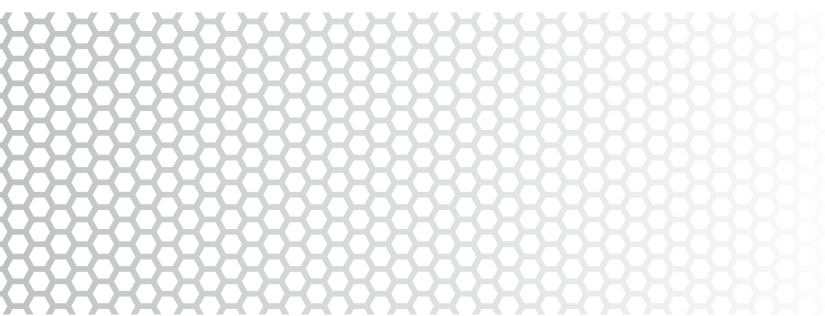
Ice-class Operations

In 2012, a 30-mile-long ice flow forced Shell to shut down its Burger-A well in the Chukchi Sea and the company later announced that as a "precautionary measure" it was suspending offshore drilling in Alaska for the remainder of 2013. Statoil quickly followed suit, shifting its focus to drilling projects in the Norwegian Barents Sea and exploration wells on the east coast of Canada.

Ola M. Johannessen, founding director of the Nansen Environmental and Remote Sensing Center (NERSC) and a world-leading oceanographer, explains how a better understanding of sea ice and its accelerating decline is now central to the success of upstream oil and gas operations in the extreme north:

"A serious risk assessment must be undertaken into the future development of sea ice in the Arctic, and its impact on the offshore industry and shipping."

"Icebergs are always a threat and their drift patterns are not easy to predict. In the Barents Sea and the Russian Arctic, grounded icebergs and those caught in strong tidal currents can potentially cause a lot of problems for underwater installations and pipelines."

"A significant number of very large icebergs are also being produced around the Greenland continental shelf. Smaller icebergs known as growlers are also risky, because they are very heavy, and difficult to observe using satellites and ship radar."

Operators need to mitigate risks posed by conditions as well as the threat the asset can pose to the environment.

Combatting the Cold

Camera specification is particularly important for offshore oil and gas operations located in harsh northerly sea locations and is an area where new technologies are emerging all the time.

Camera stations manufactured to withstand salt corrosion, operate at extreme temperatures (high or low), counter the impact of motion and vibration while capturing high-definition footage night or day, in the face of fog, storm conditions, or solar glare, are vital for offshore conditions.

Choosing cameras that are designed specifically for hazardous areas in marine environments ensures visual data is 'always on'. This level of dependability has become mission-critical for extreme offshore locations. Thermal imaging cameras are particularly important. In addition to providing imaging in complete darkness, they enable crew to detect floating ice hazards and assess surface ice thickness.

Combining reliable visual data into an integrated surveillance command and control platform can assist with safer navigational practices. When rapid support and emergency response crews are simply not feasible due to sheer remoteness, these benefits become hugely important. This is one of the main reasons why offshore oil and gas operators, in particular tanker operators, need to be clear what to look out for in the camera stations they specify.

For more information on the subject of surveillance solutions for ice-class marine applications, a separate dedicated white paper is available at bit.ly/marine-white-paper.

Operational Incident Detection and Prevention
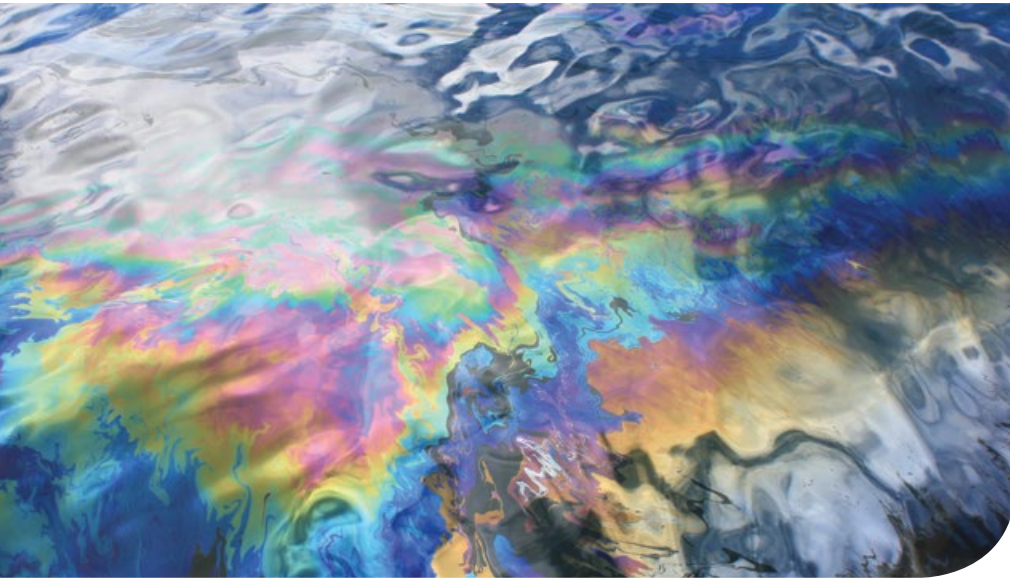
Over the years, the media has highlighted major oil spills and the catastrophic effects they can have on the environment. An oil spill in the Gulf of Mexico in April 2010 is officially the largest accidental oil spill in world history.

Given the severity of potential consequences, oil spill detection and verification are of paramount importance to the offshore oil and gas industry. Once again, this is an area where an integrated and proactive approach to threat detection affords significant advantages.

Detecting Oil Spills

Through combining data sets from multiple site systems, the time required to detect and respond to suspected leakage can be greatly reduced.

An oil spill can be initially detected by radar, followed by visual verification from footage captured by a thermal camera station located closest to the spill area.

The thermal camera station is able to detect spillage by demonstrating variations in temperature and thermal

emissivity between the oil and the water. Generally, due to the thermal conductivity of oil, it will become warmer than the surrounding water in the day by absorbing heat more quickly. During night-time, however, the oil will lose heat quicker than the surrounding water.

To detect oil spills effectively, the thermal imaging camera and the radar need to be tightly integrated together to ensure that the camera can quickly transition to focus on the area once identified by the radar. This is particularly important when the sea state can range from being glassy-calm to storm-force.

Flare Monitoring

Another important area where surveillance solutions can play a key role in threat detection and risk mitigation is flare monitoring.

While it is possible to use UV sensors for conventional flare monitoring, there are situations – for example when there is excessive smoke – when this mode of incident detection becomes less effective.

Thermal cameras, however, do not have this issue and can be used to measure the difference in 'thermal signature' between the flare and the surrounding environment – sky or clouds. Due to the spectral response of the camera, a moisture-free window in the atmosphere enables the cameras to obtain a good image of the flare or igniter flame – irrespective of whether the flame is visible to the naked eye.

Daylight cameras can also help to detect smoke or poor flame color, indicating an unoptimized stoichiometric mixture.

Finally, thermal cameras can be used to monitor the relative temperature of equipment and generate an alarm if the temperature changes beyond predetermined limits. Tank monitoring and pipeline leak detection are also widely used applications for thermal cameras.

The Complete Package

The right camera for the right job has a key role to play with regards to operational incident detection and prevention. However, as with external threat detection, the true power of this data comes from pairing it with further site systems via a command and control platform – using visual data to drive responses such as area or whole site shutdown (depending on pre-programmed risk assessment levels).

This process could involve evacuations, changing access control specifications, personnel tracking, and response team deployment. Operating multiple systems separately takes time and can impact an efficient co-ordinated response, two challenges single unified control environment can easily overcome.

Make the Connection

'Remote site protection' is a phrase used by many industries to reflect security and safety requirements for a wide range of location types. In terms of achieving this ambition, however, few face the same volume of challenges as the offshore market.

As this white paper has explained, potential threats are plentiful – both in terms of threats posed to and threat posed by operations. Combine that with at-sea inaccessibility, dangerous processes, and hazardous weather and the scale of difficulty is clear.

And it's the scale of this challenge that makes a connected approach to threat detection so suitable for this market. Offshore operators already use some of the most sophisticated technology available for safety, security, and process management; unifying these systems and managing them using a surveillance command and control platform unleashes a level of awareness that is otherwise difficult, time-consuming, and expensive to achieve.

Disparate systems monitored and managed individually leaves scope for threats to fall through the gaps. Operators that 'make the connection' will undoubtedly boost detection, prevention, and ultimately, whole-site protection

For more information about Synectics technology solutions, visit our website: synecticsglobal.com.

> **Operators that 'make the connection' will undoubtedly boost detection, prevention, and whole-site protection.**

Synectics designs integrated end-to-end surveillance control systems for the world's most demanding security environments. We excel at complex projects that require innovative, tailored solutions with high reliability and flexibility, specifically for casinos, oil and gas, marine, public space, banking, transport and critical infrastructure applications.

With over 30 years of high security systems experience, field proven products, and expert support personnel in the UK, US, Europe, UAE and Asia Pacific, Synectics offers its clients turnkey networked solutions for comprehensive protection and peace of mind.

Synectics' Systems division is part of Synectics plc, a global leader in advanced surveillance, security and integration technologies and services.

Synectics
sales@synecticsglobal.com
synecticsglobal.com

Americas   Asia   Europe   Middle East   United Kingdom