Designing IP video surveillance networks for flexibility, performance and security

In conjunction with DATASAT TECHNOLOGIES

Introduction

Real-time video surveillance has become an essential weapon in the armoury of public and private organisations worldwide as they look to address a wide range of security challenges.

The number of video cameras installed is growing rapidly as new and innovative video surveillance solutions are used for everything from military operations and border security to public safety and crime prevention. Applications such as traffic monitoring and management are becoming increasingly popular uses of video surveillance technologies.

With an increase in cameras comes an increase in the need for network infrastructure to support them. Wired systems cannot provide the cost and flexibility advantages necessary. Based on the fundamental principles of surveillance, reliability and resilience, wireless technology is fast emerging as the ideal method to take the capabilities of video surveillance to the next level.

The increased implementation of IP video surveillance has widened the possibilities of what this technology can deliver. Compared to traditional CCTV solutions, there is an increase in the capabilities, effectiveness and return on investment (ROI) of IP-based video surveillance.

By delivering the ability to integrate advanced video analytics and superior video management within the network, this approach allows the organisation to place intelligence much closer to the network edge – the actual area under surveillance – making the network more effective at delivering the correct information to the correct people wherever and however they connect to the network. Building intelligence into the network facilitates advanced operation while reducing the operators required.

This white paper identifies the key design considerations when developing an effective wireless IP video surveillance network.

The advantages of wireless infrastructure

The majority of video surveillance systems deployed today are still analogue CCTV connected to a wired network transmitted to a local or central control room. In situations where there is an area with an existing wired infrastructure and where the amount of cameras will remain static, this may still be viable but is expensive and extremely difficult to upgrade.

Where the area to be covered is remote or the implementation has to be flexible to scale up or down quickly, a wired network approach is likely to be prohibitive in terms of both the time and cost associated with delivering the systems. In fact, one estimate put the saving of a wireless video surveillance system as compared to a wired approach as over 90% on most occasions. When the wired implementation includes trenching – digging and channelling for the correct cabling, the requirements for permits and licenses may render this approach redundant from the outset.

It is easy to see how the costs of implementing a wired solution where there is no existing wired infrastructure soon mount. However, it is the time taken to deliver the surveillance solution that will tip the balance for most scenarios. Where putting in place the wired infrastructure can take months, a well designed and planned wireless surveillance network can be implemented in a matter of days. New cameras and network equipment can be installed in hours. It is simple to scale the network up to meet operational requirements and then scale the network down and redeploy equipment as operational demands change.

Where the surveillance operation is temporary and has to be rapidly deployed – such as for crime prevention activities or at music festivals and sporting events – wireless networks are likely to be the only viable, cost-effective solution. When implementing video surveillance into remote locations – such as the perimeter of mining and utility operations or monitoring national borders – wireless technologies can overcome the topology and roll-out issues faced by wired, fibre alternatives.

In this situation, it may be that wireless technology will provide the local networking infrastructure but will connect to satellite or fixed backbone for backhaul to a central management facility. Especially where an organisation is monitoring a number of remote locations in a number of different geographies from a central location, a hybrid networking approach allows the creation of a high performance, cost-effective solution that deploys the optimum technologies at each stage of the design.

The 802.11 wireless protocol has always been seen as an excellent choice for short-range, line-of-sight applications. This solution delivers high frame rate video from remote locations to an area with high-speed connections.

Each node communicates regularly with its neighbours to create routing tables to determine how video is routed through the network. This makes a wireless mesh network flexible and resilient as it automatically reconfigures routing as a new node is added or if a node fails. One drawback to this system has been the potential for increasing and variable latency which can affect the quality and performance of video transmission and equipment control – especially with Pan/Tilt/Zoom (PTZ) cameras. Today, 802.11 is a very mature technology and effective traffic management and intelligent bandwidth provisioning are built into the network management layer of leading wireless solutions.

The development of the 802.11n protocol has increased the performance both in terms of range and transfer rates of wireless signals. In tandem with a new generation of multi-radio wireless systems, the

Ideal security applications for wireless video surveillance

- 24 hour surveillance of high crime areas
- Covert surveillance for military and police
- Real-time video feeds for mobile 'first responders'
- 24 hour monitoring of remote perimeters such as airports, ports, supply depots
- Monitoring and management of remote and unmanned equipment and locations such as pipelines or utility assets
- Traffic monitoring and management
- Rapid deploy surveillance of public venues, music and sporting events

802.11n protocol can deliver a multi-radio architecture with capacity of up to 300Mbps per radio with virtually no performance degradation between network hops.

A single network provides complete multi-service operation and concurrent wireless backhaul over the license-free 2.4GHz and 5GHz frequency bands. Advanced voice and data applications can now co-exist on the same network infrastructure as the IP video surveillance network without degradation of any network service. The increasing use of secure wireless networks on the unlicensed spectrum means that the actual planning and implementation of new surveillance networks can be completed quickly and without undue bureaucracy.

The advantage of IP networking

As surveillance systems move from analogue CCTV to digital, the ability to build the surveillance network on IP that underpins the majority of modern data networks offers a great deal of functionality and cost benefits. It is worth noting that most commentators now agree that video will soon overtake data and voice as the most common form of traffic on IP networks. The result of this is that IP networks are becoming increasingly optimised for video and rich media traffic.

The major benefit of IP compared to traditional CCTV implementations is that IP is very mature and can be cleanly integrated with existing network infrastructure. In this way, an organisation is not tied into a proprietary or expensive solution. It can simply attach standard equipment – such as hard drives and storage arrays – to the network as required.

More importantly, the video camera becomes simply another piece of IP network equipment. With IP, the organisation can place video cameras anywhere on the network as if it were another computer or network device. As IP is a common format used across computing devices, live camera feeds can be accessed from any authorised computer, laptop, tablet PC or mobile handset that has a secure wireless Internet connection.

A wireless IP video surveillance infrastructure does not require a control room at every location. In theory, it does not require a control room at all. The systems can be accessed and managed from wherever the administrator requires. In practice, however, most large surveillance networks will have a centralised control facility where the video data is stored and managed.

As the IP camera becomes simply another network device, it is easy to scale the network one camera at a time to cost-effectively meet exact requirements. This is quite different from the enforced 4 or 16 channel jumps required for digital video recorders.

Another key advantage of IP-based surveillance networks is the ability to build intelligence into the network itself. Within traditional CCTV set-ups, the camera is simply a capture device – although some later models included limited local recording and storage facilities – and most of the video was transferred back to the control room for analysis, storage and management.

The classic control room would contain a bank of monitors displaying feeds from each individual camera or camera group, watched by a group of security professionals. Although some real-time video analytics packages were available, most analytics would be conducted using an external software package to analyse the recorded footage.

The introduction of IP cameras means the potential to have a computer at the network's edge. The camera can have its own intelligence. The camera can conduct the primary video analytics itself and decide which incidents to record and transfer to the control room. It allows an event to trigger the camera to record but has the capability to record a time period prior to the incident and subsequent to it as well.

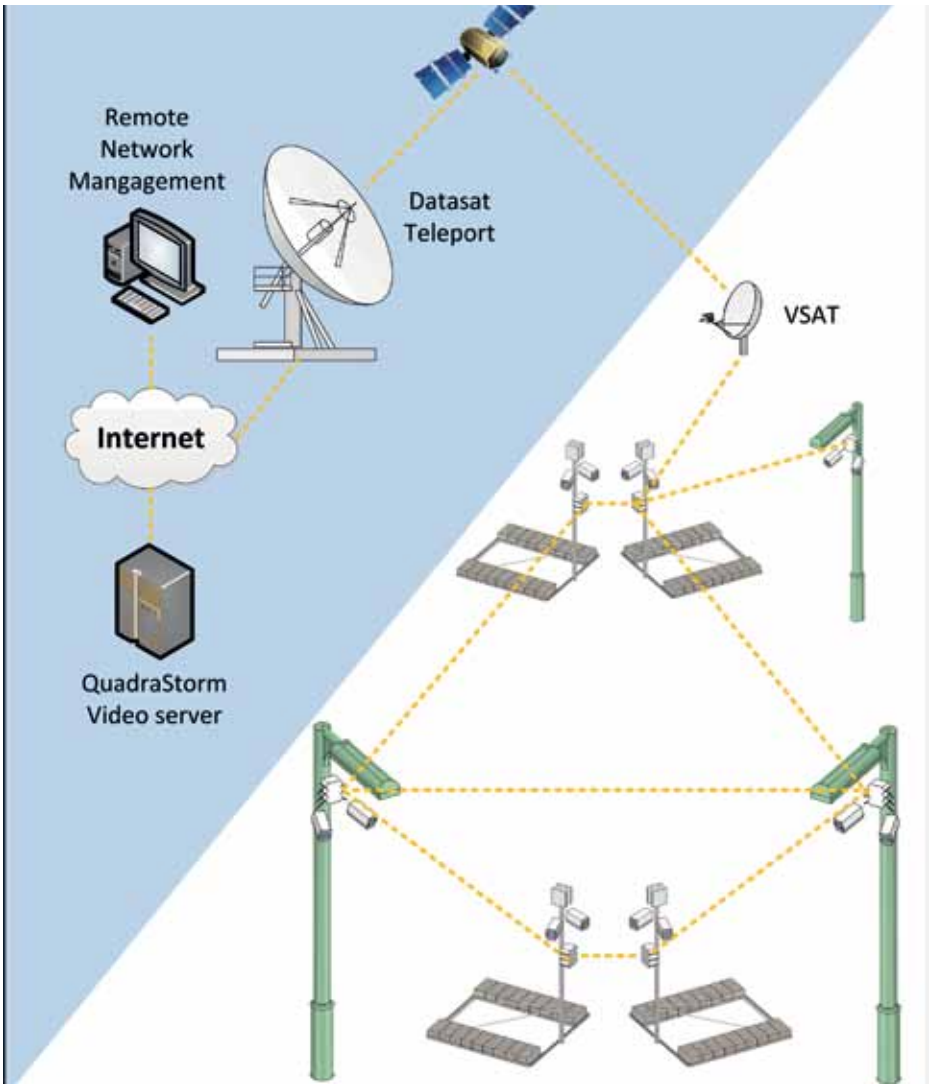
Unlike CCTV cameras that had to record everything and thus took up bandwidth to transfer unnecessary images, IP cameras only transfer images that are of interest to the monitoring professionals. In addition, IP cameras have advanced rapidly to provide many times the resolution of traditional analogue cameras. They can also monitor larger areas and offer superior zoom facilities. One organisation reported that its systems could correctly identify facial features through a glass door over 400 metres from the camera.

Finally, using a digital video format makes the storage and processing of video information much more straightforward. What would have previously required a warehouse full of video cassettes can now be stored on large disk arrays. In addition, the video captured on the camera is in exactly the same format when it is stored – an important element for evidential purposes. There is no need to extract the video and change its format for presentation in court.

Designing a wireless IP video surveillance network

From a design perspective, wireless networking can be more difficult to grasp than wired networking. With wired implementations, the wire carries a huge amount of throughput that is protected against most operating conditions. This is not the case with wireless.

The network designer needs to be aware of the geography of the installation, the characteristics of radio frequencies, the possible causes of noise and interference, the possible causes of latency and low video quality. They need to understand how the links will operate under a variety of conditions such as fading, distance and movement.



Typical video surveillance network deployment utilising the Datasat QuadraFlex multi-service, multi-radio wireless systems and the QuadraStorm video server range.

The final design will always be a balance of performance, security, reliability and cost. This all requires careful design, planning and installation. To begin, an organisation should ask the following questions:

- **Is all or part of the network outdoors?**
- **Is it monitoring high activity areas such as airport terminals, sports events or traffic?**
- **Does it need high-resolution and/or PTZ cameras?**
- **Will it be using video analytics? Where on the camera/network?**
- **Will the network have to scale easily/rapidly?**
- **Does it cover a large area?**
- **What are the geographic and environmental conditions like?**
- **Will the network carry other applications? If so, which?**
- **Who should have access to the network? How will they access it? From where?**
- **Will the surveillance network be distant from the control room?**
- **Are there video quality, storage and management standards that must be adhered to?**
- **Will recording be constant or event-triggered?**

The answers to these questions should give a clear idea of the capabilities and capacity that the wireless IP video surveillance network will require. This white paper will take each of the major elements of surveillance network design in turn to identify the key considerations to be addressed.

Planning for system reliability

Introducing effective video surveillance to remote locations primarily means creating a fully outdoor network. In the past, systems designers have often taken indoor rated equipment and placed it within temperature controlled enclosures to adapt it to outdoor conditions.

There are, as would be expected, a number of major drawbacks to this approach. Not least amongst these is the increased costs associated with heating and cooling these enclosures. There is likely to be increased demand for power that has to be supplied from alternate sources such as battery or solar. The introduction of heaters, fans and thermostats provides a number of extra points of failure that increases the need for maintenance across the network.

Network equipment for outdoor video surveillance should have the following capabilities:

- Tested for shock and vibration
- Operate in wide temperature ranges
- Require little heating or cooling
- Require few moving parts
- Provide DC operations
- Waterproof and dust proof
- Capable of operating in salt-spray and corrosive environments

In extremely remote locations, minimising the need for power and maintenance are both essential concerns. It is important that the network is designed to operate with equipment that does not require a temperature-controlled environment.

Most indoor surveillance equipment and networks operate on AC voltage as they have ready access to mains power. However, this is unlikely to be the case for surveillance networks in remote locations. All equipment – such as video cameras, wireless systems and access points – will need to function on DC to support alternate power sources. Primarily this is likely to be extremely long-life batteries although wind and solar are becoming increasingly popular alternatives.

Selecting the correct network equipment and power sources will depend on locations and the period of time the video surveillance system is expected to operate. With remote locations, it is probably sensible to design a network capable of delivering as close to continuous, unattended operations as possible.

A major part of this will be the selection of network equipment that has the fewest moving parts. Where moving parts are unavoidable – such as a PTZ camera – it is important to ensure that the equipment is resistant to temperature, weather and environmental factors such as sand and sea spray. Check that, if the parts require lubrication, this will not freeze or evaporate as climatic conditions change.

It may sound obvious but also check that all cabling is outdoor rated. Environmental elements will, over time, break down the jacket on indoor cable allowing water, sand or wind into the cable which will cause failure.

Regular maintenance visits will be required but these should be no more frequent than every 12 months. The system should be designed to be rugged and use ruggedised outdoor-specific network equipment that will minimise both power consumption and maintenance requirements.

The new 802.11n protocol increases the range and throughput that a wireless network can achieve. By designing the network in a mesh configuration, the video surveillance network can cover large areas while delivering a high degree of reliability and availability. The mesh configuration builds redundancy into the system but automatically reconfigures the route of traffic as a radio is added or one fails. If a radio – or series of radios – were to fail the network would automatically re-route traffic using the available network nodes with an almost imperceptible loss of performance.

Designing for network performance

There are a wide range of factors to consider when delivering optimum performance from a wireless IP video surveillance network. As most networks will require a balance between image quality and available bandwidth, the network design must provide the performance level that best meets the business needs of the organisation.

RESOLUTION AND IMAGE COMPRESSION

The higher the resolution of the camera, the greater the detail of the video image. Modern IP cameras can deliver resolutions of 2592x1944 and above. They enable PTZ capabilities around the image before and after the video has been stored. Of course, the higher the resolution and image quality, the larger the amount of data created and bandwidth required.

The quality of the image required will be dictated by the application. Monitoring public spaces like a car park may not require high quality images whereas applications involving accurate facial recognition will.

Video compression is an important tool to reduce the bandwidth requirements of video image transfer. Today, the H.264 standard offers an excellent trade-off between quality and bandwidth – it delivers around double the compression of MPEG-4 for the same image quality. However, MPEG-4 support may still be important for surveillance networks where the organisation needs to be able to create high quality still images from the video footage.

Data compression is greatly affected by the amount of motion occurring in the area under surveillance. The compression algorithm operates by comparing the differences between frames. More movement will result directly in greater bandwidth requirements as compression rates are much lower.

Some of the challenges of compression can be addressed by adjusting the frame rate – measured in frames per second (fps) – of the video capture. For example, 30fps provides very smooth motion but demands a good deal of bandwidth. Where motion is at a minimum as with most surveillance applications, an organisation can reduce the frame rate to help with bandwidth allocation. A person walking across an open space can be captured adequately at 4fps.

The advances in modern IP cameras mean that there are now very few situations where the system needs to be constantly recording and transmitting.

BANDWIDTH HUNGRY

The advances in modern IP cameras mean that there are now very few situations where the system needs to be constantly recording and transmitting. Instead, the camera only begins operation when a pre-defined event or set of behaviours is detected. In this way, high quality video images can be transmitted in real time in short bursts.

This approach can lead to 'data showering' where the network bandwidth is suddenly flooded as cameras switch into operation. Careful network planners have added an additional amount of bandwidth – as much as a fifth or a quarter more – to mitigate against this type of variation in traffic. More modern wireless network solutions have advanced bandwidth allocation and intelligent traffic management facilities that allow for the automatic prioritisation and bandwidth allocation of traffic to ensure that all services continue to perform well regardless of the demands of the surveillance systems.

Network throughput and latency

When designing a wireless network for video surveillance, it is essential to have a clear idea of the bandwidth the network will require across its lifetime.

The rule of thumb is that the more network throughput, the more radios will be required. Modern radios can provide throughput up to 300Mbps. However, it is the emergence of 802.11n multi-radio wireless devices that offer a breakthrough in terms of network performance.

A single radio system means that uplinks and downlinks occur over the same radio. Dual radio systems allow for the application services and backhaul functionality to occur on separate radios. The latest wireless systems can accommodate four radios that allow high performance, multi-service systems to operate over a single network infrastructure.

This approach to network design scales extremely well. The radios can be used in point-to-point or point-to-multipoint configurations to reach large geographical areas with a, theoretically, unlimited amount of video cameras. Adding more cameras does not impact the performance of existing cameras.

TACKLING LATENCY

Latency within the network is one of the key challenges for wireless systems. For video surveillance, it can result in poor image quality or patchy and pixelated images. High latency can make the remote operation of PTZ cameras extremely slow and unwieldy. Wireless mesh configurations can be prone to latency as there is likely to be a number of network hops between nodes as traffic is routed through the network.

The advanced traffic management facilities now available to wireless networks can optimise throughput while minimising latency. With low latency assured, network designers can achieve consistent performance regardless of variations in traffic loading. In this way, 802.11n wireless allows a surveillance network infrastructure that delivers real-time video to static and mobile users while concurrently supporting secure enterprise voice and data applications.

The latest wireless systems can accommodate four radios that allow high performance, multi-service systems to operate over a single network infrastructure.

Key network planning considerations:

- Protocol handling
- Assured bandwidth and traffic priority
- Traffic routing methods and mechanisms
- Methods of camera operations and security
- Load balancing and port aggregation
- System power and redundancy

Introducing Secure Wireless Anywhere Networks (SWAN)

Combining the latest innovations in 802.11 wireless technologies and advanced network intelligence, the SWAN platform from Datasat delivers new levels of advanced traffic management and rate limiting to meet the challenges of rich media services.

Granular network management allows us to intelligently allocate bandwidth and prioritise traffic types. SWAN delivers much greater control at an individual user, device or application level. Key features include:

INTELLIGENT TRAFFIC MANAGEMENT

The SWAN platform is based on hybrid layer management to allow granular control of most aspects of the wireless network. Finely tuned traffic priorities can be set, rate limiting is highly precise, congestion management is improved and interference avoidance protects against incidents capable of bringing other WiFi networks down.

VERSATILITY AND MODULARITY

Wireless devices can be added or removed to the network with the minimum of effort. Networks can be scaled up or down in a matter of hours. Networks can be designed using best-of-breed solutions and new wireless networks can be seamlessly integrated with existing communications infrastructure.

ADVANCED NETWORK MANAGEMENT

Every aspect of the network can be closely monitored and changes in the radio environment intelligently managed. Bandwidth can be dynamically allocated according to network priorities and airtime demands. In addition, complete remote network management can be provided through Infrastructure-as-a-Service.

INCREASED 'GOODPUT'

The SWAN platform intelligently adapts how traffic is handled to actively reduce contention issues and limit or eliminate data re-transmissions. Tests show that this network optimisation for video and audio delivery can achieve a significant increase in 'goodput' availability.

EFFECTIVE CONNECTION TO POPS

When designing a wireless network, it is often easy to overlook the challenge of establishing an effective Point of Presence (POP) into the fibre-based telecom infrastructure. The SWAN platform is designed to deliver a flexibility in the type of backhaul connectivity used, including fixed line fibre and VSAT satellite systems.

Find out more about the SWAN platform at www.datasattechnologies.com/technology/datasat-platform.php

Network management

It is not so surprising to find that the network management tools available for wireless are similar to wired networks. However, the sophistication of network management for wireless has been lacking.

Today, advanced wireless network management can happen at Layer 3 on the TCP/IP stack providing granularity of control in areas like:

- **Automatic bandwidth allocations**
- **Intelligent traffic monitoring**
- **Rate limiting and interference reduction**
- **Individual system, application, user and user group management**

This facilitates very stringent Service Level Agreements for performance, reliability and availability. Through intelligent Layer 3 management, wireless network infrastructures are driven by full Quality of Service (QoS) management at an individual traffic type or user group level.

There is another very important difference between wired and wireless management. Wireless networks should always be designed for remote operation and the management tools used should reflect this. These tools must be capable of over-the-air (OTA) management from facilities such as Internet-based consoles. This is essential for regular software updates as well as system configuration and monitoring. The ability to upload and install new software remotely is key to maximising network operations while minimising support costs.

An OTA management approach also increases flexibility by ensuring the administrators can manage the network from wherever they are. The administrator can receive alerts and updates directly to their tablet or mobile device. In addition, Internet-based management solutions allow organisations to benefit from Infrastructure-as-a-Service (IaaS) style management where the wireless network service provider can conduct all network management remotely while ensuring that the customer has full visibility and control over their network. Administrators can use mobile phones and tablet devices to control and manage the network wherever they are.

The key benefits of 802.1x

802.1x delivers a great deal of security benefits for wireless networks, including:

- Highly secure and scalable
- Reusability of authentication infrastructure
- Simplicity of user addition and removal
- Simplicity of authentication management
- No requirement for VPN capabilities
- With 802.1x, enterprise security can be achieved and assured in just a few clicks.

Ensuring network security

While security is an important consideration for all networks, it is doubly true for wireless networks.

As data cannot be contained behind a corporate firewall, it is possible for hackers to gain access to information as it passes between equipment on the network. Today, there are a number of tools for hacking wireless networks that are readily available.

In addition, the increasing use of the 2.4GHz and 5GHz unlicensed spectrum for 802.11 networks increases the pressure on network security. 802.11 uses very mature protocols which increases the number and variety of devices that are able to access an enterprise wireless network.

BEYOND WEP

The original wireless security capability was supplied by the Wireless Equivalency Protocol (WEP). However, WEP is too weak and vulnerable for corporate networks. Another approach is to restrict access to the network to only those 802.11 clients with authorised MAC addresses. The drawback to this approach is that it is cumbersome and costly to administer. It also lacks security as it has become straightforward to change or spoof a MAC address.

The widely accepted standard for network security is 802.1x – fulfilled by WPA2 Enterprise Security – which provides a high level of security across the network. Each client device uses a unique name and password which is checked against a LDAP server running the widely supported RADIUS security protocol.

A final note

Although there are still a number of situations where a wired surveillance network provides the best solution, the cost, flexibility and speed of implementation makes wireless a far more attractive option for the growing range of video surveillance applications required by modern public and private enterprises.

Unlike traditional CCTV networks that were single purpose and proprietary, modern surveillance systems benefit from operating over enterprise IP networks.

This not only allows for the introduction of more intelligent and higher resolution cameras as well as a new generation of video analytics, storage and management solutions, it also reduces the cost and administrative overhead involved. A video surveillance network can now be considered like any other corporate IP network, giving access to a wide range of open and affordable network devices.

In addition, the development of 802.11n multi-radio wireless devices allows for the creation of high performance WiFi networks delivering excellent throughput over very large areas. It is now possible to provide video surveillance over the same network infrastructure as other enterprise voice and data services.

By creating a video surveillance network based on a combination of wireless and IP technologies, an organisation has a platform to gain access to the optimum solution for their security requirements today that is capable of adapting to business and technological developments in the future.

About the Datasat Group

The Datasat Group comprises three companies – Datasat Digital Entertainment, Datasat Communications and Datasat Technologies. The Group develops a broad range of solutions designed to enhance the communications capabilities of individuals and organisations.

About Datasat Communications

Datasat Communications has 25 years of experience in creating complete remote communications solutions to meet customer needs virtually anywhere in the world. Specialising in satellite, wireless and terrestrial networks, it is an engineering-led company known for constructing and managing 'best fit' global communications networks. All network solutions from Datasat Communications are bespoke to customer requirements.

About Datasat Technologies

Datasat Technologies was formed in 2009 to deliver an evolution in wireless technologies specifically designed to support the latest developments in video, voice and data communications. Since then, the company has developed a range of network provision services to help customers maximise their investment in wireless and hybrid communications networks. It currently works with public and private organisations across the globe to deliver secure and reliable networks for the new generation of bandwidth-hungry, rich media applications.

Contact Us

Datasat Communications
Brookmans Park Transmission Station
Great North Road
Hatfield, Hertfordshire
AL9 6NE, UK

Tel: +44 (0)1707 665 320
Email: sales@datasat.com
Web: www.datasat.com

Datasat Technologies
5 Tavistock Estate
Ruscombe Lane
Twyford, Berkshire
RG10 9NJ, UK

Tel: +44 (0)118 982 8665
Email: sales@datasat.com
Web: www.datasattechnologies.com