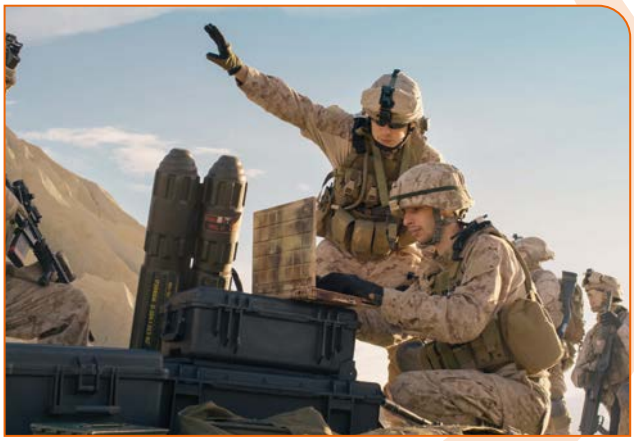
ND SAT COM

INSTALLING RELIABILITY

COMPREHENSIVE SECURITY IN SATCOM

SECURE, RESILIENT AND FLEXIBLE SATELLITE COMMUNICATIONS FOR GOVERNMENT AND MILITARY

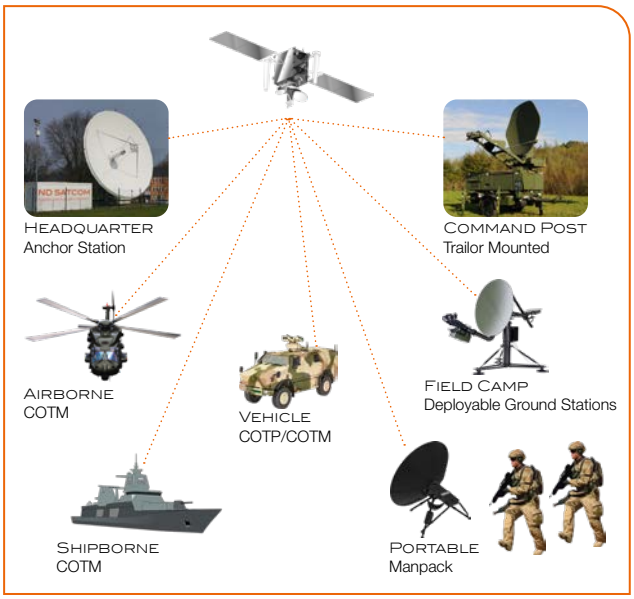
Secure, resilient, and flexible communications networks are crucial for governments and militaries to protect national security, ensure continuity of operations during emergencies, enable effective coordination and rapid response, and support changing needs.
These networks must prioritize security to prevent unauthorized access and cyber attacks. They must be resilient and able to withstand disruptions, while also being flexible to adapt to changing circumstances. By providing real-time collaboration, data sharing, and rapid decision-making, these networks can help support successful government and military operations.



TACTICAL COMMUNICATION

SATELLITE COMMUNICATIONS

Satellite communications plays a critical role in providing secure, resilient, and flexible communications networks for government and military organizations.
It can provide connectivity to remote or inaccessible locations, where traditional communication infrastructure may not be available or may have been damaged. This is particularly important for military and government organizations that need to operate in areas with limited infrastructure, such as in disaster relief or remote military operations.
In addition, satellite communications can ensure a high level of security for sensitive and classified information. It can use encryption and other security measures to protect against interception or eavesdropping, making them a valuable tool for government and military organizations that deal with highly sensitive information.
Last but not least, satellite communications can also provide resilience in the event of disasters or emergencies. Because satellite communications networks are independent of terrestrial networks, they can continue to operate even if terrestrial infrastructure is damaged or destroyed. This can help ensure continuity of operations during crises, enabling governments and armed forces to respond effectively.



TACTICAL SATELLITE COMMUNICATION IMPLEMENTED ON A WIDE RANGE OF PLATFORMS

SKYWAN

In the field of satellite communication, SKYWAN is a technology with a proven track record for government and military organizations.
One of the key features of SKYWAN is its ability to support a mesh topology, which enables direct connectivity between different nodes in the network, regardless of their location. This allows for efficient communication between different parts of the network and ensures that communications can continue even if one or more nodes become unavailable.
SKYWAN also provides both COMSEC (communications security) and TRANSEC (transmission security) to protect against interception and eavesdropping. COMSEC ensures that the contents of communications are kept secure, while TRANSEC ensures that the communications themselves are protected from interception.

SKYWAN SECURE SATELLITE COMMUNICATION TECHNOLOGY

TOPOLOGY

The hubless and mesh topology of SKYWAN provides resilience, flexibility, and security because it enables single-hop communication between different nodes in the network, without relying on a centralized hub as a single point for cyber or physical attack. This means that

the network will continue to operate even if one or more nodes become unavailable, making it highly resilient to disruptions.
The mesh topology of SKYWAN also provides flexibility by allowing for the dynamic routing of traffic. This means that if one node becomes unavailable, traffic can be rerouted through other nodes in the network, ensuring that communications can continue without interruption.
In addition, the hubless and mesh topology of SKYWAN provides security by eliminating a single point of failure in the network. Because there is no central hub that processes all network traffic, there is no single point of entry for attackers to target. This makes it more difficult for attackers to disrupt the network or intercept communications.

DEFINITION OF COMSEC AND TRANSEC

COMSEC and TRANSEC are both terms used to describe aspects of information security in communication systems.
COMSEC stands for “communications security”, which refers to the protection of the content of communication, such as voice, data, or video, from unauthorized access or interception. COMSEC measures include encryption, decryption, key management, and access control to ensure the confidentiality, integrity, and availability of the information being transmitted.
TRANSEC, on the other hand, stands for “transmission security”. Transmission security focuses on the protection of the transmission medium, such as a terrestrial wireless or a satellite link, to ensure that the communication cannot be intercepted or disrupted. TRANSEC measures include techniques like authentication, access control, and secure routing to ensure that the communication channel remains secure.
In short, COMSEC protects the user data, while TRANSEC protects the transmission link. Both COMSEC and TRANSEC are critical aspects of information security in communication systems and are often used together to provide comprehensive protection.

COMMUNICATION SECURITY

SKYWAN provides robust COMSEC (communications security) features to protect the confidentiality, integrity, and availability of information transmitted over the network.
First of all, SKYWAN uses industry-standard encryption algorithms (AES-256) to secure the content of communications, including voice, data, and video. The encryption ensures that adversaries can not access and read the information being transmitted, even if the communication is intercepted. The encryption keys are managed securely to ensure the confidentiality of the communications.
In addition to encryption, SKYWAN grants access to terminals for authorized terminals only. Users are required to authenticate themselves using their credentials, before they can log into the terminal or network management. This helps prevent unauthorized access and ensures the security of the SKYWAN network.
Overall, SKYWAN provides robust COMSEC features to protect the content of communications transmitted over the network. By using industry-standard encryption, access control, and other security measures, SKYWAN ensures that only authorized users can access and read the information being transmitted, making it a highly secure communication technology for government and military organizations.

TRANSMISSION SECURITY

SKYWAN provides robust TRANSEC (transmission security) features to protect the transmission medium, such as the satellite link, from unauthorized access or disruption.
To ensure secure transmission, SKYWAN uses a variety of techniques, including access control and authentication mechanisms, to restrict access to the network components and verify the identity of users. Only authorized users are permitted to manage the network, and they must first authenticate themselves before being allowed to use the system. This helps prevent unauthorized access and protects the transmission medium from being compromised.
SKYWAN also uses routing and packet forwarding mechanisms to ensure that communications are transmitted securely over the satellite link. SKYWAN’s mesh topology allows for multiple paths for communication to reach its destination, which ensures that there is no single point of failure that can be targeted by attackers.
Moreover, SKYWAN employs advanced link optimization and error correction techniques to ensure high-speed and reliable data transmission over the satellite link. This helps ensure that the communication is delivered quickly and reliably, even in harsh or remote environments.
In summary, SKYWAN provides robust TRANSEC features to protect the transmission medium from unauthorized access and disruption. By using techniques such as access control, authentication, routing, packet forwarding, and link optimization, SKYWAN ensures that communication is secure and reliable, even in challenging environments.

TRANSEC MEASURES

PROTECTION AGAINST INTRUSION, UNAUTHORISED NETWORK ACCESS AND TERMINAL CLONING

A SKYWAN network with its terminals is protected against unauthorized access, intrusion and terminal cloning by enforcing authentication. SKYWAN uses several authentication mechanisms to verify the identity of users. These include username and password combinations. Each user is assigned a unique set of login credentials that they must use to access the network. Also, a dedicated concept of roles is used to separate users and administrators.

On the terminal side, the authorized terminals themselves are identified by serial number and digital certificates (X.509). X.509 certificates provide a mechanism for mutual authentication between network nodes and the network, helping to prevent terminal cloning and other forms of unauthorized access.

Each terminal in the SKYWAN network is assigned a unique X.509 certificate that includes information such as the terminal's identity, public key, and other relevant data. When a terminal attempts to connect to the network, the certificate is presented to the network for verification.

The network uses its own X.509 certificate to verify the authenticity of the terminal's certificate. If the terminal's certificate is valid and matches the identity of the terminal, the network allows the terminal to connect to the network. If the terminal's certificate is invalid or does not match the identity of the terminal, the network denies access and prevents terminal cloning.

By using X.509 certificates for mutual authentication, SKYWAN is able to ensure that only authorized terminals can connect to the network, preventing terminal cloning and other forms of unauthorized access. Additionally, the use of X.509 certificates provides an additional layer of security by allowing the network to verify the identity of the terminal and ensure that it has not been tampered with or compromised.

ENSURING LOW PROBABILITY OF INTERCEPT

SKYWAN provides a low probability of intercept by using several techniques to make it difficult for eavesdroppers to intercept or decode transmissions.

- Hubless/Mesh
- Frequency Hopping
- Spread Spectrum
- Proprietary MF-TDMA

First and foremost, the mesh and hubless topology used by SKYWAN helps to decrease the probability of intercept. In a mesh topology, each terminal is connected to multiple other terminals in the network, and data is transmitted directly between terminals rather than being routed through a central hub. This decentralized approach to routing data makes it more difficult for eavesdroppers to intercept data because there is no central point of interception.

In a hubless topology, there is no central hub or point of control in the network. Instead, all terminals in the network are equal and work together to route data to its destination. This approach to networking makes it more difficult for eavesdroppers to intercept data because there is no central point of control that can be targeted or compromised.

The combination of a mesh and hubless topology in SKYWAN can help to decrease the probability of intercept by distributing data across the network and eliminating central points of control or interception. This makes it more difficult for eavesdroppers to target specific parts of the network and intercept data.

Another technique used by SKYWAN is frequency hopping, where the system changes the frequency of transmission multiple times per second over a range of 1,200 MHz. This makes it difficult for eavesdroppers to lock onto a particular frequency and intercept the transmission. SKYWAN's frequency hopping algorithm is designed to ensure that there is minimal impact on the system's performance while maintaining a high level of security.

Another technique used by SKYWAN is spread spectrum, which involves spreading the signal over a wide frequency band. This makes it difficult for eavesdroppers to detect and intercept the transmission because the signal appears as noise over a wide frequency range. SKYWAN's Multi-Frequency TMDA in addition spreads bursts of data efficiently up to 1,200 MHz to ensure a high level of security and robustness.

In addition, the proprietary TDMA (Time Division Multiple Access) structure used by SKYWAN helps to decrease the probability of intercept. TDMA is a technique used to divide a single communication channel into multiple time slots, with each time slot being assigned to a specific user group with additional dynamic sub-framing to address individual users. This allows multiple users to share the same frequency band and transmit data without interfering with each other.

SKYWAN uses a proprietary TDMA structure that allows for highly efficient use of the available bandwidth and ensures that each terminal is assigned a unique time

slot for transmission. This means that only one terminal can transmit data in a particular time slot, avoiding collisions and interference.
The use of TDMA in SKYWAN's proprietary structure also makes it more difficult for eavesdroppers to intercept transmissions because the time slot assigned to each terminal is constantly changing. This makes it difficult for an eavesdropper to identify all transmitted time slots of a particular terminal and intercept the transmission.

OBFUSCATION AND MASKING OF CHANNEL ACTIVITY

Obfuscation and masking of channel activity refer to the techniques used to make the traffic being transmitted over the satellite link appear as if it is something else. This can help to prevent unauthorized parties from intercepting, monitoring, or tampering with the data being transmitted.
Traffic pattern obfuscation refers to the techniques used to make the traffic being transmitted over the satellite link appear as if it has a different pattern or structure than it actually does. This can help to prevent attackers from recognizing and interpreting the data being transmitted, even if they are able to intercept the data.
SKYWAN conceals with free slot assignment the active spots of a SKYWAN network. All TDMA slots are filled to its maximum extent with data or dummy bits in case there is space left. This fakes a constant utilization of the satellite link regardless of traffic profiles.
The combination of adaptive slot assignment in a hubless system, free slot assignment and dummy bit insertion for obfuscating the traffic patterns makes it even more difficult for attackers to recognize and interpret the fragmented data being transmitted over the satellite link.

HANDLING OF METADATA

Metadata is information about the data being transmitted, such as the sender and recipient's IP addresses, packet size, geographical position and time stamp. This information can be used by attackers to gain insights into the traffic being transmitted and potentially compromise the security of the network.
SKYWAN does not transmit metadata as plain text over the satellite link. Instead, SKYWAN encrypts and splits user data streams in small sub-frame fragments before transmitting the data over the satellite link. This helps to ensure that the traffic being transmitted is as secure as possible, as attackers will not be able to gain insights into the traffic by analyzing the metadata.
The SKYWAN MF-TDMA waveform ensures correct timing based on local calculation for proper TDMA timing without relying on GPS information of all stations.
Overall, by not transmitting metadata in plain text and using additional techniques to further protect against the transmission of metadata, SKYWAN helps to ensure the security of the traffic being transmitted over the satellite link. This helps to prevent attackers from gaining insights into the traffic and potentially compromising the security of the network.

SUMMARY

Overall, SKYWAN provides a highly secure, resilient, and flexible communications network for government and military organizations. By supporting mesh and hubless topology, COMSEC, and TRANSEC, SKYWAN enables efficient communication, protects against interception and eavesdropping, and ensures the continuity of operations even in adverse conditions. This makes SKYWAN a valuable solution for government and military organizations that require reliable, secure communications, even in remote or challenging environments.
Due to the high level of security the SKYWAN system protects hundreds of mission critical networks worldwide and the user base includes a number of militaries.

GLOSSARY

COMSEC Communications Security – a component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material (Source: NIST Glossary).

TRANSEC Transmission Security – measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals (Source: NIST Glossary).

AES-256 – Advanced Encryption Standard with a key length of 256 bit. The primary mechanism for protecting the satellite link consists in the AES-256 encryption of traffic and signalling. AES-256 is considered as a quantum secure symmetrical encryption method.

FIPS 140-2 – Federal Information Processing Standard (FIPS) Publication 140-2. It documents the US Standard for Security Requirements for Cryptographic Modules and is published by the National Institute of Standards and Technology (NIST).

Certification / Accreditation Process – the majority of user organisations (at least the government / military organisations) require certification of the TRANSEC products and functions. The certification, which is an Information Assurance (IA) aspect, is based on standards/ rules, policies and guidelines, typically established at the national level. In the US, the certification is performed against the security requirements for cryptographic modules, as defined in the FIPS 140-2 standard.
In Germany, the certification is performed against the security requirements set by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik BSI).
The BSI is the National CIS Security Authority (NCSA) and security products approved by a NCSA are recognized by the NATO and allied nations.

X.509 Authentication – the X.509 certificate is a safeguard against malicious network impersonators as each and every network node is authenticated by an certificate authority. The X.509 standard defined by the International Telecommunication Unions's Standardization Sector (ITU-T) is the common global language for certificates used in public key infrastructure. The standard based authentication scheme allows a seamless integration into a customer's existing public key infrastructure.

MF-TDMA Waveform – SKYWAN uses Multi-Frequency Time Division Multiple Access on the physical layer. This enables capabilities with spectrum usage from enhanced BPSK up to 16APSK combined with burst hopping up to 1,200 MHz. Ressources are assigned highly dynamic on terminal request including traffic masking.

HEADQUARTERS
ND SatCom GmbH
Graf-von-Soden-Strasse
88090 Immenstaad
Germany
PHONE: + 49 7545 939 0
FAX: + 49 7545 939 8780
E-Mail: info@ndsatcom.com

CHINA
ND SatCom (Beijing) Co. Ltd.
PHONE: +86 10 8532 1826

MIDDLE EAST
ND SatCom FZE
PHONE: +971 4886 5012

March 2023, Version A.2