PERSPECTIVE

SECURING CANADA'S COMMAND AND CONTROL COMMUNICATIONS

HOW CAN BOTH SAFETY AND SECURITY BE REALIZED ON ONE RED/BLACK VOICE COMMUNICATION SYSTEM WHILE DEFENDING AGAINST CYBER-ATTACKS AND ELECTRONIC WARFARE? FREQUENTIS' MICHAEL DELUEG AND MARTIJN SACK EXPLAIN…

The Royal Canadian Air Force (RCAF) is responsible for protecting domestic and continental defence operations. It depends on classified and unclassified communications and highly reliable networks to perform its mission. When radar or digital datalinks fail, operators' mission-critical last line of control is to rely on their voice communication systems (VCS).

RCAF Air Command and Control (C2) operators need to be supported by technology that is failsafe, trusted and secure. They need to be able to execute mission-critical tasks without fear of network outages or security breaches.

How does the Frequentis Integrated Communications Systems for Command and Control, iSecCOM, provide secure, tactical communication and cybersecurity, as well as transform the disparate networks and links into a Tactical Network?

iSecCOM and Secure Communication

Civil Air Navigation Service Providers (ANSPs) and their military counterparts in C2 centres must work together to ensure safe routing for civil traffic, managing training areas, as well as en-route services for transiting military aircraft.

Meeting both security and safety requirements in one system is mandatory in mission-critical applications. Mission-critical voice communication systems for tactical and operational command and control systems within the civil and military sectors are required to provide both single (BLACK-only) and dual-security domain (RED and BLACK) capabilities.

Let's look at a typical mission scenario. When an aircraft embarks on a mission it must be able to talk to air traffic control and communicate with the tower at the airport. This communication is unencrypted, open – BLACK. Once the aircraft takes off and enters the mission area, the pilot and the control centre need to exchange classified mission-related information over secure voice channels like LINK 16 J-Voice. It is here that the pilot and the control centre now switch to encrypted, closed – RED – communication. While the mission operator is communicating over secure channels, operators should be able to receive unclassified communication via radios and telephony lines. Once the mission is complete and the aircraft returns to enter civilian airspace again the pilots voice communications mode will need to return to BLACK mode to talk with the tower again.

The Frequentis iSecCOM addresses this by providing access to all kinds of communications, be it analogue, digital, classified or unclassified radio or phone communication, on a single voice switch and human machine interface (HMI). In the past operators had to switch systems and headsets, and thus were prone to operational errors or information leaks.

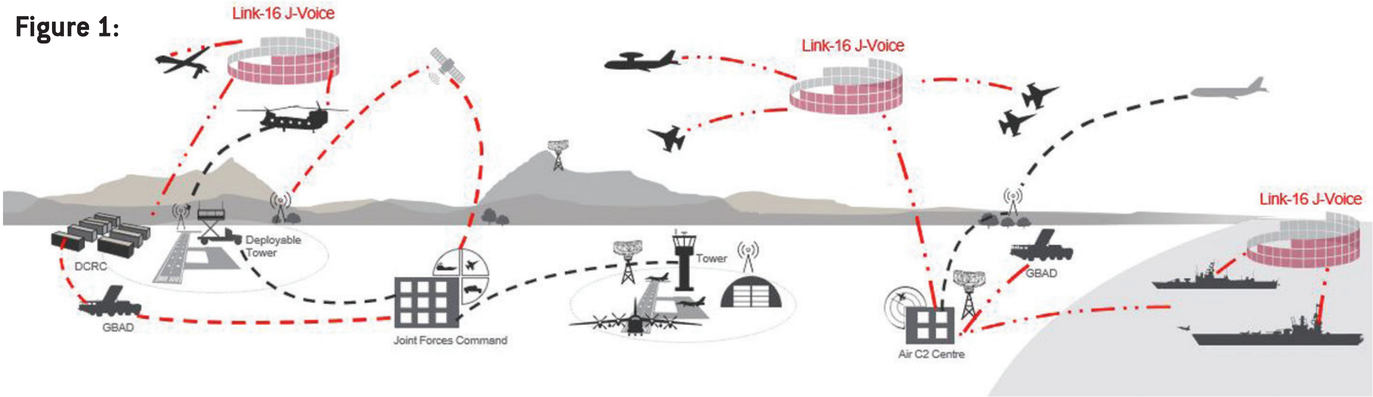
iSecCOM and Tactical Communication

When classified information is to be shared securely between centres and aircraft, it can be achieved with VINSON-compatible crypto devices which are connected to Frequentis crypto gateways and ECCM (Electronic Counter-Counter Measures) like Have Quick I/II and SATURN. The use of cryptos can be optimised with support of dynamic crypto allocation mechanisms. It is also possible to use a secure communication gateway to natively interface with LINK 16 infrastructures over J-Voice.

An extra security layer for wide area networks (WAN) which connect centres and remote radio sites can be realised with certified IP cryptos. Such crypto devices secure external network segments.

Adhering to military and industry standards gives operators everything they need for effective mission management across telephone, intercom, radio, recording, data and conference services, all via a single operator position with customisable HMI.

Figure 1:



To provide access to both security domains (RED/BLACK) on a single operator position a secure switch is needed. A central component in RED/BLACK scenarios is the Frequentis iSAS which is a unique Secure Audio Switch that meets the Common Criteria recognition arrangement for components up to EAL4+ – NATO Secret.

On request, iSecCOM installations can be TEMPEST certified to ensure maximum information security.

iSecCOM and Cybersecurity

In addition to ensuring communication channels are encrypted, it is important for preventative measures to be adopted. Safety-critical infrastructure is an attractive target in cyber warfare, so it is important to implement protective measures by design. In the past, voice communication and control systems were typically based on proprietary hardware and software running in complete isolation. Today, safety critical services run on interconnected standardised platforms, opening themselves up to highly sophisticated malware or targeted attacks.

iSecCOM's COTS IT architecture is protected by an intelligent mix of DMZ, firewalls and IT system hardening according to the CONOPS and customer specific requirements.

The Frequentis voice communication system is, from its conception, intended to serve all operations of air forces - military air traffic control applications as well as air defence operations, in static, deployed or mobile scenarios. In a C2 scenario, the solution's architecture provides a redundant coherent IP network infrastructure: voice and data, in addition to information services such as collaboration, decision support and common operational picture services -- all on the same mission-critical network.

iSecCOM and mission-critical networks

Voice Communication is not only about ground/air communication but also about base to base ground/ground communication, usually transitioning through multiple Commercial IP Service Providers through Terrestrial MPLS and satellite networks. Frequentis transforms these multiple disparate networks and links into one resilient mission-critical network.

Additional security layers increase the demand for bandwidth by up to 400%, as well as increasing network complexity. Adaptive bandwidth allocation in a multi-security domain operation is essential for efficient network use. Secure voice communication needs a resilient network as a backbone to ensure both safety and security. Such a network is called mission-critical.

A mission-critical network reacts to changing network performance and ensures communications to reach their destination with the appropriate priority and information assurance. It is of utmost importance to ensure the availability of operational systems even in the event of failure, security breaches, or an attack. Resilience is the new redundancy.

Frequentis mission-critical networks offers network scalability, situational awareness and intelligent routing and control in real time. To ensure resilience in any situation, networks must be aware that demands of applications and the capacity provided by a network will vary over time.

Network resilience can be assured with two approaches: overprovisioning and prioritization. In most cases the overprovision of capacity is technically and logistically impossible within a strict defence environment. However, by being aware of real time performance needs from applications, and the available network capabilities, prioritisation is possible.

Mission-ready

Frequentis air defence voice communication systems are operational around the world today and are fully integrated and completely modular.

Frequentis iSecCOM provides a platform that integrates legacy analogue and VoIP communications in both a classified and unclassified environment. This means that defence organisations are given the flexibility to utilise existing networks or COTS hardware to avoid being locked into proprietary stacks. This also reduces acquisition and ongoing management costs, protecting investment in legacy technologies and extending life span.

iSecCOM integrates into existing IT environments thanks to its open design for network, device and application integration. It has been developed according to interoperability standards to ensure maximum compatibility with other systems.

The minimal footprint, decentralised COTS-based scalable system architecture allows iSecCOM to fit into each context, whether it be deployable/mobile systems, or large centres with many users.

Frequentis secure communication solutions are designed for command and control operations in a tactical and mission-critical environment, supporting and integrating a broad variety of tactical communication methods for ground/air and ground/ground communications, fully supporting RCAF C2 operators to achieve their mission. ■

Sponsored Content