BY FREQUENTIS' STEFAN GALLER AND MARTIJN SACK

Network resilience IN ARCTIC CONDITIONS

Canada is the second largest country in the world and one of the most diverse in terms of landscape and climate, with the Arctic to the north and the United States to the south. Distance and weather pose a huge challenge when it comes to keeping the country secure. For the Canadian Armed Forces (CAF) this means protecting domestic and continental operations including the Canadian Arctic, by keeping watch over Canada's air, sea, land, space and cyber domains. Whether it be protection from potential terrorist threats, combat operations, humanitarian aid, peacekeeping or disaster relief, resilience is fundamental to ensuring safety.

Facing the challenges

The CAF require secure and reliable communication, situational awareness and a failsafe network infrastructure to complete its missions, but it must also plan for any eventuality and be adaptable to change.

Canada's Defence Policy, Strong, Secure, Engaged, presents its vision and approach to defending the country and keeping its military personnel safe. It also clearly highlights the Arctic as a priority region and lays the foundation for its protection.

There are factors, however, that pose new challenges for the CAF. As far back as 2000 there was concern about the impact of global warming on the future security of the country. Rising temperatures saw 2017 noted as the second warmest year on record and melting ice in the Arctic has led the CAF to expand northerly operations to adequately monitor potential threats. There are now new entrants testing their geopolitical reach and the need for Canada to protect its sovereignty in an evolving global climate is growing.

An increase in tourism in the Arctic Archipelago, in addition to a growth in mineral exploration and exploitation, is adding to the number of ships passing through the region's waters, putting a strain on naval operations and search and rescue.

In the air, polar flights such as New York to New Delhi have also been rising thanks to extended flight routes provided by NAV CANADA and Russian airspace opening for commercial traffic. With these flights connecting directly over the North Pole, the responsibility and risk for Canada's air traffic management has increased. Online, the increasing threat of cyber terrorism and electronic warfare poses another risk to the internal security of the country. Here preventative measures are crucial to maintaining its safety.

Ongoing integration with partners like NATO, NORAD, Five Eyes and the federated mission networking initiative (FMN) adds additional dimensions to meeting Canada's defence obligations.

To respond to these challenges the CAF need to be able to exchange large amounts of data reliably and in real-time. The CAF is committed to enhancing its capabilities and capacity with long-term investments, but how can it protect against the unexpected?

Ensuring operational readiness in every eventuality

To adequately monitor air, land and sea operations, shared situational awareness is key. By providing a common operational picture across all domains, real-time intelligence, information sharing and tactical decision-making is possible, and in turn supports the sharing of resources.

Frequentis addresses this challenge with its shared situational awareness framework, a group of solutions that can be tailored to meet customer needs in a scalable and evolving system. When integrated with Frequentis' state-of-the-art communication systems, is already in use by NAV CANADA, the Canadian Coast Guard and CAF, it provides a unique cross-domain command and control tool. This tool is currently operational in Germany, fusing numerous data sources from widely disparate military and civilian systems into a single, easy to use HMI coupled with a fully integrated red/black communication system. This gives a level of access to red/black landline and radio communications, together with 'click-to-dial' functionality, not achieved with conventional systems. In addition to customization, the solution is layered on top of existing IT systems. This provides operators with real-time access to a wide range of data sources, providing intuitive interfaces and instantly accessible functions.

However, the integration of land, air and naval forces, while enabling joint capabilities in a national and international context, adds an additional layer of complexity to the case for network resilience.

Previously, networking was usually handled as a sub-element of each application, resulting in a patchwork of different networks, each managed and procured separately. Operating in this way makes allocating the correct level of security and priority to each type of communication increasingly challenging, especially when different networks offer varying levels of performance.

Members of 42 Radar Squadron install the TPS-70 Radar. Resolute Bay, Nunavut, May 22, 2015. Photo: Cpl Patrick Drouin, 4 Wing Imaging

Building on more than 70 years of experience in safety-critical communication, Frequentis is using its experience with cross-industry requirements to propose a more effective approach, based on its vitalsphere™ network portfolio for mission-critical networks. A mission-critical network reacts to changing network performance ensuring communications reach their end destination with the appropriate priority and protection.

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 and something that Frequentis vitalsphere™ provides.

Mission-critical networks

Three additional layers turn a conventional enterprise network into a mission-critical network:

1. Network scalability
2. Situational awareness
3. Intelligent routing and control.

Most mission critical applications rely on information sharing across multiple stakeholders, enabled by underlying networks. To ensure resilience in any situation, networks must combine multiple technologies from different vendors. In the defence domain, the mobility and flexibility to deploy ad-hoc networks is vital.

Both the demands of applications and the capacity provided by a network will vary over time. Consistent and reliable network performance without service interruption is essential for mission-critical defence environments. In mission-critical networks it is right to assume that communication demands will spike during a critical situation, while the infrastructure itself may be affected and unable to deliver its full capacity. Consequently, if the network demands of applications are not met, outages will occur.

Members of 8 Air Communications & Control Squadron. Exercise AMALGAM DART 15-2 in Resolute Bay, Nunavut on May 22, 2015. Photo: Cpl Patrick Drouin, 4 Wing Imaging

There are two approaches to planning network capacity for resilience: 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, prioritization is possible.

Networks based on the Frequentis vitalsphere™ portfolio use real-time network performance information and application specific performance targets to automatically and seamlessly switch between networks when performance is reduced. By removing the need for user intervention, the operator can continue executing mission-critical tasks.

Conventional networks only react to total link loss, known as black-outs, while vitalsphere™-based networks can detect degradation in performance known as brown-outs. It also allows dynamic re-routing based on application priorities and bandwidth availability, enabling automatic rerouting, which eliminates loss of service or reduced image quality.

If all traffic cannot pass through a single carrier because of a lack of capacity, the network must be aware of the operational and application demands of each user and the business processes supporting it. If there is a higher demand than the capacity on one network segment, the network should know which services to decline and which to accept. Resilience is more than just redundancy of components: it must allow end-devices to intelligently select the right course of action. To tackle such challenges, the concept of operations must be supported within the network.

Additional network security layers

Cyber security is not new and is finding its way from core segments of networks through network edges towards all end-points. In international contexts and joint contexts, multi-security domain operations are becoming the standard. This not only impacts the concept of operations, but also the network. Additional security layers increase the demand for bandwidth by up to 400%, as well as increasing the network complexity. Adaptive bandwidth allocation in a multi-domain operation is essential for efficient network use.

Disruptive factors like electronic warfare (EW), atmospheric influences, Distributed Denial of Service (DDOS) attacks, the loss of a carrier due to hardware failure, as well as regular traffic growth, increase the need for intelligent network controls which support application-aware traffic prioritization and network admission.

Ultimate understanding

Frequentis' experience with safety-critical applications has allowed it to design not only a solution for seamless situational awareness across multiple domains, but a resilient network to meet modern demands.

Resilience is about keeping operations up-and-running while managing an incident. In time-critical situations, where life is at risk, flexibility and intelligent routing based on application priorities and a real-time overview of the network is vital. To achieve this, the network and the network integrator must understand the applications and their use cases.

In the event of an incident, vitalsphere™ provides a level of safety and end-to-end performance not available on conventional networks. By perceiving possible problems with bandwidth, based on network conditions and the application requirements, vitalsphere™ selectively re-routes high-demand application traffic ensuring continuous voice and data transfer without loss of service.

To support complex and evolving defence needs, and the transfer of large amounts of data in real-time, a shared situational awareness framework and a network solution like vitalsphere™ should be considered.

Stefan Galler, Frequentis
Director ATM Networks

Martijn Sack, Frequentis
Solutions Architect, Defence