HUGHES®
An EchoStar Company

SOLUTIONSHEET

The Next-Generation Resilient, Unified Military Space Network

Satellite Communications with Enterprise Management and Control and Flexible Modem Interface

Executive Summary

Today's global enterprises are powered by networks that are becoming more resilient, efficient, and cost-effective. Software-Defined Wide-Area Networks (SD-WAN) have effectively transformed the network landscape by leveraging multiple network paths and transport technologies to and from distributed locations. In the commercial space, SD-WAN is largely composed of terrestrial services like cable, fiber, and 5G—all connected into an intelligent router that assigns local traffic to a network path based on determining factors such as packet type, path availability, and application priority. Today, the military enterprise sees a similar need in the space domain. The United States Department of Defense (DoD) is seeking more resilient satellite communication (SATCOM) and terrestrial networks to fulfill missions in an increasingly contested battlefield domain.

This is a significant change because, over the last 30 years, the DoD held an asymmetric advantage over its adversaries in space, which has long been considered a sanctuary domain. Now the DoD must transform its strategy and capabilities as "near-peer" international militaries continue to invest in new, disruptive Electronic Warfare (EW) technologies. Soldiers and decision makers must have uninterrupted and always-available SATCOM, even in contested environments. Achieving this requires increased redundancy and diversity in SATCOM network pathways. Advanced commercial network technology can bring this strength to DoD SATCOM networks.

Hughes Defense has worked with the DoD to strengthen SATCOM operations and build readiness for this adversarial future. Hughes has introduced modem and service management technology that brings much-needed autonomy and flexibility for enhanced, protected communications even when using legacy modems and waveforms. Packaged as Flexible Modem and Terminal Interface (FMI and FTI), this technology was first demonstrated to the DoD in 2018. To offset advancing global threats that can disrupt satellite communications, the Hughes concept described here leverages advanced Artificial Intelligence (AI) and software-defined networking techniques. Using these techniques, terminals can autonomously select a modem and service based on policy rules assigned to various factors, such as mission priority, satellite availability, cost considerations, and active threats.

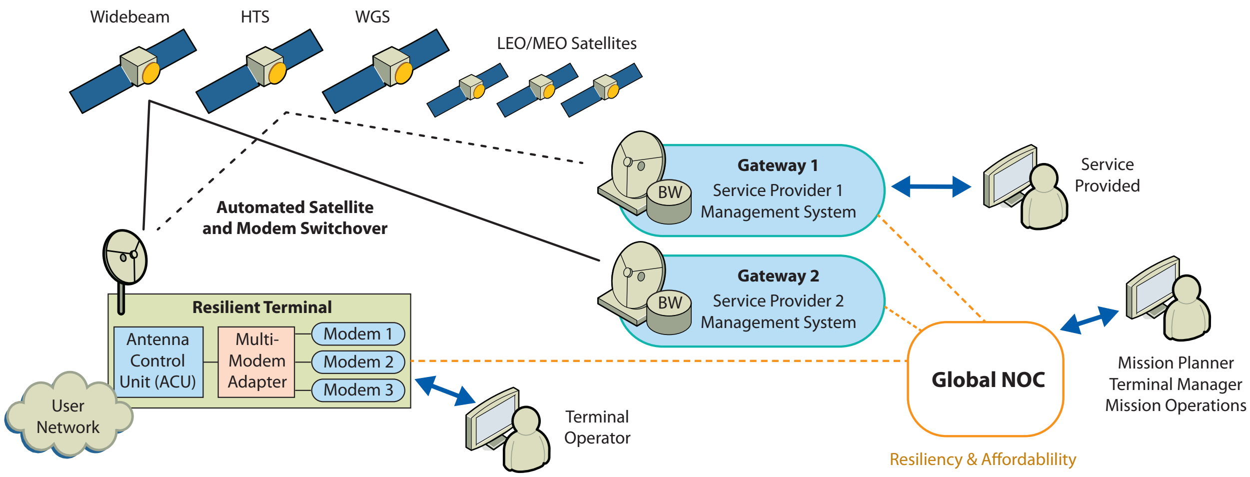
Standards for Network Interoperability

The current satellite communications landscape for defense operations includes various closed networks and hybrid commercial/military networks, which made up of modular technologies, including waveforms, interfaces, modems, antennas, and more. The DoD can gain significant efficiency, cost, and performance benefits across these networks by leveraging common industry standards used with an Enterprise Management and Control (EMC) concept that encompasses FTI, Service Provider Interface, and global EMC capabilities. This would allow interoperability and orchestration between the various networks. It would also allow the DoD to benefit from commercial enhancements delivered by managed services that provide all the EMC elements as an end-to-end service.

Many interfaces within the proposed EMC concept currently function based on existing standards. If the EMC model is adopted, new interfaces can be added and standardized to increase compatibility and competition within the growing industry base. EMC standards adopted by technology and service providers would support future missions using a common interface across the enterprise, moving from the satellite terminal to the Gateway Hub to the EMC capability and from a Service Provider Management System (SPMS) back to the EMC. This EMC framework can automate the global Situational Awareness/Common Operational Picture (SA/COP) and Mission Planning, along with support capabilities such as orchestration, brokering, and cybersecurity.

The EMC Architecture

The enterprise management concept can direct a flexible terminal to roam rapidly and autonomously among heterogeneous modems and services supplied by various providers regardless of whether the satellite link comes from geostationary or non-geostationary orbits. In addition to supporting satellites in various orbits, this Modular Open Systems Architecture (MOSA) can incorporate links provided by airborne platforms and even terrestrial infrastructure when available. With multiple providers involved, military end users will benefit from continuous service and technology improvements, real-time information, and improved cost efficiencies.



Enterprise Management and Control Architecture for Interoperable Networks

Using multi-modem terminals, a variety of service options, and dynamic network management, EMC can also allow the military to procure modular system components like modems, antennas, and services that meet mission-specific requirements. With Hughes' new software-defined networking approaches, embedded AI functions can simplify operations and increase automation by provisioning services and supporting on-demand usage.

The EMC architecture can provide rules-based policies to the terminals equipped with the flexible FTI software. EMC can manage terminal, service provider gateway, and satellite registries and use them for dynamic mission planning and resource allocations. Dynamic planning can further improve traditional Primary, Alternate, Contingency, and Emergency (PACE) frameworks for faster orchestration of resources. With these plans, the flexible terminals can execute the EMC policies and use the appropriate modem, satellites, and service based on the predetermined service priority and the hardware's operational environment. The terminal would then make rapid, autonomous decisions based on factors like availability, latency, signal interference, and blockage. The terminal would ultimately connect to the best-available network without user oversight or management, saving significant amounts of time compared to current network operations. This autonomy provides the terminal with a "self-healing" capability to maintain connectivity using alternate networks and increased resiliency.

Autonomous Decision Making

Building on the core FTI capabilities, intelligent terminal control features can enhance modem interoperability by increasing terminal autonomy. For the terminal to make decisions, it uses a set of rules. A rule is an "if" followed by a condition to issue a "then" action command. The terminal's operational policies are executed based on the following processes in the terminal, which are then sorted by their priority attribute.

Step 1: The terminal state is determined based on current and relevant environmental data available from the terminal.

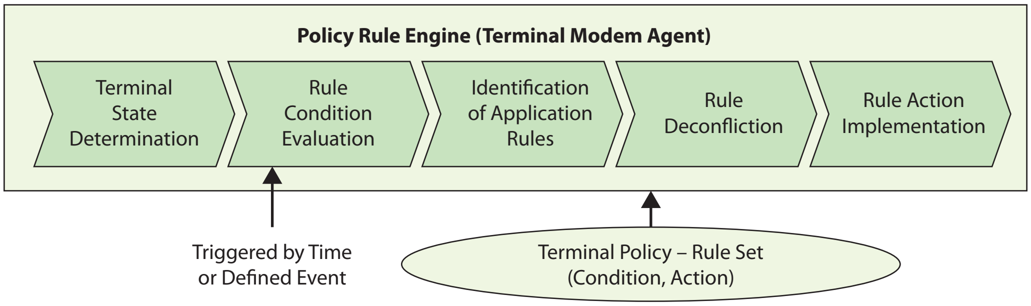
Step 2: A rule-condition evaluation repeats overall policy rule sets and identifies all applicable rules.

Step 3: A no-conflict process is implemented between the actions of two applicable rules. For example, the individual actions of two applicable rules could point to two different satellites. Such a conflict is resolved by selecting the action related to the higher priority rule.

Step 4: Once all applicable rules have been identified, their respective actions are executed, which completes one rule-set execution cycle.

Greater specificity in the processes leads to better decision making. A factor "weight" can be used with each rule's priority level. For example, the weight might have a discrete value, such as {irrelevant, desirable, highly desirable, required, must-have-required}. Each factor can be weighted when computing an overall score by mapping them to weight numbers. This helps determine the best command prompt within the terminal.

The terminal's state is determined using raw terminal performance and fault data, which is indicative of the behavior of various terminal components and the varied external conditions surrounding their operation. The raw data helps to determine a more granular state of the terminal and its environmental condition. This approach ensures that the EMC capability can easily configure the terminal-state determination software by refining the number of states and events (raw attribute values), which control transitions across these states. In addition to managing the rules for the terminals, the EMC also collects performance, security, and accounting data from the enterprise's gateways and terminals for overall situational awareness across the network.



Example Policy Rule Set Execution Cycle with a Rule-Engine in the Terminal Management Agent

Cybersecurity

With cyberthreats continuing to evolve, the EMC concept incorporates a new, highly responsive cyberthreat management feature. This capability uses a COTS Intrusion Prevision System/Intrusion Detection System (IPS/IDS) software appliance in the FTI software that can monitor traffic coming and going via the common L2/L3 packet switch. To manage and configure the behavior of the IPS/IDS system, security policies are pushed from the EMC via the FMI rules engine and data analytics. The IPS/IDS software appliance provides packet-level policing, filtering, and policy control in both directions (from and to the user network)—all orchestrated by the core EMC framework.

It is imperative that the military stays ahead of the evolving landscape and bring security measures to the network's edge. The capability outlined in the EMC architecture would fortify terminals against localized jamming by enabling automated switching between different modems and services. When implemented with specialized waveforms, the military enterprise will realize a truly resilient network that can withstand potential threats regardless of their distance from the terminal.

Next Steps

The EMC concept and the supporting framework, including FTI elements underwent initial testing and review by DoD users in December 2018 with Geosynchronous Earth Orbit (GEO) satellites, and was further enhanced for the U.S. Army over the next three years under the Narrowband controller program. More recently, Hughes included additional capabilities, including Low Earth Orbit (LEO) satellite terminals during the 2023 Rapid Tiger and 2024 Hawaii PACE and 5G demonstration for the U.S. Navy. Hughes plans to enhance this new enterprise architecture by adding multiple antennas for concurrent use across services to manage load balancing and traffic-prioritization objectives, as well as support non-geostationary orbits. A fully digital design is also in development to accommodate Intermediate Frequency (IF) switching Field Programmable Gate Array (FPGA), FMI (computer), packet switching (computer), IPS/IDS (computer), and modems with Software-Defined Radios (SDR) (FPGA and computer) to significantly reduce FTI form factor and unit cost.

As the DoD continues to move into a multi-domain, big-data environment, its data networks must efficiently leverage new technologies like those discussed here. Without flexible and intelligent software-defined networks that provide path diversity, SATCOM operations will degrade as space networks become contested. Hughes and others in the commercial satellite industry have listened to the DoD's requirements and proposed resilient solutions like this one for EMC. The DoD has adopted interoperable, wireless enterprise networks to ensure continued strength. Now satellite networks must follow the same modernization path to help maintain long-term, resilient communications for warfighters.

Visit government.hughes.com or contact us at globalsales@hughes.com.

HUGHES
An EchoStar Company
11717 Exploration Lane Germantown, MD 20876 USA
www.hughes.com

H64536 JUL 24