2020 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
CYBER/VEA TECHNICAL SESSION
AUGUST 11-13, 2020 - NOVI, MICHIGAN

MISSION ENABLING TECHNOLOGIES DEMONSTRATOR REMOTE OPERATIONS AND MANAGEMENT

[1]David Jedynak, [2]David Gregory, [2]Jeff Nelson

[1]Defense Solutions Division, Curtiss-Wright, Austin, TX
[2]Pacific Star Communications, Portland, OR

ABSTRACT

Given the system complexity of the Mission Enabling Technologies Demonstrator (MET-D) it is necessary to consider a robust communications management solution capable of consolidating network management onto a "unified interface" while providing distributed, hierarchical, and efficient management of network attached nodes on multiple platforms regardless of the vendor or implemented technology.

Citation: D. Jedynak, C. Kawasaki, D. Gregory, "Managing Next Generation Open Standard Vehicle Electronics Architectures", In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, Aug. 13-15, 2019.

1. INTRODUCTION

The Army's Next Generation Combat Vehicle (NGCV) Cross Functional Team's Mission Enabling Technology Demonstrator (MET-D) is a cutting edge experimental system of vehicles developed as a tool to help Army leaders determine how best to integrate unmanned robotic vehicles, advanced networking technologies, and future sensor capability into ground combat formations. MET-D provides a forward looking window 10-20 years into the future of what military operations may look like, with a primary objective of reducing risk to Soldiers.

The MET-D platforms leverage the latest sensor technology, data display and consolidation capabilities, modular open standards, innovative graphical user interfaces, drive-by-wire capability, unmanned aerial vehicle surveillance video, and advanced communications systems to support Soldiers. Robotic Combat Vehicles (RCV), operated from the MET-D Manned Fighting Vehicle (MFV), are unmanned robotic platforms which can be used to make contact with the enemy before the Soldiers, and simultaneously provides overmatch against additional operating environment threats.

MET-D marks the early stages of a multi-year process where the Army is establishing an experimental architecture to determine the best way to integrate new robotic, networking, sensor, and autonomous vehicles technologies into the way it fights.

Network situational awareness, maintainability, and cybersecurity resiliency are essential for ad-hoc distributed network architectures, on-vehicle LANs, and off-vehicle WAN connections to support MET-D. The "difficulty-to-manage" of the MET-D experimental architecture is anticipated to continually increase as the system capability and complexity evolves, and the resulting complexity trend promises significant modernization challenges.

A partial solution to sustain MET-D's modernization efforts is to consolidate and

simplifying MET-D's network visualization, device integration, and configuration management while supporting remote operational monitoring and management for both the MFVs (on-platform) and remote node RCVs (off-platform) integrated networks.

Remote Operations and Management (ROAM) solutions for MET-D's relevant tactical networks will need to address network visualization, remote node status and management, support cybersecurity administration, configuration management challenges, and aggregated node reporting - all aimed at providing robust operational support and situational awareness while driving down complexity, downtime, and configuration errors.

Furthermore, significant effort is being applied in developing comprehensive "standards based communication" to address interoperability issues, data bus functionality, and standardized messaging services for interconnected system components. ROAM will need to support the modernization standards - such as C4ISR/EW Modular Open Suite of Standards (CMOSS) – to include:

- *Vehicular Integration for C4ISR/EW Interoperability (VICTORY):* provides network based interoperability using to share services such as Time and Position.
- *OpenVPX:* a hardware form factor for fielding capabilities as cards in a common chassis
- *Modular Open RF Architecture (MORA):* drives functional decomposition to share resources such as antennas and amplifiers
- *Software frameworks:* includes REDHAWK, Software Communications Architecture (SCA), and Future Airborne Capability Environment (FACE) to enable software portability

Distributed software management technology – running locally on each node – is necessary to efficiently achieve ROAM functionality and consolidate the management plane of network infrastructure under a "unified interface" providing network situational awareness to crewmembers and administrators regardless of the type of technology or vendor used on the network. Further, a robust ROAM solution deployed on each node would support collaborative management between local on-platform, lightly-trained or untrained crewmembers, on-platform administrators, and remote administrators – to include disconnected, intermittent or limited WAN conditions - while simultaneously providing full control at remote, higher-echelons or Network Operation Centers (NOC) that can be staffed with fewer technical experts providing assistance to remote nodes.

Given the existing and anticipated complexity of MET-D networks it is necessary to consider a robust communications management software solution for remote operations and management - that consolidates the management plane of networks onto a unified interface regardless of the type of technology or vendor – capable of providing distributed, hierarchical, and efficient management of network attached nodes.

2. Challenges and Opportunities

Continuous functional enhancements and integration of unmanned robotic vehicles, advanced networking technologies, and future sensor capability into MET-D's experimental architecture may pose a complex configuration management challenge. Also, it may be possible to shorten the innovation life-cycle by increasing the consistency of MET-D's experimental architecture to fully achieve network situational awareness, effective maintainability and configuration management, and support cybersecurity related concerns.

Network Situational Awareness – Providing an intuitive, meaningful, and unified interface across the entire MET-D experimental network – while sharing essential network information to users at any echelon – possess a significant challenge.

ROAM will need to operate on both central and distributed nodes for – redundancy and continuous monitoring – with extensive real-time status, alerts, and auditing to provide enhanced network situational awareness between core and the edges of the MET-D network.

ROAM would provide:

- *Unified Interface:* An intuitive interface to underlying technologies for both administrators and users – with important data at-a-glance – improving network situational awareness at every level and reducing configuration time

Maintainability – Sensors, AI/ML technology, RCVs, and communication system features continue to increase in complexity and often increase time needed to configure/reconfigure components, troubleshoot connectivity issues, or correct network defects. At any given time, MET-D's experimental architecture may consist of advanced – often unique – hardware or software capability and will require administrative expertise beyond local crewmember knowledge.

Further, as components are added/removed from MET-D's experimental architecture it will be necessary to save or apply known configuration baselines, compare configurations side by side, and remotely share and apply configurations to make quick adjustments. Continually making manual changes introduces potential for human error and downtime.

Remotely monitoring and managing MET-D's network configuration – with automation ability to rapidly revert or reset configuration changes – is possible with a ROAM solution. Additionally, enabling collaborative troubleshooting and management between remote administrators (at the NOC) and lightly-trained crewmembers (in the MFV) will make communications set-up and operation quick, easier to learn, and repeatable even in disconnected, intermittent, or limited WAN conditions.

ROAM would provide:

- *Reduces Configuration Errors:* Significantly reduces configuration errors, assisting in maintaining uptime
- *Facilitates Remote Management:* Facilitates remote management with the ability to monitor, remotely troubleshoot, and rapidly change device configurations
- *Simplifies Troubleshooting:* Simplifies troubleshooting for integrated technologies for crewmembers and advanced network administrators

Cybersecurity - Given existing and emerging Electronic Warfare and Cyber threats, it is assumed the overall network security posture of MET-D experimental architecture will increase in sophistication and complexity. Additionally, vendor software diversity, mixed training requirements, technical retention, and integration lifecycle for necessary components (i.e. cryptographic key provisioning and management, continuous system monitoring solutions; intrusion detection, prevention and adaptation; etc.) will continue to increase as vendors rapidly respond to the interoperability standards used in MET-D's experimental architecture.

ROAM would:

- *Automated Response:* Automated detection and response capabilities for protecting tactical communications and complying with cybersecurity requirements
- *Save Time:* Automates complex, time-consuming, and error-prone tasks with powerful wizards with standard user interfaces across components
- *Monitor Cyber Services:* Monitors hosted cyber network services, supports analytics, provides alerts, response management

3. TECHNICAL APPROACH

It has been conceptually shown, in collaboration efforts between Curtiss-Wright Corporation (CW) and Pacific Star Communications (PacStar), that PacStar's IQ-Core Network Communication Management (NCM) software with Remote Operations and Management (ROAM) capability – designed to reduce administration complexity and provides a unified interface under an intuitive dashboard – could possibly manage with MET-D's MFV and RCV network infrastructure components through the VICTORY framework

Figure 1 - Multi-Tier Remote Operations and Management (ROAM) example for MET-D

and connect with various technologies using SNMP, SSH, REST application programming interfaces (APIs), etc. (Figure 1).

IQ-Core ROAM is a light-weight application and can operate on CW Mission Computers or VPX Single Board Computers (SBC) running within each MET-D node to interact and manage other on-platform and off-platform network components. The IQ-Core ROAM component adds robust capabilities to enable centralized management of distributed network nodes at multiple tiers in a hierarchical and efficient manner.

3.1. Network Situational Awareness

IQ-Core ROAM is designed to manage networks in disconnected, intermittent and limited (DIL) environments – making optimal use of network bandwidth and working reliably where loss of connectivity is a regular occurrence. Additionally, it also works well for enterprise networks with multiple, distributed, remote locations by converging management of all essential systems.

Originally developed to meet the stringent demands of tactical and enterprise deployments for the US DoD, the National Guard, and state and local emergency responders, IQ-Core is adoptable to the VICTORY framework on ground vehicles and offers the following field-proven, key benefits:

- *Intuitive User Interface* (Figure 2) - upper network tiers (echelons) and NOCs that mirrors remote systems, offering simplifying navigation and consistent management throughout the network.

Figure 2 – Intuitive User Interface (Summary Dashboard)

- *Auto-Generated Network Diagrams* (Figure 3) – dashboard showing the logical structure of hierarchical nodes (including ability to drill-down and see important data at-a-glance.)

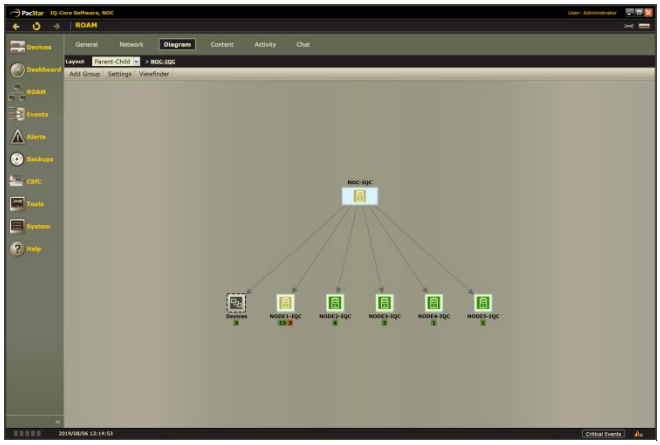

Figure 3 - Auto-generated logic diagrams

- *Reduced Configuration Errors* – automates deployment of network planning and configuration files across the network, ensuring consistent configuration of all network devices.
- *Optimized for Situational Awareness* - designed for tactical and distributed networks to provide enhanced network situational awareness, with extensive real-time visibility of connected nodes. Operates seamlessly in disconnected, intermittent, and limited environments.
- *Automated Cyber Defenses* – improves cyber visibility by securing, consolidating and forwarding alerting information at each tier of the network.
- *Streamlined Integration* - interoperates with IQ-Core Software-managed nodes at any tier in the network, streamlining innovation and adoption of new COTS technologies at the network edge.
- *Field Proven* – based on the widely deployed IQ-Core Software communications management platform.
- *Unified View* – provides network monitoring and diagnostics in a unified interface with real-time snapshot of the health of the network, and ability to provide backup and restorations of entire network.
- *Adapts to User Level* – intuitively designed for non-specialists, it offers the flexibility and capabilities to meet the needs of advanced power users.
- *Enhanced Ability to Meet Mission Objectives* – Reduces setup time – allowing communication systems to adapt to rapidly changing circumstances. Improves up-time – allowing personnel to focus on fighting the fight, not fighting the network.
- *Vendor-Agnostic Interoperability* – Unlike many enterprise software solutions that only integrate with specific product families and lock customers into one path, IQ-Core NCM integrates with a broad range of tactical and enterprise communications hardware and systems, enabling organizations to easily upgrade, replace, or reconfigure deployable systems.

These ROAM benefits would empower crewmembers, auditors, power users, and advanced administrators to effectively and efficiently maintain the MET-D architecture.

3.2. Maintainability and Configuration Management

To address the maintainability complexity and training burdens imposed by extensive security requirements and evolving technologies IQ-Core includes robust configuration management tools to simplify component provisioning, integration, and maintaining consistency throughout the MET-D experimental architecture. IQ-Core ROAM can further extend configuration management by comparing configuration differences and imposing necessary changes onto remote MFV and RCV nodes from upper tiers while preserving the change records. These tools can simplify the

setup, configuration, and management of the underlying equipment used in VICTORY environment. Such tools can provide a base level of capabilities, including:

- Enabling the provisioning and integration of system components, with attendant benefits, while reducing the amount of added complexity and training
- A unified interface ("single pane of glass") to underlying equipment from multiple sites and/or multiple vendors (Figure 2)
- A means to monitor multiple sets of equipment (Figure 4), from fixed or mobile locations and tactical settings, and enabling lightly trained crewmembers to manage equipment in the field if necessary

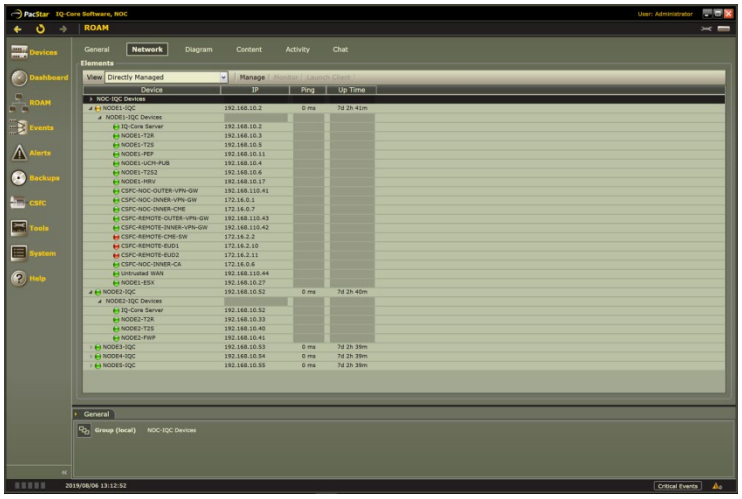

Figure 4 - Monitoring multiple device sets

- Setup Wizards - SNMP, VPN setup and certificate generation wizards reduce the complexity of providing the correct information to devices by providing interactive step-by-step wizards, insulating lightly-trained users from dealing with the command line interfaces and multiple UIs
- VPN monitoring capabilities include the ability to display, in real time, the connection and configuration status of one or more VPN devices. Status indicators should include status of the active authentication and bulk encryption settings in use
- Built in secure file transfer to send authorized configuration files to one or more nodes
- Auto-triggered configuration backup on any device a change/commit is made
- Optionally activate (apply) a configuration, OS update, or other content.
- View, compare, edit, and commit configurations of remote nodes, from upper tiers
- Update IQ-Core Software remotely on any node

3.3. Cybersecurity

IQ-Core ROAM management includes Cyber Defenses functionality used to improve network visibility, threat detection, and automated responses and would enable MET-D to tailor cyber capabilities across the experimental architecture. Complex and error-prone process can be automated - reducing the occasion for costly mistakes and ensuring communications uptime - and allows security administrators to focus on more important tasks. Further, crewmembers could have local access to the IQ-Core ROAM cyber tools at every node in DIL connected environments. Cybersecurity related capabilities of IQ-Core ROAM include:

- Automates deployment of network planning and device configuration files across the network, ensuring consistent configuration all network devices.
- Simplifies security procedures
- Improves cyber visibility by securing, consolidating and forwarding alerting information at each tier of the network.
- Field proven - easy to deploy, program, and maintain network communication management tools

- Provides the same network management capabilities at every node in the experimental architecture
- Provides an intuitive, uniform, easy to use interface at every tier
- Simplifies certificate management process at either the deployed systems and NOC
- Providing certificate revocation checking via built-in OCSP and CDP functions.

3.4. Additional Benefits

Multiple second order effects would result from managing MET-D's experimental architecture and VICTORY components with IQ-Core ROAM solution:

- *Supports aggregated reports* across nodes aiding in network situational awareness
- *Real-time views* – node and device status including interfaces and alerts with at-a-glance diagram views allowing drill-down and launching of a complete administrative interface to a node – enabling and simplifying remote management of remote nodes
- *Drives Down Costs* – Deploy Commercial off the Shelf (COTS) solutions and reduce the number of communication specialists required to stand up and manage communications equipment while minimizing the training required to operate equipment.

Evidence found in an independent Human Factors Engineering Analysis [1] depicts dramatic savings for entry-level and advanced administrators in time savings and reduction in

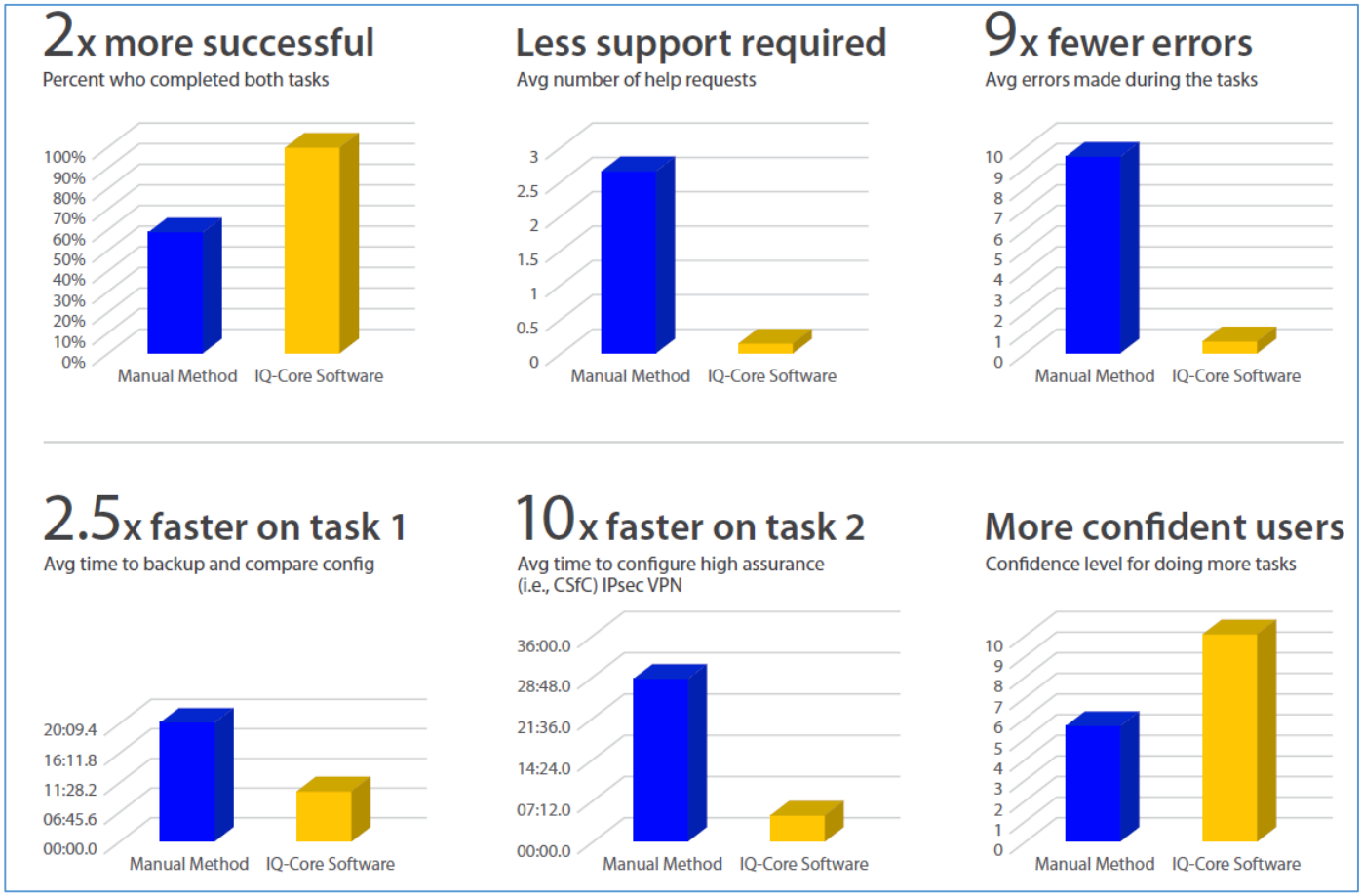

Figure 5 - Dramatic savings using integrated management tools

errors when using IQ-Core to implement high assurance configurations (i.e. CSfC) IPsec VPN and general network administration-related tasks. IQ-Core users required less training support, were able to perform tasks significantly faster - and felt twice as confident using IQ-Core management tools - versus using traditional command-line interfaces to make configuration changes. (Figure 5)

4. CONCLUSION

The Army's NGCV Cross Functional Team's MET-D program should be able to address critical needs to simplify and improve network situational awareness, system maintainability, and cybersecurity defense in the MFV/RCV experimental architecture by overlaying remote operations and management tools – such as IQ-Core ROAM – across interoperable and network-based standards.

Such combinations will deliver benefits in tactical settings, improve network management and enabling new classes of communication applications, while reducing management complexity and training burdens. Implementing ROAM solutions will consolidating the management plane of these networks onto a unified interface and is capable of providing distributed, hierarchical, and efficient management of network attached nodes on multiple platforms and at multiple tiers in the MET-D experimental architecture.

5. REFERENCES

[1] Pacific Star Communications, Inc. (PacStar®) and Thug Design, *IQ-Core® Software Comparison Study 2016: Results from comparing IQ-Core® Software with manual methods.* Portland, OR, 2016.