2019 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
CYBER/VEA TECHNICAL SESSION
AUGUST 13-15, 2019 - NOVI, MICHIGAN

MANAGING NEXT GENERATION OPEN STANDARD VEHICLE ELECTRONICS ARCHITECTURES

[1]David Jedynak, [2]Charlie Kawasaki, [2]David Gregory

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

ABSTRACT

Given the complexity of existing and anticipated ground vehicle networks it is necessary to consider a robust communications management software solution - that consolidates the management plane of networks onto a "single pane of glass" regardless of the type of technology or vendor – that is capable of providing distributed, hierarchical, and efficient management of network attached nodes on multiple platforms and at multiple tiers.

1. INTRODUCTION

US Army and Marine Corps ground vehicle and tactical networking programs have a widely-acknowledged critical need to both simplify and improve configuration control, management, and system awareness of, on-platform and off-platform systems, dismounted communication solutions, and network operation centers.

New IP-based networking architectures integrated into vehicles are able to unify the communications, and shared hosting of services, between functions that used to be discrete hardware devices – significantly reducing space, weight, power, and cost (SWaP-C) of the system of systems as a whole; however the planned and anticipated capabilities of on-platform COTS technology, for example, is ever increasing and complexity ever growing.

Additionally, the IP network architectures moving onto platforms are frequently derived from enterprise-class functions in order to benefit from the robust networking capabilities, cybersecurity maturity, development pace, and innovation, research, and development (IRAD) shared with the commercial sector. This trend promises significant technology cost savings and an increased pace of modernization, but includes a significant complication with respect to usability and manageability.

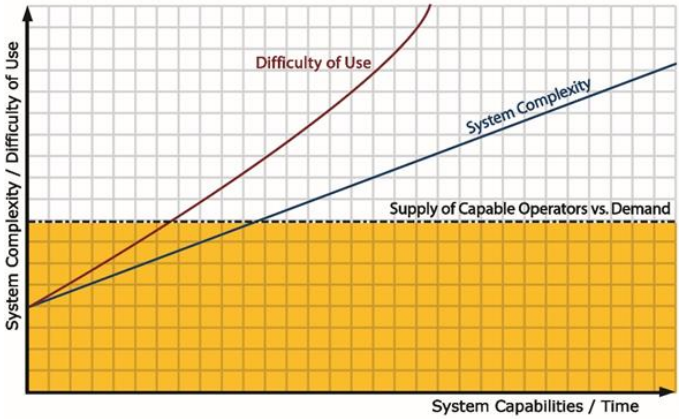

Figure 1 - General Capability/Time vs Complexity of use

The new on-platform integrated networks will be composed of heterogeneous networks (including functions such as routing, switching, timing/A-PNT, encryption, cybersecurity, voice/video/data integration, remote control, sensor integration, logging and more) – in the form of software and equipment from multiple commercial vendors – many with enormous feature sets required to meet

interoperability and cybersecurity requirements for DoD systems, and requiring a level of training and expertise for operation and maintenance that far exceeds available specialists.

Significant effort is being applied in developing comprehensive "standards based communication", like the on-platform Vehicular Integration for C4ISR/EW Interoperability (VICTORY). Standards address interoperability issues, data bus functionality, and standardized messaging services for interconnected system components. However, standards typically do not address the network operation, configuration and management challenges of hybrid (multi-media, multi-classification, multi-platform) DoD-ready networks themselves. Work currently underway in PM Tactical Networks (PEO-C3T) is aimed at driving down complexity, downtime, and configuration errors in current and next generation tactical and expeditionary C2 networks.

Given the existing and anticipated complexity of hybrid networks it is necessary to consider a robust communications management software solution - that consolidates the management plane of networks onto a "single pane of glass" regardless of the type of technology or vendor – that is capable of providing distributed, hierarchical, and efficient management of network attached nodes on multiple platforms and at multiple tiers.

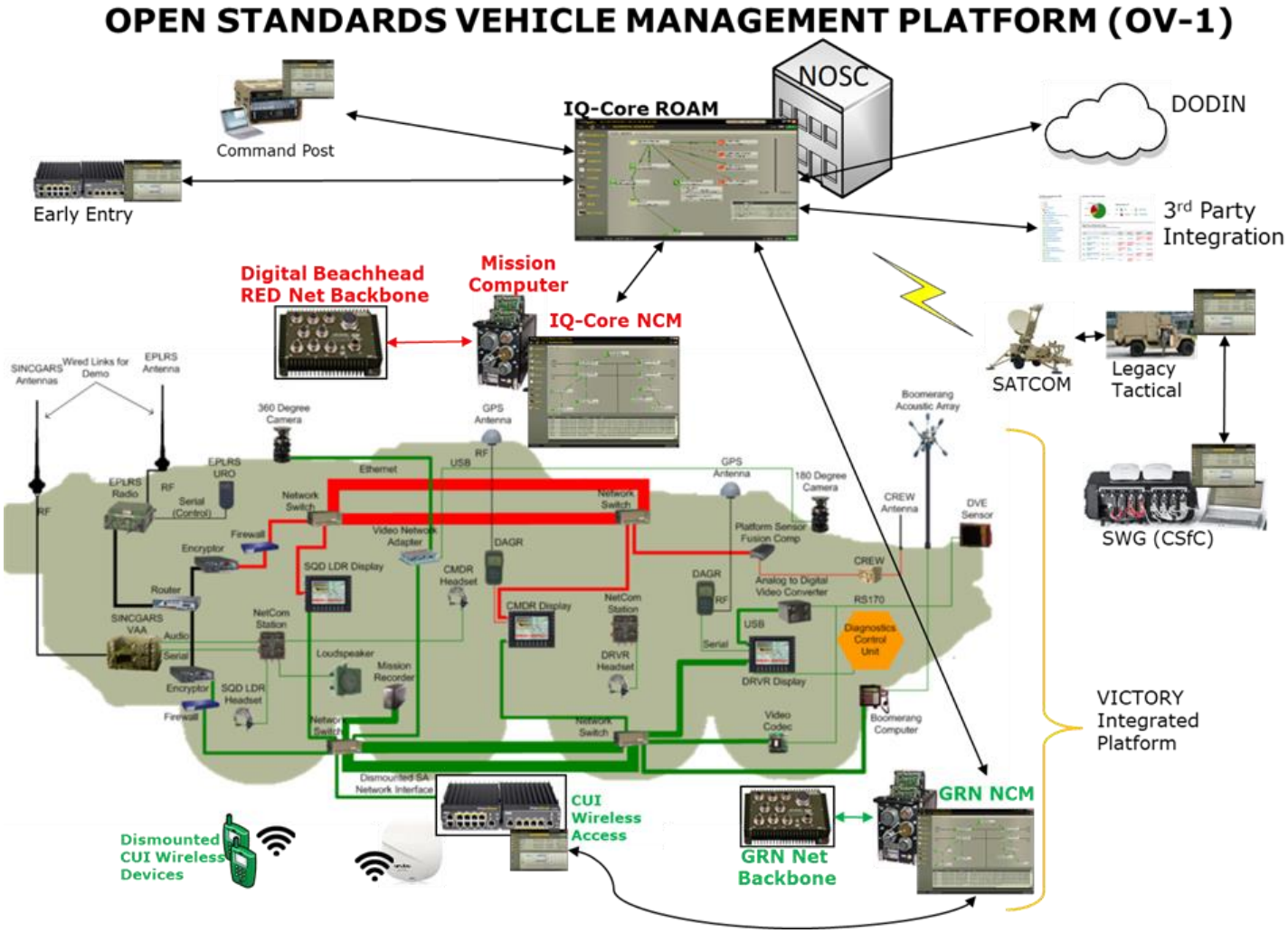

Figure 2 - Open Standard - Vehicle Management Platform (OV-1)

2. Challenges and Opportunities

"Bolt on" system integration has reached critical levels relative to essential capability versus available space and power in ground vehicles. Standardizing physical interconnections, shared processing, and communication messaging protocols intuitively should reduce SWaP-C and/or provide additional capacity. Similarly, a movement to an open framework standard is a good idea, and frankly necessary, to shorten the innovation life-cycle and increase the overall efficiencies of ground vehicle systems.

However, it will not be enough to only govern connectivity standards of interoperable network-based architecture for integrating electronic systems to fully achieve the US Army's and USMC's objectives to reduce complexity, downtime, and configuration errors.

Given existing and emerging EW and Cyber threats the overall system functionality of ground vehicle networks will continue to be unavoidably diverse, sophisticated, and complex. Additionally, vendor software diversity, assorted training requirements, technical retention, and integration lifecycle costs for a myriad of 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 adapt and adhere to a robust set of interoperability standards.

Training and proficiency will continue to be a significant barrier as systems evolve. IT systems continue to increase in complexity and drive up training requirements. It is often necessary to train soldiers to maintain - often outdated - applications, infrastructure, and security architecture, while simultaneously only focusing on security fundamentals - given time and budget constraints - leaving little to no time for advanced training.

Further, introducing multiple classifications and cross-domain functionality increases the necessity for robust, intuitive, and consolidated monitoring and management of the underlying infrastructure. In many cases there can be significant differences between classified and unclassified systems, further fueling the need to increase training for personnel going to the tactical edge.

However, it is possible to overcome and offset these inherent challenges by employing an intuitive solution capable of running across platforms that enables collaborative management between lightly-trained operators and provide on-platform network situational awareness in disconnected, intermittent or limited WAN conditions; while simultaneously providing full control from higher-echelons that can be staffed with a limited number of experts providing technical assistance across large numbers of remote platforms.

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 can interface with infrastructure components through the VICTORY framework.

Similar to the OV-1 depicted in figure 2, IQ-Core NCM can operate on CW Mission Computers installed on-platform within each unclassified and classified network to interact and manage with other on-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.

Figure 3 - Parvus DuraCOR Mission Computer

IQ-Core ROAM is designed to manage networks in disconnected, intermittent and limited 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.

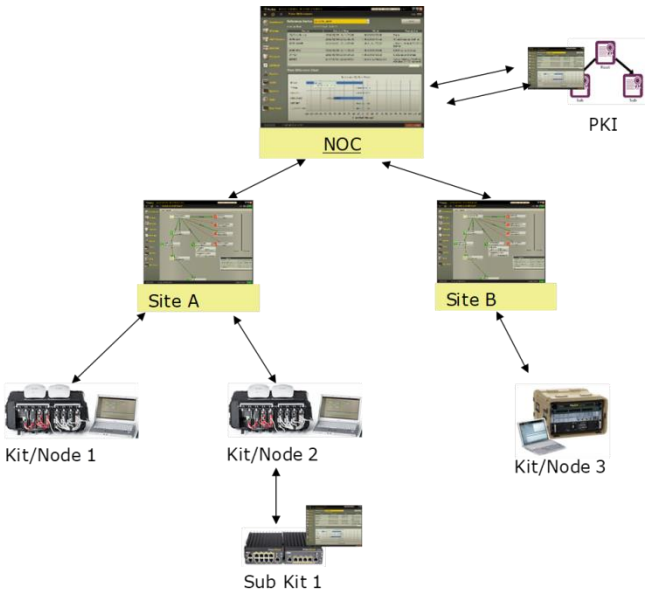

Figure 4 - Tiered ROAM example

Originally designed 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 - upper network tiers (echelons) and NOCs that mirrors remote systems, offering simplifying navigation and consistent management throughout the network.

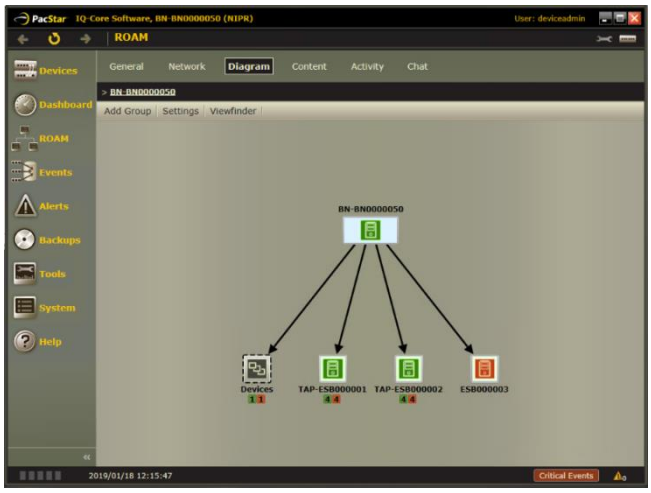

Figure 5 - Auto-generated logic diagrams

- Auto-Generated Network Diagrams (Figure 5) – dashboard showing the logical structure of hierarchical nodes (including ability to drill-down and see important data at-a-glance.)
- 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 provides 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 benefits empower lightly-trained operators, auditors, power users, and advanced administrators to effectively and efficiently maintain mission critical systems of systems.

3.1. Configuration Management and Monitoring

To address the added complexity and training burdens imposed by extensive security requirements and evolving technologies IQ-Core includes configuration management tools to simplify component provisioning, integration, and maintaining consistency throughout the network. IQ-Core ROAM can further extend configuration management by comparing configuration differences and imposing necessary changes onto remote 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 (“a single pane of glass”) to underlying equipment from multiple sites and/or multiple vendors (Figure 6)

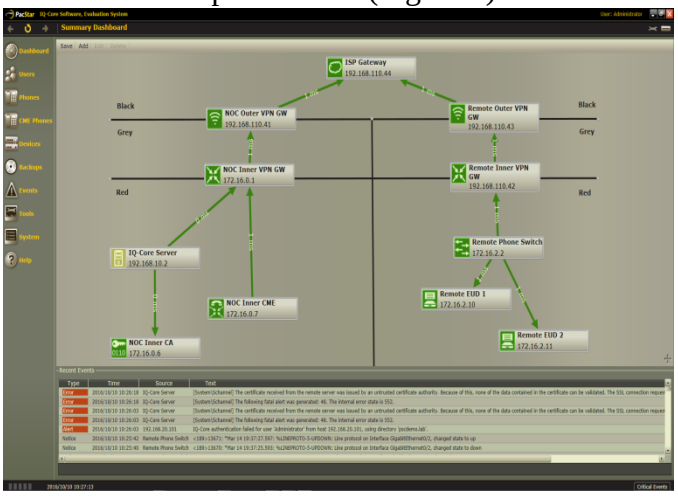

Figure 6 - Unified Dashboard

- A means to monitor multiple sets of equipment, from fixed or mobile locations and tactical settings, enabling lightly trained operators to manage the equipment
- 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

3.2. Certificate Management

Management capabilities include automating the process of managing device certificates, a process that is error-prone, and historically requires extensive training. Reducing the occasion for errors in this complex process helps ensure communications uptime and allows security administrators to focus on more important tasks. Capabilities related to certificates should include:

- Generation of certificate signing requests
- Display of certificate details and expiration dates, including expiration alerts
- Encrypted transmission of certificate signing requests
- Management of the signing process at either the deployed systems or at the NOSC
- Management/monitoring of certificate authorities
- Providing certificate revocation checking via built-in OCSP and CDP functions.

IQ-Core provides a robust certificate manager and certificate generation wizard – which can be used to implement the necessary CSfC compliant VPN certificates – that performs the above mentioned tasks. Additionally, it can interface with well know Certificate Authorities (such as Microsoft CA and ISC CertAgent) to take advantage of certificate templates. Leveraging this IQ-Core's certificate management tool mitigates the chance for human error, dramatically simplifies the certificate issuance process, and greatly improves certificate consistency across the network.

3.3. Additional Benefits

Multiple second order effects result from managing VICTORY components with IQ-Core's NMC and ROAM solutions:

- 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.

An independent Human Factors Engineering analysis found dramatic savings for entry-level and advanced administrators in time savings and reduction in errors when using IQ-Core for CSfC 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 7)

management tools – such as IQ-Core NMC and ROAM – on interoperable network-based standards such as VICTORY.

Such combinations deliver the benefits in tactical settings, reducing command post setup time and enabling new classes of communication applications, while limiting management

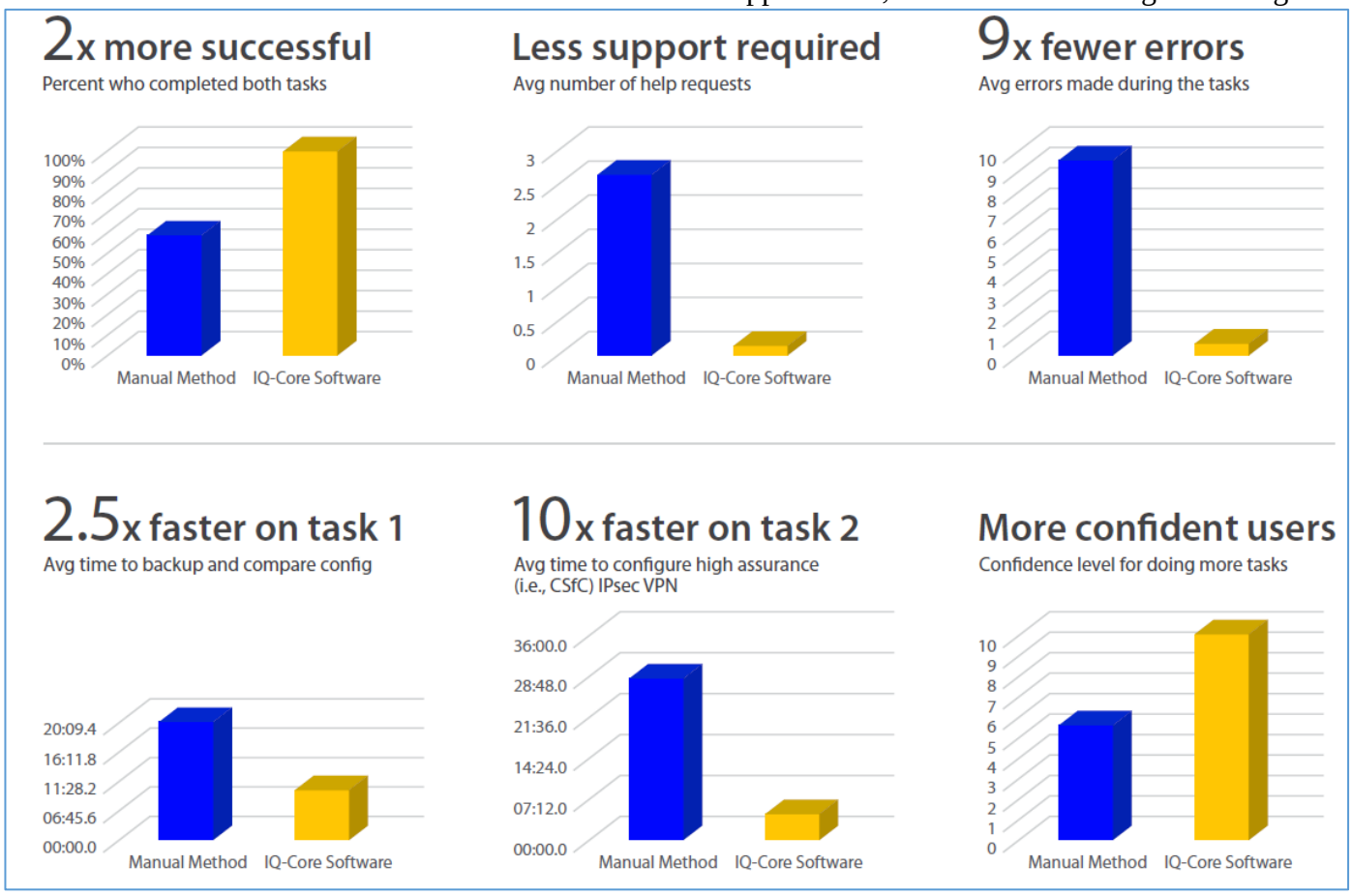

Figure 7 - Dramatic savings using integrated management tools

4. CONCLUSION

US Army and Marine Corps ground vehicle and tactical networking programs should be able to address critical needs to simplify and improve configuration control, management, and system awareness of ground vehicles by overlaying complexity and training burdens, by consolidating the management plane of these networks onto a "single pane of glass"– that is capable of providing distributed, hierarchical, and efficient management of network attached nodes on multiple platforms and at multiple tiers.