ENABLING THE TACTICAL EDGE IN DEGRADED ENVIRONMENTS

All-domain sensor-to-shooter situational Understanding

Author: Dominic Perez, CISSP (Certified Information Systems Security Professional), Chief Technology Officer, Curtiss-Wright Defense Solutions

To optimize overall situational understanding (SU) in the battlefield, the U.S. Army, Air Force, Navy and SOF are seeking new programs. These programs will adopt a variety of compute and bandwidth intensive technologies, such as cloud-based networks, and will drive far greater use of sensor data, video, big data analytics, artificial intelligence (AI), and machine learning (ML) to deliver the command and control information that warfighters need.

These new programs, such as ***Joint All-Domain Command and Control*** (***JADC2***) and the ***US Air Force Advanced Battle Management System*** (***ABMS***), will enable better coordination of deployed forces and enable the fielding of new capabilities to ensure that our warfighters have maximum SU and high-speed decision support.

Army Chief of Staff Gen. ***James McConville*** calls that "*decision dominance*" as described in his March 2021 report entitled ***Army Multi-Domain Transformation: Ready to Win in Competition and Conflict***. The report describes an expanded battlefield — coupled with short-, mid-, and long-range precision fires to engage and destroy adversary land, air, and sea capabilities — that necessitates a transformation of how command control is executed at every echelon.

"*Decision dominance is a desired state in which commanders sense, understand, decide, act, and assess faster and more effectively than their adversaries*," the report states. "*Decision dominance is enabled by convergence, the ability to see, sense, communicate, shoot, and move at speed and scale, connecting all sensors with the best shooter and the right C2 node.*"

Next generation capabilities, including video, AI and ML, are compute and bandwidth hungry. As they proliferate in the battlefield, processing needs to happen locally at maximum speeds.

As warfighters become increasingly dependent on the cloud to deliver these capabilities, solutions need to be developed to ensure that access is maintained in disconnected, intermittent, limited (DIL) environments. To enable the next generation of SU capabilities, the DoD is looking to deploy cloud replication between remote computing nodes and the cloud to provide a backup that ensures continuity of operations in the case of network outages or low bandwidth.

Several programs provide examples of how the DoD is seeking to deliver these cloud-based capabilities. The ***Air Force ABMS program*** establishes a federated cloud system that will provide secure processing from a security cloud called ***CloudONE***. It also defines a local cloud, ***EdgeONE***, that will provide continued security in case communications with CloudONE are disconnected.

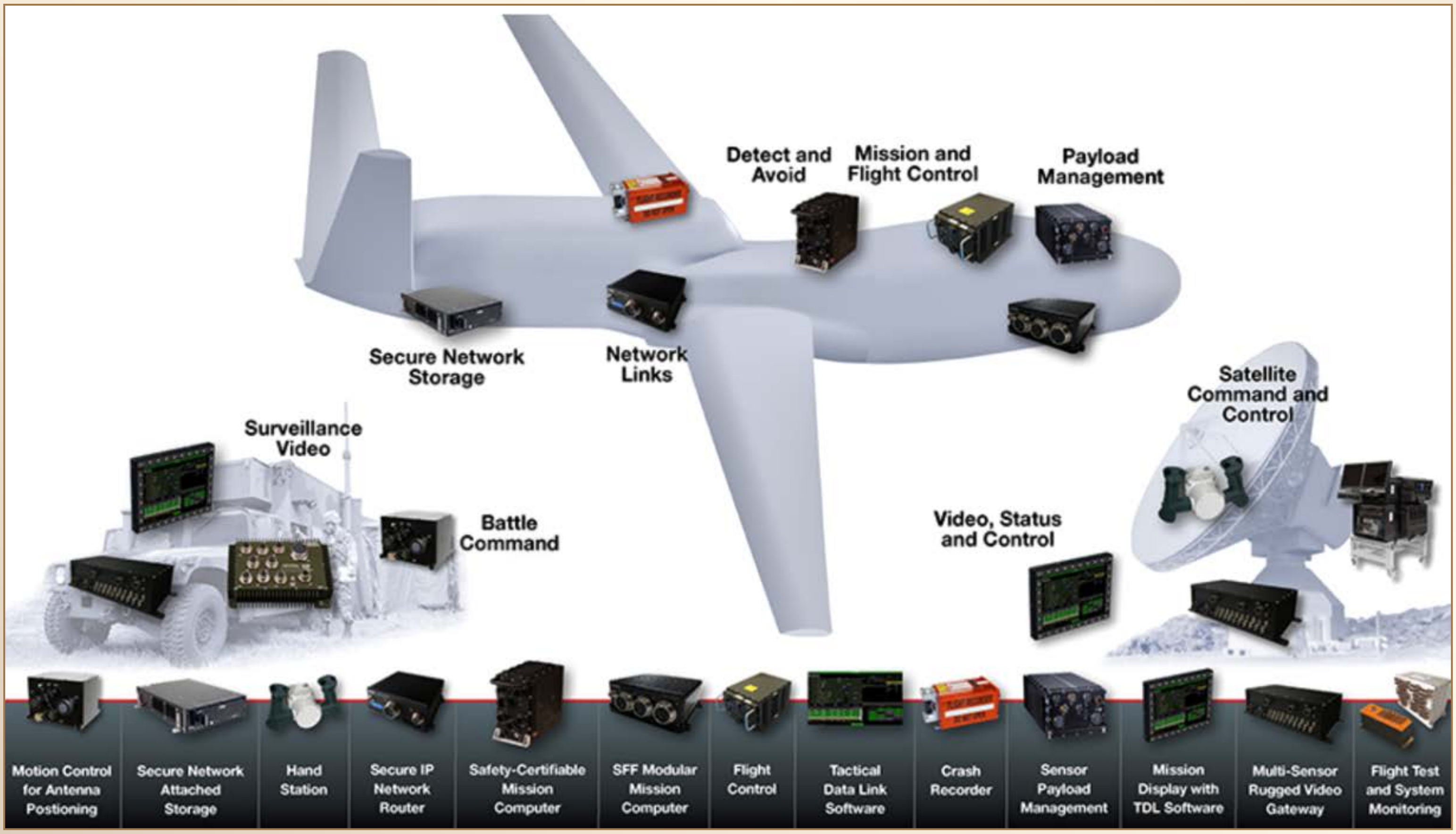
Another example is provided by a recently issued ***request for proposal*** (**RFP**) from the U.S. Navy to industry to support ***Manned-Unmanned Air Vehicle Team Tactical Cloud analysis.*** The Navy is seeking an approach for providing backup services in case the tactical unit becomes temporarily disconnected from the wider tactical network.

Complicating the matter, no single cloud provider can meet all of the DoD's requirements. As the JEDI fight dragged on for years, the cloud industry was undergoing rapid change from the single-source contract approach the Defense Department was then taking toward a so-called "multi-cloud" model of more than one vendor.

"*What you're seeing is across every enterprise — healthcare, financial services, government agencies, retail. Enterprises are choosing multi-cloud to meet service complexity*," ***Will Grannis***, managing director of Google Cloud's office of the CTO, told *MarketWatch* in October of 2021. "*Multi-cloud is here to stay, and that is reflected by what is happening with the [DoD's] Joint Warfighting Cloud Capability (JWCC.).*"

The ***U.S. Army's Integrated Visual Augmentation System (IVAS) program*** provides example of the potential and challenges surrounding these capabilities. IVAS, which includes a new ***Ruggedized Heads-Up Display*** (**HUD**), and body-borne compute pack, integrates next generation 24/7 situational awareness tools and high-resolution digital sensors to improve the warfighter's sensing, decision making, target acquisition, and target engagement.

PROGRAM EXECUTIVE OFFICE SOLDIER
Integrated Visual Augmentation System PM IVAS


Detect and Avoid
Mission and Flight Control
Payload Management
Secure Network Storage
Network Links
Satellite Command and Control
Surveillance Video
Battle Command
Video, Status and Control
Motion Control for Antenna Postioning
Secure Network Attached Storage
Hand Station
Secure IP Network Router
Safety-Certifiable Mission Computer
SFF Modular Mission Computer
Flight Control
Tactical Data Link Software
Crash Recorder
Sensor Payload Management
Mission Display with TDL Software
Multi-Sensor Rugged Video Gateway
Flight Test and System Monitoring

These capabilities will provide the increased lethality, mobility, and situational awareness necessary to achieve overmatch against our current and future adversaries in any domain. While the IVAS contract is currently embroiled in contacting and funding battles with Congress, it does represent the long-term vision for sensor-to-shooter connectivity.

To realize IVAS in the field will require a tremendous amount of data to be acquired, processed, augmented and redistributed.

The data IVAS uses will be far more than can be transported across the WAN to large datacenters, even with enterprise grade connection. What's more, when operating in DIL environments, this intensive processing must be done locally to the warfighter at the tactical edge.

To make these new capabilities a reality, these programs must overcome several key challenges:

> **a)** ***The need to maintain and improve mobility, giving commanders options to maneuver without being tied down to large fixed computing infrastructure***
>
> **b)** ***The need to maintain SA, and ensure C2 services are available, even in communications DIL environments – in the era of electronic warfare and contested spectrum***
>
> **c)** ***The ability to support multiple types of cloud infrastructure, as no one cloud offering is expected to meet all need***

To realize the capabilities required to support sensor-to-shooter SU at the tactical edge, military organizations will require a new class of rugged, fieldable, network processing and data storage solutions that can provide tactical and expeditionary teams access to all the data and compute resources they need.

These systems will need to be able to provide cloud-like services, maintaining high operational availability of applications and data, even in DIL environments where WAN connectivity is not assured. What's more, these systems will need to integrate seamlessly with leading public, government and private cloud providers.

The good news is that new technologies are becoming available that can address these challenges. They include high performance, low size, weight and power (SWaP) tactical, standards-based computing and storage platforms that can be deployed at the tactical edge – and that can host any number of compute and storage replication software infrastructure.

Another critical emerging technology is computing and storage infrastructure and infrastructure software capable of multi-cloud replication, along with support for virtualization and containers.

Earlier efforts to bring these levels of performance and service to the battlefield involved trying to deploy huge sets of standard datacenter equipment, installed in shipping containers or 19" data-center-like equipment racks.

These systems proved to be too large and hard to transport, significantly limiting their mobility. In addition, these standard solutions are power hungry, which adds additional burden on mobility

Higher performance, small form factor servers, combined with new approaches to distributed processing, offer the potential to move smaller slices of processing even closer to the edge and improve mobility.

Standard 19" rack mount datacenter equipment is not designed to withstand harsh environments and not designed to operate on the move – leading to concerns about equipment failure and loss of availability of mission critical communications. Instead, systems designed to meet military environmental standards, such as **MIL-STD-810**, should be used. These rugged systems can operate optimally when exposed to the harsh temperatures, vibration, shock and EMI typical of battlefield conditions.

To meet requirements for mobility, and support integration into the types of platforms on which they might be mounted, sensor-to-shooter solutions will need to provide high reliability compute and storage in a small SWaP-optimized form factor designed for mission-critical applications.

Solutions that can deliver the high-density compute, storage and networking infrastructure needed to handle such large data loads are available today.

These modular systems can be optimized for program needs, so that functionality, including the number of CPU cores, GPU cores, and solid-state storage density can be maximized depending on program needs.

When these systems are based on industry standard processors and GPUs from vendors such as Intel and NVIDIA, they are compatible with a wide variety of applications and can meet the needs of a vast array of C5ISR use cases including data gathering, analytics/AI, ML and SA.

That means a new class of modular datacenter can be fielded designed to support emerging distributed processing, storage/replication and the hyper-convergence infrastructure software needed to deliver mobile cloud services.

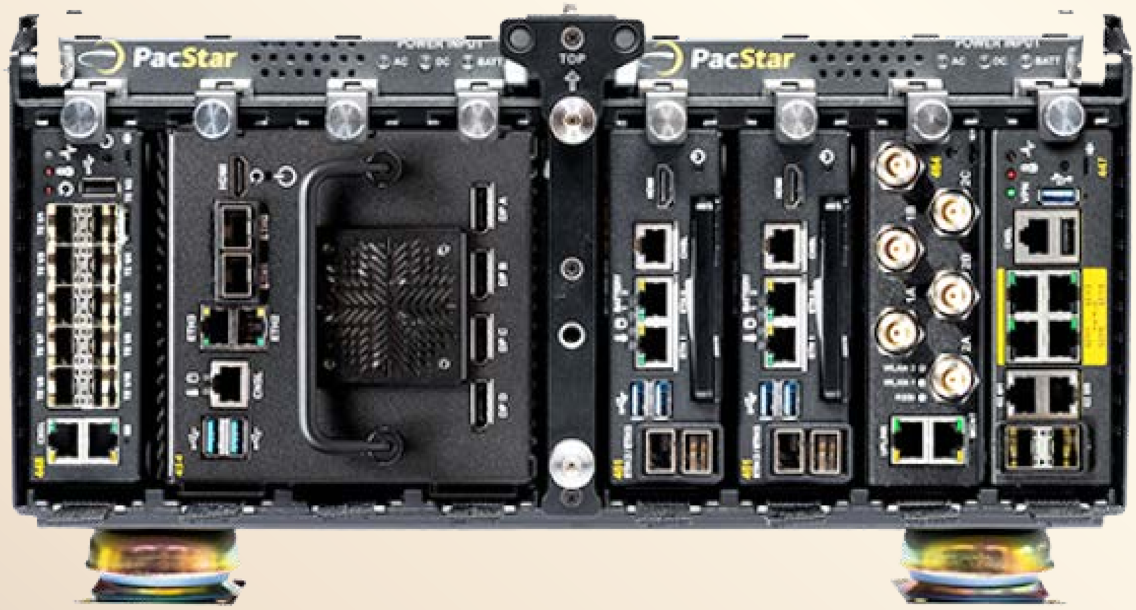
An example of two such systems available today that can support sensor fusion and mobile cloud applications at the tactical edge are ***Curtiss-Wright's PacStar Modular Data Center (MDC)*** and the ***Tactical Fusion System (TFS)***

These COTS-based, modular tactical and expeditionary rugged systems (*both pictured below*) use proven small form factor modules for compute, storage, and networking functions and feature industry leading reduction in SWaP.

They can be deployed dismounted, in FOBs, command posts, ground vehicles, and aircraft, as well as in upper echelons – for military, intelligence, law enforcement, and Homeland Security use.

Depending on the specific use case, PacStar MDC and TFS configurations can include a mix of compute modules, storage modules, and GPU modules, along with the company's switching/routing modules.

Curtiss-Wright PacStar's Modular Data Center (MDC).



Curtiss-Wright PacStar's Tactical Fusion System (TFS).

With this new class of high capacity, rugged, small form-factor hardware, it's now possible to deploy emerging software infrastructures to automate the distributed processing and storage, communications and cloud replication required to ensure SA is maintained to the edge of the battlefield.

Today, large enterprise software companies are rapidly developing new technologies to ensure that data and applications can move seamlessly from the cloud to the edge and back, with little operator intervention.

Several key technologies enabling this include application virtualization and containerization, network virtualization, and ***hyper-converged storage infrastructure*** (**HCI**).

Application virtualization and containerization are technologies that decouple applications from the underlying hardware, allowing multiple applications to run securely on a single server.

This approach optimizes SWaP by reducing the number of servers required to deliver the needed processing. Virtualization and containerization also enable applications to be replicated or moved from server to server, and from cloud to edge, to balance the availability of computing resources or minimize latency over network connections.

For tactical organizations, this offers the potential to move applications closer to the warfighter to reduce processing delays and provide processing even in DIL environments.

HCI technologies decouple the storage of application data from hardware. They eliminate reliance on today's legacy network attached storage (NAS) or storage area network (SAN) architectures.

These new technologies are foundational for replication of data between cloud and edge processing — enabling warfighters to take copies of cloud data into theater, and replicate changes to data over DIL connections when appropriate.

HCI also provides local data replication for deployed organizations with a need for high reliability – ensuring that data is available in-theater even in the event of a server or disk failure.

New advances in these technologies are rapidly improving the ability of tactical organizations to replicate data between any of the major cloud providers and move applications between the edge and cloud, providing maximum mobility and maneuver options for our warfighters.

As the DoD moves forward with awarding contracts under the ***Joint Warfighting Cloud Capability*** (JWCC) it's important that the infrastructure software deployed to the field is not tied to a single cloud vendor or application stack.

In the long term, this can be achieved by rewriting legacy applications in cloud native applications that use containers and **Kubernetes**, an open-source container-orchestration system for automating computer application deployment, scaling, and management.

Until we reach the day where all applications use these modern software development and deployment models, a path must be established for the blending of legacy and new developments and continuous, evolutionary improvements.

VMware Virtual Cloud Foundation provides one possible path forward. This powerful collection of software, which bundles the hypervisor, hyper-converged storage, container support, and advanced security features, has the ability to synchronize with multiple public and private cloud infrastructures.

The benefits of a converged compute/GPU/storage/networking system combined with a modern software infrastructure at the edge of tactical network are numerous. This approach can support a diverse array of use cases when operating in DIL environments, including:

- *Processing and analyzing video in visible and IR spectrum for target identification, tracking and handoff,*
- *Integrating multiple sensor input from multiple end points, including from wireless sources*
- *Supporting situational awareness, C2 and mission command applications,*
- *Distributing data, including geographic information and point-of-interest information to tactical squads,*
- *Executing computer vision, AI and ML algorithms with low latency.*

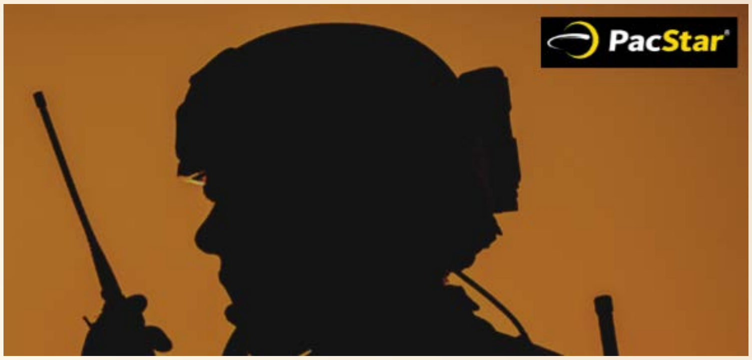
The hardware and software are available today to realize the goal of the new all-domain situational awareness-driven warfighting doctrine.

These rugged, deployable systems, with support for sensor-to-shooter SU and connectivity at the tactical edge in degraded environments, are poised to bring the benefits of cloud-based computing and the new capabilities it supports to the warfighter.

www.curtisswrightds.com

CURTISS-WRIGHT
DEFENSE SOLUTIONS

pacstar.com



Author Dominic Perez, CISSP (Certified Information Systems Security Professional), Chief Technology Officer, Curtiss-Wright Defense Solutions, has been with PacStar for more than 13 years and, in that time, he has supported development of PacStar's rugged, tactical hardware and IQ-Core Software serving as the subject matter expert for compute, virtualization and virtualized network functions. Dominic is part of the PacStar team that won tactical networking equipment and software awards for numerous DoD tactical programs including the US Army T2C2, US Army SFAB, US Army ESB-E, PM TN Secure Wireless Small Form Factor, PEO-C3T TCNO, and US Marine Corps NOTM vehicle-mount and deployable communications programs

Dominic currently leads the teams developing PacStar's Commercial Solutions for Classified, Modular Data Center, and Tactical Fusion System product lines deploying cutting edge secure communications, edge data processing, and rapid sensor to shooter situational awareness to the warfighter at the tactical edge systems in the face of disconnected, limited, and intermittent (DIL) comms environments.