Defense Unicorns

Rapid Software Deployment in Disconnected Environments

Published
April 2nd 2025

Darian Chavira
Product Manager

Wayne Starr
Technical Lead

Rapid Software Deployment in Disconnected Environments

"The battlefield is unpredictable - the only certainty is things don't go according to plan, and software often needs patches, updates, and even brand new solutions. Jamming, cyberattacks, and broken connections are constant threats. UDS changes the way we act - we can patch, update, and deploy on the move. This is more than a technology - it is a lifeline for those in combat operations."

-Volodymyr Kondratenko, CEO of Edge Solutions Lab

This paper is for military commanders, program managers, acquisitions officers, and defense technology enthusiasts who want to solve the problem of operating software applications in resource constrained airgapped environments without dedicated IT engineering support.

Solving this problem is critical to maintaining a decisive advantage against near-peers in Denied, Degraded, Intermittent, and Low-bandwidth (DDIL) combat environments (DoD DDIL Strategy, 2024).

A fundamental principle of maneuver warfare is the ability to shoot, move, and communicate; however, in DDIL environments, our weapons systems and platforms often fail due to connectivity issues. This principle has become tightly coupled with software and the Battlefield Internet of Things (BIoT) (JADC2 Summary).

A critical dilemma of the BIoT and the DoD's reliance on cloud and internet technologies is how can a unit operate in these restrictive environments without internet connectivity.

Reliance on the internet (connectivity) has become a center of gravity under constant attack from near-peer threats. Without secondary and tertiary means of deploying software into these DDIL environments, the DoD's reliance on the internet could become our fighting forces' Achilles heel.

UDS | Tactical Edge

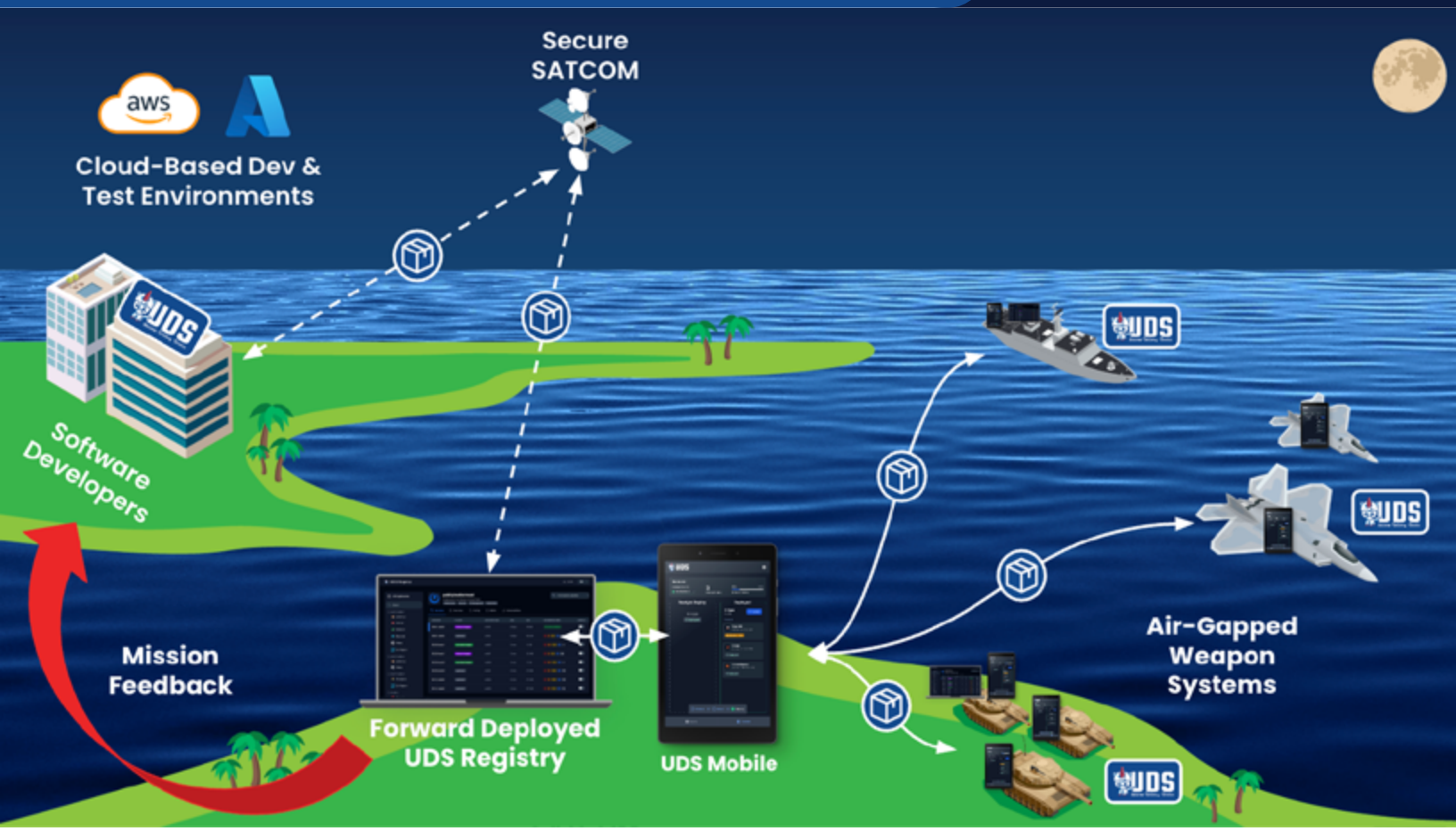
- Enables deployment of applications with or without access to the internet
- Intuitive interface created for those on-the-move (in-flight, vehicle ops, etc.)
- Runs on small devices (2GB RAM)-small enough for small-drone operations

⚠ The Problem

Imagine a typical battlespace scenario where multiple platforms and weapons systems rely on connectivity and real-time data while contending with offensive cyber attacks. A common scenario will arise.

- A critical Common Vulnerabilities and Exposures (CVE) is detected.
- A forward-deployed operator requires an immediate patch to maintain system effectiveness.
- A decentralized unit managing software needs to push an update to the forward-deployed operator as quickly as possible.

The ability to move through the processes of software cycle time faster than your adversary will be the differentiator between weapon systems ready and in position or deadlined and out of the fight.



Demonstration

In order to show how Defense Unicorns can help solve this scenario, the team conducted the following product demonstration (Demonstration). Here is a summary of the steps taken in this demonstration

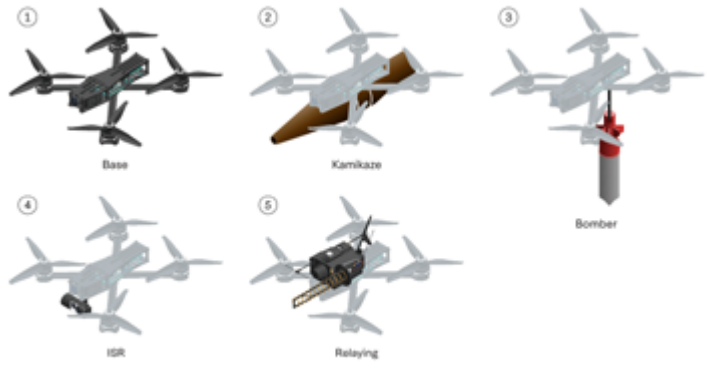
1. Representatives were stationed in two locations, one in the U.S. and one in Ukraine.
2. The Ukrainian team has an application down, impacting their ability to run mission-critical software. A common combat scenario occurs when active jamming, cyber CVE exploitation, or rapid battlefield changes disrupt operations.
3. The U.S. based team uploads a software package into the secure UDS Registry.
4. The Ukrainian team connects to the secure operational satellite and pulls down and installs the application from the UDS Registry.
5. The drone the Ukrainian team is getting operational is fully disconnected (airgap environment).
6. The only thing that connects to the drone is the tablet.
7. With one click, “install,” the new hardened application is on the tablet and then connected to the drone.
8. This process takes a matter of minutes to get mission systems back in the fight.

Click to View Real-World Application on Youtube

Success

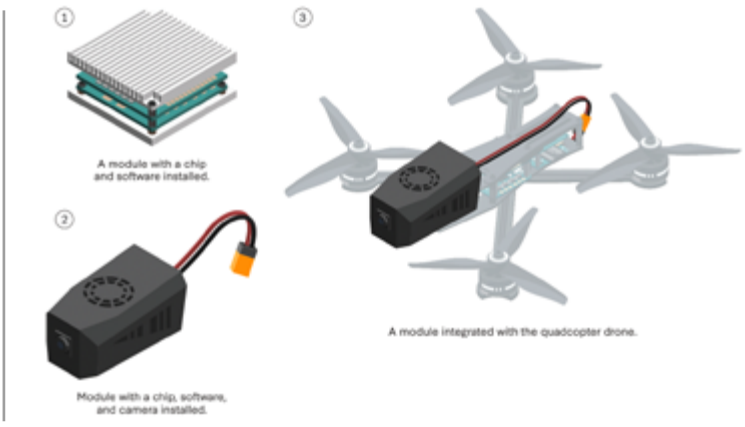
By leveraging UDS, hardened software repositories, and satellite communications, this demonstration showcases how modern warfighters can maintain operational superiority even in air-gapped and cyber-contested environments. This capability aligns with key findings in Kateryna Bondar's report, "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare" (CSIS, 2025).

Figure 1: Types of FPV Drones Used for Various Missions



Source: CSIS analysis.

Figure 2: Examples of Modules Enabling Autonomous Capabilities



Source: CSIS analysis.

The Technical Solution

The following section gives a walkthrough of the technical implementation of how UDS works in tactical edge environments. To learn more, go to UDS Technical Documentation. UDS Tactical Edge is built on a foundational philosophy: all updates should be modular, self-contained, declarative, and based on open transport and storage standards. This design ensures maximum flexibility, portability, and recoverability across diverse environments.

The update process begins with a standard Kubernetes deployment using familiar components such as manifests, Helm charts, and Docker (or OCI) images. These artifacts are then bundled into a Zarf package, creating a single, self-contained software unit (Learn about Zarf). This packaging approach simplifies distribution, ensuring that all necessary components remain intact and travel together.

To integrate with UDS Core, an additional manifest—the UDS Package Custom Resource (CR)—is included within the Zarf package. This manifest enables the UDS Operator to dynamically configure essential platform resources, such as ingress, single sign-on (SSO), monitoring, network policies, and more. Unlike a rigid, one-size-fits-all approach, this integration is highly adaptable: layers of UDS Core can be selectively added or removed based on the deployment size and application context. This flexibility enables deployments on a wide range of hardware, including edge nodes as small as a Raspberry Pi 4 (RAM 2 GB). Additionally, since the operator generates these resources dynamically, they are tailored to the target environment, reducing the need for extensive manual configuration.

Once fully integrated, the package is published to the UDS Registry which is OCI-compliant (Open Container Initiative). From there, it can be stored, referenced, mirrored to other registries, or transferred via physical media. The package can also make use of cross-domain solutions that support OCI/Docker image transfer, ensuring secure and flexible distribution.

When the package reaches its final destination, it is pulled onto the UDS mobile application. This enables software updates to be physically transported to edge machines that operate independently of traditional infrastructure. Once the package is delivered, the edge machine—running its own UDS stack (and optionally its own UDS Registry for self-sufficiency)—installs and syncs the new or updated applications. The UDS mobile application orchestrates this process, ensuring seamless deployments even in disconnected environments.
By adhering to open standards and a declarative model, UDS enables organizations to remain agile and self-sufficient, even in resource-constrained or air-gapped settings. UDS packages do not simply contain software binaries and configurations—they define the entire end-to-end declarative state of an application. This guarantees consistency across environments, reducing variability and making testing and debugging significantly more predictable and efficient.

Conclusion

This approach not only simplifies software updates but also reinforces the resilience and adaptability of applications deployed in dynamic, constrained, or disconnected environments. In our hyper-software defined battlespaces, the Department of Defense needs a tool to move from connected to disconnected and from data rich to tactical edge environments rapidly - join Defense Unicorns on the journey to revolutionize Defense Technology.

For more information, contact hello@defenseunicorns.com

Citations

Bondar, Kateryna. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare. Center for Strategic and International Studies (CSIS) Wadhwani AI Center, March 2025.*

Department of Defense. (2022, March 17). Summary of the Joint All-Domain Command and Control Strategy.

Open Containers Initiative. Open Container Standards. https://opencontainers.org/, accessed [03/14/2025].

Defense Unicorns. Zarf: DevSecOps for Air-Gapped Deployments. https://zarf.dev/, accessed [03/14/2025].

U.S. Department of Defense, Chief Information Officer (DoD CIO). Fulcrum: Advancing Strategic Principles. Washington, D.C., [year of publication]. Available at: https://dodcio.defense.gov/ .

