Leveraging the Expeditionary Processing, Exploitation and Dissemination (Ex-PED) Model at Enterprise Challenge 2016 (EC-16) Using ARL's Roll-On Roll-Off (RORO) PED

Scott Ross, Paul Wernet, and George Pulig
U.S. Army Research Laboratory
2800 Powder Mill Road, Adelphi, MD 20783
Veranox Corporation
4560 King Edward Court
Annandale, VA 22003
EOIR Technologies, Inc. – A Polaris Company
6165 Guardian Gateway, Suite J
Aberdeen Proving Ground, MD 21005
Email: scott.m.ross.civ@mail.mil, paul.g.wernet.ctr@mail.mil, gpulig@eoir.com

ABSTRACT

Coalition exercises have historically excelled at aggregating and utilizing sensor data at the enterprise network level (e.g., Distributed Development and Test Enterprise (DDTE) or Combined Federated Battle Laboratories Network (CFBL)), where individual component sensor data is aggregated and displayed on a central Common Operating Picture (COP) or exploited in some similar manner. This data is collected in a bottom-up model from individual capabilities that are designed for deployment at the tactical edge. Typically, each such capability passes its data through a guard or similar enterprise network protection mechanism. Once collected at the enterprise network level, the data and products can be further exploited and disseminated as the mission requires (e.g., displayed on a COP, shared with a coalition partner). This exploitation and dissemination tends to remain at the enterprise level.

At the tactical edge, however, components remain blind to what their coalition partners (not to mention complementary U.S. functions) may have available. The data flows up; it does not flow back down very easily. How, then, does a tactical component access and/or make use of this data?

The same data aggregation and exploitation technologies available on the higher end networks is possible at the tactical edge using an appropriately designed and deployed Ex-PED.

At EC-16, RORO successfully supported the ARL mission at the tactical edge, demonstrating a number of enterprise PED capabilities. General capabilities included deploying a system that collected data from disparate sources (air, ground, and coalition) operating in the same environment at a tactical level, made that data available to users on the ground (on two different PED platforms both hosted by RORO), and passed the same data up through the enterprise to DDTE and CFBL networks.

EC-16 was conducted in July and August 2016. This paper highlights the success and lessons learned from participation in that exercise. Specifically, this paper discusses how RORO facilitates a bottom-up tactical edge approach to collection, publication, discovery and utilization of sensor data across connected networks and how this could have a direct impact on the Theme 8, "Sensing for Decision Making."

1. INTRODUCTION

ARL leveraged its background in PED development, wide-area imagery and intelligence aggregation to develop a mobile, small footprint PED system called Roll-On Roll-Off (RORO). RORO uses a VMware platform designed to host virtual machines running selected operating systems and their hosted applications. RORO includes a fast 10 Gigabit network switch and provides high density, high performance mass storage capability. This highly portable, scalable system is self-contained in four 4U transit cases.

2. RORO PED CONFIGURATION

The RORO PED hardware as show in Figure 1 consists of four Dell R720 servers (two hypervisor hosts, one vCenter host, one virtual machine storage server), one Dell MD3820i data storage server (8 TB flash and 12 TB mechanical drives [raw capacity]), one Netgear M7100 10GbE production switch, one Cisco 3750E 1GbE management switch, one TrippLite KVM switch with console, two Dell Precision M6800 analyst laptops, and two APC Uninterrupted Power Supplies (UPS) units. All of the hardware is contained in four 4U transit cases with the exception of the UPS units. The physical footprint is approximately the size of a standard half-height server rack with total palletized shipping weight coming in just under 700 lbs.

The RORO PED baseline software configuration is based on the VMware vSphere 5.5 platform and includes the ESXi 5.5 hypervisor, vCenter Server, and Horizon 7 Enterprise. The vCenter server software is running on a Windows 2008 R2 server and uses a Microsoft SQL Server 2008 R2 database. The data storage server is managed by a virtualized Windows 7 workstation via iSCSI targets providing shared folders for access by other RORO supported systems (physical or virtual). Other storage access technologies (e.g., NFS) can be configured as required.

The VMware platform is a de facto industry standard and ensures support for deploying most virtual machine file formats quickly and easily. Non-virtual systems can be converted to virtual machines (using VMware conversion tools or a direct rebuild) or connected via the switch in the case of specialized hardware requirements. The 10 Gigabit production switch provides plenty of throughput for data intensive applications and copy/edit processes.

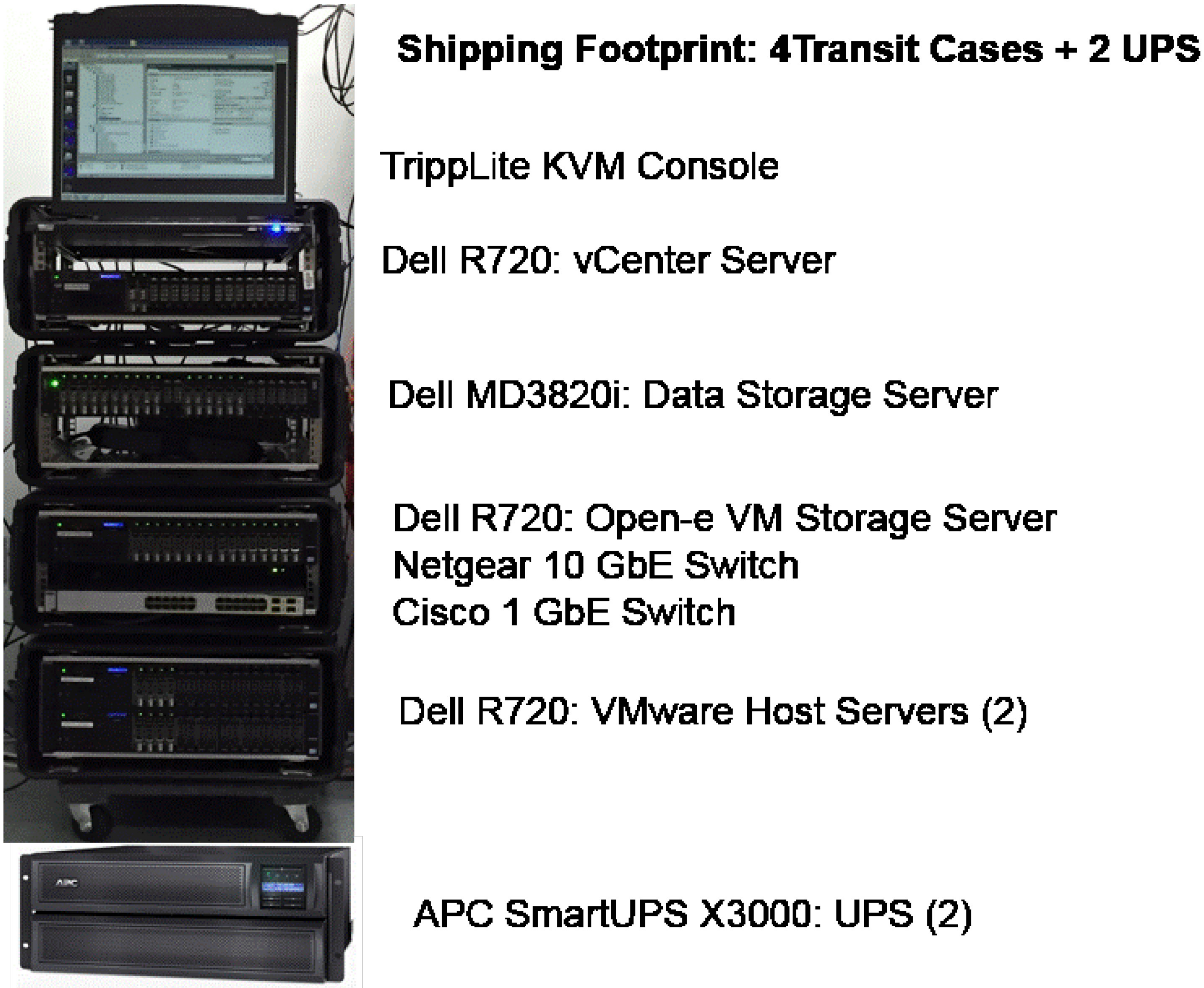

Figure 1- RORO Hardware

3. DEPLOYMENT OF A CAPABILITY AS A VIRTUAL MACHINE(S) ON RORO

The Distributed Common Ground Station Army DCGS-A Intelligence Fusion Server (DCGS-A IFS) version 3.2.4 is directly available in virtual machine format. Because of the RORO industry standard hardware and software configurations, deployment of the DCGS-A version 3.2.4 software was performed in less time than is traditionally needed on currently fielded hardware for the baseline. Operators were able to perform all the basic storage and networking configurations in one day, upload VMs in one day, and complete the configuration in one day. A typical DCGS-A IFS installation can take up to a week performing the same process. Additionally, because of the performance characteristics of the RORO, maintenance and sustainment task times were reduced, such as loading Information Assurance (IA) hot fixes and feature patches. Performance of the DCGS-A 3.2.4 VMs on the RORO were also above par to a currently fielded DCGS-A IFS. Operators noticed that storage operations and CPU intensive tasks were handed more efficiently by the RORO during the exercise. Additionally, it should be noted that none of the VMs needed to be reconfigured for the RORO specifically; rather, operators were able to simply upload them to the RORO and start working with them immediately. Even though the DCGS-A Multi-Function Workstations (MFWS) were deployed as virtual machines, physical laptops were required to connect to the system and interface with the virtual machines due to the Graphics Processing Unit (GPU) requirements for viewing/processing FMV. Connecting the physical MFWS laptops to the virtualized DCGS-A MFWS workstations was as simple as expected.

Note also that for security reasons, in some instances we were required to revert to a previous version of the MFWS that had been approved for use in coalition environments. The virtualized infrastructure made this as simple as having an analyst switch from one virtual machine to another with no need to deploy additional hardware to support the requirement.

The National MASINT Office Measures and Signatures Intelligence Enterprise Service Bus (NMO MASBUS) software was also quickly deployed on RORO as an application on a pre-existing standard virtual machine running Windows 7 Enterprise. The configurations required to connect MASBUS to Open Standard Unattended Sensors (OSUS) and publish resulting data sets to the RORO data repository were completed in a matter of minutes with telephone support from NMO.

4. CONNECTING EXTERNAL (NON-VM) SYSTEMS TO THE RORO NETWORK

Once deployed at EC-16, integration of the RORO to the event network was also a simple, straightforward process. Much of that is due to the use of industry standard components and configurations on the RORO, which allowed it to properly interconnect to networks it had not connected to previously.

The OSUS Gateway was connected to the RORO network via a single static IP. All of the configuration was completed using the MASBUS and OSUS software applications, with no RORO specific accommodations.

The 3D Sensor COP was deployed on a laptop utilizing specialized hardware for 3D imagery and was not a candidate for virtualization. Connecting it to the RORO network and providing access to RORO data repositories and other network assets was straightforward and required minimal effort.

The Infrared Motion Detction (IrMD) analyst workstation was deployed on a laptop utilizing specialized hardware for IrMD imagery and was not a candidate for virtualization. Connecting it to the RORO network and providing access to RORO data repositories and other network assets was straightforward and required minimal effort.

Integration of the Cross Domain Guard with the RORO network was not without issues. Exercise network support staff provided an instance of the Guard API Gateway on a 1U server that would be installed on the RORO rack. Network configuration on the RORO side was straightforward, requiring little more than assignment of a static IP address and user credentials to access the data repositories. Issues arose during the configuration process to pass data through the Gateway filters, and is addressed later in this paper. These issues are independent of the successful connection between RORO and the Gateway/Guard.

5. DATAFLOW

5.1 MASBUS AND UGS DATA DISSEMINATION

As shown in Figure 2 below for the EC-16 exercise, the NMO MASBUS software was used to ingest Unattended Ground Sensors (UGS) data from the OSUS Gateway and produce two data repositories. MASBUS was deployed as an application on a Windows 7 workstation listening on a specified port for activity from the UGS Gateway. First, MASBUS would write one copy of the raw data to a shared repository (drop box). Second, MASBUS would convert the ingested raw data to another Guard-friendly format and write the converted data to a separate repository for the Guard. Both formats would be available to any connected capability for retrieval/use. In this case, that included the 3D Sensor COP, the DCGS-A MFWS, and the Guard. The Guard was not without issues and will be considered in depth in a subsequent section of this paper.

The 3D Sensor COP was able to access the UGS data as written by MASBUS to the shared repository and display it correctly on the COP. Some minimal modifications were required to some of the data elements coming from the OSUS Gateway, but this was resolved quickly between the COP and OSUS teams without RORO reconfigurations or alterations.

The DCGS-A MFWS, however, was initially not able to access the UGS data. Once the RORO team was deployed in the operational environment for the EC-16 exercise, it was discovered that the DDF (Distributed Data Framework) version in the current MASBUS implementation was a higher version that what is available in the DIB in the DCGS-A 3.2.4 system, and the MFWS relies on the local DIB. Because the MASBUS system was the core solution to bringing much of the sensor data into the system, an adapter was necessary to allow for proper publishing of the incoming sensor data to the DCGS-A DIB.

Using a Government off-the-shelf (GOTS) adapter solution developed by the Intelligence and Information Warfare Directorate (I2WD), the RORO Team created a solution which allowed for sensor collections to be exported in real time from MASBUS and moved to the DCGS-A system via a drop box. The adapter would monitor the drop box for new files, parse the various data types into the proper version 3 DIB schemas, and publish them to the DCGS-A v3 DIB. This allowed the RORO operators to visualize the sensor data in Ozone application on the 3.2.4 MFWS client systems as well as the 3.1.7 MFWS client systems. Sensor data was of various types, from ground based sensors as well as detections from sensors on board Exercise aircraft. Many of these systems also publish more than simply detections, they also provide platform information, health and battery status, and more. Each of these sensor types as well as their various message types were made available by MASBUS and parsed by the I2WD adapter for the Exercise.

Adding this additional capability to the RORO was simple and straightforward. A new VM was instantiated and the adapter loaded. The data conversion and publishing process functioned properly with no need for reconfiguration of any other aspects of the network.

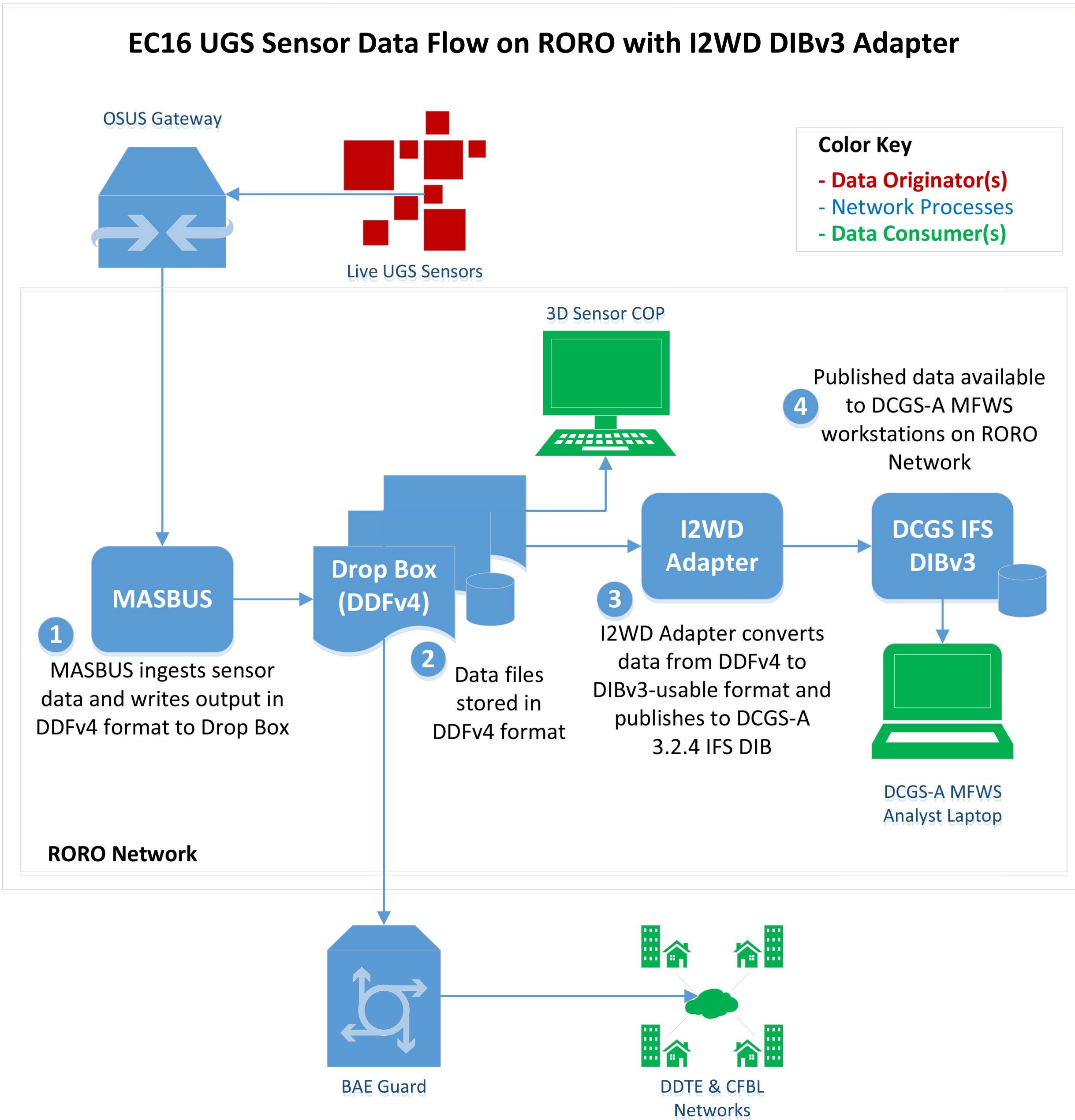

Figure 2- EC-16 UGS Sensor Data Flow on RORO with I2WD DIBv3 Adapter

5.2 GUARD 5 INTEGRATION

Configuration of the Guard to support systems on the RORO network was not without issues.

Once the gateway was successfully connected to the RORO network and communications were verified between RORO and the gateway and between the gateway and the guard itself, we were able to start sending data and test the configuration of the Gateway application. To accomplish this and keep track of files so that data would only be sent once, the RORO team wrote a script to copy sensor data in real time to yet another folder for access by the gateway. Once the gateway picked up a file, it would delete it from the folder. This provided a user friendly way to monitor activity and status on gateway activity. The script used by the gateway to validate the files was complex and required significant modification by a gateway/guard technical team to enable successful passing of files from RORO through the gateway and guard. This took several days and could only be accomplished once we were at the exercise, as this was the first time a guard/gateway was available. Nevertheless, some files were never successfully processed by the gateway, including some types of JPEGs (e.g., JPEG 2000). This is a guard issue and not related to the RORO PED.

Fortunately, the RORO team only had to work through this process once for all the RORO-supported sensors and analyst products (versus having to integrate each asset and capability with the guard separately).

6. RORO LIMITATIONS AND PLANNED IMPROVEMENTS

The EC-16 exercise provided an opportunity to evaluate the RORO PED system in a production-type environment and identify limitations as well as successes. Limitations serve as useful indicators as to where improvements can be planned for the benefit of the military in future implementations. Noted limitations included:

- Some latency was noticed in retrieving data and starting up virtual machines even with a 10 Gb switch. This issue was identified only at the initial load (e.g., when an analyst first brings up a Wide Area Motion Imagery (WAMI) dataset), and the delays were momentary (albeit unexpected). The exact cause is being investigated.
- Needed to deploy full workstations or laptops (complete with dedicated GPU cards) for FMV and WAMI data viewing and analysis at real time speeds. A software virtual GPU solution was not adequate for practical use for an analyst.
- Two UPSs were required and added ~200 lbs. weight plus space requirements (not included in the 4 4U transit cases that housed RORO). The power fluctuations even in ground power were such that a

UPS is a mandatory requirement just for power conditioning even if no actual power failures occur. The added weight, however, could be an issue.

- Environmental issue: Produced a lot of heat in the trailer. Required addition of two standalone AC units to the trailer.
- Hardware redundancy was achieved by bringing additional hardware (on site spares). If either of the two ESXi hosts were to fail, then either the vCenter Server host or the VM Storage Server could be re-purposed as an ESXi host to continue the mission. This change would not be immediate, and would likely take up to a day to implement.
- Throughput / data transport limitations: while not a factor at EC-16, the current switches do not support 40 Gb connections. This appears to be a requirement for some sensor packages that are expected be deployed at future exercises.

After operating the RORO in the EC Exercise and identifying the limitations just described, the RORO Team took another look at some of the best of breed components available in industry and began a trade study aimed at looking to refresh the hardware platform. After some testing, the following suggestions were put forward by the Team:

- Virtualize the vCenter Server instance itself within the vSphere deployment. This allows the elimination of the physical host used to host vCenter Server as well as the KVM and associated console. A laptop will be added and used for system configuration and management. This will further reduce the space requirements and weight, as well as power requirements.
- Add a third hypervisor host to the existing two-host configuration. This would provide real-time system redundancy, virtually eliminating system downtime in the event of a host failure. Three hosts would also enable the deployment of more robust hypervisor and storage management technologies, such as virtual Storage Area Network (vSAN).
- Eliminate separate storage server for virtual machines. Utilize vSAN instead. Storage will be local to the host running the virtual machine, plus the vSAN software is implemented as a kernel module and is therefore in the I/O path, which further increases the data access rate. Added benefit of vSAN implementation: provides true, automated virtual machine redundancy and high-availability (vs. current manual method). vSAN is not just a fancy RAID implementation; it deals with full host failures as well as data/disk errors.
- Implement zero-client terminals in combination with advanced GPU cards in the hypervisor host servers. This eliminates the need to transport/maintain independent workstations for full analyst capabilities and enables all of the work to be done on the hypervisor host servers. Also enables analysts to use larger monitors vs. limitations of laptop screens.
- Reduce power requirements and drop from two UPSes to a single UPS. For example, research identified a single 3U UPS that will meet the reduced power requirements and also support both 120 and 240 volt inputs to increase flexibility in diverse deployment scenarios. Reduced power consumption also means reduced cooling requirements. Eliminates need to acquire separate UPS equipment for deployment in 240 volt environments.
- Upgrade the core network to a single 48 port 10 Gb switch with a minimum of two 40 Gb ports. This would reduce the rack space required for switching from 2U to 1U and enable the production network to accommodate sensors with higher bandwidth requirements. Saves 1U of rackspace, some weight, and reduces power requirements.

- Consolidate all elements into three 5U cases, including the UPS. Previous system was four 4U cases PLUS two 4U ½ depth UPSes. Reduces total weight by over 150 lbs. (just for the eliminated UPS and the vCenter server physical host).

All of these improvements, taken together, will result in an upgraded PED system that is physically smaller and easier to transport, supports faster processing with reduced latencies, eliminates the need for physical analyst workstations, and is more fault-tolerant due to real time hardware redundancy and vSAN implementation vs. on site spares.

Making the updates described above will ensure that the RORO is ready and capable for the next missions for which it is targeted, most likely including increased sensor data ingestion and processing, additional 3D and video capabilities, and the use of the RORO as a core infrastructure solution at future Exercises. This will allow the RORO to not only work independently as a PED solution, but also serve as a central system capable of supporting multiple processing types at these Exercises.

7. BOTTOM-UP APPROACH FACILITATED BY RORO

RORO served as a centralized network for data networking, data storage and retrieval, as well as a single integration point with the enterprise networks for a number of capabilities at EC-16.

Specifically, RORO demonstrated its ability to field a number of systems as virtual machines, including an unclassified implementation of the DCGS-A Intelligence Fusion Server (IFS) stack with Multi-Function Workstations (MFWS), ARL's 3D Sensor COP, ARL analyst workstations, a virtualized data storage server, and the National MASINT Office (NMO) Measures and Signatures Intelligence Enterprise Service Bus (MASBUS) software. RORO was used for real-time data collection for both Full Motion Video (FMV) and Infrared Motion Detection (IrMD) tracks from an aircraft as well as ingesting ground sensor data from the Open Standards Unattended Sensors (OSUS) Gateway. Ingested sensor data was published to the 3D Sensor COP, MASBUS including DCGS-A Information Backbone (DIB) v4, and the DCGS-A COP running on the MFWS via DIB v3. Finally, RORO was used to forward sensor data, observation data and analyst products across the EC-16 Cross Domain Solution (CDS), providing a single point of integration with the CDS for all of the RORO-supported sensor systems. After passing the CDS, the data was available for further exploitation and dissemination on the classified Distributed Development and Test Enterprise (DDTE) and Combined Federated Battle Lab (CFBL) networks.

Disparate nodes that exist typically at the bottom of the enterprise data collection paradigm were able to connect and share information including sensor description data and sensor data in real time (or near real time) in the tactical environment. All of this collected information was then funneled through the guard for distribution on the Enterprise networks (DDTE and CFBL) through a single integration point. Moreover, consuming systems, such as the ARL 3D Sensor COP and the DCGS-A MFWS were able to access and utilize the data, thus enabling analysis of sensor data and facilitating decision making based on that data at the tactical edge.

All of this coalesces to show how a properly designed and deployed Ex-PED system such as RORO can facilitate a bottom-up tactical edge approach to collection, publication, discovery and utilization of sensor data across connected networks and how this could have a direct impact on the Theme 8, "Sensing for Decision Making."