Almeria Analytics – Street Legal Industries Joint Capability Statement

August 24, 2015

Prepared by Steven Fernandez, Principal
Operational Energy and Programs Strategy
Almeria Analytics
75 Spring Rd NE
Rio Rancho, NM 87124-2561
(505) 603 4959
Fernandezsj0@aol.com
DUNS Number 079646681
Cage Number 79Y75
TIN 47-2488347

Almeria Analytics is a small Hispanic owned company

There is no GSA Schedule Contract

BACKGROUND

The Street Legal –Almeria Analytics Team owns a VERDE licensed technology (license held by Almeria Analytics) to engineer a prototype cyber secure complete spectrum Common Operating Picture (COP) including the strategy, requirements, architecture, and design specifications for Enterprise wide deployment.

Almeria Analytics (AA-SLI) has the unique background and experiences to assist with this common operating picture. During times of threat to US critical infrastructure Oak Ridge National Laboratory activates to provide data, analysis, and situation visualization across a wide spectrum of missions. To provide this fast response capability to DOE, AA-SLI and its principal that set up the original ORNL capability, has integrated a national visualization COP capability, VERDE (Visualizing Energy Resources Dynamically on Earth), to provide real time -wide-area situational awareness of the status of the electric grid both in the US and internationally. Originally developed to support ESF-12 during the North American hurricane season, it has been expanded to include non-proprietary feeds for non-federal users and for humanitarian response.

VERDE's novel approach of leveraging the commercial Google Earth® browser to display spatially and temporally tagged power system data has given traditional power utilities a new lens with which to view their system status. Output layers from VERDE analysis and modeling components, the standard Google Earth layers, and external system feeds provide further valuable spatial context, creating a dramatically more informative system view.

REQUIREMENTS DEVELOPMENT

In 2014, The Almeria Analytics principal delivered to NETCOM a Requirements document for a common operating picture to develop the impact of critical infrastructure on the core missions. This project assisted the Department of Defense by providing a prototype Common Operating Picture (COP) of the physical and cyber layers across the entire spectrum of strategic, expeditionary, joint, and combined environments for priority critical infrastructure sectors.

The U.S. Army Network Enterprise Technology Command (NETCOM) is the Army's single information technology service provider for all network communications. NETCOM plans, engineers, installs, integrates, protects, and operates the Army's LandWarNet, enabling mission command through all phases of joint, interagency, intergovernmental, and multinational operations. With the expertise of nearly 16,000 soldiers, civilians, and contractor personnel stationed around the globe, NETCOM provides support to organizations across DoD. This report summarizes the project activities of Almeria Analytics (AA-SLI) in deployed the VERDE (Visualizing Energy Resources Dynamically on Earth) platform within the NETCOM framework.

The COP strategy consolidated and documented design considerations and approaches for the full

spectrum COP requirements based on a generic test installation. The design is documented as a listing, description and justification for a common operating picture. The COP architecture is based upon the questions a commander requires for continued operation in a high-threat physical, cyber, communications environment. The detail of the system will be dependent upon comment resolution among sponsor designated performers responsible for implementation.

Distinguishing features of this COP include organization of the interdependencies of the 18 critical sectors of the National Infrastructure Plan, prioritized according to the following Critical Infrastructure sectors: Energy Sector, Communications Sector, Information Technology Sector, Emergency Services Sector, Defense Industrial Base Sector/ Government Facilities Sector,

Transportation Services Sector, Water and Waste Water Systems Sector. This documentation describes data layers to be accessed dynamically and statically, look ahead forecast models, and presentation concepts to the decision makers.

In a crisis situation, the effort that ensures all individuals and teams involved in operations or command have the same information is commonly referred to as a common operational picture (COP. The function of a COP is not to simply communicate response plans but also support an overall program. This functionality is critical to ensuring the strategic plans are effective, as well as easily understood and implemented. The results from the modeling phase can be used to document agreed-upon prevention, interdiction, mitigation, and response requirements and training needs. Maps, building diagrams, and other preplan data could be used as illustrations within the written procedures, providing more effective communication, or for training exercises.

A COP can be obtained through the use of multiple technologies and/or media synthesized on their common location element. It is important to equip a command center with as much connectivity to information sources as possible, including live news feeds, weather data, live map data, remote-sensing data, tabular data, building plans, and charts/graphs. The end user then has the opportunity to "turn on" the data needed that is relevant to the mission to create actionable information.

This report supplied NETCOM foundational documentation for the COP needed to deploy an existing COP capability on NETCOM's operational network for pilot demonstration. Almeria Analytics (AA-SLI) used VERDE lessons learned to design and suggest a first prototype of a full spectrum Common Operating Picture (COP) including the strategy, requirements, architecture, and design. The vision of this COP is to monitor in real time the Supervisory Control and Data Acquisition (SCADA) systems, Power Grids, Spectrum, Network, Continuous mapping of the Network, Network Operations (NETOPS) tools, etc. The Army can then use the ingest engine to gather the data and parse it into different buckets and display visually the information the commander requires for actionable decisions.

PROTOTYPE EVALUATION AT ACOIC

In 2014, following this assessment, SLI principals then at Oak Ridge National Laboratory provided

US Army NETCOM foundational documentation for VERDE and COP. The COP vision is to monitor in real time the Supervisory Control and Data Acquisition (SCADA) systems, SLI has since updated its design of a transformation version of VERDE (DoD VERDE), so that the DoD can use the ingest engine to gather the system status and external threat data and parse it into different analytics and display threats to the physical infrastructure in real time. This prototype will include behavioral models as well as physical models to extend the COP into cyber battle space. The SLI technical objective is to give DOD/U.S. Army leadership a view of the cyber battle space within the physical layer to support decision-making and efficient energy management.

A legacy version of VERDE was installed at the Army Cyber Operation Integration Center

(ACOIC) and placed into beneficial use. In addition new features and modifications were suggested making this system deployable Enterprise wide. Output layers from VERDE analysis and modeling components were integrated through the DAGGER tool to trigger the other tools within the Army Cyber Analytics Laboratory to the other Constellation tools.

Functional testing was completed at the Army Cyberspace Operations Integration Center (ACOIC) at the Army Research Laboratory (ARL) in a single phase on May 16, 2014. All aspects of VERDE passed the tests except for three which were traced to inadequate training. Improved training procedures were subsequently instituted and placed in the VERDE user manual.

CAPSTONE EXERCISE JULY 14-16, 2014

As the ultimate exercise to the NETCOM Futures VERDE project, a Capstone exercise was conducted July 14-16 2014. The premise of the exercise was maintenance of operations at the USMA during a SQL injection in the aftermath of a Hurricane Irene similar event damaging the external power grid. The constellation partners integrated VERDE into the flow of information the constellation used to hunt the exploit. VERDE was well received by the Army observers.

As the ultimate exercise to the NETCOM Futures VERDE project a Capstone exercise was conducted July 14-16 2014. Senior Observing Officials include:

- Lt. Gen. Edward C. Cardon, Army Cyber Command/2d U.S. Army commanding general,
- Brig. Gen. John B. Morrison, Jr., Commanding General of the Army Network Enterprise Technology Command at Fort Huachuca, Ariz.
- Brig. Gen. Paul M. Nakasone, Director, Army Cyber Operations Integration Center/G-3, Second Army/U.S. Army Cyber Command, Fort Belvoir, Va
- Brig. General Patricia Frost, Deputy Commander (Operations), U.S. Army Cyber Command, Fort Belvoir, Va.
- Mr. Daniel Q. Bradford, Deputy to the NETCOM commander and senior technical director and chief engineer of the command. Bradford has the equivalent rank of a Brigadier General.

- Colonel Randy Taylor serves as the Chief Information Officer and J6 for the United States Southern Command (SOUTHCOM).

The Commanding General Officers received demonstrations on Tuesday and Senior O6 and SMEs from NSA and DISA were demonstrated on Wednesday. Overall, 25 senior officials from DISA, NSA, Army CyberCom and RDECOM attended the exercise.

The VERDE system performed flawlessly during two live presentations Monday to the CPT team and to ARL personnel. No issues were identified. During the Monday demonstrations we identified that there was a 30-50% chance of the ACAL losing power during the night which had a high probability of corrupting the demonstration data. A decision was made to power down the cluster based on VERDE predictive analytics.

COL Robert McVay, Program Executive Office for Enterprise Information Systems, PEO-EIS, stated during the hot wash that the only critical analytic was the VERDE system. LT COL Stanton re-iterated that this was the only real evaluation that mattered in the final analysis.

The separate evaluation by CPT 150 provided some development suggestions for follow-on work. During the conduct of the evaluation it was the intention to have VERDE play a role during the time between 1 Jan 2014 and 1 May 2014 by introducing a hurricane event on the East Coast. The hurricane event was inserted in Dagger dated 30 April 2014 and caused the Dagger screen to flash red for the next three days through May 2nd. The CPT was supposed to be able to see indicators of this event in Dagger and then reference VERDE for more information. The assigned CPT member was shown how the Dagger dashboard essentially flashed the cascading outages as the signature to be looking for and the Hurricane Irene folder location where the exercise file was located within VERDE. However, during the exercise the CPT was unable to identify in Dagger any specific event from VERDE or failed to access the exercise file instead of the current conditions. Based on this mismatch in performance, we developed the following lessons:

1. The AA-SLI team validated Dagger was correctly reading the VERDE alerts and passing the vulnerability through the other layers.

2. VERDE has been used in other exercises as the platform that other links simultaneously show up in both places. So perhaps having a DAGGER screen that shows up similar to the stream gauge plots might provide the better way to link the two tools together.

3. Additional training for the CPT would have solved the issue, but also we should revise our training documents.

4. Future exercises should use a wild card for large weather events.

As a result of this project, it has been shown that VERDE can provide NETCOM with a valuable tool for visualizing the physical layers related to mission operations. It allows a real-time COP to

be created and shared across the command. By using the commodity Google Earth platform for viewing, installation issues are minimized. VERDE is extensible allowing additional layers and infrastructure to be displayed. The VERDE analytic modules provide situational awareness of asset conditions, threat conditions, projected impact, and recovery estimates all in a single package. Overall, senior leadership was impressed with the demonstrated capability.

SUMMARY CAPABILITY

1. The VERDE decision tool had a scoring mechanism and methodology to benchmark the energy security assessment and integrate those scores to the DAGGER assessment tool.
2. The look ahead models are integrated to provide those scores based upon scenarios for the organizations core missions.
3. The repeatable, standardized methodology is documented in manuals and training to be implemented consistently across organizations.
4. Operational ways to develop scenarios and courses of action exist within the VERDE lessons learned.

Recent and Relevant Contracts

Almeria Analytics has no recent and relevant contracts. However, the Principal at Almeria Analytics was the Principal Investigator for an Oak Ridge National Laboratory contract for FY2014 with the scope described in the summary of capability. NETCOM, Dr David Bradford was the point of contact. The value of the contract was $400,000.