Memorandum

From: Craig Miller (PI) and Robert Larmouth (PM)

To: Carol Hawk, James Briones

Re: Analysis and Discussion in support of recommendation of the finding that the final Go/No-Go milestone on the Essence project (DE-OE0000684) has been met

Date: 4 December 2015

The Essence project is progressing according the plan and schedule established in the Project Management Plan and Statement of Project Objectives. Per the plans, the team have been working on improvements to the software as deployed in the first field test (Release 1, June 2015) and should be at the point of having the second, more complete version of the system (Release 2) ready for a second, more challenging field test. Release 2 extends the functionality of Essence Release 1 and addresses deficiencies identified in the first round of testing. The decision on whether to proceed (the Go/No-Go decision G6 associated with the final milestone M11), is based on the determination of whether the Release 2:

1. successfully addresses the deficiencies in the first release,
2. is feature complete per the plan’s design,
3. is relevant and useful in extending the cyber security capabilities of electric utilities, and
4. is technically ready for field testing.

During the past two weeks we have conducted a detailed review of the current system to determine whether we are sufficiently confident in the system and ongoing development to proceed to schedule the next utility field-test in mid-January. The final preparatory review was conducted on 2 December. Two deficiencies were noted and some areas where further improvements should be made were identified. While the system was not complete, the team agreed that the critical work can be completed by 15 December, and have set that date as the deadline to be feature complete and to cease work on new functionality. This will allow about 30 days for more internal and laboratory testing before the field test.

Based on this review, we believe that the essential criteria have been met and that we should proceed. The basis for this conclusion is reviewed below, but first we offer some observations on the project, Essence, and reactive cyber security in general.

The concept for Essence was tightly defined at the outset of the project. We had a definite idea of the product. In the course of the project, however, we have explored the value and concept of reactive cyber security based on AI-driven anomaly detection. This has led to an expanded and refined vision. Release 2 meets the original requirements but the team have identified several areas for extension and improvement that we have not yet implemented and cannot be addressed until after the project is completed.

More fundamentally, the project has solidly confirmed the value of anomaly based detection for utilities. Since the start of the project, research by Mandiant has shown that there is an exceptionally long period from initial cyber penetration of a system until detection and the start of remediation. The most recent data indicate that this period is slightly in excess of 200 days. The length of this period is indicative of the residual weakness of current protection and detection methods and the exceptional potential for improving cyber security overall by shortening the interval to detection The potential gain in reducing the time to detect is far greater than the potential for improvement in the other methods such as perimeter detection which are more fully developed.

What has also become clear is that electric utility operation offers a huge *advantage* in building cyber security systems versus general purpose business or control networks. In general discussion there is much correct emphasis on the vulnerability of utility systems, but there is less recognition of their inherent strength. Electric utilities have definite patterns to their communications. Meter readings, for example, are usually metronomic with meter readings at predetermined intervals – every 15 minutes, every hour, every day, etc. Further, communication between devices frequently use tightly documented protocols such as MultiSpeak®, and values within the messages tend to have well defined ranges and consistent values. Voltages are almost always in the ANSII band, for example, and monthly bills for a meter usually vary within a narrow range, seasonally adjusted. These patterns provide a solid basis for machine learning. It is easy to detect deviations from the norms which may indicate a technical or cyber problem. General purpose cyber systems do not take advantage of the special, highly-constrained nature of utility communications and operations. We are making use of this regularity in Essence which is precisely targeted at reducing time to detection.

# The Five Layer Abstraction Model

The assessment of progress and the state of Essence system will be discussed in terms of the basic five layer abstraction model that underlies its design. Essence is built in five layers, as illustrated in the figure below. This structure is described in detail in earlier documents, but a brief reprise is provided here to provide context for the discussion of progress.

|  |
| --- |
|  |
| Essence Abstraction Model |

Essence is built from the bottom up. The first step is collection of raw data (the Data Layer). Essence is designed to collect data in transit, in parallel to the operational system, so that Essence cannot interfere with utility operations or present another attack surface. The second layer (the Information Layer) organizes and structures the information for provision to analytical tools (Analysis Layer) that employ different methods for anomaly detection. The concept is that additional tools can be developed and “plugged into” the Essence structure at low cost, taking advantage of an open interface to the Data and Information Layers. The final two layers (Decision and Action Layers) support the operators’ decision on how to deal with a detected anomaly and implement that decision.

The assessment will compare the state of Release 1 and Release 2 by layer.

# Release 2 Improvements by Data Layer

## Data Layer

The data layer collects the raw data. The concept in Release 1 was to collect data through a dedicated device. A custom device was constructed which created a port which replicated the flow of data across a network cable. The device provides isolation from the utility network by means of an optical data diode.

In the June test, the team determined that the device was not sufficient in itself for data collection. Utilities commonly employ virtualization software. A physical device obviously cannot collect data from a virtual system. Software was developed to provide collection from SPAN ports and a virtual SPAN port that provides connection to VMWare. This extension of capability constitutes the Release 2 improvement to Essence. Given the urgent need for these capabilities, they were developed during the first field test, and have been tested extensively.

**Improvements in Release 2:**

**Data collection from SPAN port and implementation of virtual SPAN port**

**Work required before field test:**

**None**

# Information Layer

In the development of the first release, the team evaluated several database options. The critical criteria were that the database be:

1. Open source,
2. Optionally distributed, and
3. Very fast.

An initial calculation showed that the potential flow of data in a future utility with extensive deployment of advanced meters, phasor measurement units, and other sensors could reach a level that would stress non-distributed, SQL databases, leading to the investigation of higher performance options. The team identified Cassandra as the best option. See [www.Cassandra.apache.org](http://www.Cassandra.apache.org). An advanced, multi-technology, dynamically reconfiguring database concept was developed and described in an earlier Essence document, but the team decided not to proceed with implementation as a straightforward implementation of Cassandra proved abundantly sufficient for the expected data flows. There have been no database performance issues in testing.

Cassandra is widely used at an extremely large scale. Apple, for example, operates a 75,000 node system for its cloud services. Netflix also uses Cassandra. We believe that there is no foreseeable need to develop fundamental database technologies or architectures for utility applications. The Data Layer of Release 2 is little different from Release 1 with the exception that it has been extended to integrate data from multiple sources to accommodate the changes to Layer 1, and an interface was written to feed data to the machine learning engine. Data from different sources are integrated based on the time of primary collection. We expect some additional work over the next month to accelerate the feed to the AI application, but the current version of Layer 2 meets all requirements.

**Improvements in Release 2:**

**Integrate data from multiple sources, interface to machine learning application, extension to the data model to include support for Layers 4 and 5.**

**Work required before field test:**

**Performance improvements in the feed of data to the machine learning engine. The system is fast enough for current scale utility applications, but could be improved.**

## Analysis Layer

The analysis layer in Release 1 mapped the network and detected changes and also included a “rules engine” that allowed users to specify tests on message origin, destination, message frequency, and content. These tests allowed deep-packet inspection so that tests could examine the values in messages as well as structure and routing. Release 1 did not include the machine learning anomaly detection application, as this could not be developed until sufficient data was collected in the first field test.

Substantial improvements were made in Release 2. The user interface to the rules engine was improved. The network mapping software was more closely integrated into the overall framework. In particular, anomalies detected by the rules engine or the AI engine can be displayed on the network screen and the underlying data (addresses, type of error, root cause, prior remediation …) can be queried. The AI engine, which develops models of normal behavior, was added as the third application.

**Improvements in Release 2:**

1. **Improved user interface to the rules engine**
2. **Improved network mapping display**
3. **Integration of rules and AI anomaly detection modules to display results through the network mapping display**
4. **Extension of network mapping display to allow query of underlying details of node or link**
5. **Implementation of machine learning capability**
6. **Integration of machine learning anomaly engine with overall framework**

**Work required before field test:**

**Minor improvements to display of anomalies in network mapping display. This will be completed, without risk, by 15 December.**

## Decision Layer

Release 1 relied on manual processes for remediation. Layer 4 was not automated.

Release 2 includes Decision Layer functionality to:

1. allow annotation of remediative strategy,
2. labeling severity of anomalies
3. offering of software defined networking (SDN) options if available such as shutting down a link or node,
4. determine if the anomaly was a new problem or one seen earlier,
5. retrieval of notes on remediation from prior similar events.

**Improvements in Release 2:**

**Listed above**

**Work required before field test:**

**None**

## Action Layer

Release 1 did not have an automated Action Layer.

Release 2 has elements of an Action Layer. Specifically, if the system being monitored has software defined networking (SDN) capable components that support the OpenDaylight™ standard, Essence will offer options to enable or shut down a link or node and block or temporarily quarantine data. This capability has been implemented but not developed to the extent originally envisioned. The problem is that few such components are available; the OpenDaylight™ standard is immature. Documentation is poor and sometimes inaccurate and much of the available software does not work as specified and cannot be readily implemented. The development of this layer has taken longer and cost more than originally estimated due to severe technical complications. Further development is not currently practical and further efforts in this area should not be undertaken until OpenDaylight™ is more mature and proven or another SDN system reaches sufficient stability and functionality. Despite the challenges, Release 2 does have an SDN management capability, but deployment could be problematic due to the scarcity of available SDN components and the likelihood that these components do not conform to a tight standard.

**Improvements in Release 2:**

**Implementation of basic SDN management capability using OpenDaylight™**

**Work required before field test:**

**None**

Overall, the team does not see any barriers to the next field test.

# Assessment of Progress vs. Plan Post the First Field Test

Immediately after the first field test, the team met to plan the developments leading to Release 2. The text below is a copy of the memorandum that the management developed to shape Release 2 development at a high level. This maps to the task list in the updated design document which was submitted to DOE.

|  |
| --- |
| 1. Deepen the connection between the rules engine and the network graphing engine. Display the rules when you click on a link, show the rules and, if possible, allow the editing and creation of the rules. 2. Improve the annotation of connections. Allow user to create, retrieve, and edit a notes field 3. Demonstrate a rule based on deep packet data, E.g. a meter reading that is too high or low 4. Build Layer 4. Provide a screen to act on and analyze an alert    1. Display information    2. Determine if this is new or prior    3. Update log    4. If not new, retrieve notes from prior instances, offer the user the same action, or provide notes field to describe a different response    5. If new, offer new notes field    6. Offer SDN action if available    7. Optionally export a description of what was found and action taken 5. On SDN –    1. get ability to shut down link or IP address going    2. provide option to take SDN action as part of Layer 4    3. Update remediation log when SDN is initiated    4. Provide option to embargo and store data rather than shut down link    5. Provide option to restore IP address or connection after problem is solved    6. Prepare a narrative and demonstration of the SDN capability 6. Test, demonstrate, and integrate the AI engine |

The notes in the earlier section indicate how each of these has been achieved. All technical objectives scheduled for this point in the project have been achieved, with the exception that the capability for control of software defined networking capable components is limited by deficiencies of the commercially available hardware and software.