RESEARCH PERFORMANCE PROGRESS REPORT

Energy Sector Security through a System for Intelligent,

Learning Network Configuration Monitoring and Management

National Rural Electric Cooperative Association

Cooperative Research Network



Federal Agency: United States Department of Energy

Identifying Number: DE-OE0000684

Contents

[1. DATA ELEMENTS 4](#_Toc433888654)

[2. ACCOMPLISHMENTS 5](#_Toc433888655)

[2a Major goals of the project 5](#_Toc433888656)

[2b What was accomplished under these goals? 8](#_Toc433888657)

[Accomplishments of Task 1 – Project Management 8](#_Toc433888658)

[Accomplishments of Task 2 – High Level Design 9](#_Toc433888659)

[Accomplishments of Task 3 – Component Design 9](#_Toc433888660)

[Accomplishments of Task 4 – Network System Design 10](#_Toc433888661)

[Accomplishments of Task 5 – Laboratory Testing 10](#_Toc433888662)

[Accomplishments of Task 6 – Field testing 11](#_Toc433888663)

[Accomplishments of Task 7 – Commercialization 12](#_Toc433888664)

[Summary of Accomplishments for the Reporting Period 12](#_Toc433888665)

[2c What opportunities for training and professional development has the project provided? 12](#_Toc433888666)

[2d How have the results been disseminated to communities of interest? 12](#_Toc433888667)

[3. PRODUCTS 13](#_Toc433888668)

[3a Publications, conference papers, and presentations 13](#_Toc433888669)

[3b Websites or other Internet sites 13](#_Toc433888670)

[As noted previously, the team does not plan to publish externally until after Cycle 2 testing and engagement with a commercialization partner. 13](#_Toc433888671)

[3c Technologies or techniques 13](#_Toc433888672)

[3d Inventions, patent applications, and/or licenses 13](#_Toc433888673)

[3e Other products 13](#_Toc433888674)

[4. PARTICIPANTS & OTHER COLLABORATING ORGANIZATIONS: 14](#_Toc433888675)

[4a What Individuals have worked on the project? 14](#_Toc433888676)

[4b Other organizations involved as partners 15](#_Toc433888677)

[4c Have other collaborators or contacts been involved? 16](#_Toc433888678)

[5. IMPACT 16](#_Toc433888679)

[5a Impact on the development of the principal discipline(s) of the project 16](#_Toc433888680)

[5b Impact on other disciplines 17](#_Toc433888681)

[5c Impact on the development of human resources 17](#_Toc433888682)

[5d Impact on physical, institutional, and information resources that form infrastructure 17](#_Toc433888683)

[5e Impact on technology transfer 17](#_Toc433888684)

[5f Impact on society beyond science and technology 17](#_Toc433888685)

[5g What dollar amount of the award’s budget is being spent in foreign countries? 17](#_Toc433888686)

[6. CHANGES/PROBLEMS 17](#_Toc433888687)

[6a Changes in approach and reasons for change 17](#_Toc433888688)

[6b Actual or anticipated problems or delays and actions or plans to resolve them 18](#_Toc433888689)

[6c Changes that have a significant impact on expenditures 18](#_Toc433888690)

[6d Significant changes in use or care of human subjects, vertebrate animals, and/or Biohazards 18](#_Toc433888691)

[6e Change of primary performance site location from that originally proposed 18](#_Toc433888692)

[7. SPECIAL REPORTING REQUIREMENTS 18](#_Toc433888693)

[8. BUDGETARY INFORMATION 18](#_Toc433888694)

[APPENDIX A 19](#_Toc433888695)

[Essence Network Dashboard Examples 19](#_Toc433888696)

RESEARCH PERFORMANCE PROGRESS REPORT

# 1. DATA ELEMENTS

Federal Agency: United States Department of Energy

Identifying Number: DE-OE0000684

Project Title: Energy Sector Security through a System for Intelligent, Learning Network Configuration Monitoring and Management (“Essence”)

Project Manager: Robert Larmouth

Email: [robert.larmouth-contractor@nreca.coop](mailto:robert.larmouth-contractor@nreca.coop)

Phone: 603-930-9199

Principal Investigator: Dr. Craig Miller

Email: [craig.miller@nreca.coop](mailto:craig.miller@nreca.coop)

Phone: 703-626-9683

Submission Date: October 30, 2015

DUNS Number: 045497427

Recipient Organization: National Rural Electric Cooperative Association

Address: 4301 Wilson Boulevard

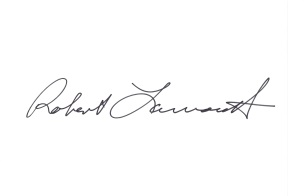
Arlington, VA 22203-1860

Grant Period: October 1, 2013 through April 30, 2016

Reporting Period End Date: September 30, 2015

Report Term or Frequency: Quarterly

Signature of Submitting Official:



Robert Larmouth

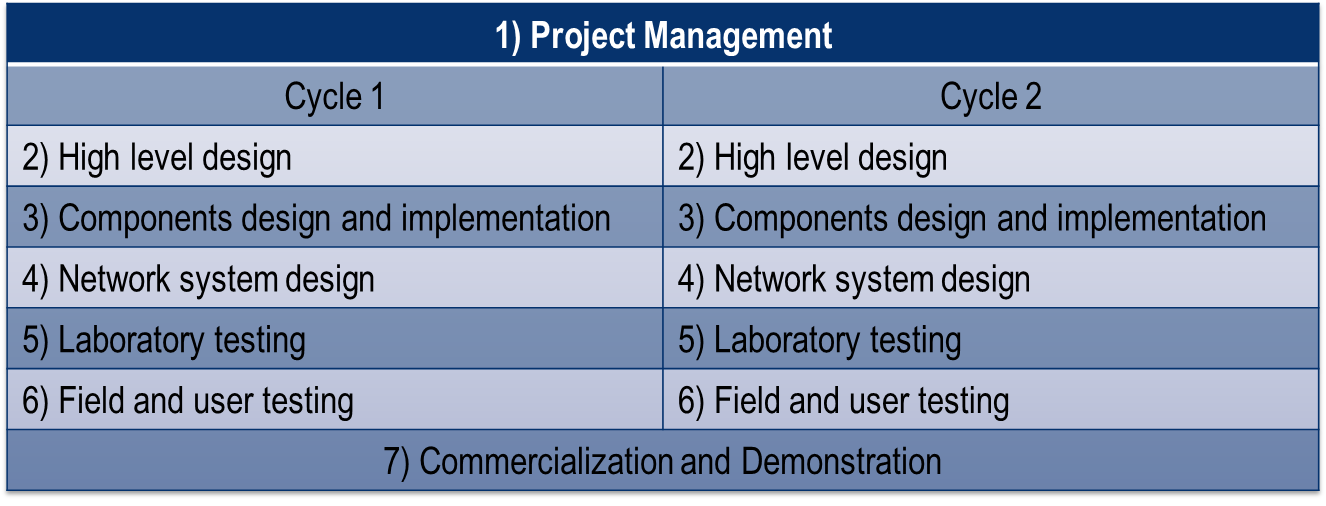
# 2. ACCOMPLISHMENTS

## 2a Major goals of the project

There are several important goals of this project, including development of the following capabilities:

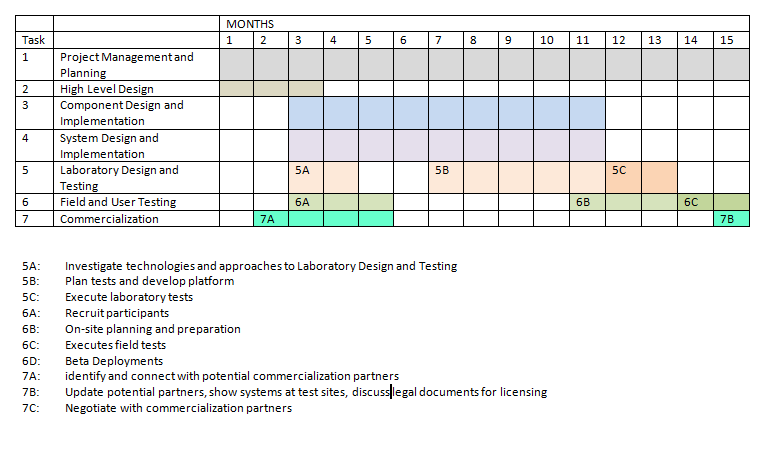
* A capability to establish, maintain, and monitor an alignment between OT security policy and network configuration and settings
* A capability to detect and prevent potentially malicious traffic flows within an electric utility’s operational network, by creating protocol-specific (e.g., specific to MultiSpeakTM, DNP3), semantically rich, and context-aware filtering rules to identify disallowed or anomalous traffic patterns.
* A capability to enable an electric utility to define and enforce its operational network security policies with fewer IT staff members and less reliance on significant internal security expertise.
* A capability to align an electric utility’s operational network security management with the broader trends of software-defined networking, virtualization, and the ongoing migration of utility IT and operational systems into the cloud environment (where they can be provided as a managed service). This alignment is particularly important for smaller electric utilities that have limited IT staffs and capabilities.
* A capability to simplify functions such as security reporting and compliance as they relate to an electric utility’s operational network assets and traffic flows.

To achieve these goals, the Project Management Plan defines seven (7) major tasks as summarized below:

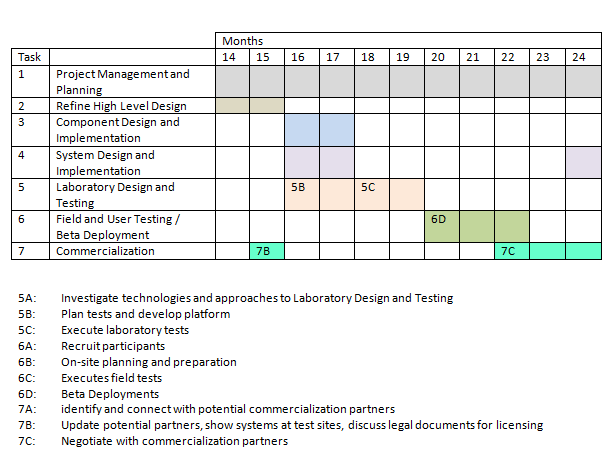


Tasks 2 through 6 will be executed twice – first in a prototype cycle and second through a refinement cycle that benefits from the testing and analysis conducted in the first cycle. The timeline for these tasks (from the Project Management Plan) is shown below.

Cycle 1 Schedule



Cycle 2 Schedule



As of September 30, 2015, no significant changes were made regarding the tasks and associated schedule. A project briefing was held at DOE offices in September. As shown below in the task status, work is essentially on schedule.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CYCLE 1: PROTOTYPE DEVELOPMENT** | | | | |  |
| **Task**  **No.** | **Task** | **START**  **(week)** | **END**  **(week)** | **DURATION**  **(weeks)** | **Status as of Sept 30, 2015** |
| **1** | Project Management and Planning | 0 | 130 | 130 | Ongoing |
| **2** | High-Level Design | 2 | 11 | 9 | 100% |
| **3** | Component Design and Implementation | 12 | 49 | 37 | 100% |
| **4** | Network System Design | 12 | 49 | 37 | 100% |
| **5** | Laboratory Testing | 48 | 66 | 18 | 100% |
| **6** | Field and User Testing | 56 | 67 | 11 | 100% |
| **CYCLE 2: REFINEMENT AND COMMERCIALIZATION** | | | | |  |
| **2** | Refine High-Level Design | 68 | 88 | 20 | 100% |
| **3** | Refine Component Design And Implement | 68 | 88 | 20 | 95% |
| **4** | Refine System Design and Implement Changes | 88 | 102 | 14 | 85% |
| **5** | Laboratory Testing | 102 | 106 | 4 | Ongoing |
| **6** | Refined Field and User Testing | 106 | 114 | 8 | Not started |
| **7** | Commercialization | 84 | 122 | 38 | Ongoing |

The Project Management Plan (previously submitted file “CurrentPMP.docx”) lists fourteen (14) milestones, six (6) of which are go/no-go decisions as shown in the following table:

|  |  |  |
| --- | --- | --- |
| **When (week)** | **Milestone** | **Go/No-go Decision?** |
| **11** | M3: Prototype Design Complete and meets objectives | Complete |
| **67** | M6: Utilities successfully recruited and ready for field testing | Complete |
| **67** | M6: Lab testing completed and meets objectives of first design | Complete |
| **79** | M7: Field testing complete and results meet objectives | Complete |
| **88** | M8: Cycle 2 design complete and meets objectives | Complete |
| **114** | M11: Testing of Cycle 2 design complete and meets objectives to proceed to field testing | Underway |

The task progress status shown above should support the Milestone plans. The Cycle 2 lab testing is proceeding in concert with the integration and development efforts.

## 2b What was accomplished under these goals?

The major accomplishments during this period include the following:

* Completed and delivered the Cycle 2 Design Document
* Implemented 2-step anomaly detection as part of the machine learning integration
* Demonstrated functionality of the annotated network graph
* Successfully implemented Action Layer (Layer 5) connection to OpenDaylight for software defined network control
* Improved capability to generate large virtual networks for testing
* Demonstrated Cycle 2 integration via briefing at DOE

These and other accomplishments are described in greater detail in the following sections of the report.

### Accomplishments of Task 1 – Project Management

The entire team continues to hold weekly conference calls and Webex demos as well as specific discussions on tasks. As an example of the latter, a working meeting was conducted with Cigitial, CMU and NRECA personnel to develop the detailed plans for integrating the machine learning component into the Essence framework. As a result of the team’s agile development approach and the continuous refinement of tasks, certain work was shifted among team members, along with the corresponding budget resources. Overall, the project remains on budget and no major concerns were identified regarding the PMP.

### Accomplishments of Task 2 – High Level Design

This task (Cycle 1) was completed previously. However, the 5-layer abstraction model developed as a part of that task continues to evolve and be used as the architectural model for work on all tasks. For reference, the 5-layer model is reprised below:

Data

Information

Analysis

Decision

Action

This overarching model continues to be enhanced through:

* Revised anomaly submission and retrieval API
* Active Directory support for network data enrichment and operational impact from Decision and Action layers
* Identification of requirements for enhanced captured data to provide support for broader set of protocols

### Accomplishments of Task 3 – Component Design

During this quarter, the team focused on integrating its machine learning software with the rest of the system. CMU worked with Cigital to design the REST API for interacting with the databases and the front-end. Together the team produced a PDF document to describe the API and document the expected usage. They then implemented code using this specification.  
  
Using this new API, the machine learning component can now perform a two-step anomaly detection. In the first step, the Cassandra database is queried for the latest packet information. For any anomalies that are detected, the Essence REST API is then queried for the previous anomaly information. Specifically, the purpose is to generate user annotations describing the causes of the previous anomalies. Using this information, the second step attempts to predict the causes of the new anomalies. This prediction is intended as a guide for the user who is triaging the anomaly and obviously is not suggesting definitive claims about the cause. Whether or not a prediction can be generated, the anomaly information is sent to Essence via the REST API. The newly submitted anomalies immediately appear in the Essence UI.

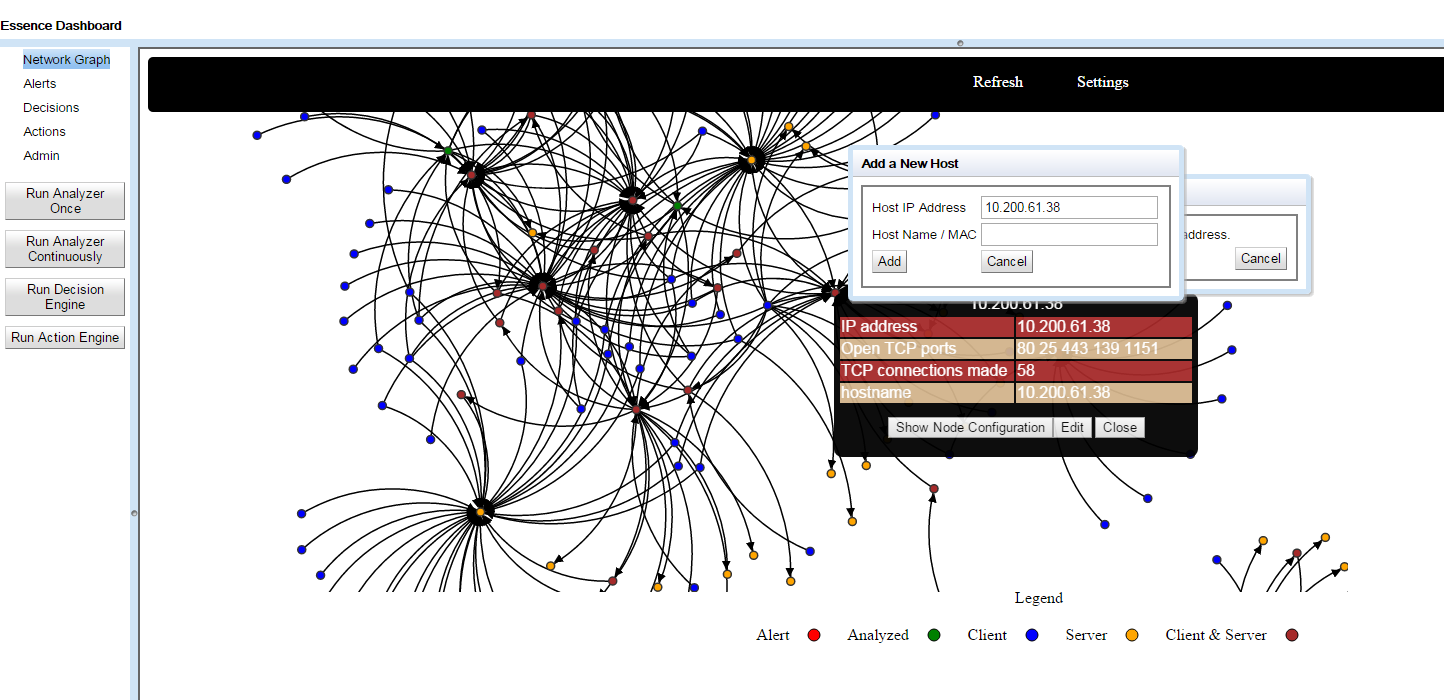
The unsupervised machine learning components have now been integrated into the Essence system. The integration of supervised learning components will be completed early in the next quarter.

The team continues to refine and insert functionality components into Essence including the following:

* Built an integrated Essence dashboard
* Integrated Opendaylight’s SDN controller into Essence
* Implemented faster Multispeak™ packet capturing tools
* Replayed coop datasets to fix software bugs
* Designed infrastructure for full scale network topology simulation in MiniNet.

### Accomplishments of Task 4 – Network System Design

The team has made significant progress in developing and refining the Essence Network Dashboard. One example of the resulting integrated user interface is shown below - this illustration is the “add a new host” function. Additional illustrations are included in the appendix.

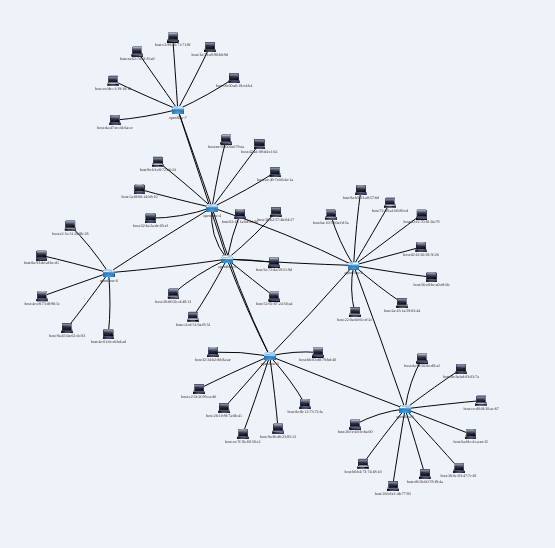


### 

### Accomplishments of Task 5 – Laboratory Testing

All software related to the synthetic generation and capture of MultiSpeaker network traffic (I.e. MultiSpeaker and listener.py) using the Python module, Mininet, has been installed and tested in a single virtual machine.  This virtual machine has been exported in Open Virtualization Format so that it may be imported into many common virtual machine managers, including VirtualBox or VMWare.  The resulting OVF file is approximately 6GB.  By capturing all of this software and its related dependencies and configurations in one location, it makes the use of MultiSpeaker much easier for researchers and developers to generate and export network packet captures (I.e. PCAP files) of the MultiSpeak™ protocol. The OVF files are accessed by the Essence team via a shared Amazon EC2 project server.

The MiniNet testing on virtual networks is typically done on a small network to remain agile and accelerate development work. However, to address scalability, the team built a large network for testing; this network is representative of one of NRECA’s larger cooperative utilities. To do this, the team wrote a large network generator that uses a bounded random number generator.   In this way the team can generate many different large scale networks for very rich testing.    The illustration below is one of the current test networks.    This is on the smaller end, but is not much different than what one would see at a 5,000 meter cooperative or municipal utility.



### Accomplishments of Task 6 – Field testing

There was no field testing work scheduled for the past quarter. Cycle 2 field testing will commence in late December or early January. As in Cycle 1, the goal is to test at more than one utility in preparation for the full demonstration later in January or early February. The team has received informal commitments from one large cooperative utility and one investor-owned utility to host the full demonstration.

### Accomplishments of Task 7 – Commercialization

Discussions with General Electric and Intel have been previously discussed and are ongoing. The team believes that Intel’s contribution, at the least, can be the application of their expertise in user interfaces for commercial products. In November, the team is planning to meet with Southeastern Data Cooperative to discuss a potential product strategy.

The team has started to develop an outline of the commercialization strategy. The underlying premise is that the plan must define the path to a marketable, packaged product – not just specifications or standards. This task will ramp up at year’s end and continue through Q1 of 2016.

### Summary of Accomplishments for the Reporting Period

Major Activities:

* Weekly communication, demos and quarterly team meeting
* Machine learning integration
* Layer 4/5 functionality and integration
* Cycle 2 high level design completion and submission
* Essence Network Dashboard development
* Large network generation tool refinement

Specific Objectives:

* Refine Cycle 2 integration for field testing
* Develop outline for commercialization
* Finalize software code

Significant Results:

* Cycle 2 functionality demonstration
* Integrated user interface

Key Outcomes:

* Project status briefing at DOE
* NRECA management buy-in to commercialization strategy
* Project schedule management to ensure that no significant delays occur as a result of refinements

## 2c What opportunities for training and professional development has the project provided?

The project and product are not sufficiently advanced for use in training.

## 2d How have the results been disseminated to communities of interest?

Information is continuously updated for ongoing communication with the NRECA cooperative community. Also, please see section 3a.

# 3. PRODUCTS

## 3a Publications, conference papers, and presentations

As planned, Craig Miller (PI) continued an active speaking schedule during the past quarter. His engagements specifically related to the Essence project included:

1. Demonstration and integration discussion with Intel, 4,5 August
2. Southeastern Data Cooperative CEO User Conference. Live demo and briefing for 72 Co-op CEOs, 10 August
3. Duke Power, live demo and briefing, 14 August
4. Major presentation to EPRI membership planned for 6 October.
5. One on one discussion with SEDC regarding commercialization (12 Sept), with due diligence scheduled for November
6. Renewed early stage discussion with General Electric
7. Discussion in late September with San Diego Gas and Electric re testing and demonstration
8. Article on Essence in the October issue of RE Magazine.

## 3b Websites or other Internet sites

At this stage the project is focusing on live, in-person discussions rather than general web presentations as the team is seeking feedback and input. The only web discussion is in the online version of RE magazine and Cooperative.Com. The article was picked up by T&D magazine on line.

## As noted previously, the team does not plan to publish externally until after Cycle 2 testing and engagement with a commercialization partner.

## 3c Technologies or techniques

* MultiSpeaker software
* Virtual appliance operation
* Annotated network graph
* Software defined networks
* Large network generator

## 3d Inventions, patent applications, and/or licenses

The patent and licensing strategy remains unchanged; however, schedule conflicts delayed the start of the patent preparation. This had been planned for Q3, but cannot start until November. The team realizes that this cannot be delayed further, as it will be an element of commercialization plans.

## 3e Other products

All work products to date are listed above.

# 4. PARTICIPANTS & OTHER COLLABORATING ORGANIZATIONS:

## 4a What Individuals have worked on the project?

For all individuals listed, there has been no collaboration with individuals in foreign countries and no foreign travel. The following information reflects activity for the period July 1 through September 30. The activity is expressed as an annualized rate where 12 person-months = full time.

Name: Robert Larmouth – NRECA

Role: Project Manager

Person-months: 2

Contribution: Direction of teams, schedules and reporting

Funding source(s): DOE and NRECA

Name: Craig Miller – NRECA

Role: Principal Investigator

Person-months: 3

Contribution: Technical direction, outreach, database

Funding source(s): DOE and NRECA

Name: Maurice Martin - NRECA

Role: Liaison Team Leader

Person-months: 1

Contribution: Outreach to electric utility co-ops

Funding source(s): DOE and NRECA

Name: Nikhil Singh - NRECA

Role: Software Engineer

Person-months: 9

Contribution: Decision/action development

Funding source(s): DOE and NRECA

Name: Evgeny Lebanidze - Cigital

Role: Development Team Leader

Person-months: 1

Contribution: Direction of the high level design team

Funding source(s): DOE

Name: Chandu Ketkar - Cigital

Role: Chief Technologist

Person-months: 0

Contribution: End-to-end solution design

Funding source(s): DOE

Name: Ping Ning - Cigital

Role: Senior Architect

Person-months: 1

Contribution: Network design

Funding source(s): DOE

Name: Bob Wintemberg - Cigital

Role: Associate Consultant

Person-months: 11

Contribution: Network design

Funding source(s): DOE

Name: Andre Joseph - Cigital

Role: Security Analyst

Person-months: 10

Contribution: Network design/testing/team lead

Funding source(s): DOE

Name: Terrence Wong - CMU

Role: Senior Research Programmer

Person-months: 8

Contribution: Software development

Funding source(s): DOE

Name: Zico Kolter - CMU

Role: Machine Learning Engineer

Person-months: 3

Contribution: Machine learning algorithm development

Funding source(s): DOE

Name: Will Hutton - PNNL

Role: Test development

Person-months: 1

Contribution: Data sets for learning algorithm, methods for passive data collection

Funding source(s): DOE through PNNL

Name: Lance Irvine - PNNL

Role: Technical Contributor

Person-months: 1

Contribution: Software development

Funding source(s): DOE through PNNL

## 4b Other organizations involved as partners

The participating organizations are those listed in the Project Management Plan previously submitted. These “core team” organizations are:

* Cigital
* Pacific Northwest National Laboratory
* Carnegie Mellon University
* Honeywell, Inc.

The following electric utility cooperatives have been in communication with the team, expressing interest and/or offering participation: (two utilities added since last report)

* Great River Energy, Maple Grove, MN
* Rappahannock REC, VA
* Laurens Electric (SC)
* Southwest Transmission Cooperative (AZ)
* Vermont Electric (VT)
* Wake Electric (NC)
* Platte Clay EC (MO)
* Navopache EC (AZ)
* Central Alabama (AL)
* Boone EC (MO)
* San Bernard EC (TX)
* Southwest Mississippi EPA (MS)
* San Diego Gas and Electric
* Duke Power

The following companies have expressed interest in becoming industry partners in the project and have also provided insight from a commercial perspective: (no change since last report)

* Intel / McAfee
* General Electric
* IBM

## 4c Have other collaborators or contacts been involved?

All collaborators to date, engaged and potential, are listed above.

# 5. IMPACT

## 5a Impact on the development of the principal discipline(s) of the project

As reported previously, the targeted area of impact is the electric utility sector, especially that segment characterized by the hundreds of small utility cooperatives spread across the United States. The impact is expected to be significant improvement in the resistance of utilities’ networks to cyber attacks. Examples include but are not limited to:

* Open source tools and/or “devices” that can be integrated into the utility’s network
* Improved utility staff awareness of industry standards for cyber security
* Better internal procedures at co-ops (policy = practice)
* Commonality in network configuration

The ultimate realization of the proposed system will require an ultra-high performance database using heterogeneous database technology. A prototype of this has been designed by Craig Miller.

## 5b Impact on other disciplines

The secondary impact is expected to be a higher level of cross-fertilization among leading technologists in industry, academia and government organizations. Although there are cyber security activities, conferences and committees in place across industry boundaries, the unique approach embodied in this project is expected to have a beneficial impact in high profile areas such as banking, insurance, defense, and retailing.

## 5c Impact on the development of human resources

One of the likely outcomes of the project is to reduce the level of expertise required in utilities to manager cyber security.

## 5d Impact on physical, institutional, and information resources that form infrastructure

The open, abstraction model will allow many organizations or individuals to develop or improve components which can be integrated to the framework to work with components developed by others.

## 5e Impact on technology transfer

The project is expected to have an impact on the development of broad, new policies in the energy sector with respect to network configuration and monitoring. The open approach, as noted above, will accelerate the development of more advanced approaches to cyber security and, potentially, grid control.

## 5f Impact on society beyond science and technology

World events and virtually unlimited media access often combine to create a public sentiment of fear with respect to cyber-terrorism. Beyond personal safety, the general public is often concerned for the security of the nation’s infrastructure. The electric grid is usually at the top of that list because of its socio-economic impact on society. Decreasing the risk of cyber-attack events on the grid should have a positive impact on the attitude and therefore behavior of the general public. Safe, secure public systems instill confidence in society’s attitude to government policy and initiatives.

## 5g What dollar amount of the award’s budget is being spent in foreign countries?

None to date and none planned.

# 6. CHANGES/PROBLEMS

## 6a Changes in approach and reasons for change

As of September 30, 2015, the team did not make any substantive changes to the project plan. Development work based on the Cycle 2 design document has progressed according to plan.

The personnel changes report last quarter have been assimilated into the project without issue. As planned, Zico Kolter of CMU rejoined the team in August and is supporting the machine learning integration work. Maurice Martin has left NRECA. Maurice will be replaced by NRECA, but in the meantime his role has been successfully absorbed by others on the team. Nikhil Singh of NRECA has joined the project to develop network generation and support integration work. As a result of Honeywell’s departure from the project and slightly reduced effort by CMU, Cigital’s SOW has been revised to allow for the commensurate redistribution of budgeted resources.

## 6b Actual or anticipated problems or delays and actions or plans to resolve them

Substantial work in the past quarter focused on the integration of a software defined network capability using OpenDaylight. This has proven to be very difficult as the SDN software is fragile and does not always function as documented. The team has worked around the problems, and has implemented limited functionality. It is not clear whether these problems can be fully resolved until the OpenDaylight product or an alternative are more fully developed. If the team cannot implement the planned capability, it will provide a specification for OpenDaylight integration a later time when the SDN package is more stable.

## 6c Changes that have a significant impact on expenditures

There are no changes that have a significant impact on expenditures. Spending to date is in line with the budget.

## 6d Significant changes in use or care of human subjects, vertebrate animals, and/or Biohazards

Not applicable

## 6e Change of primary performance site location from that originally proposed

No changes planned or expected.

7. SPECIAL REPORTING REQUIREMENTS

N/A at this time.

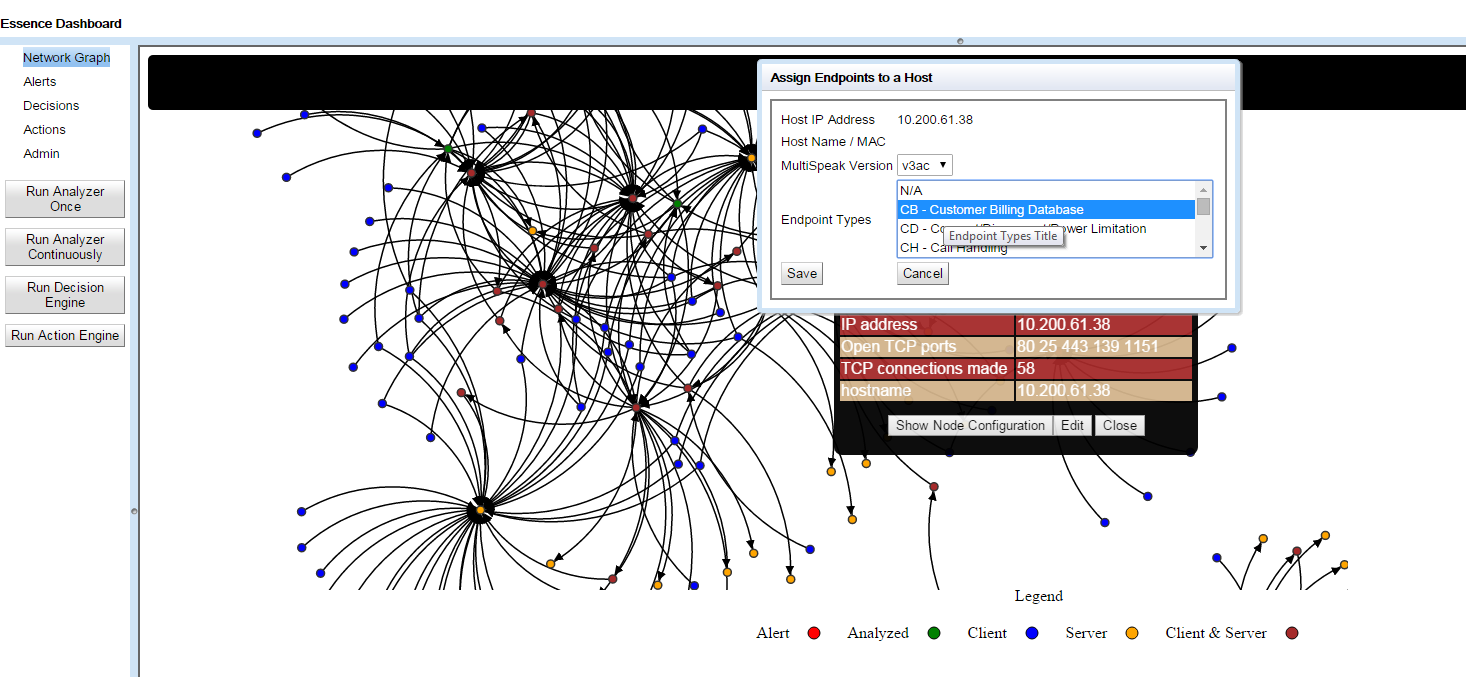
# 8. BUDGETARY INFORMATION

Please refer to the “Cost Plan Status Report” file submitted separately.

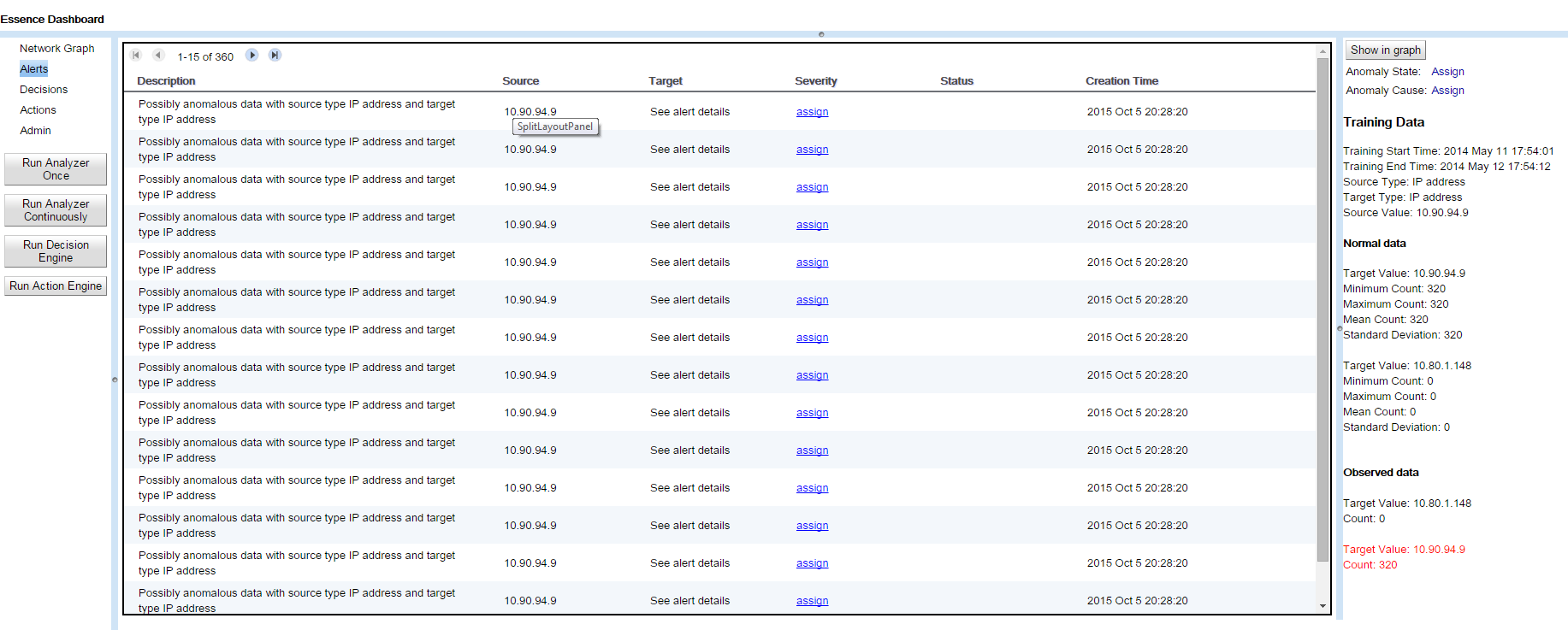
# **APPENDIX A**

## Essence Network Dashboard Examples

Examples of the integrated user interface are shown below.



Essence Network Dashboard – Assign Endpoints to a Host Function



Essence Network Dashboard – Alerts Function