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](#_Toc441755413)

[2. ACCOMPLISHMENTS 5](#_Toc441755414)

[2a Major goals of the project 5](#_Toc441755415)

[2b What was accomplished under these goals? 8](#_Toc441755416)

[Accomplishments of Task 1 – Project Management 8](#_Toc441755417)

[Accomplishments of Task 2 – High Level Design 9](#_Toc441755418)

[Accomplishments of Task 3 – Component Design 9](#_Toc441755419)

[Accomplishments of Task 4 – Network System Design 11](#_Toc441755420)

[Accomplishments of Task 5 – Laboratory Testing 11](#_Toc441755421)

[Accomplishments of Task 6 – Field testing 12](#_Toc441755422)

[Accomplishments of Task 7 – Commercialization 12](#_Toc441755423)

[Summary of Accomplishments for the Reporting Period 13](#_Toc441755424)

[2c What opportunities for training and professional development has the project provided? 14](#_Toc441755425)

[2d How have the results been disseminated to communities of interest? 14](#_Toc441755426)

[3. PRODUCTS 14](#_Toc441755427)

[3a Publications, conference papers, and presentations 14](#_Toc441755428)

[As noted previously, the team does not plan to publish externally until after Cycle 2 testing and engagement with a commercialization partner. 14](#_Toc441755429)

[3b Websites or other Internet sites 14](#_Toc441755430)

[3c Technologies or techniques 15](#_Toc441755431)

[3d Inventions, patent applications, and/or licenses 16](#_Toc441755432)

[3e Other products 16](#_Toc441755433)

[4. PARTICIPANTS & OTHER COLLABORATING ORGANIZATIONS: 16](#_Toc441755434)

[4a What Individuals have worked on the project? 16](#_Toc441755435)

[4b Other organizations involved as partners 17](#_Toc441755436)

[4c Have other collaborators or contacts been involved? 18](#_Toc441755437)

[5. IMPACT 18](#_Toc441755438)

[5a Impact on the development of the principal discipline(s) of the project 18](#_Toc441755439)

[5b Impact on other disciplines 19](#_Toc441755440)

[5c Impact on the development of human resources 19](#_Toc441755441)

[5d Impact on physical, institutional, and information resources that form infrastructure 19](#_Toc441755442)

[5e Impact on technology transfer 19](#_Toc441755443)

[5f Impact on society beyond science and technology 19](#_Toc441755444)

[5g What dollar amount of the award’s budget is being spent in foreign countries? 19](#_Toc441755445)

[6. CHANGES/PROBLEMS 20](#_Toc441755446)

[6a Changes in approach and reasons for change 20](#_Toc441755447)

[6b Actual or anticipated problems or delays and actions or plans to resolve them 20](#_Toc441755448)

[6c Changes that have a significant impact on expenditures 20](#_Toc441755449)

[6d Significant changes in use or care of human subjects, vertebrate animals, and/or Biohazards 20](#_Toc441755450)

[6e Change of primary performance site location from that originally proposed 20](#_Toc441755451)

[7. SPECIAL REPORTING REQUIREMENTS 20](#_Toc441755452)

[8. BUDGETARY INFORMATION 20](#_Toc441755453)

[APPENDIX A 21](#_Toc441755454)

[Milestone M11 Report 21](#_Toc441755455)

[The Five Layer Abstraction Model 22](#_Toc441755456)

[Release 2 Improvements by Data Layer 23](#_Toc441755457)

[Data Layer 23](#_Toc441755458)

[Information Layer 23](#_Toc441755459)

[Analysis Layer 24](#_Toc441755460)

[Decision Layer 24](#_Toc441755461)

[Action Layer 25](#_Toc441755462)

[Assessment of Progress vs. Plan Post the First Field Test 25](#_Toc441755463)

[APPENDIX B 27](#_Toc441755464)

[Test Plan Scenarios 27](#_Toc441755465)

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: January 30, 2016

DUNS Number: 045497427

Recipient Organization: National Rural Electric Cooperative Association

Address: 4301 Wilson Boulevard

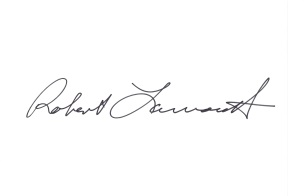
Arlington, VA 22203-1860

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

Reporting Period End Date: December 31, 2015

Report Term or Frequency: Quarterly

Signature of Submitting Official:



Robert Larmouth

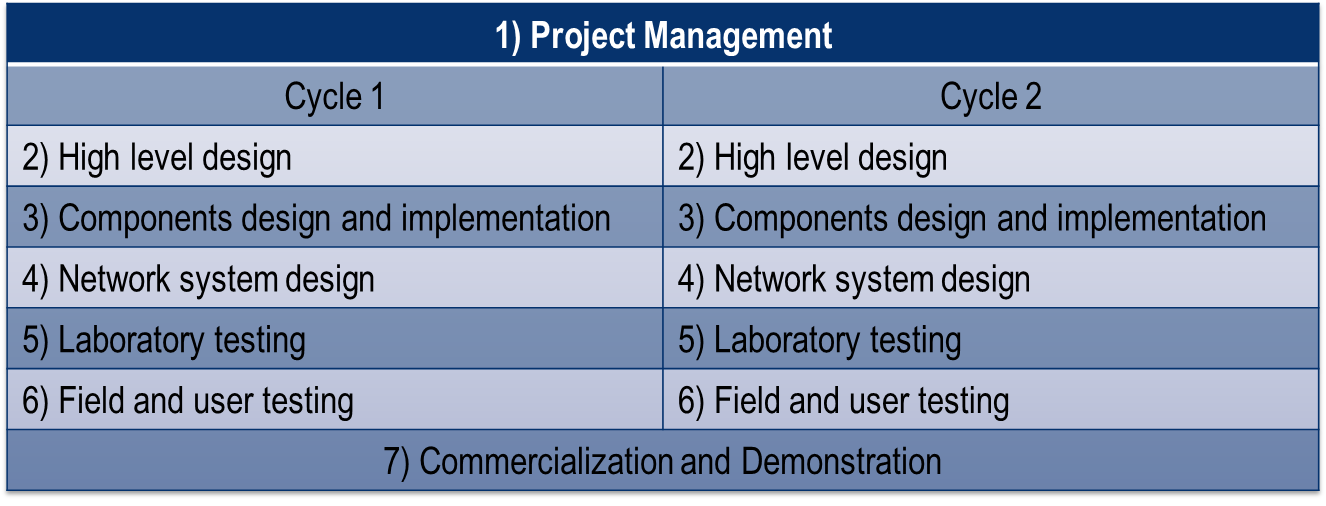
# 2. ACCOMPLISHMENTS

## 2a Major goals of the project

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

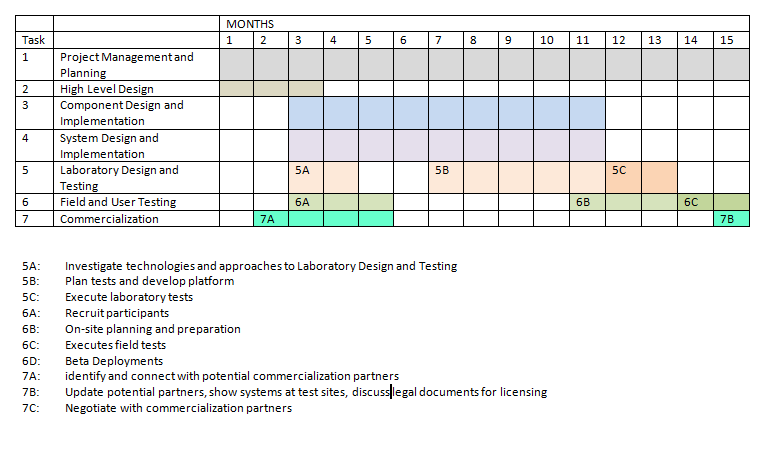
* A capability to establish, maintain, and monitor an alignment between OT security policy and network configuration and settings
* A capability to detect and prevent potentially malicious traffic flows within an electric utility’s operational network, by creating protocol-specific (e.g., specific to 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:

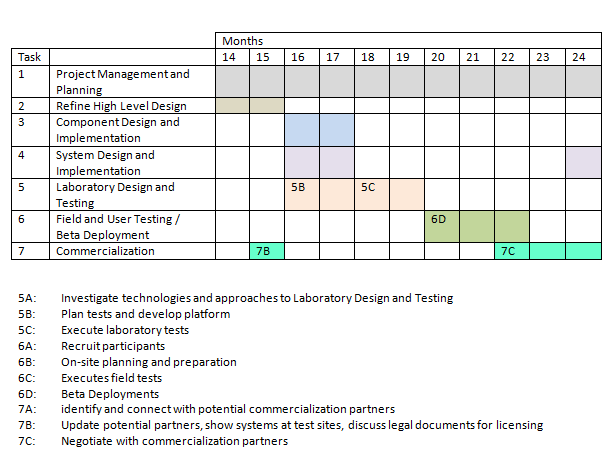


Tasks 2 through 6 will be executed twice – first in a prototype cycle and second through a refinement cycle that benefits from the testing and analysis conducted in the first cycle. The timeline for these tasks (from the Project Management Plan) is shown below.

Cycle 1 Schedule



Cycle 2 Schedule



As of December, 2015, no significant changes were made regarding the tasks and associated schedule. 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 | 100% |
| **4** | Refine System Design and Implement Changes | 88 | 102 | 14 | 95% |
| **5** | Laboratory Testing | 102 | 106 | 4 | 95% |
| **6** | Refined Field and User Testing | 106 | 114 | 8 | Planned for February |
| **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 | Complete |

The task progress status shown above should support the remaining Milestones. The Cycle 2 lab testing is complete and work has begun on the field test plan and arrangements.

## 2b What was accomplished under these goals?

The major accomplishments during the reporting period were on code development, lab testing, and commercialization. A list of additional features and a minor list of bugs were completed at the end of the prior period. A date of 15 December was set to be feature complete with no known bugs. This deadline was met. Since then, the team has conducted additional testing and refinement, but major development is complete.

A detailed plan for the final field test was started and the team worked on arranging a time for the test. The test will not take place as originally scheduled due to logistical problems in getting all of the critical staff, including utility staff, together. The test is expected to be held in late February or early March.

There was substantial progress on commercialization with meetings with three potential developers. These are Intel, South Eastern Data Cooperative (SEDC) and the National Rural Telecommunications Cooperative (NRTC). DOE is, without a doubt familiar with Intel, but SEDC and NRTC are possibly less so. Both are cooperatives providing services to electric utilities, each with more than 200 customers. NRECA has been developing a proposal and term sheet for each entity.

### 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. Working meetings have increased in frequency among Cigital, CMU and NRECA personnel to further develop and integrate features ahead of the December 15 date. The resource re-allocations discussed in the previous report have proven to be beneficial. The project remains on budget and no major concerns were identified regarding the PMP schedule.

### Accomplishments of Task 2 – High Level Design

Data

Information

Analysis

Decision

Action

The High Level design is unchanged from the prior period. However, the details of the design have been advanced with improvements in the integration of AI algorithms and an improved user interface. Also, the team revised the anomaly submission and retrieval API. The laboratory testing results were analyzed layer by layer to show the end-to-end readiness of the system.

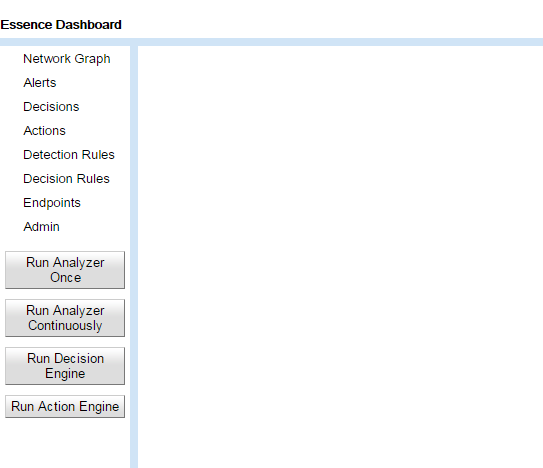
### Accomplishments of Task 3 – Component Design

All basic functionality is complete. Work in the last period focused on testing and refinement. In general, these were changes in detail, but some substantial work was required in three areas:

1. Improvement to the user interface. As we test with larger networks, the UI must deal with analysis and interaction with much more complex data sets. There is no very clear and obvious way to display and query 1000+ node systems. We are experimenting, but the inherent scale means that the UI will never be simple.
2. Machine Learning. Work continued on implementing *supervised* learning to reduce the number of false positives. We use the term “positives” for alerts even though they are clearly negative events. The REST API developed in the prior period was improved and the documentation updated. In addition, an end-to-end demonstration of the code's functionality was done. With the Essence platform and the CMU machine learning application both running, the team trained the anomaly detection code using a packet capture received from Great River Electric. Fake network data was then injected into the machine learning application and showed that it considered those anomalous. Next, a collection of anomalies and user annotations for those anomalies was generated. The team showed that the machine learning code correctly used those annotations to predict the causes of any new anomalies that appeared. This demo not only shows the power of the anomaly detection software, it also shows the successful integration of the software with the Essence platform.
3. Control of Software Defined Network. The SDN functionality is still limited. This is due, entirely, to the immaturity of the SDN software. It is likely that initial commercial deployment of Essence will not include an SDN Control capability due to the state of the software and the very limited penetration of SDN systems. Though this aspect of the work may not have near-term commercial value, this sort of exploratory implementation is a necessary first step towards something that will, undoubtedly be of value in coming years.

Selected examples of developments are highlighted and illustrated below:

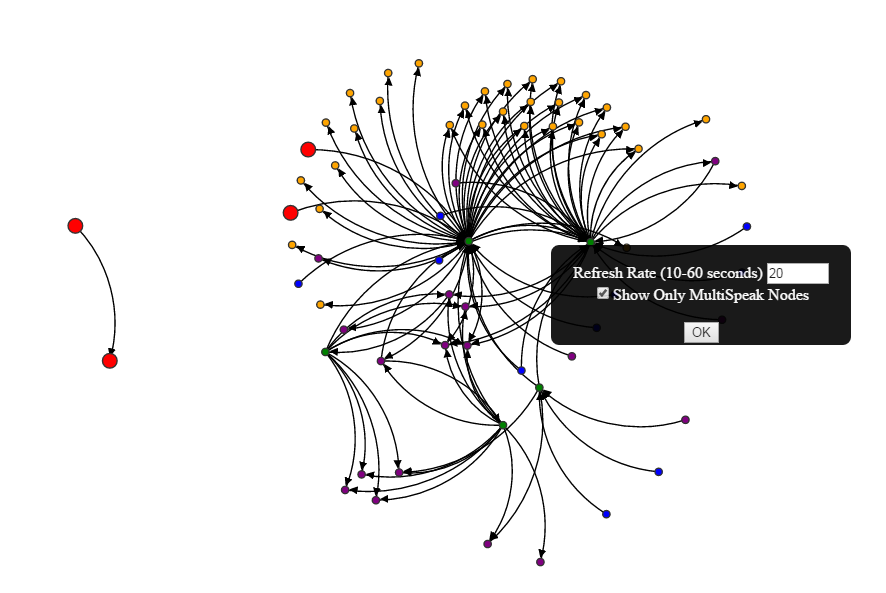
* Redesigned Essence Dashboard layout to allow easier access to critical functions (see below)



* Improved the alerts interface to show necessary alert details in table and allowing user to select alert to view more detailed information (see below)

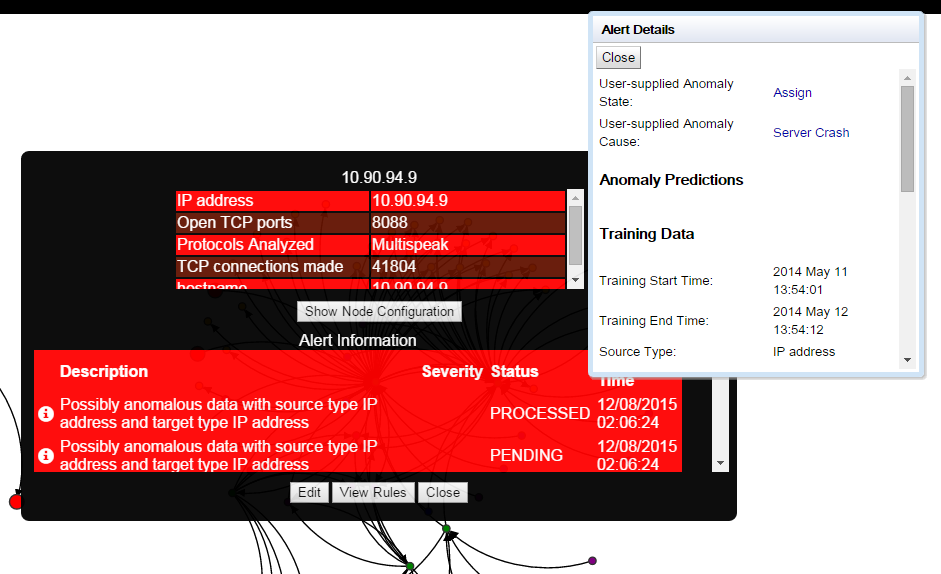


* Implemented ability to revert an action in Essence (for instance: would unblock network traffic in OpenDaylight’s SDN controller)
* Fixed software bugs in MultiSpeak packet capturing tool
* Fixed a bug where Cassandra connections were being exhausted when capturing packets
* Generated a customized network topology within mininet
* Added filtering of non-MultiSpeak packets to network graph



### Accomplishments of Task 4 – Network System Design

The network analysis component of Essence is essentially unchanged from the prior version. Work in this period has focused on testing and refinement of the AI, and improved usability of the alerts interface within the network graph (the latter shown below).



### Accomplishments of Task 5 – Laboratory Testing

During this reporting period the team continued to run the system internally monitoring increasingly complex MiniNet systems. MiniNet is a flexible network simulator. The Essence team has developed a capability to configure quasi-utility networks on the fly. This capability should be made available to other CEDS teams. Through the period the laboratory work focused on identify any weaknesses in the system and validating fixes.

The major accomplishment during this reporting period was the achievement of the final go/no-go milestone (M11): “Laboratory testing of second prototype complete”. The GO/NO GO DECISION (G6) was: “Assessment of whether the tested second generation prototype meets project objectives”. During the quarter, the lab testing was done in parallel with the feature development, integration and refinement. This agile approach streamlined this phase of the project and resulted in some features that exceeded the original design goals. Testing results were analyzed for each layer of the architectural model. A report summarizing the testing results was submitted to DOE with a subsequent response, affirming that the project was ready to proceed to Cycle 2 field testing. The test report is included in Appendix A.

### Accomplishments of Task 6 – Field testing

The team decided that the Cycle 2 field testing planned for Central EMC in NC would be enhanced through the involvement of additional parties, including South East Data Cooperative (SEDC) and National Rural Telecom Cooperative (NRTC). SEDC is one of the potential commercialization partners and a supplier to Central EMC. NRTC is also interested in Essence and Doug Lambert (formerly of NRECA and was a primary resource in the Cycle 1 testing) would represent NRTC. The involvement of five different organizations created scheduling difficulties. The team made a decision to delay the test rather than proceed with an incomplete team as this will be the final opportunity in the project to test and work together. Testing is now projected to occur in late February.

During the reporting period the team began work on the Cycle 2 field test plan – significantly more comprehensive than the Cycle 1 tests. The major elements of the test plan are shown below:

* Building network graph
* Executing value out of bounds rule
* Executing denial of service rule
* Executing connectivity violation rule
* Executing unsupervised component of machine learning engine
* Executing supervised component of machine learning engine
* Reacting to value out of bounds rule result
* Reacting to denial of service rule result
* Reacting to connectivity violation rule result
* Reacting to unsupervised component of machine learning engine result
* Reacting to supervised component of machine learning engine result

Each of the elements above contains many steps. As of December 31 the plan was still a work in progress, but it is shown in Appendix B. The elements/steps that are incremental to the Cycle 1 test are shown in red to illustrate the increased complexity of the Cycle 2 test plan.

### Accomplishments of Task 7 – Commercialization

There was much progress in Commercialization during this reporting period. The team is evaluating commercialization model options. NRECA has developed a product development process model, but this is in the early stages. NRECA does not yet have a commercial software development capability or sales organization, and would need to strengthen technical support resources. The structural and legal aspects of a commercial operation would also need to be carefully developed. As the team monitors these developments, it remains committed to the DOE deliverable of a commercialization plan.

Accordingly, the team is exploring the potential transfer of Essence technology to an entity that will operate security as a service for electric utilities - offering Essence in conjunction with other services such as firewall management. Detailed meetings were held during the period with three potential commercialization entities:

1. Intel
2. South Eastern Data Cooperative (SEDC)
3. National Rural Telecommunications Cooperative (NRTC)

All three discussions are proceeding. Beyond the technical meetings, executive level meetings were held with SEDC and NRTC. Both have explicitly stated that they wish to pursue Essence commercialization. Follow-up meetings are scheduled and representatives from both companies will participate in the final field test as part of technical due diligence.

In an interesting twist, NRTC has already deployed elements of Essence. They are using Essence Layer 1 and Layer 2 technology to collect data from Sensus meters. They drafted an application to detect “hot sockets” which can be an indication of a fire or electrical overload. The system has been deployed at San Bernard Electric Cooperative and has already detected problems including one which coincidentally occurred during a live demonstration. The problem was excess current at a welding shop. There was no fire or failure this time, but persistent overload of this type should be addressed before failure. NRTC plans to deploy this application to other co-ops and to develop additional apps.

### Summary of Accomplishments for the Reporting Period

Major Activities:

* Weekly communication, demos and team meetings
* Machine learning refinement
* Feature development
* Laboratory testing across all layers
* Essence Network Dashboard refinement

Specific Objectives:

* Complete feature development
* Develop outline for commercialization
* Develop strategy for field test

Significant Results:

* Demonstration at DOE headquarters
* Preliminary plan for Cycle 2 field testing

Key Outcomes:

* Two additional commercialization partners identified
* Approval of lab test results – final go/no-go decision
* Limited commercial deployment for detecting hot sockets
* 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

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

1. Meetings with and demonstrations to
   1. South Eastern Data Cooperative
   2. National Rural Telecommunications Cooperative
2. Presentation to about 40 utility staff at the EPRI annual power system meeting
3. Presentation and demonstration to the NRECA board of directors
4. Presentation to about 50 utility CEOs at the NRECA annual CEO Close-up conference
5. Detailed discussion with the Arkansas Electric Cooperative Corporation
6. Installation of Essence Layer 1 and 2 and San Bernard Electric Cooperative

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

## 3b Websites or other Internet sites

As noted previously, the project is focusing on live, in-person discussions rather than general web presentations as the team is seeking feedback and input. Nevertheless, the Essence project has received substantial press. The image below is from a Google search of “NRECA Essence”. It lists 6,710 pages. Without a doubt, many of these are not relevant, but there are still many good references.

|  |
| --- |
|  |

## 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

An extensive draft patent has been largely completed but not filed as it lacks the claims section. Work on this was interrupted by time-critical proposal activity. DARPA is creating a program for rapid anomaly detection in the electrical grid. DARPA is aware of Essence and much of the Broad Agency Announcement (BAA) aligns well with Essence. A DARPA project would provide ample funding for massive expansion of Essence functionality, testing and demonstration at scale, training National Guard in the use of Essence and its incorporation into cyber-response, and commercialization.

## 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 October 1 through December 31. The activity is expressed as an annualized rate where 12 person-months = full time.

Name: Robert Larmouth – NRECA

Role: Project Manager

Person-months: 1

Contribution: Direction of teams, schedules and reporting

Funding source(s): DOE and NRECA

Name: Craig Miller – NRECA

Role: Principal Investigator

Person-months: 7

Contribution: Technical direction, outreach, database

Funding source(s): DOE and NRECA

Name: Nikhil Singh - NRECA

Role: Software Engineer

Person-months: 5

Contribution: Decision/action development

Funding source(s): DOE and NRECA

Name: Evgeny Lebanidze - Cigital

Role: Development Team Leader

Person-months: 0.2

Contribution: Direction of the high level design team

Funding source(s): DOE

Name: Chandu Ketkar - Cigital

Role: Chief Technologist

Person-months: 0.1

Contribution: End-to-end solution design

Funding source(s): DOE

Name: Ping Ning - Cigital

Role: Senior Architect

Person-months: 2

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: 4

Contribution: Network design/testing/team lead

Funding source(s): DOE

Name: Terrence Wong - CMU

Role: Senior Research Programmer

Person-months: 6

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: Eric Wong - CMU

Role: Programming support

Person-months: 6

Contribution: Machine learning code

Funding source(s): DOE

## 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

The following electric utility cooperatives have been in communication with the team, expressing interest and/or offering participation:

* 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
* Arkansas Electric Cooperative Corporation 🡨 new since last period

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 December 31, 2015, the team did not make any substantive changes to the project plan, except for a possible slight delay in Cycle 2 field testing. Feature development work based on the Cycle 2 design document has been completed as of December 15.

Other than normal fluctuations in the schedules and availability of key personnel, there have been no significant changes during the past quarter. CMU has added a PhD student, Eric Wong, to assist in the programming and code completion. PNNL’s period of performance ended prior to this reporting period.

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

Other than the potential for a slight delay in Cycle 2 field testing as discussed earlier in the report, there are no additional problems or delays anticipated.

## 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**

## Milestone M11 Report

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.

# APPENDIX B

## Test Plan Scenarios

Shown below is the state of the plan as of December 31. Test tasks/steps in red were not part of the Cycle 1 testing.

**Building network graph**

1. Test drawing of non-MultiSpeak nodes after capturing raw traffic
   1. Start raw-capture Python script
   2. Replay packets from PCAP file
   3. Run network graph Python script
   4. Open network graph in web browser
   5. Verify that nodes are displayed
   6. Click on a node an verify that details about the node are displayed such as IP address, ports open, connections, etc
2. Test drawing of MultiSpeak nodes after capturing raw traffic and MultiSpeak traffic
   1. Start MultiSpeak capture Python script
   2. Replay packets from PCAP file
   3. Run network graph Python script
   4. Open network graph in web browser
   5. Verify that green nodes are displayed
   6. Click on a green node an verify that details about the node are displayed such as IP address, ports open, connections, etc
3. Test filtering nodes to only show MultiSpeak nodes
   1. Capture traffic as in #1 and #2 test cases
   2. Run network graph Python script
   3. Open network graph in web browser
   4. Verify that only green and red nodes and nodes that are directly connected to green/red nodes are displayed
4. Test searching for nodes by IP address
   1. Capture traffic as in #1 and #2 test cases
   2. Run network graph Python script
   3. Open network graph in web browser
   4. Enter the IP address of a known node in the search box and click search
   5. Verify that graph zooms to node
   6. Verify that node tooltip is displayed
   7. Verify that node is highlighted
   8. Enter partial IP address of a known node(s) in search box and click search
   9. Verify that graph zooms and displays all selected nodes
   10. Verify that nodes that match partial IP address have tooltips displayed
   11. Verify that nodes that match partial IP address are highlighted
5. Test editing of node annotations
   1. Capture traffic as in the #1 test case
   2. Run network graph Python script
   3. Open network graph in web browser
   4. Click on a node
   5. Click the edit button in the dialog
   6. Change the hostname value
   7. Add text to the notes field
   8. Click save
   9. Click on the same node in the graph and verify that the saved information is displayed

**Executing value out of bounds rule**

1. Test creating a value out of bounds rule
   1. Determine what endpoint type, endpoint message, and values are desired for rule
   2. Open Essence application in web browser
   3. Click on Detection Rules menu item
   4. Select VALUE\_OUT\_OF\_BOUND from Rule Type drop down
   5. Click the Create New Detection Rule button
   6. Choose MultiSpeak v3ac for the Protocol Version
   7. Choose the Endpoint Code
   8. Choose the Endpoint Message
   9. Provide a Title for the rule
   10. Choose the conditions and input values based on decision made in the first step of the test case
2. Test executing analyzer engine with captured MultiSpeak traffic
   1. Start MultiSpeak capture Python script
   2. Replay packets from PCAP file
   3. Open Essence application in web browser
   4. Click the Run Analyzer Once button in the menu
   5. Allow time to analyzer engine to execute
   6. Ensure no error message is displayed
3. Test viewing of value out of bounds alerts and ensure rule violation details are present
   1. Execute the first two value of out of bounds test cases
   2. Open the Alerts page within the Essence application
   3. Find a value out of bounds alert in the alert list
   4. Verify that values (other than severity) for alert are populate in the list
   5. Click on the alert in the list
   6. Verify that the details of the alert are displayed in the right panel
4. Test assigning severity to the alert
   1. Execute the first two value of out of bounds test cases
   2. Open the Alerts page within the Essence application
   3. Find a value out of bounds alert in the alert list
   4. Click on the assign link in the severity column
   5. Choose a severity an click the Save button
   6. Verify that the alert list is updated with the assigned severity
5. Test network graph by verifying that nodes with the new alert(s) are red
   1. Execute the first two “Build network graph” test cases
   2. Enter the IP address of a known value out of bounds alert in the search box and click the search button
   3. Verify that the node displayed is red
6. Test network graph by verifying that alert information is displayed when clicking on node
   1. Execute the “Test network graph by verifying that nodes with the new alert(s) are red”
   2. Click on the displayed node
   3. Verify that the alert information in the dialog
   4. Click on the “I” image next to an alert
   5. Verify that a new dialog is displayed with the additional alert details

**Executing denial of service rule**

1. Test creating a denial of service rule
2. Choose the conditions and input values based on decision made in the first step of the test case
3. Test executing analyzer engine with captured MultiSpeak traffic
4. Test viewing of denial of service alerts and ensure rule violation details are present
5. Test assigning severity to the alert
6. Test network graph by verifying that nodes with the new alert(s) are red
7. Test network graph by verifying that alert information is displayed when clicking on node

**Executing connectivity violation rule**

1. Test creating a connectivity violation rule
2. Test executing analyzer engine with captured MultiSpeak traffic
3. Test viewing of connectivity violation alerts and ensure rule violation details are present
4. Test assigning severity to the alert
5. Test network graph by verifying that nodes with the new alert(s) are red
6. Test network graph by verifying that alert information is displayed when clicking on node

**Executing unsupervised component of machine learning engine**

1. Test the execution of machine learning using web interface with supervised learning disabled
2. Test engine by sending unexpected message from one machine to another
3. Test alert interface by viewing anomaly alert for unexpected message(s)
4. Test engine by stop expected messages from one machine
5. Test alert interface by viewing anomaly alert for gap in messages
6. Test network graph by verifying that nodes with the new alert(s) are red
7. Test network graph by verifying that alert information is displayed when clicking on node

**Executing supervised component of machine learning engine**

1. Test the execution of machine learning using web interface with supervised learning enabled
2. Test engine by sending unexpected message from one machine to another
3. Test alert interface by viewing anomaly alert for unexpected message(s)
4. Test assigning state and cause to anomaly alert
5. Retest engine by sending unexpected message from one machine to another
6. Test alert interface by viewing anomaly alert an ensuring that new anomaly alert(s) have predictions
7. Test engine by stop expected messages from one machine
8. Test alert interface by viewing anomaly alert for gap in messages
9. Test assigning state and cause to anomaly alert
10. Retest engine by stop expected messages from one machine
11. Test alert interface by viewing anomaly alert an ensuring that new anomaly alert(s) have predictions
12. Test network graph by verifying that nodes with the new alert(s) are red
13. Test network graph by verifying that alert information is displayed when clicking on node

**Reacting to value out of bounds rule result**

**Reacting to denial of service rule result**

**Reacting to connectivity violation rule result**

**Reacting to unsupervised component of machine learning engine result**

**Reacting to supervised component of machine learning engine result**