NRECA/DOE DE-OE0000684 Task 4 – Network System Design

October 7, 2014

Table of Contents

[Table of Contents 2](#_Toc400429845)

[1 Introduction 1](#_Toc400429846)

[1.1 Assumption 1](#_Toc400429847)

[2 Evaluation vs. Success Criteria 2](#_Toc400429848)

[3 Logical View 5](#_Toc400429849)

[3.1 Layer 1 Logical Model 5](#_Toc400429850)

[3.1.1 Layer 1 Components 5](#_Toc400429851)

[3.2 Layer 2 Logical Model 6](#_Toc400429852)

[3.2.1 Layer 2 Components 6](#_Toc400429853)

[3.3 Layer 3 Logical Model 8](#_Toc400429854)

[3.3.1 Layer 3 Components 8](#_Toc400429855)

[3.4 Layer 4 Logical Model 11](#_Toc400429856)

[3.4.1 Layer 4 Components 12](#_Toc400429857)

[3.5 Layer 5 13](#_Toc400429858)

[4 Lab Testing View 14](#_Toc400429859)

[4.1 Lab Testing Components 14](#_Toc400429860)

[5 Deployment View 15](#_Toc400429861)

[5.1 Deployment Diagram 15](#_Toc400429862)

[6 Contacts 16](#_Toc400429863)

**Document Change Control Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 10/01/2014 | 0.1 | Initial Draft | Dev. Team |
| 10/02/2014 | 0.9 | Draft submitted for project team comment | All Teams |
| 10/07/2014 | 1.0 | Final Version, submitted to DOE | Project Mgr |

# Introduction

This document satisfies the requirements of Task 4 (Network System Design), Milestone M5 in the Essence PMP. Milestone M5 is not a go/no-go decision, but it illustrates how the system components are integrated into a functional network.

## Assumption

* MultiSpeak® version 3 build ac and 5.03 are supported, so “MultiSpeak® specification” below refers to these two particular versions.
* Co-op network hardware of interest is physically collocated with DEVICE-1.1 to support traffic capturing

# Evaluation vs. Success Criteria

* Are the project’s technical objectives being met?

The network system design presented in this document will perform all of the functions identified in the initial concept paper. In addition, it addresses additional functionality that the team believes is valuable and achievable within the project scope. This table below lists key functionality. The items in bold extend the originally conceived functionality.

1. Allow specification of the network configuration in a manner that allows for machine review and validation
2. Collect network traffic
   1. Actively, in-line devices
   2. **Passively through custom developed device**
3. Organize the information into a high speed, secure, **redundant** database for analysis

**Investigate ultra-high performance, heterogeneous database structure that will allow for a very high degree of scaling in the message rate (1000x)**

1. **Facilitate conventional validation of network traffic**
2. Provide sufficient data to characterize “normal” network traffic
3. Validate network flow
   1. Map the network
   2. Compare “as-is” network to “as-understood”
   3. **Implement checks that can be determined in advance**
      1. **Message structure**
      2. **Ranges of values**
      3. **Deviation from normal frequency of messages**
      4. **Rate of receipt**
      5. **Other, TBD**
   4. Detect deviations from normal by means of artificial intelligence
   5. Alert on discrepancies in (6b, 6c, or 6d)
4. Update model of normal operation using machine learning methods
5. On alert (6e), determine remediation actions based on risk analysis
6. Affect changes through:
   1. Changes to the network using software defined network capabilities
   2. **Communications to SCADA to affect grid operations**
   3. **Messages to human operators to make manual changes to network and/or grid**

The design meets all technical objectives.

* Do we realistically expect the product to meet its technical and cost goals?

At this point, the team’s research into commercial and available laboratory software provide a reasonable level of confidence that the designed system will meet its technical and cost goals. The team is conducting mini-research projects (“sprints”) to address high-risk areas, but to date the team has not found any insurmountable barriers to the achievement of the goals.

* Are the technical objectives still relevant or have changes in requirements or have any of the following obviated the need for the project and its products:
  1. New or improved competing products or solutions
  2. Changing security requirements (e.g., the nature of threats and attacks)
  3. Changing grid cyber security regulations

As part of its design work, the team has been investigating available commercial security projects. To date we have not found any that provide the non-prescriptive approach at the heart of the system under development.

* Is spending consistent with the plan and are there sufficient resources available from all sources to carry the project through to a successful conclusion?

Spending is on track. Since the start of the project, we have sought material assistance from major organizations in the space. NRECA has since started a complementary project with DOE to enrich the data and information layers of the project. Programming and technical support from a major commercial partner could add funding to the project allowing for the richer scope of work defined above.

* Have tests to date been successful or, if not, have we identified issues and either corrected the problem or gotten on the path to doing so?

Per the schedule, the project has not yet reached the system testing phase. Unit testing to date has been completely successful. The next round of tests will focus on testing higher message rates and an expanded range of message types, extending to legacy versions of MultiSpeak® that are still in common use.

* Is the team working as designed and are all partners still committed? Are changes needed?

The team is all under contract and working well. No changes are needed at this time.

* Is there still commercial interest in the product?

There is strong and growing commercial interest in the project. In additional to Honeywell and Cigital, who are the core members of the team, there have been expressions of interest from GE, IBM and Intel as well as several smaller firms. We are accelerating the patent process to get the intellectual property into licensable form.

* Summary/Recommendation

The team proposed to amend the PMP to deal with a scheduling issue. We propose to delay the start of field testing by three weeks to February 20th. This is to accommodate preparatory work in early January. In examining the schedule, we found that some critical on site work would be required at the end of December and we were concerned that the requisite co-op staff might not be available because of the holidays.

# Logical View

The logical view describes the logical components of the network system.

## Layer 1 Logical Model



Figure 1 – Layer 1 Logical Diagram

### Layer 1 Components

**IN-1.1** – Interface IN-1.1 will make a layer 1 line speed copy of Ethernet frames on the monitored interface (using, for example, SPAN port(s), network taps, etc.). Multiple Layer 1 Inputs (Ethernet ports) will be available to copy traffic from multiple layer 1 network interfaces.

**COM-1.1** – The capturing program monitors the IN-1.1 interface and captures Ethernet frames from this interface. The capturing program also records a timestamp for each captured Ethernet Frame. The capturing program is also responsible for connecting to the Grid State Database (DATA-1.1) and sending the data as specified in OUT-1.1.

**DEVICE-1.1 –** The physical component on which COM-1.1 is deployed. Multiple instances of COM-1.1 will be available on the device to monitor multiple layer 1 line speed interfaces.

**OUT-1.1** – The output to the Grid State Database consists of a timestamp and an Ethernet frame pair. This data is sent to the Grid State Database.

**DATA-1.1 –** The Grid State Database. It captures all the network traffic in the form of Ethernet frames within a time window to reflect the state of the network segment that is being monitored. The time window is sliding across time and DATA-1.1 at the minimum makes available all the data contained within the latest time window, which reflects the real-time current state of the network segment that is being monitored. For each network frame DATA-1.1 maintains the data as specified in OUT-1.1.

## Layer 2 Logical Model



Figure 2 – Layer 2 Logical Diagram

### Layer 2 Components

**IN-2.1/2.2/2.3** – Each Layer 2 service maintains a separate link to the Grid State Database. Each Layer 2 Service queries the database for new information (based on timestamp). The input interface passes the timestamp and the Ethernet frame into the Layer 2 COM element for filtering and parsing.

**COM-2.1** – The MultiSpeak® parser first checks to ensure that the Ethernet frame delivered by IN-2.1 contains a MultiSpeak® payload. The MultiSpeak® parser implements a message reassembly algorithm that takes as input multiple Ethernet frames and combines them into one MultiSpeak® message. This is necessary because large MultiSpeak® messages may be split across multiple Ethernet frames. The MultiSpeak® parser then extracts the source IP address, destination IP address, MultiSpeak® endpoint code, MultiSpeak® message name, and MultiSpeak® message payload from the Ethernet Frame. The time of capture is also formatted as a timestamp value in milliseconds.

**COM-2.2** – The network mapping parser reads Ethernet frames and extracts elements of interest for the network discovery application cluster.

**COM-2.3** – The machine learning parser filters all packets that are not MultiSpeak®. The parser then extracts 5 fields for analysis including: source IP address, destination IP address, MultiSpeak® endpoint code, MultiSpeak® message name and timestamp.

**OUT-2.1** – The following fields are output from COM-2.1 and stored into the MultiSpeak® application cluster database: source IP address, destination IP address, MultiSpeak® endpoint code, MultiSpeak® message name, MultiSpeak® message payload, and timestamp.

**OUT-2.2** – The following fields are output from COM-2.2 and stored into the network discovery application cluster database: source IP address, destination IP address, destination port, and timestamp.

**OUT-2.3** – The following fields are output from COM-2.3 and stored into the machine learning application cluster database: source IP address, destination IP address, MultiSpeak® endpoint code, MultiSpeak® message name and timestamp.

**DATA-2.1** – This database is used by the Layer 3 MultiSpeak® Deep Packet Inspector Application. It contains the fields output by OUT-2.1. This database can be accessed by applications needing MultiSpeak® data.

**DATA-2.2** – This database is used by the Layer 3 Network Mapping application. It contains the fields output by OUT-2.2.

**DATA-2.3** – This database is used by the Layer 3 Machine Learning application. It contains the fields output by OUT-2.3.

## Layer 3 Logical Model



Figure 3 – Layer 3 Logical Diagram

### Layer 3 Components

**Data-2.1/2.2/2.3** is described above in Layer 2 services.

**IN-3.1** – Information Record, each containing

* + 1. Source IP address
    2. Destination IP address
    3. Capturing Timestamp
    4. Full packet content
    5. Extracted values, from the packet content in name-value pair format, currently including
       1. Endpoint type
       2. Message name

The deep packet inspection application depends on data stored in the AppDB-3.1 database. AppDB-3.1 stores the rule definitions and metadata as follows:

1. Detection Rules, each containing:
   1. Rule Identifier – an integer unique to each detection rule
   2. Detection Rule Type – category of detection rule, currently supported rule types are:
      1. MS\_EP\_CONNECTIVITY
      2. DENIAL\_OF\_SERVICE
      3. VALUE\_OUT\_OF\_BOUND
      4. WRONG\_MSG\_TO\_MS\_EP
      5. ERR\_MSG\_FROM\_MS\_EP
   3. Source Endpoint Type – Endpoint type code as defined in the MultiSpeak® specification, for MultiSpeak® connectivity rules
   4. Destination Endpoint Type – Endpoint type code as defined in the MultiSpeak® specification, for MultiSpeak® connectivity rules
   5. Source IP Address – IP address to match the source in packets for certain IP address based rules
   6. Destination IP Address – IP address to match the destination in packets for certain IP address based rules
   7. Number of Packets Threshold – For Denial of Service rules, the number of packets beyond which a DoS alert would be triggered
   8. DoS Time Window in Seconds – For Denial of Service rules, the sliding time window in seconds for counting the number of packets for DoS attack detection purpose
   9. Rule Action Type – in some rules, for example, connectivity rules, whether the connection is Allowed or Disallowed
2. Endpoint Configuration, each containing:
   1. Host IP Address – IP address for a host that is visible to the network under analysis
   2. Host Name or MAC Address – name assigned to a host or the MAC address of the host
   3. MultiSpeak® Endpoint Type Codes - Endpoint type codes assigned to a host as defined in the MultiSpeak® specification
3. MultiSpeak® Service Message Map, each containing:
   1. MultiSpeak® Endpoint Service Name – Endpoint service name as defined in the MultiSpeak® specification
   2. MultiSpeak® Endpoint Service Code – Endpoint service code as defined in the MultiSpeak® specification
   3. Operation Name – name of the operation on a service endpoint defined in the endpoint WSDL
   4. Request Message Name – name of the SOAP request message defined in the endpoint WSDL for the operation
   5. Response Message Name – name of the SOAP response message defined in the endpoint WSDL for the operation
   6. SOAP Action Name – name of the SOAP action defined in the endpoint WSDL for the operation

**IN-3.2** – The Network Mapping Layer 3 application uses this link to query data elements from the Network Discovery application cluster database. The elements in this database are described in OUT-2.2.

**IN-3.3** – The Machine Learning Layer 3 application uses this link to query data elements from the Machine Learning application cluster database. The elements in this database are described in OUT-2.3.

**APP-3.1** – The MultiSpeak® deep packet inspection application maintains detection rules and analyzes MultiSpeak® traffic for rule violations. The application also supports tagging network devices with MultiSpeak® endpoint types for usage in detection rules. Detection rules can be specified for the MultiSpeak® specification for any endpoint and for any message type.

**APP-3.2** – The network mapping application discovers new devices on the monitored network. It maintains a graphical depiction of the current network topology and the connection state of discovered network devices. The network mapping application also discovers connections between devices. This application provides a service for querying host information about the network.

**APP-3.3** – The machine learning application analyzes MultiSpeak® metadata (described in OUT-2.3) to identify anomalies in MultiSpeak® traffic patterns.

**OUT-3.1** – Finding Record, each containing:

1. Finding Identifier – an integer unique to each finding
2. Detection Timestamp - system time in milliseconds when the finding was detected
3. Detection Rule Type - category of detection rule, currently including MS\_EP\_CONNECTIVITY and DENIAL\_OF\_SERVICE, with the following future additions: VALUE\_OUT\_OF\_BOUND, WRONG\_MSG\_TO\_MS\_EP, ERR\_MSG\_FROM\_MS\_EP, WRONG\_MSG\_FORMAT, NW\_SEGMENTATION, NEW\_HOST, applicable when there is a direct detection rule matching
4. Source IP Address – source IP address from the original packet associated with the finding
5. Destination IP Address – destination IP address from the original packet associated with the finding
6. Number of Packets Detected – for DoS rule violation, the number of packets that exceeds a preset DoS limit in the associated rule
7. DoS Time Window – for DoS rule violation, the time window in seconds the detection run associated with this finding covered
8. Detection Rule Identifier – identifier linked back to the applicable rule that has been matched
9. Description – details regarding the violation, for user consumption

**OUT-3.2** – The network mapping application produces a notification when new network elements are discovered. The notification contains the IP address of the newly discovered element, and the timestamp of discovery. The network mapping application also outputs a list of nodes to which the current network element can connect.

**OUT-3.3** – The machine learning application produces an anomaly score, IP address and data used to identify an anomaly.

**DATA-3.1** – This database will contain the records described in OUT-3.1. This data will be used by Layer 4 applications to make decisions based on detected rule violations.

**DATA-3.2** – This database will contain entries for devices discovered on the network, and a list of nodes to which each device can connect.

**DATA-3.3** – The machine learning alerts database will contain a list of anomalies which Layer 4 applications can use to make decisions.

## Layer 4 Logical Model

|  |  |
| --- | --- |
| Figure 4 – Layer 4 Logical Diagram | |
|  | |

### Layer 4 Components

**DATA 3.1, DATA 3.2, DATA 3.3.. DATA 3.N.** These data components reside in Layer 3. Each is associated with a specific application that generates description of anomalies. In this first embodiment of the Essence Cyber Security system, three layer 3 applications are specified (network change, violation of user specified rules, and anomaly detected by variation from established patterns). These are designated 3.1, 3.2, and 3.3. Future Layer 3 applications will be designated 3.4 …

**DB 4.1** – This database will be a concatenation of DATA 3.1 … DATA 3.n in chronological order.

**APP 4.1** – The application will receive notice of new entries and determine if multiple new entries (from one Layer 3 application or several) should be treated as a single event or multiple events.

**APP 4.2** - This is the key decision making application. Here, the event defined in App 4.1 and the information about the underlying anomalies is analyzed according to pre-defined rules developed over a period of operation. For some patterns – e.g. there is sufficient information to determine that a specific source of link is not trustworthy, a predetermined action can be initiated automatically or, alternatively, it can be presented for human review before an action is initiated. Known patterns will be stored in the Remediation Rules Database (DB-4.2)

In some cases, and particularly in the early days of operation of the system the pattern will not be recognized. In this case, the application will present as much information as possible regarding the nature of the anomalies and the possible (and possibly recommended) network changes to address the compromise. A human operator will determine a course of action. This can, optionally, be saved to the Remediation Rules Database (DB-4.2)

**DB 4.2** - The Remediation Rules Database will store known patterns of compromise in the form of source or link, and severity of compromise or risk and a remediation strategy such as (a) simply noting the event and not making any network changes, (b) shutting down a source of link, (c) embargoing the data, (d) substituting default value for the untrusted information, etc. Rules can be established through a-prior specification or saving a decision make in APP 4.2 in response to an actual event.

**APP 4.3** – This application IS NOT part of the initial implementation of the Essence Cyber Security Framework. It is listed here as a placeholder for future applications which can be used to assess the consequences of potential remediative network changes. This can range from models to reconfigure the network to dynamic power flow modeling to assess power flows under reduced control operations. An interface standard will be defined to allow open extension of the tolls available for analyzing consequences.

**DB 4.4** – Database 4.4 is a serial list of network change instructions from AP 4.2. It will also include a status field to show whether the change has been affected.

APP 4.4 - This application translates remediation actions determined in APP 4.2 and stored in DB 4.4 in the internal format of the Essence Cyber Security Framework (ECSF) into the format of the software defined networking package being used in Layer 5. It is likely, but not definite at this point, that the ECSF will use Openflow as its internal format because it is an established and tested open standard.

## Layer 5

Based on the availability, success, and continued development of software defined networking systems, including open systems such as Openflow, the Essence project will not develop a new Action layer. To do so is unnecessary and would dilute the drive towards an approach that can be shared within the industry. Therefore, we will develop to support and Openflow compliant system and possibly another system after discussion with other developers.

# Lab Testing View

This section describes the elements that are different from the logical design in the lab testing environment.

## Lab Testing Components



# Deployment View

The deployment view describes how the logical components in the logical view are deployed to physical network and servers. Performance, scalability, and capacity planning are key considerations, in addition to capturing the physical constraints and boundaries of the deployment environment. Each Layer 3 application will be deployed on an individual application server, and will be able to connect to the database server through the use of a LAN switch. The lab testing server (shown in blue below) will only be used for lab testing, and will not need to be deployed for the field testing phase.

## Deployment Diagram



# Contacts

| Contact | Title | Organization | Phone # | Email Address |
| --- | --- | --- | --- | --- |
| Robert Larmouth | Project Manager | NRECA | 603-930-9199 | robert.larmouth-contractor@nreca.coop |
| Craig Miller | Principal Investigator | NRECA | 703-626-9683 | Craig.Miller@nreca.coop |
| Evgeny Lebanidze | Managing Consultant, Development Team | Cigital, Inc. | 703-404-9293 x1237 | elebanidze@cigital.com |
| Chandu Ketkar | Technical Manager, Development Team | Cigital, Inc. | 703-404-9293 x1256 | cketkar@cigital.com |
| Ping Ning | Senior Security Consultant, Development Team | Cigital, Inc. | 703-404-9293 x1359 | pning@cigital.com |
| David Cleckley | Security Consultant, Development Team | Cigital, Inc. | 703-404-9293 x1231 | dcleckley@cigital.com |
| Jeff Schneider | Development Team | CMU | 412-268-2339 | schneide@cs.cmu.edu |
| Zico Kolter | Development Team | CMU | 412-268-4733 | zkolter@cs.cmu.edu |
| William Hutton | Testing Team | PNNL | 509-371-6695 | William.hutton@pnnl.gov |
| Philip Craig | Testing Team | PNNL | 509-430-1153 | [Philip.craig@pnnl.gov](mailto:Philip.craig@pnnl.gov) |