INL/EXT-11-23408
Rev. 1

INL Control System Situational Awareness Technology Annual Report 2012

Gordon Rueff
Bryce Wheeler
Todd Vollmer
Tim McJunkin
Robert Erbes

October 2012

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

PROJECT TEAM: INL NSTB PROGRAM TEAM

INL Management:
DOE-ID Project Lead: John Yankeelov
INL Management Liaison: Curtis St Michel
Program Manager: David Kuipers

Technical Team:
Program Cyber Researcher Support Team:
Jared Verba, Corey Thuen, Ken Rohde, Robert Erbes, Kent Kvarfordt, James Thomas, Larry Wellman, Ann Egger

Program Researcher Support Team:
John Buttles, Eric Larsen, Mark McKay, Karen Miller

Academic Team:
Milos Manic (Univ of Idaho), Grad Students (Univ of Idaho)

Program Support:
Program Financial Consultant: Ben Watts
Program Legal Consultant: Rick Evans
Senior Writer: Zack Adams
Administrative Support: Karen Daniel, Julie Irving
Web Support: Shad Staples, Desiree Reagan, David Loynd
Commercialization: Mark Kaczor, Charity Follet, Kathleen Bohachek

INL/EXT-11-23408
Rev. 1

INL Control System INL Control System Situational Awareness Technology Annual Report 2012

Gordon Rueff (Sophia)
Bryce Wheeler (Mesh Mapper)
Todd Vollmer (Intelligent Cyber Sensor)
Tim McJunkin (Data Fusion)
Robert Erbes (Demonstration)

October 2012

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

ABSTRACT

This report provides project status for FY 2012 work performed on the Sophia Tool, Mesh Mapper (MM) Tool, Intelligent Cyber Sensor (ICS) Tool, and Data Fusion Tool (DFT) situational awareness projects based on requirements of the Idaho National Laboratory (INL) Control System Situational Awareness Technology proposal (July 2010). This report is derived from status reports provided by five individual principle investigators who are the leads over the tasks associated with this project.

EXECUTIVE SUMMARY

Securing the country's energy sector infrastructure from cyber attack is critical to the well-being of the American people, which can be adversely affected by a successful cyber attack on energy sector utilities. Idaho National Laboratory (INL) is addressing this challenge through research and development of an interoperable set of tools that safeguard critical energy sector infrastructure. Each is designed to function either as a stand-alone capability or they can be integrated in a variety of customized configurations based on the end user's risk profile and security needs. Each tool is listed below with a brief description of capabilities.

The **Sophia Tool** provides users a thorough view of their control system and wired sensor networks, allowing a detailed review of conversations that are occurring.

The **Mesh Mapper (MM) Tool** was intended to collect the routes taken by Supervisory Control and Data Acquisition (SCADA) system Wireless Mesh Network (WMN) data messages and track them in such a way the operator can readily observe any abnormal behavior of wireless sensor networks.

The **Intelligent Cyber Sensor Tool** distinguishes between component failure and cyber security incidents and monitors the overall health of a system.

The **Data Fusion System** identifies, reduces, and characterizes data, providing integrated situational awareness of the cyber and operational health of the control and sensor system.

A **Demonstration** task was included in year 2 of this project to show interoperability of the tools in the Situational Awareness Suite. The tools included in this project were demonstrated to DOE-OE and industry attendees on August 29, 2012.

Each of the above tools or technologies and the demonstration task comprises one main section of this report. In addition to FY 2012 task completion, each section provides additional detail and addresses development, test, and demonstration results and commercialization activities as required by the INL Control System Situational Awareness Technology proposal (July 2010) work scope, Task 8.0, "Final Report," Page 32.

CONTENTS

TABLES

ACRONYMS

ADMT	Advanced Data Mining Technique
AMI	Advanced Metering infrastructure
AP-title	Access Point Title
CAES	Center for Advanced Energy Studies
CI	Computational Intelligence
CR	Cell Relay
CRADA	Cooperative Research and Development Agreement
DFT	Data Fusion Tool
DHP	Dynamic Honeypot
DOE	Department of Energy
FLA	Fujitsu Laboratories of America, Inc.
FLS	Fuzzy Logic System
GUI	Graphical User Interface
HUD	heads-up display
IAA	Intelligent Anomaly Assessment
ICS	Intelligent Cyber Sensor
IDR	Invention Disclosure Records
IFP	Idaho Falls Power
INL	Idaho National Laboratory
IP	Internet Protocol
IT2 FL	Interval Type-2 Fuzzy Logic
MM	Mesh Mapper
NEI	Network Entity Identification
NetAPT	Network Access Policy Tool
POC	Proof of Concept
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
WMN	Wireless Mesh Network

INL Control System Situational Awareness Technology Annual Report 2012

1. SOPHIA PROJECT

The Sophia Tool is a software development research effort to create a new tool for fingerprinting and monitoring Supervisory Control and Data Acquisition (SCADA) systems. Sophia is intended to provide users with reliable information for decision-making that enhances the security and resilience of their SCADA system. The Sophia concept is designed as a passive, real-time tool for inter-device communication discovery and monitoring of the active elements in a SCADA system.

This section provides an update on the FY 2011 and 2012 task completion and final reporting requirements for the Sophia project, as defined in the Idaho National Laboratory (INL) Control System Situational Awareness Technology proposal (July 2010).

1.1 Summary of FY 2011 Tasks for the Sophia Project

The project work scope identified three FY 2011 tasks for the Sophia project: Beta Software Development, Roll Out Alpha Software to Asset Owner Collaboration companies, and Identify and Establish Commercialization Partnership. Year 1 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 28:

1.1.1 Subtask 1.1.1 – Beta Software Development

This task will include activities to develop the Sophia Beta software including basic architecture, data collector, data aggregator, client, graphical user interface, and security software development.

Task Status: Complete FY 2011. Copyright assertion was granted April 8, 2011 for the alpha Sophia software, CW-11-03.

1.1.2 Subtask 1.1.2 – Roll Out Alpha Software to Asset Owner Collaboration companies

Install software in asset owner alpha sites. Collect feedback from beta sites and incorporate into system configuration. Perform formal final design review. Document issues and responses and mitigate findings.

Task Status: Complete FY 2011.

1.1.3 Subtask 1.1.3 – Identify and Establish Commercialization Partnership

Determine best candidate companies to rollout the production version of Sophia in year 2. Select best prospect and establish a tech transfer partnership to support year 2 work scope associated with product rollout to industry.

Task Status: Technical deployment of Sophia is ongoing in year 2. The process of intellectual property capture and application, legal documentation, and commercialization activities has

required more effort than originally anticipated. The effort was initiated in year 1 with capture of intellectual property and processing of copyright and patents. Market surveys were completed by the technical deployment department. Selection of best candidate will not occur until last quarter of year 2 of the project.

1.2 Summary of FY 2012 Tasks for the Sophia Project

The project work scope identified three FY 2012 tasks for the Sophia project: Advanced Functionality Software Development, Tech Transfer Production Software to Commercialization Entity, and Support Commercial Distribution to Industry. Year 2 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 28-29:

1.2.1 Subtask 1.2.1 – Advanced Functionality Software Development

Task description from the work scope: This task will include activities to develop advancements to the Sophia software. Work with University of Illinois (collaboration partner) to develop a standard format for data communications of network objects between the INL Tool Set technologies and add-in applications, e.g. NetAPT.

Task Status: Copyright assertion for the Sophia Beta software was granted August 23, 2011. Task was completed, Aug 29, 2012. While specification of intercommunications between the Sophia software and NetAPT was initiated in year 1, the subcontract for University of Illinois was let in year 2 and interoperability design and testing were completed.

1.2.2 Subtask 1.2.2 – Tech Transfer Production Software to Commercialization Entity

Task description from the work scope: Transfer the Sophia Production Software to the commercialization entity.

Task Status: See Section 1.1, Subtask 1.1.3 status. Concurrence was received from DOE-OE CEDS PM to move Subtask 1.2.2 to January 31, 2013.

1.2.3 Subtask 1.2.3 – Support Commercial Distribution to Industry

Task description from the work scope: Support broad rollout of the software through existing asset owner and vender relationships. Provide support for technical issues in the initial rollout period during year 2.

Task Status: See Section 1.1, Subtask 1.1.3 status.

1.3 Summary of FY 2012 Reporting Requirements for the Sophia Project

The project work scope identifies the following FY 2012 reporting requirements for the Sophia project: development, test, and demonstration results; and commercialization activities.

1.3.1 Development, Test, and Demonstration Results

Software development has resulted in some high-quality alpha software that exhibits the features identified in the proposal. The development process was hindered slightly in its goals by not acquiring the

desired level of feedback from industry during alpha testing. This lack of feedback and its integration into the development process needs to be corrected during the beta development process.

Alpha testing occurred on a smaller scale than anticipated. The issues causing the smaller rollout have been fixed and beta rollout has occurred smoothly. None of the alpha testers provided feedback that resulted in changes to Sophia; however, the testers consistently needed better documentation from the developers on how to use Sophia.

Feedback from alpha testing prompted improvements in documentation and user feedback tools for the beta test. Documentation control methods were put in place to make sure that the use of a feature is fully documented and available to the testers during the beta. This documentation was provided through a Wiki developed and maintained by the Sophia project team. Software distribution mechanism for Sophia and its documentation along with feedback collection mechanism for testers is a MediaWiki-based Internet portal. This website is available at https://sophia.inl.gov to approved beta test participants.

Sophia was undergone 638 software revisions as of 9-18-2012 during FY 2012. These include feature additions, bug fixes and minor code changes. Here is a list of some of the more significant features and refinements made.

Features:

- Inter-device SSL communications based on GnuTLS library.
- Display Sophia alerts in OglNet with heads-up display (HUD) 3D integration.
- OglNet supports camera position saving and move to functionality.
- Fully implemented builder mode with bubbling, host and subnet user relocation and configuration saving.
- Implemented a plugin architecture for networking that allows Sophia to quickly use different transport layers such as Transmission Control Protocol (TCP), TLS, libssh, etc.
- Added fly to host capability to OglNet.
- Packet replay speed is controlled by up / down arrows.
- Added a menu system to OglNet's HUD.
- Implemented a disperser plugin architecture that allows Sophia to quickly add new output types such as MySQL and IF-MAP.
- OglNet now supports toast and status messages.
- Implemented VruiNet which is a virtual reality enhancement to OglNet.
- Implemented IF-MAP communications to support integration with NetAPT, Intelligent Cyber Sensor (ICS), and Data Fusion Tool (DFT).

Refinements:

- Improved scrolling in OglNet HUD.
- Easier installation process.
- Integrated the command line option parsing with help message so that CLI help messages will always match actual use.
- Updated logging facilities to support separate developer and release settings while also reducing logging computation time.
- Started to use static code analysis tools to improve code quality.
- Graphical improvements to world map.
- Mousing over a channel in the tree makes the 3D representation "glow".

- Separated the packet capture functionality of sophiad into its own executable packetd.
- Updated GeoIP code to use MaxMind's latest database set and allow testers to update the database at will.

There are still 2 outstanding feature requests that the Sophia developers would like to implement with the additional time gained by commercialization delay: alerts via email and logging via Syslog. Most of the feedback in feature requests concentrated on additional output modes rather than input modes such as consuming NetFlow. This surprised the development and seems to indicate that the testers making the requests are looking to integrate Sophia information into an existing security / alert architecture rather than using Sophia as an end tool. This was not unforeseen but use of Sophia directly was expected to occur first with additional input requests.

While 29 beta testers were sufficient to receive feedback on most features, it was significantly short of reaching the critical mass necessary to create a self sustaining user group. What this means is that there were not enough testers to receive feedback on other tester feedback. This largely eliminated the usefulness of using a Wiki and public ticket tracker since each interaction was only engaged by a single tester and the development team. Future projects should try to engage a larger testing demographic, preferably anyone that is interested, and then prioritize feature requests on which organization is making the request. Bug reports would receive developer attention based on the normal factors that affect bug fixing regardless of the demographic of the bug submitting entity.

Integration

In order to integrate Sophia with other tools in the Situational Awareness suite, Sophia had to implement an IF-MAP interface. This interface needed to publish Sophia channels, hosts, and alerts and subscribe to alerts generated by NetAPT.

The integration between Sophia and NetAPT highlighted a number of potential use-cases:

- Use Sophia to identify hosts and communications that are not already present in the firewall configurations or policy.
    - Identify communications that bypass the firewalls.
    - Identify specific hosts and channels within a subnet for a more precise firewall.
- Use Sophia to identify unused holes in a firewall.
- Use NetAPT to flag communications that violate policy or firewall rules.
    - These communications may violate policy but not the current firewall configurations.
    - Some communications may violate firewall configurations by using alternate routing methods.

The integration was successful; however, the technology used to integrate should be avoided in future work. IF-MAP is buggy and not actively developed anymore. The main reason that the Sophia team liked the idea of using IF-MAP was its publisher / subscriber model. Unfortunately to get the IF-MAP library to function that model had to be ditched in favor of regular polling and pushing. This could have been accomplished using any SQL based database and would have been much less time consuming to implement. The disperser plug-in architecture of Sophia allows it to quickly switch integration communication methods if that becomes necessary.

1.3.2 Commercialization Activities

Commercialization collaborator selection is being supported in the last quarter of year 2 to meet fairness of opportunity requirements and refine the criteria used to select the commercial collaborator. Final criteria have been finalized.

1.3.3 Milestones

Title: Beta Software Ready for Field Testing
Planned Date: 12 months after project initiation

Verification Method: Software review. Status: Beta software was published September 30, 2011 to the SophiaWiki website.

Title: Complete Tech Transfer of Production Software
Planned Date: 24 months after project initiation

Verification Method: Software delivered to Commercialization entity. Milestone changed to January 31, 2013 with DOE-OE CEDS concurrence.

1.4 Summary

1.4.1 Accomplishments

In year 2 for Sophia, 29 beta testers are using Sophia in some capacity in their utility operations. Commercialization is on track to be completed in January 2013. Integration between Sophia and other Situational Awareness tools was shown as viable and useful by DOE-OE and industry reviewers in multiple forums.

1.4.2 Path Forward

Sophia software development is almost done but commercialization has been delayed until January 2013. During this time extension:

- Beta testing has been extended until a commercialization partner is ready.
- Select features will be implemented based on feedback and available funding.
- Commercialization will finish with the selection of a commercialization partner.

2. MESH MAPPER PROJECT

The Mesh Mapper (MM) Tool was intended to passively collect the route information of a Wireless Mesh Network (WMN) and graphically present this information for quick analysis. This section provides an update on the FY 2011 and 2012 task completion and reporting requirements for the MM project, as defined in the project work scope.

2.1 Summary of FY 2011 Tasks for the Mesh Mapper Project

Three MM tasks are defined for FY 2011: Proof of Concept (POC) Functional Requirements Development, Proof of Concept Software Development, and End of Year 1 Design Review and Go/NoGo Decision. Year 1 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 29:

2.1.1 Subtask 2.1.1 – Proof of Concept Functional Requirements Development

This task will include research activities to develop the WMN methods and technologies used in industry. The task focus shall be on standards-based systems that have obtained significant market penetration. Collect data from various sources, including INL collaboration partners, Work with asset owner and vendor companies to establish relationships that will lead to collaboration in analysis of routing data sets and testing sites for the tool.

Task Status: Complete FY 2011.

2.1.2 Subtask 2.1.2 – Proof of Concept Software Development

Analyze the routing data sets to develop functional requirements for the tool design. Develop the Proof of Concept software for the Mesh Mapping Tool. Operate Proof of Concept software in WMN system to demonstrate functionality and collect feedback on operation.

Task Status: Complete FY 2011.

2.1.3 Subtask 2.1.3 – End of Year 1 Design Review and Go/NoGo Decision

Perform an informal design review with collaboration partners, task team and peers to document successes and issues with the software design. Document the feedback and response from the review. Task lead, team, program manager, and DOE PM will make a Go/No-Go decision on how to proceed.

Task Status: Complete FY 2011. The MM project has been cancelled based on a No-Go recommendation provided by the project team and concurrence received from the DOE-OE CEDS PM.

2.2 Summary of FY 2012 Tasks for the Mesh Mapper Project

Three MM tasks are defined for FY 2012: Beta Software Development and Commercialization Partnerships, Roll Out Beta Software to Asset Owner Collaboration companies, and Identify and Establish Commercialization Partnership. Year 2 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 29:

2.2.1 Subtask 2.2.1 – Beta Software Development and Commercialization Partnerships

This task will include activities to develop the beta software. Determine best candidate companies to rollout the production version of the software. Select best prospect and establish a tech transfer partnership to support product rollout to industry.

Task Status: Cancelled, see Section 2.1.3, Task Status.

2.2.2 Subtask 2.2.2 – Roll Out Beta Software to Asset Owner Collaboration companies

Install software in asset owner beta sites. Collect feedback from beta sites and incorporate into system configuration. Perform formal final design review. Document issues and responses and mitigate findings.

Task Status: Cancelled, see Section 2.1.3, Task Status..

2.2.3 Subtask 2.2.3 – Identify and Establish Commercialization Partnership

Tech Transfer Production Software to Commercialization Entity and support broad rollout of the software through existing asset owner and vender relationships. Provide support for technical issues in the initial rollout period.

Task Status: Cancelled, see Section 2.1.3, Task Status..

2.3 Progress made up to No-Go decision

The MM team implemented a base framework that is capable of parsing, storing, analyzing, and displaying mesh network data. The only protocol analysis module currently implemented is for the Internet Protocol (IP). However, the modular design of the framework makes it easier to add other protocol analysis modules in the future. The reason for only implementing the analysis module for IP is two-fold. The first is because vendors like Itron are moving towards standards-based smart metering communications (e.g., Itron partnership with Cisco to provide full IPv6 smart metering communications[a]). The second is that we were unable to identify any widely used mesh protocols that contain Dynamic Source Routing (DSR) information that can be extracted passively from backhaul links.

Routes exhausted in an effort to engage industry:

- The project team worked directly and through Idaho Falls Power (IFP) to establish a dialogue with Elster and Tropos to collect data sets. This route was very hopeful, but to date has not resulted in successful teaming with the vendor.
- IFP is a participant in an ARRA-funded demonstration project to field many smart grid technologies and is a very willing partner with the INL to further research and development work; however, they are just initiating their Advanced Metering Infrastructure (AMI) installation project.
- Itron was our initial partner but they were not able to support the project due to business constraints.

[a] Reference: https://www.itron.com/partners/Pages/Cisco.aspx

- Fujitsu Laboratories of America (FLA), Inc., is very interested in participating and we have a Cooperative Research and Development Agreement (CRADA) with them to support AMI system tasks on a microgrid configuration; however, they reviewed their protocol specification and indicated it does not contain required DSR data.
- Data collection efforts were also worked through Austin Energy and Oncor Electric to work with their Landis+Gyr vendor. Business constraints and other issues outside our control prevented success with the utilities to share data.

Without the ability to track the routes a packet takes through the mesh it is not possible to achieve the MM project goal to track a packets route within the mesh network. The basis for this conclusion comes from a previous analysis of the Itron C12.22 protocol and input from FLA that no current industry mesh protocols appear to provide the information necessary to effectively monitor a mesh network. Initially, it was believed that ITRON and related protocols contained sufficient data that could be passively extracted to determine packet routes. It was this notion which prompted the MM tool concept. However, vendor feedback from FLA and Elster along with research of the Itron protocol c12.22 showed that DSR is not part of the main industry protocols. Conversation with a senior scientist with Applied Communication Sciences revealed a similar belief that based on current knowledge about industry protocols there do not appear to be any mechanisms to support sufficient mesh monitoring. Thus, it is the recommendation of the MM team that a No-Go decision be made for continuing development of the currently proposed MM tool at this time. However, feedback from Applied Communication Sciences, IFP, FLA, Elster, and the research community suggest that there is sufficient interest in this topic to warrant further research.

A presentation covering the work of MM was presented to DOE-OE and industry on August 29, 2012. The presentation covered a timeline of the work and challenges faced over the course of the project. It also discussed the reasons behind the recommendation of a no-go decision. It also offered suggestions for moving forward with additional research and developing partnerships with industry.

2.4 Summary of FY 2012 Reporting Requirements for the Mesh Mapper Project

The project work scope identifies the following FY 2012 reporting requirements for MM: development, test, and demonstration results; and commercialization activities.

2.4.1 Development, Test, and Demonstration Results

The current MM tool is able to parse Itron's C12.x protocol and store information about communications of the high-level meters into a database. The visualization engine was in the design phase when work was stopped on MM. Integration of the packet parsing engine and the visualization engine remains to be completed.

Testing of the MM tool using the traffic captures obtained during the Itron assessment shows that the tool operates as designed, but limitations of the data set do not thoroughly test its ability to parse the C12.x protocol; therefore, additional testing with industry-provided data or site testing is needed to fully validate parsing algorithms.

2.4.2 Commercialization Activities

No commercialization efforts will be performed for this project as the task has been cancelled.

2.4.3 Milestones

Title: POC Informal Design Review; Go/No-Go Decision

Planned Date: 12 months after project initiation

Verification Method: POC informal design review. Status: A No-Go decision was recommended by the project team and concurrence was received from the DOE-OE CEDS PM based on the outcome of the Informal Design Review.

Title: Complete Tech Transfer of Production Software
Planned Date: 23 months after project initiation

Verification Method: Software delivered to Commercialization entity. Status: Cancelled

2.5 Summary

2.5.1 Accomplishments

The initial functional design requirements were completed at the beginning of FY 2011. The core functionality for a parsing engine for the C12.X protocol has successfully been developed. The parsing engine can currently do the following:

- Display unique Access Point-Titles (AP-titles) associated with a meter, cell relay, and the collection engine.
- Determine and display the node type of a given AP-title: meter, cell relay, or collection engine.
- Identify and display who has communicated with a given AP-title.
- Record and display the last time an AP-title communicated.
- Record and display the number of times an AP-title was either calling or being called.
- Determine and display the current Cell Relay (CR) that a meter is using.
- Calculate and display total number of known meters/devices on the network.
- Began development of a Java Graphical User Interface (GUI) front end and the design for integrating it with the parsing engine.

2.5.2 Path Forward

Based on the overall efforts of the MM project there is a need to research current mesh network monitoring capabilities and provide recommendations for enhancing them in the future. Research efforts should focus on:

- Existing vendor and third party monitoring capabilities and developments,
- Utility and asset owner desired capabilities for mesh network monitoring, current protocol capabilities and developments to support mesh monitoring,
- Analysis of the current mesh network standards.

The results of this research could be published in a white paper that details the findings and could provide recommendations for enhancing current and new standards that will be used by industry to improve mesh network monitoring capabilities.

3. INTELLIGENT CYBER SENSOR PROJECT

The Intelligent Cyber Sensor (ICS) looks at the expected traffic for each group of smart grid sensors and has a highly efficient mechanism of monitoring and filtering network performance data. When integrated with NetATP, the ICS seeks to more effectively implement security policy, flag degradation trends in the associated sensor subsystem, and present information in an efficient, ergonomic fashion.

This section provides an update on the FY 2011 and 2012 task completion and reporting requirements for the ICS project, as defined in the project work scope. All references to a test or development system refer to a wireless test bed maintained by INL at the Center for Advanced Energy Studies (CAES). The details of the test bed are described in the Data Fusion section.

3.1 Summary of FY 2011 Tasks for the Intelligent Cyber Sensor Project

The project work scope identifies three FY 2011 tasks for the Intelligent Cyber Sensor Project: Alpha Technology Development, Identify and Establish Commercial Partner(s), and Verification Testing. Year 2 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 30:

3.1.1 Subtask 3.1.1 – Alpha Technology Development

This task will include activities to develop the Alpha technology and perform a mid-yr informal design review. Document issues and responses from the design review and perform mitigations to the technology design.

Task Status: Completed in 2011, with Go decision outcome.

3.1.2 Subtask 3.1.2 – Identify and Establish Commercial Partner(s)

Identify and develop partnerships with commercial partners for testing and potential commercialization of technology.

Task Status: CRADA with FLA as a potential participant in testing technology. Completed 2012.

3.1.3 Subtask 3.1.3 – Verification Testing

Perform verification testing of the cyber sensor against design specifications. Use feedback from partners in verification testing to incorporate into the tool configuration. Perform a year end informal design review based on design specifications and perform mitigations to the software design.

Task Status: Testing performed with design review complete. Completed 2012.

3.2 Summary of FY 2012 Tasks for the Intelligent Cyber Sensor Project

The project work scope identifies three FY 2012 tasks for the Intelligent Cyber Sensor Project: Alpha Technology Integration and Commercial Involvement, Develop Beta Version of Technology for Demonstration, and Roll Out Beta Software to Collaboration Partners and Demonstration Technology. Year 2 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 30:

3.2.1 Subtask 3.2.1 – Alpha Technology Integration and Commercial Involvement

Task description from the work scope: Finalize commercial partner(s) and install the alpha version with a commercial system(s) for integrated testing. This task will include activities to collect data that will be used to develop the beta version of the technology. Document issues and responses from the design review and perform mitigations to the technology design. A Go/No-Go decision will be made when ready to proceed to Task 3.1.2.

Task Status: CRADA was signed with FLA . The design review was performed, a Go decision was recommended by the project team, and concurrence given by DOE-OE CEDS PM.

3.2.2 Subtask 3.2.2 – Develop Beta Version of Technology for Demonstration

Task description from the work scope: Develop a beta version of the technology for final demonstration. Revise the data communications interface specification based on lessons learned from Data Fusion Tool (DFT) Task 4.1.2.

Task Status: Beta version of the ICS was developed and tested in the final project demonstration task integrated with the Data Fusion project and Sophia. Completed August 29, 2012. On August 29, 2012 a successful public demonstration showed the integration of ICS with the Data Fusion and Sophia components. The systems used a 'cleansed' version of operational network data from Idaho Falls Power. The ICS detected the network hosts, created virtual honeypots and delivered anomaly behavior messages.

3.2.3 Subtask 3.2.3 – Roll Out Beta Software to Collaboration Partners and Demonstration Technology

Task description from the work scope: Install technology in commercial partner beta site(s) for demonstration. Collect feedback from beta sites and incorporate into system configuration. Perform formal final design review. Document issues and responses and mitigate findings.

Task Status: We established a CRADA with FLA to explore implementation possibilities in areas of security and data fusion. An Invention Disclosure Record (IDR) was filed with the INL Technology Deployment group. The review of the IDR submitted is that the technology is not patentable due to publications. The project will not be commercialized in this work scope. The current deliverable consists of the technology as developed at the end of the project as well as the publications that have been and will continue to be developed in support of the research and development process.

The technical deployment of the ICS was discussed during the integrated demonstration meeting. With the small but operationally significant error rates in the alerts of the sensor, the technology needs further development prior to technical deployment. Our hope was that the R&D would take us to that point by 9/30/12, however further work is needed to attain that production level goal. While this milestone was not technically achieved, the research and development team have made great strides in moving this work forward and this project has been a very significant success as noted by vendors and utilities that attended the demonstration meeting.

Error Discussion Details

To enhance the cyber security of a network system various approaches can be applied. One approach, utilized by the ICS is anomaly detection. An anomaly detection system is trained on a set of 'normal' network behavior. The extracted behavior model is then used to detect anomalous behavior in newly observed testing data. Two possible difficulties with this approach are identified as follows. First, building a single comprehensive normal behavior model for a specific network communication system is difficult due to the complexity of the network and the presence of multiple diverse communication streams. Second, the performance of our anomaly detection algorithms can be tuned by adjusting a sensitivity threshold. The selection of a specific threshold value inevitably results in a tradeoff between false negative and false positive rate. Hence, determining the suitable sensitivity threshold value constitutes an important design problem.

The project proposed and implemented a novel anomaly detection architecture to alleviate these two issues. The system first identifies individual communication streams in the overall network traffic and then individually applies a developed network security cyber-sensor algorithm to selected streams. This approach allows for learning accurate normal behavior models specific to each network communication stream. In addition, an Interval Type-2 Fuzzy Logic System (IT2 FLS) is used to model human background knowledge about the network system and to dynamically adjust the sensitivity threshold of the anomaly detection algorithms. The IT2 FLS is used to model the linguistic uncertainty in describing the relationship between various network communication attributes and the possibility of a cyber attack. For instance, if only a small number of distinct communication protocols is expected to be used during the normal network communication, a linguistic rule can be created that sets a lower sensitivity threshold when a high number of distinct communication protocols appear in the network communication. Hence, the IT2 FLS is not used directly for detecting anomalous network traffic, but it is only used to utilize the provided human domain knowledge to tune the performance of the clustering based anomaly detection algorithm by dynamically adjusting the sensitivity threshold.

The proposed anomaly detection system was implemented and tested on an experimental control system test-bed. It was demonstrated that the system does learn normal behavior models for each selected communication stream and performs accurate anomaly detection. In addition, it was also demonstrated that the availability of domain knowledge can improve the performance of the anomaly detection method.

Table 1. Classification Performance for Stream 1.

Threshold	Correct Rate	False Pos.	False Neg.
0.3	99.8539%	0.1461%	0.0000%
0.6	99.8705%	0.1295%	0.0000%
0.9	99.8788%	0.1212%	0.0000%
IT2 FLS	99.8722%	0.1278%	0.0000%

Table 2. Classification Performance for Stream 2.

Threshold	Correct Rate	False Pos.	False Neg.
0.3	99.9037%	0.1217%	0.0275%
0.6	99.5504%	0.1082%	1.3753%
0.9	99.3799%	0.1082%	2.0079%
IT2 FLS	99.9111%	0.1116%	0.0275%

Tables 1 and 2 show results from monitoring two different hosts on the network while testing with intrusive activity. For comparison purposes the first three values in the Threshold column represent a fixed sensitivity value. The IT2 FLS row depicts the results of a sensitivity value that changes according to the human created logic rules. At first glance, a correct identification rate of 99.8722% and 99.9111% looks good. However, on our test network with 46 directly connected devices, 635,560 packets were captured over a 5 hour interval. If we assume that the performance monitoring of Stream 1 and 2 are representative of monitoring all devices, then 813 and 565 packets, respectively, would be misidentified. This equates to 813 false positives or alerts from the Stream 1 performance. For Stream 2 performance this means 462 alerts and 103 missed malicious packets. From a human operator perspective this number of alerts is relatively high in a 5 hour time frame. There is some variability in actual numbers as the intention is not to monitor all the devices and each device does not have an equivalent network volume.

3.3 Summary of FY 2012 Reporting Requirements for the Intelligent Cyber Sensor Project

The project work scope identifies the following FY 2012 reporting requirements for the Intelligent Cyber Sensor Project: development, test, and demonstration results; and commercialization activities.

3.3.1 Development, Test, and Demonstration Results

With the University collaborator, prototype software for the intelligent anomaly assessment (IAA), network entity identification (NEI), and the Dynamic Honeypot (DHP) has been implemented. These systems have been utilized on the development test system at CAES to generate results for evaluation of program operation.

3.3.2 Commercialization Activities

The project team worked with Tofino and FLA in identifying interest and potential participation in technology commercialization. As a result of the error rate issue remaining in this technology, however minute it is, significance is great enough that it is not yet ready for commercialization.

3.3.3 Milestones

Title: Alpha Informal Design Review; Go/No-Go Decision
Planned Date: 8 months after project initiation

Verification Method: Mid-year informal design review. Status: Completed, Year 1 with Go decision.

Title: Complete Tech Transfer of Production Technology
Planned Date: 23 months after project initiation

Verification Method: Technology delivered to Commercialization entity. Status: Not completed, see Section 3.1.3; Error Discussion Details.

3.4 Summary

3.4.1 Accomplishments

- Developed a deployable modular framework on a commonly available hardware platform with components that provide network host information, identify anomalous network traffic behaviors, and deploy dynamic virtual honeypots. Configuration burden is mostly removed from the human operator.

- System developed on a network containing wireless systems from Emerson, Honeywell and Archrock. PLC's from National Instrument and Rockwell were attached as well. Finally an AMI solution from FLA completed the network hardware tested.

- An Alpha integration test with Sophia and Data Fusion was conducted using real world data from IFP.

- Advanced the state of Autonomic Computing by applying fundamentals from the concept to security systems in industrial control networks.

- Advanced the state of Art in anomaly detection by applying domain knowledge encoded using IT2 FL rules. These rules linguistically describe the relationship between various features of the

network communication and the possibility of a cyber attack and improve the performance of anomaly detection.

- Identified deficiencies and corrections for a commonly used open source Honeypot implementation.
- Published details of research in 4 IEEE conference proceedings and 2 pending IEEE Transaction special sessions.

3.4.2 Path Forward

The original plan for this project was to move the ICS technology to industry deployment. However, due the remaining error rate discussion detailed in Section 3.2.3, the project was not able to attain that goal. The project recommendation is to move this concept to an Industry led project to seek a workable solution to deal with the remaining error rate in order to make this technology a viable product for use in a production utility environment.

4. DATA FUSION SYSTEM PROJECT

The Computational Intelligence (CI) Advanced Data Mining Techniques (ADMTs) combine multiple temporal/spatial, highly diverse data streams into a unified data model, then identify relationships and frequent data patterns that are common to SCADA and sensor systems, such as typify smart grids. As a result, resilient data fusion (generation of actionable intelligence) is achieved via various CI techniques. The Data Fusion Tool (DFT) is intended to couple the cyber health and operational performance aspects of a sensor network, including smart grid components, to provide an overall network performance indicator.

This section provides an update on the FY 2011 and 2012 task completion and reporting requirements, where applicable, for the Data Fusion project, as defined in the project work scope.

4.1 Summary of FY 2011 Tasks for the Data Fusion Project

The project work scope identifies three FY 2011 tasks for the Data Fusion System project: Research Data Fusion Tool Requirements, Develop the Proof of Concept Data Fusion Software, and Verification Testing. Year 1 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 30-31:

4.1.1 Subtask 4.1.1 – Research Data Fusion Tool Requirements

Develop design specification for tool functionality.

Task Status: Completed in 2011.

4.1.2 Subtask 4.1.2 – Develop the Proof of Concept Data Fusion Software

Develop the Data Fusion software applications. Develop the Cyber Sensor Tool data communications interface specification.

Task Status: Completed in 2011.

4.1.3 Subtask 4.1.3 – Verification Testing

This task will perform a verification test of the POC technology and perform a year end informal design review based on design specifications. Document issues and responses from the design review and perform mitigations to the software design.

Task Status: Completed in 2011, with Go decision outcome.

4.2 Summary of FY 2012 Tasks for the Data Fusion Project

The project work scope identifies three FY 2012 tasks for the Data Fusion System project: Proof of Concept Software Development, Integration with Intelligent Cyber Sensor, and Demonstrate Tool Operation. Year 2 tasks are shown, with status, below:

Excerpt from "INL Control System Situational Awareness Technology" Project Plan, Sec 4.7.3, pg 31:

4.2.1 Subtask 4.2.1 - Proof of Concept Software Development

Task description from the work scope: Continue software design based on end of yr 1 design review.

Task Status: Complete.

4.2.2 Subtask 4.2.2 - Integration with Intelligent Cyber Sensor

Task description from the work scope: Verify communications interface of the Data Fusion Sensor with the Intelligent Cyber Sensor and sensor networks. Perform a design review of results against design specifications.

Task Status: Completed in 2012 with Design Review performed and documented.

4.2.3 Subtask 4.2.3 - Demonstrate Tool Operation

Task description from the work scope: Demonstrate interoperability of the data fusion, cyber sensor and sensor networks in ergonomically identifying and indicating cyber and operational health, and degradations thereof. Perform a final design review. Document issues and responses and mitigate findings

Task Status: Completed August 29, 2012 at the project Demonstration.

4.3 Summary of FY 2012 Reporting Requirements for the Data Fusion Project

The project work scope identifies the following FY 2012 reporting requirements for the Data Fusion project: development, test, and demonstration results; and commercialization activities.

4.3.1 Development, Test, and Demonstration Results

The following tasks have been performed:

- Combine diverse data streams from a sensor network, typical of a Smart Grid
  - Unified Data Structure for Sensor Data and Cyber Sensor Data
  - Integration with ICS and Sophia data.
- Identify relationships in data patterns through Computational Intelligence—Advanced Data Mining Techniques.
  - Metrics: correct detection of anomaly vs. false positives, time to detection
  - ADMT: assist in pointing to most important/interesting data even in the event of no detection alarm.
- Continue development of the graphical interface and integrate with the data source server.
- Show integration with Sophia and the ICS technologies at Demonstration

4.3.1.1 Demonstration Results

The system parts have been demonstrated individually to show a POC of the DFT at this time in the project. Concentration has been on the tools that are not application specific. Several aspects still pending testing within the DFT are mentioned here.

Geographical Context Visualization Tool

Concept has been shown to portray the graphical context with drill down capability. The prototype display is configurable to multiple data types and has features to enable play back or live data feed modes. The concept of responding to alerts created by Sophia or ICS have been defined but not yet tested.

Unified Data Model Tools

Data feeds enumerated have been input into SQL server through a standardized mechanism. SQL based data mining has been validated on previous data sets and is in process of evaluation for prioritization and prediction feasibility to this application. The focus has been on developing the keystone metric. One cost scenario has been run on data sets from a local utility to validate the capability with the SQL server.

Using measurements of total load and output, we are able to simulate estimated costs to users connected to the power grid. By normalizing the data, we have simulated what prices might be like during stage 1-3 power alerts and how they can be adjusted by changing power levels in our local grid.

Application Specific Acquisition

Each type of sensor provides data through different paths. The system has been successfully acquiring the available data for five months. The process sets of data are maintained on a data server in CAES for use by the DFT and ICS teams freely. Data sets have been provided to developers and collaborators. Yet to be completed is the interface to bring the AMI units data into the fold. The data sets are currently being archived but have only test loads. The AMI systems may indeed be an asset for future work when it is possible to install the meters in more interesting environments. The AMI sensors made their way into the project too late to have a significant impact but will have impact in future work with the team.

4.3.2 Commercialization Activities

There were no commercialization activities for the Data Fusion project; however, collaboration with FLA may produce a positive commercialization activity in the coming year.

4.3.3 Milestones

Title: POC Informal Design Review; Go/No-Go Decision
Planned Date: 12 months after project initiation

Verification Method: POC informal design review. Status: Completed, Year 1 with Go decision.

Title: POC Design Review; Go/No-Go Decision
Planned Date: 20 months after project initiation

Verification Method: POC informal design review. Status: Completed, Year 2 with Go decision.

4.4 Summary

4.4.1 Accomplishments

Team Completed demonstration of the DFT integrated with Sophia and ICS in September.

DFT progress is focused on the Geographic Context Visualization Tool (GCVT) and the integration with ICS and Sophia alerts through the IF-MAP publish/subscribe communication platform. Data prioritization methods have been applied to sensor data to determine correlated data feeds. This prioritization and correlation are captured in the visualization tool as with methods to show alternative

data when a particular data feed is compromised as identified by a cyber alert or system malfunction. Integration of Situational Awareness Tools was accomplished through IF-MAP interface.

Collaborative efforts with FLA continued. Discussions on interest in visualization tool are ongoing. They have potential interest in the GCVT. Continued to collaborate in forming value based metrics for health monitoring and potential optimization for energy systems.

Adaptive Critic and power models continue to develop and provide an additional virtual data feed to the data fusion tools. The work completed on this will be an asset for future INL and DOE projects. Two conference publications have been produced from collaborators at University of Idaho with funding credit to the project.

4.4.2 Path Forward

Potential for future use of the products of the project within INL and other projects are being pursued. Specifically, use for integrating a suite of resilient control system tools will carry on through LDRD support through the ICIS distinctive signature. Some interest found through discussions with industry representatives at the integration demonstration will be pursued as potential use of the technology and possible future funding. A small amount of funds for this task at INL and the subcontract with U or Idaho have been carried over to produce a technical article and consolidate and archive the tools that have been developed.

Many potential paths forward exist for this platform. Additional features for driving the GCVT via "backroom" data mining to automatically bring the most important information to the forefront and provide a comfortable but attention stimulating display for operators are possible and should be pursued with the input of human factor engineering principles. The DFT is adaptable to any analysis and prediction capability that the advanced data mining may provide. Any application requires analysis of the system for the "keystone" attributes for given operator, supervisor, and stakeholder contexts. This platform is readily adaptable to the needs of applications that require geographic context of the process information with a cyber aware need. Smart grids are just one such application for the GCVT data fusion tool. Higher-level decision advice can be provided by an adaptive critic mechanism through implementation of cost functions that provide guidance for demand response and utilization of dispatched local resources (e.g., energy generation or storage).

5. DEMONSTRATION PROJECT

INL researchers staged an integrated demonstration using a test bed. In the demonstration, data was collected by the Sophia Tool, which characterized the network conversations. Relying on feedback from Sophia, the NetAPT tool verified notional firewall configurations against high-level abstract specification of global access policy. The ICS was integrated with the Data Fusion system to ensure dynamic conformance to policy on an ongoing basis and suggest unexpected behavior. The Data Fusion mechanism demonstrated reduction, characterization, and identification of cyber health concerns to a visualization mechanism for ease of prioritization and response. The demonstration objectives for the Integrated Technologies of the proposed project are as follows:

- Test components in a real-world environment with varying configurations and connectivity
- Show interoperability between the complementary situational awareness project components to create a control systems security set of technologies.

5.1 Summary of FY 2012 Tasks for the Demonstration Project

The project work scope identified one FY 2012 task for the demonstration project, Interoperability Demonstration, which includes the following subtasks.

5.1.1 Subtask 5.2.1 – Commercial Integration

This task will include activities to demonstrate interoperability of technologies such as Sophia with the identified commercial partner's needs. This will include testing integrated with the commercial partner's parameters and technology needs.

Task Status: This task was completed through implementation of the NetAPT and Sophia tools in the IFP test. Completed Aug 29, 2012.

5.1.2 Subtask 5.2.2 – INL Tool Set Integration

This task will include activities to integrate all four of the technologies into an integrated solution in preparation for the integrated demonstration. Technologies will be tested in concert at the INL SCADA Test Bed on the INL site.

Task Status: Two interoperability demonstrations were developed due to differences in maturity level of the technologies. Completed Aug 29, 2012.

5.1.3 Subtask 5.2.3 – Integrated Demonstration

All four technologies will be demonstrated as an integrated control systems cyber security solution. The demonstration will include a variety of configurations and variables to show the full capabilities of the tools.

Task Status: Two interoperability demonstrations were performed. Completed Aug 29, 2012.

5.1.4 Subtask 5.2.4 – Final Report

A final report will be generated detailing the development, test and demonstration results, and commercialization activities of each technology and the tool set as a whole.

Task Status: Complete upon submission of this report.

5.1.5 Milestones

Interoperability Demonstration:
Title: Successful Integrated Demonstration
Planned Date: 24 months after project initiation

Verification Method: Demonstration is successful at INL SCADA Test Bed Status: Completed August 29, 2012.

Title: Annual Reports
Planned Date: 12 and 24 months after project initiation

Verification Method: Annual Reports delivered to PM. Status: Complete with delivery of this report.

5.2 Summary of FY 2012 Reporting Requirements for the Demonstration Project

The project work scope identifies the following FY 2012 reporting requirements for the Demonstration project: final report detailing the demonstration results.

5.2.1 Development, Test, and Demonstration Results

- Two demonstrations were successfully completed on 28 September 2012
    - The first, showing interoperability via IF-MAP between Sophia and University of Illinois Urbana Champagne's Network Access Policy Tool (NetAPT)
    - The second, showing interoperability via IF-MAP between Sophia and ICS and the (DFT).I
    - All tools (Sophia, NetAPT, ICS, and DFT) are integrated using the common IF-MAP schemas developed in Q3 FY 2012.
    - Demonstrations were run within a simulated representation of a small electrical utility's computer network.