SIEMENS

# Development and Demonstration of a Security Core Component

## Final Scientific/Technical Report

## Award Information


DOE Award Number
DE-OE0000517



Recipient
Siemens Industry, Inc.
10900 Wayzata Blvd.
Ste. 400
Minnetonka MN 55305-5602


Project Title
Development and Demonstration of a Security Core Component


Principal Investigator
Andy Turke, Siemens

Team Members
Bill Steiner, Siemens
David Taylor, Siemens
Wayne Olfert, Siemens
Bruce Oliver, Sacramento Municipal Utility District (SMUD)
Sabrina Poock, Siemens
Mark Flanary, Siemens



Acknowledgment
This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000517.

# Executive summary

In recent years, the convergence of a number of trends has resulted in Cyber Security becoming a much greater concern for electric utilities. A short list of these trends includes:

- Industrial Control Systems (ICSs) have evolved from depending on proprietary hardware and operating software toward using standard off-the-shelf hardware and operating software. This has meant that these ICSs can no longer depend on "security through obscurity.
- Similarly, these same systems have evolved toward using standard communications protocols, further reducing their ability to rely upon obscurity.
- The rise of the Internet and the accompanying demand for more data about virtually everything has resulted in formerly isolated ICSs becoming at least partially accessible via Internet-connected networks.
- "Cyber crime" has become commonplace, whether it be for industrial espionage, reconnaissance for a possible cyber attack, theft, or because some individual or group "has something to prove."

Electric utility system operators are experts at running the power grid. The reality is, especially at small and mid-sized utilities, these SCADA operators will by default be "on the front line" if and when a cyber attack occurs against their systems. These people are not computer software, networking, or cyber security experts, so they are ill-equipped to deal with a cyber security incident.

Cyber Security Manager (CSM) was conceived, designed, and built so that it can be configured to know what a utility's SCADA/EMS/DMS system looks like under normal conditions. To do this, CSM monitors log messages from any device that uses the *syslog* standard. It can also monitor a variety of statistics from the computers that make up the SCADA/EMS/DMS: outputs from host-based security tools, intrusion detection systems, SCADA alarms, and real-time SCADA values – even results from a SIEM (Security Information and Event Management) system. When the system deviates from "normal," CSM can alert the operator in language that they understand that an incident may be occurring, provide actionable intelligence, and informing them what actions to take. These alarms may be viewed on CSM's built-in user interface, sent to a SCADA alarm list, or communicated via email, phone, pager, or SMS message.

In recognition of the fact that "real world" training for cyber security events is impractical, CSM has a built-in Operator Training Simulator capability. This can be used stand alone to create simulated event scenarios for training purposes. It may also be used in conjunction with the recipient's SCADA/EMS/DMS Operator Training Simulator.

In addition to providing cyber security situational awareness for electric utility operators, CSM also provides tools for analysts and support personnel; in fact, the majority of user interface displays are designed for use in analyzing current and past security events. CSM keeps security-related information in long-term storage, as well as writing any decisions it makes to a (*syslog*) log for use forensic or other post-event analysis.

# Project goals

The first paragraph of the project's proposal in response to Funding Opportunity Number: DE-FOA-0000359 was:

> *This project will develop and demonstrate a Cyber Security Manger (CSM) component for a Supervisory Control and Data Acquisition/Energy Management System (SCADA/EMS, referred to as "EMS" hereinafter). CSM will monitor a wide variety of security-related components of a SCADA or EMS system and provide a centralized cyber security situational awareness and control capability for EMS operators. The project specifically addresses Topic Area 3, Situational Awareness Data Collection, Analyses, and Visualization, and supports Topic Area 1, Response to Cyber Attack in Progress, of the DE-FOA-0000359, although it is related to several other topic areas. CSM will be developed using or perhaps extending industry standards in such a way as to be open and adaptable to a number of SCADA and EMS system vendor platforms.*

The consensus at the time of the project's proposal was that it certainly was possible to determine the security posture of a complex system. However, it was necessary to use many tools to gather the required information. The long list of examples includes:

- Many anti-malware scanners available for Unix (Linux) systems store their results in proprietary log files, each of which must be examined at least daily.
- Modern systems employ digital certificates for various security purposes. Some large EMS systems may have hundreds to thousands of digital certificates. Because certificates have an expiration date and because the expiration of a digital certificate can result in loss of functionality, it was necessary to monitor their expiration dates.
- Firewalls issue *syslog* messages when a connect attempt is denied. It is important to monitor these, as large numbers may be indicative of an attempt by a bad actor to access a secure system.
- Some services (e.g., ftp, telnet) are typically not allowed in a highly secure SCADA system. Attempts to use such services may be indicative of an attack or reconnaissance attempt. As a result, it is necessary to monitor for attempts to access such services.
- Netflow data is very useful in detecting deviations from normal network traffic patterns. However, even in a modest sized network, the volume of Netflow data can be huge – millions of records per day – which is impossible to analyze without tools.

The intent was to build a tool that could provide situational awareness of the security posture of a large and complex SCADA/EMS/DMS system to an electric utility operator without requiring the operator to learn to use the array of tools that have been traditionally required. Furthermore, it would provide information and proposed actions in the operator's own language. Finally, the product would provide analytical tools that would allow support personnel to perform in-depth analysis both in near real time and post-event. The tool would be highly configurable to meet the needs of a range of utility customers and it would be easily portable to function with a range of vendor-supplied systems.

## Comparison of actual implementation to original goals

### Data Sources: comparison to original goals

Table 1: Data Sources lists a number of data sources that were mentioned in the project's proposal:

Table 1: Data Sources

| Data Source | Handling by CSM |
|---|---|
| EMS alarm subsystem | CSM uses the WBEM standard to exchange data with any host (server) that supports the WBEM standard. Because CSM is designed to use Perl "scripts" to implement this monitoring capability, it is easily expanded and easily ported. |
| EMS health monitoring subsystems, including independent health monitoring systems | WBEM implementations provide the capability to obtain performance statistics from monitored (Windows, Unix/Linux) servers. |
| Alerts and statistics from | Almost all computers and networking devices use *syslog* as a |

| Data Source | Handling by CSM |
|---|---|
| Intrusion Detection Systems (IDS) | log sink. Windows computers can be adapted to log to a *syslog* server.<br><br>The CSM design is quite *syslog*-centric. It includes the capability for an administrator to use a familiar Regular Expression Processor (RegEx) to parse and process the content of *syslog* messages. Systems which create *syslog* messages may be configured to send those messages directly to CSM (and) or CSM can receive messages from a log manager/SIEM.<br><br>Importantly (for forensics and other post-event analysis), CSM creates its own *syslog* messages to record decisions it makes, summaries of data collected, etc. |
| EMS communications subsystem | CSM uses the WBEM standard to monitor SCADA/EMS communications front end processors. |
| EMS RTU and ICCP link status | Because CSM can exchange data with the SCADA/EMS real-time database, it is a simple matter to obtain the current status from the SCADA/EMS. |
| EMS security-related telemetry (e.g. “gate open”, “door open” sensors) | This too is made possible by CSM’s ability to exchange data with the SCADA/EMS real-time database. Typically, a substation “door open” sensor is monitored by the SCADA as an RTU “point.” As described above, CSM can obtain this information from the SCADA database. |
| Network infrastructure components (e.g. routers, switches, firewalls) | CSM monitors network equipment through two mechanisms: 1) CSM’s ability to receive, parse, and process *syslog* messages and 2) its ability to receive and process Netflow data.<br><br>As described above, a router/firewall (for example) can be configured to issue a “connection denied” *syslog* message when a connect<br>attempt violates one of its firewall rules. CSM can be configured to parse these messages and issue an alarm if the number of connection denials exceeds a configured maximum in a configurable time period.<br><br>Netflow is a protocol originally provided by Cisco for use in their “high-end” switches. It has become quite popular and is now being offered in a wide variety of equipment from a growing number of vendors. Netflow data contains very detailed information about “conversations” through a network device. CSM receives and analyzes Netflow data to determine deviations from “normal” network traffic. |
| Log management (SIEM) system | CSM can receive *syslog* information from a Log Manager/SEM/SIEM. Testing with a LogRhythm device is part of the CSM demonstration project at Sacramento Municipal Utilities District (SMUD). Specifically, a sample configuration was implemented in the device to perform log message correlation using the LogRhythm “AI Engine;” when one of the correlation rules “fires,” a new *syslog* message is created which is, in turn, parsed and processed by CSM. |
| System statistics | As stated above, CSM uses the WBEM standard to obtain system statistics (e.g. CPU utilization, disk space, number of processes, etc.) WBEM implementations provide the capability to obtain performance statistics from monitored (Windows, Unix/Linux) servers. |

The project's proposal contained another table entitled "Sample CSM Inputs and Sources" (Table 1 on page 10-11 of the proposal). These sources are processed largely in the manner discussed in the proposal. However, there are some exceptions/changes that should be noted:

- Netflow was not specifically mentioned in the proposal. Although Netflow was originally implemented in 1990, it did not begin to achieve wide acceptance until the mid- to late-1990s. When detailed design of CSM began, it quickly became obvious that Netflow could serve as an important source of security-related data.

  To be more specific, devices which support Netflow collect detailed statistics about "conversations" (connections): source and destination IP addresses, source and destination ports/services, protocols, port changes, packet counts and sizes, etc. By comparing data obtained via Netflow which what is expected to be seen on a network, it becomes possible to detect deviations from "normal". This includes such things as:

  - Presence packets from unknown hosts on a network -- either an unknown host actually connected to the network or traffic from an unexpected source that managed to pass through a firewall.
  - Use of prohibited insecure ports/services (e.g., telnet, ftp).
  - Excessive traffic between known hosts. (CSM can also detect "below normal" traffic amounts between hosts.).

  Incorporating Netflow into CSM's design necessitated additional changes as well. Traffic between two hosts may pass through a number of network devices, each of which reports the same statistics (twice – once for the ingress and egress port). As a result, statistics are always reported at least twice and often many times. This necessitated development of a lossless mechanism to condense Netflow data; this was not part of the project's original proposal.

- The project team's original perceptions about how some data would be obtained did change. For example:

  - Through investigation, it was learned that some malware scanners write their results to proprietary log files (rather than *syslog*). This necessitated development of a process to scan those logs.
  - The ability to detect pending expiration of digital certificates became more important because of real-world reports of system malfunctions due to certificate expirations.

### Architecture: comparison to original proposal

The project's proposal contained a high-level diagram of a proposed conceptual architecture (Figure 1):

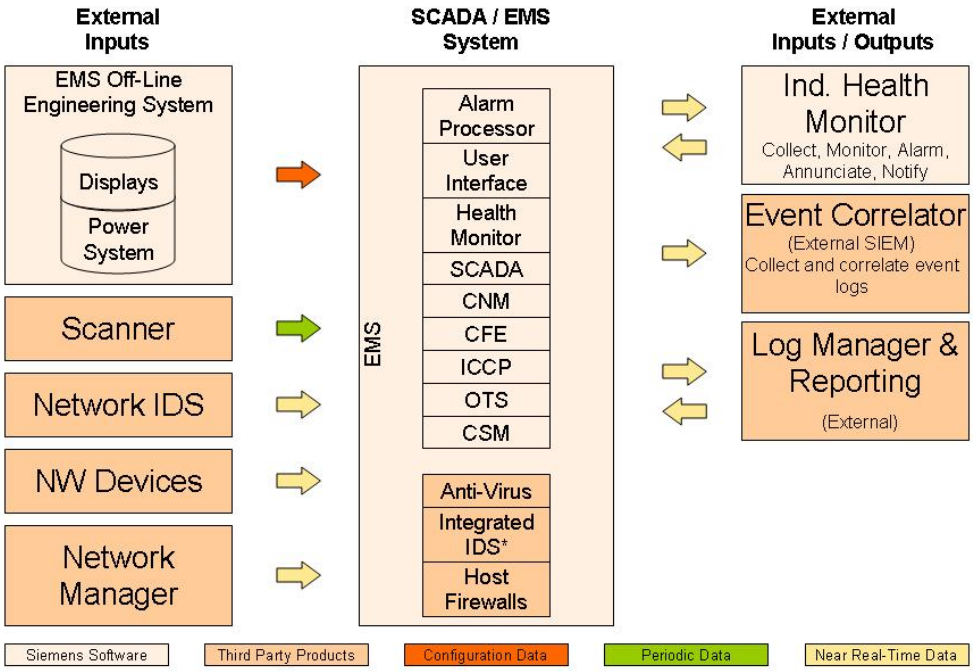


Figure 1: Proposed Conceptual Architecture

While the final architecture does contain all of the elements shown in this illustration, it does differ conceptually – most obviously in the fact that this illustration shows CSM as a component of the SCADA/EMS system. In the actual implementation, CSM resides on a separate computer system and (except for data exchange mechanisms) shares very little with the SCADA/EMS. The original architectural view made a number of assumptions about the architecture of the system to be monitored. As implemented, the architecture eliminates these assumptions, thereby facilitating use of CSM with SCADA/EMS products from other vendors.

A current high-level architectural view (from CSM product documentation) is shown in

Figure 2. This view gives a better representation of the data flows between CSM and those systems that it monitors. Notably, CSM is decoupled from the systems being monitored; this decoupling forces CSM to make fewer assumptions about the architecture of monitored systems. Furthermore, since the modified architecture makes use of industry standards for interaction with the systems being monitored, it minimizes requirements for creating gateways or "monitor daemon" processes that would otherwise reside on the monitored systems. This departure from the original proposal greatly simplifies portability for use with other SCADA/EMS systems, including those from vendors other than the award recipient (Siemens). It also allows CSM to "scale down" for possible use with a broader range of SCADA systems. This opens the possibility of use with Industrial Control Systems used for gas, oil, or water distribution – possibly even with systems used for "factory floor" automation.

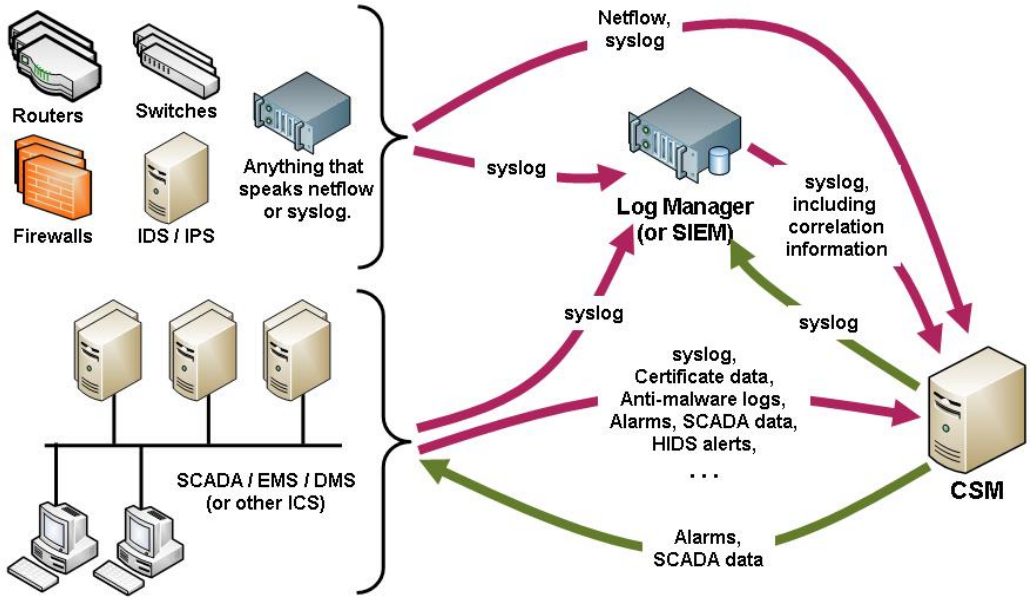


Figure 2: High Level (Current) Architectural View

### User Interface: comparison to original proposal

Although the CSM Project Team was originally somewhat concerned at DOE's suggestion that an Industry Advisory Group be formed and quarterly meetings held, this turned out to be very useful – especially early in the development phase. We now heartily endorse having an Advisor Team for projects where it is important to understand how a proposed product will "fit" into an existing operational environment.

The Advisor Team was made up of experienced utility personnel. Meetings were held quarterly; early development meetings were held either at Siemens' facility, one of the team member's home sites, or concurrently with a meeting of the Siemens Energy Automation Customer Association. Attendance was generally quite good; DOE representatives attended some meetings by
teleconference.

The Advisor Team provided invaluable advice about User Interface design, arguing convincingly for a simplified "at-a-glance" UI for operators. The result was a single display specifically designed for operators that presents:

- Alarms, classified into six (configurable) categories.
- Operator instructions, accessible by clicking on one of the alarm categories.
- Who to call for assistance.
- A window for operators to make notes about actions that have been initiated.
- A mechanism to change CSM's "sensitivity." (This concept was not present in the project's original proposal. It allows CSM's sensitivity to events to be changed if, for example, an attack is known to be in progress at a neighbor or partner utility. For example, if it is known that a partner utility is experiencing a cyber security incident, CSM can be "tuned" to issue an alarm about failed connection attempts after fewer such attempts than under normal conditions).
- "At-a-glance" security posture (situational awareness) indicator.
- The ability to "drill down" to see more details about elements on the display through a simple mouse click (for example, while talking to support staff on the telephone).

The Advisor Team also understood the potential use of CSM as an analytic tool, both in real-time and post-event. This resulted in creation of a large number of displays designed specifically for analysts/engineers.

The Advisor Team also played a prominent role in CSM's capability to make entries into a SCADA/EMS system's "alarm lists." This is the mechanism by which many utility operators receive the majority of information about malfunctions or other problems in their systems; the Advisor Team wanted to ensure that CSM could fit into this mode of operation.

### Operator Training Simulator: comparison to original proposal

An Operator Training Simulator (OTS) capability was a prominent feature of the originally proposed CSM, and the project's end product included the feature set described in that proposal.

During development and with the help of the Advisor Team, those concepts evolved to include additional capabilities. To summarize the OTS capability at a high level:

- CSM's ability to simulate security events not only creates the visual displays that would be seen in a real-world version of an event, but also create (for example) the *syslog* messages that would be seen during that event. For example, CSM simulates a "connection denied" *syslog* message from a firewall by actually creating the same message that would be issued by the firewall and inserting it into the *syslog* data stream.
- CSM has a "stand-alone" OTS capability. Using this capability, a trainer (instructor) can create simulations of security events, combine them into a script, and play that script as part of a training scenario.
- CSM can work in conjunction with the award recipient's existing Operator Training Simulator used for training grid operators. Specifically, the OTS interfaces with CSM in such a way that a grid operator training "program" can cause scripts to be executed on CSM to simulate security-related events.
- The manner in which CSM's simulation capability has been implemented facilitates its use by persons who are responsible for configuring CSM. The ability to use the OTS/simulation capability in this way was not envisioned in the original proposal.

  This is easily understood through an example. Assume that an engineer wants to configure CSM to issue an alarm based upon issuance of 100 "connection denied" syslog messages from a firewall in one minute.

  - In an off-line CSM scenario, the engineer creates the CSM "rule" (actually by defining structures CSM calls a "Security Info Type" and "Security Event Criteria"). These recognize and parse the firewall's syslog messages and tabulate their occurrences.
  - The engineer then creates an "OTS script" to issue those same firewall syslog messages.
  - The engineer activates his "rule," then runs the script.

# Funding period project activities

This project was comprised of two phases: Development and Demonstration. As expected, the Development phase of the project consumed the majority of costs and schedule. For the Development phase, Siemens drew upon electric utility experts to serve as industry advisors and also consulted with technical experts from The Pacific Northwest National Laboratory (PNNL). For the Demonstration phase we worked with the EMS team from the Sacramento Municipal Utility District (SMUD).

The project kicked off on October 1, 2010, following the plans laid out in the award proposal documents. The first order of business was to organize and familiarize the team within Siemens and document the functionality of the Cyber Security Manager (CSM). The functional description document was shared with the project advisors in advance of the first quarterly advisor meeting, which was held in January 2011. At that meeting the functional definition of CSM was approved by the advisor team. Following that, the project team met with the DOE in February 2011 to review status and solidify the technical plans for the project. Siemens also met with PNNL that February to gather technical recommendations and discuss design plans. Upon the completion of the aforementioned meetings, Siemens embarked on the task of defining CSM's detailed design. As elements of that design were completed, the project development team began their software development.

The April 2011, advisor meeting included the first of many discussions of one dominant topic for the project, which was how to most effectively provide the control room operator with cyber security situational awareness of the system. The insight of the advisor experts was instrumental in creating a very simple yet concise user interface for conveying that awareness.

During the first half of 2011, the CSM core software development environment was established and the work of coding and building the CSM was very active. The first notable milestones included CSM being able to collect *syslogs along with* the CSM User Interface up and running with the first draft of the operator workflow implemented. Enough progress was made so that demonstration to the advisors of the Netflow collector and the initial CSM User Interface was possible in July 2011.

The second half of 2011 continued the heavy emphasis on development, incorporating the input from the advisors. Notable additions were the introduction of persistent aggregation of *syslogs*, creating events and alarms within CSM, completion of the Netflow collection engine, and inclusion of a Common Vulnerability Scoring System (CVSS).

Also during this period, Siemens and PNNL met to review PNNL designs for a Security Inference Detection Engine (SIDE). The SIDE component is an extension to the base CSM application that can analyze multiple CSM-generated security events. The SIDE uses logical combinations of CSM-generated events occurring within a timeframe of each other. The existence of logical combinations of CSM events within a configured time frame of each other would generate a SIDE event which would be forwarded to CSM. CSM in turn could be configured to generate further CSM events, alarms and operator notification based on the SIDE event. Additionally, PNNL provided Siemens with their recommendations for implementing cyber security protections within CSM.

In November of 2011, the team conducted Netflow tests at SMUD. The outcome of that activity was that a valuable sample collection of electric utility control room Netflow data became available to the development team for use in the development and testing of CSM's Netflow processing code. In addition, the testing allowed us to conclude that Netflow was supported for bridged traffic, a common network configuration used in control systems.

CSM development progress in the first quarter of 2012 included creation of an API for sending CSM alarms to SMUD's EMS and incorporation of advisor-recommended user roles. During this quarter, PNNL completed their work on the SIDE design and documented the results in a functional description, detailed design specification, and GUI description. The SIDE design and User Interface description were presented to and discussed with the Advisor group. Advisor feedback was then incorporated back into the design and User Interface description. Lastly for this quarter, in anticipation of the project's Demonstration phase, a CSM server was installed at SMUD with an early version of the software. The installed system was used to collect more production EMS Netflow data and provided data to help the team develop CSM event processing rules.

Integration of CSM with SMUD's support EMS in Siemens' facility was completed in the second quarter of 2012. This resulted in CSM events and alarms being displayed in the EMS UI, a significant technical milestone. Also added to CSM during this quarter was the collection of virus and certificate data. During this time, the new Netflow data collected by the CSM on-site at SMUD was proving useful as it revealed some deficiencies in the initial Netflow data processing implementation. Those deficiencies were successfully remedied.

By mid-2012, the advisor UI recommendations had solidified and were incorporated into the CSM. This allowed the second half of 2012 to be devoted mainly to completing the remaining core CSM software development and unit testing.

The last of the quarterly advisor meetings was held in January of 2013. At this point, the core CSM development was sufficiently complete such that the system was ready to be demonstrated to the public. The first such demonstration was made at the DistribuTech Conference and Exhibition in January 2013. The demonstrations were successful and the feedback from attendees positive. From this point, significant ramp-up of Demonstration phase activities was made possible.

Siemens conducted the Factory Acceptance Test in January 2013. A number of defects were found and corrected. In preparation for SMUD's execution of Site Acceptance Test (SAT), Siemens visited SMUD in April 2013 and provided informal training on CSM usage and configuration of servers and services. SMUD then conducted their SAT in June. Tests related to integrated OTS and EMS were deferred until later integrations of CSM with those systems would be performed.

In February 2013, Siemens and PNNL met to review CSM design in light of the Inference Engine design that PNNL was developing. It was observed that SIDE functionality to correlate multiple events is included in many Security Information and Event Management (SIEM) systems. It was therefore concluded that the SIDE component would only be needed on CSM installations where no SIEM is present. Considering this, plus the fact that inclusion of a LogRhythm SIEM in the SMUD Demonstration configuration was planned, Siemens determined that implementation of the SIDE component would not be pursued further under this project.

By early 2013 development of the core CSM was essentially complete but a number of important additional development items remained to be done. The CSM UI Framework software (developed outside of this project) had a newer release available and it was decided that it would be best for the CSM that it be delivered with that newer and improved version. Integration of CSM with SMUD's EMS OTS also needed to be done. That integration allowed for an EMS OTS training session to incorporate CSM alarms into operator training scenarios. Integration of the LogRhythm SIEM was also performed. The AI component of the LogRhythm system provided the important ability to have security event correlation detection and alarming. The integration resulted in the capability of having multi-event correlation alarms generated in LogRhythm to be sent to and displayed in CSM. Example multi-event correlation alarm configurations were included in the final CSM. The final major remaining item to be developed was the creation of an installation package comprised of a DVD and an installation guide which, together, assure a reliable and trusted installation of the CSM system on an AIX server. During the work on these remaining Development items we ran into some technical complications that resulted in a combined five-month delay in the project schedule. While the delays were disappointing, the good news was that no cost increases were incurred on the project.

In the final collaboration between Siemens and PNNL on this project, PNNL visited Siemens in September 2013 and performed a cyber security evaluation of CSM.

As completions of the final Development items occurred, the team completed the remaining Demonstration tasks with SMUD. In this realm, SMUD's LogRhythm SIEM, along with the code for facilitating event correlation, was configured and shipped in August. That was followed in the fourth quarter by completing the Integration of CSM with SMUD's EMS and OTS, SMUD completing the remaining SAT steps involving the EMS and OTS, providing formal CSM user and analyst training classes to SMUD, and commencement of the deployment of CSM into SMUD's production environment.

Finally, in January and February of 2014, we worked closely with SMUD to complete the installation and commissioning of CSM into the production environment per SMUD policies. The final SAT defects were satisfactorily resolved and closed by the end of February, bringing a successful end to the project.

### CSM Design Requirements

The following design concepts were defined for the project in order to achieve acceptance, integration with other systems and with existing customer systems.

- Minimization of false positive alarms.
- CSM will maintain a light integration footprint with a SCADA/EMS system. The core CSM server is vendor system neutral. No proprietary or vendor specific interfaces are required on the CSM server. Exchange of data will be through industry standard communication interfaces.
- SCADA/EMS interfaces to CSM:
    - Alarm messages
    - SCADA/EMS database values
- CSM interfaces to SCADA/EMS:

  - CSM will generate and send operator alarms to the SCADA/EMS.
  - CSM will send data item values to the SCADA/EMS.
- All security inputs are logged to syslog. The syslog repository is the primary source of security inputs to the CSM security event detection engine. The syslog repository is the input to a SIEM system or syslog archive product such as LogRythm.
- The OTS PSM interface to CSM is through syslog entries.
- The CSM GUI can be integrated with a SCADA/EMS system's Single Sign On capabilities. The SCADA/EMS GUI will initiate a connection with the CSM GUI.
- CSM User Interface will be implemented with the Siemens WebUI SDK.
- The CSM server will initially be AIX based. However, the use of AIX or Unix specific features will be minimized so that the CSM server could be deployed on a Linux or Windows platform.
- An Engineering System can be used to populate the CSM operational database. The specific Engineering System implementation will be project dependent. Siemens Spectrum Power provides PDM and IMM Engineering Systems.
- The Netflow collector process requires that all Netflow exports be sent to a single UDP port on the CSM server for aggregation of netflows.
- Users, passwords and database connect strings will be stored and accessed using the AIX version of Get Connect String. API's are available for access from Java, C++ and Perl.

### Results of the Project

The final tangible outputs from the project were:

- CSM Core Software
- CSM API for EMS and OTS
- CSM Factory Acceptance Test Book
- CSM Installation Guide
- CSM User Guide
- CSM Design Document
- CSM User and Analyst Training Documents

# Products developed and technology transfer

### Cyber Security Manager (CSM) product

Spectrum Power™ Cyber Security Manager is now a product offered by Siemens Industry Inc. for use with the Siemens Spectrum Power Energy Management System. A pricing and support model has been developed. CSM is being offered as an option/upgrade to Spectrum Power 3 customers (and prospective customers).

### Sales and marketing activities

CSM is routinely offered as an option to those who are contemplating purchase of a Spectrum Power Energy Management System (or upgrading an existing system).

- CSM has been installed at Sacramento Municipal Utility District as part of the DOE-funded Demonstration Project.
- CSM has been sold to a US EMS customer.
- Siemens is in negotiations with other customers regarding addition of CSM to their existing Spectrum Power systems.
- CSM is now offered as an option on proposals for Spectrum Power EMSs (including upgrades of existing systems).
- Although CSM has not been tested with other Siemens SCADA/EMS systems, the effort to port to another system will be small; CSM is therefore being offered as an option to selected Spectrum Power TG customers as well.
- Presentations have been made to additional utilities that are Siemens customers, but use another vendor's SCADA/EMS.
- Siemens is in discussion with at least one university which is contemplating enhancement of its computer science offerings with a cyber security program.
- Marketing materials (brochure) have been developed; others are in progress.
- Sales staff are aware of CSM.
- Sales support staff have been trained in the use of CSM and have taken over (from the CSM Development Team) the work of regularly providing presentations and demonstrations at pre-sales meetings with prospects. Future presentations and
  demonstrations at industry conferences will be performed by sales support representatives.

### Trade journals

- T&D World, July 2012: When Security Matters (http://tdworld.com/asset-management-service/when-security-matters) by Valentine Emesih of CenterPoint Energy and Bruce Oliver of Sacramento Municipal Utility District.
- T&D World has a policy against accepting articles from vendors; this article was written with collaboration of Dave Taylor, CSM's Principal Investigator.

### Industry conventions and trade shows

- DistribuTECH, February 2013

o CSM was demonstrated in the Siemens booth at DistribuTECH. Response was quite good; we conducted demos for a number of Siemens customers, for partners (and a few competitors), and others (including representatives from DOE). The product was well received.

o A presentation on the product was given by Valentine Emesih (CenterPoint Energy), assisted by Dave Taylor of Siemens. The presentation was well attended. A number of good questions were fielded, and a number of attendees stayed after the presentation for additional discussion. The T&D World article (above) was written as a result of a discussion with a representative of T&D World which took place after this presentation.

- The Siemens Energy Automation Customer Association (SECA) is an organization of (primarily) Siemens SCADA/EMS customers which meets twice annually. Siemens representatives attend these meetings by invitation. CSM has been presented at SECA's Cyber Security Working Group for the past several meetings. CSM has been demonstrated at the SECA "Product Fair" twice.

- Siemens currently consists of four sectors: Energy, Industry, Infrastructure & Cities, and Healthcare. Approximately four years ago, the topic of Cyber Security began to increase in importance for the Energy and Industry divisions. In response, a small group of Siemens Industry and Energy employees who had an interest in Cyber Security began to hold annual "Security Hub" meetings to share experiences. Over the years, these meetings have become much more widely attended.

  Presentations and demonstrations of CSM have been made at two Security Hub meetings. These meetings are dominated by persons who work with industrial (i.e., "factory floor") automation systems. There has been considerable interest in CSM; it is hoped that the product can be tailored for this type of application.

### Other Demonstrations

- CSM has been presented and demonstrated to a number of Siemens' SCADA/EMS customers and prospective customers as an add-on to existing Siemens SCADA/EMS/DMS systems as well as to competitor systems. It is a regular part of Siemens EMS proposals.
- CSM has been demonstrated to and discussed (at industry trade shows) with some competitors in the industrial automation field.

### Patent

Prior to applying for DE-FOA-0000359, Siemens filed a Patent Application (WO 2009/128905A1) in April 2009, entitled "Method and System for Cyber Security Management of Industrial Control Systems." The Operator Training Simulator capability is included in the patent. The application was approved and Patent Number US 8,595,831 B2 was awarded on Nov 26, 2013.