

Hallmark Project Final Technical Report

June 29, 2012

Secure Control Systems for the Energy Sector
Funding Number: DE-FC26-07NT43311
Project Director: Rhett Smith, SEL
Principal Investigator: Jack Campbell, CenterPoint
Principal Investigator: Mark Hadley, PNNL
Schedule Status: Completed
Project Period: Oct 2007 March 2012

Project Team:

Schweitzer Engineering Laboratories, Inc.
Pacific Northwest National Laboratory
CenterPoint Energy Houston Electric

Project Summary

Schweitzer Engineering Laboratories (SEL) will conduct the Hallmark Project to address the need to reduce the risk of energy disruptions because of cyber incidents on control systems. The goal is to develop solutions that can be both applied to existing control systems and designed into new control systems to add the security measures needed to mitigate energy network vulnerabilities. The scope of the Hallmark Project contains four primary elements:

1. Technology transfer of the Secure Supervisory Control and Data Acquisition (SCADA) Communications Protocol (SSCP) from Pacific Northwest National Laboratories (PNNL) to Schweitzer Engineering Laboratories (SEL). The project shall use this technology to develop a Federal Information Processing Standard (FIPS) 140-2 compliant original equipment manufacturer (OEM) module to be called a Cryptographic Daughter Card (CDC) with the ability to directly connect to any PC enabling that computer to securely communicate across serial to field devices. Validate the OEM capabilities with another vendor.
2. Development of a Link Authenticator Module (LAM) using the FIPS 140-2 validated Secure SCADA Communications Protocol (SSCP) CDC module with a central management software kit.
3. Validation of the CDC and Link Authenticator modules via laboratory and field tests.
4. Creation of documents that record the impact of the Link Authenticator to the operators of control systems and on the control system itself. The information in the documents can assist others with technology deployment and maintenance.

Project Objectives

The Hallmark Project has four primary objectives:

1. Bring the Secure SCADA Communications Protocol (SSCP) technology into commercial form to support legacy, current, and future control system equipment.
2. Implement the SSCP in a manner that will not negatively impact reliable operations or personnel safety.
3. Provide for in-band and out-of-band maintenance and configuration activities.
4. Develop a FIPS 140-2 validated OEM solution that is commercially available to the market and OEM validation results.

Accomplishing these objectives brings forth cost-effective, low-maintenance solutions for strong authentication to the electronic perimeters designed for our nation's energy infrastructure. The Hallmark Project objectives provide the end-users with a possible method to comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements and improve the reliability, efficiency, and robustness of their control systems.

Results for Success Criteria

To be considered successful, the project had the following objectives and was successful on all goals:

- 1) Knowledge will be transferred from PNNL to SEL. PNNL and SEL worked very close for the 5 year duration of the Hallmark project refining the SSCP specification, design decisions, and testing.

- 2) The CDC will be designed and commercially released with FIPS 140-2 Level 2 validation. The Hallmark team successfully completed the commercial release of the FIPS validated cryptographic technology.
- 3) The interface to other products for interoperability will be identified. The Hallmark team has the SSCP specification effort to integrate with IEEE underway and Siemens had proof of concept where their products were talking to SEL products proving interoperability.
- 4) The CDC will be integrated into a stand-alone product built for bump in the wire application to secure existing serial links and offer operational tools like a PC driver and central management software commercially available. The Hallmark team successfully released all products and software solutions making serial cryptographic solution complete
- 5) The product will be OEM, laboratory, and field tested with successful results. The Hallmark team had the pleasure of completing all tasks and deliverables which resulted in commercial release of the technology and most importantly commercial deployment of the technology on our nation's power systems.

In the first phase the Hallmark team developed the OEM Cryptographic Daughter Card (CDC) Solution and the Integration of the CDC into a Link Module.

Transfer of Knowledge Between PNNL and SEL was overwhelming successful. The geographically closeness offered the team many face to face meetings. This resulted in the SSCP specification being refined and optimized for an economical commercial solution. The team kept this close working relationship through the entire project with test development and execution as well as onsite lab testing and results review.

FIPS Validation was achieved shortly after release.

SEL and PNNL staff worked to identify, design and test to level 2. The various functions required for the FIPS validation include:

FIPS Security Requirements Section	FIPS Security Level
Cryptographic Specification	2
Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2

The Hallmark team performed the documentation and testing requirements to submit and achieve FIPS 140-2 level 2 validation on the CDC running the SSCP serial crypto protocol. This provides the industry security assurance and confidence to use this technology.

Identify Additional Components Still to be Developed

The Hallmark team successfully developed the CDC and now CenterPoint lead the design of what needed to be done to provide the means to deploy this technology on the existing serial

infrastructure. Four products needed to be developed and released to make this happen. The Hallmark project was successful in the development and release of all these products which include:

SEL-3045 cryptographic daughter card running SSCP



SEL-3025 serial shield bump in the wire module



PC Serial Security Kit allowing any PC to use the CDC



Central Management software to manage the SSCP keys



The Hallmark team captured all the lessons learned and recommended use cases for this technology in 8 reports detailed below:

1. Topical Report - System Specification – describes what the product does and how the product is envisioned for use on the system level.
2. Topical Report - Software and Hardware Requirements Specifications– details the exact needs, technical requirements, and methods used to achieve the system specification requirements.
3. Topical Report – Functional and Type Test Plans – details the tests ran on the product to check the correctness of technical functions.
4. Topical Report – Functional and Type Test Results – details the successful test results of functional and type test runs on the product ensuring proper and robust design for the electric sector.
5. Topical Report – Control System and Personnel Impact Report – describes the impacts on control system operations and the people that use the product.

6. Topical report on the evaluation Siemens provided for the technology
7. Topical report on lab and field testing results
8. Topical report on control system and personnel impact report after all technical development was complete and spotlights how it reduced operational and technical expenses and burden. This report included how the PC interface to the cryptographic card and the central management software reduced the impact and improved the maintainability and scalability of the SSCP technology.

SEL went to production with the Hallmark technology

The Hallmark team knows this project was successful with the metric that many end users are now testing and deploying this technology on their existing infrastructure and new designs are working to integrate it for systems of tomorrow. The Hallmark project resulted in improvements to the electric sector cybersecurity and our systems are more secure today than before this project.

CenterPoint Energy Houston Electric

CenterPoint Energy (CNP) is very proud to be a member of the Hallmark project team. Our involvement in this project has been a rewarding experience. The project team included members with a combination of skill sets that complimented each other very well. This project was a unique experience for CNP to work with PNNL and SEL to define requirements for a product, test prototypes and see the final results of a commercialized product release. Through our work on the project, CNP gained a lot of insight and appreciation for the amount of work it takes to develop a product and then release a commercial product to the market.

SEL worked closely with CNP to gather our ideas and find out what was important to us, how we planned to use the product and what the impact would be on daily operations. Bit protocols are very difficult to deal with and implementing a security solution for a bit protocol proved to be extremely challenging due to the critical bit timing and message structure of the protocol. The CNP team working on the project has many years of Energy Management System (EMS) experience, including extensive knowledge of SCADA bit and byte oriented protocols. The CNP team members were able to validate the work on the product at different intervals in the development. We provided feedback to SEL on changes or new features that we thought would enhance the usability for daily operations and maintenance. SEL was able to implement the majority the ideas that we had provided feedback on.

The security and reliability of the SCADA infrastructure is very important to CNP. SCADA data and RTU communications are an essential part of our EMS used to monitor and control the bulk electric grid. It was extremely important that any device that would become part of the SCADA infrastructure be rigorously tested, easy to manage and work with different types of communications media (i.e. analog and digital). The expertise joined together by the Hallmark project was able to accomplish all of these goals. We are confident the products produced as a result of the work performed by SEL, PNNL and CNP will improve the security and reliability of the SCADA infrastructure.

The project team worked very well together. This was a very exciting project to be a part of and the contributions and cooperative nature of this team is what help make the Hallmark project such a successful project.

Pacific Northwest National Laboratories

The involvement of the Pacific Northwest National Laboratories (PNNL) in the Hallmark project has been a very enriching and beneficial experience. Throughout the project our involvement helped us learn industry issues, vendor constraints, and how to improve technology transfers.

When the SSCP effort began, we were fortunate to have the support of many great partners on an advisory committee. From those discussions we learned about the needs and problems of industry players. Witnessing the integration of a new security tool at a utility opened our eyes to the many ancillary challenges security technologies present to a utility. The operational burden of managing and maintaining security solutions can be much more of a challenge than the integration of the new technology. The knowledge gained about the industry by participating in the Hallmark project has, and will hopefully continue to, impact our perspective, approach and projects.

The Hallmark project has also provided a great view into the operations and processes utilized by vendors. Learning the manufacturing and development constraints SEL has when producing a commercial product offering was eye opening and profound. As scientists we can sometimes have incorrect perceptions by working within a laboratory space. Gaining insight into the hardware constraints (cost, physical limitations, hardware lifetime, etc.) led to improvements to the SSCP to accommodate a market ready product.

Working so closely with SEL has provided numerous benefits that ultimately led to a successful transfer of laboratory developed technology to a commercial entity. We learned that there is a large gap between the output of a successful research project and the readiness level necessary to begin the technology transfer process. From our involvement of the full TRL life cycle for the SSCP technology, we have gained invaluable experience regarding the requirements to move research technology to the market where it can provide benefit to real world environments.

In closing, being part of the Hallmark project has been an enriching experience, and it was a privilege to be part of this DOE sponsored project. Our hope is that we have made DOE proud of our success, and that the Hallmark project can be used as the example for laboratory / vendor / utility collaboration and technology transfer. The SSCP is commercially available and protecting our nation's infrastructure. Making this type of impact is the driving force for those of us performing research at national laboratories. The Hallmark project validates our desires and demonstrates the positive effect of our work.

Schweitzer Engineering Laboratories Inc.

SEL is proud to have been involved with the Hallmark project. The team that came together in 2007 had a vision to tackle the tough challenge to secure serial communications in the energy sector. SEL worked a total of almost 47,000 hours on the Hallmark Project. SEL had experience in serial security with the SEL-3021 commercially

available for many years but knew that more work needed to be done to secure the remaining use cases and do it in a manner that allowed for easy compliance to then new NERC CIP standards. PNNL had been working on the SSCP specifications and had a proof of concept code working which provided an immediate work platform the team could use. CenterPoint had the system and know how to evaluate the technology to make sure it not only secured the data but it fit within the operational requirements of their power system. Combining these three entities to work together has been the most successful approach to industry collaborative research SEL has seen. This resulted in five new commercial products, beginning work to integrate the SSCP into an IEEE standard, and most importantly technology deployed and protecting many serial communications channels across power systems today. The main methods the Hallmark team used to be successful was asking lots of questions to find out how the system operates today and how the end users wanted the system to operate in the future, research all the existing standards and regulations that must be met (FIPS and NERC CIP), and finally testing the technology to the highest level possible to ensure reliability is first. SEL was the project lead on the Hallmark project and was supported by two very professional organizations resulting in a team environment. All tasks were accomplished and a few had surprising results. The major shift in the project came when the latency evaluations were complete and the team identified the SSCP technology to be best for engineering access and in some cases a lower latency solution was required for SCADA. The team also engaged with another vendor with Siemens and they were happy with the Hallmark tools and felt the technology could easily be integrated into products. The project has built a solid professional relationship between SEL and PNNL that I'm sure will continue on many more projects in the future. It has also improved a working development partnership between CenterPoint and SEL. Our two companies were already working together but more of a vendor end user role, it is now a much more open and has developed past the Hallmark project to many other large projects CenterPoint is working on. The same recipe exists to gather requirements and specifications, communicate through the engineering trade-offs, research and develop technology and then validate objectives are met to commercialize. DOE has structured and funded a project in such a way that enabled the industry partners to succeed in identifying how to accomplish a milestone on the DOE Roadmap that resulted in power system security improvements today. The results of the Hallmark project are deployed and protecting power systems today. Thank you to everyone.

Estimated vs. Actual Accomplishments

Milestone Description	Estimated Completion	Actual Completion
Project Start Date	October 2007	October 2007
Product Concept Complete	December 2007	December 2007
PNNL to SEL Technology Transfer Complete	February 2008	February 2008
Topical Report: System Specification	February 2008	February 2008

Milestone Description	Estimated Completion	Actual Completion
Biannual Review #1	April 2008	April 2008
CDC Specification Complete	April 2008	April 2008
LM Specification Complete	Nov 2008	Nov 2008
Identify FIPS Validated Components	June 2008	June 2008
Topical Report: Software and Hardware Requirements Specifications	July 2008	July 2008
Biannual Review # 2 and Program Peer Review #1	October 2008	May 2008
CDC Prototype Complete	January 2009	January 2009
Topical Report: Functional and Type Test Plans	February 2009	February 2009
Biannual Review #3	April 2009	April 2009
Biannual Review #4	October 2009	September 2009
Prototypes delivered to PNNL and CenterPoint Energy	October 2009	November 2009
Prototype Tests Complete	November 2009	November 2009
Topical Report: Test Results	January 2010	January 2010
Topical Report: Control System and Personnel Impact Report	February 2010	March 2010
CDC FIPS Validation Complete	May 2010	June 2010
Manufacture Product – CDC and Link Module Pilot Build Complete	October 2010	July 2010
Revise project management plan	Oct 2010	Oct 2010
Identify another asset owner for lab testing	Oct 2010	Oct 2010
Identify another manufacturer to OEM the CDC	Oct 2010	Oct 2010
Identify business requirements and write specifications for the driver for direct interface between the card and any PC	Dec 2010	Dec 2010
Identify business requirements and write specifications for the central management software	Dec 2010	Dec 2010
Create lab and field test plan	Feb 2011	Feb 2011

Milestone Description	Estimated Completion	Actual Completion
OEM update report completed	March 2011	March 2011
Perform interoperability tests between PNNL, SEL, and additional vendor	April 2011	April 2011
Topical Report: OEM vendor integration	June 2011	June 2011
Complete develop the central management software	Aug 2011	Sept 2011
Complete develop the driver for direct interface between the card and any PC	Aug 2011	Sept 2011
Topical report: Lab and Field Testing Results	March 2012	March 2012
Topical report: Impact Report update with the PC interface and central management software results	March 2012	March 2012
Project Closeout Review	March 2012	March 2012

Conclusions

The Hallmark Project completed all project tasks on schedule and within the budget. SEL exceeded the cost share requirements.

The Hallmark Project provided a large solution to one of goals in the DOE Roadmap to Achieve Energy Delivery Systems Cybersecurity; "Develop and Implement New Protective Measures to Reduce Risk". The Hallmark project commercialized technology for the laboratory at PNNL which has resulted in the security technology successfully being applied to existing power systems.

Not all tasks were accomplished as expected and it is important to highlight these findings.

- 1) Time is a difficult source to use in a cryptographic system. The Hallmark team worked hard to adjust the SSCP specification to eliminate the potential weakness in using time as an input and instead used a simple counter.
- 2) The manufacturing process for small form factor PCMCIA cards that achieve FIPS validation with tamper evidence is very difficult and SEL had to design a customer potting process to achieve it.

- 3) CenterPoint realized the communication channel diagnostics must be enhanced in the communication front ends because the inline sniffing of the SCADA messages is no longer possible. This has driven some of the SCADA master improvements.
- 4) Cryptographic latency and overhead calculations must be addressed before any wide scale system can work reliably. This becomes clear when scaling the testing up from one point to point communications to a large multidrop system with tight poll windows. The Hallmark team worked to streamline the overhead and balance system configurations.
- 5) The Hallmark team realizes that there is a tremendous amount of education that needs to be shared with respect to applying cryptographic solutions to serial communications and how that impacts the SCADA system and the people who work these systems.
- 6) The Hallmark team is seeing continuation efforts from the “teaming” efforts that were started under the DOE project that most likely would not have occurred if these contacts and shared work environments were not set up. An example of this is a new project that SEL and Siemens is working jointly on to integrate more cryptographic technology into our respective products that will be tested for interoperability. Another is the adoption of the serial cryptography in applications outside the electric sector in oil & gas, and transportation to name a few.
- 7) Lastly the Hallmark team has watched as NERC CIP moves to mandate “encryption” of all communications leaving or entering the security perimeter including serial. The commercialized technology resulting from Hallmark provides this solution and the ability to use it in large systems with centralized control.

This project shows the power of pulling industry subject matter experts together to tackle a tough problem. The different viewpoints when combined painted a clear picture of the issues and requirements to be solved. After that the engineers could design and develop solutions and bring them back for testing and validation. A complete technology development life cycle has been completed in Hallmark where the team started with an idea and vetted that idea against the real world problems in advancing serial cybersecurity. The team stayed close working for four and a half years to complete a turnkey example on how to solve the issues of securing serial communications. The industry has commercialized products they can purchase, reference designs to follow, and lessons learned documentation they can leverage as a result of this DOE sponsored project. All of this provides a roadmap that any industry participant can follow whether you're an end user and want to purchase the technology or a vendor who wants to integrate the technology into their product line. In short our Nation's power systems are more secure because the deliverables of the Hallmark project are applied and protecting serial communications that run power systems today.