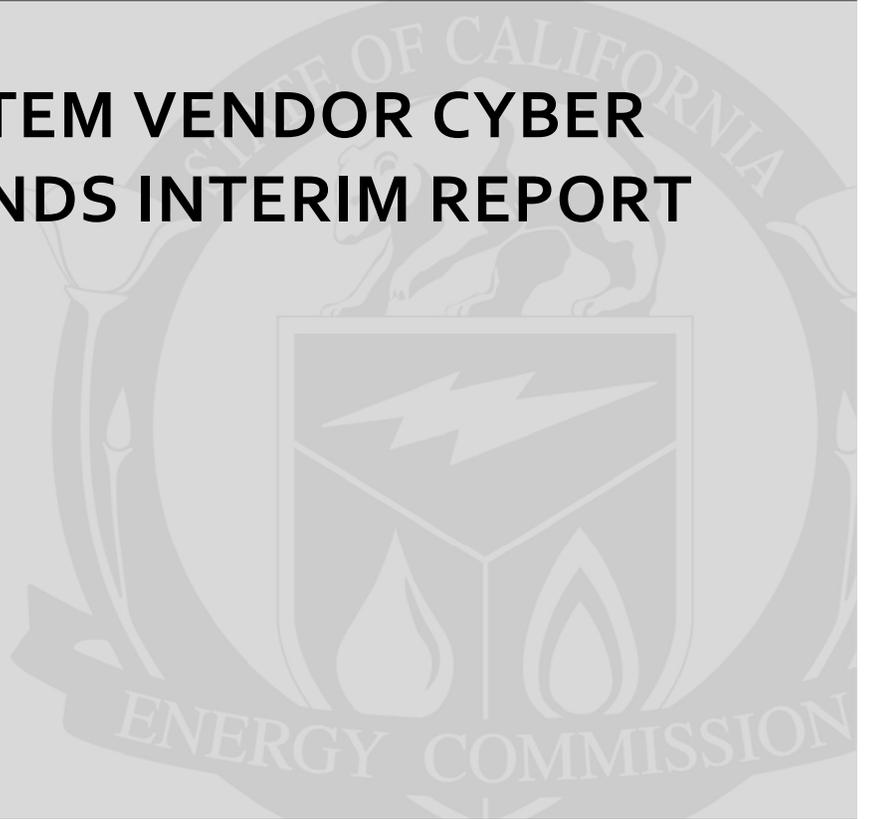


Energy Research and Development Division
FINAL PROJECT REPORT

**CONTROL SYSTEM VENDOR CYBER
SECURITY TRENDS INTERIM REPORT**



Prepared for: California Energy Commission
Prepared by: KEMA, Inc.



MAY 2014
CEC-500-2012-078

PREPARED BY:

Primary Author(s):

Karin Corfee
Chris J. Decker

KEMA, Inc.
Oakland, CA 94612

Contract Number: KEMA-06-007-P-S

Prepared for:

California Energy Commission

David Chambers
Contract Manager

Fernando Pina
Office Manager
Energy Systems Research Office

Laurie ten Hope
Deputy Director
ENERGY RESEARCH AND DEVELOPMENT DIVISION

Robert P. Oglesby
Executive Director

DISCLAIMER

This report was prepared as the result of work sponsored by the California Energy Commission. It does not necessarily represent the views of the Energy Commission, its employees or the State of California. The Energy Commission, the State of California, its employees, contractors and subcontractors make no warranty, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Energy Commission nor has the California Energy Commission passed upon the accuracy or adequacy of the information in this report.

ACKNOWLEDGEMENTS

Thanks to Karin Corfee, John Holt, and Paul Schuler of KEMA, Inc. for their support in preparing this report.

PREFACE

The California Energy Commission Energy Research and Development Division supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The Energy Research and Development Division conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The Energy Research and Development Division strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

Energy Research and Development Division funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

Control System Vendor Cyber Security Trends Interim Report is the final report for the Cyber Security Technical Assistance - Phase 2 project (contract number KEMA-06-007-P-S) conducted by KEMA, Inc.. The information from this project contributes to Energy Research and Development Division's Energy Systems Integration Program.

For more information about the Energy Research and Development Division, please visit the Energy Commission's website at www.energy.ca.gov/research/ or contact the Energy Commission at 916-327-1551.

ABSTRACT

This report identified control system vendor trends and issues regarding implementation of cyber security for control systems applicable to the California electrical system from generation to end-use needs. A questionnaire was submitted to three commonly known control system vendors who develop and market energy management systems, supervisory control and data acquisition systems and general security assurance systems. Control system vendors were aware of the urgent need to secure their systems. They have made strides in system design and implementing cyber security for control systems in response to requests from electric utility customers, government regulators and technical working groups and were using industry's cyber security best practices. Researchers concluded that although vendors were more proactive than before there was much room for improvement. Vendors understood that they needed to increase their efforts or potentially face a decline in sales of new systems. The legacy systems that were purchased by utility customers will also have to be considered as part of these efforts. Researchers also concluded that continued participation in vulnerability testing at the national laboratories was essential. This testing provides an excellent way for vendors to benchmark their individual systems against their competition and to mitigate vulnerabilities that need to be addressed before deploying their systems to customers. Researchers also recommended that an annual evaluation of cyber security measures by control system vendors should be conducted and that the results of this research should be shared and presented to California's utilities so that they could be prepared to make cyber security-based decisions in their operating environment.

Keywords: Cyber Security, Supervisory Control and Data Acquisition Systems (SCADA), Energy Management System (EMS), Quality Assurance Systems (QAS), Control System

Please use the following citation for this report:

Corfee, Karin; Chris J. Decker. (KEMA, Inc.). 2009. *Control System Vendor Cyber Security Trends Interim Report*. California Energy Commission. Publication number: CEC-500-2012-078.

TABLE OF CONTENTS

Acknowledgements	i
PREFACE	ii
ABSTRACT	iii
TABLE OF CONTENTS	iv
EXECUTIVE SUMMARY	1
Introduction	1
Project Purpose.....	1
Project Results.....	1
Project Benefits	1
CHAPTER 1: Introduction	2
CHAPTER 2: Project Approach	3
CHAPTER 3: Project Outcomes	4
3.1 Trends from Vendors of Electric Energy Management Systems.....	4
3.1.1 Personnel and Training	4
3.1.2 Security as Fundamental Design	4
3.1.3 Patching Trends.....	5
3.1.4 Research and Development.....	6
3.2 Control System Delivery and Deployment	6
3.2.1 System Hardening.....	6
3.2.2 Remote Connectivity	7
3.2.3 Other Forms of Securing Remote Connection Encryption.....	8
3.2.4 Secure Inter Control Center Protocol (ICCP)	8
3.2.5 Use of Routable Protocols (SCADA Over IP).....	8
3.3 Third-Party Vendors of SCADA Security Systems	8
3.4 Trends from Vendors of General Security Assurance Systems.....	8
CHAPTER 4: Conclusions and Recommendations	9
GLOSSARY	10

EXECUTIVE SUMMARY

Introduction

Paramount to the cyber security of control systems is the willingness of control system vendors to participate in initiatives to design, deploy and support cyber-secure systems. Control systems that control California's transmission and distribution system and the customers they serve are vulnerable to loss or degradation of safe and reliable electric power without the assistance of vendors.

Project Purpose

The purpose of this project was to identify vendor cyber security trends and issues regarding implementation of cyber security for control systems applicable to the California electrical system from generation to end-use needs. Researchers intended to gain an understanding of what progress has been made by vendors in the past five years, what they are doing now and how they intend on positioning themselves in years to come.

Project Results

A questionnaire was submitted to three commonly known control system vendors who develop and market energy management systems, supervisory control and data acquisition systems and general security assurance systems. Control system vendors were aware of the urgent need to secure their systems. They have made strides in system design and implementing cyber security for control systems in response to requests from electric utility customers, government regulators and technical working groups and were using industry's cyber security best practices.

Vendors were more proactive than before but there was much room for improvement. Vendors understood that they needed to increase their efforts or potentially face a decline in sales of new systems. The legacy systems that were purchased by utility customers will also have to be considered as part of these efforts.

Researchers concluded that continued participation in vulnerability testing at the national laboratories was essential. This testing provides an excellent way for vendors to benchmark their individual systems against their competition and to mitigate vulnerabilities that need to be addressed before deploying their systems to customers.

The primary conclusion of this report as it pertains to the end-user needs of California's transmission and distribution system is that this process should be repeated on an annual basis to determine what if any progress has been made by control system vendors over the prior year. The subsequent results of this research should be shared and presented to California's utilities so that they can be prepared to make cyber security-based decisions in their operating environment.

Project Benefits

This project demonstrated that control system vendors were paying attention to cyber security issues and investing in enhanced cyber security system design for control systems. Enhanced cyber security will help ensure a reliability electricity supply for California consumers.

CHAPTER 1:

Introduction

Control systems that monitor and control California's transmission and distribution systems lagged behind more conventional information technology systems (IT) specifically cyber security for many years. The above-mentioned legacy systems had cyber security controls that were essentially limited to physical access. This was acceptable given that these control systems were designed with proprietary hardware and software. In recent years a paradigm shift has occurred as control system vendors have experienced new expectations from utilities to create, enhance, and extend their product's security posture to include cyber access.

This increased need for interconnectivity of control systems and to provide information across the utility's service area is putting an ever increasing demand on California's utilities and control system vendors. Many of the interconnectivity requirements for control systems and IT systems have lead to the introduction of mainstream technologies such that vendors are no longer using proprietary hardware and software. This progression has left vendors and California's utilities with a unique challenge in protecting their "off the shelf" systems from targeted cyber attacks, as well as, much broader cyber security vulnerabilities.

The intent of this project was to assist the Energy Commission in recommending appropriate cyber security research and development priorities to identify, prevent, prepare for, mitigate and respond to cyber vulnerabilities in and around electric control centers and transmission and distribution operations systems. More specifically, the authors will describe some of the initiatives vendors have considered in recent years to meet these challenges.

CHAPTER 2: Project Approach

Three supervisory control and data acquisition system (SCADA)/energy management system's (EMS) vendors responded with commentary to a questionnaire submitted for their consideration. The answers to the questionnaire were analyzed, as a whole, and presented in the Project Outcomes section of this report.¹

Below are the questions that were submitted as part of this task:

1. How does [VENDOR NAME] view cyber security as a whole?
2. How does [VENDOR NAME] respond to Windows (or other) security updates?
3. How are patches and upgrades applied to the SCADA/EMS software throughout the product lifecycle? Is there any follow-up to make sure the software upgrade doesn't impact cyber security?
4. What measures are being taken to secure systems before leaving the facilities?
5. What measures are being taken to secure systems following deployment?
6. Is there a full-time security specialist on staff?
7. Are security patches applied to systems on a regular basis, if so; is this a fee-based service?
8. Are there any R&D funds appropriated to security now? If so, what percentage of the budget is put towards these efforts?
9. Is there a strategic plan to address cyber security?
10. What are the most vulnerable pieces of the system? How are these vulnerabilities being addressed? (optional)
11. Do you have any partnerships with IDS/IPS or other security companies to aid in protecting, and or architecting the system?
12. What are the challenges [VENDOR NAME] faces regarding cyber security?
13. What was [VENDOR NAME]'s cyber security effort like 5 or so years ago and where do you intend on taking your program in the future?
14. Are you an active participant with the national test beds (INL)? How often to you use their resources and expertise?

¹ Specific answers to the questionnaire have not been provided in this report at the request of the vendors

CHAPTER 3:

Project Outcomes

3.1 Trends from Vendors of Electric Energy Management Systems

This sections reviews and comments on security-related trends for vendors of EMS and SCADA systems.

Cyber security is becoming part of the vendors offering and an essential component of their system. In efforts to advance their product, but still address security concerns, vendors have included cyber security in their business model and have begun to set a strategy for cyber security in product development. KEMA surveyed a number of EMS vendors to gain an understanding of their cyber security efforts and discover trends in these initiatives. ²

Security has evolved into a strategic initiative for control system vendors. The survey identified that control system vendors have recognized the need for cyber-secure systems and have invested resources to meet this need. Most notably, one of the respondents to the survey said that, “[They have] made cyber security one of the 4 major strategic initiatives.” Another control system vendor committed to, “Providing integration services for deploying our systems in heterogeneous environments securely, and achieving compliance to industry regulations.”

3.1.1 Personnel and Training

Hiring security personnel has become a common trend among vendors. In the case of one vendor, a full time security architect, security patch tester, a security company owner who participates in security implementation, operations, network security and project deliveries are on staff. Other initiatives include training current technical staff and providing a security awareness focus for them and for customers.

3.1.2 Security as Fundamental Design

In the past five years, vendors have promoted cyber security as a fundamental component of their design. Pressure from regulators and customer’s expectations for cyber-secure systems has prompted control system security at all-phases of the system life cycle. One of the respondents of the survey indicated that, “process improvements (with a specific focus on security) have been added throughout all development phases.”

This focus is very encouraging since the majority of control system vendor’s core applications, used for processing real-time data, were developed using older programming languages and compilers. Although their systems are robust and available, consideration for the support and maintenance of these modules, by way of competent computer programmers and their associated skill-sets, may increase the trend to re-engineer these core modules for processing SCADA information.

² Vendor names and their products will not be disclosed in this report.

Conversely, supporting systems that comprise the greater EMS system, such as user interfaces, data historians, and Inter-control Center Communications Protocol (ICCP) servers, are being developed using object-orientated programming (OOP) languages such as JAVA™ and relational databases like Oracle™. These solutions support web-based interfaces for other stakeholders in the organization who have a need to view control system data, but are not responsible for system (grid) operations. Remote viewing of system operations in this capacity is commonly referred to as 'view-only' access to the control systems. Using web-based applications is also advantageous because it is largely platform independent and easy to deploy. However, in some cases, view-only users open up another access point to the control system and sensitive data.

This new support system software is also platform-independent. By developing platform-independent software, customers have the ability to leverage their business systems, internal technical support personnel, and economies of scale for purchasing enterprise-wide hardware used for both control systems and business systems. Utilities that standardize on one enterprise-wide hardware platform are able to leverage existing purchasing contracts, annual maintenance agreements, and technical support against the costs of purchasing and supporting multiple platforms.

Another advantage to object-oriented programming is the capability of the software to run effectively on multiple operating systems. As in the case of hardware, software vendors offer enterprise-wide site licenses, which are not only advantageous financially, but can also be aligned with their internal support staff's skill sets. For example, some utilities may favor Microsoft products and have hired, trained, and cultivated employees with advanced certifications to specifically support Microsoft products.

By allowing utilities to select their choice of hardware and operating system software, control system vendors are now faced with the prospect of supporting multiple operating systems running on multiple hardware platforms. For non-critical systems, this trend would not be as challenging, but for control systems, with their expectation to perform at an unprecedented level of availability, are difficult to support. This trend puts vendors in difficult situations, especially when it comes to basic change and configuration management for security patching.

3.1.3 Patching Trends

Automating the patching of control systems is widely-known in the industry to be a high risk and generally not a good practice. Therefore, it becomes a time-consuming, risky, and costly effort for utilities to apply patches. Some control system vendors, aware of this issue, have started to offer on-going system patching as a service through email notifications, factory testing, to installation on the customer's control system. However, the turn-around time for patch installation, once released from the original equipment manufacturer (OEM) can take days, if not weeks, to deploy. The latency between the time it takes to evaluate and certify a patch against the control system vendor's product is a major issue; especially, when considering the additional time it took the OEM to recognize the vulnerability, mitigate the risk, and distribute the patch to their end-user community. Furthermore, most control systems now reside on non-proprietary hardware and software increasing the threat.

3.1.4 Research and Development

The survey asked EMS vendors to provide an estimate of what percentage of their budgets fund cyber security research and development. Respondents provided answers ranging from: spreading their research and development dollars in overall security enhancements to their existing products; participation in consortiums; to activities such as system testing with Idaho National Laboratory (INL).³

3.2 Control System Delivery and Deployment

This section seeks to describe some challenges and commonly used solutions that control system vendors and California's utilities are considering when deploying control systems to meet the needs of California's transmission and distribution system's customers.

3.2.1 System Hardening

Vendors will deliver security 'hardened' systems or will harden them on site for site acceptance testing, but may not tightly control security when those systems are on the factory floor unless the customer purchase EMS support. In order to ensure control systems meet the minimum requirements of government regulators and cyber security best practices, KEMA has been intimately involved in assisting utility EMS customers procure and take acceptance of control systems according to these requirements. During the process, control system vendors are required to provide cyber security documentation of all network configurations, including network access control lists (ACLs) for firewalls used to secure the electronic perimeter(s) surrounding the component systems of the EMS. These documents are used to provide evidence that vendors are following through with contractual expectations and their design.

Also required in the documentation, are network configurations, including network access control rules (NACs) implemented in firewalls used to secure the electronic perimeter(s) surrounding the component systems of the EMS, as well as network addresses, protocol service, and direction of initiation for each documented access. Documentation plays an essential role in network analysis, both for customers and for vendors to verify that adequate controls are in place.

Some of the documentation should include detailed security configuration, information, instructions and parameters; the necessary minimum file and user accounts permissions, and privileges, for system administrators, maintenance, and normal users (including operators/dispatchers and external users). A list of required services and executables, with ports required; login and password requirements should be documented. In addition, all accounts required for all software and systems, with explanations for their purpose, and the impact if the

³ Based on a recent presentation at the SANS Security Conference in 2008, 13 on-site assessments were conducted which included a cross-section of critical infrastructure that included generation and distribution. Most of the major SCADA and/or DCS vendors were represented.

account is renamed, deleted or the password is changed; and security procedures to be followed should be documented.

This analysis of these documents is then used in EMS factory acceptance testing (FAT) and is a benchmark for the necessary verification needed to deploy cyber-secure field equipment. Basically, FAT is the final accountability for EMS vendors to provide evidence that customer's expectations for a secure system are tested and verified accordingly.

EMS vendors have extended system hardening services to integrity checking software; that is, when used appropriately it will alarm system administrators that changes to critical system files are malicious. This configuration of integrity checking software is best used for monitoring operating systems (OS) files that should not have an immediate effect on control system availability depending on the severity of the attack.

3.2.2 Remote Connectivity

Support following the EMS deployment at the customer site is facilitated through remote connectivity. Remote connections to control system are necessary for vendor support. Historically, this support has been via dial-up modem and in some cases may still be used. A growing trend, supported by vendors, is a customer provided virtual private network (VPN) connection encrypted for communications. This has replaced the need for dial-up modems. A VPN provides secure connections and authentication. However, two-factor authentication should also be used.

In the past, vendors did not encrypt sensitive data such as user credentials, namely user login and passwords, and insecure protocols. This data can easily be intercepted and used by an attacker to gain unauthorized access to data or to an actual control system. Recent trends by vendors include offering services to protect this traffic by using secure shell terminal emulation (SSH) or secure sockets layers (SSL), which are based on specifications aligned with the Department of Homeland Security: Cyber Security Procurement Language for Control Systems.⁴

Two-factor authentication requires users to provide two forms of identification. Examples of identification are, a single factor of identification, such as a password, plus a second factor in the form of an authentication token. A simple two-factor method --- based on something the user knows plus something the user possesses -- provides a more reliable level of user authentication than reusable passwords.⁵

This is also the case for engineering workstations and end-users that request data and connectivity to the control system environment.

⁴ Department of Homeland Security Cyber Security Procurement Language for Control Systems (2008)

⁵ Access Manager for e-business (Revised November 2006), Version 6.0

3.2.3 Other Forms of Securing Remote Connection Encryption

Secure Shell (SSH) provides communication between two devices to protect critical data from being exposed to attacks through encryptions; specifically, user authentication. Another form of encryption is Secure Sockets Layer (SSL).

3.2.4 Secure Inter Control Center Protocol (ICCP)

Control Centers have standardized on a method to exchange information between control centers, or even some devices. The standard communications is known as TASE.2 or Inter Control Center Protocol (ICCP). This protocol has been used for a number of years to exchange operating data between utility control centers, RTO/ISOs, and market systems. In recent years the ICCP protocol has been extended to enable encryption of the data. This is commonly referred to as Secure ICCP. Using Secure ICCP allows for an additional layer of security when exchanging data outside the control center. Typically the ICCP servers are also located in the DMS of the control center.

3.2.5 Use of Routable Protocols (SCADA Over IP)

A key driver in determining the trends in security for control systems has been the migration to routable protocols, essentially SCADA over IP.

System operations involving distributed real-time applications have been primary drivers of the technology choices, architecture, configuration, and network operations among all utilities. Traditionally, the communications architectures supporting these applications have been utilizing traditional synchronous networks.

3.3 Third-Party Vendors of SCADA Security Systems

There are a number of third-party vendors who have recognized that many legacy SCADA systems need to be brought into compliance with security best practices and government regulations. The general approach of these vendors is to install equipment that is essentially a front-end device (often an appliance) placed at access points to electronic security perimeters (ESP). These devices provide general security best practice technical security and enforce compliance with government regulation-enforced standards (e.g. CIP). Standard intrusion prevention system (IPS) on the perimeter of network access devices are one such deployment of a third-party device.

3.4 Trends from Vendors of General Security Assurance Systems

There are many vendors of best practice and policy compliance systems. These systems essentially audit cyber systems by inspecting configuration and configuration parameters and comparing them to various policy 'templates'. Many of these vendors now include the NERC CIP standards as a template.

CHAPTER 4: Conclusions and Recommendations

Control system vendors are aware of the urgent need to secure their systems. They have made strides in system design and implementing cyber security for control systems. These efforts are being funded, at the request of electric utility customers, government regulators, technical working groups, and industry's cyber security best-practices.

Vendors are more proactive than before, but there is much room for improvement. Vendors understand that they need to increase their efforts or potentially face a decline in sales of new systems. The legacy systems that were purchased by utility customers will also have to be considered as part of these efforts.

Finally, continued participation in vulnerability testing at the National Laboratories is essential. This is an exceptional way to benchmark their individual systems against their competition, but to mitigate vulnerabilities that need to be addressed before deploying their systems to customers.

The authors recommend the Energy Commission consider an annual research and review of the progress control system vendors are making in their cyber security initiatives. The review may be benchmarked against the information provided in this report and subsequent progress should be noted whereby the industry can gauge what, if any, progress is being made. Finally, future reports that track vendor trends should be presented to California's electric utilities on an annual basis such that it benefits the state.

GLOSSARY

ACL	Network Access Control List
CIP	Critical infrastructure Protection
EMS	Energy Management System
ESP	Electronic Security Perimeter
FAT	Factory Acceptance Test
ICCP	Inter-control Center Communication Protocol
INL	Idaho National Laboratory
IP	Internet Protocol
IPS	Intrusion Protection System
ISO	Independent System Operator
IT	Information Technology
NAC	Network Access Control rules
NERC	North American Electric Reliability Corporation
OEM	Original Equipment Manufacture
OOP	Object Oriented Programming language
OS	Operating System
PIER	Public Interest Energy Research
QAS	Quality Assurance Systems
RD&D	Research Development and Demonstration
RTO	Regional Transmission Organization
SANS	SysAdmin, Audit, Network, Security Institute
SCADA	Supervisory Control and Data Acquisition
SSH	Secure Shell terminal emulator
SSL	Secure Socket Layer

TASE.2	Telecontrol Application Service Element - 2
VPN	Virtual Private Network