CYBER SECURITY RESEARCH AND DEVELOPMENT

INTERIM PIER PROJECT REPORT

Prepared For:
California Energy Commission
Public Interest Research Program

Prepared By:
KEMA Inc.

May 2008
CEC-500-2008-021

Prepared By:
KEMA Inc.
Joe Weiss
Oakland, CA
Contract No. 500-06-014
Work Authorization 006-P-06

Prepared For:
Public Interest Energy Research (PIER) Program
California Energy Commission

David Chambers
Contract Manager

Mike Gravely
Office Manager
Energy System Research

Martha Krebs, Ph.D
Director
Public Interest Energy Research

Thom Kelly
Deputy Director
ENERGY RESEARCH & DEVELOPMENT DIVISION

Melissa Jones
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 warrant, 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, Jay Abshier, and Joe Bucciero of KEMA Inc. for their support in preparing this report.

CITATION

Weiss, Joe (KEMA Inc.). 2008. *Cyber Security Research and Development*. California Energy Commission, PIER Energy Systems Integration Program. CEC-500-2008-021.

PREFACE

The Public Interest Energy Research (PIER) Program 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 PIER Program, managed by the California Energy Commission (Energy Commission), conducts public interest energy research, development, and demonstration (RD&D) projects to benefit California.

The PIER program 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.

PIER funding efforts focus 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
- Renewable Energy Technologies
- Transportation.

This report is an interim report summarizing activity on the Cyber Security Research and Development project. The findings summarized in this report are not necessarily those of KEMA but rather of its principal research consultant.

For more information about the PIER Program, please visit the Energy Commission's website at www.energy.ca.gov/pier/ or contact the Energy Commission at 916-654-5164.

TABLE OF CONTENTS

California Energy Commission i
Acknowledgements i
CITATION i
Preface iii
Table of Contents v
List of Figures v
Abstract vii
Executive Summary 1
Introduction 3
Cyber security background information 5
Activity summary 9
Task 1 9
Task 2 9
Task 3 10
Task 4 10
Budget Expenditures 10
Project Results 10
Conclusions and Recommendations 13
Conclusions 13
Recommendations 13
Appendix 1 Automated Metering Infrastructure (AMI) Interview Guide 15
Background 15
Appendix 2 Substation Automation (SA) Interview Guide 17
Background 17
Appendix 3 Draft Energy Commission Management Presentation 19

LIST OF FIGURES

Figure 1 Typical SCADA Interface 6
Figure 2 Typical PLC Hardware 6

ABSTRACT

The Public Interest Energy Research (PIER) Security Research Program seeks to improve the ability of California's energy infrastructure stakeholders to prevent, prepare for and respond to threats, hazards, and supply disruptions, both natural and man-made. The PIER Security Research Program aims to accelerate transfer and exploration of technologies relevant to energy infrastructure security to enhance the reliability and survivability of California's electricity grid. These technologies, when developed specifically to protect electricity-related infrastructure, could help reduce vulnerabilities that are not being adequately addressed. This project focuses on cyber security of the critical infrastructure. Specific topics include Substation Automation and Automated Metering Infrastructure.

Keywords: Cyber security, substation automation, automated metering infrastructure

EXECUTIVE SUMMARY

The Public Interest Energy Research (PIER) Security Research Program seeks to improve the ability of California's energy infrastructure stakeholders to prevent, prepare for and respond to threats, hazards, and supply disruptions, both natural and man-made. The PIER Security Research Program aims to accelerate transfer and exploration of technologies relevant to energy infrastructure security to enhance the reliability and survivability of California's electric grid. These technologies, when developed specifically to protect electricity-related infrastructure, could help reduce vulnerabilities that are not being adequately addressed.

To improve the reliability of the electric infrastructure, the Energy Commission's PIER program initiated a project to provide support in preparing a feasibility study. The study will provide sufficient information to make an informed decision on further pursuit of cyber security control system research, development and demonstration. The informational content will contain technology and policy assessment and institutional considerations..

The electric transmission and distribution system is characterized by aging infrastructure and limited communication capabilities. This older infrastructure does not have the capability to perform or adequately use modern capabilities such as reliability-centered maintenance, which is a proven set of procedures for analyzing assets and structuring the tailor-made predictive and preventive maintenance tasks warranted by the asset's criticality and failure modes. Existing electromechanical devices with point-to-point communications with intelligent electronic devices, advanced communications, data warehouses, and system integration are being replaced by new technologies such as "Substation Automation" (SA), [1] which is comprised of intelligent electronic devices for protection and control of the electric transmission and distribution system by collecting, processing and transmitting data and information for the faster location and fixing of problems.

Demand-side automation is being implemented throughout California[2], which is expected to reduce consumers' costs and the need for new substations and power plants. The demand-side automation is also known as Automated Metering Infrastructure (AMI). Similar to SA, AMI also relies on digital electronics and new communication technologies. Both of these technologies will improve the reliability of the electric system but at a cost- cyber vulnerabilities.

The intent of this project is to assist the Energy Commission security research program manager in recommending appropriate cyber security research and development (R&D) priorities.

Due to a change in employment status of the principal researcher, a termination notice was issued on this work authorization in the initial stages of the project. Thus, this report serves

---

1. Substation Automation is comprised of intelligent electronic devices for protection and control of the electric transmission and distribution system by collecting, processing and transmitting data and information for the faster location and fixing of problems.
2. Demand-side automation is a communication system at the distribution level that can control customer load and can reduce peak-load generation through load management. Gönen, Turan. Electric Power Distribution System Engineering. McGraw-Hill, 1986. ISBN:0070237077.

as a final report summarizing activities conducted prior to the termination notice being issued. It is recommended that the project be concluded under a new work authorization.

INTRODUCTION

The PIER Security Research Program seeks to improve the ability of California's energy infrastructure stakeholders to prevent, prepare for and respond to threats, hazards, and supply disruptions, both natural and man-made. The PIER Security Research Program aims to accelerate transfer and exploration of technologies relevant to energy infrastructure security to enhance the reliability and survivability of California's electric grid. These technologies, when developed specifically to protect electricity-related infrastructure, could help reduce vulnerabilities that are not being adequately addressed.

To improve the reliability of the electric infrastructure, the Energy Commission's PIER program initiated a project to improve the cyber security of the selected electric energy applications and improve awareness of control system cyber security.

The electric transmission and distribution system is characterized by aging infrastructure and limited communication capabilities. This older infrastructure does not have the capability to perform or adequately utilize modern capabilities such as reliability-centered maintenance, integrated call management and automated fault location. New technologies, such as substation automation, replace existing electromechanical devices with point-to-point communications with intelligent electronic devices, advanced communications, data warehouses, and system integration.

Demand-side automation is being implemented throughout California, which is expected to reduce consumers' costs and the need for new substations and power plants. Demand-side automation is also known as Automated Metering Infrastructure. Similar to substation automation, automated metering infrastructure also relies on digital electronics and new communication technologies. Both of these technologies will improve the reliability of the electric system but at a cost - cyber vulnerabilities.

The intent of this project is to assist the Energy Commission security research program manager in recommending appropriate cyber security research and development priorities. Consequently, the project is composed of four tasks:

1. Identification of control system vulnerabilities for electric energy applications. This consists of identifying control system vulnerabilities for electric energy applications such as demand-side automation and automated metering infrastructure and preparation of a white paper.

2. Identify cyber security issues and ramifications. Provide two detailed presentations on cyber security issues and ramifications – one for Energy Commission technical staff and another for Energy Commission management.

3. Identify potential "beta" cyber security solutions and field demonstration opportunities. This includes assessing existing cyber security programs being performed by National Laboratories and universities and providing recommendations for demonstration projects with California utilities. Summarize results of research in a white paper.

4. Develop a utility cyber security metric for California investor own utilities. This includes developing a white paper.

All work related to this project was assigned to Joe Weiss of KEMA, Inc. Prior to the completion of the tasks, Joe Weiss ceased to be an employee of KEMA and no longer authorized to perform work under the KEMA contract. At that time, two of the four tasks were partially completed and approximately 20% of budget had been expended. This final report summarizes all activity that took place on the project prior to the termination of the authorization.

CYBER SECURITY BACKGROUND INFORMATION

The microprocessor, the Internet, and advanced telecommunications have significantly affected California's electric infrastructure both in enhancing productivity and changing how the industry responds to natural and man-made threats. These modern technologies are being back-fit or designed into the control and monitoring equipment used to generate, transmit, and distribute electric energy.

Control systems generally consist of an operator interface and field devices. The operator interface is usually the Supervisory Control and Data Acquisition (SCADA) Systems or plant Distributed Control System (DCS). Those systems are migrating toward off-the-shelf technologies and operating systems such as Windows, UNIX, and LINUX (Figure 1). Field devices such as Programmable Logic Controllers (PLCs), Remote Terminal Units, Intelligent Electronic Devices, field instrumentation and meters use proprietary operating systems and have operating requirements that are more stringent than traditional information technology systems (Figure 2). Consequently, the field devices are technically and operationally different than traditional information technology computing systems. Just like any information technology system dedicated to a special, critical function, companies should apply cyber security policy templates, software and hardware tools and testing with care. Inappropriate application of cyber security controls will have a negative impact on a systems function.

Figure 1
Typical SCADA Interface

Figure 2
Typical PLC Hardware

Along with the expected productivity improvements has come an unexpected impact – cyber vulnerabilities. For this project, the term cyber security refers to any electronic threat that could impact the performance of control systems. This definition includes intentional threats not specifically directed at the control system (e.g., viruses and worms), malicious threats specifically targeting the control system (e.g., hackers, but may include a virus or worm), and unintentional threats (e.g., inappropriate practices and testing). Based on many sources, the probability of unintentional threats occurring exceeds the probability of intentional threats. Some unintentional threats have caused significant damage. The

probability of unintentional threats occurring is reduced when robust policies and procedures are followed and the systems are monitored.

A common misunderstanding is equating the terms safety, reliability, and security. They are related but not the same. Making a system safe should, but does not necessarily, mean it is cyber secure. As an example, ProfiSafe is actually connected to Profibus making a safety-instrumented system less secure than when it was hard-wired and isolated.[3] Making a system more reliable also does not mean it is more secure. Following the Northeast Outage, many "cyber dumb" electro-mechanical switches and relays were replaced with "cyber-alive" intelligent electronic devices, which significantly improved system reliability but at the cost of new cyber security vulnerabilities. In some cases, making systems safer or more reliable may actually increase cyber vulnerabilities. How a device is implemented affects whether it is secure.

Properly implemented, protected, and monitored, a Transmission Control Protocol/Internet Protocol (TCP/IP) device that has a single generic user id and no passwords can be secured.[4] Conversely, a transmission control protocol/internet protocol device with the latest security features, if improperly implemented, protected and monitored is at risk of eventual compromise.

Control system cyber vulnerabilities are real and have impacted industrial control systems in California and elsewhere. There have been more than 80 cases reported world-wide involving the compromise of a control system due to the occurrence of a cyber security threat. These cases have encompassed all manufacturing industries including electric power, water, oil/gas, chemicals, and manufacturing. Control system cyber security threats have been both intentional and unintentional with impacts ranging from trivial to significant environmental and/or equipment damages.

In many business applications, the productivity of computer systems can be enhanced by integrating multiple systems and applications and sharing data throughout the enterprise. The same is true for control systems that enhance productivity by utilizing wireless communications, advanced computing algorithms and automated metering infrastructure. Using automated metering infrastructure as an example, communications include residential and commercial alternating current connections, IEEE 802.x wireless,[5] broadband over power line, power line carrier, satellite communications and the Internet. Integration includes linking the residential and commercial smart meters to electric distribution substation automation systems and from there to distribution and transmission supervisory control and data acquisition system. Utilizing a parallel path, the meter billing information is sent from the same smart meter to the billing collection center. As can be seen from these examples, integration and data sharing come with a potential price - cyber vulnerabilities.

The goal of cyber security is to implement security controls that mitigate the vulnerabilities, monitor for the occurrence of threats, and at the same time do not impact the functionality of the secured system. Most cyber security standards are actually guidelines. The North American Reliability Council (NERC) Critical Infrastructure Program (CIP) Cyber Security

---

3. ProfiSafe is an off the shelf secure communication software package. Profibus is an off the shelf secure networking package.
4. Transmission Control Protocol/Internet Protocol is the fundamental communication language or protocol of the internet and intranets.
5. Institute of Electrical and Electronics Engineers standards dealing with local area networks and metropolitan area networks.

Standards (CIP 002-009) are the first mandatory cyber security standards that have been formulated for the control system environment at the operational level. All previous standards have been either "guidelines" (e.g.: Industrial Automation and Control System Security -ISA SP99) or have been focused on the technical level, usually dealing with protocols. In fact, most of the cyber security standards throughout IT that are operational are at the technical, protocol level. The standards affecting credit card transactions, privacy and Sarbanes Oxley are some of the few exceptions.

The NERC CIP Standards mostly focus on the process used, and are heavy on documentation. In most cases, it is left up to the utility to decide the best way to protect critical assets. While there has been some criticism of this approach, it is essential for the standard to not proscribe solutions in order to have a longer lifetime. Also, it is advisable that those wishing to threaten the control systems controlling critical infrastructure not be able to read the CIP Standard and deduce the tools, techniques and security controls that utilities are using. Consequently, there is a need to understand the vulnerabilities, threats, and trade-offs between security and productivity, and identify potential solutions, while allowing individual utilities to implement the solutions appropriate for their situation.

However, the argument that the CIP Standards should be more prescriptive has merit. And, while Federal Energy Regulatory Commission (FERC) staff has recommended to the FERC Board that CIP 002-009 be approved, they have also asked NERC to consider updating the standard to address this issue. While currently not prescriptive, the existing NERC CIP Standards and cyber security industry best practices can yield metrics regarding monitoring and perimeter protection. Also, there persists a concern at FERC that the interconnections of utilities can yield vulnerabilities that are not mitigated and monitored. Therefore, a metric to evaluate the security of the interconnections between utilities would be valuable to assess the cyber security posture of the California utilities. There is the potential for many metrics that the California Energy Commission can use for these assessments.

ACTIVITY SUMMARY

Task 1

The project approach for Task 1 was to develop two interview guides on automated metering infrastructure and substation automation, recruit the utilities to participate in the surveys, administer the surveys, analyze findings and produce a white paper based on the results.

Task 1 activities were partially complete prior to termination of work. The activities consisted primarily of developing survey instruments to interview utilities on potential cyber vulnerabilities in substation automation and automated metering infrastructure. The survey instruments were developed collaboratively by KEMA and the CEC and are included in the Appendices of this report. The two interview guides developed included:

- Automated Metering Infrastructure Interview Guide (Appendix 1)
- Substation Automation Interview Guide (Appendix 2).

A technical presentation was to be prepared, to provide an overview of the cyber security research and development project for the utilities. The presentation was to include background information on the cyber security research and development project, including the specific goals of the research effort, project roadmap, technical issues to be addressed, potential benefits and questions to be examined. However, no technical presentation was prepared prior to the termination of work.

For Task 1, the security contacts at Pacific Gas and Electric (PG&E), Southern California Edison (SCE) and San Diego Gas and Electric (SDG&E) were identified and contacted. Each utility had different priorities and sensitivities that were briefly explored. Two of the three utilities appeared interested in participating in the research provided that they could obtain approval from upper management. However, no surveys were administered prior to the termination of work.

The next step will be to survey the investor-owned utilities in California – PG&E, SCE and SDG&E - and develop a white paper on cyber security vulnerabilities for electric energy applications. We recommend that this work be pursued under a subsequent work authorization.

Task 2

The scope for Task 2 consisted of developing two presentations for Energy Commission staff – one for Energy Commission technical staff and one for Energy Commission management.

Task 2 activities consisted of identifying cyber security issues and ramifications and developing a draft presentation directed at Energy Commission management (Appendix 3). The key objective of the presentation is to provide a high level overview of the technical and liability issues related cyber security and the control systems that make up the critical infrastructure.

Remaining work to be done under Task 2 includes development of a presentation for the technical staff at the Energy Commission. We recommend that this work be pursued under a subsequent work authorization.

Task 3

The scope for Task 3 consisted of conducting research to identify potential "beta" cyber security solutions and field demonstration opportunities. Once the research was conducted, a white paper would be developed to summarize key findings.

No activities on Tasks 3 were initiated prior to the work being terminated.

Remaining work to be done under Task 3 includes the entire task. We recommend that this task be pursued under a subsequent work authorization.

Task 4

The basic approach for Tasks 4 was to conduct research to support development of an utility cyber security metric for the California investor-owned utilities. Once the research was conducted, a white paper would be developed summarizing key findings.

No activities on Task 4 were initiated prior to the work being terminated.

Remaining work to be done under Task 4 includes the entire task. We recommend that this task be pursued under a subsequent work authorization.

Budget Expenditures

Approximately 20% of the original budget was expended prior to the work being terminated.

PROJECT RESULTS

Activities related to the project prior to termination of work include the following:

Task 1

- Development of two survey instruments, Automated Metering Infrastructure and Substation Automation

- Development of presentation for utilities summarizing cyber security research and development project

- Discussions with representatives from PG&E, SCE and SDG&E about cyber security research and development project and recruitment to participate in surveys

All three investor-owned electric utilities in California - PG&E, SCE, and SDG&E - were approached to provide input to the cyber security research and development project. The utility representatives at two of the utilities expressed willingness to participate in the surveys, provided they could obtain approval from their management. One utility representative declined to be interviewed.

Task 2

- Development of presentation for Energy Commission management

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Any device, depending on how it is implemented, can be vulnerable. However, the vulnerability is real only if the device can be accessed by unauthorized people.

Researchers have previously noted the generic cyber vulnerabilities in modern networking and communication technologies. However, there is a need to determine how these generic vulnerabilities manifest themselves in modern electric utility operations including substation automation and automated metering infrastructure applications. Furthermore, there is confusion regarding what are the specific technical and operational issues that make control system cyber security different than traditional corporate information technology security. Consequently, there is a need to provide additional awareness as to the technical, administrative, and safety implications associated with control system cyber security.

Without the participation of the utilities, the proposed outcome of the originally planned project will be severely constrained. If the utilities choose not to participate, the identified cyber vulnerabilities will be of a generic nature and the recommended research and development may not be as directly applicable to the California market. Consequently, we recommend further detailed discussions with each of the three utilities in the subsequent project focused on building a collaborative research project that is mutually beneficial to all parties with a vested interest. Also, it might be desirable to develop an approach that will allow participants to maintain as much anonymity as possible.

Recommendations

The primary recommendation is to complete the activities of all four tasks under a new work authorization. Additionally, we recommend that the project team place more emphasis on developing a more collaborative process with the California investor-owned utilities to enhance their willingness to participate in the surveys and contribute to identifying cyber security and research and development priorities. In addition to the tasks outlined in the original work authorization, the project team should consider holding public workshops and/or roundtables to explore issues related to cyber security and research and development priorities.

Additional considerations for future research include the following:

- Cyber Security trends in vendor products
- Control System Cyber Security Benchmarks.

APPENDIX 1 AUTOMATED METERING INFRASTRUCTURE (AMI) INTERVIEW GUIDE

Interview Guide

Contact Information

Name
Title
Function
Organization
Phone
Fax
E-mail
Mailing Address

Background

The California Energy Commission's Critical Energy Infrastructure Security (CEIS) Program is attempting to identify research and development opportunities to address critical vulnerabilities and interdependencies not being addressed by the private sector and public sector entities at the federal and state levels, with the aim of enhancing the security of the energy infrastructure. The Program is seeking to identify high priority research initiatives that support California's energy policy. High priority research initiatives are those that:

- Address critical vulnerabilities or interdependencies that are not being addressed by the private sector or state/federal agencies
- Will enable promising technology or create critical knowledge
- Support the public interest.

One area upon which we are focusing is the Automated Metering Infrastructure (AMI). We would appreciate your input to better understand your perception of energy infrastructure vulnerabilities for which security may be greatly enhanced through analysis and research supported by the CEIS Program.

NOTE: Please refrain from sharing any information that may be considered confidential or sensitive. This effort is seeking to gather information at a high, generalized level to inform policy and future work.

DATE:

1. What organizations within the utility and vendors are you interfacing with on the AMI project? Is cyber security a part of the interface discussions?

2. What cyber security functionality are you requiring from the meter vendor and AMI meter integrator? What was the vendors reaction?

3. What cyber security controls are you implementing from the meter to the meter data repository? Do these controls include telecommunications?

4. Have you conducted cyber security vulnerability assessments on the design (including telecommunications) and if completed, have you commissioned a penetration test to see if the system can be hacked? If these assessments were performed, were they performed by in-house staff or consultants?

5. . Where do you think state funding for AMI security R&D research, such as that from the CEIS Program, can most effectively be put to use?

6. Would you be willing to host a demonstration project to evaluate proposed AMI security technologies?

APPENDIX 2 SUBSTATION AUTOMATION (SA) INTERVIEW GUIDE

Interview Guide

Contact Information

Name
Title
Function
Organization
Phone
Fax
E-mail
Mailing Address

Background

The California Energy Commission's Critical Energy Infrastructure Security (CEIS) Program is attempting to identify research and development opportunities to address critical vulnerabilities and interdependencies not being addressed by the private sector and public sector entities at the federal and state levels, with the aim of enhancing the security of the energy infrastructure. The Program is seeking to identify high priority research initiatives that support California's energy policy. High priority research initiatives are those that:

- Address critical vulnerabilities or interdependencies that are not being addressed by the private sector or state/federal agencies
- Will enable promising technology or create critical knowledge
- Support the public interest.

One area upon which we are focusing is Substation Automation (SA). We would appreciate your input to better understand your perception of energy infrastructure vulnerabilities for which security may be greatly enhanced through analysis and research supported by the CEIS Program.

NOTE: Please refrain from sharing any information that may be considered confidential or sensitive. This effort is seeking to gather information at a high, generalized level to inform policy and future work.

DATE:

1. What organizations within the utility and vendors are you interfacing with on the SA projects? Is cyber security a part of the interface discussions?

2. What cyber security functionality are you requiring from the vendors and system integrator? What was the reaction from the vendor and system integrator?

3. For communication to the data warehouse, what cyber security controls will be implemented?

4. Have you performed a vulnerability assessment on the design? If completed, have you performed a penetration test? If these were done, were they performed by in-house staff or consultants?

5. Where do you think state funding for SA security R&D research, such as that from the CEIS Program, can most effectively be put to use?

6. Would you be willing to host a demonstration project to evaluate either proposed SA security technologies?

APPENDIX 3 DRAFT ENERGY COMMISSION MANAGEMENT PRESENTATION

Cyber Security of Control Systems-A Management Primer for the California Energy Commission

Cyber Security of Control Systems - A Management Primer for the California Energy Commission

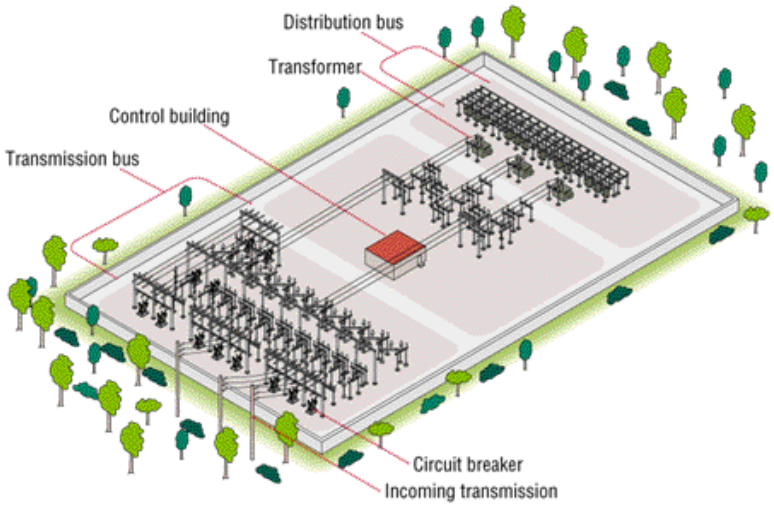
April, 2007

What are Industrial Control Systems

Industrial Control Systems

- SCADA – Supervisory Control and Data Acquisition
- DCS – Distributed Control System
- PLC – Programmable Logic Controller
- RTU – Remote Terminal Unit
- IED – Intelligent Electronic Device
- Field devices – Sensors, drives, etc

Supervisory Control and Data Acquisition (SCADA)



SCADA is used extensively in the electricity sector. Other SCADA applications include gas and oil pipelines, water utilities, transportation networks, and applications requiring remote monitoring and control. Similar to real-time process controls found in buildings and factory automation.

CONTROL

•Generator Set Points
•Transmission Lines
•Substation Equipment

DATA

•Critical Operational Data
•Performance Metering
•Events and Alarms

Communication Methods

•Directly wired
•Power line carrier
•Microwave
•Radio (spread spectrum)
•Fiber optic

Control Center

Provides network status, enables remote control, optimizes system performance, facilitates emergency operations, dispatching repair crews and coordination with other utilities.

KEMA

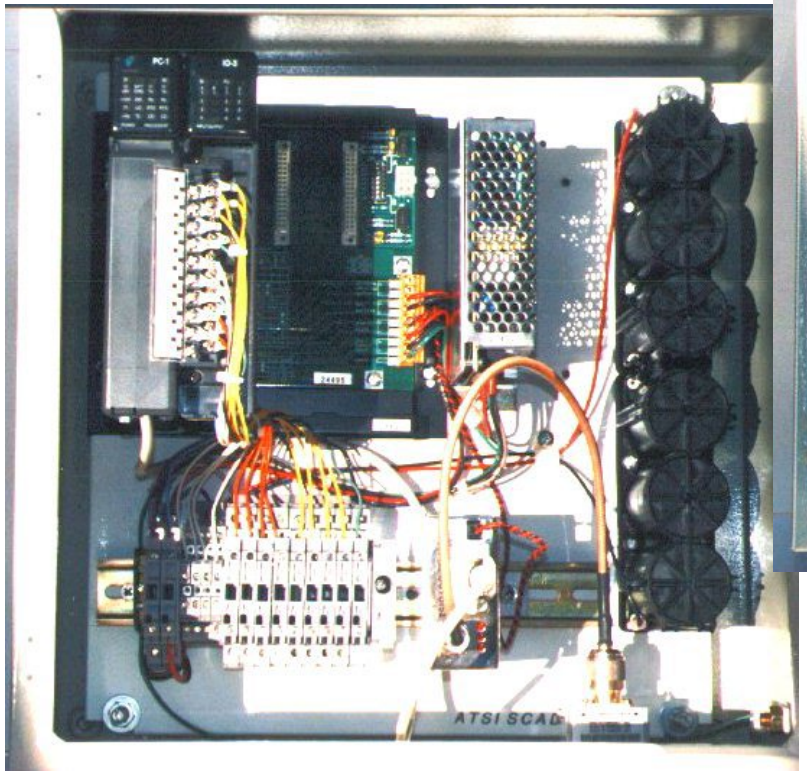
Typical Control Room Layout

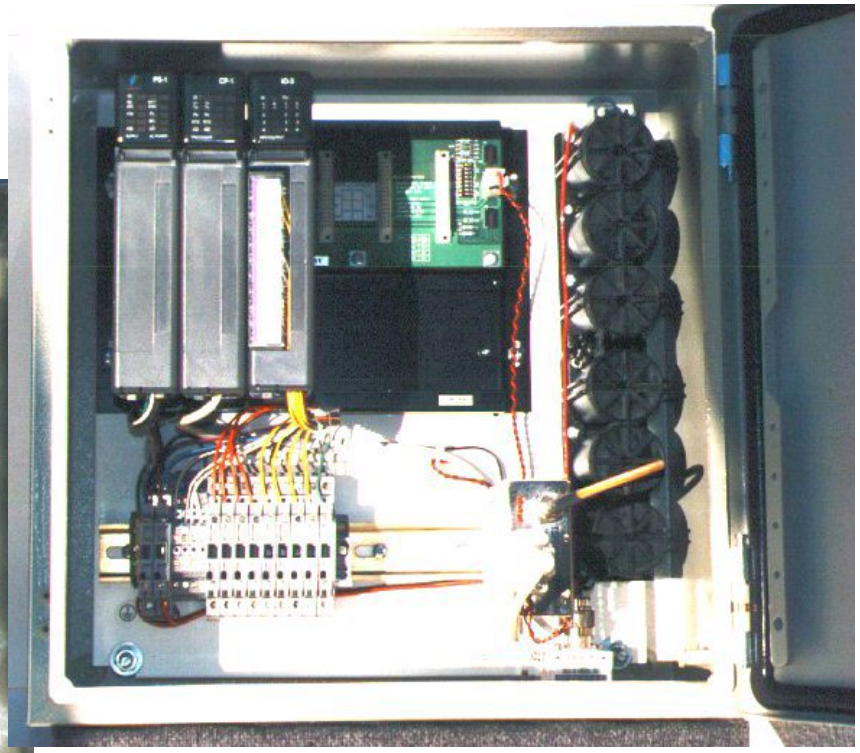
Industrial Control Systems

- Digital systems designed to provide real time control and/or monitoring of processes
- Control Center systems
  - Operator interface – usually Windows, UNIX, LINUX
  - SCADA Servers – usually UNIX, LINUX
  - This is what most people think about
- Field controller – Proprietary Real Time Operating System
  - This part generally has been ignored

Typical Operator Interface

Typical RTU Hardware





What Makes Control Systems Vulnerable

SCADA Trends

- Open Protocols
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Interconnected to Other Systems
  - Connections to business and administrative networks to obtain productivity improvements and mandated open access information sharing

SCADA Interconnections

- Business and Engineering Networks
  - The IT link between engineering and business services is crucial for business operation
  - Improperly implemented, this is a typical hacker pathway into the Control System.
- Market Systems
  - Interconnection into market systems is relatively new
  - Some disagree this should be done
  - Few agree on how it should be done securely
- Other Systems
  - GIS, Call Management, others

KEMA

Sharing of Telecommunications

- Many utilities no longer have stand-alone isolated systems for SCADA communications networks under their sole control
- In some cases, utilities have purchased bandwidth from telecommunications providers
- In other cases, utilities sell excess bandwidth to others
  - Either other business units within the enterprise, or outside entities
- Often, multiple communication technologies (e.g., fiber optic, microwave, spread spectrum, twisted pair, etc) and/or bandwidth owners/operators for a single SCADA system (particularly for larger utilities)
  - Mixture of legacy communication systems with other solutions

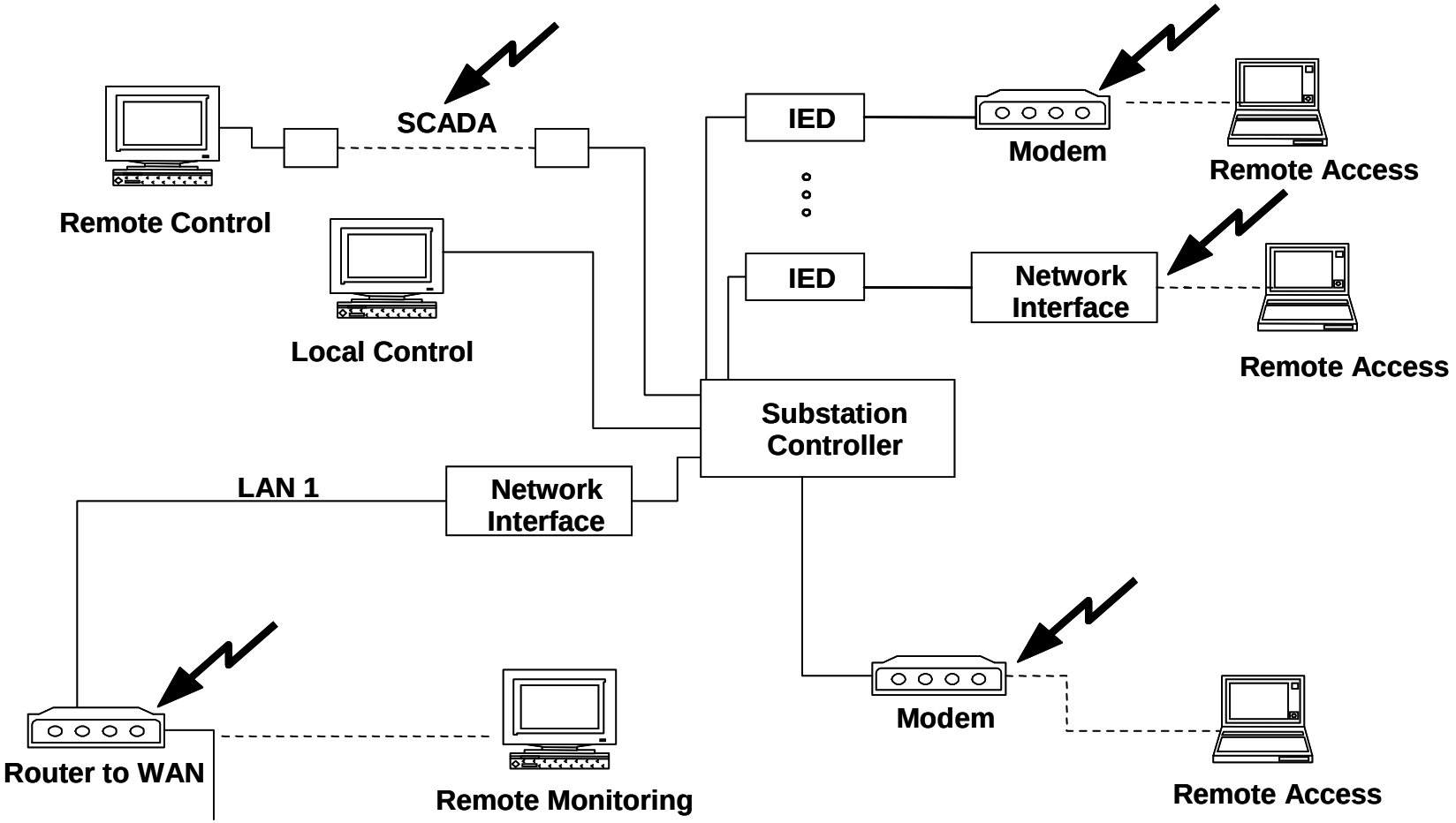
KEMA

Cyber Security Will Impact How New Technology Is Implemented

- New technology and information flow is improving productivity
  - Telecom including BPL, VOIP, Bluetooth, 802.11
  - RFID, Smart Dust
  - Reliability Centered Maintenance (RCM)/Machinery monitoring
  - Smart grid, Substation automation, Automated meter reading
  - Boiler control, Condenser/cooling tower system optimization
  - Advanced field devices
  - System integration, Data warehousing
- They will be used, but… they come with a price tag cyber vulnerabilities
  - Need to address how to best utilize these technologies

KEMA

Vulnerable Points



Graphic courtesy of Paul Oman, Schweitzer Engineering Laboratories, Pullman Washington

KEMA

SCADA Vulnerabilities

- Few data security safeguards
  - Authenticity and integrity is assumed
  - Confidentiality requirements are unknown and ignored
- Few control safeguards
  - Check-before-operate is often the only authentication mechanism
  - Some control signals are not authenticated at all
- Some control networks depend on outside sources
- Control is highly centralized
- PSTN Modem links must be secured
- Password policies and security administration of legacy equipment are substandard

KEMA

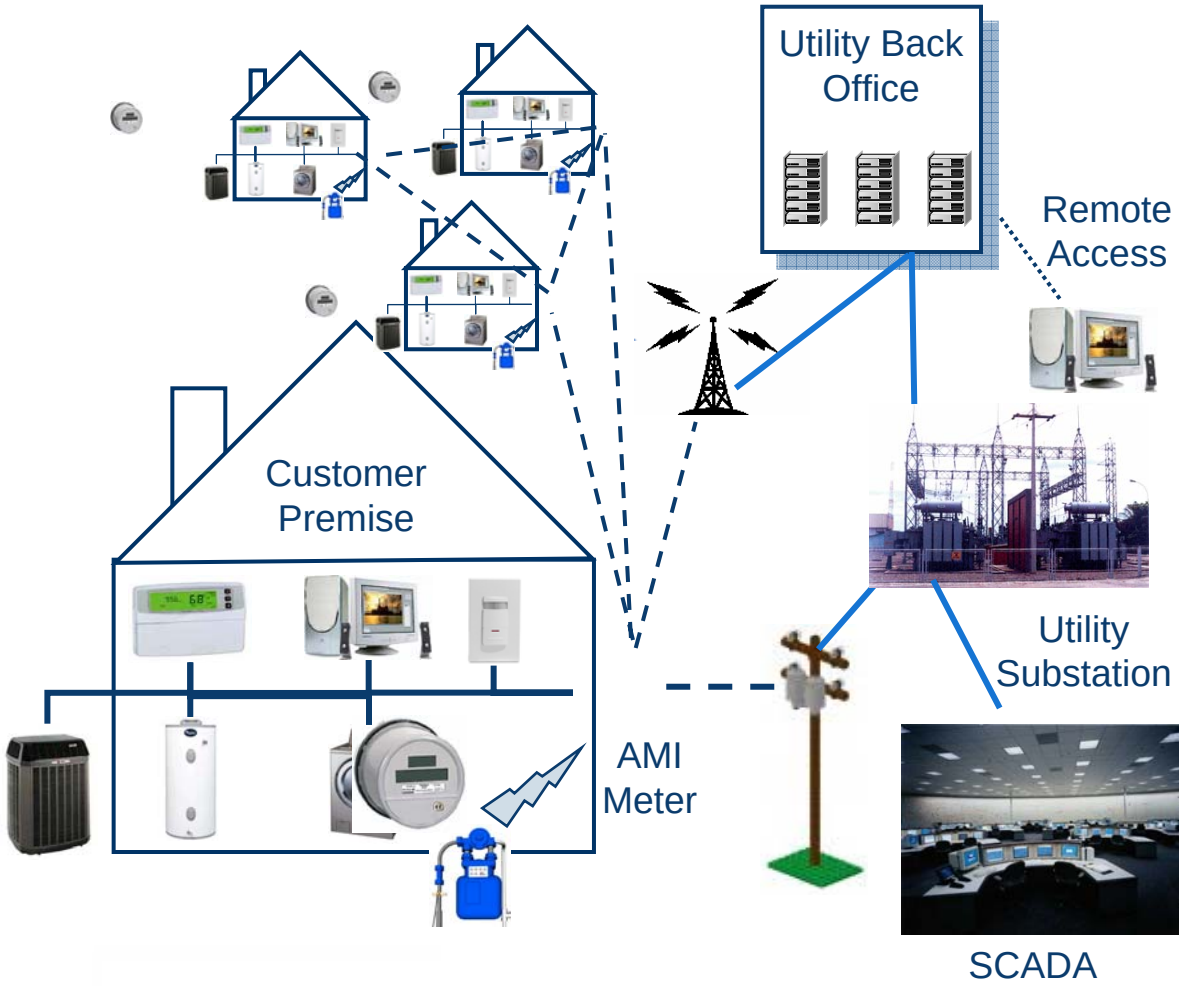
SCADA Vulnerabilities (cont)

- SCADA information links can be are prone to snooped and interrupted
- Configuration management usually is practiced beyond systems directly affecting physical operations
- Interconnectivity and interdependencies not widely understood
  - Boundaries of systems and authorities (particularly information systems) are becoming blurred
  - Level of trust granted is frequently unwarranted
  - Partitioning logical systems to control access and limit influence is not widely practiced
  - No explicit vendor security validation
- Limited incident detection, reporting, recovery, and forensics capability

KEMA

Automated Metering Infrastructure*

AMI Connectivity (illustrative)



AMI Communications Trends

- Full two-way (bi-directional)
- Near real-time
- Higher bandwidth
- Increasing number of communications nodes
- Utility price signals to smart appliances
- Peer-to-peer mesh networks
- Distributed generation control
- Multiple backhaul integration
- Meter as a premise "portal"
- Device interoperability
- Open communications protocols
- Self-diagnostics and programming
- Minimal network administration
- Self-registry capabilities
- Improved substation productivity
- Improved economic dispatch

*Source, KEMA Inc.

Cyber Security is On-going

- System vulnerabilities and threats are constantly changing
  - Any modification, integration, upgrade, or test can affect cyber vulnerability
  - Vulnerability assessments are a snap-shot in time
- There is NO silver bullet
  - No single technology is sufficient to protect control systems
  - Change and Configuration Control are required
  - Frequent Vulnerability Assessments and Penetration Tests are required.

KEMA

What Makes Control Systems Different Than IT

Comparison of Corporate IT to Control Systems

Attribute	Office IT	Control Systems
System Life Cycle	3-5 years	15-25 years
Security skills/awareness	Good	Usually poor
Patching	Frequent	Slow or impossible
Software changes	Frequent, formal, and documented	Rare, informal, not always coordinated
Automated tools	Widely used	Limited, used with care

KEMA

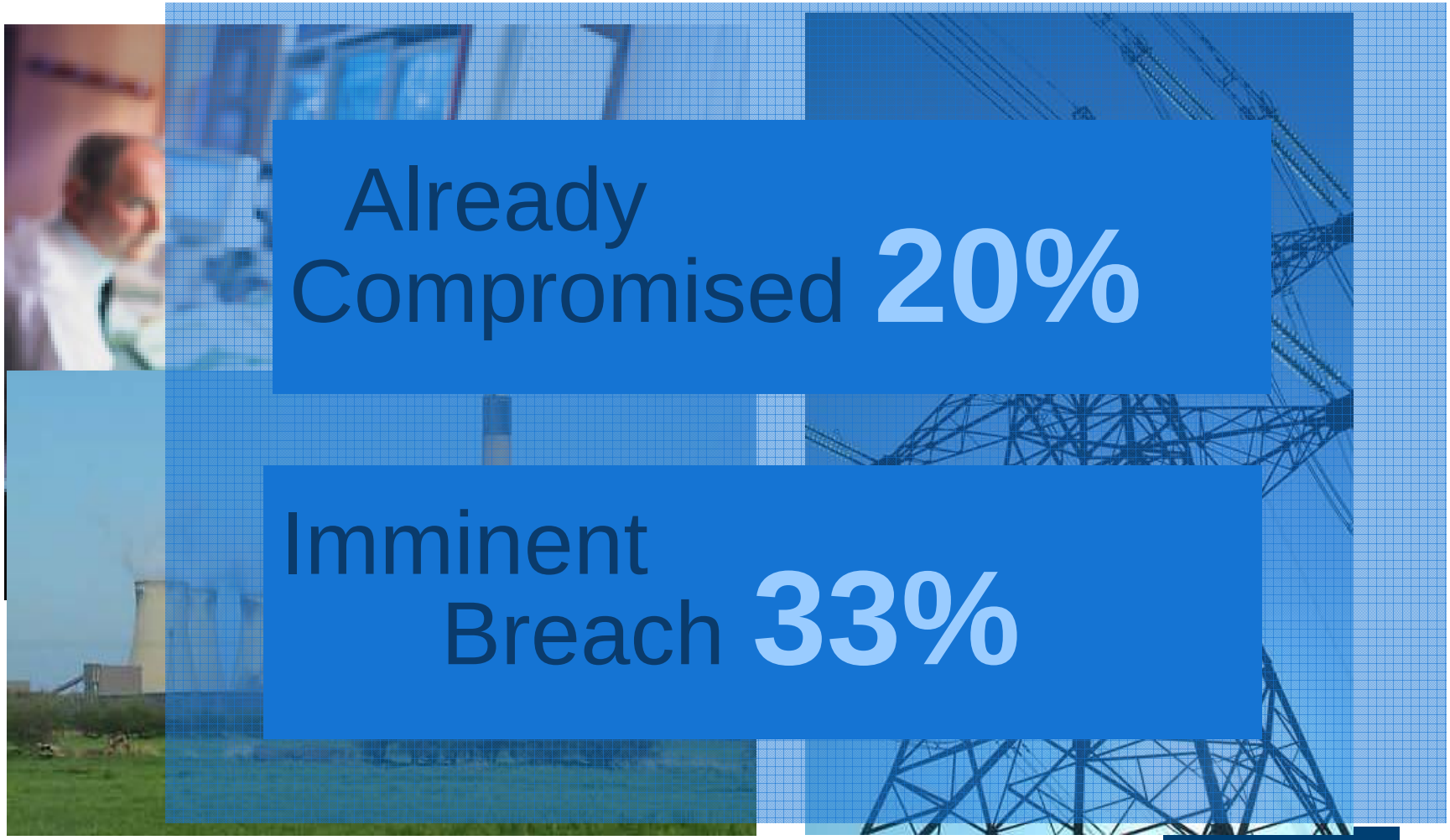
Comparison of Corporate IT to Control Systems

Attribute	Office IT	Control Systems
Communication protocols	IP, X.25	IP, DNP, ICCP, Modbus
Communications	Telco, wi-fi, satellite, Microwave	Telco, radio, satellite, power line carrier, wi-fi
Computing resources	High	Very limited
Bandwidth	High	Limited
Security standards	ISO-17799, PCI, SOX	ISA SP99, NERC CIP, etc
Administration	Centralized and Localized	Localized
Operating systems	COTS (Windows, UNIX, LINUX)	COTS for HMI, proprietary real time for field devices
Security impacts	Business, Financial, Privacy, Intellectual Capital, Competitiveness	Business, equipment, personnel safety, and environment

KEMA

Awareness and Confusion

Utilities Rate SCADA Threats – 50 Utilities



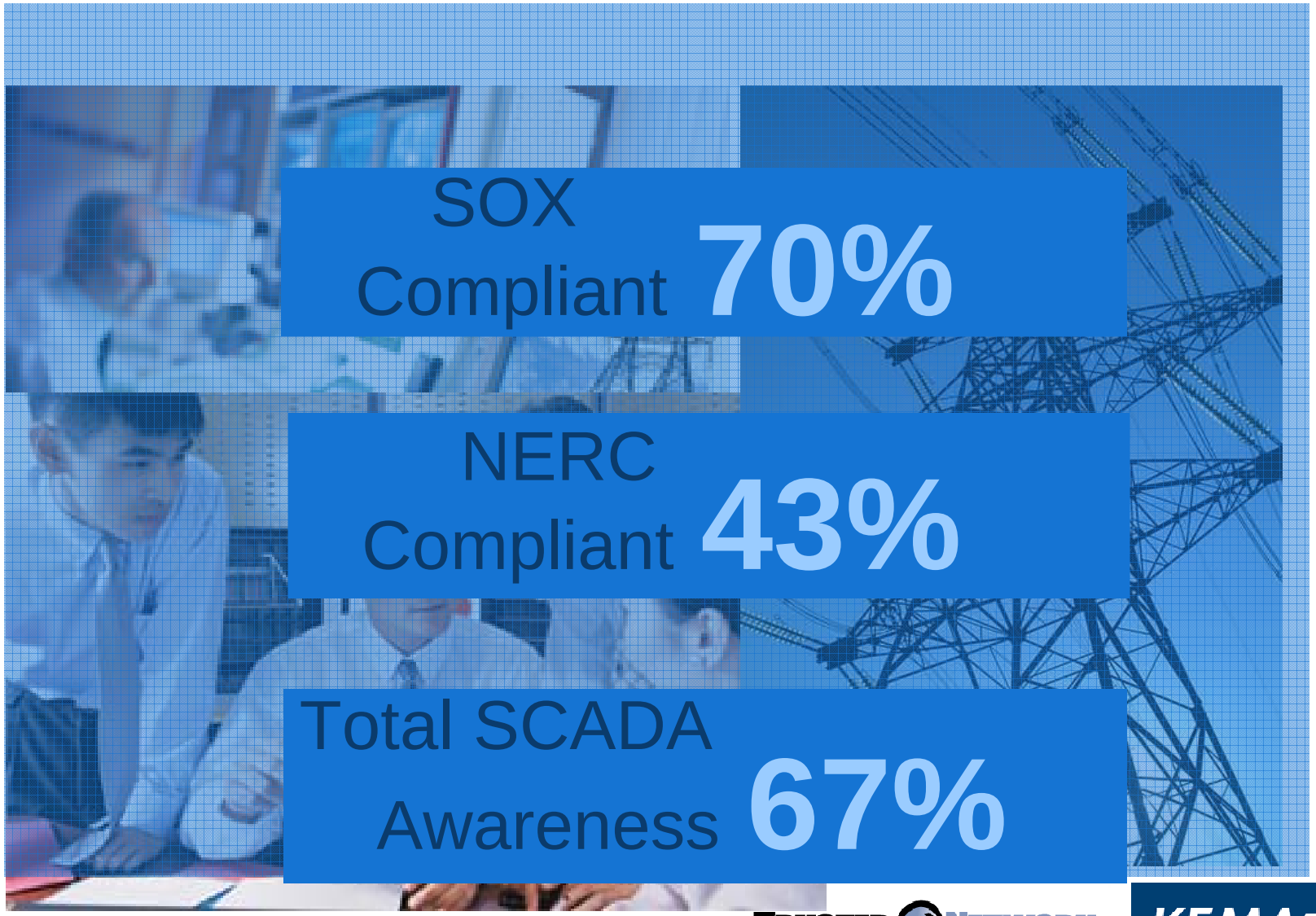
Already Compromised **20%**

Imminent Breach **33%**

TRUSTED NETWORK TECHNOLOGIES

KEMA

How Do They Think They're Doing?



SOX Compliant **70%**

NERC Compliant **43%**

Total SCADA Awareness **67%**

TRUSTED NETWORK TECHNOLOGIES

KEMA

Problems

- For 50%-60%, most relevant problems related to internal IT infrastructure
  - Maintainability on change in CC system, data consistency among data stores, proprietary (vendor) APIs of CC software
- IT security a concern for 42%

→Same concerns as for any enterprise-wide system: data consistence, maintainability, IT security

From CIGRE WG C2.01 DE Questionnaire presented at CIGRE San Antonio, October 6, 2005

Selected Case Histories

The Threat is Real

- More than 80 known cases (intentional and unintentional)
- All industries
  - Electric (T&D, fossil, hydro, and nuclear)
  - Oil/gas
  - Water
  - Chemicals
  - Manufacturing
  - Railroads
- Damage ranging from trivial to equipment damage and death

KEMA

Types of Threats

- Intentional target threat
- Unintended consequence (eg, viruses, worms)
- Unintentional (eg, inappropriate or inadequate testing, procedures, etc)
- Incidental impacts
  - Security impacting performance – need to balance

Queensland, Australia

- April 23, 2000: Vitek Boden, 48, caught with stolen computer, radio transmitter during his 46th successful intrusion….
- Until then, utility managers didn't know why the system was leaking hundreds of thousands of gallons of sewage into parks, rivers, and the Hyatt Regency hotel grounds
- Attack method:
  - Software on his laptop identified itself as "pumping station 4".
  - He then suppressed alarms, and became the "central control system" with unlimited command of 300 SCADA nodes
- Disgruntled former SCADA (NOT utility) employee
- Convicted and sentenced to two years in prison

KEMA

Gasoline Pipeline Explosion

- June 10, 1999: 237,000 gallons of gasoline leak from 16" pipeline, ignited 1.5 hours later - 3 deaths, 8 injuries, $45 Million property damage
- "Immediately prior to and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation."
- Warning issued to other pipeline operators by the Office of Pipeline Safety July 1999
- NTSB report issued October 2002 Key recommendation:
  - Utilize an off-line development system for implementing and testing changes to the SCADA database
- Olympic Pipe Line Co. filed for Chapter 11 Bankruptcy March 27, 2003

Targeted SCADA Attack

- **Event**: Insecure GIS mapping system with no firewall into SCADA led to vulnerability allowing targeted attack from Internet resulting in loss of SCADA
- **Industry**: Electric Transmission & Distribution
- **Location**: North America
- **Information Source**: SCADA Engineer's presentation at 4th KEMA Cyber Security Workshop – August 2004
- **Impact**:
  - SCADA servers and mapping system lost for two weeks
  - Installation of firewalls, proxy servers, IDS and LAN monitors
  - Neighboring utility networks went from trusted to untrusted
  - 4 Man-months to recover
- **Lessons learned**:
  - Isolate SCADA system from corporate LAN
  - Install firewall between the DSL router and the corporate LAN
  - Install group of firewalls between the frame relay and neighbors to isolate all ports that are not business-related

Viruses/Worms

- **Event**: Substation communication failure caused by Slammer worm traffic. Failures caused by virus traffic jamming frame relays.
- **Unintentional** side effect caused by intentional virus attack
- **Industry**: Electric Power T&D
- **Location**: North America
- **Information Source**: SCADA List server report followed up with telecom confirmation
- **Impact**: SCADA failed resulting in loss of control of switchyards
- **Lessons learned:** Assess and assure Telco (e.g., frame relays) has no Internet connections and they are appropriately secure
  - Effective cyber security protection is required

KEMA

Sneakernet

- **Event**: Plant shutdown from “contaminated” game disc input into PLC workstation
- **Industry:** Food Processing
- **Location:** North America
- Information Source: Control system integrator
- **Impact:** Several days lost production
- **Lessons learned:** Do not allow external devices or files to be connected to plant network

Testing Impacts

- **Event:** Virus fix erased licensing keys
- **Industry:** Manufacturing
- Location: North America
- **Information Source**: Electrical Systems Manager
- **Impact:** System down until licensing keys replaced
- **Lessons learned:** Test all patches under field conditions before installation

Wireless Substation Vulnerabilities

- Evaluators drove to a remote substation. Without leaving their vehicle, they noticed a wireless network antenna. They plugged in their wireless LAN cards, fired up their notebook computers, and connected to the system within five minutes because it wasn't using passwords.
- Within 10 minutes, they had mapped every piece of equipment in the facility. Within 15 minutes, they mapped every piece of equipment in the operational control network. Within 20 minutes, they were talking to the business network and had pulled off several business reports. They never left the vehicle.

Regulation

Cyber Security Requirements

- NERC CIP 002-009 (Transmission and selected fossil generation)
- NEI-0404 (Nuclear)
- Chemical Industry rulemaking

NERC Compliance – CIP 002-009

- Status
  - Approved by NERC Board
  - Implementation schedule defined
  - FERC Staff Recommended Approval
  - FERC Staff Requested NERC consider enhancements

NERC Compliance

- Benefits
  - Establishes a structured, documented approach
- Shortcomings
  - Fundamentally based on modern SCADA; not field control systems
  - Heavily focused on documentation
  - Implementation may not be consistent

What Can Energy Commission Do?

Energy Commission Opportunities

- Provide leadership in helping to secure the California critical infrastructure
- Identify and develop R&D portfolio to address AMI and substation automation cyber vulnerabilities
- Provide awareness to key California stakeholders
- Provide control system cyber security technology evaluations and demonstrations with California utilities
- Evaluate “green” technologies for cyber security considerations

KEMA

Other Issues for Energy Commission and Industry

- Inter-organization coordination
  - These systems are interconnected- who's in charge
- Inter-project coordination
  - Most new Energy Commission projects such as renewables, reliability, etc are affected by cyber- who's in charge
- Liability
  - Who is responsible
- Insurance
  - Is it an "act of war"
- Rate relief for security improvements
  - Does this require "books to be reopened"
- Other

Summary

- Securing control systems is a business, state, and national security issue
- Energy Commission can help with targeted R&D and leadership

Thank you for your attention.