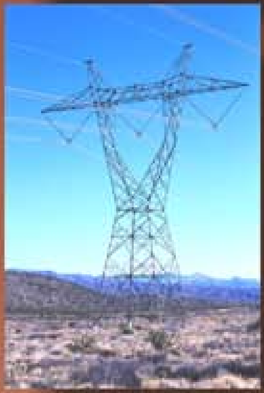
Roadmap to Secure Control Systems in the Energy Sector



January 2006

Sponsored by

U.S. Department of Energy

U.S. Department of Homeland Security

Prepared by

Energetics Incorporated
Columbia, Maryland

Roadmap to Secure Control Systems in the Energy Sector

January 2006

Sponsored by the
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy

and the
Science and Technology Directorate
U.S. Department of Homeland Security

in collaboration with
Energy Infrastructure Protection Division
Natural Resources Canada

Prepared by
Jack Eisenhauer
Paget Donnelly
Mark Ellis
Michael O'Brien
ENERGETICS
Columbia, Maryland

Foreword

This document, the **Roadmap to Secure Control Systems in the Energy Sector**, outlines a coherent plan for improving cyber security in the energy sector. It is the result of an unprecedented collaboration between the energy sector and government to identify concrete steps to secure control systems used in the electricity, oil, and natural gas sectors over the next ten years. The Roadmap provides a strategic framework for guiding industry and government efforts based on a clear vision supported by goals and time-based milestones. It addresses the energy sector's most urgent challenges as well as longer-term needs and practices.

A distinctive feature of this collaborative effort is the active involvement and leadership of energy asset owners and operators in developing the Roadmap content and priorities. The Roadmap synthesizes expert input from the control systems community, including owners and operators, commercial vendors, national laboratories, industry associations, and government agencies. The Roadmap project was funded and facilitated by the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability in collaboration with the U.S. Department of Homeland Security's Science and Technology Directorate and the Energy Infrastructure Protection Division of Natural Resources Canada.

The members of the Control Systems Roadmap Steering Group wish to thank members of the diverse control systems community who contributed their valuable ideas, insights, and time to make this Roadmap possible. In addition, we commend Hank Kenchington of DOE for his outstanding leadership in this important project.

We strongly encourage industry and government to adopt this Roadmap as a template for action. The Roadmap marks a beginning rather than an end. It will require continued support, commitment, and refinement from industry and government to fulfill its promise in the years ahead.

Control Systems Roadmap Steering Group

Michael Assante
International Electricity
Infrastructure
Assurance Forum

Tommy Cabe
Sandia National Laboratories

Jeff Dagle
Pacific Northwest National
Laboratory

David Darling
Natural Resources Canada

Kimberly Denbow
American Gas Association

Thomas R. Flowers
CenterPoint Energy

Tom Frobase
Teppco Partners, LP

Gary Gardner
American Gas Association

Robert Hill
Idaho National Laboratory

Hank Kenchington
U.S. Department of Energy

Tom Kropp
Electric Power Research Institute

Douglas Maughan
U.S. Department of Homeland
Security—Science & Technology
Directorate

Linda M. Nappier
Ameren

David Poczynek
Williams

Al Rivero
Chevron (now with Telvent)

William F. Rush
Gas Technology Institute

Lisa Soda
American Petroleum Institute

Table of Contents

Executive Summary

Control systems form the central nervous system of the North American energy infrastructure. They encompass vast networks of interconnected electronic devices that are essential in monitoring and controlling the production and distribution of energy in the electric grid and the oil and gas infrastructure. The ability of these cyber systems to provide automated control over a large, dispersed network of assets and components has helped to create the highly reliable and flexible energy infrastructure we have today. However, this span of control requires control systems to communicate with thousands of nodes and numerous information systems—thus exposing energy systems and other dependent infrastructures to potential harm from malevolent cyber attack or accidents.

> "Securing [control systems] is a national priority. Disruption of these systems could have significant consequences for public health and safety."
>
> National Strategy to Secure Cyberspace (pg. 32)
> The White House, February 2003

An Urgent Need

Energy control systems are subject to targeted cyber attacks. Potential adversaries have pursued progressively devious means to exploit flaws in system components, telecommunication methods, and common operating systems found in modern energy systems with the intent to infiltrate and sabotage vulnerable control systems. Sophisticated cyber attack tools require little technical knowledge to use and can be found on the Internet, as can manufacturers' technical specifications for popular control system equipment. Commercial software used in conventional IT systems, which offers operators good value and performance but poor security, is beginning to replace custom-designed control system software.

Efforts by the energy sector to uncover system vulnerabilities and develop effective countermeasures have so far prevented serious damage. However, attacks on energy control systems have been successful. The need to safeguard our energy networks is readily apparent: energy systems are integral to daily commerce and the safe and reliable operation of our critical infrastructures. Any prolonged or widespread distruption of energy supplies could produce devastating human and economic consequences.

Industry Leadership

The urgent need to protect our energy control systems from cyber attack has prompted industry and government leaders to step forward and develop an organized strategy for providing that protection. Their efforts have produced this **Roadmap to Secure Control Systems in the Energy Sector**, which presents a vision and supporting framework of goals and milestones for protecting control systems over the next ten years. This strategic framework enables industry and government to align their programs and investments to improve cyber security in an expedient and efficient manner. The Roadmap integrates the insights and ideas of a broad cross-section of asset owners and operators, control system experts, and government leaders who met for a two-day workshop in July 2005 and contributed to subsequent reviews. Their purpose was simple: create an effective plan and execute it.

The Vision

Asset owners and operators believe that within ten years control systems throughout the U.S. energy sector will be able to survive an intentional cyber assault with no loss of critical function in critical applications. This is a bold vision that confronts the formidable technical, business, and institutional challenges that lie ahead in protecting critical systems against increasingly sophisticated cyber attacks.

Vision for Securing Control Systems in the Energy Sector

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.

Utilities and energy companies have long recognized that it is neither practical nor feasible to fully protect *all* energy assets from natural, accidental, or intentional damage. However, the sector's track record of excellent reliability reflects an effective protective approach that balances preventive measures with rapid response and recovery in a competitive business environment. Accordingly, the industry's vision for securing energy control systems focuses on critical functions of the most critical applications. These are the functions that, if lost, could result in loss of life, public endangerment, environmental damage, loss of public confidence, or severe economic damage. This risk-based approach builds on the established risk-management principles now in use throughout the energy sector.

Roadmap Scope

This Roadmap addresses all of the following aspects of energy control systems:

- Electricity, oil, gas, and telecommunication sectors
- Legacy and next-generation systems
- Near-, mid-, and long-term activities
- Research and development (R&D), testing, best practices, training and education, policies, standards and protocols, information sharing, and implementation

A Strategic Framework

To achieve this vision, the Roadmap outlines a strategic framework featuring four main goals that represent the essential pillars of an effective protective strategy:

Measure and Assess Security Posture. Companies should thoroughly understand their current security posture to determine system vulnerabilities and the actions required to address them.

2015 *Within 10 years, the sector will help ensure that energy asset owners have the ability and commitment to perform fully automated security state monitoring of their control system networks with real-time remediation capability.*

Develop and Integrate Protective Measures. As security risks are identified, protective measures should be developed and applied to reduce system risks.

2015 *Security solutions will be developed for legacy systems, but options will be constrained by the limitations of existing equipment and configurations. Within 10 years, next-generation control system components and architectures that offer built-in, end-to-end security will replace many older legacy systems.*

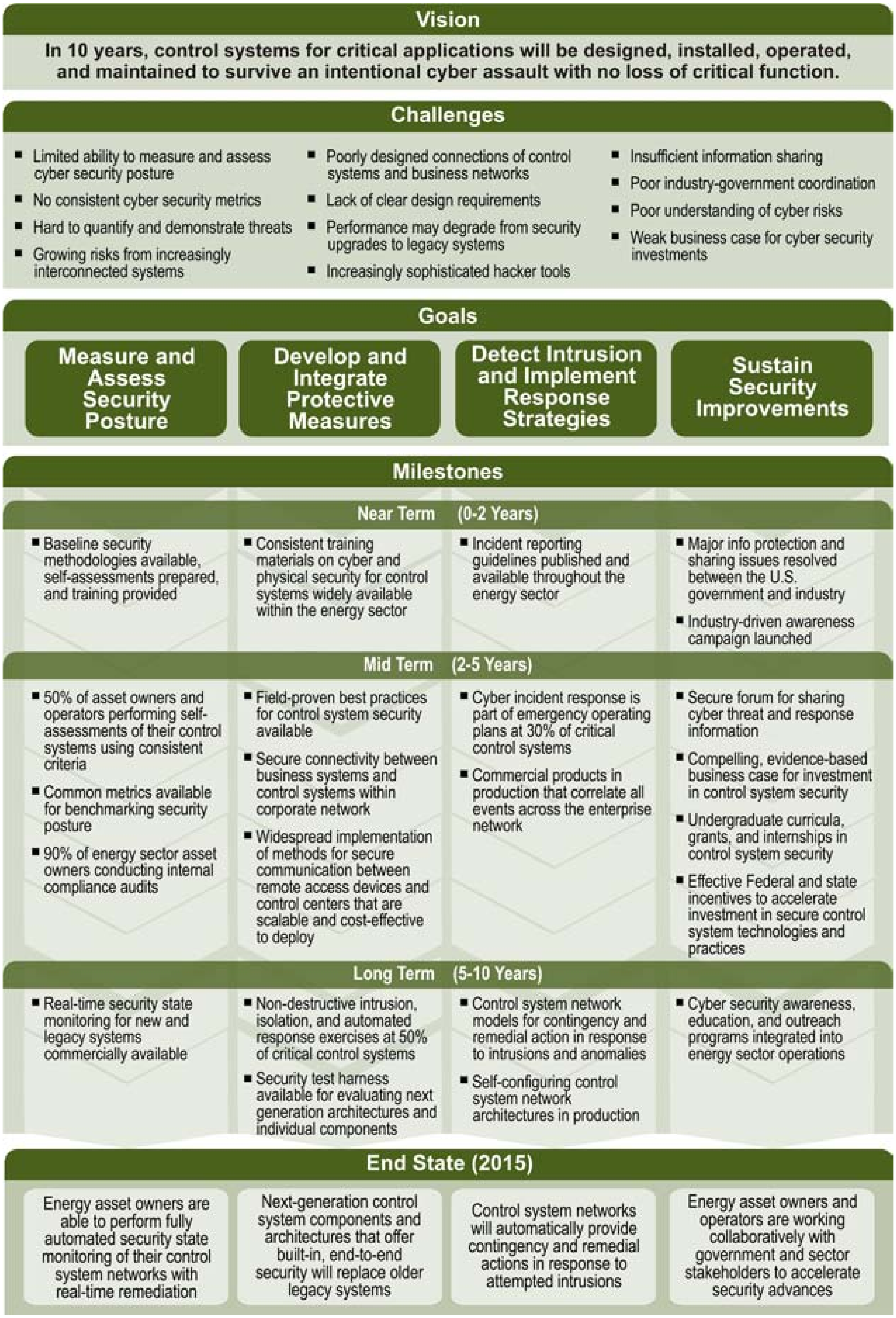
Detect Intrusion and Implement Response Strategies. Because few systems can be made totally impervious to cyber attacks all the time, companies should possess sophisticated intrusion detection systems and a sound response strategy.

2015 *Within 10 years, the energy sector will operate control system networks that automatically provide contingency and remedial actions in response to attempted intrusions into the control systems.*

Sustain Security Improvements. Maintaining aggressive and proactive control system security over the long term will require a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders.

2015 *Over the next 10 years, energy asset owners and operators are committed to working collaboratively with government and sector stakeholders to accelerate security advances.*

To achieve these four goals, the Roadmap contains key milestones tied to distinct time frames, as shown in Exhibit E.1. This structure introduces a coherent framework for mapping efforts currently underway in the public and private sectors and helping to launch new projects that advance the security of control systems.



Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.

Challenges

- Limited ability to measure and assess cyber security posture
- No consistent cyber security metrics
- Hard to quantify and demonstrate threats
- Growing risks from increasingly interconnected systems
- Poorly designed connections of control systems and business networks
- Lack of clear design requirements
- Performance may degrade from security upgrades to legacy systems
- Increasingly sophisticated hacker tools
- Insufficient information sharing
- Poor industry-government coordination
- Poor understanding of cyber risks
- Weak business case for cyber security investments

Goals

Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion and Implement Response Strategies	Sustain Security Improvements

Milestones

Near Term (0-2 Years)			
▪ Baseline security methodologies available, self-assessments prepared, and training provided	▪ Consistent training materials on cyber and physical security for control systems widely available within the energy sector	▪ Incident reporting guidelines published and available throughout the energy sector	▪ Major info protection and sharing issues resolved between the U.S. government and industry ▪ Industry-driven awareness campaign launched
Mid Term (2-5 Years)			
▪ 50% of asset owners and operators performing self-assessments of their control systems using consistent criteria ▪ Common metrics available for benchmarking security posture ▪ 90% of energy sector asset owners conducting internal compliance audits	▪ Field-proven best practices for control system security available ▪ Secure connectivity between business systems and control systems within corporate network ▪ Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy	▪ Cyber incident response is part of emergency operating plans at 30% of critical control systems ▪ Commercial products in production that correlate all events across the enterprise network	▪ Secure forum for sharing cyber threat and response information ▪ Compelling, evidence-based business case for investment in control system security ▪ Undergraduate curricula, grants, and internships in control system security ▪ Effective Federal and state incentives to accelerate investment in secure control system technologies and practices
Long Term (5-10 Years)			
▪ Real-time security state monitoring for new and legacy systems commercially available	▪ Non-destructive intrusion, isolation, and automated response exercises at 50% of critical control systems ▪ Security test harness available for evaluating next generation architectures and individual components	▪ Control system network models for contingency and remedial action in response to intrusions and anomalies ▪ Self-configuring control system network architectures in production	▪ Cyber security awareness, education, and outreach programs integrated into energy sector operations

End State (2015)

Energy asset owners are able to perform fully automated security state monitoring of their control system networks with real-time remediation	Next-generation control system components and architectures that offer built-in, end-to-end security will replace older legacy systems	Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions	Energy asset owners and operators are working collaboratively with government and sector stakeholders to accelerate security advances

Exhibit E.1 – Strategy for Securing Control Systems in the Energy Sector

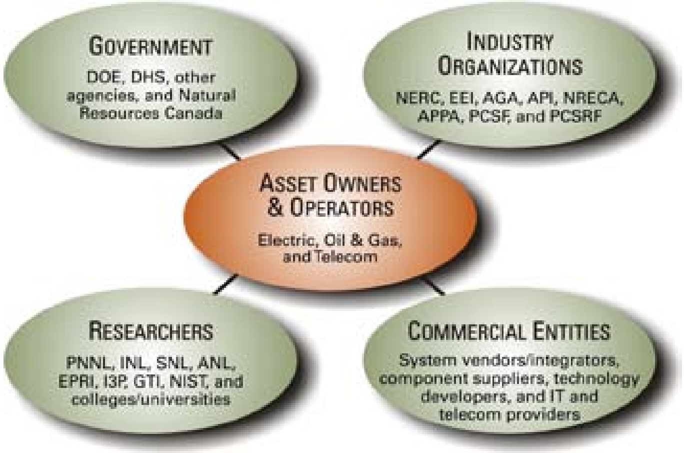
The Challenges Ahead

Achieving these milestones will be challenging. Many energy companies today have limited ability to measure and assess their cyber security posture. They lack consistent metrics or reliable tools for measuring their risks and vulnerabilities. Threats, when known, are often difficult to demonstrate and quantify in terms that are meaningful for decision makers. Control systems are becoming increasingly interconnected and often operate on open software platforms with known vulnerabilities and risks. Poorly designed connections between control systems and enterprise networks introduce further risks. Security upgrades for legacy systems may degrade performance due to the inherent limitations of existing equipment and architectures. New architectures with built-in, end-to-end security will take years to develop and even longer to deploy throughout the energy sector.

Cyber intrusion tools are becoming increasingly sophisticated. When attacks occur, information about the attack, consequences, and lessons learned are often not shared beyond the company. Outside the control system community, there is poor understanding of cyber security problems, their implications, and need for solutions. Coordination and information sharing between industry and government is also inadequate, primarily due to uncertainties in how information will be used, disseminated, and protected. Finally, even when risks, costs, and potential consequences are understood, it is difficult to make a strong business case for cyber security investment because attacks on control systems so far have not caused significant damage.

A Call to Action

Implementing this Roadmap will require the collective commitment of key stakeholders throughout the control systems value chain. Asset owners and operators bear the chief responsibility for ensuring that systems are secure, making the appropriate investments, and implementing protective measures. They are supported by the software and hardware vendors, contractors, IT and telecommunications service providers, and technology designers who develop and deliver system products and services. Researchers at government laboratories and universities also play a key role in exploring long-term solutions and developing tools to assist industry. Industry organizations and government agencies can provide the needed coordination, leadership, and investments to address important barriers and gaps. Each of these stakeholder groups brings distinct skills and capabilities for improving control system security.


Government
DOE, DHS, other agencies, and Natural Resources Canada
Industry Organizations
NERC, EEI, AGA, API, NRECA, APPA, PCSF, and PCSRF
Asset Owners & Operators
Electric, Oil & Gas, and Telecom
Researchers
PNNL, INL, SNL, ANL, EPRI, I3P, GTI, NIST, and colleges/universities
Commercial Entities
System vendors/integrators, component suppliers, technology developers, and IT and telecom providers

Roadmap implementation will entail three main steps.

1. Ongoing industry and government efforts to enhance control system security should be aligned with Roadmap goals, and current activities mapped to the milestones. This will help to highlight any gaps that are not being addressed and identify areas of overlap that would benefit from better coordination.
2. New projects should be initiated that address the critical needs identified in the Roadmap. Leaders in the energy sector and government must step forward to organize, plan, resource, and lead projects that provide solutions to known security flaws. Additional new projects may also be launched as gaps in existing activities are identified.
3. A mechanism should be developed to provide ongoing oversight and coordination for pursuing the Roadmap. Existing sector coordinating councils and control system forums are strong candidates for fulfilling this important function.

1. Introduction

Leaders from the energy sector and the government have recognized the need to plan, coordinate, and focus ongoing efforts to improve control system security. These leaders concur that an *actionable* path forward is required to address critical needs and gaps and to prepare the sector for a secure future. Their commitment helped to launch a public-private collaboration to develop a **Roadmap to Secure Control Systems in the Energy Sector**. The Roadmap focuses on the goals and priorities for improving the security of control systems in the electric, oil, and natural gas sectors over the next decade.

A distinctive feature of this collaboration is the active involvement and leadership of energy asset owners and operators in guiding both the scope and content of the Roadmap. The roadmapping effort was designed and directed by a 17-member steering group composed of asset owners and operators (electricity, oil, and gas), industry associations, government agencies from the United States and Canada, and national laboratories (Appendix B). The Roadmap content is based on expert input collected during a two-day workshop and subsequent reviews of results (see Appendix C). The Roadmap project was funded by the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability in collaboration with the U.S. Department of Homeland Security's Science and Technology Directorate – Homeland Security Advanced Research Projects Agency and Natural Resources Canada.

Roadmap Purpose

The purposes of this Roadmap are to

- Define a consensus-based strategy that articulates the cyber security needs of owners and operators in the energy sector.
- Produce a comprehensive plan for improving the security, reliability, and functionality of advanced energy control systems over the next 10 years.
- Guide efforts by industry, academia, and government and help clarify how each key stakeholder group can contribute to planning, developing, and disseminating security solutions.

The Roadmap builds on existing government and industry efforts to improve the security of control systems within the private sector by working through (1) the Electricity Sector Coordinating Council (coordinated by the North American Electric Reliability Council) and (2) the Oil and Natural Gas Sector Coordinating Council (coordinated by the American Petroleum Institute and the American Gas Association). The Roadmap is also intended to help coordinate and guide related control system security efforts, such as the Process Control Systems Forum (PCSF), Process Control Security Requirements Forum (PCSRF), Institute for Information Infrastructure Protection (I3P), International Electricity Infrastructure Assurance Forum (IEIA), Control System Security Center, and National SCADA Test Bed.

Roadmap Scope

The Roadmap is designed to address the full range of needs for protecting the cyber security of legacy and advanced control systems across the electric, oil, and natural gas sectors (including the supporting telecommunications infrastructure). For this Roadmap, control systems are defined as the facilities, systems, equipment, services, and diagnostics that provide the functional control capabilities necessary for the effective and reliable operation of the bulk energy system. While recognizing the importance of physical protection, this Roadmap focuses on the cyber security of control systems. It does not specifically address the security of other business or cyber systems except as they interface directly with energy control systems. The Roadmap covers goals, milestones, and needs over the near (0-2 years), mid (2-5 years), and long term (5-10 years). Security needs encompass research and development, new technologies, systems testing, training and education, best practices, standards and protocols, policies, information sharing, and outreach and implementation.

National Context

The U.S. Department of Energy (DOE) and U.S. Department of Homeland Security (DHS) are collaborating on ways to improve critical infrastructure protection within the energy sector. This Federal effort is part of a much larger government-wide initiative to strengthen and protect key sectors in partnership with all the major critical infrastructures in the United States. This Roadmap implements Federal policies that encourage Federal agencies to collaborate effectively with industry to create a national strategy that reflects the needs and expectations of both government and industry (see Exhibit 1.2). Because the U.S. electric grid and oil and gas pipeline networks are interconnected across North America, this Roadmap was developed in collaboration with Natural Resources Canada, a department of the Canadian Government that addresses the use of natural resources, including energy. The Roadmap priorities and recommendations help inform and strengthen government programs designed to improve protection of energy control systems in both countries.

Exhibit 1.2 – Federal Policy Guidance on Control Systems Security

- In the 1990's, the **President's Commission on Critical Infrastructure Protection** report, Critical Foundations, noted that "The widespread and increasing use of Supervisory Control and Data Acquisition (SCADA) systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means." **Presidential Decision Directive 63** acted on those findings and created the framework for government-industry partnerships to address physical and cyber security concerns in critical infrastructures, including energy.
- The **National Strategy for Homeland Security** and the **Homeland Security Act of 2002** responded to the attacks of 9/11 by creating the policy framework for addressing homeland security needs and restructuring government activities, which resulted in the creation of DHS.
- In early 2003, the **National Strategy to Secure Cyberspace** outlined priorities for protecting against cyber threats and the damage they can cause. It called for DHS and DOE to work in partnership with industry to ". . . develop best practices and new technology to increase security of DCS/SCADA, to determine the most critical DCS/SCADA-related sites, and to develop a prioritized plan for short-term cyber security improvements in those sites."
- In late 2003, the President issued **Homeland Security Presidential Decision 7 (HSPD-7)** — Critical Infrastructure Identification, Prioritization, and Protection to implement Federal policies. HSPD-7 outlined how government will coordinate for critical infrastructure protection and assigned DOE the task of working with the energy sector to improve physical and cyber security in conjunction with DHS. Responsibilities include collaborating with all government agencies and the private sector, facilitating vulnerability assessments of the sector, and encouraging risk management strategies to protect against and mitigate the effects of attacks. HSPD-7 also called for a national plan to implement critical infrastructure protection.
- The **National Infrastructure Protection Plan** has been under development since mid-2004. It establishes a partnership model for collaboration, consisting of a Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) for each sector. DOE is leading the government's effort to prepare the **Energy Sector-Specific Plan** and is working with the energy SCCs for Electricity and Oil and Natural Gas. This Plan will specifically address the cyber needs of control systems in the energy sector.

The Path Forward

The intent of this Roadmap is to provide a strategic framework for investment and action in industry and government. It outlines specific milestones that must be accomplished over the next 10 years and identifies the challenges and activities that should be addressed. While the Roadmap contains many actionable items, it is not intended to be prescriptive. However, plans are only useful if they translate into productive projects, activities, and products. Execution will require financial resources, intellectual capability, commitment, and leadership. Chapter 4, Roadmap Implementation, proposes a process endorsed by the Control Systems Roadmap Steering Group for turning ideas into actions.

2. The Control Systems Landscape

The United States and Canada are fortunate to have one of the most reliable and sophisticated energy infrastructures in the world. It provides the energy crucial to the economy and enables reliable operation of our critical infrastructures, including telecommunications, transportation, banking and finance, water supply, and public health. The need to safeguard our energy infrastructure against malicious attack is readily apparent. Any prolonged interruption in the flows of electricity, natural gas, or petroleum products could be devastating to the U.S. economy and the American people.

Over the past decade, market restructuring and new technologies have redefined how we use energy, who provides it, and where it flows. Modern utilities and energy companies have grown highly sophisticated in how they manage energy operations and allocate resources to optimize system assets. This level of sophistication would have been impossible without the reliability and responsiveness afforded by electronic control systems. As these control systems became increasingly integral to the operation of the U.S. energy sector, however, they evolved in ways that have made the sector increasingly vulnerable to malicious cyber attack.

Facilitating Energy Sector Operation

The electric power industry relies on control systems to manage and control the generation, transmission, and distribution of electric power. Similarly, the oil and gas industry uses control systems to help manage refining operations and remotely monitor and control pressures and flows in oil and gas pipelines. These systems allow operators to centrally monitor and control a large, often geographically distributed, network of sites and troubleshoot problems. Such centralized monitoring and control is indispensable for reliable and efficient management of large energy systems that may contain up to 150,000 real-time monitoring and control points.

Energy control systems include a hierarchy of networked physical and electronic sensing, monitoring, and control devices connected to a central supervisory station or control center. Control systems encompass supervisory control and data acquisition (SCADA) systems used to monitor vast, widely dispersed operations; distributed control systems (DCS) used for a single facility or small geographical area; and remote components such as remote terminal units (RTU) and programmable logic controllers (PLC) that monitor system data and initiate programmed control activities in response to input data and alerts. Exhibit 2.1 depicts a typical control system configuration for electricity.

What Are Control Systems?

Control systems are computer-based facilities, systems, and equipment used to remotely monitor and control sensitive processes and physical functions. These systems collect sensor measurements and operational data from the field, process and display this information, then relay control commands to local or remote equipment.

Evolution of Control Systems

Many control systems used today were designed for operability and reliability during an era when security received low priority. These systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and communications technology. Infiltrating these systems often required specific knowledge of individual system architectures and physical access to system components.

Under the pressures of continuous expansion, deregulation, and increased market competition, the energy sector shifted toward scalable control system architectures. Asset owners and operators gained immediate benefits by extending the connectivity of their control systems. They increasingly adopted commercial off-the-shelf (COTS) technologies that provided the higher levels of interoperability required among today's energy sector constituents. Standard operating systems, such as Windows or UNIX, are increasingly used in central supervisory stations, which are now typically connected to remote controllers via private networks

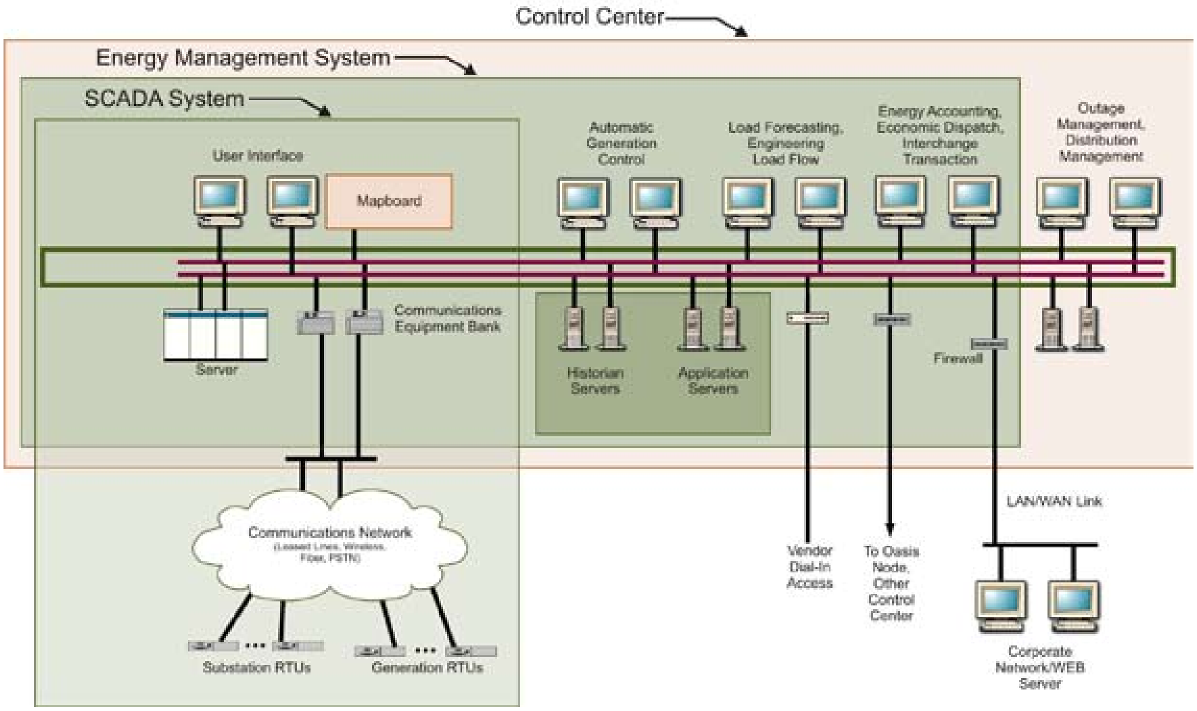

Control Center
Energy Management System
SCADA System
User Interface
Mapboard
Automatic Generation Control
Load Forecasting, Engineering Load Flow
Energy Accounting, Economic Dispatch, Interchange Transaction
Outage Management, Distribution Management
Communications Equipment Bank
Server
Historian Servers
Application Servers
Firewall
Communications Network
(Leased Lines, Wireless, Fiber, PSTN)
Substation RTUs
Generation RTUs
Vendor Dial-In Access
To Oasis Node, Other Control Center
LAN/WAN Link
Corporate Network/WEB Server

Exhibit 2.1 – Typical Control System Configuration for Electricity Source: Barnes and Johnson 2004

that are provided by telecommunications companies. Common telecommunications technologies, such as the Internet, public-switched telephone networks, or cable or wireless networks are also used.

Further integration of shared telecommunications technologies into normal business operations has spawned increased levels of interconnectivity among corporate networks, control systems, other asset owners, and the outside world. Continued expansion of the U.S. energy sector and the addition of new and often remote facilities have dictated still greater reliance on public telecommunications networks to monitor and communicate with those assets. Each auxiliary connection, however, provides a fresh point of entry for prospective cyber attacks and increases the burden on asset owners to manage the progressively complex paths of incoming and outgoing information. This elevated system accessibility exposes network assets to potential cyber infiltration and subsequent manipulation of sensitive operations in the energy sector.

The total assets of the North American energy sector represent an investment valued in the trillions of dollars (DHS 2005). The control systems used to monitor and control the electric grid and the oil and natural gas infrastructure represent a total investment worth an estimated $3 to $4 billion (Newton-Evans 2005b). The thousands of remote field devices represent an additional investment of $1.5 to $2.5 billion. Each year, the energy sector spends over $200 million for control systems, networks, equipment, and related components and at least that amount in personnel costs. Just over half of the 3,200 power utilities are estimated to have some form of SCADA system, while 85 percent of gas pipeline companies and 95 percent of oil pipeline companies use one or more SCADA systems to control their operations (Newton-Evans 2005b).

Escalating Threats and New Vulnerabilities

Potential adversaries have pursued progressively devious means to exploit the connectivity of the energy sector to infiltrate and then sabotage vulnerable control systems. Increasingly sophisticated cyber attack tools exploit flaws in COTS system components, telecommunication methods, and common operating systems found in modern energy systems. Some of these attack tools require little technical knowledge to use (see Exhibit 2.2) and can be found on the Internet, as can manufacturers' technical specifications for popular control system components and equipment. The ability of energy asset owners to discover and understand such emerging threats and system vulnerabilities is a prerequisite to developing effective countermeasures.

Disabled or compromised control systems could produce dire national consequences, particularly if instigated with insider knowledge or timed in tandem with physical attacks. Although prevailing expert opinion holds that an external cyber attack alone is unlikely to cause devastating harm to the North American energy system, some security experts claim it is now possible for skilled computer hackers to use the Internet to disable large portions of the grid for brief periods and smaller portions for extended periods of time (Dubiel et al. 2002). Direct impacts of such outages would be compounded by secondary damage to other critical infrastructure components that rely on the energy sector. Analysts estimate that routine power outages alone already cost the U.S. economy $104 billion to $164 billion per year (EPRI 2001). Indeed, a major security breach of energy sector control systems could gravely affect U.S. citizens, businesses, and government.

Cases In Point: Control System Attacks

- **Unsuspected code hidden in transferred product** *(USSR, 1982)*
  While the following cannot be confirmed, it has been reported that during the Cold War the CIA inserted malicious code into control system software leaked to the Soviet Union. The software, which controlled pumps, turbines, and valves on a Soviet gas pipeline, was programmed to malfunction after a set interval. The malfunction caused the control system to reset pump speeds and valve settings to produce pressures beyond the failure ratings of pipeline joints and welds, eventually causing an enormous explosion.
- **Hacker exploits cross-sector interdependence** *(Massachusetts, USA, 1997)*
  A teenager hacked into and remotely disabled part of the public switching network, disrupting phone service for local residents and the fire department and causing a malfunction at a nearby airport.
- **Insider hacks into sewage treatment plant** *(Australia, 2001)*
  A former employee of the software developer hacked into the SCADA system that controlled a Queensland sewage treatment plant, causing a large sewage discharge over a sustained period. He was caught and sentenced to two years in prison in 2001.
- **Worm exploits interconnected business and operations networks, standard O/S** *(Ohio, USA, 2003)*
  The SQL Slammer worm infiltrated the operations network of the Davis-Besse nuclear power plant via a high-speed connection from an unsecured contractor's network (after the corporate firewall had previously blocked the worm). After migrating from the business network to the operations network, the worm disabled the panel used to monitor the plant's most crucial safety indicators for about five hours and caused the plant's process computer to fail; recovery for the latter took nearly six hours. Luckily, the plant was off-line at the time.

Source: GAO 2004, Reed 2005

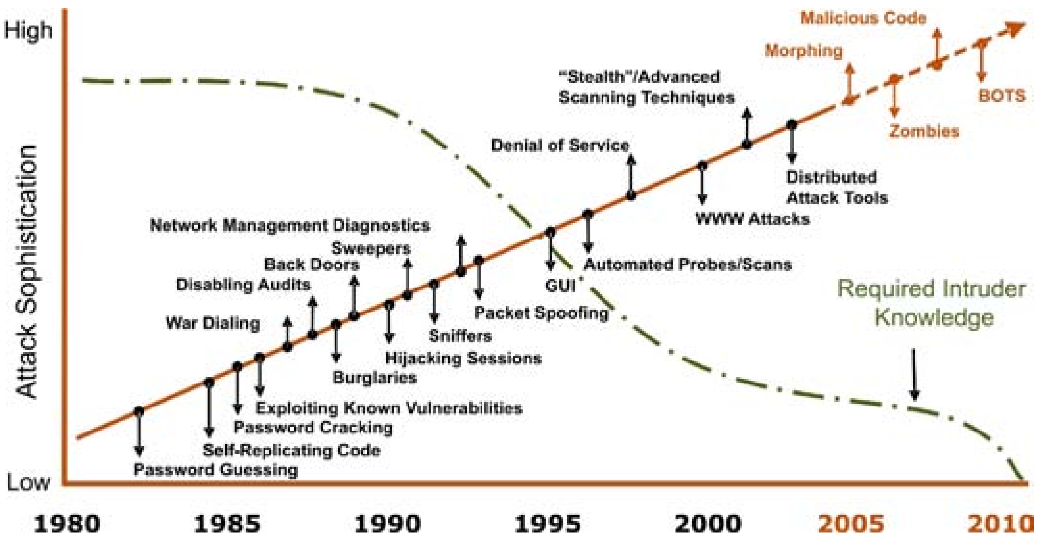


Exhibit 2.2 – Sophisticated Cyber Attacks Require Progressively Little Expertise

Source: Allen et al. 2000

While the performance and reliability of energy control systems is quite strong, security is often weak. As operating practices have evolved to allow real-time energy production, generation, and delivery over a vast service area, it has become harder to protect control

systems from cyber risks. Exhibit 2.3 summarizes some of the most serious security issues inherent in current energy control systems. Increasing connectivity, the proliferation of access points, escalating system complexity, greater interdependencies, increased outsourcing and reliance on foreign products, market restructuring, and wider use of common operating systems and platforms have all contributed to heightened security risks. Furthermore, the high level of performance afforded by electronic controls is causing energy systems to operate closer to their limits, increasing concerns that a cyber breach could produce a loss of critical function.

Exhibit 2.3 – Current Issues in Protecting Critical Control Systems

Increased Connectivity

Today's control systems are increasingly connected to a company's enterprise system, rely on common operating platforms, and are accessible through the Internet. While these changes improve operability, they have also created serious vulnerabilities because there has not been a concurrent improvement in security control systems features.

Interdependencies

The high degree of interdependency among our infrastructure sectors means failures in one sector can propagate into others. Government experts postulate that terrorists hope to cause widespread economic damage by attacking cyber systems to produce cascading impacts on the physical systems they control.

Complexity

The demand for real-time control has increased system complexity: access to control systems is being granted to more users, business and control systems are interconnected, and the degree of interdependence among infrastructures is increased. Dramatic differences in the training and concerns of those in charge of information technology (IT) systems and those responsible for control system operations have led to challenges in coordinating network security between these two key groups.

Legacy Systems

Although older legacy systems may operate in more independent modes, they tend to have inadequate password policies and security administration, no data protection mechanisms, and information links that are prone to snooping, interruption, and interception. These insecure legacy SCADA systems have very long service lives, and will remain vulnerable for years to come if the problems are not mitigated.

Market Restructuring

Restructuring has led to an increased volume of transactions on our national energy systems and narrower operating margins for energy providers. These trends have placed a premium on the efficient use of existing capacity, so the speed and number of interconnections to shift supply from one location to another have increased significantly. Distributed dynamic control has increased the number of entities involved in the power life cycle and increased connectivity with outside vendors, customers, and business partners—introducing greater vulnerability into the network.

System Accessibility

Even limited use of the Internet exposes SCADA systems to all of the inherent vulnerabilities of interconnected computer networks (e.g., viruses, worms, hackers, and terrorists). In addition, control channels use wireless or leased lines that pass through commercial telecommunications facilities, providing minimal protection against forgery of data or control messages. Legacy systems often allow "back-door" access via connections to third-party contractors and maintenance staff.

Offshore Reliance

There are no feasible alternatives to the use of commercial off-the-shelf (COTS) products in these information systems. Most software, hardware, and SCADA system manufacturers are under foreign ownership or are manufactured in countries whose interests do not always align with those of the United States.

Information Availability

Manuals and even training videos on SCADA systems are publicly available, and many hacker tools can now be downloaded from the Internet and applied with limited system knowledge. Attackers do not have to be experts in SCADA operations.

The energy sector represents a tempting target for cyber attack. Although many attacks go unreported, energy and power control systems have been the target of a number of attempted attacks in recent years. As shown in Exhibit 2.4, the somewhat limited data collected in the Industrial Security Incident Database suggest that the energy sector is a common target for control system attacks.

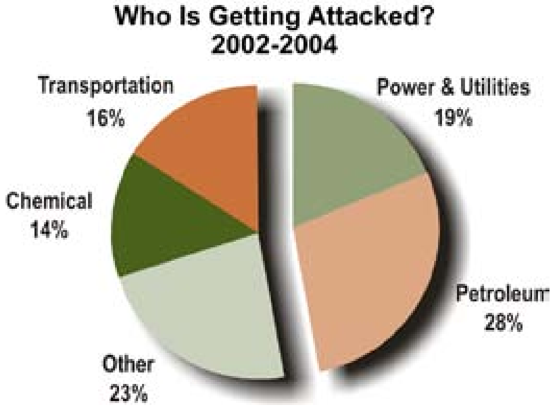


Exhibit 2.4 – Attacks on Industrial Control Systems

Source: Industrial Security Incident Database (Byres 2005)

Many owners and operators understand the potential consequences of control system failure and have taken steps over the past decade to enhance cyber security. Government is also keenly aware of the need to stimulate security improvements in a competitive energy market that inhibits investment in cyber security. Utilities use sophisticated risk management strategies that consider threats, vulnerabilities, and consequences to determine the appropriate level of security investment for a given risk profile. While most owners and operators view cyber security as a logical and necessary part of their protective profile, investments typically fall short of critical needs.

Owners and operators have begun to work collaboratively with government agencies, other sectors, universities, and national laboratories, to coordinate efforts to address control system security concerns. Exhibit 2.5 summarizes diverse efforts that have been initiated to improve control system security in the energy sector. However, no overarching framework exists to ensure that activities are aligned with clear sector goals or that these efforts address the most critical priorities while avoiding unnecessary overlaps.

Future Trends and Drivers

The cyber environment is constantly changing, challenging the ability of owners and operators to combat new threats. The security posture of the North American energy infrastructure will be increasingly challenged as technologies, business practices, and market trends continue to reshape the security landscape (see Exhibit 2.6). Attending to today's security needs without consideration of the changes ahead could find us unprepared to address tomorrow's vulnerabilities. For example, emerging changes in the structure of energy markets over the next decade, driven by new demand patterns, distributed generation, and alternative energy sources, will require bulk electric and oil and gas asset owners to adapt to a new form of connectivity with their systems. New business practices and operating requirements will also shape control system security practices. Continued expansion of networks to encompass an even larger number of remote assets may require a greater reliance on shared telecommunications technologies (especially wireless

How Can Cyber Attacks Affect Energy Systems?

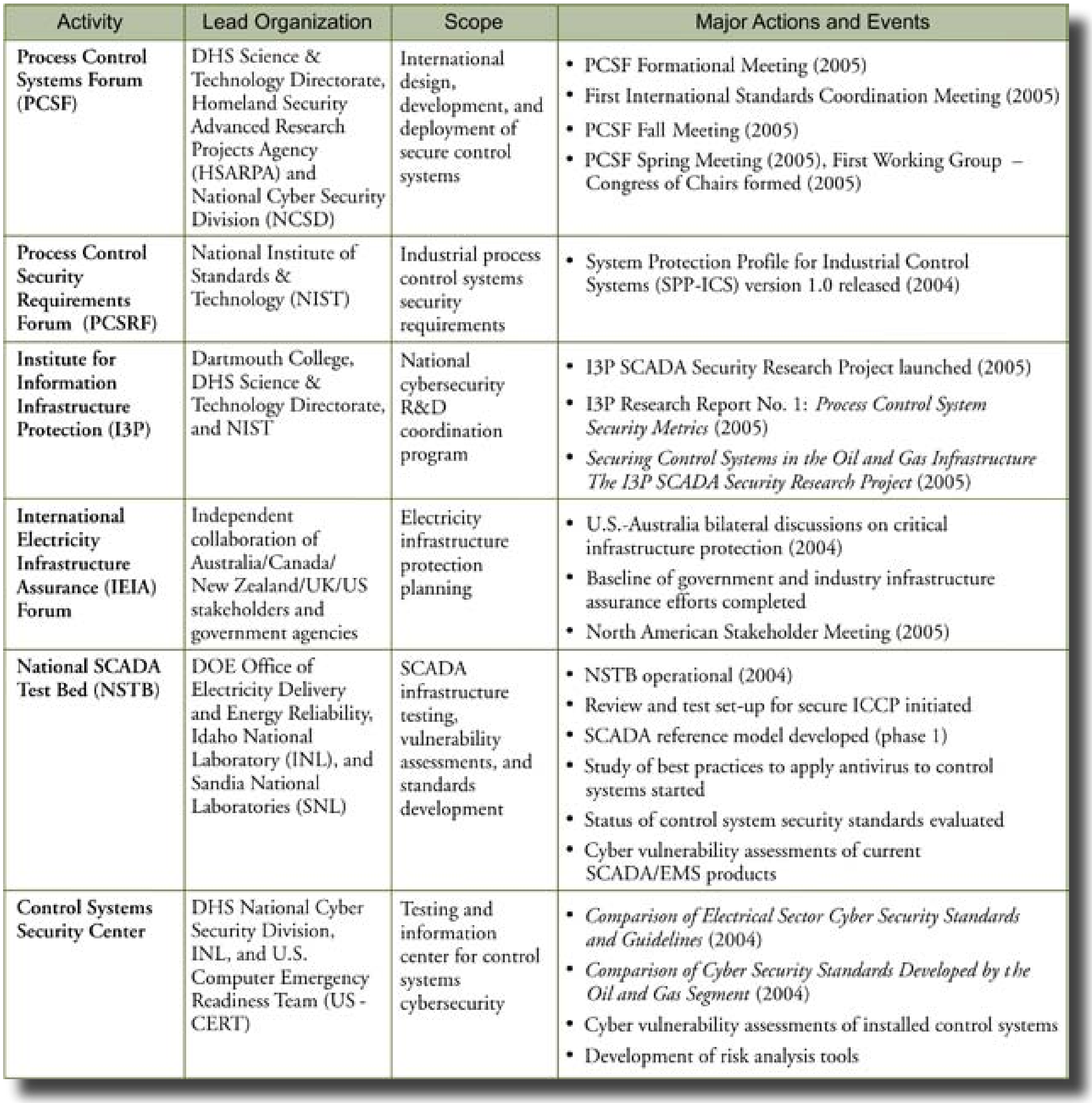
Cyber attacks can affect energy operations in a variety of ways, some with potentially devastating repercussions. Attacks can potentially do the following:

- Disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying network availability to control system operators.
- Send false information to control system operators, either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
- Modify the control system software, producing unpredictable results.
- Interfere with the operation of safety systems.
- Make unauthorized changes to programmed instructions in programmable logic controllers (PLCs), remote terminal units (RTUs), or distributed control systems (DCS) controllers; change alarm thresholds; order premature shutdown of processes (such as prematurely shutting down transmission lines); or even disable control equipment.

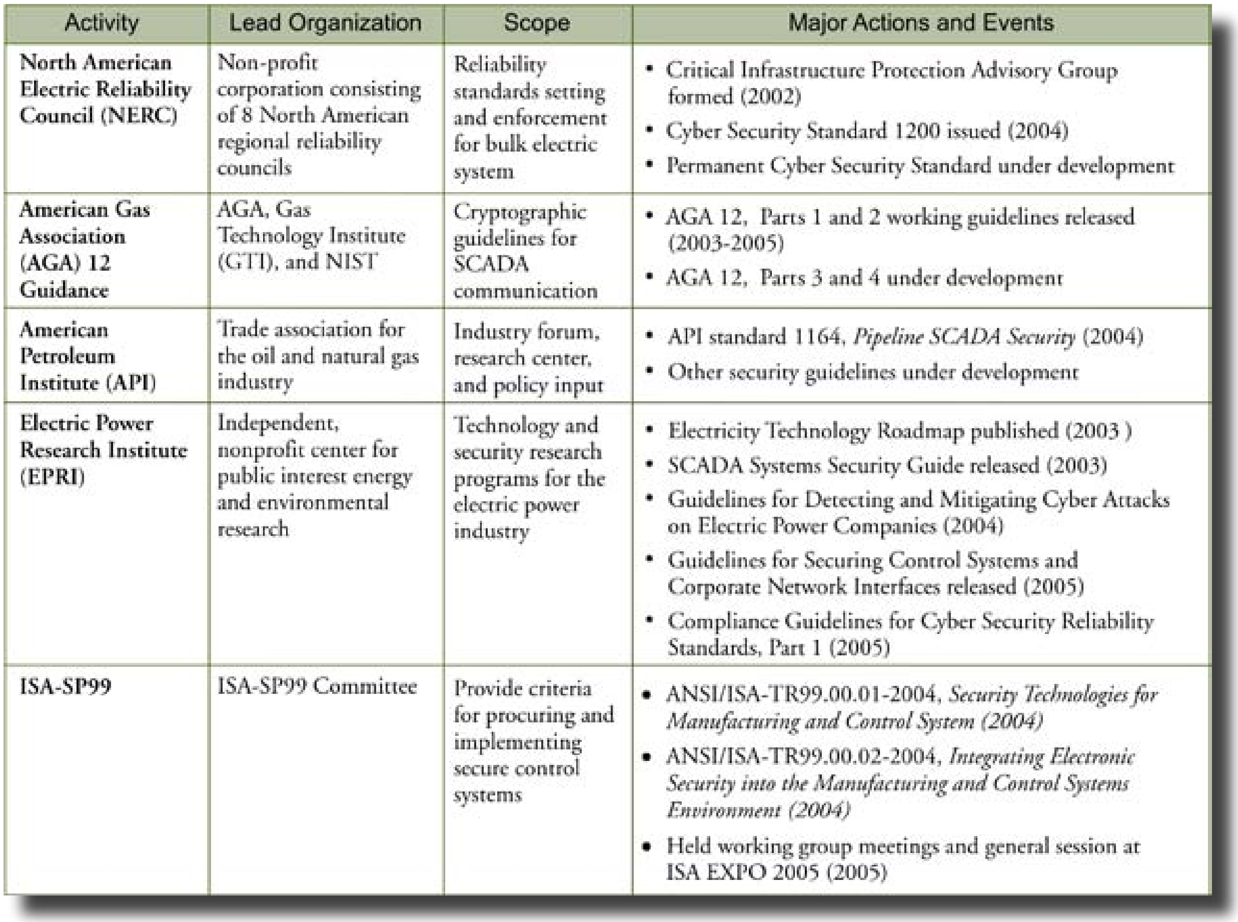
Source: GAO 2004

and standard internet protocols) to quickly receive and transmit necessary data from remote units. Each new source and transmission link not only creates another new entry point for cyber attacks, but also tasks operators with managing dramatic increases in system complexity. The challenges of keeping pace with emerging risks in today's dynamic threat and operating environments are far too large for a disparate, piecemeal approach to be successful. However, by pooling their collective knowledge and resources, energy sector stakeholders can effectively create a responsive, strong line of defense against security threats to their control systems. Novel control system architecture designs can provide compulsory segmentation between internal company networks, control systems, and external connections (e.g., the Internet)—a separation lacking in most current systems. Innovative architectures can function as a high-level deterrent promoting defense-in-depth against unwanted and potentially harmful cyber intrusion. Sophisticated tools and practices can be developed and incorporated into legacy and new control systems to quickly and continuously identify, isolate, and anticipate threats. Ongoing expansion and modernization of the energy sector creates opportunities to bring such systems online.

Exhibit 2.5 – Summary of Selected Control System Security Efforts



Activity	Lead Organization	Scope	Major Actions and Events
Process Control Systems Forum (PCSF)	DHS Science & Technology Directorate, Homeland Security Advanced Research Projects Agency (HSARPA) and National Cyber Security Division (NCSD)	International design, development, and deployment of secure control systems	• PCSF Formational Meeting (2005) • First International Standards Coordination Meeting (2005) • PCSF Fall Meeting (2005) • PCSF Spring Meeting (2005), First Working Group – Congress of Chairs formed (2005)
Process Control Security Requirements Forum (PCSRF)	National Institute of Standards & Technology (NIST)	Industrial process control systems security requirements	• System Protection Profile for Industrial Control Systems (SPP-ICS) version 1.0 released (2004)
Institute for Information Infrastructure Protection (I3P)	Dartmouth College, DHS Science & Technology Directorate, and NIST	National cybersecurity R&D coordination program	• I3P SCADA Security Research Project launched (2005) • I3P Research Report No. 1: *Process Control System Security Metrics* (2005) • *Securing Control Systems in the Oil and Gas Infrastructure The I3P SCADA Security Research Project* (2005)
International Electricity Infrastructure Assurance (IEIA) Forum	Independent collaboration of Australia/Canada/ New Zealand/UK/US stakeholders and government agencies	Electricity infrastructure protection planning	• U.S.-Australia bilateral discussions on critical infrastructure protection (2004) • Baseline of government and industry infrastructure assurance efforts completed • North American Stakeholder Meeting (2005)
National SCADA Test Bed (NSTB)	DOE Office of Electricity Delivery and Energy Reliability, Idaho National Laboratory (INL), and Sandia National Laboratories (SNL)	SCADA infrastructure testing, vulnerability assessments, and standards development	• NSTB operational (2004) • Review and test set-up for secure ICCP initiated • SCADA reference model developed (phase 1) • Study of best practices to apply antivirus to control systems started • Status of control system security standards evaluated • Cyber vulnerability assessments of current SCADA/EMS products
Control Systems Security Center	DHS National Cyber Security Division, INL, and U.S. Computer Emergency Readiness Team (US - CERT)	Testing and information center for control systems cybersecurity	• *Comparison of Electrical Sector Cyber Security Standards and Guidelines* (2004) • *Comparison of Cyber Security Standards Developed by the Oil and Gas Segment* (2004) • Cyber vulnerability assessments of installed control systems • Development of risk analysis tools



Activity	Lead Organization	Scope	Major Actions and Events
North American Electric Reliability Council (NERC)	Non-profit corporation consisting of 8 North American regional reliability councils	Reliability standards setting and enforcement for bulk electric system	• Critical Infrastructure Protection Advisory Group formed (2002) • Cyber Security Standard 1200 issued (2004) • Permanent Cyber Security Standard under development
American Gas Association (AGA) 12 Guidance	AGA, Gas Technology Institute (GTI), and NIST	Cryptographic guidelines for SCADA communication	• AGA 12, Parts 1 and 2 working guidelines released (2003-2005) • AGA 12, Parts 3 and 4 under development
American Petroleum Institute (API)	Trade association for the oil and natural gas industry	Industry forum, research center, and policy input	• API standard 1164, *Pipeline SCADA Security* (2004) • Other security guidelines under development
Electric Power Research Institute (EPRI)	Independent, nonprofit center for public interest energy and environmental research	Technology and security research programs for the electric power industry	• Electricity Technology Roadmap published (2003) • SCADA Systems Security Guide released (2003) • Guidelines for Detecting and Mitigating Cyber Attacks on Electric Power Companies (2004) • Guidelines for Securing Control Systems and Corporate Network Interfaces released (2005) • Compliance Guidelines for Cyber Security Reliability Standards, Part 1 (2005)
ISA-SP99	ISA-SP99 Committee	Provide criteria for procuring and implementing secure control systems	• ANSI/ISA-TR99.00.01-2004, *Security Technologies for Manufacturing and Control System (2004)* • ANSI/ISA-TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control Systems Environment (2004)* • Held working group meetings and general session at ISA EXPO 2005 (2005)

Exhibit 2.6 – Trends and Drivers Affecting Future Control System Security

Business Practices

- Growing corporate responsibility for control system security
- Rising integration of security concerns into standard business practices
- Aging workforce, staff turnover, and reduction in experienced manpower
- Increasing trend toward product and technology outsourcing
- Growing reliance on commercial off-the-shelf technologies

Energy Markets and Operations

- Continuing increase in interconnection of business and control system networks
- Further growth in dynamic, market-based system control
- Increasing need for real-time business information
- Increasing use of distributed and alternative energy sources
- Development of the next-generation electric grid

Technology and Telecommunications

- Increasing convergence of information technology (IT) and telecommunications functions
- Greater system interconnectivity
- Increasing use of Internet Protocol (IP)-based communications
- Increasing reliance on wireless communications
- Increasing use of distributed intelligent devices and controls
- Increasing need for remote access
- Increasing adoption of authentication and encryption techniques
- Increasingly sophisticated detection and alarming mechanisms

Threats

- Increasingly advanced cyber attack capabilities; more sophisticated tools
- Escalating terrorist and nation-state (outsider) threats

3. A Framework for Securing Control Systems

Protecting control systems in the energy sector is a formidable challenge. It requires a comprehensive approach that addresses the urgent security concerns of today's systems while preparing for the needs of tomorrow. Energy asset owners and operators must understand and manage cyber risks, secure their legacy systems, apply security tools and practices, and consider new control system architectures – all within a competitive business environment. Government has a large stake in the process because nearly all critical infrastructures depend on a reliable flow of energy, and any sustained disruption could endanger public health and safety. However, cyber security must compete with other investment priorities and many executives find it difficult to justify security expenditures without a strong business case. A coordinated national strategy is needed to articulate the essential goals for improving control system security and to align and integrate the efforts of industry and government to achieve those goals.

Vision

Through this roadmap process, the energy sector has developed the following bold vision for control system security based on sound risk management principles:

> **In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.**

The vision's emphasis on *critical* applications is noteworthy. Asset owners and operators have long recognized that it is neither practical nor feasible to protect *all* of their energy assets from malicious attack. The North American energy infrastructure encompasses an enormous network of electric transmission lines, generating stations, crude and petroleum product pipelines, refineries, interstate and intrastate gas pipelines, and control units that represent a multi-trillion dollar investment made over the past century (DHS 2005). Many of these assets are *not* threat targets, some are not vulnerable, and some would create no serious consequences if disabled. Moreover, the U.S. electric grid and pipeline networks were designed to withstand considerable loss of capability without loss of critical function. By focusing on control systems for *critical* applications to prevent loss of crucial functions, the energy sector can develop strategic goals and milestones that effectively protect the public, customers, corporate assets, and shareholders.

Vision Terms Defined

Critical Applications: Control systems for critical applications include components and systems that are indispensable to the safe and reliable operation of the energy system. Criticality of an application is determined by the severity of consequences resulting from its failure or compromise. Such components may include controls for operating circuit breakers or managing pipeline pressure.

Intentional Cyber Assault: An intentional cyber assault is a deliberate attempt to destroy, incapacitate, or exploit all or part of a control system network with the intent to cause economic damage, casualties, public harm, or loss of public confidence. The assault may target a variety of components within the control system network and may be launched by terrorist groups, disgruntled insiders, hackers, or nation states.

Loss of Critical Function: A critical function of an energy system is any operation, task, or service that, were it to fail or be compromised, would produce major safety, health, operational, or economic consequences.

Control System Security Goals

Achieving secure control systems for critical applications within a decade is a daunting challenge, but the stakes are high. To achieve this vision, stakeholders must pursue an aggressive timetable of milestones and deliverables. Fixing current security problems is not enough. New cyber threats are emerging at an accelerating pace, requiring an integrated strategy for securing systems into the future.

To meet existing and emerging threats, the sector needs a strategic framework that recognizes the need for measuring and assessing security, integrating protective measures, detecting and responding to intrusions, and continuously improving systems to sustain security as new threats surface. A framework emphasizing these four strategic areas, as shown in Exhibit 3.1 and described below, will provide a sound foundation for achieving the vision:

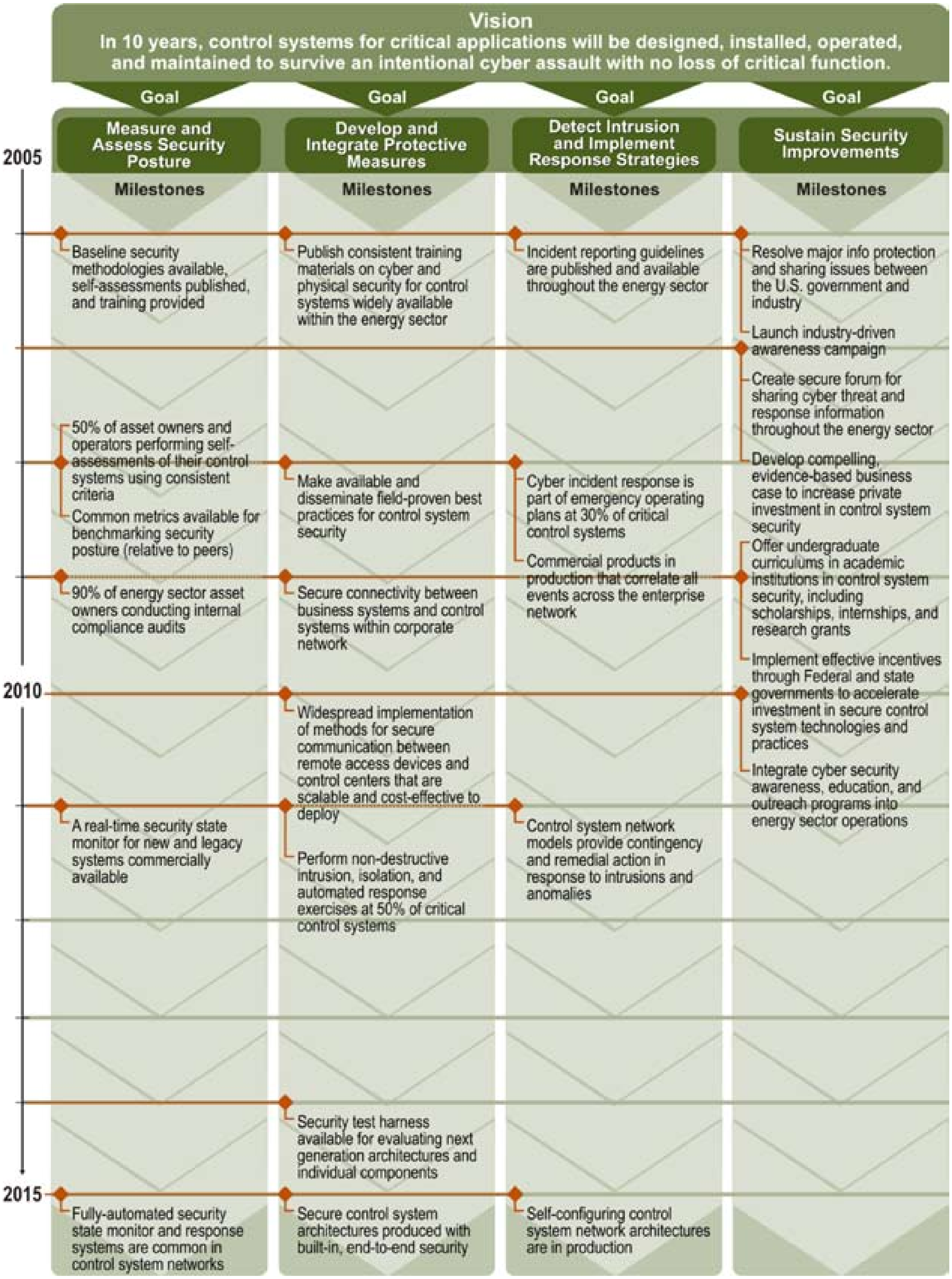
- **Measure and Assess Security Posture**. Companies should have a thorough understanding of their current security posture to determine where control system vulnerabilities exist and what actions may be required to address them. Within 10 years, the sector will help ensure that energy asset owners have the ability and commitment to perform fully-automated security state monitoring of their control system networks with real-time remediation.
- **Develop and Integrate Protective Measures**. As security problems are identified or anticipated, protective measures will be developed and applied to reduce system vulnerabilities, system threats, and their consequences. Appropriate security solutions will be devised for legacy systems, but will be constrained by the inherent limitations of existing equipment and configurations. As legacy systems age over the next decade, they will be replaced or upgraded with next-generation control system components and architectures that offer built-in, end-to-end security.
- **Detect Intrusion and Implement Response Strategies**. Cyber intrusion tools are becoming more sophisticated, and any system can become vulnerable to emerging threats. Within 10 years, the energy sector will be operating networks that automatically provide contingency and remedial actions in response to attempted intrusions.
- **Sustain Security Improvements**. Maintaining aggressive and proactive control system security over the long term will require a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders. Over the next 10 years, energy asset owners and operators are committed to working collaboratively both within the sector and with government to remove barriers to progress and create policies that will accelerate security advances.

These goals provide a logical framework for organizing the collective efforts of industry, government, and other key stakeholders to achieve the vision. To be successful, however, specific milestones and deliverables must be accomplished in the 2005-2015 period. Projects, activities, and initiatives that result from this Roadmap should be tied to the milestones shown in Exhibit 3.1.

Energy Sector Perspectives

The strategic framework described above is useful for defining cyber security *solutions*. However, stakeholders tend to view security issues in terms of their particular control system *needs*. A utility, for example, might focus on fixing vulnerabilities in their legacy system. Researchers might focus on developing advanced components with built-in security. Software vendors might focus on developing risk assessment tools for owners and operators. Four fundamental needs–legacy systems, new control systems, security tools and practices, and understanding strategic risks–drive priorities within the control systems community. These needs, outlined in Exhibit 3.2, are captured in technology product and process improvement cycles, as explained below.

Technology needs for control systems include: 1) near-term needs for installed **legacy systems** and 2) **new control system architectures** for next-generation systems. Legacy systems represent a multi-billion dollar



Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.

Goal

Measure and Assess Security Posture

Milestones

- Baseline security methodologies available, self-assessments published, and training provided
- 50% of asset owners and operators performing self-assessments of their control systems using consistent criteria
- Common metrics available for benchmarking security posture (relative to peers)
- 90% of energy sector asset owners conducting internal compliance audits
- A real-time security state monitor for new and legacy systems commercially available
- Fully-automated security state monitor and response systems are common in control system networks

Goal

Develop and Integrate Protective Measures

Milestones

- Publish consistent training materials on cyber and physical security for control systems widely available within the energy sector
- Make available and disseminate field-proven best practices for control system security
- Secure connectivity between business systems and control systems within corporate network
- Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy
- Perform non-destructive intrusion, isolation, and automated response exercises at 50% of critical control systems
- Security test harness available for evaluating next generation architectures and individual components
- Secure control system architectures produced with built-in, end-to-end security

Goal

Detect Intrusion and Implement Response Strategies

Milestones

- Incident reporting guidelines are published and available throughout the energy sector
- Cyber incident response is part of emergency operating plans at 30% of critical control systems
- Commercial products in production that correlate all events across the enterprise network
- Control system network models provide contingency and remedial action in response to intrusions and anomalies
- Self-configuring control system network architectures are in production

Goal

Sustain Security Improvements

Milestones

- Resolve major info protection and sharing issues between the U.S. government and industry
- Launch industry-driven awareness campaign
- Create secure forum for sharing cyber threat and response information throughout the energy sector
- Develop compelling, evidence-based business case to increase private investment in control system security
- Offer undergraduate curriculums in academic institutions in control system security, including scholarships, internships, and research grants
- Implement effective incentives through Federal and state governments to accelerate investment in secure control system technologies and practices
- Integrate cyber security awareness, education, and outreach programs into energy sector operations

Exhibit 3.1 – Strategic Framework for Control Systems

investment in control equipment, remote devices, software and operating systems, and communication links. Clearly, they are far too costly to replace before the end of their useful operating life—often about 15 years. As system vulnerabilities are discovered and new threats emerge, researchers and vendors can develop new technologies and design better system architectures that address these problems and even anticipate new ones. Eventually, however, the next-generation systems of today will become the legacy systems of tomorrow. This *technology improvement cycle* requires that new hardware, software, and system designs undergo continuous development to address new threats and security concerns, simultaneously maintaining as high a degree of compatibility as possible between the legacy upgrades and new generation designs.

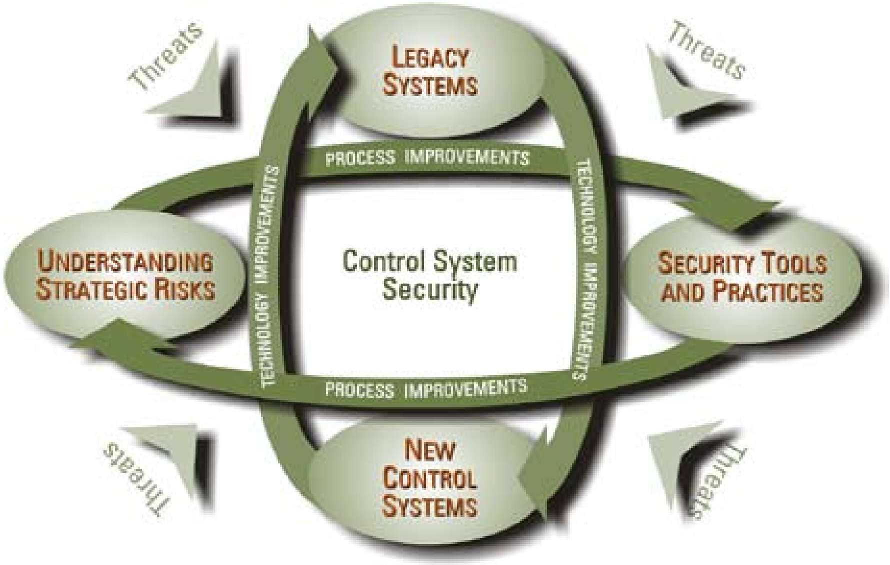


Exhibit 3.2 – Process and Technology Improvement Cycles Highlight Basic Needs of Stakeholders

Process needs of operators include: 1) **identifying and understanding security risks**, and 2) **implementing security tools and practices**. All operators, independent of the systems they operate, need to understand the emerging threat environment, determine control system risks, and develop strategies for mitigating vulnerability. Similarly, operators need security tools and practices to address risks to both new and old systems, though the protective responses may differ. All systems will benefit from the use of best practices, security procedures for operators and contractors, secure communications protocols, intrusion detection tools, and security event management.

Control system experts identified over 170 key security requirements based on these four basic needs at the July 2005 workshop (Energetics 2005). The key technology barriers and challenges as well as potential solutions that emerged from this workshop are summarized in Appendix A. This valuable groundwork provided specific content for building the Control Systems Roadmap in the strategic framework defined earlier.

Strategies for Securing Control Systems

Strategies for accomplishing the four goals presented in Exhibit 3.1 are summarized in Exhibits 3.3 through 3.6. Each goal presents distinct challenges that must be overcome, requires completion of deliverables on an established timetable, and prompts a set of priority solutions. These solutions represent examples of potential projects, initiatives, and activities that were identified by control systems experts (see Appendix A) and are not intended to be exhaustive.

Goal: Measure and Assess Security Posture

Understanding the security posture of control systems and all of their components and links allows companies to determine appropriate corrective actions. To gain this understanding, reliable and widely accepted security metrics are needed, as well as tools, techniques, and methodologies for measuring and assessing both static and real-time security states. Because of the unique configurations of many control systems, owners need the tools to conduct self-assessments. The industry eventually needs automated security state monitoring tools that trigger corrective actions within the control system, while allowing operators to override them, if necessary. An overview of the challenges, milestones, and project priorities for measuring and assessing security posture is shown in Exhibit 3.3.

Challenges

Energy companies have limited ability to measure and assess their cyber security posture. There are no consistent metrics or reliable tools that allow companies to measure security risk and vulnerabilities. Poor measurement capabilities limit the ability of companies to accurately assess their security state and determine feasible solutions. Threats, when known, are often hard to demonstrate and quantify in terms that are meaningful for decision makers. Risk factors for control systems are not widely understood by managers and technologists, making it difficult to initiate needed improvements.

Priorities

Near-term needs include collaborative development of a risk matrix that reflects consensus on how to frame and define critical challenges and match them with appropriate solutions. This should be accompanied by mid-term development of risk assessment tools that assess vulnerabilities, help prioritize protective measures, and justify the costs of remediation. Support is also needed for near-term development of activities and tools that will enable owners and operators to perform self assessments of their security postures. In the mid term, clear and consistent metrics are needed for control systems, and mandatory baseline security requirements should be established. In the long term, the sector needs to develop systems that automate security-state monitoring and remediation, similar to the way in which the energy sector currently automates and manages energy operations.

Goal: Develop and Integrate Protective Measures

As security problems are identified, known protective measures can be applied and new solutions developed to meet emerging needs. For legacy systems, protective measures often include the application of proven best practices and security tools, procedures and patches for fixing known security flaws, training programs for staff at all levels, and retrofit security technologies that do not degrade system performance. Communication between remote devices and control centers and between business systems and control systems is a common security concern that requires secure links, device-to-device authentication, and effective protocols. However, the most comprehensive security improvements are realized with the development and adoption of next-generation control system architectures that incorporate advanced plug-and-play components, which are inherently secure and offer enhanced functionality and performance. These systems can provide "defense in depth" with built-in, end-to-end security. An overview of the challenges, milestones, and project priorities for integrating protective measures are shown in Exhibit 3.4.

Challenges

Today's control systems are increasingly interconnected and operate on open software platforms that increase vulnerabilities and risks. Poorly designed connections between control systems and enterprise networks also increase risks. Security improvements for legacy systems are limited by the existing equipment and architectures that may not be able to accept security upgrades without degrading performance. New architectures must be designed to address potential threats that have not yet surfaced and to accommodate the exceptionally large number of nodes and access points that increase security concerns.

Priorities

Because each control system is unique, the sector must identify, publish, and disseminate best practices, including ones for securing connectivity with business networks and for providing physical and cyber security for remote facilities. Communications can be improved by developing innovative encryption solutions in the near term and by developing high-performance, secure communications for legacy systems in the mid term. Next-generation control systems will be developed in the long term, using a security test harness to help evaluate potential solutions. True plug-and-play components that operate with any control

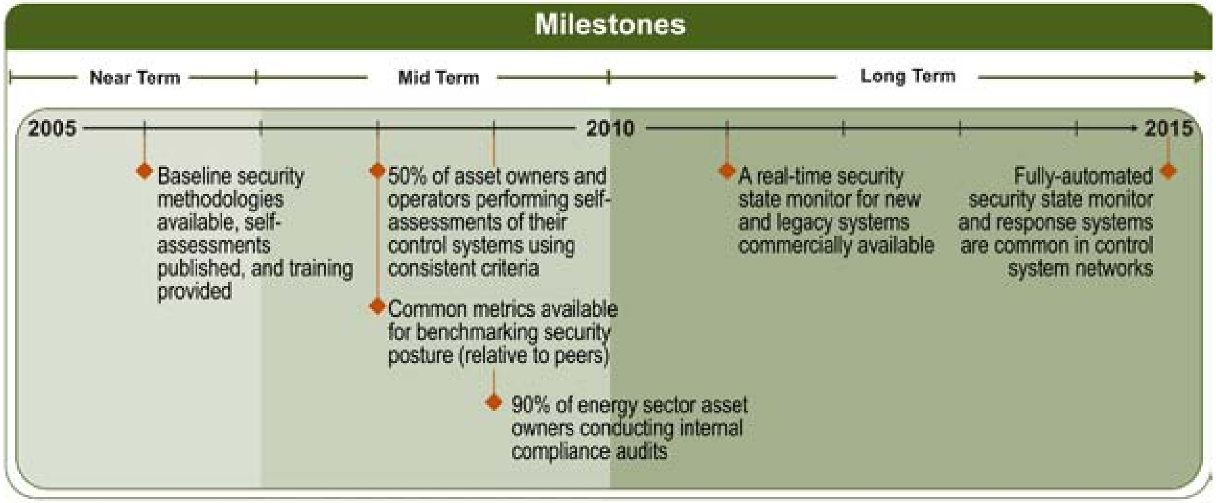
Goal

Measure and Assess Security Posture

Challenges

- Risk factors are not widely understood or accepted by technologists and managers
- Insufficient security metrics limit risk analysis capability
- Existing standards lack clear measurement specifications
- Consistent metrics are not available to measure and assess security status
- Insufficient tools and techniques exist to measure risk
- No standards exist to assess cyber vulnerabilities
- Threats are hard to demonstrate and quantify
- Intellectual property rights of asset owners are hard to protect

Milestones



Near Term — Mid Term — Long Term

2005 — 2010 — 2015

- Baseline security methodologies available, self-assessments published, and training provided
- 50% of asset owners and operators performing self-assessments of their control systems using consistent criteria
- Common metrics available for benchmarking security posture (relative to peers)
- 90% of energy sector asset owners conducting internal compliance audits
- A real-time security state monitor for new and legacy systems commercially available
- Fully-automated security state monitor and response systems are common in control system networks

Selected Priorities

Identifying Strategic Risks

- Create an environment for securely sharing collected U.S. government information on threats and real-world attacks with utilities and vendors

Legacy Systems

- Create a risk matrix that balances threat, vulnerability, and consequence
- Analyze risk and determine what action is appropriate

Security Tools and Practices

- Fund efforts to develop tool set for owners and operators to conduct self-assessments
- Set up and evaluate cyber attack and response simulators
- Develop consensus on clear and concise metrics for measuring security posture
- Develop risk assessment tools that include vulnerability assessment methodologies, frameworks for prioritizing control measures, and cost justification tools

Control Systems Architecture

- Develop baseline security requirements defined across system life cycle for fundamental, intermediate, and advanced security posture
- Develop automated security state and response support systems

Exhibit 3.3 – Strategies for Measuring and Assessing Security Posture

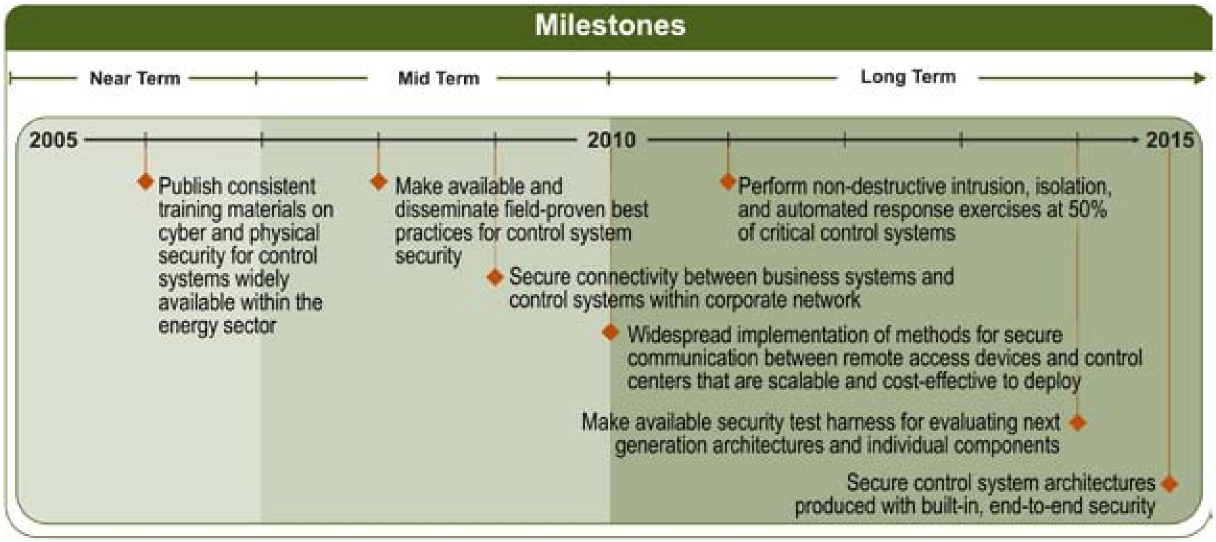
Goal

Develop and Integrate Protective Measures

Challenges

- Open and flexible control leads to increased risks
- Poorly designed connection of SCADA and business networks can dramatically increase vulnerabilities of control systems
- Security upgrades hard to retrofit to legacy systems, may be costly, and may degrade system performance
- Known technical vulnerabilities in non-vendor supporting hardware and software
- Standardized test plans and upgrades for new technology are not widely available
- Complexity increases exponentially with an increase in number of nodes
- Vendors do not have specific requirements or standards to build to

Milestones



- Publish consistent training materials on cyber and physical security for control systems widely available within the energy sector
- Make available and disseminate field-proven best practices for control system security
- Perform non-destructive intrusion, isolation, and automated response exercises at 50% of critical control systems
- Secure connectivity between business systems and control systems within corporate network
- Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy
- Make available security test harness for evaluating next generation architectures and individual components
- Secure control system architectures produced with built-in, end-to-end security

Selected Priorities

Legacy Systems

- Put non-intrusive, cost-effective, and robust SCADA encryption solutions into production
- Identify best practices for connecting SCADA and business networks
- Improve performance of legacy communications to enable the application of security solutions

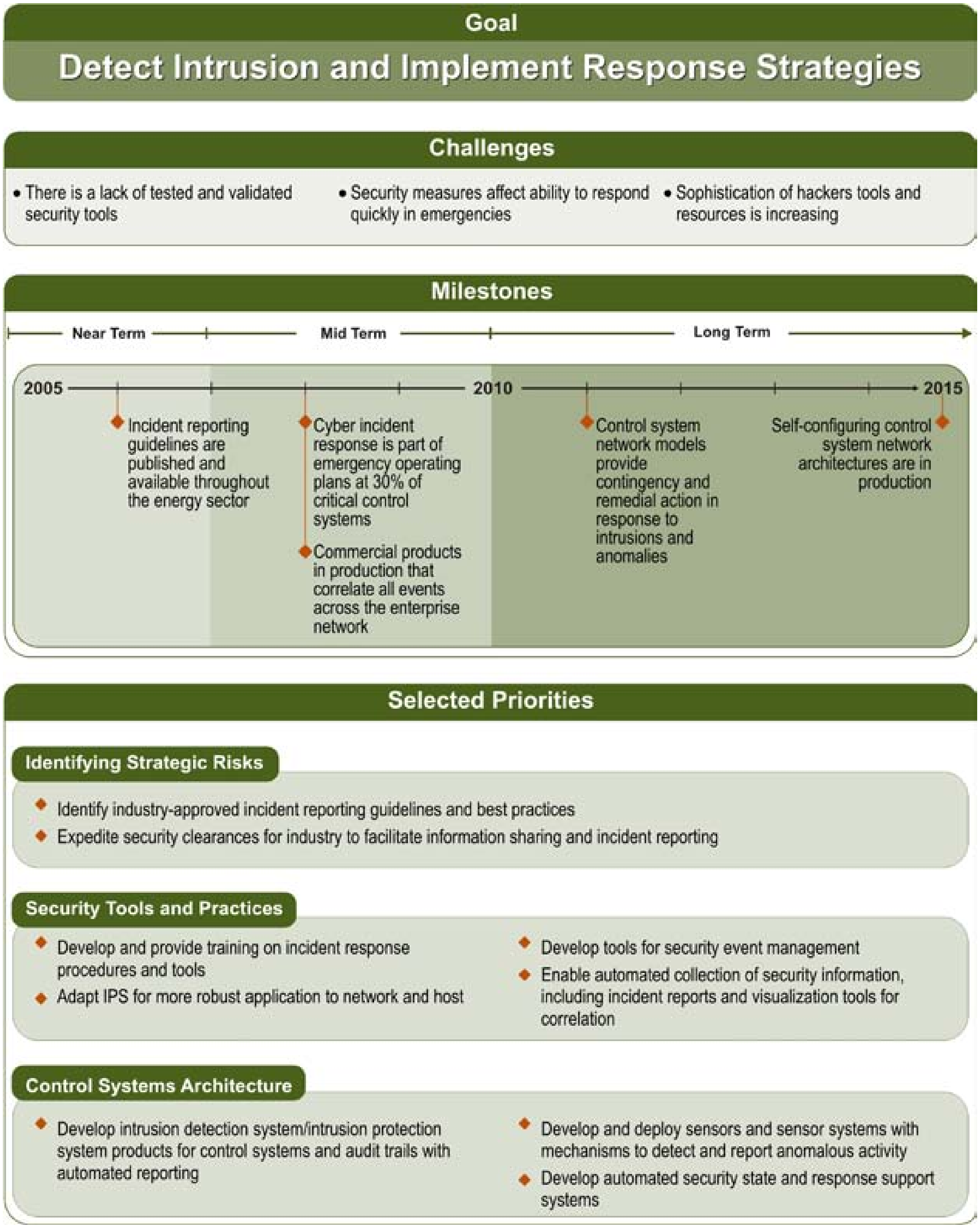
Security Tools and Practices

- Identify best practices for physical and cyber security of substations and control centers
- Develop patching technologies that do not impact 24/7 operations of operating systems
- Develop hardened operating systems for the control systems environment
- Maintain National SCADA Test Bed to work with vendors and asset owners to test equipment, architectures, and processes for both cyber and physical security

Control Systems Architecture

- Develop a security test harness with testing architecture and guidelines
- Develop true plug-and-play components that are secure
- Develop cost-effective gateway security that includes firewalls, intrusion detection, and anti-virus protection with minimum host impact

Exhibit 3.4 – Strategies for Developing and Integrating Protective Measures



Goal

Detect Intrusion and Implement Response Strategies

Challenges

- There is a lack of tested and validated security tools
- Security measures affect ability to respond quickly in emergencies
- Sophistication of hackers tools and resources is increasing

Milestones

Near Term — Mid Term — Long Term

2005 — 2010 — 2015

- Incident reporting guidelines are published and available throughout the energy sector
- Cyber incident response is part of emergency operating plans at 30% of critical control systems
- Commercial products in production that correlate all events across the enterprise network
- Control system network models provide contingency and remedial action in response to intrusions and anomalies
- Self-configuring control system network architectures are in production

Selected Priorities

Identifying Strategic Risks

- Identify industry-approved incident reporting guidelines and best practices
- Expedite security clearances for industry to facilitate information sharing and incident reporting

Security Tools and Practices

- Develop and provide training on incident response procedures and tools
- Adapt IPS for more robust application to network and host
- Develop tools for security event management
- Enable automated collection of security information, including incident reports and visualization tools for correlation

Control Systems Architecture

- Develop intrusion detection system/intrusion protection system products for control systems and audit trails with automated reporting
- Develop and deploy sensors and sensor systems with mechanisms to detect and report anomalous activity
- Develop automated security state and response support systems

Exhibit 3.5 – Strategies for Detecting Intrusion and Implementing Response

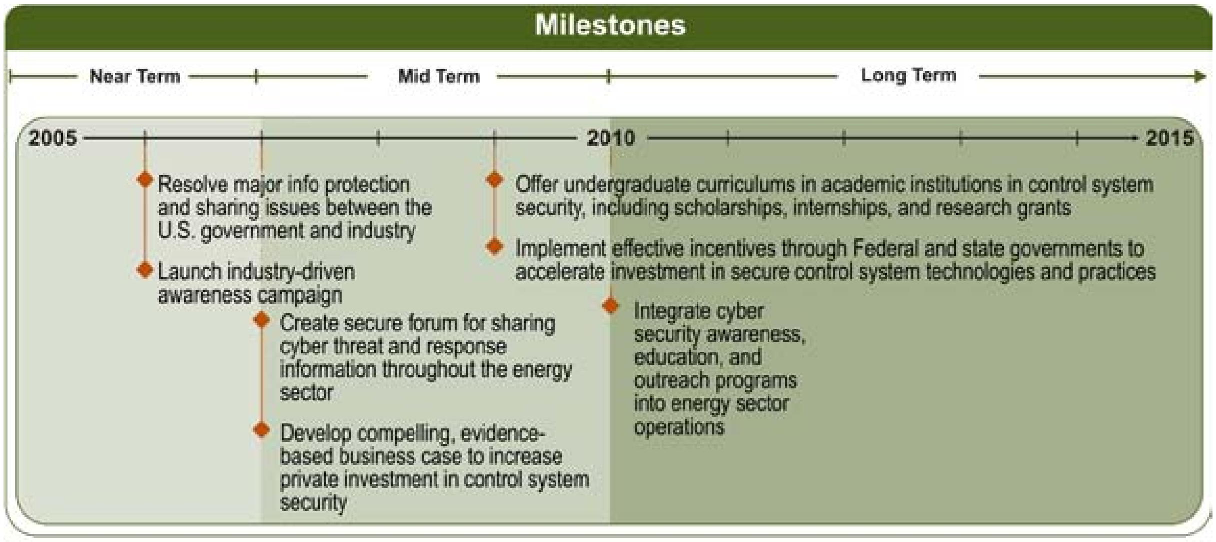
Goal

Sustain Security Improvements

Challenges

- Limited resources are available within businesses to address security needs
- Cyber security is a difficult business case
- Technology change is inhibited by lack of expertise, high costs, and corporate inertia
- Limited knowledge, understanding, and appreciation of control systems security risks inhibit action
- Insufficient sharing of threat and incident information among government and industry entities
- Effective security-oriented partnerships between government and industry have been difficult to establish
- Poor coordination among government agencies creates confusion and inefficiencies
- New regulations may impose requirements beyond the functional capability of legacy systems
- Highly educated staff with broad skill sets is needed to manage future operations

Milestones



Near Term — Mid Term — Long Term

2005 — 2010 — 2015

- Resolve major info protection and sharing issues between the U.S. government and industry
- Launch industry-driven awareness campaign
- Create secure forum for sharing cyber threat and response information throughout the energy sector
- Develop compelling, evidence-based business case to increase private investment in control system security
- Offer undergraduate curriculums in academic institutions in control system security, including scholarships, internships, and research grants
- Implement effective incentives through Federal and state governments to accelerate investment in secure control system technologies and practices
- Integrate cyber security awareness, education, and outreach programs into energy sector operations

Selected Priorities

Identifying Strategic Risks

- Develop standards and/or regulations for secure data exchange and communications
- Facilitate information sharing by guaranteeing protection of industry critical infrastructure protection (CIP) information through legislation of other means
- Identify a single Federal office to work with energy sector owners and operators on cyber security threats and issues
- Conduct analysis of incentives and benefits of implementing security to help fortify the business case
- Create appropriate incentives to invest in control systems security
- Create a cost-shared control systems security consortium that is protected from anti-trust issues

Security Tools and Practices

- Develop and implement security training for all employees and contractors
- Develop curriculums and university programs to improve education about control systems, security and risks, and associated economics

Exhibit 3.6 – Strategies for Sustaining Security Improvements

system, as well as gateway security solutions, can provide systems that offer built-in security, rather than the layered-on security of legacy systems. It will remain important to maintain interoperability between near-term and longer-term security solutions.

Goal: Detect Intrusion and Implement Response Strategies

No control system can be totally secure at all times. Utilities must be able to detect intrusions with sophisticated alarming tools, analyze anomalies and monitor system integrity, manage security events, and develop automated incident reporting processes that include complete audit trails. The long-term objective is to develop self-configuring networks that automatically provide contingency and remedial actions in response to intrusions. An overview of the challenges, milestones, and project priorities for detecting intrusions and implementing response strategies is shown in Exhibit 3.5

Challenges

Cyber intrusion tools are becoming increasingly sophisticated so that less knowledge is needed to launch a harmful attack. When attacks happen, the event and its consequence are often not shared beyond the company. This failure to share lessons learned means that a company is unlikely to have the knowledge required to respond quickly to control system emergencies, even when appropriate security measures are available.

Priorities

In the near term, industry should identify best practices and approved guidelines for incident reporting and find ways to share information confidentially among owners and operators. Proper training on incident response procedures is also needed. Intrusion detection systems need to be developed that include complete audit trails and automated reporting. Tools that help visualize data and communication patterns are needed to identify anomalies and correlate suspicious patterns with potential threats. Tools for security event management are needed in the mid term to help prioritize corrective actions through alarming, trending, forensics, and audits.

Goal: Sustain Security Improvements

The need for strong control system security has emerged as an important requirement within the energy sector. However, both industry and government are struggling with how best to accelerate security improvements within companies, recognizing that control system security is not a traditional part of information technology (IT) security or the business model. While a sustained effort is needed to provide the resources, incentives, and collaboration required for facilitating and increasing security improvements, government and industry are still clarifying their respective roles and responsibilities in this emerging area, and multiple efforts are underway to improve control systems. Leadership and commitment are needed to remove barriers, facilitate information sharing, and support R&D for technology improvements that are hard to justify within the sector's current business model. An overview of the challenges, milestones, and project priorities for sustaining security improvements is shown in Exhibit 3.6

Challenges

Outside of the control system community, there is a poor understanding of cyber security problems, their implications, and needed actions. Information sharing between industry and government is limited, primarily due to uncertainty on how information will be used, disseminated, and protected. Private investment for control system improvements, especially the development of advanced components and systems, is limited because it is difficult to make a strong business case for cyber security. In addition, aging of the workforce within the sector is cause for growing concern.

Priorities

There is an immediate need to guarantee that sensitive industry information submitted to the government is fully protected. Standards and/or regulations for data exchange and communication also may be needed. Ultimately, an environment must be created that facilitates sharing of U.S. government information on threats and real-world attacks with utilities and vendors. Security training is needed for owners, operators, and contractors at all corporate levels. The development of meaningful incentives to accelerate investment in control systems security is needed in the mid term.

Key Stakeholders

Control systems security is a shared responsibility among businesses and stakeholders throughout the control system value chain. As shown in Exhibit 3.7, the control systems stakeholder community consists of bulk energy asset owners and operators, government agencies, industry organizations, commercial entities, and researchers, each of which brings specialized skills and capabilities for improving control system security:

- **Asset Owners & Operators** bear the main responsibility for ensuring that control systems are secure, for making the appropriate investments, for reporting threat information to the government, and for implementing protective practices and procedures.

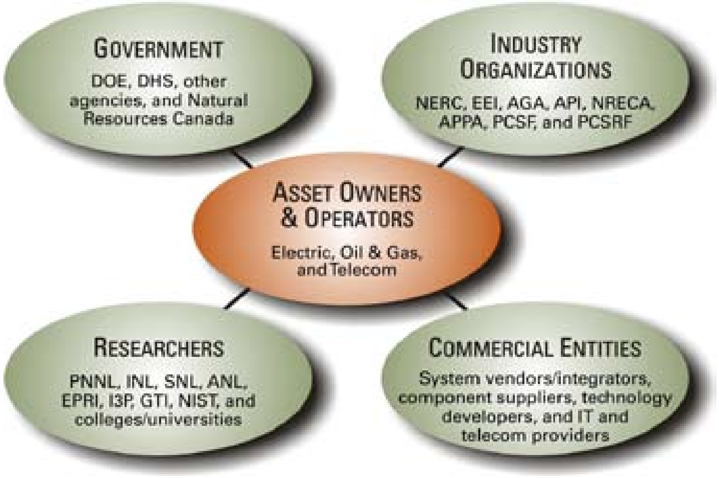

Government
DOE, DHS, other agencies, and Natural Resources Canada
Industry Organizations
NERC, EEI, AGA, API, NRECA, APPA, PCSF, and PCSRF
Asset Owners & Operators
Electric, Oil & Gas, and Telecom
Researchers
PNNL, INL, SNL, ANL, EPRI, I3P, GTI, NIST, and colleges/universities
Commercial Entities
System vendors/integrators, component suppliers, technology developers, and IT and telecom providers

Exhibit 3.7 – Key Stakeholder Groups and Sample Members

- **Government** agencies provide secure sharing of threat information and collaborate with industry to identify and fund gaps in control systems security research, development, and testing efforts.
- **Industry Organizations** provide coordination and leadership across multiple sectors to help address important barriers, form partnerships, and develop guidelines.
- **Commercial Entities** develop and deliver control system products and services to asset owners and operators.
- **Researchers**, funded by government and industry, explore long-term security solutions, develop new tools, and test control system vulnerabilities, hardware, and software.

4. Roadmap Implementation

This Roadmap contains a structured set of priorities that address specific control systems needs within the next ten years. The energy sector will pursue a focused, coordinated approach that 1) aligns current activities to roadmap goals and milestones, 2) initiates specific projects to address critical gaps, and 3) provides a mechanism for collaboration, project management, and oversight. The aim of this approach is to accomplish clearly defined activities, projects, and initiatives that contain time-based deliverables tied to roadmap goals and milestones.

Exhibit 4.1 outlines the main roadmap implementation steps that will result in an industry-managed process for launching and managing essential control systems projects. Strong leadership and commitment will be needed at each step to ensure that important requirements do not fall through the cracks. The Control Systems Roadmap Steering Group will conduct roadmap Outreach and Partnership Development to obtain industry feedback and commitment to participate in needed activities. Asset owners and operators must take the lead for initiating business-critical projects that will ensure reliable, secure operation of energy systems. A Roadmap Implementation Forum can provide a means to solicit new ideas for the most time-sensitive projects. Government agencies must accelerate funding of priorities that are appropriate for Federal action and aligned with departmental missions. These priorities often focus on long-term needs or efforts that provide limited incentive for business investment.

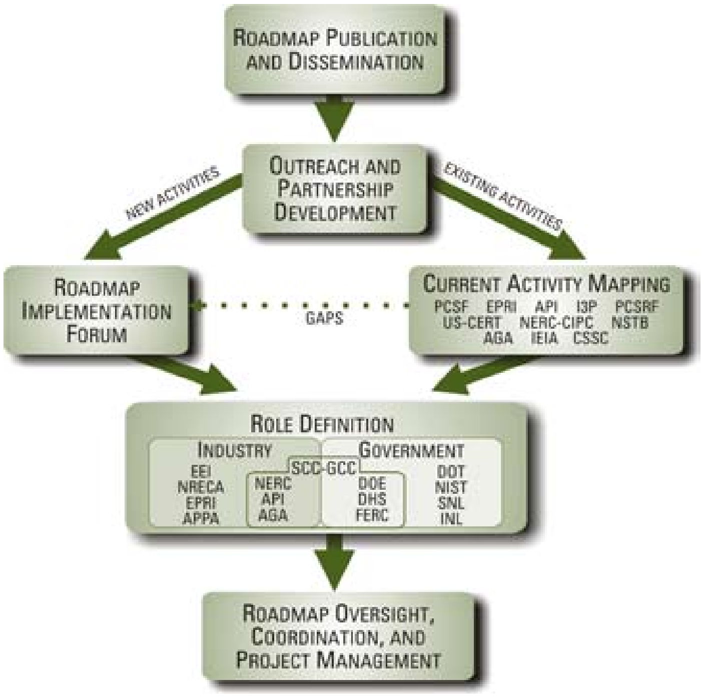


Exhibit 4.1 – Roadmap Implementation Process

The precise roles of companies and organizations in implementing this roadmap have not yet been determined. These roles will take shape as the roadmap is disseminated and reviewed by the key sector stakeholders. Proposals will likely emerge from leading industry organizations, consortia, or other institutions that can provide effective oversight and administration. The Electric Sector Coordinating Council (led by the North American Electric Reliability Council [NERC]) and the Oil and Natural Gas Sector Coordinating Council (led by the American Petroleum Institute [API] and the American Gas Association [AGA]) are established bodies that represent asset owners and operators. These Councils have good sector representation, exercise strong cross-sector coordination, and may serve as logical starting points for defining organizational roles and leadership. Their counterpart, the Energy Sector Government Coordinating Council, provides an established body for coordinating government efforts within the Department of Energy, Department of Homeland Security, Federal Energy Regulatory Commission, Department of Transportation, and other relevant agencies.

Guiding and Aligning Existing Efforts

The energy sector has actively pursued projects over the past five years to identify and address a variety of control system security concerns (see Exhibit 2.5). The Outreach and Partnership Development step shown in Figure 4.1 will help to map existing industry and government activities to roadmap milestones. This

mapping will uncover gaps that may require new projects and may uncover areas of overlap where better coordination could optimize available resources. The resulting map will be used to align and guide ongoing activities and will be updated periodically to track progress.

Addressing Critical Needs and Gaps

The strategic framework described in Chapter 3 contains four main goals and 25 time-dependent milestones (see Exhibit 3.1). If it is determined that a particular roadmap milestone is not being addressed through ongoing efforts, energy sector leaders will need to step forward and indicate their interest in planning and investing in projects or initiatives to address known gaps. This investment may be directed toward basic research, applied research, technology commercialization, product integration, field testing, scaled roll-out, training/outreach, or any other means or method that advances a particular milestone.

Prior to launching new projects, the energy sector must clearly define the desired outcomes, resources, and capabilities required and how the results will contribute to achieving a particular milestone. Each of these factors will be integrated into requests for proposals to solicit innovative solutions and projects from vendors, researchers, or the technical community. Each proposal must demonstrate that the proposed approach will accomplish project objectives, the proposing organization poses distinct capabilities and strengths to effectively complete the project, and the project deliverables will help achieve a particular milestone. A Roadmap Implementation Forum is envisioned as a structured meeting or meetings that bring together interested parties to define projects and solicit new proposals and concepts.

Proposed Mechanism for Oversight and Project Management

This Roadmap encourages organizations to participate in ways that will best capitalize on their distinct skills, capabilities, and resources for improving control system security. This affords companies and organizations the flexibility to pursue projects that correspond with their special interests. However, without a unified structure it will be difficult to adequately identify, organize, resource, and track the diverse activities and their corresponding roadmap milestones. A mechanism is needed to provide the required oversight, collaboration, and decision making to initiate and resource projects and activities. In addition, a project management organization will likely be needed to provide operational, logistical, and administrative support.

Effective roadmap implementation will require the following oversight and support functions:

Management. A coordinating entity, such as a Roadmap Project Management Committee, should be established to identify and resolve program issues, interface among stakeholders, and resolve technical, transition, and program management issues that could stand in the way of success. The Committee would also conduct reviews of proposals, sanction work efforts, manage expectations, provide operational support, and develop dissemination strategies.

Structure and Workflow. Workflow support will be required to support Roadmap projects and initiatives. This support would include electronically publishing and tracking deliverables and outcomes of projects, creating a feedback mechanism, electronic posting of Calls for Proposals and Responses to Proposals, and controlled on-line access for decision-making actions. The review process workflow, including notification, document collaboration, voting, and post-decisional steps should be maintained in an access-controlled space. Project planning framework details, including milestones, level of effort, timelines, roles and responsibilities, and deliverables, will be automatically generated upon approval of concept/proposal.

Operational Oversight. Logistical assistance will be required to support meetings, including the provision of adequate meeting space, facilitation, and workshops that will provide needed continuity for Roadmap efforts. Allowance should also be made for collaboration tools, such as separate electronic space, teleconference meetings, and Web-based meetings.

Appendix A: Key Challenges and Solutions

Many of the ideas contained in this Roadmap were gathered from 60 topic experts who attended a two-day facilitated workshop on July 13 and 14, 2005, in Baltimore, Maryland. During this workshop, leading energy sector owners and operators, researchers, technology developers, security specialists, and equipment vendors worked together to examine control systems issues in four breakout sessions:

A-1 Identifying Strategic Risks

A-2 Legacy Systems

A-3 Security Tools and Practices

A-4 Control Systems Architecture

The results of these sessions are summarized in this Appendix, and key findings are incorporated into Chapter 3 of this Roadmap. Results of these workshop sessions were previously published in *Workshop Summary Results for the Roadmap to Secure Control Systems in the Energy Sector*, prepared by Energetics Incorporated, August 2005.

A-1. Identifying Strategic Risks

By systematically documenting and prioritizing known and suspected control system vulnerabilities and their potential consequences, energy sector asset owners and operators will be better prepared to anticipate and respond to existing and future threats. Risk identification will provide the necessary foundation for a solid cyber security strategy, and enable the energy sector to more effectively implement mitigation and response plans to improve system reliability and resilience over the long term.

Identification of energy sector cyber threats, vulnerabilities, and consequences will facilitate development of standards for cyber security best practices, performance criteria for baseline control system security, and design requirements for hardware and software. Continuous identification and sharing of current and emerging strategic risks among energy sector stakeholders will promote a more proactive, holistic approach to control system security and design.

Challenges and Barriers

Identifying strategic risks to control systems is complicated by the proprietary nature of vulnerability assessments, the lack of adequate and reliable threat information, and difficulties in determining the return on security investments—particularly in rate-regulated energy industries. Concerted risk management efforts across the energy sector will require the formation of new partnerships and the redefinition of traditional regulatory relationships.

Institutional, Cultural, & Business Practices

Lack of clarity on stakeholder roles and responsibilities in improving cyber security has created serious inefficiencies, including gaps and overlaps in research and development. In addition, trust and liability concerns hinder disclosure of information on known vulnerabilities and risks, further hampering coordination. Under these circumstances, security specialists often find it difficult to convince sector decision-makers of the criticality of cyber security, and a reactive approach toward cyber security has become standard operating practice. The lag in regulatory policies and costs of training also make it difficult to stay ahead of hackers and others with malicious intent. Key institutional challenges to identifying strategic risks include the following:

- Most organizations lack existing groups, teams, or committees that bring together the right mix of people or fields of expertise to find solutions.
- Security awareness has not been a priority in system development and use.
- Security stakeholder roles and responsibilities are not clearly understood.
- Government information protection issues (e.g., Protected Critical Infrastructure Information and the Freedom of Information Act) and confidentiality concerns still linger.
- No clear vision of the threat has been articulated.
- No secure mechanism exists for sharing information on threat vulnerabilities.

Business Case

Developing and integrating security advances into electric or oil and gas SCADA architectures can be extremely costly. These costs can be difficult to justify—particularly because threats are not easy to identify or model and because the energy sector has yet to experience a major cyber attack. Decision-makers may remain unconvinced of the costs they may incur by not adequately investing in security improvements. System complexity also makes it difficult to assign costs and accountability among stakeholders. Resources

Identifying Strategic Risks

2005 2015

	Near Term (0-2 years)	Mid Term (2-5 years)	Long Term (5-10 years)
Information Sharing	**Develop standards and/or regulations for secure data exchange and communications** **Expedite security clearances for industry to facilitate info sharing and incident reporting** Apply data gathered from cyber vulnerabilities testing to educate best practices, standards, and training efforts Identify industry-approved incident reporting guidelines and best practices	**Create an environment for securely sharing collected U.S. government information on threats and real-world attacks with utilities and vendors**	
Business Case	**Conduct analysis of incentives and benefits of implementing security to help fortify the business case** Coordinate with state entities for cost recovery	Create appropriate incentives to invest in control systems security	
Regulatory Environment	**Identify a single Federal office to work with energy sector owners and operators on cyber security threats and issues** **Facilitate information sharing by fully guaranteeing protection of industry critical infrastructure protection (CIP) information through legislation or other means** Channel government funding to cyber security initiatives	Issue regulations that articulate serious civil and criminal penalties for physical and cyber attacks	Organize long-term, sustained government efforts for cyber security
Collaboration, Partnership and Outreach	Industry should define expectations for government, encourage unified government response and action, and change the way industry approaches government PCSF could be used as coordination mechanism for security focus, standards, awareness, and business case Government shall pursue aggressive outreach effort to gain industry consensus and buy-in on proposed solutions that will identify ways to cooperate among competitive entities	**Create a cost-shared control systems security consortium that is protected from antitrust issues**	

Bold denotes priority activities

Exhibit A.1 – Potential Solutions for Identifying Strategic Risks

are limited and many areas need funding. The challenges in developing the business case may be summarized as follows:

- The return on investment (ROI) for security cannot be demonstrated via any tangible measure; this applies to R&D, implementation, and time and effort.
- Some decision-makers see no economic penalty associated with minimizing funding for cyber threat deterrence.
- Assigning financial responsibility for security costs is problematic.
- Designing and implementing new security features is a high-cost undertaking.

Potential Solutions

Specific, actionable solutions to overcome current challenges in identifying strategic risks have been identified for each of the following four areas: Information Sharing; Business Case; Regulatory Environment; and Collaboration, Partnership, and Outreach. Exhibit A.1 summarizes these potential solutions by time frame (near term [0-2 years], mid term [2-5 years], and/or long term [5-10+ years]) with high-priority solutions shown in bold. A more detailed explanation of each category is provided below.

Information Sharing

Informed decision-making is essential to clarify the threat environment, perform associated vulnerability analyses, and identify risk priorities. Sharing information, technologies, and best practices while avoiding redundant research will help to optimize and accelerate R&D on security tools and practices and on designs for next-generation control systems.

Business Case

Without sufficient means to fully quantify and demonstrate the potential impacts of cyber attacks on energy sector control systems, asset owners are hard-pressed to justify SCADA control system security as a top funding priority. The result is a reactionary policy to cyber security that places our bulk electric and critical oil and gas assets at greater risk to emergent cyber threats. Industry stakeholders must cooperate to organize a strategic paradigm shift among key decision-makers, ultimately leading to a more proactive approach supporting SCADA cyber security advances. This step is essential to engage disparate corporate cultures and cultivate the resources necessary to support continuous investment and innovation in control system management and design.

Regulatory Environment

A single Federal office should be designated as the responsible entity for overseeing control system security within the energy sector. This step would simultaneously simplify regulatory development and compliance and provide the energy sector with a central point of contact for control system cyber security issues. Such unified administration would also boost energy sector confidence that all asset owners and operators are being held to the same standards across the board, thus fostering greater trust among key stakeholders. Such trust is particularly important in today's closely interconnected power grid. The designated agency could potentially serve as a secure clearinghouse for energy sector cyber threat and vulnerability data—with necessary protective measures in place to guard all disclosed proprietary information.

Collaboration, Partnership, & Outreach

The energy sector must realign its strategic risk outlook to embrace a sustained, longer-term investment in security as part of its standard business operations. Planning and collaboration among key stakeholders will help both the bulk electric and oil and gas industries maximize limited resources for cyber security.

A-2. Legacy Systems

Most legacy control systems were engineered and implemented to maximize efficiency, reliability, and functionality, with relatively little emphasis on security. Protecting the extensive array of legacy control systems throughout the energy sector is a growing concern among legacy asset owners and operators. The diverse nature of the existing legacy system landscape, which emerged in the absence of shared design standards, precludes a "one size fits all" approach to improved security.

The number and value of legacy control systems employed by the energy sector make it economically infeasible to completely replace those assets and their supporting communications networks with new technology. At present, only a small portion of the sector's control system assets are upgraded annually. This replacement rate should increase as new and more secure systems are developed that also offer better functionality and other business benefits.

The task of securing legacy assets from cyber attack will continue, even as newer systems are gradually brought online. At some phase in their service lifetimes, all control systems, no matter how state-of-the-art, will inevitably assume legacy status. This truth means asset owners and operators will need to plan for maintaining a base level of security through constant technology transition. In short, energy sector asset owners and operators must collectively form an enabling infrastructure that facilitates coordinated security practices and technology uptake processes applicable to both present and future legacy systems. Such an environment is necessary to provide enduring security and keep pace with continuous control system technology and communication improvement cycles.

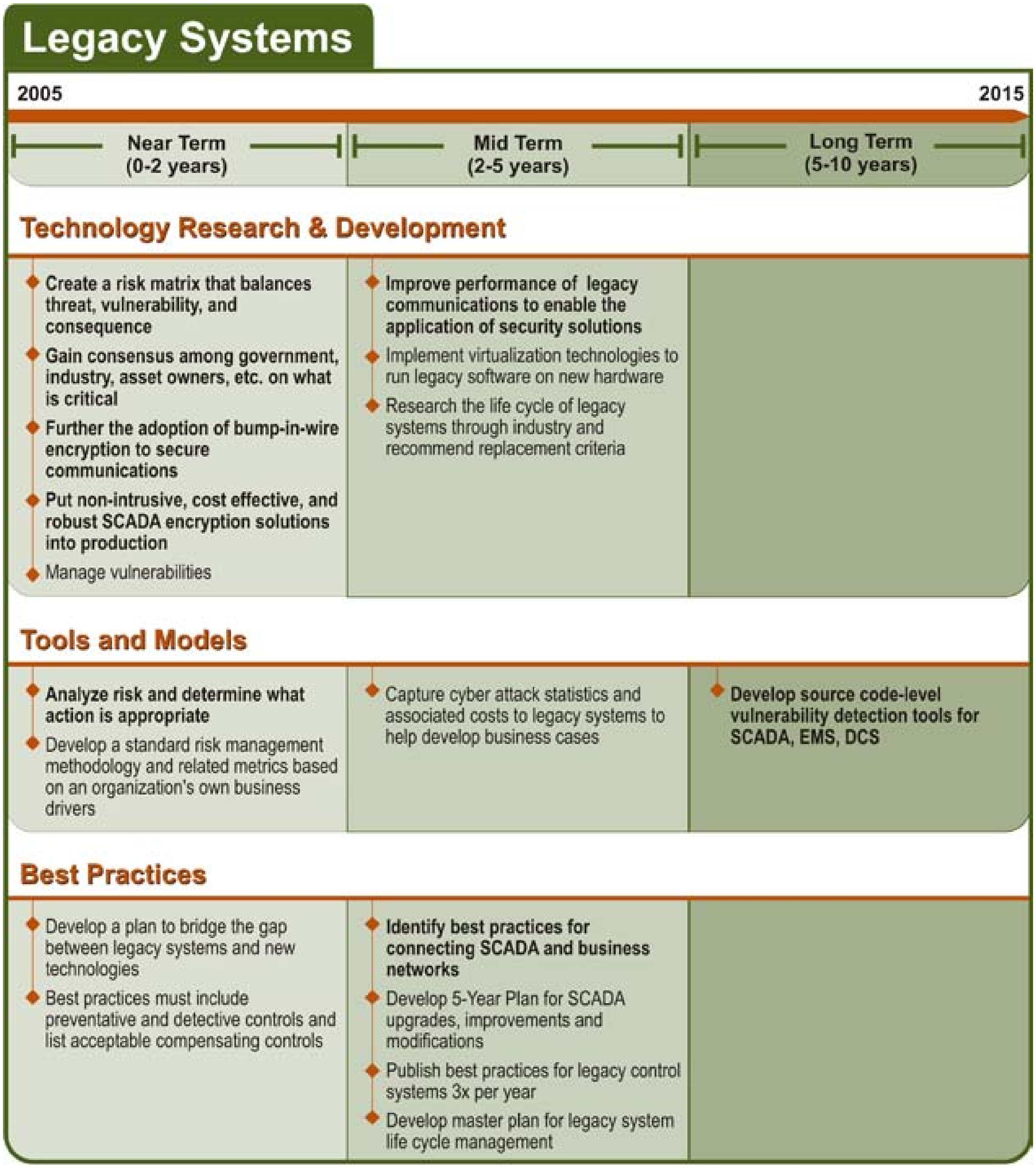
Challenges and Barriers

Adapting legacy systems to today's technology and security standards presents considerable challenges, often unique to individual systems. The complex assortment of systems, vendors, and patches or bolt-on fixes available typically works against efforts to find simple or broadly applicable solutions. At the same time, modern operating requirements placed on legacy systems may be stretching those systems to the limits of their operating abilities.

Standards and Regulations

Legacy systems that were originally developed in an era of proprietary designs and specifications must now conform to industry-wide standards and government regulation. Defining broadly applicable standards for the exceptionally diverse array of legacy systems is a major challenge. Setting effective standards or regulations is further complicated by the number and variety of stakeholders, from immediate system owners and operators to regulatory agencies and control system vendors. Some of the challenges include:

- Clear direction on developing minimum standards has not been provided by government.
- Uncertainty exists regarding methods for consistently and correctly measuring security.
- New regulations may impose requirements beyond the inherent functional capabilities of legacy systems.
- No standards were in existence when many legacy systems were implemented.
- Standards often lack specification of a measurable goal or end state, leading to trial and error in applications, discrepancies in auditing, and lack of consistency.
- Without certification, corporate officers are uncertain how their companies conform to standards.



Legacy Systems

2005 — 2015

	Near Term (0-2 years)	Mid Term (2-5 years)	Long Term (5-10 years)
Technology Research & Development	**Create a risk matrix that balances threat, vulnerability, and consequence** **Gain consensus among government, industry, asset owners, etc. on what is critical** **Further the adoption of bump-in-wire encryption to secure communications** **Put non-intrusive, cost effective, and robust SCADA encryption solutions into production** Manage vulnerabilities	**Improve performance of legacy communications to enable the application of security solutions** Implement virtualization technologies to run legacy software on new hardware Research the life cycle of legacy systems through industry and recommend replacement criteria	
Tools and Models	**Analyze risk and determine what action is appropriate** Develop a standard risk management methodology and related metrics based on an organization's own business drivers	Capture cyber attack statistics and associated costs to legacy systems to help develop business cases	**Develop source code-level vulnerability detection tools for SCADA, EMS, DCS**
Best Practices	Develop a plan to bridge the gap between legacy systems and new technologies Best practices must include preventative and detective controls and list acceptable compensating controls	**Identify best practices for connecting SCADA and business networks** Develop 5-Year Plan for SCADA upgrades, improvements and modifications Publish best practices for legacy control systems 3x per year Develop master plan for legacy system life cycle management	

Bold denotes priority activities

Exhibit A.2 – Potential Solutions for Legacy Systems

Technology and Risk Management

Many legacy systems within the energy sector share similar vulnerabilities. However, the inherently complex and varied nature of these sytems prevents stakeholders from capitalizing on economies of scale in efforts to upgrade their security. Legacy system security solutions thus remain costly, requiring highly customized technology management plans. Many of the issues involved in designing and implementing retrofit solutions for legacy systems are encountered across the energy sector. Some of these issues include the following:

- Connection of SCADA and business networks can dramatically increase the vulnerabilities of legacy systems if not designed properly.
- Applying bolt-on security systems may adversely affect vital performance levels.
- Bolt-on solutions to legacy control systems will be highly customized and costly, including replacement of software and/or hardware.
- Integrating new technology with a legacy system typically bears a much higher cost than with a standardized system.
- Mitigating known technical vulnerabilities is difficult with hardware and software no longer supported by vendors.
- Little or no guidance is available for migrating from legacy systems to new, advanced systems.

Potential Solutions

Providing security throughout the life cycles of legacy control systems will require the combined expertise of asset owners and operators, hardware and software vendors, and government stakeholders. By implementing solutions in the categories below, stakeholders can achieve a proactive security stance throughout the service life of control systems.

The full portfolio of potential solutions will include specific action items for immediate implementation as well as multi-year and decade-long strategies. Exhibit A.2 suggests the complete spectrum of potential solutions, organized in near-term (0-2 years), mid-term (2-5 years), and long-term (5-10 years) time frames.

Technology Research & Development

The energy sector has a number of opportunities to invest in research and development to reconcile the obsolete technology of legacy systems with advanced hardware, software, and communication tools. By coordinating among industry, government, and vendor stakeholders, the energy sector can benefit from shared knowledge in developing strategic and secure technology management plans. Multi-year efforts to develop specific technologies that mediate between legacy systems and advanced components hold great potential for enhancing legacy system security and value.

Tools and Models

Strategies for accomplishing legacy system reconciliation often require tailored security solutions. These solutions entail advanced detection tools to identify vulnerabilities, advanced risk modeling to determine costs of prevention versus recovery, and more accurate real-time modeling. Developing a portfolio of tools and modeling capabilities for legacy control systems would help expedite and focus the energy sector's security efforts.

Best Practices

Despite the diverse range of legacy systems throughout the energy sector, the industry would benefit from a collection of best practices for managing control systems throughout their life cycles. Such best practices should address extending the fleet of existing legacy systems to new functionality, incorporating advanced components, and migrating to fully advanced systems.

A-3. Security Tools and Practices

Cyber attack tools are increasing in sophistication and ease of use, threatening to outpace security efforts for control systems. By developing an advanced portfolio of security tools and practices, the energy sector can maintain reliable operations in the modern threat environment.

Security tools and practices that remove or reduce vulnerabilities in hardware and software, and provide powerful self-assessment capabilities, can be employed across the sector, enabling a more resilient security posture. In addition, security awareness and education levels must be raised throughout the industry to facilitate adoption and use of effective security practices. By coordinating efforts and combining resources, the energy sector can pursue advanced tools and practices to manage the new generation of risks.

Critical Challenges and Barriers

For the energy industry to continue to provide uninterrupted, reliable service to American consumers and businesses, control system security must overcome several critical challenges and barriers to developing advanced security tools and practices. State-of-the-art security tools often require more processing power or memory than existing control system components can provide. Without specific customer demand, however, vendors will not rapidly provide advances in security tools. Security enhancements must also be thoroughly validated before customers will consider deploying the technology. Key challenges include adequately testing and validating new tools and practices as they are developed and improving personnel cross-training in information technology (IT) and control systems.

Testing and Validation

New security tools and practices must be rigorously tested to expose any weaknesses, to maintain or enhance system performance and responsiveness, and to avoid inadvertent introduction of new flaws. Similarly, any retrofit technologies must address the wide variety of possible vulnerabilities in legacy systems. Key challenges include the following:

- Existing SCADA and DCS security tools often have “back-door” system access and other known vulnerabilities.
- Multi-layered or complex data authentication processes may slow response time to emergency situations.
- Vendors supply products in response to demonstrated customer demand, while customers are simultaneously waiting for proven products—creating a “Catch-22” situation.
- Insufficient coordination among operating system vendors, applications vendors, and users hampers development and testing of new tools and practices.

Tools and Models

Although cyber attacks have not yet caused a serious outage, they threaten to outpace the energy sector’s ability to manage them. Today’s assessment tools have not been properly shaped by the modern threat environment, and the reactive security posture of many asset owners and operators may no longer be successful. Metrics for measuring security using existing tools and practices are rudimentary at best. Difficulties in developing better tools and models include the following:

- Metrics for measuring security are inconsistent, varying in terms of methodology, contributors, and oversight.
- Risk factors are a “moving target” not widely recognized by technologists and management.
- The energy sector has historically employed a reactive (not proactive) security posture for control systems.

Best Practices

Security enhancement processes, such as migrating system components to newer technologies or installing security patches, can be challenging to implement without interrupting operations. Upgrading can be a lengthy process, and the collective benefits of such security enhancements may not be fully realized until the entire system has been upgraded. Further challenges include the following:

- Standardized test plans and updates for new technology are not publicly available.
- Owners cannot change their operating environments rapidly.

Training and Education

Continuing cost pressures will require businesses to maintain a leaner, more flexible workforce, placing increased reliance on automation to provide greater security. However, current IT security personnel tend to focus primarily on securing the enterprise systems, while control system operators are primarily concerned about reliable performance of the control systems. These two groups do not always understand each other's requirements and may not optimally collaborate to implement secure control systems. Two major challenges include:

- A more highly educated work force with broad skill sets is needed to manage control system security.
- Knowledge sharing and cross-training between corporate IT planners and control systems security staff are inadequate.

Potential Solutions

Maintaining reliable control systems and managing new risks require an advanced portfolio of security tools and practices. By developing solutions outlined in each of the following areas, the energy sector can improve its security posture and manage threats proactively. These solutions are designed to prevent attacks, assess the potential for damage from successful intrusions, and mitigate vulnerabilities. Development of these solutions can be expedited via secure information sharing between industry and government.

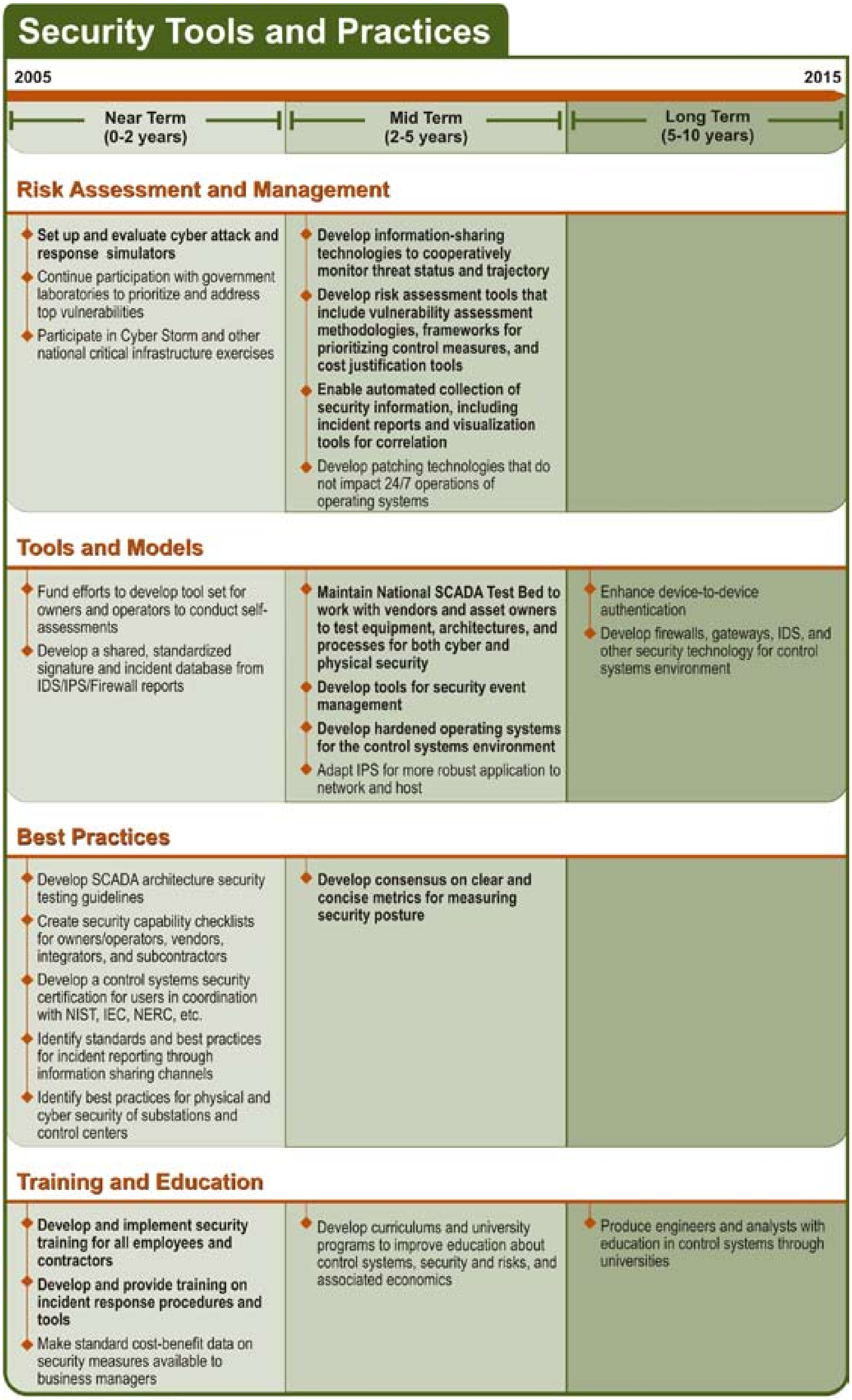
Developing successful tools and practices for control system security requires immediate action and long-term planning. The solutions outlined below are presented in near-term (0-2 years), mid-term (2-5 years) and long-term (5-10 years) time frames for generating a complete and adequate battery of tools to manage control system risks.

Risk Assessment and Management

Effective security metrics, modeling, and assessment tools will aid businesses in making prudent security investments. Tools that integrate energy sector threat and vulnerability information with the analytical power to generate actionable solutions for specific stakeholders will similarly contribute toward cost-effective security programs. The energy sector can continue to pursue tabletop exercises and simulations within a virtual environment to gather time-critical baseline security data on existing vulnerabilities. Such knowledge will enable stakeholders to prioritize threats and implement comprehensive risk management strategies that promote system survivability and recovery.

Tools and Models

New technologies, tools, and models are needed to protect control systems against increasing malicious cyber threats. Although many generic security products are available, they must be tailored to the process control system environment of the energy sector. Vendors and energy sector customers should collaborate on design requirements for intrusion detection and prevention systems (IDS, IPS), firewalls, and hardened operating systems. The National SCADA Test Bed (NSTB) has demonstrated its potential for providing assessment tools and models; continued NSTB funding, in conjunction with industry participation in NSTB activities, should enable development of highly useful and eagerly anticipated tool sets for the energy sector.



Security Tools and Practices

2005 — 2015

Near Term (0-2 years)	Mid Term (2-5 years)	Long Term (5-10 years)
Risk Assessment and Management		
◆ **Set up and evaluate cyber attack and response simulators** ◆ Continue participation with government laboratories to prioritize and address top vulnerabilities ◆ Participate in Cyber Storm and other national critical infrastructure exercises	◆ **Develop information-sharing technologies to cooperatively monitor threat status and trajectory** ◆ **Develop risk assessment tools that include vulnerability assessment methodologies, frameworks for prioritizing control measures, and cost justification tools** ◆ **Enable automated collection of security information, including incident reports and visualization tools for correlation** ◆ Develop patching technologies that do not impact 24/7 operations of operating systems	
Tools and Models		
◆ Fund efforts to develop tool set for owners and operators to conduct self-assessments ◆ Develop a shared, standardized signature and incident database from IDS/IPS/Firewall reports	◆ **Maintain National SCADA Test Bed to work with vendors and asset owners to test equipment, architectures, and processes for both cyber and physical security** ◆ **Develop tools for security event management** ◆ **Develop hardened operating systems for the control systems environment** ◆ Adapt IPS for more robust application to network and host	◆ Enhance device-to-device authentication ◆ Develop firewalls, gateways, IDS, and other security technology for control systems environment
Best Practices		
◆ Develop SCADA architecture security testing guidelines ◆ Create security capability checklists for owners/operators, vendors, integrators, and subcontractors ◆ Develop a control systems security certification for users in coordination with NIST, IEC, NERC, etc. ◆ Identify standards and best practices for incident reporting through information sharing channels ◆ Identify best practices for physical and cyber security of substations and control centers	◆ **Develop consensus on clear and concise metrics for measuring security posture**	
Training and Education		
◆ **Develop and implement security training for all employees and contractors** ◆ **Develop and provide training on incident response procedures and tools** ◆ Make standard cost-benefit data on security measures available to business managers	◆ Develop curriculums and university programs to improve education about control systems, security and risks, and associated economics	◆ Produce engineers and analysts with education in control systems through universities

Bold denotes priority activities

Exhibit A.3 – Potential Solutions for Security Tools and Practices

Best Practices

Industry and government should apply best practices identified through prior experience and information sharing to help mitigate and respond to cyber attacks. Use of strong and consistent metrics, testing guidelines, and certification processes will create measurable successes for control system security. These practices can help to benchmark control systems security across the energy sector.

Training and Education

Educating stakeholders on cyber security best practices and vulnerability awareness is critical to promoting safe, reliable operation of SCADA systems in today's evolving threat environment. Training and education should be facilitated so those employees in critical positions can better prepare for, respond to, and mitigate incidents and threats. The energy sector will also benefit from investments in targeted university programs that explore security risk economics and control system security and operations.

A-4. Control Systems Architecture

The cyber threat environment is constantly changing, challenging the ability of control system owners and operators to combat new threats. Hackers, terrorists, and others with malicious intent actively seek to exploit flaws in the existing control equipment, telecommunication methods, and operating systems prevalent throughout current energy systems. Novel control system architectures can provide the compulsory segmentation between internal company networks, SCADA servers, and external connections (e.g., the Internet) that is currently lacking in most systems. Innovative architectures can provide a high-level, purpose-built deterrent to unwanted and potentially harmful cyber intrusion. Ongoing expansion and modernization of the energy grid creates opportunities to bring such systems online.

Control system architectures in the energy sector involve complex networks comprised of power generation sites, energy management systems (EMS), grid management devices, substation remote terminal units (RTUs), SCADA control servers, SCADA workstations, and all supporting communications media and protocols. The architecture refers to the design of these networks: how the components are arranged, how they communicate with each other, and how they are controlled. Layering-on of patches to legacy system architectures can create gaps in security, whereas next-generation control system architectures provide new designs that enable built-in security. Novel architecture designs transparently incorporate pervasive security to promote appropriate network compartmentalization and defense in depth throughout the system. Future systems will use predictive security systems to continuously monitor for, provide appropriate action against, and automatically alert operators to, any atypical activity. Data transfer will take advantage of embedded encryption, based on a common standard to facilitate secure interoperability among network components and connected users. Plug-and-play compatibility will permit rapid upgrades to, and customization of, SCADA architectures to meet the needs of individual operators. Turning these goals into reality will require effective cooperation among energy sector stakeholders.

Critical Challenges & Barriers

Future threats are difficult to anticipate and define, risks are hard to measure, systems are becoming more complex, and vendors have no specific requirements upon which to base their designs. Even after these challenges are met, many companies may still find it difficult to justify the additional cost of next-generation control systems unless they offer enhanced functionality in addition to superior security.

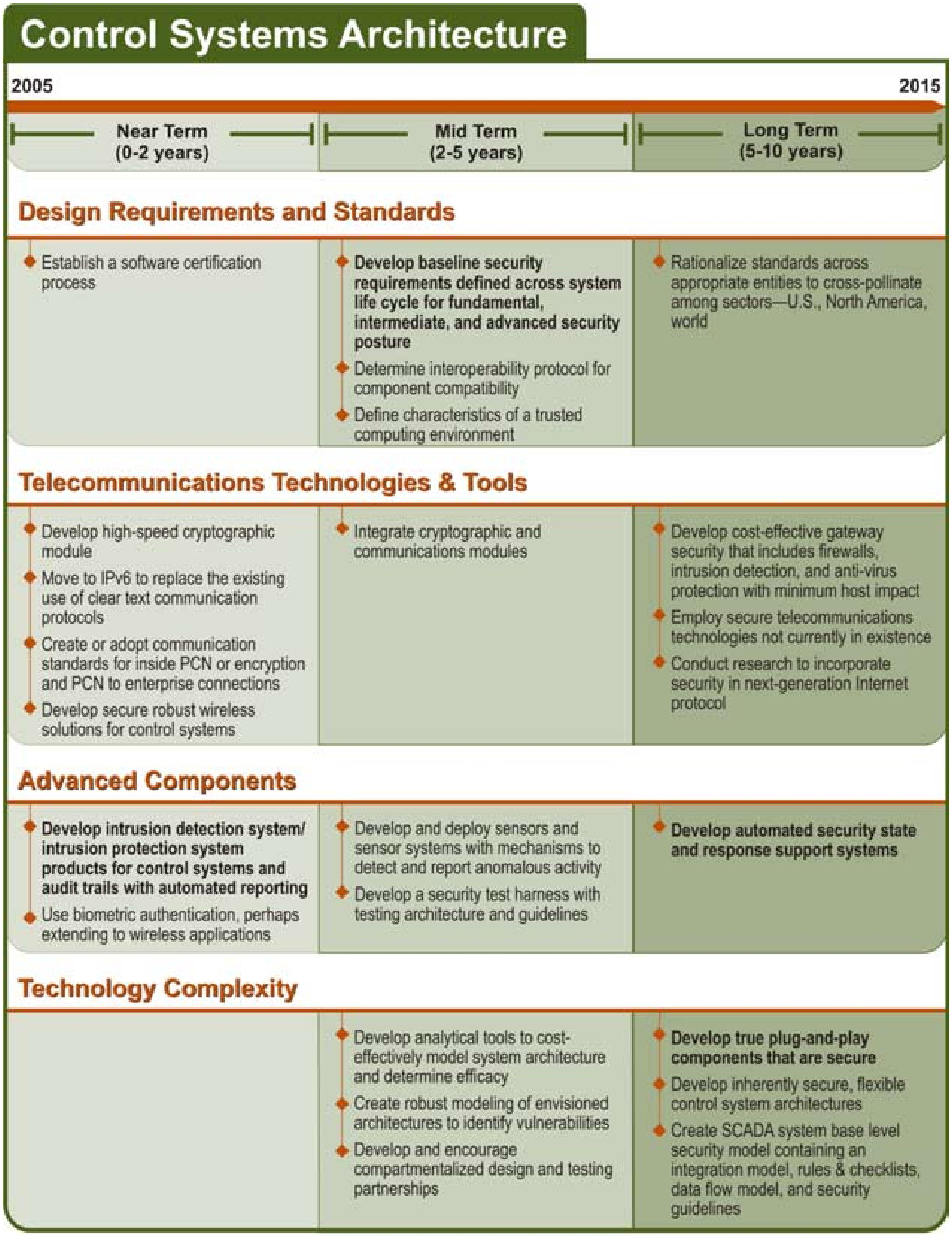
Design Requirements and Standards

Equipment vendors and software developers lack guidance on baseline security requirements. In the absence of specific design standards, incompatibility and interoperability issues may also arise during efforts to upgrade and/or patch control system architectures with new security hardware and software. Such disparate efforts could lead to new control system components that are less than fully secure or operational. Challenges entail the following:

- No interoperability standard addresses integration of cyber security components.
- Equipment vendors lack specific requirements to guide their design work.
- No set security goals have been established to guide software developers.

Threats & Vulnerabilities

Cyber threats are hard to demonstrate because asset owners lack the necessary tools to accurately measure risks to their control system architectures and to subsequently model the adverse effects each risk poses for their assets. Challenged to anticipate, demonstrate, and quantify rapidly growing cyber threats, asset owners struggle to prioritize architecture weaknesses with confidence and justify security investment.
Key challenges include the following:



Control Systems Architecture

2005 — 2015

	Near Term (0-2 years)	Mid Term (2-5 years)	Long Term (5-10 years)
Design Requirements and Standards	Establish a software certification process	**Develop baseline security requirements defined across system life cycle for fundamental, intermediate, and advanced security posture** Determine interoperability protocol for component compatibility Define characteristics of a trusted computing environment	Rationalize standards across appropriate entities to cross-pollinate among sectors—U.S., North America, world
Telecommunications Technologies & Tools	Develop high-speed cryptographic module Move to IPv6 to replace the existing use of clear text communication protocols Create or adopt communication standards for inside PCN or encryption and PCN to enterprise connections Develop secure robust wireless solutions for control systems	Integrate cryptographic and communications modules	Develop cost-effective gateway security that includes firewalls, intrusion detection, and anti-virus protection with minimum host impact Employ secure telecommunications technologies not currently in existence Conduct research to incorporate security in next-generation Internet protocol
Advanced Components	**Develop intrusion detection system/ intrusion protection system products for control systems and audit trails with automated reporting** Use biometric authentication, perhaps extending to wireless applications	Develop and deploy sensors and sensor systems with mechanisms to detect and report anomalous activity Develop a security test harness with testing architecture and guidelines	**Develop automated security state and response support systems**
Technology Complexity		Develop analytical tools to cost-effectively model system architecture and determine efficacy Create robust modeling of envisioned architectures to identify vulnerabilities Develop and encourage compartmentalized design and testing partnerships	**Develop true plug-and-play components that are secure** Develop inherently secure, flexible control system architectures Create SCADA system base level security model containing an integration model, rules & checklists, data flow model, and security guidelines

Bold denotes priority activities

Exhibit A.4 – Potential Solutions for Control Systems Architecture

- Future threats are hard to predict, demonstrate, and quantify.
- Globalization and increased outsourcing of hardware and software.

Technology Complexity

Asset owners and operators face a constant challenge to maintain and elevate the security of their control systems despite an increasingly open communications environment and proliferating cyber threats. The need to expand control system architectures to monitor and operate progressively more numerous, complex, and distant assets further confounds this problem. Some major challenges include the following:

- Architecture complexity is increasing exponentially as the number of control system nodes increases.
- A "big picture" view of potential problems is lacking.
- Creation of a ubiquitous security envelope remains elusive.
- Supporting continuous technological advancement requires high levels of expertise and incurs excessive costs.
- Limited means are available to detect unexpected outcomes arising from greater system complexity.

Potential Solutions

Success in advancing SCADA architecture security depends on effective integration and use of the specialized skills, knowledge, and resources of various stakeholders in each of the areas listed below. Effective collaboration will leverage synergies with related security efforts to create a more prepared front against the threat of potential cyber attacks aimed at energy sector assets.

Each of these areas contains specific, actionable solutions in near-term (0-2 years), mid-term (2-5 years), and/or long-term (5-10+ years) time frames. A more detailed explanation of each category is provided below. Potential solutions are also summarized in Exhibit A.4, with high-priority solutions shown in **bold**.

Design Requirements and Standards

Mandatory security standards and interoperability protocols must be established and implemented to guide continuous development of reliable, highly functional control system technology and software, without which the integrity of next-generation control system architectures will be severely compromised. Standards should be defined across the full life cycle of the control system to facilitate technology transition.

Telecommunications Technologies & Tools

Advanced telecommunications technologies can be harnessed to protect data transmission throughout SCADA network architectures. Next-generation control system architectures must incorporate elaborate cryptographic units and high-level gateway security to secure critical systems.

Advanced Components

Growing threat sophistication demands progress in advanced components to enhance the security of next-generation control system architectures. Advanced components must rapidly detect and log irregular cyber activity and instantly report events to control system operators. This may be accomplished through technologies such as integrated intrusion detection systems (IDS) and intrusion prevention system (IPS) products with built-in audit trails. Ultimately, such components can help achieve a more responsive, automated SCADA system protection capability.

Technology Complexity

Escalating interconnectedness among energy suppliers, paralleled by substantial growth in physical assets, has tremendously increased the complexity of control system architectures in the energy sector. Cost-effective modeling and simulation tools to design and test innovative control system architectures are needed to help users manage the wide array of information flowing through their networks. Highly valued, secure plug-and-play components will serve an integral function in these designs and must be continuously enhanced alongside next-generation system architectures to assure security and technology compatibility.

Appendix B: Contributors

Control Systems Roadmap Steering Group

Michael Assante
International Electricity Infrastructure Assurance Forum

Tommy Cabe
Sandia National Laboratories

Jeff Dagle
Pacific Northwest National Laboratory

David Darling
Natural Resources Canada

Kimberly Denbow
American Gas Association

Thomas R. Flowers
CenterPoint Energy

Tom Frobase
Teppco Partners, LP

Gary Gardner
American Gas Association

Robert Hill
Idaho National Laboratory

Hank Kenchington
U.S. Department of Energy

Tom Kropp
Electric Power Research Institute

Douglas Maughan
U.S. Department of Homeland Security—Science & Technology Directorate

Linda M. Nappier
Ameren

David Poczynek
Williams

Al Rivero
Chevron (now with Telvent)

William F. Rush
Gas Technology Institute

Lisa Soda
American Petroleum Institute

Roadmap Workshop Presenters

Dr. Jane A. "Xan" Alexander
Deputy Director
Homeland Security Advanced Research Projects Agency
U.S. Department of Homeland Security

Michehl R. Gent
President and CEO,
North American Electric Reliability Council

Hank Kenchington
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy

Paul B. Kurtz
Executive Director
Cyber Security Industry Alliance

Al Rivero
Manager, Regulatory Strategy and Compliance
Chevron (now with Telvent)

Dr. Samuel G. Varnado
Director, Information Operations Center
Sandia National Laboratories

Roadmap Workshop Participants

Michael Assante
International Electricity Infrastructure Assurance Forum

Suresh Babu
Gas Technology Institute

Regis Binder
Federal Energy Regulatory Commission

Rene Bourassa
Hydro-Quebec

Brent Brobak
AREVA T&D

Tommy Cabe
Sandia National Laboratories

Chris Carlson
KEMA

Jay Cribb
Southern Company

Frederick Curry
Energen Corporation

Jeff Dagle
Pacific Northwest National Laboratory

Kimberly Denbow
American Gas Association

Terry Doern
Bonneville Power Administration

Jack Edwards
Nortel

Carl Eng
Dominion Virginia Power

Gary Finco
Idaho National Laboratory

Thomas R. Flowers
CenterPoint Energy

Steven Fulton
Enbridge Pipelines

Tom Frobase
Teppco Partners, LP

Gary Gardner
American Gas Association

Tom Glock
Arizona Public Service

Michael Hagee
Duke Energy

Ken Hall
Edison Electric Institute

Matthew Harris
Peoples Energy

Carolyn Hicklin
Schweitzer Engineering Laboratories

Robert Hill
Idaho National Laboratory

Rob Hoffman
Idaho National Laboratory

Michael Huber
Marathon Ashland Pipe Line, LLC

Jason Johnson
Dominion

Hank Kenchington
U.S. Department of Energy

Steve Koenig
ConocoPhillips Pipe Line

Tom Kropp
Electric Power Research Institute

Barry Kuehnle
Schweitzer Engineering Laboratories

Roger Lampila
New York Independent System Operator

Ron Larson
General Electric

Lou Leffler
North American Electric Reliability Council

Eric Lightner
U.S. Department of Energy

Robert Mathews
Pacific Gas and Electric Company

Doug Maughan
U.S. Department of Homeland Security—
Science & Technology Directorate

Rob McComber
Telvent

Phillip McCrory
TXU Electric Delivery

Patrick Miller
PacifiCorp

Jim Mlachnik
Southwest Gas Corporation

David Poczynek
Williams

Ernest Rakaczky
Invensys Process Systems

Al Rivero
Chevron (now with Telvent)

Pete Sauer
University of Illinois at Urbana-Champaign

Gary Sevounts
Symantec Corporation

Paul Skare
Siemens

Phil Sobol
Aquila, Inc.

Lisa Soda
American Petroleum Institute

Eric Solberg
American Transmission Company

Kevin Staggs
Honeywell

Keith Stouffer
National Institute of Standards and
Technology

Lynn Terwoerds
Microsoft

Michael Torppey
Mitretek Systems

Breakout Session Facilitators and Rapporteurs

Control Systems Architecture

Jack Eisenhauer
Energetics Incorporated
(Facilitator)

Mark Ellis
Energetics Incorporated
(Rapporteur)

Security Tools & Practices

Keith Jamison
Energetics Incorporated
(Facilitator)

Brian Marchionini
Energetics Incorporated
(Rapporteur)

Identifying Strategic Risks

Ross Brindle
Energetics Incorporated
(Facilitator)

Michael O'Brien
Energetics Incorporated
(Rapporteur)

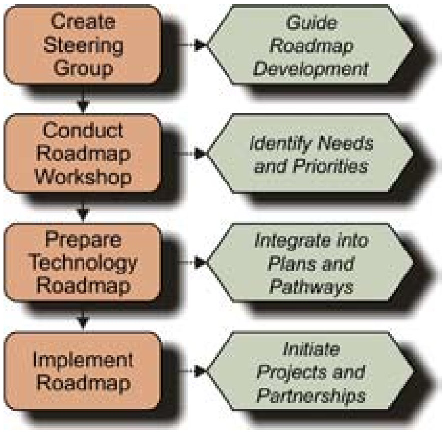
Legacy Systems

Joe Badin
Energetics Incorporated
(Facilitator)

Brad Spear
Energetics Incorporated
(Rapporteur)

APPENDIX C: ROADMAP PROCESS

This roadmap was developed through four main steps, as shown at right and described below:


Create Steering Group
Guide Roadmap Development
Conduct Roadmap Workshop
Identify Needs and Priorities
Prepare Technology Roadmap
Integrate into Plans and Pathways
Implement Roadmap
Initiate Projects and Partnerships

Roadmap Development Steps

Steering Group

A 17-member, executive-level Roadmap Steering Group was established to guide the planning process for the Roadmap. This Group represents a cross-section of control system experts from the energy sector and government who appreciate the needs of energy asset owners and operators (Steering Group members are listed in Appendix B). Primary functions of the Steering Group were established as follows:

- Guide and recommend workshop topics, content, and technical scope.
- Identify and help attract nationally respected and highly qualified individuals to participate in the workshop.
- Review the final workshop results and roadmap drafts for completeness and accuracy.
- Provide leadership in roadmap implementation.

Expert Workshop

Ideas contained in this roadmap came from 60 experts who convened for a two-day facilitated workshop that took place July 13-14, 2005, in Baltimore, Maryland. The workshop brought together leading energy sector owners and operators, researchers, technology developers, security specialists, and equipment vendors who worked together to examine four control systems issues: 1) Identifying Strategic Risks, 2) Legacy Systems, 3) Security Tools and Practices, and 4) Control Systems Architecture. The workshop results were published separately in *Workshop Summary Results for the Roadmap to Secure Control Systems in the Energy Sector*, prepared by Energetics Inc., August 15, 2005.

Roadmap Preparation

The Steering Group synthesized the workshop results within a goal-based strategic framework, as presented in Chapter 3 of this document. The group members also developed a set of milestones that are based on the workshop priorities. The draft Roadmap was circulated to experts within the control systems community for comments, which have been incorporated into the final Roadmap document.

Implementation

The plan for implementing the Roadmap is outlined in Chapter 4 of this document. Key steps involve mapping existing activities to the Roadmap's strategic framework, launching new activities identified by the Roadmap or via gap analysis after the mapping process, and development of a mechanism to provide ongoing coordination and oversight for the Roadmap implementation process.

Appendix D: References

Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. 2000. "State of the practice of intrusion detection technologies." Carnegie Mellon University. Software Engineering Institute. CMU/SEI-99-TR-028 ESC-TR-99-028
www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028title.html

Ananth, Dr. K.P. 2005. "SCADA and the terrorist threat: Protecting the nation's critical control systems." Testimony before the House Committee on Homeland Security, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity and the Subcommittee on Emergency Preparedness, Science, and Technology, U.S. House of Representatives. Media Packet. October 18, 2005. Washington, DC. hsc.house.gov/files/TestimonyAnanth.pdf

Asenjo, J. 2005. "Cybersecurity for legacy SCADA systems." *Utility Automation & Engineering T&D.* PennWell Publishing.

Associated Press. 2002. "Hackers hit power companies." *CBSNews.com.* July 8.
www.cbsnews.com/ stories/2002/07/08/tech/main514426.shtml

Barnes, K., and B. Johnson. 2004. *Introduction to SCADA protection and vulnerabilities.* Report INEEL/EXT-04-01710. Idaho National Engineering and Environmental Laboratory. Idaho Falls.

Barnes, K., B. Johnson, and R. Nickelson. 2004. *Review of supervisory control and data acquisition (SCADA) systems.* Report INEEL/EXT-04-01517. Idaho National Engineering and Environmental Laboratory. Idaho Falls.

Bush, President George W. 2003. *Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection.* Washington, DC.
www.whitehouse.gov/news/ releases/2003/12/20031217-5.html.

Byres, E. 2005. "Who turned out the lights?: Analysis of cyber attacks on control systems." British Columbia Institute of Technology. Presentation slides for InfraGard 2005 national conference.
www.infragard.net/library/congress_05/scada_systems/Critical_Infrastructure_Industrial%20Security%20Incident%20Database%202005%20Report%20(Byres).pdf

Clinton, President Bill. 1998. *Presidential Decision Directive 63*. Washington, DC.
www.fas.org/irp/offdocs/pdd-63.htm

Department of Homeland Security. 2005. *Interim National Infrastructure Protection Plan.* Annex 4, 56.

Eisenhauer, J. 2003. *Meeting brief: DOE/DHS SCADA meeting.* Prepared for the U.S. Department of Energy, Office of Energy Assurance. Energetics Incorporated. www.oe.netl.doe.gov/docs/prepare/scada.pdf

Energetics, 2005. Energetics Incorporated. *Workshop summary results for the roadmap to secure control systems in the energy sector.* Prepared for the U.S. Department of Energy, Office of Energy Assurance, August 2005.

EPRI. 2001. Electric Power Research Institute. *The cost of power disturbances to industrial and digital economy companies.* Consortium for Electric Infrastructure to Support a Digital Society. Report 1006274.

Fouda, H. 2005. "The role of SCADA in securing our critical infrastructure." Control Microsystems.
whitepapers.techrepublic.com/whitepaper.aspx?scname=Cyber+Security&docid=120232

GAO. 2004. Government Accountability Office. *Critical infrastructure protection: Challenges and efforts to secure control systems* (GAO-04-354). Washington, DC. www.gao.gov/new.items/d04354.pdf.

Dubiel, J., K. Steenstrup, and P. Pechersky. 2002. *Prepare for cyberattacks on the power grid.* Gartner Research. europe.gartner.com/pages/story.php.id.2727.s.8.jsp

Gellman, B. 2002. “Cyber-attacks by Al Qaeda feared: Terrorists at threshold of using Internet as tool of bloodshed.” *WashingtonPost.com,* June 26, 2002. www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26

I3P or Institute for Information Infrastructure Protection. 2005. “Process Control System Security.” *National Cyber Infrastructure Bulletin*, No. 1, October 2005. www.thei3p.org/about/i3pbulleting1.pdf

INEEL. 2004. *National strategy for control system security*. Prepared for the U.S. Department of Homeland Security. Idaho National Engineering and Environmental Laboratory. Idaho Falls.

Lindqvist, U. 2005. *Securing control systems in the oil and gas infrastructure: The I3P SCADA security research project*. Slides presented at the Trust Seminar at the University of California – Berkeley, November 17, 2005. http://trust.eecs.berkeley.edu/pubs/11.html

LaCommare, K.H., and J. H. Eto. 2004. “Understanding the cost of power interruptions to U.S. electricity consumers.” Lawrence Berkeley National Laboratory. Paper LBNL-55718. http://repositories.cdlib.org/lbnl/LBNL-55718

Newton-Evans Research Company, Inc. 2005a. Vol. I: “North American Market Survey and Analysis.” *World market study of SCADA, energy management systems and distribution management systems in electrical utilities: 2005-2007.* June 2005. www.newton-evans.com/servicesreports.asp.

Newton-Evans Research Company, Inc. 2005b. Correspondence addressed to J. Eisenhauer from C. Newton of Newton-Evans Research Co., December 11, 2005.

Newton-Evans Research Company, Inc. 2005c. *SCADA systems security measures: Current adoption and usage rates among North American electric power and gas utilities and petrochemical transmission pipelines*. Slides presented at Infragard national conference.” August 2005. www.infragard.net/library/congress_05/scada_systems/Critical_Infrastructure_Adoption%20of%20Security%20Measures%20(Newton).pdf

Paller, A. 2005. “SCADA and the terrorist threat: Protecting the nation’s critical control systems.” Testimony before the House Committee on Homeland Security, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity and the Subcommittee on Emergency Preparedness, Science, and Technology, U.S. House of Representatives. Media Packet. October 18, 2005. Washington, DC. homeland.house.gov/files/TestimonyPaller.pdf

Piller, C. 2002. “Hackers target energy industry.” *The Los Angeles Times,* July 8, 2002. www.theptrgroup.com/LATimes.html

President’s CIP Board and DOE. 2002. *21 steps to improve cyber security of SCADA networks*. President’s Critical Infrastructure Protection Board and the U.S. Department of Energy, Office of Energy Assurance. www.ea.doe.gov/pdfs/21stepsbooklet.pdf

Purdy, D. 2005. “SCADA and the terrorist threat: Protecting the nation’s critical control systems.” Testimony before the House Committee on Homeland Security, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity and the Subcommittee on Emergency Preparedness, Science, and Technology, U.S. House of Representatives. Media Packet. October 18, 2005. Washington, DC. homeland.house.gov/files/TestimonyPurdy.pdf

Reed, T. 2005. *At the abyss: An insider's history of the cold war.* Random House. www.randomhouse.ca/catalog/display.pperl?isbn=9780891418375

Riptech, Inc. 2002. *Riptech internet security threat report: vol. II.* www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf

Rush, Dr. W. 2005. "SCADA and the terrorist threat: Protecting the nation's critical control systems," Testimony before the House Committee on Homeland Security, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, and the Subcommittee on Emergency Preparedness, Science, and Technology, U.S. House of Representatives. Media Packet. October 18, 2005. Washington, DC. homeland.house.gov/files/TestimonyRush.pdf

Stamp, J., J. Dillinger, W. Young, and J. DePoy. 2003. *Common vulnerabilities in critical infrastructure control systems.* Sandia National Laboratories. SAND2003-1772C. www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf

Symantec. 2005a. Symantec Corporation. *Best practices for securing SCADA networks and systems in the electric power industry.* enterprisesecurity.symantec.com/industry/power/default.cfm.

Symantec. 2005b. Symantec Corporation. *Understanding SCADA system security vulnerabilities,* 2005. enterprisesecurity.symantec.com/industry/power/default.cfm.

Symantec. 2005c. Symantec Corporation. *Symantec Internet security threat report: Trends for July 04 – December 04,* vol. VII, March 2005. enterprisesecurity.symantec.com/content.cfm?articleid=1539

Todd, L. 2005. "SCADA and the terrorist threat: Protecting the nation's critical control systems," Testimony before the House Committee on Homeland Security, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, and the Subcommittee on Emergency Preparedness, Science, and Technology, U.S. House of Representatives. Media Packet. October 18, 2005. Washington, DC. homeland.house.gov/files/TestimonyTodd.pdf

US-CERT. 2005. U.S. Computer Emergency Readiness Team. "Control systems cyber security awareness." US-CERT informational focus paper. www.us-cert.gov/reading_room/Control_System_Security.pdf

Varnado, Dr. S.G. 2005. "SCADA and the terrorist threat: Protecting the nation's critical control systems," Testimony before the House Committee on Homeland Security, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, and the Subcommittee on Emergency Preparedness, Science, and Technology, U.S. House of Representatives. Media Packet. October 18, 2005. Washington, DC. hsc.house.gov/files/TestimonyVarnado.pdf

White House. 2003. *The National Strategy to Secure Cyberspace,* 2003. www.whitehouse.gov/pcipb/

Appendix E: Acronyms

AGA	American Gas Association
ANL	Argonne National Laboratory
API	American Petroleum Institute
APPA	American Public Power Association
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection
CIPC	Critical Infrastructure Protection Committee
COTS	Commercial Off-The-Shelf
CSSC	Control Systems Security Center
DCS	Distributed Control Systems
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DOT	Department of Transportation
EEI	Edison Electric Institute
EMS	Energy Management System
EPRI	Electric Power Research Institute
FERC	Federal Energy Regulatory Commission
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
GAO	U.S. Government Accountability Office
GCC	Government Coordinating Council
GTI	Gas Technology Institute
GUI	Graphical User Interface
HSARPA	Homeland Security Advanced Research Projects Agency
HSPD	Homeland Security Presidential Directive
I3P	Institute for Information Infrastructure Processing
ICCP	Inter-Control Center Communications Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEIA	International Electricity Infrastructure Assurance Forum
INL	Idaho National Laboratory
IPv6	Internet Protocol Version 6
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
NERC	North American Electric Reliability Council
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
NRECA	National Rural Electric Cooperative Association
NSTB	National SCADA Test Bed
O/S	Operating System
PCII	Protected Critical Infrastructure Information
PCN	Process Control Network
PCSF	Process Control Systems Forum
PCSRF	Process Control Systems Requirements Forum
PDD	Presidential Decision Directive
PLC	Programmable Logic Controller
PNNL	Pacific Northwest National Laboratory
PSTN	Public Switched Telephone Network
R&D	Research and Development
ROI	Return On Investment
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SNL	Sandia National Laboratory
SPP-ICS	System Protection Profile for Industrial Control Systems
TCP	Transmission Control Protocol
US-CERT	U.S. Computer Emergency Readiness Team
WAN	Wide Area Network