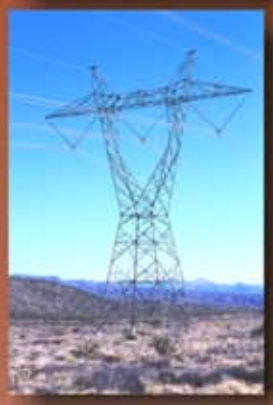
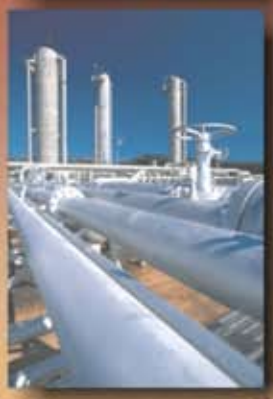
Roadmap to Secure Control Systems in the Energy Sector





Executive Summary

January 2006

Sponsored by
U.S. Department of Energy
U.S. Department of Homeland Security

Prepared by
Energetics Incorporated
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

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

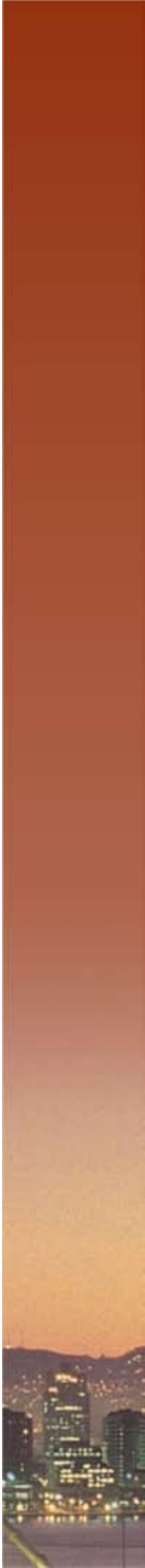
The urgent need to protect our energy control systems from cyber attack has prompted industry and government leaders to step forward and develop an organized strategy for providing that protection. Their efforts have produced this **Roadmap to Secure Control Systems in the Energy Sector**, which presents 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)

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

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

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

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

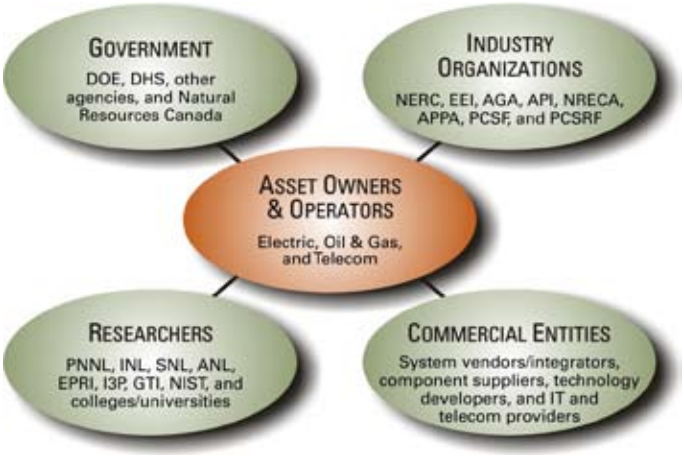
The Challenges Ahead

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.



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.