



# Roadmap to Secure Control Systems in the Energy Sector

## Vision

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

Challenges			
<ul style="list-style-type: none"> <li>■ Limited ability to measure and assess cyber security posture</li> <li>■ No consistent cyber security metrics</li> <li>■ Hard to quantify and demonstrate threats</li> <li>■ Growing risks from increasingly interconnected systems</li> </ul>	<ul style="list-style-type: none"> <li>■ Poorly designed connections of control systems and business networks</li> <li>■ Lack of clear design requirements</li> <li>■ Performance may degrade from security upgrades to legacy systems</li> <li>■ Increasingly sophisticated hacker tools</li> </ul>	<ul style="list-style-type: none"> <li>■ Limited resources to mitigate risk</li> <li>■ Difficult or impossible to integrate new technologies into legacy systems</li> <li>■ Managing change in mission critical systems</li> </ul>	<ul style="list-style-type: none"> <li>■ Insufficient information sharing</li> <li>■ Poor industry-government coordination</li> <li>■ Poor understanding of cyber risks</li> <li>■ Weak business case for cyber security investments</li> </ul>

Goals			
Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion and Implement Response Strategies	Sustain Security Improvements
<b>Milestones</b>			
<b>Near Term (0-2 Years)</b>			
<ul style="list-style-type: none"> <li>■ Baseline security methodologies available, self assessments prepared, and training provided</li> </ul>	<ul style="list-style-type: none"> <li>■ Consistent training materials on cyber and physical security for control system widely available within the energy sector</li> </ul>	<ul style="list-style-type: none"> <li>■ Incident reporting guidelines published and available throughout the energy sector</li> </ul>	<ul style="list-style-type: none"> <li>■ Major info protection and sharing issues resolved between the U.S. government and industry</li> <li>■ Industry-driven awareness campaign launched</li> </ul>



Mid Term (2-5 Years)			
<ul style="list-style-type: none"> <li>■ 50% of asset owners and operators performing self-assessments of their control systems using consistent criteria</li> <li>■ Common metrics available for benchmarking security posture</li> <li>■ 90% of energy sector asset owners conducting internal compliance audits</li> </ul>	<ul style="list-style-type: none"> <li>■ Field-proven best practices for control system security available</li> <li>■ Secure connectivity between business systems and control systems within corporate framework</li> <li>■ Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy</li> </ul>	<ul style="list-style-type: none"> <li>■ Cyber incident response is part of emergency operating plans at 30% of critical control systems</li> <li>■ Commercial products in production that correlate all events across the enterprise network</li> </ul>	<ul style="list-style-type: none"> <li>■ Secure forum for sharing cyber threat and response information</li> <li>■ Compelling, evidence-based business case for investment in control system security</li> <li>■ Undergraduate curricula, grants and internships in control system security</li> <li>■ Effective Federal and state incentives to accelerate investment in secure control system technologies and practices</li> </ul>
Long Term (5-10 Years)			
<ul style="list-style-type: none"> <li>■ Real-time security state monitoring for new and legacy systems commercially available</li> </ul>	<ul style="list-style-type: none"> <li>■ Non-destructive intrusion, isolation, and automated response exercises at 50% of critical control systems</li> <li>■ Security test harness available for evaluating next generation architectures and individual components</li> </ul>	<ul style="list-style-type: none"> <li>■ Control system network models for contingency and remedial action in response to intrusions and anomalies</li> <li>■ Self-configuring control system network architecture in production</li> </ul>	<ul style="list-style-type: none"> <li>■ Cyber security awareness, education, and outreach programs integrated into energy sector operations</li> </ul>
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 architecture 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

16 Chestnut Street · Suite 300  
 Foxborough, MA · USA · 02035  
 T: +1-508-718-6700  
 F: +1-508-718-6701  
 E: [info@industrialdefender.com](mailto:info@industrialdefender.com)  
[www.industrialdefender.com](http://www.industrialdefender.com)