

# Gap Assessment



Siemens Energy is proud to offer a Gap Assessment consultation that leverages Siemens Energy domain expertise to provide comprehensive OT cyber security analysis and industry regulation compliance reporting

Problem	Cause	Solution	Benefit
<ul style="list-style-type: none"> <li>Increasing cyber security threats</li> <li>Regulatory required assessments</li> <li>Security gaps within critical infrastructure</li> <li>Organizations not prepared for the latest NERC-CIP standard version 6 and other standards</li> <li>Customers unsure how to address ongoing regulatory revisions, especially in Supply Chain Management</li> </ul>	<ul style="list-style-type: none"> <li>Regulatory requirements</li> <li>Zero day vulnerabilities, misconfigurations, ever-changing best practices</li> <li>Increased targeting of OT environment by the hacker community</li> </ul>	<ul style="list-style-type: none"> <li>Security Gap Assessment</li> <li>Can be executed against ISO27001, NIST CSF, NERC-CIP, IEC 62443 and other frameworks</li> </ul>	<ul style="list-style-type: none"> <li>Comprehensive view of the organization's existing security posture</li> <li>Expose risks and vulnerabilities in existing infrastructure and practices</li> <li>Leverage results to create ongoing operational policies and procedures to maintain compliance</li> </ul>

What We Deliver?
<ul style="list-style-type: none"> <li>Complete Site walk down of the Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP)</li> <li>Asset Identification and Inventory Documentation (Identification of ESP and PSP)</li> <li>System and software security gap identification</li> <li>Interviews of business staff for security related procedural controls</li> <li>Analysis of the effectiveness of the security policies and procedures</li> <li>Development of the recommended security plans and strategy</li> </ul>

How We Deliver?			
Design	Site Visit	Analysis	Service
<ul style="list-style-type: none"> <li>- Customer kickoff</li> <li>- Document collection and review</li> <li>- Site coordination and logistics</li> </ul>	<ul style="list-style-type: none"> <li>- Plant walk-through and interviews</li> <li>- Evaluation of multiple security controls</li> <li>- Review of DR procedures</li> <li>- Evaluation of firmware, software advisories, malware updates and security patches (samples)</li> </ul>	<ul style="list-style-type: none"> <li>- Gap analysis</li> <li>- Regulatory and standards review</li> <li>- Investment and needs prioritization</li> <li>- High level roadmap development</li> <li>- Cost benefit consideration</li> </ul>	<ul style="list-style-type: none"> <li>- Report readout and workshop</li> <li>- Key gaps and findings</li> <li>- Priority activities</li> <li>- Roadmap discussion</li> <li>- Next steps</li> </ul>