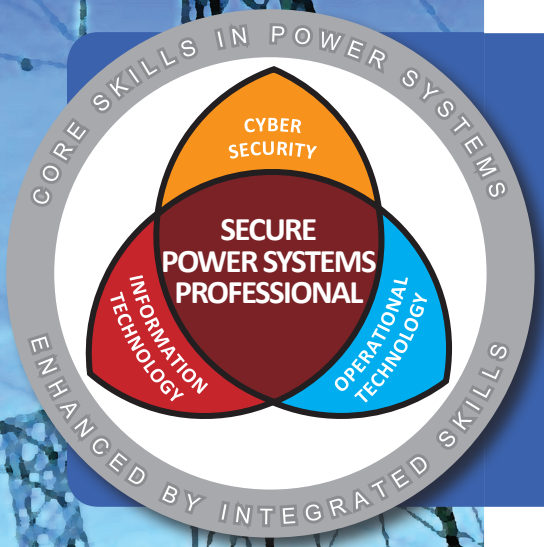
U.S. Department of Energy Secure Power System Professional Project

Guide to Developing Secure Power Systems Professionals

Overview of Emerging Modern Power Systems

Information and communication technologies have become one of the pillars of the electric sector. The emerging smart grid has complex, technology-reliant operations, resulting in a critical need to establish and maintain a viable cybersecurity workforce. As the smart grid matures, this workforce will require continuing education to advance their cybersecurity capabilities.



Secure Power Systems Professionals Job Functions

As this diagram illustrates, the job complexity of Secure Power Systems Professionals (SPSPs) requires core skills in power systems enhanced by integrated skills spanning information technology (IT) and operational technology (OT) with a critical emphasis on cyber security to support the reliable and secure operation of modern power systems.

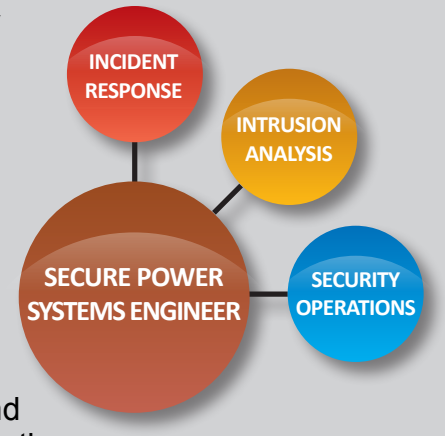
How to Accelerate Development of Secure Power Systems Professionals

- Tap emerging interest from industry to clearly define modern power systems security operations job roles, skills, and competencies—Contact Secure Power Systems Professionals (SPSP) Project Team
- Grow and better align education and training programs with OT/modern power systems application. Hybrid teams need hybrid training; invest in industry training exercise opportunities —See Secure Power Systems Professionals Phase II Report
- Leverage U.S. Department of Energy (DOE)-led investments to identify and apply new methods for assessing OT competency —See Secure Power Systems Professionals Phase III Report

How Are SPSP Skills Acquired?

Experience: Working as power engineers in utilities with experience in

- cyber security
- information security
- IT
- OT
- data management
- smart grid security
- networking and telecommunications
- SCADA protocols



Certification: The SPSP Project examined existing certification programs and identified the following SPSP-specific certifications:

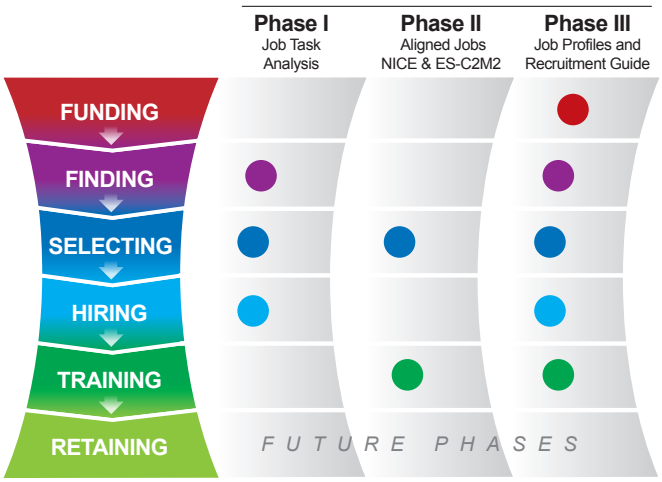
- Certified Ethical Hacker (EC-Council)
- Certified Incident Handler (GIAC)
- Certified Information Security Manager (ISACA)
- Certified Intrusion Analyst (GIAC)
- Certified Information Systems Security Professional (ISC^2)
- Certified SCADA Security Architect (IACRB)
- Control Systems Engineer license (ISA)
- System Operator Certification (NERC)
- Global Industrial Cyber Security Professional (GIAC)

How DOE SPSP Project Contributes to SPSP Workforce Development

This three-phase project identified the following critical junctures in the SPSP workforce development lifecycle:

- justifying **funding** for the position
- **finding** qualified candidates
- **selecting** cyber aware power engineers
- **hiring** qualified staff
- **training** new employees to work within the organization
- **retaining** SPSPs through professional development

Major outcomes and impacts of each phase of the SPSP project are shown in the figure at right.



SPSP Project Meeting Key Secure Power Systems Challenges

Education Resources

- Energy Providers Coalition for Education (EPCE)
- NSA Centers of Academic Excellence Institutions
- IEEE
- SANS ICS
- ICS-CERT
- InfoSec Institute
- CYBATI
- SCADAhacker

Contact

Lori Ross O'Neil
Pacific Northwest National Laboratory
509-375-6702, lro@pnnl.gov

https://www.controlsystemsroadmap.net/efforts/Pages/SPSP.aspx

U.S. DEPARTMENT OF ENERGY | Office of Electricity Delivery and Energy Reliability