

SUPERVISORY CONTROL AND DATA ACQUISITION CONTROLLER SPECIALIST

RESOURCE CATEGORY	Cybersecurity
RESOURCE KIND	Not Specified
OVERALL FUNCTION	
COMPOSITION AND ORDERING SPECIFICATIONS	<ol style="list-style-type: none"> 1. This position can be ordered as a single resource. 2. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment 3. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days

Each type of resource builds on the qualifications of the type below it. For example, Type 1 qualifications include the qualifications in Type 2, plus an increase in capability. Type 1 is the highest qualification level.

COMPONENT	SINGLE TYPE	NOTES
DESCRIPTION	The Supervisory Control and Data Acquisition (SCADA) Controller Specialist provides technical support relating to the operation, repair and restoration of SCADA controllers and associated hardware, firmware and software, including environmental, process, access control, and distribution systems	Not Specified
EDUCATION	Not Specified	Background, education, knowledge and experience reflect that this position aligns better with an engineering position than an Information Technology (IT) position
TRAINING	Completion of the following: <ol style="list-style-type: none"> 1. IS-100: Introduction to Incident Command System, ICS-100 2. IS-200: Incident Command System for Single Resources and Initial Action Incidents 3. IS-700: National Incident Management System, An Introduction 4. IS-800: National Response Framework, An Introduction 5. Training in accordance with Occupational Safety and Health Administration (OSHA), First Responder Awareness level training or equivalent 	Not Specified

Superseded

COMPONENT	SINGLE TYPE	NOTES
EXPERIENCE	<p>Authority Having Jurisdiction (AHJ)-validated knowledge, skills, and abilities demonstrated in the following areas:</p> <ol style="list-style-type: none"> 1. Remote controlled sensors and equipment 2. Human machine interfaces (HMI's) 3. Common two and three wire hardware control buses 4. Front-end servers 5. Physical security 6. Basic electronics 7. Network security architecture concepts, including topology, protocols, components, and principles 8. Physical security practices as they apply to Incident Command System (ICS) and SCADA systems, devices and networks 9. Industry standards and best practices 10. Securing network communications 11. Developing, testing, and implementing network infrastructure contingency and recovery plans 12. Recovering ICS/SCADA networks <p>AHJ-documented and validated experience demonstrated in the following areas:</p> <ol style="list-style-type: none"> 1. Controllers, control systems, and networks 2. Master/central control terminal units 3. Controller boards, sensors, and common bus protocols 4. Programmable logic controllers (PLCs), HMI's, and remote telemetry/terminal units (RTUs) 5. Creating network, data cables, and communication cables 6. Desktop, server, and mainframe operating systems including Windows, Unix, Linux, Mac OS 7. Data Communications diagnostics tools and fault identification techniques 8. Basic physical computer network component and architectures, including the functions of various components and peripherals 9. Configuring and supporting industrial controls and SCADA devices on a data network, including HMI's, PLCs, and RTU's 10. Documenting control systems and networks 11. Control systems design and implementation 12. Mainstream automation (hardware and software) platforms 13. Diagnosing and troubleshooting SCADA issues 14. Tracing network connections and performing technical audits of ICS and SCADA networks 15. Hardening ICS and SCADA networks and updating field devices 	<p>The knowledge, skills, and abilities align with the National Institute of Standards and Technology's National Initiative for Cyber Education (NICE) Workforce Structure.</p>
PHYSICAL/MEDICAL FITNESS	Not Specified	Not Specified
CURRENCY	<ol style="list-style-type: none"> 1. Participates in an exercise, drill, or simulation at least once every year 2. Background checks as applicable law permits and requires 3. Active security clearance 	<p>Provider must carry out and use any background checks as applicable law specifies. This may include a background check completed within past 12 months; sex-offender registry check; and a local, state, and a local, state, and national criminal history.</p>



Position Qualification for Cybersecurity
Cybersecurity

COMPONENT	SINGLE TYPE	NOTES
PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS	Computer Hacking Forensic Investigator Certification	Not Specified

Superseded



Position Qualification for Cybersecurity Cybersecurity

NOTES

Nationally typed resources represent the minimum criteria for the associated category.

REFERENCES

1. U.S. Department of Commerce, National Institute of Standards and Technology, National Initiative for Cybersecurity Education, Cybersecurity Workforce Structure, 2010
2. National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014
3. Occupational Safety and Health Administration (OSHA) 29 Code of Federal Regulations (CFR) Part 1910.120: Hazardous Waste Operations and Emergency Response

Superseded