

## SUPERVISORY CONTROL AND DATA ACQUISITION CONTROLLER SPECIALIST

TYPE	TYPE 1	NO TYPE 2
<b>DESCRIPTION</b>	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 Applicable
<b>CATEGORY</b>	<b>CRITERIA</b>	<b>CRITERIA</b>
<b>EDUCATION</b>	Not Specified	Not Applicable
	<b>NOTES:</b> Background, education, knowledge and experience reflect that this position aligns better with an engineering position than an Information Technology (IT) position	
<b>TRAINING</b>	Completion of the following: 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 Applicable
	<b>NOTES:</b> Not Specified	

Superseded



TYPE	TYPE 1	NO TYPE 2
EXPERIENCE	<p>Authority Having Jurisdiction (AHJ)-validated knowledge, skills, and abilities demonstrated in the following areas:</p> <ol style="list-style-type: none"> <li>1. Remote controlled sensors and equipment</li> <li>2. Human machine interfaces (HMIs)</li> <li>3. Common two and three wire hardware control buses</li> <li>4. Front-end servers</li> <li>5. Physical security</li> <li>6. Basic electronics</li> <li>7. Network security architecture concepts, including topology, protocols, components, and principles</li> <li>8. Physical security practices as they apply to Incident Command System (ICS) and SCADA systems, devices and networks</li> <li>9. Industry standards and best practices</li> <li>10. Securing network communications</li> <li>11. Developing, testing, and implementing network infrastructure contingency and recovery plans</li> <li>12. Recovering ICS/SCADA networks</li> </ol> <p>AHJ-documented and validated experience demonstrated in the following areas:</p> <ol style="list-style-type: none"> <li>1. Controllers, control systems, and networks</li> <li>2. Master/central control terminal units</li> <li>3. Controller boards, sensors, and common bus protocols</li> <li>4. Programmable logic controllers (PLCs), HMIs, and remote telemetry/terminal units (RTUs)</li> <li>5. Creating network, data cables, and communication cables</li> <li>6. Desktop, server, and mainframe operating systems including Windows, Unix, Linux, Mac OS</li> <li>7. Data Communications diagnostics tools and fault identification techniques</li> <li>8. Basic physical computer network component and architectures, including the functions of various components and peripherals</li> <li>9. Configuring and supporting industrial controls and SCADA devices on a data network, including HMIs, PLCs, and RTU's</li> <li>10. Documenting control systems and networks</li> <li>11. Control systems design and implementation</li> <li>12. Mainstream automation (hardware and software) platforms</li> <li>13. Diagnosing and troubleshooting SCADA issues</li> <li>14. Tracing network connections and performing technical audits of ICS and SCADA networks</li> <li>15. Hardening ICS and SCADA networks and updating field devices</li> </ol>	Not Applicable
	<p><b>NOTES:</b> The knowledge, skills, and abilities align with the National Institute of Standards and Technology's National Initiative for Cyber Education (NICE) Workforce Structure.</p>	

Superseded



TYPE	TYPE 1	NO TYPE 2
PHYSICAL/MEDICAL FITNESS	Not Specified	Not Applicable
	NOTES: Not Specified	
CURRENCY	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	Not Applicable
	NOTES: 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.	
PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS	Computer Hacking Forensic Investigator Certification	Not Applicable
	NOTES: Not Specified	

Superseded

## ORDERING SPECIFICATIONS OR DESIGNATIONS

---

1. (X) Can be ordered as an individual asset
2. ( ) Can be ordered in conjunction with a NIMS typed team
3. ( ) Can be ordered in conjunction with a NIMS typed unit
4. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment
5. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days

## 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

## NOTES

---

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

**Superseded**