Operational Technology Systems Analyst

NICE Framework Reference	None.
Functional Description	Responsible for providing advice and ensuring effective cybersecurity within operations technology (OT) contexts (ICS/OCS/SCADA). Works in concert with systems engineers/technologists from different disciplines that are associated to the systems that are managed through OT (e.g. fluid, power, mechanical systems engineers).
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in catastrophic failure of OT and related systems that they are used for management. In many cases, this can have a significant impact on the organizational operations and in some cases can directly result in significant human harm (e.g. in critical infrastructure systems).
Development pathway	Following technical education, often employed in IT or OT systems activities which provide the foundation for more specialized cybersecurity work in the OT environment. Similarly, cybersecurity professionals that normally work in an IT environment, may cross over to OT systems with the benefit of specialized training and education in OT and systems integration.
Other titles	OT security advisor OT security technician Security Analyst - ICS/OCS/SCADA
Related NOCs	2133 Electrical and electronics engineers 2147 Computer engineers (except software engineers and designers) 2171 Information systems analysts and consultants 2241 Electrical and electronics engineering technologists and technicians
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program across the OT environment. ▪ Research and support design of cybersecurity solutions within OT context ▪ Ensure compliance with the changing laws and applicable regulations ▪ Draft, implement, and maintain IT/OT security policies, standards, and procedures. ▪ Monitor and manage cybersecurity requirements and controls across the OT environment ▪ Assess and analyze cybersecurity posture across OT systems and recommend remediation/risk management for vulnerabilities. ▪ Working with other stakeholders, support design and development of security solutions to enable business and technical requirements within the OT environment ▪ Manage the technical integration between IT and OT ▪ Define and maintain tool sets and procedures that support monitoring and management of OT ▪ In concert with other stakeholders, develop cybersecurity incident response plans clearly defining the role of those engaged in management and maintenance of OT systems ▪ Prepare technical reports

<table>
<tr><td></td><td colspan="2">▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to OT</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Bachelor’s degree in computer science, computer engineering or related discipline or equivalent training and experience.</td></tr>
<tr><td>Training</td><td>Specialized training associated with OT cybersecurity as well as system specific tools and techniques required.</td></tr>
<tr><td>Work experience</td><td>Preferred experience for entry level role requires moderate experience 2-3 years working in the OT environment.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Strategic and business plans
▪ Threat and risk assessments
▪ OT Vulnerability management processes and vulnerability assessments
▪ Incident management processes and procedures
▪ Security event and incident management systems and/or incident reporting systems and networks that may be used for OT cybersecurity incidents,
▪ Cybersecurity risk management processes & policies
▪ Privacy and security legislation
▪ Organizational security infrastructure and reporting systems
▪ OT security tools, techniques and procedures</td></tr>
<tr><td>Competencies</td><td colspan="2">Appreciating that not all OT analysts will necessarily have an IT background, the following basic application of the following KSAs are relevant:

☐ Telemetry systems, data communications, data acquisition and process control
☐ Operating systems, networking, and communications systems concepts
☐ Electrical distribution networks, power system equipment, transformer station operation and electrical theory
☐ Computer and networking troubleshooting and maintenance procedures
☐ Network administration principles and practices
☐ System life cycle management principles, including software security and usability
☐ Database management systems and applications;
☐ Database administration and optimization
☐ System testing and evaluation methodologies and processes
☐ Measures or indicators of system performance, availability, capacity, or configuration problems
☐ Analysis tools and network protocols
☐ Diagnostic tools and fault identification techniques

Advanced application of the following KSAs:

☐ OT systems software and hardware, programmable logic controllers, and digital and analog relaying;
☐ Threat and risk assessment to internet connected OT (including implications and assessment of IoT devices)</td></tr>
</table>

	☐ Legal and compliance requirements including organizational responsibilities for workplace and public safety related to OT/ production ☐ Industry standards and best practices, especially related to industrial environments in the cybersecurity space ☐ Cybersecurity program management, measures and monitoring Control systems – applicable to industry/production environments ☐ IT/OT integration and convergence ☐ Process safety and hazard analysis ☐ Systems analysis and integration ☐ Problem-solving in complex systems environments ☐ Technical communications including report writing to address cross- disciplinary technical issues
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks and specifically those that relate to OT and remote operation and access. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and remote monitoring and operations through IoT and devices. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to OT requirements, procedures, and policies. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. For encryption within OT systems, this will require knowledge and skills related to implementing a quantum safe strategy within the organization.