

Control Systems Analyst I/II Flex Advancement.

1. Training, Complete the Following:

a. Rockwell Automation Technologies:

- i. Level 1 Training: **Instructor Led or E-Learning** (CCP146(-EL) or (CCP299) or **Previous Experience**
- ii. Level 2 Training: **Instructor Led or E-Learning**(CCP151(-EL) or CCP153(-EL))
- iii. Level 3 Training: **Instructor Led or E-Learning** (CCP143(-EL))
- iv. Level 4 Training: **Instructor Led or E-Learning** (CCP152(-EL))
- v. PlantPAx System Design and Configuration: : **Instructor Led or E-Learning** (PRC201(-EL))
- vi. Factory Talk View: **Instructor Led or E-Learning** (CCV207(-EL))

b. Schneider Electric Automation Technologies:

- i. 9001 EcoStructure Control Expert (formerly Unity Pro): **Instructor Led Training or Virtual Instructor Led**

c. Aveva Wonderware

- i. Application Server 2014 R2 Rev C
<https://industrialtraining.aveva.com/global/portal/catalog.cfm?fuseaction=coursedetails&calendarID=183&courseContentID=16955>
- ii. InTouch for System Platform 2014 R2 Rev C
<https://industrialtraining.aveva.com/global/portal/catalog.cfm?fuseaction=coursedetails&calendarID=183&courseContentID=15088>

d. Aveva PI System

- i. PI System Basics (**self-paced, on-demand**)
- ii. PI System Administration (**self-paced, on-demand**)
- iii. PI Vision Basics (**self-paced, on-demand**)
- iv. PI DataLink Basics (**self-paced, on-demand**)
- v. Asset Framework Basics (**self-paced, on-demand**)

e. Cybersecurity

- i. **Complete 10 hours of Industrial Control System (ICS) Cybersecurity Training.** Any combination of virtual or instructor lead training offered by the Cybersecurity & Infrastructure Security Agency (CISA) or courses approved by your supervisor. Complete the test at the end of each lesson and submit the certificate to your supervisor.

1. CISA Virtual Learning Portal

- a. Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- b. Differences in Deployments of ICS (210W-1) – 1.5 hours

- c. Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- d. Common ICS Components (210W-3) – 1.5 hours
- e. Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- f. Cybersecurity Risk (210W-5) – 1.5 hours
- g. Current Trends (Threat) (210W-6) – 1.5 hours
- h. Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- i. Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- j. Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- k. Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- l. Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- m. Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

2. Instructor-Led Training

- a. Introduction to Control Systems Cybersecurity (101) - 4 hrs
- b. Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
- c. Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
- d. ICS Cybersecurity (301V)
- e. ICS Cybersecurity (301L) - 4 days
- f. ICS Evaluation (401) - 5 days
- g. ICS Evaluation (401V)

2. Experience.

- a. Two years of experience as a Control Systems Analyst I (a bachelor's degree or higher in Electrical Engineering, Computer Science, Information Systems, or related field may be used to satisfy this requirement)
- b. An equivalent of 5 years experience in the ICS / SCADA field, including work experience from previous employers.

Notes:

1. Training from a previous employer may be used to satisfy one or more of the subjects listed above, provided that the training is equivalent, and documentation of successful completion is provided.
2. Local distributor training is provided at various times throughout the year. Some courses are offered at low or no cost. Check with the distributor (Royal Industrial Solutions, Graybar Electric, Wonderware California) for dates offered.
3. Self-paced training can be taken at any time using Agency equipment and software.
4. Where a listed course is not available, substitutions may be made if approved by the department manager.