Chelan PUD Control System Engineer Level Guide

	Control Systems Engineer I	Control Systems Engineer II	Control Systems Engineer III	Control Systems Engineer IV
Essential Functions	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will work primarily on low risk and low complexity work assignments. Must be available to respond to call-outs 24x7x365	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will work primarily on low-moderate risk and low-moderately complex work assignments. Must be available to respond to call-outs 24x7x365	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will work primarily on moderate-high risk and moderately-highly complex work assignments. Must be available to respond to call-outs 24x7x365	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will primarily work on the highest risk, broadest scope and most complex work assignments. Must be available to respond to call-outs 24x7x365
SCADA (EMS/GMS)	Learn about and perform work under close supervision on systems with a low level of risk to operational compliance, revenue stream, equipment and human safety, including: • Implement, document and maintain the following for systems including Distribution, Generation, Hatcheries, Water/Wastewater and Compliance: o Read-only Human Machine Interfaces o Communication topology using Ethernet o Work practices • Provide Control Room Operators, Energy Planning & Trading, Outage Coordinators, Engineers and Project teams with the following: o Procedures that enhance system reliability and departmental/ organizational efficiencies o Engineering analysis and technical support to ensure continuing reliable operations of the electric power grid and District services • Provide integration and interoperability for small-scale systems • Maintain servers and workstations and associated hardware throughout its lifespan • Configure 1 or more operating systems • Research new display and tool technologies • Serve as a contributor to the development strategy for the tools and applications needed by District Operations and Planning	Perform work under general supervision on networked systems with a low-moderate level of risk to operational compliance, revenue stream, equipment and human safety, including: • Implement, document and maintain the following for systems including Transmission, Distribution, Generation, Hatcheries, Water/Wastewater, Security and Compliance: o Interactive Human Machine Interfaces, automation interfaces and database structures for 1 or more systems o Communication topology using serial and Ethernet o Code for control automation, calculations, generation and energy management o Change Management o Work Practices o Historical data storage o Tools and procedures to monitor and control 2 or more systems • Provide Control Room Operators, Energy Planning & Trading, Outage Coordinators, Engineers and Project teams with the following: o Analysis and visualization of data needed to maintain the reliability of District control system operations o Development and prototyping of operational awareness and analytical tools o Development tools, processes and procedures that enhance	Perform work on advanced, networked systems with a moderate-high level of risk to operational compliance, revenue stream, equipment and human safety, including: • Design, develop, implement, document and maintain the following for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Mid-Columbia Hourly Coordination, Security and Compliance: o Interactive Human Machine Interfaces with embedded custom code, automation interfaces, and database structures that control 2 or more systems o Single-order control system models o Interconnected system architecture for 3 or more systems o Communication topology using serial, fiber and Ethernet o Code for control automation, calculations, generation and energy management, contract compliance (water rights, reliability, environment requirements), energy accounting, database management, fish ladder control o Change Management o Work Practices o Historical data storage and maintenance for critical utility information	Perform work on highly complex, interconnected, interdependent systems with the highest levels of risk to operational compliance, revenue stream, equipment and human safety, including: • Design, develop, implement, document and maintain the following for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Mid-Columbia Hourly Coordination, Security and Compliance: o Interactive Human Machine Interfaces with embedded custom code using custom data structures, automation interfaces, and database structures that control 3 or more systems o Multi-order control system models o Interconnected system architecture for 4 or more systems o Communication topology using serial, microwave, fiber and Ethernet o Code for Mid-C coordination, slice and encroachment contracts, control and process automation, advanced calculations, generation, water and energy management, contract compliance (water rights, reliability, environment requirements), energy accounting, custom communication protocols, custom

Chelan PUD Control System Engineer Level Guide

	• Provide documentation for the development of training and training material • Maintain asset information for assets critical to the reliability of the grid using Maximo, Primavera and other tools • Attend industry meetings, discussions and forums pertinent to CSE areas of responsibility	system reliability and departmental efficiencies o Engineering analysis and technical support to ensure continuing reliable operations of the electric power grid and District services. o Documentation and guidance needed by Project teams in order to deploy new tools • Maintain servers and workstations and associated hardware throughout its lifespan • Configure and manage 2 or more operating systems • Serve as the Subject Matter Expert for 1 or more system performance standards and contributes to the development strategy for the tools and applications needed by District Operations and Planning • Act as mentor and advisor to less experienced engineers • Maintain asset information for assets critical to the reliability of the grid using Maximo, Primavera and other tools • Maintain knowledge of emerging trends and industry best practices • Represent the District in industry meetings, discussions and forums pertinent to CSE areas of responsibility	o Tools and procedures to monitor and control 3 or more systems • Provide Control Room Operators, Energy Planning & Trading, Outage Coordinators, Engineers and Project teams with the following: o Analysis and visualization of data needed to maintain the reliability of District control system operations o Development and prototyping of operational awareness and analytical tools o Development tools, processes and procedures that enhance system reliability and departmental/organizational efficiencies o Engineering analysis and technical support to ensure continuing reliable operations of the electric power grid and District services. o Documentation and guidance needed by Project teams in order to deploy new tools • Provide integration and interoperability for 3 or more systems • Analyze operational data to develop solutions for current and future system issues and report findings and recommendations • Purchase, implement, document and maintain servers, workstations, network equipment and associated hardware throughout its lifespan • Configure and manage 3 or more operating systems • Develop vendor applications through changes in software, processes and training • Develop test scripts and test the functionality of tools developed • Investigation, evaluation, and bench-marking of new display and tool technologies	interfaces, database management, river control, fish ladder control o Change management o Work Practices o Historical data storage, maintenance, and optimization for critical utility information o Tools and procedures to monitor and control 4 or more systems • Provide Control Room Operators, Energy Planning & Trading, Outage Coordinators, Engineers and Project teams with the following: o Analysis and visualization of data needed to maintain the reliability of District control system operations o Development and prototyping of operational awareness and analytical tools o Development of operational impact assessment studies and mitigation plans o Development tools, processes and procedures that enhance system reliability and departmental/organizational efficiencies o Engineering analysis and technical support to ensure continuing reliable operations of the electric power grid and District services o Documentation and guidance needed by Project teams in order to deploy new tools • Provide integration and interoperability for 4 or more systems • Analyze operational data to develop solutions for current and future system issues and report findings and recommendations • Purchase, implement, document and maintain servers, workstations, network equipment, appliances and associated hardware throughout its lifespan

			• Serve as the Subject Matter Expert for 2 or more system performance standards and contributes to the development strategy for the tools and applications needed by District Operations and Planning • Provide documentation and guidance for the development of training and training material • Act as mentor and advisor to less experienced engineers • Maintain asset information for assets critical to the reliability of the grid using Maximo, Primavera and other tools • Maintain knowledge of emerging trends and industry best practices • Represent the District in industry meetings, discussions and forums pertinent to CSE areas of responsibility	• Configure and manage 4 or more operating systems • Develop vendor applications to their fullest extent through changes in software, processes and training • Develop test scripts and test the functionality of tools developed • Investigation, evaluation, bench-marking and implementation of new display and tool technologies • Serve as the Subject Matter Expert for 3 or more system performance standards and contributes to the development strategy for the tools and applications needed by District Operations and Planning • Provide documentation and guidance for the development of training and training material • Act as mentor and advisor to less experienced engineers • Maintain asset information for assets critical to the reliability of the grid using Maximo, Primavera and other tools • Maintain knowledge of emerging trends and industry best practices • Represent the District in industry meetings, discussions and forums pertinent to CSE areas of responsibility
Cyber Security	Learn about and perform work under close supervision on systems with a low level of risk to operations, regulatory compliance and company reputation, including: • Provide support to internal teams to define and develop secure architecture and solutions for projects • Prepare and maintain technical user guides, System Operating Procedures, security architecture documentation and diagrams • Participate in project meetings • Monitor alerts and logs • Maintain security tools and technologies, including:	Perform work under general supervision on networked systems with a low-moderate level of risk to operations, regulatory compliance and company reputation, including: • Provide support to internal teams to define and develop secure architecture and solutions for projects, conduct discovery sessions to gain the necessary background and review findings to ensure sustained compliance • Assist with the assessment and documentation of the design of secure solutions • Assist with the implementation of technical security solution policies in alignment with	Perform work on advanced, networked systems with a moderate-high level of risk to operations, regulatory compliance and company reputation, including: • Define and develop secure architecture and solutions for projects, conduct discovery sessions to gain the necessary background and review findings to ensure sustained compliance, remediation of control gaps and escalation of possible critical issues • Guide, assess and document design of secure solutions • Implementation of technical security solution policies in alignment with	Perform work on highly complex, interconnected, interdependent systems with the highest levels of risk to operations, regulatory compliance and company reputation, including: • Define, develop, and implement secure architecture and solutions for projects, conduct discovery sessions to gain the necessary background and review findings to ensure sustained compliance, remediation of control gaps and escalation of possible critical issues • Guide, assess, implement and document design of secure solutions • Architect and direct implementation of

	o Logging o Anti-Virus/Malware Detection o Configuration management • Support security-focused tools and services • Participate in cyber security incident response plan tests	business risk • Prepare and maintain technical user guides, System Operating Procedures, security architecture documentation and diagrams • Participate in project meetings and provide recommendations and strategies for ensuring remediation of gaps and deficiencies as projects develop • Monitor alerts and logs • Maintain security tools and technologies, including: o Logging and monitoring o Data restoration o Anti-Virus/Malware Detection o Software and security updates o Configuration management o Asset management/Baseline monitoring • Maintain established security requirements • Implement defense in depth controls to mitigate risk • Provide technical review of standardized District security framework • Implement, support and evaluate security-focused tools and services • Conduct and participate in cyber security incident response plan tests • Assist with third-party penetration tests • Evaluate and recommend new and emerging security products and technologies	business risk • Prepare and maintain technical user guides, System Operating Procedures, security architecture documentation and diagrams • Participate in project meetings and provide recommendations and strategies for ensuring remediation of gaps and deficiencies as projects develop • Monitor alerts and logs • Continuously audit security controls • Perform Security Risk Assessments, identify security issues and risks, and develop mitigation plans • Develop, implement and maintain security tools and technologies, including: o Security Information and Event Management (SIEM) o Multi-factor authentication o Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) o Logging, alerting and monitoring o Data retention and restoration o Anti-Virus/Malware Detection o Software and security updates o Configuration management o Asset management/Baseline monitoring o System hardening o Network Access Control (NAC) o Least access privilege implementation o Vulnerability assessments • Implement and maintain security requirements • Develop and implement defense in depth controls to mitigate risk • Provide technical review of standardized District security framework • Develop, implement, support and evaluate security-focused tools and services • Conduct and participate in cyber security incident response plan tests • Coordinate third-party penetration tests • Define network standards for IPS/IDS and	technical security solution policies in alignment with business risk • Design, create and maintain technical user guides, System Operating Procedures, security architecture documentation and diagrams • Participate in project meetings and provide recommendations and strategies for ensuring remediation of gaps and deficiencies as projects develop • Monitor alerts and logs • Continuously audit security policies and controls • Perform Security Risk Assessments, identify security issues and risks, design and develop mitigation plans • Design, develop, implement and maintain security tools and technologies, including: o Security Information and Event Management (SIEM) o Multi-factor authentication o Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) o Logging, alerting and monitoring o Data retention and restoration o Anti-Virus/Malware Detection o Software and security updates o Configuration management o Asset management/Baseline monitoring o System hardening o Network Access Control (NAC) o Least access privilege implementation o Vulnerability assessments • Analyze and validate established security requirements and recommend additional security requirements and safeguards • Design, develop and implement defense in depth controls to mitigate risk • Provide technical review of and implement standardized District security framework • Design, develop, implement, support and evaluate security-focused tools and services

			authentication and authorization controls • Evaluate and recommend new and emerging security products and technologies	• Conduct and participate in cyber security incident response plan tests • Coordinate third-party penetration tests • Define and implement network standards for IPS/IDS and authentication and authorization controls • Evaluate, recommend and implement new and emerging security products and technologies
Reliability Compliance	Learn about and perform work under close supervision on systems with a low level of risk to regulatory compliance, including: • Maintain Program Documentation and perform applicable processes in order to meet NERC CIP requirements • Provide support for internal and external audits including: o Annual self-certifications o Peer review • Act as a Contributor to NERC CIP Standards • Research regulations by reviewing regulatory bulletins and other sources of information • Prepare reports by collecting, analyzing and summarizing information • Attend compliance working groups, forums and related industry events • Document and maintain technical tools and security controls required to meet compliance objectives identified in the program documentation	Perform work under general supervision on systems with a low-moderate level of risk to regulatory compliance, including: • Create and maintain Program Documentation and perform applicable processes in order to meet NERC CIP requirements • Provide support for internal and external audits including: o Annual self-certifications o Standards peer review o Reliability Standard Audit Worksheets maintenance • Contribute to the evaluation of NERC Alerts • Implement mitigation actions to resolve potential compliance concerns • Create work orders for other work groups to address NERC CIP-related requirements • Act as a Standard Owner, Subject Matter Expert or Contributor to NERC CIP Standards • Research regulations by reviewing regulatory bulletins and other sources of information • Prepare reports by collecting, analyzing, and summarizing information • Attend compliance working groups, forums and related industry events • Implement, document and maintain technical tools and security controls required to meet compliance objectives identified in the program documentation	Perform work on advanced networked systems with a moderate-high level of risk to regulatory compliance and company reputation, including: • Create and maintain Program Documentation and perform applicable processes in order to meet NERC CIP requirements • Provide support for internal and external audits including: o Annual self-certifications o Standards peer review o Reliability Standard Audit Worksheets development and maintenance o Audit interviews • Evaluate NERC Alerts • Develop and implement mitigation actions to resolve potential compliance concerns • Create work orders for other work groups to address NERC CIP-related requirements • Act as a Standard Owner, Subject Matter Expert and Contributor to NERC CIP Standards • Research regulations by reviewing regulatory bulletins and other sources of information • Prepare reports by collecting, analyzing, and summarizing information • Attend compliance working groups, forums and related industry events • Develop, implement, document and maintain technical tools and security controls required to meet compliance objectives identified in the program documentation	Perform work on highly complex, interconnected, interdependent systems with the highest levels of risk to regulatory compliance and company reputation, including: • Create, maintain, and optimize Program Documentation and perform applicable processes in order to meet NERC CIP requirements • Provide support for internal and external audits including: o Annual self-certifications o Standards peer review o Reliability Standard Audit Worksheets development and maintenance o Audit interviews • Evaluate and respond to NERC Alerts • Design, develop and implement mitigation actions to resolve potential compliance concerns • Create work orders for other work groups to address NERC CIP-related requirements • Act as a Standard Owner, Subject Matter Expert and Contributor to NERC CIP Standards, including those that may include other groups in the District • Research regulations by reviewing regulatory bulletins and other sources of information • Prepare reports by collecting, analyzing, and summarizing information • Represent the District at compliance working groups, forums and related industry events • Design, develop, implement, document and maintain technical tools and security

Chelan PUD Control System Engineer Level Guide

				controls required to meet compliance objectives identified in the program documentation
Project Management	Learn about and perform work under close supervision on projects with a low level of risk to operations and revenue stream, including: • Work with others in EMS group to provide tasks and time estimates for projects requiring CSE time • Technical resource for project teams assigned to implementing or modifying District control systems • Participate in technical meetings associated with project work that impacts SCADA design	Perform work under general supervision on projects with a low-moderate level of risk to operations and revenue stream, including: • Lead small project teams that may include consultants, contractors, legal, procurement, and other District departments • Work with others in EMS group to provide tasks and time estimates for projects requiring CSE time • Technical resource for project teams assigned to implementing or modifying District control systems • Organize technical meetings associated with project work that impacts SCADA design	Perform work on advanced projects with a moderate-high level of risk to operations and revenue stream, including: • Lead multi-disciplinary project teams that may include consultants, contractors, legal, procurement, and other District departments • Work with District Project Managers to provide tasks and time estimates for projects requiring CSE time • Technical resource for project teams assigned to designing, implementing or modifying District control systems • Perform project intake processes to add project work to DWP • Organize technical meetings associated with project work that impacts SCADA/EMS design	Perform work on highly complex, multi-system projects with the highest levels of risk to operations and revenue stream, including: • Perform project management activities including schedule, budget and execution for complex projects • Lead multi-disciplinary and multi-functional teams that may include consultants, contractors, legal, procurement, and other District departments • Work with Contractor, Vendor and District Project Managers to provide tasks and time estimates for projects requiring CSE time • Technical resource for project teams assigned to designing, implementing or modifying District control systems and similar or related systems • Perform project intake processes to add project work to DWP • Organize technical meetings associated with project work that impacts SCADA/EMS design
Education	• BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field.	• BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field.	• BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field.	• BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field. Master's Degree preferred.
Experience	• Entry level. No experience required.	• Typically requires two (2) years of experience performing as a Level I or closely related experience. • Candidates with a Master's degree who also have at least 6 months experience in the Utility industry working with SCADA systems may be hired as a Level II.	• Typically requires three (3) years of experience performing as a Level II, or a total of five (5) years progressively responsible experience with Control System Engineering. • Candidates with a Master's Degree may reduce total experience by 2 years.	• Master's Degree preferred. • Typically requires three (3) years of experience performing as a Level III or a total of eight (8) years progressively responsible experience with Control System engineering. • Candidates with a Master's Degree may reduce total experience by 2 years.
Knowledge	• Engineering and Industrial Control Systems security principles and practices • Control systems theory • Computer programming in 1 or more object-oriented or script language • Data communications protocols and computer operating systems	• Industrial control systems design, selection and specification of equipment and design of industrial communication and control networks for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Security and	• Industrial control systems design, selection and specification of equipment and design of industrial communication and control networks for systems including Transmission, Distribution, Generation, Hatcheries, Water/Wastewater, Mid-Columbia Hourly Coordination, Security	• Industrial control systems design, selection and specification of equipment and design of industrial communication and control networks for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Mid-Columbia Hourly

	• Mathematical concepts such as scaling, conversions and raising to a power, logic ops (AND/OR/XOR) • Open-loop and closed-loop control theory algorithms for linear systems	Compliance • Engineering and Industrial Control Systems security principles and practices • Distributed control (DCS), host centric (SCADA) and Embedded System environments utilizing 1 or more computing platforms, PLCs and RTUs • Control systems theory and its practical application to process control and field instrumentation • Computer programming in 2 or more languages, preferably one object-oriented and one script language • Control protocols including DNP and Allen-Bradley • Data communications protocols, networking equipment and computer operating systems • Operating system hardening, configuration, troubleshooting and maintenance techniques • Automation, system and communications integration methodologies • Power generation for hydro unit operation • Regulatory laws, standards and requirements including NERC CIP Reliability Standards • Complex spreadsheets and database applications • Basic knowledge of project management concepts, principles and practices	and Compliance • Engineering and Industrial Control Systems security principles and practices • Distributed control (DCS), host centric (SCADA) and Embedded System environments utilizing 2 or more computing platforms, PLCs and RTUs • Control systems theory and its practical application to process control and field instrumentation • Computer programming in 3 or more languages, preferably a combination of object-oriented and script languages • Control protocols including DNP, OPC, Allen-Bradley and MODBUS • Data communications protocols, networking equipment and computer operating systems • Operating system hardening, configuration, troubleshooting and maintenance techniques • Automation, system and communications integration methodologies • Mid-Columbia control and hourly coordination • Power generation for hydro unit operation • Energy accounting • Regulatory laws, standards and requirements including FERC/ NERC Reliability Standards • Complex spreadsheets and database applications • Project management concepts, principles and practices	Coordination, Security and Compliance • Engineering and Industrial Control Systems security principles and practices • Distributed control (DCS), host centric (SCADA) and Embedded System environments utilizing 3 or more computing platforms, PLCs and RTUs • Control systems theory and its practical application to process control and field instrumentation • Computer programming in 4 or more languages, preferably a combination of object-oriented and script languages • Control protocols including DNP, OPC, ICCP, Allen-Bradley, L&G 8979 and MODBUS • Data communications protocols, networking equipment and computer operating systems • Operating system hardening, configuration, troubleshooting, maintenance, and optimization techniques • Automation, system and communications integration methodologies • Mid-Columbia control and hourly coordination • Power generation for hydro unit operation • Energy accounting • Regulatory laws, standards and requirements including FERC/ NERC Reliability Standards • Complex spreadsheets and database applications • Project management concepts, principles and practices
Systems & Technical Skills	• Work with a field support team to diagnose issues.	• Collect, process, preserve, analyze, and present computer-related evidence in support of network vulnerability mitigation, counterintelligence or law enforcement investigations. • Work with a field support team to diagnose issues and propose resolution • Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Use mitigation, preparedness, and response	• Vulnerability Assessment and Management - Conduct assessments of threats and vulnerabilities. Determine deviations from acceptable configurations, enterprise or local policy. Assess the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations. • Synthesize and place intelligence information in context; draws insights	• Analyze threat information from multiple sources, disciplines, and agencies across the Intelligence Community. • Vulnerability Assessment and Management - Conduct assessments of threats and vulnerabilities. Determine deviations from acceptable configurations, enterprise or local policy. Assess the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational

		and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities. • Participates as a reviewer in technical reviews	about the possible implications. • Collect, process and preserve computer-related evidence in support of network vulnerability mitigation, counterintelligence or law enforcement investigations. • Work with a field support team to diagnose issues and propose resolution • Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities. • Participates as a reviewer in technical reviews	situations. • Use defensive measures and data from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. • Synthesize and place intelligence information in context; draws insights about the possible implications. • Collect, process, preserve, analyze, and present computer-related evidence in support of network vulnerability mitigation, counterintelligence or law enforcement investigations. • Work with a field support team to diagnose issues and propose resolution • Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities. • Participates as a reviewer in technical reviews
Other Skills	• Strong reasoning, analytical and problem solving skills • Data analysis and research • Communicate logically and clearly, both orally and in writing • Communicate technical information effectively to non-department and non-technical staff • Technical writing	• Strong reasoning, analytical and problem solving skills • Data analysis, research and report development • Communicate logically and clearly, both orally and in writing • Interpret engineering problems and solutions and communicate technical information effectively to non-department and non-technical staff • Technical writing • Estimates project cost and schedule • Actively look ahead to plan for and respond to project challenges • Contribute to the development of department policies, procedures, and standards.	• Strong reasoning, analytical and problem solving skills • Data extraction, data analysis, research and report development • Understand contract documents • Communicate logically and clearly, both orally and in writing • Interpret engineering problems and solutions and communicate technical information effectively to non-department and non-technical staff • Technical writing • Estimates project cost and schedule • Seek long term benefits to the overall project when determining system and control design approach • Actively look ahead to plan for and respond to project challenges	• Strong reasoning, analytical and problem solving skills • Data extraction, data analysis, research and report development • Understand, interpret and contribute to the development of contract documents • Communicate logically and clearly, both orally and in writing • Interpret engineering problems and solutions and communicate technical information effectively to non-department and non-technical staff • Technical writing • Estimates project cost and schedule • Aware of the "business" of control engineering as well as the technical design issues • Seek long term benefits to the overall

Chelan PUD Control System Engineer Level Guide

			• Reviews company policies and industry practices, and develops and implements procedures, and standards.	project when determining system and control design approach • Actively look ahead to plan for and respond to project challenges • Reviews company policies and industry practices, and develops and implements procedures, and standards.
Systems & Technical Abilities	• Learn new computer systems from documentation and training • Diagnose problems to isolate cause • Maintain, troubleshoot and modify program HMI components • Analyze programming, observe monitoring signals, troubleshoot systems • Think beyond past approaches and propose practical approaches to control design • Follow test plans for Security Controls and Automation • Apply the principles of software management to organize and maintain software integrity • Act as a Contributor for assigned SCADA and associated supporting systems	• Learn new computer systems from documentation and training • Act as a Subject Matter Expert for 2 or more SCADA, Compliance and associated supporting systems • Diagnose problems to isolate cause • Maintain, troubleshoot and modify program HMI components • Analyze programming, observe monitoring signals, troubleshoot systems • Think beyond past approaches and propose practical approaches to control design • Identify solutions of low complexity by analyzing data, evaluating alternatives and recommending an appropriate course of action • Write clear system requirements and test plans for Security Controls and Automation • Apply the principles of software management to organize and maintain software integrity • Apply mathematical concepts such as scaling, conversions, raising to a power and logic ops (AND/OR/XOR) • Apply open-loop and closed-loop control theory algorithms for linear systems • Carry out complex technical tasks	• Learn new computer systems from documentation and training • Act as a Subject Matter Expert for 3 or more SCADA, Compliance and associated supporting systems • Diagnose problems to isolate cause • Maintain, troubleshoot and modify program HMI components • Analyze programming, observe monitoring signals, troubleshoot systems • Think beyond past approaches to propose and implement practical approaches to control design • Identify solutions of moderate complexity by analyzing data, evaluating alternatives and recommending an appropriate course of action • Apply technical knowledge of legacy systems to design new functionality • Write clear system requirements and test plans for Security Controls and Automation • Apply the principles of software management to organize and maintain software integrity • Apply mathematical concepts such as scaling, conversions, raising to a power, logic ops (AND/OR/XOR), integration, and totalization • Apply open-loop, closed-loop, time-weighted, and weighted-sum control theory algorithms for linear systems • Act as a Subject Matter Expert as it relates to cyber security in industrial control systems • Carry out highly complex technical tasks	• Learn new computer systems from documentation and training • Act as a Subject Matter Expert for 4 or more SCADA, Compliance and associated supporting systems • Diagnose problems to isolate cause • Maintain, troubleshoot and modify program HMI components • Analyze programming, observe monitoring signals, troubleshoot systems • Think beyond past approaches to propose and implement practical approaches to control design • Identify solutions of high complexity by analyzing data, evaluating alternatives and recommending an appropriate course of action • Apply technical knowledge of legacy systems to design new functionality • Write clear system requirements and test plans for Security Controls and Automation • Apply the principles of software management to organize and maintain software integrity • Apply mathematical concepts such as scaling, conversions, raising to a power, logic ops (AND/OR/XOR), integration, totalization, linear fit approximation and extrapolation • Design and apply open-loop, closed-loop, time-weighted, and weighted-sum control theory algorithms for linear and non-linear systems • Provide technical direction and act as a Subject Matter Expert as it relates to cyber security in industrial control systems

				• Carry out highly complex technical tasks
Other Abilities	• Identify, research and gather relevant information from a variety of sources • Meet deadlines on multiple simultaneous priorities for multiple stakeholders • Respond to after-hours call-outs • Attend industry meetings and conferences, which may involve travel • Contribute training material to other engineers and dedicated District training professional staff • Clearly communicate technical information to end users and stakeholders	• Identify, research and gather relevant information from a variety of sources • Meet deadlines on multiple simultaneous priorities for multiple stakeholders • Respond to after-hours call-outs • Represent District at industry meetings and conferences, which may involve travel • Train other engineers and dedicated District training professional staff • Clearly communicate technical information to end users and stakeholders	• Identify, research and gather relevant information from a variety of sources • Meet deadlines on multiple simultaneous priorities for multiple stakeholders • Respond to after-hours call-outs • Represent District at industry meetings and conferences, which may involve travel • Train other engineers and dedicated District training professional staff • Clearly communicate technical information to end users and stakeholders	• Identify, research and gather relevant information from a variety of sources • Meet deadlines on multiple simultaneous priorities for multiple stakeholders • Respond to after-hours call-outs • Represent District at industry meetings and conferences, which may involve travel • Train other engineers and dedicated District training professional staff • Clearly communicate technical information to end users and stakeholders
Leadership	• None	• None	• Mentor lower level engineers	• Train and mentor lower level engineers and provide effective feedback
Decision making	• Works to achieve established goals under close supervision • Consults supervisor or lead when problems occur • Regularly provides work status updates to the responsible lead	• Works to achieve established goals under general supervision • Consults supervisor or lead when problems occur • Regularly provides work status updates to the responsible lead • Work is reviewed by senior engineers for application of sound engineering judgment	• Informs lead or supervisor of unusual, complex, difficult or controversial problems • Performs moderately complex assignments under limited supervision • Regularly provides work status updates to the responsible lead • Required to make decisions that will affect project objectives • Exercise sound and independent judgment, conduct independent analyses and make recommendations on difficult and sensitive issues	• Informs lead or supervisor of unusual, complex, difficult or controversial problems and is expected to propose and be able to implement effective solutions • Independently performs complex and high priority assignments with limited supervision and guidance regarding overall objectives, critical issues, priorities and policy matters • Regularly provides work status updates to the responsible lead • Required to make decisions that give direction to project teams and significantly affect project outcomes • Exercise sound and independent judgment, conduct independent analyses and make recommendations on difficult and sensitive issues
Complexity	• Requires basic knowledge of Industrial Control Systems principles, practices and engineering theory • Work on systems is limited to assignments with little to no impacts on worker safety and asset operations	• Working knowledge of Industrial Control Systems principles, practices and engineering theory • Work on systems has limited impact on worker safety and asset operations	• Intermediate knowledge of Industrial Control Systems principles, practices and engineering theory • Basic knowledge of other functions across the District • Work assignments have moderate impacts on worker safety and asset operations	• Expert knowledge of Industrial Control Systems principles, practices and engineering theory • Working knowledge of other engineering disciplines across the District • Work assignments have significant impacts on worker safety and asset operations
Career Path/Advancement	This is the entry-level position within the Control Systems Engineering Job Family.	This is the second level position within the Control Systems Engineering Job Family.	This is the third level position within the Control Systems Engineering Job Family.	This is the highest level individual contributor (non-leadership) position within the Control Systems Engineering Job Family.

Chelan PUD Control System Engineer Level Guide

	To advance to Level II, incumbents must be able to perform all the essential functions of the higher level position, at a basic level. Advancement is subject to approval of the business need for a higher level position and salary budget availability. Employees in Level I are expected to advance to Level II within a reasonable time frame. The typical timeline for advancement is 2 years from entry into the Level I classification.	To advance to Level III, incumbents must be able to perform all the essential functions of the higher level position, at a higher level of competency than a level II. Advancement is subject to approval of the business need for a higher level position and salary budget availability. The typical timeline for advancement is 3 years from entry into the Level II classification.	To advance to Level IV, incumbents must be able to perform all the essential functions of the higher level position, at a higher level of competency than a level III. Advancement is subject to approval of the business need for a higher level position and salary budget availability. The typical timeline for advancement is 3 years from entry into the Level III classification.	Advancement to the Lead Level will generally be the result of a competitive recruitment process and is subject to availability of a vacant approved position.