Position description

Position title	OT Cyber Delivery Specialist
Group / Branch	*Enterprise Transformation & Delivery / Enterprise Delivery*
Reports to (Title)	Head of Delivery- Enterprise Systems
Competency level	*Individual Contributor*

Job Purpose

The Operational Technology (OT) Cyber Delivery Specialist provides hands-on operational technology engineering and cyber security capability across South East Water's OT and cyber portfolio. The role is intended for an experienced OT practitioner who can work directly with industrial control systems and field equipment, not solely provide governance, vulnerability management or security advisory services.

The role designs, configures, programs, commissions, migrates, tests and troubleshoots OT systems including Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), SCADA platforms, historians, communications infrastructure and OT-adjacent applications. It applies this practical engineering knowledge to deliver secure IT/OT separation, dedicated OT identity, secure remote access, industrial protocol security, resilient operations and defensible cyber controls.

Working across Operational Technology (OT), Cyber Security, Enterprise Delivery, Architecture, Technology Services, Risk and Assurance, Procurement and delivery partners, the role translates operational needs, cyber risks and regulatory obligations into safe implementation plans, tested configurations, evidence and sustainable operational outcomes.

Role emphasis: This is a delivery and engineering role. The incumbent must be able to operate across the full telemetry and control path, from field device and industrial communications through SCADA and historian platforms, while applying cyber security controls without compromising safety, availability or operational integrity.

Key Accountabilities

- 1. OT Engineering, Programming and Commissioning
- Configure, program, commission and troubleshoot RTUs, PLCs and related field equipment, including point mapping, control logic, communications settings, addressing and diagnostic testing.
- Plan and execute RTU reconfiguration and outstation renumbering, including IP addressing, routing, communications paths, firewall requirements and updates to SCADA channels and outstations.
- Perform site and laboratory testing, cutover support and operational verification across analogue values, digital points, alarms, Sequence of Events (SOE), polling, integrity scans, event scans and control functions.
- Validate select-before-operate and command execution, confirm safe failure behaviour, maintain configuration backups and golden configurations, and establish practical rollback and console-access arrangements.

- Work with operations and engineering teams to ensure implementation activities respect safety, process availability, change windows and operational acceptance requirements.

2. SCADA, Historian and OT Platform Delivery

- Administer, migrate, configure and troubleshoot GeoSCADA or equivalent SCADA platforms, including servers, channels, outstations, drivers, security settings, operator interfaces, alarms and failover arrangements.
- Support PI Historian or equivalent historian platforms, interface nodes and data flows, and verify complete data collection from field equipment through SCADA into the historian.
- Discover and map operational dependencies such as OPC servers, SQL connections, service accounts, scheduled tasks, authentication dependencies, hardcoded credentials, security groups, domain trusts and legacy integrations.
- Plan and deliver migration of SCADA, historian and associated servers into a dedicated OT Active Directory domain, using development and test validation, controlled cutovers, rollback planning and operational acceptance testing.
- Test point updates, alarm generation and acknowledgement, operator screens, historian updates, failover and complete end-to-end telemetry and control paths before operational handover.

3. Industrial Communications and Protocol Security

- Configure and troubleshoot industrial communications, with strong practical knowledge of DNP3 and DNP3 Secure Authentication (DNP3-SA); experience with other relevant protocols such as Modbus TCP, OPC, IEC 60870-5-104 or vendor-specific protocols is advantageous.
- Deploy and manage DNP3-SA configurations including certificates or keys, trust relationships, challenge-response authentication, secure session establishment, authentication diagnostics and recovery strategies.
- Diagnose communications failures across field devices, serial or IP communications, routing, firewalls, SCADA drivers and authentication layers, and restore service through controlled technical recovery.
- Produce and maintain protocol, communications and certificate documentation sufficient for operations, cyber assurance and future support.

4. OT Cyber Security Architecture and Segmentation

- Deliver practical OT segmentation and separation outcomes using security zones and conduits, restrictive firewall rules, secure routing, dedicated OT identity, controlled remote access, jump hosts and monitored interfaces between IT and OT.
- Review OT network and application architectures, configurations and rulesets; identify excessive privileges, shared accounts, default credentials, unsecured communications, flat networks, unmanaged service identities and obsolete components.
- Apply least privilege, role-based access control, named accounts, secure credential storage, TLS where supported, logging, monitoring, resilience and recovery while accounting for legacy-device compatibility and operational constraints.
- Design safer integration patterns for OT-adjacent applications, including broker or API service layers that reduce direct access to SCADA platforms and centralise authentication, authorisation and auditing.

- Assess and support applications that use .NET wrappers or SCADA SDKs, including API abstraction, SDK encapsulation, connection management, error handling, secure coding and protected credential handling.
- Deliver and maintain OT asset discovery, inventory and visibility capabilities by integrating relevant security tools, network telemetry and asset management platforms, while accounting for passive-monitoring requirements and the operational sensitivity of legacy OT devices.
- Implement and maintain controlled remote access for vendors, contractors and engineering personnel, including MFA, named accounts, least-privilege access, formal approvals, time-bound access, session logging and periodic access reviews

5. Cyber Delivery, Assurance and Operational Transition

- Translate OT hazards, cyber threat scenarios, architecture principles, regulatory obligations and operational needs into clear functional, non-functional, control and acceptance requirements.
- Maintain traceability across requirements, design decisions, configurations, test results, risks, exceptions, evidence and residual-risk approvals from discovery through transition to operations.
- Prepare and execute implementation, migration, commissioning, verification and rollback plans, including rigorous testing in representative non-production environments where practicable.
- Partner with project managers, architects, cyber specialists, OT engineers, operators, testers and vendors to resolve delivery issues and ensure controls operate as intended.
- Produce operational documentation, support models, training material, evidence packs and handover artefacts that enable sustainable business-as-usual ownership and audit-defensible outcomes.

6. Regulatory Alignment and Stakeholder Engagement

- Support alignment with the Security of Critical Infrastructure Act and Critical Infrastructure Risk Management Program, Victorian Protective Data Security Standards, ASD Essential Eight and Information Security Manual, NIST Cybersecurity Framework, ISO/IEC 27001 and IEC 62443.
- Communicate technical OT risks, dependencies, outage implications and treatment options clearly to operational, technical and executive stakeholders.
- Engage suppliers and system integrators on technical requirements, design quality, configuration, testing, commissioning, supportability and evidence.
- Balance cyber security uplift with safety, reliability, maintainability, delivery constraints, cost and the need for uninterrupted critical services.

Knowledge, Skills & Experience

- Substantial hands-on OT engineering experience in utilities, water, energy, transport, manufacturing or another safety- or availability-critical industrial environment.
- Demonstrated ability to program, configure, commission and troubleshoot RTUs and PLCs. Experience must extend beyond network segmentation, cyber governance, SOC operations or vulnerability reporting.
- Practical SCADA experience, preferably with GeoSCADA, including server and database dependencies, channels, outstations, drivers, alarms, operator interfaces, security configuration, diagnostics and failover.
- Practical historian experience, preferably PI Historian, including interfaces, data collection, point verification and troubleshooting across the complete telemetry path.

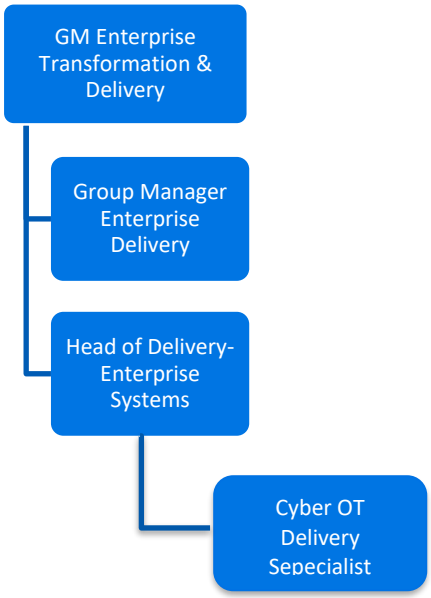
- Strong knowledge of DNP3 addressing and communications, with practical exposure to DNP3-SA, certificate or key management, secure authentication and operational verification.
- Experience migrating OT platforms and dependencies into a dedicated Active Directory domain, including service identities, security groups, authentication dependencies and rollback planning.
- Working knowledge of OT networks, firewalls, routing, switching, IP addressing, industrial communications, remote access, jump hosts, network segmentation and secure connectivity.
- Ability to interpret and modify technical designs and configurations, investigate faults using system and network diagnostics, and work safely under operational change control.
- Experience with OT-adjacent software integration, APIs, SCADA SDKs and .NET-based applications is highly desirable.
- Experience defining cyber security requirements, acceptance criteria and assurance evidence and embedding them into procurement, solution design, testing, commissioning and handover.
- Strong written communication, stakeholder facilitation, vendor engagement and technical documentation skills, with sound judgement across safety, operational reliability, cyber risk and cost.

Education and Formal Certifications

- Bachelor's degree or trade/technical qualification in Electrical Engineering, Control Systems, Automation, Instrumentation, Mechatronics, Computer Systems, Cyber Security or a related discipline, or equivalent relevant industry experience.
- Relevant vendor training or certification for RTUs, PLCs, SCADA or historian platforms is highly desirable.
- GICSP, ISA/IEC 62443 Cybersecurity certificates or equivalent industrial cyber security certification is advantageous.
- Professional certifications such as CISSP, CISM, CISA, CRISC, PRINCE2 or equivalent are desirable but do not replace the mandatory requirement for substantial hands-on OT engineering experience.
- Current Victorian driver licence and willingness to attend operational sites and participate in planned commissioning or cutover activities where required.

Dimensions

Organisational Chart



Number of people managed:

N/A

Size of budget managed:

N/A

Value of Assets managed:

N/A