HOPE AUTOMATION & CONTROLS LLC
200 Naomi Ln.
Newcastle, OK 73605
866-HOPE-565
support@hopeautomation.com
www.hopeautomation.com

QUOTE PROPOSAL FOR WORK

Date: April 2, 2026

BILL TO
City of Mangum
130 North Oklahoma Avenue
Mangum, OK 73554

LOCATION
City of Mangum
130 North Oklahoma Avenue
Mangum, OK 73554

DESCRIPTION	QTY	UNIT PRICE	TOTAL
HopeAutomation SCADA RAT 100 – Complete remote monitoring, control, alarm, and data logging system including: • Voice call-out alarm notification • Web-based SCADA dashboard for remote monitoring and control • Automated data logging and cloud database historian storage • Local HMI for setpoint configuration and real-time monitoring • Discrete and analog I/O for full pump station monitoring and control	1	$5,100.00	$5,100.00
SCADA RAT 100 Installation Labor – On-site installation, wiring, configuration, and commissioning.	10 hrs	$150.00/hr	$1,500.00
Radar Level Transducer – Top-down radar level sensor in stainless steel housing. Continuous level measurement integrated into SCADA RAT 100 for monitoring and pump control.	1	$485.00	$485.00
High/Low Level Float Switches (2) – Backup level control floats providing high and low level alarm and pump control redundancy.	2	$150.00	$300.00
		Quote Total	**$7,385.00**

Terms & Conditions	
Payment Terms: Net 15. Payment in full is due within 15 days of invoice date.	
Late Payment Fee: Payments not received by the due date will incur a late fee of 1.5% per month (18% APR) on the outstanding balance, or the maximum amount allowed by law, whichever is less.	
Validity: This quote is valid for 30 days from the date of issue (April 2, 2026) unless otherwise agreed in writing.	
By signing below, the undersigned acknowledges and accepts the terms, conditions, and pricing outlined in this proposal (Document Number SOW-402)	
Accepted by:	
Printed Name:	
Title:	
Date:	

HOPE AUTOMATION & CONTROLS LLC

Defense in Depth — Security Across Every Layer

OSI Model Cybersecurity Overview | March 2026

How We Think About Security — Layers, Not a Single Wall

A common mistake in industrial cybersecurity is treating security as a single line of defense — a firewall, a password, or a locked door. Hope Automation takes a different approach called Defense in Depth: we apply independent security controls at every layer of the communication stack, so that if one measure is ever bypassed, the next layer is already in place.

The OSI model is the standard seven-layer framework that describes how data moves from physical hardware up through software applications. The table below shows where each threat lives and exactly what we do to address it.

Layer	Name	What It Is	How Hope Automation Secures It
7	**Application**	User-facing software and dashboards	View-only dashboard, OTP login, no command capability, HMAC-signed alarms, unique credentials per user and device
6	**Presentation**	Data formatting and encryption	TLS 1.2+ on all MQTT and HTTPS; AES-256 on all backups; WireGuard for remote access — no plain-text communications
5	**Session**	Managing login sessions and connections	One-time-password login, time-limited engineering sessions, multi-factor authentication, automatic session expiry
4	**Transport**	Reliable data delivery between endpoints	Port 8883 (TLS-MQTT) only; all other ports blocked at host firewall; no inbound ports open on field or plant equipment
3	**Network**	Routing data between networks	OT and IT networks fully segmented; Tailscale zero-trust VPN for remote access; no direct internet route to PLCs or HMIs
2	**Data Link**	Local device-to-device communication	MAC address allowlist on SCADA RAT WiFi; hidden SSID; cellular-only WAN for remote sites; managed switches at plant
1	**Physical**	Hardware, cables, and physical access	Locked enclosures on field devices; USB ports disabled on SCADA PC; no physical console access without engineering credentials

Layer 7 — Application | Who Can Do What in the Software

This is the layer your operators actually interact with — dashboards, logins, and alarm messages. It is also the most commonly targeted layer in water utility attacks because it is the most visible.

How we secure it:

- The operator dashboard is view-only. It has no ability to send commands to field equipment under any circumstances.
- Every user logs in with a one-time password sent to their email address. There is no permanent password to intercept or brute-force.
- Every person and every device has unique credentials. A compromised operator account cannot be used to access engineering tools, and vice versa.
- Outbound alarm messages (phone calls and SMS) include a cryptographic signature (HMAC). This prevents attackers from injecting fake alarm commands into the system.
- All application-level events — logins, alarms, and setpoint changes — are logged with timestamps and user identity.

Layer 6 — Presentation | Keeping Data Unreadable in Transit and at Rest

The Presentation layer is responsible for how data is formatted and encoded before it travels across a network. This is where encryption lives.

How we secure it:

- All MQTT data from field devices is transmitted using TLS 1.2 or higher — the same encryption standard used by banks and financial institutions.
- The operator dashboard and all web-based access require HTTPS. Unencrypted HTTP is not permitted.
- Engineering remote access uses WireGuard, a modern VPN protocol with encryption reviewed and trusted by the security research community.
- Nightly database backups are encrypted with AES-256 before being uploaded to cloud storage. Backup files are unreadable without the key — a ransomware attack on the storage bucket cannot expose your data.
- We do not use any unencrypted protocols — no plain-text MQTT, no plain-text HTTP, no unencrypted remote desktop.

Layer 5 — Session | Managing Who Is Connected and For How Long

The Session layer controls how connections are established, maintained, and terminated. Unmanaged sessions — connections that stay open indefinitely — are a significant risk in industrial environments.

How we secure it:

- Operator dashboard sessions use one-time-password login. Each code expires after use and cannot be replayed.
- Engineering VPN connections require multi-factor authentication. A stolen password alone is not sufficient to connect.
- Remote engineering access is time-limited. There is no permanently open connection to plant equipment. Sessions are terminated after the task is complete.
- Future control-capable sessions will have a hard 20-minute time limit with automatic disconnection and a full audit trail.

Layer 4 — Transport | Controlling Which Traffic Is Allowed

The Transport layer defines which ports and protocols are used to carry data. Open ports are potential entry points — every unnecessary open port is a door that does not need to exist.

How we secure it:

- Field devices and the SCADA PC only use outbound port 8883 (TLS-encrypted MQTT). No inbound ports are open.
- The SCADA PC host firewall explicitly blocks all ports not required for operation — both inbound and outbound.
- The Tailscale VPN used for engineering access does not require any open inbound ports on the plant network. The encrypted tunnel is established outbound, so the plant firewall never needs to accept an incoming connection.
- Remote SCADA RAT units communicate exclusively over cellular. There are no open ports on the cellular connection — only outbound MQTT is permitted.

Layer 3 — Network | Keeping OT and IT Traffic Completely Separated

The Network layer controls how data is routed between different networks. The most important network-level security decision in any industrial control system is keeping the operational technology (OT) network — PLCs, HMIs, field instruments — completely separate from the information technology (IT) network and the internet.

How we secure it:

- At treatment plant installations, the OT network (PLCs, HMIs) has no connection to the internet. It is physically and logically isolated.
- The SCADA PC sits at the boundary. It can read from the OT network and send data outward, but it cannot receive inbound connections from the internet, and it cannot write back to PLCs.
- Firewall rules enforce this boundary at the network level — not just at the software level.
- Engineering remote access uses Tailscale, a zero-trust VPN. Engineers connect to a specific, named device — not to the entire network. Access is scoped to the minimum required.
- For remote SCADA RAT sites (wells, towers, booster stations), each unit connects via its own cellular data connection. Remote sites are never connected to each other through a shared local network.

Layer 2 — Data Link | Controlling Which Devices Can Join the Local Network

The Data Link layer manages direct communication between devices on the same local network — Ethernet, WiFi, and similar connections. At this layer, the question is: which physical devices are allowed to talk to each other at all?

How we secure it:

- Every SCADA RAT field unit provides a local WiFi access point for on-site configuration. This access point enforces a hardware-level (MAC address) allowlist — only devices pre-programmed at the time of manufacture are permitted to connect, regardless of whether they have the password.
- The SCADA RAT WiFi SSID is hidden and does not broadcast. A device cannot discover the network by scanning — it must already know the name.
- Remote SCADA RAT units use cellular modems for all WAN traffic. There is no local Ethernet connection to exploit at unmanned remote sites.
- At treatment plant installations, managed network switches enforce port-level access controls, ensuring only known and authorized devices can communicate on the OT network segment.

Layer 1 — Physical | Protecting the Hardware Itself

Physical security is the foundation of every other layer. No software protection matters if an attacker can walk up to a device and plug something in.

How we secure it:

- All SCADA RAT field enclosures are lockable. Electrical panels housing PLCs and HMIs are secured with keyed locks.
- USB ports on the SCADA PC are disabled at the operating system level on all installations, both Windows and Linux. A USB drive plugged into the machine will not mount — malware cannot be loaded and data cannot be extracted this way.
- The SCADA PC does not have an exposed physical console for general use. The operator account (read-only) is the only account accessible without Hope Automation engineering credentials.
- PLC and HMI devices have unique device-level passwords set at commissioning. Physical access to the device does not grant access to programming or configuration without the correct credentials.
- Default manufacturer passwords are always changed before any system goes live. This closes the single most common physical attack vector documented in water utility incidents.