IKT217 Assignment 3

Owner: Jonathan Fedje
Reviewer: Jonathan Fedje
Contributors:
Date Generated: Wed Oct 29 2025

OWASP Threat Dragon

Executive Summary

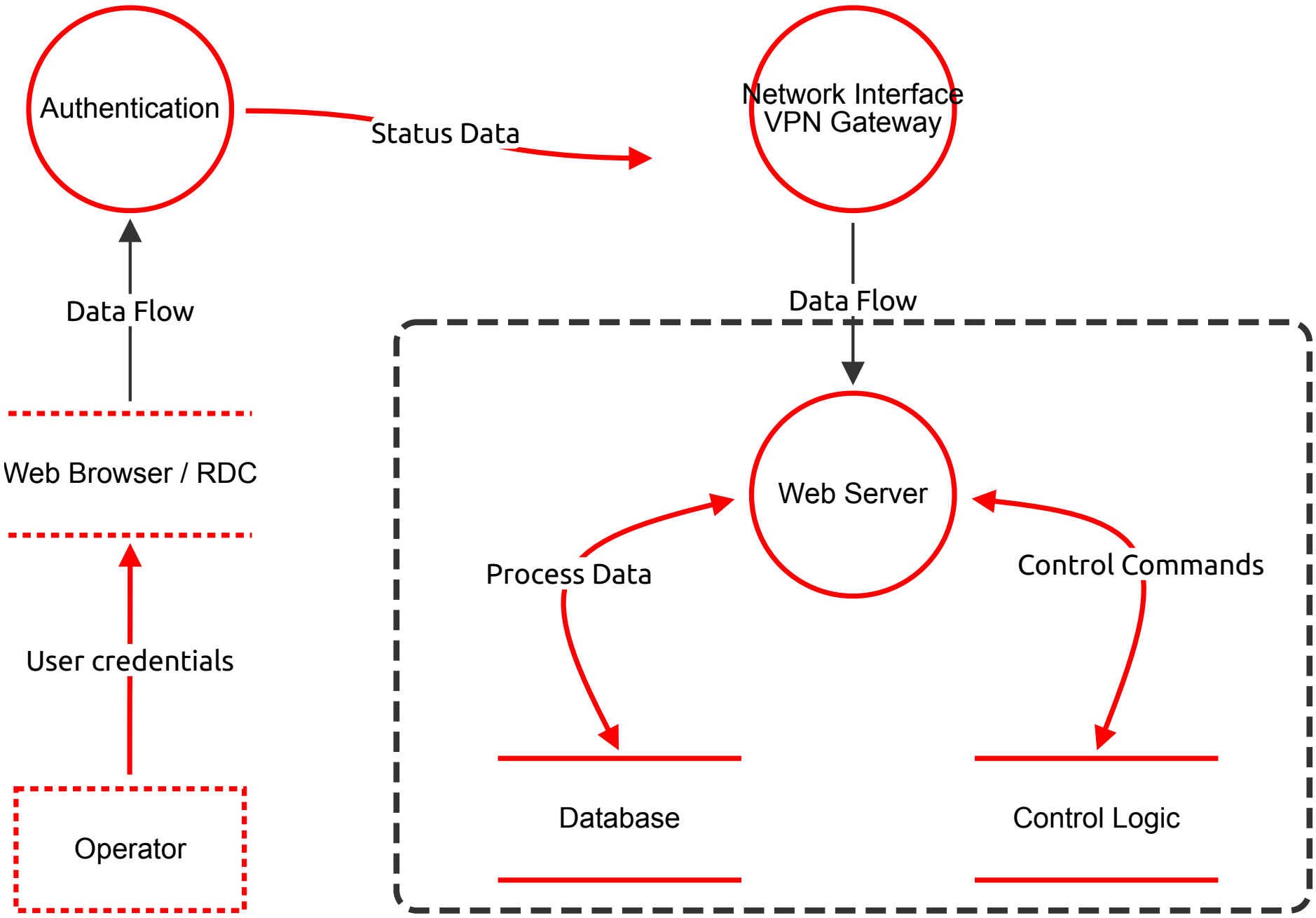
High level system description

A SCADA system / interface solution used for monitoring and controlling a water treatment process.
Remote controlling and monitor sensor data through a terminal accessible from the web.
It collects sensor data

Summary

Total Threats	24
Total Mitigated	0
Total Open	24
Open / Critical Severity	7
Open / High Severity	13
Open / Medium Severity	4
Open / Low Severity	0

STRIDE Diagram



STRIDE Diagram

Trust Boundary (threatmodel.shapes.boundaryBox)

Description: Internal SCADA / OT network

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	Direct Internet exposure of OT network	Elevation of Privilege	Critical	Open		The SCADA environment is reachable from outside without strict network isolation, allowing remote attackers to directly reach OT assets.	Introduce segmented networks, DMZ, and VPN-only access with firewall rules restricting inbound sources.
2	Lateral movement inside trust boundary	Tampering	High	Open		Once an attacker is inside the trust boundary, weak internal segmentation allows pivoting between Web Server, Database, and Control Logic.	Use internal firewalls/microsegmentation and per-service authentication between components.

Web Browser / RDC (Store) *- Out of Scope*

Reason for out of scope:

Description: Operator endpoint used to access SCADA remotely

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
3	Weak credential verification / no MFA	Spoofing	High	Open		If the browser or RDP client only sends username/password, an attacker with stolen credentials can impersonate an operator.	Require MFA for remote access and lock accounts after repeated failures.
4	Credentials sent over public network	Information Disclosure	High	Open		Login credentials or session cookies may be exposed if sent over unencrypted channels.	Force TLS/VPN tunnels for all traffic and disable plaintext protocols.

Operator (Actor) *- Out of Scope*

Reason for out of scope:

Description: Remote operator responsible for monitoring and issuing commands

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Operator impersonation	Spoofing	Critical	Open		An attacker pretends to be the operator and attempts to access or control the SCADA system.	Strong identity verification (MFA, per-user accounts, no shared logins).

Number	Title	Type	Severity	Status	Score	Description	Mitigations
6	Action denial / lack of accountability	Repudiation	Medium	Open		If actions are not logged with operator identity and timestamp, the operator (or attacker) can deny having sent unsafe commands.	Enable tamper-evident audit logging tied to operator identity.

Network Interface VPN Gateway (Process)

Description: Public-facing gateway / firewall / VPN concentrator providing remote access into SCADA network

Properties: Privilege Level: Gateway / Edge

Number	Title	Type	Severity	Status	Score	Description	Mitigations
9	Unsecured remote access (public IP)	Spoofing	High	Open		If the gateway allows direct login from the Internet without MFA or IP restrictions, attackers can impersonate remote staff.	Enforce MFA on VPN, restrict source IP ranges, and disable direct exposure of SCADA ports.
10	Gateway DoS / Flooding	Denial of Service	High	Open		Attackers can overwhelm the public interface, preventing operators from issuing safety commands.	Rate limiting, lockouts, upstream firewall/WAF, redundant paths.

User credentials (Data Flow)

Description: Credentials from operator to login endpoint

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
7	Credentials interception / modification	Tampering	High	Open		Attacker-in-the-middle can alter or inject credentials if the login flow is not protected with TLS/VPN.	Enforce TLS 1.3 or VPN tunnels for all credential flows. Reject plaintext auth.
8	Credential leakage over public network	Information Disclosure	High	Open		If transmitted in cleartext, credentials can be harvested and reused for remote compromise.	Never allow HTTP/RDP without encryption; require MFA.

Process Data (Data Flow)

Description: Operational telemetry and historical values

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
11	Manipulation of process data	Tampering	High	Open		Attacker alters process values shown to operators, hiding unsafe conditions or faking stability.	Sign data from PLCs / logic, validate ranges, alert on anomalies.
12	Sensitive process visibility	Information Disclosure	Medium	Open		Exposure of live plant telemetry can give attackers insight into process state and safety margins.	Enforce least-privilege read access and encrypt traffic in transit.

Control Commands (Data Flow)

Description: Commands issued to change actuators / dosing / pumps

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
13	Unauthorized or altered control commands	Tampering	Critical	Open		Attacker injects or modifies control commands (e.g. over-chlorination, pump shutdown).	Command signing, role-based authorization, rate limiting of control actions.
14	PLC/control logic overload	Denial of Service	Critical	Open		Rapid or malformed commands can overload/lock the PLC or logic, preventing safe operation.	Watchdog timers, sanity checks in logic, throttle high-frequency writes.

Status Data (Data Flow)

Description: Status / health info sent back toward client display

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
15	Sensitive status exposure	Information Disclosure	Medium	Open		Detailed plant status and alarm conditions could leak operational secrets or safety weaknesses.	Redact sensitive fields for low-privilege users; encrypt traffic.

Data Flow (Data Flow)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Database (Store)

Description: Credential store, process history, audit log

Properties: Stores Credentials

Number	Title	Type	Severity	Status	Score	Description	Mitigations
16	Plaintext credentials in database	Information Disclosure	High	Open		Credentials or sensitive config are stored unencrypted, which could be leaked or exfiltrated.	Hash+salt passwords (bcrypt/Argon2), encrypt sensitive fields at rest.
17	Unauthenticated/unauthorized DB writes	Tampering	High	Open		An attacker who reaches the DB can change setpoints, user roles, or disable alarms.	Harden DB access controls, separate application and admin accounts, monitor integrity.
18	No immutable audit trail	Repudiation	Medium	Open		If logs in the DB can be edited or deleted, malicious actions cannot be traced to a user.	Write-protect audit logs, sign log entries, forward to SIEM.

Web Server (Process)

Description: SCADA App (includes authentication / HMI / control interface)

Properties: Web Application, Privilege Level: High (can control plant)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
19	Single privilege level / no RBAC	Elevation of Privilege	High	Open		If every authenticated user can execute control actions, compromise of one account = full control.	Implement role-based access control and least privilege (operator vs admin vs maintenance).
20	Unpatched web server / SCADA app	Elevation of Privilege	Critical	Open		Known vulnerabilities in the web stack could allow remote code execution or admin shell.	Keep OS/SCADA app patched, vulnerability scan regularly, restrict management interfaces.
21	Application-layer DoS / flooding	Denial of Service	High	Open		Attackers can overload the web server, preventing monitoring or emergency actions.	WAF/rate limiting, timeout abusive sessions, failover / HA deployment.

Control Logic (Store)

Description: PLC / automation logic / actuator control state

Properties: Stores Inventory

Number	Title	Type	Severity	Status	Score	Description	Mitigations
22	Unauthorized modification of control logic	Tampering	Critical	Open		Attackers can alter PLC logic/setpoints to create unsafe process states (wrong dosage, wrong pH, etc.).	Require signed/approved logic changes, restrict who can push new control logic.

Authentication (Process)

Description: Login/session handling, part of the SCADA web server logic

Properties: Privilege Level: High

Number	Title	Type	Severity	Status	Score	Description	Mitigations
3	Authentication disabled / bad credentials handling	Spoofing	Critical	Open		The system indicates 'Authentication disabled', allowing anyone to access SCADA controls without verifying identity.	Enable authentication, enforce MFA, lock out default/guest accounts.

Number	Title	Type	Severity	Status	Score	Description	Mitigations
23	No role-based authorization after login	Elevation of Privilege	High	Open		Even if login succeeds, all authenticated users may inherit high-level privileges.	Implement RBAC and least privilege on sensitive actions (chemical dosing, pump control).