CYBERSECURITY &

SECURITY ARCHITECTURE

OptiZeus SCADA Platform · Version 2.5.4

Document: SEC-OZ-SCADA · Classification: Client Confidential

EXECUTIVE SUMMARY

OptiZeus SCADA is designed from the ground up with industrial cybersecurity as a core requirement — not an afterthought. This document describes the security architecture, controls, and compliance posture of the OptiZeus platform to assist clients in their risk assessment, vendor qualification, and regulatory compliance activities.

The platform is aligned with **IEC 62443** (Industrial Cybersecurity), **NIST SP 800-82** (Guide to ICS Security), **21 CFR Part 11** (FDA Electronic Records), and **GAMP5** (Pharmaceutical Computer Validation). It implements 14+ independent security controls spanning network transport, authentication, access control, data integrity, audit logging, and OT/IT network separation.

APPLICABLE STANDARDS & FRAMEWORKS

IEC 62443
Industrial Automation & Control Systems Security
Aligned with SL1–SL2 requirements for IACS cybersecurity

NIST SP 800-82
Guide to Industrial Control Systems Security
Follows NIST guidance for ICS/SCADA network hardening

21 CFR Part 11
FDA Electronic Records & Signatures
Full compliance — audit trail, e-signatures, access control

GAMP5 Cat. 4
ISPE Good Automated Manufacturing Practice
Configured product with full validation documentation suite

ISA-62443
ISA Industrial Cybersecurity Standards
Defense-in-depth security zones and conduits model

ISO/IEC 27001
Information Security Management
Security controls aligned with ISO 27001 Annex A principles

SECURITY CONTROLS OVERVIEW (14+ Independent Layers)

01	**Transport Security** HTTPS / TLS 1.2+ encryption on all connections	02	**Authentication** Username + password with MFA/TOTP second factor
03	**Access Control** 5-level RBAC — Admin, Engineer, Supervisor, Operator, Viewer	04	**Directory Integration** LDAP / Active Directory SSO with group mapping
05	**Brute Force Protection** Login rate limiting with automatic account lockout	06	**SQL Injection Defense** Parameterized queries — zero dynamic SQL in codebase
07	**API Rate Limiting** Per-endpoint throttling prevents automated abuse	08	**Session Management** JWT tokens with configurable expiry and rotation
09	**Timing-Safe Auth** Prevents timing-based credential enumeration attacks	10	**Audit Trail** Immutable log of every action — user, timestamp, IP, value
11	**E-Signatures (CFR 11)** Password re-authentication with reason code on critical ops	12	**OT/IT Separation** DMZ with OPC-UA Proxy/Broker — physical network isolation
13	**Auto Session Timeout** Configurable inactivity logout for unattended workstations	14	**Secure Defaults** Principle of least privilege — no open ports by default

OT / IT NETWORK SEPARATION ARCHITECTURE

LEVEL 4 — Enterprise / Business Network (IT)
ERP · LIMS · Email · Corporate Infrastructure

■ FIREWALL + IEC 62443 CONDUIT

LEVEL 3 — OptiZeus MES / Supervisory (DMZ)
OptiZeus MES Server · Historian · Reporting · Remote Access

■ FIREWALL + IEC 62443 CONDUIT

LEVEL 2 — OptiZeus SCADA / HMI (OT Supervisory)
OptiZeus SCADA Server · HMI Clients · Alarm Management

■ OPC-UA PROXY / BROKER

LEVEL 1 — Control Network (OT)
PLCs · DCS · Zeus IPC Controllers · OPC UA Servers

■ OPC-UA PROXY / BROKER

LEVEL 0 — Field / Process Level
Sensors · Actuators · Odot Remote I/O · Instruments

AUTHENTICATION & ACCESS CONTROL

OptiZeus implements a multi-layer authentication system designed to meet 21 CFR Part 11 and IEC 62443 requirements.

Primary Auth	**Username + password (bcrypt hashed)**
2nd Factor	**TOTP / MFA — Google Auth, Authy, etc.**
SSO	**LDAP / Active Directory integration**
AD Group Sync	**AD groups auto-mapped to SCADA roles**
User Auto-Create	**New AD users provisioned on first login**
Sync Schedule	**Configurable periodic AD sync**
Password Policy	**Min length, complexity, expiry enforced**
Account Lockout	**Auto-lock after configurable failed attempts**
Session Tokens	**JWT with configurable expiry & rotation**
Auto-Logout	**Inactivity timeout per role**
Concurrent Login	**Configurable max sessions per user**

AUDIT TRAIL (21 CFR Part 11)

Every action in OptiZeus is recorded in an immutable audit trail. Records cannot be modified or deleted by any user, including administrators.

Scope	**All logins, logouts, config changes, control op**
Record Fields	**Timestamp, user, IP address, action, old/new v**
Storage	**SQL Server — tamper-evident append-only log**
Retention	**Configurable — default unlimited**
Export	**PDF and CSV export with date/user filtering**
E-Signatures	**Password re-auth + reason code on critical ops**
Sig. Fields	**Signed by, date/time, reason, hash verification**
Deploy Audit	**Every Test→Production change logged with di**
Alarm Journal	**All alarm events with operator response logge**
Batch Records	**Full EBR with operator signatures per step**
Access to Log	**Admin read-only — no edit/delete capability**

ROLE-BASED ACCESS CONTROL (5 Levels)

ADMINISTRATOR	Full system access — config, users, deploy
ENGINEER	Tag config, screens, alarms, recipes
SUPERVISOR	Acknowledge alarms, approve batch records
OPERATOR	Monitor, control, operate HMI screens
VIEWER	Read-only access — monitoring only

TRANSPORT & DATA SECURITY

Protocol	**HTTPS enforced — HTTP auto-redirect**
TLS Version	**TLS 1.2 minimum / TLS 1.3 preferred**
Certificates	**Self-signed or CA-issued · OPC UA PKI**
OPC UA Security	**Sign & Encrypt mode · Certificate auth**
SQL Queries	**Parameterized — injection-proof by design**
API Auth	**JWT Bearer token on all API endpoints**
Rate Limiting	**Per-endpoint throttling — configurable**
Timing Safety	**Constant-time auth — prevents enumeration**
CORS Policy	**Strict origin control on web API**
Headers	**Security headers: HSTS, CSP, X-Frame-Option**

PHARMACEUTICAL COMPLIANCE (21 CFR Part 11)

CFR §	Requirement	OptiZeus Implementation
§11.10(a)	Validation	GAMP5 IQ/OQ/PQ docs auto-generated
§11.10(b)	Legible copies	PDF/CSV export of all records
§11.10(c)	Record protection	DB-level + app-level access controls
§11.10(d)	Audit trail	Immutable log — all record changes
§11.10(e)	Authorized access	5-level RBAC + MFA enforcement
§11.10(f)	Operational checks	Role-based action authorization
§11.10(g)	Authority checks	User identity verified before action
§11.10(h)	Device checks	Input validation on all controls
§11.10(i)	Training records	User accounts with role assignment
§11.50	E-Signature	Full name, date, time, reason code
§11.70	Sig. linking	Cryptographic hash to record
§11.100	Sig. uniqueness	Per-user unique credentials enforced

GAMP5 VALIDATION POSTURE

Category	**GAMP5 Category 4 — Configured Product**
Auto-Docs	**10 documents auto-generated by AI assistant**
URS	**User Requirements Specification template**
Design Spec	**System design and architecture document**
IQ	**Installation Qualification protocol + report**
OQ	**Operational Qualification with test scripts**
PQ	**Performance Qualification with acceptance**
Risk Assessment	**FMEA-based risk identification & mitigation**
Traceability	**Requirements → tests → results matrix**
VSR	**Validation Summary Report with sign-off**
Change Control	**Version-controlled config with audit trail**
Revalidation	**Impact assessment on every software update**

DEPLOYMENT HARDENING GUIDE

Recommended configuration steps for production deployment in regulated environments:

Network

- ✓ Deploy on isolated OT network segment
- ✓ Enable firewall — allow only required ports (443, OPC UA)
- ✓ Use DMZ for IT/OT boundary — OPC-UA Proxy between zones
- ✓ Disable all unused server ports and services

Authentication

- ✓ Enable MFA/TOTP for all engineer and admin accounts
- ✓ Integrate with Active Directory for centralized user mgmt
- ✓ Set password policy: min 12 chars, complexity, 90-day expiry
- ✓ Configure auto-logout: 10 min operators, 5 min admins

TLS / Certificates

- ✓ Install CA-issued TLS certificate (not self-signed in prod)
- ✓ Configure OPC UA with Sign & Encrypt + certificate auth
- ✓ Set TLS minimum version to 1.2 in server config
- ✓ Rotate JWT secret keys on every major deployment

Access Control

- ✓ Apply principle of least privilege — start with Viewer role
- ✓ Create named accounts for every operator (no shared logins)
- ✓ Disable default demo/test accounts before go-live
- ✓ Review and document all RBAC assignments in IQ

Audit & Monitoring

- ✓ Configure audit trail export schedule (weekly minimum)
- ✓ Set up alarm notifications for repeated failed logins
- ✓ Enable automated backup of audit trail database
- ✓ Test e-signature workflow before regulatory go-live

CLIENT SECURITY ACCEPTANCE CHECKLIST

- ✓ TLS certificate installed and verified
- ✓ MFA enabled for all privileged accounts
- ✓ AD/LDAP integration configured and tested
- ✓ OT/IT network separation implemented
- ✓ Firewall rules reviewed and documented
- ✓ Audit trail storage and backup confirmed
- ✓ RBAC roles assigned per site access matrix
- ✓ Auto-logout timeouts set per policy
- ✓ E-signature workflow tested and approved
- ✓ GAMP5 IQ/OQ/PQ documents reviewed and signed
- ■ Annual security review scheduled
- ■ Incident response contact established

SECURITY CONTACT & RESPONSIBLE DISCLOSURE

For security questions, vulnerability reports, or penetration test coordination:
security@zeus-automation.com · info@zeus-automation.com · zeus-automation.com