ZEUS AUTOMATION

OptiZeus SCADA

Cybersecurity & Compliance Overview

Enterprise-grade security built into every layer. Protecting your industrial control systems from cyber threats while maintaining regulatory compliance.

Security Architecture Overview

1 Authentication & Access Control

Multi-factor authentication (TOTP/MFA), Active Directory / LDAP SSO, role-based access control with security letters (A-Z), session timeout management, and password complexity enforcement.

2 Data Protection & Encryption

AES-256-CBC hardware-locked licensing, bcrypt password hashing (12 salt rounds), HTTPS/SSL/TLS transport encryption, JWT token management with expiration, and encrypted database backups.

3 Audit & Accountability

Complete audit trail logging every user action with timestamps, IP addresses, and change details. Non-repudiation through electronic signatures. Tamper-evident log records with checksums.

4 Network Security

Rate limiting on authentication endpoints, input sanitization against injection attacks, CORS configuration, CSP headers, and configurable firewall rules. No inbound ports required for client access.

Authentication Methods

Method	Description	Use Case
Local Accounts	Username + bcrypt password. Configurable complexity, expiry, and history.	Standalone installations
Active Directory / LDAP	Enterprise SSO with AD group-to-role mapping. Mixed auth supported.	Corporate environments
TOTP / MFA	Time-based one-time password (Google Authenticator, Authy). Per-user enforcement.	High-security areas
Security Letters (A-Z)	26 access levels assignable per role. Objects on screens require specific letters.	Granular access control
Session Management	Configurable timeout per user. Auto-logout on inactivity. Concurrent session limits.	Shared operator stations

Role-Based Access Control (RBAC)

Role	Permissions	Typical Users
Administrator	Full system access. User management, configuration, deployment, backup/restore.	System integrators, IT admins
Operator	Screen viewing, tag writing, alarm acknowledgment, recipe execution, notes.	Plant operators, shift leads
Viewer	Read-only access to screens, trends, alarms, and reports. No write capability.	Managers, auditors, visitors
Custom Roles	Configurable permission sets with security letter requirements per screen/action.	Quality, maintenance, safety

Regulatory Compliance

21 CFR Part 11 (FDA)

- Electronic signatures with dual approval
- Complete audit trail with user attribution
- Record integrity verification (checksums)
- System access controls (RBAC + MFA)
- Closed system controls per §11.10
- Electronic record retention and retrieval

GAMP5 (ISPE)

- Category 4 software (configured product)
- IQ/OQ/PQ validation protocols included
- Risk assessment templates (FMEA)
- Traceability matrix documentation
- Change control procedures
- Validation summary report template

IEC 62443 (Industrial Cybersecurity)

- Defense-in-depth architecture
- Network segmentation support
- Least privilege access model
- Security event monitoring
- Patch management capability
- Incident response procedures

ISO 27001 Alignment

- Information classification support
- Access control policies
- Cryptographic controls (AES-256)
- Operations security (logging, monitoring)
- Supplier relationship management
- Business continuity (backup/restore)

OWASP Top 10 Mitigation

#	Threat	OptiZeus Mitigation
A01	Broken Access Control	RBAC with security letters, session management, JWT expiration, API endpoint authorization
A02	Cryptographic Failures	AES-256-CBC encryption, bcrypt hashing, HTTPS/TLS, no plaintext credentials
A03	Injection	Parameterized SQL queries (better-sqlite3), input sanitization, CSP headers
A04	Insecure Design	Defense-in-depth, least privilege, staging-to-production deployment model
A05	Security Misconfiguration	Secure defaults, no debug in production, configurable CORS, rate limiting
A06	Vulnerable Components	Regular dependency updates, npm audit, minimal dependency footprint
A07	Auth Failures	MFA/TOTP, account lockout, password history, inactivity auto-disable
A08	Data Integrity Failures	Checksum verification on records, staging deployment with review, audit trail
A09	Logging Failures	Comprehensive audit trail, security event logging, log export capability
A10	SSRF	Allowlist for external connections, no user-controlled URL fetching

Audit Trail & Electronic Signatures

Audit Trail Records

Every configuration change, tag write, alarm acknowledgment, user login/logout, and system event is logged with:

- Timestamp (millisecond precision)
- Username and role
- Action type and description
- Before/after values for changes
- Client IP address
- Record checksum for integrity

Electronic Signatures

21 CFR Part 11 compliant signatures for critical operations:

- Dual approval (performer + approver)
- Configurable reason codes
- Custom reason text support
- Non-repudiation (signed by authenticated user)
- Linked to audit trail records
- Per-screen security letter requirements

Backup & Disaster Recovery

Database Backup	Automated scheduled backups with configurable retention. Full SQLite DB + WAL file snapshot.

Project Export	Complete project ZIP with database, configurations, screens, recipes. Portable across installations.
Multi-Server Sync	Staging-to-production deployment with selective sync. Hot standby capability.
Version Control	Pending changes staging with deploy/rollback. Change history with timestamps.
Auto-Update	Check, download, install updates with rollback. Patch-based incremental versioning.

Request a Security Assessment

Our team will review your cybersecurity requirements and demonstrate OptiZeus compliance capabilities.

www.optizeus.org

security@optizeus.org | sales@optizeus.org | support@optizeus.org