# SYNTHETIC VENTILATOR MODEL 1X

### Technical Specification Document

Version 2.0 - Security Enhanced Edition

## EXECUTIVE SUMMARY

The Synthetic Ventilator Model 1X (SVM-1X) represents a next-generation medical ventilator designed with comprehensive security features to ensure patient safety, data protection, and reliable operation in critical care environments. This specification details the security characteristics implemented across five key domains: Confidentiality, Integrity, Availability, Human/Trust, and Authentication.

## SECURITY FEATURES OVERVIEW

| Characteristic | Implementation Level | Compliance |
|---|---|---|
| Confidentiality | AES-256 Encryption | HIPAA, GDPR |
| Integrity | Digital Signatures | FDA 21 CFR Part 11 |
| Availability | 99.999% Uptime | IEC 60601-1 |
| Human/Trust | Intuitive UI Design | IEC 62366 |
| Authentication | Multi-factor Auth | ISO 27001 |

# 1. CONFIDENTIALITY

## *1.1 Data Encryption*

The SVM-1X implements AES-256 encryption for all patient data at rest and in transit. Patient records, ventilation parameters, and monitoring data are encrypted using FIPS 140-2 validated cryptographic modules. The encryption keys are managed through a secure key management system with automatic key rotation every 90 days.

## *1.2 Access Control*

Role-based access control (RBAC) restricts data access based on user roles: Physician, Respiratory Therapist, Nurse, and Technician. Each role has predefined permissions for viewing and modifying patient data. Audit logs track all access attempts and data modifications.

## *1.3 Network Security*

All network communications use TLS 1.3 with mutual authentication. The ventilator operates on a segregated medical network with firewall protection. External connectivity is limited to approved hospital information systems through encrypted VPN tunnels.

***Requirements:***

• REQ-CONF-001: Implement AES-256 encryption for all patient data

• REQ-CONF-002: Deploy RBAC with minimum privilege principle

• REQ-CONF-003: Use TLS 1.3 for all network communications

• REQ-CONF-004: Maintain audit logs for 7 years per HIPAA requirements

# 2. INTEGRITY

## *2.1 Data Validation*

All ventilator parameters undergo real-time validation against clinically acceptable ranges. The system implements checksums and digital signatures for critical data transfers. Any data corruption is immediately detected and alerts are generated.

## *2.2 Firmware Protection*

Firmware updates are digitally signed by the manufacturer and verified before installation. Secure boot ensures only authorized firmware can run on the device. The system maintains firmware integrity through continuous monitoring and tamper detection.

## *2.3 Calibration Integrity*

Automated calibration checks occur every 24 hours with results digitally signed and timestamped. Manual calibration requires two-person verification with biometric authentication. All calibration data is immutably logged in the system.

***Requirements:***

• REQ-INTG-001: Implement real-time parameter validation

- REQ-INTG-002: Deploy secure boot with firmware signature verification
- REQ-INTG-003: Perform automated calibration checks every 24 hours
- REQ-INTG-004: Use blockchain for immutable calibration logging

# 3. AVAILABILITY

## *3.1 Redundancy Systems*

The SVM-1X features dual redundant control systems with automatic failover in <100ms. Critical components including power supplies, processors, and sensors have N+1 redundancy. The system maintains full functionality even with single component failure.

## *3.2 Power Management*

Triple power source capability: mains power, internal battery (8-hour runtime), and external battery connection. Automatic power source switching with zero interruption. Battery health monitoring with predictive replacement alerts 30 days in advance.

## *3.3 Fault Tolerance*

Self-diagnostic routines run continuously to detect potential failures. Predictive maintenance algorithms analyze component wear and schedule preventive maintenance. Emergency ventilation mode ensures basic life support even during system failures.

***Requirements:***

• REQ-AVAIL-001: Achieve 99.999% uptime (less than 5.26 minutes downtime/year)

• REQ-AVAIL-002: Implement N+1 redundancy for all critical components

• REQ-AVAIL-003: Provide 8-hour battery backup minimum

• REQ-AVAIL-004: Enable emergency ventilation mode within 2 seconds

# 4. HUMAN/TRUST

## *4.1 User Interface Design*

Intuitive touchscreen interface with context-sensitive help and guided workflows. Color-coded alarms follow international standards (red: high priority, yellow: medium, blue: informational). Large, clear displays visible from 5 meters distance.

## *4.2 Alarm Management*

Smart alarm system reduces false positives by 70% using AI-based pattern recognition. Alarm fatigue prevention through intelligent alarm suppression and escalation. Customizable alarm limits based on patient condition with clinical decision support.

## *4.3 Training Integration*

Built-in simulation mode for training without patient connection. Interactive tutorials for each ventilation mode with competency verification. Continuous learning system tracks user proficiency and suggests refresher training when needed.

***Requirements:***

• REQ-TRUST-001: Implement intuitive UI with <3 clicks to any function

• REQ-TRUST-002: Reduce false positive alarms by minimum 70%

- REQ-TRUST-003: Provide built-in training mode with certification tracking
- REQ-TRUST-004: Display confidence intervals for all measurements

# 5. AUTHENTICATION

## *5.1 Multi-Factor Authentication*

Two-factor authentication combining smart card and biometric (fingerprint or facial recognition). Emergency override available with dual-person authentication and automatic incident reporting. Session timeout after 15 minutes of inactivity.

## *5.2 User Management*

Centralized user management integrated with hospital Active Directory. Automatic deprovisioning when staff leave the organization. Regular access reviews every 90 days with manager approval required for continued access.

## *5.3 Audit Trail*

Comprehensive audit trail captures all authentication attempts, parameter changes, and system access. Tamper-proof logging with cryptographic signatures. Real-time alerts for suspicious authentication patterns or unauthorized access attempts.

***Requirements:***

• REQ-AUTH-001: Implement two-factor authentication for all users

• REQ-AUTH-002: Integrate with hospital LDAP/Active Directory

• REQ-AUTH-003: Maintain tamper-proof audit logs for 7 years

• REQ-AUTH-004: Enable emergency override with dual authentication

# IDENTIFIED SECURITY GAPS

| Gap ID | Characteristic | Description | Recommendation |
|---|---|---|---|
| GAP-001 | Confidentiality | No quantum-resistant encryption | Plan migration to post-quantum cryptography by |
| GAP-002 | Human/Trust | Limited multilingual support | Add support for 10 additional languages |
| GAP-003 | Authentication | No continuous authentication | Implement behavioral biometrics monitoring |
| GAP-004 | Integrity | Manual supply chain verification | Deploy blockchain for component tracking |