1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) document outlines the functional and non-functional requirements for the **DeepPrevent: Multi-Modal AI System for Industrial Equipment Predictive Maintenance & Hazard Detection**, version 1.0.
DeepPrevent is designed to proactively identify and predict equipment faults and industrial hazards by leveraging deep learning, sensor fusion, and explainable AI techniques. It integrates inputs from thermal cameras, acoustic sensors, visual feeds, and time-series logs to deliver actionable insights to plant safety and maintenance personnel.
This document defines the scope, system behavior, performance expectations, constraints, and integration interfaces. The target audience includes the project stakeholders at IOCL/ONGC, developers, quality assurance teams, and future maintainers of the system.

1.2 Document Conventions

This SRS follows the conventions below for clarity, traceability, and structured requirement classification:

 Requirement Indicators

Keyword	Meaning
REQUIRED	A critical requirement without which the system will not function correctly.
RECOMMENDED	A strong requirement that enhances performance, usability, or safety but is not strictly essential.
OPTIONAL	A feature that adds value but is not necessary for initial operation.
DESIRED	A future or stretch goal considered valuable in later phases.
CONDITIONALLY REQUIRED	Required only under specific circumstances or configurations (e.g., when edge deployment is active).

Requirement Identifiers

- **[FR-XXX]**: Functional Requirements (e.g., [FR-002])
- **[NFR-XXX]**: Non-Functional Requirements (e.g., [NFR-005])
- **[UIR-XXX]**: User Interface Requirements
- **[EIR-XXX]**: External Interface Requirements
- **[PR-XXX]**: Performance Requirements
- **[SR-XXX]**: Security Requirements

Text Formatting Conventions

- **Bold Text**: Section headings, keywords, or identifiers.
- *Italic Text*: Emphasis or citations.
- `Monospace Text`: Code snippets, API names, paths, and file names.

1.3 Intended Audience and Reading Suggestions

This Software Requirements Specification (SRS) is intended for a diverse group of stakeholders involved in the design, development, deployment, and use of the DeepPrevent system. Each audience is encouraged to focus on the sections most relevant to their role or interest area.

1. System Developers and Engineers

- **Software Developers and AI Engineers**: Will refer to this document for understanding functional requirements, data pipelines, machine learning components, sensor integration, and performance expectations.
  Recommended Sections: Functional Requirements (Section 3), System Architecture (Section 2.2), External Interfaces (Section 4)
- **Embedded Systems and Hardware Engineers**: Will focus on hardware-level requirements, sensor connectivity, and system integration with existing industrial equipment.
  Recommended Sections: Hardware Interfaces (Section 4.2), Non-Functional Requirements (Section 5)

2. Industrial Partners and Plant Operators

- **Maintenance Engineers**: Will use the system for real-time monitoring, predictive maintenance alerts, diagnostics, and historical trend analysis.
  Recommended Sections: Functional Requirements (Section 3), System Features (Section 2.3)
- **Safety and Compliance Officers**: Will rely on hazard detection features, early warning systems, and risk assessment functionalities.
  Recommended Sections: Hazard Detection Features (FR-010 to FR-018), Security and Reliability Requirements (Section 5.3)

3. Quality Assurance and Test Engineers

- Responsible for verifying the system's accuracy, reliability, compliance with standards, and overall performance.
  Recommended Sections: Functional Requirements (Section 3), Non-Functional Requirements (Section 5), Appendix: Test Cases (Appendix A)

4. Cybersecurity and Compliance Teams

- Ensure the system adheres to industrial security policies, data protection laws, and secure integration protocols.
  Recommended Sections: Security Requirements (Section 5.3), Data Governance and Privacy (Section 5.4)

5. Project Stakeholders and Managers

- Require an overarching view of the system's purpose, features, scope, milestones, and constraints to manage project deliverables effectively.
  Recommended Sections: Overall Description (Section 2), Scope (Section 1.4), Glossary (Appendix B)

6. Academic Researchers and Interns

- May explore DeepPrevent for research into AI applications in industrial safety, predictive analytics, and real-time anomaly detection.
  Recommended Sections: System Overview (Section 2), Functional Requirements (Section 3), Architecture and Data Flow Diagrams (Appendix C)

1.3 Product Scope

DeepPrevent is an AI-powered, multi-modal industrial monitoring system designed to provide predictive maintenance and hazard detection capabilities in real-time. The system integrates sensor data, visual analytics, machine learning models, and industrial process knowledge to forecast potential equipment failures and identify hazardous conditions proactively.

The core objectives of DeepPrevent include:

- Reducing unplanned downtimes through accurate predictive maintenance.
- Preventing workplace accidents by early detection of fire, gas leaks, overheating, and other critical hazards.
- Improving operational efficiency by providing data-driven insights into equipment health and process anomalies.
- Supporting industrial digital transformation initiatives through intelligent automation and proactive safety management.

1.4 References

- **IEEE Std 830-1998**: IEEE Recommended Practice for Software Requirements Specifications. A foundational guideline for organizing and presenting software requirements.

- **WCAG (Web Content Accessibility Guidelines)**: Accessibility standards that may apply to the monitoring dashboards to ensure inclusive usability.
  https://www.w3.org/WAI/standards-guidelines/wcag/

- **OWASP (Open Web Application Security Project)**: Guidelines and tools to ensure the security of the web-based and cloud-accessible components of DeepPrevent.
  https://owasp.org/

- **NIST SP 800-82 Revision 2**: Guide to Industrial Control Systems (ICS) Security. Relevant for designing secure architecture and communication in industrial environments.
  https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

- **ISO 13374-1:2003**: Condition monitoring and diagnostics of machines — Data processing, communication, and presentation. Applicable to predictive maintenance workflows.

---

1. Overall Description

1.1 Product Perspective

DeepPrevent is an advanced, cloud-native multi-modal AI system tailored for predictive maintenance and hazard detection in industrial environments, specifically targeting IOCL and ONGC facilities. The system integrates thermal imaging, visual inspection, acoustic analysis, and sensor data into a unified predictive framework to foresee equipment failures and safety hazards weeks in advance. Unlike traditional single-modality monitoring tools, DeepPrevent leverages state-of-the-art deep learning architectures including convolutional neural networks (CNN), transformers, and recurrent neural networks (LSTM) to provide comprehensive, explainable, and actionable insights. It is designed as a scalable, modular platform that can be deployed on cloud infrastructure or edge devices, enabling real-time hazard detection with minimal latency.

1.2 Product Functions

DeepPrevent offers the following key functionalities:

- **Thermal Signature Evolution Analysis:** Tracks and analyzes thermal patterns over time using CNNs and temporal transformers to identify early signs of equipment degradation.
- **Visual Anomaly Detection:** Employs Vision Transformers (ViT) combined with object detection to detect visual defects or irregularities in equipment.
- **Acoustic Health Monitoring:** Utilizes 1D CNN and LSTM models to analyze sound patterns for identifying anomalous acoustic signatures indicative of faults.
- **Sensor Fusion and Time-Series Prediction:** Aggregates multi-source sensor data through a multi-head attention-based transformer and LSTM architecture for robust failure prediction and health scoring.
- **Explainable AI Dashboard:** Integrates SHAP, LIME, and Grad-CAM methods to provide transparent and interpretable insights into model decisions, sensor importance, and anomaly localization.
- **Real-Time Risk Prediction:** Fuses multi-modal inputs to generate unified health scores and predict failure timelines, enabling proactive maintenance actions.
- **Data Augmentation & Synthetic Failure Simulation:** Enhances model robustness by generating synthetic thermal, acoustic, and sensor data to simulate rare or critical failure modes.
- **Interactive Monitoring Interface:** Offers a user-friendly dashboard for real-time visualization, alert management, and historical analysis.

1.3 User Classes and Characteristics

- **Maintenance Engineers and Technicians:** Primary users who monitor equipment health, interpret AI-driven risk scores, and schedule maintenance activities. Require intuitive visualization tools and clear failure explanations to make timely decisions.
- **Facility Safety Officers:** Use the system to detect and respond to safety hazards, relying on real-time alerts and hazard localization.
- **Data Scientists and AI Engineers:** Responsible for system training, evaluation, and improvement. They interact with data pipelines, model training workflows, and experiment tracking tools.
- **Operations Managers:** Oversee facility performance and maintenance budgets; leverage system analytics to optimize resource allocation and reduce downtime costs.
- **IT/DevOps Teams:** Manage deployment, integration, and scaling of the DeepPrevent platform across cloud or edge environments.

1.4 Operating Environment

DeepPrevent operates in a hybrid cloud and on-premise industrial setting, utilizing cloud providers such as AWS or Google Cloud for scalable compute resources and container orchestration (Docker/Kubernetes). It interfaces with various hardware sensors including thermal cameras, visual cameras, microphones, and IoT sensor arrays deployed on industrial equipment. The system supports access via modern web browsers through a responsive dashboard built using Streamlit, and offers real-time inference APIs based on FastAPI for seamless integration with existing facility monitoring systems. Data processing pipelines are optimized for batch and streaming workloads with robust versioning and augmentation capabilities.

1.5 Design and Implementation Constraints

- **Real-Time Performance:** Must deliver hazard detection and failure prediction with latency under 2 seconds to ensure timely response.
- **Scalability:** Designed to handle multi-facility deployment scenarios with horizontal scaling to support thousands of equipment units.
- **Explainability:** AI decisions must be transparent, enabling maintenance teams to trust predictions and understand contributing factors.
- **Data Security and Privacy:** Compliance with industrial data security standards and secure integration with existing infrastructure.
- **Robustness:** Models trained with synthetic and augmented data to handle rare failure scenarios and noisy sensor inputs.
- **Hardware Compatibility:** Support for edge deployments on industrial IoT devices with limited compute, enabling federated learning extensions.
- **Integration:** RESTful APIs with thorough documentation to enable integration with IOCL monitoring systems and digital twin platforms.

1.1 User Documentation

User documentation for DeepPrevent will include tutorials, FAQs, and how-to guides focused on system setup, sensor integration, and interpreting AI-driven predictive maintenance alerts. A searchable knowledge base will provide quick access to troubleshooting tips and best practices. Clear instructions on using the real-time hazard detection dashboard and explainable AI features will support effective decision-making. Regular updates will keep users informed about new features and system improvements, ensuring safe and efficient operation in industrial environments.

1.2 Assumptions and Dependencies

User Competency Assumptions:

- Maintenance engineers have basic digital literacy and industrial equipment knowledge
- Safety officers understand hazard detection protocols and emergency response procedures
- Data scientists have machine learning fundamentals and Python/AI framework experience
- Operations managers can interpret KPIs, predictive analytics dashboards, and maintenance reports

Industrial Environment Dependencies:

- Facilities have reliable network connectivity for real-time sensor data transmission
- Thermal cameras, acoustic sensors, and visual monitoring equipment are properly calibrated
- DeepPrevent integrates with existing SCADA systems and maintenance management software
- Industrial-grade edge computing infrastructure supports local AI model inference
- Expertise validation through **recognized industrial certifications** (API, ASME, etc.)

2. External Interface Requirements

2.1 User Interfaces

I. **Multi-Role Industrial Dashboard:** Responsive web interface accessible via industrial tablets, control room displays, and mobile devices

II. **Role-Specific Interfaces:**

- **Maintenance Engineers:** Equipment health monitoring, predictive alerts, maintenance scheduling
- **Safety Officers:** Hazard detection dashboard, emergency response protocols, risk assessment tools
- **Data Scientists:** Model performance monitoring, training pipelines, experiment tracking
- **Operations Managers:** Facility-wide KPIs, cost analysis, resource optimization insights

III. **Knowledge Exchange Portal:** Cross-facility expertise sharing, best practices documentation, collaborative problem-solving forums

2.2 Hardware Interfaces

Industrial IoT Sensors: Thermal cameras, acoustic sensors, vibration monitors, pressure/temperature sensors

Edge Computing Devices: NVIDIA Jetson, Intel NUC, or equivalent for local AI inference

Industrial Displays: Control room monitors, HMI panels, ruggedized tablets for field use

Video Conferencing Integration: For remote expert consultation during critical equipment failures

2.3 Software Interfaces

SCADA/DCS Integration: Real-time data exchange with existing industrial control systems

Maintenance Management Systems: Integration with SAP PM, Maximo, or similar CMMS platforms

Authentication Services: Integration with corporate Active Directory and industrial security protocols

Cloud Services: AWS/Azure integration for scalable AI model training and data analytics

Notification Systems: Email, SMS, and industrial alarm system integration for critical alerts

2.4 Communications Interfaces

Industrial Network Protocols: OPC-UA, Modbus, Ethernet/IP for equipment communication

Secure HTTPS/TLS: For web-based dashboard access and API communications

RESTful APIs: For integration with existing industrial software and third-party analytics tools

Edge-to-Cloud Sync: Secure data transmission protocols for model updates and historical analysis

1. System Features

1.1 User Management Subsystem

- **[FR-001] User Registration and Authentication (REQUIRED):**
  Users shall be able to register and authenticate securely using email/password or enterprise credentials. Secure password management, including reset and change functionalities, shall be implemented to ensure user account safety.
- **[FR-002] Profile Management (REQUIRED):**
  Users shall create, view, and update profiles containing personal information, role designation (e.g., Operator, Maintenance Engineer, Safety Inspector), contact details, and assigned equipment or zones of responsibility. Optionally, users may link to certifications or training records.
- **[FR-003] User Roles and Permissions (REQUIRED):**
  The system shall define roles such as Operator, Engineer, Safety Officer, and Administrator, each with distinct permissions for accessing system features, data, and control interfaces, ensuring appropriate authorization.

1.2 Equipment & Sensor Data Management Subsystem

- **[FR-004] Equipment Taxonomy and Categorization (REQUIRED):**
  A hierarchical classification of industrial equipment and sensors shall be maintained for structured management, enabling efficient search and filtering by equipment type, model, location, and status.
- **[FR-005] Sensor Data Collection and Storage (REQUIRED):**
  The system shall collect real-time data streams from multiple sensor modalities (vibration, temperature, acoustic, visual, etc.) and securely store them for analysis and historical trending.
- **[FR-006] Data Validation and Quality Assurance (RECOMMENDED):**
  Mechanisms for validating sensor data integrity, detecting anomalies, and flagging inconsistent or missing data shall be implemented to ensure reliable inputs for AI modules.

1.3 Predictive Maintenance and Hazard Detection Subsystem

- **[FR-007] Predictive Analytics and Failure Forecasting (REQUIRED):**
  AI models shall analyze sensor data to predict equipment degradation, estimate remaining useful life (RUL), and forecast potential failures before occurrence.
- **[FR-008] Hazard Identification and Alerting (REQUIRED):**
  The system shall detect hazardous conditions (e.g., gas leaks, overheating, mechanical faults) and generate timely alerts to relevant personnel with severity classification.
- **[FR-009] Model Training and Updating (RECOMMENDED):**
  Support for periodic retraining and fine-tuning of AI models using new labeled data shall be provided to improve accuracy and adapt to evolving operational conditions.

1.4 Communication and Collaboration Subsystem

- **[FR-010] Real-time Alerting and Messaging (REQUIRED):**
  Users shall receive instant notifications via multiple channels (mobile app, email, SMS) for critical alerts and maintenance requests. Secure messaging shall enable communication between operators and maintenance teams.
- **[FR-011] Scheduling and Task Management (REQUIRED):**
  The system shall support scheduling maintenance activities and follow-up inspections, integrating with organizational calendars and providing task tracking features.

1.5 Feedback and Reporting Subsystem

- **[FR-012] Maintenance Feedback and Incident Reporting (REQUIRED):**
  Users shall submit feedback and incident reports post-maintenance or hazard resolution, facilitating continuous improvement and record keeping.
- **[FR-013] Performance Metrics and Reporting (REQUIRED):**
  The system shall generate reports on equipment health trends, maintenance effectiveness,

incident frequency, and AI model performance, viewable by authorized roles.

1.6 Security and Compliance Subsystem

- **[FR-014] Data Security and Privacy (REQUIRED):**
  The system implemens data encryption at rest and in transit, role-based access control, and audit logging to comply with industrial cybersecurity standards.
- **[FR-015] Regulatory Compliance Support (RECOMMENDED):**
  Features to assist in compliance with safety and environmental regulations, including automatic documentation and report generation, shall be supported.

1.7 Analytics and Future Enhancements Subsystem

- **[FR-016] Usage and System Analytics (OPTIONAL - Future):**
  Collect and analyze system usage data to optimize workflows, user experience, and AI model deployment strategies.
- **[FR-017] Advanced AI Model Monitoring (OPTIONAL - Future):**
  Provide dashboards to monitor AI model drift, accuracy, and operational impact for administrators and data scientists.

---

2. Other Non-Functional Requirements

2.1 Performance Requirements

- **[PR-001] Response Time (REQUIRED):** Core system interactions such as equipment status dashboard loading, alert display, and sensor data queries **MUST** respond within 2 seconds.
- **[PR-002] Concurrency (RECOMMENDED):** The system **SHOULD** support at least 200 concurrent users, including operators, engineers, and administrators.
- **[PR-003] Data Processing Latency (REQUIRED):** Real-time sensor data ingestion and anomaly detection **MUST** process data with latency under 500 milliseconds.

2.2 Security Requirements

- **[SR-001] Authentication (REQUIRED):** Users **MUST** authenticate using email/password with multi-factor authentication **RECOMMENDED**.
- **[SR-002] Data Protection (REQUIRED):** All sensitive data such as user credentials, sensor information, and analytics results **MUST** be encrypted both in transit (HTTPS) and at rest.
- **[SR-003] Authorization (REQUIRED):** Access to system functionalities **MUST** be role-based with permissions strictly enforced.
- **[SR-004] Vulnerability Management (RECOMMENDED):** Regular security assessments and penetration testing **SHOULD** be conducted.

2.3 Usability Requirements

- **[UIR-001] Intuitiveness (REQUIRED):** The user interface **MUST** be intuitive and easy to navigate for all user roles.
- **[UIR-002] Accessibility (REQUIRED):** The system **MUST** comply with WCAG 2.1 AA accessibility guidelines.

2.4 Reliability Requirements

- **[NFR-001] Uptime (RECOMMENDED):** The system **SHOULD** maintain an uptime of 99.9%.
- **[NFR-002] Data Backup and Recovery (REQUIRED):** Regular data backups **MUST** be performed to ensure data integrity and disaster recovery.

2.5 Scalability Requirements

- **[NFR-003] Horizontal Scalability (REQUIRED):** The system **MUST** be horizontally scalable to handle increasing sensor data and user load.

2.6 Maintainability Requirements

- **[NFR-004] Code Maintainability (RECOMMENDED):** The codebase **SHOULD** be well-structured, documented, and follow coding best practices.
- **[NFR-005] Deployment (RECOMMENDED):** The system **SHOULD** support automated deployment.

---

3. Other Requirements

- **[NFR-006] Legal and Regulatory Compliance (REQUIRED):** DeepPrevent **MUST** comply with all applicable industrial safety, environmental, and data privacy regulations.
- **[EIR-001] API Documentation (RECOMMENDED):** Comprehensive API documentation using ‘OpenAPI’ **SHOULD** be provided to enable future integrations.

- **[NFR-007] Internationalization (RECOMMENDED):** The platform **SHOULD** support internationalization (i18n) to accommodate multiple languages and locales.
- **[NFR-008] Data Retention Policy (REQUIRED):** A clear data retention policy **MUST** be defined and implemented, detailing data storage duration and secure disposal methods.

User Interface Requirements (UIR)

- **[UIR-001] Intuitive Dashboard Design (REQUIRED):** The user interface provides a clear and intuitive dashboard displaying real-time equipment status, alerts, and maintenance schedules.
- **[UIR-002] Responsive Design (RECOMMENDED):** The UI is fully responsive and accessible across devices including desktops, tablets, and smartphones.
- **[UIR-003] Accessibility Compliance (REQUIRED):** The interface complies with WCAG 2.1 AA standards to support users with disabilities.
- **[UIR-004] Customizable Views (OPTIONAL):** Users customize dashboard widgets to prioritize information relevant to their role.
- **[UIR-005] User-Friendly Error Handling (REQUIRED):** The UI provides clear, actionable error messages and guidance for user errors.

External Interface Requirements (EIR)

- **[EIR-001] Sensor Data Integration (REQUIRED):** The system supports integration with industrial IoT sensors using standard protocols such as MQTT and OPC-UA.
- **[EIR-002] Third-Party API Support (RECOMMENDED):** The system provides APIs for integration with external maintenance management and alerting platforms.

- **[EIR-003] Cloud Service Integration (DESIRED):** The platform supports integration with cloud services for data storage and analytics.
- **[EIR-004] External Authentication Systems (OPTIONAL):** The system supports single sign-on (SSO) via external identity providers such as OAuth2 or SAML.

Performance Requirements (PR)

- **[PR-001] Real-Time Data Processing (REQUIRED):** The system processes incoming sensor data and detects anomalies within 500 milliseconds.
- **[PR-002] Dashboard Load Time (REQUIRED):** Dashboard pages load within 2 seconds under normal operating conditions.
- **[PR-003] Concurrent User Support (RECOMMENDED):** The system supports a minimum of 200 concurrent users without performance degradation.
- **[PR-004] Alert Notification Latency (REQUIRED):** Alert notifications deliver to users within 1 second of anomaly detection.
- **[PR-005] Data Query Performance (REQUIRED):** Queries on historical sensor data return results within 3 seconds.

Security Requirements (SR)

- **[SR-001] User Authentication (REQUIRED):** Users authenticate using secure email/password credentials and support multi-factor authentication.

- **[SR-002] Role-Based Access Control (REQUIRED):** The system enforces role-based permissions to restrict access to sensitive functions and data.
- **[SR-003] Data Encryption (REQUIRED):** All sensitive data encrypt at rest and in transit using industry-standard protocols (e.g., TLS 1.2+).
- **[SR-004] Audit Logging (RECOMMENDED):** The system maintains audit logs for critical operations and access events.
- **[SR-005] Security Vulnerability Management (RECOMMENDED):** The system conducts regular security vulnerability assessments and penetration testing.
- **[SR-006] Incident Response (OPTIONAL):** The system maintains a documented incident response plan to address security breaches promptly.