ThermalDIAG – API-Integrationsübersicht

Öffentliche Übersicht über Integrationsmöglichkeiten, Sicherheitsmodell und unterstützte Einsatzbereiche.

Dokumenttyp	**API-Integrationsübersicht**	API-Vertrag	**External API Contract V1**
Version	**1.0**	Stand	**2026-08-31**
Status	**Öffentliche Information**		
Autor	**JC-Technology GmbH**		

Inhalt

1. Zweck und Zielgruppe

ThermalDIAG ist eine lokal betriebene Anwendung zur gemeinsamen Überwachung und Dokumentation thermischer, elektrischer, mechanischer und digitaler Anlagenzustände. Die authentifizierte REST-API ermöglicht es freigegebenen externen Systemen, ausgewählte Betriebsinformationen zu lesen und klar begrenzte Arbeitsabläufe anzustoßen.

Diese Übersicht richtet sich an technische Entscheider, Systemintegratoren und IT-/OT-Verantwortliche. Sie beschreibt die verfügbaren Integrationsbereiche, ohne interne Implementierungsdetails, vollständige Datenmodelle oder konkrete Endpunktpfade offenzulegen. Autorisierte Integrationspartner erhalten bei Bedarf ein separates technisches Integrationshandbuch.

2. Integrationsmodell

Die primäre externe Schnittstelle ist eine HTTP-basierte REST-API auf der jeweiligen ThermalDIAG-Installation. ThermalDIAG bleibt dabei das führende System für Projektstruktur, Messwerte, Incidents, Tickets und Nachweise. Externe Clients greifen nur innerhalb des freigegebenen Projekts und der ihnen zugewiesenen Rolle zu.

Typische Integrationen sind:

- Übergabe eines kompakten Anlagen- oder Projektstatus an übergeordnete Systeme;
- Abruf aktueller Messwerte und historischer Zeitreihen;
- Anzeige von Incidents, Ereignisverläufen und eingefrorenen Nachweisen;
- Einbindung des Ticket-Workflows in Instandhaltungsprozesse;
- Abruf von Snapshots und Berichten für technische Dokumentation;
- kontrollierte Bedienhandlungen durch ausdrücklich berechtigte Benutzer.

Die API ist keine sicherheitsgerichtete Steuerung und ersetzt weder eine SPS, eine Schutzeinrichtung noch eine fachlich freigegebene Anlagenlogik.

3. Authentifizierung und Rollen

Jeder API-Zugriff erfolgt mit einem eigenen ThermalDIAG-Benutzer. Für technische Clients wird ein API-Token angefordert und anschließend als Bearer Token übertragen. Zugangsdaten und Token dürfen nicht in Quellcode, Konfigurations-Repositories, Screenshots oder Protokollen abgelegt werden.

Das Berechtigungsmodell folgt dem Prinzip der geringsten Rechte:

- `viewer`: schreibgeschütztes Monitoring ausgewählter Übersichten;
- `technician`: technische Diagnose und Arbeit an zugewiesenen Tickets;

- `operator`: Incident-Bearbeitung und freigegebene operative Änderungen;
- `admin`: kundenseitige Administration und Überwachung;
- `supervisor`: reservierte Service- und Freigaberolle.

Ein externer Client soll immer die engste für seinen Zweck ausreichende Rolle erhalten. Schreibzugriffe bleiben zusätzlich an Objektzustand, Projektkontext und Workflow-Regeln gebunden.

4. Unterstützte Datenbereiche

Der External Integration V1 Vertrag umfasst ausgewählte, authentifizierte Funktionen aus folgenden Bereichen:

- Projekte, Projektstatus und Dashboard-Zusammenfassungen;
- Standorte, Geräte und Messbereiche (ROIs);
- aktuelle Messwerte und historische Datenreihen;
- Incident-Zeitachsen, Details, Ereignisse und Trigger-Nachweise;
- Tickets, Einträge, Checklisten, Messungen und Anhänge;
- Snapshots, Snapshot-Jobs und druckbare Berichte;
- ausgewählte, rollenabhängige Incident- und Ticket-Workflows.

Interne Benutzeroberflächen-, Administrations-, Wartungs-, Lösch-, Regelbearbeitungs- und Analytics-Publishing-Schnittstellen gehören nicht zum öffentlich beschriebenen Integrationsumfang.

5. Datenkonventionen

API-Zeitstempel werden als ISO-8601-Datetime-Werte übertragen. Speicherung und Datenaustausch erfolgen UTC-basiert; die Darstellung in lokaler Zeit richtet sich nach der Projektzeitzone. Externe Systeme sollen keine formatierten UI-Zeitangaben parsen.

Temperaturwerte werden über die API in Grad Celsius bereitgestellt. Eine Fahrenheit-Darstellung ist ausschließlich eine Anzeige- oder Berichtsfunktion. IDs sind stabile technische Referenzen, dürfen aber nicht als Ersatz für eine Berechtigungsprüfung behandelt werden.

Antworten verwenden strukturierte JSON-Daten. Dateien wie Snapshots, Anhänge und Berichte werden über authentifizierte Datei- oder Reportantworten bereitgestellt.

6. Sicherheit und Betrieb

Die API soll innerhalb einer kontrollierten Kundenumgebung betrieben werden. Bei Zugriff über nicht vollständig vertrauenswürdige Netze sind TLS, eine restriktive Firewall- oder VPN-Freigabe und eine klare Client-Identität erforderlich.

ThermalDIAG-Installationen sollen nicht unkontrolliert direkt aus dem Internet erreichbar sein.

Empfohlene Betriebsregeln:

- dedizierter Benutzer je Integration;
- nur notwendige Rolle und Projekte freigeben;
- Token geschützt speichern und regelmäßig erneuern;
- Schreibaufrufe nicht blind wiederholen;
- Fehler, Zeitüberschreitungen und unklare Ergebnisse protokollieren;
- Schnittstellenversion und ThermalDIAG-Version bei Abnahme dokumentieren;
- Integrationen nach Updates mit einem definierten Smoke-Test prüfen.

7. Bewusste Grenzen von External Integration V1

External Integration V1 ist bewusst REST-basiert. Nicht Bestandteil des aktuellen Vertrags sind:

- MQTT und OPC UA;
- ein ThermalDIAG-seitiger Modbus-TCP-Server;
- Modbus RTU und allgemeines PLC-Register-Mapping;
- bidirektionale PLC-Befehlsverarbeitung;
- frei konfigurierbare Webhook-Aktionen;
- eine öffentliche, anonyme Monitoring-API;
- allgemeine Service-Accounts oder dauerhaft gültige API-Keys.

Einfache industrielle Signale können projektspezifisch über freigegebene Regelaktionen und vorhandene Geräteausgänge umgesetzt werden. Dies ist keine allgemeine Datenbus- oder Sicherheitssteuerung.

8. Detaillierte Dokumentation und Freigabe

Das separate REST-API-Integrationshandbuch enthält die unterstützten Endpunktpfade, Rollen, Parameter, Antwortmodelle und getestete Beispiele. Es wird versionsbezogen an autorisierte Kunden und Integrationspartner bereitgestellt.

Vor einer produktiven Integration werden gemeinsam festgelegt:

1. Zielsystem und Datennutzung;
2. benötigte Projekte und Datenbereiche;
3. Benutzerrolle und Token-Lebensdauer;
4. Netzwerkweg, TLS und Firewallregeln;
5. zulässige Lese- und Schreibabläufe;

6. Fehlerbehandlung, Abnahmetest und Versionspflege.

Kontakt für Integrationsanfragen: `office@jc-technology.at`