PlantBeat im Werksnetz

Für die IT-Abteilung: welche Verbindungen PlantBeat aufbaut, wie der Zugriff auf die Steuerung abgesichert ist, welche Daten das Werk verlassen und was wir für den Betrieb empfehlen.

AUF EINEN BLICK

Lokal im Werk

Verlauf, Alarme und Dashboards liegen auf dem PlantBeat-Rechner. Die Messwerte und Datensätze kannst du auch in deine eigene Datenbank legen. Kein Cloud-Zwang.

Nichts von außen

PlantBeat braucht keine eingehende Verbindung aus dem Internet und keine Portfreigabe.

Direkt zur SPS

S7-Protokoll über TCP 102. Kein OPC-Server, kein Agent auf der Steuerung.

Schreiben mit Rechten

Mit Zugangsschutz (ab Werk aus) erst ab Rolle „Bediener“, auf Wunsch mit Bestätigung, protokolliert. Oder ganz aus: „Nur lesen“ je Verbindung.

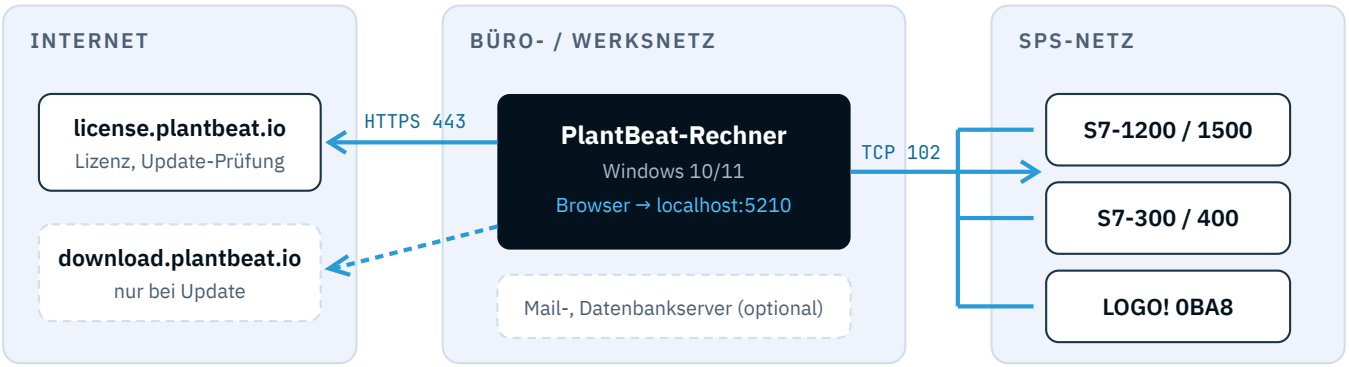
Verschlüsselt zur S7-1500

Gesicherte S7-1500 (Firmware ab V2.9) über TLS 1.3, mit Schutzstufen-Passwort. TLS handelt PlantBeat selbst aus.

Telemetrie ab Werk aus

Nutzungsdaten und Fehlerberichte nur, wenn du sie einschaltest. Ohne Zusatzfunktionen geht nach außen nur HTTPS zu plantbeat.io: Aktivierung, Update-Prüfung, Update-Download.

NETZBILD



Alle Verbindungen gehen vom PlantBeat-Rechner aus. Gestrichelt: nur bei Bedarf. Weitere optionale Ziele (smartlife BI, Kartenbilder) nennt die Tabelle auf Seite 2.

Smartlife Software Solutions GmbH · Erlenweg 12 · 8200 Eggersdorf bei Graz · Österreich
+43 3117 / 93080 · support@plantbeat.io · plantbeat.io

1 · VERBINDUNGEN

Was PlantBeat im Netz tut

Ziel	Protokoll	Wann	Inhalt
Steuerungen	`S7 · TCP 102`	dauernd, solange erfasst wird	Variablen lesen; schreiben nur über Bedienelemente und Datensatz-Fertig-Meldungen, bei „Nur lesen“ nie. Gesicherte S7-1500: TLS 1.3.
license.plantbeat.io	`HTTPS 443`	einmalig bei der Aktivierung	Bestell-Token, Fingerabdruck (Hashwert), Kennungen von Prozessor, Mainboard und Netzwerkkarte (MAC), Rechnername, Produktkennung
license.plantbeat.io	`HTTPS 443`	stündlich	Update-Prüfung: nur IP-Adresse und Programmversion
download.plantbeat.io	`HTTPS 443`	nur wenn ein Update ansteht	Installationspaket
dein Mailserver	`SMTP 587 · STARTTLS`	nur wenn eingerichtet	Alarm-, Wartungs- und Berichts-Mails mit Messwerten an deine Empfänger
dein Datenbankserver	`TCP · DB-Port`	nur wenn unter „Datenspeicher“ eingerichtet	Messwerte und Datensätze (Standardports: SQL Server 1433, PostgreSQL 5432, MySQL 3306)
license.plantbeat.io	`HTTPS 443`	nur wenn eingeschaltet (ab Werk aus)	Nutzungsdaten ohne Variablennamen und Werte; Fehlerberichte mit Hashwert der Hardware-Kennung, also nicht anonym
gateway.smartlifebi.com	`HTTPS/WSS 443`	nur wenn mit smartlife BI gekoppelt	nur die freigegebenen Datenquellen, nur auf Abfrage
tile.openstreetmap.org	`HTTPS 443`	nur mit Karten-Widget	Kartenbilder, abgerufen vom Browser auf diesem Rechner

Eingehend

Die Weboberfläche lauscht unter Windows ab Werk nur auf dem Rechner selbst (`localhost`, Port 5210, bei der Installation wählbar). Aus dem Netz ist sie nicht erreichbar, eine Firewall-Freigabe ist nicht nötig. Einen Hallenmonitor schließt du direkt an diesen Rechner an.

Firewall-Empfehlung

- TCP 102 nur zu den IP-Adressen der Steuerungen
- HTTPS 443 zu license.plantbeat.io und download.plantbeat.io
- nur bei Bedarf: SMTP zum eigenen Mailserver, Datenbankport zum eigenen Datenbankserver, HTTPS zu gateway.smartlifebi.com und tile.openstreetmap.org
- sonst nichts, auch nicht eingehend

Getrenntes SPS-Netz

Wir empfehlen ein eigenes Netz für die Steuerungen und zwei Netzwerkkarten im PlantBeat-Rechner: eine ins SPS-Netz, eine ins Werksnetz. PlantBeat leitet keinen Verkehr zwischen den Netzen weiter.

2 · ZUGRIFF AUF DIE STEUERUNG

Lesen ist die Regel, Schreiben die Ausnahme

Lesen	S7-1200/1500 symbolisch, so wie ein HMI; S7-300/400 und LOGO! 0BA8 über Adressen, die du einmal anlegst. PlantBeat verändert dabei nichts an der Steuerung und lädt kein Programm.
Schreiben	Nur in zwei Fällen, die jemand bewusst einrichtet: Bedienelemente im Dashboard (Schalter, Taster, Sollwert u. a.) und die Fertig-Meldung eines Datensatz-Abrufs (Fertig-Wert, Satznummer oder Leseindex). Sonst schreibt PlantBeat nicht.
Nur lesen	Je Verbindung schaltbar: Dann sendet PlantBeat keinen Schreibbefehl an diese Steuerung, auch keine Fertig-Meldung und keinen CPU-Start oder -Stopp. Durchgesetzt im Verbindungskern, nicht in der Oberfläche.
Rechte	Mit Zugangsschutz ab Rolle „Bediener“, geprüft auf dem Server; je Bedienelement optional mit Rückfrage vor dem Schreiben.
Protokoll	Jede Bedienung mit Benutzer, Variable und Wert im Protokoll, auch abgelehnte Versuche.
TLS	Gesicherte S7-1500 (Firmware ab V2.9): TLS 1.3 mit X25519, automatisch ausgehandelt. Das Schutzstufen-Passwort wirkt nur bei TLS-gesicherten CPUs; bei anderen muss die Schutzstufe den Zugriff ohne Passwort erlauben.

Was TLS hier leistet und was nicht

Die Verbindung zur CPU ist gegen Mitlesen geschützt, das CPU-Zertifikat prüft PlantBeat aber derzeit nicht gegen eine Vertrauenskette. Gegen einen Angreifer, der sich aktiv ins SPS-Netz schaltet, schützt deshalb vor allem die Netztrennung.

3 · ZUGANGSSCHUTZ UND ROLLEN

Drei Rollen, eine Regel

Betrachter	Bediener	Verwalter
sieht Dashboards, Verlauf und Diagnose	zusätzlich Alarme, Wartung, Datensätze und Berichte; darf schreiben	richtet Verbindungen, Benutzer, Benachrichtigungen und Einstellungen ein

Ab Werk	Zugangsschutz aus, damit die Einrichtung ohne Konto gelingt; bis dahin darf jeder alles bedienen. Für den Betrieb: Einstellungen → Zugangsschutz einschalten, Rollen vergeben.
Ansehen	„Ansehen ohne Anmeldung erlauben“ ist beim Einschalten angehakt; abwählen, wenn auch Dashboards, Verlauf und Diagnose eine Anmeldung verlangen sollen.
Anmeldung	Kennwörter als PBKDF2-SHA256-Hash (210.000 Durchläufe, Salt); 5 Fehlversuche sperren 5 Minuten; Sitzung endet nach 8 Stunden ohne Aktivität
Datei beschädigt	Ist die gespeicherte Zugangseinstellung beschädigt, gilt der Zugangsschutz als an (Ansehen nur nach Anmeldung), sobald es einen aktiven Verwalter gibt; ohne Verwalter bleibt PlantBeat offen, damit sich niemand aussperrt. Diagnose und Einstellungen zeigen das an; einmal speichern repariert die Datei.

4 · DATEN

Was bleibt, was geht

Speicherort	lokal unter `%ProgramData%\Smartlife\SelfService`; Messwerte und Datensätze optional in einer externen Datenbank (SQL Server, PostgreSQL, MySQL)
Aufbewahrung	je Wert einstellbar; Standard 30 Tage Messwerte, 90 Tage Alarme
Geheimnisse	Passwörter für SPS, Mailserver und externe Datenbank verschlüsselt mit Windows DPAPI
Nach außen	nur was die Tabelle auf Seite 2 nennt. Prozessdaten verlassen das Werk nur, wenn du es einrichtest: Mails mit Alarmen und Berichten über deinen Mailserver oder die Kopplung an smartlife BI; dazu eine externe Datenbank, falls du sie unter „Datenspeicher“ einrichtest.

Die vollständige Liste steht in der Datenschutzerklärung, Abschnitt 7: plantbeat.io/datenschutz

5 · UPDATES UND BETRIEB

Aktuell bleiben

Prüfung	stündlich über HTTPS beim Lizenzserver
Integrität	Paket wird vor der Installation gegen die SHA-256-Prüfsumme geprüft, die der Lizenzserver liefert
Installer	derzeit ohne Code-Signatur; Prüfsumme steht auf plantbeat.io/downloads
Dienst	optional als Windows-Dienst: startet beim Hochfahren, ohne Anmeldung
Lizenz	wird lokal anhand der digitalen Signatur geprüft, ohne Verbindung

CHECKLISTE FÜR DIE INBETRIEBNAHME

- SPS-Netz vom Werksnetz trennen, PlantBeat-Rechner mit zwei Netzwerkkarten
- Firewall: TCP 102 nur zu den Steuerungen, alles andere nur zu den Zielen aus der Tabelle auf Seite 2
- Bei gesicherten S7-1500: Schutzstufe mit Passwort setzen und das Passwort in der Verbindung hinterlegen; TLS handelt PlantBeat selbst aus
- Zugangsschutz einschalten und Rollen vergeben; „Ansehen ohne Anmeldung erlauben“ abwählen, wenn auch das Ansehen eine Anmeldung verlangen soll
- Steuerungen, die nur beobachtet werden, auf „Nur lesen“ stellen
- Für kritische Werte „Bestätigung vor dem Schreiben“ einschalten
- Für den Hallenmonitor ein Dashboard ohne Steuer-Widgets nehmen: Schalter, Sollwert und Co. bleiben auch im Wandmodus bedienbar
- Updates einspielen, sobald PlantBeat sie meldet
- Aufbewahrung je Wert passend zu deinen Vorgaben einstellen

Fragen aus der IT?

Wir beantworten Fragebögen zur Informationssicherheit und gehen das Netzbild gern mit dir durch.

→ plantbeat.io/anfrage
→ +43 3117 / 93080
→ plantbeat.io/datenschutz

Änderungen und Irrtümer vorbehalten. Gilt für PlantBeat unter Windows, Stand Version 1.10.4.
Siemens, S7 und LOGO! sind Marken der Siemens AG.