Lenze

Datensicherheit, -integrität und -vertraulichkeit

Lenze

Der Inhalt dieser Publikation wurde auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Abweichungen können dennoch nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Publikation werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Die angegebenen Daten dienen allein der Produktbeschreibung und dürfen nicht als garantierte Beschaffenheit des Produkts im Rechtssinn aufgefasst werden. Beschaffenheitsvereinbarungen bleiben dem konkreten Vertragsverhältnis vorbehalten. Etwaige Schadensersatzansprüche gegen uns - gleich aus welchem Rechtsgrund - sind ausgeschlossen, soweit uns nicht Vorsatz oder grobe Fahrlässigkeit trifft.

Inhaltsverzeichnis

Datensicherheit, Integrität and Vertraulichkeit

"Datenschutz hat oberste Priorität und ist der Eckpfeiler des täglichen Betriebs von x4 Remote."

Sicherheit prägt das Tagesgeschäft, die Art und Weise, wie wir die x4 Remote-Plattform-Infrastruktur entwickeln und vieles mehr. Dieses Whitepaper gibt einen Überblick über die Maßnahmen, die in den x4 Remote-Produkten und dem zugehörigen x500 IoT-Gateway ergriffen werden, um die oben genannten Ziele zu erreichen.

Die x4 Remote-Produkte und das zugehörige x500 IoT-Gateway können einen wichtigen Teil Ihres gesamten Sicherheitskonzepts bilden.

Verwaltung der Informationssicherheit

Um die hohe Qualität der x4 Remote Solution und des zugehörigen x500 IoT-Gateways sicherzustellen, arbeitet Lenze mit spezialisierten Lieferanten, externen Entwicklungsteams und externen Produktionsabteilungen zusammen, die mit allen relevanten Sicherheitsaspekten bestens vertraut sind. Der Lieferant der x4 Remote Plattform, das Entwicklungsteam und die Produktionsabteilung für das x500 IoT-Gateway haben ein umfassendes Informationssicherheits-Managementsystem (ISMS) implementiert, das nach dem ISO 27001-Standard zertifiziert ist.

Alle Server der x4 Remote-Plattform befinden sich in Datenzentren, die den höchsten Sicherheitsstandards entsprechen und nach ISO 27001 zertifiziert sind. Alle Cloud-Logging-Daten werden in einem Zeitreihen-Datenbank-Cluster gespeichert, das in einem Rechenzentrum in Deutschland gehostet wird. Andere Daten (z.B. Kundendaten) werden nur in Amsterdam gespeichert.

Die Einhaltung von ISO 27001 zeigt, dass die Lieferanten und externen Teams umfassende Sicherheitsprogramme und -kontrollen implementiert haben, die ihre Informationen und die ihrer Kunden nach international anerkannten Standards schützen.

Der Zugang für Plattform-Entwickler folgt einem streng abgestuften System hinsichtlich der Zugriffsrechte und der damit verbundenen Authentifizierungsmechanismen.

Plattformverfügbarkeit und Integrität

Dank eines systematischen Ansatzes identifizieren, verhindern und verteidigen wir die x4 Remote-Plattform gegen potentielle Schwachstellen und schützen die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer geschäftskritischen Informationen, was zu einer Erfolgsbilanz von

- ✓ Keine Sicherheitsvorfälle
- ✓ Kein Datenverlust
- ✓ > 99% Verfügbarkeit der Cloud

Auf der Grundlage der folgenden Maßnahmen halten wir den Grad der Verfügbarkeit unserer Plattform und die Integrität Ihrer Daten aufrecht.

Lebenszyklus der Software-Entwicklung

Der x4 Remote Softwareentwicklungs-Lebenszyklus konzentriert sich auf die Bereitstellung sicherer, qualitativ hochwertiger Software. Die gesamte Software wird durch ein fortschrittliches Software-Versionsverwaltungssystem verwaltet. Neuer Code wird nach sprachspezifischen Codierungskonventionen und sicheren Codierungstechniken entwickelt.

Alle Software-Änderungen werden von mindestens einem anderen Entwickler überprüft und durch manuelle und vollautomatische Tests gründlich getestet. Das Software-Versionsverwaltungssystem wurde für eine kontinuierliche Integration, Lieferung und Bereitstellung konzipiert. Das bedeutet, dass bei den meisten Software-Aktualisierungen der gesamte Code

- ✓ Automatisch getestet wurde, mit 100% Code Abdeckung;
- ✓ Nach Bestehen der Tests wurde das Release der Software Änderungen automatisch geplant und die
- ✓ Software wurde automatisch released, ohne menschlichen Eingriff.

Diese Methode des automatisierten Testens und Freigebens von Software-Änderungen reduziert die Risiken für jede neue Version erheblich und ermöglicht es Entwicklern, wertvolle Funktionen und Verbesserungen schnell und nachhaltig umzusetzen.

Intelligente Überwachung und Anomalie-Erkennung

Die x4 Remote-Plattform wird rund um die Uhr überwacht, und die Protokolle werden auf einer zentralisierten Protokollierungsplattform gespeichert und analysiert. Die zentralisierte Protokollierungsplattform konzentriert sich hauptsächlich auf die Serverleistung und -stabilität. Sie nutzt künstliche Intelligenz, um kritische Ereignisse und Anomalien in Echtzeit zu erkennen, bevor sie sich auf den Benutzer auswirken.

Ihre Daten sind Ihr Eigentum

Alle vom Benutzer der x4 Remote-Plattform gespeicherten Daten bleiben Eigentum der Benutzer. Sie sind jederzeit verfügbar und vollständig exportierbar.

"Wichtiger Hinweis: Lenze hat keinen Zugriff auf Ihre Daten, es sei denn, Sie laden uns auf Ihr Firmenkonto ein."

x4 Remote-Architektur und Sicherheit

Dienste und Server

Die x4 Remote-Plattform ist ein komplexes Netzwerk von über 50 Servern, die weltweit verteilt sind. Sie ist so strukturiert, dass sie die beste Leistung, Verfügbarkeit und Sicherheit bietet. Es besteht aus zahlreichen Server- und Datenbanktypen, von denen die wichtigsten Typen im Folgenden näher erläutert werden.

API-Dienste

Die API-Dienste (Application Programming Interface) sind das Herzstück von x4 Remote und befinden sich in Datenzentren in Amsterdam. Sie wickeln Schlüsselprozesse in der x4 Remote-Plattform ab, einschließlich Autorisierung, Konfiguration von VPN-Verbindungen und Verbindung zu unseren Datenbanken.

Die API-Dienste sind nicht öffentlich zugänglich, können aber von x4 Remote-Benutzern genutzt werden, nachdem ein eindeutiger API-Schlüssel von Lenze bereitgestellt wurde. Benutzer können die API-Dienste dann für die Erstellung benutzerdefinierter Anwendungen oder Integrationen mit Dritten nutzen.

MQTT-Broker-Dienstleistungen

Die x4 Remote-Plattform verwendet für die Datenübertragung das Message Queuing Telemetry Transport (MQTT)-Protokoll. Das MQTT-Protokoll ist ideal für das industrielle Internet der Dinge, da es hocheffizient und sicher ist, minimalen Overhead hat und die Bandbreitennutzung stark reduziert.

Die MQTT-Brokerdienste werden für das Pushen von Routerkonfigurationen, Firmware-Upgrades und für die Übertragung von Cloud Logging- und Cloud Notify-Daten verwendet. Sie befinden sich physisch in Rechenzentren in Amsterdam.

VPN-Server

VPN-Server befinden sich in Datenzentren auf der ganzen Welt, um Verbindungen mit niedriger Latenz zu ermöglichen. Das VPN-Servernetzwerk ist redundant, d. h. wenn ein VPN-Server ausfällt, übernehmen die anderen Server automatisch die Arbeit. Die API entscheidet anhand des physischen Standorts des x500 IoT-Gateways und des nächstgelegenen VPN-Servers, welcher VPN-Server für die Einrichtung eines sicheren VPN-Tunnels am besten geeignet ist. Sie müssen lediglich unseren VPN-Client (verfügbar im x4 Remote-Portal) installieren, um eine sichere Verbindung von Ihrem Browser zu Ihrem Rechner einzurichten.

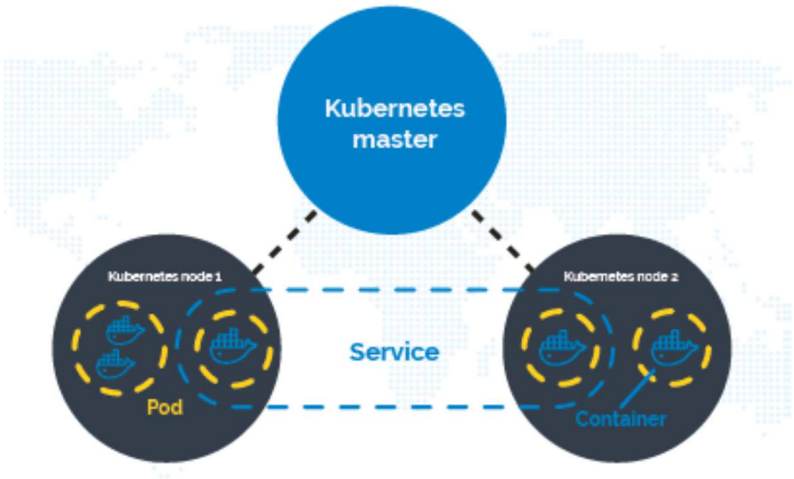
Unser VPN-Client ist eine schlanke Anwendung, die im Hintergrund auf Ihrem Computer läuft und es Ihnen ermöglicht, von Ihrem Browser aus eine sichere VPN-Verbindung zu Ihrem Rechner einzurichten.

Diese VPN-Server werden auch für die Einrichtung von Zugangsverbindungen zu Ihrer HMI oder webbasierten Steuerung verwendet. Es wird ein sicherer VPN-Tunnel vom x500 IoT-Gateway zum Server erstellt, und seine Inhalte werden dann über eine HTTPS- oder sichere WebSocket-Verbindung an Ihren Browser gestreamt.

Kubernetes Cluster

Die x4 Remote-Plattform enthält mehrere Kubernetes-Cluster zur Aktivierung und Verwaltung von Microservices. Dieser moderne Architekturstil gewährleistet eine optimale Skalierbarkeit und Verfügbarkeit der x4 Remote-Plattform. Microservices ermöglichen es, große Anwendungen als eine Sammlung lose gekoppelter, kleinerer Anwendungen (Dienste) zu strukturieren, die individuell und ohne Ausfallzeiten verwaltet und aktualisiert werden können. Jeder Microservice ist als Docker-Container aufgebaut und Kubernetes wird für die Verwaltung all dieser Mikrodienste verwendet.

Der Master des Kubernetes fungiert als Manager für Docker-Container. Er kann diese Container individuell verwalten und aktualisieren, um eine moderne, schnelle und skalierbare Anwendung aufzubauen.



Relationales Datenbank-Cluster

Die relationale Datenbank speichert Informationen über x4 Remote-Benutzer, Firmen, Geräte usw. (Kundendaten). Sie ist redundant mit einer Master-Slave-Struktur über mehrere Rechenzentren in Amsterdam aufgebaut. Der Master empfängt und verarbeitet alle Anfragen zur Ansicht oder Bearbeitung der Datenbank.

Der Slave repliziert alle Schreib-/Aktualisierungsereignisse auf dem Master und erstellt alle vier Stunden ein Backup. Im Falle von Problemen mit dem Master können die Rollen getauscht werden, um die Verfügbarkeit der Datenbank zu gewährleisten. Nur die API, der Slave und der Kubernetes-Cluster können mit dem Master kommunizieren; alle anderen Verbindungen werden gänzlich abgelehnt.

Nicht-relationale Datenbank-Cluster

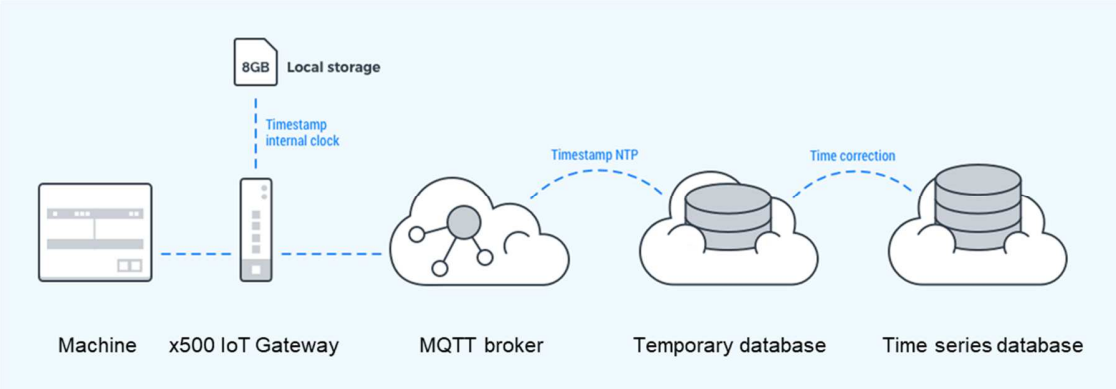
Die nicht-relationale Datenbank speichert Daten über Ereignisse der x4 Remote-Plattform, generierte Alarme, Protokolle usw. Diese Datenbank ist als Replikationssatz konfiguriert, von dem der primäre Server alle Anfragen empfängt und verarbeitet, während der sekundäre Server den primären Server repliziert.

Diese Konfiguration gewährleistet hohe Verfügbarkeit und Redundanz für die nicht-relationale Datenbank. Nur die x4 Remote-API, andere Server im Replikatsatz oder Kubernetes-Cluster können mit der nicht-relationalen Datenbank kommunizieren; alle anderen Verbindungen werden gänzlich abgelehnt. Die Datenbankserver befinden sich in mehreren Datenzentren in Amsterdam.

Zeitreihen-Datenbank-Cluster

Maschinendaten, die mit Cloud Logging gesammelt werden, werden über das schlanke und hocheffiziente MQTT-Protokoll gesendet. Dieses Protokoll verwendet den MQTT-Broker: eine zentrale Station zum Empfangen und Senden von Datennachrichten. Nachdem das x500 IoT-Gateway die Daten gesammelt hat, werden sie zunächst an einen MQTT-Broker weitergeleitet. Dort werden sie mit einem Zeitstempel versehen und in einer Pufferdatenbank gespeichert. Als nächstes wird eine Zeitkorrektur vorgenommen, um mögliche Diskrepanzen zwischen der internen Uhr des x500 IoT-Gateways und der NTP-Zeit (tatsächliche Zeit) zu berücksichtigen.

Schließlich werden die Daten in einem Zeitreihendatenbank-Cluster (InfluxDB) gespeichert, das in einem Datenzentrum in Frankfurt, Deutschland, gehostet wird. Der Hauptvorteil einer Zeitreihendatenbank besteht darin, dass sie für den Umgang mit zeitgestempelten Daten optimiert ist. Dies ermöglicht es Benutzern, Daten über einen großen Zeitraum in nur wenigen Millisekunden abzufragen und Operationen, wie z.B. die Berechnung des Mittelwerts, schnell und hocheffizient durchzuführen. Darüber hinaus ermöglichen Zeitreihendatenbanken erweiterte Optionen für das Daten-Lebenszyklusmanagement, wie z. B. Aggregation oder Down-Sampling Ihrer Maschinendaten.



Sicherheitskontrollen

Verschlüsselte Verbindungen

Verschlüsselte Verbindungen sind notwendig, um Angriffe zu verhindern, durch die Angreifer Zugang zu Konten und sensiblen Informationen erhalten können.

Alle Verbindungen zur und von der x4 Remote-Plattform und zwischen den Plattformdiensten werden daher über HTTPS mit TLS 1.2 oder höher verschlüsselt. MQTT-Verbindungen sind ebenfalls TLS-verschlüsselt, um die Vertraulichkeit Ihrer Maschinendaten zu gewährleisten. VPN-Verbindungen verwenden Einweg-VPN-Zertifikate und werden mit AES-256-CBC mit SHA512 verschlüsselt.

x4 Remote-Benutzer-Passwörter werden als Hashes unter Verwendung von PBKDF2 mit 12 Bytes Salt, 12000 Iterationen und SHA512 + HMAC gespeichert.

Die Auswahl der verwendeten Algorithmen richtet sich nach den NIST-Richtlinien.

Interne Zugriffskontrolle

Alle Teilnehmer, die an der Entwicklung und Wartung von x4 Remote beteiligt sind, haben ein strenges Kontrollsystem für den Zugriff auf die Server implementiert. Nur wenige leitende Entwickler sind in der Lage, auf die Server der x4 Remote-Plattform zuzugreifen. Anderen Entwicklern kann vorübergehend Zugang zu einem Server gewährt werden, wenn dies für ihre Aufgabe erforderlich ist, und zwar unter der direkten Aufsicht eines leitenden Entwicklers. Entwickler melden sich mit ihrem eigenen, eindeutigen, SSH-Schlüssel bei den Servern an. Alle Server-Anmeldungen und -Änderungen werden rund um die Uhr überwacht und zur Analyse auf der zentralisierten Protokollplattform protokolliert.

Schwachstellen-Management

Eine Schwachstellenlösung eines Drittanbieters scannt die x4 Remote-Plattform regelmäßig auf externe Schwachstellen. Die Scan-Ergebnisse werden in einer zentralisierten Übersicht gemeldet und vom Sicherheitsbeauftragten bewertet. Darüber hinaus werden die x4 Remote-Server täglich von einer anderen Drittpartei geprüft, die auf Serversicherheit und Systemhärtung spezialisiert ist. Das Server-Auditing zielt darauf ab, den Systemzustand zu bestimmen, indem interne Schwachstellen oder Schwachstellen im Konfigurationsmanagement aufgedeckt werden. Es gibt auch interne Penetrationstests und jedes Jahr einen zusätzlichen externen Penetrationstest.

Eine zentralisierte Übersicht der Auditergebnisse zeigt den Status jedes Servers und gibt Hinweise für Verbesserungen. So können wir schnell auf eventuelle Schwachstellen reagieren und bestätigen, dass jeder Server den höchsten Sicherheitsstandards entspricht.

x4 Remote-Benutzerportal-Sicherheit

Login-Sicherheit (mit optionaler Zwei-Faktor-Authentifizierung)

Auf die x4 Remote-Plattform kann über einen modernen Webbrowser von Ihrem mobilen Gerät zugegriffen werden. Benutzer melden sich mit ihrem Benutzernamen und Passwort an. Wenn die Zwei-Faktor-Authentifizierung aktiviert ist, werden die Benutzer auch aufgefordert, ein Einmal-Passwort einzugeben. Einmal-Passwörter fügen Ihrem Konto eine zusätzliche Sicherheitsebene hinzu. Sie werden von einer App (z. B. Google Authenticator) auf Ihrem Mobilgerät generiert und bleiben 30 Sekunden lang gültig.

Bei erfolglosen Anmeldeversuchen kehrt der Benutzer zum Anmeldebildschirm zurück. Nach fünf fehlerhaften Versuchen wird der Benutzer für einige Sekunden von seinem Konto gesperrt. Diese Zeit erhöht sich exponentiell (bis zu 1 Stunde) bei nachfolgenden fehlerhaften Versuchen.

Benutzerverwaltung

Über das x4 Remote-Benutzerportal können administrative Rollen und Benutzerprivilegien von Unternehmensadministratoren konfiguriert und kontrolliert werden. Das bedeutet, dass einzelne Benutzer in einem Unternehmen auf bestimmte Dienstleistungen zugreifen oder diese verwalten oder Zahlungen vornehmen können, ohne Zugriff auf alle Einstellungen und Daten zu erhalten. Beispielsweise kann einem Benutzer nur Zugriff auf bestimmte Geräte gewährt werden.

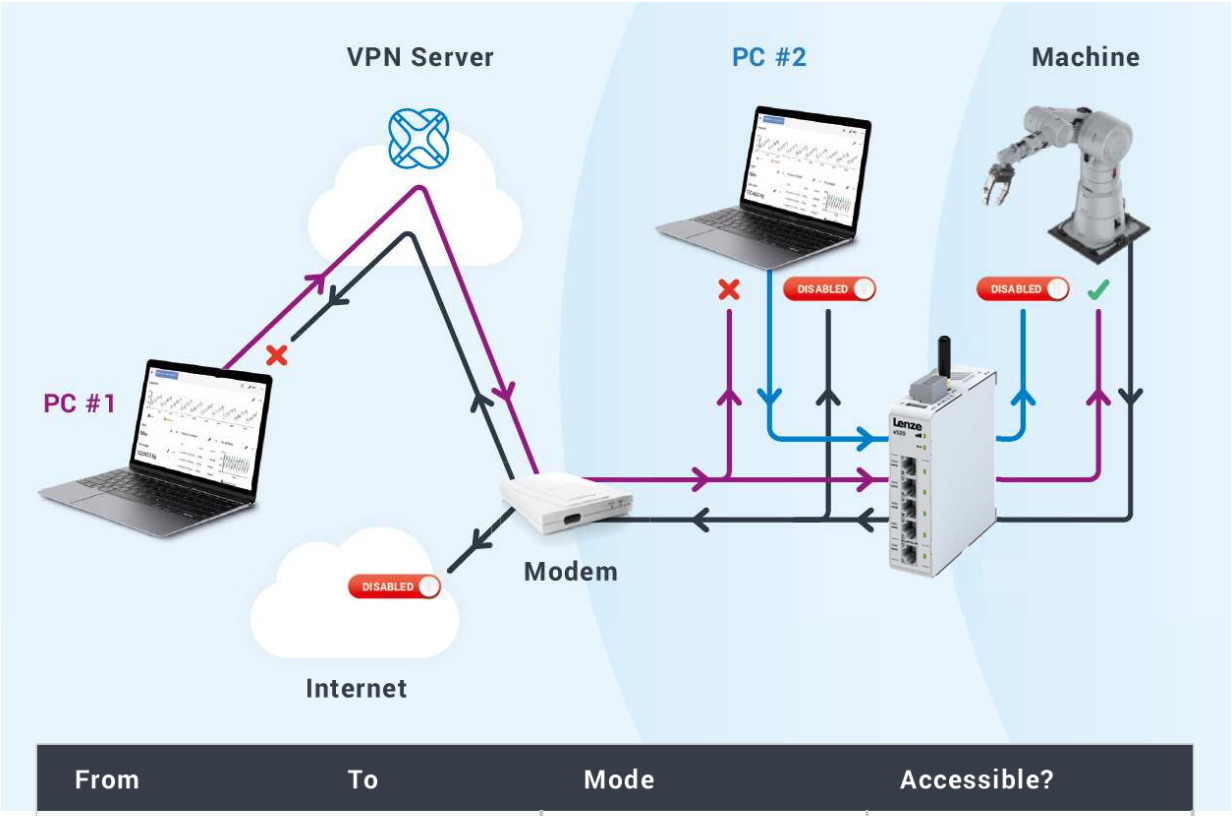
x500 IoT-Gateway-Sicherheit

Integrierte Firewall

Maschinensteuerungen wurden nie für die Sicherheit konzipiert. Ihre Betriebssysteme werden nicht aktualisiert und enthalten nicht die neuesten Sicherheitsmechanismen. Es ist zwingend erforderlich, dass diese Maschinensteuerungen niemals mit einem Firmennetzwerk verbunden werden, während sie mit anderen Geräten verbunden sind. Das x500 IoT-Gateway kann diese mit seiner integrierten Firewall vom Firmennetzwerk isolieren.

Das x500 IoT-Gateway ist ein robuster und kompakter Industrierouter, der Maschinen mit der x4 Remote-Plattform verbindet. Seine integrierte Firewall trennt den WAN-Port (Firmennetzwerk) vollständig von den LAN-Ports (Maschinennetzwerk). Er blockiert die gesamte Kommunikation mit Ausnahme von autorisierten und verschlüsselten Daten, die durch ein gültiges Identitätszertifikat verifiziert wurden. Das bedeutet, dass nur autorisierte Benutzer über die x4 Remote-Plattform auf das Maschinennetz zugreifen können.

"Die Firewall blockiert standardmäßig alle Verkehr vom WAN zu den LAN-Ports - und umgekehrt.”



From		To	Mode	Accessible?
PC #1	›	Machine	VPN	✓
PC #1	›	PC #2	VPN	✗
PC #2	›	Machine	TCP	DISABLED (1)
Machine	›	PC #2	TCP	DISABLED (1)
Machine	›	Internet	TCP	DISABLED (1)
Machine	›	PC #1	VPN	✗

(1) Disabled by default.

Nur ausgehende Ports

Das x500 IoT-Gateway verwendet nur ausgehende Ports, um eine sichere Verbindung zur x4 Remote-Plattform herzustellen, so dass es nicht notwendig ist, eingehende Ports auf der lokalen Firewall im Firmennetzwerk zu öffnen.

Port	Protokoll	Applikation
443, 8443 (1)	TCP	HTTPS, MQTT (TLS), OpenVPN
53 (2)	TCP UND UDP	DNS

(1) Port 8443 wird nur verwendet, wenn der Stealth-Modus für die Konnektivität über eine überwachte Internetverbindung aktiviert ist (d.h. wenn sich der Standort in China befindet).

(2) DNS-Anfragen werden häufig von lokalen DNS-Servern bearbeitet. In diesen Fällen kann der aufgeführte DNS-Port ignoriert werden.

Beschränkung des Netzzugangs

MAC-Adresse

Die lokale IT-Abteilung kann sich dafür entscheiden, nur bestimmten Geräten Internetzugang zu gewähren, basierend auf der MAC-Adresse oder der IP-Adresse des Geräts. Die MAC-Adresse kann vom Aufkleber an der Seite des x500 IoT-Gateways oder von der Info Panel in der x4 Remote-Plattform abgerufen werden.

IP-Adresse

Die IP-Adresse kann auf eine statische IP-Adresse eingestellt werden. Standardmäßig ist die IP-Adresse jedoch so eingestellt, dass sie automatisch über DHCP bezogen wird.

Hardware-Trennung

Die VPN-Verbindung kann lokal über einen Hardware-Schalter (digitaler Eingang) abgeschaltet werden.

Ausfallsicherheit

Netzwerk-Fallback-Optionen

Sollte Ihre bevorzugte Verbindung abbrechen, verbindet sich das x500 IoT-Gateway automatisch mit einem anderen Netzwerk. Dies ist für Wi-Fi, 4G und Ethernet vollständig konfigurierbar. Jede Verbindung wird ständig überprüft, indem alle paar Sekunden Keep-Alive-Nachrichten an eine öffentliche IP-Adresse gesendet werden.

Wenn die Verbindung mehrmals hintereinander ausfällt, gilt die Verbindung als unterbrochen, und das x500 IoT-Gateway verbindet sich automatisch mit dem ersten (oder zweiten) Fallback. Wenn das bevorzugte Netzwerk wieder verfügbar ist, schaltet das x500 IoT-Gateway automatisch wieder auf das bevorzugte Netzwerk um. Die IP-Adresse für Keep-Alive-Meldungen und das Zeitintervall können je nach Bedarf geändert werden.

Offline-Datenprotokollierung

Internetverbindungen sind nicht immer stabil und können von Zeit zu Zeit ausfallen. In manchen Situationen, wie z.B. auf einem Schiff, kann es sogar vorkommen, dass überhaupt keine Internetverbindung zur Verfügung steht. Dies ist problematisch für Benutzer, die ihre Maschinendaten unter solchen Bedingungen protokollieren möchten.

Um dieses Problem zu lösen, verfügt das x500 IoT-Gateway über einen separaten 8-GB-Flash-Speicher, der es ermöglicht, Maschinendaten wochenlang offline zu speichern. Sobald das x500 IoT-Gateway wieder online ist, werden alle Maschinendaten automatisch über eine verschlüsselte Verbindung an die x4 Remote-Plattform gesendet.

Darüber hinaus können Benutzer mit der Cloud Notify-Funktion Benachrichtigungen erhalten, wenn das x500 IoT-Gateway für eine bestimmte Zeitspanne (normalerweise eine Stunde) offline war. Auf diese Weise können Benutzer schnell auf etwaige Konnektivitätsprobleme reagieren und diese Probleme so schnell wie möglich beheben.

Eine sichere, zuverlässige und vertrauenswürdige IoT-Lösung

Mit der x4 Remote-Plattform bietet Lenze Maschinenbauern eine hochsichere und fortschrittliche Plattform für das industrielle Internet der Dinge. Umfassende Sicherheitskontrollen und redundante Server weltweit sind der Schlüssel für eine sichere, zuverlässige und vertrauenswürdige IoT-Lösung um Ihre Daten gemäß den „best Practice“ der Branche zu schützen.

Unternehmen auf der ganzen Welt vertrauen Lenze ihr wertvollstes Gut an: Informationen. Lenze wird auch weiterhin in Sicherheit und neue Innovationen investieren, damit die Nutzer der x4 Remote-Plattform ihr volles Potenzial auf sichere Art und Weise nutzen können.