Lenze

Data security, integrity & confidentiality

Lenze

The content of this publication has been checked for consistency with the hardware and software described. Deviations can nevertheless not be excluded, so that we can not guarantee for the complete conformity. The information contained in this publication is regularly checked and necessary corrections are included in the subsequent editions.

All specifications are only of a descriptive nature and must not be understood as guaranteed product properties in a legal sense. Exact properties and characteristics shall be agreed in the specific contract. Claims for damages against us - on whatever reasons - are excluded, except in instances of deliberate intent or gross negligence on our part.

Table of Content

Data Security, Integrity and Confidentiality

"Data protection is the number one priority and the cornerstone of everyday operations of X4 Remote."

Security shapes the day-to-day business, how we develop the x4 Remote platform infrastructure, and more. This white paper gives an overview of the measures taken in the x4 Remote products and the associated x500 IoT gateway to achieve the above mentioned goals.

The x4 Remote products and the associated x500 IoT gateway can build an important part of your overall security concept.

Information Security Management

To ensure the high quality of the x4 Remote Solution and the associated x500 IoT gateway Lenze works with specialized suppliers, external Development Teams and external Production Departments which are very familiar with every relevant Aspect of Security.
The supplier of the x4 Remote Platform, the Development Team and Production Department for the x500 IoT Gateway have implemented a comprehensive information security management system (ISMS) that is certified according to the ISO 27001 standard.

All servers of the X4 Remote platform are located in data centers which uphold the highest security standards and have obtained ISO 27001 certification. All cloud logging data are stored in a time-series database cluster, which is hosted in a data center in Germany. Other data (e.g. customer data) only stored in Amsterdam.

Compliance with ISO 27001 shows that the suppliers and external Teams have implemented comprehensive security programs and controls that protect their information and those of their customers in accordance with internationally recognized standards.

The access for platform developers follows a strict graded system regarding access rights and associated authentication mechanisms.

Platform Availability and Integrity

Thanks to a systematic approach, we identify, prevent and defend the X4 Remote platform against potential vulnerabilities and we safeguard the confidentiality, integrity and availability of your business-critical information, resulting in a track record of

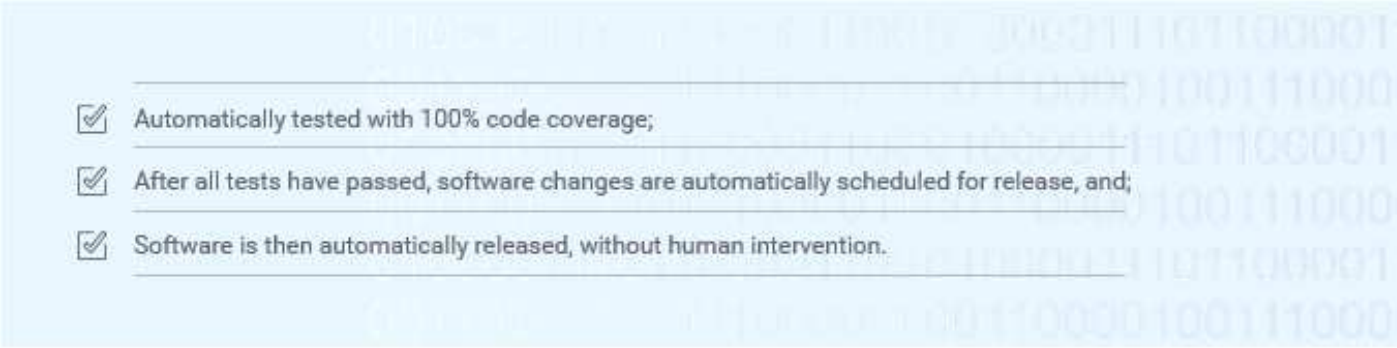
- ✓ No security incidents
- ✓ No data loss
- ✓ >99% uptime of the cloud

Based on the following measures we are committed to continue the level of availability of our platform and the integrity of your data.

Software development life cycle

The X4 Remote software development life cycle is focused on delivering secure, high quality software. All software is tracked through an advanced software versioning management system. New code is developed following language-specific coding conventions and secure coding techniques.

All software changes are reviewed by at least one other developer and are thoroughly tested through manual and fully automated tests. The software versioning management system has been designed for continuous integration, delivery and deployment. This means that for most software updates, all code is:



This method of automated testing and releasing software changes greatly reduces risks for each release and enables developers to get valuable features and improvements out fast and in a sustainable way.

Smart monitoring and anomaly detection

The X4 Remote platform is monitored 24/7 and logs are stored and analyzed on a centralized logging platform. The centralized logging platform is mainly focused on server performance and stability. It uses artificial intelligence to detect critical events and anomalies in real time before they affect user.

Your Data is Your Property

All data stored by user of the X4 Remote platform remains the property of its users. Always available and fully exportable.

> “Important Note: Lenze has no access to your data, unless you invite us to your company account.”

X4 Remote Architecture and Security

Services and Servers

The X4 Remote platform is a complex network of over 50 servers, distributed worldwide. It is structured to provide the best performance, availability and security. It consists of numerous server and database types, of which the key types are discussed below in more detail.

API services

The application programming interface (API) services are the heart of X4 Remote and are located in data centers in Amsterdam. They handle key processes in the X4 Remote platform, including authorization, configuring VPN connections and connecting to our databases.

The API services are not publicly accessible, but can be used by X4 Remote users after a unique API key is provided by Lenze. Users are then able to use the API services for creating custom applications or integrations with third parties.

MQTT broker services

The X4 Remote platform uses the Message Queuing Telemetry Transport (MQTT) protocol for data transfer. The MQTT protocol is ideal for the Industrial Internet of Things, because it is highly efficient, secure, has minimal overhead and greatly diminishes bandwidth use.

The MQTT broker services are used for pushing router configurations, firmware upgrades and for the transmission of Cloud Logging and Cloud Notify data. They are physically located in data centers in Amsterdam.

VPN servers

VPN servers are located in data centers around the world to provide low-latency connections. The VPN server network is redundant, so if one VPN server goes down, the other servers will take over automatically. The API decides which VPN server is best for setting up a secure VPN tunnel, based on the physical location of the x500 IoT Gateway and its nearest VPN server. All you need to do is install our VPN client (available in the X4 Remote portal) for setting up a secure connection from your browser to your machine.

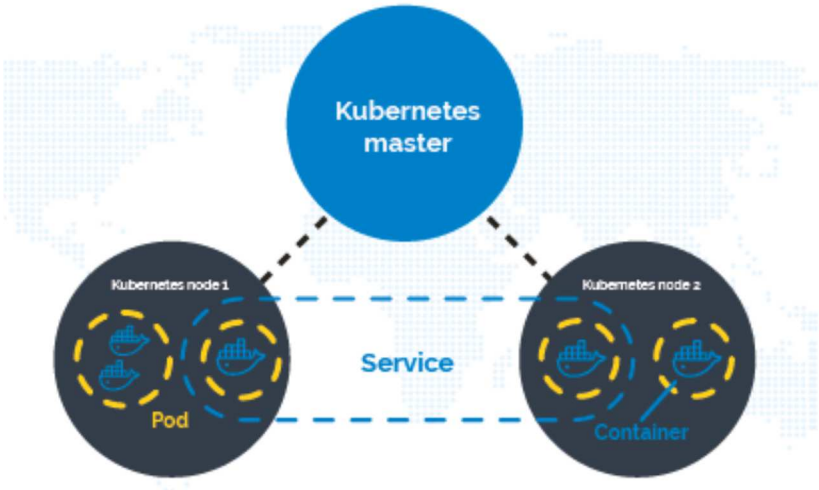
Our VPN client is a lightweight application, running in the background on your computer that enables you to set up a secure VPN connection to your machine from within your browser.

These VPN servers are also used for setting up access connections to your HMI or web-based controls. A secure VPN tunnel is created from the x500 IoT Gateway to the server and its contents are then streamed to your browser using an HTTPS or secure WebSocket connection.

Kubernetes cluster

The X4 Remote platform contains multiple Kubernetes clusters for enabling and managing microservices. This modern architectural style ensures optimal scalability and availability of the X4 Remote platform. Microservices allow large applications to be structured as a collection of loosely coupled, smaller applications (services) that can be managed and updated individually, without downtime. Each Microservice is built as a Docker container and Kubernetes is used for managing all these Microservices.

The Kubernetes master acts as a manager for Docker containers. It can manage and update these containers individually, in order to build a modern, fast and scalable application.



Relational database cluster

The relational database stores information about X4 Remote users, companies, devices, etc (customer data). It is set up redundantly using a master-slave structure across multiple data centers in Amsterdam. The Master receives and processes all requests to view or edit the database.

The Slave replicates all write/update events on the Master and creates a backup every four hours. In case of any issues with the Master, the roles can be switched to ensure database availability. Only the API, Slave and Kubernetes cluster are able to communicate with the Master; all other connections are refused outright.

Non-relational database cluster

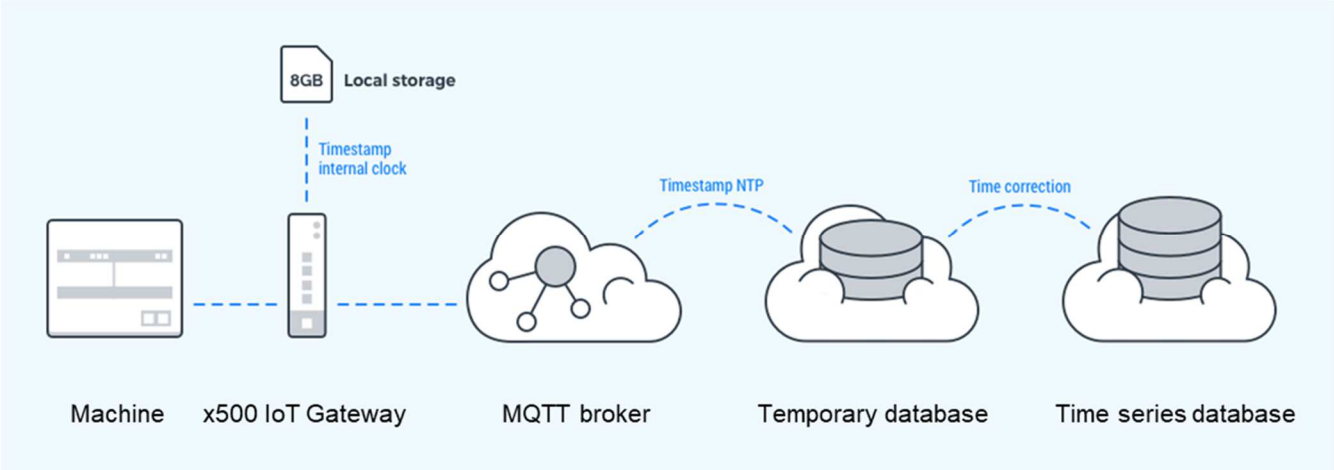
The non-relational database stores data on X4 Remote platform events, generated alarms, logs, etc. This database is configured as a replica set, of which the primary server receives and processes all requests, and the secondary server replicates the primary server.

This configuration ensures high availability and redundancy for the non-relational database. Only the X4 Remote API, other servers in the replica set or Kubernetes cluster are able to communicate with the non-relational database; all other connections are refused outright. The database servers are located across multiple data centers in Amsterdam.

Time series database cluster

Machine data gathered with Cloud Logging is sent to the lightweight and highly efficient MQTT protocol. This protocol uses the MQTT broker: a central station for receiving and sending data messages. After the x500 IoT Gateway collects the data, it is first passed to our MQTT broker. There it is time stamped and stored in a buffer database. Next, a time correction is applied to account for any possible discrepancies between the x500 IoT Gateway's internal clock and the NTP time (actual time).

Finally, the data is stored in a time series database cluster (InfluxDB), which is hosted in a data center in Frankfurt, Germany. The main advantage of a time series database is that it's optimized for handling time stamped data. This allows users to request data over a large period of time in just a few milliseconds and perform operations, such as calculating the mean value, in a fast and highly efficient manner. Furthermore, time series databases allow for advanced data lifecycle management options, such as aggregation or down sampling of your machine data.



Security Controls

Encrypted connections

Encrypted connections are necessary to prevent attacks which can let attackers gain access to accounts and sensitive information.

All connections to and from the X4 Remote platform and between platform services are therefore encrypted using HTTPS with TLS 1.2 or higher. MQTT connections are also TLS encrypted to ensure the confidentiality of your machine data. VPN connections use single-use VPN certificates and are encrypted using AES-256-CBC with SHA512.

X4 Remote user passwords are stored as hashes using PBKDF2 with 12 bytes salt, 12000 iterations and SHA512 + HMAC.

The selection of the used Algorithms is based on NIST Guidelines.

Internal access control

All participants that are involved in development and maintenance of X4 Remote have implemented a strict control system for accessing servers. Only a few senior developers are able to access the X4 Remote platform servers. Other developers may be given access to a server temporarily, if this is necessary for their task, under the direct supervision of a senior developer. Developers log into servers using their own unique SSH key. All server logins and changes are monitored 24/7 and logged to the centralized logging platform for analysis

Vulnerability management

A third-party vulnerability solution scans the X4 Remote Platform regularly for any external vulnerabilities. Scan results are reported in a centralized overview and assessed by the security officer. In addition, X4 Remote servers are audited daily by another third party specialized in server security and system hardening. Server auditing is aimed at determining system health by detecting any internal vulnerabilities or configuration management weaknesses. There are also internal penetration tests and an additional external penetration test every year.

A centralized overview of the audit results shows the status of each server and provides guidance for improvement. This enables us to quickly react to any vulnerabilities and to confirm that each server matches the highest security standards.

X4 Remote User Portal Security

Login Security (with optional Two-Factor Authentication)

The X4 Remote platform can be accessed via modern web browser on your mobile device. Users log in with their username and password. If two-factor authentication is enabled, users are also prompted to enter a one-time password. One-time passwords add an extra layer of security to your account. They are generated by an app (e.g. Google Authenticator) on your mobile device and remain valid for 30 seconds.

Unsuccessful login attempts return the user to the login screen. After five incorrect attempts, the user is locked out of his/her account for a number of seconds. This time increases exponentially (up to 1 hour) with subsequent incorrect attempts.

User Management

From the X4 Remote user portal, administrative roles and user privileges can be configured and controlled by company administrators. This means that individual users in a company can access or manage certain services or make payments without gaining access to all settings and data. For instance, a user may only be given access to certain devices.

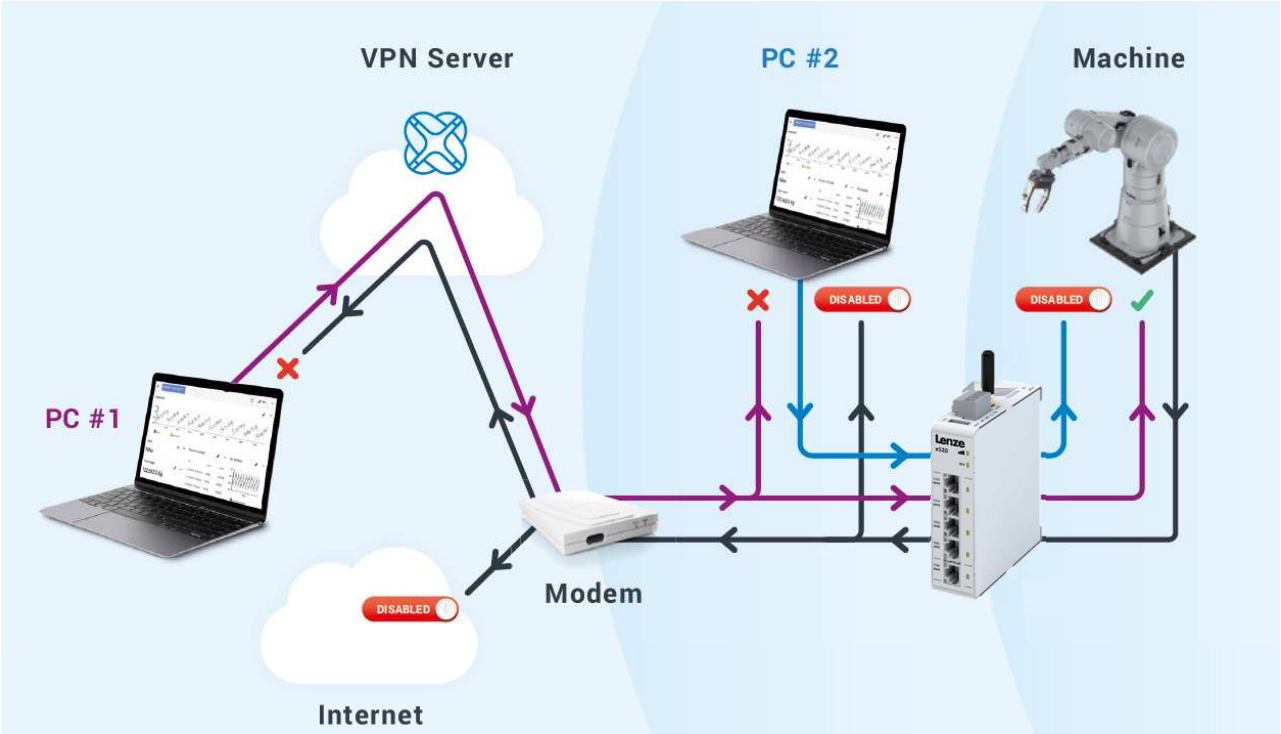
x500 IoT Gateway Security

Built-in Firewall

Machine controllers were never designed for security. Their operating systems are not updated and do not contain the latest security mechanisms. It is imperative that these machine controllers are never connected to a company network while linked to other devices. The x500 IoT Gateway can isolate these from the company network with its built-in firewall.

The x500 IoT Gateway is a robust and compact industrial router that connects machines to the X4 Remote platform. Its built-in firewall completely separates the WAN port (company network) from the LAN ports (machine network). It blocks all communication except for authorized and encrypted data verified by a valid identity certificate. This means that only authorized users can access the machine network via the X4 Remote platform.

"The firewall blocks all traffic from the WAN to the LAN ports - and vice versa - by default."

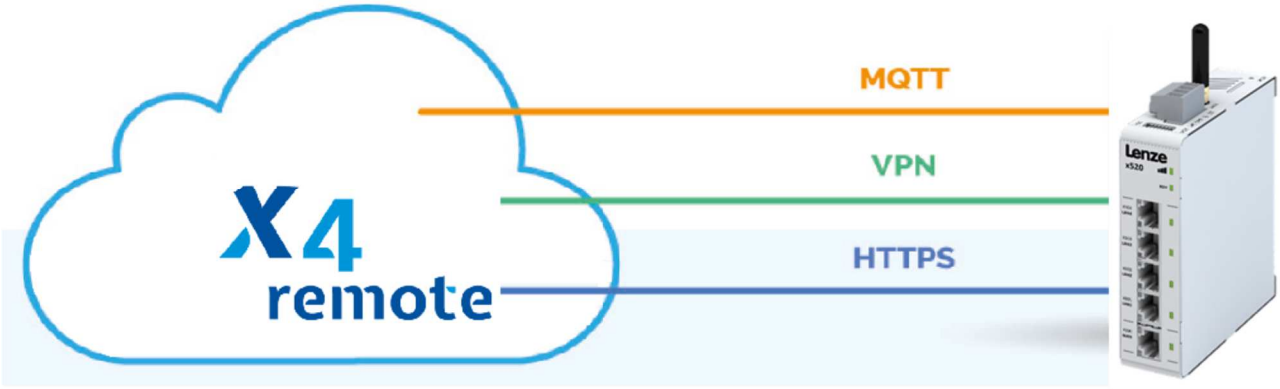


From	To	Mode	Accessible?
PC #1	Machine	VPN	✓
PC #1	PC #2	VPN	✗
PC #2	Machine	TCP	DISABLED (1)
Machine	PC #2	TCP	DISABLED (1)
Machine	Internet	TCP	DISABLED (1)
Machine	PC #1	VPN	✗

(1) Disabled by default.

Outgoing Ports Only

The x500 IoT Gateway only uses outgoing ports to establish a secure connection to the X4 Remote platform, so there is no need to open any incoming ports on the local firewall in the company network.



Port	Transport	Application
443, 8443 (1)	TCP	HTTPS, MQTT (TLS), OpenVPN
53 (2)	TCP & UDP	DNS

(1) Port 8443 is only used when stealth mode is activated for connectivity via a censored internet connection (i.e. when located in China).

(2) DNS requests are often handled by local DNS servers. In those cases the listed DNS port can be ignored.

Network Access Restriction

MAC address

The local IT department may choose to only grant specific devices internet access, based on the MAC address or IP address of the device. The MAC address can be obtained from the label on the side of the x500 IoT Gateway or from the info panel in the X4 Remote platform.

IP address

The IP address can be set to a static IP address. However, by default the IP address is set to be obtained automatically via DHCP.

Hardware disconnect

The VPN connection can be locally turned off via hardware switch (digital Input).

Failover Capabilities

Network fallback options

Should your preferred connection drop, the x500 IoT Gateway will automatically connect to another network. This is fully configurable for Wi-Fi, 4G, and Ethernet. Each connection is constantly checked by sending keep-alive messages to a public IP address every few seconds.

If the connection fails multiple consecutive times, the connection is considered down and the x500 IoT Gateway will automatically connect to the first (or second) fallback. If the preferred network is up again, the x500 IoT Gateway will automatically switch back to the preferred network. The IP address for keep-alive messages and time interval can be changed according to individual needs.

Offline data logging

Internet connections are not always stable and may go down from time to time. In some situations, such as on a ship, there might not even be an internet connection available at all. This is problematic for users who wish to log their machine data in such conditions.

To solve this, the x500 IoT Gateway has an separate 8GB flash memory which allows machine data to be stored offline for weeks at a time. As soon as the x500 IoT Gateway comes back online again, all machine data is automatically sent to the X4 Remote platform over an encrypted connection.

Additionally, users are able to receive notifications when the x500 IoT Gateway has been offline for a specified number of time (typically one hour) with the Cloud Notify functionality. This allows users to quickly react to any connectivity problems and fix these issues as soon as possible.

A safe, reliable and trustworthy IoT solution

With the X4 Remote platform, Lenze offers machine builders a highly secure and advanced Industrial Internet of Things platform. Comprehensive security controls and redundant servers worldwide are key in achieving a safe, reliable and trustworthy IoT solution. Protecting your information is our top priority and we will do anything to secure your data, following industry best practices.

Companies across the globe trust Lenze with their most valuable asset: information. Lenze will continue to invest in security and new innovations to allow X4 Remote platform users to benefit from its full potential in a secure manner.