CLAIMS

1. A gateway device comprising:

a first interface configured to receive command signals encrypted according to a first encryption protocol from a server and to send data signals encrypted according to the first encryption protocol to the server;

a second interface configured to send command signals encrypted according to a second encryption protocol to a bridge device and to receive data signals encrypted according to the second encryption protocol from the bridge device;

cryptographic key storage configured to store cryptographic keys for the first encryption protocol and cryptographic keys for the second encryption protocol; and

a processor configured to:

decrypt command signals encrypted according to the first encryption protocol using the cryptographic keys for the first encryption protocol and encrypt the command signals according to the second encryption protocol; and

decrypt data signals encrypted according to the second encryption protocol using the encryption keys for the second encryption protocol and encrypt the data signals according to the first encryption protocol,

wherein the first encryption protocol and / or the second encryption protocol is a hybrid of pre-quantum encryption algorithms and post-quantum algorithms.

2. A gateway device according to claim 1, wherein the first encryption protocol is a transport layer security (TLS) protocol.

3. A gateway device according to claim 1 or claim 2, wherein the second encryption protocol is a lightweight secure data communications protocol.

4. A gateway device according to any preceding claim, wherein the processor is further operable to initiate a key exchange with the server and / or the bridge device.

5. A gateway device according to any preceding claim, wherein the processor is further configured to check and / or transform, and / or filter, and / or consolidate the command signals after decryption and before encryption.

6. A gateway device according to any preceding claim, wherein the processor is further configured to check and / or transform, and / or filter, and / or consolidate the data signals after decryption and before encryption.

7. A gateway device according to any preceding claim, wherein the processor is further configured to analyze the data signals and determine integrity of the data signals.

8. A gateway device according to any preceding claim, wherein the processor is further operable to monitor a power supply and / or tamper inputs to detect physical intrusions.

9. A gateway device according to claim 8, wherein the processor is operable to delete the cryptographic keys stored in the cryptographic key storage if a physical intrusion is detected.

10. A bridge device comprising:

a device interface configured to send command signals to an actuator device and to receive data signals from a sensor device;

a gateway interface configured to receive command signals encrypted according to an encryption protocol from a gateway device and to send data signals encrypted according to the encryption protocol to the gateway device;

cryptographic key storage configured to store encryption keys for the encryption protocol; and

a processor configured to decrypt command signals encrypted according to the encryption protocol and to send the decrypted command signals to the actuator device and to encrypt data signals received from the sensor device according to the encryption protocol and send the encrypted data signals to the gateway device,

wherein the first encryption protocol and / or the second encryption protocol is a hybrid of pre-quantum encryption algorithms and post-quantum algorithms.

11. A bridge device according to claim 10, wherein the encryption protocol is a lightweight secure data communications protocol.

12. A bridge device according to any one of claims 10 to 11, wherein the processor is further configured to check and / or transform, and / or filter, and / or consolidate the command signals after decryption and before sending to the actuator device.

13. A bridge device according to any one of claims 10 to 12, wherein the processor is further configured to check and / or transform, and / or filter, and / or consolidate the data signals before encryption.

14. A bridge device according to any one of claims 10 to 13, wherein the processor is further configured to analyze the data signals and determine integrity of the data signals.

15. A bridge device according to any one of claims 10 to 14, wherein the processor is further operable to monitor a power supply and / or tamper inputs to detect physical intrusions.

16. A bridge device according to any one of claims 10 to 15, wherein the processor is operable to delete the cryptographic keys stored in the cryptographic key storage if a physical intrusion is detected.

17. A monitoring system comprising a gateway device according to any one of claims 1 to 8; a bridge device according to any one of claims 10 to 16; at least one sensor coupled to the bridge device; and at least one actuator coupled to the bridge device.