CRA SAMPLE

D05 Network and system architecture

Example after one year of operation, status 28.02.2028 · Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect

Publisher	OT-Cyber.de, Max Gilg, Rosenheim
Sample company	Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect (fictitious)
Note	Free sample, not legal advice

Company, people, data and numbers are fictitious. This is how the document looks after one year of operation.

1 Purpose and scope

Zones and conduits according to IEC 62443-3-2, permitted data flows, remote maintenance and update chain.

2 Document control

Field	Entry
Document no.	NWT-CE-D05
Version, status	1.3, approved
Scope	NWT HACKTHERM 60 connect (18 to 60 kW), controller, gateway, portal and app
Author	Jonas Weiß, Engineering and Product Security (PSO)
Checked by	Ingenieurbüro Lechner (safety), Sichtwerk Security (security)
Approval	Michael Berger, Managing Director, 28.02.2028
Next review	15.03.2029 or in the event of a substantial modification
Confidentiality	internal
Filing	Technical documentation NWT-TD-HT60C, retained for at least 10 years after the last unit is placed on the market

3 Overview drawing

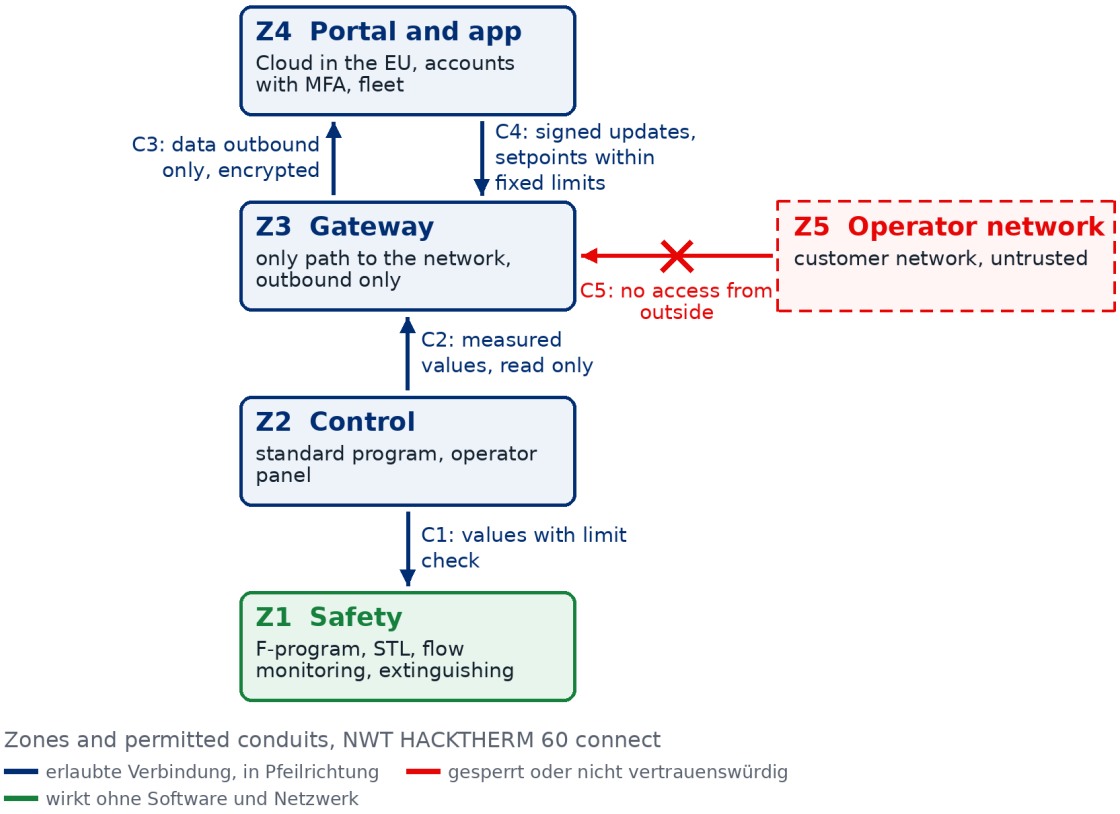


Figure: Zones and permitted conduits, NWT HACKTHERM 60 connect

How to read the drawing: each box is a zone with its own protection, each arrow is a permitted connection in the direction of the arrow. Everything else is blocked. Safety (Z1, green) does not depend on any external connection; an attack via the portal or the gateway cannot disable it.

4 Zones

Zone	Content	Target SL	Responsible
Z1 Safety	F-program, F-I/O, STL	SL 2	Weiß
Z2 Control	Standard program, operator panel	SL 2	Weiß
Z3 Gateway	Gateway, only path to the network	SL 2	Datenwerk
Z4 Portal and app	Cloud, accounts, fleet	SL 2	Datenwerk
Z5 Operator network	Customer network, untrusted	outside	Customer

Legend: Z = zone; target SL = target security level according to IEC 62443-3-2 (1 to 4).

5 Conduits

Conduit	From, to	Permitted	Protection
C1	Z2 to Z1	Values via F-interface	Limit check in F-program
C2	Z2 to Z3	Modbus TCP read only	Dedicated cable, no writing
C3	Z3 to Z4	MQTT TLS 1.3 outbound	Certificate per device
C4	Z4 to Z3	Comfort setpoints, updates	Signed, limits
C5	Z5 to Z3	Nothing inbound	Gateway firewall

Legend: conduit = permitted connection between two zones.

Remote maintenance takes place via the portal only: the operator approves a session in the app, with a time limit of no more than four hours, MFA for the service account and logging. All commands that trigger movement or change safety data remain blocked. Updates are signed and are rolled out first to 1% of the fleet and, after 48 hours, to all devices; the gateway verifies the signature before installation and retains the previous version.

6 Terms and abbreviations

CE: CE marking: the manufacturer declares that the product meets EU requirements

MFA: multi-factor authentication

MQTT: messaging protocol between device and portal

NWT: abbreviation of the sample company in document and ticket numbers

SL: security level according to IEC 62443, from 1 to 4

STL: safety temperature limiter

TCP: transport protocol in the network

TLS: encryption of the connection

7 Revision history and approval

Version	Date	Change	Approval
1.0	15.03.2027	First issue for placing on the market (CE)	M. Berger
1.1	20.06.2027	Update chain with staged rollout documented	M. Berger
1.2	20.11.2027	Maintenance approval in the portal (Gateway 1.5.0)	M. Berger
1.3	28.02.2028	Drawing of zones and conduits with reading guide	M. Berger

Approved: Michael Berger, Managing Director, 28.02.2028 (signed in the original). Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.