CRA-MUSTER

D05 Netzwerk- und Systemarchitektur

Beispiel nach einem Jahr Betrieb, Stand 28.02.2028 · Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Musterbetrieb	Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect (frei erfunden)
Hinweis	Kostenfreies Muster, keine Rechtsberatung

Firma, Personen, Daten und Nummern sind frei erfunden. So sieht das Dokument nach einem Jahr gelebtem Betrieb aus.

1 Zweck und Geltungsbereich

Zonen und Verbindungen (Conduits) nach IEC 62443-3-2, erlaubte Datenflüsse, Fernwartung und Updatekette.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	NWT-CE-D05
Version, Status	1.3, freigegeben
Geltungsbereich	NWT HACKTHERM 60 connect (18 bis 60 kW), Steuerung, Gateway, Portal und App
Ersteller	Jonas Weiß, Technik und Product Security (PSO)
Geprüft	Ingenieurbüro Lechner (Safety), Sichtwerk Security (Security)
Freigabe	Michael Berger, Geschäftsführer, 28.02.2028
Nächste Prüfung	15.03.2029 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	Technische Dokumentation NWT-TD-HT60C, aufbewahrt bis mindestens 10 Jahre nach Inverkehrbringen der letzten Einheit

3 Übersicht als Zeichnung

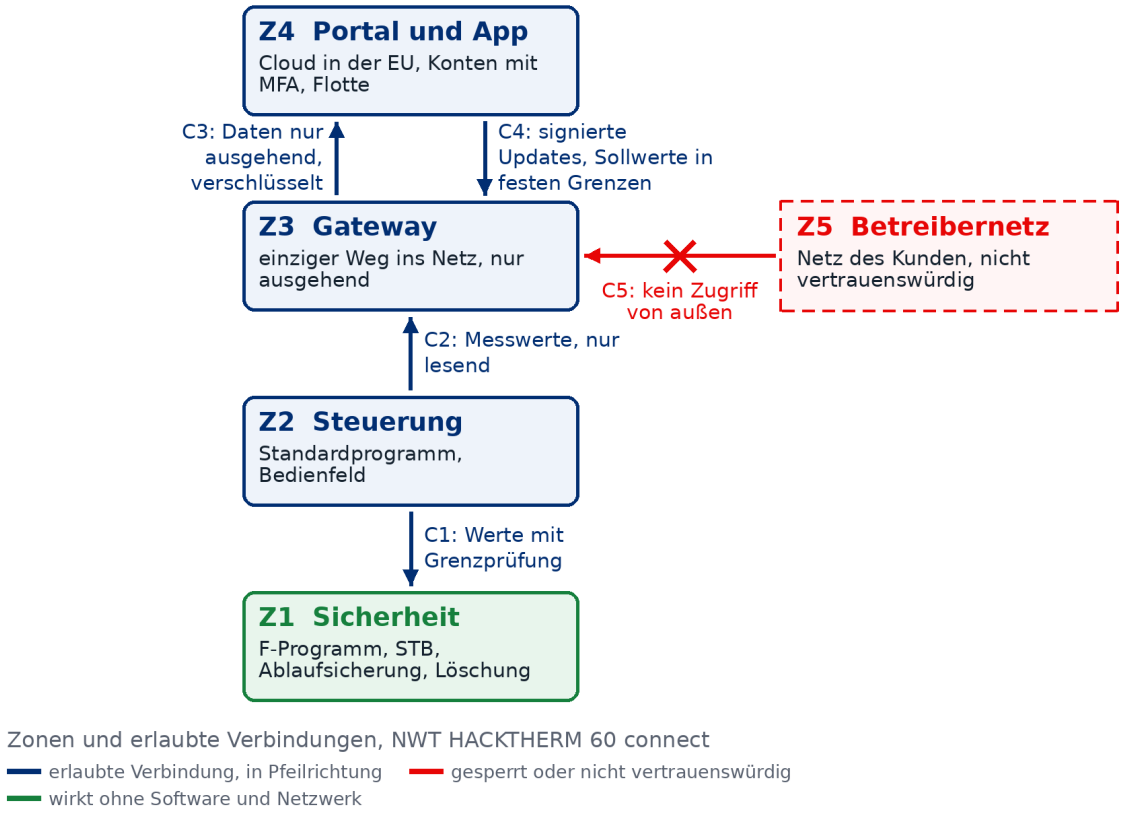


Abbildung: Zonen und erlaubte Verbindungen, NWT HACKTHERM 60 connect

So liest man die Zeichnung: Jeder Kasten ist eine Zone mit eigenem Schutz, jeder Pfeil eine erlaubte Verbindung in Pfeilrichtung. Alles andere ist gesperrt. Die Sicherheit (Z1, grün) hängt an keiner Verbindung nach außen; ein Angriff über Portal oder Gateway kann sie nicht abschalten.

4 Zonen

Zone	Inhalt	Ziel-SL	Verantwortlich
Z1 Sicherheit	F-Programm, F-Peripherie, STB	SL 2	Weiß
Z2 Steuerung	Standardprogramm, Bedienfeld	SL 2	Weiß
Z3 Gateway	Gateway, einziger Weg ins Netz	SL 2	Datenwerk
Z4 Portal und App	Cloud, Konten, Flotte	SL 2	Datenwerk
Z5 Betreibernetz	Netz des Kunden, nicht vertrauenswürdig	außerhalb	Kunde

Legende: Z = Zone; Ziel-SL = Ziel-Security-Level nach IEC 62443-3-2 (1 bis 4).

5 Verbindungen (Conduits)

Conduit	Von, nach	Erlaubt	Schutz
C1	Z2 zu Z1	Werte über F-Schnittstelle	Grenzprüfung im F-Programm
C2	Z2 zu Z3	Modbus TCP nur lesend	eigenes Kabel, kein Schreiben
C3	Z3 zu Z4	MQTT TLS 1.3 ausgehend	Zertifikat je Gerät
C4	Z4 zu Z3	Komfortsollwerte, Updates	signiert, Grenzen
C5	Z5 zu Z3	nichts eingehend	Firewall des Gateways

Legende: Conduit = erlaubte Verbindung zwischen zwei Zonen.

Fernwartung erfolgt nur über das Portal: Der Betreiber gibt eine Sitzung in der App frei, mit Zeitlimit von höchstens vier Stunden, MFA für das Servicekonto und Protokoll. Gesperrt bleiben alle Befehle, die Bewegung auslösen oder Sicherheitsdaten ändern. Updates sind signiert, werden erst auf 1 % der Flotte und nach 48 Stunden auf alle Geräte verteilt; das Gateway prüft die Signatur vor dem Einspielen und behält die Vorversion.

6 Begriffe und Abkürzungen

MFA: Anmeldung mit zweitem Faktor, z. B. Code aufs Handy

MQTT: Nachrichtenprotokoll zwischen Gerät und Portal

SL: Security Level nach IEC 62443, von 1 bis 4

STB: Sicherheitstemperaturbegrenzer

TCP: Transportprotokoll im Netzwerk

TLS: Verschlüsselung der Verbindung

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	15.03.2027	Erstausgabe zum Inverkehrbringen (CE)	M. Berger
1.1	20.06.2027	Updatekette mit gestuftem Ausrollen dokumentiert	M. Berger
1.2	20.11.2027	Wartungsfreigabe im Portal (Gateway 1.5.0)	M. Berger
1.3	28.02.2028	Zeichnung der Zonen und Verbindungen mit Lesehilfe	M. Berger

Freigegeben: Michael Berger, Geschäftsführer, 28.02.2028 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Firma, Personen, Seriennummern und Daten frei erfunden.