CRA-MUSTER

D04 Steuerungs- und Sicherheitskonzept

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

Sicherheitssteuerung, Grundsatzentscheidungen, Sicherheitsfunktionen mit PLr nach EN ISO 13849-1, erreichter PL und Validierung. Belegt, dass Sicherheit ohne Software und Netzwerk hält.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	NWT-CE-D04
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 Steuerung und Sicherheitsfunktionen

Sicherheitssteuerung: Siemens SIMATIC S7-1200 G2, CPU 1214FC G2 mit F-DI, F-DQ, F-AI; Komponente mit IEC-62443-4-2-Zertifikat, Abdeckung der F-Variante vom Hersteller schriftlich bestätigt (Akte D04-03)

F-Programm: Version 3.0.0, Gesamtsignatur in der Akte, eigenes F-Passwort, Änderung nur lokal mit neuer Validierung

4 Grundsätze

✓ G1: STB, Ablaufsicherung, Sicherheitsventil und Löschung wirken ohne Software und Netzwerk

✓ G2: Kein Fernzugriff auf F-Daten, das Gateway hat keinen Schreibzugriff

✓ G3: Werte vom Standard- zum F-Programm werden gegen feste Grenzen geprüft

✓ G4: Kein gefahrbringender Wiederanlauf ohne geschlossene Verriegelung und lokale Quittierung (MVO 1.2.6)

5 Sicherheitsfunktionen: wie zuverlässig jede sein muss

So lesen Sie die Tabelle

Für jede Sicherheitsfunktion beantworten wir drei Fragen nach EN ISO 13849-1. S: Wie schwer wäre die Verletzung, wenn sie versagt? F: Wie oft ist jemand der Gefahr ausgesetzt? P: Kann die Person noch ausweichen? Aus den drei Antworten folgt der erforderliche Performance Level PLr, von a (gering) bis e (sehr hoch). Die Steuerung muss mindestens diesen Wert erreichen; das zeigt die Spalte „PL erreicht“. Die Kategorie sagt, wie die Steuerung dafür aufgebaut ist.

SF	Sicherheitsfunktion	S	F	P	PLr	Kat.	PL erreicht	Validiert (F09)
SF1	Rückbrandschutz: Zellrad zu, Austragung aus	S2	F1	P2	d	3	d	02.03.2027
SF2	Übertemperatur Kessel, Feuerung aus	S2	F1	P2	d	3	d	02.03.2027
SF3	Not-Halt und Heizungsnotschalter	S2	F1	P1	c	3	d	03.03.2027
SF4	Lagerraumtür offen, Austragung aus	S2	F1	P2	d	3	d	03.03.2027
SF5	Wartungsdeckel offen, Antriebe aus	S2	F1	P2	d	3	d	04.03.2027
SF6	Unterdruck fehlt, Brennstoff aus	S2	F1	P1	c	2	c	04.03.2027
SF7	Zündfreigabe nur nach Vorspülung	S2	F1	P1	c	2	c	05.03.2027
SF8	Wiederanlaufsperre nach Wiederkehr	S2	F1	P2	d	3	d	05.03.2027
SF9	Aschebox offen, Schnecken aus	S2	F1	P1	c	2	c	08.03.2027
SF10	Fernbefehle nur in festen Grenzen	S2	F1	P1	c	2	c	08.03.2027

Legende: SF = Sicherheitsfunktion; S = Schwere der Verletzung: S1 leicht, S2 schwer oder tödlich; F = Häufigkeit oder Dauer, mit der jemand der Gefahr ausgesetzt ist: F1 selten, F2 häufig; P = Möglichkeit, der Gefahr auszuweichen: P1 möglich, P2 kaum möglich; PLr = erforderlicher Performance Level nach EN ISO 13849-1 (a bis e); Kat. = Kategorie, also der Aufbau der Steuerung von B (einfach) bis 4 (zweikanalig mit Selbsttest); PL erreicht = nachgewiesener Performance Level.

6 Was wir mit der Tabelle tun

Beispiel SF1 Rückbrandschutz: Ein Rückbrand ins Lager kann schwer verletzen (S2), jemand ist dort nur selten (F1), ausweichen ist kaum möglich (P2). Daraus folgt PLr d.

Daraus folgt der Aufbau: Für d bauen wir Kategorie 3, also zweikanalig. Ein einzelner Fehler, etwa ein Kabelbruch, schaltet die Funktion nicht ab, sondern wird erkannt.

Das Ingenieurbüro berechnet den erreichten PL mit den Kennwerten der Bauteile (Bericht in der Akte). Erreicht muss mindestens der PLr sein; bei SF3 liegt er mit d sogar darüber.

Die Validierung in F09 prüft jede Funktion mit eingebautem Fehler. Erst dann ist der Wert in der Tabelle belegt.

Ändert sich etwas an einer Sicherheitsfunktion, beginnt die Bewertung für diese Zeile von vorn (F08).

7 Aufbau der Steuerung

Kategorie 3: zwei Kanäle über F-DI mit Querschlusserkennung, zwei Abschaltpfade (F-DQ und Schütz mit Rückführkreis); codierte Sicherheitsschalter an Tür und Deckeln

Kategorie 2: die F-CPU testet die Funktion beim Anlauf und zyklisch

Kennwerte für PL d: Ausfallwahrscheinlichkeit PFHd unter 10^{-6} pro Stunde, Fehler gemeinsamer Ursache mindestens 65 Punkte, Lebensdauer der Bauteile hoch; Werte aus Herstellerangaben und PL-Bericht

Mit dem Standardprogramm 3.0.3 (NWT-CHG-2027-005) wurde nur die Brennerregelung optimiert. Die Gesamtsignatur des F-Programms ist unverändert; das hat das Ingenieurbüro Lechner am 05.09.2027 geprüft und bestätigt. Eine neue Validierung war deshalb nicht nötig, die Prüfung der Signatur ist in F09 vermerkt.

8 Begriffe und Abkürzungen

CHG: Änderungsantrag (Nummernkreis)

CPU: Rechenkern der Steuerung

F-AI: sicherer Analogeingang der Sicherheitssteuerung

F-DI: sicherer Digitaleingang der Sicherheitssteuerung

F-DQ: sicherer Digitalausgang der Sicherheitssteuerung

MVO: Maschinenverordnung (EU) 2023/1230, gilt ab 20.01.2027

NWT: Kürzel des Musterbetriebs in Dokument- und Ticketnummern

PFHd: mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde

PL: Performance Level nach EN ISO 13849-1, von a (niedrig) bis e (hoch)

PLr: erforderlicher Performance Level

SF: Sicherheitsfunktion

STB: Sicherheitstemperaturbegrenzer

9 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	10.01.2027	Konzept mit SF1 bis SF10	M. Berger
1.1	15.03.2027	Validierung abgeschlossen, PL eingetragen	M. Berger
1.2	05.09.2027	Standardprogramm 3.0.3, F-Programm unverändert, Signatur geprüft	M. Berger
1.3	28.02.2028	Tabelle erklärt: S, F, P, Kategorie, Lesehilfe und Beispiel	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.