CRA SAMPLE

D04 Control and safety concept

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

Safety controller, basic design decisions, safety functions with PLr according to EN ISO 13849-1, achieved PL and validation. Shows that safety is maintained without software and without the network.

2 Document control

Field	Entry
Document no.	NWT-CE-D04
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 Control and safety concept: overview

Safety controller: Siemens SIMATIC S7-1200 G2, CPU 1214FC G2 with F-DI, F-DQ, F-AI; component with IEC 62443-4-2 certificate, coverage of the F variant confirmed in writing by the manufacturer (file D04-03)

F-program: Version 3.0.0, collective signature on file, dedicated F-password, changes only locally and with new validation

4 Principles

✓ G1: STL, thermal discharge safety device, safety valve and extinguishing system work without software and without the network

✓ G2: No remote access to F-data, the gateway has no write access

✓ G3: Values passed from the standard program to the F-program are checked against fixed limits

✓ G4: No hazardous restart without a closed interlock and local acknowledgement (MR, Annex III, section 1.2.6)

5 Safety functions: how reliable each one must be

How to read the table

For each safety function we answer three questions according to EN ISO 13849-1. S: How severe would the injury be if the function failed? F: How often is someone exposed to the hazard? P: Can the person still avoid it? The three answers give the required Performance Level PLr, from a (low) to e (very high). The control system must reach at least this value; the column 'PL achieved' shows this. The category states how the control system is designed to achieve it.

SF	Safety function	S	F	P	PLr	Cat.	PL achieved	Validated (F09)
SF1	Burn-back protection: rotary valve closed, discharge off	S2	F1	P2	d	3	d	02.03.2027
SF2	Boiler overtemperature, firing off	S2	F1	P2	d	3	d	02.03.2027
SF3	Emergency stop and heating emergency switch	S2	F1	P1	c	3	d	03.03.2027
SF4	Storage room door open, discharge off	S2	F1	P2	d	3	d	03.03.2027
SF5	Maintenance cover open, drives off	S2	F1	P2	d	3	d	04.03.2027
SF6	No negative pressure, fuel off	S2	F1	P1	c	2	c	04.03.2027
SF7	Ignition enabled only after pre-purge	S2	F1	P1	c	2	c	05.03.2027
SF8	Restart interlock after power return	S2	F1	P2	d	3	d	05.03.2027
SF9	Ash box open, augers off	S2	F1	P1	c	2	c	08.03.2027
SF10	Remote commands only within fixed limits	S2	F1	P1	c	2	c	08.03.2027

Legend: SF = safety function; S = severity of injury: S1 slight, S2 serious or fatal; F = frequency or duration of exposure: F1 rare, F2 frequent; P = possibility of avoiding the hazard: P1 possible, P2 scarcely possible; PLr = required performance level according to EN ISO 13849-1 (a to e); Cat. = category, the structure of the control system from B (simple) to 4 (dual channel with self test).

6 How we use the table

Example SF1 burn-back protection: a burn-back into the storage room can cause serious injury (S2), someone is rarely present there (F1), and avoiding the hazard is hardly possible (P2). This gives PLr d.

This determines the design: for d we build category 3, i.e. two-channel. A single fault, such as a broken cable, does not disable the function but is detected.

The engineering firm calculates the achieved PL from the component parameters (report on file). The achieved PL must be at least the PLr; for SF3 it is even higher at d.

Validation in F09 tests each function with an injected fault. Only then is the value in the table verified.

If anything changes in a safety function, the assessment for that row starts again from the beginning (F08).

7 Control system architecture

Category 3: two channels via F-DI with cross-circuit detection, two shutdown paths (F-DQ and contactor with feedback circuit); coded safety switches on door and covers

Category 2: the F-CPU tests the function at start-up and cyclically

Parameters for PL d: probability of dangerous failure PFHd below 10^{-6} per hour, common cause failure score at least 65 points, high component lifetime (MTTFd); values from manufacturer data and the PL report

Standard program 3.0.3 (NWT-CHG-2027-005) only optimised the burner control. The collective signature of the F-program is unchanged; the Lechner engineering firm checked and confirmed this on 05.09.2027. A new validation was therefore not required, and the signature check is recorded in F09.

8 Terms and abbreviations

CHG: change request (number range)

CPU: processing unit of the controller

F-AI: fail-safe analogue input

F-DI: fail-safe digital input

F-DQ: fail-safe digital output

MR: Machinery Regulation (EU) 2023/1230, applies from 20 January 2027

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

PFHd: average probability of a dangerous failure per hour

PL: performance level according to EN ISO 13849-1, from a (low) to e (high)

PLr: required performance level

SF: safety function

STL: safety temperature limiter

9 Revision history and approval

Version	Date	Change	Approval
1.0	10.01.2027	Concept with SF1 to SF10	M. Berger

Version	Date	Change	Approval
1.1	15.03.2027	Validation completed, PL entered	M. Berger
1.2	05.09.2027	Standard program 3.0.3, F-program unchanged, signature checked	M. Berger
1.3	28.02.2028	Table explained: S, F, P, category, reading guide and example	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.