CRA-MUSTER

D04 Steuerungs- und Sicherheitskonzept

Leere Vorlage · 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

Felder ausfüllen, mit Datum und Unterschrift freigeben, in der Ablage nach Dokumentenlenkung führen.

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.

So füllen Sie dieses Formular aus

Füllen Sie die Felder mit den Angaben Ihres Betriebs aus. Unter jeder Tabelle und neben jedem Feld steht ein Beispiel aus dem Musterbetrieb als Orientierung. Verweisen Sie auf Nachweise mit Nummer (z. B. Ticket oder Formular). Zum Schluss mit Datum und Unterschrift freigeben und nach der Dokumentenlenkung ablegen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	
Version, Status	
Geltungsbereich	
Ersteller	
Geprüft	
Freigabe	
Nächste Prüfung	
Vertraulichkeit	
Ablage	

3 Steuerung und Sicherheitsfunktionen

Feld	Eintrag	Beispiel aus dem Muster
Sicherheitssteuerung		Siemens SIMATIC S7-1200 G2, CPU 1214FC G2 mit …
F-Programm		Version 3.0.0, Gesamtsignatur in der Akte, …

4 Grundsätze

	Punkt	Wer / bis wann
☐	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)

Beispielzeile aus dem Muster: SF: SF1 · Sicherheitsfunktion: Rückbrandschutz: Zellrad zu, Austragung … · S: S2 · F: F1 · P: P2 · PLr: d · Kat.: 3 · PL erreicht: d · Validiert (F09): 02.03.2027

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 aus dem Muster: Beispiel SF1 Rückbrandschutz: Ein Rückbrand ins Lager kann schwer verletzen (S2), jemand ist dort nur selten (F1), …

7 Aufbau der Steuerung

Feld	Eintrag	Beispiel aus dem Muster
Kategorie 3		zwei Kanäle über F-DI mit Querschlusserkennung, …
Kategorie 2		die F-CPU testet die Funktion beim Anlauf und …
Kennwerte für PL d		Ausfallwahrscheinlichkeit PFHd unter 10^{-6} pro …

Beschreiben Sie hier Ihren Stand, konkret und mit Datum. Beispiel aus dem Muster: Mit dem Standardprogramm 3.0.3 (NWT-CHG-2027-005) wurde nur die Brennerregelung optimiert.

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

Version	Datum	Änderung	Freigabe

Freigegeben (Name, Funktion, Datum, Unterschrift): _____ · Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Firma, Personen, Seriennummern und Daten frei erfunden.