8.2.16 Erdbaumaschinensteuerung mit Bussystem – Kategorie 3 – PL d (Beispiel 16)

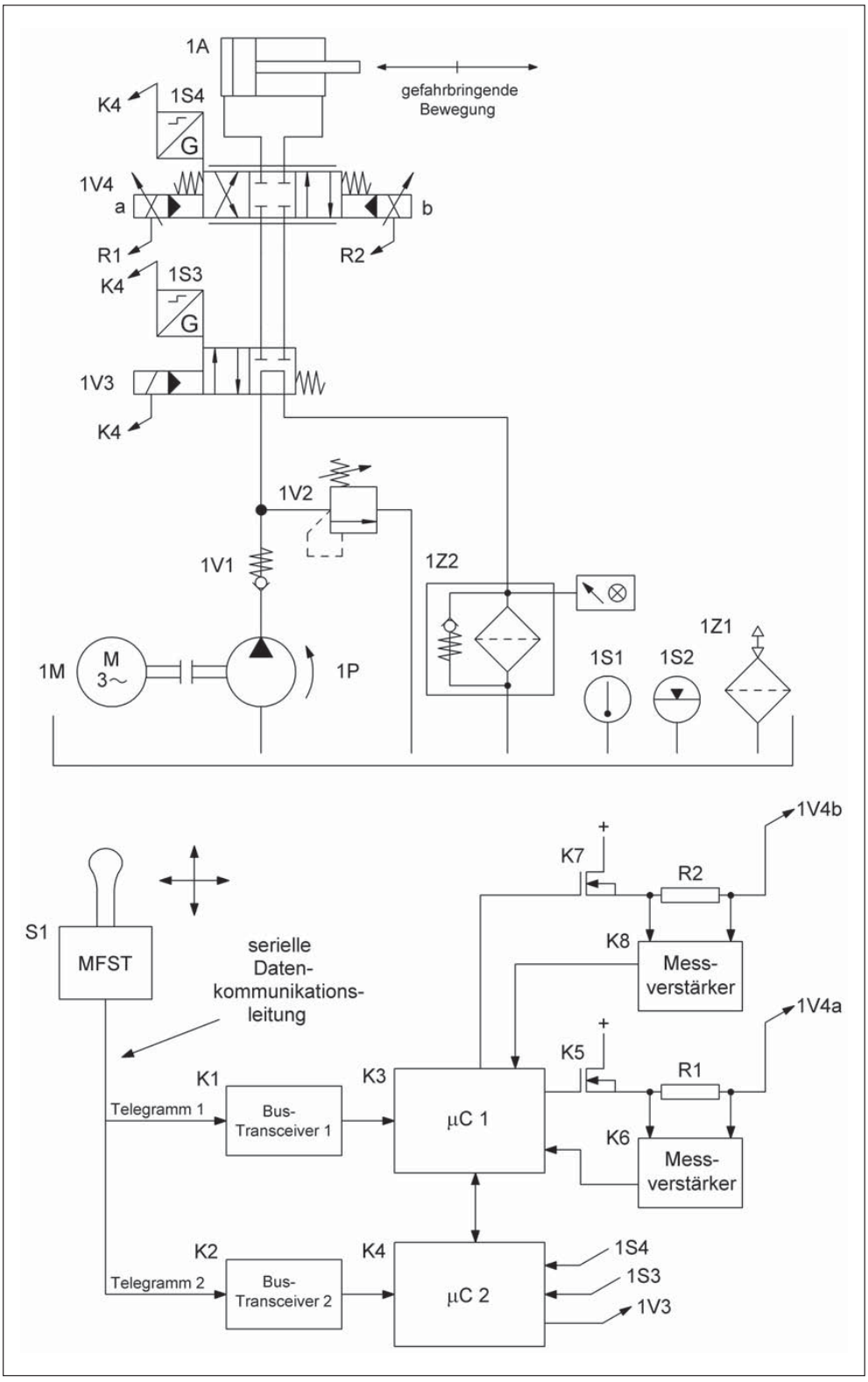
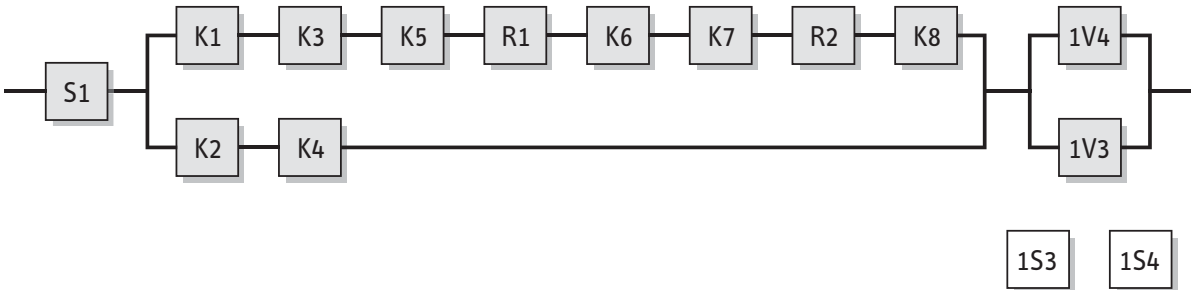


Abbildung 8.27: Ansteuerung von gefahrbringenden Bewegungen einer Erdbaumaschine



Sicherheitsfunktion

- Verhinderung des unerwarteten Anlaufs: Vermeidung unerwarteter Bewegungen der Arbeitsgeräte von Erdbaumaschinen

Funktionsbeschreibung

- Das Multifunktionsstellteil (MFST) S1 wandelt die vom Bediener ausgeführte manuelle Auslenkung des MFST in elektronische Datentelegramme um. Es sendet diese Telegramme zyklisch über eine serielle Datenkommunikationsleitung (Bussystem) zur Logiksteuerung, die Ansteuersignale für die Hydraulik zur Ausführung der vom Bediener vorgesehenen Arbeitsbewegung der Erdbaumaschine erzeugt.

- Das vom MFST S1 gesendete Telegramm 1 gelangt über den Bus-Transceiver K1 in den Mikrocontroller K3. Dieser erzeugt aus Telegramm 1 gemäß den in der Software abgelegten Algorithmen die erforderlichen analogen Signale zur Ansteuerung des Proportionalventils 1V4. Die Widerstände R1/R2 und die Messverstärker K6/K8 dienen zur Regelung der Ausgangsströme für das Proportionalventil. Der Mikrocontroller K4 erhält ein redundantes Telegramm 2 von S1 über den Bus-Transceiver K2. K4 prüft die korrekte Auslenkung des Proportionalventils 1V4 über das in 1V4 integrierte Weg-Messsystem 1S4 auf Plausibilität gegen die aus Telegramm 2 ermittelte Sollstellung. Bei erkannten Fehlern schaltet K4 übergeordnet über ein Wegeventil 1V3 den hydraulischen Druck ab und bringt das System in den sicheren Zustand.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z.B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.

- Bei dem MFST handelt es sich um ein für den Einsatz in PL d geeignetes Sicherheitsbauteil, das der Kategorie 3 entspricht.

- Das Proportionalventil 1V4 und das Wegeventil 1V3 haben eine Sperrstellung bzw. Sperr-Mittelstellung, Federrückstellung bzw. Federzentrierung und eine ausreichend positive Überdeckung.

- Die Programmierung der Software (SRESW) von K3 und K4 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.

- Die Datenübertragung vom MFST zur Logiksteuerung ist nach GS-ET-26 bzw. DIN EN 61784-3 abgesichert. Das verwendete Datenkommunikationsprotokoll beinhaltet redundante Telegramme und Maßnahmen, um folgende Übertragungsfehler zu erkennen: Wiederholung, Verlust, Einfügung, falsche Abfolge, Verfälschung und Verzögerung (siehe auch Abschnitt 6.2.17). Die Restfehlerrate Λ ist geringer als $1 \cdot 10^{-8}$/Stunde und trägt damit wie von den Beurteilungsgrundlagen vorgesehen weniger als 1 % zur maximal zulässigen Ausfallwahrscheinlichkeit der Sicherheitsfunktion bei. Dieser geringe Anteil ist in der Berechnung der Gesamtausfallwahrscheinlichkeit vernachlässigbar.

Bemerkung

- Eine eventuell erforderliche Notlauffunktion der Erdbaumaschine ist hier nicht dargestellt und übergeordnet zu realisieren.

Berechnung der Ausfallwahrscheinlichkeit

- Das MFST S1 liegt als handelsübliches Sicherheitsbauteil vor. Die zugehörige Ausfallwahrscheinlichkeit wird am Ende der Berechung addiert ($PFH_{MFST} = 3{,}0 \cdot 10^{-7}$/Stunde [G]). Für den übrigen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.

- $MTTF_d$ der Logiksteuerung: Für die Bus-Transceiver K1 und K2 wird eine $MTTF_d$ von 11 415 Jahren [D] angesetzt. Für die Mikrocontroller K3 und K4 einschließlich ihrer Peripherie wird nach SN 29500-2 eine $MTTF_d$ von 878 Jahren [D] berücksichtigt. Für die restlichen Bauteile werden folgende Kenndaten angesetzt [D]: 45 662 Jahre für die Schalttransistoren K5 und K7, 228 310 Jahre für die Widerstände R1 und R2 und 1 141 Jahre für die Messverstärker K6 und K8. Die $MTTF_d$ der Kanäle beträgt damit 329 Jahre und 815 Jahre. Nach Kürzen auf 100 Jahre ergibt dies einen symmetrisierten $MTTF_d$-Wert von 100 Jahren.

- DC_{avg} der Logiksteuerung: DC = 99 % für K1 und K2 durch Kreuzvergleich der Telegramme in den Mikrokontrollern K3 und K4; DC = 60 % für K3 und K4 durch Kreuzvergleich und Selbsttests einfacher Wirksamkeit durch Software; DC = 90 % für die restlichen Bauteile durch Fehlererkennung in K4 mittels Weg-Messsystem 1S4. Die Mittelungsformel für DC_{avg} ergibt 74 % („niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10)

- Die Logiksteuerung entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und niedrigem DC_{avg} (74 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}36 \cdot 10^{-8}$/Stunde.

- $MTTF_d$ des hydraulischen Teils der Steuerung: Für das Proportionalventil 1V4 und das Wegeventil 1V3 wird eine $MTTF_d$ von 150 Jahren [N] angesetzt. Nach Kürzen ergibt dies einen symmetrisierten $MTTF_d$-Wert von 100 Jahren.

- DC_{avg} des hydraulischen Teils der Steuerung: DC = 99 % für 1V4 und 1V3 durch direkte Überwachung der Stellung über 1S4 bzw. 1S3 in K4. Die Mittelungsformel für DC_{avg} ergibt 99 % („hoch“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), Verwendung bewährter Bauteile (5), Schutz gegen Überdruck (15) und Umgebungsbedingungen (25 + 10).

- Der hydraulische Teil der Steuerung entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde.

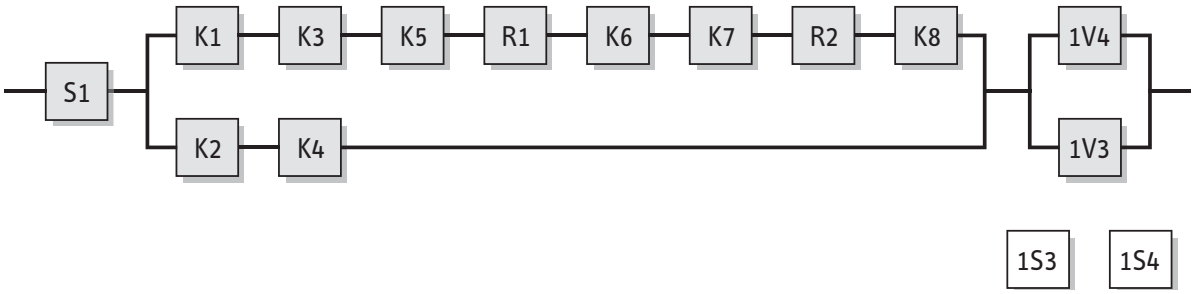
- Die mittlere Wahrscheinlichkeit gefährlicher Ausfälle der Sicherheitsfunktion ergibt sich durch Addition der Anteile des MFST, der Logiksteuerung und des hydraulischen Teils. Die Summe beträgt $3{,}98 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- ISO 15998: Earth-moving machinery – Machine control systems (MCS) using electronic components – Performance criteria and tests (Normentwurf) (11.03). Beuth, Berlin 2003

- DIN EN 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2007) (11.08). Beuth, Berlin 2008

- Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS–ET–26. Hrsg.: Fachausschuss Elektrotechnik, Köln 2002
  www.dguv.de, Webcode d14884



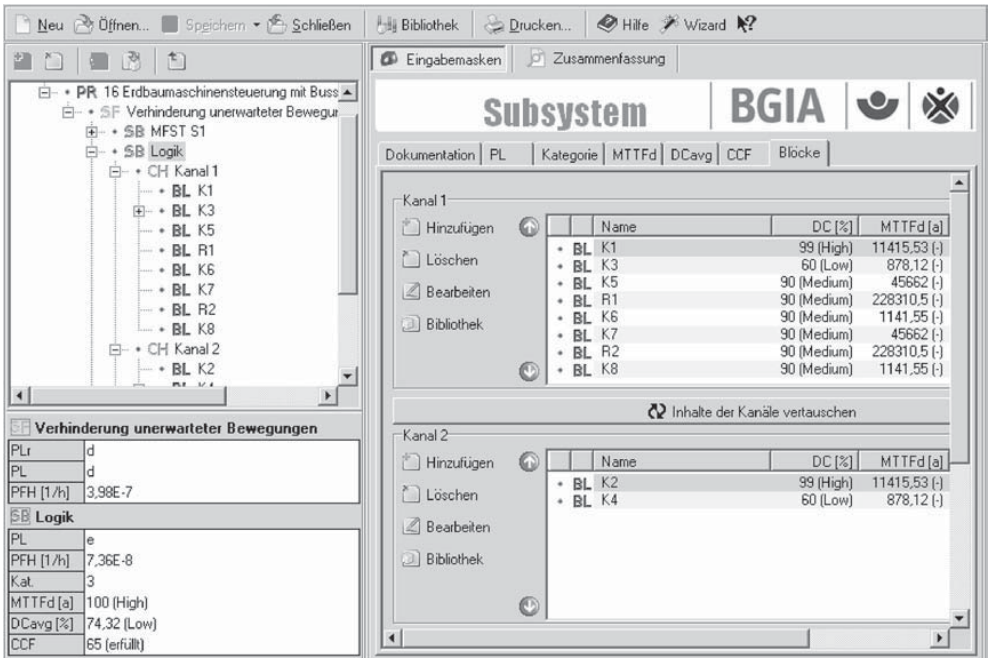


Abbildung 8.28: PL-Bestimmung mithilfe von SISTEMA