Erratum von Juni 2009 zum BGIA-Report 2/2008 „Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849 –“, 2. geänderte Aufl. Dezember 2008

- **Seite 14, 2. Absatz, 6. Zeile**

  Statt „November“ lies „Dezember“.

- **Seite 21, Tabelle 4.1, drittletzte Zeile, erste Spalte**

  Statt „Diagnosedeckungsgrad“ lies „Mittlerer Diagnosedeckungsgrad“.

- **Seite 29, Abbildungen 5.6 und 5.7**

  Statt „Stellungsüberwachung“ lies „Stellungserfassung“.

- **Seite 44, Abschnitt „Beispiel 2: Versagen von …“, 1. Absatz, 12. Zeile**

  Statt „Weiterhin ist … Toleranzen und Herstellungsverfahren.“ lies „Weiterhin sind in Tabelle C.1 und C.2 in ähnlicher Weise die Anforderungen an hydraulische Bauteile festgelegt. Auch hier müssen „*ausreichende Maßnahmen zur Vermeidung von Verunreinigung des Druckmediums*“ getroffen und auf die „*richtige Dimensionierung und Formgebung*“ geachtet werden“.

- **Seite 54, letzter Absatz, 24. und 25. Zeile**

  Statt „Ausfallrate λ_d (= 1/$MTTF_d$) bzw. als die mittlere Anforderungsrate der Sicherheitsfunktion“ lies „Ausfallrate λ_d (= 1/$MTTF_d$) (für Kategorie 3 oder 4) oder als die mittlere Anforderungsrate der Sicherheitsfunktion (für Kategorie 2)“.

- **Seite 54, letzter Absatz, viertletzte Zeile**

  Statt „Tests so“ lies „Tests gleichzeitig mit der Anforderung der Sicherheitsfunktion so“.

- **Seite 131/132, Abschnitt „Berechnung der Ausfallwahrscheinlichkeit“, vorletzter Spiegelstrich**

  Statt „Kategorie 3“ lies „Kategorie 4“.

- **Seite 142, Abschnitt „Berechnung der Ausfallwahrscheinlichkeit“, 2. Spiegelstrich, letzter Satz**

  Statt „57 %, der im Toleranzbereich von „niedrig“ liegt“ lies „64 %.“

- **Seite 142, Abschnitt „Berechnung der Ausfallwahrscheinlichkeit“, 4. Spiegelstrich**

  Statt „57 %“ lies „64 %“. Statt „1,83“ lies „1,62“.

- **Seite 185, letzter Spiegelstrich im Abschnitt „Konstruktive Merkmale“**

  Statt „K2, Q1, Q2“ lies „Q1 und Q2“.

- **Seite 247, Abschnitt „H1 Was kann SISTEMA?“, 2. Absatz, 5. und 6. Zeile**

  Statt „mittlere Testqualität (DC_{avg})“ lies „Testqualität (DC)“.

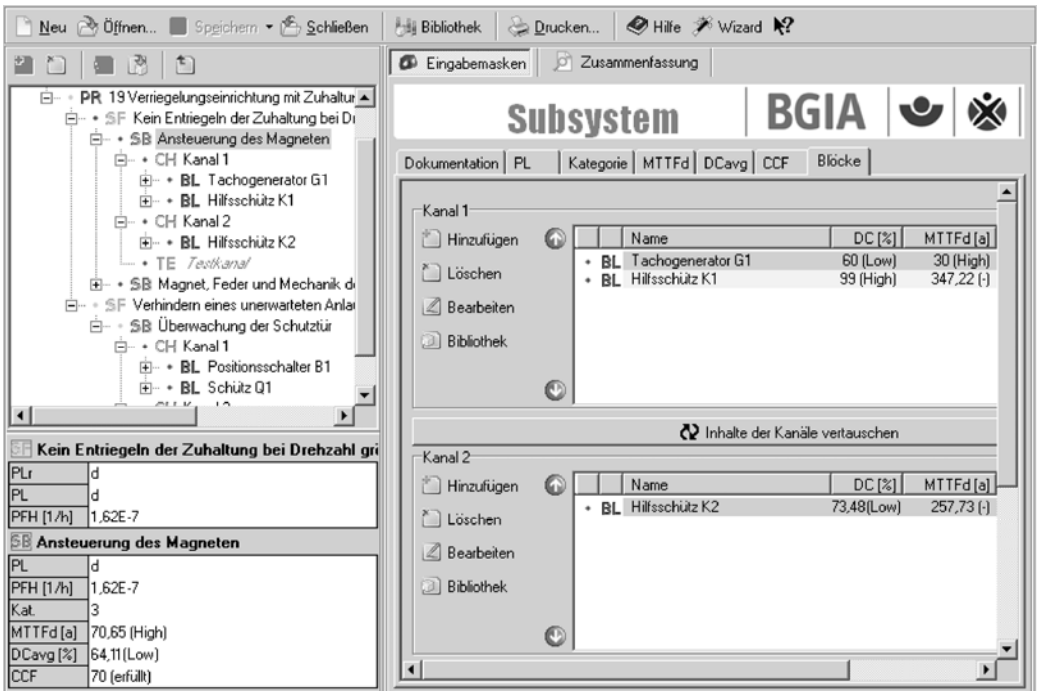
- **Seite 248, linke Spalte, 1. Absatz, 3. Zeile**

  Statt „Blöcke“ lies „Elemente, Blöcke“.

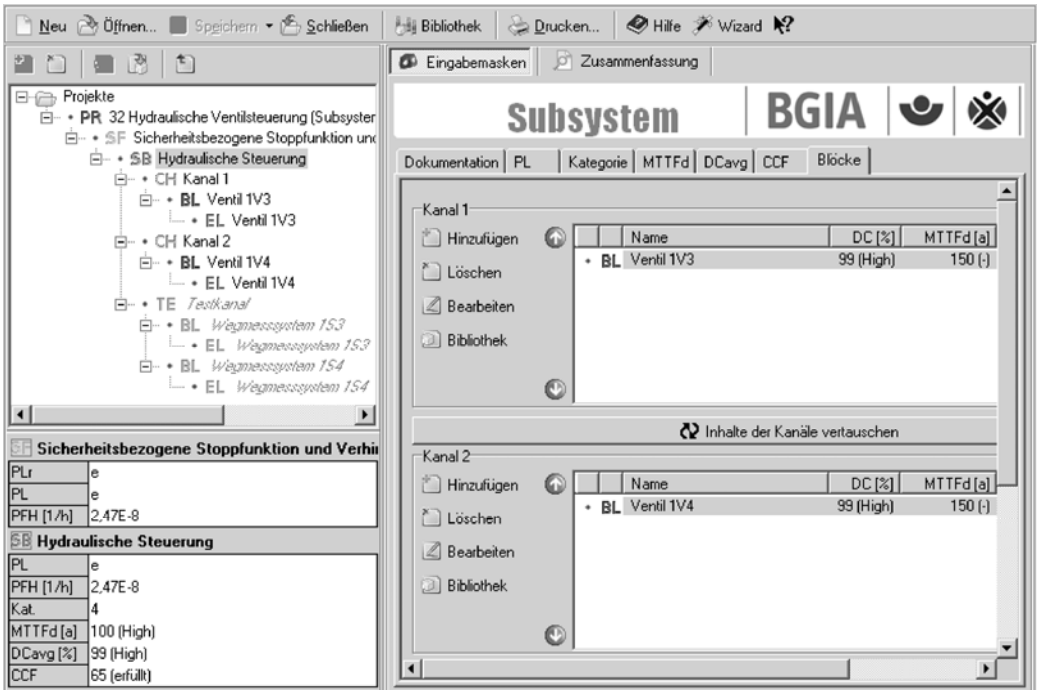
- **Seite 248, Abschnitt „H4 Wo ist SISTEMA zu erhalten?“, 2. Zeile**

  Statt „deutscher“ lies „deutscher und englischer“.

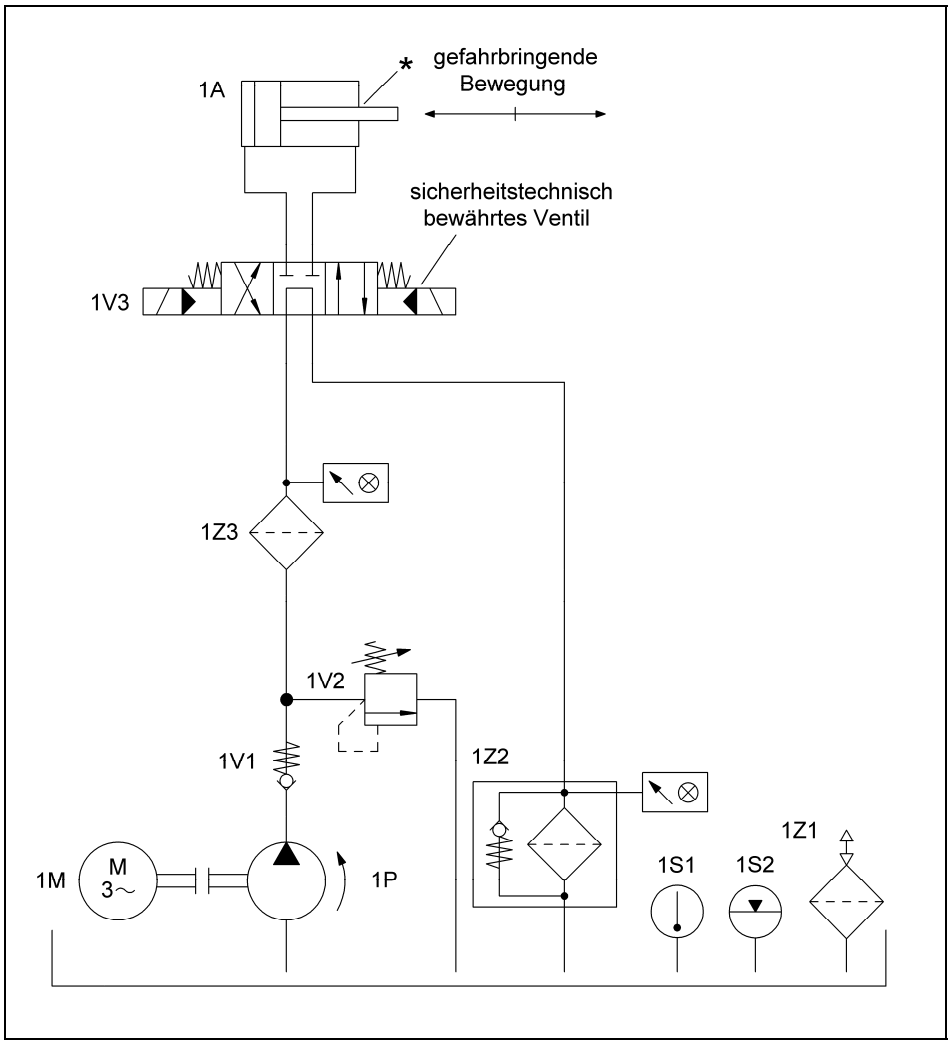
- **Seite 143, Abbildung 8.33 –** Ersetze Abbildung 8.33.



- **Seite 179, Abbildung 8.52 –** Ersetze Abbildung 8.52.



- **Seite 96, Abbildung 8.6 –** Ersetze Abbildung 8.6:



Ersetze Seite 180 bis 182.

8.2.33 Elektrohydraulische Pressensteuerung – Kategorie 4 – PL e (Beispiel 33)

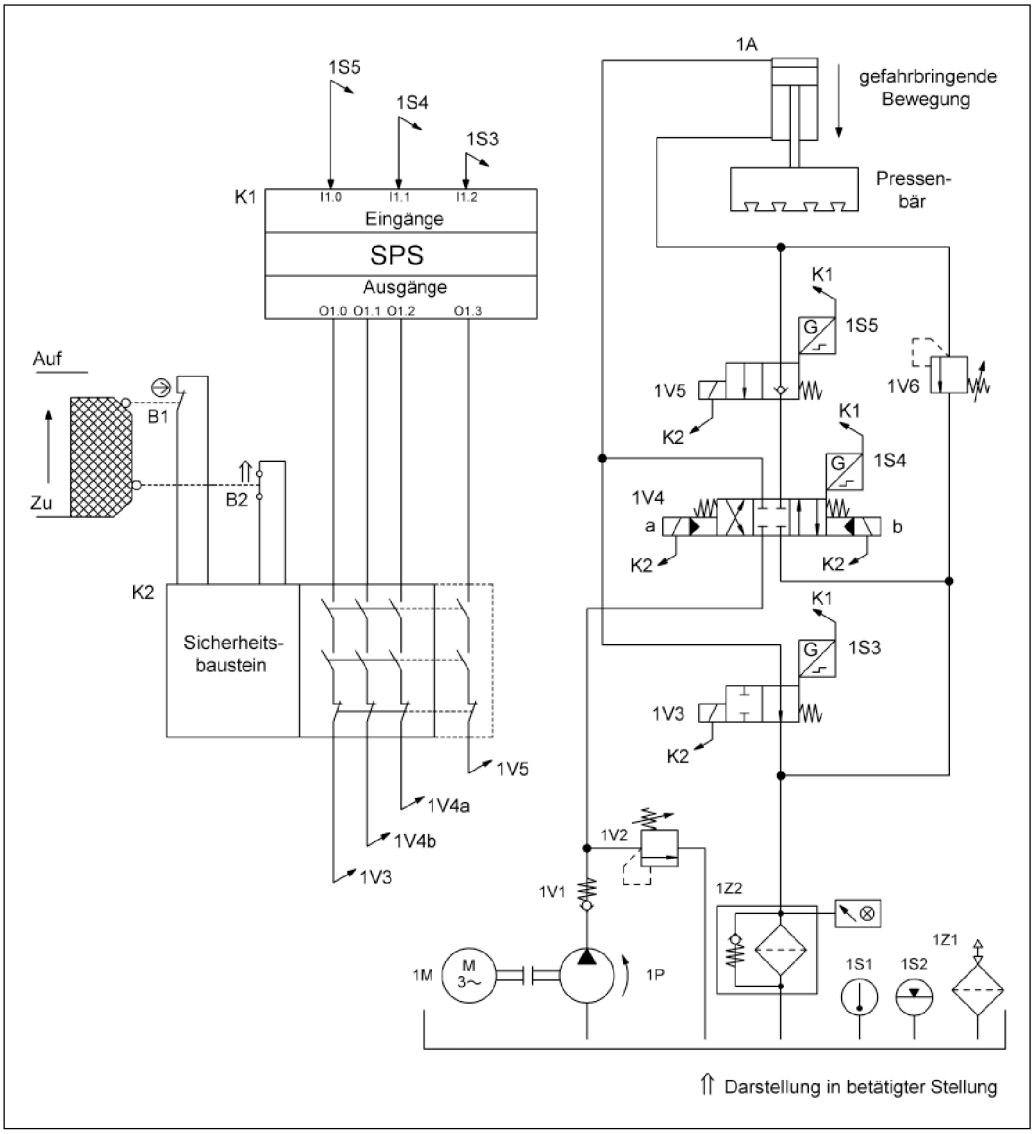


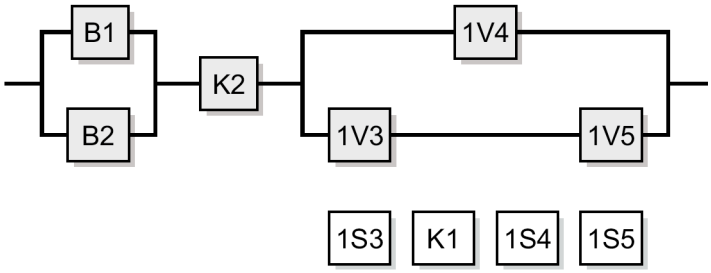
Abbildung 8.53: Pressensteuerung, elektrische Überwachung einer beweglichen trennenden Schutzeinrichtung mit hydraulischem Stillsetzen der gefahrbringenden Bewegung

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Stillsetzen der gefahrbringenden Bewegung.

Funktionsbeschreibung

- Der Gefahrenbereich ist mittels einer beweglichen trennenden Schutzeinrichtung gesichert, deren Stellung von zwei Positionsschaltern B1 und B2 in Öffner-Schließer-Kombination erfasst wird. Die Signale werden in einen handelsüblichen Sicherheitsbaustein K2 eingelesen, der in den Freigabepfad der elektrischen Vorsteuerung K1 (herkömmliche SPS) für die hydraulischen Aktoren eingeschleift ist. Gefahrbringende Bewegungen oder Zustände werden aktorseitig durch drei Wegeventile (1V3, 1V4 und 1V5) gesteuert.



- Bei Anforderung der Sicherheitsfunktion werden alle Ventile durch K2 stromlos geschaltet und gehen aufgrund der vorhandenen Rückstellfedern in die Sperr-Mittelstellung (1V4) bzw. in die Sperr-Stellung (1V3 und 1V5). Dabei wird der Ölrückfluss von der Kolbenunterseite des Zylinders zum Tank durch die Ventile 1V4 und 1V5 gleichzeitig unterbrochen. Bei dem Ventil 1V5 handelt es sich um ein Sitzventil, das aufgrund seiner Konstruktion den Volumenstrom leckagefrei absperrt. Das Ventil 1V4, das auch die Bewegungsrichtung des Zylinders steuert, ist ein Wegeventil in Schieberbauweise, das auch in der Sperr-Mittelstellung eine gewisse Leckage aufweist. Obwohl das Ventil 1V3 nur mittelbar an der Stoppfunktion beteiligt ist, kann es die Sicherheitsfunktion in gefährlicher Weise beeinträchtigen. Würden 1V3 und 1V4 gleichzeitig hängen bleiben, so würde auf der Kolbenoberseite Druck aufgebaut, während die Kolbenunterseite durch 1V5 abgesperrt bleibt. Wegen der Druckübersetzung im Zylinder würde dann das Druckbegrenzungsventil 1V6 öffnen und der Pressenbär absinken.
- Der Ausfall eines Ventils führt nicht zum Verlust der Sicherheitsfunktion. Alle Ventile werden zyklisch angesteuert.
- An allen Ventilen ist jeweils eine Stellungsabfrage 1S3, 1S4 bzw. 1S5 zur Fehlererkennung vorgesehen. Der Ausfall jedes der drei Ventile wird in der herkömmlichen SPS K1 erkannt, die nach einem Fehler das Einleiten der nächsten gefahrbringenden Bewegung verhindert.
- Ein einzelner Fehler in einer sicherheitstechnischen Komponente führt nicht zum Verlust der Sicherheitsfunktion. Darüber hinaus werden einzelne Fehler bei oder vor der nächsten Anforderung erkannt. Eine Anhäufung von unerkannten Fehlern führt nicht zum Verlust der Sicherheitsfunktion.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B werden eingehalten. Schutzbeschaltungen (z.B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- Der Schalter B1 ist ein zwangsöffnender Positionsschalter entsprechend DIN EN 60947-5-1, Anhang K.
- Der Sicherheitsbaustein K2 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Zuleitungen zu den Positionsschaltern sind getrennt oder geschützt verlegt
- Für K1 wird eine handelsübliche SPS ohne Sicherheitsfunktionen verwendet
- Die Ventile 1V3, 1V4 und 1V5 haben eine Sperr-Mittelstellung bzw. Sperr-Stellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung und sind stellungsüberwacht.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Das Druckbegrenzungsventil 1V6 zum Schutz des Zylinders 1A und der darunter liegenden Bauteile gegen „Druckübersetzerwirkung“ erfüllt die Anforderungen der DIN EN 693:2001, Abs. 5.2.4.4.

Berechnung der Ausfallwahrscheinlichkeit

- K2 wird als Subsystem mit einer Ausfallwahrscheinlichkeit von $2{,}31 \cdot 10^{-9}$/Stunde [H] betrachtet. Der übrige Steuerungsteil wird getrennt nach Elektromechanik und Hydraulik zu zwei Subsystemen der Kategorie 4 zusammengefasst, deren Ausfallwahrscheinlichkeit im Folgenden berechnet wird.

- $MTTF_d$: Für den Positionsschalter mit Zwangsöffnung B1 ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt von Positionsschalter B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 35 040 Zyklen/Jahr und die $MTTF_d$ beträgt 285 Jahre für B1 bzw. 142 Jahre für B2. Für die Ventile 1V3, 1V4 und 1V5 wird jeweils eine $MTTF_d$ von 150 Jahren [N] angenommen. Dies ergibt einen $MTTF_d$-Wert pro Kanal von 100 bzw. 88 Jahren („hoch“) für beide Subsysteme.
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitäts-Überwachung beider Schaltzustände in K2. Der DC von 99 % für die Ventile beruht auf der direkten Überwachung der Schaltzustände durch die SPS K1. Dies ergibt einen DC_{avg} von 99 % („hoch“) für beide Subsysteme.
- Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte) für beide Subsysteme: Trennung (15), bewährte Bauteile (5), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Der elektromechanische und der hydraulische Teil der Steuerung entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (100 bzw. 88 Jahre) und hohem DC_{avg} (99 %). Damit ergeben sich mittlere Wahrscheinlichkeiten gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde und $2{,}84 \cdot 10^{-8}$/Stunde. Für die komplette Sicherheitsfunktion ergibt sich durch Addition inklusive K2 eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}54 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

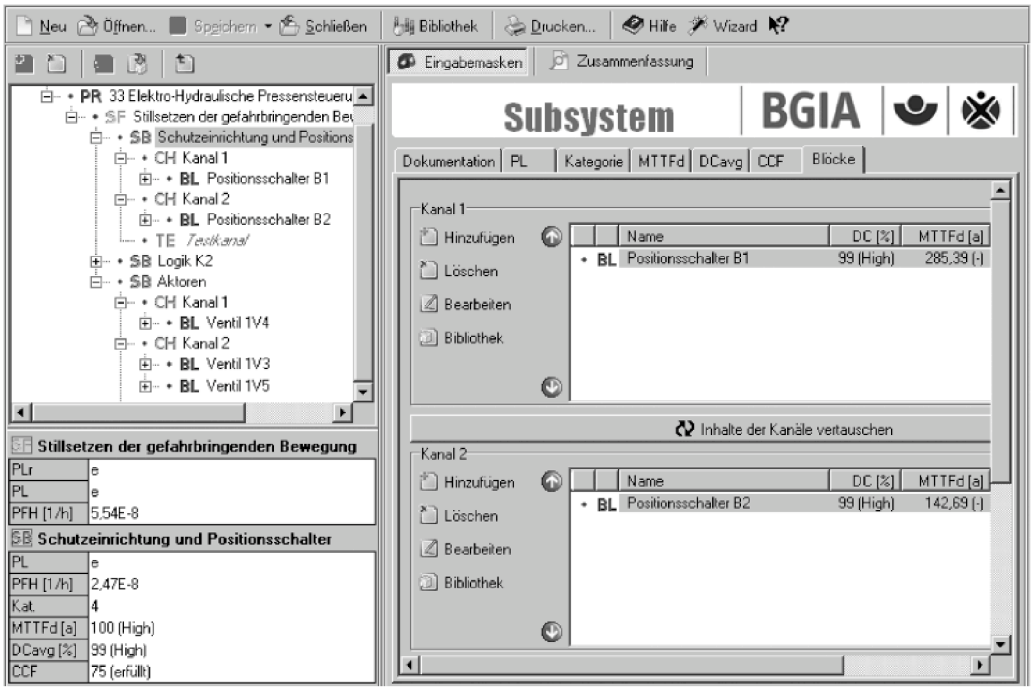


Abbildung 8.54: PL-Bestimmung mithilfe von SISTEMA