Bericht

zur Planvor- und Abnahmeprüfung der elektrischen und elektronischen Ausrüstung einer Steuerung

Berichtsnummer: 936611/ DS

TÜV SÜD Industrie Service

Mehr Sicherheit. Mehr Wert.

Auftraggeber: BMW AG
Abteilung PF-51 (Herr Biller)
80788 München

Datum: 12.11.2007

Unsere Zeichen:
IS-EG1-MAN/Ja/Ga

Prüfobjekt: Steuerung der maschinentechnischen Einrichtung: Drehscheibe

Das Dokument besteht aus 8 Seiten
Seite 1 von 8

Standort: BMW-Welt, München

Kennz.-Nr.: Theatertechnik

Bearbeiter: Dieter Jakob

Datum der Abnahmeprüfung: 02.10. 2007

Bestätigung der Mängelbeseitigung: 22.10.2007

Prüfungsergebnis:

Die Steuerung entspricht im Bereich „Not-Aus" den sicherheitstechnischen Anforderungen gemäß EN 61508/ VDE 0803 (SIL 3).
Die Gesamtanlage erfüllt die Sicherheitskategorie 3 (EN954-1) nach Implementierung der zusätzlichen Sicherheitsmaßnahmen (siehe Abschnitt 7.2).
SIL 3 nach EN 61508/ VDE 0803 wird nicht erreicht.
▶ Nur Einrichtbetrieb zulässig.

Einer Inbetriebnahme des Dauerdrehens wird, nach Implementierung der zusätzlichen Sicherheitsmaßnahmen (siehe Abschnitt 7.2), zugestimmt.
▶ Schlüsselschalter muss abgezogen werden.

Die Softwareänderungen wurden durch Herrn Müller (Greenmotion) im Protokoll „TÜV-Nacharbeiten, Protokoll_01" vom 22.10.2007 bestätigt.

Anlage: „TÜV-Nacharbeiten, Protokoll_01"

Certified System SWISSTS ISO 9001

Dieter Jakob
Telefon: +49 621 395-242
Telefax: +49 621 395-818
www.tuev-sued.de
TÜV®

TÜV SÜD Industrie Service GmbH
Niederlassung Mannheim
Abteilung Elektro- und Gebäudetechnik
Dudenstraße 28
68167 Mannheim
Deutschland

Inhaltsverzeichnis

1. Aufgabenstellung

Prüfung der sicherheitsrelevanten Teile der Rechner-Steuerung und der Hardware-Sicherheitsstromkreise auf Einhaltung der Sicherheitsanforderungen gemäß derzeit gültiger Regelwerke.

2. Prüfergebnis

Die Steuerung entspricht im Bereich „Not-Aus" den sicherheitstechnischen Anforderungen gemäß EN 61508/ VDE 0803 (SIL 3). Die Gesamtanlage erfüllt die Sicherheitskategorie 3 (EN954-1) nach Implementierung der zusätzlichen Sicherheitsmaßnahmen (siehe Abschnitt 7.2).
SIL 3 nach EN 61508/ VDE 0803 wird nicht erreicht.
► Nur Einrichtbetrieb zulässig.

Einer Inbetriebnahme des Dauerdrehens wird, nach Implementierung der zusätzlichen Sicherheitsmaßnahmen (siehe Abschnitt 7.2), zugestimmt.
► Schlüsselschalter Pult muss abgezogen werden.

2.1 Anlagenumfang

Forum Obermaschinerie		
Antrieb	**Parameter**	**Stück**
Drehscheibe	Asynchronmaschinen SPS-Steuerung, geregelt	1 Stück, 4 Antriebe

Bedienstellen		
	Ausführung	**Stück**
Funkpult	Fernwirkanlage FW, Hersteller: TELETEC GmbH Ges. für Elektronische Systeme	1 Stück.

Elektrische Anlage, Elektronische Steuerung		
Bezeichnung	**Elektrische Anlagen**	**Stück**
Einspeisung	DS	
Batterien	DS	4
Steuerspannungserzeugung	DS	
Steuer- und Regelschränke, drehzahlgeregelte Antriebe	Schaltkästen DS	
Bezeichnung	**Elektronische Steuerung**	
Bedienung, Fahrhebel	Im Funkpult integriert	
Achs -SPS	pro DS - Achse	
Kommunikations-SPS	Auf DS von/ zum Funkpult, von/ zu den Slave-SPS'n	

3. Allgemeine Angaben

3.1 Prüfgrundlagen

- BGV C1 (GUV 6.15) „Unfallverhütungsvorschrift - Veranstaltungs- und Produktionsstätten für szenische Darstellung“ (April 1998)
- DIN 56950 „Veranstaltungstechnik - Maschinentechnische Einrichtungen - Sicherheitstechnische Anforderungen und Prüfung“
- DIN EN 954-1 „Sicherheit von Maschinen“
- DIN EN 292-2 „Sicherheit von Maschinen“
- DIN EN 418 „Sicherheit von Maschinen; Not-Aus-Einrichtungen“
- DIN EN 60204-1 „Sicherheit von Maschinen; Elektrische Ausrüstung“
- **VDE 0803** **„Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme“**
- GUV 66.15 „Grundsätze für die Prüfung von sicherheitstechnischen und maschinentechnischen Einrichtungen in Bühnen und Studios“
- Schlussentwurf des Fachausschusses Elektrotechnik für die Prüfung und Zertifizierung von **„Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“**

3.2 Prüfunterlagen

- Beschreibungen
- Stromlaufpläne
- SPS- Konfiguration
- Software im Antriebsbereich

4. Technische Daten der Anlage

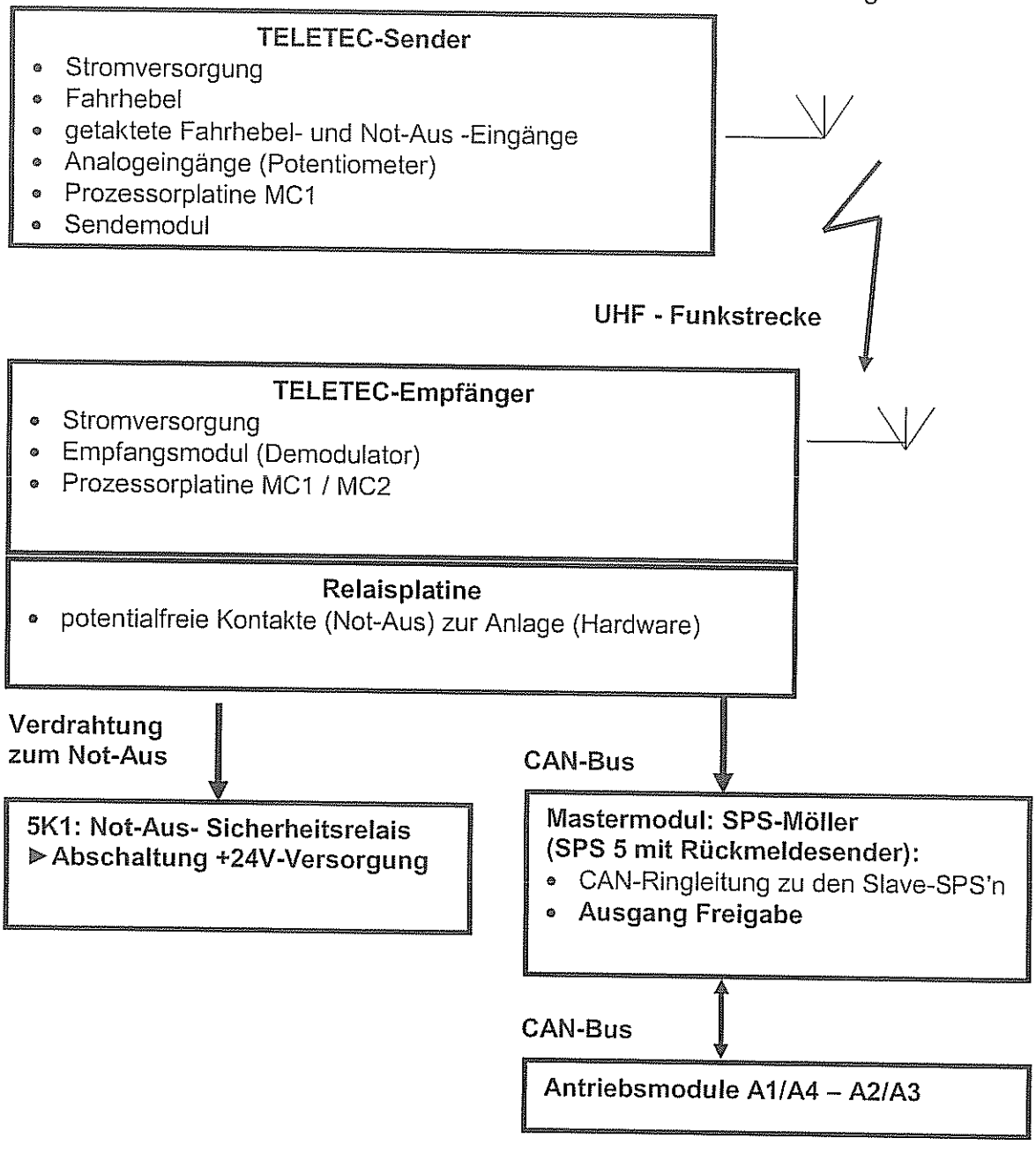
4.1 Konfiguration Funk

Allgemein

- Schlagfestes Gehäuse
- Nenntemperaturbereich: -20°C - +80°C
- Lagertemperatur: -40°C - +100°C
- Vibrationsbeständigkeit: 20g, 100h, 50...150Hz nach DIN EN 60068-2-6
- Schutzart: IP 21 nach EN 60529/ IEC 529
- Bedien -Teil → Funkstrecke → Steuerung
- Fahrhebel: TM, Drehrichtung fahren/ drehen → Sendemodul (TELETEC)

- Fahrmodischalter → Sendemodul (TELETEC)
- Not-Aus-Taster → Sendemodul (TELETEC)
- Resettaster → Sendemodul (TELETEC)
- TEL-S: Analogeingang, getaktete digitale Eingänge, Prozessor MC 1→ HF-Funkstrecke
- TEL-E: Prozessor MC 1→ Analogausgang/ digitale FH-Signale → Master-SPS
- TEL-E: Prozessor MC 2→ NA/ TM-Signale → Hardware/ Software
- Master- SPS mit Rückmeldung

Systemaufbau TELETEC, Verarbeitung der Fahrhebel- und Not-Aus-Signale



4.2 Hardwarekonfiguration Drehscheibe

Hersteller: Green Motion GmbH
Kirchstraße 2A
39326 Wolmirstedt - Elbau

- Drehscheibenwagen mit 4 Antriebsmodulen 0,8kW.
- Master- SPS (SPS 5 mit Rückmeldung zum Sender)
- Slave - SPS: Möller pro Antrieb,
- CAN-Bus-Ringleitung,
- Batteriehauptschalter, 4 Batterien (48V), Batterieladegerät,
- DC/DC-Wandler,
- Schleifring,
- Singleturn - Absolutwertgeber Drehwinkel ⇒ Slave-SPS
- Motore: Vectorregler,
- Bremsen: Robastop Silenzio Größe 4,
- SPS-Positionssteuerung,
- Not-Aus: Sicherheitsrelais,
- Wartungsschalter: Schlossschalter; abziehbar in Ausstellung

Funkpult:

- Schlüsselschalter EIN/ AUS; abziehbar,
- Fahrmodi-Schalter

4.3 Kommunikation

- Teletec-Funkstrecke
- Sicherung des Datentelegrammes, CRC-16 = Hammingdistanz 4,
- CAN-Bus: Master- SPS ↔ Slave- SPS'n
- Kommunikationsstörung (Ausfall Lebenszeichen) ⇒ Time-out Antriebsebene
  ⇒ Abschaltung der Antriebe und Löschung Fahrbefehle

4.4 Eingesetzte Steuerungskonfiguration

- Zertifizierte Funksteuerung
- nicht sicherheitsgerichtete Bedienebene
- Hardware – Not-Aus ⇒ Sicherheitsschütz Anlage
- Empfängerseite ⇒ Master -SPS mit Rückmeldung,
- Slave-SPS'n Antriebsebene

5. Prüfverfahren und eingesetzte Hilfsmittel

Bei der Prüfung der Steuerung wurden folgende Prüfschritte durchgeführt:

- Prüfung der Stromlaufpläne
- Fehlerbetrachtung
- Prüfung der Software im sicherheitsrelevantem Bereich
- Abnahmeprüfung der Anlagen hinsichtlich Funktionalität, sicherheitsgerichtete Abschaltung von Antrieb und Bremsen nach eigener Checkliste
- Fehlersimulation nach Checkliste

6. Prüfumfang

Bei der Prüfung wurden die Funktionalität und die funktionale Sicherheit der Steuerung betrachtet. Sie beinhaltete die Verschaltung aller sicherheitsrelevanten Sensoren, Aktoren sowie die Verknüpfungslogik.

Weitere Prüfungen sind:

- die Kontrolle der Kommunikationsverbindungen,
- Wirksamkeit der Not-Aus-Abschaltung ⇒ sichere Stillsetzung der Antriebe,
- die Wirksamkeit der CAN – Lebenszeichenerkennung,
- die Prüfung der Sicherheitskriterien,
- Prüfung der Not-Aus- und Totmannrampen,
- die Abfallüberwachung aller sicherheitsrelevanter Relais/ Schütze,
- die Absicherung der Steuerspannungsstromkreise,
- die Energieeinspeisung und Steuerspannungserzeugung

7. Prüfbefund

Stillsetzung von Antrieb und Bremsen:

- bei Not-Aus: sicherheitsgerichtet (5K1),
- bei Antriebsstörungen: einkanalige SPS,
- bei Kommunikationsstörungen: einkanalige SPS pro Antrieb

7.1 Prüfungen/ Tests

- Not-Aus: ⇒ Not-Aus-Rampe, o.k.
  ▶ nach Quittierung: Keine Fahrt, Start muss betätigt werden;
- Not-Aus, Fahrhebel bleibt ausgelenkt: ⇒ Not-Aus-Rampe, o.k.
  ▶ nach Quittierung: DS läuft; ⇒ Mangel
- Ausfall 24VDC am Drehzentrum während der Fahrt:
  ▶ Totmann losgelassen: DS läuft; ⇒ Mangel
- Ausfall CAN zur SPS 5 während der Fahrt:
  ▶ DS läuft ohne Fahrhebel weiter; ⇒ Mangel
- Ausfall SPS 5 während der Fahrt:
  ▶ DS läuft ohne Fahrhebel weiter; ⇒ Mangel
- Ausfall Rückmeldesender während der Fahrt:
  ▶ DS läuft ohne Fahrhebel weiter; ⇒ Mangel

Die mit Mangel bezeichneten Punkte resultieren aus der nicht vorhandenen Lebenszeichenüberwachung des CAN-Bussystems.

Diese Überwachung muss zwingend nachgerüstet werden.

7.2 Erreichte Sicherheitsanforderungen

Not-Aus: Gemäß Teletec -Zertifizierung AK5 nach DIN V VDE 19250 / 0801.

Fahrsignale: Gemäß Teletec -Zertifizierung AK3 nach DIN V VDE 19250 / 0801.

Bemerkungen:
- Diese Normen sind seit August 2004 nicht mehr gültig (zurück gezogen).

Nach Prüfung durch den Autor dieses Berichtes.
Not-Aus:
- ▶ TELETEC - Not-Aus: gemäß EN61508/VDE0803: SIL 3 –konform.
- ▶ Anlagen – Not-Aus: Ohne Zusatzmaßnahmen nicht zugelassen (Fehler: siehe Abschnitt 7.1).

Zu realisierende zusätzliche Maßnahmen:
Sicherung, dass die Antriebe bei den unten beschriebenen Fehlern stillgesetzt werden und Fahrbefehle in den Antriebssteuerungen zurückgesetzt werden.
- Not-Aus, Fahrhebel bleibt ausgelenkt: ⇒ Not-Aus-Rampe, o.k.
  - ▶ nach Quittierung: DS läuft; ⇒ Mangel

Bemerkung:
Not-Aus müsste wie Stromversorgung gestört behandelt werden.
- Ausfall 24VDC am Drehzentrum während der Fahrt:
  - ▶ Totmann losgelassen: DS läuft; ⇒ Mangel
- Ausfall CAN zur SPS 5 während der Fahrt:
  - ▶ DS läuft ohne Fahrhebel weiter; ⇒ Mangel

- Ausfall SPS 5 während der Fahrt:
  - ▶ DS läuft ohne Fahrhebel weiter; ⇒ Mangel
- Ausfall Rückmeldesender während der Fahrt:
  - ▶ DS läuft ohne Fahrhebel weiter; ⇒ Mangel

Implementierung einer Buslebenszeichenerkennung (Toggelbit) zwischen SPS 5 und SPS01 – SPS04.

Bei Ausfall des Lebenszeichen:
- ▶ Auslösung Nothalt mit Rampe durch die Antriebs-SPS'n,
- ▶ Rücksetzen aller Fahrroutinen (Fahrbefehle).

Diese Softwareänderungen wurden durch Herrn Müller (Greenmotion) im Protokoll „TÜV-Nacharbeiten, Protokoll_01" vom 22.10.2007 bestätigt.

Der SV für Leit- und Automatisierungstechnik

Jakob

D. Jakob
Niederlassung Mannheim
Abteilung Elektro- und Gebäudetechnik

TÜV-Prüfung

Im Ergebnis der am 04.10.2007 durchgeführten TÜV-Prüfung durch Herrn Jakob, TÜV Süddeutschland, an o.g. BV wurden folgende Mängel festgestellt: (fernmündlich mitgeteilt)

1. NOT-HALT entspricht nicht den Anforderungen Kategorie3 nach EN954-1
2. Fehlerüberwachung CAN-Bus und Stillsetzen sämtlicher Antriebe im Fehlerfall
3. Fehlerüberwachung Antriebe und Stillsetzen sämtlicher Antriebe im Fehlerfall

Fehlerbehebung

Die Fehler wurden wie folgt behoben/ abgestellt:

Zu 1. Schaltpläne der Servoregler wurden übersandt. Daraus ist ersichtlich und wurde von Herrn Jakob fernmündlich akzeptiert, daß eine zweikanalige redundante Abschaltung der Antriebe bei Betätigen der NOT-HALT-Einrichtung gegeben ist. Der erste Abschaltweg wird über das Batterie-Hauptschütz realisiert, welches die Leistungsspannung für die Regler-Endstufen schaltet. Dieses Hauptschütz wird bei jedem Einschaltvorgang auf Verschweißen überprüft. Der zweite Abschaltweg schaltet über ein Sicherheits-Zeitrelais direkt die Steuer- und Freigabespannung des Servoreglers ab. Ein Erzeugen eines Pulsmusters und somit Drehmomenterzeugung durch die Endstufentransistoren ist somit nicht mehr möglich. Das Versagen eines der beiden Schaltwege wird spätestens beim erneuten Wiedereinschalten bemerkt.

Zu 2: Die Software wurde wie folgt ergänzt:

1. **Fehlererfassung und –meldung „Betriebsbereit (BTB)" der Servoregler 01...08**

   a) Dazu ist von SPS_01...SPS_04 eine Sendeanforderung über CAN-Bus an den Servoregler zu schicken
   b) Auslesen sämtlicher Fehlermeldungen aus dem Antworttelegramm jedes einzelnen Servoreglers an SPS_01...SPS_04
   c) Im Fehlerfall (1 oder 2 Servoregler senden einen von sämtlichen möglichen Fehlern, siehe Auflistung unten) erfolgt NOT-HALT mit Rampe, Stoppen und Rücksetzen jeder momentan ausgeführten Fahrroutine in der Software der SPSen_01...04
   d) Erzeugen und Senden Fehlertelegramm von SPS_01...04 → SPS_05
   e) Im Fehlerfall erfolgt NOT-HALT, Stoppen und Rücksetzen jeder momentan ausgeführten Fahrroutine in der Software der SPS_05
   f) Erzeugung und Senden Fehlertelegramm von SPS_05 → Rückmeldesender
   g) Erzeugung Fehlermeldung auf dem Bedienpult (s. Bildschirm „Servoregler-Fehler")

Mögliche Fehlermeldungen aus Servoregler:

- Parameter beschädigt
- Endstufen-Fehler-Temperatur,Überspannung,Kurzschluß
- Übertragungsfehler CAN-Bus
- Resolversignal fehlerhaft
- Leistungsspannung fehlt
- Motortemperatur zu hoch
- Strom zu hoch
- Strom 1 außerhalb Toleranz
- Strom 2 außerhalb Toleranz
- Strom 3 außerhalb Toleranz
- CAN - Fehler (Hardware)
- ADC - Fehler (Hardware)
- Inkrementalgebersignal fehlerhaft
- Software Fehler

2. Fehlererfassung und –meldung „Störung CAN-Teilnehmer" SPS_01...SPS_05

Fehlerannahme: SPS_05 gestört (Störung SPS, SPS in Stop, CAN-Bus Übertragung gestört, SPS nicht eingeschaltet, Stromversorgung gestört, Batterie-hauptschalter AUS)

a) SPS_05 sendet Toggle-Bit an jede SPS_01...04, bleibt dieses Toggle-Bit aus, so wird eine fehlende/gestörte SPS_05 angenommen (CAN-Bus gestört, SPS_05 gestört)
b) Im Fehlerfall (fehlendes Toggle-Bit) erfolgt NOT-HALT mit Rampe, Stoppen und Rücksetzen jeder momentan ausgeführten Fahrroutine in der Software der SPSen_01...04
c) Bei fehlender/gestörter SPS_05 erfolgt keine Fehlermeldung auf dem Bedienpult, da bei vom CAN-Bus getrennter SPS_05 auch keine Verbindung zum Rückmeldesender besteht, in diesem Fall wird der Bildschirm „Rückmeldekanal gestört" ausgegeben

Fehlerannahme: SPS_01...SPS_04 gestört (Störung SPS, SPS in Stop, CAN-Bus Übertragung gestört, SPS nicht eingeschaltet, Stromversorgung gestört, Batterie-hauptschalter AUS)

a) SPS_01...04 senden Toggle-Bit an SPS_05, bleiben diese Toggle-Bits aus, so wird eine fehlende/gestörte SPS_01...04 angenommen (CAN-Bus gestört, SPS_01...04 gestört)
b) Im Fehlerfall (1 von 4 SPSen_01...04 „CAN-Bus gestört") erfolgt NOT-HALT, Stoppen und Rücksetzen jeder momentan ausgeführten Fahrroutine in der Software der SPS_05
c) Erzeugung und Senden Fehlertelegramm von SPS_05 → Rückmeldesender (Fehlertelegramm 0x651, Bit 2.0...2.3)
d) Erzeugung Fehlermeldung auf dem Bedienpult (s. Bildschirm „CAN-Bus Fehler")

Die Änderungen wurden am Mittwoch, 17.10.07, in München vorgenommen und in jeder möglichen Betriebsart geprüft

greenmotion
Theater-, Film- & Fernsehtechnik
Kirchstr. 2A, 39326 Wolmirstedt/Elbeu
Telefon: 039201 - 62060
Fax: 039201 - 62061
mail: info@green-motion.de
www.green-motion.de

Andreas Müller	Michael Gruber	Herr Jakob
Green motion	Waagner-Biro	TÜV Süddeutschland