TÜV EURO RAIL

TÜV PRODUCT SERVICE

Bericht zur Zertifizierung für bahnspezifische Produkte

Konformität der SIMATIC S5-95F mit Anforderungen der Bahntechnik

Hersteller:

Siemens AG
Elektronikwerk Amberg

Bericht-Nr: SN103295C Version 1.3
vom 18. August 1998

Prüf- und Zertifizierungsstelle:

TÜV PRODUCT SERVICE GmbH
Mitglied im TÜV EURO RAIL
Automation, Software and Electronics - IQSE
D-80339 München

INHALTSVERZEICHNIS:

Prüfung der Konformität des Automatisierungsgeräts SIMATIC S5-95F mit Anforderungen der Bahntechnik

1 Auftraggeber

Die TÜV Product Service Gmbh, Automation, Software and Electronics - IQSE wurde mit Schreiben vom 08.09.1997 von der Firma Siemens AG, AUT 151 mit der Prüfung der Konformität des sicherheitsgerichteten Automatisierungsgeräts SIMATIC S5-95F mit Anforderungen der Bahntechnik gemäß den Prüfgrundlagen (siehe Kapitel 3) beauftragt. Grund für die Versionerhöhung waren außer Softwareänderungen der Einsatz des Controllers SAB-C509-L DB-Step in der Stufe 2.

2 Gegenstand der Prüfung und Prüfunterlagen

Gegenstand der Prüfung ist das sicherheitsgerichtete Automatisierungsgerät SIMATIC S5-95F (Abk: AG S5-95F) der Fa. SIEMENS AG mit den im Anhang A des Berichts "Bericht zur Zertifizierung für das Automatisierungsgerät S5-95F" (Bericht-Nr. SA75794C, Revision 3.3 vom 8.10.1997 und Bericht-Nr. SN50897C, Revision 1.1 vom 28. Juli 1998) genannten Baugruppen und SW-Komponenten. Das AG S5-95F ist ohne Anwenderprogramm und entsprechende Parametrierung und Konfigurierung ein anwendungsunabhängiges sicherheitsgerichtetes programmierbares elektronisches System, das in bahntechnischen Sicherungsanlagen eingesetzt werden soll.

Die Prüfung der Konformität mit Anforderungen der Bahntechnik beruht auf den im folgenden aufgeführten Unterlagen und den in diesen Unterlagen referenzierten Dokumenten. Diese Unterlagen sind bei der Prüfstelle hinterlegt:

- "Prüfbericht zur Prüfung der Änderungen im Betriebssystem von Version ZO2 nach Version ZO3 für das AG S5-95F"
  Bericht Nr. SA94795 vom 7.04.1995
- "Prüfbericht zur Baumusterprüfung des Automatisierungsgeräts S5-95F"
  Bericht Nr. SA94895 vom 7.04.1995
- "Technischer Bericht zur Änderungsprüfung des Automatisierungsgeräts S5-95F"

- "Technischer Bericht (Nachprüfung) des Automatisierungsgeräts S5-95F" Bericht Nr. SA50977 Revision 1.0 vom 29.09.1997
- "Technischer Bericht (Nachprüfung) des Automatisierungsgeräts S5-95F" Bericht Nr. SN50557 Revision 1.1 vom 20.07.1998
- "Bericht zur Zertifizierung für das Automatisierungsgerät S5-95F" Bericht Nr. SA75794C Revision 3.3 vom 8.10.1997
- "Bericht zur Zertifizierung für das Automatisierungsgerät S5-95F" Bericht Nr. SN50897C Revision 1.1 vom 28.07.1998
- Checkliste EMV, V.1.1 vom 03.11.1995
- Checkliste Mü8004, VDE 0831, 31.10.1995
- Checkliste Mü8004, 50128, 31.10.1995
- Checkliste 50129, 31.10.1995
- Ausfallraten S5-95F, 30.10.1995
- Checkliste 50159-1, 27.08.1996
- Erprobungsprofil AG 95F und COM 95F, Version A0.2, 8.4.93
- Systemtestberichte AG 95F Betriebssystem Z02, 31.3.94
- Systemtestberichte COM 95F, Version 1.0, 30.3.94

3 Prüfgrundlagen

3.1 Vorschriften aus dem Bereich Bahntechnik

- **Mü 8004** "Anweisung zu den technischen Anforderungen für die technische Zulassung von Sicherungsanlagen", Stand 1/1996
- **ENV 50129/06.97** „Railway Applications: Safety Related Electronic Systems
- **Final Draft EN 50128/06.97** „Railway Applications: Software for Railway Control and Protection Systems"
- **Draft prEN 50159-1/7.96** „Railway Applications: Requirements for Safety-Related Communication in Closed Transmission Systems Version: 1.0"
- **DIN VDE 0831** „Elektrische Bahnsignalanlagen", August 1990
- **ENV 50121.4/02.96** „Railway Application: Electromagnetic Compatibility Part 4: Standard for Emission and Immunity of the Signalling and Telecommunications Apparatus"
- **ENV 50121.3-2/02.96** „Railway Application: Electromagnetic Compatibility Part 3-2: Requirements for Rolling Stock Apparatus"

3.2 Auszug aus den Prüfgrundlagen, die dem Zertifizierungsbericht zugrunde lagen:

3.2.1 Funktionale Sicherheit

- **DIN V 19250** "Leittechnik - Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen" entsprechend Anforderungsklasse (AK) 1 bis 6
  Ausgabe: 05.94
- **DIN V 19251** "Leittechnik - MSR-Schutzeinrichtungen - Anforderungen und Maßnahmen zur gesicherten Funktion" entsprechend Anforderungsklasse (AK) 1 bis 6; Ausgabe: 12.93 (Entwurf)
- **DIN V VDE 0801** "Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben", entsprechend Anforderungsklasse (AK) 1 bis 6
  Ausgabe: 01.90 und Änderung A1 Ausgabe 10.94
- **DIN 25448** "Ausfalleffektanalyse", Ausgabe: 05.90
- **FDIS IEC 1508** "Functional safety of electrical/electronic/programmable electronic safety-related systems"
  Part 1: General requirements: 1997
  Part 3: Software requirements: 1997
  entsprechend Safety Integrity Level (SIL) 1 bis 3
- **CDV IEC 1508** "Functional safety of electrical/electronic/programmable electronic safety-related systems"
  Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems: 1997
  entsprechend Safety Integrity Level (SIL) 1 bis 3

3.2.2 Elektrische Sicherheit, Umweltprüfungen und elektromagnetische Verträglichkeit

- **DIN VDE 0110** "Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen"Teil 1: "Grundsätzliche Festlegungen"
  Ausgabe: 01.89
  Teil 2: "Bemessung der Luft- und Kriechstrecken", Ausgabe: 01.89

- **DIN VDE 0160** "Bestimmungen für die Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln"
  Ausgabe: 05.88 und VDE 0160A1 Ausgabe: 04.89
- **prEN 50178** " Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln"
  Ausgabe: 10.96
- **IEC 1131-2** " Speicherprogrammierbare Steuerungen"
  Betriebsmittelanforderungen und Prüfungen
  Ausgabe: 09.92
- **EN 50081-2** "Elektromagnetische Verträglichkeit (EMV)
  Fachgrundnorm Störaussendung
  Teil 2: Industriebereich, Ausgabe: 08.93
- **EN 50082-2** "Elektromagnetische Verträglichkeit (EMV)
  Fachgrundnorm Störfestigkeit
  Teil 2: Industriebereich, Ausgabe: 03.95
- **EN 55011** (identisch mit DIN VDE 0871 Teil 11 Ausgabe: 07.92)
  "Grenzwerte und Meßverfahren für Funkstörungen von industriellen und wissenschaftlichen und medizinischen Hochfrequenzgeräten"
  Klasse A, Ausgabe: 07.91
- **IEC 801** "Elektromagnetische Verträglichkeit von Meß-, Steuer- und Regeleinrichtungen in der industriellen Prozeßtechnik"
  entsprechend Schärfegrad II/III (teilweise IV)
  Teil 1: "Allgemeine Einführung" Ausgabe: 09.87
  Teil 2: "Störfestigkeit gegen die Entladung statischer Elektrizität"
  (identisch mit DIN VDE 0843 Teil 2 Ausgabe: 01.91
  und DIN EN 60801-2 Ausgabe 03.94)
  Teil 3: "Störfestigkeit gegen elektromagnetische Felder"
  (identisch mit DIN VDE 0843 Teil 3 Ausgabe: 02.88)
  ersetzt durch ENV 50140 Ausgabe 1994 mit gleichen Anforderungen
  Teil 4: "Störfestigkeit gegen schnelle transiente Störgrößen; Burst"
  IEC 65 (CO) 39 /12.85 identisch mit E DIN VDE 0843 Teil 4
  Ausgabe 09.87
  sowie nur für die zertifizierten sicherheitsgerichteten Baugruppen nach Anhang A
  Teil 5: "Störfestigkeit gegen Stoßspannungen"
  IEC 65A/77B(Sec) 120/87 identisch mit E DIN VDE 0843 Teil 5 Ausgabe 02.92
  Teil 6: "Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder über 9 kHz"

IEC 65A/77B (Sec) 131/91 identisch mit E DIN VDE 0843 Teil 6 Ausgabe 08.92

- **DIN IEC 68** "Grundlegende Umweltprüfverfahren"
  Teil 1-1 "Allgemeines und Leitfaden" Ausgabe 11.90
  Teil 2-1 Prüfgruppe A: "Kälte", Ausgabe 08.85
  Teil 2-2 Prüfgruppe B: "Trockene Wärme", Ausgabe 03.80
  Teil 2-6 Prüfung Fc: "Schwingungen sinusförmig", Ausgabe 06.90
  sowie nur für die zertifizierten sicherheitsgerichteten Baugruppen nach Anhang A
  Teil 2-3 Prüfung Ca: "Feuchte Wärme", Ausgabe 12.86
  Teil 2-14 Prüfgruppe N: "Temperaturwechsel" Ausgabe 06.87
  Teil 2-27 Prüfung Ea und Leitfaden "Schocken" Ausgabe 08.89
  Teil 2-30 Prüfung Db und Leitfaden: "Feuchte Wärme, zyklisch", Ausg. 09.86
  Teil 2-32 Prüfgruppe Ed: "Frei Fallen", Ausgabe 05.84

3.2.3 Prüfgrundlagen für Maschinenanwendungen gemäß Prüfbericht von BIA (/Z02/)

- **DIN EN 60204** Teil 1: "Sicherheit von Maschinen, Elektrische Ausrüstung von Maschinen, Teil 1 Allgemeine Anforderungen", 06.93
- **EN 418** "Sicherheit von Maschinen NOT-AUS-Einrichtung, funktionale Aspekte Gestaltungsleitsätze", 11.92
- **EN 954-1** Teil 1: "Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze", 12.96

3.2.4 Anwendungsspezifische Prüfgrundlagen

- **VDE 0832** "Straßenverkehrs-Signalanlagen", Ziffer 4.1 Ausgabe: 03.90 und Änderung von 07.90

3.2.5 Produktbezogene Qualitätssicherung

- **DIN ISO 9001** "Qualitätssicherungssysteme; Modell zur Darlegung der Qualitätssicherung in Design/Entwicklung, Produktion, Montage und Kundendienst", Ausgabe 05.90
- **93/465/EWG** Beschluss des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE-Konformitätskennzeichnung.

- **QSH IQSE** "Qualitätssicherungshandbuch des IQSE"
  Version 1.5

4 Sicherheitstechnische Systemeigenschaften

4.1 Systemkonfiguration

Das Automatisierungsgerät S5-95F ist eine sicherheitsgerichtete speicherprogrammierbare Steuerung auf der Basis einer homogenen Redundanz mit sicherheitsgerichtetem Vergleich und automatischen Selbsttests. Das Automatisierungsgerät besteht aus zwei identischen Teilgeräten, die mittels Lichtwellenleiter gekoppelt sind.

In der Grundkonfiguration stehen 20 sicherheitsgerichtete Eingänge, zwei sicherheitsgerichtete Zähler, acht sicherheitsgerichtete Ausgänge und acht nicht sicherheitsgerichtete Ausgänge zur Verfügung. Alle sicherheitsgerichteten Eingänge können auch als Alarmeingänge parametriert werden. Wahlweise können vier dieser Eingänge als Alarmeingänge mit sehr schnellen Reaktionszeiten parametriert werden.

Mittels externen BUS-Modulen kann das Automatisierungsgerät um bis zu 16 redundante sicherheitsgerichtete externe digitale E/A-Baugruppen bzw. 32 nicht-sicherheitsgerichteten Baugruppen erweitert werden (siehe Liste der geprüften Baugruppen im Anhang A).

Aufgrund der Ringstruktur und durch die zyklischen und ergänzenden Tests ist die Rückwirkungsfreiheit des seriellen BUS (Extern-Peripherie) für alle die Baugruppen gewährleistet, deren BUS-Schnittstelle mittels einem BUS-ASIC aus der Familie der AG-100 Busbaugruppen realisiert ist. Andere Baugruppen müssen separat zur Genehmigung vorgelegt werden.

Das Automatisierungsgerät hat drei Betriebsarten (siehe Gerätehandbuch [GHB] Kap.2.5.2): Testbetrieb, Quasi-Sicherheitsbetrieb und Sicherheitsbetrieb. Im Testbetrieb (z.B. während der Inbetriebnahme) ist das Anwenderprogramm im RAM gespeichert. In dieser Betriebsart ist ein Ändern des Anwenderprogramms möglich. Die sicherheitstechnischen Überwachungen sind dabei reduziert (ev. verlängerte Reaktionszeiten im Statusbetrieb, keine Anlauftests, jedoch Durchführung aller zyklischen Hintergrundtests). Die Betriebsart Quasi-Sicherheitsbetrieb entspricht dem Sicherheitsbetrieb, mit dem Unterschied, daß das Anwenderprogramm im RAM gespeichert ist. Nach erfolgter Fertigstellung muß das Anwenderprogramm in EPROMs gespeichert werden. Dies ist der sicherheitstechnisch zugelassene "Sicherheitsbetrieb". In den Betriebsarten Quasi-Sicherheitsbetrieb und Sicherheitsbetrieb werden zusätzlich beim STOP-RUN Übergang die Anlauftests durchgeführt und die schreibende Bedienung mittels Programmiergerät ist eingeschränkt.

4.2 E/A-Peripherie-Konfiguration

Die in Kapitel 18.2.1 des Gerätehandbuchs genannten sicherheitsgerichteten Schaltschemas für E/A-Peripherie sind für sicherheitsrelevante Anwendungen geeignet. Bei Einsatz der nicht sicherheitsgerichteten Schaltschemas ist die Rückwirkungsfreiheit bezüglich den sicherheitsgerichteten E/A Baugruppen gewährleistet.

4.3 Alarmbearbeitung

Das AG S5-95F bietet neben der zyklischen Programmbearbeitung auch zwei Arten der schnellen interruptgesteuerten Alarmbearbeitung von Prozeßereignissen. Die überwachten Alarmreaktionszeiten betragen für OB2-Alarme (EB59) im worst-case ca. 10 ms, für OB3-Alarme liegen diese im Bereich von 5 bis 30 ms zuzüglich den Alarmbearbeitungszeiten (siehe Gerätehandbuch Kap. 18.12 ff).

4.4 Parametrierung und Sicherung des Anwenderprogramms gegen Verfälschungen im Programmiergerät

Das AG 95F wird mit der Parametrierungs- und Dokumentationssoftware COM 95F entsprechend den Anforderungen der jeweiligen Applikation parametriert.

Die Erzeugung und Übertragung der Parametrierungsdaten (im DB1) mit COM 95F ist mittels diversitärer Rückübersetzung und Vergleich gesichert.

Zur Sicherung des Anwenderprogramms gegen Verfälschungen durch das Programmiergerät wird mit COM 95F ein Verfälschungs- und Änderungsvergleicher zur Verfügung gestellt. Dieser stellt über diversitäre Verfahren sicher, daß alle Veränderungen zwischen implementiertem Anwenderprogramm (auf EPROM) und dem geprüften und getesteten Anwenderprogramm (auf Diskette, bzw. auf Papier) aufgezeigt werden.

Die Sicherung des in EPROMs gespeicherten Anwenderprogramms erfolgt mittels einem hochwertigen CRC.

4.5 Kommunikation

Es sind sowohl sicherheitsgerichtete als auch nicht sicherheitsgerichtete Kommunikationsmöglichkeiten vorhanden. Die folgende Tabelle zeigt beispielhaft die Möglichkeiten auf.

Kopplungspartner der S5-95F zu	Sicherheitsgerichtete und rückwirkungsfreie Kopplungsmöglichkeiten	Rückwirkungsfreie Kopplungsmöglichkeiten
S5-95F oder S5-115F	- SINEC-L1 (sicherheitsgerichtet) - SINEC-L1 (sicherheitsgerichteter Broadcast = sicherheits-gerichtete Rundruftelegramme) - SINEC-L1 mit redundanten BUS (sicherheitsgerichtet und hochverfügbar auch mit Broadcast) - digitale E/A-Kopplung (zweikanalige sicherheitsgerichtete Anschaltung)	- SINEC-L1 (nicht sicherheitsgerichtet) - CP521 SI - E/A-Kopplung (einkanalig, nicht sicherheitsgerichtet)
1) U- oder H- Geräte der Simatic S5-Reihe 2) Fremdgeräte	nicht möglich	- SINEC-L1 (nicht sicherheitsgerichtet) - CP521 SI - E/A-Kopplung (einkanalig, nicht sicherheitsgerichtet)

Legende:

SINEC-L1	Kopplung über SINEC-L1 BUS
CP521	Kopplung über CP521-Baugruppe
E/A-Kopplung	direkte digitale Ausgangs/Eingangskopplung zwischen zwei Geräten

(siehe Gerätehandbuch Kap. 18)

4.6 Weitere sicherheitsrelevante Systemeigenschaften

Die sicherheitsrelevanten Systemeigenschaften wie z.B. Reaktionszeiten, Remanenzverhalten von Merkern, Daten und Zählern, anwenderprogrammierbares Fehlerreaktionsverhalten (Passivierung, Einheitswertbildung, Diskrepanzzeiten, Diskrepanzwerte) werden im Gerätehandbuch Kapitel 18ff näher spezifiziert. Die Einhaltung der sicherheitstechnischen Anforderungen ist anwendungspezifisch zu prüfen.

5 Durchführung der Prüfungen und Begutachtung

Die Prüfung der Konformität der S5-95F mit den Anforderungen der Bahntechnik (siehe Kapitel 3.1) basiert auf einem Vergleich und einer Bewertung der in dem Prüf- bzw. Zertifizierungsbericht (siehe Kapitel 2) dokumentierten Prüfergebnisse. Gemäß dem Prüf- bzw. Zertifizierungsbericht wurde eine Fehlerbetrachtung durchgeführt, die bis zu 3 einzeln ungefährliche und unerkannte Fehler kombiniert. Damit wurden bei der Prüfung der S5-95F höhere Anforderungen zugrunde gelegt als gemäß Anforderungsklasse 6 nach DIN V VDE 0801 A1 gefordert sind (Kombination von 2 Fehlern). Darüberhinaus wurde gemäß IEC 65A(Sec)123 eine Fail-to-Danger-Berechnung durchgeführt, die probabilistische Ausfallkenngrößen liefert, wie sie in Mü 8004 gefordert werden. Damit war die Grundlage für die Beurteilung gegeben, daß die Anforderungen der Mü 8004 hinsichtlich Ausfallauswirkungen (Ausfalloffenbarungszeit, Mehrfach-Fehlerbetrachung) von der S5-95F erfüllt werden können.

Die an dem vorliegenden Prüfbericht beteiligten Personen waren nicht bzw. mit anderen Aufgabenstellungen bei der Erstellung des Prüf- bzw. Zertifizierungsberichts beteiligt. Die Ergebnisse des Vergleichs und der Bewertung wurden in Checklisten festgehalten.

6 Zusammenfassung der Prüfergebnisse

6.1 Konformität mit Mü 8004

6.1.1 Funktionsnachweis (42000)

Der Funktionsnachweis baut auf der firmeneigenen Validierung des AG S5-95F und den zusätzlichen Systemtests auf. Die Beschreibung der technischen Lösung erfüllt die gestellten Anforderungen. Die Firma Siemens AG Bereich AUT besitzt ein zertifiziertes und überwachtes Qualitätsmanagement-System nach DIN ISO 9001. Zusätzlich wird die Zertifizierungsstelle der TÜV Product Service GmbH einen auf das beurteilte Produkt abgestimmten Follow-Up Service als Bestandteil der Zertifizierung durchführen.
Der Funktionsnachweis ist gegeben.

6.1.2 Ausfallauswirkungen (43000)

Durch die vorliegende Systemstruktur des AG S5-95F (homogen redundantes System mit gegenseitigem Vergleich, identische Teilsysteme sind durch Lichtwellenleiter gekoppelt) ist die Ungefährlichkeit von Einzelausfällen bzw. die Unabhängigkeit der Betrachtungseinheiten gegeben.

Unabhängige, einzeln ungefährliche und unerkannte Fehler wurden bis zu einer Kombination von 3 Fehlern betrachtet. Für die Fehlerbetrachtung wurde unterstellt, daß ein unabhängiger Zweitfehler frühestens nach der sog. „Zweitfehlereintrittszeit" eintritt (1 Stunde). Der sichere Zustand blieb für alle untersuchten Fälle bestehen, alle Selbsttests werden innerhalb einer Stunde durchgeführt.

Für das AG S5-95F wurde eine Berechnung der Sicherheitsausfallrate (fail-to-danger rate) auf der Basis eines Markov-Modells auf Systemebene durchgeführt (vgl. Bericht Nr. 103395 vom 30.10.95). Die Sicherheitsausfallrate setzt sich zusammen aus gefährlichen, unerkennbaren Fehlern und aus gefährlichen, erkennbaren Fehlern und Fehlerkombinationen, die durch die automatischen Tests erkannt wurden (spätestens innerhalb einer Stunde). Unerkennbare, gefährliche Fehler werden frühestens beim Austausch der Anlage behoben oder verbleiben für die gesamte Lebensdauer in der Anlage. Somit muß als „worst-case" für die Fehleroffenbarungszeit die Lebensdauer angenommen werden.

Lebensdauer	T_{life}	=	**10 Jahre**		
Sicherheitsausfallrate	a_{Sich}	=	**4,12*10-9/h**		
Anforderung nach 43310 (T0 = 1/(1000*a))	a_{43310}	=	**10*10-9/h**		
Sicherheitsfaktor	**Fs**	=	**10/4,12**	=	**2,77**

Bei der errechneten Ausfallrate müßte eine Lebensdauer von mehr als 27,7 Jahren angenommen werden, damit die Anforderung nicht erfüllt ist. Daraus läßt sich unter Berücksichtigung eines angenommenen Sicherheitsabstands die Forderung ableiten, daß nach 20 Jahren das AG S5-95F entweder ausgetauscht oder so ausführlich geprüft wird, daß durch die Selbsttests nicht aufgedeckte Fehler entdeckt werden.

Die Anforderungen an die Ausfallauswirkungen sind erfüllt.

6.1.3 Sichere Datenübertragung

Die qualitativen Anforderungen der pr EN 50159-1 (Kapitel 5, 6 und 7.1) für die sichere Datenübertragung sind erfüllt. Die quantitativen Anforderungen für die sichere Datenübertragung (u.a. Restfehler-Wahrscheinlichkeit der Datenübertragung) hängen von den quantitativen Sicherheitsanforderungen für das gesamte sicherheitsgerichtete Kommunikationssystem („hazardous failure rate for the entire system $R_{h''}$ - siehe Kapitel 7.2 und 7.3 aus pr EN 50159-1) ab. Da die Sicherheitsausfallrate R_h gemäß EN 50126 und EN50129 bestimmt wird und derzeit noch nicht endgültig festgelegt ist, kann die Erfüllung der quantitativen Anforderungen für die Sicherheitsausfallrate erst dann überprüft werden, wenn R_h für die konkrete Anwendung bestimmt ist.

6.1.4 Störauswirkungen (44000)

Die speziellen Anforderungen hinschtlich Elektromagnetischer Verträglichkeit (EMV) gemäß der „Leitlinie für die Prüfung der Hardware im E1 L-Stellwerk" sind bis auf den Walky Talky-Test nach IEC 801-3, der in der speziellen Form nicht durchgeführt wurde, erfüllt (siehe dazu auch Kapitel 6.4 Konformität mit ENV 50121).

6.1.5 Sicherheitsbezogene Anwendungsvorschriften (45000)

1. Die im Kapitel 10 des Berichts "Bericht zur Zertifizierung für das Automatisierungsgerät S5-95F, Bericht Nr. SA75794C" aufgeführten Auflagen für Errichtung und Betrieb einer Automatisierung mit S5-95F sind zu beachten.

2. Bei dem Einsatz des Automatisierungsgeräts S5-95F in Sicherungsanlagen ist darauf zu achten, daß das Beanspruchungprofil des AG S5-95F hinsichtlich mechanischen,klimatischen, thermischen, chemischen Beanspruchungen, Einwirkungen durch Fremstoffe (Staub und Wasser) und elektromagnetischen Einwirkungen eingehalten wird (siehe dazu Mü8004, Richtlinie 34200 Regel 3,4,5).

3. Bezüglich den Anforderungen an die sichere Datenübertragung ist die Erfüllung der quantitativen Anforderungen (u.a. Bestimmung der Restfehler-Wahrscheinlichkeit) anwendungsbezogen nachzuweisen, sofern die Anforderungen nach EN 50159 zur Anwendung kommen.

4. Die speziellen Anforderungen der „Leitlinie für die Prüfung der Hardware im E1 L-Stellwerk" gemäß dem Walky Talky-Test nach IEC 801-3 sind zu erfüllen (siehe dazu auch Kapitel 6.4 Konformität mit ENV 50121).

5. 20 Jahre nach Errichtung einer Sicherungsanlage mit einem AG S5-95F ist dieses so zu prüfen, daß alle Fehler entdeckt werden, die durch automatische Selbsttests nicht aufgedeckt werden konnten.

6.1.6 Vorgaben zur Erprobung (12000)

Da das AG S5-95F eine anwendungunabhängige Sicherungsanlage darstellt, sind Vorgaben zur Erprobung erst dann relevant, wenn die Bedingungen für eine Betriebs-, Zuverlässigkeits- oder Sicherheitserprobung vor Ort festgelegt sind.

6.1.7 Allgemeine Bestimmungen

Die Anforderungen hinsichtlich
Schutzmaßnahmen (33100, 33200),
Einsatzbedingungen (34100),
Anforderungen an Betriebsmittel (Signalanlagen auf Fahrzeugen (35080): Nennspannungen),
Isolation (37200, 37210) sind erfüllt.

Die Anforderungen hinsichtlich
Einsatzbedingungen (Allgemeine Klimabedingungen (34200): Innenraum Höchstwert, Außenraum Höchst- und Tiefstwert),
Anforderungen an Betriebsmittel (Signalanlagen auf Fahrzeugen (35080): Betriebs- und Lagertemperatur, mechanische Beanspruchungen) sind nicht erfüllt.

Die Einsatzbedingungen müssen entsprechend dem jeweiligen Einsatzfall durch andere Maßnahmen (z.B. entsprechende Klimatisierung) erfüllt werden.

6.1.8 Gesamtergebnis

Die Anforderungen der Mü8004 hinsichtlich dem Funktionsnachweis, den Ausfall- und Störauswirkungen für das anwendungsunabhängige sicherheitsgerichtete Automatisierungssystem SIMATIC S5-95F sind unter Beachtung der Sicherheitsbezogenen Anwendungsvorschriften (siehe Kapitel 6.1.4) erfüllt. Die zertifizierten Baugruppen und SW-Komponenten sind im Anhang A des Berichts "Bericht zur Zertifizierung für das Automatisierungsgerät S5-95F" (Bericht-Nr. SA75794C, Revision 3.3 vom 8.10.1997 und Bericht-Nr. SN50897C, Revision 1.1 vom 28.07.1998) aufgelistet.

6.2 Konformität mit DIN VDE 0831

Folgende Anforderungen sind erfüllt:

- Schutzanforderungen/Kapitel 3,
- Allgemeine Anforderungen für ortsfeste Betriebsmittel der Signalanlagen/Kapitel 4
  (Nennspannungen, allgemeine Klimabedingungen Innenraum, Einhaltung der zulässigen Grenztemperaturen der Betriebsmittel, Isolation),
- Anforderungen an elektrische Betriebsmittel/Kapitel 5
  (Transformatoren, spezielle Bauelemente, auch solche der Elektronik).
- Signaltechnische Anforderungen/Kapitel 6 sind analog Richtlinie 43000 Ausfallauswirkungen, Mü 8004, erfüllt.

Die in Kapitel 6.1.4 definierten sicherheitsbezogenen Anwendungsvorschriften für das AG S5-95F sind zu beachten.

Folgende Anforderungen sind nicht erfüllt:

- Allgemeine Anforderungen für ortsfeste Betriebsmittel der Signalanlagen/Kapitel 4
  (allgemeine Klimabedingungen in Freiluft),
- Anforderungen an Betriebsmittel der Signalanlagen auf Fahrzeugen/Kapitel 7.6
  (Mechanische Beanspruchungen 7.6.3, Umgebungstemperaturen 7.6.4).

6.3 Konformität mit EN 50129, 50128

Die Analyse und Bewertung der Dokumentation des Herstellers und der Prüfergebnisse hat ergeben, daß die grundsätzlichen Anforderungen an
- das Qualitätsmanagement,
- das Sicherheitsmanagement und
- die funktionale und technische Sicherheit erfüllt sind. Eine Zuordnung einzelner Maßnahmen zu Safety Integrity Levels (SIL) ist möglich. Da eine endgültige Zuordnung der Maßnahmen zu Safety Integrity Levels nach dem derzeitigen Bearbeitungsstand der EN 50129 und EN 50128 nicht vorliegt (insbesondere hinsichtlich der „hazadous failure rate"), wurde es nicht für sinnvoll erachtet, das AG S5-95F einem Safety Integrity Levels zuzuordnen.

6.4 Konformität mit EN 50121 (EMV)

6.4.1 Konformität mit prEN 50121-4 (signalling apparatus)

Die Anforderungen an die Emission sind erfüllt.

Die Anforderungen an die Immission sind bis auf die Einwirkung von Magnetfeldern nach EN 61000-4-8 bzw. 61000-4-19 erfüllt.

6.4.2 Konformität mit prEN 50121-3-2 (rolling stock app.)

Die Anforderungen an die Störaussendung/Emission sind erfüllt.

Die Anforderungen an die Störbeeinflußbarkeit/Imission sind erfüllt.

7 Zertifikatsnummer

Für das sicherheitsgerichtete Automatisierungssystem SIMATIC S5-95F wird unter Beachtung der unten genannten Bedingungen das Zertifikat mit der Zertifikatsnummer: **95/M/001** erteilt.

TÜV Product Service GmbH
Mitglied im TÜV EURO RAIL
Automation, Software and Electronics - IQSE

i. V. Bosch