TÜV Rheinland
Berlin Brandenburg

Automation, Software und Informationstechnologie

Stellungnahme zu einem Konzept des Bussystems der Firma RK TEC Rauchklappen-Steuerungssysteme GmbH & Co. KG zur Ansteuerung von Entrauchungsklappen

Bericht-Nr.: 968/EL 210.00/03
Datum: 2003-03-31

**Stellungnahme zu einem Konzept des Bussystems
der Firma RK TEC Rauchklappen-Steuerungssysteme GmbH & Co. KG
zur Ansteuerung von Entrauchungsklappen**

Bericht-Nr.:	968/EL 210.00/03
Datum des Berichtes:	2003-03-31
Seitenzahl ohne Anlagen:	8
Prüfgegenstand:	Konzept für ein sicheres Busprotokoll der Firma RK TEC
Auftraggeber/Hersteller:	RK TEC Rauchklappen-Steuerungssysteme GmbH & Co. KG Morsestraße 9a 50769 Köln
Auftrags-Nr. des Auftraggebers/Datum:	B0221OlympBerlin-2TÜV vom 2002-10-15
Prüfinstitut:	TÜV Anlagentechnik GmbH Automation, Software und Informationstechnologie Am Grauen Stein D-51105 Köln
Auftrags-Nr. des Prüfinstitutes/Datum:	968/264218 vom 2002-11-07
Angebots-Nr. des Prüfinstitutes/Datum:	968/117102 vom 2002-09-25
Bearbeiter:	Dipl. Phys. Erich Janoschek
Prüfort:	siehe Prüfinstitut
Zeitraum der Prüfung:	Oktober 2002 bis März 2003

Die Prüfergebnisse beziehen sich ausschließlich auf die Prüfgegenstände.

Inhaltsverzeichnis **Seite**

1. Aufgabenstellung

Das von der Firma RK TEC entwickelte Bussystem soll die konventionelle Ansteuerung von Entrauchungsklappen ersetzen.

Im Rahmen dieser Konzeptbeurteilung soll untersucht werden, ob das verwendete Busprotokoll geeignet ist, die Anforderungen, die an ein sicheres Busprotokoll gestellt werden, bis zum Sicherheits-Integritätslevel 2 zu erfüllen.

Die Betrachtungen der sicherheitsgerichteten Busteilnehmer ist nicht Gegenstand dieser Konzeptprüfung.

2. Prüfgrundlagen

[1] IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems ”, Part 1 - 7, 2000

[2] MBO, 01.12.1997, Musterbauordnung

[3] EN 60870-5-1:1993 Fernwirkeinrichtungen und -systeme
Teil 5: Übertragungsprotokolle

[4] Prüfgrundsatz für die Prüfung und Zertifizierung von Bussystemen
BG Fachausschuss Elektrotechnik, Ausgabe 05.02

3. Prüfgegenstand

Prüfgegenstand ist das Konzept für ein sicheres Busprotokoll der Firma RK TEC Rauchklappen-Steuerungssysteme GmbH & Co. KG.

3.1 Prüfunterlagen

Buskonzept der Firma RK TEC Rauchklappen-Steuerungssysteme GmbH & Co. KG vom 23.08.2003

4. Durchführung der Prüfung und Prüfergebnisse

4.1 Ermittlung des Istzustandes und Übertragung der Anforderungen auf ein Bussystem

Bisher wurde in Brandmeldeanlagen die Ansteuerung der Entrauchungsklappen in konventioneller Technik ausgeführt. Die Ausführung erfolgte gemäß einschlägigem Normenwerk (z. B. MBO, DIN 4102).

Der Einsatz von Bussystemen erfordert eine Erweiterung der bisherigen Betrachtungsweise und die Anwendung von Normen, die den Einsatz von Bussystemen auch in anderen Anwendungen im Bereich der Sicherheitstechnik regelt, wie z. B. die IEC 61508 Teil 1 - 7.

Entsprechend dieser Norm werden technischen Anlagen, die dem Schutz von Personen dienen, und darunter fallen die Entrauchungsanlagen, in sogenannte Sicherheitsklassen, auch SIL (Safety Integrity Level) genannt, eingeteilt. Insgesamt gibt es vier Level. Je höher der SIL-Level, desto größer ist das Risiko für den Menschen und desto höher sind die sicherheitstechnischen Anforderungen an die im Gebäude einzusetzende Technik.

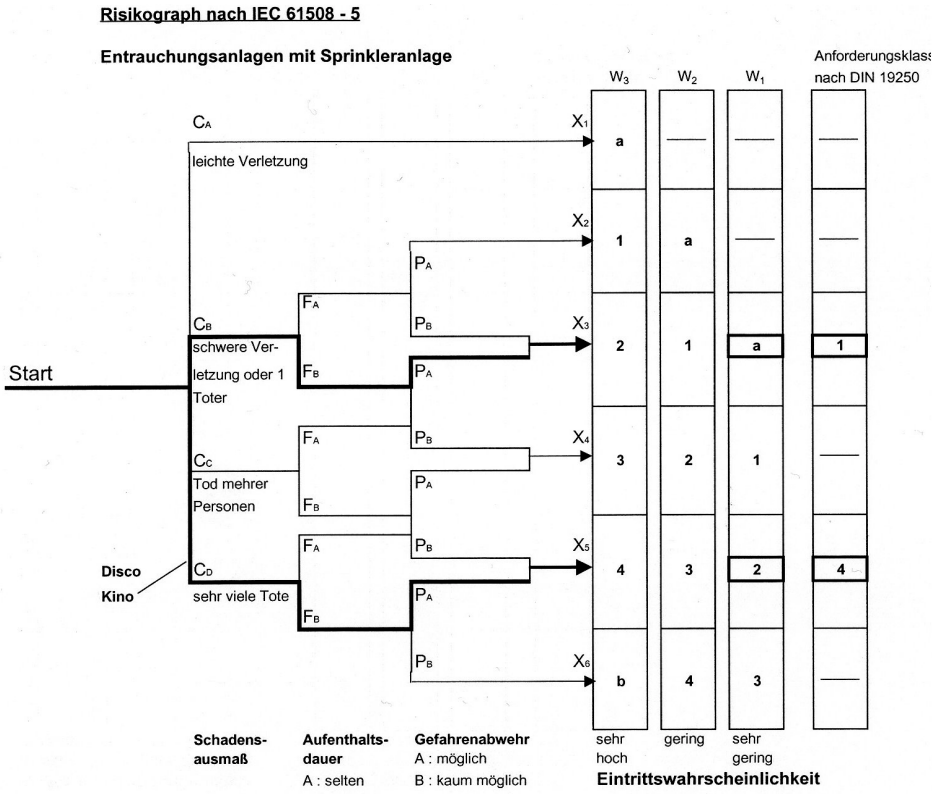
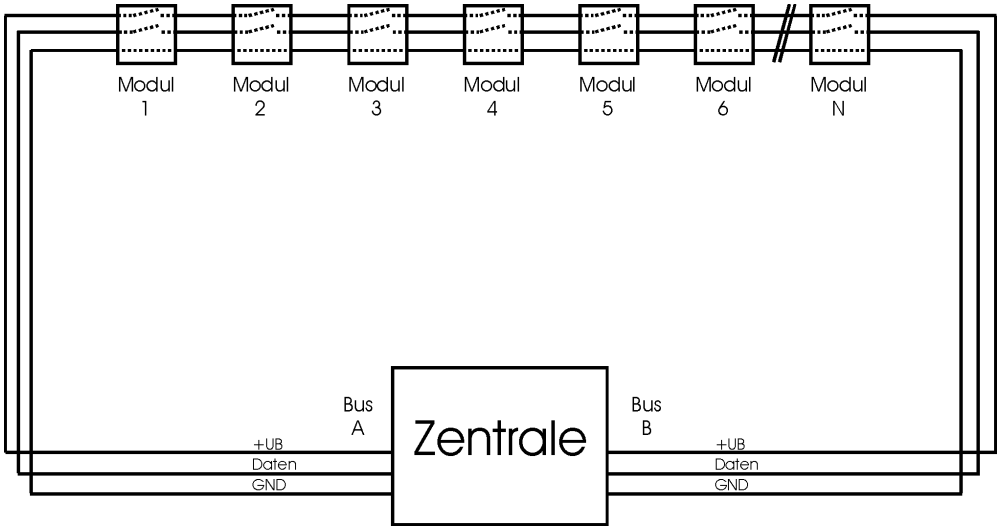


Abbildung 1 Risikograph und Anforderungsklassen nach IEC 61508

Anhand verschiedener Risikountersuchungen hat sich gezeigt, dass im Normalfall Brandschutzeinrichtungen in Gebäuden die Anforderungen der SIL-Klassen SIL 1 oder SIL 2 einzuhalten haben. Die zu erfüllenden Anforderungen sind detailliert in der IEC 61508 beschrieben und entsprechende Überprüfungen können von autorisierten Prüfinstituten durchgeführt werden.

4.2 Konzept des Busprotokolls der Firma RK TEC

4.2.1 Beschreibung des RK TEC-Systems



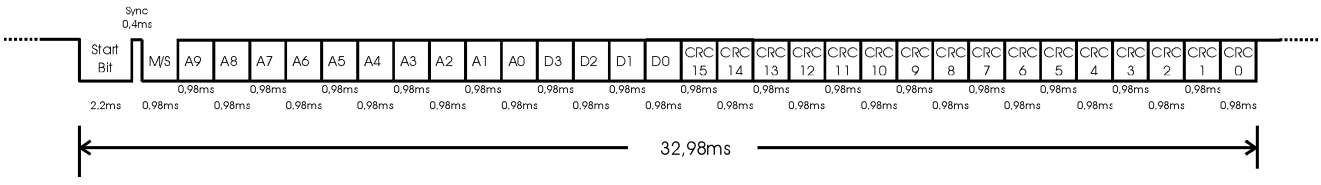
Das System besteht aus einer Zentrale und aus bis zu 1000 Modulen. M/MFW-Module bieten Anschlussmöglichkeiten für Rauchklappenmotoren und deren Endschalter. Die Zentrale ist im Bussystem nur einmal vertreten, kann aber auch redundant ausgelegt werden und steuert den Ablauf der Bus-Kommunikation.

Die Module und die Zentrale sind miteinander durch einen Drei-Draht-Ringbus verbunden. Zwei der Leitungen dienen zur Versorgung der Module. Die dritte Leitung wird als Datenleitung mit Bezug zur Masseleitung der Versorgungsspannung verwendet. Die Datenleitung wird durch die Zentrale von einer Stromquelle gespeist. Die Module und die Zentrale modulieren diese Stromquelle zur Datenübertragung mit „OPEN COLLECTOR“ Ausgängen.

4.2.2 Aufbau der Datentelegramme

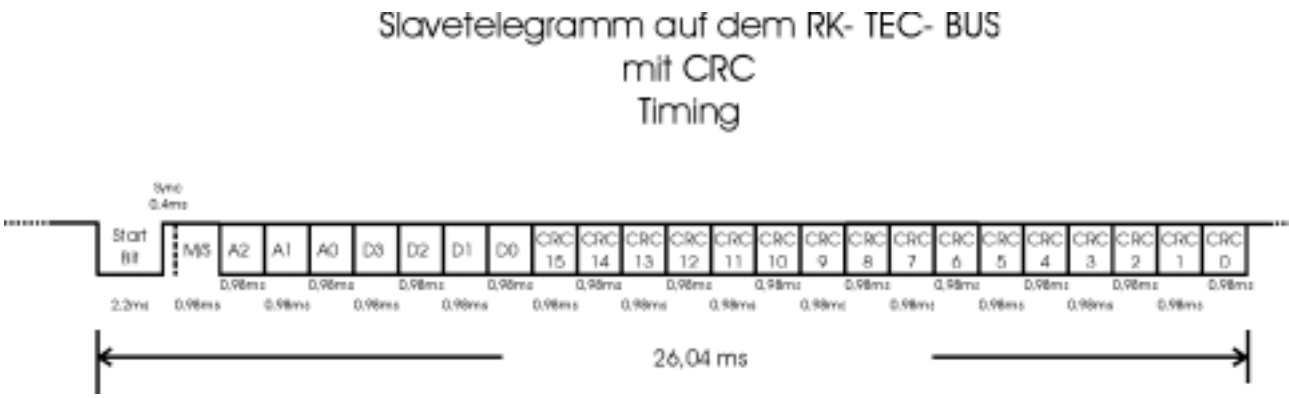
Die Kommunikation wird komplett durch den Master (die Zentrale) gesteuert. Das Master Telegramm besteht aus einem Startbit, einem kurzen Sync-Bit und einem Master-Slave-Bit. Darauf folgen zehn Adressbits und vier Datenbits. Anschließend werden 16 CRC-Bits übertragen. Insgesamt dauert eine Datensendung vom Master zu einem Slave 32,98 ms.

Mastertelegramm auf dem RK- TEC- BUS
mit CRC
Timing



Nach einer Masteransprache erfolgt, nach einer bestimmten Verarbeitungszeit durch das Modul, eine Antwort von dem angesprochenem Modul.

In dieser Antwort sind ebenso wie im Mastertelegramm ein Startbit, ein Syncbit und ein Master-Slave-Bit enthalten. Darauf folgen als zusätzliche Kennung die Bits A2 bis A0, welche die Adressbits A2 bis A0 des Mastertelegramms als Kopie enthalten. Es folgen vier Datenbits und 16 CRC Bits. Das Antworttelegramm dauert insgesamt 26,04 ms.



4.3 Analyse der Maßnahmen im Datenübertragungsprotokoll der Firma RK TEC zur Erkennung und Behandlung von Kommunikationsfehlern

Gegen folgende Übertragungsfehler sind die angegebenen Maßnahmen zur Fehlerbeherrschung in der Spezifikation vorgesehen:

Wiederholung

In den Modulen erfolgt eine Sendefreigabe nur dann, wenn eine bestimmte Verarbeitungsreihenfolge eingehalten wurde. Nachdem die Nachricht gesendet wurde, wird sie im Modul gelöscht. Neue Telegramme müssen erneut aufgebaut werden.

Verlust

Durch die vorgegebene feste Abfolge des Datenaustausches mit Abfrage der Zentrale und daraufhin zu erfolgender Modulantwort, wird ein Datenverlust erkannt. Bei Telegrammverlust wird die Anfrage wiederholt, bis eine korrekte Antwort erfolgt. Es sind maximal 20 Wiederholungen zugelassen, danach erfolgt von der Zentrale eine Fehlerreaktion.

Einfügung

Das Einfügen von Informationen in ein Telegramm wird durch die CRC-Prüfsumme erkannt. Durch das Master/Slave-Prinzip und ein zusätzliches Zeitfenster wird auch das Einfügen von ganzen Telegrammen in der Zentrale aufgedeckt.

Falsche Abfolge

Die Reihenfolge der Modulanfragen ist ausschließlich durch die Zentrale gesteuert, somit besteht nicht die Möglichkeit das es in der Abfolge zu Vertauschungen kommt. Das Bussystem enthält keine telegrammspeichernden Elemente, wie Repeater oder Router.

Datenverfälschung inkl. Adressdaten

Durch Verwendung einer 16 Bit CRC-Prüfsumme werden Störungen auf dem Übertragungsmedium erkannt.

Nach EN 60870-5-1 kann bei Verwendung einer 16 Bit CRC-Checksumme eine Hamming-Distanz von 6 für Berechnungen verwendet werden. Zusammen mit den typischen Bitfehlerraten für die verwendete Kabelform (< 10 E-2) ergeben sich bei den Berechnungen Restfehlerwahrscheinlichkeiten, welche die Anforderungen der Sicherheitskategorie SIL 2 für Systeme mit niedriger Anforderungsrate erfüllen.

Verzögerung

Die Zentrale steuert als Master den gesamten Busablauf. Alle Module im Bus werden zyklisch angesprochen. Somit sind Überlastungen des Bussystems durch zu viel Datenaustausch nicht möglich.

Kopplung zwischen sicherheitsrelevanten und nicht sicherheitsrelevanten Nachrichten

Es gibt nur sicherheitsrelevante Daten auf dem Bus deshalb keine Kopplung möglich

5. Zusammenfassung

Die Firma RK TEC Rauchklappen-Steuerungssysteme GmbH & Co. KG beabsichtigt in Zukunft, die feste Verdrahtung zur Ansteuerung von Rauchgasklappen durch ein Bussystem zu ersetzen.

Im Rahmen dieser Untersuchung wurde überprüft, inwieweit die Maßnahmen im Datenprotokoll der Firma RK TEC geeignet sind, verschiedene Kommunikationsfehler zu erkennen.

Die Prüfung zeigte, dass das beschriebene Konzept des RK TEC-Datenformates für den Einsatz bis zum Sicherheits-Integritätslevel SIL 2 geeignet ist.

Die Betrachtung der sicherheitsgerichteten **Busteilnehmer** war nicht Gegenstand dieser Konzeptprüfung.

Köln, 2003-03-31
ASI/Kst. 968 ja-nie

Der Sachverständige

Dipl.-Phys. Erich Janoschek