Redundanzen elektrischer Fahrantriebe

Dr.-Ing. Ulrich Horn, SAM Electronics GmbH, Hamburg

Important objectives in design of electrcal propulsion systems are redundancy and independence of propulsion components: Electrical drives, generator sets and switchboard units are each divided in separate groups and placed in at least two separate compartments. This design is nevertheless only good if supported by automation design, field-bus structure and auxiliary components. The problems and the solutions found should be addressed by this report using the example of new double-end ferry „Coastal Reanaissance“.

1 Einleitung

Dieser Beitrag beschäftigt sich mit der Redundanz elektrischer Propulsion am Beispiel der Doppelendfähre „Coastal Renaissance“ und ihrer Schwesterschiffe. Diese Schiffe wurden durch die Flensburger-Schiffbau-Gesellschaft für die kanadische Fährreederei BC Ferries gebaut und von SAM Electronics elektrisch ausgestattet.

Es stellte sich bald heraus, dass es für redundante elektrische Antriebe ein klassisches, erprobtes Konzept gibt. Dieses Konzept spiegelt sich aber nur unzureichend in den konventionellen leittechnischen Systemen wieder.

2 Redundanz und Diversität

Für hochwertige Schiffe (Fähren, Bohrinselversorger, Kreuzfahrtschiffe) wird eine Redundanzklasse vergeben, die eine Aussage darüber macht, wieviel Prozent der Antriebsleistung nach allen denkbaren Schäden noch zur Verfügung stehen. Der Begriff **Redundanz** führt hier in die Irre, weil es im eigentlichen Sinne nicht um die Vorhaltung zusätzlicher, im Normalfall nicht erforderlicher Betriebsmittel geht: Eine Standby-Pumpe ist redundant, da sie wirklich nur im Fall der Störung der arbeitenden Pumpe zum Einsatz kommt. Beim Einsatz der Standby-Pumpe kann weiterhin das volle Betriebsprogramm gefahren werden. **Diversität** läge für die Standby-Pumpe vor, wenn sichergestellt wäre, dass sie auch nicht durch das gleiche Ereignis in Mitleidenschaft gezogen werden kann, wie die arbeitende Pumpe.

Die Antriebstechnik der „Coastal Renaissance“ enthält redundante Elemente, wichtiger ist aber, dass die Betriebsmittel elektrisch und räumlich so angeordnet sind, dass kein denkbarer Schaden zu einem Totalausfall der Antriebsanlage führt. Es werden also räumlich und elektrisch **diversitäre** Strukturen geschaffen.

1 Betrachtung der Antriebstechnik

1.1 Betriebskonzept

Die Fähren werden in einem engen Fahrplan in schwierigem Fahrwasser eingesetzt. Sie besitzen an beiden Enden jeweils einen elektrischen Fahrmotor mit Verstellpropeller, während der normalen Fahrt ist nur einer in

Betrieb. Vor dem Anlegen wird jeweils der in Fahrtrichtung vorn liegende Asynchron-Fahrmotor mit Hilfe eines Drehstromstellers gestartet, so dass zum Manövrieren beide Propeller zur Verfügung stehen. Die elektrische Antriebsleistung wird von vier Dieselgeneratorsätzen aufgebracht. Im Regelbetrieb werden davon drei benutzt, ein eingeschränkter Betrieb ist mit zwei Generatoren möglich, dann kann allerdings nur ein Fahrmotor zur Zeit benutzt werden.

Das 600-V-Bordnetz wird über zwei Transformatoren aus dem 6,6-kV-Netz der Generatoren versorgt. Die Fahrmotoren sind die einzigen Mittelspannungsverbraucher, alle anderen Verbraucher werden aus Niederspannungsanlagen gespeist. Die Niederspannungsverteilungen können während Betriebspausen von Landanschlüssen versorgt werden, in besonderen Fällen ist eine Versorgung des Niederspannungsnetzes durch den Notgenerator möglich. In beiden Fällen erfolgt der Wechsel von der Speisung über Mittelspannungsgenerator und Transformator auf direkte Niederspannungsversorgung ohne Spannungsunterbrechung.

Die Mittelspannungsanlage besteht aus zwei Schalttafeln (PSB 1 und PSB 2), die normalerweise mit geschlossenen Kuppelschaltern betrieben werden, da der Regelbetrieb drei Generatorsätze erfordert.

1.2 Struktur

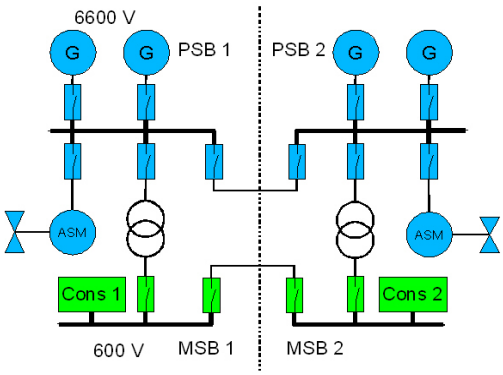

Abb. 1: Elektrische Struktur des Bord- und Fahrnetzes

Es ist möglich, die Kuppelschalter der Niederspannungsschalttafeln gleichzeitig mit den Trafoschaltern und den Kuppelschaltern der Mittelspannungsschalttafeln geschlossen zu betreiben, so dass sich hier ein Ringnetz ergeben kann.

1.3 Ausfallszenarien

Für eine Analyse des Ausfallverhaltens der energietechnischen Komponenten wurden folgende Annahmen getroffen:

- Betrachtung erfolgt raumorientiert
- nur „Elektro“-Räume berücksichtigt
- komplette Räume fallen aus
- alle Komponenten sind dort gestört

Nachzuweisen ist, dass bei jedem denkbaren Schaden (Ausfall eines Raumes) zumindest noch folgende Forderungen erfüllt sind:

- der eingeschränkte Betrieb mit zwei Generatoren bleibt möglich

— mindestens eine Niederspannungsschalttafel (MSB 1 oder MSB 2) kann über Transformator versorgt werden

Es befinden sich jeweils eine Mittelspannungsschalttafel, ein Transformator und ein Fahrmotor in jeweils einem Raum an den Enden des Schiffes. In zwei Räumen dazwischen befinden sich jeweils zwei Generatorsätze und eine Niederspannungsschalttafel.

In der folgenden Abbildung wird der Ausfall eines Fahrmotorraumes dargestellt: Für den Betrieb fällt dadurch ein Fahrmotor aus, ebenso stehen zwei Generatorsätze nicht mehr zur Verfügung, da die zugeordneten Generatorfelder in der Mittelspannungsschalttafel ausfallen. Die obigen Forderungen sind erfüllt.

Gleiches gälte für den anderen Fahrmotorraum.

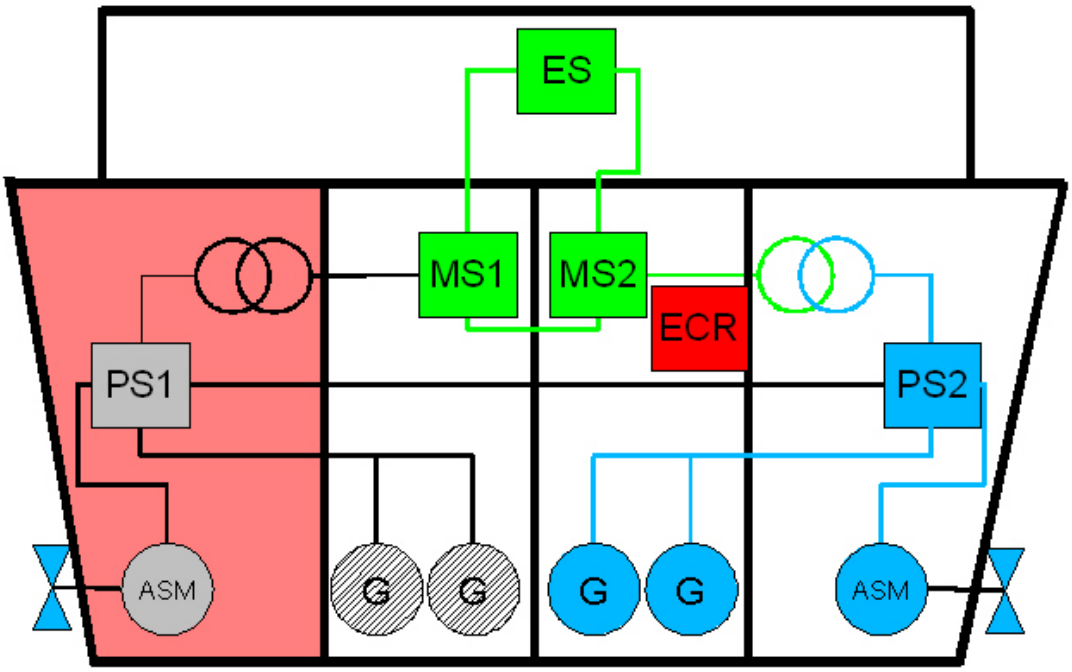

Abb. 2: Räumliche Aufteilung des Fahr- und Bordnetzes

Bei Ausfall eines Generatorraumes würde neben den Generatoren auch eine Niederspannungs-Schalttafel in Mitleidenschaft gezogen, auch hier wären die beiden Forderungen erfüllt. Eine Unsymmetrie ergibt sich durch die Überleitung zur Notschalttafel: Bei Verlust der Niederspannungs-Schalttafel **MS**B **1** könnte das Notnetz nur durch den Notgenerator versorgt werden. Dies würde man bei einem Schiff für die hohe See vermeiden und die Überleitung zur Notschalttafel **ES**B symmetrisch ausbilden, da ein längerer Betrieb des Notgenerators häufig weder möglich noch erwünscht ist. Bei diesen Kurzstrecken-Fähren ist aber ein Betrieb des Notgenerators bis zur Bendigung der Reise unproblematisch.

2 Automation

2.1 Standard-Struktur

Um entsprechende Ausfallszenarien für die Automationsanlage untersuchen zu können, sollen die wesentlichen Komponenten erläutert werden :

— Bedienstationen (**O**perator **W**ork **S**tation), die die Schnittstelle für den Nutzer darstellen und auf die Daten der ...

— Feldrechner (**F**ield **P**rocessing **D**evice) zugreifen, die ihrerseits entweder direkt oder über Feldbusse und in der Anlage verteilte Geräte Signale sammeln und ausgeben

Für die Kommunikation der Bedienstationen und Feldrechner wird in der Regel ein leistungsfähiger Feldbus (Profibus-FMS, Ethernet) verwendet. Auf dieser Ebene ist keine sogenannte „Master-Slave“-Kommunikation möglich, weil sehr vielfältige Kommunikations-Beziehungen existieren. Potentiell kann jede OWS mit jedem Feldrechner ebenso kommunizieren wie auch Feldrechner untereinander! Zwei Forderungen wird man an solche Systeme haben

— Der Datenverkehr der nicht gestörten Geräte darf nicht durch eine einzelne Gerätestörung beeinflusst werden

— Die Funktionen sind so auf die Feldrechner zu verteilen, dass das Schiff bei Ausfall eines Feldrechners weiterhin weitgehend unter der Kontrolle der Bediener an den OWS bleibt und automatische Funktionen möglichst ungestört ablaufen zu lassen

Aus der ersten Forderung folgt unmittelbar die Forderung nach redundanten Buskabeln: Ein gestörter Schnittstellentreiber eines Gerätes kann andernfalls die Kommunikation nicht gestörter Geräte verhindern!

Wir finden also Redundanz in Bezug auf das Buskabel (und die OWS) und Diversität in Bezug auf die Verteilung der Funktionen über die Feldrechner.

2.2 Ausfallszenarien

Diese Struktur ist allerdings ursprünglich für zentrale Leitwarten in der Industrie entwickelt worden, bei denen die OWS und Feldrechner räumlich konzentriert waren. Mit zunehmender räumlicher Verteilung der Feldrechner erwachsen für das Konzept des redundanten Busses neue Risiken:

Zwangsläufig werden die redundanten Buskabel durch verschiedene Feuerzonen eines Schiffes geführt und sind den gleichen Gefahren ausgesetzt. Es ist in Grenzen möglich, die Kabel auf getrennten Wegen zu führen, es ist aber nicht zu vermeiden, dass sich die redundanten Buskabel in allen Räumen begegnen, in denen OWS oder Feldrechner angeordnet sind.

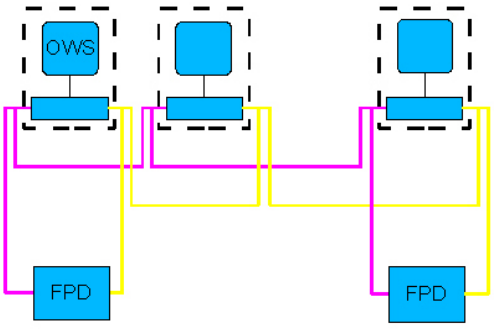

Abb.3: Prinzipieller Aufbau eines Leitsystems mit redundantem Feldbus

Alle leistungsfähigen Feldbusse erfordern den Abschluss der Datenkabel mit Abschlusswiderständen, man kann daher davon ausgehen, dass ein Feldbus sowohl bei Kurzschluss wie auch bei Unterbrechung funktionsunfähig wird. Daher müssen diese Fälle nicht unterschieden werden:

Man kann unterstellen, dass jede äußere Ereignis, das einen Busteilnehmer zerstört, auch zu einem Totalausfall der Kommunikation und damit der gesamten Leittechnik führt.

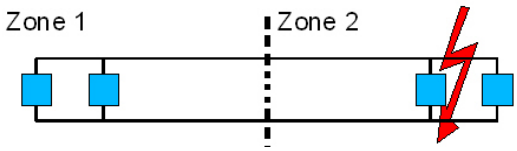

Abb. 4: Ausfall redundanter Bus-Paare durch einen Fehler

Auf den Doppelendfähren wird der Einsatz der Dieselgeneratorsätze durch ein zusätzliches, in den Schalttafeln verteilt angeordnetes Power-Management-System (PMS) bewirkt. Die Kommunikation innerhalb dieses Systems erfolgt durch einen redundanten CAN-Bus, für den prinzipiell die gleiche Problematik wie für den Bus des Leitsystem besteht. Allerdings verschärft durch die Tatsache, dass die Komponenten des PMS naturgemäß direkt in Schalttafeln eingebaut sind.

Aufgrund der oben in Kürze wiedergegebenen Überlegungen wurde der redundante Bus des PMS umgestaltet und in Abschnitte begrenzter Länge zerlegt.

3 Rückwirkungsfreie Kopplung

Die Überlegungen des vorigen Abschnitts zeigen, dass Feldbusse nicht mehrere Feuerzonen oder wasserdichte Abteilungen durchqueren sollten. Wenn ein solcher Abschnitt durch Feuer oder Wasser ausfällt, sind Nachbarabschnitte durch den Ausfall des Feldbusses mit betroffen, obwohl man eine Beeinflussung der Nachbarabschnitte durch schiffbauliche, maschinenbauliche und elektrotechnische Massnahmen verhindern möchte.

Es ist andererseits nicht zu vermeiden, Datenverkehr über Abschnittsgrenzen hinaus zu betreiben, ebenso wie es nicht zu vermeiden ist, dass Gase, Flüssigkeiten und elektrischer Strom eine Abschnittsgrenze passieren. Gesucht wird also das informationstechnische Äquivalent zu Schiebern, Feuertüren und Trennschaltern. Das dafür erforderliche Bauelement bezeichnen wir als Koppler, unabhängig von ggf. unterschiedlichen logischen Funktion im Netzwerk. Koppler sind unverzichtbar, um redundant und diversitär aufgebaute Leitsysteme zu erhalten und müssen folgende Eigenschaften haben:

- mindestens zwei Schnittstellen
- Leitungsunterbrechungen an einer Schnittstelle des Kopplers haben keinen Einfluss auf den Datenverkehr der Leitungen an den nicht betroffenen Schnittstellen
- Kurzschlüsse an einer Schnittstelle des Kopplers haben keinen Einfluss auf den Datenverkehr der Leitungen an den nicht betroffenen Schnittstellen
- besitzt ein Koppler mehr als zwei Schnittstellen, soll der Datenverkehr zwischen den nicht beteiligten Schnittstellen nicht gestört werden, wenn eine Schnittstelle mit einer gestörten Leitung verbunden ist

Es ist dabei unerheblich, ob ein Koppler vollkommen transparent ist und einfach alle Nachrichten von einer Schnittstelle zu allen anderen Schnittstellen überträgt oder ob nur die erforderlichen Nachrichten übertragen werden. In der Informationstechnik unterscheidet man verschiedene Baugruppen dieser Art:

- **Repeater** oder **Hubs** stellen nur eine galvanische Trennung der Busabschnitte her, jedes Signal an einer Schnittstelle taucht mit sehr geringer Latenzzeit an allen anderen Schnittstellen auf. Damit ändert sich das Kollisionsverhalten des Busses nicht, auch fehlerhafte Telegramme werden unverändert weitergegeben. Die Übertragungsraten an allen Schnittstellen sind gleich, weil keine Datenspeicherung erfolgt.
- **Switch** und **Router** werten Adressinformationen aus und leiten Nachrichten nur an die erforderlichen Schnittstellen weiter. Sie besitzen häufig Puffer für Nachrichten und können dadurch Kollisionen vermeiden. Da sie ein Telegramm analysieren müssen, um es korrekt weiterzuleiten, können fehlerhafte Telegramme nicht übertragen werden. In der Regel können sie auch Abschnitte mit unterschiedlichen Datenübertragungsraten verbinden. Ein Switch der Netzwerk-Technik leitet nur die erforderlichen Nachrichten durch, er lernt selbsttätig, welche Teilnehmer an welchen Schnittstellen sitzen.

Für das PMS-Netzwerk wurde als Koppler eine einem Switch entsprechende Technik gewählt in Bezug auf die Verwendung von Puffern, allerdings erfolgt zur Zeit keine Auswertung von Adressinformationen, die Weiterleitung der Nachrichten erfolgt ohne Berücksichtigung der Adressaten an alle Schnittstellen. Bei dem PMS-Netzwerk an Bord der „Coastal Renaissance“ und ihrer Schwesterschiffe handelt es sich um ein redundantes CAN-Netzwerk. Da CAN im wesentlichen mit Broadcast-Nachrichten arbeitet (Nachrichten, die an alle Teilnehmer gerichtet sind), wurde kein Mechanismus zur Filterung implementiert.

Für das CAN-Netzwerk hat die Verwendung von Kopplern verschiedene Folgen:

- im Gegensatz zu einem durchverbundenen Netzwerk erhalten nicht mehr alle Geräte eine Nachricht exakt gleichzeitig
- der Koppler gibt auf allen Schnittstellen für eine eingehenden Nachricht die CAN-spezifische Hardwarequittung, damit können die beteiligten Geräte einen Fehler hinter dem Koppler nicht mehr feststellen. Die Alarmierung eines Bus-Fehlers erfolgt also nur noch für einen Abschnitt zwischen Kopplern.
- Die Laufzeit der Nachrichten erhöht sich um etwa 10 ms
- CAN nutzt einen Mechanismus der Kollisionsbehandlung, bei dem die Nachricht höherer Priorität ohne Verzögerung weiter befördert wird, während die Nachricht niedriger Priorität anschliessend noch einmal gesendet werden muss. Dieser Mechanismus ist im Koppler ausser Funktion, weil die Sendepuffer des Kopplers wie Schieberegister arbeiten und die Nachrichten in der Reihenfolge des Eingangs versenden.

Koppler erhöhen die Diversität des Bussystems nur dann, wenn der Koppler seine Entsprechung in der verteilten Software findet. Der Nutzen eines weiterlaufenden Datenverkehrs auf einem Abschnitt ist nur gering, wenn Informationen aus einem gestörten Abschnitt für eine spezielle Funktion unbedingt benötigt werden.

4 Modifizierte Struktur für BC-Ferries-Doppelendfähren

4.1 Busstruktur des Power-Management-Systems

Durch den Einsatz von Kopplern mit drei oder mehr Schnittstellen verwandeln sich lineare Busse in sternförmige Strukturen, im Falle eines redundanten Busses also in zwei sternförmige Strukturen. Es ist nicht sinnvoll, die beiden Strukturen parallel anzulegen:

Die Koppler und Busverbindungen sind so zu platzieren, dass nicht beide Bus-Strukturen durch ein Schadensereignis ausfallen können. Die Verbindung zwischen zwei beliebigen nicht betroffenen Geräten muss auf mindestens einem System erhalten bleiben.

Auf den BC-Ferries-Fähren werden zwei Koppler mit drei Schnittstellen eingesetzt, diese Sternknoten sind in verschiedenen Räumen (Niederspannungsschalttafeln MS1 und MS2) angeordnet:

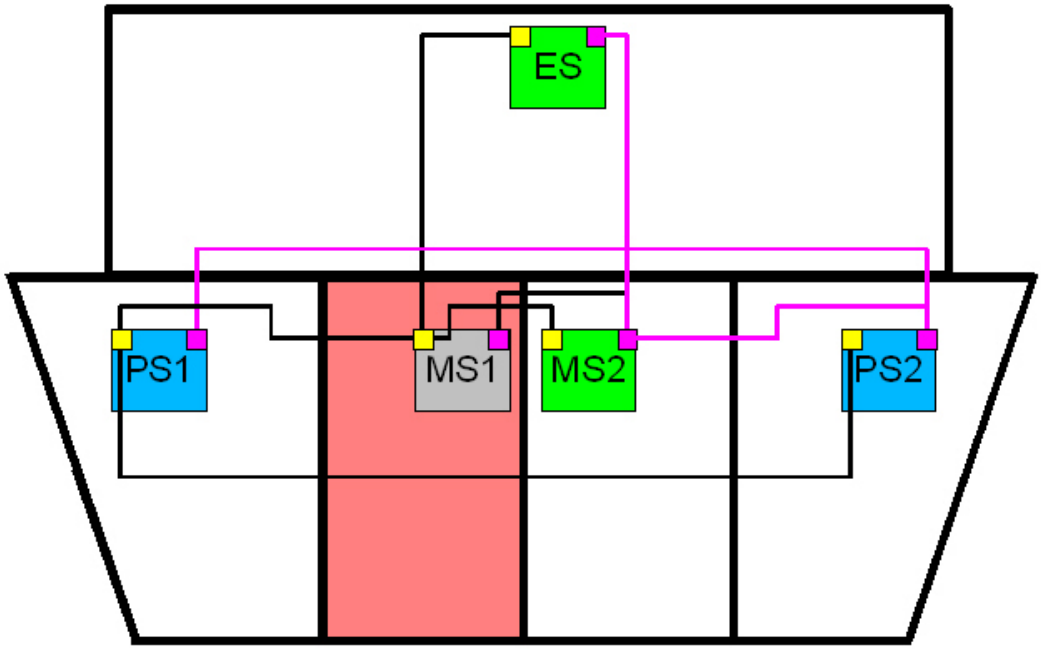

Abb.5: CAN-Bus Anordnung

Es ist zu erkennen, dass bei Zerstörung der Schalttafel MS1 die vier anderen Schalttafeln miteinander mit dem Netz verbunden bleiben, dessen Sternkoppler in MS2 sitzt. Die redundanten Netze sind so aufgebaut, dass bei jedem Fehlerort in einem der redundanten Netze nur ein Endzweig betroffen ist, der keine Verbindung zu weiteren Tafeln herstellt.

Koppler brauchen als aktive Bauelemente eine Spannungsversorgung. Die Spannungsversorgung ist so aufgebaut, dass ein einzelner Fehler nicht die Koppler beider redundanten Bus-Systeme außer Betrieb setzt.

4.2 Softwarestruktur

Die Bus-Struktur sorgt dafür, dass die Kommunikation nicht direkt betroffener Geräte nicht ausfällt. Dies hat aber nur dann Sinn, wenn die Software der nicht betroffenen Geräte mit dem Ausfall der Informationen der betroffenen Geräte zurechtkommt.

Letzlich bedeutet das für alle Informationen, das überlegt werden muss, welche Annahmen beim Ausbleiben der Information getroffen werden muss.

Ein Beispiel aus dem Projekt „BC-Ferries“: Das verteilte PMS-System verfügt über eine Logik für den automatischen Start von Dieselgeneratorsätzen bei Spannungsausfall (sogenannter Blackout-Start). Bei der Versorgung der Niederspannungs-Schalttafeln von einem Landanschluss sind die Mittelspannungs-Schalttafeln spannungsfrei. Damit wäre die Bedingung für einen Blackout-Start der Mittelspannungs-Generatorsätze erfüllt. Um das zu verhindern, wird das Spannungs-Signal der Niederspannungs-Schalttafeln mit in die Blackout-Lgik der Mittelspannungs-Generatorsätze eingebunden.

Damit stellt sich aber die Frage, was passieren soll, wenn die Datenverbindung zwischen Nierderspannungs- und Mittelspannungs-Schalttafel verloren geht? Unter dem Aspekt der Sicherheit im Seebetrieb ist die einzige sinnvolle Aktion des verteilten PMS dann, einen Mittelspannungsgenerator zu starten, um die Versorgung von dort aufzubauen. Das bedeuetet, daß ein fehlendes Spannungssignal im Sinne fehlender Spannung interpretiert werden muss. Entsprechende Entscheidungen müssen für verschiedene Signale vorgenommen werden.

Die Erstellung von verteilten Systemen, die mit dem Ausbleiben von Daten zurechtkommen und den Verlust

eines Teil-Sytems verkraften können, ist eine komplexe Aufgabe.

5 Zusammenfassung

Die automatischen Abläufe, Fernsteuerung und Fernüberwachung eines Schiffes sind bei Störungen, die über Gerätefehler hinausgehen, nicht gesichert. Auch bei Schiffen mit redundanter Propulsionsanlage werden diese Mechanismen zusammenbrechen. Durch Umschalten vom automatischen, ferngesteuerten Betrieb auf einen manuellen Betrieb vor Ort kann die Besatzung das Schiff weiter betreiben.

Aus diesem Grund ist bisher die weitere Funktion des Leitsystems im Falle massiver Störungen wie Feuer und Wassereinbruch bisher nicht besonders behandelt worden. Es scheint aber nicht mehr zeitgemäß, zahlenmäßig geschrumpfte und tendenziell weniger qualifizierte Besatzungen gerade in kritischen Momenten der gewohnten automatischen Mechanismen zu berauben.

Redundanz und Diversität in der Propulsion muss daher heute auf verschiedenen Ebenen erreicht werden:

- energietechnische Struktur
- Feldbus-Struktur
- Software-Struktur

Im Rahmen dieses Berichtes wurde eine Lösung vorgestellt, die die Erhaltung automatischer Funktionen bei schweren Störungen sicherstellt.

Nach erfolgreicher Umsetzung des Konzeptes bleiben weitere Aufgaben:

- Diagnose der Koppler via Bus
- Spannungsversorgung Koppler (redundant) überwachen
- Lichtwellenleiter-Strecken zwischen entfernten Kopplern
- Tunnelung von CAN via Ethernet (Plattformbus)
- Priorisierung in Kopplern