MSS54
Modulbeschreibung

Arbeitsversion
Egas Sicherheitskonzept
(vorläufig)

	Abteilung	Datum	Name	Filename
Bearbeiter	EE-221	5.12.03		3.05

1. ALLGEMEINES 4

2. SICHERHEITSKONZEPT HARDWARE 4

3. SICHERHEITSKONZEPT SOFTWARE 4

4. PWG-NOTLAUFPROGRAMME 6

4.1. STUFE A - PWG-NOTFAHREN MIT EINEM PWG-SENSOR 6
4.2. STUFE B - PWG-NOTFAHREN OHNE PWG-SENSOR 6

5. EGAS-NOTLAUFPROGRAMME 7

5.1. STUFE 1 - DK-NOTFAHREN MIT EINEM DK-SENSOR 7
5.2. STUFE 2 - NOTFAHREN ÜBER LEERLAUFSTELLER SYSTEM 7
5.3. STUFE 3 - NOTFAHREN ÜBER LEERLAUFSTELLERSYSTEM MIT OFFENEN DROSSELKLAPPEN 8
5.4. STUFE 4 - NOTFAHREN ÜBER LEERLAUFSTELLERSYSTEM AUFGRUND EINES STEUERGERÄTE INTERNEN FEHLERS 9

6. ÜBERGÄNGE IN DIE NOTLAUFPROGRAMME 10

6.1. ÜBERGANG NACH STUFE A - PWG NOTFAHREN MIT EINEM PWG-SENSOR 10
6.2. ÜBERGANG NACH STUFE B - PWG NOTFAHREN OHNE PWG-SENSOR 10
6.3. ÜBERGANG NACH STUFE 1 - DK NOTFAHREN MIT EINEM DK-SENSOR 10
6.4. ÜBERGANG NACH STUFE 2 - NOTFAHREN ÜBER LEERLAUFSTELLER SYSTEM 10
6.5. ÜBERGANG NACH STUFE 3 - NOTFAHREN MIT OFFENEN DROSSELKLAPPEN 11
6.6. ÜBERGANG NACH STUFE 4 - NOTFAHREN MIT SG-INTERNEM FEHLER 11

7. REALISIERUNG NOTLAUFPROGRAMME 12

7.1. BEGRENZUNG INDIZIERTES MOTORMOMENT 12
7.2. MOMENTENREDUKTION ÜBER ZÜNDWINKELEINGRIFF 12
7.3. MOMENTENREDUKTION ÜBER EINSPRITZAUSBLENDUNGEN 12
7.4. BEGRENZUNG DER FAHRZEUGGESCHWINDIGKEIT 12
7.5. BEGRENZUNG DER FAHRZEUGBESCHLEUNIGUNG 12
7.6. BEGRENZUNG DER MOTORDREHZAHL 13
7.7. BEGRENZUNG DER EGAS STELLMOTORDYNAMIK 13
7.8. ABSCHALTEN DES EGAS STELLMOTORS 13

8. ÜBERWACHUNG SENSORIK / EINGÄNGE 14

8.1. ANALOGE SIGNALE 14
8.1.1. Bordnetzspannung Klemme 87 (Hauptrelais) 14
8.1.2. Sensorversorgung 14
8.1.3. Pedalwertgeber 15
8.1.4. HFM-Signal 16
8.1.5. Drosselklappen Potentiometer 17
8.1.6. Kühlwassertemperatur (Motortemperatur) 19
8.1.7. Öltemperatur 19
8.1.8. Ansauglufttemperatur 19
8.1.9. Umgebungsdruck 20
8.2. DIGITALE SIGNALE 20
8.2.1. Schalter Bremslicht 20
8.2.2. Schalter Kraftschluß 20
8.3. SERIELLE SCHNITTSTELLEN 21
8.3.1. CAN 21

8.3.2. MFL *23*

9. ÜBERWACHUNG AKTUATORIK / AUSGÄNGE **24**

9.1. STELLEINHEIT (H-BRÜCKE, STELLMOTOR, DK-MEACHNIK) 24
9.1.1. Elektrische Treiberdiagnose *24*
9.1.2. Soll-/Istvergleich Egas-Position *24*
9.2. LEERLAUFSTELLER 28

10. ÜBERWACHUNG STEUERGERÄTE HARDWARE **29**

10.1. PRE DRIVE CHECK STEUERGERÄT 29
10.1.1. Speichertests *29*
10.1.2. Prozessor Synchronisation *29*
10.1.3. Pre Drive Check Egas-Stelleinheit *30*
10.2. ÜBERWACHUNG STEUERGERÄT IM LAUFENDEN BETRIEB 32
10.2.1. Speichertests *32*
10.2.2. Überwachung HW-Initialisierung *32*
10.2.3. Prozessor Kommunikation *33*
10.2.4. Programmablaufkontrolle *33*
10.2.5. Reset Überwachung *34*
10.3. ÜBERWACHUNG STEUERGERÄT IN DER NACHLAUFPHASE 34
10.3.1. Speichertests *34*

11. LOGISCHE ÜBERWACHUNGEN FUNKTIONSRECHNER **35**

11.1. ABSICHERUNG MOMENTENBERECHNUNG 35
11.2. ÜBERWACHUNG SOLLMOMENT ZU ISTMOMENT 35
11.2.1. Überwachung Soll-/Istmoment über gesamten Betriebsbereich *36*
11.2.2. Überwachung Soll-/Istmoment bei PWG-Vorgabe = 0 ..... *36*

12. LOGISCHE ÜBERWACHUNGEN SICHERHEITSRECHNER **37**

12.1. ÜBERWACHUNG ADC FUNKTIONSRECHNER 37
12.2. ÜBERWACHUNG RECHNERKERN 37
12.3. ÜBERWACHUNG FGR-ABSCHALTUNG 38

1. ALLGEMEINES

2. SICHERHEITSKONZEPT HARDWARE

Das Design der Steuergeräte Hardware wurde speziell auf die Belange eines sicherheitskritischen Egas-Systems hin ausgerichtet. Es weist eine Reihe von Merkmalen auf, die eine lückenlose Überwachung und einen sicheren Fail Save des Egas-Systems gewährleisten.

Kurzübersicht der Designmerkmale

Zwei Prozessor System mit zwei gleichwertigen, leistungsfähigen 32-Bit Prozessoren

mit Ausnahme der Spannungsversorgung, vollkommen unabhängige Prozessoren mit eigener Taktversorgung und Programm-/Datenspeichern

Einsatz eines Spannungsreglers mit Resetauslösung bei Unterspannung

Aufteilung der Funktionalität unter der Prämisse, daß jeder Prozessor eine autarke Eingriffsmöglichkeit in die Momentenabgabe des Motor hat.

Funktionsrechner:	Egas-System, Leerlaufstellersystem, Zündung
Sicherheitsrechner:	Einspritzung incl. Drehzahlbegrenzung

Einsatz einer H-Brücke zur Ansteuerung des Egas-Stellmotors mit zwei Abschaltpfaden, wobei je ein Abschaltpfad von einem Prozessor kontrolliert wird.

Redundante Aufteilung des Bremslichtschalters an beide Prozessoren

Redundante Aufteilung der beiden Analogsignale Pedalwertgeber 1 und Drosselklappengeber 1 an beide Prozessoren

Verwendung eines Pedalwertgebers mit zwei Potentiometern PWG1 und PWG2 mit unabhängiger Spannungsversorgung und unterschiedlicher Kennlinie.

Verbau zweier Drosselklappengeber mit unabhängiger Spannungsversorung und gekreuzter Kennlinie.

Zweifache 5V-Sensorversorgung. Rücklesen der Versorgungsspannung innerhalb der DME

Anschluß der Resetleitung eines Prozessors an einen Portpin des anderen Prozessors. Portpin wahlweise als Interrupteingang oder Ausgang konfigurierbar

3. SICHERHEITSKONZEPT SOFTWARE

Um einen sicheren Egas-Betrieb gewährleisten zu können, sind in der MSS54 eine Reihe von Softwaremodulen implementiert, die alle möglichen SG-externen (Sensorik, Aktorik, Kabelbaum) als auch SG-internen (Prozessor, Speicher, Treiber, Spannungsversorgung) Fehler erkennen und das System in einen Fail Save Zustand überführen sollen.

Die Überwachungsmodule lassen sich dabei in drei Ebenen aufteilen:

Ebene 1:	Überwachung der SG-Peripherie (Sensorik bzw. Aktorik)
Ebene 2:	Überwachung der Regelkreise, Sollwertvorgaben Plausibilisierung zueinander redundanter Informationen
Ebene 3:	Überwachung der Steuergeräte-Hardware und des ordnungsgemäßen Programmablaufs

Die Überwachungsmodule der Ebene 3 sind auf beiden Prozessoren implementiert und laufen unabhängig voneinander, sodaß ein Ausfall einer Rechnereinheit kein Risiko darstellt, da das parallel laufende Überwachungsmodul noch einwandfrei arbeitet.

Kurzübersicht der Überwachungsmodule:

Sensorik:
- Sensorversorgung Uext : Bereichsüberwachung
- Pedalwerterfassung pwg : Bereichsüberwachung, Kanalvergleich
- Drosselklappenposition wdk : Bereichsüberwachung, Kanalvergleich
- HFM-Lastsignal ml : Bereichsüberwachung
- Bremslichtschaltersystem : Kanalvergleich

Aktorik:
- Leerlaufsteller : elektrische Treiberdiagnose
- Egas-Stellmotor : elektrische Treiberdiagnose

Vergleichstests:
- Soll-/Istvergleich der Drosselklappenposition
- Plausibilisierung Fahrerwunschmoment zu Motor-Istmoment
- Plausibilisierung Lastsignal zu Drosselklappenposition (nur bei Ausfall eines DK-Potis)

Bereichsüberwachungen:
- Plausibilsierung der Momentenberechnung inclusive momentenerhöhender Eingriffe
- Überwachung DK-Postion bei Nullmomentenvorgabe
- Überwachung FGR-Abschaltung bei betätigter Bremse

Schnittstellenüberwachungen:
- CAN-Schnittstelle - Bus Fehler, Telegramm Timeout
- DSC-Eingriffe - Überprüfung der Signalredundanz
- MFL-Schnittstelle - Timeout, Telegrammformat, Tastencodierung

Überwachungen SG-Hardware:
- QADC : Ergebnisvergleich Funktions- und Sicherungsrechner
- Speichertests
- Testaufgaben für CPU-Überwachung

Testabläufe / Systemtests
- Pre Drive Check Egas-System
- Programmablaufkontrolle
- Resetüberwachung
- Kommunikationsüberwachung Funktions- / Sicherungsrechner

4. PWG-NOTLAUFPROGRAMME

4.1. STUFE A - PWG-NOTFAHREN MIT EINEM PWG-SENSOR

Kennzeichnung des Notlaufprogramms:
Zweifelsfrei detektierter Ausfall eines Pedalwertgebers und somit Verlust der Redundanz.

Voraussetzung für PWG-Betrieb in Stufe A:
Verbleibender Pedalwertgeber ist plausibel.
Bremsschaltersystem ist fehlerfrei
keine steuergeräte-internen Fehler

Notlaufprogramm:
- Umschaltung der Pedalwert-Progressionskennlinien auf eine Notlauf-Progressionskennlinie wird.
- Begrenzung der positiven PWG-Dynamik durch Notlauffilterung der Sollwertes - langsame Aufwärtsfilterung + schnelle Abwärtsfilterung
- Sicherheitsabschaltung über Bremslichtschalter
  sobald die Bremse betätigt wird, wird ein Pedalwert von Null ausgegeben. Ein erneuter Pedalwert ungleich Null wird erst dann wieder akzeptiert, wenn der verbleibende Pedalwertgeber zwischenzeitlich auf den Wert Null zurückgegangen ist.

Anmerkungen:
- Der Tempomatbetrieb ist weiterhin uneingeschränkt möglich.

4.2. STUFE B - PWG-NOTFAHREN OHNE PWG-SENSOR

Kennzeichnung des Notlaufprogramms:
Ausfall beider Pedalwertgeber - ein Fahrerwunsch ist somit nicht mehr erfaßbar.

Voraussetzung für PWG-Betrieb in Stufe A:
keine sg-internen Fehler

Notlaufprogramm:
- Fahrerwunsch stets gleich Null
- Fahren mit Leerlaufdrehzahl

Anmerkungen:
- Der Tempomatbetrieb ist weiterhin uneingeschränkt möglich, falls die Mindestgeschwindigkeit für den FGR-Betrieb erreicht werden kann.

5. EGAS-NOTLAUFPROGRAMME

5.1. STUFE 1 - DK-NOTFAHREN MIT EINEM DK-SENSOR

Kennzeichnung des Notlaufprogramms:
Zweifelsfrei detektierter Ausfall eines Drosselklappengebers und somit Verlust der Redundanz, bzw. zueinander unplausible DK-Werte der beiden Geber ohne den defekten Geber erkannt zu haben. In diesem Fall verwendet die Egas-Lageregelung den größeren und damit unkritischeren Wert als Istposition der Drosselklappe, bis über die HFM Plausibilisierung der fehlerhafte Geber detektiert werden kann.

Voraussetzung für DK-Betrieb in Stufe 1:
Verbleibender Drosselklappegeber ist plausibel.
HFM arbeitet fehlerfrei.
Plausibilisierung verbleibender DK-Wert zu HFM-Lastsignal in Ordnung
keine steuergeräte-internen Fehler

Notlaufprogramm:
- Begrenzung des Tastverhältnisses für Egas-Stellmotor - Begrenzung der Motordynamik
- Begrenzung des maximalen Motormoments
- Plausibilsierung verbleibendes Poti über HFM-Lastsignal
- Sperren der interenen füllungserhöhenden Eingriffe wie Katheizen, Momentenreserve
- Begrenzen der Fahrzeugbeschleunigung
- Begrenzen der Maximalgeschwindigkeit

Anmerkungen:

5.2. STUFE 2 - NOTFAHREN ÜBER LEERLAUFSTELLER SYSTEM

Kennzeichnung des Notlaufprogramms:
Die Sollposition der Drosselklappe kann nicht mehr zuverlässig eingeregelt werden, weil
- die Istposition aufgrund eines Doppelfehlers (DK1, DK2, HFM) bzw. Ausfall der Sensorversorgung nicht mehr erfaßbar ist
- das Stellglied (Treiber, Leitung, Stellmotor, DK-Mechanik) ausgefallen ist
- ein Problem in der Drosselklappenkinematik vorliegt

Voraussetzung für Notbetrieb in Stufe 2:
mindestens noch ein Lastsignal verfügbar (HFM oder eine verlässliche Drosselklappenposition)
keine steuergeräte-internen Fehler

Notlaufprogramm:
- Abschalten der Stellmotoransteuerung und Überwachung, ob Drosselklappen geschlossen sind.
- Begrenzung des maximalen Motormoments
- Sperren der interenen füllungserhöhenden Eingriffe wie Katheizen, Momentenreserve
- Herabsetzen der Drehzahlbegrenzung
- Begrenzen der Fahrzeugbeschleunigung
- Begrenzen der Maximalgeschwindigkeit

Anmerkungen:

5.3. STUFE 3 - NOTFAHREN ÜBER LEERLAUFSTELLERSYSTEM MIT OFFENEN DROSSELKLAPPEN

Kennzeichnung des Notlaufprogramms:
Die Luftzufuhr des Motors kann nicht mehr direkt kontrolliert werden, da zum Beispiel die Drosselklappen in einem geöffneten Zustand festklemmen. Das Fahrerwunschmoment, bzw. die Motordrehzahl muß somit über Zündung und Einspritzung auf ein gewünschtes Maß reduziert werden.

In der Regel kann in diesem Betrieb davon ausgegangen werden, daß ein Defekt in der Ansteuerung der Drosselklappen vorliegt, die Istpositionen aber noch erfaßbar sind.

Voraussetzung für Notbetrieb in Stufe 3:
kein SG-interner Fehler

Notlaufprogramm:
- Abschalten der Stellmotoransteuerung.
- Begrenzung des maximalen Motormoments
- Freischalten der Zündwinkeleingriffe Momentenmanager (Eingriff wird aktiv, wenn Motor-Istmoment überhalb Wunschmoment liegt).
- Freischalten der Einspritzausblendungen Momentenmanager (Eingriff wird aktiv, wenn Motor-Istmoment überhalb Fahrerwunschmoment + max. erlaubtes Delta liegt)
- Sperren der interenen füllungserhöhenden Eingriffe wie Katheizen, Momentenreserve
- Herabsetzen der Drehzahlbegrenzung
- Begrenzen der Fahrzeugbeschleunigung
- Begrenzen der Maximalgeschwindigkeit

Anmerkungen:
Dieses Notprogramm stellt den Worst-Case“ im Egas-Betrieb dar. Der Motor erzeugt mehr Moment als es der Fahrer wünscht und das Fahrzeug könnte ungewollt beschleunigen. Da allerdings auch ein Abstellen des Motors als äußerst sicherheitskritisch erachtet wird, soll über dieses Notprogramm noch ein stark eingeschränkter, aber dennoch beherrschbarer Motorbetrieb aufrecht erhalten werden.

5.4. STUFE 4 - NOTFAHREN ÜBER LEERLAUFSTELLERSYSTEM AUFGRUND EINES STEUERGERÄTE INTERNEN FEHLERS

Kennzeichnung des Notlaufprogramms:
Eine der Überwachungsfunktionen des Steuergerätes hat einen Fehler innerhalb der DME detektiert, durch den eine ordnungsgemäße Abarbeitung der Programm nicht mehr sicher garantiert werden kann. Da in diesem Fall die Auswirkungen des Fehlers nicht vorhersehbar sind, werden eine Reihe von parallelen und voneinander unabhängigen Maßnahmen ergriffen, die gewährleisten, daß durch diesen Fehler das Fahrzeug nicht ungewollt stark beschleunigen kann.

Voraussetzung für Notbetrieb in Stufe 4:

Notlaufprogramm:
- Abschalten der Stellmotoransteuerung.
- Begrenzung des maximalen Motormoments
- Freischalten der Zündwinkeleingriffe Momentenmanager
- Freischalten der Einspritzausblendungen Momentenmanager
- Sperren der interenen füllungserhöhenden Eingriffe wie Katheizen, Momentenreserve
- Herabsetzen der Drehzahlbegrenzung
- Begrenzen der Fahrzeugbeschleunigung
- Begrenzen der Maximalgeschwindigkeit

Anmerkungen:
Durch den Aufbau der DME als Zweiprozessorsystem und der Aufteilung von Luftzufuhr und Kraftstoffzufuhr auf jeweils einen Prozessor, ist die DME in der Lage, auch bei einem gravierenden internen Problem noch einen sicheren Notlaufbetrieb zu gewährleisten. Jeder Prozessor ist dabei in der Lage, unabhängig von der Funktionsfähigkeit des anderen Prozessors, das erzeugte Motormoment zu kontrollieren.
Die Fahrbarkeit des Notprogramms hängt allerdings sehr stark davon ab, in wie weit die für den Motorbetrieb benötigten Funktionen wie Lasterfassung, Zündung, Einspritzung, etc noch fehlerfrei ablaufen können.

6. ÜBERGÄNGE IN DIE NOTLAUFPROGRAMME

Im Rahmen des Egas-Sicherheitskonzepts liegt ein besonderer Schwerpunkt in den Übergängen in die entsprechenden Notlaufprogramme. Denn während ein Notlaufprogramm durch geeignete Gegenmaßnahmen beherrschbar erscheint, ist dies bei den Übergängen immer von der gerade aktuellen Fahrsituation abhängig. Diese ist aber der Steuerung meist nicht bekannt.

Als besonders kritisch wird hierbei das Abschalten des Motors bzw. eine plötzliche Leistungsreduktion des Motors erachtet, da dies eventuell erst einen sicherheitskritischen Fahrzustand provoziert. Stichpunkte dazu sind: Überholen bei Gegenverkehr, Fahren im Grenzbereich mit abrupten Lastwechselreaktionen, Verlust der Lenkkraft- und Bremskraftunterstützung.

Deshalb wird im Rahmen des Sicherheitskonzepts versucht, in bestmöglichem Umfang den Fahrzustand sowie die Fahrerreaktionen zu beurteilen und damit einen langsameren, vom Fahrer noch beherrschbaren Übergang in das Notlaufprogramm zu erreichen.

Dies ist allerdings nur soweit möglich, wie es die Technik erlaubt.

6.1. ÜBERGANG NACH STUFE A - PWG NOTFAHREN MIT EINEM PWG-SENSOR

Mit dem Übergang in die Stufe A wird auf eine PWG-Notlaufprogressionskennlinie umgeschaltet, welche einen Sprung auf eine kleinere PWG-Sollwertvorgabe und somit einen Lastsprung zur Folge haben kann.

Dieser negative Pedalwertsprung wird deshalb nicht direkt zum Momentenmanager weitergeleitet, sondern das Delta (aktueller Wert - Zielwert) rampenförmig abgeregelt. Änderungen des Fahres werden sofort und ungefiltert weitergegen. Betätigt während der Abregelzeit der Fahrer die Bremse oder die Kupplung, wird sofort der Pedalwert Null ausgegeben.

6.2. ÜBERGANG NACH STUFE B - PWG NOTFAHREN OHNE PWG-SENSOR

Der Übergang in die Stufe B erfolgt analog dem Übergang in die Stufe A.

6.3. ÜBERGANG NACH STUFE 1 - DK NOTFAHREN MIT EINEM DK-SENSOR

Das Notprogramm Stufe 1 beinhaltet eine Drehmomentenbegrenzung und eine Begrenzung des Egas-Sollwertes. Auch hier soll es nicht zu plötzlichen Drehmomentensprüngen des Motor kommen, sondern das Motormoment in einem für den Fahrer beherrschbaren und einschätzbaren Gradienten auf die neuen Sollwerte reduziert werden.

Dazu wird, ähnlich wie bei Stufe A, das Maximalmoment, ausgehend vom aktuellen Motormoment rampenförmig auf das Maximalmoment der Notlaufstufe reduziert.

6.4. ÜBERGANG NACH STUFE 2 - NOTFAHREN ÜBER LEERLAUFSTELLER SYSTEM

Der Übergang in das Notprogramm Stufe 2 ist sehr stark von der Art des Fehlers abhängig. Liegt zum Beispiel ein Defekt in der Stellmotoransteuerung vor, so werden die Drosselklappen automatisch über Federn geschlossen ohne daß die DME darauf einen Einfluß hätte.

Bei zueinander unplausiblen Signalen der DK-Geber 1 und 2, bei welchen aber nicht zweifelsfrei der fehlerhafte Sensor bestimmt werden kann, ist unter Umständen ebenfalls ein sofortiges Abschalten des Stellmotors erforderlich.

In den Fällen, in denen man noch über eine Rückmeldung der Istposition verfügt und die Sollposition noch einregeln kann, erfolgt das Schließen der Drosselklappen nicht abrupt, sondern wiederum über eine rampenförmige Abregelung (sofern es der Fahrer nicht anders wünscht). Dazu wird ausgehend von dem Istmoment des Motors das Sollmoment solange reduziert, bis die Sollpositionsvorgabe für die Drosselklappen den Wert Null erreicht. Anschließend wird der Stellmotor abgeschaltet und die Drehzahl- und Geschwindigkeitsbegrenzung aktiviert.

6.5. Übergang nach Stufe 3 - Notfahren mit offenen Drosselklappen

Das Notlaufprogramm der Stufe 3 wird aktiv, wenn die DK-Istposition für einen definierten Zeitraum die DK-Sollposition übersteigt und die Drosselklappen trotz Bestromen des Stellmotors in Richtung Schließen nicht geschlossen werden konnten.
Da dieser Fall zu einer ungewollten Fz-Beschleunigung führen kann, ist die Reaktionszeit der DME auf diesen Fehler relativ kurz. So werden nach Ablauf einer Filterzeit von K_EDKSI_T_BL_AUF_R die Momenteneingriffe über Zündung und Einspritzung zur Reduktion des überschüssigen Motormoments freigegeben. Ist der Fehlerzustand auch nach Ablauf der Filterzeit K_EDKSI_T_BL_AUF_F noch immer vorhanden, wechselt das Egas-System in die Notprogrammstufe 3.

In dieser Stufe wird analog zu den anderen Übergängen trotzdem versucht, das Motormoment rampenförmig abzuregeln und anschließend die Egas-Stellbrücke abgeschaltet. Das aus dem Lastsignal abgeleitete Motoristmoment wird mittels Teilfeuerung und ZW-Spätverstellung auf das Fahrerwunschmoment grob eingeregelt.

Ein Fahrbetrieb - insbesonders bei Nullmomentenvorgabe des Fahrers und bei aufgetrenntem Kraftschluss - hängt stark von der Istposition der Drosselklappen ab und kann nicht gewährleistet werden.

6.6. Übergang nach Stufe 4 - Notfahren mit SG-internem Fehler

Das Notlaufprogramm der Stufe 4 wird immer dann aktiv, wenn ein steuergeräte-interner Fehler erkannt wurde. Da in diesen Fällen das Fehlverhalten des Egas-Systems nicht exakt vorhersehbar ist, wird die Motorleistung über redundante Maßnahmen auf ein sicheres Minimum reduziert.

So wird der Treiber des Stellmotors von beiden Prozessoren über voneinander unabhängige Enable-Leitungen hardwaremäßig abgeschaltet. Der Funktionsrechner (Masterprozessor) verfügt mit der Zündung und der Füllungsregelung über zwei Eingriffsmöglichkeit in die Momentenabgabe des Motors. Dem Überwachungsprozessor steht mit der Einspritzung (Teilfeuerung bzw. Komplettabschaltung) ebenfalls eine wirkungsvolle Eingriffsmöglichkeit zur Verfügung.

7. REALISIERUNG NOTLAUFPROGRAMME

7.1. BEGRENZUNG INDIZIERTES MOTORMOMENT

In den Notlaufprogrammen der Stufe 1 - 4 wird das Fahrerwunschmoment auf den Wert KL_MD_MAX_SK (x-Achse = Nr. des Notlaufprogramms) beschränkt. Eine Übergangsfunktion sorgt dafür, daß die Begrenzung nicht schlagartig wirkt, was ebenfalls einen sicherheitskritischen Fahrzustand hervorrufen kann, sondern ausgehend vom aktuellen Fahrerwunsch, dieser auf den neuen Zielwert mit der Rampe KL_MD_GRAD_SK abgeregelt wird. Die Abregelung ist beendet, bzw. wird abgebrochen, wenn der Zielwert erreicht ist, der Fahrer bremst oder das DSC eingreift. Sinkt dagegen der Fahrerwunsch unter den Begrenzungswert, wird diese nicht abgebrochen, sondern läuft im Hintergrund weiter, um den Fahrer ein kurzes Lupfen bzw. Schalten zu erlauben.

7.2. MOMENTENREDUKTION ÜBER ZÜNDWINKELEINGRIFF

Mit dem Auftreten eines Egas-Notprogramms der Stufen 3 oder 4 wird der Zündwinkeleingriffspfad des Momentenmanagers freigegeben. Dieser errechnet sich aus der vom HFM gemessenen relativen Füllung und der aktuellen Motordrehzahl das momentane indizierte Moment, welches der Motor am aktuellen Betriebspunkt mit seinen Grundzündwinkeln abgibt. Unterschreitet das Fahrerwunschmoment das aktuelle Motormoment, wird der Momentenüberschuß durch eine Spätziehen der Zündwinkel kompensiert. Maximal ist ein Spätziehung bis zu den definierten Minimalzündwinkeln tz_min möglich, womit sich eine Momentenreduktion von bis zu 40% ergeben kann.

7.3. MOMENTENREDUKTION ÜBER EINSPRITZAUSBLENDUNGEN

In den Notprogrammstufen 3 und 4 wird parallel zu dem Zündwinkeleingriff auch ein Momenteneingriff über die Einspritzung freigegen. Aufgabe dieses Eingriffs ist es, einen Momentenüberschuß, welcher durch die ZW-Spätziehung nicht komplett ausgeglichen werden kann, über eine Teilfeuerung der Zylinder zu kompensieren.
Dazu wird das mittels ZW-Spätverstellung darstellbare minimale Istmoment des Motors, berechnet aus einem Drehzahl-Last-Kennfeld und dem minimalen ZW-Wirkungsgrad, in Verhältnis mit dem Fahrerwunschmoment nach Berücksichtigung aller Momenteneingriffe gesetzt. Unterschreitet das Verhältnis den Wert Eins (md_sk_soll / md_sk_ist), werden über die Einspritzung einzelne Zylinder abgeschaltet und somit die Momentenabgabe des Motors in Schritten von 1/Zylinderanzahl reduziert. Das noch verbleibende Überschußmoment kann dann wieder mittels des ZW-Eingriffs reduziert werden.

Die Berechnung und die Ausführung der Teilfeuerung obliegt dem Slaveprozessor und ist bis auf die Berechnung des Istmoments unabhängig vom Funktionsrechner.

7.4. BEGRENZUNG DER FAHRZEUGGESCHWINDIGKEIT

implementiert, aber noch nicht dokumentiert

7.5. BEGRENZUNG DER FAHRZEUGBESCHLEUNIGUNG

Befindet sich das Egas-System in einem Notprogramm der Stufen 1- 4, wird die maximale Längsbeschleunigung des Fahrzeuges auf einen für diese Stufe definierten Wert begrenzt. Die aktuelle Längsbeschleunigung wird dabei vom DSC berechnet und der Motorsteuerung über CAN übermittelt.

Die Beschleunigungsbegrenzung ist als PI-Regler aufgebaut. Der P-Anteil berechnet sich aus der Kennlinie KL_MD_SK_AX_P = f(delta_ax) und wird noch über die gangabhängige Kennlinie KL_MD_SK_AX_GANG gewichtet. Die Schrittweite des I-Reglers berechnet sich aus der Kennlinie KL_MD_SK_AX_IPOS = f (delta_ax). Unterschreitet die Fz-Beschleunigung wieder den zulässigen Maximalwert, wird der I-Anteil über die Kennlinie KL_MD_SK_AX_INEG auf Null abgeregelt.

7.6. Begrenzung der Motordrehzahl

Eine weitere Sicherungsmaßnahme besteht in einem Herabsetzen der Drehzahlbegrenzung. Dazu ist in der Kennlinie KL_N_MAX_SK für jede Notprogrammstufe eine Maximaldrehzahl definiert. Überschreitet die Motordrehzahl diesen Grenzwert, werden über die Einspritzung sofort alle Zylinder abgeschaltet.

Dieser Sicherungsmechanismus läuft ebenfalls auf dem Slaveprozessor und ist komplett unabhängig vom Funktionsrechner, da der Prozessor auch über eine eigene Drehzahlerfasssung verfügt.

7.7. Begrenzung der Egas Stellmotordynamik

Diese Maßnahme wirkt eigentlich nur in dem Notprogramm 1, da in allen anderen Notprogrammen die Ansteuerung des Stellmotors abgeschaltet ist. Sie soll über eine Reduzierung des maximalen Ansteuer-Tastverhältnisses die Dynamik des Stellmotors begrenzen und damit eine einfachere Plausibilisierung des DK-Potis über das HFM-Lastsignal ermöglichen.

7.8. Abschalten des Egas Stellmotors

Die Abschaltung des Egas Stellmotors erfolgt parallel über drei Abschaltpfade.

- feste Sollwertvorgabe = Null für Egas-Lageregler
- Deaktivieren der Enable-Leitung des Funktionsrechners für die H-Brücke
- Deaktivieren der Enable-Leitung der Überwachungsrechners für die H-Brücke

Die Wirksamkeit der Abschaltung wird über das HFM-Lastsignal überwacht, in dem die gemessenen Luftmasse einen Grenzwert, welcher oberhalb der über das Leerlaufstellersystem erreichbaren Wert liegt, nicht übersteigen darf.

8. ÜBERWACHUNG SENSORIK / EINGÄNGE

8.1. ANALOGE SIGNALE

8.1.1. BORDNETZSPANNUNG KLEMME 87 (HAUPTRELAIS)

Die über Klemme 87 geschaltete Bordnetzspannung versorgt einen Großteil der Aktuatoren und die SG-internen Spannungsregler. Die Bordnetzspannung wird analog erfaßt und auf Min-/Max-Werte überprüft. Während des Startvorgangs, wo Spannungseinbrüche auftreten können, wird die untere Diagnoseschwelle auf 5V gesetzt, da bei diesem Wert der Spannungsreglerreset aktiv sein muß und die Prozessoren nicht mehr laufen können.

Mit Verlassen des gültigen Bereichs wird ein Fehlerfilter gestartet und die Versorgungsspannung sofort auf einen Ersatzwert gesetzt (Schutz der Zündendstufen).

Da die Sensorversorgung von der Kl87-Bordnetzspannung abgeleitet wird, besteht bei einem zeitverzögert anziehenden Hauptrelais die Gefahr, daß die Überwachungsmodule der Sensoren schon aktiv sind, und somit auf Fehler Versorgungsspannung bzw. Fehler Sensor erkennen, was einen Wechsel in das Egas-Notprogramm zur Folge hätte. Deshalb werden die betroffenen Module erst freigegeben, wenn die Versorgungsspannungen als vorhanden erkannt wurden. Liegt die Versorgungsspannung nach einer definierten Zeitspanne immer noch nicht an, wird auf Fehler Hauptrelais erkannt.

8.1.2. SENSORVERSORGUNG

Die MSS54 verfügt über zwei getrennte 5V-Versorgungsspannungen Uext1 und Uext2 für die PWG- und DKG-Potis und HFM´s. Die Sensorversorgung wird im Steuergerät zurückgelesen und überwacht und bei der Berechnung der PWG- und DK-Positionen mit berücksichtigt. Verläßt eine Versorgungsspannung den zulässigen Bereich, wird ein Fehlerfilter gestartet. Bis zum Ablauf des Fehlerfilters wird der Uext-Wert auf den Min- bzw. Maxwert begrenzt. Nach Ablauf des Fehlerfilters wird der Uext-Wert auf den Ersatzwert gesetzt und alle an dieser Versorgungsspannung angeschlossenen Sensoren als fehlerhaft betrachtet.

Bei Ausfall der Sensorversorgung Uext 1 fallen somit ebenfalls die Sensoren PWG1, DKG1 und der HFM aus, so daß das Egas-System in die Notlaufstufe A - Notfahren über einen Pedalwertgeber und in die Notlaufstufe 2 - Fahren über Leerlaufsteller (Redundanz über HFM nicht mehr gegeben), wechselt.

Bei Ausfall der Sensorversorgung Uext2 fallen die Sensoren PWG2 und DK2 aus. Das Egas-System wechselt in die Notlaufstufe A und in die Notlaufstufe 1 - Notfahren mit einem DK-Geber (Redundanz über HFM gegeben).

8.1.3. PEDALWERTGEBER

Aus Sicherheitsgründen ist die Erfassung des Gaspedalstellung redundant ausgeführt. Der Pedalwertgeber besteht aus zwei getrennten Potentiometern mit unterschiedlicher Kennlinie und voneinander unabhängigen Masse- und Spannungsversorgungen.

Die Überwachung der Pedalwertgeber ist in zwei Bereiche unterteilt - die Überwachung eines jeden Sensorkanals und in den Vergleich der beiden Pedalwerte.

Min/Max-Überwachung Pedalwertgeber pwg1 oder pwg2

Die Überwachung ist aktiv, sobald die Sensoren versorgt sind. Unterschreitet die Sensorspannung eine festgelegte Minimalschwelle, bzw übersteigt sie eine Maximalschwelle, wird der Meßwert verworfen und die Fehlerfilterung gestartet. Nach Ablauf der Fehlerfilterung wird der Sensor als fehlerhaft gekennzeichnet.

Kanalvergleich pwg1 zu pwg2

Der Kanalvergleich hat die Aufgabe, die beiden pwg-Signale auf ihre Plausibilität zueinander zu überwachen. Übersteigt die Differenz der Pedalpositionen einen Grenzwert, wird auf Fehler PWG-Kanalvergleich erkannt und die Fehlerfilterung gestartet. Die erlaubte Differenz ist abhängig von dem Wert der kleineren pwg-Position, um leerlaufnahe Differenzen anders als Differenzen im Vollastbereich behandeln zu können.

Entscheidungsmatrix PWG-Überwachung

Alle Diagnoseinformationen, die für die Erfassung der Pedalwertgeber relevant sind, werden mittels einer Entscheidungsmatrix miteinander verknüpft und daraus ein PWG-Betriebsmode und ein Führungsgeber bestimmt. Die Verwendung einer Matrix hat den Vorteil, daß die vollständig und leicht überschaubar ist und die entprechende Software relativ einfach und somit auch testbar bleibt.

In der Matrix sind folgende Diagnoseinformation als Eingangssignal berücksichtigt:

- Fehler in Sensorversorgung pwg1
- Fehler in Sensorversorgung pwg2
- Bereichsfehler pwg1 bestätigt
- Bereichsfehler pwg2 bestätigt
- Fehler Kanalvergleich im Filter
- Fehler Kanalvergleich bestätigt

Das Ergebnis der Entscheidungsmatrix ist einer von drei möglichen PWG-Betriebsmodies:

- Mode 0 : PWG-Modul fehlerfrei
- Mode 1 : Ausfall eines PWG
  Wechsel in Notlaufprogramm Stufe A
- Mode 2 : Ausfall beider PWG
  Wechsel in Notlaufprogramm Stufe B

Sonderfall: Hochohmigkeit eines Potis im unteren Umkehrpunkt

Durch Ablagerungen oder durch Abreiben der Schleiferbahn können im unteren Umkehrpunkt Hochohmigkeiten entstehen, die dazu führen, daß das Sensorsignal kleiner wird. Dies hat zur Folge, daß die Nullpunktadaption für diesen Geber nach unten gezogen wird und unter Umständen das Sensorsignal sogar unter den Minimalwert wandert. Da dieser Effekt nur auf den unteren Umkehrpunkt beschränkt ist, der Geber im Restbereich aber ordnungsgemäß arbeitet, soll in diesem Fall kein Notprogramm aktiviert werden, sondern nur ein Fehlerspeichereintrag für die Werkstatt erfolgen.

Die PWG-Erfassung bzw. Überwachung verhält sich bei einer Hochohmigkeit im Umkehrpunkt folgendermaßen: Die Nullpunktadaption folgt dem kleiner werdenden Sensorsignal nur bis zu einer unteren Adaptionsgrenze und verharrt anschließend an dieser. Parallel dazu wird der Fehler PWG-Hochohmigkeit eingetragen. Die Überwachung auf die Minimalwert wird solange deaktiviert, wie das zweite Gebersignal noch im Leerlaufbereich liegt. Bei Verlassen des Leerlaufbereichs muß auch der andere Geber den hochohmigen Bereich verlassen. Ansonsten wird entweder auf Fehler Min-/Max-Überwachung oder auf Fehler Kanalvergleich erkannt.

genaue Beschreibung PWG-Erfassung und Überwachung: siehe **Modulbeschreibung PWG**

8.1.4. HFM-SIGNAL

Die Überwachung des Heißfilm-Luftmassenmessers erfolgt über Min-/Max-Schwellen, innerhalb der das gemessene ML-Signal liegen muß.
Eine Plausibilisierung HFM-Signal zu DK-Position im laufenden Betrieb wird dagegen nicht durchgeführt, da die Einflüsse aus Luftdruck, Lufttemperatur und Vanos (Katheizen, Vanosfehler) eine zu große Aufweitung der Toleranzgrenzen erfordern würden.
Bei Ausfall eines DK-Gebers, wird das verbleibende DK-Poti mittels des HFM-Signals überwacht. Dies ist in diesem Fall leichter möglich, da sich das System dann in einem Notprogramm befindet und die Motordynamik begrenzt und die Katheizfunktion gesperrt sind. Ein parallel auftretender Vanosfehler könnte allerdings weiterhin dazu führen, daß das Toleranzband verlassen wird, was aber nur noch einen Wechsel in ein noch schärferes Notprogramm - Notfahren über das Leerlaufstellersystem - zur Folge hätte.

Min-/Maxwertüberwachung:
Jeder berechnete ML-Wert des HFM (beim 8-Zylinder : Einzelwerte der beiden HFM´s) wird auf die definierten Min-/Maxgrenzen überprüft. Liegt der Meßwert außerhalb der Grenzen, wird er verworfen und statt dessen der ml-Ersatzwert verwendet. Außerdem erfolgt nach Ablauf der Fehlerfilterung ein Fehlerspeichereintrag.

Vergleich HFM-Signal mit Ersatzwert

Voraussetzung: fehlerfreier HFM , Fehler in DK-System (Ausfall eines Gebers, bzw. Fehler Kanalvergleich)

Bei bestätigtem Ausfall eines DK-Gebers wird das HFM-Signal zur Überwachung des verbleibenden Potis verwendet. Bei Fehler DK-Kanalvergleich wird versucht, über das HFM-Signal das fehlerhafte Poti zu lokalisieren.
Dazu wird unter Berücksichtigung des Tastverhältnis Leerlaufsteller, der Ansauglufttemperatur und des Umgebungsdruckes für jeden DK-Geber ein RF-Ersatzwert berechnet. Dieser Ersatzwert wird mit dem vom HFM gemessenen RF-Signal verglichen. Liegt der gemessene und der berechnete Wert innerhalb eines Toleranzbandes, gilt der DK-Wert als plausibel und es wird ein Flag in einem 16 Einträge fassenden Ringpuffer gesetzt. Unterschreitet die Anzahl der IO-Flags im Ringpuffer für einen definierten Zeitraum eine

vorgegebenen Schwelle, gilt der DK-Wert als unplausibel und es erfolgt ein Wechsel in das Notprogramm 2 - Notfahren über das Leerlaufstellersystem.

Gleiches gilt, wenn die Überwachung wegen eines bereits erkannten HFM-Fehlers nicht möglich ist.

8.1.5. DROSSELKLAPPEN POTENTIOMETER

Aus Sicherheitsgründen ist die Erfassung der Drosselklappenposition redundant ausgeführt. Es sind zwei getrennte DK-Geber mit zueinander inverser Kennlinie und voneinander unabhängigen Masse- und Spannungsversorgungen verbaut.

Da die Drosselklappenposition die Istgröße für den Egas-Lageregler darstellt und dieser sofort auf eventuell fehlerhafte Sensorgrößen reagiert, muß der DK-Überwachung besondere Aufmerksamkeit geschenkt werden.

Die Überwachung der Drosselklappengeber ist in zwei Bereiche unterteilt - in die Überwachung eines jeden Sensorkanals und in den Vergleich der beiden DK-Werte.

Min/Max-Überwachung DK-Geber dk1 oder dk2

Die Überwachung ist aktiv, sobald die Sensoren versorgt sind. Unterschreitet die Sensorspannung eine festgelegte Minimalschwelle, bzw übersteigt sie eine Maximalschwelle, wird sofort auf den zweiten Meßwert umgeschaltet und die Fehlerfilterung gestartet. Nach Ablauf der Fehlerfilterung wird der Sensor als fehlerhaft gekennzeichnet und in das Notprogramm Stufe 1 gewechselt.

Kanalvergleich dk1 zu dk2

Der Kanalvergleich hat die Aufgabe, die beiden DK-Signale auf ihre Plausibilität zueinander zu überwachen. Übersteigt die Differenz der DK-Positionen einen Grenzwert, wird auf Fehler DK-Kanalvergleich erkannt und die Fehlerfilterung gestartet. Die erlaubte Differenz ist abhängig von dem Wert der kleineren DK-Position, um leerlaufnahe Differenzen anders als Differenzen im Vollastbereich behandeln zu können.

Als äußerst problematisch erweist sich hierbei der Fall, wenn beide DK-Signale für sich betrachtet plausibel sind, zueinander aber eine zu große Differenz aufweisen. Die Vorgehensweise des PWG-Kanalvergleichs - Verwendung des unkritischeren (kleineren) Wertes - ist hier nicht so einfach. Aus Sicherheitsgründen muß beim DK-Kanalvergleich der größere Wert für die Istposition verwendet werden. Ist dies aber der fehlerbehaftete Wert, führt das zu einem sofortigen Schließen der Drosselklappen und somit zu einem spontanen Leistungsverlust des Motors.

Deshalb wird versucht, daß fehlerhafte Sensorsignal durch eine Plausibilisierung mit dem HFM-Signal zu lokalisieren. Ist eine Lokalisierung des fehlerhaften Gebers nicht möglich, wird weiterhin der größere Wert als Istwert verwendet.

Entscheidungsmatrix DK-Überwachung

Alle Diagnoseinformationen, die für die Erfassung der Drosselklappengeber relevant sind, werden analog der PWG-Überwachung mittels einer Entscheidungsmatrix miteinander verknüpft und daraus ein DK-Betriebsmode und ein Führungsgeber bestimmt.

In der Matrix sind folgende Diagnoseinformation als Eingangssignal berücksichtigt:

- Fehler in Sensorversorgung dk1
- Fehler in Sensorversorgung dk2
- Bereichsfehler dk1 bestätigt
- Bereichsfehler dk2 bestätigt
- Fehler Kanalvergleich im Filter
- Fehler Kanalvergleich bestätigt

Das Ergebnis der Entscheidungsmatrix ist einer von vier möglichen DK-Betriebsmodies:

- Mode 0 : DK-Modul fehlerfrei
- Mode 1 : Fehler Kanalvergleich - Plausibilisierung mit HFM-Signal noch nicht erfolgreich
  Wechsel in Notlaufprogramm Stufe 1
- Mode 1 : bestätigter Ausfall eines DK-Gebers
  Wechsel in Notlaufprogramm Stufe 1
- Mode 2 : Ausfall beider DK-Geber
  Wechsel in Notlaufprogramm Stufe 2

Sonderfall: Hochohmigkeit eines Potis im unteren Umkehrpunkt

Die Problematik mit der Poti-Hochohmigkeiten im unteren Umkehrpunkt ist bei den Drossel-klappen noch komplizierter als bei den Pedalwertgebern. Um im Falle eines Leitungsabrisses nicht einen kritischen Zustand zu erzeugen, müssen die Signale SG-intern mit Pull Up bzw. Pull Down Widerständen so beschaltet werden, daß als DK-Wert ein größerer Wert erkannt wird.
Für hochohmige Umkehrpunkte bedeutet dies, daß hier ebenfalls zu große DK-Positionen erkannt werden. Der Kanalvergleich würde eine zu große Abweichung detektieren und der Vergleich mit dem HFM-Signal den DK-Geber mit der Hochohmigkeit als fehlerhaft ermitteln. Aus Sicherheitsgründen sollte man nicht versuchen, diese Fälle von tatsächlich falschen Sensorsignalen zu unterscheiden, sondern den Sensor abschalten und in das Notprogramm Stufe 1 wechseln.

genaue Beschreibung DK-Erfassung und Überwachung: siehe **Modulbeschreibung DK**

8.1.6. KÜHLWASSERTEMPERATUR (MOTORTEMPERATUR)

Die Motortemperatur (Temperatur Kühlwasser Motoraustritt) wird innerhalb des Momentenmanagers für die Berechnung des Schleppmoments verwendet. Da dieses sehr stark von der Motortemperatur abhängig ist, ist dessen Einfluß auf das Egas-System nicht zu unterschätzen.

Die Überwachung der Motortemperatur erfolgt zweistufig:

- Min-/Maxgrenzwerte
- Mindestmotortemperatur in Abhängigkeit von Starttemperatur und Motorlaufzeit

Eine weitere Sicherheit gegen kurzzeitige Störungen bildet eine langsame Zeitkonstante des Tiefpaßfilters.

Im Fehlerfall wird oberhalb einer Öltemperaturschwelle die Öltemperatur als Ersatzwert verwendet. Unterhalb der Schwelle oder bei gleichzeitigem Ausfall des TOG wird die Ansauglufttemperatur als Ausgangswert für einen Ersatzwert verwendet, welcher anschließend über eine Zeitrampe erhöht wird.

8.1.7. ÖLTEMPERATUR

Der Einfluß der Öltemperatur ist ähnlich dem der Motortemperatur. Gemesssen wird die Ölsumpf-temperatur, interessant für die Bestimmung der Reibmomente ist allerdings die Motoreingangs-temperatur. Da die M-Motoren über Öl/Wasser (8 Zylinder) bzw. Öl/Luft-Wärmetauscher (6 Zylinder) verfügen, differieren beide Temperaturen stark voneinander. Deshalb sind für die Berechnung der Öltemperatur Modelle notwendig, die den Einfluß von Motortemperatur, Fz-Geschwindigkeit und Lufttemperatur mit berücksichtigen.

Die Ölsumpftemperatur wird über den Thermischen Ölniveau Geber TOG erfaßt. Dieser Sensor liefert ein PWM-Signal, in dessen Frequenz das Ölniveau und in dessen Pulsdauer die Öltemperatur übertragen wird. Natugemäß ist diese Schnittstelle relativ unempfindlich gegenüber Störungen.

Als Überwachungen sind folgende Mechanismen aktiv:

- Timeout-Überwachung
- minimale bzw. maximale Pulsdauer
- Min-/Maxwerte der Öltemperatur

Im Fehlerfall wird die Motortemperatur als Ersatzwert verwendet (auch bei Ausfall des Motortemperatur-sensors)

8.1.8. ANSAUGLUFTTEMPERATUR

Die Kennfelder für die Bestimmung der Ist- und der Maximalmomente des Motors werden auf Normbedingungen (Lufttempertur 20°C, Luftdruck 960mbar) bezogen. Bei der Berechnung der Momente wird die aktulle Lufttemperatur in Form eines Korrekturfaktors mit berücksichtigt.

Gemessen wird die Ansaugluft über einen in den HFM integrierten NTC-Sensor. Die Überwachung erfolgt über eine Min-/Maxwertplausibilisierung. Im Fehlerfall wird ein fester Ersatzwert verwendet und der Korrekturfaktor für die Momentenberechnung auf den Wert 1,0 gesetzt.

8.1.9. UMGEBUNGSDRUCK

Der Einfluß des Umgebungsdruckes auf die Momentenberechnung ist analog dem der Lufttemperatur.

Der Luftdruck wird durch einen in die MSS54 integrierten Drucksensor gemessen und über Min-/Maxschwellen überwacht. Im Fehlerfall wird ebenfalls ein fester Ersatzwert verwendet und der Korrekturfaktor für die Momentenberechnung auf den Wert 1,0 gesetzt.

8.2. DIGITALE SIGNALE

8.2.1. SCHALTER BREMSLICHT

Der Bremslichtschalter hat auf das Egas-System folgende Einflüsse:

- Abschaltbedingung für den Fahrgeschwindigkeitsregler
- Sicherheitsfunktion für PWG-Notfahren
- Sicherheitsfunktion im Egas-Notlaufprogramm

Ferner übernimmt die Motorsteuerung für das DSC-System die Plausibilisierung des Bremslichtschalters und übermittelt das Ergebnis über CAN an das DSC.

Die Information „Bremse betätigt“ liegt in der MSS54 mehrfach redundant vor:

- Bremslichtschalter Funktionsrechner, digital eingelesen
- Bremslichtschalter Sicherheitsrechner, digitial eingelesen
- Bremstestschalter Funktionsrechner, digital eingelesen
- Bremslichtschater DSC, über CAN eingelesen (kann optional ausgewertet werden)

Sobald einer der drei bzw. vier Schalter den Zustand „Bremse betätigt“ signalisiert, gilt diese als betätigt (Veroderung - keine Mehrheitsentscheidung). Unterscheiden sich die Informationen für mehr als einen definierten Zeitraum, gilt das Bremsschaltersystem als defekt. Die Bremse wird für den Rest des Fahrzykluses als permanent betätigt betrachtet und der Fehler Bremsschaltersystem eingetragen.

8.2.2. SCHALTER KRAFTSCHLUß

Der Schalter Kraftschluß besteht im Prinzip aus zwei in Reihe geschalteten Schaltern - einem Kupplungsschalter und einen Schalter im Getriebe, welcher die Leergasse detektiert. Aufgabe des Schalters ist es, einen durchgeschalteten bzw. offenen Antriebsstrang zu detektieren.

Der Einfluß des Schalters ist vielfältig. Die Bedingung „kein Kraftschluß“ wird verwendet, als

- Abschaltbedingung für den Fahrgeschwindigkeitsregler
- Freigabebedingung für die Leerlaufregelung
- Überbrückung des Momentenfilters
- Sperrbedingung für die Gangerkennung (kein Gang eingelegt)

Die Überwachung des Schalters erfolgt getrennt für die Zustände geschlossen oder offen. Bei Fahrzeugstillstand muß bei laufendem Motor der Schalter keinen Kraftschluß erkennen. Im Schubbetrieb hingegen muß der Schalter Kraftschluß erkennen, wenn die Motordrehzahl oberhalb einer Schwelle verharrt.

8.3. SERIELLE SCHNITTSTELLEN

8.3.1. CAN

Überwachung CAN-Busleitung

Die Überwachung der CAN-Busleitungen übernimmt direkt der CAN Controller. Dazu ließt er jedes seiner gesendeten Telegramme zurück und vergleicht diese. Ferner werden die empfangenen Telegramme auf ihr Telegrammformat und auf die Check Sum überwacht. Kommt es hierbei zu Fehlererkennungen, wird ein internes Fehlerregister inkrementiert. Nach Überschreiten einer Fehlerschwelle koppelt sich der Controller selbständig vom CAN ab und signalisiert dies der CPU über ein Statusbit. Dieses Statusbit wird von der CPU zyklisch alle 100ms ausgelesen. Im Fehlerfall erfolgt ein Fehlerspeichereintrag und der CAN Controller wird neu initialisiert.

Den Fail Save für die Empfangsbotschaften übernimmt eine Timeout-Überwachung, falls der CAN innerhalb der Timeoutzeit nicht wieder funktioniert.

Timeout-Überwachung der Empfangstelegramme

Die Timeout-Überwachung kontrolliert den zyklischen Empfang der CAN-Telegramme. Unterbleibt dieser für einen telegrammspezifischen Zeitraum, erfolgt ein Fehlerspeichereintrag und die CAN-Variablen dieses Telegramms werden auf neutrale Werte gesetzt.

Die Timeoutüberwachung ist aktiv, sobald

- Klemme 15 ein
- und Bordnetzspannung > K_CAN_UBMIN
- und Zeit seit letzter Unterspannung > K_CAN_ED_TSPERR
- und Zeit seit letzter SG-Initialsierung > K_CAN_ED_TSPERR

Überwacht werden zur Zeit folgende CAN-Telegramme

Telegramm	Sender	Timeoutwert
ASC1	DSC	300ms
ASC2	DSC	300ms
ASC3	DSC	300ms
LWS1	Lenkwinkelsensor	300ms
INSTR2	Kombiinstrument	1000ms
INSTR3	Kombiinstrument	1000ms

Um die Anzahl der Fehlerorte nicht ausufern zu lassen, führen nur das Ausbleiben der CAN-Telegramme ASC1, LWS1 bzw. INSTR2 zu Fehlerspeichereinträgen, da davon ausgegangen wird, daß bei Ausfall eines Senders alle Telegramme dieses Senders ausbleiben.

Plausibilisierung der DSC Momenteneingriffe

Da das DSC über die Momentenschnittstelle die Motorleistung erhöhen als auch stark reduzieren kann, müssen die DSC-Eingriffe plausibilisiert werden. Dies erfolgt mittels redundant übertragenen Informationen, die zueinander plausibel sein müssen. Anderenfalls wird ein Fehlerfilter gestartet, nach dessen Ablauf ein Fehlerspeichereintrag erfolgt und ein eventuell noch aktiver DSC-Eingriff abgebrochen.

Die Art der Plausibilisierung entspricht dem im CAN-Lastenheft 11H, Rev 1.4 geforderten Umfang. Die Filterzeit für unplausible Eingriffe beträgt 300ms. Der Alive-Zähler zur besseren Überwachung der MSR-Eingriffe wird seitens der DME unterstützt. (Konfigurationsparameter K_ASC_ALIVE), kann allerdings zur Zeit noch nicht verwendet werden, da das DSC3 von Bosch ihn nicht liefern kann.

Abbruch eines DSC Momenteneingriffs

Bei Ausfall des CAN, Timeout der ASC-Botschaft bzw. unplausiblen Eingriffen wird nach Ablauf der Fehlerfilterung ein eventuell noch aktiver DSC-Momenteneingriff beendet. Dabei werden MSR-Eingriffe (momentenerhöhend) sofort abgebrochen. ASC-Eingriffe (momentenreduzierend) hingegen über eine Rampe auf das Fahrerwunschmoment aufgeregelt.

Sicherung gegen zu hohe Interruptlast

Die MSS54 arbeitet auf der Empfangsseite interrupt gesteuert. Das heißt, daß jedes empfangene Telegramm sofort eine CPU-Aktion zur Folge hat. Dies birgt die Gefahr, daß durch einen fehlerhaften CAN-Teilnehmer, welcher permanent sendet, der Programmablauf in der Motorsteuerung stark beeinträchtigt werden kann. Um sich dagegen zu schützen, wurde eine maximale Interruptlast pro Empfangskanal definiert, bei dessen Überschreiten der Empfangskanal für den Rest des Motorlaufes abgeschaltet wird.

8.3.2. MFL

Die MSS54 verfügt über einen integrierten Fahrgeschwindigkeitsregler FGR, welcher vom Fahrer über ein Multi-Funktions-Lenkrad MFL bedient wird. Das MFL selbst beinhaltet vier Taster für die Bedienung des FGR:

- Ein-/Aus
- Setzen/Beschleunigen
- Verzögern
- Wiederaufnahmen

Die Kommunikation zwischen DME und MFL erfolgt über eine unidirektionale, serielle Ein-Draht Schnittstelle. Zur Absicherung der Kommunikation und der übertragenen Daten werden die vier Tasterinformationen in eine redundante 7-Bit Information umgesetzt und um weitere 24 Bit, deren Wertigkeit fest vordefiniert ist, erweitert. Um auch die zyklische Erneuerung der Information überwachen zu können, wird noch ein weiteres Bit, das sogenannte Toggle-Bit, welches sich in einem definierten Zeitraster ändern muß, ergänzt. In der Summe ergibt sich somit ein 32-Bit Datenstrom, welcher zyklisch ca. alle 20ms vom MFL an die DME gesendet wird.

Die MFL-Überwachung innerhalb der DME ist somit in der Lage, die Schnittstelle auf folgende Fehler hin zu überwachen:

- Timeout des Telegramms
- Fehler Toggle-Bit (keine Änderung im definierten Zeitraster)
- Formatfehler der fest vorgegebenen 24 Bits
- ungültige Kombination der 7-Bit Tasterinformation

Detektiert die DME einen dieser Fehlerzustände, werden Fehlerfilter gestartet. Nach deren Ablauf erfolgt ein Fehlerspeichereintrag und ein eventuell aktiver FGR-Betrieb wird abgebrochen.

Nähere Information zum FGR-Modul: siehe Modulbeschreibung fgr.doc

9. ÜBERWACHUNG AKTUATORIK / AUSGÄNGE

9.1. STELLEINHEIT (H-BRÜCKE, STELLMOTOR, DK-MEACHNIK)

9.1.1. ELEKTRISCHE TREIBERDIAGNOSE

Die Motorola H-Brücke, welche den Egas-Stellmotor ansteuert, verfügt über einen Statusausgang, welcher vom Funktionsrechner mit jedem Reglerzyklus ausgewertet wird. Über den Statusausgang meldet die H-Brücke folgende Zustände:

- Unterspannung der Brückenversorgung
- Übertemperatur
- Überstrom
- Abschaltpfad Funktionsrechner aktiv
- Abschaltpfad Sicherheitsrechner aktiv
- Unterbrechung Abschaltpfad Funktionsrechner
- Unterbrechung Abschaltpfad Sicherheitsrechner

In all diesen Fällen schaltet sich die H-Brücke automatisch ab (die Ausgänge werden hochohmig) und muß vom Funktions- oder Sicherheitsrechner wieder aktiviert werden.

Da unter extremen Betriebsbedingungen die Zustände Unterspannung, Übertemperatur bzw. Überstrom nicht ausgeschlossen werden können, wird ein Aktivieren des Statusausganges nur im Fehlerspeicher abgelegt. Er hat aber keine Auswirkungen auf den Betriebsmode des Egas-Systems, da der Soll-/Istvergleich der Egas-Position all diese Fälle mit abdeckt.

9.1.2. SOLL-/ISTVERGLEICH EGAS-POSITION

Der Vergleich der Sollposition der Drosselklappen mit deren Istpostion ist einer der wichtigsten Überwachungsfunktionen im Egas-Sicherheitskonzept. Anhand ihm lassen sich folgende Fehler erkennen:

- Prozessormodule
  - CTM-Modul (Prozessor): generiert Ansteuertastverhältnis für Stellmotor generiert
  - Prozessor Port C: Drehrichtung des Stellmotors
  - Prozessor Port C: Freigabe Stellmotor Funktionsrechner
  - Prozessor Port C: Freigabe Stellmotor Sicherheitsrechner

- H-Brücke Stellmotor
  - H-Brücken Defekt
  - Übertemperaturabschaltung
  - Strombegrenzung H-Brücke
  - Überstromabschaltung H-Brücke

- Verkabelung Stellmotor
  - Leitungsunterbrechung
  - Kurzschluß nach Masse, Ub, bzw. der Leitungen untereinander

- Stellmotor
  - Wicklungsdefekt
  - Mechanikschaden
  - Getriebeschaden

- DK-Kinematik

- Mechanikschaden

- Drosselklappen
  - festklemmende Klappen

- Drosselklappen Adaption
  - Verschiebung des Nullpunktes
  - Verschiebung des Anschlagpunktes

Fall1: Die Drosselklappen sollen über eine Schwelle geöffnet werden, die Klappen bleiben aber geschlossen.

Gründe: Prozessormodul defekt
H-Brücke defekt oder kurzfristig abgeschaltet
Sicherheitsabschaltung aktiviert
Stellmotorverkabelung
Stellmotor defekt
DK-Kinematik defekt

Fehlererkennung:

Egas-Sollposition > K_EDKSI_POS_ZU + K_EDKSI_HYS_ZU
und Egas-Istposition < K_EDKSI_POS_ZU
für Zeit > K_EDKSI_T_ZU

Reaktion: Wechsel in Egas-Notprogramm Stufe 2 - Fahren über Leerlaufsteller

Beurteilung: Die Drosselklappen bleiben geschlossen bzw. werden über die Federpakete selbständig geschlossen, ohne daß das Steuergerät darauf Einfluß nehmen kann. Ebensowenig kann der Momentenabbau bei Schließen der Klappen beeinflußt werden (kritischter Zustand für Fall 1). Sind die Klappen geschlossen, ist eine Weiterfahrt im Notprogramm problemlos möglich, wenn sichergestellt wird, daß die Klappen sich nicht mehr öffnen können.

Fall2: Die Drosselklappen sollen geschlossen werden, bleiben aber einen Spalt offen.

Gründe: Drosselklappe klemmt bzw extrem schwergängig
geringfügiges Verdrehen des Führungspotis der Drosselklappenanlage
falsche Nullpunktadaption

Fehlererkennung:

Egas-Sollposition = 0
und K_EDKSI_POS_ZU < Egas-Istposition < K_EDKSI_HYS_BL_AUF
für Zeit > K_EDKSI_T_SPALT

Reaktion: kein Egas-Notprogramm - Beibehaltung der aktuellen Betriebsstufe
Fehlerspeichereintrag

Beurteilung: Da die Drosselklappen trotz Zudücken über den Stellmotor einen Spalt offen bleiben, deutet auf ein größeres Problem in der DK-Anlage hin, welches einen Fehlerspeichereintrag rechtfertigt. Die Grenze K_EDKSI_HYS_BL_AUF ist allerdings so bemessen, daß sie im Leerlauf eine erhöhte Leerlaufdrehzahl zur Folge hätte, für den Fahrbetrieb aber nicht als sicherheitskritisch angesehen wird und somit kein Wechsel in ein Egas-Notprogramm erfolgen muß.

Anmerkung: Durch Beobachten der Drehzahl im Leerlauf könnte zwischen Mechanikproblem und Adaptionsproblem unterschieden werden:
LL-Drehzahl kann eingeregelt werden : Adaptionsproblem
LL-Drehzahl zu hoch : Klappenproblem

Fall3: Die Drosselklappen sollen geöffnet werden, die Klappen reagieren, erreichen den Sollwert allerdings nicht.

Gründe: H-Brücke kurzfristig abgeschaltet
schwergängiges DK-System
Drosselklappe klemmt unterhalb Sollposition
Unterspannung

Fehlererkennung:

Egas-Sollposition - Egas-Istposition > K_EDKSI_HYS_U_SOLL
und K_EDKSI_POS_ZU < Egas-Istposition <= K_EDKSI_POS_N_GANZ
und ub > K_ED_UBMIN
für Zeit > K_EDKSI_T_U_SOLL

Reaktion: Wechsel in Egas-Notprogramm Stufe 2 - Fahren über Leerlaufsteller

Beurteilung: Da die Zuverlässigkeit des Egas-Systems nicht mehr gewährleistet ist, werden die Klappen gezielt geschlossen und anschließend die Ansteuerung deaktiviert. Bei klemmenden Klappen ist eine Wechsel in den Fall 2 bzw. 5 möglich, sobald sich der Sollwert unterhalb dem Istwert befindet, bzw je nach Istposition auch der Fall 4 (gehen nicht ganz auf).

Fall4: Bei Vollast gehen die Drosselklappen nicht vollständig auf

Gründe: Klappen an VL-Anschlag - falsche Adaption
Unterspannung

Fehlererkennung:

Egas-Sollposition - Egas-Istposition > K_EDKSI_HYS_N_GANZ
und Egas-Istposition > K_EDKSI_POS_N_GANZ
und ub > K_ED_UBMIN
für Zeit > K_EGAS_T_N_GANZ

Reaktion: kein Egas-Notprogramm
Umschaltung der Steigung der DK-Potikennlinie auf definierte Maximalsteigung (Stellmotorschutz)
Start einer neuen VL-Adaption im Nachlauf
Fehlerspeichereintrag

Beurteilung: Dieser Fall hat nur eine Leistungseinbuße im Vollastbereich zur Folge und ist somit nicht sicherheitskritisch. Es müssen allerdings Maßnahmen zum Schutz des Stellmotors ergriffen werden.

Fall5: Die Drosselklappen klemmen im geöffneten Zustand

Gründe: Defekt Prozessormodul - 100% Ansteuerung, falsche Drehrichtung
H-Brücke durchlegiert
Kurzschluß in Stellmotorverkabelung
schwergängiges DK-System
Drosselklappe klemmt oberhalb Sollposition

Fehlererkennung:

Egas-Istposition - Egas-Sollposition > K_EDKSI_HYS_BL_AUF
für Zeit > K_EDKSI_T_BL_AUF_R (Erkennungs- und Reaktionszeit)
bzw. Zeit > K_EDKSI_T_BL_AUF_F (Fehlerfilterzeit)

Reaktion: Nach Ablauf der Erkennungszeit werden aufgrund der möglichen Auswirkungen des Fehlers sofort momentenbegrenzende Maßnahmen über Zündwinkeleingriffe und Einspritzausblendungen ergriffen.

Nach Ablauf der Fehlerfilterzeit erfolgt ein Wechsel in das Egas-Notprogramm der Stufe 3 - Fahren mit offenen Drosselklappen

Beurteilung: In diesem Fall erzeugt der Motor mehr Leistung als der Fahrer wünscht und es kann zu ungewollten Fahrzeugbeschleunigungen kommen. Dadurch ist eine schnelle Reaktion auf diesen Zustand erforderlich. Das Steuergerät hat aber Möglichkeiten, über Zündwinkeleingriffe und Zylinderausblendungen die Motorleistung auf einen Bereich zu drosseln, den der Fahrer vorgibt.

9.2. LEERLAUFSTELLER

Die Motoren der M GmbH verfügen mit dem Leerlaufstellersystem noch über ein zweiten, von der Egas-Anlage unabhängiges Luftliefersystem. Der maximale Luftdurchsatz durch den Leerlaufsteller beträgt ca. 100 kg/h im Vergleich zu den 1200 kg/h durch die Drosselklappen. Die damit erreichbar Maximaldrehzahl beträgt bei betriebswarmen Motor und offenen Antriebsstrang ca. 3000 Upm, die Maximalgeschwindigkeit im 6.Gang, ebener Fahrstrecke und langem Anlaufweg ca. 80 km/h.

Die damit erreichbaren Fahrleitstungen werden als vom Fahrer beherrschbar eingestuft, so daß bei allen Fehlern - auch bei SG-internen - ein Notfahren über das Leerlaufstellersystem weiterhin erlaubt wird.

Das Leerlaufstellersystem selbst besteht aus einem Zwei-Wicklungs-Drehsteller ZWD mit einer Öffner- und einer Schließerwicklung, welche über eine gemeinsame Versorgungsleitung mit der Klemme 87 verbunden ist. Sind beide Wicklungen stromlos, wird über eine interne Feder ein Notluftquerschnitt eingestellt, welcher einem ungefähren Ansteuertastverhältnis von 30% entspricht.

Die Ansteuerung seitens der DME erfolgt über zwei PWM-Signale, wobei die Schließerwicklung mit dem inversen Signal der Öffnerwicklung betrieben wird. Die für die Ansteuerung eingesetzten Treiber sind diagnosefähig und überwachen die Ansteuerleitung in Bezug auf

- Leitungsunterbrechung
- Kurzschluß nach Masse
- Kurzschluß nach Ub

Nach Detektion eines elektrischen Fehlers erfolgt sofort eine Reaktion in der Ansteuerung des ZWD. Die Ablage eines Fehlers im Fehlerspeicher der DME erfolgt nach Ablauf eines Fehlerfilters.

Die Reaktionen auf alle mögliche Fehlerkombinationen sollen, soweit dies möglich ist, die Auswirkungen auf den Motorbetrieb dämpfen und sind in einer 4x4-Matrix abgelegt. So wird bei Kurzschluß einer Ansteuerleitung nach Masse die verbleibende Wicklung ebenfalls voll bestromt, so daß sich ein effektives Ansteuerverhältnis von ca. 50% ergibt. Bei Ausfall einer Leitung (Unterbrechung oder Kurzschluß nach Ub) wird die verbleibende Wicklung mit einem minimalen Tastverhältnis betrieben und es stellt sich ein Öffnungsquerschnitt im Bereich des Notluftquerschnittes ein.

Die Aufteilung der Sollfüllung auf Leerlaufsteller und Drosselklappe, sowie die Berechnung der ml-Ersatzwerte berücksichtigt die Notlaufmaßnahmen in der Leerlaufstelleransteuerung.

10. ÜBERWACHUNG STEUERGERÄTE HARDWARE

10.1. PRE DRIVE CHECK STEUERGERÄT

10.1.1. SPEICHERTESTS

In der Initialisierungsphase des Steuergerätes werden die beiden internen RAM-Speicher eines jeden Prozessors einem vollständigen Schreib-/Lesetest unterzogen. Wird dabei ein RAM-Fehler festgestellt, wird sofort auf SG-internen Fehler erkannt und das System startet im Notprogramm der Stufe 4.

Eine Checksum-Überprüfung der Programm und Datenspeicher erfolgt in der Regel nicht in der Initialisierungsphase des Steuergerätes, da diese Tests den Motorstart unakzeptabel verzögern würde. Wurde allerdings in dem davorliegenden Betriebszylus des Steuergerätes ein entsprechender Fehler vermerkt, werden auch diese Test in der Initialisierungsphase nochmals vollständig durchgeführt. Wird der Fehler hierdurch bestätigt, erfolgt ebenfalls ein Wechsel in das Notprogramm 4.

Näheres zu den Speichertests siehe Modulbeschreibung : sk_check.doc

10.1.2. PROZESSOR SYNCHRONISATION

Die MSS54 ist ein Zweiprozessorsystem, wobei beide Prozessoren etwa 50 Prozent der Funktionalität der Motorsteuerung übernehmen. Die Kommunikation zwischen den beiden Prozessoren erfolgt über ein Dual Ported RAM (DPR). Weiterhin sind die beiden Prozessoren über eine hochpriore Interruptleitung gekoppelt, die jedem Prozesssor ermöglicht, dem Partner einen „Non Maskable Interrupt“ auszulösen.

Eine weitere Sicherungsstufe besteht darin, daß die Reseteingänge der Prozessoren und Ports des Partners geführt sind, so daß bei Bedarf ein Prozessor den anderen zurücksetzen kann.

Prozessorsynchronisation bei der SG-Initialisierung

Bei der Intialisierung des Steuergerätes besteht das Problem, daß die Prozessoren über ein Dual Ported RAM kommunizieren. Da bei der Initialisierung der einzelnen Softwaremodule aber bereits auf Größen vom anderen Prozessor zugegriffen wird, muß sichergestellt sein, daß die entsprechenden Variablen im Dual Ported RAM bereits mit sinnvollen Werten vorinitialisiert sind. Das DPR kann hingegen nicht von einer Seite aus initialisiert werden, da dies bei einem unverhofften Reset eines Prozessors bedeutet, daß er auch die Variablen des anderen Prozessors mit neu initialisieren würde.

Deshalb wurde in die Initialisierungphase der einzelnen Prozessoren eine Synchronisationsebene eingeführt, die sicherstellen soll, daß die Prozessoren beim Hochlauf erst mit der Initialisierung der Funktionsmodule beginnen, wenn beide Seiten ihre DPR-Variablen initialisiert haben.

Realisiert wird die Synchronisation über das Modul Inter-Prozessor-Kommuniaktion (IPK) des Betriebssystems OSKAR. Die IPK ist ein über Handshake-Mechanismen, Checksum und Timeout-Überwachung abgesicherter Kommunikationskanal, welcher dem Partnerprozessor Befehle und Daten übermitteln kann und von diesem einen Ausführungsstatus rückgemeldet bekommt.

Bei der Initialisierung sendet jeder Prozessor eine Synchronisationsaufforderung über die IPK an den Partner. Hat dieser zu diesem Zeitpunkt bereits seine DPR-Größen initialisiert, wird ein OK-Status zurückgemeldet. Ist die Initialisierung noch nicht erfolgt, unterbleibt eine Antwort. Der Sender der Synchronisationsaufforderung wartet nun auf den OK-Status. Wird dieser innerhalb der Timeoutzeit der IPK von zur Zeit 32ms nicht erkannt, wiederholt er noch bis zu vier Mal den Synchronisationsversuch. Bleiben auch diese unbeantwortet, initialisiert der Prozessor auf die DPR-Größen des Partners mit neutralen

Werten und setzt den weiteren Programmablauf fort. Der Motorbetrieb bleibt solange gesperrt, bis die Kommunikation zwischen den beiden Prozessoren aufgebaut werden konnte.

Wird ein Prozessor im laufenden Betrieb zurückgesetzt, muß er sich in der Initialisierung ebenfalls wieder mit dem normal weiterlaufenden Prozessor synchronisieren.

10.1.3. PRE DRIVE CHECK EGAS-STELLEINHEIT

Der Pre Drive Check der Egas-Stelleinheit hat folgende Aufgaben.

- Phase 1 : Nullpunktadaption der Drosselklappen Potentiometer
- Phase 2 : Prüfen der Freigängigkeit der Klappen und des Egas-Regelkreises
- Phase 3 : Prüfen der Sicherheitsabschaltung Egas des Überwachungsrechners und Prüfen der Rückziehfedern der Klappen

Der Pre Drive Check wird nach jedem Power On des Steuergerätes durchgeführt, sobald die Versorgungsspannung der Treiber und der Sensoren vorliegt.

Die Phase 1 wird immer durchgeführt. in Phase 2 und 3 wird der Pre Drive Check abgebrochen, sobald die Klemme 50 aktiv wird, die Motordrehzahl ungleich Null ist oder das Fahrzeug sich bewegt.

Phase 1: Nullpunktadaption der Drosselklappen Potentiometer

Nach jedem Power On des Steuergerätes wird zwingend ein Adaptionslauf für die Bestimmung der Nullpunktlage der Drosselklappenpotis durchgeführt. Dies ist notwendig, da das DK-Gebersignal den Istwert für den Egas-Regelkreis darstellt und bei einer falschen Nullpunktadaption die Drosselklappen nicht mehr korrekt geschlossen werden könnten, bzw es zu Fehldiagnosen der DK-Überwachung kommt.

Die Adaption erfolgt, indem der Stellmotor die Drosselklappen mit einer definierten Kraft zudrückt. Anschließend wird die Potispannung mehrmals erfaßt, und falls alle Meßwerte plausibel sind, daraus über eine Mittelwertbildung die neue Nullpunktlage für jedes Drosselklappenpoti bestimmt.

Einzelheiten zum Adaptionsvorgang sind der Modulbeschreibung Drosselklappen zu entnehmen.

Phase 2: Prüfen der Freigängigkeit der Klappen und des Egas-Regelkreises

In der Phase 2 wird die Freigängigkeit der Drosselklappen und das Einregelverhalten des Egas-Regelkreises überprüft.

Dazu wird der Sollwert egas_soll auf den Wert K_PDR_EDK_SOLL gesetzt. Parallel dazu wird der Soll-/Istvergleich des Egassystems und die Diagnose der Drosselklappenpotis inclusive dem Kanalvergleich aktiviert. Nach Ablauf der Wartezeit K_PWD_T_PHASE2 werden die Informationen der entsprechenden Überwachungsmodule ausgewertet. Arbeitet das Egas-System fehlerfrei, müßte die Sollposition eingeregelt sein und alle Diagnosen einen i.O-Zustand melden.

Im Detail werden für den Pre Drive Check - Phase 2 folgende Diagnosen ausgewertet:

- Soll-/Istvergleich der Drosselklappenposition
- Sensordiagnose DK1-Geber

- Überwachung Sensorversorgung DK1
- Sensordiagnose DK2-Geber
- Überwachung Sensorversorgung DK2
- Kanalvergleich DK1/DK2-Wert

Tabelle: Auswertung Diagnoseinformation Pre Drive Check

Soll-/Ist Vergleich	Kanal-vergleich	Diagnose DK1	Diagnose DK2	Bewertung	Verzweigung in Notlaufprogramm
0	**0**	**0**	**0**	System in Ordung	---
0	**x**	**0**	**1**	Ausfall DK2	Stufe 1
0	**x**	**1**	**0**	Ausfall DK1	Stufe 1
0	**1**	**0**	**0**	DK1 zu DK2 unplausibel	Stufe 2
0	**x**	**1**	**1**	Kombination unmöglich	Stufe 4
1	**0**	**0**	**0**	Istposition wird nicht erreicht Istposition zu klein Istposition zu groß	 Stufe 2 Stufe 3
1	**1**	**0**	**0**	Istposition wird nicht erreicht DK1 zu DK1 unplausibel	Stufe2
1	**x**	**0**	**1**	Istposition wird nicht erreicht Ausfall DK1	Stufe2
1	**x**	**1**	**0**	Istposition wird nicht erreicht Ausfall DK2	Stufe2
1	**x**	**1**	**1**	Ausfall beider Geber	Stufe 2

0 := in Ordnung
1 := fehlerhaft
x := nicht relavant

Die Phase 2 wird bei einem Startversuch (Klemme 50 aktiv oder Motordrehzahl ungleich Null oder Fz-Geschwindigkeit ungleich Null) sofort abgebrochen.

offene Punkte: Wartezeit evtl abhängig von der Motortemperatur

Phase 3: Prüfen der Sicherheitsabschaltung und der Schließfedern

Aufgabe der Phase 3 ist es, den Abschaltpfad des Sicherheitsrechners für die H-Brücke, sowie die Schließfedern der Drosselklappen zu überprüfen.

Dazu wird vom Funktionsrechner weiterhin für die Drosselklappen der Sollwert K_PDR_EDK_SOLL vorgegeben. Parallel dazu wird der Sicherheitsrechner aufgefordert, seinen Abschaltpfad für die H-Brücke zu aktivieren. Im fehlerfreien Zustand müßten nun die Drosselklappen durch die Federpakete zugezogen werden. Unterschreitet die Istposition innerhalb der Zeit K_PDR_T_PHASE3 eine vorgegebene Schwelle nicht, wird der Sollwert auf Null gesetzt,die H-Brücke bleibt abgeschaltet.

Lassen sich die Drosselklappen nun schließen, funktioniert der Abschaltpfad nicht. Es wird ein SG-interner Fehler eingetragen und in das Egas-Notlaufprogramm der Stufe 2 verzweigt. Bleiben die Klappen weiterhin offen, wird anschließend die Sicherheitsabschaltung wieder deaktiviert. Lassen sich die Klappen nun schließen, sind die Schließfedern defekt. Es wird der entsprechende Fehler eingetragen und ebenfalls in das Notlaufprogramm Stufe 2 verzweigt. Bleiben die Klappen weiterhin offen wird das Notlaufprogramm Stufe 3 aktiviert.

Die Phase 3 wird bei einem Startversuch (Klemme 50 aktiv oder Motordrehzahl ungleich Null oder Fz-Geschwindigkeit ungleich Null) sofort abgebrochen.

10.2. ÜBERWACHUNG STEUERGERÄT IM LAUFENDEN BETRIEB

10.2.1. SPEICHERTESTS

Im laufenden Betrieb werden die Programm-, Daten- und Variablenspeicher der DME einem permanenten, zyklischen Test unterzogen. Die RAM-Speicher werden dabei mittels eines Schreib-/Lesetests überprüft, während die ROM-Speicher (Programm und Daten) über CRC16-Checksums überwacht werden.
Wird hierbei ein Fehler detektiert und bestätigt, wechselt das System in das Notprogramm 4 - SG-interner Fehler.

Eine Sonderstellung beim Speichertest weist das DPR auf. Da auf diesen Speicher asynchron von zwei Seiten zugegriffen wird, verbietet sich hier ein Schreib-/Lesetest. Eine Detektion fehlerhafter Speicherzellen ist deshalb nicht möglich. Seitens dem Sicherheitskonzept wird hierdurch begegnet, indem das DPR von sicherheitskritischen Variablen freigehalten wird. Das heißt, daß alle für die Füllung des Motors und somit für die Momentenabgabe relevanten Variablen in einem internen Speicher des Prozessors liegen, welcher dem RAM-Test unterliegt, und das DPR nur Kopien dieser Werte besitzt, wobei die Kopien nur für unkritische Programmteile verwendet werden.
In Fällen, wo auch ein sicherheitskritischer Austausch von Werten über das DPR notwendig ist, erfolgt dies nicht direkt durch Ablage dieser Werte im DPR, sondern über den Checksum-geschützten Transportmechanismus der Inter Prozessor Kommunikation.

10.2.2. ÜBERWACHUNG HW-INITIALISIERUNG

implementiert, aber noch nicht dokumentiert

10.2.3. PROZESSOR KOMMUNIKATION

Die Überwachung der Prozessor Kommunikation bzw. auf deren Betriebsbereitschaft erfolgt über zwei Kontrollfunktionen.

Eine sehr einfache, aber dennoch sehr effektive Überwachungsfunktion besteht in der Kontrolle der beiden Systemtimer auf deren Gleichlauf. Dazu legt jeder Prozessor eine Kopie seines Systemtimers im DPR ab. Erkennt ein Prozessor über einen Zeitraum von K_PCNTRL_TIMEOUT keine Veränderung der Timers des Partnerprozessors, so wird daraus auf ein Problem in dessen Programmabarbeitung geschlossen, und das System mittels eines Resets zurückgesetzt und neu initialisiert.

Ein zweiter, etwas aufwendiger Kontrollmechanismus überwacht den Austausch der sicherheitskritischen Variablen über die IPK. Wie bereits erwähnt, arbeitet dieser Austauchmechanismus mit abgesicherten Telegrammen, deren Sicherungsmechanismen folgendes beinhalten:

- Überprüfung der Telegrammkennung
- Überprüfung der Telegrammchecksum
- Bestätigung des einwandfreien Empfangs des Telegramms
- Rückgabewert der Auswertefunktion des Telegramms an Sender
- Timeoutüberwachung auf Senderseite bezüglich Empfangsquittung

Kommt für einen Zeitraum von K_SK_IPK_TIMEOUT keine einwandfreie Kommunikation zwischen den beiden Prozessoren zustande, wird das System ebenfalls mittels Reset neu initialisiert.

10.2.4. PROGRAMMABLAUFKONTROLLE

Jeder Prozessor der MSS54 verfügt über einen prozessorinternen Hardware-Watchdog. Dieser muß innerhalb der Watchdogzeit von einer Sekunde mindestens einmal aus der Background-Task(langsamste Task) und der 10ms-Task (wichtigste Task für Egas-System) bedient werden.

Um zusätzlich den Ablauf aller für das Egas-System relevanten Programmteile gewährleisten zu können, wurde parallel zum Hardware-Watchdog, eine Programmablaufkontrolle implementiert. Diese wird zyklisch von der watchdogüberwachten 10ms-Task aufgerufen, und kontrolliert, ob innerhalb eines applizierbaren Zeitraum alle für das Egas-System relevanten Funktionen mindestens einmal ausgeführt wurden.

Realisiert ist dies mittels einer Flagvariablen, in der für jede Funktion ein Bit reserviert ist, und welches bei der Ausführung der Funktion gesetzt wird. Erkennt die Programmablaufkontrolle, daß eines dieses Bits nicht gesetzt ist erfolgt ein Fehlerspeichereintrag und der Prozessor wird zurückgesetzt. Tritt dieser Zustand mehrmals während eines Motorbetriebs auf, geht das Egas-System in das Notlaufprogramm der Stufe 2 - Notfahren über Leerlaufsteller.

Überwacht werden zur Zeit folgende Module:

Masterprozessor :

- Erfassung Pedalwertgeber
- Überwachung Pedalwertgeber
- Erfassung Drosselklappenpoti
- Überwachung Drosselklapppenpoti

- Soll-/Istvergleich Egas-Position
- Hauptfunktion Sicherheitskonzept

10.2.5. RESET ÜBERWACHUNG

In der MSS54 sind eine Reihe von Überwachungsmechanismen implementiert, die zu einem Auslösen eines Resets und damit zum Neustart des System führen. Beispiele für solche Überwachungsfunktionen sind:

- interner Watchdog
- auftreten eines nicht initialisierten Interrupts
- Fehler in der Programmabarbeitung (Zero Devide, Bus Error, Illegal Opcode, ...)
- Timeout in der Prozessorkommunikation
- Fehler in den Testrechnungen
- Timeout in der Programmablaufkontrolle

Im regulären laufenden Betrieb soll das System jedoch resetfrei laufen. Übersteigt aber während einer Betriebsphase die Resethäufigkeit des Systems eine definierten Grenzwert, deutet dies auf ein schwerwiegendes Problem innerhalb der DME hin. Da der Grund für das Problem und dessen Auswirkungen allerdings nicht vorhersehbar sind, erfolgt aus Sicherheitsgründen ein Wechsel in das Egas-Notprogramm 4 - SG interner Fehler.

Für die Resetüberwachung sind die Resetleitung eines jeden Prozessors ist an einen Interrupteingang des Partners geführt. So ist dieser in der Lage, jeden Reset des Partners sofort zu erkennen, ihn zu dokumentieren und entsprechende Schutzmaßnahme bis zur erneuten Betriebsbereitschaft des Systems zu ergreifen.

10.3. ÜBERWACHUNG STEUERGERÄT IN DER NACHLAUFPHASE

10.3.1. SPEICHERTESTS

In jeder Nachlaufphase des Steuergerätes wird ein vollständiger Checksum-Test der Programm- und Datenspeicher durchgeführt. Wird hierbei ein Fehler festgestellt, wird dies vermerkt und der komplette Test in der nächsten Initialisierungsphase des Steuergerätes wiederholt.

11. LOGISCHE ÜBERWACHUNGEN FUNKTIONSRECHNER

11.1. ABSICHERUNG MOMENTENBERECHNUNG

Der Hauptpfad der Momentenberechnung und alle auf ihn einwirkenden Offsetmomente anderer Module werden innerhalb des Momentenmanagers auf ihre Plausibilität hin überprüft. Wird ein unplausibler Wert erkannt, wird dieser Wert sofort in einen neutralen Wert umgewandelt und ein Fehlerfilter gestartet. Nach Ablauf der Fehlerfilterung wird die Egas-Überwachungsfunktion benachrichtigt, welche dann das Egas-System in die Notlaufstufe 2 - Notfahren über das Leerlaufstellersystem schaltet.

Bei den Wirkungsgradkorrekturen (Zündwinkel, Lambda) innerhalb des Momentenmanagers erfolgt nur eine Begrenzung des Wirkungsgrades nach unten, jedoch kein Fehlereintrag bzw. Wechsel in ein Notprogramm, da nicht ausgeschlossen werden kann, daß im normalen Betrieb der Grenzwert unterschritten werden kann.

Sicherheitsabfragen (Fehlerbedingungen):

- indiziertes Motorschleppmoment „md_ind_schlepp“ < 0
- minimales indiziertes Motormoment „md_ind_min“ > maximales indiziertes Motormoment „md_ind_max“
- Verlustmomentes des Motors > K_MD_SK_MAX_MDMIN oberhalb der Drehzahlschwelle K_MD_SK_N_MDMIN
- indiziertes Wunschmoment „md_ind_wunsch“ > Maximalmoment „K_MD_SK_MAX“
- Ausgang MD-Dynamikfilter > Maximalmoment „K_MD_SK_MAX“
- resultierendes Wunschmoment „md_ind_wunsch_red_korr“ > K_MD_SK_MAX
- Wunschmoment für Zündwinkelpfad „md_ind_wunsch_tz_red“ > K_MD_SK_MAX
- Sollfüllung „md_rf_soll“ > Maximalfüllung „K_MD_RFMAX“
- Lambda Abmagerungsfaktor > 2 (Überlauf)

Überwachung Momenteneingriffe

- Eingriff I-Anteil der Leerlaufregelung „md_llri“ > Maximaleingriff „K_MD_SK_LLR_MAX“
- Eingriff PD-Anteil der Leerlaufregelung „md_llrp“ > Maximaleingriff „K_MD_SK_LLR_MAX“

11.2. ÜBERWACHUNG SOLLMOMENT ZU ISTMOMENT

Eine Plausibilisierung des Istmomentes des Motors zum Fahrerwunschmoment über den gesamten Betriebsbereich ist nur sehr schwierig möglich, da in diesem Fall sehr viele Eingangsparameter, alle instationären Zustände, sowie alle Momenteneingriffe anderer Module mit berücksichtigt werden müßten. Dies würde erfordern, daß fast der komplette Berechnungspfad redundant nochmals abgelegt ist, was mangels Resourcen nicht möglich ist, oder die entsprechenden Toleranzgrenzen stark aufgeweitet werden müßten.

In der MSS54 wurden deshalb zwei Momentenüberwachungsfunktionen implementiert. Eine Funktion, welche das Istmoment mit dem Wunschmoment unter Berücksichtigung aller Momenteneingriffen vergleicht und über weiter gesteckte Toleranzgrenzen verfügt. Und über eine Momentenüberwachung, welche sich auf eine Nullmomentenvorgabe des Fahrers (PWG = Null) beschränkt, dort aber entsprechend scharf geschaltet ist. Dies hat den Vorteil, daß in diesem Betriebspunkt die Momentenberechnung wesentlich besser abgeschätzt werden kann, und somit die Tolernazgrenze somit enger gesteckt werden können. Ferner kann davon ausgegangen werden, daß der Fahrer, falls der Motor ein unerwünscht hohes Moment abgibt, automatisch vom Gas gehen wird und somit die Aktivierungsbedingungen für diesen Test erfüllt sind.

11.2.1. ÜBERWACHUNG SOLL-/ISTMOMENT ÜBER GESAMTEN BETRIEBSBEREICH

Definition des Istmomentes md_sk_vergl_ist =

	md_ind_ne	tatsächlich erzeugtes indiziertes Istmoment des Motor, ermittelt aus Kennfeld über Drehzahl und Last (n, rf) und ZW-Wirkungsgrad unter Berücksichtigung aller Eingriffe

Definition des Sollmomentes md_sk_vergl_soll =

	md_fw_filter	gefiltertes Fahrerwunschmoment aus PWG-Position oder Fahrgeschwindigkeitsregler
+	md_ind_min_ges	Verlustmomente des Motors incl. aller Verbraucher
+	md_ar	Eingriffsmoment der Antiruckelregelung
+	md_llri	Eingriffsmoment des I-Reglers der Leerlaufregelung
+	md_llrp	Eingriffsmoment des P-Reglers der Leerlaufregelung

Im Falle eines momentenerhöhenden MSR-Eingriffs wird das Maximum aus Anforderungsmoment und md_sk_vergl_soll aks Sollmoment verwendet.

Übersteigt das Istmoment des Motors das Sollmoment für den Zeitraum K_MD_SK_TIMER_MD um den Betrag K_MD_SK_OFFSET + (1 - K_MD_SK_GEWICHTUNG) * md_sk_vergl_ist, wird auf einen Fehler im Egas-System geschlossen und es erfolgt ein Wechsel in das Notprogramm 2 - Fahren über das Leerlaufstellersystem.

11.2.2. ÜBERWACHUNG SOLL-/ISTMOMENT BEI PWG-VORGABE = 0

Aktivierungsbedingung für die Überwachung

- Betriebszustand Motor läuft
- kein FGR-Betrieb
- kein MSR Eingriff
- Dashpotfunktion des Dynamikfilters abgeregelt
- Pedalwertvorgabe <= K_MD_SK_PWGMAX

Übersteigt in diesem Fall das errechnete Fahrerwunschmoment den Wert K_MD_SK_FWMAX oder die errechnete DK-Sollposition den Wert K_MD_SK_WDK_MDMIN für den Zeitraum K_MD_SK_TIMER, wird auf einen Fehler in der Momentenberechnung geschlossen und das Egas-System wechselt ebenfalls in das Notprogramm der Stufe 2.

12. LOGISCHE ÜBERWACHUNGEN SICHERHEITSRECHNER

Bei der Definition des Sicherheitskonzeptes wurde folgende Philosophie vertreten:

Alle Fehler in der Sensorik, Aktorik bzw. Momentenberechnung sollen vom Funktionsrechner selbst erkannt und durch entsprechende Maßnahmen ein unkritischer Zustand erreicht werden.

Die Aufgabe des Sicherheitsrechners besteht darin, den Funktionsrechner auf seine Betriebsfähigkeit zu überwachen, sofern seine eigenen Mechanismen dies nicht erkennen. Zu diesen Überwachungsfunktionen des Sicherheitsrechners gehören neben den bereits erklärten Kommunikationstests und der Resetüberwachung noch die Überwachung der Analog-/Digital-Wandler und des Rechnerkerns beider Prozessoren.

12.1. ÜBERWACHUNG ADC FUNKTIONSRECHNER

Dieser Test soll den Analog/Digital Wandler ADC eines jeden Prozessors auf seine Funktionalität hin überwachen. Dazu sind zwei Analogsignale - PWG1 und DKG1 - parallel an die ADC der beiden Prozessoren geführt, und werden von diesen zyklisch eingelesen. Die Wandler der beiden Prozessoren müßten somit das gleiche Ergebnis liefern.

Überschreitet die Differenz der beiden Ergebnisse einen Grenzwert für einen definierten Zeitraum, wird dies als Problem eines der AD-Wandler gedeutet, ein SG-interner Fehler abgelegt und in das entsprechende Notprogramm gewechselt.

Um die Laufzeitunterschiede zwischen den beiden Prozessoren zu berücksichtigen, wird der Test ausgeblendet, wenn beide AD-Wandler eine zu große Dynamik des Analogwertes erkennen.

Anmerkung: zur Zeit wird nur ein Analogsignal - PWG1 - für die Überwachung verwendet

12.2. ÜBERWACHUNG RECHNERKERN

Die Überwachung beider Rechnerkerne erfolgt mittels Testrechnungen, die parallel in beiden Prozessoren ausgeführt werden und deren Ergebnis vom Sicherheitsrechner auf Übereinstimmung kontrolliert werden.

Dazu sind sind zur Zeit 14 Testaufgaben mit folgenden Schwerpunkten definiert:

Testaufgabe	1:	Kennfeldinterpolation vom Typ unsigned short
	2:	Kennlinieninterpolation vom Tpy singed short
	3:	Kennfeldinterpolation vom Typ signed char
	4:	Kennlinieninterpolation vom Typ unsigned char
	5:	Fehlerfilterung
	6:	Fehlereintrag
	7:	Fehlerheilung
	8:	Fehleraustrag
	9:	CPU-Test: Schwerpunkt arithmetische und logische Operationen
	10:	CPU-Test: Schwerpunkt Bit-Operationen und Sprungbefehle
	11:	CPU-Test: Schwerpunkt Adressarithmetik
	12:	CPU-Test: unbenutzt
	13:	Tiefpaßfilter
	14:	unbenutzt

Diese 14 Testaufgaben werden zyklisch mit 11 unterschiedlichen Parametersätzen durchgerechnet, so daß sich in Summe 154 unterschiedliche Aufgaben ergeben.

Der Ablauf des Rechnerkerntest läuft prinzipiell nach folgendem Schema ab:

- der Sicherheitsrechner wählt eine Testaufgabe und einen Parametersatz aus
- der Sicherheitsrechner rechnet die Testaufgabe durch und speichert das Ergebnis ab
- die ausgewählten Aufgabe wird in Form einer Aufgabennummer und einer Parametersatz-nummer mittels IPK dem Funktionsrechner zur Bearbeitung übergeben
- der Funktionsrechner berechnet das Ergebnis der Testaufgabe und schickt dieses mit der Empfangsquittung der IPK an den Sicherheitsrechner zurück
- der Sicherheitsrechner vergleicht die beiden Ergebnisse

Eine Testrechnung gilt als fehlerhaft, wenn die Ergebnisse nicht übereinstimmen. In diesem Fall wird die Testaufgabe mit dem gleichen Parametersatz noch bis zu K_SK_TR_MAX-mal wiederholt. Sollten die Ergebnisse noch immer differieren, wird ein Fehler abgelegt und das System mittels eines Resets neu initialisiert.

Da durch diesen Mechanismus nur der Funktionsrechner durch den Sicherheitsrechner kontrolliert wird, wurde in diesen Test ein weiteres Feature implementiert, durch den der Funktionsrechner die Möglichkeit hat, auch die korrekte Abarbeitung der Überwachungsfunktion am Sicherheitsrechner zu gewährleisten. Dazu gibt der Funktionsrechner bewußt bei jeder K_SK_TR_MANIPULATION-ten Testrechnung ein falsches Rechenergebnis an den Sicherheitsrechner zurück. Dieser muß das falsche Ergebnis erkennen und die Testaufgabe mit dem gleichen Parametersatz wiederholen. Ist dies nicht der Fall, wird ebenfalls auf einen Fehler in der Programmabarbeitung geschlossen und das System mittels Reset zurückgesetzt.

Fehler in der Übermittlung der Testrechnung werden als Kommunikationsfehler behandelt.

12.3. ÜBERWACHUNG FGR-ABSCHALTUNG

Im FGR-Betrieb ist keine Plausibilisierung zwischen Fahrerwunsch (Gaspedalposition) und Istmoment des Motors möglich, da die Sollmomentenvorgabe vom Fahrgeschwindigkeitregler bestimmt wird und zwischen 0 und 100% der möglichen Motorleistung liegen kann. Um diesen Betriebszustand aber nicht von der Momentenüberwachung komplett ausschließen zu müssen, ist am Sicherheitsrechner eine Überwachungsfunktion implementiert, welche die Abschaltung des FGR bei betätigter Bremse kontrolliert.

Grundlage für die Überwachung ist die Annahme, daß der Fahrer auf ein ungewolltes Beschleunigen des Fahrzeugs im FGR-Betrieb mit dem Betätigen der Bremse reagieren wird. In diesem Fall muß der FGR-Betrieb sofort abgebrochen werden und die implementierten Vergleiche von Fahrerwunsch zu Istmoment werden wieder aktiv.

Diese Abschaltbedingung über die Bremsbetätigung wird vom Sicherheitsrechner überwacht. Erkennt dieser, daß trotz betätigter Bremse der FGR-Betrieb nicht abgebrochen wird, schließt dieser daraus, daß die FGR-Funktion am Funktionsrechner nicht mehr ordnungsgemäß läuft. Er legt somit einen Fehler im Fehlerspeicher ab und wechselt in das Notprogramm 4 - SG interner Fehler.