MSS54

module description

working version

Egas safety concept

(provisional)

	Department	Date	name	Filename
editor EE-221		5.12.03		3.05

.1201.04.20
13 12:30:00

1st GENERAL

2nd SECURITY CONCEPT HARDWARE

The design of the control unit hardware was specifically tailored to the needs of a safety-critical Egas system. It has a number of features that ensure seamless monitoring and a safe fail-safe of the Egas system.

Brief overview of design features

Two-processor system with two equivalent, powerful 32-bit processors

with the exception of the power supply, completely independent processors with their own clock supply and program/data storage

Use of a voltage regulator with reset trigger in case of undervoltage

Division of functionality under the premise that each processor has an independent ability to intervene in the torque output of the engine.

Function calculator:	Egas system, idle control system, ignition
Security calculator:	injection including speed limitation

Use of an H-bridge to control the Egas actuator with two shutdown paths, each of which is controlled by a processor.

Redundant distribution of the brake light switch to both processors

Redundant distribution of the two analog signals pedal sensor 1 and throttle valve sensor 1 to both processors

Use of a pedal value sensor with two potentiometers PWG1 and PWG2 with independent power supply and different characteristics.

Installation of two throttle valve sensors with independent power supply and crossed characteristic curve.

Dual 5V sensor supply. Reading back the supply voltage within the DME

Connection of the reset line of one processor to a port pin of the other processor. Port pin can be configured as interrupt input or output

3. SECURITY CONCEPT SOFTWARE

In order to ensure safe Egas operation, a series of software modules are implemented in the MSS54, which are designed to detect all possible SG-external (sensors, actuators, wiring harness) and SG-internal (processor, memory, drivers, power supply) errors and to transfer the system to a fail-safe state.

The monitoring modules can be divided into three levels:

Level 1:	Monitoring of the SG periphery (sensors or actuators)
Level 2:	Monitoring of control loops, setpoint specifications Plausibility check of mutually redundant information
Level 3:	Monitoring the control unit hardware and the proper program execution

The level 3 monitoring modules are implemented on both processors and run independently of each other, so that a failure of one computer unit does not pose a risk, since the parallel monitoring module still works perfectly.

Brief overview of the monitoring modules:

Sensory:	• Sensor supply Uext •	:	area monitoring
	Pedal value detection pwg •	:	area monitoring, channel comparison
	Throttle position wdk : • HFM load		area monitoring, channel comparison
	signal ml • Brake light	:	area monitoring
	switch system	:	channel comparison
actuators:	• Idle speed controller	:	electrical driver diagnosis
	• Egas servomotor	:	electrical driver diagnosis

Comparison tests: • Target/actual comparison of the throttle position
- Plausibility check of driver request torque to actual engine torque
- Plausibility check of load signal to throttle position (only in case of failure of one DK-Potis)

area monitoring:
- Plausibility check of the moment calculation including moment-increasing interventions
- Monitoring DK position at zero moment setting
- Monitoring FGR shutdown when brake is applied

Interface monitoring:
- CAN interface - bus error, telegram timeout
- DSC interventions - checking signal redundancy
- MFL interface - timeout, telegram format, key coding

Monitoring SG hardware:
- QADC : Result comparison of functional and security calculator
- Memory tests
- Test tasks for CPU monitoring

test procedures / system tests
- Pre Drive Check Egas System
- Program flow control
- Reset monitoring
- Communication monitoring function / security computer

4. PWG EMERGENCY OPERATION PROGRAMS

4.1. LEVEL A - PWG EMERGENCY DRIVING WITH A PWG SENSOR

Identification of the emergency program:
Unequivocally detected failure of a pedal sensor and thus loss of redundancy.

Prerequisite for PWG operation in Level A:
Remaining pedal sensor is plausible.
brake switch system is error-free
no internal control unit errors

Emergency program:

- Switching the pedal value progression characteristic to an emergency running progression characteristic.
- Limitation of the positive PWG dynamics by emergency filtering of the setpoint - slow Upstream filtering + fast downstream filtering
- Safety shutdown via brake light switch
  As soon as the brake is applied, a pedal value of zero is output. A new pedal value not equal to zero is only accepted again if the remaining pedal value sensor has returned to the value zero in the meantime.

Notes:

- Cruise control operation is still possible without restrictions.

4.2. LEVEL B - PWG EMERGENCY DRIVING WITHOUT PWG SENSOR

Identification of the emergency program:
Failure of both pedal sensors - a driver's request can therefore no longer be detected.

Prerequisite for PWG operation in Level A:
no sg-internal errors

Emergency program:

- Driver's request always zero
- Driving at idle speed

Notes:

- Cruise control operation is still possible without restrictions if the minimum speed for the FGR operation can be achieved.

5th EGAS EMERGENCY RUNNING PROGRAMS

5.1. LEVEL 1 - DK EMERGENCY DRIVING WITH A DK SENSOR

Identification of the emergency program:
Failure of a throttle valve sensor detected without doubt and thus loss of redundancy, or implausible DK values of the two sensors without having detected the defective sensor. In this case, the Egas position control uses the larger and therefore less critical value as the actual position of the throttle valve until the faulty sensor can be detected via the HFM plausibility check.

Prerequisite for DK operation in level 1:
Remaining throttle position sensor is plausible.
HFM works flawlessly.
Plausibility check of remaining DK value to HFM load signal OK
no internal control unit errors

Emergency program:
• Limitation of the duty cycle for Egas servo motor - limitation of the motor dynamics
• Limitation of the maximum motor torque •
Plausibility of remaining potentiometer via HFM load signal
• Blocking of internal filling-increasing interventions such as catalyst heating, torque reserve
• Limiting vehicle acceleration • Limiting
maximum speed

Notes:

5.2. STAGE 2 - EMERGENCY DRIVING VIA IDLE SPEED CONTROLLER SYSTEM

Identification of the emergency program:
The target position of the throttle valve can no longer be reliably adjusted because
• the actual position can no longer be detected due to a double error (DK1, DK2, HFM) or
failure of the sensor supply • the
actuator (driver, cable, servomotor, DK mechanism) has failed
• there is a problem with the throttle valve kinematics

Prerequisite for emergency operation in level 2:
at least one load signal available (HFM or a reliable throttle position)
no internal control unit errors

Emergency program:
• Switching off the actuator control and monitoring whether the throttle valves are closed.
• Limitation of the maximum engine torque •
Blocking of internal filling-increasing interventions such as catalyst heating, torque reserve
• Reducing the speed limit
• Limiting vehicle acceleration • Limiting
maximum speed

Notes:

5.3. STAGE 3 - EMERGENCY DRIVING VIA IDLE SPEED CONTROL SYSTEM WITH OPEN THROTTLE VALVES

Identification of the emergency program:
The air supply to the engine can no longer be controlled directly because, for example, the throttle valves are stuck in an open position. The driver's desired torque or engine speed must therefore be reduced to a desired level via ignition and injection.

As a rule, in this operation it can be assumed that there is a defect in the control of the throttle valves, but the actual positions can still be detected.

Prerequisite for emergency operation in level 3:
no SG-internal error

Emergency program:

• Switching off the actuator control.
• Limitation of the maximum engine torque •
Activation of the ignition angle intervention torque manager (intervention becomes active when the actual engine torque is above the desired torque).
• Activation of the injection suppression torque manager (intervention is activated when engine Actual torque is above driver's desired torque + max. allowed delta)
• Blocking of internal filling-increasing interventions such as catalyst heating, torque reserve
• Reducing the speed limit
• Limiting vehicle acceleration • Limiting
maximum speed

Notes:
This emergency program represents the worst-case scenario in Egas operation. The engine generates more torque than the driver wants and the vehicle could accelerate unintentionally. However, since switching off the engine is also considered to be extremely safety-critical, this emergency program is intended to maintain a very limited but still manageable engine operation.

5.4. STAGE 4 - EMERGENCY DRIVING VIA IDLE SPEED CONTROL SYSTEM DUE TO AN INTERNAL ERROR IN THE CONTROL UNIT

Identification of the emergency program:

One of the control unit's monitoring functions has detected an error within the DME, which means that correct execution of the program can no longer be guaranteed. Since the effects of the error cannot be predicted in this case, a series of parallel and independent measures are taken to ensure that the vehicle cannot accelerate too quickly inadvertently due to this error.

Prerequisite for emergency operation in level 4:

Emergency program:

• Switching off the actuator control.
• Limitation of the maximum engine torque • Activation of
the ignition angle interventions torque manager • Activation of the injection
suppression torque manager
• Blocking of internal filling-increasing interventions such as catalyst heating, torque reserve
• Reducing the speed limit
• Limiting vehicle acceleration • Limiting maximum speed

Notes:

By designing the DME as a two-processor system and dividing the air supply and fuel supply into one processor each, the DME is able to ensure safe emergency operation even in the event of a serious internal problem. Each processor is able to control the engine torque generated independently of the functionality of the other processor.

However, the drivability of the emergency program depends very much on the extent to which the functions required for engine operation, such as load sensing, ignition, injection, etc., can still run without errors.

6. TRANSITIONS TO EMERGENCY OPERATION PROGRAMS

As part of the Egas safety concept, a particular focus is on the transitions to the corresponding emergency running programs. While an emergency running program appears to be manageable with suitable countermeasures, the transitions always depend on the current driving situation. However, this is usually not known to the control system.

Switching off the engine or a sudden reduction in engine power is considered particularly critical, as this may provoke a safety-critical driving situation. Key points in this regard are: overtaking oncoming traffic, driving at the limit with abrupt load change reactions, loss of steering and braking power assistance.

Therefore, as part of the safety concept, an attempt is made to assess the driving condition and the driver's reactions to the best possible extent and thus to achieve a slower transition to the emergency running program that the driver can still control.

However, this is only possible to the extent that technology allows.

6.1. TRANSITION TO STAGE A - PWG EMERGENCY DRIVING WITH A PWG SENSOR

With the transition to stage A, a switch is made to a PWG emergency running progression characteristic, which can result in a jump to a smaller PWG setpoint and thus a load jump.

This negative pedal value jump is therefore not passed on directly to the torque manager, but the delta (current value - target value) is regulated in a ramp-like manner. Changes in the driver's position are passed on immediately and unfiltered. If the driver operates the brake or clutch during the regulation time, the pedal value zero is immediately output.

6.2. TRANSITION TO STAGE B - PWG EMERGENCY DRIVING WITHOUT PWG SENSOR

The transition to level B is analogous to the transition to level A.

6.3. TRANSITION TO STAGE 1 - DK EMERGENCY DRIVING WITH A DK SENSOR

The emergency program level 1 includes a torque limit and a limit on the Egas setpoint. Here, too, there should be no sudden jumps in the engine torque, but rather the engine torque should be reduced to the new setpoints in a gradient that the driver can control and estimate.

For this purpose, similar to stage A, the maximum torque is reduced in a ramp-like manner starting from the current engine torque to the maximum torque of the emergency running stage.

6.4. TRANSITION TO STAGE 2 - EMERGENCY DRIVING VIA IDLE SPEED CONTROLLER SYSTEM

The transition to the emergency program level 2 depends very much on the type of error. If, for example, there is a defect in the servomotor control, the throttle valves are automatically closed via springs without the DME having any influence on this.

If the signals from DK sensors 1 and 2 are implausible to each other, but the faulty sensor cannot be determined with certainty, it may also be necessary to switch off the servo motor immediately.

In cases where there is still feedback of the actual position and the target position can still be adjusted, the throttle valves are not closed abruptly, but rather via a ramp-like reduction (unless the driver requests otherwise). To do this, the target torque is reduced based on the actual torque of the engine until the target position for the throttle valves reaches zero. The servo motor is then switched off and the rpm and speed limit is activated.

6.5. TRANSITION TO STAGE 3 - EMERGENCY DRIVING WITH OPEN THROTTLE VALVES

The level 3 emergency program is activated when the actual throttle position exceeds the target throttle position for a defined period of time and the throttle valves could not be closed despite the servo motor being energized in the closing direction.

Since this case can lead to unwanted vehicle acceleration, the DME's reaction time to this error is relatively short. After a filter time of K_EDKSI_T_BL_AUF_R has elapsed, the torque interventions via ignition and injection are enabled to reduce the excess engine torque. If the error state is still present after the filter time K_EDKSI_T_BL_AUF_F has elapsed, the Egas system switches to emergency program level 3.

In this stage, analogous to the other transitions, an attempt is made to reduce the engine torque in a ramp-like manner and then the Egas adjustment bridge is switched off. The actual engine torque derived from the load signal is roughly adjusted to the driver's desired torque using partial firing and ZW retardation.

Driving operation - especially when the driver specifies zero torque and when the traction is interrupted - depends heavily on the actual position of the throttle valves and cannot be guaranteed.

6.6. TRANSITION TO STAGE 4 - EMERGENCY DRIVING WITH SG-INTERNAL ERROR

The level 4 emergency program is always activated when an internal control unit error is detected. Since the malfunction of the Egas system cannot be precisely predicted in these cases, the engine power is reduced to a safe minimum using redundant measures.

The driver of the servomotor is switched off by hardware from both processors via independent enable lines. The function computer (master processor) has two options for intervening in the engine's torque output: ignition and filling control. The monitoring processor also has an effective option for intervening: injection (partial firing or complete shutdown).

7th IMPLEMENTATION OF EMERGENCY OPERATION PROGRAMS

7.1. LIMITING INDICATED ENGINE TORQUE

In the emergency programs of levels 1 - 4, the driver's desired torque is limited to the value KL_MD_MAX_SK (x-axis = number of the emergency program). A transition function ensures that the limitation does not take effect suddenly, which can also cause a safety-critical driving condition, but rather, based on the current driver's request, this is regulated to the new target value using the ramp KL_MD_GRAD_SK. The regulation ends or is aborted when the target value is reached, the driver brakes or the DSC intervenes. If, however, the driver's request falls below the limit value, it is not aborted but continues in the background to allow the driver to briefly lift or change gear.

7.2. TORQUE REDUCTION VIA IGNITION ANGLE INTERVENTION

When an Egas emergency program of levels 3 or 4 occurs, the ignition angle intervention path of the torque manager is released. This calculates the current indicated torque that the engine delivers at the current operating point with its basic ignition angles from the relative filling measured by the HFM and the current engine speed. If the driver's desired torque falls below the current engine torque, the excess torque is compensated by retarding the ignition angle. A maximum of retarding is possible up to the defined minimum ignition angle tz_min, which can result in a torque reduction of up to 40%.

7.3. TORQUE REDUCTION VIA INJECTION BLANKING

In emergency program stages 3 and 4, a torque intervention is also released via the injection in parallel to the ignition angle intervention. The purpose of this intervention is to compensate for an excess of torque, which cannot be completely compensated by the ignition timing retardation, by partially firing the cylinders.

For this purpose, the minimum actual torque of the engine, which can be represented by means of the timing retardation, calculated from a speed-load map and the minimum timing efficiency, is set in relation to the driver's desired torque after taking all torque interventions into account. If the ratio falls below the value of one (md_sk_soll / md_sk_ist), individual cylinders are switched off via the injection and the engine's torque output is thus reduced in steps of 1/number of cylinders. The remaining excess torque can then be reduced again using the timing intervention.

The calculation and execution of the partial firing is the responsibility of the slave processor and is independent of the function computer except for the calculation of the actual torque.

7.4. LIMITING VEHICLE SPEED

implemented but not yet documented

7.5. LIMITING VEHICLE ACCELERATION

If the Egas system is in an emergency program of levels 1-4, the maximum longitudinal acceleration of the vehicle is limited to a value defined for this level. The current longitudinal acceleration is calculated by the DSC and transmitted to the engine control via CAN.

The acceleration limitation is designed as a PI controller. The P component is calculated from the characteristic curve KL_MD_SK_AX_P = f(delta_ax) and is weighted by the gear-dependent characteristic curve KL_MD_SK_AX_GANG. The step size of the I controller is calculated from the characteristic curve KL_MD_SK_AX_IPOS = f (delta_ax). If the vehicle acceleration falls below the permissible maximum value again, the I component is regulated to zero via the characteristic curve KL_MD_SK_AX_INEG.

7.6. LIMITING THE ENGINE SPEED

Another safety measure is to reduce the speed limit. For this purpose, a maximum speed is defined in the KL_N_MAX_SK characteristic curve for each emergency program level. If the engine speed exceeds this limit, all cylinders are immediately switched off via the injection system.

This safety mechanism also runs on the slave processor and is completely independent of the functional computer, since the processor also has its own speed detection.

7.7. LIMITATION OF EGAS ACTUATOR DYNAMICS

This measure actually only works in emergency program 1, since the control of the servomotor is switched off in all other emergency programs. It is intended to limit the dynamics of the servomotor by reducing the maximum control duty cycle and thus enable easier plausibility checks of the DK potentiometer via the HFM load signal.

7.8. SWITCHING OFF THE EGAS ACTUATOR

The Egas servomotor is switched off in parallel via three switch-off paths.

- fixed setpoint value = zero for Egas position controller
- Deactivating the enable line of the function calculator for the H-bridge
- Deactivating the enable line of the monitoring computer for the H-bridge

The effectiveness of the shutdown is monitored via the HFM load signal, in which the measured air mass must not exceed a limit value which is above the value achievable via the idle control system.

8. MONITORING SENSORS / INPUTS

8.1. ANALOG SIGNALS

8.1.1. ON-BOARD NETWORK VOLTAGE TERMINAL 87 (MAIN RELAY)

The on-board voltage connected via terminal 87 supplies most of the actuators and the SG's internal voltage regulators. The on-board voltage is recorded analogously and checked for min/max values.
During the boot process, where voltage drops can occur, the lower diagnostic threshold is set to 5V, since at this value the voltage regulator reset must be active and the processors can no longer run.

When the valid range is left, an error filter is started and the supply voltage is immediately set to a substitute value (protection of the ignition output stages).

Since the sensor supply is derived from the Kl87 on-board power supply voltage, if the main relay is activated with a time delay, there is a risk that the monitoring modules of the sensors are already active and will therefore detect a supply voltage or sensor error, which would result in a switch to the Egas emergency program. Therefore, the affected modules are only released when the supply voltages have been detected as being present. If the supply voltage is still not present after a defined period of time, a main relay error is detected.

8.1.2. SENSOR SUPPLY

The MSS54 has two separate 5V supply voltages Uext1 and Uext2 for the PWG and DKG potentiometers and HFMs. The sensor supply is read back and monitored in the control unit and taken into account when calculating the PWG and DK positions. If a supply voltage leaves the permissible range, an error filter is started. Until the error filter expires, the Uext value is limited to the minimum or maximum value. After the error filter expires, the Uext value is set to the substitute value and all sensors connected to this supply voltage are considered faulty.

If the sensor supply Uext 1 fails, the sensors PWG1, DKG1 and the HFM also fail, so that the Egas system switches to emergency running level A - emergency driving via a pedal value sensor and to emergency running level 2 - driving via idle speed adjuster (redundancy via HFM no longer exists).

If the sensor supply Uext2 fails, the sensors PWG2 and DK2 fail. The Egas system switches to emergency mode A and to emergency mode 1 - emergency operation with a DK sensor (redundancy provided via HFM).

8.1.3. PEDAL SENSOR

For safety reasons, the accelerator pedal position is detected redundantly. The pedal position sensor consists of two separate potentiometers with different characteristics and independent ground and voltage supplies.

The monitoring of the pedal value sensors is divided into two areas - the monitoring of each sensor channel and the comparison of the two pedal values.

Min/Max monitoring pedal value sensor pwg1 or pwg2

Monitoring is active as soon as the sensors are supplied with power. If the sensor voltage falls below a specified minimum threshold or exceeds a maximum threshold, the measured value is discarded and error filtering is started. After error filtering has finished, the sensor is marked as faulty.

Channel comparison pwg1 to pwg2

The channel comparison is designed to monitor the plausibility of the two pwg signals. If the difference between the pedal positions exceeds a limit, a PWG channel comparison error is detected and error filtering is started. The permitted difference depends on the value of the smaller pwg position in order to be able to treat differences close to idle differently than differences in the full load range.

decision matrix PWG monitoring

All diagnostic information relevant to the detection of the pedal value sensors is linked together using a decision matrix, and a PWG operating mode and a reference sensor are determined from this. The use of a matrix has the advantage that it is complete and easy to understand, and the corresponding software remains relatively simple and therefore testable.

The following diagnostic information is taken into account as input signal in the matrix:

- Error in sensor supply pwg1
- Error in sensor supply pwg2
- Range error pwg1 confirmed
- Range error pwg2 confirmed
- Error channel comparison in the filter
- Error channel comparison confirmed

The result of the decision matrix is one of three possible PWG operating modes:

- Mode 0 : PWG module error-free
- Mode 1 : failure of a PWG
  Switch to emergency program level A
- Mode 2 : failure of both PWGs
  Switch to emergency program level B

Special case: High impedance of a potentiometer at the lower reversal point

Deposits or abrasion of the slider track can cause high resistances at the lower reversal point, which leads to the sensor signal becoming smaller. This means that the zero point adaptation for this sensor is pulled downwards and the sensor signal may even move below the minimum value. Since this effect is only limited to the lower reversal point, but the sensor works properly in the remaining range, no emergency program should be activated in this case, but only an error log entry should be made for the workshop.

The PWG detection or monitoring behaves as follows in the case of high impedance at the reversal point: The zero point adaptation follows the decreasing sensor signal only up to a lower adaptation limit and then remains at this. In parallel, the PWG high impedance error is entered. Monitoring for the minimum value is deactivated as long as the second sensor signal is still in the idle range. When leaving the idle range, the other sensor must also leave the high impedance range. Otherwise, either a min/max monitoring error or a channel comparison error is detected.

Detailed description of PWG detection and monitoring: see **module description PWG**

8.1.4. HFM-SIGNAL

The hot film air mass meter is monitored via min/max thresholds within which the measured ML signal must lie.

However, a plausibility check of the HFM signal to the DK position during operation is not carried out, since the influences of air pressure, air temperature and Vanos (catalyst heating, Vanos errors) would require an excessive widening of the tolerance limits.

If a DK sensor fails, the remaining DK potentiometer is monitored using the HFM signal. This is easier in this case because the system is then in an emergency program and the engine dynamics are limited and the catalytic converter heating function is blocked. A Vanos error occurring in parallel could, however, still lead to the tolerance band being exceeded, which would only result in a change to an even more severe emergency program - emergency driving via the idle control system.

Min/max value monitoring:

Each calculated ML value of the HFM (in the 8-cylinder: individual values of the two HFMs) is checked for the defined min/max limits. If the measured value is outside the limits, it is discarded and the ml replacement value is used instead. In addition, an error log entry is made after the error filtering has been completed.

Comparison of HFM signal with substitute value

Prerequisite: error-free HFM , Error in DK system (failure of a sensor or error in channel comparison)

If a DK sensor failure is confirmed, the HFM signal is used to monitor the remaining potentiometer. If the DK channel comparison fails, an attempt is made to locate the faulty potentiometer using the HFM signal.

For this purpose, an RF substitute value is calculated for each DK sensor, taking into account the duty cycle of the idle speed controller, the intake air temperature and the ambient pressure. This substitute value is compared with the RF signal measured by the HFM. If the measured and calculated values are within a tolerance band, the DK value is considered plausible and a flag is set in a ring buffer with 16 entries. If the number of IO flags in the ring buffer falls below a specified threshold, the DK value is considered implausible and a change to emergency program 2 - emergency driving via the idle control system takes place.

The same applies if monitoring is not possible due to an HFM error that has already been detected.

8.1.5. THROTTLE VALVE POTENTIOMETER

For safety reasons, the throttle valve position is detected redundantly. Two separate throttle valve sensors with inverse characteristics and independent ground and voltage supplies are installed.

Since the throttle valve position represents the actual value for the Egas position controller and this immediately reacts to any faulty sensor values, special attention must be paid to throttle valve monitoring.

The monitoring of the throttle valve sensors is divided into two areas - the monitoring of each sensor channel and the comparison of the two throttle valve values.

Min/Max monitoring DK encoder dk1 or dk2

Monitoring is active as soon as the sensors are supplied with power. If the sensor voltage falls below a specified minimum threshold or exceeds a maximum threshold, the system immediately switches to the second measured value and starts error filtering. After the error filtering has finished, the sensor is marked as faulty and switches to emergency program level 1.

Channel comparison dk1 to dk2

The channel comparison has the task of monitoring the two DK signals for their plausibility with each other. If the difference between the DK positions exceeds a limit value, a DK channel comparison error is detected and error filtering is started. The permitted difference depends on the value of the smaller DK position in order to be able to treat differences close to idle differently than differences in the full load range.

The case where both DK signals are plausible on their own, but the difference between them is too great, proves to be extremely problematic. The procedure for PWG channel comparison - using the less critical (smaller) value - is not so simple in this case.

For safety reasons, the larger value for the actual position must be used when comparing the DK channels. However, if this is the incorrect value, this leads to an immediate closing of the throttle valves and thus to a spontaneous loss of engine power.

Therefore, an attempt is made to locate the faulty sensor signal by checking the plausibility with the HFM signal. If it is not possible to locate the faulty sensor, the larger value continues to be used as the actual value.

decision matrix DK monitoring

All diagnostic information relevant for the detection of the throttle valve sensors is linked together using a decision matrix, analogous to the PWG monitoring, and a DK operating mode and a control sensor are determined from this.

The following diagnostic information is taken into account as input signal in the matrix:

- Error in sensor supply dk1
- Error in sensor supply dk2
- Range error dk1 confirmed
- Range error dk2 confirmed
- Error channel comparison in the filter
- Error channel comparison confirmed

The result of the decision matrix is one of four possible DK operating modes:

- Mode 0 : DK module error-free
- Mode 1 : Error channel comparison - plausibility check with HFM signal not yet successful
  Switch to emergency program level 1
- Mode 1 : confirmed failure of a DK encoder
  Switch to emergency program level 1
- Mode 2 : failure of both DK sensors
  Switch to emergency program level 2

Special case: High impedance of a potentiometer at the lower reversal point

The problem with the potentiometer high impedances at the lower reversal point is with the throttle valves even more complicated than with the pedal value sensors. In order to avoid a critical state in the event of a line break, the signals must be wired internally in the SG with pull-up or pull-down resistors so that a larger value is recognized as the DK value.
For high-impedance reversal points, this means that too large DK positions are also detected here. The channel comparison would detect too large a deviation and the comparison with the HFM signal would identify the DK sensor with the high impedance as faulty. For safety reasons, one should not try to distinguish these cases from actually incorrect sensor signals, but rather switch off the sensor and switch to the emergency program level 1.

detailed description of DK recording and monitoring: see **module description DK**

8.1.6. COOLANT TEMPERATURE (ENGINE TEMPERATURE)

The engine temperature (engine outlet cooling water temperature) is used within the torque manager to calculate the drag torque. Since this is very dependent on the engine temperature, its influence on the Egas system should not be underestimated.

The engine temperature is monitored in two stages:

- Min/max limits
- Minimum engine temperature depending on starting temperature and engine running time

A further safeguard against short-term disturbances is a slow time constant of the low-pass filter.

In the event of an error, the oil temperature above an oil temperature threshold is used as a substitute value. Below the threshold or if the TOG fails at the same time, the intake air temperature is used as the starting value for a replacement value, which is then increased over a time ramp.

8.1.7. OIL TEMPERATURE

The influence of the oil temperature is similar to that of the engine temperature. The oil sump temperature is measured, but the engine inlet temperature is of interest for determining the friction torque.
Since the M engines have oil/water (8 cylinders) or oil/air heat exchangers (6 cylinders), the two temperatures differ greatly from each other. Therefore, models that take into account the influence of engine temperature, vehicle speed and air temperature are necessary to calculate the oil temperature.

The oil sump temperature is measured by the thermal oil level sensor TOG. This sensor delivers a PWM signal, the frequency of which transmits the oil level and the pulse duration of which transmits the oil temperature.
Naturally, this interface is relatively insensitive to interference.

The following mechanisms are active as monitoring:

- Timeout monitoring
- minimum or maximum pulse duration
- Min/max values of oil temperature

In case of error, the engine temperature is used as a substitute value (even if the engine temperature sensor fails)

8.1.8. INTAKE AIR TEMPERATURE

The characteristic maps for determining the actual and maximum torques of the engine are based on standard conditions (air temperature 20ÿC, air pressure 960mbar). When calculating the torques, the current air temperature is taken into account in the form of a correction factor.

The intake air is measured using an NTC sensor integrated in the HFM. Monitoring is carried out using a min/max value plausibility check. In the event of an error, a fixed replacement value is used and the correction factor for the torque calculation is set to 1.0.

8.1.9. AMBIENT PRESSURE

The influence of the ambient pressure on the moment calculation is analogous to that of the air temperature.

The air pressure is measured by a pressure sensor integrated in the MSS54 and transmitted via /Max thresholds are monitored. In the event of an error, a fixed replacement value is also used and the correction factor for the torque calculation is set to the value 1.0.

8.2. DIGITAL SIGNALS

8.2.1. BRAKE LIGHT SWITCH

The brake light switch has the following influences on the Egas system:

- Switch-off condition for the cruise control
- Safety function for PWG emergency driving
- Safety function in the Egas emergency program

Furthermore, the engine control unit for the DSC system checks the plausibility of the brake light switch and transmits the result to the DSC via CAN.

The information “brake applied” is available redundantly in the MSS54:

- Brake light switch function computer, digitally read
- Brake light switch safety computer, digitally read
- Brake test switch function computer, digitally read
- Brake light switch DSC, read via CAN (can be evaluated optionally)

As soon as one of the three or four switches signals the status "brake applied", it is considered to be applied (ORing - no majority decision). If the information differs for more than a defined period of time, the brake switch system is considered to be defective. The brake is considered to be permanently applied for the rest of the driving cycle and the brake switch system error is entered.

8.2.2. SWITCH FORCE LOCK

The power-lock switch basically consists of two switches connected in series - a clutch switch and a switch in the gearbox that detects the idle position. The switch's job is to detect a fully engaged or open drive train.

The influence of the switch is manifold. The condition “no frictional connection” is used as

- Switch-off condition for the cruise control
- Release condition for idle control
- Bridging the torque filter
- Locking condition for gear detection (no gear engaged)

The switch is monitored separately for the closed and open states. When the vehicle is stationary and the engine is running, the switch must not detect any traction. In overrun mode, however, the switch must detect traction if the engine speed remains above a threshold.

8.3. SERIAL INTERFACES

8.3.1. CAN

CAN bus line monitoring

The CAN controller directly monitors the CAN bus lines. It reads back each of the telegrams it sends and compares them. The received telegrams are also monitored for their telegram format and checksum. If errors are detected, an internal error register is incremented. After an error threshold is exceeded, the controller automatically disconnects from the CAN and signals this to the CPU via a status bit. This status bit is read out by the CPU cyclically every 100ms. In the event of an error, an error memory entry is made and the CAN controller

is reinitialized.

The fail save for the received messages is provided by a timeout monitoring if the CAN does not work again within the timeout period.

Timeout monitoring of received telegrams

The timeout monitoring controls the cyclical reception of CAN telegrams. If this does not happen for a telegram-specific period, an error log entry is made and the CAN variables of this telegram are set to neutral values.

The timeout monitoring is active as soon as
- Terminal 15 on
- and vehicle electrical system voltage > K_CAN_UBMIN
- and time since last undervoltage > K_CAN_ED_TSPERR
- and time since last SG initialization > K_CAN_ED_TSPERR

The following CAN telegrams are currently monitored

Telegram	sender	timeout value
ASC1	DSC	300ms
ASC2	DSC	300ms
ASC3	DSC	300ms
LWS1	steering angle sensor	300ms
INSTR2	instrument cluster	1000ms
INSTR3	instrument cluster	1000ms

In order to avoid an excessive number of error locations, only the absence of CAN telegrams ASC1, LWS1 or INSTR2 leads to error memory entries, since it is assumed that if a transmitter fails, all telegrams from this transmitter will be absent.

Plausibility of DSC torque interventions

Since the DSC can increase or significantly reduce engine power via the torque interface, the DSC interventions must be checked for plausibility. This is done using redundantly transmitted information that must be plausible to one another. Otherwise, an error filter is started, after which an error memory entry is made and any DSC intervention that may still be active is aborted.

The type of plausibility check corresponds to the scope required in CAN specifications 11H, Rev 1.4. The filter time for implausible interventions is 300ms. The alive counter for better monitoring of MSR interventions is supported by the DME (configuration parameter K_ASC_ALIVE), but cannot be used at present because the DSC3 from Bosch cannot provide it.

Aborting a DSC torque intervention

If the CAN fails, the ASC message times out or implausible interventions occur, any DSC torque intervention that may still be active is terminated after the error filtering has expired. MSR interventions (torque-increasing) are immediately aborted. ASC interventions (torque-reducing), on the other hand, are regulated up to the driver's desired torque via a ramp.

Protection against excessive interrupt load

The MSS54 operates on the receiving side using interrupt control. This means that every telegram received immediately results in a CPU action. This poses the risk that the program sequence in the engine control system can be severely impaired by a faulty CAN participant that is constantly transmitting. To protect against this, a maximum interrupt load per receiving channel has been defined; if this is exceeded, the receiving channel is switched off for the rest of the engine run.

8.3.2. MFL

The MSS54 has an integrated speed controller (FGR), which is operated by the driver via a multi-function steering wheel (MFL). The MFL itself contains four buttons for operating the FGR:

- On/Off
- Set/Accelerate
- Delay
- Resumptions

Communication between DME and MFL takes place via a unidirectional, serial one-wire interface. To secure communication and the transmitted data, the four button information is converted into redundant 7-bit information and expanded by a further 24 bits, the value of which is predefined. In order to be able to monitor the cyclical renewal of the information, another bit, the so-called toggle bit, which must change in a defined time frame, is added. In total, this results in a 32-bit data stream, which is sent cyclically from the MFL to the DME approximately every 20ms.

The MFL monitoring within the DME is thus able to check the interface for the following errors monitor:

- Telegram timeout
- Toggle bit error (no change in the defined time frame)
- Format error of the fixed 24 bits
- invalid combination of the 7-bit button information

If the DME detects one of these error states, error filters are started. After they have expired, an error memory entry is made and any active FGR operation is aborted.

For further information on the FGR module, see module description fgr.doc

9. MONITORING ACTUATORS / OUTPUTS

9.1. ACTUATOR (H-BRIDGE, ACTUATOR, DK-MECHANISM)

9.1.1. ELECTRICAL DRIVER DIAGNOSIS

The Motorola H-bridge, which controls the Egas servomotor, has a status output, which is evaluated by the function computer with each controller cycle. The H-bridge reports the following states via the status output:

- Undervoltage of the bridge supply
- Overtemperature
- Overcurrent
- Shutdown path function computer active
- Shutdown path safety computer active
- Interruption of shutdown path function computer
- Interruption of shutdown path safety computer

In all these cases, the H-bridge switches off automatically (the outputs become high-impedance) and must be reactivated by the function or safety computer.

Since under extreme operating conditions the conditions of undervoltage, overtemperature or overcurrent cannot be excluded, activation of the status output is only stored in the error memory. However, it has no effect on the operating mode of the Egas system, since the target
/Actual comparison of the Egas position covers all these cases.

9.1.2. TARGET/ACTUAL COMPARISON EGAS POSITION

Comparing the target position of the throttle valves with their actual position is one of the most important monitoring functions in the Egas safety concept. It can be used to identify the following errors:

- Processor modules
  - CTM module (processor): generates control duty cycle for actuator motor
  - Processor Port C: Direction of rotation of the servo motor
  - Processor Port C: Enable actuator function computer
  - Processor Port C: Enable actuator safety computer
- H-bridge actuator
  - H-bridge defect
  - Overtemperature shutdown
  - Current limiting H-bridge
  - Overcurrent shutdown H-bridge
- Wiring actuator
  - Line interruption
  - Short circuit to ground, Ub, or between the lines
- Actuator
  - Winding defect
  - Mechanical damage
  - Transmission damage
- DK kinematics

  - Mechanical damage

- Throttle valves
  - jammed flaps

- Throttle valve adaptation
  - Shift of the zero point
  - Displacement of the anchor point

Case 1: The throttle valves are to be opened above a threshold, but the valves remain closed.

Reasons:
processor module defective
H-bridge defective or temporarily switched off
Safety shutdown activated
actuator wiring
actuator defective
DK kinematics defective

Error detection:
Egas target position > K_EDKSI_POS_ZU + K_EDKSI_HYS_ZU
and Egas actual position < K_EDKSI_POS_ZU
for Time > K_EDKSI_T_ZU

Reaction: Switch to Egas emergency program level 2 - driving via idle speed control

Assessment: The throttle valves remain closed or are closed automatically via the spring assemblies without the control unit being able to influence this.
The torque reduction when the flaps are closed cannot be influenced either (critical condition for case 1). If the flaps are closed, it is possible to continue driving in the emergency program without any problems if it is ensured that the flaps can no longer open.

Case 2: The throttle valves should be closed, but remain slightly open.

Reasons:
Throttle valve is stuck or extremely stiff
slight twisting of the throttle valve control potentiometer
incorrect zero point adaptation

Error detection:
Egas target position =
0 and K_EDKSI_POS_ZU < Egas actual position < K_EDKSI_HYS_BL_AUF
for Time > K_EDKSI_T_SPALT

Reaction: no Egas emergency program - maintaining the current operating level
error log entry

Assessment: The fact that the throttle valves remain slightly open despite being closed using the servomotor indicates a major problem in the throttle control system, which justifies an error log entry. The limit K_EDKSI_HYS_BL_AUF is, however, set in such a way that it would result in an increased idle speed when idling, but is not considered to be safety-critical for driving and therefore no change to an Egas emergency program is necessary.

Note: By observing the speed at idle, a distinction could be made between a mechanical problem and an adaptation problem:
LL speed can be regulated: adaptation problem
LL speed too high : flap problem

Case 3: The throttle valves should be opened, the valves react but do not reach the setpoint.

Reasons:
H-bridge temporarily switched off
stiff DK system
Throttle valve stuck below target position
undervoltage

Error detection:
Egas target position - Egas actual position > K_EDKSI_HYS_U_SOLL
and K_EDKSI_POS_ZU < Egas actual position <= K_EDKSI_POS_N_GANZ
and ub > K_ED_UBMIN
for Time > K_EDKSI_T_U_SOLL

Reaction: Switch to Egas emergency program level 2 - driving via idle speed control

Assessment: Since the reliability of the Egas system can no longer be guaranteed, the flaps are deliberately closed and then the control is deactivated. If the flaps are stuck, a change to case 2 or 5 is possible as soon as the setpoint is below the actual value, or depending on the actual position also case 4 (do not open completely).

Case 4: At full load, the throttle valves do not open completely

Reasons:
Flaps at VL stop - incorrect adaptation
undervoltage

Error detection:
Egas target position - Egas actual position > K_EDKSI_HYS_N_GANZ
and Egas actual position > K_EDKSI_POS_N_GANZ
and ub > K_ED_UBMIN
for Time > K_EGAS_T_N_GANZ

Reaction:
no Egas emergency program
Switching the slope of the DK potentiometer characteristic to a defined maximum slope (actuator protection)
Start of a new VL adaptation in the follow-up
error log entry

Assessment: This case only results in a loss of performance in the full load range and is therefore not safety-critical. However, measures must be taken to protect the actuator.

Case 5: The throttle valves are stuck in the open position

Reasons:

Defective processor module - 100% control, wrong direction of rotation
H-bridge alloyed
Short circuit in actuator wiring
stiff DK system
Throttle valve stuck above target position

Error detection:

Egas actual position - Egas target position > K_EDKSI_HYS_BL_AUF for time > K_EDKSI_T_BL_AUF_R (detection and reaction time)
or time > K_EDKSI_T_BL_AUF_F (error filter time)

Reaction: After the detection time has elapsed, torque-limiting measures are immediately taken via ignition angle interventions and injection suppression due to the possible effects of the error.

After the error filter time has expired, the system switches to the Egas emergency program. Level 3 - Driving with open throttle

Assessment: In this case, the engine produces more power than the driver wants and this can lead to unwanted vehicle acceleration. This requires a quick response to this situation. However, the control unit has the option of throttling the engine power to a range specified by the driver by intervening in the ignition angle and suppressing cylinders.

9.2. IDLE ADJUSTER

The engines from M GmbH have a second air supply system, the idle speed adjuster system, which is independent of the Egas system. The maximum air flow through the idle speed adjuster is approx. 100 kg/h compared to the 1200 kg/h through the throttle valves. The maximum speed that can be achieved with this is approx. 3000 rpm when the engine is warm and the drive train is open, and the maximum speed in 6th gear, on a flat road and with a long starting distance is approx. 80 km/h.

The driving performance that can be achieved in this way is classified as being controllable by the driver, so that in the event of all errors - even those internal to the SG - emergency driving via the idle control system is still permitted.

The idle speed control system itself consists of a two-winding rotary control ZWD with one break and one make winding, which is connected to terminal 87 via a common supply line. If both windings are de-energized, an emergency air cross-section is set via an internal spring, which corresponds to an approximate control duty cycle of 30%.

The DME is controlled via two PWM signals, whereby the normally open winding is operated with the inverse signal of the normally closed winding. The drivers used for the control are diagnostic-capable and monitor the control line with regard to

- Line interruption
- Short circuit to ground
- Short circuit to Ub

After an electrical fault is detected, the ZWD control system reacts immediately. An error is stored in the DME error memory after an error filter has expired.

The reactions to all possible error combinations are intended to dampen the effects on motor operation as far as possible and are stored in a 4x4 matrix. If a control line is short-circuited to ground, the remaining winding is also fully energized, resulting in an effective control ratio of approx. 50%. If a line fails (interruption or short circuit to Ub), the remaining winding is operated with a minimum duty cycle and an opening cross-section in the range of the emergency air cross-section is established.

The distribution of the target filling between the idle speed actuator and throttle valve, as well as the calculation of the ml replacement values, takes into account the emergency running measures in the idle speed actuator control.

10. MONITORING CONTROL UNITS HARDWARE

10.1. PRE DRIVE CHECK CONTROL UNIT

10.1.1. MEMORY TESTS

During the initialization phase of the control unit, the two internal RAM memories of each processor are subjected to a complete read/write test. If a RAM error is detected, an error is immediately detected as an internal control unit error and the system starts in the level 4 emergency program.

A checksum check of the program and data memory is usually not carried out during the initialization phase of the control unit, since these tests would delay the engine start unacceptably.
However, if a corresponding error was noted in the previous operating cycle of the control unit, these tests are also carried out again in full in the initialization phase. If the error is confirmed by this, a switch to emergency program 4 also occurs.

For more information about the memory tests, see the module description: sk_check.doc

10.1.2. PROCESSOR SYNCHRONIZATION

The MSS54 is a two-processor system, with both processors taking over about 50 percent of the functionality of the motor control. Communication between the two processors takes place via a dual ported RAM (DPR). Furthermore, the two processors are linked via a high-priority interrupt line, which enables each processor to trigger a "non-maskable interrupt" for the partner.

A further security level consists in the reset inputs of the partner processors and ports being managed so that one processor can reset the other if necessary.

Processor synchronization during SG initialization

When initializing the control unit, there is a problem that the processors communicate via a dual ported RAM. However, since the individual software modules are already accessing values from the other processor when they are initialized, it must be ensured that the corresponding variables in the dual ported RAM are already pre-initialized with meaningful values. The DPR, on the other hand, cannot be initialized from one side, since if one processor is unexpectedly reset, it would also re-initialize the variables of the other processor.

Therefore, a synchronization level was introduced into the initialization phase of the individual processors to ensure that the processors do not start initializing the function modules until both sides have initialized their DPR variables.

Synchronization is implemented via the Inter-Processor Communication (IPK) module of the OSKAR operating system. The IPK is a communication channel secured by handshake mechanisms, checksum and timeout monitoring, which can transmit commands and data to the partner processor and receives an execution status feedback from it.

During initialization, each processor sends a synchronization request to the partner via the IPK. If the partner has already initialized its DPR sizes at this point, an OK status is reported back. If initialization has not yet taken place, no response is received. The sender of the synchronization request now waits for the OK status. If this is not recognized within the IPK timeout time of currently 32ms, it repeats the synchronization attempt up to four more times. If these remain unanswered, the processor initializes to the partner's DPR sizes with neutral values and continues the program flow. Motor operation remains blocked until communication between the two processors has been established.

If a processor is reset during operation, it must also synchronize itself again with the processor that is still running normally during initialization.

10.1.3. PRE DRIVE CHECK EGAS CONTROL UNIT

The Pre Drive Check of the Egas actuator has the following tasks.

- Phase 1: Zero point adaptation of the throttle potentiometer
- Phase 2: Checking the freedom of movement of the flaps and the Egas control circuit
- Phase 3: Checking the safety shutdown Egas of the monitoring computer and checking the return springs of the flaps

The Pre Drive Check is carried out after each power on of the control unit as soon as the supply voltage of the drivers and sensors is available.

Phase 1 is always carried out. In phases 2 and 3, the Pre Drive Check is aborted as soon as terminal 50 becomes active, the engine speed is not zero or the vehicle is moving.

Phase 1: Zero point adaptation of the throttle valve potentiometer

After each power-on of the control unit, an adaptation run is mandatory to determine the zero point position of the throttle valve potentiometers. This is necessary because the throttle valve sensor signal represents the actual value for the Egas control circuit and if the zero point adaptation is incorrect, the throttle valves may no longer be closed correctly or the throttle valve monitoring may be incorrectly diagnosed.

The adaptation takes place when the servo motor closes the throttle valves with a defined force. The potentiometer voltage is then measured several times and, if all measured values are plausible, the new zero point position for each throttle potentiometer is determined by averaging.

Details of the adaptation process can be found in the throttle valve module description.

Phase 2: Checking the freedom of movement of the flaps and the Egas control circuit

In phase 2, the freedom of movement of the throttle valves and the control behavior of the Egas control circuit are checked.

For this purpose, the target value egas_soll is set to the value K_PDR_EDK_SOLL. At the same time, the target/actual comparison of the Egas system and the diagnosis of the throttle valve potentiometers including the channel comparison are activated. After the waiting time K_PWD_T_PHASE2 has elapsed, the information from the corresponding monitoring modules is evaluated. If the Egas system is working correctly, the target position should be adjusted and all diagnostics should report an OK status.

In detail, the following diagnoses are evaluated for the Pre Drive Check - Phase 2:

- Target/actual comparison of the throttle valve position
- Sensor diagnosis DK1 encoder

- Monitoring sensor supply DK1
- Sensor diagnosis DK2 encoder
- Monitoring sensor supply DK2
- Channel comparison DK1/DK2 value

Table: Evaluation of diagnostic information Pre Drive Check

Should, is Comparison	channel comparison	diagnosis DK1	diagnosis DK2	Evaluation	branching into emergency program
0	0	0	0	system in order	---
0	x	0	1	failure DK2	Level 1
0	x		0	failure DK1	Level 1
0	1	1	0	DK1 to DK2 implausible	level 2
0	x	0 1	1	combination impossible	level 4
1	0	0	0	Actual position is not reached Actual position too small Actual position too large	level 2 level 3
1	1	0	0	Actual position is not reached DK1 to DK1 implausible	level 2
1	x	0	1	Actual position is not reached failure DK1	level 2
1	x	1	0	Actual position is not reached failure DK2	level 2
1	x	1	1	failure of both sensors	level 2

0 := OK
1 := faulty
x := not relevant

Phase 2 is immediately aborted if a start attempt is made (terminal 50 active or engine speed not equal to zero or vehicle speed not equal to zero).

Open points: Waiting time possibly depending on the engine temperature

Phase 3: Checking the safety shutdown and the closing springs

The task of phase 3 is to check the shutdown path of the safety computer for the H-bridge, as well as the closing springs of the throttle valves.

For this purpose, the function computer continues to specify the setpoint K_PDR_EDK_SOLL for the throttle valves. At the same time, the safety computer is requested to activate its shutdown path for the H-bridge. In an error-free state, the throttle valves should now be closed by the spring assemblies. If the actual position does not fall below a specified threshold within the time K_PDR_T_PHASE3, the setpoint is set to zero and the H-bridge remains switched off.

If the throttle valves can now be closed, the shutdown path does not work. An internal SG error is entered and the system branches to the Egas emergency program level 2. If the valves remain open, the safety shutdown is then deactivated again. If the valves can now be closed, the closing springs are defective. The corresponding error is entered and the system also branches to the emergency program level 2. If the valves remain open, the emergency program level 3 is activated.

Phase 3 is immediately aborted if a start attempt is made (terminal 50 active or engine speed not equal to zero or vehicle speed not equal to zero).

10.2. MONITORING THE CONTROL UNIT DURING OPERATION

10.2.1. MEMORY TESTS

During operation, the DME's program, data and variable memories are subjected to a permanent, cyclical test. The RAM memories are checked using a write/read test, while the ROM memories (program and data) are monitored using CRC16 checksums.

If an error is detected and confirmed, the system switches to emergency program 4 - SG internal error.

The DPR has a special position in the memory test. Since this memory is accessed asynchronously from two sides, a write/read test is not possible here. It is therefore not possible to detect faulty memory cells. The safety concept counteracts this by keeping the DPR free of safety-critical variables. This means that all variables relevant to filling the motor and thus to torque output are located in an internal memory of the processor, which is subject to the RAM test, and the DPR only has copies of these values, whereby the copies are only used for non-critical parts of the program.

In cases where a security-critical exchange of values via the DPR is necessary, this is not done directly by storing these values in the DPR, but via the checksum-protected transport mechanism of the inter-processor communication.

10.2.2. MONITORING HW INITIALIZATION

implemented but not yet documented

10.2.3. PROCESSOR COMMUNICATION

The monitoring of the processor communication and its operational readiness is carried out via two control functions.

A very simple but very effective monitoring function is to check that the two system timers are synchronized. To do this, each processor stores a copy of its system timer in the DPR.
If a processor does not detect any change in the partner processor's timer over a period of K_PCNTRL_TIMEOUT, this indicates a problem in its program execution and the system is reset and reinitialized.

A second, somewhat more complex control mechanism monitors the exchange of safety-critical variables via the IPK. As already mentioned, this exchange mechanism works with secured telegrams, whose security mechanisms include the following:

- Checking the telegram identifier
- Verification of the telegram checksum
- Confirmation of correct receipt of the telegram
- Return value of the evaluation function of the telegram to the sender
- Timeout monitoring on the sender side regarding receipt acknowledgement

If proper communication between the two processors is not established for a period of K_SK_IPK_TIMEOUT, the system is also reinitialized by means of a reset.

10.2.4. PROGRAM FLOW CONTROL

Each MSS54 processor has an internal hardware watchdog. This must be operated at least once within the watchdog time of one second from the background task (slowest task) and the 10ms task (most important task for the Egas system).

In order to ensure that all program parts relevant to the Egas system are executed, a program execution control was implemented in parallel to the hardware watchdog. This is called cyclically by the watchdog-monitored 10ms task and checks whether all functions relevant to the Egas system have been executed at least once within an applicable period of time.

This is implemented using a flag variable in which a bit is reserved for each function, and which is set when the function is executed. If the program flow control detects that one of these bits is not set, an error memory entry is made and the processor is reset. If this condition occurs several times during engine operation, the Egas system goes into the emergency program of level 2 -
Emergency driving via idle control.

The following modules are currently monitored:

Master processor:

- Pedal sensor detection
- Monitoring pedal sensor
- Throttle potentiometer detection
- Monitoring throttle valve potentiometer
- Target/actual comparison of Egas position
- Main function security concept

10.2.5. RESET MONITORING

A number of monitoring mechanisms are implemented in the MSS54 that trigger a reset and thus restart the system. Examples of such monitoring functions are:

- internal watchdog
- occurrence of an uninitialized interrupt
- Errors in program execution (Zero Device, Bus Error, Illegal Opcode, ...)
- Timeout in processor communication
- Errors in the test calculations
- Timeout in the program flow control

However, during normal operation the system should run without resets. However, if the system reset frequency exceeds a defined limit during an operating phase, this indicates a serious problem within the DME. However, since the cause of the problem and its effects cannot be predicted, a switch to the Egas emergency program 4 - SG internal error is made for safety reasons.

For reset monitoring, the reset line of each processor is connected to an interrupt input of the partner. This enables the partner to immediately recognize any reset of the partner, document it and take appropriate protective measures until the system is ready for operation again.

10.3. MONITORING THE CONTROL UNIT IN THE RUN-OFF PHASE

10.3.1. MEMORY TESTS

In each run-on phase of the control unit, a complete checksum test of the program and data memory is carried out. If an error is detected, this is noted and the complete test is repeated in the next initialization phase of the control unit.

11. LOGICAL MONITORING FUNCTION CALCULATOR

11.1. SECURING MOMENT CALCULATION

The main path of the torque calculation and all offset torques from other modules that affect it are checked for plausibility within the torque manager. If an implausible value is detected, this value is immediately converted to a neutral value and an error filter is started. After the error filtering has been completed, the Egas monitoring function is notified, which then switches the Egas system to emergency running level 2 - emergency driving via the idle control system.

When making efficiency corrections (ignition angle, lambda) within the torque manager, the efficiency is only limited downwards, but no error entry or change to an emergency program occurs, since it cannot be ruled out that the limit value may be undercut during normal operation.

Security queries (error conditions):

- indicated engine drag torque “md_ind_schlepp” < 0
- minimum indicated engine torque “md_ind_min” > maximum indicated engine torque "md_ind_max"
- Loss torque of the motor > K_MD_SK_MAX_MDMIN above the speed threshold K_MD_SK_N_MDMIN
- indicated desired torque “md_ind_wunsch” > maximum torque “K_MD_SK_MAX”
- Output MD dynamic filter > maximum torque “K_MD_SK_MAX”
- resulting desired moment “md_ind_wunsch_red_korr” > K_MD_SK_MAX
- Desired torque for ignition angle path “md_ind_wunsch_tz_red” > K_MD_SK_MAX
- Target filling “md_rf_soll” > Maximum filling “K_MD_RFMAX”
- Lambda lean factor > 2 (overflow)

monitoring torque interventions

- Intervention I-part of the idle control “md_llri” > maximum intervention “K_MD_SK_LLR_MAX”
- Intervention PD component of the idle control “md_llrp” > maximum intervention “K_MD_SK_LLR_MAX”

11.2. MONITORING TARGET TORQUE TO ACTUAL TORQUE

It is very difficult to verify the plausibility of the actual torque of the engine in relation to the driver's desired torque over the entire operating range, since in this case a large number of input parameters, all non-stationary conditions, and all torque interventions from other modules would have to be taken into account.
This would require that almost the entire calculation path be stored redundantly, which is not possible due to a lack of resources, or the corresponding tolerance limits would have to be greatly expanded.

Two torque monitoring functions have therefore been implemented in the MSS54. One function compares the actual torque with the desired torque, taking all torque interventions into account, and has wider tolerance limits. And one torque monitoring function that is limited to a zero torque specified by the driver (PWG = zero), but is activated accordingly. This has the advantage that the torque calculation can be estimated much better at this operating point, and the tolerance limit can therefore be set more narrowly. It can also be assumed that if the engine delivers an undesirably high torque, the driver will automatically take his foot off the accelerator, thus fulfilling the activation conditions for this test.

11.2.1. MONITORING DESIRED/ACTUAL TORQUE ACROSS THE ENTIRE OPERATING RANGE

Definition of the actual moment md_sk_vergl_ist =

md_ind_ne   actually generated indicated actual torque of the engine, determined from the characteristic map over speed and load (n, rf) and ZW efficiency under consideration of all interventions

Definition of the target torque md_sk_vergl_soll =

md_fw_filter   filtered driver request torque from PWG position or cruise control

+ md_ind_min_ges +   Loss torques of the engine including all consumers
md_ar +   intervention moment of the anti-jerk control
md_llri +   intervention torque of the I-controller of the idle control
md_llrp   intervention torque of the P-controller of the idle control

In the case of a torque-increasing MSR intervention, the maximum of the requested torque and md_sk_vergl_soll as the target torque is used.

If the actual torque of the engine exceeds the target torque for the period K_MD_SK_TIMER_MD by the amount K_MD_SK_OFFSET + (1 - K_MD_SK_GEWICHTUNG) * md_sk_vergl_ist, it is concluded that there is an error in the Egas system and a change is made to emergency program 2 - driving via the idle control system.

11.2.2. MONITORING DESIRED/ACTUAL TORQUE WITH PWG SPECIFICATION = 0

activation condition for monitoring

Operating state Engine running
no FGR operation
no MSR intervention
Dashpot function of the dynamic filter reduced
Pedal value specification <= K_MD_SK_PWGMAX

If in this case the calculated driver request torque exceeds the value K_MD_SK_FWMAX or the calculated DK target position exceeds the value K_MD_SK_WDK_MDMIN for the period K_MD_SK_TIMER, an error in the torque calculation is concluded and the Egas system also switches to the emergency program of level 2.

12. LOGICAL MONITORING SECURITY COMPUTER

The following philosophy was used in defining the security concept:

All errors in the sensors, actuators or torque calculation should be detected by the function computer itself and a non-critical state should be achieved by taking appropriate measures.

The task of the safety computer is to monitor the functional computer for its operational capability, provided that its own mechanisms do not detect this. In addition to the communication tests and reset monitoring already explained, these monitoring functions of the safety computer also include monitoring of the analog/digital converters and the computer core of both
processors.

12.1. MONITORING ADC FUNCTION CALCULATOR

This test is intended to monitor the functionality of the analog/digital converter ADC of each processor. For this purpose, two analog signals - PWG1 and DKG1 - are fed in parallel to the ADC of the two processors and are read in cyclically by them. The converters of the two processors should therefore deliver the same result.

If the difference between the two results exceeds a limit value for a defined period of time, this is interpreted as a problem with one of the AD converters, an internal SG error is stored and the system switches to the corresponding emergency program.

In order to take into account the runtime differences between the two processors, the test is hidden if both AD converters detect too large a dynamic range of the analog value.

Note: currently only one analog signal - PWG1 - is used for monitoring

12.2. MONITORING COMPUTER CORE

Both computer cores are monitored by means of test calculations that are executed in parallel in both processors and whose results are checked for consistency by the security computer.

For this purpose, 14 test tasks have currently been defined with the following focus areas:

Test task 1: 2: 3: 4: map interpolation of type unsigned short
Characteristic interpolation of the type singed short
map interpolation of type signed char
Characteristic interpolation of type unsigned char
error filtering
error entry
error healing
error reporting
CPU test: focus on arithmetic and logical operations
5: CPU test: Focus on bit operations and jump instructions
6: CPU test: Focus on address arithmetic
7: CPU test: unused
8: low-pass filter
9: 10: 11: 12: 13: 14: unused

These 14 test tasks are calculated cyclically with 11 different parameter sets, resulting in a total of 154 different tasks.

The computer core test basically follows the following pattern:

- the safety computer selects a test task and a parameter set
- the security computer calculates the test task and saves the result
- the selected task is transferred to the function computer for processing in the form of a task number and a parameter set number using IPK
- the function calculator calculates the result of the test task and sends it with the Receipt of IPK back to the security computer
- the safety calculator compares the two results

A test calculation is considered faulty if the results do not match. In this case, the test task is repeated up to K_SK_TR_MAX times with the same parameter set. If the results still differ, an error is stored and the system is reinitialized by means of a reset.

Since this mechanism only controls the functional computer through the safety computer, an additional feature was implemented in this test, which enables the functional computer to also ensure the correct processing of the monitoring function on the safety computer.
To do this, the function computer deliberately returns an incorrect calculation result to the safety computer for each K_SK_TR_MANIPULATION test calculation. The safety computer must recognize the incorrect result and repeat the test task with the same parameter set. If this is not the case, it is also assumed that there is an error in the program processing and the system is reset.

Errors in the transmission of the test invoice are treated as communication errors.

12.3. MONITORING FGR SHUTDOWN

In FGR mode, no plausibility check is possible between the driver's request (accelerator pedal position) and the actual torque of the engine, since the target torque is determined by the speed controller and can be between 0 and 100% of the possible engine power. In order not to have to completely exclude this operating state from torque monitoring, a monitoring function has been implemented on the safety computer, which controls the shutdown of the FGR when the brake is applied.

The basis for the monitoring is the assumption that the driver will react to an unintentional acceleration of the vehicle in FGR mode by applying the brake. In this case, FGR mode must be aborted immediately and the implemented comparisons of driver request to actual torque become active again.

This shutdown condition via brake application is monitored by the safety computer. If it detects that the FGR operation is not aborted despite the brake being applied, it concludes that the FGR function on the function computer is no longer running properly. It therefore stores an error in the error memory and switches to emergency program 4 - SG internal error.