Swedish Defence Research Establishment
Department of Information Technology
P.O. Box 1165
S-581 11 LINKÖPING
SWEDEN

FOA report
E 30010-3.3
May 1988
ISSN 0281-9937

RISK ASSESSMENT OF CRUISE CONTROL

Mats Gunnerhed

Project No: 53338511
Distribution: TSV, ESRIN, NTIS
FOA 3: 300, 301, 314, 380

Issuing organization

Swedish Defence Research Establishment
Department of Information Technology
P.O.Box 1165
S-581 11 LINKÖPING
SWEDEN

Document name and doc. ref. No.
FOA Report E 30010-3.3

Date of issue
May 1988

Item designation

Project name (abbrev. if necessary)

Author

Mats Gunnerhed

Initiator or sponsoring organization
Swedish Road Safety Office

Project manager
Mats Gunnerhed

Scient. and techn. responsible
Mats Gunnerhed

Document title

RISK ASSESSMENT OF CRUISE CONTROL

Abstract

With the wider use of electronic devices and systems in cars, the safety implications of electronic systems have become evident. According to reports from USA, numerous lethal accidents have occurred due to sudden acceleration. Accidents in Sweden have also been reported.

At the request of the Swedish Road Safety Office, the Swedish Defence Research Establishment has carried out a risk assessment of a cruise control system in order to establish its safety performance. This system, made by HELLA, is an optional device in many common cars. It comprises electronic as well as mechanical and pneumatic subsystems.

By means of reliability analysis methods such as Fault Tree Analysis and Fault Modes and Effects Analysis, some single-point-fault modes are disclosed.

The risk assessment, verified in tests, shows that a single fault such as a bad solder joint causes sudden acceleration. This means that the alleged events are possible. This disclosed single-point-fault mode establishes an upper limit for the safety of this cruise control.

Key words
Car, reliability, risk analysis, cruise control, electronic, safety, single point fault mode, acceleration

Further bibliographic information

Language English

This is an English version of FOA report E 30009-3.3

ISSN 0281-9937

ISBN

Pages 33 p

Price SEK 100:-

( ) restricted distribution

Distributor (if not issuing organization)

Dokumentets utgivare

Försvarets Forskningsanstalt
Huvudavd. för Informationsteknologi
Box 1165
581 11 LINKÖPING

Dokumentnamn och dokumentbeteckning
FOA Rapport E 30010-3.3

Dokumentets datum
Maj 1988

Uppdragsnr.
53338511

Projektnamn (ev förkortat)

Upphovsman

Mats Gunnerhed

Uppdragsgivare
Trafiksäkerhetsverket

Projektansvarig
Mats Gunnerhed

Fackansvarig
Mats Gunnerhed

Dokumentets titel

RISKANALYS AV FARTHÅLLARE

Huvudinnehåll

Elektronik ersätter i snabb takt äldre teknik i bilar. Detta har dock ifrågasatts från säkerhetssynpunkt. Enligt rapporter, främst från USA, har ett stort antal olyckor inträffat p g a plötsligt accelererande bilar. Även i Sverige har sådana olyckor rapporterats.

Trafiksäkerhetsverket har därför lagt ett uppdrag på Försvarets Forskningsanstalt i avsikt att klarlägga säkerhetsnivån i en s k farthållare, som utgör ett exempel på en säkerhetskritisk utrustning. Den undersökta farthållaren, som är av fabrikat HELLA, förekommer på flera vanliga bilfabrikat. Den innehåller förutom elektronik också mekanik och pneumatik.

Analysen har utförts med hjälp av metoder från området tillförlitlighetsteknik såsom "Felträdsanalys" och "Feleffektanalys".

Analysen, som kompletterats med praktiska prov, visar att det räcker att man får ett enda fel för att bilen ska "skena". Felmöjligheten, som inte framgår av elektronikschemat, kan t ex utgöras av en dålig lödning eller av ett avbrott i en ledare på kretskortet. De plötsliga accelerationer, som påstås ha inträffat, är alltså inte alls omöjliga. Upptäckten innebär att en övre gräns fastställts vad beträffar farthållarens säkerhetsnivå.

Nyckelord
Bilar, tillförlitlighet, riskanalys, farthållare, elektronik, säkerhet, enkelfel, acceleration

Övriga bibliografiska uppgifter

Språk Engelska

Detta är en engelsk version av FOA rapport E 30009-3.3

ISSN 0281-9937

ISBN

Omfång 33 sidor

Pris SEK 100:-

Begränsad distribution

CONTENTS

1 BACKGROUND

Car manufacturers try to facilitate driving and to make driving safer. Today even advanced ideas can be realized at reasonable costs by means of modern electronic circuits.

However, the use of sensible electronics in cars has become questioned. In the US, several mishaps due to cars suddenly accelerating have been reported. Also in Sweden, some events of this kind have occurred. Given this background, the Swedish Road Safety Office, TSV, has assigned the Swedish Defence Research Establishment to carry out a risk assessment of a cruise control in order to establish its safety level.

Experience tells us that failures will occur in equipment as complex as a cruise control. Most failures will certainly be harmless but some may lead to unacceptable consequences.

Faults can be permanent or intermittent. Among the latter are malfunctions caused by electromagnetic fields emanating from other equipment in the car or from the outside environment. Disturbances, however, will not be dealt with in this report.

A rough way to grade the safety of a system is to count the number of component failures necessary to make the system break down in a hazardous way. If it can be shown that a single, credible, failure is enough for system failure, then the safety level of the system must be questioned. A corresponding level of safety is not accepted for airplanes.

2 RISK ASSESSMENT OF CRUISE CONTROL

2.1 Introduction

This assessment was aimed at defining system features which could affect road safety. The system investigated was made by HELLA and is an optional device in many cars of different manufacture.

SYSTEM DESIGNATION: HELLA GR-Steurgerät 12V 5GA 003 828-00

DOCUMENTATION: -Schaltplan GR-Steurgerät 12V 5GA 003 828-00, 431 907 305C
(A micro processor version exists, designated 5GA 004 397-00, 443 907 305. The two versions are fully interchangeable.)

-Pneumatic Cruise Control, Design and Function

The cruise control holds the car at a preset speed. It is said in the description of design and function that: "The automatic cruise control permits long distance concentrated driving without getting tired. Therefore it is no luxury but an essential safety factor."

This statement may be true when the system works as intended, but what will happen when it breaks down? Experience shows that it is unrealistic to expect technical equipment to work as intended for ever. Failures will occur. Therefore the effects of failures on the conduct of the car have been investigated. Faults may contribute to accidents.

This assessment was started from scratch i.e. it was not taken for granted that the system could create hazards at all.

2.2 Causes of malfunction

In principle, there are two causes of malfunction:

1. COMPONENT FAULTS; Permanent or intermittent

2. DISTURBANCIES; From the car itself or from the environment

A system should only be accepted if the following requirements are fulfilled:

1. The system design is such that any credible component fault will not result in traffic hazard.

2. With regard to road safety, the system is insensitive to electromagnetic interference during its lifetime.
   Comment: The EMI emission in society tends to grow.

This assessment only considers component faults.

The assumption that component failures will occur does not imply that the system is unsafe. The interesting matter is the consequences of failures i.e. the fault effects. Obviously, a fail-safe# behaviour is desirable.

Definition of fail-safe:

A designed property of an item which prevents its failures from resulting in critical faults.

3. FAULT TREE ANALYSIS

3.1 System Description

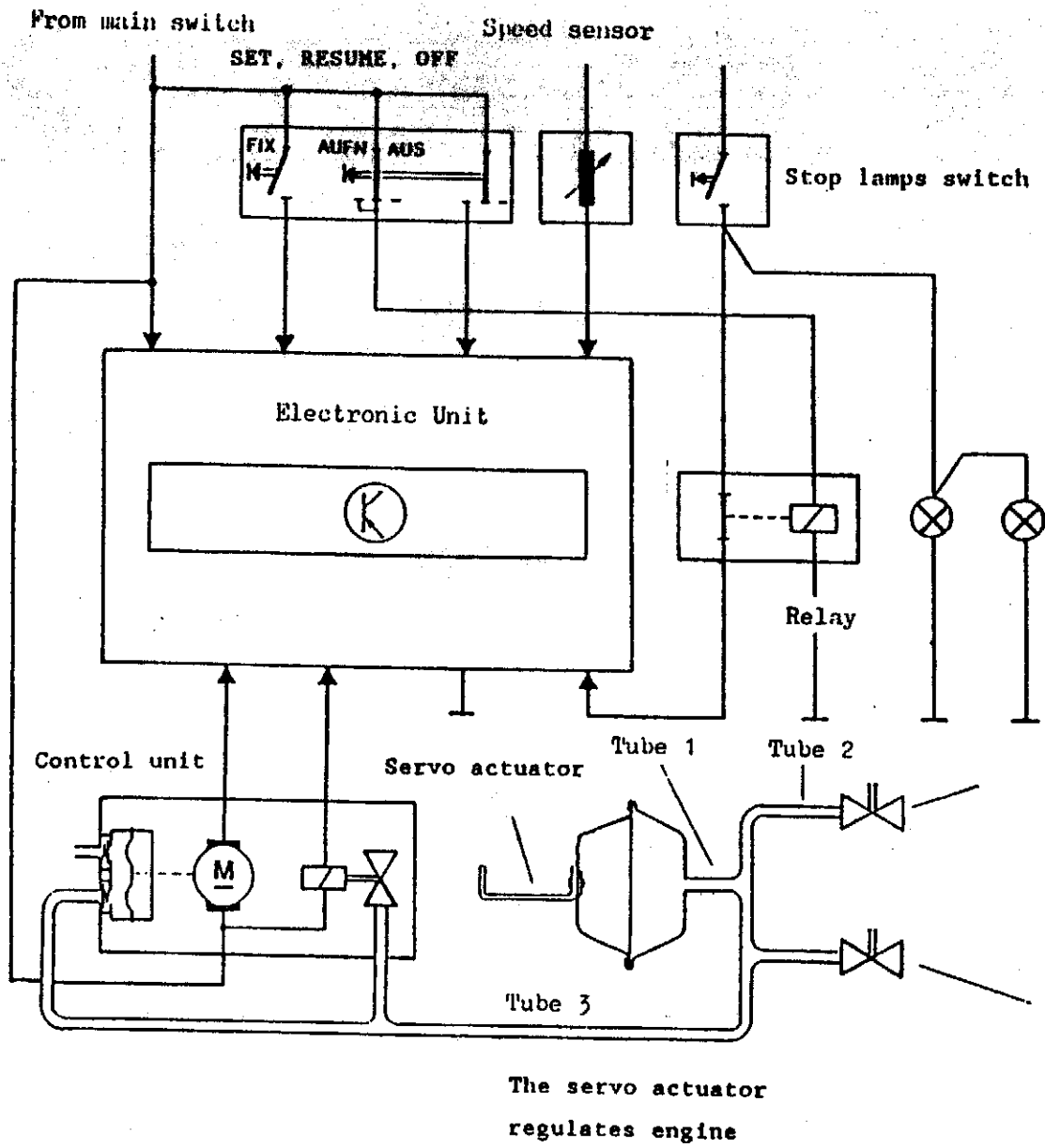
The investigated cruise control is based on pneumatics and electronic circuitry. The actuator, which consists of rubber bellows, is pneumatically controlled by an electric pump. The pump motor is controlled by means of an electronic regulator. See figure 1.

The cruise control is equipped with a 3-position switch; OFF, ON and RESUME (spring-loaded). There is also a SET switch. By pressing RESUME, the stored speed is resumed after brake pedal actuation.

The speed sensor tells the actual speed

he electronic unit ont inously compares ctual speed with esired speed and egulates car engine is the control unit

he control unit receives mpulses from the elec- ronic unit and creates a orresponding partial vacuum



The brake pedal quick valve lets air into the system when the brake pedal is depressed and disengages the cruise control

Clutch quick valve (only for manually geared cars)

The servo actuator regulates engine

Figure 1. The Cruise Control.

3.2 Methods

In order to disclose possible weaknesses in the cruise control, fault trees have been constructed. Fault Tree Analysis is an important risk analysis method. Starting out from a hazardous event, possible causes to this Top Event are searched for. The relationships are described by means of logic gate symbols. (For fault tree symbols see APPENDIX 1.) The analysis is continued down to a level where further dissolution is not motivated.

All risks associated with the object must be covered by top events.

Every top event has to be analyzed separately.

The assessment has been complemented by Fault Modes and Effects Analysis. FMEA is an inductive analysis that systematically details, on a component-by-component basis, all possible fault modes and identifies their resulting effects on the system.

3.3 Prerequisites

This analysis is valid for a car equipped with automatic transmission. In the fault trees it has been anticipated that:

1. Car engine is running

2. Cruise control switch ON

3. Gear: Drive or 2

It is supposed that many drivers leave the control switch in the ON-position even when they do not intend to use the device. Obviously this does not affect normal driving. The cruise control is automatically deactivated when the brake pedal is depressed and it is not reactivated until the driver gives a certain command.

3.4 Start

The following top events have been chosen:

1. The cruise control is not deactivated by braking

2. Unintended throttle increase

3.5 Comments on the top events

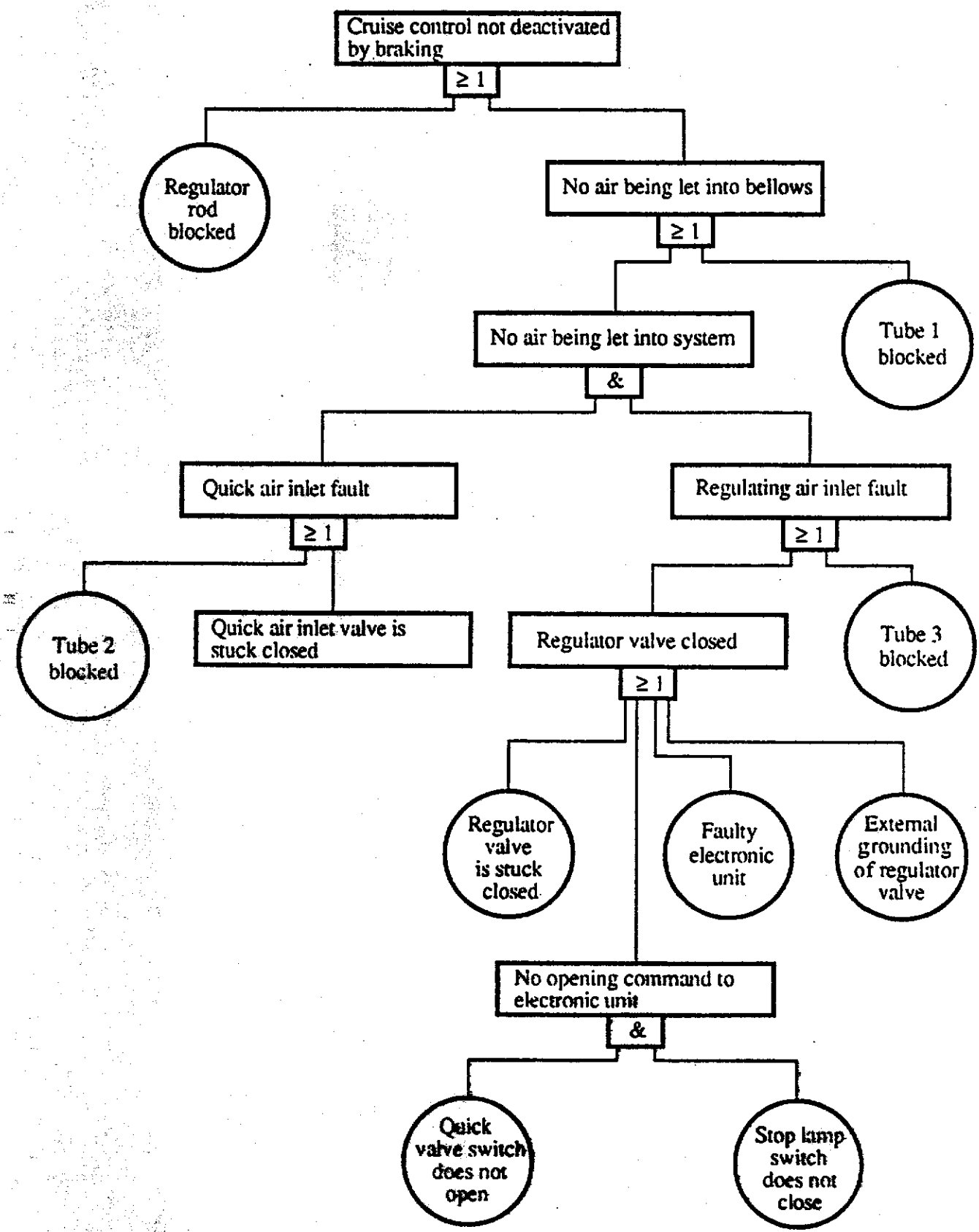
Top event 1, the cruise control is not deactivated by braking, can lead to a collision with other retarding vehicles or suddenly appearing obstacles due to cruise control counteraction with the brakes. (See 5. VERIFICATION.)

Top event 2, unintended throttle increase, requires that the cruise control switch is ON. Unintended acceleration can lead to collision with a vehicle ahead or other obstacles if the driver does not manage to stop the car in time.

A particularly interesting case is when the cruise control unintendedly accelerates the car from standstill.

From a general point of view, surprise must be considered hazardous in itself. Even if the driver always has the possibility to stop the car by depressing the brake pedal, he might "freeze" and be unable to react in time.

3.6 Fault tree for top event 1: The cruise control is not deactivated by braking



3.6.1 Comments on top event 1

As shown in the fault tree, either a stuck regulator rod or no air being let into the bellows when depressing the brake pedal would be sufficient to cause the top event.

Possible causes to prevent air let into the bellows are stoppage in tube 1 or no air passing into the pneumatic system via any valve.

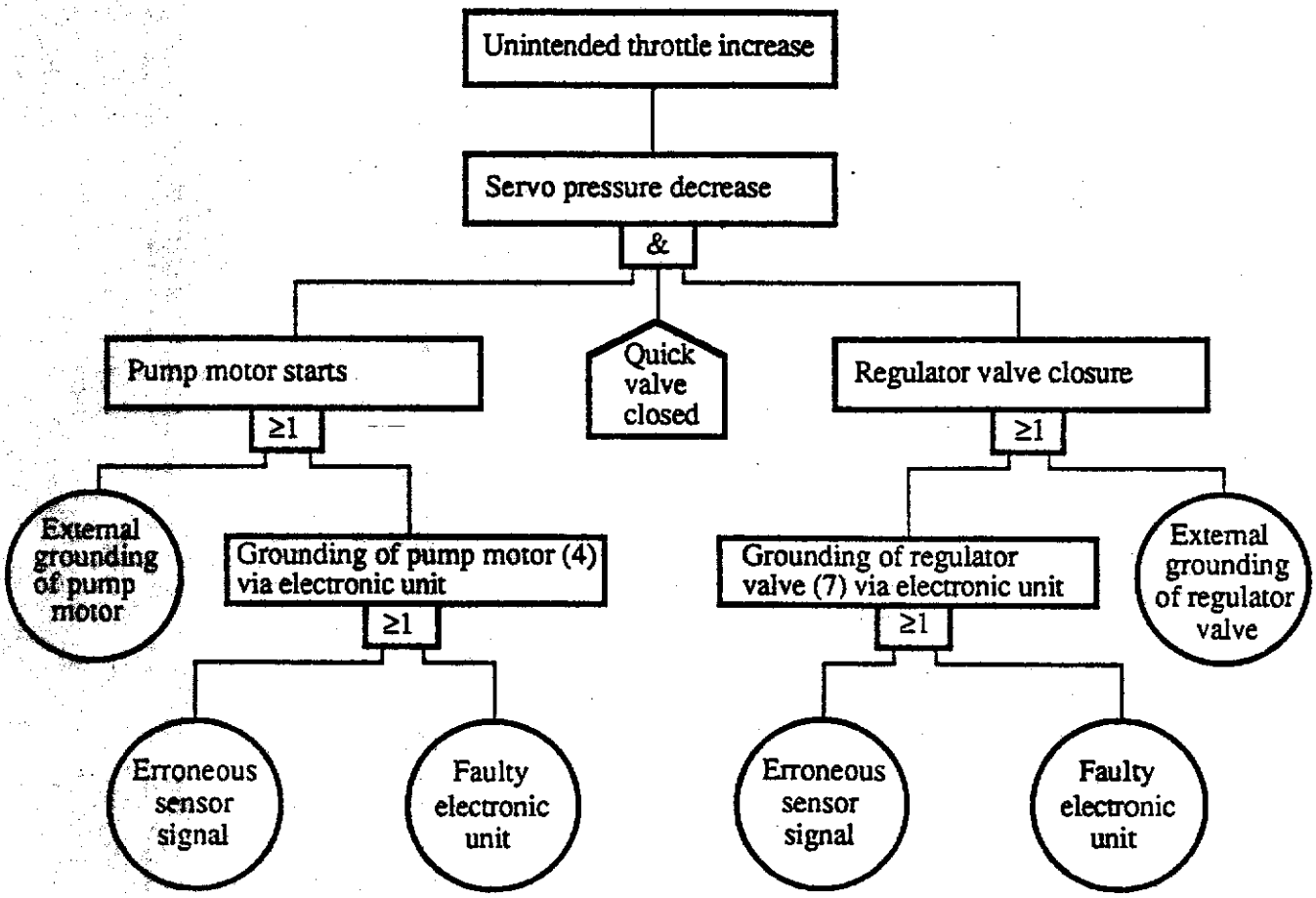
When the brake pedal is depressed, the regulator valve is opened whereby the bellows are inflated even if the quick valve should be stuck. The capacity of the regulator valve is not known. Therefore possible delay cannot be known either. Actual system behaviour should be tested.

The quick valve is not forced to open by the brake pedal. Thus, it can get stuck in closed position. Faults in the electronic regulator alone cannot lead to the top event. If the system works as intended, the brake pedal will override the cruise control.

Stoppage in tube can be found at several positions in the fault tree. The most important tube is tube 1 close to the bellows, see figure 1. Possible causes are: tube bent, tube pinched or stoppage due to foreign particles, possibly ice.

Tests are recommended to show whether top event 1 is hazardous or not.

3.3 Fault tree for top event 2: Unintended throttle increase



3.2.1 Comments on top event 2: Unintended throttle increase

Unintended throttle increase requires unintended pressure decrease in the bellows. This requires three conditions:

1. Start of pump motor

2. Regulator valve closed

3. Quick valve closed

During normal driving condition 3 is fulfilled. The driver doesn't normally rest his foot on the brake pedal. Therefore this condition is indicated with a "house" symbol which precisely designates a normally fulfilled condition.

Unintended pressure decrease in the bellows consequently requires start of pump motor and regulator valve closure. This valve closes when electrically energized.

Thus, the top event requires double faults; One fault in each of the left and right branches of the tree. External grounding of two different points is not considered very likely.

Far more interesting are the two branches which contain the electronic unit. Certainly, grounding of two separate outputs is required, but this is the very state when the cruise control is working as intended in order to increase speed to the desired value. I will come back to this possibility.

An additional fault mode in both branches is an erroneous sensor signal from the speedometer. This signal tells the electronic unit the actual speed. An erroneous signal causes the electronic unit to react incorrectly without being faulty itself. This is designated a "Command Fault".

A completely missing speedometer signal is an example of a command fault. However, the electronic unit has a "watch-dog" that requires a pulse frequency exceeding a certain value. The cruise control is deactivated automatically when the actual speed is <35 km/h. It is not considered likely that only a fraction of the pulses should reach the electronic unit, thereby deceiving it to believe that the actual speed is lower than the desired speed, which would lead to increased throttle.

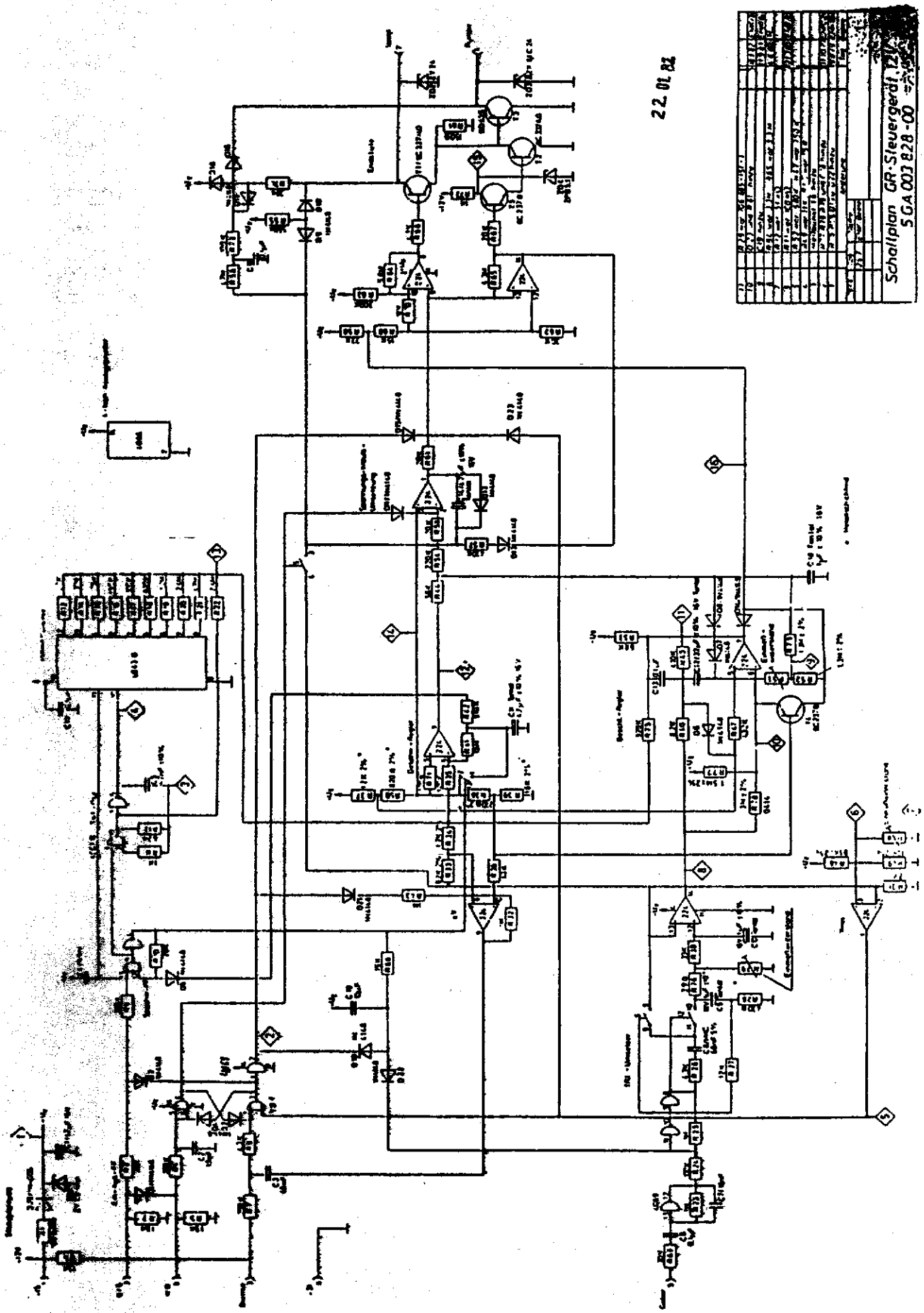


Figure 2 Electronic unit diagram

Comments on design

It cannot be excluded that the grounding of the pump motor may lead to increased throttle. The capacity of the regulator valve may be too low to counteract the pump. Tests are recommended. (See 5. VERIFICATION.)

Faults in the electronic unit can cause increased throttle.
Examples:

* The speed-limit controller V_{min} 224 is a critical circuit. It indicates if the actual speed exceeds 35 km/h. If this circuit is stuck in the state corresponding to >35 km/h. the cruise control can be activated by touching RESUME even at standstill. A component fault and a human error are required.

* At speeds >35 km/h, one fault in the RESUME-circuits is enough to cause acceleration to the preset speed. This means that the cruise control automatically takes over when the actual speed exceeds 35 km/h and increases it to the preset value.

The electronic unit continuously compares actual speed with desired speed. The desired value is stored by the binary counter 4040B. The actual value is derived via one of the four operational amplifiers in the IC 224. The comparison is performed by another operational amplifier in the same IC 224.

Any component fault that leads to a difference between actual speed and desired speed will immediately cause increased or decreased throttle.

* One example is a fault in the binary counter 4040B leading to an increase of the desired value. The binary counter stores the desired value by setting a certain combination of its outputs high thereby giving a potential to the comparator corresponding to the desired value. A poor connection at some of these outputs may lead to increased speed. One such fault has been tested. See APPENDIX 3.

* The comparator (Geschw - Regler) is another critical circuit. A single-point-fault# such as a bad solder joint in this circuitry may lead to the erroneous result of starting the pump motor. The faults can be permanent or intermittent.

The fault modes mentioned above are sufficient for the fault effect: Unintended throttle increase. The system believes that the actual speed is too low. Therefore the regulator valve does not open either.

A common safety design requirement states that "no single-point fault shall result in injury to personnel". It is equivalent to specifying that the system will still be safe after one failure although it may not be functional. Thus a single-point-fault is a fault mode caused by a single event, defect, or error whose consequence is defined as critical in the particular system.

4. RESULTS OF THEORETICAL ANALYSIS

The theoretical analysis shows that single-point-faults are sufficient for the following fault effects:

1. The cruise control is not deactivated by braking

2. Unintended throttle increase

Most technical equipment will not work as intended for ever. Faults will occur. Due to the type of equipment, faults may have unacceptable consequences. If a single credible fault results in hazardous consequences, then the design must be changed.

It should be a design goal that the consequencies of any credible fault are acceptable.

Techniques for achieving this goal are well known in Reliability Technology. This technology is of vital importance for the design and use of complex technical equipment such as airplanes, spacecraft and nuclear power stations.

Today, reliability data are readily available for most electronic components. With reference to such data it can be concluded that among the great number of cars throughout the world equipped with this cruise control, some faults in accordance to 1. and 2. above are likely to occur.

However, the theoretical results should be verified in tests. See next paragraph.

5. VERIFICATION

5.1 Mechanical and pneumatic subsystems

Some of the results from the theoretical analysis have been verified on an automatic car.

It was shown that the brakes easily overcame the engine.

In spite of full throttle, the car could always be brought to a standstill by depressing the brake pedal.

The tests also showed that the quick valve has sufficient overcapacity. This was proved by depressing the brake pedal in order to open the quick valve while the pump was running. The bellows inflated rapidly.

In another test the quick valve was kept closed during braking. This means that the electric switch mounted on the valve does not open either. Yet, the bellows inflated fairly rapidly. This was because input 3."BREMSE" (brake) of the electronic unit, that should go high in order to deactivate the cruise control was forced high by the stop-lamps switch. This stopped the pump and opened up the regulator valve.

When the quick valve works as intended, input 3. goes high by means of the resistor R6 in the electronic unit. Therefore, an open circuit in this input is fail-safe.

The tests above have not disclosed any serious safety problems in the mechanical and pneumatical subsystems.

However, the tests showed that the car may accelerate slowly if the pump motor gets started due to a grounding fault. The regulator valve capacity seems to be of the same magnitude as the pump capacity. The result depends on parking brake tightening as well as idling speed.

5.2 Electronic unit

Tests show that necessary conditions for a pressure decrease in the bellows are:

1. Pump running

2. Quick valve closed

3. Regulator valve closed

The quick valve is normally closed as the brake pedal is not depressed. The regulator valve closes when energized. This is a safety feature. Open circuit in the valve magnet coil results in inflated bellows. The design is fail-safe with respect to this fault mode.

The aim of this analysis has been to search for possible single-point-fault modes leading to traffic hazards. So, the question is: "Are there any single-point-fault modes in the electronic unit which lead to pump motor start and closing of the regulator valve?"

As shown in the circuit diagram, figure 2, the pump motor and the regulator valve are connected to separate outputs. Therefore outputs 4 and 7 must be grounded via their two transistors respectively. This means that double faults are required at the outputs.

However, the analysis has disclosed a single critical point before the outputs. This consists of inputs 9 and 12 for the regulator valve and the pump respectively of the operational amplifier which are interconnected. If this point goes low, the result will be simultaneous closure of the regulator valve and start of the pump, thus causing full throttle.

Since this point is situated behind the accelerator controller (Beschaunigungsregler), there will be no limiting of the acceleration.

At all driving speeds less than the desired speed, the operational amplifier connected to the resistor R61 is trying to lower this point but when the actual speed is <35 km/h this attempt is counteracted by the two diodes D15 and D23. This means that two faults, e.g. open circuits in both diodes, are required for a pressure decrease. So, the cruise control is not safe if two failures occur, but this was expected. Independent double faults, however, are considered very unlikely.

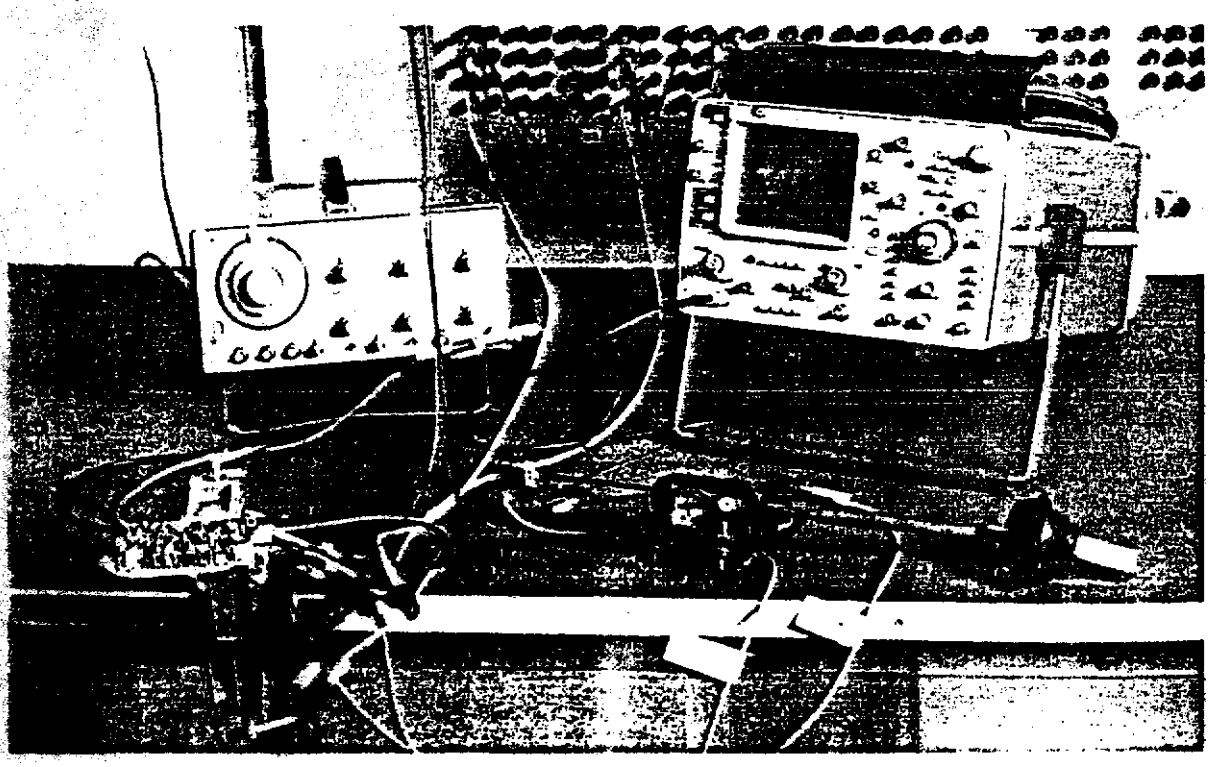
Electrically the printed-circuit layout corresponds to the diagram. Nevertheless, from a reliability point of view, this is not the case. A check of the circuit layout reveals a fault mode that has very severe consequences. This single-point-fault mode, which is not easily found, is described in APPENDIX 2. The complex fault mode effects, however, are listed under 6. TESTS.

6 TESTS

6.1 Simulations

The servo system was set up in a laboratory. The speedometer sensor was replaced by a signal generator. See picture 1. The system fault reaction was simulated.

In addition, tests were carried out on an automatic car at standstill. In this case the speedometer was driven by means of an electric drilling machine at variable speed.



Picture 1 Simulation

6.2 Driving experiments

In order to remove any doubts, an electronic unit with deliberately introduced single-point-fault was tested during real driving. According to these tests a single-point-fault as described in APPENDIX 2. will have the consequences listed below. A necessary condition, however, is the cruise control main switch being set in the ON-position, but this is considered a common habit with many drivers.

The conduct of the car at fault occurrence depends on the situation. Therefore, the fault effects have been divided into two groups.

Faults can be permanent or intermittent. In the latter case, the fault may depend on some environmental factor such as vibrations or changes in temperature.

6.2.1 If the fault is present when engine is started

A If the cruise control is faulty when the engine is started, changing gear into drive or 2 results in full throttle. The cruise control can be deactivated by depressing the brake pedal, but as soon as the pedal is released the car is accelerated again.

B If the cruise control is faulty when the engine is started, changing gear into drive or 2 results in full throttle. If then, when speed exceeds 35 km/h, RESUME is pressed (but not SET), the cruise control is deactivated. However, as soon as speed falls below 35 km/h, the cruise control is reactivated and causes full throttle.

C If the cruise control is faulty when the engine is started, changing gear into drive or 2 results in full throttle. If then, when speed exceeds 35 km/h, SET is pressed, the actual speed is stored in the memory. The cruise control works as intended, but depressing the brake pedal and releasing it again results in full throttle. By pressing RESUME, stored speed will be resumed.

6.2.2 If the cruise control becomes faulty when the engine is running

A If the car is parked with idling engine and gear is drive or 2 when the fault occurs, the result is full throttle. The car will accelerate suddenly even if the parking brake is tightened firmly.

B If driving at any speed on gear drive or 2 without activated cruise control when the fault occurs, the cruise control is activated and full throttle results.

C If driving on gear drive or 2 and SET has been pressed in order to hold speed >35 km/h, nothing happens. The cruise control works. But as soon as the brake pedal is depressed and released again or if speed temporarily falls below 35 km/h, the cruise control will command full throttle. By pressing RESUME, the desired speed is resumed. Compare 6.2.1.

7. CONCLUSIONS

Top event 1, the cruise control is not deactivated by braking, is not considered hazardous. Tests show that the brakes easily overcome the engine.

However, top event 2, unintended throttle increase, cannot be waved aside. Tests show that:

There is a single-point-fault mode that leads to sudden acceleration at high power.

This discovery means that an upper limit for the system safety level has been established.

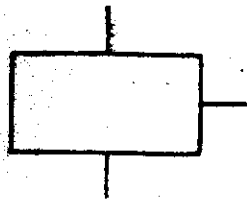
Tests also show that there are a number of fault modes leading to an increase in the desired speed during the drive. However, this fault effect is not considered hazardous but it can certainly disturb the driver.

We can conclude that the fault effects of the single-point-fault mode, disclosed in this investigation, are in accordance with the reported events. Therefore, the alleged events should be taken seriously.

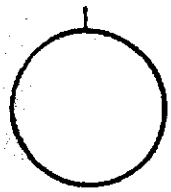
The weaknesses disclosed in this report may be the causes of malfunction in some of the alleged cases. However, no conclusions should be made from this investigation concerning the causes of malfunction in any specific case.

The results of this investigation indicate that HELLA has tried hard to meet very high safety goals in this device. The designer has certainly been aware of the fact that some single-point-faults can lead to an increase of the desired speed, but he has probably not been aware of the fact that a single-point-fault can cause sudden acceleration.

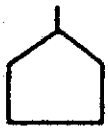
APPENDIX 1. FAULT TREE SYMBOLS



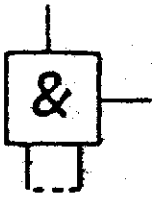
Event Description Block — Name of the event



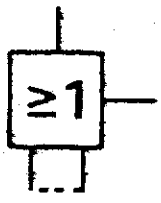
Basic Event. — Event which will not be subdivided



House. — Event which will happen with certainty



AND-gate. — Output event occurs if all input events occur simultaneously



OR-gate. — Output event occurs if any one of the input events occur

APPENDIX 2. HAZARDOUS FAULT MODE

This investigation has been aimed at grading the HELLA cruise control with respect to safety. Therefore the work has been focused on finding some weak point in the system.

The electronic unit consists of both analog and digital circuits. No detailed functional descriptions have been available for the analysis. Nevertheless, the main features of the design have been figured out.

The analysis shows that there is at least one single-point-fault mode with severe effects. Due to the printed circuit layout, a break in a specific connection leads to pump motor start and simultaneous closure of regulator valve.

The disclosed single-point-fault mode consists of a bad solder joint at terminal 9 of the op amp 224 on the component side of the board or a crack in the thin foil connecting terminal 9 to the two diodes D15 and D23.

The investigation is herewith finished but other hazardous fault modes cannot be excluded.

The interesting part of the diagram is shown in figure 3. The real circuit however, which is electrically equivalent to the diagram, is shown in figure 4. The hazardous single-point-fault mode is depicted in figure 5. The printed circuit board is shown in picture 4.

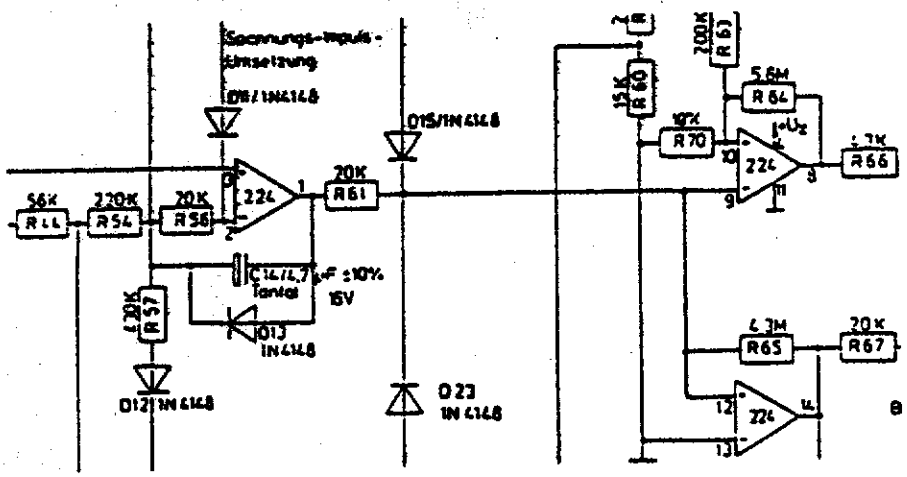


Figure 3. Part of diagram.

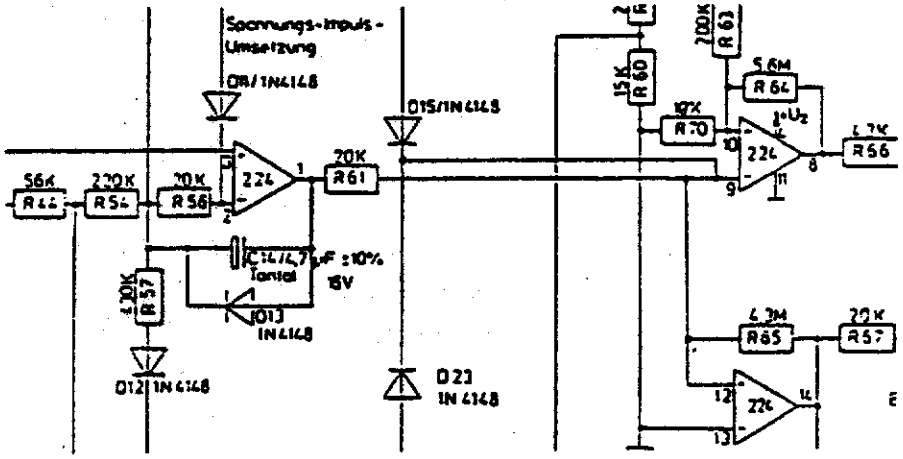


Figure 4. Real design.

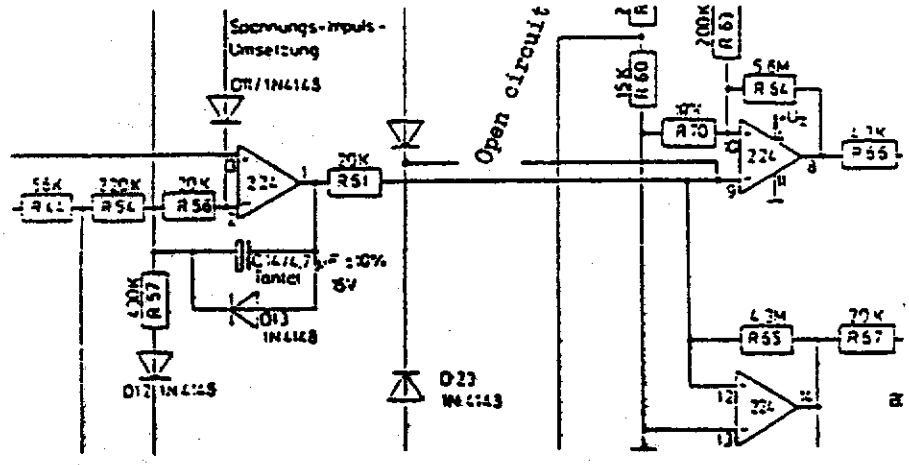
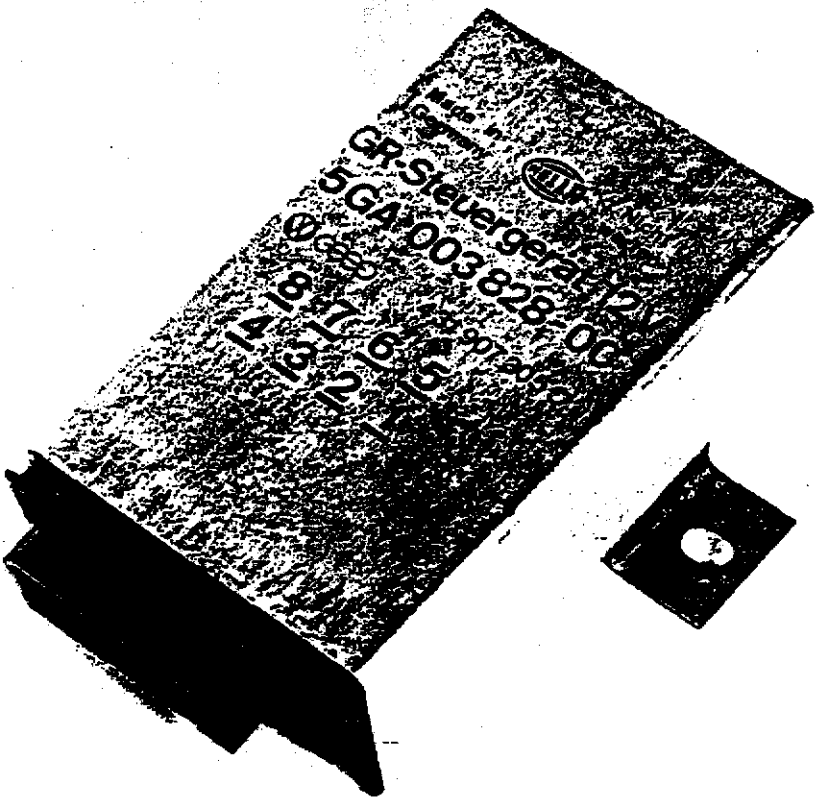
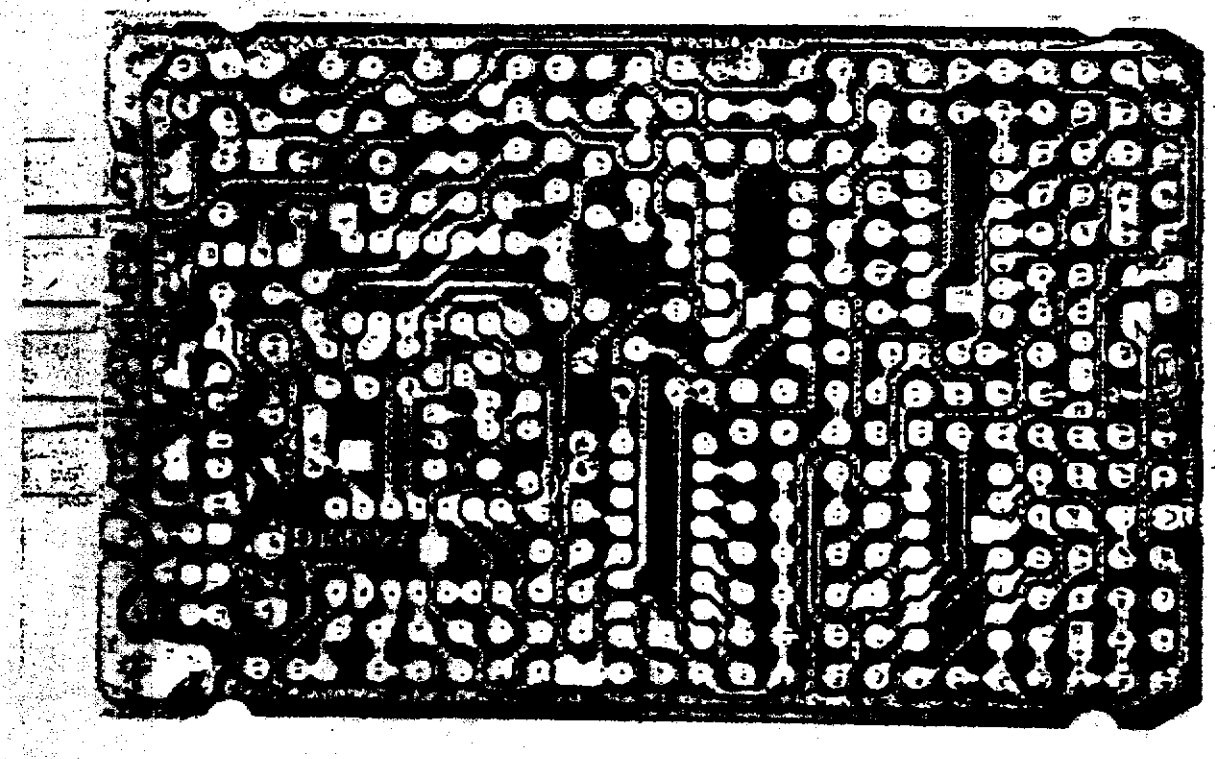


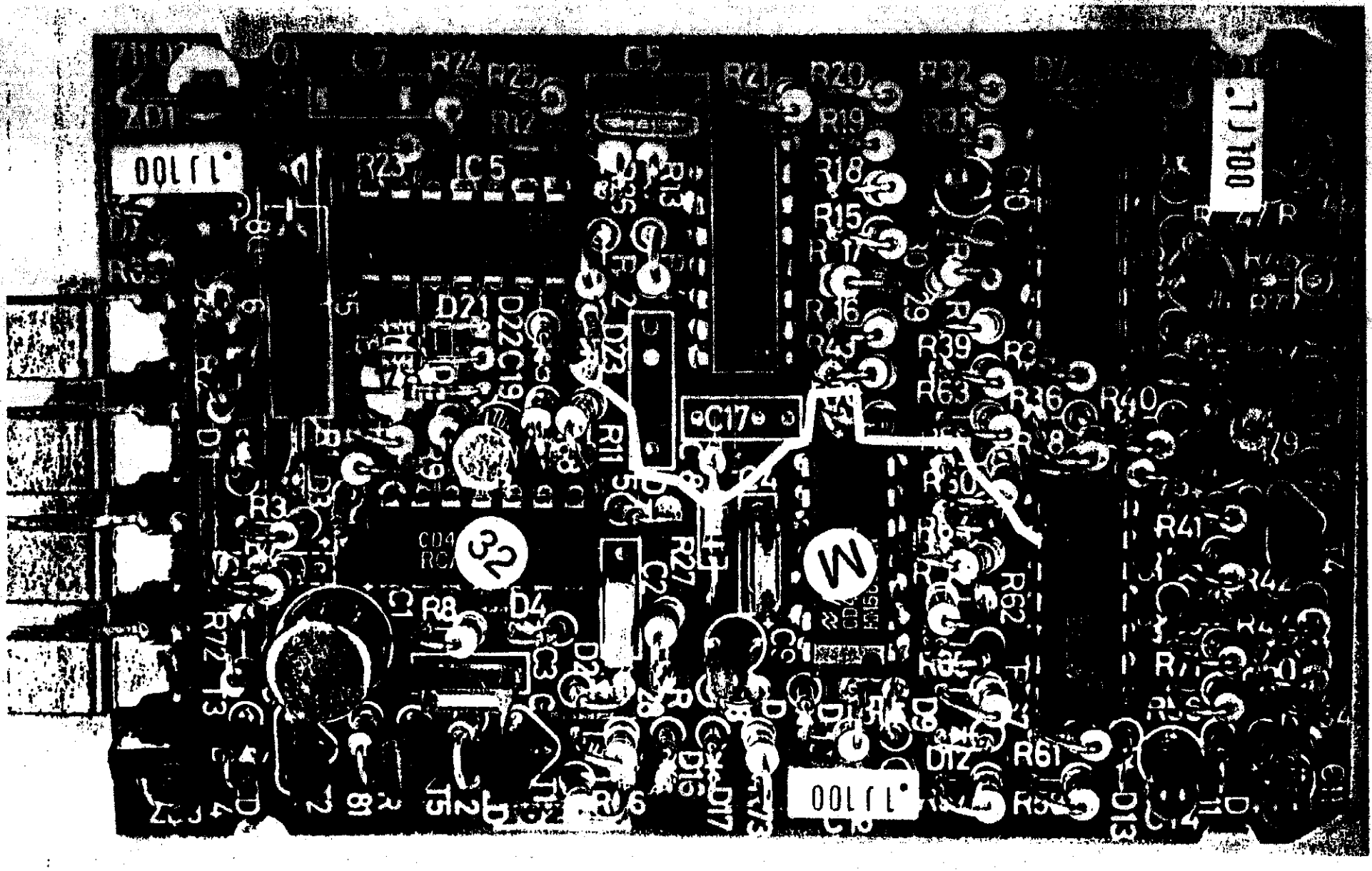
Figure 5. Hazardous fault mode.



Picture 2. Electronic unit.



Picture 3. Printed circuit board, solder side.



Picture 4. Electronic unit printed circuit board. Critical connection marked in white. Two capacitors have been removed in order not to conceal the connection. Diodes D15 and D23 can be found to the left and the operational amplifier, marked 0124DP, to the right. Terminal 9 of the operational amplifier is used as connection to the solder side of the board where terminals 9 and 12 are connected to resistors R61 and R65.

APPENDIX 3. OTHER FAULT MODES

In the comments to the design under 3.8 some vulnerable points in the diagram were mentioned. An example was the binary counter 4040B, that stores the desired speed by setting an apropriate combination of its outputs high. By doing this a voltage corresponding to the desired speed is created and fed to the comparator. The resistors R13 - R23 are essential for this function. The effect of an open circuit in R15 has been tested with the following results:

When the cruise control was activated at

70 km/h speed decreased to 55 km/h

80 km/h speed increased to 100 km/h

90 km/h speed increased to 110 km/h

100 km/h speed increased to 120 km/h

Open circuits in other branches will lead to varying changes of speed. Whether the effect will be an increase or a decrease depends on the desired speed value.