

# TÜV Rheinland Sicherheit und Umweltschutz GmbH

Institut für Software, Elektronik, Bahntechnik (ISEB)

Akkreditiert als Prüflaboratorium und  
Zertifizierungsstelle  
TTI-P-G002/92-01 • DTI-ZE-G001/92-00  
Deutscher Akkreditierungsrat

**COPY**



**TÜV Rheinland  
Gruppe**

Wir sichern Lebensräume

# ZERTIFIKAT CERTIFICATE

Nr./No. 945/EL 337/96

Prüfgegenstand Product tested	HEIDRUN Emergency Shut Down (ESD) and Fire & Gas (F&G) System	Hersteller Manufacturer	SIMRAD Norge AS P.O. Box 483 N-3601 Kongsberg
Bezeichnung Designation	Simrad AIM 1000 with SBC 3003	Verwendungszweck Intended application	Emergency Shut Down (ESD) System according to requirement class 6 (DIN V 19250) and Fire & Gas System according to requirement class 4 (DIN V 19250) on the HEIDRUN platform.
Prüfgrundlagen Codes and standards forming the basis of testing	DIN V 19250/04.94 DIN V VDE 0801/01.90 and A1/94 IEC 0801 (DIN VDE 0843) Microcomputers in safety technique (TÜV handbook) MB-J-SD-003 Specification for Distributed Control and Safety Systems (DCSS) CONOCO, Norway Inc.		DIN VDE 0160/04.89 DIN VDE 0110/01.89
Prüfungsergebnis Test results	The ESD and F&G System for the HEIDRUN platform is built on basis of the AIM 1000 System. As implemented it is suitable as system to activate the emergency shutdown and to handle fire & gas alarms in an appropriate manner.		
Besondere Bedingungen Specific requirements	The System Operators and Maintenance Manuals (Doc. No. MB. EI 171-0426 . - Doc. No. MB. EI 171-0428) have to be followed. The suggested measures of the TÜV report no. 945/EL 337/96 must be implemented during maintenance working packages.		

Der Prüfbericht Nr. 945/EL 337/96 vom 1996-10-28 ist Bestandteil dieses  
Zertifikates.

The test report No. 945/EL 337/96 dated 1996-10-28 is an integral part of  
this certificate.

**TÜV Rheinland**  
Sicherheit und Umweltschutz GmbH  
51105 KÖLN (Poll)  
Am Grauen Stein / Konstantin-Wille-Straße 1  
Postanschrift: Postfach 91 09 51, 51101 Köln  
Telefon 02 21 / 806-0 • Telefax 02 21 / 806-17 36

1996-10-28

*R. Jacobs*

Datum/Date

Firmenstempel/Company seal

Unterschrift/Signature

COPY

**Microelectronics and Process Automation**

**Verification of the Heidrun Emergency  
Shut Down (ESD) and Fire & Gas (F&G) System**

**Report-No.: 945/EL 337/96**  
**Date: 1996-10-28**

1996-10-28

**Verification of the Heidrun Emergency  
Shut Down (ESD) and Fire & Gas (F&G) System**

**Report-No.:** 945/EL 337/96

**Date** 1996-10-28

**Pages:** 39

**Test object:** Heidrun Emergency Shut Down (ESD)  
and Fire & Gas (F&G) System

**Customer:** SIMRAD Norge AS  
Heidrun Project  
P.O. Box 483  
N-3601 Kongsberg  
Norway

**Manufacturer:** SIMRAD Norge AS

**Order-No./Date:** A33732 dated 1995-05-22

**Test Institute:** TÜV Rheinland  
Sicherheit und Umweltschutz GmbH  
Institute for Software, Electronics  
and Railroad Technology (ISEB)  
Postfach 91 09 51  
D-51101 Köln  
Am Grauen Stein  
D-51105 Köln

**Department:** Microelectronics and Process Automation

**TÜV-Order-No./Date:** 945/553021 dated 1995-01-31

**Offer-No./Date:** 945/17494 dated 1994-11-15

**Inspector(s):** Dipl.-Ing. Johannes Buschmann  
Dipl.-Phys. Ekkehard Pofahl

**Test Location:** TÜV Rheinland  
Sicherheit und Umweltschutz GmbH, Cologne

**Test Duration:** February 1995 until October 1996

The test results are exclusively related to the test samples.

This report must not be copied in an **abridged version** without the written permission of the test institute.

Contents		Page
1.	Abstract	6
2.	Scope	6
3.	Definitions and standards	7
3.1	Definition and explanation of terms	7
3.2	Basic standards and references	8
3.3	Documentation on the test object	10
4.	Object of inspection	10
4.1	ESD application	11
4.2	F&G application	12
4.3	Description of the test sample	13
4.3.1	Used AIM components	14
4.3.2	Implemented ESD part for the test system	15
4.3.3	Implemented F&G part for the test system	16
5.	Inspections and results	17
5.1	Procedure of the inspection	17
5.2	Safety concept	17
5.3	Hardware	17
5.3.1	Theoretical hardware assessment	17
5.3.1.1	Hardware related ESD considerations	18
5.3.1.1.1	ESD requirements	18
5.3.1.1.2	ESD system design	18
5.3.1.1.3	ESD fault detection	19
5.3.1.1.3.1	Input wiring	19
5.3.1.1.3.2	Analog input (ESD)	19
5.3.1.1.3.3	CPUs	19
5.3.1.1.3.4	Digital outputs	19
5.3.1.1.3.5	Digital input	19

Contents	Page
5.3.1.1.4 System design - mimic panel -	20
5.3.1.1.5 Fault detection - mimic panel -	20
5.3.1.2 Hardware related F&G considerations	20
5.3.1.2.1 F&G requirements	20
5.3.1.2.2 F&G system design	20
5.3.1.2.3 F&G fault detection	21
5.3.1.2.3.1 Analog input (F&G)	21
5.3.1.2.3.2 Access to bus controller	21
5.3.1.2.3.3 CPU	21
5.3.1.2.3.4 Digital outputs	21
5.3.1.2.3.5 System design for the mimic panel	21
5.3.1.2.3.6 Communication paths	21
5.3.1.2.4 Interconnection of ESD and F&G system	22
5.3.1.2.5 Fault detection of the interconnection of ESD and F&G system	22
5.3.2 Detailed fault assessment on module level	22
5.3.2.1 Central unit SBC 3003	22
5.3.2.2 Digital output PDO 120	22
5.3.2.3 Digital input PDI 120	23
5.3.2.4 Analog input PAI 121	23
5.3.2.5 MPC 101	24
5.3.3 Hardware tests	24
5.3.3.1 Fault simulation	24
5.3.3.2 Electromagnetic compatibility (EMC)	24
5.3.3.3 Climatic and environmental tests	27
5.4 Software	28
5.4.1 Operating system of the PCU SBC 3003	29
5.4.2 Firmware on modules of the system	30
5.4.3 Modular panel controller MPC 101	30
5.4.4 Configuration software for I/O modules	31
5.4.5 Programming software	31

<b>Contents</b>	<b>Page</b>	
5.4.6	Simulation of the AIM system	32
5.4.7	BITE system	32
5.4.8	Software changes	33
5.4.8.1	Software changes to the operating system	33
5.4.8.2	Software changes to the application program	33
5.4.9	Quality assurance measures for software	33
5.4.10	Integration test	34
5.5	Fire and Gas fault detection system	34
5.6	Consideration on the AUTRONICA BS 100	34
5.6.1	Environmental tests on BS 100	35
5.6.2	Software architecture	35
5.6.3	Operation experience	35
5.7	EX-protection	35
5.8	Test protocols, used investigation and measuring tools	36
6.	Suggested measures	36
6.1	Operator and maintenance handbooks	36
6.2	Power supplies	37
6.3	EMC compatibility	37
6.4	Modular Panel Controller MPC 101	37
6.5	ESD: Field wiring to actuators	38
6.6	F&G: Periodic check of duplicated PCUs	38
7.	Summary of the verification	39

#### **Appendix A**

AIM 1000 system documentation (5+2+1 pages)

#### **Appendix B**

AUTRONICA BS 100 documentation (3 pages)

## 1. Abstract

The application for ESD and F&G in the Heidrun project is implemented with SIMRAD AIM 1000 and additional devices. A verification was done to testify, that the implemented application complies to its specification. Furthermore it is shown, that safety categories according 6 (ESD system) and 4 (F&G System) according to the standard DIN V 19250 (Fundamental safety aspects to be considered for measurement and control equipment) are met by using the methods as stated in standard DIN V VDE 0801 (Principles for computer in safety related systems).

## 2. Scope

The Heidrun Emergency Shut Down (ESD) and Fire & Gas (F&G) System shall be verified to comply to its specification. The specification is detailed in document MB-J-SD-003, "Specification For Distributed Control And Safety System (DCSS)", issued by CONOCO Norway. Furthermore it shall be checked if the safety categories according to the German standard DIN V 19250 are met.

After the "Concept Review of the ESD- and F&G-Systems for the Heidrun-Project ..." [12] was done on the system with focus on the AIM 1000 system (CPU 3003) from SIMRAD, the Heidrun installation shall be investigated on basis of the findings of the concept review by investigation of a test sample and on document basis. Both, the ESD and the F&G system, are based on a duplicated AIM 1000 system. The checking will be done on base of the standard DIN V VDE 0801, which identifies the measures needed to comply to a specific safety class. The ESD part shall comply to requirement class 6, the Fire & Gas part shall comply to requirement class 4 according to the standard DIN V VDE 0801.

On base of the installed system on Heidrun a sample system with all active elements of the actual system, including an AUTRONICA BS 100 fire central, and simulated loads was built to investigate the overall system as it is installed in the Heidrun field. The original software was taken and adopted for those parts, which are actually installed on the test system.

Using this system it has been investigated, if the implemented system is sufficient to fulfil the intended operation.

### 3. Definitions and standards

#### 3.1 Definition and explanation of terms

##### CCS (Continuous control system)

Structure of a more than one-channel system, which is able to perform a function in the presence of a fault and which has no safe direction, e. g. F&G-system.

##### DIN

"Deutsche Industrie Norm"  
German system of Industry-Standards

##### ESD (Emergency shutdown system)

Structure of one or more channel of a system which shuts down a process according to the specified structure in a safe direction.

##### EX (Explosion)

Usually this abbreviation means explosion and is used in conjunction with other words, e.g. EX-barrier, which separates dangerous voltages from explosive areas.

##### Fail-safe

A design property of an item in which the specified failure mode is predominantly in a safe direction.

##### Fault tolerance

The attribute of an item that makes it able to perform a required function in the presence of certain given sub-item faults.

##### F&G (Fire & Gas application)

Applies to systems which monitor the environment for the presence of fire, gas, smoke, heat, toxic gas, high temperature, etc. Depending on the application also responsible to start fire pumps, extinguishers etc.

##### m oo n-structure (American notation)

"m"-channels of a "n"-channel system have to command shutdown before a shutdown takes place.

##### m v n-structure (German notation)

At least "m" channels of a "n"-channel system have to work correctly. If less than "m"-channel work the system shuts down.



### OCU (Operator Control Unit)

A software unit implementing the AIM operator interface on a visual display unit (VDU). In this document, OCU also means a complete operator station comprising VDU, functional keyboard, SBC 3000 single board computer and software.

### PCU (Process Control Unit )

A software unit implementing the distributed AIM process control functions. Each PCU is implemented on a dedicated SBC 3003 single board computer. In this document, PCU also means a complete AIM process control node comprising SBC 3003, backplane, wiring and software.

### PES (Programmable electronic system)

A system based on one or more programmable electronic devices, connected to sensors and/or actuators, for the purpose of control, protection or monitoring.

### PLC (Programmable electronic controller)

Comparable with PES but without sensors and actuators.

### Redundancy

The existence of more than one channel of a system for performing a required function.

## 3.2 Basic standards and references

The required inspections and tests of the verification are carried out according to the designated field of application and are based on the following fundamental and application-dependent standards:

[1] DIN V 19250/1994

Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen

Control Technology, Fundamental Safety Aspects to be considered for Measurement and Control Equipment

[2] DIN 19251/1993

MSR-Schutzeinrichtungen, Anforderungen und Maßnahmen zur gesicherten Funktion

Control Technology, MC-Protection Equipment Requirements and Measures for Safeguarded Function

- [3] **DIN V VDE 0801/1990** including alteration A1  
Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben  
Principles for Computers in Safety-Related Systems
- [4] **DIN VDE 0116/1989**  
Elektrische Ausrüstung von Feuerungsanlagen  
Electrical Equipment of Furnaces
- [5] **DIN EN 54**  
Bestandteile automatischer Brandmeldeanlagen  
Components of Automatic Fire Detection Systems, Control and Indicating Equipment
- [6] **DIN EN 61131**  
Speicherprogrammierbare Steuerungen, Teil 1 - 3  
Programmable Controllers, part 1 - 3
- [7] **MB-J-SD-003**  
Specification for Distributed Control and Safety Systems (DCSS)  
CONOCO, Norway Inc.
- [8] **Regulation relating to safety and communication systems on installations in the petroleum activities**  
(Norwegian Petroleum Directorate, 07. February 1992)
- [9] **DIN VDE 0160**  
Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln  
Electronic Equipment used in Electrical Power Installations
- [10] **DIN IEC 68 Normenreihe**  
Elektrotechnik; Grundlegende Umweltprüfverfahren  
Electrical Engineering, Basic Environmental Testing Procedures
- [11] **IEC 801 Normenreihe**  
Electromagnetic compatibility for industrial-process measurement and control equipment
- [12] **Concept Review of the ESD- and F&G-Systems for the Heidrun-Project from SIMRAD Albatross A/S**  
**Report-No.: 945/EL 243/94 - Date: 30. August 1994**

### 3.3 Documentation on the test object

The specific behaviour of the ESD and F&G system, as installed on the Heidrun platform, is explained in the following four documents.

**[13] Heidrun ESD System Operators' Manual**

MB. EI 171- 0426

**[14] Heidrun ESD System Maintenance Manual**

MB. EI 171- 0427

**[15] Heidrun F&G System Operators' Manual**

MB. EI 171- 0428

**[16] Heidrun F&G System Maintenance Manual**

MB. EI 171- 0429

The complete set of documents supplied by SIMRAD is listed as appendix A. This includes all AIM 1000 specific documentation and the documentation on the test set-up.

Appendix B includes all documentation received directly from AUTRONICA regarding the BS 100 fire central.

### 4. Object of inspection

The system is installed on the Platform Heidrun with an ESD and a F&G part as detailed in the engineering documents. It is made out of components of the AIM 1000 product family, a BS 100 fire central from AUTRONICA, and barriers from STAHL and PEPPERL & FUCHS. The principal applications are described in section 4.1 and 4.2. The provided test sample as basis for the verification is described in section 4.3.

#### 4.1 ESD application

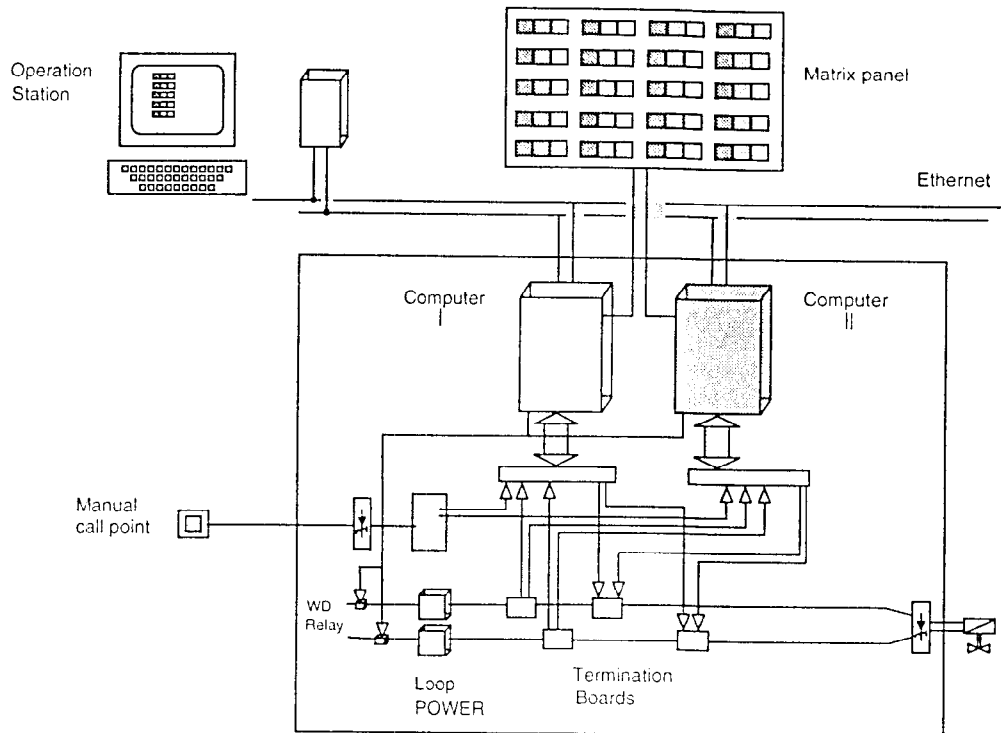


Figure 1: ESD System (two redundant channel)

The function of the ESD-system is to detect abnormal operational conditions within the wellhead/flare/instrument/air system and initiate appropriate actions. Inputs from the F&G system or from manual initiation from various locations around the platform, including the control room, will initiate emergency shutdowns. The ESD matrix panel (duplicated) in the control room is the main operator interface. Activation of one button is sensed by two panel controllers and two LED's. The matrix consist of input and output status fields and a general ESD system status field. Activated lamps indicate when the ESD input is activated. Each input can be manually overridden by a panel switch.

The ESD system (see figure 1) has full redundancy, which means a complete duplication of both hardware and software on two independent PLC's including power supply.

An operation station is connected to the PLC via a redundant Ethernet. The net is used upon start-up of the system for downloading the application program into the RAM of the PLC and to report detailed information of the ESD-system. There is only a data exchange between the two systems over the network during the start-up. The interface between the two PLC's are four hardwired status signals. Each channel senses by these signals if there is a fault detected in the other system. By these signals the status of the watch-dog relays is signalled. The connection is also used to synchronise the sequence of output tests. The output tests are done by alternatively changing the supply voltage to the field and measuring the expected difference in the current flow.

The input signals (digital and analog) are read by both channels. The output loop is redundant and normally energised. A shutdown is activated when there is no current in the loop.

The matrix panel is the main operator interface and consists of input-, output-fields and a general ESD status-field.

The ESD-system is specified for the Heidrun application as a 1oo2-system, each PLC is capable of doing the shutdown independent from the other channel. A fault in one system shall not lead to a shutdown, or prevent activation of a shutdown from the other system. It is also a 1v2 system: One channel may continue operation, if the other channel fails.

## 4.2 F&G application

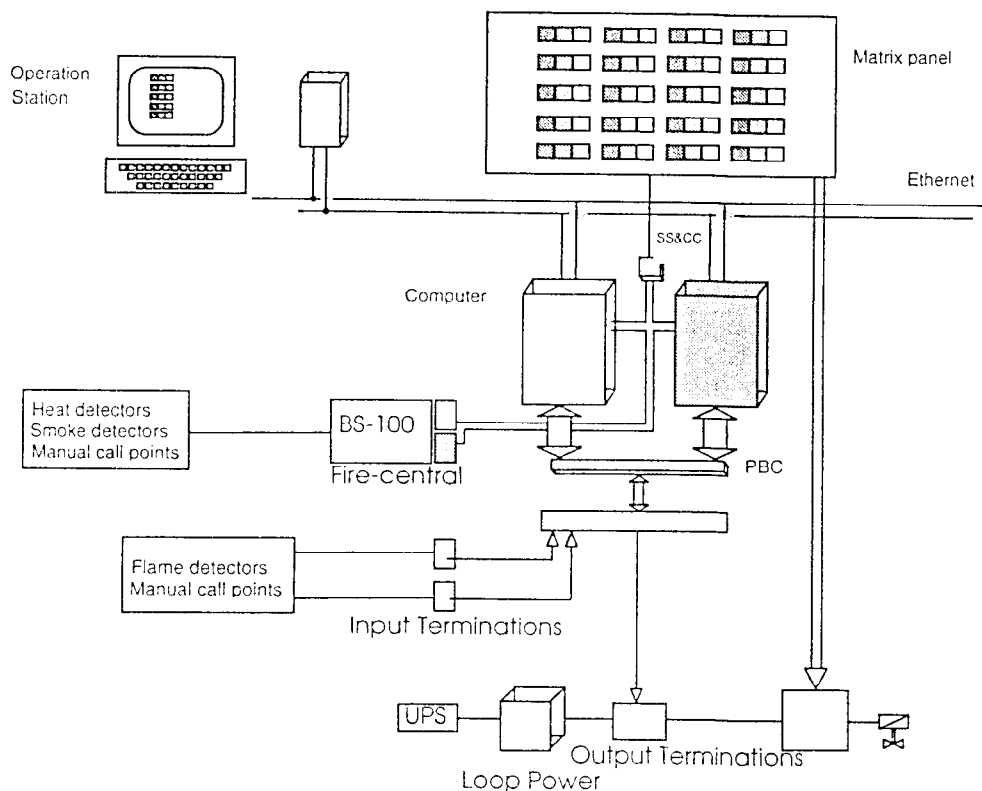


Figure 2: Fire and gas system

The object of the F&G-system is to provide rapid and reliable detection of fire condition and gas leaks by monitoring smoke-, heat-, flame-, gas-detectors and manual call points. It shall automatically or upon manual intervention, initiate the necessary safety actions like initiation of alarms, shutdown of systems and equipment, activate fire protection systems and indicate the status of the supervised area. The location and arrangement of all sensors are specified.

The F&G-system (see figure 2) is based on AIM 1000 technology and is configured as a system of two CPUs and one single I/O. The ethernet interface is the same as for the ESD system. Both CPUs are connected to the I/O-modules via an I/O-bus controller (process bus controller, PBC) and work in a hot standby principle. The I/O-bus controller (PBC) controls that only one CPU, the active one, sets the output. The selection of the active CPU is done by means of the watchdog signals of the CPU's. In cases of a failure of one CPU, the other one takes over the control. The two channels communicate with each other by status signals on PBC and by sensing and setting status and signal lines of the serial line switch (SS&CC).

The power supply is also redundant. Digital and analog inputs and serial lines serve the inputs from the field sensors to both CPU. The wiring to the field is monitored with regard to open/short circuit and earth fault. Analog addressable detectors of F&G are connected hardwired to a detector station (BS 100 DYFI) and transferred by redundant serial links to both CPU's. The BS 100 can handle up to 16 loops, each up to 99 addressable analog detectors. Each fire area is equipped with several detectors and call points. Heat detectors, smoke detectors and manual call points of one area connected to the fire-central BS 100, where flame detectors and manual call points are direct connected to the input termination's of the F&G-system.

Output signals to fire protection are normally de-energised. The connection to the ESD system is normally energised.

#### 4.3 Description of the test sample

The set-up of the test system on base of the Heidrun design is described in detail in the engineering documentation. It consists of four cabinets, a video display unit (VDU), two keyboards and a printer.

There are two PCUs (no. 60 and 61) for the ESD part, two PCUs (no. 80 and 84) for the F&G part, and one OCU implemented. All PCUs and the OCU are connected by a redundant TCP/IP network (net A and net B).

All binaries of the system were stored on a fixed disc. A laptop computer under DOS was used to make necessary software changes to the system during the inspection. Also single stepping through the software was possible by using the tool "Softscope" on the PC. Physical connection was made, dependant on which function was needed, by terminal emulation through a serial line (V.24) or by directly connecting to the system by means of an TCP/IP connection for file exchange.

The ethernet network and the operator control unit (OCU) were excluded from the detailed analysis. These components were used, however, during the investigation of the test sample to operate the AIM 1000 system. During the investigation it was also checked, that the ESD and F&G system worked correctly without the OCU and the two ethernet lines in operation.

### 4.3.1 Used AIM components

The test system was made of the following components which are identified by the numbers of columns ESD, F&G, OS, BS 100, Terms and mimic panel:

Type designator	Description	ESD	F&G	OS, BS 100, Terms	mimic panel
SBC 3003	Single Board Computer			1	
AIM 1000 BP	Backplane for SBC 3003	2	2	1	
SBG 3000	Graphic Card for SBC 3000			1	
AIM Disk	Disk System 52Mb			1	
MPC 101	Modular Panel Controller				9
TBMPC-GEN	General MPC Adapter				9
TBMPC 16SL	Interface between TBMPC and switches/LED				9
PAI 121	Analog Input	6	1		
PDI 120	Digital Input	6	2		
PDO 120	Digital Output	6	1		
PB 115	Connections between PCU Bus and I/O-Card	2	1		
PBC 100	Process Bus Controller		1		
PBC BP	Process Bus Interconnection		1		
TB AIR 2	Interf. between Analog Input Card and field			4	
TB CNTRL 2.5A	Term board for current and voltage sense	2			
TB-DI ISO	Term board for digital input	2	1	4	
TB ESD 1	Term board for digital output	2		2	
TBSL	Motherboard for Serial Lines	2	2	1	
TBSL	Power Adapter for Serial Lines	2	2	1	
TBSL	Galvanic Isolation for Serial Lines RS 232				
TBSL	Galvanic Isolation for Serial Lines RS 422	2	2		
SS&CC	Serial Switch and Current Controller		1		
Netswitch	Interface between LAN Equipment				
Cheapernet Rep.	Interface between Cheapernet and Ethernet	2	2	2	
AIM Keyboard	Operator Keyboard			1	
-	Alarm Keyboard			1	
-	Watchdog Relay	2			
-	Net Transceivers	2	2	2	
48 V Powec SBC	Power Supply	4	2	2	
24 V Powec TB-Cards	Power Supply				
25 V Powec Output 1	Power Supply				
24 V Powec Output 2	Power Supply	8	2	3	
24 V Powec BS 100	Power Supply				
BS 100	Central Station			1	
48 V/12 V/5 V			1	1	
48 V/5 V			4		

### 4.3.2 Implemented ESD part for the test system

The system was inspected on basis of the documentation and by installing a system with reduced I/O compared to the full installation on Heidrun. The same elements were used on the test system as on the original system. The test system contained at least one sample of each actual used component.

To properly document the revision of the software a dedicated file on the SIMRAD software generation system is used. The file is put under SCCS version control to ensure to have full control with all alterations. The file is called std\_3000.txt and is produced automatically by the software generation system after the system has been generated.

The file documents both the PCU and the OCU systems, both on the 376 and the 386 side. The files that have been manually brought into the system is documented under the header:

#### 14: Lokal kilde-kode

Other details like PROM and PAL versions are documented as part of SIMRADs FAT documentation.

The software used in the two PCUs as part of the ESD system for the test sample is characterised by the following table:

	PCU 60	PCU 61
SBC type	SBC 3003	SBC 3003
Date of generation	960416 12:36	960416 12:36
Release	/aimrel/5.1/upd/u4	/aimrel/5.1/upd/u4
AK 386	3.2.1D/960409	3.2.1D/960409
AK 376	3.2.1D/960409	3.2.1D/960409
386 boot prom	2.3P/930622	2.3P/930622
376 boot prom	2.3D/920630	2.3D/920630
No. of modules	814	809
No. of redundant modules	760	760
No. of alarms	1121	1121

**Table 1:** Used software revisions ESD part of the test system

The release and the date of generation defines the reference to a list, which includes all versions of all modules used for the test.

The MPC 101 is driven by the software "MPC 100/101 Version E". The Eproms were labelled with "ART 37762614 E, VER 94.12.13, MPC Panel".



### 4.3.3 Implemented F&G part for the test system

The system was inspected on basis of the documentation and by installing a system with reduced I/O compared to the full installation on Heidrun. The system included the BS 100 fire central and samples of the used barriers from STAHL and PEPPERL & FUCHS. The same elements were used on the test system as on the original system. The test system contained at least one sample of each actual used component.

To properly document the revision of the software a dedicated file on the SIMRAD software generation system is used. The file is put under SCCS version control to ensure to have full control with all alterations. The file is called std\_3000.txt and is produced automatically by the software generation system after the system has been generated.

The file documents both the PCU and the OCU systems, both on the 376 and the 386 side. The files that have been manually brought into the system is documented under the header:

#### 14: Lokal kilde-kode

Other details like PROM and PAL versions are documented as part of SIMRADs FAT documentation.

The software used in the two PCUs as part of the F&G system for the test sample is characterised by the following table:

	PCU 80	PCU 84
SBC type	SBC 3003	SBC 3003
Date of generation	960416 12:36	960416 12:36
Release	/aimrel/5.1/upd/u4	/aimrel/5.1/upd/u4
AK 386	3.2.1D/960409	3.2.1D/960409
AK 376	3.2.1D/960409	3.2.1D/960409
386 boot prom	2.3P/930622	2.3P/930622
376 boot prom	2.3D/920630	2.3D/920630
No of modules	1047	1048
No. of red. mod.	1033	1033
No of alarms	1402	1401

**Table 2:** Used software revisions for the F&G part of the test system

The release and the date of generation defines the reference to a list, which includes all versions of all modules used for the test.

The MPC 101 is driven by the software "MPC 100/101 Version E". The Eproms were labelled with "ART 37762614 E, VER 94.12.13, MPC Panel".

## 5. Inspections and results

### 5.1 Procedure of the inspection

The system was investigated with focus on

- system software
- application software
- basic hardware components
- error detection measures
- system integration

### 5.2 Safety concept

The safety concept is described in the document [7] **MB-J-SD-003** Specification for Distributed Control and Safety Systems (DCSS) CONOCO, Norway Inc. [4]. How it is implemented is best shown in the 4 documents Operator and Maintenance manuals for the ESD and F&G [13 - 16].

The basic concept was investigated during the concept review. The result is documented in the report "Concept Review of the ESD- and F&G System for the Heidrun - Project from SIMRAD Albatross A/S", Report-No.: 945/EL 243/94.

After the concept review and during the course of the verification modifications and additions with respect to the results of the concept review were implemented in the AIM 1000 system.

With these modifications and additions the safety concept is sufficient to control the safety of the Heidrun platform according to the specified application.

### 5.3 Hardware

#### 5.3.1 Theoretical hardware assessment

The first step of the theoretical hardware assessment was an analysis of the test sample.

A comparison between the installed system and the layout documentation was performed.

During the course of the inspection drawings of the system were prepared in parallel to the mentioned comparison. The drawings show the system as connected modules and are used to point out the major points for the failure mode and effect analysis.

During the second step of the theoretical hardware inspection the functionality of each hardware board was analysed. This included the circuitry's that perform the self tests of the board.

The functionality of the boards are listed in a table and the possible failure modes are found by making the assumption that the board is not able to perform the intended function.

Because the ESD and F&G part of the system is different the further theoretical hardware inspection is divided into three steps:

- investigation on ESD
- investigation on F&G
- investigation on the connections between the two systems.

### 5.3.1.1 Hardware related ESD considerations

#### 5.3.1.1.1 ESD requirements

Emergency shutdown systems must be able to shut down the application in the case of safety relevant problems. Usually the zero signal, no voltage, is used as the safe state of each signal connected to the field. This measure ensures protection against broken wires and power outages.

#### 5.3.1.1.2 ESD system design

The system design for emergency shutdown is divided in several layers. The safety related inputs, e.g. emergency push buttons, are read in via analog inputs. The normally closed switch is connected to the Ex-barrier and further to the analog termination module.

The analog value is converted to a digital number by two analog inputs modules, one for each channel.

The corresponding CPU reads the digital number via the process bus.

Digital outputs are connected by the process bus to the CPU. Each digital output module is connected to the termination module for ESD application. The digital output switches are supplied with power from the power supplies.

The current from the switches and the actuators is converted to a corresponding voltage in the TB control module. The voltage is converted and read by both CPUs by means of an analog input module.

Between the actuator and the ESD termination module an EX Barrier is installed.

The actual state of the actuator is read back via an EX-barrier, termination module for digital inputs and a digital input module.

### **5.3.1.1.3 ESD fault detection**

#### **5.3.1.1.3.1 Input wiring**

The circuitry of the ESD push button includes two resistors. By this measure all potential faults of the wiring to the analog input can be detected.

#### **5.3.1.1.3.2 Analog input (ESD)**

The detailed fault assessment is explained in a subsequent chapter. The fault assessment shows, that the fault coverage rate of this board is application dependant and depends on the number of input channels actually used in an application. The analog input module includes a self test circuitry, where two test voltages can be set and read back by the CPU. With this test a part of the analog to digital conversion is checked.

The range for the ESD button being read as “not activated is very small, from the software point of view. Therefore all values that are out of this range will cause an alarm in the ESD system. Furthermore the analog input modules are redundant for the ESD application. Two modules must fail with the same fault effect to cause the ESD button not to be read correctly.

#### **5.3.1.1.3.3 CPUs**

Outputs from the CPU are written via the process bus to the output modules. Faults in the CPU cause the external watchdog circuitry to expire. The watch-dog relays disconnects the connected power supply for the ESD outputs.

#### **5.3.1.1.3.4 Digital outputs**

The actuators are switched on or off by digital output modules. Each CPU with is corresponding digital output can perform the switching. For each actuator two power sources are available. The power supplies provide an input to change voltage by some 100 mV. This input is controlled by digital outputs of CPU A and CPU B. The current for the actuators is looped through the TB control module and read by an A/D converter by both CPUs.

The contacts of the digital output module are checked by switching one output off and subsequent current sensing.

Because the actuators have two dedicated power supplies no interruption of the current will happen during the test of the output switches.

By changing the voltage of the power supplies all potential faults in the output wiring, except shorts between different points of one output board, are found.

#### **5.3.1.1.3.5 Digital Input**

The actuators of the ESD system include read back switches. The switches are read back by digital input modules. Open or shorts of feed back contacts of the switches are monitored by PEPPERL & FUCHS modules and read independent by both CPUs via digital input modules.

#### 5.3.1.1.4 System design - mimic panel -

Switches on the ESD mimic panel consist of two separate contacts per switch. The contacts are read by the two modular panel controllers (MPC). These MPCs are connected to the two CPUs via an TBSL Board with serial protocol.

All indicators on the ESD panel consist of two lamps within one housing per indicator point. The two lamps of indicators are connected via the MPCs to the two CPUs.

#### 5.3.1.1.5 Fault detection - mimic panel -

The communication between the CPU and the MPC and the communication between master and slave MPCs is checked by telegram checksums. Fault effects are discussed in a subsequent chapter. The fault assessment showed, that fault detection by self tests has low efficiency.

Two channels must fail to cause the mimic panel not to be able to read in commands or set indicators.

#### 5.3.1.2 Hardware related F&G considerations

##### 5.3.1.2.1 F&G requirements

In F&G applications the safe state cannot be reached by simply removing power or bringing actuators in pre-defined position. F&G system have to pertain operation even after the occurrence of a fault and after degradation from two system operation to single system operation.

##### 5.3.1.2.2 F&G system design

The signals for flame detectors are read in as analog values by an analog input module. A current represents the state of the flame detector. Between the analog input and the detector an EX-barrier and an analog termination module is installed.

The analog to digital converted value is read by the two CPU's via one PBC module.

The input/output area for F&G is single channelled. The PBC is used to connect the I/O of the process bus to both processor busses of the two redundant CPUs. The processing is done by one master CPU, the slave CPU is running in an hot standby mode. The outputs are commanded by the master CPU, inputs are read by both CPUs.

Digital outputs are used to drive the actuators via digital output termination modules and an EX-barrier. The state of the actuator is read back by an analog input module and an analog termination module via an EX-barrier.

A current in the range of 1 to 20 mA represents the state of the actuator.

### **5.3.1.2.3 F&G fault detection**

Faults in the wiring to the analog input module are detected by changes to expected value. Any changes to the expected value represent an alarm state and are signalled accordingly.

#### **5.3.1.2.3.1 Analog input (F&G)**

The considerations are the same as for the ESD system, except that in the F&G application analog input is a single channel system. One failure in the analog input module can cause the CPU to read a wrong value.

#### **5.3.1.2.3.2 Access to bus controller**

A failure in the PBC or on the single process bus can prevent the CPUs from setting the outputs.

If communication on the process bus to the output modules is lost, the outputs switch to a pre-defined state.

#### **5.3.1.2.3.3 CPU**

Between the master and the slave CPU a hardwired link is established. When the master CPU fails, the slave CPU takes over to control the output modules.

#### **5.3.1.2.3.4 Digital outputs**

The fault assessment for the digital output showed, that one fault can prevent the correct setting of the output.

The CPUs can detect this fault, when the actuator is driven and the feedback by the analog input shows no response.

Furthermore a fault in the digital output module can drive the actuator to an unintended state.

#### **5.3.1.2.3.5 System design for the mimic panel**

Switches on the mimic panel are read in by one MPC with one contact only. The communication to the master and slave CPU is via an SS&CC card. The SS&CC card is controlled by the watchdog of the two CPUs. The master CPU can command the MPC to set outputs. The CPU can also command the MPC to send its input values. Both CPUs can receive the messages from the MPC. Indicators on the mimic panel consist of one lamp per housing.

#### **5.3.1.2.3.6 Communication paths**

The communication between the CPU and the MPC and the communication between master and slave MPCs is checked by telegram checksums. Fault effects are discussed in a subsequent chapter.

#### 5.3.1.2.4 Interconnection of ESD and F&G system

The F&G system is connected to the ESD system by means of two digital output points. The digital output points are read by the ESD system via analog inputs. Activating these outputs from the F&G system will cause the ESD system to activate the ESD-level NAS 2.2.

#### 5.3.1.2.5 Fault detection of the interconnection of ESD and F&G system

As detailed in the detailed analysis, the F&G system can unintentionally set an NAS level, or may not be able to set the NAS level.

The failures will not be detected by self tests or other automated measures.

These cases must be detected during maintenance intervals or by the installed network over duplicated ethernet cabling.

### 5.3.2 Detailed fault assessment on module level

All used modules were investigated on a component level. Possible faults and failures were considered in a fault and effect analysis.

#### 5.3.2.1 Central unit SBC 3003

The main processor board is made out of two microprocessor units. One unit contains the INTEL 80386, the other the INTEL 80376 microprocessor. This design was chosen to do a load sharing between the different tasks of the system. The two processors supervise the operation of each other and give alarm signals, should there be a problem on the CPU board.

Fault detection measures for the are covered by the BITE as described in the subsequent chapter.

#### 5.3.2.2 Digital output PDO 120

The PDO is an interface between the Process Bus and sixteen digital outputs. The digital output is a normally open relay contact with both terminals available for the user. A fail-safe state for each output can be defined by setting hardware straps (DIP switches) on the card. The fail-safe logic forces each output to the pre-defined state whenever the a "dead" BUS situation occurs. The status of each relays can be read back by a second set of contacts.

The following fault assessment was made:

- A failure in the address-decoder circuitry may cause the card to be selected never, always or at more than one address.
- A failure in the "dead" BUS circuitry may cause that the outputs will not be set to the safe state if a "dead" BUS situation occurs.

- A failure in the relays and relays driver circuitry may cause the outputs not to go to the commanded state.
- A failure in the relays read back circuitry may cause the read back of data which does not represent the actual state of the relays.

The correct operation of the relays is exercised during the maintenance inspections. The maintenance checks are necessary, because the used relays do not have positively guided contacts. Therefore the read back contacts do not guarantee to show the actual state of the relays.

### 5.3.2.3 Digital input PDI 120

The PDI 120 is an interface between the Process Bus and sixteen isolated digital inputs.

The digital input can be tested by writing test data to it and reading it back.

The following fault assessment was made:

- A failure in the address-decoder circuitry may cause the card to be selected never, always or at more than one address.
- A failure in the input circuitry where two input points are shorted is only detected when the input points are neighbouring. This is due to the fact that the inputs are not tested per point but with four pattern only.  
A failure in the test circuitry can cause that the data which are read by the PCU are the test data instead of the actual input data.  
A failure in the optocoupler can cause that a change of the input can not be detected.

This case would be detected by different behaviour of the two channels in the emergency shutdown system.

### 5.3.2.4 Analog input PAI 121

The PAI is an interface between the Process Bus and sixteen analog inputs. Optocouplers isolate the PCU Process Bus galvanically from the analog inputs.

Fault assessment:

A failure in the analog to digital conversion circuitry will be detected only if the failure is revealed by the two test voltages. Furthermore the fault detection depends on the selected input signal range for the analog input.

Some possible failures in the analog multiplexer will be detected by the test voltages. Some failures can be detected only if all analog inputs are connected to the field.



### 5.3.2.5 MPC 101

The MPC is a controller which can interface a host computer to a LED Matrix of max. 8x10 LEDs and a switch matrix of max. 8x12 switches. Large panels can be built from up to 16 MPCs controlled by the host computer through only one serial line.

Fault assessment:

A failure in the output circuitry of the MPC will not be detected.

A failure in the input circuitry of the MPC will not be detected.

Faults can lead to the situation that the MPC sends a wrong switch state to the host.

Faults can lead to the situation that the MPC is not able to switch the indicators to the commanded state or that the MPC switches indicators although no command was received from the host.

### 5.3.3 Hardware tests

The data of the used test- and measuring equipment is archived together with the testing protocols. The storage is done within the premises of the testing institute together with the other supplied documentation.

#### 5.3.3.1 Fault simulation

A set of fault insertion procedures was compiled and described in the documents MB.EI171 - 4004, "FAT Procedure Emergency Shutdown System TÜV Verification Phase 2" and MB.EI171 - 4004, "FAT Fire & Gas System TÜV Verification Phase 2". Parts of these tests were repeated, both on randomly chosen and on deterministicly points.

All inserted faults on signal lines, which were shorted against ground, signal ground or supply voltage were detected by the system.

Due to the construction of the test of the output cards a short between adjacent supply lines to the field will not be detected. The problem can be solved as described under the chapter "Suggested Measures", "Field Wiring to ESD actuators".

#### 5.3.3.2 Electromagnetic compatibility (EMC)

For EMC testing for the Heidrun installation the set-up, as installed in the premises of TÜV Rheinland, was used. All testing was performed on the system while it was running. The tests were done to stress both, hardware and software of the system.

Main attention during the tests was paid to the overall system behaviour. It was tolerable, that parts of the system during some tests showed functional disturbances. However, the whole system should not behave dangerous or unpredictable.

The following table lists the performed tests.

Test No.	Test name	Referenced standard	severity						
1	ESD, electrostatic discharge	IEC 801-2	level 3: 8 kV (air) 6 kV (contact)						
2	burst test	IEC 801-4	levels: signal lines, analog and digital I/O-lines: 1 (0,25 kV) power lines of boards: 1 (0,5 kV) internal power lines: 2 (1 kV) power lines AC or DC: 3 (2 kV) I/O-lines > 24 V: 3 (1 kV) duration: 10 sec.						
3	surge	IEC 801-5	levels: power lines: 3 (2 kV) signal lines, analog and digital, I/O-lines: 2 (1 kV) pulses: 10 pos. and 10 neg.						
4	immunity to conducted disturbances	IEC 801-6	range: 0,15 - 80 MHz levels: signal lines, data lines: 2 (3 V) power lines: 3 (10 V)						
5	variation of frequency of AC-power sources	DIN EN 61131-2	<table border="1"> <thead> <tr> <th><u>rated frequency</u></th> <th><u>range</u></th> </tr> <tr> <th>Hz</th> <th>Hz</th> </tr> </thead> <tbody> <tr> <td>50</td> <td>47,5 - 52,5</td> </tr> </tbody> </table> duration: 30 min.	<u>rated frequency</u>	<u>range</u>	Hz	Hz	50	47,5 - 52,5
<u>rated frequency</u>	<u>range</u>								
Hz	Hz								
50	47,5 - 52,5								

**Table 3:** Suite of electromagnetic compatibility (EMC) tests:  
 (Device under test in operation)

Compared to the test suite proposed in the concept review the suite of tests was slightly adjusted to take into account the specific conditions on the Heidrun platform.

The tests were performed as means of in situ measurements. All test equipment was moved to the test system. The results of the tests are compiled in the separate report TÜV Rheinland Product Safety with No. P 9611 443 E01. The EMC testing ended with positive result for the whole system. The following was observed during the tests:

**- Susceptibility to electrical noise**

The system is susceptible to electrical noise (surge and burst). If parts of the system were affected by "electrical noise", the safety action by the operator panel of the test cabinet could be done in each case (Manual callpoint worked). This is why the overall result is positive.

- **Unknown system state**

There was a system state, during that the system could not be reset by "kvittering" and "tilbakestill" from the operator panel of the test cabinet. However, "kvittering" and "tilbakestill" worked from the operator control unit (OCU). This system state could be repeatedly reached by putting burst pulses to the power-lines. This state can also be reached, from time to time, after a power restart. This state is obviously a software problem. It is not evident, whether it is caused by application, or by system software.

Because intensive re-testing is required after a software change, this problem should be solved only when a major change of the software is done.

- **AIM 1000 keyboard**

The multi-purpose AIM 1000 keyboard was extremely sensitive to electrical noise. Although the OCU was not considered during Heidrun approval (because OCUs are not needed for the operation), it has to be remarked, that the keyboard had to be disconnected during the test to get no further perturbation during testing. After disconnection of the keyboard, system information could be observed on the screen of the OCU during the tests.

The alarm-keyboard, which is the special keyboard with all area configured to fixed buttons, did not show these problems.

- **Serial lines**

The serial lines were susceptible to electrical noise as used in the test plan. Serial lines are used between the OCU and the two keyboards and as a connection between the BS 100 and the PCUs. The effects were not repeatable in each case. The operator keyboard of the AIM 1000 had to be disconnected from the OCU. In this case it was not clear, which part of the installation (OCU, shielding of the serial line or the keyboard) was responsible for the problem.

- **Reset of BS 100**

There were many resets on the BS 100 fire central during testing. In each case the reset brought the BS 100 back to normal operation. It could not be distinguished between BS 100 internally commanded resets, and reset command caused by faulty telegrams on the serial line from the SBC 3003.

- **Ethernet network**

The ethernet network (which is not needed for system operation) was disturbed during testing. This could be observed by lost connections from the PCUs to the OCU.

- **Panel controller MPC 101**

The panel controller also stopped in two cases and could be brought back to operation only by switching them on and off again. This behaviour was not considered critical because of the redundancy of the MPC in the ESD installation.

- **Stop of PCU**

During the EMC measurements the PCUs stopped during the direct influence phases to the individual PCUs. Because of the redundant PCUs, both in the ESD and the F&G cabinet, the operation of the whole system was guaranteed in each case.

**5.3.3.3 Climatic and environmental tests**

The temperature and shock tests were done on board basis. The boards were out of operation. The steps 1, 2 and 3 were combined. After this test a function test of the modules was done. Also the tests 4 and 5 were combined. The main scope of this test was to detect systematic hardware or production faults of the components.

Most of the components used in the Heidrun installation were already tested environmentally according to the suggested test suite by TÜV Rheinland. For those components copies of the test reports were handed over to TÜV or sent over directly by the manufacturer (AUTRONICA).

On basis of these considerations one sample of the following components was checked out of operation:

- MPC 101
- SBC 3003
- PAI 121
- PDI 120
- PDO 120
- PIOC 100
- SS & CC
- power supply D 6017 (48 Volt to +/- 5, +/- 12 Volt)
- power supply SIMRAD PSU-100 (48 Volt to + 5 Volt)
- power supply POWEC PMP 6.24 SIC (220 Volt to 24 Volt)
- power supply POWEC PMP 6.48 SIC (220 Volt to 48 Volt)

The following table shows the suite of tests, which was performed:

Test No.	Test name	Referenced standard	severity
1	cold, test Ab	IEC 68-2-1	- 25°C, 96 h
2	dry heat, test Bb	IEC 68-2-2	+ 70°C, 96 h
3	damp heat, cyclic test Db	IEC 68-2-30	high temp.: 55°C cycles: 2
4	shock, test Ea	IEC 68-2-27	halfsine, 15 g, 11 ms, 3 shocks in each axis
5	vibration, test Fc	IEC 68-2-6	range: 10 - 57 Hz amplitude: 0,075 mm range: 57 - 150 Hz, 1,0 g speed: 1 oct./min. cycles: 10 in each axis

**Table 4:** Climatic and environmental tests:  
 (Device under test out of operation)

All modules passed the tests.

#### 5.4 Software

The Extent of the software to be considered can be subdivided into the following categories:

- Firmware on the PCU (SBC 3003)
- operating system on the PCU
- application program
- configuration software

The specific modules are covered under the subsequent chapters. The inspection the software was divided into the following steps:

- Inspection of the software documents with regard to  
 completeness  
 consistency
- Inspection of specification documents of the software with regard to  
 completeness  
 interfacing  
 test procedures  
 compliance with the module specification
- inspection of source code  
 compliance to the specification  
 checking the software structure with applicable tools (lint for "C", PROMET for assembly language)
- Working out of test procedures and test patterns
- Carrying out of function tests during the integration test

#### 5.4.1 Operating system of the PCU SBC 3003

The operating system of the PCU SBC 3003 consists of several layers and is identical for the ESD and the F&G system. The operational parts are extensively exercised by the normal operation of the system. The storage of the operating system AIM 1000 is different from many other programmable systems and PLCs, where the firmware is kept within an EPROM and the application program is stored in battery back-upped RAM memory. In the AIM system a very small bootstrap loader is kept within the EPROM, all other software is loaded via ethernet from one of the connected server discs.

The layers are Basic Software, AIM Basic, Modules.

The Bite System (see separate paragraph) as part of the operational software was implemented to perform a permanent self check of all relevant parts of the microprocessor system.

The operating system of the CPU was checked in a walk through manner during the visits at SIMRAD in Kongsberg with the responsible persons for the several layers.

Most of the source-code is written in the "C" programming language. A few time critical parts are coded in assembly language.

The procedures and standards, how software has to be developed within SIMRAD, are documented within the company software handbook.

Tools have been used to make the software development more reliable. Among them are the advanced syntax checker lint, GNU - pedantic, and Purify for on-line supervision of the programs (array subscripts out of bound, using freed memory, using uninitialised memory, use of null pointer, memory leaks).

Originally it was planned to assess the software by means of an additional static analysis for the "C" sources. It turned out, that static analysis of the sources was already done as part of the development process. During the inspection the analysis methods and used tools within SIMRAD were discussed. Suggestions were made for additional future coding standards.

During the inspections of the operating system no problems or errors could be identified.

#### 5.4.2 Firmware on modules of the system

All peripheral cards (digital and analog I/O) are made of components, which do not carry a microprocessor. Therefore no firmware is used on these components.

Microprocessors, and hence firmware, is used on two other parts of the Heidrun ESD and F&G system: on the modular panel controller and the BS 100 fire central.

The firmware in the BS 100 fire central is covered in a separate chapter.

Several modular panel controller are used within the alarm panels and within the alarm keyboard. The firmware for the MPC is written in "C" and parts of it have been written in assembly language.

The software was inspected for measures to detect failures. The sources were written in a way, that they could be understood very well. The assembly parts of the software were checked by means of a static analysis of the sources (PROMET). The static analysis gave normal figures regarding complexity, length of the modules and other significant figures.

No evident problems regarding the source code of the MPC could be identified.

#### 5.4.3 Modular panel controller MPC 101

The modular panel controller is used at different places within the set-up:

- panel for ESD (duplicated)
- panel for F&G (single)

The following table shows the measures within the software of the MPC to detect failures:

Functional element	Implemented test
Communication to PCU	Test, high efficiency (Checksum)
I2c Communication to other MPC	Test, high efficiency (Checksum)
Stackpointer	Test, simple efficiency
Watchdog ( within CPU)	Used, not tested
External RAM	Test, simple efficiency
Internal RAM	No test
EPROM	No test
CPU	No test

**Table 5:** Overview of implemented MPC tests

The MPC alone is not suitable for safety critical applications. The most critical parts of the MPC are the communication paths to and from the PCU and to the other MPCs. These paths are supervised by measures of high quality. In addition to the measures on the electronic part of the MPCs there is constant supervision of the MPCs by an operator, as the MPCs are used as operator interfaces.

A failure effect analysis on top level shows, that the measures, which are implemented, are sufficient for this specific application:

	Assumed Fault	Fault detection	Reaction
1	Lamp lit, but no command sent	Operator sees lamp, conflict to reality	- Lamp test, - Replacement
2	Lamp defect	lamp test	Replacement
3	No communication MPC <-> PCU	Communication supervision times out	Maintenance
4	Loss or disturbance of telegrams	telegram check	Re-transmission
5	MPC sends button pressed, but no button pressed	Operator recognises	Not specified
6	Button pressed, but corresponding lamp not lit	Operator recognises	Not specified
7	One button pressed, but two or more lamps are lit	Operator recognises	not specified
8	Buzzer defect	Operator recognises during "lamp test"	maintenance

Table 6: Fault effect analysis for MPC tests

#### 5.4.4 Configuration software for I/O modules

The configuration is done on a host system using configuration tools in combination with a manual change procedure. The configuration, which was chosen for the system, can be checked on-line with the combination of PCU and OCU. It was possible with the installed system to do the basic check of the connected signals to the field. Also the used software modules and their parameter can be checked on-line. It is, however, not easy to get an overview over the complete application without a printed copy of the application program.

#### 5.4.5 Programming software

The programming of the system is done in several steps on a UNIX environment. The system is very flexible and can be programmed in many different ways, using computer based tools, databases and data-dictionaries for support.

The application is represented in form of cause and effect matrices. The correct implementation of these matrices is verified during the commissioning process. This process covers all layers of the implemented application program.

Samples of the used cause and effect matrices used to derive the application program were inspected. No anomalies were found.



#### **5.4.6 Simulation of the AIM system**

The total AIM system (PCU and OCU) is simulated on the development computer system at SIMRAD. This simulation includes the possibility to run the identical application program (Heidrun application) to the program as used on the actual AIM 1000 computer. The SIMRAD computer system is based on the UNIX operating system.

This simulation is a very powerful method to find and identify errors in the software, both in the application program, and in parts of the system software.

Two different systems exercise the same application program. As long as both systems react the same way, the probability for hidden errors is low.

The measure of complete emulation, resp. simulation, of the software is a measure of high quality and efficiency to detect systematic faults. These faults could be hidden in one software and the effects of the fault could be masked out in one system. The probability, that faults identical software are undetected in two systems with different operating system, which vary in many components, is low.

This simulation covers aspects of system and application software.

#### **5.4.7 BITE system**

The BITE system (Built In Test Equipment) was developed in direct response to the findings of concept review of the Heidrun verification project.

The BITE system is able to detect problems and faults, which are related to the electronic parts of the CPU boards PCU 3003. Also timing problems can be detected by the BITE system.

The BITE system was installed on the test system during the phase II verification and was exercised on the test system for over six month on the actual installed test system.

The test procedures for the BITE program, which were worked out by SIMRAD to check the BITE system, were repeated with success. The programmers handbook was checked by a walk through together with the author of the BITE system. The parts of the tests, which could not be repeated, were checked on document basis.

There are several modes of the BITE system to allow a controlled way of introduction of the system into an existing application. Depending on the requirements detected errors can be indicated and alarmed by the BITE system, but the CPU is not shut down on detection of errors.

In a redundant, operator controlled application (like e.g. Heidrun) there is no gain in safety by shutting a PCU down in the event of an detected error by the BITE system. It is guaranteed, that BITE messages on the operator controls (OCUs) are not overseen, because they have high priority (they are printed in red colour). By operational measures it is guaranteed, that these messages are recognised and a feedback is triggered to SIMRAD, should there be any messages and hence problems.

## 5.4.8 Software changes

### 5.4.8.1 Software changes to the operating system

Software changes to the operating system should be done with great care. Normally there should be no need to change the operating software. Even if problems are found within the operating system, the overall impact of a change should be considered.

### 5.4.8.2 Software changes to the application program

Each software change of the application program should be considered very carefully. After each software change the system should be checked on the simulation system. The changes all related parts of the system have to be re-inspected.

Software in this regard means the operational change of connections between function blocks. Necessary changes to values within SW Modules (which might be necessary for drift reasons) must be documented, but don't need this extent of re-testing.

Addition or removal of additional logic elements should only be done after a well documented procedure, e.g. using a form sheets of the SIMRAD software handbook.

## 5.4.9 Quality assurance measures for software

Within SIMRAD a programming standard is established and documented in the Software Handbook "Retningslinjer for styring av software-utvikling og produksjon".

During the inspection of the software a copy of the handbook "Retningslinjer for styring av software-utvikling og produksjon", Kopie 133, 01-Jul-1994, was available. This document describes the measures for quality assurance within SIMRAD Norge.

Besides description of the software life cycle model used within SIMRAD, also the requirements for software production are specified.

Forms are given to handle all phases of the software life cycle, including software test and software modification.

The forms, which are documented within the software handbook have been used for software development. Samples of filled out forms were shown during the visits at SIMRAD in Kongsberg.

#### 5.4.10 Integration test

With the knowledge of the detailed analysis of hardware and software the installed system was investigated according to a specified test scenario. The integration test was performed by triggering all inputs and checking that the correct reaction of the system occurred. After the update to the latest operating system version the system ran without interruption for over six months. The protocol printer was connected to the system all the time to print out any unexpected event.

No safety relevant faults have been observed.

#### 5.5 Fire and Gas fault detection system

The design goal of the Heidrun system was to be able to handle each single fault. This obviously guaranteed by the complete redundant system design of the Emergency Shutdown System.

The Fire and Gas part of the system is dual channel in the CPU portion, single channelled in the I/O part. The following table shows on top level consideration, that one failure of the system can also be handled by the system.

Assumed Fault	Fault detection	Reaction
Event (Heat, Fire, etc.) not detected by one sensor	Discrepancy to redundant sensors	Sensor repair
Event (Heat, Fire, etc.) detected falsely by one sensor	discrepancy to redundant sensors	Sensor repair
redundant sensors don't detect an event	diversity of sensor signals (smoke, heat, flame, manual call point)	Repair
Both F&G PCU stop	Watchdog times out	Digital Out Card goes to pre-selected value
Digital Out Card goes to pre-selected value	ESD system recognises F&G demand	Partial shutdown
Stuck of Interprocessor link and Slave PCU fault	Alarm via ethernet connection	Repair

Table 7: Fault detection in the F&G section of Heidrun

#### 5.6 Consideration on the AUTRONICA BS 100

The fire central AUTRONICA BS 100 is an integral part of the Fire and gas system of Heidrun. The unit is capable of working standalone. In this case it is used and interfaced as a part the fire & gas system, which is commanded by the SIMRAD SBC 1000 system.

### 5.6.1 Environmental tests on BS 100

Tests comparable to the tests proposed in this test plan were done on all parts of the BS 100 fire central. The documentation of the performed tests was provided directly by the manufacturer AUTRONICA and is listed in the appendix.

Because the BS 100 is integral part of the Heidrun system (via cabling), the influences of the performed EMC tests listed in table 3 were imposed also to the BS 100.

During all performed tests and during the integration testing no failures or outages could be observed on the BS 100.

### 5.6.2 Software architecture

The software of the AUTRONICA BS 100 was developed with the high level language Modula-2. A structured design method (Yourdon Workbench) was chosen for the specification and development of the system.

The used run time system on the BS 100 supports run time handling of software errors, e.g. a division by zero would be detected and accordingly alarmed to the controlling system.

The communication paths to the sensors are software controlled in the fire central. The actual sensors contain no microcontrollers, but are made of discrete logic. The protocol of the individual sensors is adjusted by means of hardware straps.

During the inspection cycle the overall concept and the software specification was discussed in a walk through manner with the software developer. No anomalies were found.

### 5.6.3 Operation experience

The parts, which are used within the Heidrun system are proven in operation. The parts are taken from normal production line. The adaptation to the AIM 1000 system is done by means of a serial connection. During the test of the test-sample it was verified, that alarms from the AUTRONICA systems are signalled in each case to the main system. A polling algorithm within the AIM 1000 system guarantees, that each alarm will be signalled to the operator.

### 5.7 EX-protection

Proper isolation against field influence is guaranteed by using barriers from the companies STAHL and PEPPERL & FUCHS. These components are certified by the PTB (Physikalisch Technische Bundesanstalt, Braunschweig) to be sufficient for the use in EX-areas. Therefore these components were not further investigated.

## 5.8 Test protocols, used investigation and measuring tools

The used investigation and measuring tools are documented together with the protocols of the respective investigation. This is also true for all material stored on electronic media and printouts of source code and listings. This material will be stored for a period of ten years within the rooms of the test location, together with all other documentation supplied for the investigation.

## 6. Suggested measures

The system operators and maintenance manuals (doc.no. MB EI 171-0426 to doc.no. MB EI 171-0429) have to be followed. The suggested measures of this report must be implemented during maintenance working packages.

### 6.1 Operator and maintenance handbooks

The Operator and Maintenance manuals for the ESD and F&G part describe the system. During operation of the system it should be evaluated, if the people, who use it, want to have changes to it.

One addition must be made concerning the sounders of the ESD system:

The alarm sounders (buzzer) on the alarm panel of the ESD system are duplicated. This ensures an audible alarm, even if one buzzer fails. To ensure, that one buzzer fault on the ESD panel is detected, the buzzers are at different pitch.

By this measure the tone is an interference between two pitches. The two different pitches of the sounders can be heard during the lamp test on the ESD system, when the tests on the two PCU don't start simultaneously, but with a short time delay.

Because of the relevance of an audible alarm to the whole system, a reference to this behaviour must be included in the manual, including the check of the sounders.

## 6.2 Power supplies

At the test set-up which was used at TÜV, the removal of one power supply in the ESD system was not detected under certain circumstances. This is equivalent to the possibility, that these supplies could fail in a mode, which is not detected by the system.

The ESD power supply system is redundant, and within each channel the power-supplies are again redundant. In addition, the complete loss of power would bring the system into a safe state. For these reasons the observed behaviour is not safety critical.

On the F&G part only the power supplies for the I/O area are redundant. The removal of all other power supplies is detected.

The actual implementation of the power supplies on the Heidrun platform for the ESD system and the I/O part of the F&G system should be checked regarding the behaviour of the system, when individual power supplies are being removed. It is recommended, that additional periodic measures shall be included in the maintenance manual to ensure the integrity of the power supplies.

## 6.3 EMC compatibility

During the investigations of the test set-up we observed a high sensitivity for electromagnetic fields as defined in the test plan. This behaviour has been detected before by other investigations and adequate measures for shielding have already been made.

During the tests many partial problems of the set-up could be seen. In no case the overall application run into a situation, where the safety action could not be performed.

The specific EMC - conditions of the Heidrun installation should be analysed. If there are reports from Heidrun about electromagnetic compatibility problems, appropriate changes for the Heidrun installation are recommended.

## 6.4 Modular Panel Controller MPC 101

The self test software of the MPC 101 should be made more efficient. The measures, which are already implemented in the BITE system of the SBC 3003, should be adapted and ported to the MPC 101 for better error detection. At the moment the operator has to react to certain kinds of errors. For future versions of the MPC more automatic fault detection should be implemented.

The MPC 101 hardware should be made more resistant to EMC interference. This should be done by a combination from hardware and software measures. The reaction to internal electronic faults should be done by the system rather than needing the operator intervention.

It is not recommended to exchange the already installed base of MPC 101 with an updated version according to the suggested measures. However, necessary replacements should be done with an updated MPC 101.

## 6.5 ESD: Field wiring to actuators

Testing of the outputs of the ESD system is done by variation of the field supply voltages of the redundant channels. This checking is done for a group of actuators at the same time.

For this reason any shorts between the wiring of one tested group to the actuators is not detected. This behaviour does not have an impact on safety: Removing power to one ESD actuator would shut down more actuators than the intended one.

On the other hand, if the command is given to de-energise, and the respective actuator does not react because of a short to its neighbour, this is detected by the read back devices connected directly to the actuators. This overall behaviour has, however, an impact on the availability of the application. Therefore it should be considered to test the ability to switch actuators independently within one output group on a routine basis.

## 6.6 F&G: Periodic check of duplicated PCUs

The F&G system is built with two PCU 3003. These PCU are configured as one being permanently master, and the other being permanently slave. The health status of both PCUs is supervised by the duplicated ethernet network. By this set-up the switching between master and slave is never exercised, with the exception, when the master PCU fails. To increase availability, once each year or shorter (during regular maintenance intervals) the master PCU should be reset to check the proper operation of the master/slave switching mechanism.

## 7. Summary of the verification

The Heidrun Emergency Shut Down (ESD) and Fire & Gas (F&G) System was investigated according to the German DIN 19250 and DIN V VDE 801 as microprocessor based system with safety features.

The testing was essentially divided into the following points:

- safety concept
- theoretical hardware inspection
- practical hardware testing
- software analysis
- software test
- software and integration (software/hardware) test
- user interface of the application
- quality assurance measures at SIMRAD

The tests were performed as described under the individual sections. The detailed results are archived in the test lab of the ISEB.

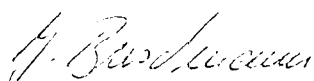
The Emergency Shut Down (ESD) part, built as complete redundant system, fulfils the requirements of safety class 6 for the designed application of the Heidrun platform.

The Fire & Gas (F&G) System is made redundant in the CPU part (hot standby), and single channel in the I/O part. It fulfils safety class 4 for the designed application of the Heidrun platform.

The system operators and maintenance manuals (doc.no. MB EI 171-0426 ff.) have to be followed. The suggested measures of this report must be implemented during maintenance working packages.

Cologne, 1996-10-28  
ISEB/Kst. 945-bu-pl-nie

The inspectors



Dipl.-Ing. Johannes Buschmann



Dipl.-Phys. Ekkehard Pofahl





## TÜV - PHASE II DOCUMENT LOG

KE/CNI DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	EMC Testing of Heidrun DCSS Scope of Work	MB-J-YS-690	0	08.02.1995	104	AL	22.03.1995
	EMC study of Heidrun DCSS Report	2355	2	24.11.1994	74	KKN	22.03.1995
	Technical Note AIM Safety Systems Health nad Modification Control	\\uv-2\dokument\health.doc	1	22.05.1995	6	LYC	22.05.1995



Appendix A of Report-No.: 945/EL 337/96

## TÜV - PHASE II DOCUMENT LOG

### HARDWARE DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	SBC 3003 Hardware Manual	\\utv\3000\coc\hw3003\*	2	27.08.1993	35		
	SBC 3003	AIF 37918281	1		28		
	AIM 1000 BP	AIF 37914942	1		20		
	SBG 3000	AIF 37914157	1		10		
	AIM Disk	AIF 37921962	1		12		
	MPC 100	\\divdoc\mpc\hwnote4.txt	4	17.12.1992	27		
	MPC 101	AIF 37925542	1		18		
	TBMPC-GEN	\\divdoc\tbmpc\gen\hwnote4.doc	4	13.05.1993	21		
	TBMPC 16SL	AIF 37928314	1		10		
	PAI 121	\\divdoc\pai121\hwnote1.doc	2	27.08.1993	12		
	PDI 120	O7784648	1	03.04.1989	4		
	PDI 120	AIF 37759206	1		16		
	PDO 120	O7784655	1	06.05.1988	4		
	PDO 120	AIF 37759172	1		17		
	PB 115	AIF 37921632	1		8		
	PBC 100	\\files1\hw\pal\pbc_100\doc\hwn.txt	1	03.03.1992	16		
	PBC 100	AIF 37923299	1		8		
	PBC BP	AIF 37923265	1		4		
	TBAIR	\\divdoc\tbair\hwnote1.doc	1	25.01.1993	11		
	TB AIR 2	AIF 37933819	1		8		
	TB-CNTRL-XX	\\divdoc\tbcntrl\hwnote1.doc	1	09.09.1992	12		
	TB CNTRL 2.5A	AIF 37926086	1		8		
	TB-DI ISO	\\divdoc\tbdiso\hwnote\hwnote_2.txt	2	22.01.1993	14		
	TB DI ISO	AIF 37926003	1		8		
	TB-ESD-1	\\divdoc\tbesd\hwnote1.doc	1	09.09.1992	12		
	TB ESD 1	AIF37926003	1		7		
	TBSL	\\divdoc\tbsl\hwnote05.txt	5	23.10.1992	23		
	TBSL	AIF 37766532	1		7		
	TBSL	AIF 37767449	1		7		
	TBSL	AIF 37767522	1		7		
	TBSL	AIF 37767563	1		7		
	SS&CC	\\divdoc\ss_cc\hwnote1.doc	1	13.08.1993	12		



Appendix A of Report-No.: 945/EL 337/96

## TÜV - PHASE II DOCUMENT LOG

### HARDWARE DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	SS&CC	AIF 37752789	1		14		
	Netswitch	AIF 37914330	1		12		
	Cheapernet Repeater	AIF 37759248	1		5		
	AIM Keyboard	AIF 37937448	1		6		
	Testproc. for PAI 121 Process Analog input	O7932346	4	31.12.1992	6	R.S.	20.03.1995
	Hardware note PAI 121	O7944259	2	27.08.1993	12	K.H.	20.03.1995
	PAI 121	3-777149	F	06.02.1990	1	I.O.	20.03.1995
	PAI 121 Process Analog input	3-7775915	-	10.08.1989	3	I.O.	20.03.1995
	Testproc. for PAO 121 Process Analog output		4	28.10.1992	6	R.S.	20.03.1995
	PAO 121 Process Analog output	4-791130	A	15.02.1990	1	I.O.	20.03.1995
	PAO 121 Process Analog output	3-791131	B	15.02.1995	4	A.U.	20.03.1995
	Process Analog output (PAO 121)	PAO-121 37911302, PAO-122 37937406	2	22.08.1988	5	K.H.	20.03.1995
	Process Analog output PAO 122	4-793740	-	30.08.1993	1	A.U.	20.03.1995
	Testproc. for PDI 120	37759206	1	12.03.1990	3	OKD	20.03.1995
	PDI 120 Digital Input	4-775920	-	01.03.1990	1	A.R.	20.03.1995
	PDI 120 Digital Input, Blocket schematic text	3-775921	-	01.03.1990	4	A.R.	20.03.1995
	Testproc. for PDO 120 Process Digital output	us\qa\dok\basism\ort\hw+proso\dy\o-kort\pdo120-3 doc	3	25.08.1992	6	R.S.	20.03.1995
	PDO 120 Process Digital output	4-775917	-	13.02.1990	1	A.U.	20.03.1995
	PDO 120 Process Digital output	3-775918	-	13.02.1995	3	A.U.	20.03.1995
	PPI 101 Process Pulse input	4-775794	A	23.03.1990	1	I.O.	20.03.1995
	PPI 10X Process Pulse input	3-775791	-	23.03.1990	5	I.O.	20.03.1995
	PBI15	3-792163	A	29.01.1992	1	B.E.	20.03.1995

## TÜV - PHASE II DOCUMENT LOG

### HARDWARE DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	PB115	3-792164	-	29.01.1992	2	B.E.	20.03.1995
	Testproc. for PBC 100, Process bus controller	37923299	1	24.02.1992	2	R.S.	20.03.1995
	Hardware note, Process bus controller	O7923360	A	03.03.1992	16	I.O.	20.03.1995
	PBC 100, Process bus controller	3-792330	-	14.01.1992	3	A.U.	20.03.1995
	PBC 100, Process bus controller	3-792329	A	14.01.1992	1	A.U.	20.03.1995
	Termineringskort TBAI	4-791306	A	09.01.1989	1	A.R.	20.03.1995
	Terminal board TBAI/DI/DO Analog input	3-791446	-	11.11.1988	2	A.R.	20.03.1995
	Terminal board TBAIR-2 Analog input	3-793382	-	22.02.1993	2	I.O.	20.03.1995
	TBAIR-2	3-793381	A	25.02.1993	1	I.O.	20.03.1995
	TBAIR	4-797106	B	09.01.1989	1	A.R.	20.03.1995
	TBAI/DI/DO Analog input	3-791446	-	11.11.1988	2	A.R.	20.03.1995
	Terminating board TBAO	4-792162	-	11.11.1988	1	A.R.	20.03.1995
	Terminal board type 10, Analog output	3-791168	-	11.11.1988	1	A.R.	20.03.1995
	TB-CNTRL-0.25A	3-792983	A	09.04.1992	1	I.O.	20.03.1995
	TB-CNTRL-XX	3-792609	-	06.04.1992	2	I.O.	20.03.1995
	TB-CNTRL-2.5A	3-792608	B	09.04.1992	1	I.O.	20.03.1995
	TB_DI_ISO	3-792582	-	23.03.1992	1	E.B.	20.03.1995
	TB_DI_ISO	3-792583	-	10.03.1992	1	E.B.	20.03.1995
	TB_DO_ISO	3-792585	-	08.04.1992	1	E.B.	20.03.1995
	TB_DO_ISO	3-792586	-	10.03.1992	1	E.B.	20.03.1995
	TBDO-ISO-2	3-793444	A	25.03.1993	1	I.O.	20.03.1995
	TBDO_ISO_2	3-793443	A	29.03.1993	1	I.O.	20.03.1995
	TB-ESD-1	3-792600	A	03.04.1992	1	I.O.	20.03.1995
	TB-ESD-1	3-792601	-	02.04.1992	1	I.O.	20.03.1995

## TÜV - PHASE II DOCUMENT LOG

### HARDWARE DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	TBDO-HS-D1	3-793753	-	10.02.1994	1	E.B.	20.03.1995
	TBDO_HSD1	793752	-	16.02.1994	1	E.B.	20.03.1995
	Termination board, Serial lines, TBSL	3-776654	B	13.08.1991	1	P.A.M.	20.03.1995
	Motherboard TBSL	3-776653	A	03.07.1991	1	T.T.	20.03.1995
	Power Adapt. TBSL	3-776744	C	09.07.1991	1	T.T.	20.03.1995
	TBSL Adapter	3-776745	-	07.06.1991	1	T.T.	20.03.1995
	RS232 Isol. Adapt. TBSL	3-776752	A	09.07.1991	1	T.T.	20.03.1995
	TBSL Adapter	3-776753	-	07.06.1991	1	P.A.M.	20.03.1995
	RS232 Unisol. Adapt. TBSL	3-776748	A	09.07.1991	1	T.T.	20.03.1995
	TBSL-Adapter Unisol. RS232 board	3-776749	-	07.06.1991	1	P.A.M.	20.03.1995
	RS422 Isol. Adapt. TBSL	3-776756	A	09.07.1991	1	T.T.	20.03.1995
	TBSL-Adapter	3-776757	-	07.06.1991	1	P.A.M.	20.03.1995
	Current Loop Adapter TBSL	3-776760	A	07.09.1991	1	T.T.	20.03.1995
	TBSL-Adapter	3-776761	-	07.06.1991	1	P.A.M.	20.03.1995
	Hardware note SS&CC	O7780687	1	13.08.1993	12	K.H.	20.03.1995
	El.sch. SS & CC	1-775279	-	30.07.1986	1	A.P.	20.03.1995
	Testproc. for MPC 100,101, Modular controller	37762606, 37764313, 37766847, 37925542	5	17.08.1994	8	P.A.M.	20.03.1995
	Hardware note, Modular Panel System	O7767957	5	14.12.1994	27	K.H.	20.03.1995
	MPC 101, Block schematic	3-792555	B	21.05.1992	6	P.A.M.	20.03.1995
	MPC 101	3-792554	B	09.06.1992	1	P.A.M.	20.03.1995
	Testproc. for termineringskort MPC	37928264	1	06.10.1992	4	R.S.	20.03.1995
	Hardware note, General MPC adapter, TBMPG-GEN	\\undivdoc\bmpcgen\hwnote5.doc	5	23.12.1994	21	P.A.M.	20.03.1995
	TBMPC-GEN General MPC Adapter	3-792827	-	27.07.1992	2	P.A.M.	20.03.1995
	TBMPC-GEN	3-792826	B	26.08.1992	1	P.A.M.	20.03.1995



Appendix A of Report-No.: 945/EL 337/96

## TJUV - PHASE II DOCUMENT LOG

### HARDWARE DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	TBMPC-16SL	3-792832	-	30.07.1992	2	P.A.M.	20.03.1995
	TBMPC-16SL	3-792831	-	28.08.1992	1	P.A.M.	20.03.1995
	Net-Switch	3-791432	B	21.07.1989	2	E.B.	20.03.1995
	Net-Switch	3-791433	B	21.07.1989	1	E.B.	20.03.1995
	Testproc. for Cheapernet Repeater	37758646, 377592248	2	21.10.1992	6	R.S.	20.03.1995
	Hardware note Cheapernet Repeater	O7932163	1	17.08.1993	10	P.A.M.	20.03.1995
	Cheapernet, Transceiver/Repeater	3-775924	F	06.09.1988	1	P.A.M.	20.03.1995
	SBC 300x Self Test SW Requirement Specification	\\qa\dok\basismod\basisssw\sbc3000\selfst1.srs	1	04.05.1995	7	HH	22.05.1995
	SBC 300x Self Test Detailed Design document	\\qa\basismod\basisssw\sbc3000\selfst1.ddd	1	16.05.1995	16	HH	22.05.1995
	Functional Description (FDS)	qa\dok\levpros\p611133\aim\s2151\dok\fdst1.doc	1	23.06.1995	44	LYC	29.06.1995



Appendix A of Report-No.: 945/EL 337/96

## TÜV - PHASE II DOCUMENT LOG

## SOFTWARE DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	AIM basic SW	type:\files5\aimprod\aim\wdoc\isprosla im\disc.doc	1	18.05.1994	1		
	BS 100	BS100MAS.TXT		18.05.1989	10 plus 8 plus 7		
	SD_DMEAS	\qa\dok\basisan\aim\ojegass\shutdown \modspec\sd_meas.m02	2	07.06.1994	14		
	SM_AMEAS	\usr\qa\dok\basisan\aim\ojegass\shutcl own\modspec\sd_ameas.m03	3	09.06.1994	16		
	SD_IN	\usr\qa\dok\basisan\aim\ojegass\shutcl own\modspec\sd_in.m02	2	09.06.1994	17		
	SD_MAIN	\usr\qa\dok\basisan\aim\ojegass\shutcl own\modspec\sd_main.m01	1	01.01.1994	11		
	SD_OUT	\qa\dok\basisan\aim\ojegass\shutdown \modspec\sd_out.m02	2	09.06.1994	15		
	RS_COMMS	\usr\qa\dok\basisan\aim\ojegass\bg\m odspect\rs_comms.m02	2	27.01.1994	2		
	FG_COM	\usr\qa\dok\basisan\aim\ojegass\bg\m odspect\fg_com.u01	1	27.01.1994	12		
	FG_IN	\usr\qa\dok\basisan\aim\ojegass\bg\m odspect\fg_in.m02	2	07.06.1994	14		
	DETECT_G	\usr\qa\dok\basisan\aim\ojegass\bg\m odspect\detect_g.m02	2	06.06.1994	19		
	SD_OTEST	\usr\qa\dok\basisan\aim\ojegass\bg\m odspect\sd_otest.m01	1	02.06.1994	20		
	FGD_STAT	\usr\qa\dok\basisan\aim\ojegass\gb\m odspect\fgd_st4.doc	4	27.01.1994	11		
	REDMOD	\usr\qa\dok\basisan\mod\sw\spec\redmod. m01	1	29.03.1993	14		



Appendix A of Report-No.: 945/EL 337/96

## TÜV - PHASE II DOCUMENT LOG

## SOFTWARE DOCUMENTATION

Doc.no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author	Date of shipment
	REDTRANS	\\usr\qa\dok\basismod\sw\spec\redtrans.m01	1	29.03.1993	9		
	SD_PANEL	\\usr\qa\dok\basisan\haim\oljegass\pcda\modman\sd_panel.m03	3	10.03.1994	10		
	MPC_CTRL	\\usr\qa\dok\basisan\haim\basis\mpmc\mod\mpc_ctrl.m03	3	17.12.1993	15		
	VALVE_DH	\\usr\qa\dok\levpros\p611101\aim\2132\sw\specer\valve_dh.m06	6	15.06.1993	13		
	ONB_IO	\\qa\dok\basisan\haim\oljegass\bg\mods\pec\onb_io.m02	2	27.01.1994	9		
	MANIN_D	\\usr\qa\dok\basisan\haim\oljegass\pcda\modman\manin_d.m04	4	18.06.1993	9		
	Functional Description (FDS)	\\qa\dok\levpros\p611133\aim\s2151\dok\fds1.doc	1	23.06.1995	44	LYC	29.06.1995



## AUTRONICA AS documents

Company	Doc. no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author
Lloyd's Register of Shipping	90/0287	Type approval certificate	Analogue addressable fire alarm panel		09.05.1991	4	
Autronica Industrial Limited	TE 80341	The Loss Prevention Council Technical Centre	Fire Alarm Systems - Technical evaluation of the Autronica Industrial Limited BS-100 automatic fire alarms system to B.S. 5839: Part 4: 1988		April 1992	42	G. Ash
Det norske Veritas Classification A/S	89-1100	Technical report	EMC Type Approval Tests of BS 100 Fire Alarm Central		29.09.1989	22	Per Gulbrandsen
Autronica Industrial Limited	294.90/G.02/JA.KHJ	Environmental Test Report C-80	BS-100, fire alarm panel		14.02.1990	8	Jens Asmul
Det norske Veritas Classification A/S	90-1048	Technical report	EMC Type Approval Tests of BS 100 Fire Alarm Central		25.06.1990	9	Per Gulbrandsen
Autronica Industrial Limited		Environmental Test Report C-97			24.11.1991	8	Jens Asmul
Det norske Veritas Classification A/S	91-1110	Report	Electromagnetic Compatibility Tests of Fire Alarm Equipment		26.11.1991	9	Per Gulbrandsen
ANPI NVBB	Verlag N° BFS/DE/163 1992.03.16	Autronica File No. C-111	Centrales BS100-BS60 Loopprocessor BS51 Detector BHH-31 Montagevoet BWA-40A/1 Kartsplitningsislator BK30		16.03.1992	62	E. d. Faille E. Briers
Det norske Veritas Classification A/S	93-1063	Technical report	EMC Testing of BS-100 Fire Alarm Central, and Auxiliary Equipment		18.03.1993	20	Per Gulbrandsen Are Larsen Pal Aksel Roum
Det norske Veritas Classification A/S	94-1144	Technical report	EMC testing of conventional and addressable fire alarm equipment		25.01.1995	21	Are Larsen Pal Aksel Roum

AUTRONICA AS documents

Company	Doc. no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author
Det norske Veritas Classification A/S	DN-121/679/94	Technical report	Autronica Fire Alarm Equipment Electrical Compatibility Addressable and Conventional Systems		25.10.1994	14 + 7	Svein Johansen Jan Oddvar Olsen
Det norske Veritas Classification A/S			Autronica Fire Alarm Equipment Electrical Compatibility Addressable and Conventional Systems		16.06.1992	10 + 7	
SISÄSIAINMINISTERIÖ	SM 794/91 4062/753/90		Akkuteollisuus Oy, PL 60, 02631 ESPOO		05.02.1991	1	
Securitas Teknik AB	RUS 113 F	Försäkrings Förbundet			April 1993	3	
Registro Italiano Navale	5/148/93	Free Translation of Certificate	Fire detection and fire alarm system type BS-100		28.07.1993	2	Giovanni Rebaudengo
USSR Register of Shipping	900.259.262	Type Approval Certificate	Fire Alarm Control Panel type BS-100, addressable system		11.06.1990	1	A. Samsonov
Sjofartsdirektoratet Norwegian Maritime Directorate	A-60726/90 JUF/TF	Sertifikat fortyegodkjennelse av skipsutstyr	Brannalarmsentraler - Fire Alarm Panels		10.07.1990	1	J. U. Follesdal
Norges Forsikringsforbund	94-1555/G. 11/MI/	Regler for Automatiske Brannalarmanlegg Pkt. 92. Materieell. Fornyelse	Sentralapparat, type BS-100. FG-godkj.nr.: S-022/89		01.12.1994	1	Erik Andersen
Department of the Interior National Chief of Fire Brigade UPEA Union Professionnelle des Entreprises d'Assurances	116/13/1993 6020z PL/AC	Certificate Anschreiben	Approval of Autronica's firealarm system		März 1993	2	Oszkar Jokai
					19.05.1992	2	P.P. Leroy

## AUTRONICA AS documents

Company	Doc. no.	Doc. title	Doc. name	Rev.	Doc. date	No. of pages	Author
American Bureau of Shipping - Equipment type approval program	GB23984-X	Certificate	Fire Alarm Panel BS-100		23.11.1994	1	Ch. Andersson
Autronica	BS100MAS.TXT	engineering document	BS-100 Software description (program overview)		18.05.1989	10	Svein Skogstad
Autronica		engineering document	program diagrams			8	
Autronica	ASAP-BS100-60	Technical description	Fire alarm system, type BS100	V6.0		8	Svein Skogstad Roar B. Johansen
Autronica	ASAP-BS100-60		Autronica Standard ASCII Protocol		95-10-26	19	