

2010-04-09

Automation, Software and Information Technology

**Test report about the examination of the changes
to the AIM Safety PLC System between
release 7.3.8 and 8.3.3**

**Report-No.: 968/EL 161.04/10
Date: 2010-04-09**

**Test report about the examination of the changes
to the AIM Safety PLC System between
release 7.3.8 and 8.3.3**

Report-No.: 968/EL 161.04/10

Date: 2010-04-09

Pages: 12

Test object: Changes to the AIM Safe System from AIM release 7.3.8
to AIM release 8.3.3

Customer/Manufacturer: KONGSBERG MARITIME AS
Kirkegardsveien 45, Carpus
3601 Kongsberg
Norway

Order-No./Date: JB-70371 dated 2010-01-24

Test Institute: TÜV Rheinland Industrie Service GmbH
Am Grauen Stein
51105 Köln (Poll)
Germany

Department Automation, Software and Information Technology

TÜV-Offer-No./Date: 968/150/07 dated 2007-06-04

TÜV-Order-No./Date: 10355325 dated 2010-02-01

Inspector(s): Dr. Peter Kocybik
Dipl.-Ing. Robert Heinen

Test Location: see Test Institute

Test Duration: August 2007 until April 2010

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. Scope	4
2. Standards forming the basis for the requirements	4
3. Identification of the test object	4
3.1. Test object	4
3.2. Documentation	4
3.3. Test samples	5
3.4. Previous test reports	5
4. Tests and test results	5
4.1. General	5
4.2. Description of changes between release AIM 7.3.8 and AIM 8.3.3	6
4.3. Description and evaluation of the changes associated with the implementation of the RBUS	6
4.4. Description and evaluation of the changes associated with the implementation of the PROFIsafe protocol	8
4.5. Description and evaluation of the updates to the NetIOSafe communication protocol	10
4.6. Description and evaluation of the changes associated with the implementation of the Redundancy Switch and System Surveillance	10
4.7. Description and evaluation of the changes associated with the implementation of the Software Watchdog	10
4.8. Description and evaluation of new hardware	11
4.9. Description and evaluation of changes to the development process	11
5. Summary	12

Appendix A1

1. Scope

Object of this inspection is the AIM Safe System from Kongsberg Maritime, 3601-Kongsberg, Norway, which has previously been type approved for release 7.3.8 (see /T3/). In the meantime the manufacturer has done several changes to the system. The changes are detailed in chapter 4.2.

Purpose of this type approval is to inspect whether the changed AIM Safe system still fulfils the requirements up to SIL 3 according to IEC 61508 for the use in safety relevant applications with low demand mode of operation.

2. Standards forming the basis for the requirements

- /N1/ IEC 61508 Part 1 to 7, 1998 and 2000**
Functional safety of electrical/electronic/programmable electronic safety-related systems
- /N2/ IEC 61511, Part 1 to 3, 2003 and 2004**
Functional safety - Safety instrumented systems for the process industry sector
- /N3/ IEC 61131-2:2007**
Programmable Controllers
Part 2: Equipment requirements and tests
- /N4/ IEC 60945:2002 (for environmental testing)**
Maritime navigation and radio communication equipment and systems -
General Requirements-Methods of testing and required test results
- /N5/ EN 50156-1:2004 (as far as applicable)**
Electrical equipment for furnaces and ancillary equipment -
Part 1: Requirements for application design and installation
- /N6/ EN 54-2:1999+AC:1999+A1:2006(as far as applicable)**
Fire detection and fire alarm systems -
Part 2: control and indicating
- /N7/ NFPA 72:2010 (as far as applicable)**
National Fire Alarm Code
Handbook

3. Identification of the test object

3.1. Test object

The AIM Safety PLC system from Kongsberg Maritime, Kirkegardsveien 45, 3601-Kongsberg, Norway, is a PLC system based on hardware and software components.

Object of the inspection are the incremental changes from AIM 7.3.8 to AIM 8.3.3 which are described in the AIM release notes, documents: 340594 and 343640.

3.2. Documentation

The documents provided by the manufacturer for the type approval are listed in the document list:

/D1/ Document_List_BT 1.4.4 (AIM 8.3.3)_rev2.xls, dated 2010-03-30

The following documents have been prepared by the test institute during the course of the inspection:

**/D2/ Functional and fault insertion testing for module RMP420S,
Kongsberg_FIT_RMP420_V5_2009-09-22.doc, dated 2009-09-22**

- /D3/** Functional and fault insertion testing Profisafe, Kongsberg_FIT_AIM8_x_Profisafe_V1_1_2009-09-28.doc, dated 2009-02-28
- /D4/** Functional and fault insertion testing RBUS and program sequence monitoring, Kongsberg_FIT_AIM8_x_RBUS_&_Prog_Seq_Mon_V1_1_2009-12-16.doc, dated 2009-12-16
- /D5/** Acceptance of test results for environmental and EMC testing, Anerkennung Umwelt EMV Kongsberg 8_3, dated 2009-12-08

3.3. Test samples

During the testing of the RMP420S the module with the serial number 21185 has been used, see /D2/. The sample will be archived by Kongsberg Maritime.

For the functional and fault insertion testing of Profisafe /D3/, RBUS and program sequence monitoring /D4/ no hardware test samples will be achieved by Kongsberg Maritime, because based on the test description the hardware can be re-constructed exactly as used during the tests.

3.4. Previous test reports

The following documents have been prepared during previous type approvals:

- /T1/** Type approval of AIM Safe Fault Tolerant and Fail Safe Controller System of Kongsberg Simrad
Report-No.: 968/EL 161.00/02, Date: 2002-01-31
- /T2/** Test report of the type approval of Remote Control Unit RCU including the upgrade of the AIM Safe System
Report-No.: 968/EL 161.01/04, Date: 2004-12-01
- /T3/** Test report about the inspection of the changes to the K Safe System from AIM release 7.2.0 to AIM release 7.3.8
Report-No.: 968/EL 161.02/08, Date: 2008-07-08
- /T4/** Test report about the examination of the changes to the AIM Safety PLC System release 7.3.8 and 8.3.3
Report-No.: 968/EL 161.03/10, Date: 2010-02-09
- /T5/** Test report about the examination of the software driver NetIOSafe Driver for a Safe network Communication system
Report-No.: 968/EL 606.00/09, Date: 2009-05-29

4. Tests and test results

4.1. General

The measuring and test equipment, which has been used by the TÜV Rheinland Group in the tests described in the following, is subject to regular inspection and calibration. Only devices with valid calibration have been used. The devices used in the various tests are recorded in the inspector's documentation.

All considerations concerning uncertainty of the measurements, so far applicable, are stated in the inspector's documentation, too.

In cases where tests have been executed in an external test lab or in the test lab of the manufacturer and where the results of these tests have been used within the here documented approval, this has occurred after a positive assessment of the external test lab and the achieved test results in detail according to the Quality Management procedure QMA 3.310.05.

4.2. Description of changes between release AIM 7.3.8 and AIM 8.3.3

The changes performed between AIM release 7.3.8 and AIM release 8.3.0 are described in document 340594. The main changes are detailed in the following. The previously certified communication bus PBUS has been replaced by a new communication bus called RBUS. The connection of certain devices using the Profibus with ProfiSafe protocol has been implemented. A new communication protocol called NetIO Safe has been defined. Further a new hardware module called RMP420S has been introduced which allows connection of analog input devices to the system. Further bug fixes and minor upgrade of the software functionality have been performed.

Between AIM release 8.3.0 and AIM release 8.3.3 the main change is to enable latching of fail-safe states for remote I/O (RIO) modules see document 343640. Further bug fixes and minor upgrades of the software functionality have been implemented.

4.3. Description and evaluation of the changes associated with the implementation of the RBUS

The new RBUS IO System provides geographically distributed (remote) IO controlled by redundant Process Stations (PSes) over a dedicated serial communication interface. The system provides a framework for developing different general purpose or specialized remote IO modules. The RBUS physical layer is a standard RS-485 communication line.

The 1oo2 RIO module configurations can be used for safety purposes. Two Process Stations read process input and are in control of the process simultaneously. It is a requirement that each Process Station makes decisions independently. When a Process Station fails, it will isolate itself from the process. The process is then controlled by the remaining Process Station alone. If this Process Station also fails, it will normally also isolate itself from the process and thereby cause a shutdown. This redundancy type does not support analog output signals and may be only used on low demand safety systems.

The following two 1oo2 RIO module configurations were examined:

- 1oo2 Single RIO
- 1oo2 Dual RIO

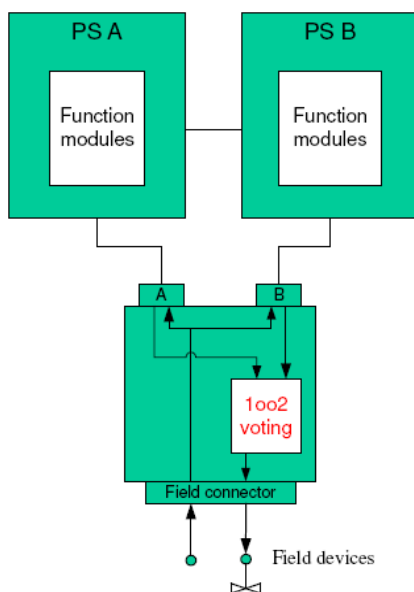


Figure: 1oo2 Single RIO (SIL 2)

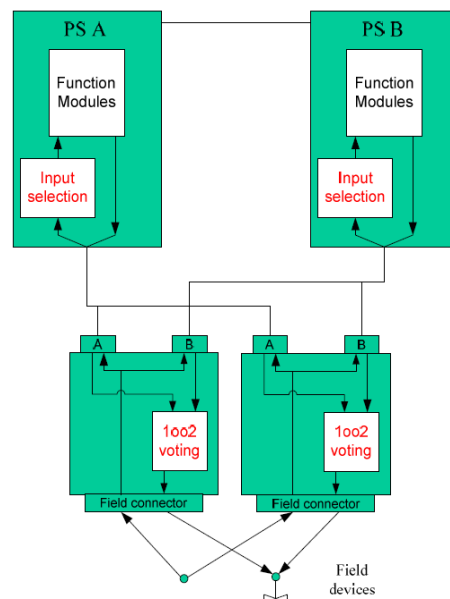


Figure: 1oo2 Dual RIO (SIL 3)

The RIO modules are in both cases connected to the Process Stations via two separate, independent RBUSes.

A special Input Signal Selection applies to the 1oo2 dual RIO redundancy topology. It ensures that the two Process Stations use separate input sources for their safety logic during normal operation.

Input Signal RIO A	Input signal RIO B	PS A Selection		PS B Selection	
		RIO	Status	RIO	Status
OK	OK	A	OK	B	OK
OK	Loop fault	A	OK	A	OK
OK	Not available	A	OK	A	OK
Loop fault	OK	B	OK	B	OK
Loop fault	Loop fault	Freeze	IO Error	Freeze	IO Error
Loop fault	Not available	Freeze	IO Error	Freeze	IO Error
Not available	OK	B	OK	B	OK
Not available	Loop fault	Freeze	IO Error	Freeze	IO Error
Not available	Not available	Freeze	IO Error	Freeze	IO Error

Figure: Input signal selection

The Output Signal Voting combines output values from two Process Stations into one field IO value. The output values are produced at fixed intervals and the RIO unit keeps the last value received from each Process Station. If valid data with an acceptable age is not available or if a Process Station is not online, than the output value from that Process Station is considered invalid and a fault is pending. Faults will be handled by the overall alarm system.

Output from PS A	Output from PS B	Field output
Safety action	Safety action	Safety action
Safety action	Normal	Safety action
Safety action	Fault	Safety action
Normal	Safety action	Safety action
Normal	Normal	Normal
Normal	Fault	Normal
Fault	Safety action	Safety action
Fault	Normal	Normal
Fault	Fault	The defined fault action

Figure: Output signal voting

The concept and the implementation of the RBUS have been inspected based on the documentation provided by the manufacturer, see /D1/. Further the test activities concerning the correct implementation of the RBUS performed by the manufacturer have also been inspected. Finally functional and fault insertion testing for the RBUS implementation has been successfully performed at the manufacturer’s site, see /D4/.

The RIO firmware uses the DSP BIOS provided by the company Texas Instruments as operating system. The DSP BIOS revision 5.20.5 build 34 was also analysed regarding confidence in use.

The inspection showed that the relevant requirements of the above standards are fulfilled.

Further the residual error rate of the communication system was calculated to $\Lambda = 5.76 \times 10^{-17}$ 1/h under the assumption that 10 message with a length of 2048 bit are send in a second and two Process Stations are communicating with a single RIO module. Therefore 1% of the total SIL3 specified rate of failures in continuous mode of transmission system will not be exceeded for up to approximately 10^7 dual master - single RIO relations being part of a safety loop. That is such a huge number that no further investigation is necessary.

It can be concluded that the new RBUS IO System fulfils the requirements for use in safety related applications. A 1oo2 Single RIO module can be used in SIL2 safety applications. A 1oo2 Dual RIO configuration can be used in SIL3 applications.

4.4. Description and evaluation of the changes associated with the implementation of the PROFIsafe protocol

The implementation of the PROFIsafe protocol is an addition to the already existing PROFIBUS implementation. The PROFIsafe protocol is used for exchanging safety data over a PROFIBUS channel. The PROFIsafe implementation is tailored solely to get input information from S-AIMH safety analog input modules of the company STAHL.

The Process Stations (RCUs) are connected via standard PROFIBUS and via CPM-modules (module provided by company STAHL responsible for power and standard PROFIBUS) with the S-AIMH- modules (Safe Analog Input Module provided by company STAHL including PROFIsafe)

The following four module configurations were examined:

- Single RCU – Single CPM with S-AIMH modules
- Redundant RCU – Single CPM with S-AIMH modules
- Single RCU – Redundant CPM with S-AIMH modules
- Redundant RCU – Redundant CPM with S-AIMH modules

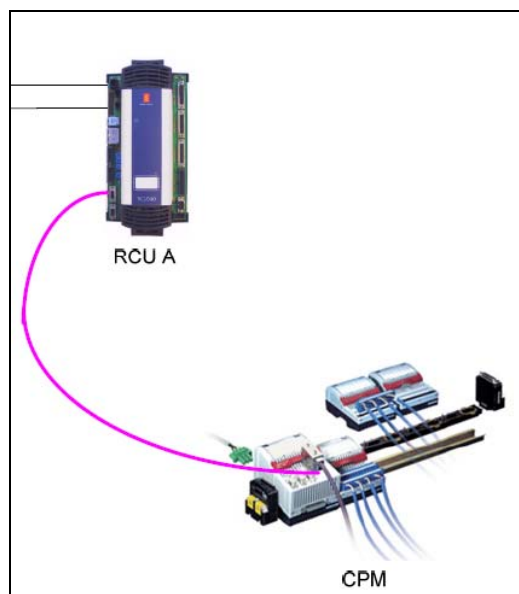


Figure: Single RCU – Single CPM with S-AIMH modules

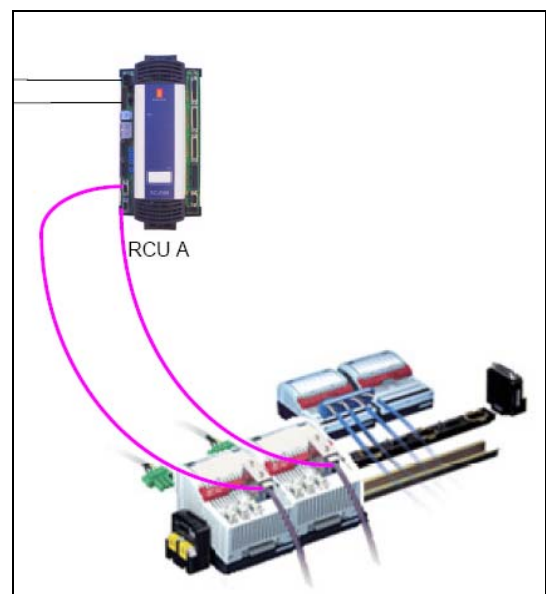


Figure: Single RCU – Redundant CPM with S-AIMH modules

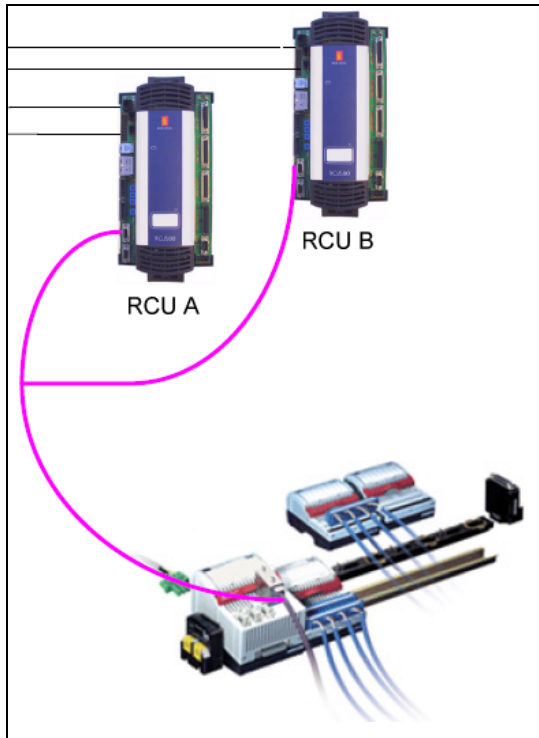


Figure: Redundant RCU – Single CPM with S-AIMH modules

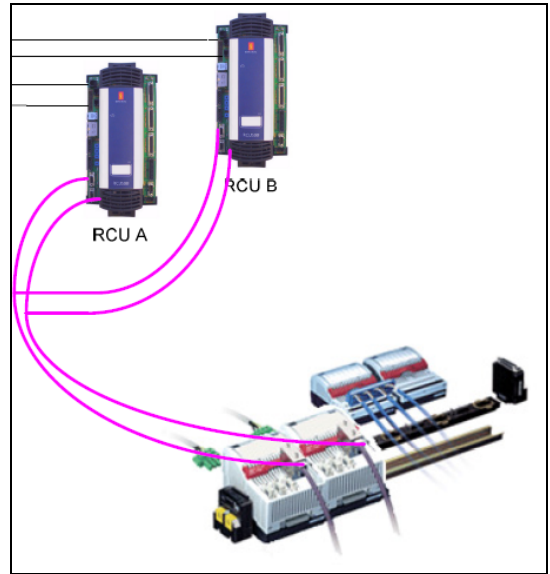


Figure: Redundant RCU – Redundant CPM with S-AIMH modules

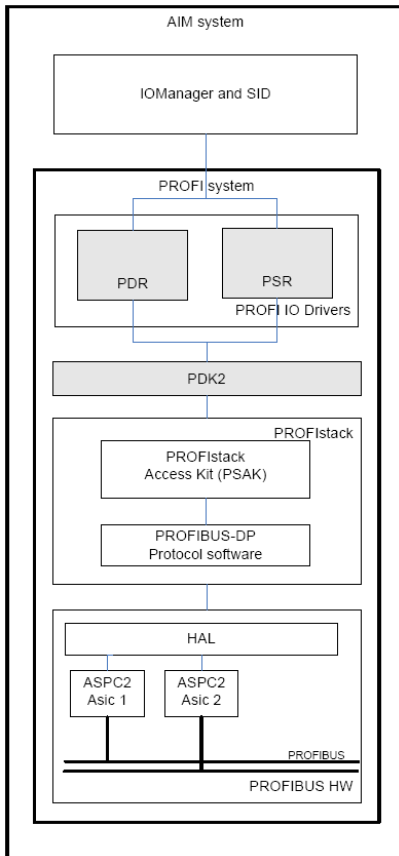


Figure: PROFIBUS subsystem

The concept and the implementation of the PROFIsafe protocol have been inspected based on the documentation provided by the manufacturer, see /D1/. Further the test activities concerning the correct implementation of the PROFIsafe protocol performed by the manufacturer have also been inspected. Finally functional and fault insertion testing for the PROFIsafe protocol implementation has been successfully performed at the manufacturer's site, see /D3/.

The PROFIBUS subsystem was changed to add master redundancy mode and PROFIsafe functionality. The PDK2 layer now includes also the PROFIsafe protocol stack. The standard PROFIBUS protocol stack was bought from the company Softing. The PROFIsafe revision 6.01.0.06 was analysed regarding confidence in use.

The Process Station (RCU) firmware uses VxWorks provided by the company Wind River as an operating system. The VxWork operating system revision 5.4 was analysed regarding confidence in use.

The inspection showed that the relevant requirements of the above standards are fulfilled. It can be concluded that the implemented PROFIBUS subsystem fulfils the requirements for use in safety related applications up to SIL2. But it can only be used together with the dedicated S-AIMH-modules of the company STAHL because no standard PROFIsafe Conformance Tests have been performed.

4.5. Description and evaluation of the updates to the NetIOSafe communication protocol

The release 1.1 of the NetIOSafe driver was already been separately approved, see test report /T5/. The following changes were done for release 1.2 of the NetIOSafe driver.

The new release 1.2 of the NetIOSafe driver now suppresses IO errors on start-up and includes updated verification methods for code testing to reach 90% decision coverage.

The concept and the implementation of the changes to the NetIOSafe driver have been inspected based on the documentation provided by the manufacturer, see /D1/. Further the test activities concerning the correct implementation of the NetIOSafe driver performed by the manufacturer have also been inspected.

The inspection showed that the relevant requirements of the above standards are fulfilled. It can be concluded that the implemented NetIOSafe driver release 1.2 fulfils the requirements for use in safety related applications up to SIL3.

4.6. Description and evaluation of the changes associated with the implementation of the Redundancy Switch and System Surveillance

The 1oo2 redundancy type including System Surveillance was examined. The redundancy switching is needed to determine the active master station if two Process Stations (RCUs) are used as a 1oo2 redundancy group. The redundancy switching procedure will assure that the healthier Process Station takes over this responsibility.

The concept and the implementation of the changes to the Redundancy Switch and System Surveillance have been inspected based on the documentation provided by the manufacturer, see /D1/. Further the test activities concerning the correct implementation of the Redundancy Switch and System Surveillance performed by the manufacturer have also been inspected.

The inspection showed that the relevant requirements of the above standards are fulfilled. It can be concluded that the implementation of the 1oo2 Redundancy Switch including System Surveillance fulfils the requirements for use in safety related applications up to SIL3.

4.7. Description and evaluation of the changes associated with the implementation of the Software Watchdog

The already previously implemented Software Watchdog has been modified in order to provide logical monitoring of the program sequence. Further the temporal monitoring has been improved. The Hardware Watchdog acting as a second shut-down path needs to be re-triggered by the Software-Watchdog on Process Stations (RCUs).

The concept and the implementation of the Software Watchdog have been inspected based on the documentation provided by the manufacturer, see /D1/. Further the test activities concerning the correct implementation of the Software Watchdog performed by the manufacturer have also been inspected. Finally functional and fault insertion testing for the Software Watchdog implementation has been successfully performed at the manufacturer's site, see /D4/.

The inspection showed that the relevant requirements of the above standards are fulfilled. It can be concluded that the implemented Software Watchdog together with the Hardware Watchdog provides a high diagnostic coverage concerning the detection of random hardware failures as required for SIL3 applications. Further this measure is also able to control systematic failures caused by software, hardware or environmental influences up to a high degree.

4.8. Description and evaluation of new hardware

A new remote analog input module called RMP420S has been introduced. The purpose of the new module is to interface to analog input current and/or analog input voltage channels. The RMP420S has the same structure as the previously already approved remote IO modules. The main difference being that the module provides a multi-purpose front-end. During functional and fault insertion testing it has been shown that the new hardware module RMP420S is capable of reading in analog current and analog voltage signals with the required hardware safety integrity. In particular it has been shown through a combination of analysis, see document 339381, and testing see D2, that the required safe failure fraction of 90% will be reached. Further calculations performed by Kongsberg Maritime show that the safety related reliability of the new hardware module is comparable to the previously approved modules, see document 339381. The RMP420S module can be used with defined safety loops as specified in the user manual, see document 323935.

The central processing unit called RCU500 has been upgraded to a new version called RCU501 in order to accommodate the change of the communication bus from PBUS to RBUS. Similarly the previously approved remote digital input module RDIO401S has also been updated in order to implement the new communication bus. These changes have been successfully tested during the functional and fault insertion testing of the RBUS components, see /D4/.

All new hardware components have been tested regarding their environmental and EMC behaviour in an accredited test laboratory. The environmental testing has been conducted using the requirements described in /N4/. For the EMC testing additionally the testing with higher EMC levels according to EN 62061 has been performed. For the test results see documents 198508-1, 198696 and 1910541. The test reports show that the testing has been performed successfully and that the relevant requirements are fulfilled. The test results are accepted by the test institute, see /D5/.

The new hardware components are powered through a 24 V supply. Therefore the electrical safety of the new components is ensured.

It can be concluded that the new hardware modules RCU501, RDIO420S and RMP420S fulfil the requirements for use in safety related applications up to SIL 3 with low demand mode of operation.

4.9. Description and evaluation of changes to the development process

The previous certification found that the development process did not fulfil all the requirements regarding the avoidance of faults during the different relevant life cycle phases of the AIM release, see report /T3/. During the course of the current certification Kongsberg Maritime has introduced a requirement's tracking process using the tool DOORS. The new requirement's tracking is applied to all new documents being generated.

Also Kongsberg Maritime has started to re-write the AIM specification and the AIM architecture specification, see documents 331443 and 331444. The AIM specification has been generally agreed. The AIM architecture specification needs further work which will be performed during the certification of the next AIM release. A V&V plan for the AIM Safe system has also been established, see 338369. Further a test specification for the AIM Safe system has been generated, see 338370.

All these measures have helped to greatly improve the process of establishing proper specifications, doing appropriate designs based on these specifications and defining the required testing for these designs. Although the process of establishing the system level requirements is not yet complete it can nevertheless be said that for all new components and functionality the required measures for the avoidance of faults as detailed in 338369 have been effectively applied during the development, design and testing of the AIM Safe system.

Further the procedure for performing minor changes, bug fixes and updates to the AIM Safe system, the so called Track Procedure, has been substantially revised, see PRO-2099. In particular the procedure now includes detailed provisions in order to identify the safety relevance of changes, the requirement for performing an impact analysis and determining the required change activities depending on the safety relevance of the change. The revised change procedure has already been applied to the latest changes performed on the system.

It can be said that the revised track procedure provides the necessary requisites in order to ensure that upcoming minor changes to the AIM Safe system will be executed in a manner which guarantees the safety integrity of the AIM Safe system under the assumptions that it will be properly applied.

It can be concluded that the implemented changes to the development process have been pivotal in order to fulfil the requirements regarding the avoidance of faults during the different relevant life cycle phases of the AIM Safe system. It has been agreed that further improvements will be implemented during the course of the next certification.

5. Summary

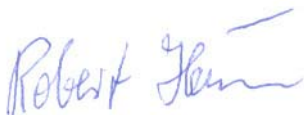
The inspection of the changes between AIM release 7.3.8 and 8.3.3 showed that the changes have been performed in agreement with the requirements of the standard /N1/. It can therefore be concluded that the changes performed have no negative impact on the safety of the system. Further it can be stated that the AIM release 8.3.3 still fulfils the requirements for use in safety related applications up to SIL 3 with low demand mode of operation according to IEC 61508.

The software and hardware versions for the current approval of the AIM Safe system are documented in appendix A1 of this report.

The restrictions and conditions of the previous approvals apply. In particular for all applications a safe state must exist (e.g. de-energized for ESD systems) and the demand to trip must be defined. The frequency of demands must be low (low demand mode of operation according to the IEC 61508). The user has to ensure that the complete safety function for his application conforms to the required Safety Integrity Level.

Cologne, 2010-04-09
TIS/ASI/Kst. 968 dr.ko-hei-nie

The inspectors



Dipl.-Ing. Robert Heinen



Dr. Peter Kocybik

Report released after review:
Date: 2010-04-09



Dipl.-Ing. Heinz Gall