Automation, Software and Information Technology

Test report of the type approval of the Remote Control Unit RCU500 including the upgrade of the AIM Safe System

KONGSBERG MARITIME AS

Report-No.: 968/EL 161.01/04
Date: 2004-12-01

Test report of the type approval of the Remote Control Unit RCU500 including the upgrade of the AIM Safe System

Report-No.:	968/EL 161.01/04
Date:	2004-12-01
Pages:	14
Test object:	Type approval of the RCU500 including the upgrade of the AIM Safety System
Customer/Manufacturer:	KONGSBERG MARITIME AS Kirkegardsveien 45, Carpus N-3601 Kongsberg Norway
Order-No./Date:	JB-80677 and JB-80924 dated 2003-12-05 and 2004-10-22
Test Institute:	TÜV Industrie Service GmbH Am Grauen Stein D-51105 Köln (Poll)
Department	Automation, Software and Information Technology
TÜV-Order-No./Date:	9000109 dated 2003-12-09
Offer-No./Date:	968/50/03 dated 2004-03-12
Inspector(s):	Dipl.-Ing. Jürgen Schön Dipl.-Ing. Matthias Haynl
Test Location:	see Test Institute
Test Duration:	January 2004 until November 2004
Distributor	2 x customer

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 and regulations for the type approval	4
3.	Object of inspection	5
3.1.	Test object	5
3.2.	General safety requirements	5
3.3.	Documentation	6
3.4.	Available test reports	7
4.	Review and results of the approval	7
4.1.	Inspection of basic requirements	7
4.1.1.	Inspection of the measures to avoid systematic failures	7
4.1.2.	Inspection of the measures for the control of systematic failures	8
4.1.3.	Inspection of the system behaviour on fault detection	8
4.1.4.	Review of the documentation	9
4.2.	Inspections and tests of the safety relevant software changes	9
4.2.1.	Static analysis	9
4.2.2.	Dynamic analysis	9
4.2.3.	Influences of the AIM changes to other Units	9
4.2.4.	Inspection of the track management system	10
4.3.	Description of the RCU500 in different architectures of the AIM Safe System	10
4.4.	Hardware inspection of the new RCU-Module	11
4.4.1.	Inspection of the Safety Requirement Specification, Doc. No.: 163927, Issue D	11
4.4.2.	Inspection of the design, FMEA	12
4.4.3.	Inspection of the measures for the control of random hardware faults	12
4.4.4.	Inspection of the reliability data and PFD calculations	12
4.4.5.	Inspection of the electrical safety	13
4.4.6.	Inspection of the environmental and EMC tests	13
5.	Summary of the results	13

Appendix A1: Reviewed AIM Safe System Versions; Rev. 1.0; 2 pages

Appendix B1: Technical Note; Default set-up of AIM Safe systems forming part
of an IEC 61508 function; 3 pages

1. Scope

Object of the inspection is the Albatross Integrated Multifunction System (AIM Safe) from Kongsberg Maritime, N-3601-Kongsberg, Norway, which has been type approved for release 6.9 (see /U 17/).

This report is the summary of the results of the type approval with regard to the safety relevant applications for the new AIM release 7.2. The release AIM 7.2 consists of a new Remote Controller Unit (RCU500), which combines the functionality of the approved units SBC400 and SPBUS400 together in one unit.
This report must also be considered for design, installation and setting into operation of all safety related applications.

Purpose of this type approval is to clarify, that the AIM Safe-System for release 7.2 including the new RCU500 still fulfils the requirements up to SIL 3 in accordance with the standard /N 1/ for the use in safety relevant applications with low demand mode of operation and safe states.

The process, plant or other safety relevant applications under the control of the AIM Safe system must have a defined safe state (de-energized or energized). For normally energized applications (NE), e.g. ESD systems, the safe state is the de-energized state, for normally de-energized applications (NDE), e.g. F&G-systems, the demand to trip must be defined.

The type approval should also clarify, that the requirements of the standard /N 2/, which is a typical application standard for safety integrity level 3 according to the standard /N 1/, are fulfilled.

2. Standards and regulations for the type approval

/N 1/ **IEC 61508 Part 1 - 7, 1998 and 2000**
Functional safety of electrical/electronic/programmable electronic safety-related systems

/N 2/ **DIN EN 50156/2004-11-22**
Electrical Equipment of Furnaces

/N 3/ **EN 50178/04.98**
Electronic equipment to be used in electrical power installations and their assembly into electrical power installations

/N 4/ **DIN IEC 60068**
Basic environmental testing procedures

part 2:	Tests
part 2-1/03.80:	Cold
part 2-2/03.80:	Dry heat
part 2-6/06.90:	Vibration (sinusoidal)
part 2-30/09.81:	Damp heat, cyclic

/N 5/ **IEC 61000**
part 4-3
Radiated radio-frequency electromagnetic fields
part 4-2
Electrostatic discharge requirements
part 4-4
Electrical fast transient/burst requirements
part 4-5
Surge
Part 6-2
Immunity for industrial environments
Part 6-3
Emission standard for residential, commercial and light-industrial environments

/N 6/ **EN 61131-2/2003**
Programmable Controllers
part 2/4.00
Equipment requirements and tests

/N 7/ **NFPA 72/2002**
National Fire Protection Association, part 72
Fire Suppression System

/N 8/ **NFPA 8501/1997**
National Fire Protection Association, part 8501
Standard for single burner operation

/N 9/ **NFPA 8502/1999**
National Fire Protection Association, part 8502
Standard for the prevention of furnace explosions/implosions in multiple burner boilers

/N 10/ **DIN EN 54-2/December 1997**
Fire detection and alarm systems
part 2: Control and indicating equipment

/N 11/ **IEC 945/96 (EN 60945/97)**
Maritime navigation and radio communication equipment and system
General Requirements-Methods of testing

/N 12/ **IEC 61511/12.2003**
Functional safety - Safety instrumented systems for the process industry sector -
Part 1: Framework, definitions, system, hardware and software requirements
Part 2: Guidelines for the application of IEC 61511-1

3. Object of inspection

3.1. Test object

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

Object of the software inspection are the changes from AIM 6.9 to AIM 7.2, which are described in /U 1/. The AIM 6.9 has been already approved, see /U 17/.

Object of the hardware inspection is the new RCU500 Module, which is described in /U 7/. The RCU500 contains in principle the combined functionality of the SBC400 and the SPBUS400 in a single box for DIN rail mounting. The RCU500 communicates via the SPBUS with all kind of RIO-Units.

3.2. General safety requirements

The AIM Safe System with the new RCU500 Module must cover SIL classes up and to 3 under the aspect of low demand mode of operation and safe states.

The RCU500-Module is classified as “type B” according to /N 1/, due to the lack of information of the failure mode of all electronic components.

By using two RCU500-Modules with diagnostic functions the hardware failure tolerance (HFT) amounts to 1. To achieve the necessary safety-integrity the safe failure fraction (SFF), according to /N 1/, (part 2, table 3), must be ≥ 90 %.

The process, plant or other safety relevant applications under the control of the AIM Safe System must have a defined safe state (de-energized or energized) according to the table 1.

	Normally energized	**Normally de-energized**
Safety Function	De-energize to trip	Energize to trip
Safe State	De-energized outputs	De-energize the output or hold last state and perform alarm

Table 1: Definition of Safe State

The proof test interval for ESD (Emergency Shut Down) and F&G (Fire & Gas) Systems must be minimum every 12 month.

3.3. Documentation

The following documents were used inter alia for the type approval:

/U 1/ **Change and impact analysis AIM 6.9 to 7.1 revision pA of 2004-06-02**
Kongsberg Maritime AS

/U 2/ **AIM Release 7.2 and updates of 2004-07-07**
Kongsberg Maritime AS

/U 3/ **Safety Requirement Specification AIM Safe revision D of 2004-10-11**
Kongsberg Maritime AS

/U 4/ **System Requirement Specification revision A of 2003-12-17**
Kongsberg Maritime AS

/U 5/ **Coding standard of 2003-06-26**
Kongsberg Maritime AS

/U 6/ **Track procedure of 2003-26-06**
Kongsberg Maritime AS

/U 7/ **Hardware Module Specification revision A, doc. No.; 176827**
Kongsberg Maritime AS

/U 8/ **Environmental Specification revision 2 of 2003-06-03**
Kongsberg Maritime AS

/U 9/ **Environmental test report, doc. No.: 310-03-319**

/U 10/ **Failure Mode and Effect Analysis of RCU500 revision A of 2004-03-22**
Kongsberg Maritime AS

/U 11/ **Description of built in testing and monitoring in the AIM Safe system 7.1 revision B of 2004-03-08**
Kongsberg Maritime AS

/U 12/ **Tool for developing the RCU, dated 2004-03-22**
Kongsberg Maritime AS

/U 13/ **RCU500 schematics, dated 2003-12-19**
Kongsberg Maritime AS

/U 14/ **RCU System Requirements Specification, revision A of 2003-05-27**
Kongsberg Maritime AS

/U 15/ **Aim Topology Requirements - System Requirements Specification, revision A of 2003-12-17**
Kongsberg Maritime AS

/U 16/ **Hardware changes of the RIO Modules**

- HW Change RAIV400
- HW Change RDIO400
- HW Change RDIO400S
- HW Changes RDIO400S

3.4. Available test reports

The following documents were prepared during previous approval testing.

/U 17/ **Type approval of Albatross Integrated Multifunction System (AIM Safe) Fault Tolerant and Fail Safe Controller System of Kongsberg Simrad**
Report-No.: 968/EL 161.00/02 Date: 2002-01-31
TÜV Anlagentechnik GmbH

4. Review and results of the approval

The inspections and tests contained the following main tasks:

- Type approval of the new RCU500
- Inspection of the software upgrade of the AIM Safe System from release 6.9 to 7.2
- Hardware changes of the approved RIO modules
- Inspection of the AIM Safe System in different configurations

During the type approval the following documents were generated, in which the details of the tests have been recorded. These documents are deposited in the Test Institute.

/D 1/ **Integration Test Description, SBC/RCU built in self test of 2004-10-27**
Kongsberg Maritime AS

/D 2/ **Integration Test Description, SW Watchdog of 2004-10-26**
Kongsberg Maritime AS

/D 3/ **Integration Test Description, Redundancy switch of 2004-10-27**
Kongsberg Maritime AS

/D 4/ **Software FMEA and failure protocol AIM 7.2, version 1.0 of 2004-10-28**
TÜV Industrie Service GmbH

4.1. Inspection of basic requirements

4.1.1. Inspection of the measures to avoid systematic failures

To avoid systematic failures in the specification, in the design of the architecture as well as in the test and integration phase, techniques and measures according to Annex B of IEC 61508-2 must be performed with reference to the required SIL.

A software safety validation plan for the RCU500 according to IEC 61508-3, chapter 7.3 must be implemented to demonstrate that the software satisfies the safety requirements. If non safety functions are implemented to the software of a safety system all software must be treated as safety-related, unless adequate independence between the functions can be demonstrated (IEC 61508-3, 7.4.2.7).

Results:

Kongsberg Maritime maintains a quality management system according to the standard ISO 9001 (KONGSBERG SIMRAD, Company Handbook, Doc.-No.: CH-001, 2000-01-10).

The overall lifecycle activities, which are necessary to achieve the required safety integrity level (SIL) regarding to IEC 61508 part 1, are documented in the Safety Requirements Specification (SRS) /U 3/. The manufacturer used a special tool for the development of the RCU500 /U 11/.

The measures to avoid systematic failures have been verified in accordance with /N 1/, and are sufficient.

4.1.2. Inspection of the measures for the control of systematic failures

The measures to control systematic failures caused by environmental stress or influence are listed in the Safety Requirement Specification AIM Safe /U 3/.

Results:

The measures to control systematic failures caused by hardware and software design were verified and are sufficient.

4.1.3. Inspection of the system behaviour on fault detection

The behaviour of a safety related system after the detection of a dangerous fault depends on the fault tolerance of the system (grade of redundancy), the facility of the system to localize the faulty component and to isolate this component from operating and the degradation designation.

In NE applications for higher SIL levels (> 2) a Shut-down (SD) must be initiated if a fault tolerance of zero is achieved by a degradation of the system due to fault detection and localization if the system is not restored to normal operation before the shutdown timer expires.

In NDE, e.g. F&G applications a SD is normally not acceptable for those cases. Therefore, necessary actions must be specified for each safety function in cases of the detection of dangerous faults.

For safety related systems with an inherent fault tolerance of 0 the system must be repaired within the mean time to restoration (MTTR, 8 hours for AIM Safe). During the repair time the continuing safety of the application shall be ensured by additional measures. (e.g. manual observations, trips and overrides, applicable for applications with a high processing time). The necessary action shall consider this requirement.

Results:

The inspection of the system behaviour on fault detection have been verified and are sufficient.

All necessary actions required to achieve and/or to maintain a safe state in cases of dangerous faults must be specified in the Operation and Maintenance procedure.

4.1.4. Review of the documentation

The documentation has been presented by the client with the documents in chapter 3.3. The documents have been assessed concerning the completeness, consistency and conformity in accordance with /N 1/.

Results:

The documentation is complete, consistent and comprehensible.

4.2. Inspections and tests of the safety relevant software changes

The design review has been divided into the static and dynamic analysis as well as the inspection of the track management system /U 6/.

The results of the analysis are contained in /D 1/ to /D 3/.

4.2.1. Static analysis

Content of the static analysis was the assessment of the changes from AIM 6.9 to AIM 7.2 in accordance with the coding standard /U 5/.

Results:

The coding standard /U 5/ is generally in accordance with the „guidelines for safety C“ of the Test Institute. In addition the sources have been complied to different targets and it was shown, that the warning levels of the compilers exceed sometimes the requirements to the „guidelines for safety C”. For example the GNU compiler gcc is used with -*Wall* option and this provides an additional argument checking. For safety-related development the static fault checking provided only by compiler is usually not sufficient because compilers are traditionally designed around the notions of performance (speed of the compiler itself and efficiency of the generated code).

By static analysis of the design no generally deviations from the relevant standard have been shown.

4.2.2. Dynamic analysis

The failure detection and failure control measures have been assessed by this analysis and inspection of the code description. The implementation of the failure detection and failure control measures have been inspected according to the standard /N 1/.

During the inspection measures such as stack,- task and zero-pointer monitoring as well as code checksum have been tested. The results of the analysis are contained in /D 1/ to /D 3/.

Results:

The inspection of the failure detection and failure control measures has not shown evidence of deviations according to /N 1/.

4.2.3. Influences of the AIM changes to other Units

As a result of the new RCU500 the certified RIO units have been slightly changed in the firmware and hardware. The versions of the firmware are summarised in appendix A1. The hardware changes are described in the specific documentations, which are listed under /U 16/.

The software of the SPBUS400 has also been changed. The changes are described in the document "SPBUS400 Firmware release, revision A of 2003-10-31. Extensive tests have been performed by the manufacturer. The results of these tests are documented in /D 1/ until /D 3/.

Results:

Inspection of the tests and fault simulations has not shown any dangerous failure.

4.2.4. Inspection of the track management system

The track management system is the major source of information for the change and impact analysis /U 1/ as well as the verification and validation procedure. The track management system /U 6/ has been analysed for the ability to cover the requirements for modifications and validation/verification parts of the software live cycle.

Results:

It was shown that the track management system, which is linked to the code vision system, is able to cover the requirements for modification and validation/verification according to the standard /N 1/.

4.3. Description of the RCU500 in different architectures of the AIM Safe System

The Remote Control Unit RCU500 is a computer dedicated for the AIM Safe System. The RCU500 interfaces the field equipment on one side, and to the operator Station on the other side. An overview of the system architectures of the RCU500 is shown in the Hardware Module Specification /U 7/. The RCU500 can replace the certified SBC400 and SPBUS400 units. The RCU500 houses in a single box for DIN rail mounting and combines in principle the functionality of the SBC400 and the SPBUS400. All kind of RIO-Units can be accessed via the SPBUS.

The AIM Safe System consists of different topologies (architectures), which have been qualified for AIM Safe Release 6.9. All different topologies based on the previous SBC400H module with IO400 and RIO400 series input/output modules. Detailed descriptions can be found in the TUV report /U 17/.

The following topologies (architectures) which utilizes the new RCU500 computer, were object of the type approval as well the new software for Release 7.2. Detailed descriptions of the RCU500 and RIO architectures can be found in the System Requirement Specification /U 15/. A detailed description can also found in the SRS /U 3/ (Safety Requirements Specification doc. No.: 163927, dated 2004-02-13).

Topologies	**Line monitoring**	**FOST/ ..otest**	**SIL class**
AIM Safe3, 1002 dual IO, SBC or RCU with IO, RIO and/or redundant fire central, NE or NDE outputs.	Active	Active	3
AIM Safe2, 1002 shared IO, SBC or RCU with RIO & fire central. NE or NDE outputs.	Active	Active	2
AIM Safe2, 1002 shared IO, SBC with monitored input signals and NE non-monitored output relays. Single fire central allowed.	Active	No	2

Topologies	**Line monitoring**	**FOST/ ..otest**	**SIL class**
AIM Safe2, 1002 shared IO, SBC redundancy with monitored input signals and NDE output relays. Single fire central allowed.	Active	Active	2
AIM Safe1, Single RCU&RIO, RIO Ex or fire central. Redundant power. NE or NDE outputs.	Active	Optional	1
AIM Safe1, Single SBC and IO or RCU and RIO. Redundant power. NE or NDE outputs	Active	Optional	1

Table 2: Hardware configuration

4.4. Hardware inspection of the new RCU-Module

Inspections and tests of the Remote Control Unit (RCU500) were carried out with the view to

- General requirements for NDE and NE systems
- Requirements of application standards, e.g. requirements for Fire and Gas systems in accordance with EN 54 /N 10/

The general requirements of the standards IEC 61508, parts 2 and 3 and application standards are listed under clauses 2. A detailed description of the RCU500 requirements can be found in the “System Requirement Specification of the RCU500”, Rev. A. /U 14/. The basic design techniques of the RCU500 have been analysed by the manufacturer according to table 17 of the IEC 61508-2.

Results:

The hardware of the new RCU500 module has been verified by TÜV together with the manufacturer. The results are documented in the “Integration Test Description (SW Test Report)” /D 1/. The RCU500 can be used alternative to the approved SBC400 in the different application.

4.4.1. Inspection of the Safety Requirement Specification, Doc. No.: 163927, Issue D

The above mentioned document no.: 163927 is the product Safety Requirement Specification (SRS) for Kongsberg Maritime’s NE and NDE systems, called AIM Safe. The SRS describes the required behaviour of the AIM Safe system in terms of input data, required processing, output data, operational scenarios, interfaces and the attributes of a system including performance, security, maintainability, reliability, audibility, availability, diagnostic and design constraints.

Results:

The SRS provides all information needed for the assessment of the AIM Safe system in accordance with IEC 61508 and must be adhered to during upgrades and modifications to any parts of the AIM Safe.

Due to the fact that the responsibility of safety for every realized AIM Safe System will completely remains by the manufacturer, KS must prepare an SRS for every application and a VVPLAN for validation and verification of the SRS.

4.4.2. Inspection of the design, FMEA

A failure mode and effect analysis on component level has been performed by the manufacturer. The results of the FMEA are reported in /U 10/. The schematics /U 13/ of the RCU500 have been verified by the Test Institute.

Within the framework of the hardware inspection, an FMEA on component level, was carried out by the manufacturer to check the failure control mechanism on the RCU500. This was done by assuming representative failures and analysing the effect of these failures. If necessary the analysis was extended to the system level if the fault detection was assured by the structure of the system or by the operating software. The FMEA was completed by fault insertion for those cases where an analysis could not lead to definite results.

Results:

All assumed or inserted failures resulted in fault detection or the system reacted to the safe state (break down). Therefore the RCU500 fulfils the requirements up to SIL 3 according to the IEC 61508.

4.4.3. Inspection of the measures for the control of random hardware faults

All measures to control latent hardware faults implemented in the AIM Safe system are described in /U 11/. The measures were inspected and partly tested within a test system installed by the manufacturer.

Results:

With the inspections and tests it was demonstrated that the levels of safe failure fractions as required for the targeted SIL levels according to IEC 61508 and listed in the Safety Requirement Specification /U 3/ are reached.

4.4.4. Inspection of the reliability data and PFD calculations

The basic failure rates of the single parts on the units are calculated according to the methods of the MIL-HDBK-217E in a Navy Sheltered (NS) environment at +35°C or from reliability sources available from the manufacturer of the components, and was demonstrated by the manufacturer. Only 15 % of the allowed Critical Safety Unavailability (CSU) have been available for the AIM Safety System and the remaining 85 % consists for the field devices. The architectures, which includes the fire central includes 20 % of the allowed Critical Safety Unavailability (CSU).

The PFD figures for the additional system types (architectural constraints) are calculated according to the PDS-method which is developed by SINTEF. Representative samples for the PFD calculations are shown in the Safety Requirement Specification.

Results:

It could be demonstrated that this method is quite similar to the requirements of the IEC 61508.

The responsibility of safety for every realized AIM Safe System will completely remains by the manufacturer, KM must prepare PFD calculations for every application to demonstrate that the required PFD values for the targeted SIL levels will be met.

4.4.5. Inspection of the electrical safety

The inspection of the electrical safety (clearance and creepage) was observed under the requirements of EN 61131-2 /N 6/ and DIN EN 50178 /N 3/ (Replacement for DIN VDE 0160, Electronic Equipment for use in power installations). The RCU500 must fulfil the following requirements:

Pollution degree	2
Overvoltages category	II
Working voltage	0 V < U ≤ 50 V
Clearances	0.2 mm
Creepages	0.04 on printed boards

Results:

The results of the manufacturer have been verified by the Test Institute. The theoretical inspection came to the result, that the requirements are fulfilled.

4.4.6. Inspection of the environmental and EMC tests

The environmental and EMC tests for the RCU510 were carried out according to the requirements of the EN 61131-2, Programmable Controllers, Equipment requirements and tests /N 6/. Due to the fact, that the RCU510 is slightly different to the RCU500 (RCU500 contains redundant serial line, redundant Ethernet), the results of the tests were recognized for the RCU500.

The tests were carried out by the accredited test laboratory at

The National Institute of Technology,
Laboratory Services
Material Technolgy, Environmental Test
Laboratory
Postboks 1019
N-3601 Kongsberg

The test procedure is documented in document No.: SPEC-001_v2, dated 2003-06-03 /U 8/.

The test results are documented in the following test report: Environmental Test Report Verification Test of the FS120, NDU and NDU MINI, doc. No.: 310-03-0319, dated 2004-04-29 /U 9/.

Results:

The results of the tests are in accordance to the IEC 61131 /N 6/. The results have been verified by the Test Institute and will be recognized.

5. Summary of the results

The type approval of the system architectures, which uses the new RCU500 Unit was performed according to the requirements of the relevant parts of the standard /N 1/. During the proper course of the type approval no faults or deficiencies were observed which are in conflict with the requirements of the Safety Integrity Levels (SIL) up to and include 3 according to the standard /N 1/.

The system architectures of the AIM Safe system with the hardware and software configurations as listed in appendix B1 are appropriate for the use in safety relevant NDE (Normaly De-energized) and NE (Normaly energized) applications for Safety Integrity Levels (SIL) up to and include 3 according to the IEC 61508. They extent the system architectures, which have been already approved (see /U 17/). For all application either a safe state must exist (e.g. de-energized for ESD systems) or the demand to trip must be defined. The frequency of demands must be low (low demand mode of operation according to the IEC 61508) and the average probability of failure to perform the safety function on demand (PFD) must be within the limits of the intended Safety Integrity Level (SIL).

The inspection of the software upgrade form AIM 6.9 to AIM 7.2 has not shown any defects or failures, which are in conflict with the requirements of IEC 61508 for SIL 3.

The reviewed versions of the AIM 7.2, the results of the MD5 hash function of the binary file and the used tools are listed in appendix A1.

Berlin/Cologne, 2004-12-01
TIS/ASI/Kst. 968 hy-sn

The inspectors

Matthias Haynl

J. Schön

Dipl.-Ing. Matthias Haynl

Dipl.-Ing. Jürgen Schön