TÜVRheinland®
Precisely Right.

Automation, Functional Safety

Test report about the type approval of changes to the AIM Safe System for AIM releases 8.3.4 to 8.6.0

Report-No.: 968/EL 161.05/14
Date: 2014-01-27

Test report about the type approval of changes to the AIM Safe System for AIM releases 8.3.4 to 8.6.0

Report-No.:	968/EL 161.05/14
Date:	2014-01-27
Pages:	12
Test object:	AIM Safe System
Customer /Manufacturer:	Kongsberg Maritime AS Kirkegardveien 45 3616 Kongsberg Norway
Order-No./Date:	BR-218264 dated 2010-09-01
Test Institute:	TÜV Rheinland Industrie Service GmbH Automation, Functional Safety Am Grauen Stein 51105 Köln Germany
TÜV-Offer-No./Date:	968/260/10 dated 2010-06-14
TÜV-Order-No./Date:	10482816 dated 2010-09-02
Inspector:	Dr. Peter Robben (responsible for project) Dipl.-Ing. Robert Heinen
Test location:	see Test Institute
Test duration:	September 2010 - January 2014

The test results are exclusively related to the test samples.

Contents **Page**

1. Scope

Object of this type approval are the changes performed on the AIM Safe System from company Kongsberg Maritime. The AIM Safe System has previously been type approved by the Test Institute. The last approved version is AIM release 8.3.3, see /T5/.

The main change is the introduction of a new controller module called RCU502 intended to replace the current controller module RCU501. The different software components of the AIM Safe System have been modified for the introduction of the new controller. Further bug fixes and minor upgrades of the software functionality have been performed.

It shall be inspected whether the modified AIM Safe System still fulfils the requirements up to SIL 3 according to IEC 61508 for the use in safety related applications with a low demand mode of operation.

2. Standards forming the basis for the requirements

/N1/ IEC 61508 Part 1 to 7:2010
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 60945:2002+Cor.1:2008 (for environmental testing)
Maritime navigation and radio communication equipment and systems - General Requirements - Methods of testing and required test results

/N4/ EN 50156-1:2004 (as far as applicable)
Electrical equipment for furnaces and ancillary equipment - Part 1: Requirements for application design and installation

/N5/ EN 54-2:1997+AC:1999+A1:2006 (as far as applicable)
Fire detection and fire alarm systems - Part 2: Control and indicating equipment

/N6/ NFPA 72:2013 (as far as applicable)
National Fire Alarm and Signalling Code Handbook

3. Identification of the test object

3.1. Description of the device under test

The AIM Safe System from company Kongsberg Maritime is a safety related controller system consisting of several hardware and software components. The currently approved hardware and software components with their current versions are listed in the annex to the certificate No.: 968/EL 161.05/14.

Object of the inspection are the modifications to the AIM Safe System since the last approved AIM release 8.3.3. The modifications are described in detail in the AIM release documents:

/D1/ AIM 8.3.3 – 8.3.12, document 367451, revision A, dated 2012-04-04

/D2/ AIM 8.4.0 – 8.4.3, document 367469, revision A, dated 2012-06-05

/D3/ AIM 8.5.0 – 8.5.1, document 370460, revision A, dated 2012-05-04

/D4/ AIM 8.6.0, document 378306, revision A, dated 2013-12-11

3.2. Documents

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

/D5/ Document plan RCU502, revision B, dated 2013-12-16

The following document has been prepared by the Test Institute detailing the results of the functional and fault insertion tests performed together with the manufacturer:

/D6/ Test report Functional and Fault Insertion Testing for RCU502, version 5.0, dated 2012-10-26

The following document has been prepared by the manufacturer documenting the results of the remaining fault insertion tests performed by the manufacturer:

/D7/ Test record TUV Fault-Insertion Tests RCU502, version 3.1, dated 2012-10-15

3.3. Test samples

During the functional and fault insertion testing of the RCU502 module at the manufacturer's site the test sample with serial number 4075 has been used, see /D6/. The test sample will be archived by the manufacturer.

3.4. Previous test reports

The following reports document the results of the previous type approvals for the AIM Safe System:

/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 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

/T6/ 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 included in AIM releases 8.3.4 to 8.6.0

The changes included in AIM releases 8.3.4 to 8.3.12 are described in document /D1/. The only change with a potential impact on the safety of the system is the modification of the RBUS driver in order to allow the use of the RTB420 module in 1oo2 applications. As the RTB420 module is not being used for IEC 61508 related applications it must be shown that this modification has been performed in a way which did not change the existing safety functionality of the RBUS driver. Further bug fixes and minor upgrades of the software functionality have been performed.

The changes included in AIM releases 8.4.0 to 8.4.3 are described in document /D2/. No safety related change of the system functionality has been introduced. Only bug fixes and minor upgrades of the software functionality have been performed.

The changes included in AIM releases 8.5.0 to 8.5.2 are described in document /D3/. A new controller module called RCU502 including hardware and firmware has been developed. Several software components have been modified in relation to the introduction of the new controller module RCU502. Further bug fixes and minor upgrades of the software functionality have been performed.

The changes included in AIM release 8.6.0 are described in document /D4/. Mainly further verification activities have been performed for the new controller module RCU502. Further the system has been modified for future use of the new RMP422S I/O module. Additionally availability problems have been solved and bug fixes and minor software upgrades have been implemented.

4.3. Description and evaluation of the changes associated with the introduction of the new controller module RCU502

4.3.1. Description of the new controller module RCU502 and the use of the module in the AIM Safe System

The new controller module RCU502 serves as a replacement of the current controller module RCU501. The new controller module is described in the System Requirements Specification RCU502 and in the System Architecture Specification RCU502, see /D5/ documents: 351158 and 351812.

The RCU502 module receives safety related input information from external devices like remote I/O modules and/or other controller modules via safety related interfaces. The RCU502 will process this information using the specified application program and will generate safety related output information which will be transmitted to external devices like I/O modules and/or controller modules again via safety related interfaces. The basic structure for the use of the RCU502 module in the AIM Safe System is shown in figure 1.

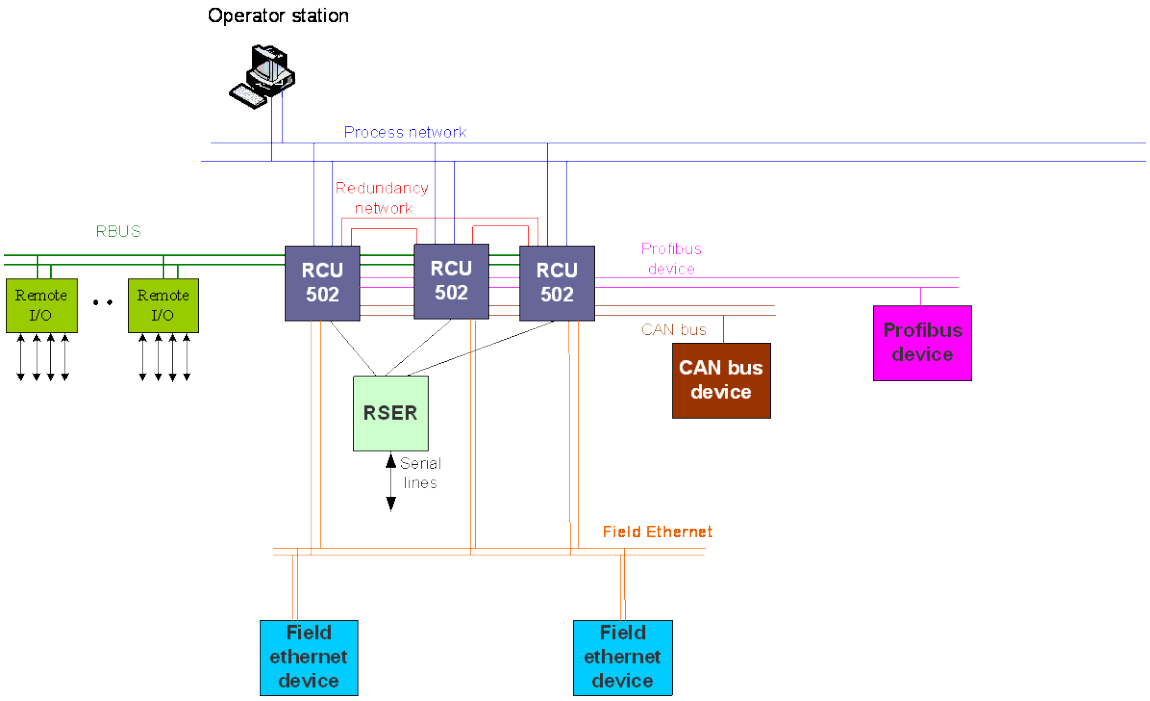

Figure 1: Basic structure for the use of the RCU502 module in the AIM Safe System

The internal structure of the RCU502 module is shown in figure 2.

RCU502

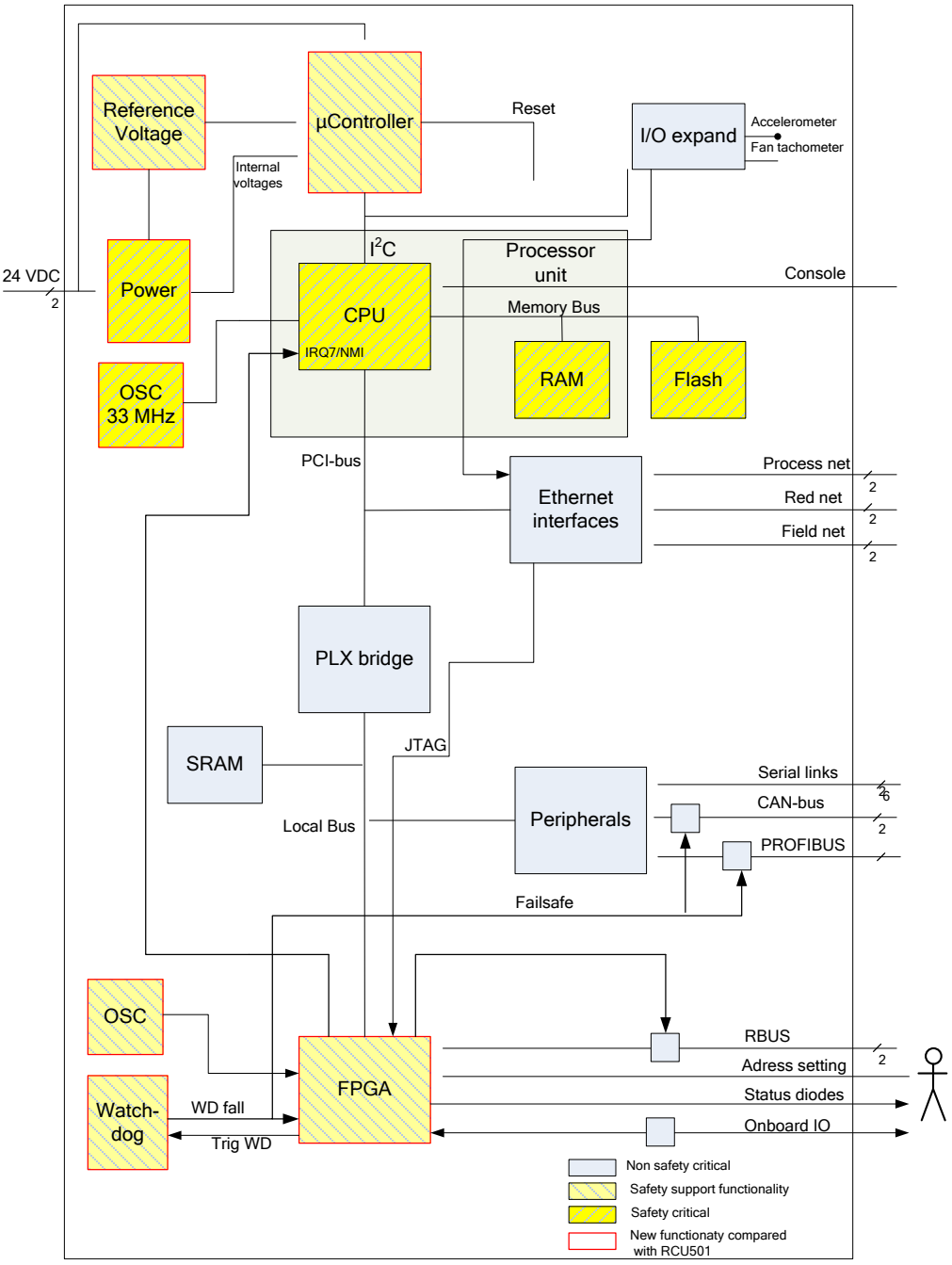

Figure 2: RCU502 hardware architecture

The safety related information received via the different interfaces will be processed by the CPU. The CPU will generate the new safety related information to be transmitted via the different interfaces. The microcontroller serves in order to monitor the different internal voltages and to control the module reset. The FPGA and the watchdog component implement a monitoring of the CPU functionality and initiate a module shut-down in case of detected safety problems.

The module contains a single channel structure for the processing of safety related information. A hardware fault tolerance (HFT) of 0 is realised.

The module will be used in a 1oo2 topology for SIL 2 and SIL 3 applications and in 1oo1 topology for SIL 1 applications.

The software structure for the AIM Safe System is shown in figure 3.

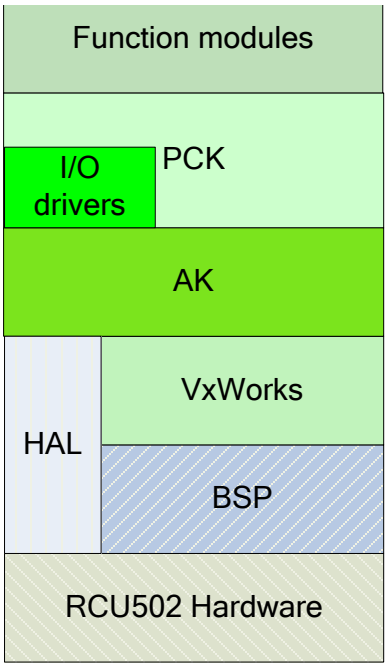

Figure 3: RCU502 and AIM software architecture

The lowest software layers BSP, HAL and VxWorks form part of the firmware for the module RCU502. The module will be loaded with the common higher software layers AK, PCK, I/O drivers and the application software.

Additionally the software for the diagnostic microcontroller and the diagnostic FPGA are also part of the firmware.

The architecture of the AIM Safe System complies with the requirements of IEC 61508.

4.3.2. Evaluation of the Systematic Safety Integrity for the module RCU502

The manufacturer has defined a Safety Plan and a Verification and Validation Plan (V&V Plan) for the development of the module RCU502, see /D5/ document: 363044. This document defines the required development activities for the safety related development of the RCU502 module including the required measures for fault avoidance during the different development steps and the required test activities for both the module hardware and module firmware.

The defined development activities have been judged to be sufficient by the Test Institute for the development of a module for use in safety applications up to SIL 3.

Further the review of the design and test documents generated during the course of the development of the RCU502, see /D5/ various documents, have shown that the requirements for the avoidance of faults during the different development steps have been successfully implemented. It can therefore be concluded that the module reaches the required Systematic Safety Integrity for the use in applications up to SIL 3.

4.3.3. Evaluation of the Hardware Safety Integrity for the module RCU502

The manufacturer has defined measures for the detection and avoidance of random hardware faults for the different components of the module, see System Architecture Specification RCU502 and Safety Plan RCU502 (/D5/ documents: 351812 and 363044). These measures have been judged to be sufficient by the Test Institute in order to achieve the required diagnostic coverage (DC) of minimum 90% for the module.

The implemented measures for fault detection and avoidance have been successfully tested by the manufacturer, see /D5/ various documents. Further the Test Institute has performed functional and fault insertion tests in cooperation with the manufacturer, see /D6/ and /D7/. The tests have shown that the intended safety functionality has been correctly implemented and that the relevant random hardware faults will be successfully detected.

The new module has been tested regarding the environmental and EMC behaviour according to the requirements of /N3/ and using the increased EMC test levels as defined in IEC 62061, annex E, see /D5/ document: DANAK-1911523. The testing has been performed by the accredited test laboratory Delta and the test results show that the module successfully meets the relevant requirements described in the standards. The test results are accepted by the Test Institute.

The new controller module will be powered by a 24 V SELV power supply. The electrical safety of the module is therefore ensured.

The manufacturer has performed calculations of the safety related reliability of the module with the support of an external organisation. The calculations show that the required safe failure fraction (SFF) of minimum 90% will be achieved.

Further using the recommended proof test interval of 1 year a value of:

PFD_{avg} = 2.6 E-04

will result for the module when used in a 1oo1 topology. The details of the reliability calculations can be found in the FMEDA, see /D5/ document: 335925.

The module therefore fulfils the requirements for the safety related reliability for applications up to SIL 3.

For applications according to SIL 2 or SIL 3 the module RCU502 needs to be used in a redundant 1oo2 topology. For SIL 1 applications the module RCU502 can be used in a single channel topology, see /D5/ document: 351158. The user needs to determine the resulting safety related reliability for his application based on the information provided by the manufacturer.

In summary it can be stated that the new controller module RCU502 fulfils the Hardware Safety Integrity requirements for applications up to SIL 3 when operated in a low demand mode and if utilized as described above.

4.3.4. Evaluation of the changes to other AIM components associated with the introduction of the new controller module RCU502

Due to the introduction of the new controller module RCU502 some of the software components in the AIM Safe System needed to be modified. In particular the software components AK, PCK and RBUS required changes. The changes are in detail described in /D3/.

In particular changes have been implemented to the internal self-test of the modules (BITE) due to the new architecture of the RCU502 module, see /D5/ documents: 369607 and 369606.

The changes have been performed following the agreed procedure for software modifications, the so-called track procedure, see /D5/ document: PRO-2099, Version 3.0.0.

Based on a review of the updated documentation for the different components, see /D5/ various documents, and spot checks of the execution of the modification procedure, see /D6/, it can be confirmed that the implemented changes have no negative influence on the safety of the AIM Safe System. The modified software can therefore still be used in applications up to SIL 3.

4.4. Evaluation of other changes to the AIM Safe System which are not associated with the introduction of the new controller module RCU502

Other changes to the AIM Safe System are changes which implement bug fixes and minor upgrades of the software functionality. These changes are in detail described in the AIM release notes, see /D1/, /D2/, /D3/ and /D4/.

The changes have been performed following the agreed procedure for software modifications, the so-called track procedure, see /D5/ document: PRO-2099, Version 3.0.0.

During a visit to the manufacturer's site spot checks have been performed whether the agreed modification procedure has been successfully observed, see /D6/. It can be confirmed that the agreed procedure for modifications has been successfully applied for the implementation of the software changes.

It can therefore be concluded that the required Systematic Safety Integrity has not been negatively influenced by the implementation of the modifications and the software can still be used in applications up to SIL 3.

Further a hardware change has been performed to the non-safety related frequency inputs of the I/O module RMP420S. Due to availability issues additional resistors have been added on the input side. An impact analysis has been performed for the change and appropriate test activities have been defined and executed, see /D5/ document: CO14963_DRB. The change has no impact on the safety functionality of the device.

4.5. Evaluation of the changes to the modification procedure (Track Procedure)

The procedure for the implementation of modifications, the so-called track procedure, has been updated from version 3.0.0 to version 4.0.0., see /D5/.

The main change is the introduction of a detailed description for the track states like creation, evaluation, resolution etc. The tasks and responsibilities associated with each state have been defined in detail. Further the documentation requirements have also been specified in more detail.

Additionally some minor clarifications and extensions have been added to the track procedural flow.

The changes introduced to the track procedure improve the usability of the procedure and can increase the overall quality for the execution of the modifications.

In summary it can be concluded that the updated track procedure, version 4.0.0, is still suitable to perform modifications according to the requirements for SIL 3 according to IEC 61508.

4.6. Application standards

The AIM Safe System complies with the relevant requirements of EN 54-2 and can be used within fire detection and fire alarm systems if used in accordance with the application requirements described in EN 54-2.

Further the AIM Safe System complies with the relevant requirements of EN 50156-1 can be used within burner management systems if used in a 1oo2 topology and in accordance with the application requirements described in EN 50156-1.

The AIM Safe System also complies with the relevant requirements of NFPA 72 and can be used within fire alarm and emergency communication systems if used in accordance with the application requirements described in NFPA 72.

5. Summary

The inspection of the changes to the AIM Safe System from AIM release 8.3.4 to 8.6.0 has shown 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 Safe System still complies with the requirements of the relevant standards (SIL CL 3 acc. to IEC 61508 and IEC 61511) and can be used in applications up to SIL 3 acc. to IEC 61508 and IEC 61511.

The software and hardware versions for the current approval of the AIM Safe System are documented in the appendix to certificate No.: 968/EL 161.05/14.

The restrictions and conditions of the previous approvals apply. In particular for all applications a safe state must exist 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, 2014-01-27
TIS/A-FS/Kst. 968 dr.ro-nie

The inspectors

Dr. Peter Robben

Dipl.-Ing. Robert Heinen

Report released after review:
Date: 2014-01-27

Dipl.-Ing. Gernot Klaes