

2009-05-04

**Automation, Software and Information Technology**

**Test report about the examination of the  
software driver NetloSafe Driver for a Safe Network  
Communication System**

**Report-No.: 968/EL 606.00/09  
Date: 2009-05-04**

**Test report about the examination of the  
software driver NetloSafe Driver for a Safe Network  
Communication System**

**Report-No.:** 968/EL 606.00/09

**Date:** 2009-05-04

**Pages:** 10

**Test object:** NetloSafe Driver Version 1.1

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

**Order-No./Date:** RSB-105553 dated 2009-02-09

**Test Institute:** TÜV Rheinland Industrie Service GmbH  
Automation, Software and Information Technology (ASI)  
Am Grauen Stein  
51105 Köln  
Germany

**Department:** Automation, Software and Information Technology (ASI)

**TÜV-Offer-No./Date:** 968/33/09 dated 2009-01-27

**TÜV-Order-No./Date:** 10156803 dated 2009-02-17

**Inspectors:** Dr. Peter Kocybik  
Dipl.-Ing. Robert Heinen

**Test location:** see Test Institute

**Test duration:** April 2008 to May 2009

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.

<b>Contents</b>	<b>Page</b>
1. Scope	4
2. Standards forming the basis for the requirements	4
3. Test object	5
3.1 Identification of the test object	5
3.2 Documents	8
3.3 Released software revisions	8
4. Tests and test results	8
4.1 General	8
4.2 Test sequence	8
4.3 Definition of the safety requirements	9
4.4 Description and result of the inspection of the safety structure	9
4.5 Assessment of the requirements in accordance with IEC 61508 and IEC 62280-2	9
4.5.1 Definition of general requirements	9
4.5.2 Documentation of the entire software element life cycle	9
4.5.3 Assessment of the measures for avoiding failures	9
4.5.4 Requirements in accordance with IEC 62280-2	10
5. Summary	10

## 1. Scope

The following report details the results of the examination of the NetloSafe Driver. The NetloSafe Driver is a software driver for a Safe Network Communication System - developed by Kongsberg Maritime AS for safe exchange of binary IO data between controller nodes. It is planned to utilize the NetloSafe Driver as a re-usable software element in the Albatross-Integrated-Multifunction (AIM) 7 and AIM 8 Software Platforms. The NetloSafe Driver was subject to an assessment in accordance with IEC 61508 Safety Integrity Level 3 (SIL 3).

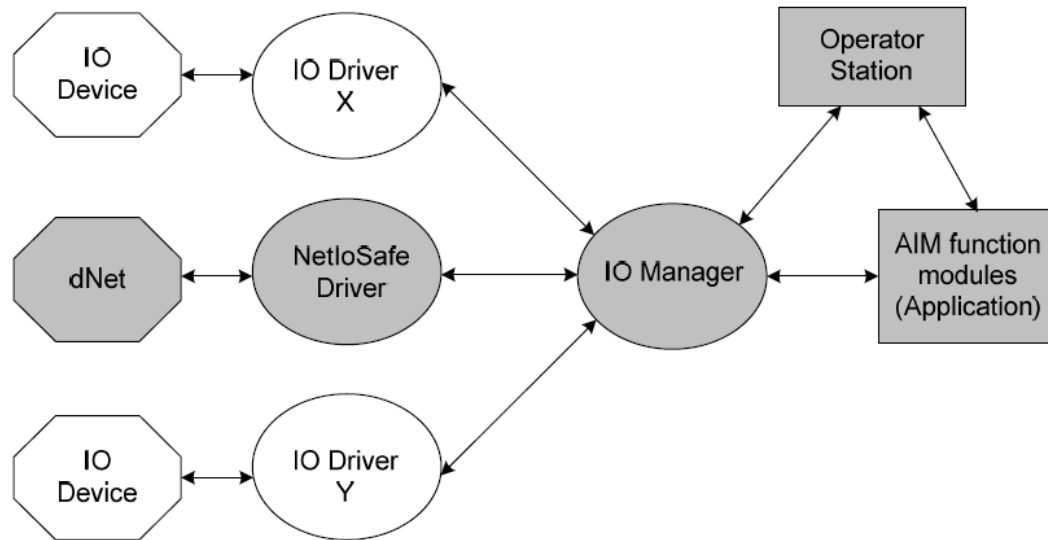


Figure 1: Context of NetloSafe-Driver

This test report will provide traceable evidence, that the test object complies with the functional and safety-related requirements of the NetloSafe Driver Specification, see [D2], satisfies the requirements of the relevant standards and can thus be used as software element in the Albatross-Integrated-Multifunction (AIM) system if the information given in the NetloSafe-Driver Safety Manual and referenced documents is followed. The use of the NetloSafe Driver within the AIM system is illustrated in figure 1.

This test report contains the essential safety engineering aspects, which were assessed during the concept-, design- and test-phases and identifies the various test steps, which have been performed to provide evidence that the test object complies with the safety-relevant requirements of the NetloSafe Driver Specification and the relevant standards. Further it is described which tests were performed, who performed them and which results were obtained.

## 2. Standards forming the basis for the requirements

### [N1] IEC 61508 Part 1 - 7:1998 and 2000

Functional safety of electrical/electronic/programmable electronic safety-related systems

### [N2] IEC 65A/524/CDV, IEC 61508-2 Ed 2, Annex D

Functional safety of electrical/electronic/programmable electronic safety-related systems

Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

Annex D: Safety manual for compliant items

**[N3] IEC 65A/524/CDV, IEC 61508-3 Ed 2, Annex D**

Functional safety of electrical/electronic/programmable electronic safety-related systems

Part 3: Software requirements

Annex D: Safety manual for compliant items: additional requirements for software elements

**[N4] IEC 62280-2:2002**

Railway applications - Communication, signalling and processing systems

Part 2: Safety-related communication in open transmission systems

**3. Test object**

**3.1 Identification of the test object**

The NetloSafe Driver provides an end to end transport service for safety messages containing binary safety IO data which operates above existing potentially unreliable communication channels. The deployment of the NetloSafe Driver is limited to installations employing exclusively wired communications channels. The NetloSafe Driver is designed to operate in private networks only without any connection to the Internet or telephone lines. The service shall guarantee that the rate of undetected communication failures does not exceed 1% of the total SIL 3 specified rate of failures for continuous mode of operation transmission systems according to IEC 61508-1. It is planned to use the communication system in the Albatross-Integrated-Multifunction (AIM) system, which is an on-demand mode respectively low-demand mode of operation safety system.

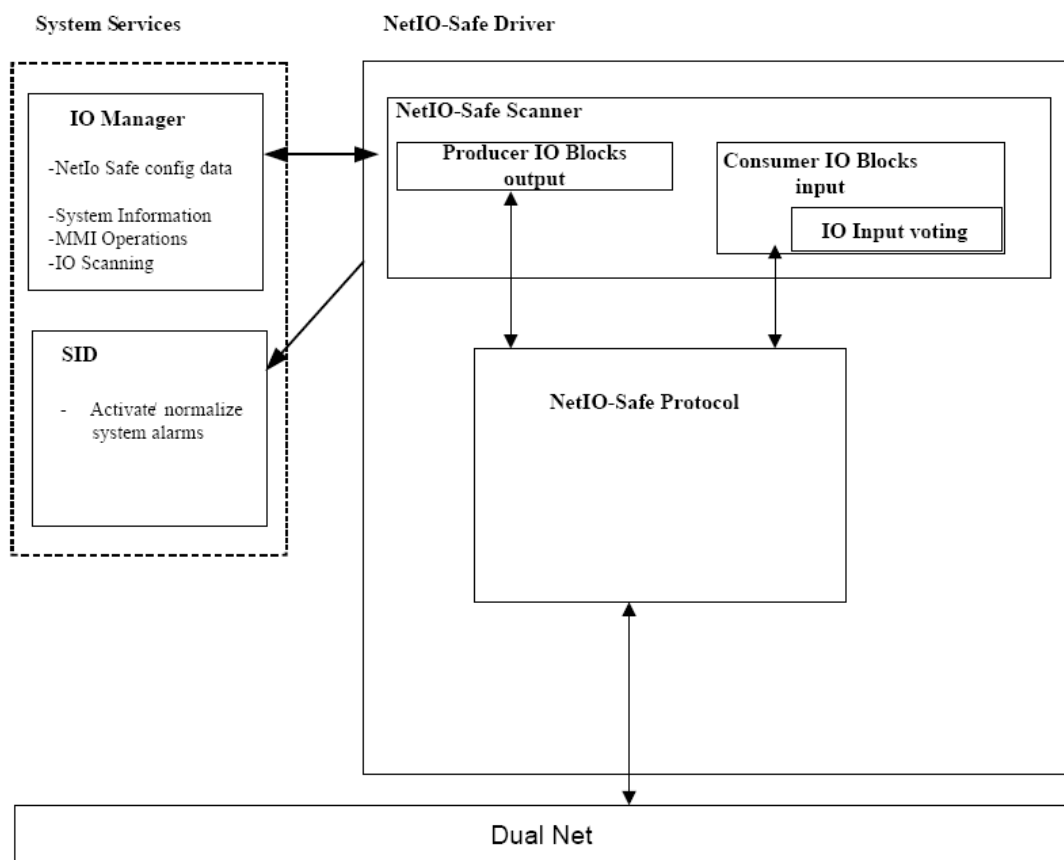


Figure 2: NetloSafe Driver block-diagram

The NetloSafe Driver is designed to interface with the generic framework of the AIM system IO Manager, see figure 2. The generic framework of the IO Manager provides an abstract higher level IO driver for system design.

The System Information Database (SID) consists of SID nodes created by system components such as IO drivers. System alarm objects are the interface to the overall alarm system. A system alarm object is always linked to a SID node in order to relate the system alarm to a system component. The NetloSafe Driver uses this interface to create SID nodes and system alarms.

The Dual Net is the used standard communication system for information exchange between Process Stations (PS).

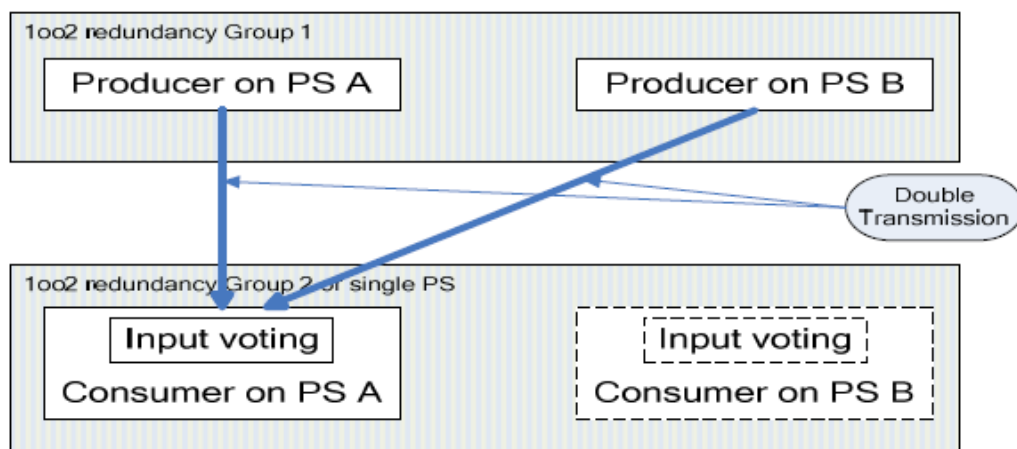


Figure 3: Double transmission

The NetloSafe protocol is an asymmetric connection based protocol where the peers in the communication are designated as a Consumer (SDcon) or a Producer (SDpro) running on a Process Station, see figure 3. The connections are initiated by the consumer which is then responsible for detecting errors in the communication with the producer. This connection is called subscription. In order for a subscription and consequent data transfer between consumer and producer, they first must agree upon a version of the NetloSafe protocol to use. This will be done while Communication Establishment. After Communication Establishment the subscription has to be established before safety data will be provided by the Producer. All subscriptions have a timeout. Therefore all subscriptions have to be renewed cyclically.

The safety data has always to be sent from two different Process Stations as producers to the single consumer (double transmission) running on another Process Station. The consumer combines the values of the data blocks received from the two producers through a safe 1oo2-voting. This 1oo2-voting guarantees a safety action even in the case where only one of the data blocks carries the demand. In order to obstruct a shutdown, both data blocks must be falsified at the time of voting. It is implied that the two producers send the safety data from the same origin.

	Producer PS A IO Value	Producer PS B IO Value	Consumer		Block Alarm (SID)
			IO Value	IO Status	
1	No safety action	No safety action	No safety action	OK	No Alarm
2	No safety action	Safety action	Safety action	OK	No Alarm
3	No safety action	Fault	No safety action	OK	Alarm caused by Producer PS B
4	Safety action	No safety action	Safety action	OK	No Alarm
5	Safety action	Safety action	Safety action	OK	No Alarm
6	Safety action	Fault	Safety action	OK	Alarm caused by Producer PS B
7	Fault	No safety action	No safety action	OK	Alarm caused by Producer PS A
8	Fault	Safety action	Safety action	OK	Alarm caused by Producer PS A
9	Fault	Fault	Frozen old IO Value	IO Error	Alarm caused by both Producers

Figure 4: 1oo2-voting

The voting combines IO Values from two producers into one consumer IO Value and IO Status, see figure 4. The IO Values are sent at fixed intervals and the receiver keeps the last received valid data from each producer. If valid data with an acceptable age is not available, the IO Values of this subscription are considered to be invalid respectively faulty.

In case that the received data from one producer is faulty, the System Information Database (SID) will inform the Operator Station via the IO Manager. The human operator is requested to acknowledge the alarm within a predefined time, which is dependent on the respective system configuration. While an alarm is active the system using the NetloSafe protocol has to switch to degraded mode (SIL3 is not longer fulfilled). For the safe use of the NetloSafe Driver it is not allowed that the NetloSafe protocol alarm is activated and deactivated regularly.

In case that the data received from both producers is faulty, the IO Status hence switches from OK to IO Error, physical digital outputs which use this information as setting value must switch into the safe state. It is not allowed that the last (frozen) IO Value is further used.

The residual error rate for a one dual producer to single consumer configuration is calculated to be  $\Lambda = 7 \cdot 10^{-14}$  per hour under the constraint that the message length is not longer than 5232 bit and that not more than 10 messages are send per second.

In a system where more than one dual producer to single consumer communication is part of the safety loop, the residual error rate of each subscription being part of the safety loop must be summarized to calculate the residual error rate for the respective safety function.

In theory up to 14000 dual producer to single consumer entities may be configured in series, and the 1% of the total SIL3 specified rate of failures for continuous mode of operation transmission systems requirement is still fulfilled:

$$\Lambda = 14000 \cdot 7 \cdot 10^{-14} = 100000 \cdot 10^{-14} = 10^{-9} \text{ per hour}$$

### 3.2 Documents

The complete project documentation for development, design and quality management are summarized and stored on TÜV Rheinland's file-server:

The principal NetloSafe documents are listed in the following:

NetloSafe-Documents				
No.	Document	Document-No.	Rev.	Date
[D1]	Safety Manual Netlo Safe Driver Version 1.1	331435	A6	2009-04-21
[D2]	Specification NetIO Safe Driver	325435	D2	2009-04-02
[D3]	Architecture Specification NetloSafe Protocol	328861	D1	2009-03-30
[D4]	Architecture Specification, NetloSafe Driver	328858	D2	2009-04-15
[D5]	Test Specification, NetIO Safe Driver	328864	A4	2009-04-02
[D6]	NetloSafe Driver Test Description (Test Report)	328862	A5	2009-04-20
[D7]	Test Report: NetloSafe test.	TestReport_21_04_2009.html	-	2009-04-21

### 3.3 Released software revisions

Product Name	Product rev.
NetloSafe Driver	Version 1.1.0

## 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 Test sequence

The testing of the NetloSafe Driver was performed in parallel to the development process.

Inspections and analyses were performed at the Test Institute and at customer's premises. As part of these inspections the aspects of functional-safety and the completeness and correctness of the documentation were investigated.

The software system and software module tests documented by the manufacturer were inspected and verified through spot-checks.



2009-05-04

#### **4.3 Definition of the safety requirements**

The NetloSafe Driver must comply with the general requirements for safety-systems in accordance with:

- IEC 61508 Part 1 - 7:1998 and 2000 SIL 3
- IEC 62280-2: 2002

#### **4.4 Description and result of the inspection of the safety structure**

The NetloSafe Driver is designed for the use in the Albatross-Integrated-Multifunction (AIM) 7 and AIM 8 Software Platforms to exchange binary IO data between controller nodes safely. For further information please read chapter 3.1. The safety structure described in chapter 3.1 fulfills the requirements of the relevant standards for a safe communication service in a safe communication system.

#### **4.5 Assessment of the requirements in accordance with IEC 61508 and IEC 62280-2**

##### **4.5.1 Definition of general requirements**

The NetloSafe Driver shall meet the requirements for Safety Integrity Level 3 (SIL 3) of IEC 61508 and open transmission systems of IEC 62280-2.

The following points have been assessed:

- Documentation
- Measures for the avoidance of failures (QM)
- Measures for controlling failures during operation
- Measures against threats on open transmission systems (IEC 62280-2)

##### **4.5.2 Documentation of the entire software element life cycle**

A documentation system, which corresponds to the requirements of the V-model according IEC 61508, has been established by Kongsberg for this project. This system contains documents, which reflect the left development wing of the V-model for a software element. It further contains plans for the verification and validation activities for the software element. And it contains the test reports about the performance of all software module and integration tests, which reflect the right wing of the V-model for a software element.

A Safety Manual and further referenced documentation are available which describe the required information for using the software element. These documents have been inspected regarding completeness, consistency and conformity in accordance with [N1] - [N4].

It can be confirmed that the documentation meets the requirements of IEC 61508.

##### **4.5.3 Assessment of the measures for avoiding failures**

The applied measures for the avoidance of failures during the relevant life phases of the product from specification until the conclusion of the development, verification and validation procedures meet the requirements for SIL 3 of IEC 61508. These measures have been reviewed and inspected for compliance to the recommendations of IEC 61508.

From the manufacturer an abstract for software is available, which lists the measures being applied to meet the requirements of IEC 61508-3.

It can be confirmed that the applied measures for avoiding failures meet the requirements of IEC 61508.

#### 4.5.4 Requirements in accordance with IEC 62280-2

The applied measures against threats on open transmission systems have been reviewed and inspected for compliance to the recommendations of IEC 62280-2.

The applied measures for detecting and controlling failures during operation as defined in IEC 62280-2 have been reviewed, inspected and tested (see also file Kongsberg\_FIT\_AIM8\_x\_V1\_3\_2009-04-23.doc). These measures are also able to control faults according IEC 61508.

It can be confirmed that the applied measures for detecting and controlling failures during operation meet the requirements of IEC 62280-2.

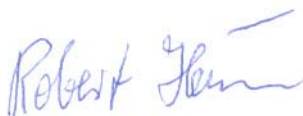
#### 5. Summary

The examination of the NetloSafe Driver Version 1.1, developed by Kongsberg Maritime AS, came to the result that the requirements of IEC 61508 and IEC 62280-2 are met if the NetloSafe driver will be used by Kongsberg Maritime AS as part of the Albatross-Integrated-Multifunction (AIM) 7 or AIM 8 Software Platforms. The integrator needs to observe the specific requirements defined in the Safety Manual [D1] and therein referenced documents. The mentioned restriction, stated in chapter 3.1, shall be observed, in particular the protocol length is restricted to a maximum of 5232 bit; the transmission rate has to be restricted to a maximum of 10 re-transmissions per second; it is not allowed that the NetloSafe protocol alarm is activated and deactivated regularly; if an IO error occurs for the Netlo communication it is required that the associated outputs must be switched to the safe state; the operator is required to take appropriate actions if a fault in the Netlo communication occurs.

The integrator of the NetloSafe Driver is further obliged to verify the correct execution of every safety related function after integration of the NetloSafe Driver into the AIM 7 or AIM 8 Software Platforms.

Cologne, 2009-05-04  
TIS/ASI/Kst. 968 hei-drko-nie

The inspectors



Dipl.-Ing. Robert Heinen



Dr.-Ing. Peter Kocybik

Report released after review:  
Date: 2009-05-04



Dipl.-Ing. Heinz Gall