KONGSBERG

TECHNICAL NOTE

Date: **24.11.04**

Issued by: Arnt Ole Lia

Subject: Default set-up of AIM Safe systems forming part of an IEC 61508 function.

References:

1. ESD and F&G Manual SW Configuration typicals, document id.: 171931 or its successor.
2. Shutdown SW Configuration typicals, document id.: 162748 or its successor.
3. F&G SW Configuration typicals, document id.: 162739 or its successor.
4. Design Manual for safety systems.
5. KS HW loop typical database, id ks\NOKBG0066.nsf

1 INTRODUCTION

This technical note describes vital set-up data for any AIM Safe system forming a part of an IEC 61508 function. Any alteration to set-up described herein must be subject to in depth formal analyses of personnel with in-dept IEC61508 knowledge.

2 DESIGN

The design of safety systems shall follow:

1. Data given in this technical note, in addition appropriate rules, regulations and class society's rules for the specific delivery must be adhered to. Further product and project specific specifications and design manuals shall be followed.

2. The design and configuration of AIM Safe systems with SIL requirements shall be performed or supervised by safety personnel within the Kongsberg group.

3 HARDWARE REQUIREMENTS

1. With respect to environmental requirements the hardware to be used in IEC 61508 compatible systems must meet the environmental requirements given in the Kongsberg Maritime AS environmental specification.

2. Hardware loop typical qualified for IEC 61508 use can be found in KS HW loop typical database. Modifications or qualifications of additional typical must be subject to qualification through FMEA and subsequent tests.

KONGSBERG SIMRAD AS

Kirkegårdsveien 45, Carpus, P.O.Box 483 N-3601 Kongsberg Norway Telephone +47 32 28 50 00
Telefax +47 32 28 50 10
Enterprise number NO 943 073 678 MVA Bank account 7139.05.23194 www.kongsberg-simrad.com

3. For each delivery probability calculations shall be prepared in accordance with Kongsberg Maritime AS for all hardware variants used in a Safety Integrity Function (SIL). Maintenance intervals used in these calculations shall be used as recommendations to customers.

4 HARDWARE CONFIGURATIONS

The following hardware configurations can form part of an IEC 61508 function:

Type	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
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

Column FOST/xotest indicates that test for moving of output stage relays or activation of output driver must be enabled.
Column Line monitoring indicates that open- and short-circuit detection must be enabled.

5 SOFTWARE CONFIGURATIONS

1. The safety systems can run with AIM release 6.9-6.11 or 7.2. The releases AIM 6.9 and 7.2 has been subject to TÜV inspection.

2. The set-up of the header of the *.ps file is crucial. The name and sequence of the parameters varies somewhat from release to release, but the functionality described below shall be fulfilled.

```
Start-up modes
Sim = 0 #Safety systems shall start in IO mode#
Passive = 0 #Safety systems shall start active#
ModuleMode = 0 #Safety systems shall start with active modules#
SetPsMode = 1 #Operator with proper access rights can change mode#

Redundancy
RedUpdateDisable = 0 #Redundancy update shall be enabled#

Misc
AcceptIoConnErr = 0 #No IO connection errors are accepted#
IoFileRequired = 1 #IO file required for start-up#
HotStart = 0 #PLC (Flexi) modules status shall not be saved#
Checksum = 1, #Errors in checksum for modules shall be reported#

Diagnostics
Bite
Mode = 3 #Stop SBC/RCU on any Bite failure#
```

```
Network
Netstorm
Protection = 1 #Netstorm protection is enabled#

FloatingPointExceptionHandling
Definitions
ForcedSuspendTask = 0 #Floating point exception behavior active#
Schema = "AimStandard" #Alarms and stops computer#


EnvironmentCheck
SbcPowerAlarm
Position = 0 #Disabled(0) on RCU solutions, 3 on SBC solutions#
24VPowerAlarm
Channel = n #Shall be enabled to relevant ONBIO#
FanAlarm
Enable = 1 #Fan alarm shall be enabled#
```

Set-up of the remaining parameters in the header file shall be decided by the delivery project.

6 TEST

1. All generic system solutions shall be subject to product tests according to Kongsberg Maritime AS internal routines.
2. All delivery systems be subject to Internal Acceptance Test (IAT), Factory Acceptance Test and Commissioning/Site Acceptance Test (SAT).
3. For systems subject to class notation the delivery systems may be required to class notation certification test, any safety system subject to class notation shall be in accordance with the class notation type approvals. In cases where class society's rules and IEC 61508 rules are in conflict the customer must be formally addressed.