Technical Report

IQ2 Pro

Manufacturer:

Rotork Controls Limited

Brassmill Lane
Bath, England BA1 3JQ
United Kingdom

Report no. RB81980T
Version 1.0 of September 26th, 2007

Test and Certification Body

TÜV SÜD Rail GMBH
Automation, Software and Electronics – IQSE
Ridlerstrasse 65
D-80339 Munich

TABLE OF CONTENTS

Revision

Version	Status	Date	Author	Modification
1.0	initial	2007-09-26	Velten-Philipp	

Table 1: Revision

Acronyms and Abbreviations

TERMS	DEFINITIONS
Common cause failure	Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure
Response time	Time from a demand to a sub-system and until the correct state on this sub-system output, is achieved.
Failure	The termination of the ability of a functional unit to perform a required function.
Fault	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.
Fault avoidance	Use of techniques and procedures, which aim to avoid the introduction of faults during any phase of the safety lifecycle of the safety-related system.
Fault detection and reaction time	Time from occurrence of a fault and until it is found and reported as an output of this sub-system.
Random hardware failure	Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.
Redundancy	Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information.
SFF	safe failure fraction

1 Scope

The objective of this report is to describe the verification and assessment activities of the type approval carried out on Rotork's IQ pro actuator system. The purpose of the type approval is to demonstrate that the actuator meets the requirements up to safety integrity level 2 according to the IEC 61508 [1] standard including the requirements, as far as applicable, of the standards listed in chapter 2 - Basis of testing.

2 Basis of testing

The regulations and guidelines which form the basis of the type testing are listed below.

2.1 Functional Safety

[N1] IEC 61508: 2000
Functional safety of electrical/electronic/programmable electronic safety-related systems

[N2] IEC 61511, Parts 1-3: 2004
Functional safety
Safety instrumented systems for the process industry sector

2.2 Basic product standard

[N3] IEC 61010-1:2001
Safety requirements for electrical equipment for measurement, control, and laboratory use

2.3 Electromagnetic Compatibility

[N4] EN 61326-1:1997 and annex A1:1998, A2:2001, and A3:2003
Electrical equipment for measurement, control and laboratory use - EMC requirements

3 Test Object

Test object is the IQ pro actuator family consisting of actuators labeled 3xxx-xxx, where x means a number to specify different actuator versions. The versions differ by

- Kind of remote indication (analogue and digital)
- Actuator power supply
- Kind of control loop
- Kind of speed control
- Kind of external power supply

All actuators of the IQ pro family have the same safety function and safety properties implemented. The IQ pro actuators are used in wide variety of different models to actuate valves in process, oil and gas industry.

4 Documentation

4.1 Specification /Requirements/Procedures

	Title	No	Rev.	Date
D1	Safety Requirements Specification for IQ Pro Actuator	ER285	3	2007-03-07
D2	Functional Specification for IQ2 Pro Safety Option PCB Assembly.doc	ER328	1	2007-02-28
D3	Safety Plan for IQ Pro SIL 2 Actuator.doc	ER331	2	2007-02-16
D4	Safety measures required for IQ Pro SIL 2 Actuator.doc	ER339	0	2007-05-09
D5	IQ Pro SIL Validation Plan.doc	ER286	1	2007-02-21
D6	Verification of the modification procedure.doc	ER338	0	2007-05-21

4.2 Design Specification

	Title	No	Rev.	Date
D7	IQ SIL option board software specification v0.4.doc	ER323	0.4	2007-03-07
D8	Functional Specification for IQ2 Pro Safety Option PCB Assembly.doc	ER328	1	2007-02-28
D9	Safety Concept Specification for IQ Pro Actuator	ER321	2	2007-05-09

4.3 Design-Verification

Software

	Title	No	Rev.	Date
D10	SIL Option Board Software Design Review.doc	---	---	2006-08-04
D11	SIL Software Functional Comparison - HC08.doc	---	---	2006-11-15
D12	SIL Software Functional Comparison - PIC.doc	---	---	2006-11-15
D13	SIL Software Review - PIC.doc	---	---	2006-12-06
D14	SIL Software Review -2 - PIC & Display Processor - Response.doc	---	---	2007-03-22

	Title	No	Rev.	Date
D15	SIL Software Review -2 - PIC & Display Processor.doc	---	---	2007
D16	46079-TN05 SIL Option Board - Statement on compiler verification.doc	TN05	---	2007
D17	46079-TN05a PIC - Transparent Galpat Listing.xls	TN05a	---	2007
D18	46079-TN05b SIL Option Board HC08 code inspection.doc	TN05b	---	2007
D19	TN04 fault insertion .doc	46079	---	2007

FMEA

	Title	No	Rev.	Date
D20	IQ Pro SFF and PFD.doc	ER329	2	2007-05-30
D21	SF1 and SF2 IQ mechanical.xls SF1 Estimation of SFF for the processors.doc SF1 Interface and interlocking FMECA overview.doc SF1 IQ Pro 48128 local controls board.xls SF1 IQ2 FMECA 46079 Drive Logic.xls SF1 IQ2 FMECA Power Module Output stage.xls SF1 IQ2 FMECA Power Module PSU.xls SF1 IQ2 Pro FMECA 48128 signal conditioning.xls SF1 IQ2 Pro FMECA - 48128 non safety components.xls SF1 IQ2 Pro FMECA 46079 buffering.xls SF1 IQ2 Pro FMECA 46079 fault relay.xls SF1 IQ2 Pro FMECA 46079 inhibit.xls SF1 IQ2 Pro FMECA 46079 processor monitors.xls SF1 IQ2 Pro FMECA 46079 PSU.xls SF1 IQ2 Pro FMECA 48128 PSU.xls SF1 IQT Estimation of SFF for the processors.doc SF1 IQT FMECA 45696 Drive Logic.xls SF1 IQT FMECA 45696 Power Module PSU.xls SF1 IQT FMECA 46079 Drive Logic.xls SF1 IQT Interface and interlocking FMECA overview.doc SF1 IQT Mechanical.xls SF1 IQT Output stage FMECA overview.doc SF1 IQT Pro FMECA 48128 signal conditioning.xls SF1 IQT Pro 48128 local controls board.xls SF1 IQT Pro FMECA - 48128 non safety components.xls SF1 IQT Pro FMECA 46079 buffering.xls SF1 IQT Pro FMECA 46079 fault relay.xls SF1 IQT Pro FMECA 46079 inhibit.xls SF1 IQT Pro FMECA 46079 processor monitors.xls	---	---	2007-03

	Title	No	Rev.	Date
	SF1 IQT Pro FMECA 46079 PSU.xls SF1 IQT Pro FMECA 48128 PSU.xls SF1 IQT PSU FMECA overview.doc SF1 Output stage FMECA overview.doc SF1 PSU FMECA overview.doc			
D22	SF2 Estimation of SFF for the processors.doc SF2 Interface and interlocking FMECA overview.doc SF2 IQ Pro local controls board.xls SF2 IQ Pro PSU FMECA overview.doc SF2 IQ2 FMECA 46079 Drive Logic.xls SF2 IQ2 FMECA Power Module Output stage.xls SF2 IQ2 FMECA Power Module PSU.xls SF2 IQ2 Pro FMECA 48128 signal conditioning.xls SF2 IQ2 Pro FMECA - 48128 non safety components.xls SF2 IQ2 Pro FMECA 46079 buffering.xls SF2 IQ2 Pro FMECA 46079 fault relay.xls SF2 IQ2 Pro FMECA 46079 inhibit.xls SF2 IQ2 Pro FMECA 46079 processor monitors.xls SF2 IQ2 Pro FMECA 46079 PSU.xls SF2 IQ2 Pro FMECA 48128 PSU.xls SF2 Output stage FMECA overview.doc	---	---	2007-03

Hardware

	Title	No	Rev.	Date
D23	C2051_IQPro_EMC_01.pdf C2052_IQTPro_EMC_01.pdf	C2051 C2052	0	2007-03-06
D24	Nodal Analysis 46079c.xls	---	---	2007

4.4 Design

	Title	No	Rev.	Date
D25	Schematics ed06388.tif ED07636-02.tif ED07680-03.TIF ED07912-03.TIF ed07971-01.pdf		 01 02 03 03 A02	

	Title	No	Rev.	Date
	ed08126-03.pdf			
D26	SIRA FM Approval IQ.pdf SIRA FM Approval IQT.pdf	3003575 3017942		2001-09 2003-10

4.5 User documentation

	Title	No	Rev.	Date
D27	E173E3_V6.doc		DRAFT	2007-09-14

4.6 Checklists

	Title	No	Rev.	Date
D28	IEC 61508-1 Checklist, TÜV		1.5	2007-07-03
D29	IEC 61508-2 Checklist, TÜV		1.4	2007-07-03
D30	IEC 61508-3 Checklist, TÜV		1.0	2007-07-03

4.7 Wiring Diagrams

IQ

3000S000 – IQ standard with SIL PCB fitted
3060S000 – IQ with CPT and SIL PCB fitted

IQT

6000S000 – IQT standard with SIL PCB fitted
6060S000 – IQT with CPT and SIL PCB fitted

IQTM

7000S000 – IQT modulating with SIL PCB fitted
7060S000 – IQT modulating with CPT and SIL PCB fitted

5 Result type approval

5.1 Management of functional safety

Rotork is an DIN ISO IEC 9001 certified company. The quality management system complies also to requirements of the ATEX directive. Rotork prepared following documents to demonstrate that management of functional safety complies to the requirements of IEC 61508:

- Safety Plan;
- Verification and Validation Plan;
- Documentation Plan

The safety plan describes the project, the life cycle and the basic principles to manage functional safety during the project. The verification and validation plan specifies in detail the activities to verify and validate the products. The documentation plan was necessary to support control of documentation, revision and status.

Result
The documents above were reviewed during the project and are suitable for SIL 2and SIL 3.
The results are documented by /D28, D29, D30/.

5.2 Safety function

The main function of the IQ pro actuator is to move remotely valves of different sizes and ranges which are used in process, oil and gas industry. The movement is induced by an electrical motor and by mechanical components like worms and gear boxes. The safety functions of the IQ pro actuator are described by the safety requirements specification /D1/.

There are two safety functions:

1 *The actuator shall not move without a valid remote open or remote close signal.*
If an internal failure is detected, the actuator will give an alarm signal.

2 *If the ESD signal is active, then the actuator will perform the commissioned ESD action.*
If an internal failure is detected, the actuator will give an alarm signal.

Safety function 1 is a high demand mode safety function in contrast to safety function 2 which operates in low demand mode.

Input for safety function 2 is the ESD command which is active if the input signal is between 0 and 3 VDC.
The above definition of safety functions guarantees that the actuator starts to perform the commanded action and alarms in case the commanded ESD cannot be performed. The safety function 2 is to move the actuator to the commissioned fully open or close position. Safety function 1 guarantees furthermore that there is no movement without command.

The safety functions specified shall fulfill SIL 2 in a 1oo1 architecture or SIL 3 in a 1oo2 architecture of the actuator.

5.3 Hardware requirements

5.3.1 Concept and Architecture

The actuator consists of mechanical components, a computer based electronic control unit, and a power supply. The mechanical components are in use for more than 4 years and sufficient reliability data is available. These components are considered as type A components according to IEC 61508-2.
The mechanical components have a fault tolerance of 0 regarding execution of the safety functions. The control unit is a microcontroller based device (type B) with 1oo2 architecture. One microcontroller performs the unit function and executes diagnostic functions; the other microcontroller supervises the function and performs also diagnostics. Both controllers are able to execute the safety functions. Figure 1shows a simplified block diagram of the actuator.

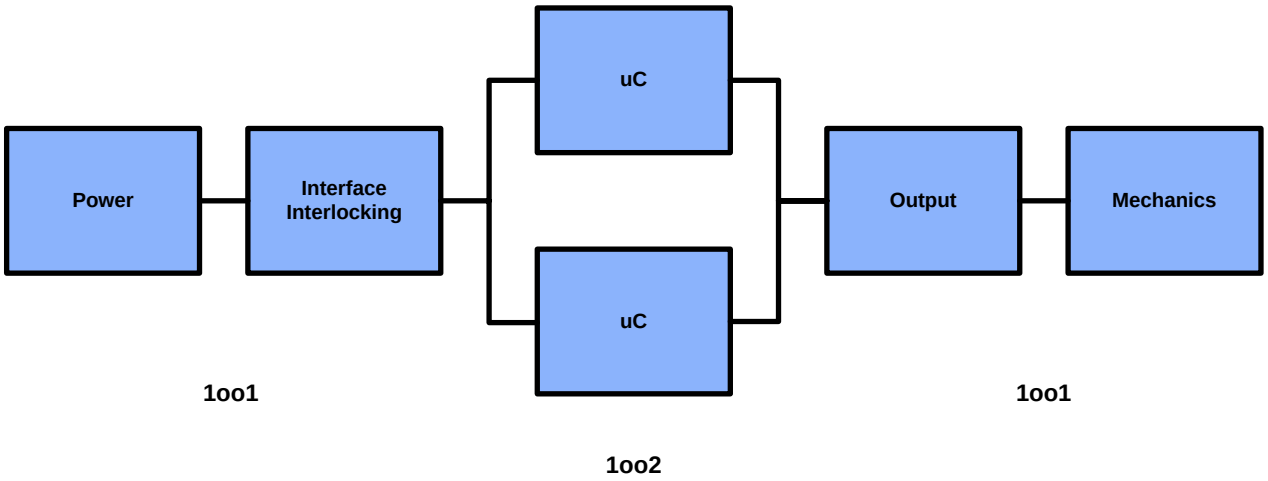

Figure 1 – Block diagram actuator

5.3.2 Measures to control faults

Rotork has implemented measures to control faults to fulfill the IEC 61508-2 requirements and to improve the diagnostic coverage of the device to reach the SFF target for the subsystems of the device. Diagnostics are mainly implemented to detect

- Failures of mechanical actuation
- Incorrect drive signals
- Dangerous failures of microcontroller hardware
- Failures of support subsystems like power supplies

The measures to control faults are described by the

- Safety requirements specification /D1/
- SIL option board software specification /D7/

Result

The measures to control faults were reviewed. Effectiveness of the measures was demonstrated by analyses and fault injection testing (see D10 to D19). The measures are suitable for SIL 2.

Note: The measures to avoid faults are suitable for SIL 3. This allows using two actuators in a 1oo2 configuration for SIL 3 applications.

5.3.3 FMEA

Rotork carried out a component based FMEA for all elements which are related to the safety function. The FMEA analyzes the actuator behavior in the presence of faults.

Result
The FMEAs /D20, D21, D22/ demonstrate that the required target SFF for each subsystem is maintained and provide the failure rates which serve as basis for the PFD and PFH calculation.
The FMEA was reviewed without any objections.

5.3.4 Probability of failure on demand -PFD how about PFH?

From the FMEA reliability data was calculated. The following table shows the results for different system configurations:

	Safety Function 1		**Safety Function 2**
Hardware	**IQ Pro**	**IQT Pro**	**IQ Pro**
Type	B	B	B
Hardware fault tolerance	0	0	0
Safe failure fraction	99.7%	99.6%	91.4%
Safe detected failure rate [/h]	2.60E-06	2.60E-09	1.36E-06
Safe undetected failure rate [/h]	9.94E-06	9.93E-09	8.67E-06
Dangerous detected failure rate [/h]	0.32E-09	0.32E-09	0.32E-09
Dangerous undetected failure rate [/h]	3.33E-08	50.32E-9	3.33E-08
SIL	2	2	2
PFH	33.6E-9	50.6E-9	
PFDavg			4.10E-3
Proof Test Interval			12 Month
Mean Time To Repair	12h	12h	12h

Result
The device is suitable for SIL 2 safety related loops.

5.3.5 Fault injection testing

Fault injection testing was carried out by Rotork and was witnessed by TÜV. The fault injection testing covers all important system components and exercised the diagnostic measures which are implemented.

Result
The fault injection testing /D19/ and the related witness testing was performed without any objections.

5.4 Software requirements

5.4.1 Measures to avoid faults

The measures to avoid faults during software development are described by /D1, D4, D7/. The measures have been reviewed and audited during the project. Rotork decided to use measures to avoid faults according to IEC 61508-3, Annex A for SIL 3 to enable redundant system configuration for SIL 3 applications.
The development bases on proven design methods within the Rotork company and uses semi formal software specifications, modularization and static code analyze. Programming rules and internal reviews were used to ensure sufficient software quality.

Result
The specified measures to avoid faults during software development are suitable for SIL 3.

5.4.2 Software verification

Rotork performed software analyses, reviews and software testing during product development.
The related documentation was review by TÜV. Furthermore all diagnostic measures were tested, analyzed and reviewed during fault injection testing.

Result
The software is suitable for SIL 3.

5.5 Basic safety, EMC and environmental testing

Electrical safety is covered by approvals /D26/ which are covering hazardous area locations.
EMC was tested according to EN 61326-1 /D23/.
To repeat complete environmental testing was not necessary as only the electronic board was modified for the safety related product.

5.6 Summary

The IQ and IQT actuators are suitable for SIL 2 in 1oo1 configuration and SIL 3 in 1oo2 configuration.

Automation, Software and Electronics - IQSE

i.V.
Günter Greil

i.A.
Wolfgang Velten-Philipp