2002-05-21

Automation, Software and Information Technology

Type approval of the DVC6000 Series for ESD Solutions Valve Controller from Emerson Process Management Fisher Controls International Inc.

Report-No.: 968/EZ 127.00/02
Date: 2002-05-21

2002-05-21

**Type approval of the DVC6000 Series for ESD Solutions
Valve Controller from Emerson Process Management
Fisher Controls International Inc.**

Report-No.:	968/EZ 127.00/02
Date:	2002-05-21
Pages:	9
Test object:	Digital Valve Controller DVC6000 Series for ESD Solutions
Customer/Manufacturer:	Emerson Process Management Fisher Controls International Inc. 205 South Center Street USA-Marshalltown, IA 50158-2823 United States of America
Order-No./Date:	325980 dated 2002-02-13
Test Institute:	TÜV Anlagentechnik GmbH Automation, Software and Information Technology (ASI) Am Grauen Stein D-51105 Köln (Poll)
Department:	Automation, Software and Information Technology (ASI)
TÜV-Offer-No./Date:	968/10402 dated 2002-01-08
TÜV-Order-No./Date:	264030 dated 2002-02-05
Inspector:	Dipl.-Ing. Wolfgang Velten-Philipp
Test location:	see Test Institute
Test duration:	January 2002 to May 2002

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.

2002-05-21

Content **Page**

2002-05-21

1. Scope

Object of the approval is the Digital Valve Controller DVC6000 Series for ESD Solutions. The DVC6000 is to be used in safety related applications, where automated Emergency Shut Down (ESD) is needed.

Purpose of the type approval is to clarify, whether the safety concept and the system (hardware, software and pneumatic unit) of the DVC6000 is suitable to be used in applications up to SIL 3 according to IEC 61508 [N3].

Basic assumption during the approval was, that the safe state of the installation is the de-energized state. That means, the low state at the input of the DVC6000 system is the demand state for the final valve.

2. Basic standards

[N1] IEC 61508, part 1-7:2000
Functional safety of electrical/electronic/programmable electronic safety-related systems

[N2] EN 61326-1:1997
Electrical equipment for measurement, control and laboratory use -
EMC requirements -
Part 1: General requirements (IEC 61326-1:1997)

[N3] EN 61010-1
Safety requirements for electrical equipment for measurement, control and laboratory use
General requirements

3. Manufacturer documentation and test object

3.1 Documentation

The complete documentation of the DVC6000 system is under a quality assurance and control system at Fisher Controls.

The quality assurance of Fisher Controls International Inc. in Marshalltown is registered under the number 01163 at QMI. This certificate covers the development of the digital valve controller.

The DVC6000 Series digital valve controller was designed at Fisher Controls International, Inc., in Marshalltown, Iowa, USA. The DVC6000 design authority remains solely in Marshalltown. Final assembly and testing activities are performed at Fisher-Rosemount Singapore Pte Ltd (Valve and Regulator Division), 1 Pandan Crescent, Singapore 128461.

The quality assurance of this factory is according ISO 9002, certified by Lloyd's Register, Certificate No: 930078.

The relevant Operation Directives for the specification, development, design and manufacturing are covered in the system safety requirement specification and the system verification and validation plan.

All documents for the DVC6000 project which are used during the inspection are listed in a documentation list and are mainly available in electronic form. All relevant engineering documents are listed there.

The following documents were used during the type approval:

/Ref/	Document	Number	Revision
1	Functional Safety Management/V&V Plan	00GY01-FSM	Rev. B
2	Documentation Plan	DocumentationPlan.xls	2002-05-23
3	Safety Requirements Specification	00GY01-SaRS	Rev. K
4	FMEDA Report, exida.com	FCI 01/05-01 R030	Rev. R1.4
5	FMDEA Relay-Single-acting	00GY01- FMDEA Relay -Single-acting	Rev. 6.1
6	FMDEA Relay-Double-acting	00GY01- FMDEA Relay -Double-acting	Rev. 6.2
7	FMEDA I/P-Relay	00GY01- FMEDA I/P-Relay	Rev. 4.1
8	ESD Fault Injection Testing of DVC6000 I/P & Relay	00GY01-PTR-02	Rev. E
9	Mechanical Fault Injection Test	00GY01-PTR-04	Rev. B
10	DVC6000 ESD FMEDA Proven in Use Analysis	00GY01-FMEDA - Proven_in_Use	Rev. I
11	Functional Tests -see /2/ -Integration Phase	See /2/, Integration Phase	---
12	DVC6000 Instruction manual	Form 5647	2001-06
13	Safety Manual for DVC6000 Series ESD Solutions	Form 5743	2002-05
14	DVC 6000 ESD Validation	00GY01-PTR-03	Rev. A
15	Type DVC6000 Series Product Final test Specification	FGS 12D90	Rev. C
16	Provisions for Control of Engineering Documents by Independent Testing Laboratories	ES102	Rev. S
17	Engineering Change Request Procedure	ES192	Rev. V
18	Impact Analysis Report Template	APPRV_7	Rev. B
19	Analysis of DVC6000 for Compliance to IEC 61508	00GY01	Rev. B

3.2 Test object

The DVC6000 system consists of an electronic subsystem which controls the I/P-converter. The I/P-converter uses an electrical coil and a nozzle to convert the electrical signal coming from the electronic circuit in an appropriate pressure signal.

This pressure signal is used by the pneumatic relay to control the valve.

The electronic subsystem (current input 0 - 20 mA or voltage input 0 - 24 VDC; HART interface) is able to control the valve position and to perform diagnostic tests.

The safety function of the digital valve controller is a deenergize to trip functionality. Therefore the safe state of the single-acting DVC6000 is gained by depressurizing the valve actuator. The safe state of the double-acting DVC6000 is gained by depressurizing the spring opposed side of the valve actuator piston and pressurizing the spring assisted side of the piston, or at a minimum, applying equal pressure on both sides of the actuator piston. The final valve can be open or closed when the DVC6000 is deenergized depending on the actuator spring orientation of the final valve.

Independent from the status of the electronic subsystem of the DVC6000, the safe state is guaranteed if power is removed from the I/P-converter. And as a matter of fact that the electronic subsystem is powered by the control signal itself, the loss of this signal means that power is definitely removed from the I/P-converter. There is no alternative power source connected to the DVC6000 system.

Therefore the electronic subsystem was not part of the type approval. (Except the evaluation that there is no other power source than the control signal itself.)

A detailed description of the system is part of the user manual.

4. Tests and test results

4.1 General approach

The type approval of the DVC6000 system was performed on basis of a review of documents provided by the manufacturer and his consultant exida.com.

The standards, which were used as a base of the testing, are listed in chapter 2.

As key generic standards the IEC 61508 and EN 61010-1 have been used.

4.2 Documentation

The examination of the documentation as listed in the project documentation list, took place as an inspection. The following points were inspected in detail:

- completeness
- consistency
- comprehensibility

Open points were described and the manufacturer carried out the related changes in the documents. The examination of the documentation was positively finished.

4.3 Life cycle and safety concept

The life cycle model from the IEC 61508 [N1] was used during the complete specification, design, development, production, verification and validation phases of the DVC6000 system. The verification and validation plan (V&V-Plan) of the project covers all life cycle phases starting with the specification up to the modification.

The project- and documentation management is also defined in this document.

The verification and validation plan fulfils the requirements according to IEC 61508.

The safety requirements of the DVC6000 system are derived from the fundamental standard [N1].

The efficiency of measures (to avoid and control failures) against the different causes of faults are also taken from this standard.

The requirements are addressed by the safety requirement specification. The SRS includes mainly the following points:

- Functional references
- Safety and technical requirements
- Environmental conditions
- Design requirements
- Conditions for operating and services

The detailed functionality of the DVC6000 system is documented in the instruction manual.

The inspection of the SRS and safety concept of the DVC6000 Series for ESD Solutions system was positively finished.

The safety requirement specification fulfils the requirements according to the IEC 61508.

4.4 Theoretical inspection of the hardware and mechanical part

All hardware components and mechanical part were checked to be consistent with the manufacturers documentation.

The hardware was subject to an FMEA performed by the manufacturer. The FMEA documentation and the report to the FMEA /4/ was inspected with a positive result.

The FMEA' s which were performed on all system components (I/P-converter, pneumatic relay) are identifying the critical components of the system.

The hardware fault tolerance of the DVC6000 is zero, the SFF for the single-acting DVC6000 is 96.6 % (Type A components) and the SFF for the double-acting DVC6000 is 96.9 % (Type A components).

The FMEA' s which were performed on all system components (I/P-converter, pneumatic relay) are identifying the critical components of the system.

4.5 Influence of software

The software is used to control, to perform system diagnostic and to set parameters of the valve controller. As described above, the software is not safety critical and was therefore not part of this approval.

4.6 Practical hardware test

The base of the performed hardware test was taken from the environmental test specification. Basis for the specification was the EN 61010-1 and the related specifications of the manufacturer. For the smart field device, the following environmental tests were performed by the manufacturer:

The environmental- and EMC tests were done with a positive result.

4.7 Function, integration test

Fisher performed functional testing together with environmental conditions. The related test documentation is listed in /2/, integration phase.

4.8 Compliance to IEC 61508

Part 1 of the IEC 61508 demands certain documentation requirements for the development of safety critical devices. As basis documents, the SRS (Safety Requirements Specification), the V&V Plan (Validation and Verification Plan) and a life-cycle orientated documentation plan were prepared.

For the specific requirements of part 2 (system architecture, safe failure fraction, diagnostic, measures against systematic faults and measures to avoid failures during design and development), the finally selected measures meet the requirements of SIL 3.

Regarding the control of failures, the following results were estimated:

1. Hardware fault tolerance is 0

2. Safe failure fraction of the pneumatic part is > 90 % (low complex component)

3. Safe failure fraction of the electronic part:

   No hardware/software fault could lead to a dangerous failure in case of a demand (Input current /voltage is zero)

From this point of view the DVC 6000 ESD system could be used up to and including SIL 3.

For the PFD calculation the final valve is dominant for the result.

The calculation procedure and the PFD contribution of the DVC6000 are provided in the safety manual.

The failure rate, safe failure fraction resp. diagnostic coverage of the final valve and the manual test time interval shall be used for the PFD calculation. Depending on this calculation and the required hardware fault tolerance of the application (some applications require explicit a hardware fault tolerance of 1) the max. SIL level is defined (see prEN50156 for an example).

If the PFD calculation does not reach SIL 3 and/or a hardware fault tolerance of 1 is required, a dual redundant configuration shall be used.

5. <u>Conditions of applications, safety manual</u>

The safety manual /13/ was reviewed during the type approval, it contains all required information and has to be considered in safety related applications.

All other information regarding installation, maintenance and operating instructions are described in the user manual and must be also considered.

6. Summary

The approval of the DVC 6000 ESD system was carried out as described in the individual sections.

The approval was finished with a positive result.

The conditions of applications for use of the system (see chapter 5) must be considered.

The approval result shows that the DVC 6000 ESD system is suitable for applications up to and including SIL 3 according to the IEC 61508.

Regarding to the control of failures (hardware fault tolerance, safe failure fraction resp. diagnostic coverage factor and PFD calculation) the safety manual from the manufacturer has to be considered. For explanation see also chapter 4.10. of this report.

Cologne, 2002-05-21
ASI/Kst. 968/wvp-nie

The inspector

Dipl.-Ing. W. Velten-Philipp