

Intelligent valve controller Neles™ NDX™ Safety manual

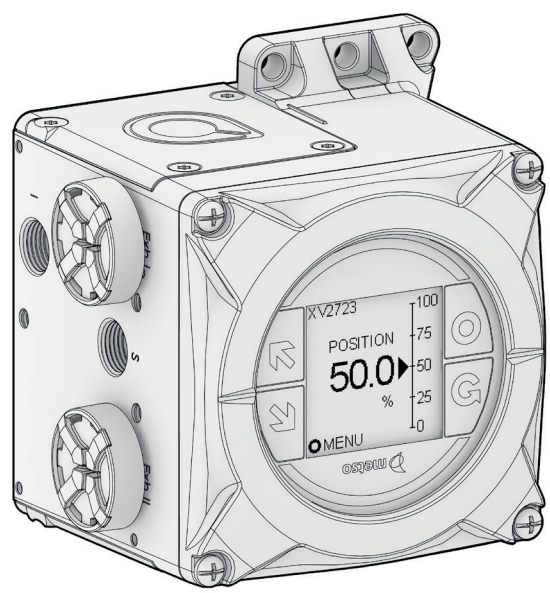
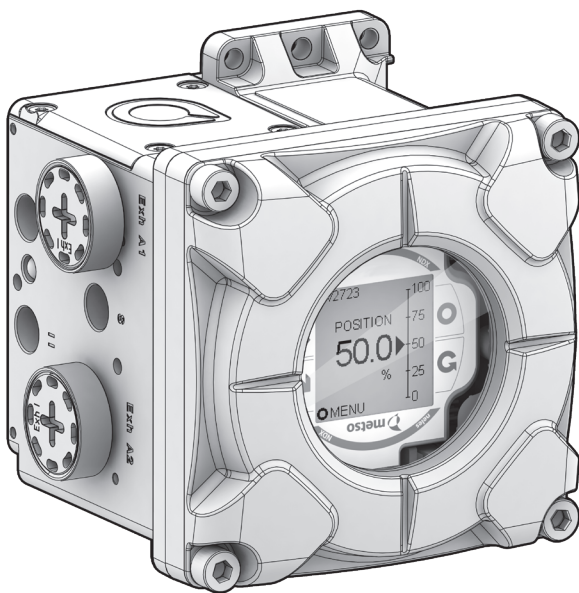


Table of Contents

1	General information	3
1.1	Purpose of the document.....	3
1.2	Description of the device.....	3
2	Structure of intelligent valve controller.....	3
2.1	System components and description of use.....	3
2.2	Permitted device types	3
2.3	Supplementary device documentation	3
3	Description of safety requirements	3
3.1	Safety function	3
3.2	Restrictions for use in safety-related applications	4
3.3	Functional safety indicators	4
3.4	Useful lifetime	5
3.5	Behavior of device	5
	3.5.1 During power-up.....	5
	3.5.2 During operation	5
	3.5.3 During emergency trip	5
	3.5.4 In the event of alarms and warnings.....	5
4	Installation	5
4.1	Hardware fault tolerance.....	5
4.2	Installation and commissioning.....	5
4.3	Diagnostics coverage	5
4.4	Parameters write protection	5
4.5	Operation	5
4.6	Maintenance	5
5	Testing	6
5.1	Partial stroke test (PST)	6
5.2	Valve proof-test.....	6
6	Repair and maintenance	6
7	SIL certificate.....	7

1. General information

1.1 Purpose of the document

This safety manual provides necessary information to design, install, verify and maintain safety instrumented function (SIF) using the Neles™ NDX™ Intelligent Valve Controller.

The document must be used as part of the safety lifecycle. Information provided in this manual is necessary for meeting the IEC 61508 or IEC 61511 functional safety standards.

1.2 Description of the device

Neles NDX is loop powered SIL 2 certified intelligent valve controller and thus a safety related product. Extra attention is required to make sure it is used in a way it is intended to be used and in a safe manner.

NOTE:

HART communication can be used for informational purposes, but is not safety certified for diagnostic annunciation.

2. Structure of intelligent valve controller

2.1 System components and description of use

See the IMO for the detailed technical description of the device and the system architecture.

2.2 Permitted device types

The information in this manual pertaining to functional safety applies to all NDX device variants mentioned in the device type coding in the IMO.

2.3 Supplementary device documentation

This manual is not intended to be used as a stand-alone document. It must be used together with the document 7NDX71en; Installation, Maintenance and Operating Instructions for Neles NDX (later referred as IMO).

It is available from your local Valmet office or for download from www.neles.com/NDX

3. Description of safety requirements

3.1 Safety function

Safety function part of NDX intelligent valve controller consists of the prestage and the output stage. They are the only components, which take part of the safety function. Prestage unit is a coil operated flapper valve, which is open when de-energized. De-energized is the safe state of the device prestage unit coil. Prestage unit is controlling the output stage, which is operated by spring force to fail safe position and by pneumatic force to the normal position. See figure 1 for the principle of operation. Prestage will be de-energized when input signal (loop current) to the device (NDX) is 0 mA. That will cause the output stage to release the air from the exhaust port ((Exh I or Exh A1 depending on the NDX type) and drive the emergency shutdown valve to close or open position depending on the application type.

Safety function is to release the air from Exh I port via the output stage exhaust. Reaction time of safety function is <200 milliseconds. The closing (or opening) time of the valve depends on the size and type of the pneumatic actuator and the valve, the supply pressure etc.

Micro controller and firmware are not part of or cannot prevent the safety action. Measurements from the pressure sensors (PS, PI) and position sensor (Pos) are used for controlling the Partial Stroke and other tests and used for the device diagnostics only.

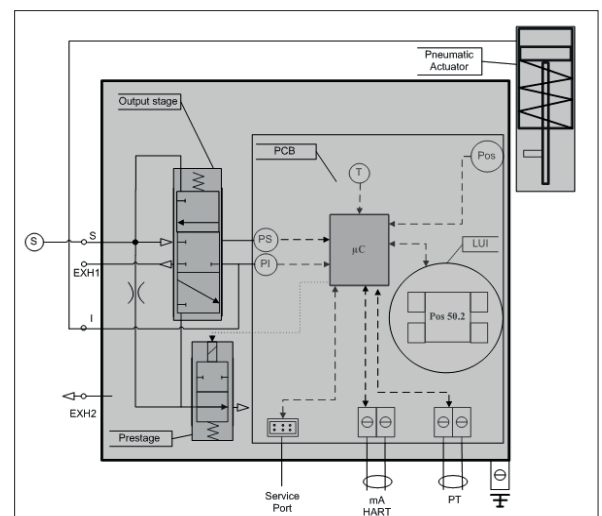


Fig. 1. Operating principle of NDX1510_

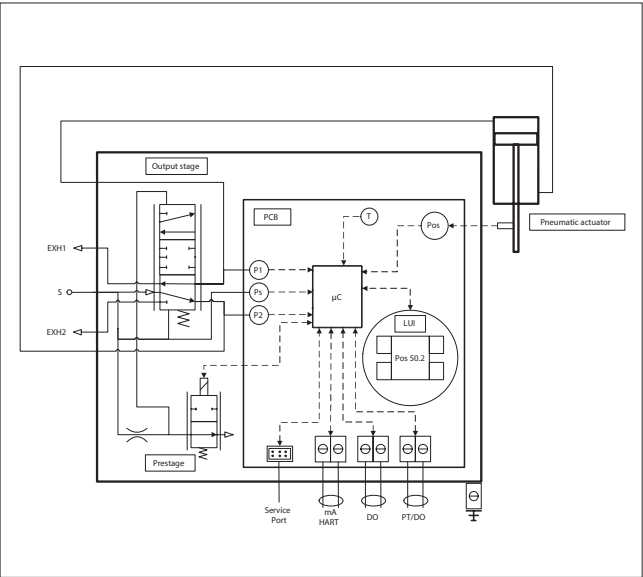


Fig. 2. Operating principle of NDX_512_

3.2 Restrictions for use in safety-related applications

Please ensure that the valve controller is used correctly for the application in question and that the ambient conditions and air supply quality are taken into account. The instructions for installation conditions, as detailed in the IMO, shall be observed. The specifications in the IMO shall not be exceeded.

3.3 Functional safety indicators

The table below shows the specific indicators for functional safety.

Route of Assessment		$2_H/1_s$	
Type of Sub-system		Type A	
Mode of Operation		Low Demand Mode	
Hardware Fault Tolerance	HFT	0	
Lambda Dangerous assumed level of calculation $1-\alpha = 95\%$	λ_D	3.50 E-07 / h	350 FIT
Lambda Dangerous Undetected assumed Diagnostic Coverage DC = 0%	λ_{DU}	3.50 E-07 / h	350 FIT
Mean Time To Dangerous Failure	MTTF _D	2.85 E+06 h	326 a
Average Probability of Failure on Demand 1001 assumed Proof Test Interval $T_1 = 1$ year	PFD _{avg} (T_1)	1.53 E-03	
Average Probability of Failure on Demand 1002 assumed Proof Test Interval $T_1 = 1$ year assumed $\beta_{1002} = 10\%$	PFD _{avg} (T_1)	1.56 E-04	

3.4 Useful lifetime

A useful lifetime of approximately 12 years is expected for NDX in safety related applications. After that period the failure rate start to increase.

3.5 Behavior of device

3.5.1 During power-up

It may take up to 30 seconds for device diagnostics to power up and the device to be fully operational in the diagnostics point of view. This is valid when the loop current is switched on and goes to 3.7 mA or above. This does not effect to the safety function of the device.

3.5.2 During operation

Once the device is powered, the device energizes the prestage and the supply air will be fed to the pneumatic actuator by output stage. That will eventually cause the valve to go to its normal operating position according to the input signal. .

3.5.3 During emergency trip

See section 3.1.

3.5.4 In the event of alarms and warnings

There are few failures (e.g. position sensor failure) which causes NDX to go to fail safe position. See the IMO for details.

4. Installation

4.1 Hardware fault tolerance

The required hardware fault tolerance of the installation is zero ($HFT = 0$). If hardware fault tolerance of one ($HFT = 1$) is required, then a dual redundant configuration of the valve installation shall be used. The overall safety integrity depends mainly on the actuator and the valve (ESD or ESV).

4.2 Installation and commissioning

The installation of the device needs to be done according to the IMO. Every parameter related to the device type in question and mentioned in the IMO needs to be checked and compared against the device settings. If any deviations exist the safety of the installation cannot be guaranteed.

The NDX shall be configured before commissioning. The parameters configured to the NDX shall be read back and verified before commissioning using the HART Device Description (DD) or Neles Valve Manager (DTM) for NDX.

4.3 Diagnostics coverage

To obtain the best possible diagnostic coverage, the various alarm limits in the NDX intelligent valve controller shall be set, see Section 13 in the IMO.

The diagnostic coverage factor for an ESD-valve (a fail to close valve) can be assumed to be around 75 % (valve + actuator), depending on the valve and actuator types. The diagnostic coverage factor for an ESV-valve (fail to open valve) can be assumed to be around 90 % (valve + actuator), depending on the valve and actuator types. For more accurate estimates contact Valmet.

4.4 Parameters write protection

The parameters programmed in the NDX shall be write protected. If the organizational procedures are established, this can be done using the user access levels in the configuration software.

4.5 Operation

See the IMO for the operation of the device.

4.6 Maintenance

See the IMO for maintenance instructions.

During maintenance work on the device, alternative safety function methods shall be taken to ensure process safety.

5. Testing

5.1 Partial stroke test (PST)

Device can perform valve partial stroke test, where the safety shutdown valve will be stroked certain amount from its normal operating position. Typically this stroke size is about 10-20% depending on the process. The stroke size shall be defined by the user and should be defined so that the upset for the process is kept as minimum.

For procedure and details see the IMO.

5.2 Valve proof-test

Safety shutdown valve proof-test is related to the required SIL level of the application. PFD calculations should define this safety shutdown valve proof test interval. To perform the proof-test check that the device is not in the fail-safe position, de-energize (0 mA) the input signal and check that the valve moves to the intended fail-safe position. See the valve safety manual for further info regarding the proof testing.

The whole safety loop shall be tested via the safety system / logic solver.

6. Repair and maintenance

Any repair and maintenance to the device shall be carried out only by the qualified person. Device failures must be reported to the manufacturer. The user shall provide a detailed report to the manufacturer describing the failure and any possible effects.

7. SIL certificate

Certificate





SIL/PL Capability

www.tuv.com
ID 0600000000

No.: 968/V 1006.02/23

Product tested	Intelligent Valve Controller	Certificate holder	Valmet Flow Control Oy Vanha Porvoontie 229 FI-01380 Vantaa Finland
Type designation	Single acting NDX 1510; 1511; 1512 Double acting NDX 2511; 2512		
Codes and standards	IEC 61508 Parts 1-2 and 4-7:2010		
Intended application	Safety Functions Single acting: De-energizing of the NDX valve controller shall drive the relay valve to safety position by pre-loaded spring and channel 1 vents pressure out to atmosphere so that the attached actuator can drive the valve to its safe state. Double acting: De-energizing of the NDX valve controller shall drive the relay valve to safety position by pre-loaded spring and one channel vents pressure out to atmosphere while the second channel will be pressurized so that the attached actuator can drive the valve to its safe state. The valve controllers are suitable for use in a safety instrumented system up to SIL 2 (low demand mode). Under consideration of the minimum required hardware fault tolerance HFT = 1 for the complete final element the valve controllers may be used up to SIL 3.		
Specific requirements	The instructions of the associated Installation, Operating and Safety Manual shall be considered.		

Summary of test results see back side of this certificate.

The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT FSP1 V3.0:2020 in its actual version, whose results are documented in Report No. 968/V 1006.02/23 dated 2023-11-09. This certificate is valid only for products, which are identical with the product tested. Issued by the certification body accredited by DAkKS according to DIN EN ISO/IEC 17065. The accreditation is only valid for the scope listed in the annex to the accreditation certificate D-ZE-11052-02-01.

TÜV Rheinland Industrie Service GmbH

Bereich Automation

Funktionale Sicherheit

Am Grauen Stein, 51105 Köln

Köln, 2023-12-21

Certification Body Safety & Security for Automation & Grid



Dipl.-Ing. (FH) Wolf Rückwart

www.fs-products.com
www.tuv.com



Deutsche
Akkreditierungsstelle
D-ZE-11052-02-01



TÜVRheinland®
Precisely Right.

10/222 12. 12 E A4 © TÜV, TÜEV and TÜV are registered trademarks. Utilisation and application requires prior approval.

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

10SM NDX EN - 2/2025

7

Valmet Flow Control Oy

Vanha Porvoontie 229, 01380 Vantaa, Finland.

Tel. +358 10 417 5000.

www.valmet.com/flowcontrol

Subject to change without prior notice.

Neles, Neles Easyflow, Jamesbury, Stonel, Valvcon and Flowrox, and certain other trademarks, are either registered trademarks or trademarks of Valmet Oyj or its subsidiaries in the United States and/or in other countries.

