

Intelligent valve controller Neles™ ND9000™, ND7000™ Safety manual

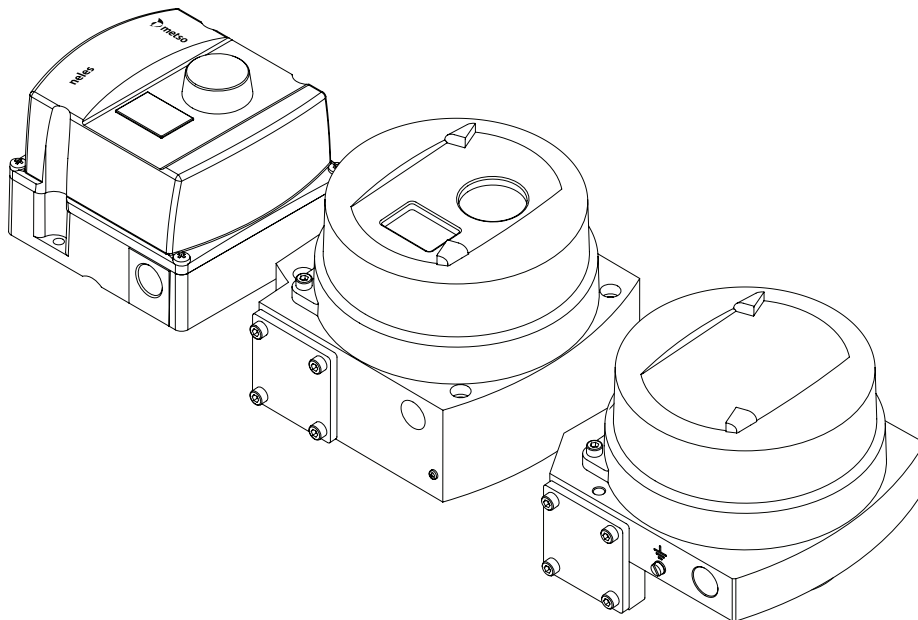


Table of Contents

1	General information	3
2	Structure of safety 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
3.1.1	Position transmitter	3
3.2	Restrictions for use in safety-related applications	3
3.3	Checking the safety function of ND9000	3
3.4	Functional safety indicators	4
3.5	Behavior of device	4
3.5.1	During power-up	4
3.5.2	During operation	5
3.5.3	During emergency trip	5
3.6	Installation	5
3.6.1	Hardware fault tolerance	5
3.6.2	Installation and commissioning	5
3.6.3	Parameters write protection	5
3.7	Maintenance	5
4	Proof-tests	5
4.1	Repair	5
5	Lifetime expectation	5

1. General information

Neles™ ND9000™ 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. ND9000 and ND7000 Installation, Maintenance and Operating Instructions 7 ND90 70 en (later referred as IMO) shall be used together with this safety manual when installing and operating this product.

2. Structure of safety 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 ND9000 and ND7000 device variants mentioned in the device type coding in the IMO.

This document is valid with devices which serial number starts from PH 13____. Serial number can be found from device machine plate. The first two numbers are showing manufacturing year and next two numbers are showing manufacturing week on that year. Example: PH1301____ = year 2013, week 1

2.3 Supplementary device documentation

1. ND7000 and ND9000 Installation, Maintenance and Operating Instructions
2. DTM User Manual 2; any DTM User Guide (later referred as DTM manual)

These are available from Valmet or for download from www.neles.com/nd9000/

3. Description of safety requirements

3.1 Safety function

Spool valve and prestage unit 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 spool valve, which is operated by spring force to fail safe position and by pneumatic force to the normal position. Fail safe is activated when device is de-energized. That will cause the emergency shutdown valve to close or open depending on the application type. The closing (or opening) time depends e.g. on the size and type of the pneumatics actuator and the valve.

3.1.1 Position transmitter

In the position transmitter part of the Neles ND9000 the feedback sensor, located in the extension housing, measures the valve position and the transmitter electronics convert the position into a 4-20 mA signal. This signal is used by the safety control system. Safety function of the position transmitter is sensing the position of the valve or actuator and translating it into a 4-20 mA value. If the position transmitter produces feedback out of range (<3 mA or >21 mA), that is considered dangerous detected failure, and the safety system must perform the safety action.

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 Checking the safety function of ND9000

To check that device is performing safety action:

- The device must not be in the safety position
- De-energize input signal
- Check that valve moves to the intended safety position

3.4 Functional safety indicators

The tables below show the specific indicators for functional safety

Results of Assessment		
Route of Assessment		$2_H/1_S$
Type of Sub-system		Type A
Mode of Operation		Low Demand Mode
Hardware Fault Tolerance	HFT	0
Systematic Capability		SC 3

De-energizing of the intelligent valve controller shall drive valve to safe position			
Dangerous Undetected Failure Rate	λ_{DU}	1.21 E-07 / h	121 FIT
Safe Failure Rate	λ_S	1.12E-07/h	112 FIT
Average Probability of Failure on Demand 1001	$PFD_{avg}(T_1)$	5.30 E-04	
Average Probability of Failure on Demand 1002	$PFD_{avg}(T_1)$	5.33 E-05	

Assumptions for the calculations above: $T_1 = 1$ year, $DC = 0$

Sensing of the position of valves or actuators ($ND_{-}/T01$) and sending the position using a 4 to 20 mA signal			
Dangerous Failure Rate (Current deviates more than 5 % from the "real" value (valve position))	λ_D	1.07 E-07 I h	107 FIT
Safe Failure Rate (Current deviates less than 5 % from the "real" value (valve position))	λ_S	2.84 E-08 I h	28 FIT
Dangerous Detected Failure Rate (Current is < 3 mA or > 21 mA)	λ_{DD}	7.03 E-08 I h	70 FIT
Dangerous Undetected Failure Rate (Current deviates more than 5 % from the "real" value (valve position), but is still within 3 to 21 mA)	λ_{DU}	3.69 E-07 I h	369 FIT
Average Probability of Failure on Demand 1001	$PFD_{avg}(T_1)$	8.1 E-04	
Safe Failure Fraction	SFF	73%	

Assumptions for the calculations above: $T_1 = 5$ years, Low Demand Mode, Diagnostic Measures: In case the current is < 3 mA or > 21 mA the sensor has an internal failure and the process has to be controlled in a way to lower the risk

3.5 Behavior of device

3.5.1 During power-up

It may take up to 8 seconds for device diagnostics to power up and the device to be fully operational in the diagnostics point of view. This does not effect to the safety function of the device. In HART version device start to follow mA signal when signal is connected.

In Foundation Fieldbus and Profibus PA versions there are parameters which define valve behavior in case of:

- Loss of cyclic communication
- Recovery of cyclic communication
- Loss of power supply
- Power-up

Those parameters have to be set correctly before use. If support is needed, please contact to local Valmet office.

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 spool valve. That will eventually cause the valve to go to its normal operating position.

3.5.3 During emergency trip

See section 3.1.

3.6 Installation

3.6.1 Hardware fault tolerance

The required hardware fault tolerance of the installation is zero. If hardware fault tolerance of 1 is required, then a dual redundant configuration of the valve installation shall be used.

3.6.2 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 ND9000 shall be configured before commissioning. The parameters configured to the ND9000 shall be read back and verified before commissioning using the Device Description (DD) or Any DTM for ND9000.

Orientation

Orientation of the device is described in the IMO.

3.6.3 Parameters write protection

The parameters programmed in the ND9000 shall be write protected. If the organizational procedures are established, this can be done using the user access levels in the configuration software. See section

5.8. in the IMO

3.6 Operation

See the IMO for the operation of the device.

3.7 Maintenance

See the IMO for maintenance instructions.

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

4. Proof-tests

To perform proof-test, see chapter 3.3 Checking the safety function.

4.1 Repair

Any repair to the device shall be carried out by the manufacturer only. 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.

5. Lifetime expectation

The useful lifetime of the ND9000 in safety related applications is approximately 12 years. After this period failure rate of ND9000 will increase.

Certificate



SIL/PL
Capability

www.tuv.com
ID 0600000000

No.: 968/V 1048.02/22

Product tested	Intelligent Valve Controller	Certificate holder	Valmet Flow Control Oy Vanha Porvoontie 229 FI-01380 Vantaa Finland
Type designation	ND9_, ND7_, SD9_, SD7_ (Versions see current "Version Release List")		
Codes and standards	IEC 61508 Parts 1-2 and 4-7:2010		
Intended application	The safety functions are defined as: 1. De-energizing the valve controller drives the internal prestage and spool valve to safe position 2. 4 – 20 mA position transmitter signal indicating the valve position 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 Programs CERT FSP1 V1.0:2017, CERT FSP1 V1.0:2017 in their actual version, whose results are documented in Report No. 968/V 1048.02/22 dated 2022-10-19. 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

Köln, 2022-12-15

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. (FH) Wolf Rückwart

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

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



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.

For more information www.neles.com/trademarks

