Czech

TÜV SÜD Czech, s.r.o
office Ostrava
Teslova 2
702 00 Ostrava-Přívoz

INSPECTION REPORT

issued pursuant to ČSN EN ISO/IEC 17020

File number 07.943.736

Purpose of inspection: **Evaluation of functional safety documentation**

Client:	**Dinel, s. r. o., U Tescomy 249, 760 01 Zlín**
Order No of date:	**OBJ1400067 from 06. 02. 2014**
Order TÜV SÜD Czech s.r.o.:	**5401401088**

Evaluated equipment

Name:		**E/E/EP system associated with safety of capacity level sensor**
Type designation:		**CSL-23**
Modification:		CLS-23N, CLS-23S
Working environment (according to ČSN EN 60079-10-1):		area without danger of explosion
Supply voltage:		6 - 30 V DC
Current consumption:	output P	max. 0,6 / 7mA (open / closed)
	output S	max. 0.6 (open)
Switching current	output P	max. 100 mA
	output S	3.3 / 40 mA (min. / max.)
Lost volts in closed state:		
	output P	max. 1.8 V
	output S	max. 6 V
Input resistance / electrical strength (electrode - casing):		1 MΩ / 250 VAC
Separating capacity / electric strength (power inputs - casing):		44 nF / 250 V AC
Delay of output signal with regard to activation of electrode:		0.1 s
Cover:		IP 68 (0.1MPa)
Type of connecting cable (basic length 2m):		
CLS-23N(NT) – output P		PVC 3x0.34 mm^2
CLS-23N(NT) – output S		PVC 2x0.34 mm^2
CLS-23S		PVC 2x0.75 mm^2

Characteristics of equipment:	capacity level sensor of the type CLS-23 serving for two-state indication of the level of various substances in tanks or containers; works on the principle of detection of electrode capacity. The electrode of the capacity level sensor is an electrically conductive item of various shapes the capacity of which related to the zero potential is measured by the sensor. This principle makes it possible to use insulated electrodes and thus eliminate the influence of the conductivity of the measured substance. The capacity level sensor CLS-23 is intended for industrial use for the limit detection of the level of various electrically conductive and non-conductive liquids (water, water solutions, coolant) in reservoirs, pipes, tanks etc.
Manufacturer:	Dinel, s. r. o., U Tescomy 249, 760 01 Zlín

The following standards and regulations were used as the specification for the conformity assessment:

Expert procedure TÜV SÜD Czech s.r.o. No E 540 – 081 Functional safety assessment,
ČSN EN 61508-1 ed.2:2011 - Functional safety of electrical/electronic/programmable electronic systems associated with safety - Part 1: General requirements,
ČSN EN 61508-2 ed. 2:2011 - Functional safety of electrical/electronic/programmable electronic systems associated with safety - Part 2: Requirements for electrical/electronic/programmable electronic systems associated with safety,
ČSN EN 61508-3 ed.2:2011 – Functional safety of electrical/electronic/programmable electronic systems associated with safety - Part 3: Software requirements
ČSN EN 61508-6 ed.2:2011 – Functional safety of electrical/electronic/programmable electronic systems associated with safety - Part 6: Methodological instructions for use of IEC 61508-2 and IEC 61508-3.

and this submitted documentation:

Functional safety of sensor CLS-23

- Management of functional safety [1]
- Annex2-Training and checks on manufacturing procedures [1.1]
- Phase 1 – Concept [2]
- Phase 2 – Definition of product [3]
- Phase 3 – Danger and risk analysis [4]
- Annex 1-FMEA_OF PROCESS [4.1]
- Phase 4 – Overall safety requirements [5]
- Phase 5 – Assigning overall safety requirements [6]
- Phase 6 – Planning of overall operation and maintenance [7]
- Phase 8 – Planning of overall installation and operational launch [8]
- Phase 9 – Specification of requirements for safety system [9]
- Phase 13 – Confirmation of validity of overall safety [10]
- Phase 14 – Overall operation, maintenance and repairs [11]
- Phase 16 – Retirement from operation or liquidation [12]
- Accompanying technical documentation - capacity level sensors CLS–23 [13]
  - Variants of sensors and design version [13.1]
  - Basic technical data [13.2]
  - Material used [13.3]
  - Resistance to temperature and pressure [13.4]
  - Process connection [13.5]
  - Mechanical version and classification of space [13.6]

- Electrical connection [13.7]
- Assembly and recommendations [13.8]
- Sensor setting [13.9]
- Signaling of states [13.10]
- Areas of use [13.11]
- Means of marking [13.12]
- Example of correct marking [13.13]
- Accessories [13.14]
- Protection, safety and compatibility [13.15]

- Functional diagram of electrical wiring of sensor CLS from 05.03.2012 [14]
- CLS-23 - block diagram [15]
- Certificate ČSN EN ISO 9001:2009 No CQS 2256/2012 [16]

Performed acts:

a) acquaintance with documentation,
b) validation of prepared documentation "Determination of safety integrity level SIL",
c) performance of selected simulations of fault states and their evaluation.

Inspection, measuring, and test equipment used

not used.

Marking used

Variants of output circuit:

CLS-23_ _-_ _-_-S-	output in version of two-wire current switch
CLS-23_ _-_ _-_-P-	output with PNP transistor with open collector
CLS-23Xi_-_ _-_-R-	NAMUR type output

Power supply of sensor:

CLS-23_ _-_ _-_-S-	from 6 to 30 V DC source (SELV type)
CLS-23Xi_-_ _-_-R-	from spark-safe source NAMUR 8 to 9 VDC with galvanic separation such as NSSU, NDSU, NLCU

Power supply for sensor via cable routed to actual electronics via:

CLS-23_ _-_ _-A-_-	short plastic cable grommet
CLS-23_ _-_ _-C-_-	connector M12x1 (Hirschmann)
CLS-23S-11-D-S	submersible version with long plastic cable bushing

Variants of Hirschmann type connector:
ELWIKA 4012 K PG7, ELKA 4012 K PG7, ELWIKA-KV 4312 (EWF 123) with cable 2m or 5m.

Modification of sensor electrodes:

CLS-23_ _-10-	uninsulated cylindrical electrode, length 30mm
CLS-23_ _-11-	cylindrical electrode with insulation (HDPE), length 30 mm
CLS-23_ _-12-	cylindrical electrode with insulation (FEP), length 30 mm
CLS-23_ _-20-	rod electrode with partial insulation 50 to 1000 mm
CLS-23_ _-21-	rod electrode with full insulation (FEP), length 50 to 1000 mm
CLS-23_ _-30-	uninsulated rod electrode capable of dismantling, length 50 to 1000 mm
CLS-23S-11-D-S	cylindrical electrode with insulation (HDPE), length 30 mm and protective basket

Variants of process connection of sensor:

CLS-23_ _ -_ _-_-_ -G3/8	tube thread G3/8
CLS-23_ _ -_ _-_-_ -G1/2	tube thread G1/2
CLS-23_ _ -_ _-_-_ -M18	metric thread M18x1.5
CLS-23_ _ -_ _-_-_ -M20	metric thread M20x1.5
CLS-23_ _ -_ _-_-_ -NPT	pressure thread 1/2-14 NPT

Marking of variants for high temperatures:

CLS-23NT-_-_-_-	variant for space without danger of explosion (except for type CLS-23_-11-_-_-)
CLS-23XiT-_-_-_-	high-temperature variant for dangerous spaces (except for type CLS-23_-11-_-_-)
CLS-23E-_-A-S	increased temperature resilience for spaces without danger of explosion

Sensor mode:

O -	the sensor closes during flooding
C -	the sensor opens during flooding

Basic functions of sensor

Operation mode A	protection against overfilling - the sensor detects flooding with a medium (detection of maximum level in such a way that the sensor switches from the closed state to the open state)
Operation mode B	protection against empty operation - the sensor detects absence of medium (detection of minimal level in such a way that the sensor switches from the closed state to the open state)

Determination of type of subsystem and mode of operation

Determination of type of subsystem – all subsystems/components of the evaluated equipment can be considered **type A** – for components used for attainment of the aforementioned safety function:

a) the fault modes of all the individual elements which make up this component are well defined;
b) it is possible to fully designate the behavior of the subsystem under fault conditions (fault states); and
c) sufficiently reliable data is available about faults gained from operation and showing that the required intensity of faults for ascertained and non-ascertained dangerous states are met.

Designation of mode of operation – mode of operation with high (large) or permanent demand, where the frequency of demand for operation of the system associated with the safety is greater than once a year or greater than twice the frequency of check (periodic) tests.

Description of software:

The software is part of the supplied single-chip control microprocessor as baked in firmware. Intensity of faults as common parameter for software and hardware designated by statistical calculation in operation of employed level sensors.

Specification of requirements

The purpose of the evaluation is a validation of meeting of requirements of the designated safety integrity level of systems associated with the safety of operation of capacity level sensors.

1. Description of system

The CLS-23 sensor is a compact device consisting of a plastic sleeve, head and sensing electrode. It is intended for screwing into the wall or lid of the vessel in which the actual detection of level occurs. The sensing electrode is adapted to the type of use and type of measured medium. The sensor sleeve contains measuring electronics controlled by a single-chip microprocessor.

The U1 microprocessor generates short positive pulses on pins 9 and 10 which charge the measured (on the electrode) and compensation capacity [8]. After this short positive pulse, the pins switch to high impedance (and they are set as comparator inputs) and the capacities start to discharge through resistance (measured to the ground via R16, compensation via R10 to voltage on C7). At the end of this discharge cycle the voltage on both capacities are compared by the comparator (part of microprocessor). The voltage on C7 is generated using PWM (pin 5), and its level depends on the configuration and state of the output. The results of the comparison are then averaged and influence the closing or opening of the output transistor. The output circuit consists of a switch transistor and overcurrent protector. Its state is shown by an LED. The sensor's supply voltage is stabilised. The sensor has a Zener diode to protect against voltage spikes and a diode to protect against polarity reversal of the supply conductors. It is set using a magnetic pen applied to a U3 Hall probe.

The level sensor has protection against faulty voltage on the electrode, pole reversal, short-term overvoltage and current overload at the output.

2. Basic data of HW for designating the safety integrity level

2.1 List of possible causes of fault states [4]

1	Ingress of liquids or gases to sensor	7	Software errors
2	Breaking of contact between electrical and mechanical part of the sensor	8	Faults caused by overvoltage
3	Faults of electronic components	9	Faults caused by physical and chemical properties of medium
4	Incorrectly prepared sealing material	10	Faults caused by soldering errors and faults of integrated circuit
5	Connection faults	11	Faults caused by incorrect installation
6	Poorly fitted components	12	Faults caused by fatigue of integrated circuit

2.2 Number of individual faults documented by monitoring of sensors employed in operation

According to paragraph 4 of document [4] -Evaluation of incidence and detection of fault, on basis of number in operation of employed sensors, time of employment and incidence of individual faults by calculation using χ^2 designation of lower estimate of median time to failure T_{SD}, then intensity of individual faults λ_D and value of probability of fault-free state $R_S(t)$.

Type CLS-23N sensors

Number of cause of fault	T_{AKU} *[h]*	*r*	*2v*	$\chi^2_{2v,C}$	T_{SD} *[h]*	λ_D $[h^{-1}]$	$R_S(t)$	Classification of incidence O
1	*4,003,320*	*1*	*4*	*4.878*	*1,641,377.6*	$6.09*10^{-7}$	*0.9841*	*7*
2	*4,003,320*	*1*	*4*	*4.878*	*1,641,377.6*	$6.09*10^{-7}$	*0.9841*	*7*
9	*4,003,320*	*0*	*2*	*2.407*	*3,326,398*	$3.01*10^{-7}$	*0.9921*	*6*
11	*4,003,320*	*1*	*4*	*4.878*	*1,641,377.6*	$6.09*10^{-7}$	*0.9841*	*7*

r…number of faults in test, v…number of degrees of freedom, C=0.7…confidence level

Type CLS-23S sensors

Number of cause of fault	T_{AKU} [h]	r	2v	$\chi^2_{2v,C}$	T_{SD} [h]	λ_D [h^{-1}]	$R_S(t)$	Classification of incidence O
1	1,781,200	14	30	33.53	106,245.1	$9.41*10^{-6}$	0.781	10
2	1,781,200	1	4	4.878	730,299.3	$1.37*10^{-6}$	0.9646	8
9	1,781,200	5	12	14.01	254,275.5	$3.93*10^{-6}$	0.902	9

r....number of faults in test, v...number of degrees of freedom, C=0.7...confidence level

Properties of dangerous faults designated by calculation of risk property number RPN [4.1]. Performance of measures to reduce incidence of specified faults (ALARP). Results given in tables - see below. Procedure of process given in document [4].

Type CLS-23N sensors

No	Potential causes / mechanisms of fault	Recommended measures	Performed measures
1	Ingress of liquids or gases to sensor	making sleeve watertight	adjustment to sleeve and electrode holder: there is no risk of insulation being pulled off, greater resistance to ingress, better possibility of fixing electrode using nut
2	Breaking of electrical contact between electrical and mechanical part of the sensor	alteration of contact pin	new pin with spring
9	Faults caused by physical and chemical properties of medium	a) reduction in sensitivity during setting b) change of insulation material	a) reduction in sensitivity of sensor – flooded state is configured for a case where the electrode of the sensor is more than half flooded. b) change of insulation material (from PE to PP)
11	Faults caused by incorrect installation	change of installation technology	change of sleeve and electrode holder: there is no risk of insulation being pulled off, better possibility of fixing electrode using nut and so there is no danger of the electrode coming loose

Number of cause of fault	T_{AKU} [h]	r	2v	$\chi^2_{2v,C}$	T_{SD} [h]	λ_D [h^{-1}]	$R_S(t)$	Classification of incidence O
1,2,9.11	4,958,160	0	2	2.407	4,119,784	$2.43*10^{-7}$	0.9936	6

Type CLS-23S sensors

No	Potential causes / mechanisms of fault	Recommended measures	Performed measures
1	Ingress of liquids or gases to sensor	change of sealing of seal	a) tighter thread of seal b) added groove on edge of seal to increase area of connection - seal - sleeve
2	Breaking of electrical contact between electrical and mechanical part of the sensor	alteration of contact pin	new pin with spring
9	Faults caused by physical and chemical properties of medium	a) reduction in sensitivity during setting b) change of insulation material	a) reduction in sensitivity of sensor – flooded state is configured for a case where the electrode of the sensor is more than half flooded. b) change of insulation material (from PE to PP)

Number of cause of fault	T_{AKU} [h]	r	2v	$\chi^2_{2v,C}$	T_{SD} [h]	λ_D [h^{-1}]	$R_S(t)$	Classification of incidence O
1	2,052,760	1	4	4.878	841,640	$1.19*10^{-6}$	0.9692	8
2	2,052,760	0	2	2.407	1,705,658.5	$5.86*10^{-7}$	0.9847	7
9	2,052,760	0	2	2.407	1,705,658.5	$5.86*10^{-7}$	0.9847	7

2.3 Assignment of safety functions for elimination of faults
Assignment of safety functions given in document [5] specifically:

No	Causes of faults	Overall safety functions
1	Ingress of liquids or gases to sensor	Prevent the ingress of liquid or gases to sensor
2	Breaking of electrical contact between electrical and mechanical part of the sensor	Prevent breaking of electrical contact or discover insufficient contact in good time.
3	Faults of electronic components	Avoid faults of electronic components and discover any faults in good time.
4	Incorrectly prepared sealing material	Avoid incorrect procedure when preparing sealing material.
5	Connection faults	Discover insufficient electrical connection in good time.
6	Poorly fitted components	Avoid errors when fitting components and discover any faults in good time.
7	Software errors	Avoid software errors and discover any faults in good time.
8	Faults caused by overvoltage	Prevent incidence of overvoltage to internal electrical circuits of sensor.
9	Faults caused by physical and chemical properties of medium	Prevent faults caused by physical and chemical properties of medium.
10	Faults caused by soldering errors and faults of integrated circuit	Discover soldering errors and faults of integrated circuit in good time.
11	Faults caused by incorrect installation	Prevent faults of caused by incorrect installation and discover any faults in good time.
12	Faults caused by fatigue of integrated circuit	Adopt preventative measures to prevent faults caused by fatigue of integrated circuit

Target safety integrity requirements given in table of document [5].

2.4 Designation of required integrity level:
According to the risk analysis and evaluation of dangerous situations applying to E/E/PES of individual capacity sensor and their functions, the following requirements for the required safety integrity level of systems associated with the safety of the specified equipment were designated by a risk diagram - see document [6] - as follows:

2.4.1 Type CLS-23N sensors
Assignment of safety integrity level (SIL) to functions 1-12 for operation mode A - for the assessed function is sufficient to reduce the risk measure at level of safety integrity **SIL 1**.
No risk reduction measures are needed for the evaluated functions of the equipment in mode B.

2.4.2 Type CLS-23S sensors
The assignment of a safety integrity level (SIL) to functions 2 and 9 for the operation mode A – for evaluated functions measures are designated at the safety integrity level for risk reduction **SIL 2**.
For the evaluated functions of the equipment in operation mode B no measures need be designated for risk reduction.
Assignment of safety integrity level (SIL) to functions 1, 3-8 and 10-12 for the operation mode A - for the assessed function is sufficient to reduce the risk measure at level of safety integrity **SIL 1**.
For the evaluated functions of the equipment in operation mode B no measures need be designated for risk reduction.

2.5 Architecture of E/E/PE system associated with safety of safety functions in operation mode A and B [15] – 1oo1, DC=0 % - see paragraph II b), III b) and IV b) of document [10].

3. The following was ascertained during the inspection performed on the date 06.02.2014 to 30.03.2015

Evaluation of documentation of system safety integrity level associated with the safety of capacity level sensors performed according to ČSN EN 61508-1 ed.2, ČSN EN 61508-2 ed.2, ČSN EN 61508-3 ed.2 with application of ČSN EN 61508-4 ed.2 and ČSN EN 61508-6 ed.2 as system associated with safety integrity level according to individual systems SIL1 to SIL2.

3.1 Scope of performed evaluation

a) Evaluation of scope of submitted documentation

Evaluation performed according to the requirements of ČSN EN 61508-1 ed.2, ČSN EN 61508-2 ed.2, ČSN EN 61508-3 ed.2, with application of ČSN EN 61508-6 ed.2.

b) Evaluation of quality control system

For the organisation of quality control the company Dinel, s. r.o. uses a certified quality control system according to ČSN EN ISO 9001:2009 No CQS 2256/2012 valid up to 12.10.2015 – certificate issued by CQS-Sdružení pro certifikaci systémů jakosti, Pod Lisem 129, Prague 8-Troja [16].

Management of functional safety prepared [1] including annex 2 – training and inspections with manufacturing procedures [1.1].

c) Evaluation of safety management process

The subject of evaluation of the safety control process were documents called Concept [2], Definition of product [3], Overall safety requirements [5], and Overall assignment of safety requirements [6]. Structure of documentation of safety life cycle given by individual mutually linked documents [2] to [12]. For assignment of responsibilities for individual phases of life cycle see Management of functional safety [1].

d) Evaluation of general requirements for the system

General requirements for system designated by the document Definition of product [3].

Drawn up Analysis of risks of system associated with safety [4] - based on the frequency and time of employment of systems in operation there was a designation of fault intensity λ_D.

Based on a designation of risk parameters with results of RPN evaluated risk functions with use of method ALARP [4.1] dangerous events designated [5] using diagram of risk of individual functions associated with safety [6] designated required properties of functional safety, this being:

- for type CLS-23N functions1-12 in operation mode A SIL1, in operation mode B SIL not required,
- for type CLS-23S functions 2 and 9 in operation mode SIL2, for functions 1, 3-8, 10-12 operation mode A SIL1, in operation mode B SIL not required.

e) Design of system

Documentation of individual systems associated with safety drawn up - see document [8] and [13], with added separate functional diagrams [14].

f) Safety review

Performance of verification and validation in course of the lifecycle of system associated with safety of equipment given in connection with individual phases in the Planning of overall installation and putting into operation [8] and in planning of overall operation and maintenance [7].

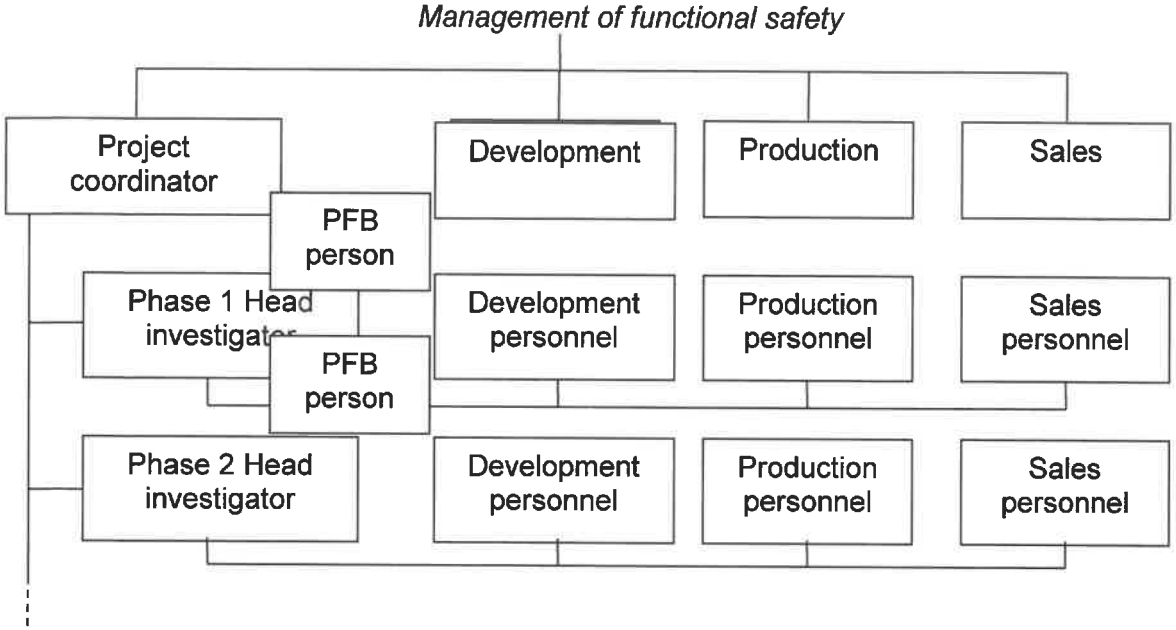
Requirements of overall safety for individual safety functions of system given in the document Requirements of overall safety [5] and Specification of requirements for safety of system [9].

For qualifications of the named workers see Management of functional safety [1], Training and inspections of production procedures [1.1] including designation of staffing of actual production –Planning of overall installation and operational launch [8].

By a verification in each phase of the lifecycle it was proven by an analysis and tests that the requirements of the relevant phase correspond with the output of the preceding phase and that the output of the relevant phase meets the requirements of this phase.
By validation - by test and analysis is was proven that from all aspects the product meets the designated requirements.

Specification of requirements of overall safety for individual safety functions of system

No	Causes of faults	Overall safety functions	Target requirements for safety integrity
1	Ingress of liquids or gases to sensor	Prevent the ingress of liquid or gases to sensor	Create a more reliable seal between the connections of the sensor parts.
2	Breaking of electrical contact between electrical and mechanical part of the sensor	Prevent breaking of electrical contact or discover insufficient contact in good time.	Ensure flexible and fault-free contact between electrical and mechanical part of the sensor. Functional inspection of side contact. Output functional inspection of sensor.
3	Faults of electronic components	Avoid faults of electronic components and discover any faults in good time.	Choose reliable components. Functional inspection of sensor.
4	Incorrectly prepared sealing material	Avoid incorrect procedure when preparing sealing material.	Check expiry date and adhere to correct procedure for preparation of sealing material.
5	Connection faults	Discover insufficient electrical connection in good time.	Functional inspection of sensor.
6	Poorly fitted components	Avoid errors when fitting components and discover any faults in good time.	Fault-free, clear documentation. Automatic fitting. Checking of fitting. Functional inspection of sensor.
7	Software errors	Avoid software errors and discover any faults in good time.	Inspection of program. Functional inspection of sensor.
8	Faults caused by overvoltage	Prevent incidence of overvoltage to internal electrical circuits of sensor.	Protective circuits on electrical input of the sensor protect from short-term overvoltage.
9	Faults caused by physical and chemical properties of medium	Prevent faults caused by physical and chemical properties of medium.	Adopt measures for problem of media sticking to electrode.
10	Faults caused by soldering errors and faults of integrated circuit	Discover soldering errors and faults of integrated circuit in good time.	Optical and functional inspection of sensor.
11	Faults caused by incorrect installation	Prevent faults of caused by incorrect installation and discover any faults in good time.	Adopt design measures to prevent faults caused by incorrect installation.
12	Faults caused by fatigue of integrated circuit	Adopt preventative measures to prevent faults caused by fatigue of integrated circuit	Adopt design and technological measures to prevent faults caused by fatigue of integrated circuit.



Description of staffing for individual activities and phases of lifecycle of system associated with safety given in document [1].

g) **Performance of validation tests** in form of tests and simulations of faults of system associated with the safety - fault of actual equipment of interruption of conductors' signals dangerous state and with this it puts the controlled equipment in a safe state - see paragraph 2 of chapter Procedure for performance of analysis FMEA of document Analysis of dangers and risks [4].

h) **Operation, maintenance, liquidation**
Documents furnished Overall operation, maintenance and repairs [11] and Retirement from operation or liquidation [12].

i) **Evaluation** – for proving sufficient safety of the evaluated system/subsystem/equipment - see document [10].

3.2 Evaluation of performed evaluation and tests

3. 2. 1 Evaluation of scope of submitted documentation

The submitted documentation contains a specification of the basic requirements for the system - documents [2], [3], [4], [4.1], [5];specification of requirements for quality control - documents [1] and [1.1]; specification of requirements for safety [2], [3], [4], [5], [6]; documents about functional and technical safety - documents [8] to [15]; documentation of definition of system and conditions for its use- documents [2], [3], [4]; documentation for project work, operation and maintenance - document [11]. In terms of scope and content of individual documents, the documentation meets the requirements of chapter 5 ČSN EN 61508-1 for the required safety integrity level.

3. 2. 2 Evaluation of quality control system

3.2.2.1 Quality assurance plan
By means of document 1] and [8] sufficient quality is ensured in the process of the lifecycle of the relevant systems.
Software (firmware) is an integral part of the logic of the purchased components (microprocessor U1 - PIC16F684), the fault intensity of which is concurrently designated with the system in document [4] and on the basis of specification MIL-HDBK-217F is confirmed in the document [10].

3.2.2.2 Quality control system
The quality control system is documented by document [16] and along with document [1] effectively ensures the quality control system in the process of the lifecycle of the system associated with safety capacities of type CLS-23 surface level sensors.

3.2.3 Evaluation of safety management processes

The process for managing the safety of systems associated with safety of equipment is described in documents [3], [4], [4.1], [5] and [6].
Confirmation of individual steps of suitable solution to safety given in paragraph 2 of this inspection report.

3.2.3.1 Safely lifecycle
The individual phases of the safety lifecycle of the system are described in consecutive documents [2] to [12] - complies.

3.2.3.2 Organisation of safety
The organisation of safety is prescribed by document [1] (see also paragraph 31 bullet f) of this report) and other prescribed roles given in documents [1], [1.1] and [8]. These documents prescribe the individual roles and also staffing. The individual roles and staffing were adhered to for the entire lifecycle of the project, i.e. from the Concept phase to the phase Operational launch.
The qualifications and competence of the workers involved in the solution for the project correspond to the requirements arising from the aforementioned standards and are confirmed by document [1.1].

3.2.3.3 Safety plan
Documents [4], [4.1], [5] and [6] - Safety plans were drawn up according to the requirements of ČSN EN 61508-1 ed.2 in compliance with the requirements of ČSN EN 61508-2 ed.2 and ČSN EN 61508-3 ed.2. In the individual documents, the requirements for the version of HW were designated in such a way that the safety integrity level met the requirements designated by the risk diagrams on the basis of the results of the risk analysis.

3.2.3.4 Specification of safety requirements
The content of the specification of safety requirements is a processing of an analysis of dangers and risks, for evaluation and classification of risks and assignment of safety integrity level of the system to equipment see documents [4], [4.1], [4] and [6].
The documents contain an Analysis of risks for the individual evaluated equipment and meet the requirements or article 7.4. ČSN EN 61508-1 ed.2.
By the evaluation of risks, compilation of Risk diagram [6], the required safety integrity levels were assigned to the designated safety functions as follows:
- for type CLS-23N functions1-12 in operation mode A SIL1,
- for type CLS-23S functions 2 and 9 in operation mode A SIL 2, for functions 1, 3-8, 10-12 operation mode A SIL 1.

3.2.4 Evaluation of requirements of system

The basic documents of the requirements for the system associated with safety of equipment is document [5] – Overall safety requirements. The requirements are also processed in the document [6] – Assignment of overall safety requirements, [9] – Specification of requirements of safety system. The anticipated activity, fault rate, implementation of requirements for individual elements applied in the architecture of the system associate with safety [15].
The defined requirements are designated in sufficient scope and unambiguously defined.
The completeness of the specification was verified by the validator.

3.2.5 Evaluation - validation of system

Validation of systems associated with the safety of individual items of equipment was performed according to the individual stages of the lifecycle.
For each phase of the safety lifecycle - see [4] to [12] divided into basic activities with designated subject of safety function - the inputs of the subsequent phase follow on from the outputs of the preceding phase of evaluation.

The documentation is processed at a level corresponding to the given phase and article 7 of ČSN EN 61508-1 ed.2. and article 7 of ČSN EN 61508-2 ed.2.

3.2.6 Review-justification of safety

3.2.6.1 Meeting requirements for functionality of operation.
The attainment of the required safety integrity level when designing the system associated with the safety of the evaluated equipment is ensured by adherence to the requirements of standards ČSN EN 61508-1 ed.2, ČSN EN 61508-2 ed.2, ČSN EN 61508-3 ed.2 and furnishing evidence of safety given in paragraph 3.1 g) of this inspection report and furnishing positive results of PFH given in document [10] – Confirmation of validity of overall safety.

3.2.6.2 Consequences of fault states
For each relevant safety function a qualitative analysis of fault states and their consequences has been drawn up. During the processing of the analysis the influence of the individual components on the performance of the individual concrete functions is respected.
The intensity of dangerous faults for each concrete function is enumerated on the basis of an analysis of faults in operation of the employed functional surface sensors.
The determination of parameters of fault states and their consequences is given in documentation [4] and [4.1].
By means of a calculation [10] the values of the safety integrity level of system were designated at minimum as they were designated by the risk diagrams [6].

3.2.6.3 Conditions of use applying to safety
The condition are described for the evaluated system associated with safety of equipment in documents [3], [4] and [11].
In order to meet the requirements applying to safety it is necessary to adhere to:
- the conditions of the working environment given in document [2] and [13],
- the fundamentals of installation must be adhered to, including connection - Planning of overall installation and operational launch [8] and conditions of accompanying technical documentation [13],
- operating and maintenance instructions given in document Overall operation, maintenance and repairs [11],
- instructions for retirement from operation given in document Retirement from operation or liquidation [12].

3.2.6.4 Tests evaluating safety
Scope of tests confirming validity of designated safety integrity of system associated with safety of evaluated equipment given in paragraph 3.1 g) of this inspection report, including furnishing of positive PFH results given in document [10] – Confirmation of validity of overall safety.

3.3 Evaluation

By an evaluation of the content and scope of the submitted documentation (see paragraph "Submitted documentation) and on the basis of performed tests, including simulation of fault states, we submit the following:

3.3.1 In terms of scope and content the submitted documentation corresponds to requirements of ČSN EN 61508-1 ed.2 (ČSN EN 61508-2 ed.2 and ČSN EN 61508-3 ed.2).

3.3.2 The individual steps, methods and procedures during the assertion of requirements of the stages of the lifecycle of the system associated with the safety of individual items of equipment were performed in compliance with the requirements of ČSN EN 61508-1 ed.2 and ČSN EN 61508-2 ed.2 for determination of the safety integrity level:

CLS-23N type sensor – safety functions 1-12 for operation mode A – **SIL 1**.

CLS-23N type sensor – safety functions 2 and 9 for operation mode A – **SIL 2,**
– safety functions 1, 3÷8 a 10÷12 for operation mode A – **SIL 1**.

For the evaluated functions of both items of equipment in operation mode B no requirements are designated for determination of safety integrity.

3.3.3 The safety functions implemented by the system associated with the safety of individual items of equipment of the system associated with the system associated with safety of surface level sensors CLS-23 are described by statistical and calculated values - paragraph 2.2 of this

inspection report, which correspond at least to the required safety integrity level. Confirmation of validity complemented by independent evaluation and tests – paragraph 3.1 g) of this inspection report, including furnishing of positive PFH results given in document [10] – Confirmation of validity of overall safety.

On the basis of the performed inspection, we submit the following inspection

conclusion:

the system associated with the safety of type CLS-23 capacity level sensors meets the requirement of the safety integrity level according to the range of standards ČSN EN 61508 ed.2. this being:
type CLS-23N sensors – safety functions 1-12 for operation mode A – SIL 1,
type CLS-23S sensors – safety functions 2 and 9 for operation mode A – SIL 2,
– safety functions 1, 3÷8 and 10÷12 for operation mode A – SIL 1.

The above inspection conclusion applies under these conditions:

During installation of the system, its operation and maintenance, the conditions given in paragraph No 3.2.6.3 of this inspection report will be met.

The inspection results submitted in this inspection report apply only to the evaluated equipment. Without the consent of TÜV SÜD Czech s.r.o. and the client, the Inspection Report cannot be reproduced other than in full.

No inspection certificate will be issued on the basis of this inspection report.

Ostrava, date 31.03.2015

inspector TÜV SÜD Czech s.r.o.: **Ing. Josef Struška**

head of office TÜV SÜD Czech s.r.o.: **Ing. Roman Prášek, Ph.D.**

The aforementioned submitted documentation constitutes an integral part of this inspection report.

This language version of the inspection report is a translation of the Czech official version dated 31 March 2015, which is considered the only correct one in the event of a dispute.