Czech

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

INSPEKČNÍ ZPRÁVA

vydaná dle ČSN EN ISO/IEC 17020

evidenční číslo 07.943.736

Účel inspekce: **Posouzení dokumentace funkční bezpečnosti**

Zákazník:	**Dinel, s. r. o., U Tescomy 249, 760 01 Zlín**
Objednávka č. ze dne:	**OBJ1400067 z 06. 02. 2014**
Zakázka TÜV SÜD Czech s.r.o.:	**5401401088**

Posuzované zařízení

Název:	**E/E/EP systém, související s bezpečností kapacitního hladinového snímače**
Typové označení:	**CLS-23**
Modifikace:	CLS-23N (CLS-23Xi), CLS-23S
Pracovní prostředí (dle ČSN EN 60079-10-1):	prostor bez nebezpečí výbuchu
Napájecí napětí:	6 - 30 V DC
Proudový odběr: výstup P	max. 0,6 / 7mA (rozepnuto / sepnuto)
výstup S	max. 0,6 (rozepnuto)
Spínaný proud: výstup P	max. 100 mA
výstup S	3,3 / 40 mA (min. / max.)
Úbytek napětí v sepnutém stavu:	
výstup P	max. 1,8 V
výstup S	max. 6 V
Vstupní odpor / elektrická pevnost (elektroda - pouzdro):	1 MΩ / 250 VAC
Oddělovací kapacita / elektrická pevnost (napájecí přívody - pouzdro):	44 nF / 250 V AC
Zpoždění výstupního signálu vzhledem k aktivaci elektrody:	0,1 s
Krytí:	IP 68 (0,1MPa)
Typ připojovacího kabelu (základní délka 2m):	
CLS-23N(NT) – výstup P	PVC 3x0,34 mm^2
CLS-23N(NT) – výstup S	PVC 2x0,34 mm^2
CLS-23S	PVC 2x0,75 mm^2

Charakteristika zařízení:	kapacitní hladinový snímač typu CLS-23 sloužící k dvoustavové indikaci hladiny různých látek v nádržích nebo zásobnících; pracuje na principu snímání kapacity elektrody. Elektroda kapacitního hladinového snímače je elektricky vodivý předmět různého tvaru, jehož kapacita vztažená k nulovému potenciálu je snímačem měřena. Tento princip umožňuje použít izolované elektrody a eliminovat tak vliv vodivosti měřené látky. Kapacitní hladinový snímač CLS-23 je určen pro průmyslové použití k limitní detekci hladiny různých elektricky vodivých i nevodivých kapalin (voda, vodní roztoky, olej, chladicí kapaliny) v jímkách, trubkách, nádržích apod.
Výrobce:	Dinel, s. r. o., U Tescomy 249, 760 01 Zlín

Jako specifikací pro posouzení shody byly použity následující normy a předpisy:

Odborný postup (Expert procedure) TÜV SÜD Czech s.r.o. č. E 540 – 081 Posouzení funkční bezpečnosti,
ČSN EN 61508-1 ed.2:2011 - Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností - Část 1: Všeobecné požadavky,
ČSN EN 61508-2 ed. 2:2011 - Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností - Část 2: Požadavky na elektrické /elektronické/programovatelné elektronické systémy související s bezpečností,
ČSN EN 61508-3 ed.2:2011 – Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností - Část 3: Požadavky na software
ČSN EN 61508-6 ed.2:2011 – Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností -Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3.

a tato předložená dokumentace:

Funkční bezpečnost snímače CLS-23

- Management funkční bezpečnosti [1]
- Příloha2-Proškolení a prověrky z výrobních postupů [1.1]
- Fáze 1 – Koncept [2]
- Fáze 2 – Definice výrobku [3]
- Fáze 3 – Analýzy nebezpečí a rizik [4]
- Příloha1-FMEA_PROCESU [4.1]
- Fáze 4 – Požadavky celkové bezpečnosti [5]
- Fáze 5 – Přiřazení požadavků celkové bezpečnosti [6]
- Fáze 6 – Plánování celkového provozu a údržby [7]
- Fáze 8 – Plánování celkové instalace a uvedení do provozu [8]
- Faze 9 – Specifikace požadavků bezpečnosti systému [9]
- Fáze13 – Potvrzení platnosti celkové bezpečnosti [10]
- Fáze 14 – Celkový provoz, údržba a opravy [11]
- Fáze16 – Vyřazení z provozu nebo likvidace [12]
- Průvodní technická dokumentace - kapacitní hladinové snímače CLS–23 [13]
  - Varianty snímačů a konstrukčního provedení [13.1]
  - Základní technické údaje [13.2]

- Materiálové provedení [13.3]
- Teplotní a tlaková odolnost [13.4]
- Procesní připojení [13.5]
- Mechanické provedení a klasifikace prostor [13.6]
- Elektrické připojení [13.7]
- Montáž a doporučení [13.8]
- Nastavení snímače [13.9]
- Signalizace stavů [13.10]
- Oblast použití [13.11]
- Způsob značení [13.12]
- Příklady správného označení [13.13]
- Příslušenství [13.14]
- Ochrana, bezpečnost a kompatibilita [13.15]

- Funkční schéma el. zapojení snímače CLS z 05.03.2012 [14]
- CLS-23 - blokový diagram [15]
- Certifikát ČSN EN ISO 9001:2009 č.CQS 2256/2012 [16]

Provedené úkony:

a) seznámení se s dokumentací,
b) validace zpracované dokumentace „Stanovení úrovně integrity bezpečnosti SIL",
c) provedení vybraných simulací poruchových stavů a jejich vyhodnocení.

Použité kontrolní, měřící a zkušební zařízení

nepoužity.

Použité značení

Varianty výstupního obvodu:

CLS-23_ _-_ _-_-S-	výstup v provedení dvoudrátový proudový spínač
CLS-23_ _-_ _-_-P-	výstup s tranzistorem PNP s otevřeným kolektorem
CLS-23Xi_-_ _-_-R-	výstup typu NAMUR

Napájení snímače:

CLS-23_ _-_ _-_-S-	ze zdroje stejnosměrného napětí 6 až 30 V DC (typu SELV)
CLS-23Xi_-_ _-_-R-	z jiskrově bezpečného zdroje NAMUR 8 až 9 VDC s galvanickým oddělením např. NSSU, NDSU, NLCU

Napájení snímače prostřednictvím kabelu, který je přiveden k vlastní elektronice přes:

CLS-23_ _-_ _-A-_-	krátkou plastovou kabelovou průchodku
CLS-23_ _-_ _-C-_-	konektor M12x1 (Hirschmann)
CLS-23S-11-D-S	ponorné provedení s dlouhou plastovou kabelovou vývodku

Varianty typů konektorů Hirschmann:
ELWIKA 4012 K PG7, ELKA 4012 K PG7, ELWIKA-KV 4312 (EWF 123) s kabelem 2m nebo 5m.

Modifikace elektrod snímačů:

CLS-23_ _-10-	válcová elektroda neizolovaná, délka 30mm
CLS-23_ _-11-	válcová elektroda s izolací (HDPE), délka 30 mm
CLS-23_ _-12-	válcová elektroda s izolací (FEP), délka 30 mm
CLS-23_ _-20-	prutová elektroda s částečnou izolací, délka 50 až 1000 mm

CLS-23_ _-21-	prutová elektroda s úplnou izolací (FEP), délka 50 až 1000 mm
CLS-23_ _-30-	prutová neizolovaná demontovatelná elektroda, délka 50 až 1000 mm
CLS-23S-11-D-S	válcová elektroda s izolací (HDPE), délka 30 mm a ochranným košíčkem

Varianty procesního připojení snímače:

CLS-23_ _ -_ _-_-_ -G3/8	trubkový závit G3/8
CLS-23_ _ -_ _-_-_ -G1/2	trubkový závit G1/2
CLS-23_ _ -_ _-_-_ -M18	metrický závit M18x1,5
CLS-23_ _ -_ _-_-_ -M20	metrický závit M20x1,5
CLS-23_ _ -_ _-_-_ -NPT	tlakový závit 1/2-14 NPT

Označení modifikací variant pro vysoké teploty:

CLS-23NT-_-_-_-	varianta do prostor bez nebezpečí výbuchu (mimo typ CLS-23_-11-_-_-_)
CLS-23XiT-_-_-_-	vysokoteplotní varianta do nebezpečných prostor (mimo typ CLS-23_-11-_-_-)
CLS-23E-_-A-S	zvýšená teplotní odolnost do prostor bez nebezpečí výbuchu

Režim snímače:

O -	snímač při zaplavení sepne
C -	snímač při zaplavení rozepne

Základní funkce snímače

Režim provozu A	ochrana proti přeplnění – snímač detekuje zaplavení médiem (detekce maximální hladiny tak, že ze sepnutého stavu se snímač přepne do rozepnutého)
Režim provozu B	ochrana proti chodu na prázdno – snímač detekuje nepřítomnost média (detekce minimální hladiny tak, že ze sepnutého stavu se snímač přepne do rozepnutého)

Stanovení typu subsystému a režimu provozu

Stanovení typu subsystému – veškeré subsystémy/součásti posuzovaného zařízení lze považovat za **typ A** – u součástí použitých pro dosažení výše uvedené bezpečnostní funkce:

a) jsou dobře definovány poruchové režimy všech jednotlivých složek, které tuto součást tvoří;
b) lze plně určit chování subsystému v podmínkách vad (poruchových stavů); a
c) jsou k dispozici dostatečně spolehlivé údaje o poruchách získané z provozu a ukazující, že jsou splněny požadované intenzity poruch pro zjištěné a nezjištěné nebezpečné poruchy.

Stanovení režimu provozu – režim provozu s vysokým (velkým) nebo trvalým vyžádáním, kde četnost vyžádání provozu systému souvisejícího s bezpečností je větší než jednou ročně nebo je větší než dvojnásobek četnosti kontrolních (periodických) zkoušek.

Popis software:

Software je součástí dodaného řídicího jednočipového mikroprocesoru jako pevně instalovaný firmware. Intenzita poruch, jako společný parametr pro software a hardware stanovena statistickým výpočtem v provozu nasazených hladinových snímačů.

Specifikace požadavků

Účelem posouzení je validace splnění požadavků stanovené úrovně integrity bezpečnosti systémů souvisejících s bezpečností provozu kapacitních hladinových snímačů.

1. Popis systému

Snímač CLS-23 je kompaktní zařízení složené z plastového pouzdra, z hlavice a ze snímací elektrody. Je určen k zašroubování do stěny nebo víka nádoby, ve které probíhá vlastní detekce hladiny. Snímací elektroda je uzpůsobena druhu použití a typu měřeného média. V pouzdru snímače je umístěna měřicí elektronika, která je řízena pomocí jednočipového mikroprocesoru.

Mikroprocesor U1 generuje na pinech 9 a 10 krátké kladné pulsy, jimiž nabíjí měřenou (na elektrodě) a kompenzační kapacitu [8]. Po tomto krátkém kladném pulsu se piny přepnou do vysoké impedance (a nastaví se jako vstupy komparátoru) a kapacity se začnou přes odpory vybíjet (měřená do země přes R16, kompenzační přes R10 do napětí na C7). Na konci tohoto vybíjecího cyklu jsou napětí na obou kapacitách komparátorem (součástí mikroprocesoru) porovnány. Napětí na C7 je generováno pomocí PWM (pin 5) a jeho velikost je odvislá od nastavení a stavu výstupu. Výsledky porovnávání jsou poté průměrovány a ovlivňují sepnutí, nebo rozepnutí výstupního tranzistoru. Výstupní obvod je tvořen spínacím tranzistorem a nadproudovou ochranou. Jeho stav je indikován pomocí LED. Napájecí napětí snímače je stabilizováno. Snímač je opatřen ochrannou Zenerovou diodou proti napěťovým špičkám a diodou proti přepólovaní napájecích přívodů. Nastavování se provádí pomocí magnetického pera přikládáním k Hallově sondě U3.

Hladinový snímač je vybaven ochranou proti poruchovému napětí na elektrodě, přepólování, krátkodobému přepětí a proudovému přetížení na výstupu.

2. Základní údaje HW pro stanovení úrovně integrity bezpečnosti

2.1 Výčet možných příčin poruchových stavů [4]

1	Vniknutí kapalin nebo plynů do snímače	7	Chyby v softwaru
2	Přerušení el. kontaktu mezi elektrickou a mechanickou částí snímače	8	Poruchy způsobené přepětím
3	Poruchy elektronických součástek	9	Poruchy způsobené fyzik. a chem. vlastnostmi média
4	Nevhodně připravená zalévací hmota	10	Poruchy způsobené chybami pájení a vadami pl. spoje
5	Poruchy připojení	11	Poruchy způsobené nesprávnou montáží
6	Špatně osazené součástky	12	Poruchy způsobené namáháním pl. spoje

2.2 Počet jednotlivých poruch, doložených sledováním snímačů nasazených do provozu.

Podle odst. 4 dokumentu [4] -Hodnocení výskytu a detekce příčiny poruchy, na základě počtu v provozu nasazených snímačů, doby nasazení a výskytu jednotlivých poruch výpočtem pomocí χ^2 stanoven dolní odhad střední doby do poruchy T_{SD}, pak intenzita jednotlivých poruch λ_D a hodnota pravděpodobnosti bezporuchového stavu $R_S(t)$.

Snímače typu CLS-23N (CLS-23Xi)

Číslo příčiny poruchy	T_{AKU} [h]	r	2v	$\chi^2_{2v,C}$	T_{SD} [h]	λ_D [h^{-1}]	$R_S(t)$	Klasifikace výskytu 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....počet poruch při zkoušce, v...počet stupňů volnost, C=0,7...konfidencí úroveň

Snímače typu CLS-23S

Číslo příčiny poruchy	T_{AKU} [h]	r	2v	$\chi^2_{2v,C}$	T_{SD} [h]	λ_D [h^{-1}]	$R_S(t)$	Klasifikace výskytu 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….počet poruch při zkoušce, v…počet stupňů volnost, C=0,7…konfidencí úroveň

Výpočtem hodnoty rizikového čísla RPN [4.1] stanoveny vlastnosti nebezpečných poruch. Provedeno opatření pro snížení výskytu uvedených poruch (ALARP). Výsledky uvedeny v tabulkách – viz. níže. Postup procesu uveden v dokumentu [4].

Snímače typu CLS-23N (CLS-23Xi)

č.	Potenciální příčiny / mechanismy poruchy	Doporučená opatření	Uskutečněná opatření
1	Vniknutí kapalin nebo plynů do snímače	úprava těsnosti pouzdra	úprava pouzdra i držáku elektrody: nehrozí přestřižení izolace, větší odolnost na zatečení, lepší možnost upevnění elektrody pomocí matice
2	Přerušení el. kontaktu mezi elektrickou a mechanickou částí snímače	úprava kontaktního kolíčku	nový kolíček s pružinkou
9	Poruchy způsobené fyzik. a chem. vlastnostmi média	a) snížení citlivosti při nastavení b) změna materiálu izolace	a) snížení citlivosti snímače – zaplavený stav je nastavený pro případ, kdy je elektroda snímače více jak z poloviny zaplavená. b) změna materiálu izolace (z PE na PP)
11	Poruchy způsobené nesprávnou montáží	úprava technologie montáže	úprava pouzdra i držáku elektrody: nehrozí přestřižení izolace, lepší možnost upevnění elektrody pomocí matice a proto nehrozí uvolnění elektrody

Číslo příčiny poruchy	T_{AKU} [h]	r	2v	$\chi^2_{2v,C}$	T_{SD} [h]	λ_D [h^{-1}]	$R_S(t)$	Klasifikace výskytu O
1,2,9,11	4 958 160	0	2	2,407	4 119 784	$2,43*10^{-7}$	0,9936	6

Snímače typu CLS-23S

č.	Potenciální příčiny / mechanismy poruchy	Doporučená opatření	Uskutečněná opatření
1	Vniknutí kapalin nebo plynů do snímače	úprava těsnosti závěru	a) těsnější závit závěru b) přidaná drážka na obvodu závěr pro zvětšení plochy spojení závěr - pouzdro
2	Přerušení el. kontaktu mezi elektrickou a mechanickou částí snímače	úprava kontaktního kolíčku	nový kolíček s pružinkou
9	Poruchy způsobené fyzik. a chem. vlastnostmi média	a) snížení citlivosti při nastavení b) změna materiálu izolace	a) snížení citlivosti snímače – zaplavený stav je nastavený pro případ, kdy je elektroda snímače více jak z poloviny zaplavená. b) změna materiálu izolace (z PE na PP)

Číslo příčiny poruchy	T_{AKU} [h]	r	2v	$\chi^2_{2v,C}$	T_{SD} [h]	λ_D [h^{-1}]	$R_S(t)$	Klasifikace výskytu 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 Přiřazení bezpečnostních funkcí pro eliminaci poruch

Přiřazení bezpečnostních funkcí uvedeno v dokumentu [5] a to:

č.	Příčiny poruch	Funkce celkové bezpečnosti
1	Vniknutí kapalin nebo plynů do snímače	Zabránit vniknutí kapaliny nebo plynů do snímače
2	Přerušení elektrického kontaktu mezi elektrickou a mechanickou částí snímače	Zabránit přerušení elektrického kontaktu nebo nedostatečný kontakt včas odhalit.
3	Poruchy elektronických součástek	Předcházet poruchám elektronických součástek a případné poruchy včas odhalit.
4	Nevhodně připravená zalévací hmota	Vyvarovat se nesprávného postupu přípravy zalévací hmoty.
5	Poruchy připojení	Nedostatečné elektrické připojení včas odhalit.
6	Špatně osazené součástky	Zabránit chybám při osazování součástek a případné chyby včas odhalit.
7	Chyby v softwaru	Zabránit chybám softwaru a případné chyby včas odhalit.
8	Poruchy způsobené přepětím	Zabránit vniknutí přepětí do vnitřních elektrických obvodů snímače.
9	Poruchy způsobené fyzikálními a chemickými vlastnostmi média	Omezit poruchy způsobené fyzikálními a chemickými vlastnostmi média.
10	Poruchy způsobené chybami pájení a vadami plošného spoje	Chyby pájení a vady plošného spoje včas odhalit.
11	Poruchy způsobené nesprávnou montáží	Omezit poruchy způsobené nesprávnou montáží a případné poruchy včas odhalit.
12	Poruchy způsobené namáháním plošného spoje	Přijmout preventivní opatření k omezení poruch způsobených namáháním plošného spoje.

Cílové požadavky na integritu bezpečnosti uvedeny v tabulce dokumentu [5].

2.4 Stanovení požadované úrovně integrity bezpečnosti:

Podle rizikové analýzy a vyhodnocení nebezpečných situací, vztahujících se na E/E/PES jednotlivých kapacitních snímačů a jejich funkce, byly diagramem rizik stanoveny následující požadavky na požadovanou úroveň integrity bezpečnosti systémů souvisejících s bezpečností uvedených zařízení – viz dokument [6] takto:

2.4.1 Snímače typu CLS-23N (CLS-23Xi)

Přiřazení úrovně integrity bezpečnosti (SIL) funkcím 1-12 pro režim provozu A - pro posuzované funkce je dostačující pro snížení rizika opatření na úrovni integrity bezpečnosti **SIL 1.**

Pro posuzované funkce zařízení v režimu B nejsou nutná žádná opatření pro snížení rizika.

2.4.2 Snímače typu CLS-23S

Přiřazení úrovně integrity bezpečnosti (SIL) funkcím 2 a 9 pro režim provozu A - pro posuzované funkce je stanoveno pro snížení rizika opatření na úrovni integrity bezpečnosti **SIL 2.**

Pro posuzované funkce zařízení v režimu provozu B nejsou nutná žádná opatření pro snížení rizika.

Přiřazení úrovně integrity bezpečnosti (SIL) funkcím 1, 3-8 a 10-12 pro režim provozu A - pro posuzované funkce je dostačující pro snížení rizika opatření na úrovni integrity bezpečnosti **SIL 1.**

Pro posuzované funkce zařízení v režimu provozu B nejsou nutná žádná opatření pro snížení rizika.

2.5 Architektura E/E/PE systému souvisejícího s bezpečností bezpečnostních funkcí v režimu provozu A i B [15] – 1oo1, DC=0 % - viz. odst. II b), III b) a IV b) dokumentu [10].

3. Při inspekci provedené dne 06.02.2014 až 30.03.2015 bylo zjištěno

Posouzení dokumentace úrovně integrity bezpečnosti systému souvisejícího s bezpečností kapacitních hladinových snímačů provedeno podle ČSN EN 61508-1 ed.2, ČSN EN 61508-2 ed.2, ČSN EN 61508-3 ed.2 při využití ČSN EN 61508-4 ed.2 a ČSN EN 61508-6 ed.2 jako systému souvisejícího s bezpečností úrovně integrity bezpečnosti podle jednotlivých systémů SIL1 až SIL2.

3.1 Rozsah provedeného posouzení

a) Posouzení rozsahu předložené dokumentace

Posouzení provedeno podle požadavků ČSN EN 61508-1 ed.2, ČSN EN 61508-2 ed.2, ČSN EN 61508-3 ed.2, za využití ČSN EN 61508-6 ed.2.

b) Posouzení systému řízení jakosti

Pro organizaci řízení jakosti využívá společnost Dinel, s. r.o. certifikovaný systém řízení jakosti podle ČSN EN ISO 9001:2009 č.CQS 2256/2012 s dobou platnosti do 12.10.2015 – certifikát vydal CQS-Sdružení pro certifikaci systémů jakosti, Pod Lisem 129, Praha 8-Troja [16].
Vypracován Management funkční bezpečnosti [1] vč. přílohy 2-proškolení a prověrky s výrobních postupů [1.1].

c) Posouzení procesu řízení bezpečnosti

Předmětem posouzení procesu řízení bezpečnosti byly dokumenty pod názvem Koncept [2], Definice výrobku [3], Požadavky celkové bezpečnosti [5], a Přiřazení požadavků celkové bezpečnosti [6]. Struktura dokumentace životního cyklu bezpečnosti dána jednotlivými na sebe navazujícími dokumenty [2] až [12]. Přiřazení odpovědností za jednotlivé fáze životního cyklu viz. Management funkční bezpečnosti [1].

d) Posouzení všeobecných požadavků na systém

Všeobecné požadavky na systém stanoveny dokumentem Definice výrobku [3].
Zpracována Analýza rizik systému souvisejícího s bezpečností [4] - z četnosti a doby nasazení systémů v provozu stanovena intenzita poruch λ_D.
Na základě určení rizikových parametrů a výsledků RPN posuzovaných rizikových funkcí s využitím metody ALARP [4.1] stanoveny nebezpečné události [5] a pomocí diagramů rizik jednotlivých funkcí souvisejících s bezpečností [6] stanoveny požadované vlastnosti funkční bezpečnosti a to:

- pro typ CLS-23N (CLS-23Xi) funkcím 1-12 v režimu provozu A SIL1, v režimu provozu B SIL nepožadována,
- pro typ CLS-23S funkcím 2 a 9 v režimu provozu A SIL2, funkcím 1, 3-8, 10-12 režimu provozu A SIL1, v režimu provozu B SIL nepožadována.

e) Návrh systému

Zpracována dokumentace jednotlivých systémů souvisejících s bezpečností- viz. dokument [8] a [13], doplněno o samostatná funkční schémata [14].

f) Přezkoumání bezpečnosti

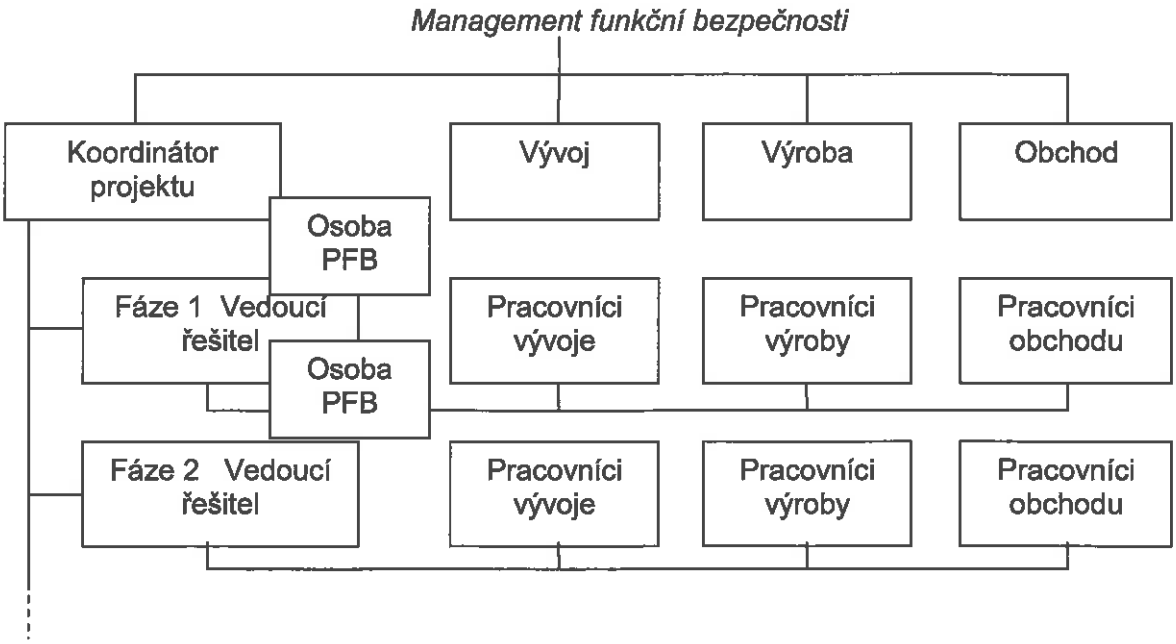
Provedení verifikací a validací v průběhu životního cyklu systému souvisejícího s bezpečností zařízení uvedeno v závislosti na jednotlivých etapách v Plánování celkové instalace a uvedení do provozu [8] a v Plánování celkového provozu a údržby [7].
Požadavky celkové bezpečnosti pro jednotlivé bezpečnostní funkce systému uvedeny v dokumentu Požadavky celkové bezpečnosti [5] a Specifikace požadavků bezpečnosti systému [9].

Kvalifikace jmenovaných pracovníků viz. Management funkční bezpečnosti [1], Proškolení a prověrky z výrobních postupů [1.1] vč. stanovení personálního obsazení vlastní výroby – Plánování celkové instalace a uvedení do provozu [8].

Verifikací v každé fázi životního cyklu bylo analýzou a zkouškami prokázáno, že požadavky příslušné fáze odpovídají výstupu předcházející fáze a že výstup příslušné fáze splňuje požadavky této fáze.
Validací - zkouškou a analýzou bylo prokázáno, že produkt splňuje ve všech ohledech stanovené požadavky.

Specifikace požadavků celkové bezpečnosti pro jednotlivé bezpečnostní funkce systému

č.	Příčiny poruch	Funkce celkové bezpečnosti	Cílové požadavky na integritu bezpečnosti
1	Vniknutí kapalin nebo plynů do snímače	Zabránit vniknutí kapaliny nebo plynů do snímače	Vytvořit spolehlivé těsnění mezi spoji dílů snímače.
2	Přerušení elektrického kontaktu mezi elektrickou a mechanickou částí snímače	Zabránit přerušení elektrického kontaktu nebo nedostatečný kontakt včas odhalit.	Zajistit pružný a bezporuchový kontakt mezi elektrickou a mechanickou částí snímače. Funkční kontrola bočního kontaktu. Výstupní funkční kontrola snímače.
3	Poruchy elektronických součástek	Předcházet poruchám elektronických součástek a případné poruchy včas odhalit.	Vybírat spolehlivé součástky. Funkční kontroly snímače.
4	Nevhodně připravená zalévací hmota	Vyvarovat se nesprávného postupu přípravy zalévací hmoty.	Kontrolovat expirační dobu a dodržovat správný postup přípravy zalévací hmoty.
5	Poruchy připojení	Nedostatečné elektrické připojení včas odhalit.	Funkční kontroly snímače.
6	Špatně osazené součástky	Zabránit chybám při osazování součástek a případné chyby včas odhalit.	Bezchybná a zřetelná dokumentace. Automatické osazování. Kontrola osazování. Funkční kontrola snímače.
7	Chyby v softwaru	Zabránit chybám softwaru a případné chyby včas odhalit.	Kontrola programu. Funkční kontroly snímače.
8	Poruchy způsobené přepětím	Zabránit vniknutí přepětí do vnitřních elektrických obvodů snímače.	Ochranné obvody na elektrickém vstupu snímače chrání před krátkodobým přepětím.
9	Poruchy způsobené fyzikálními a chemickými vlastnostmi média	Omezit poruchy způsobené fyzikálními a chemickými vlastnostmi média.	Přijmout opatření k problému s ulpíváním média na elektrodě.
10	Poruchy způsobené chybami pájení a vadami plošného spoje	Chyby pájení a vady plošného spoje včas odhalit.	Optické a funkční kontroly snímače.
11	Poruchy způsobené nesprávnou montáží	Omezit poruchy způsobené nesprávnou montáží a případné poruchy včas odhalit.	Přijmout konstrukční opatření, aby se omezili poruchy způsobené nesprávnou montáží.
12	Poruchy způsobené namáháním plošného spoje	Přijmout preventivní opatření k omezení poruch způsobených namáháním plošného spoje.	Přijmout konstrukční a technologické opatření, aby se omezili poruchy způsobené namáháním plošného spoje.



Popis obsazení pracovníků pro jednotlivé činnosti a fáze životního cyklu systému souvisejícího s bezpečností uveden v dokumentu [1].

g) **Provedení validačních zkoušek** formou funkčních zkoušek a simulací poruch systému souvisejícího s bezpečností – porucha vlastního zařízení nebo přerušení vodičů signalizuje nebezpečný stav a tím řízené zařízení uvede do bezpečného stavu - viz. odst.2 statě Postup provádění analýzy FMEA dokumentu Analýza nebezpečí a rizik [4].

h) **Provoz, údržba, likvidace**
Doloženo dokumenty Celkový provoz, údržba a opravy [11] a Vyřazení z provozu nebo likvidace [12].

i) **Vyhodnocení** – prokázání dostatečné bezpečnosti hodnoceného systému/subsystému/zařízení - viz dokument [10].

3.2 Vyhodnocení provedeného posouzení a zkoušek

3.2.1 Posouzení rozsahu předložené dokumentace

Předložená dokumentace obsahuje specifikaci základních požadavků na systém- dokumenty [2], [3], [4], [4.1], [5]; specifikaci požadavků na řízení jakosti - dokumenty [1] a [1.1]; specifikace požadavků na bezpečnost- dokumenty [2], [3], [4], [5], [6]; doklady o funkční a technické bezpečnosti - dokumenty [8] až [15]; dokumentaci definice systému a podmínek jeho použití - dokumenty [2], [3], [4]; dokumentaci pro projektování, obsluhu a údržbu - dokument [11].
Dokumentace svým rozsahem a obsahem jednotlivých dokumentů splňuje požadavky kap. 5 ČSN EN 61508-1 pro požadované úrovně integrity bezpečnosti.

3.2.2 Posouzení systému řízení jakosti

3.2.2.1 Plán zajištění jakosti

Dokumentem [1] a [8] stanoveno dostatečné zajištění jakosti v procesu životního cyklu předmětných systémů.
Software (firmware) je nedílnou součástí logiky nakupované komponenty (mikroprocesor U1 - PIC16F684), jehož intenzita poruch je současně se systémem stanovena v dokumentu [4] a na základě specifikací MIL-HDBK-217F potvrzena v dokumentu [10].

3.2.2.2 Systém řízení jakosti
Systém řízení jakosti doložen dokumentem [16] a spolu s dokumentem [1] účinně zajišťují systém řízení jakosti v procesu životního cyklu systému souvisejícího s bezpečností kapacitních hladinových snímačů typu CLS-23.

3.2.3 Posouzení procesu řízení bezpečnosti
Proces řízení bezpečnosti systému souvisejícího s bezpečností zařízení popsán v dokumentech [3], [4], [4.1], [5] a [6].
Potvrzení jednotlivých kroků vhodného řešení bezpečnosti uvedeno v odst. 2 této Inspekční zprávy.

3.2.3.1 Bezpečnostní životní cyklus
Jednotlivé fáze bezpečnostního životního cyklu systému jsou popsány v návazně po sobě jdoucích dokumentech [2] až [12] - vyhovuje.

3.2.3.2 Organizace bezpečnosti
Organizace bezpečnosti je předepsána dokumentem [1] (viz. také odst.31 odr.f) této zprávy) a dále předepsanými rolemi, uvedenými v dokumentech [1], [1.1] a [8]. Tyto dokumenty předepisují jednotlivé role a také personální obsazení. Jednotlivé role i personální obsazení bylo dodržováno po celou dobu životního cyklu projektu, tzn. od etapy Koncepce až do etapy Uvedení do provozu.
Kvalifikace a způsobilost pracovníků zainteresovaných na řešení projektu odpovídají požadavkům, které vyplývají z výše uvedených norem a jsou potvrzeny dokumentem [1.1].

3.2.3.3 Plán bezpečnosti
Dokumenty [4], [4.1], [5] a [6] - Plány bezpečnosti byly vypracovány podle požadavků ČSN EN 61508-1 ed.2 v souladu s požadavky ČSN EN 61508-2 ed.2 a ČSN EN 61508-3 ed.2.
V jednotlivých dokumentech stanoveny požadavky na provedení HW takové, aby úroveň integrity bezpečnosti splňovala požadavky, stanovené diagramy rizika na základě výsledků analýzy rizik.

3.2.3.4 Specifikace požadavků na bezpečnost
Obsahem specifikací požadavků na bezpečnost je zpracování analýzy nebezpečí a rizik, hodnocení a klasifikace rizik a přiřazení úrovní integrity bezpečnosti systému zařízení viz. dokumenty [4], [4.1], [4] a [6].
Dokumenty obsahují Analýzu rizik pro jednotlivá posuzovaná zařízení a naplňují požadavky čl.7.4. ČSN EN 61508-1 ed.2.
Vyhodnocením rizik, sestavením Diagramu rizika [6] byly pro stanovené bezpečnostní funkce přiřazeny požadované úrovně integrity bezpečnosti takto:
- pro typ CLS-23N funkcím 1-12 v režimu provozu A SIL 1,
- pro typ CLS-23S funkcím 2 a 9 v režimu provozu A SIL 2, funkcím 1, 3-8, 10-12 režimu provozu A SIL 1.

3.2.4 Posouzení požadavků na systém

Výchozími dokumenty požadavků na systém související s bezpečností zařízení je dokument [5] – Požadavky celkové bezpečnosti. Požadavky jsou dále zapracovány do dokumentů [6] – Přiřazení požadavků celkové bezpečnosti, [9] – Specifikace požadavků bezpečnosti systému.
Předpokládaná činnost, poruchovost, realizace požadavků na jednotlivé prvky uplatněny v architektuře systému souvisejícího s bezpečností [15].
Definované požadavky jsou stanoveny v dostatečném rozsahu a jednoznačně definovány.
Úplnost specifikace byla ověřena validátorem.

3.2.5 Posouzení - validace systému
Validace systémů souvisejících s bezpečností jednotlivých zařízení byla provedena dle jednotlivých etap životního cyklu.
Každá fáze životního cyklu bezpečnosti – viz. [4] až [12] rozdělena na základní činnosti se

stanoveným předmětem bezpečnostní funkce - vstupy následující fáze navazují na výstupy předchozí fáze posuzování.

Dokumentace je zpracována na úrovni, odpovídající dané etapě a čl.7 ČSN EN 61508-1 ed.2 a čl.7 ČSN EN 61508-2 ed.2.

3.2.6 Přezkoumání-zdůvodnění bezpečnosti

3.2.6.1 Splnění požadavků na funkčnost provozu.
Dosažení požadované úrovně integrity bezpečnosti při návrhu systému souvisejícího s bezpečností posuzovaného zařízení je zajištěno dodržením požadavků norem ČSN EN 61508-1 ed.2, ČSN EN 61508-2 ed.2, ČSN EN 61508-3 ed.2 a provedením důkazu bezpečnosti, uvedeného v odst.3.1 g) této Inspekční zprávy a doložením kladných výsledků PFH, uvedených v dokumentu [10] – Potvrzení platnosti celkové bezpečnosti.

3.2.6.2 Důsledky poruchových stavů
Pro každou relevantní bezpečnostní funkci je vypracována kvalitativní analýza poruchových stavů a jejich následků. Při vypracování analýzy je respektován vliv jednotlivých komponent provedení jednotlivých konkrétních funkcí.
Intenzita nebezpečných poruch pro každou konkrétní funkci je vyčíslena na základě analýzy poruchovosti v provozu nasazených funkčních hladinových snímačů.
Stanovení parametrů poruchových stavů a jejich následků uvedeno v dokumentaci [4] a [4.1].
Výpočtem [10] byly prokázány hodnoty úrovně integrity bezpečnosti systémů minimálně takové, jaké byly stanoveny diagramy rizik [6].

3.2.6.3 Podmínky použití vztahující se k bezpečnosti
Podmínky použití, vztahující se k bezpečnosti, jsou pro posuzovaný systém související s bezpečností zařízení popsané v dokumentech [3], [4] a [11].
Pro splnění požadavků vztahujících se k bezpečnosti nutno dodržet:
- podmínky pracovního prostředí uvedené dokumentu [2] a [13],
- musí být dodrženy zásady instalace vč připojení – Plánování celkové instalace a uvedení do provozu [8] a podmínky Průvodní technické dokumentace [13],
- pokyny pro provoz a údržbu uvedeny v dokumentu Celkový provoz, údržba a opravy [11],
- pokyny k vyřazení z provozu uvedeny v dokumentu Vyřazení z provozu nebo likvidace [12].

3.2.6.4 Zkoušky hodnotící bezpečnost
Rozsah zkoušek potvrzujících platnost stanovené integrity bezpečnosti systému souvisejícího s bezpečností posuzovaného zařízení uveden v odst. 3.1 g) této Inspekční zprávy vč. doložení kladných výsledků PFH, uvedených v dokumentu [10] – Potvrzení platnosti celkové bezpečnosti.

3.3 Vyhodnocení

Posouzením obsahu a rozsahu předložené dokumentace (viz. odst. „Předložená dokumentace) a na základě provedených zkoušek vč. simulací poruchových stavů podáváme následující:

3.3.1 Předložená dokumentace svým rozsahem a obsahem odpovídá požadavkům ČSN EN 61508-1 ed.2 (ČSN EN 61508-2 ed.2 a ČSN EN 61508-3 ed.2).

3.3.2 Jednotlivé kroky, metody a postupy při uplatňování požadavků etap životního cyklu systému souvisejícího s bezpečností jednotlivých zařízení byly provedeny v souladu s požadavky ČSN EN 61508-1 ed.2 a ČSN EN 61508-2 ed.2 pro stanovení úrovně integrity bezpečnosti:

Snímače typu (CLS-23Xi) – bezpečnostní funkce 1-12 pro režim provozu A – **SIL 1.**

Snímače typu CLS-23S – bezpečnostní funkce 2 a 9 pro režim provozu A – **SIL 2,**
– bezpečnostní funkce **1,** 3÷8 a 10÷12 pro režim provozu A – **SIL 1.**

Pro posuzované funkce obou zařízení v režimu provozu B nejsou stanoveny žádné požadavky na určení integrity bezpečnosti.

3.3.3 Bezpečnostní funkce realizované systémem souvisejícím s bezpečností jednotlivých zařízení systému souvisejícího s bezpečností hladinových snímačů typu CLS-23 jsou charakterizovány statickými a vypočítanými hodnotami – odst.2.2 této Inspekční zprávy, které odpovídají minimálně požadované úrovni integrity bezpečnosti. Potvrzení platnosti doplněno nezávislým hodnocením a zkouškami – odst. 3.1 g) této Inspekční zprávy vč. doložení kladných výsledků PFH, uvedených v dokumentu [10] – Potvrzení platnosti celkové bezpečnosti.

Na základě provedené inspekce podáváme následující inspekční

závěr:

systém související s bezpečností kapacitních hladinových snímačů typu CLS-23 splňuje požadavky stupně integrity bezpečnosti podle řady norem ČSN EN 61508 ed.2. a to:
snímače typu CLS-23N (CLS-23Xi) – bezpečnostní funkce 1-12 pro režim provozu A – SIL 1,
snímače typu CLS-23S – bezpečnostní funkce 2 a 9 pro režim provozu A – SIL 2,
– bezpečnostní funkce 1, 3÷8 a 10÷12 pro režim provozu A – SIL 1.

Výše uvedený inspekční závěr platí za těchto podmínek:

Při instalaci systému, jeho provozu a údržbě budou plněny podmínky uvedené v odstavci č.3.2.6.3 této Inspekční zprávy.

Výsledky inspekce podané v této inspekční zprávě se vztahují pouze k posuzovanému zařízení. Inspekční zprávu nelze bez souhlasu TÜV SÜD Czech s.r.o. a zákazníka reprodukovat jinak než vcelku.

Na základě této inspekční zprávy nebude vydán Inspekční certifikát.

v Ostravě, dne 2015-03-31

TÜV SÜD Czech s.r.o. TÜV SÜD

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

vedoucí kanceláře TÜV SÜD Czech s.r.o.: Ing. Roman Prášek, Ph.D.

Nedílnou součástí této inspekční zprávy je výše uvedená předložená dokumentace.