Funkční bezpečnost

Normy a řešení v praxi

Materiály ze 70. semináře Odborné skupiny pro spolehlivost,
konaného dne 13. 2. 2018 v Praze

Česká společnost pro jakost, Novotného lávka 5, 110 00 Praha 1, www. csq.cz

Obsah

Oborové aplikace funkční bezpečnosti a normy, které se k funkční bezpečnosti vztahují

doc. Ing. Pavel Fuchs, CSc.

Alopex, s.r.o.

e-mail: pavel.fuchs@volny.cz, pavel.fuchs@tul.cz

1 Úvod

Je nesporným faktem, že při funkční bezpečnost se kvantitativně hodnotí parametry, které jsou založeny na aplikované teorii spolehlivosti. Stanovení požadavků na funkční bezpečnost komponent či systémů je ve své podstatě stanovením požadavku na spolehlivost. Přičemž tento požadavek je formulován jako schopnost objektu odolávat nebezpečné poruše. Míra této schopnosti je kvantitativně předepisována jako číselná hodnota intenzity poruch či nepohotovosti. Sice se v příslušných normách vztahujících se k funkční bezpečnosti vyskytuje terminologie odlišná od normativní terminologie spolehlivosti, ale to nemění nic na tom, že jde o intenzitu poruch a ustálenou nepohotovost.

Specifikace požadavků na funkční bezpečnost vychází z toho, že bezpečnostní funkce má zabránit újmě (škodě). Podle velikosti a pravděpodobnosti újmy se formuluje požadavek na úroveň funkční bezpečnosti bezpečnostní funkce. Tento požadavek se alokuje na komponenty. Funkční bezpečnost je charakterizována jednak úrovněmi funkční bezpečnosti (SIL, ASIL, PL) a dále pak intervalem hodnot intenzity poruch a nepohotovosti pro příslušnou úroveň funkční bezpečnosti. Pro každou úroveň funkční bezpečnosti tedy specifikováno:

a) rozmezí hodnot intenzity poruch a nepohotovosti pro náhodné poruchy,
b) určité množství opatření pro omezení nenáhodných (systematických) poruch.

Se stoupající úrovní integrity bezpečnosti jsou požadavky na odolnost proti náhodným i systematickým poruchám náročnější.

Problematice funkční bezpečnosti, korektnosti stanovení požadavků na úroveň bezpečnosti, rozdílům v přístupu jednotlivých norem k funkční bezpečnosti byly věnovány příspěvky v 46. a 53. semináři Odborné skupiny pro spolehlivost [1], [2]. Z toho důvodu zde nejsou dříve publikované informace opakovaně publikovány.

Účelem tohoto příspěvku není detailní rozbor obsahu jednotlivých norem ani kritické posouzení správnosti příkladů určování hodnoty rizika a integrity bezpečnosti bezpečnostní funkce. Účelem příspěvku je zvýšit pochopení toho, že jde o jednu a téže problematiku přizpůsobenou specifickým požadavkům jednotlivých oborů.

2 Oborové aplikace funkční bezpečnosti

S rozvojem automatizace založené na systémech využívající elektrické, elektronické či programovatelné elektronické prvky (E/E/PE prvky), bylo třeba sjednotit přístup k jejich využití pro bezpečnostní účely. Bezpečnostní přístrojové systémy byly široce aplikovány v petrochemických, chemických, energetických a jiných průmyslových provozech. Široké spektrum výrobců, projektantů a uživatelů výrobků průmyslové automatizace by bez standardizace funkční bezpečnosti obtížně nalézalo shodu mezi požadavky a potřebami. Výsledkem dlouhodobého úsilí v této oblasti byla norma IEC 61508 složená z částí 1 až 7. Tato

norma je založena na systematickém řízení aktivit spojených s životním cyklem celkové bezpečnosti, bezpečnosti E/E/PE systémů a bezpečnosti softwaru při používání E/E/PE systémů pro plnění bezpečnostních funkcí

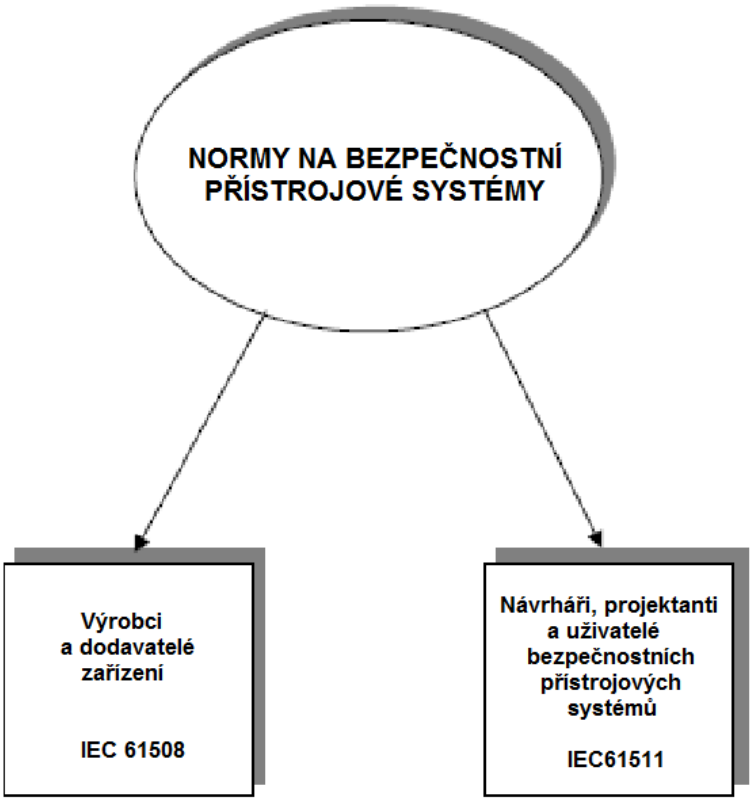
IEC 61508 je harmonizovaná norma, viz [3 až 9] a je uznávána za základní bezpečnostní normu platnou pro funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů souvisejících s bezpečností. Ostatní normy k funkční bezpečnosti jsou oborovými implementacemi této normy.

Jako oborové aplikace se v tomto příspěvku rozumí aplikace funkční bezpečnosti v určitém technickém odvětví. Popis oborových aplikací se zaměřuje na odvětví průmyslových procesů, strojních zařízení včetně robotů, drážních zařízení a automobilů.

2.1 Funkční bezpečnost průmyslových procesů

Pro funkční bezpečnost průmyslových procesů je určena norma IEC 61511 složená z částí 1, 2 a 3 a přejatá do soustavy harmonizovaných norem, viz [10, 11 a 12].

Vztah mezi IEC 61508 a IEC 61511 uvádí obr. 1. Je evidentní, že pro určení jakou úroveň SIL je třeba požadovat pro bezpečnostní funkci v průmyslovém procesu, je určena IEC 61511-3. Kdežto k tomu, jakým způsobem prokázat, že požadavky na úroveň SIL jsou splněny, slouží IEC 61508.



Obr. 1: Vztah mezi IEC 61511 a IEC 61508 [10]

Na uvedeném faktu nemění to, že v části IEC 61508-5 jsou uvedeny příklady metod určování úrovní integrity bezpečnosti. Tyto jsou základním vodítkem při aplikaci normy IEC 61508

v daném odvětví. Hodnotu přijatelného rizika je třeba stanovit při návrhu bezpečnostní funkce v rámci IEC 61511.

Norma IEC 61508 je nyní platná ve 2. vydání, kdežto u normy IEC 61511 je 2. vydání teprve připravováno a je k dispozici jako RLV (Red Line Version).

Speciálním případem využití přístupu IEC 61508 je pro jaderné elektrárny norma IEC 61513 [13]. Tato norma přijala formát prezentace podobný základní bezpečnostní normě IEC 61508 s životním cyklem celkové bezpečnosti a životním cyklem systému. Tato norma také poskytuje interpretaci obecných požadavků IEC 61508, část 1, 2 a 4 pro jadernou oblast. To zajišťuje konzistenci s požadavky IEC 61508 tak, jak byly interpretovány pro jaderný průmysl.

2.2 Funkční bezpečnost strojních zařízení

Bezpečnost strojních zařízení je pokryta normami, které mají tuto strukturu:

- **normy typu A** (základní bezpečnostní normy), uvádějí základní pojmy, zásady pro konstrukci a všeobecná hlediska, která mohou být aplikována na všechna strojní zařízení
- **normy typu B** (skupinové bezpečnostní normy), se zabývají jedním bezpečnostním hlediskem nebo jedním typem bezpečnostního zařízení, které může být použito pro větší počet strojních zařízení:
  - normy typu B1 se týkají jednotlivých bezpečnostních hledisek (např. bezpečných vzdáleností, teploty povrchu, hluku);
  - normy typu B2 se týkají příslušných bezpečnostních zařízení (např. dvouručních ovládacích zařízení, blokovacích zařízení, zařízení citlivých na tlak, ochranných krytů);
- **normy typu C** (bezpečnostní normy pro stroje), se zabývají detailními bezpečnostní požadavky pro jednotlivý stroj nebo skupinu strojů.

Elektrické, elektronické a programovatelné elektronické řídicí systémy souvisejících s bezpečností aplikované na strojním zařízení jsou pokryty IEC 62061 [14]. Je to oborová aplikace normy IEC 61508, která pracuje s úrovní integrity bezpečnosti SIL (Safety Integrity Level) a lze ji řadit do skupiny norem typu B1.

Pro bezpečnost strojních zařízení se aplikuje další norma se vztahem k funkční bezpečnosti. Jde o normu ISO 13849-1. Tato norma není odvozena od IEC 61508, stanovuje úroveň vlastností PL (Performance Level) a je řazena do skupiny norem typu B1.

Tyto normy nelze vzájemně kombinovat, konstruktér/projektant se musí předem rozhodnout, podle které normy bude postupovat. Při postupu podle ISO 13849-1 může PL aplikovat i na jiné než E/E/PE prvky (např. hydraulické, pneumatické nebo mechanické). Důležitý rozdíl mezi oběma normami je v charakteru působícího nebezpečí, jak již bylo uvedeno v [2].

Obě normy (IEC 62061 a ISO 13849-1) lze aplikovat pro zabezpečení jednouchých i složitých strojních zařízení. Jejich použití předepisuje např. norma pro roboty a robotická zařízení (norma typu C) ISO 10218-1 [16].

2.3 Funkční bezpečnost drážních zařízení

Funkční bezpečnost drážních zařízení je podřízena managementu spolehlivosti a bezpečnosti drážního zařízení v celém životním cyklu dle EN 50126 [17]. Tato norma je spolu s EN 50128 [18] a EN 50129 [19] specifickou aplikací normy IEC 61508 pro drážní zařízení.

EN 50126, jak bylo uvedeno, zajišťuje management spolehlivosti a bezpečnost. Zajišťuje systémové podmínky pro minimalizaci systematických (nenáhodných) poruch vhodným řízením procesů k naplnění požadavků spolehlivosti a bezpečnosti.

EN 50129 zajišťuje funkční bezpečnost elektronických zabezpečovacích systémů z hlediska hardwarového řešení a postupů prokazování úrovně integrity bezpečnosti.

EN 50128 se soustřeďuje na metody, které je třeba použít pro zajištění softwaru vyhovujícího požadavkům na integritu bezpečnosti.

Splnění požadavků EN 5016, EN 50128 a EN 50129 je dostatečné k zajištění toho, aby nebylo třeba dodatečně prokazovat splnění požadavků normy IEC 61508.

V současné době procházejí tyto normy zásadním přepracováním a jsou k dispozici pracovní verze pro účastníky normalizačního procesu.

2.4 Funkční bezpečnost automobilů

S nástupem elektroniky do automobilů došlo k výrazné změně v jejich řízení, resp. k posílení kontroly elektronických systémů nad chováním auta. Řada elektronických asistentů (např. ABS, ESP, TCS) se stala standardní či povinnou povinnou součástí automobilů a další přibývají (tempomat, řízení stěračů, světel, rozpoznávání pruhů, sledování odstupu vozidla, dopravních značek). Tyto asistenty pocházejí od nezávislých firem, které se na jejich vývoj specializují a automobilovým výrobcům je dodávají. Proto vznikl standard ISO 26262, který se stal nezbytnou součástí řízení funkční bezpečnosti pro společnosti vyrábějící elektrické a elektronické komponenty pro automobilový průmysl.

Norma ISO 26262 je oborovou aplikací IEC 61508 přizpůsobenou pro elektrické a/nebo elektronické (E/E) systémy používané v silničních vozidlech funkční bezpečnosti. ISO 26262 je složená z částí 1 až 10. Stejně jako IEC 61508 je založena na systematickém řízení aktivit spojených s životním cyklem bezpečnosti E/E systémů a bezpečnosti softwaru při používání E/E systémů pro plnění funkcí ve vozidle.

ISO 26262 není zavedena v ČSN a její jednotlivé části, viz [20 až 29], upravují různé aspekty funkční bezpečnosti. Z celé struktury normy je zřejmá návaznost na koncepci funkční bezpečnosti nastolenou v IEC 61508. Odlišné je však značení integrity bezpečnosti (ASIL) a úrovní integrity bezpečnosti A, B, C, D, přičemž D vyjadřuje nejvyšší úroveň integrity bezpečnosti. Principy odhadu rizika a přiřazování úrovně ASIL jsou založeny na stejných východiscích, jako jsou uváděny v IEC 61508.

3 Závěr

Z uvedeného přehledu je zřejmé zásadní úloha IEC 61508 ve funkční bezpečnosti. Jednotlivé oborové implementace pak zohledňují specifické okolnosti platné v daném průmyslovém odvětví. Tyto specifické okolnost jsou dány jednak charakteristikou objektů, na které se bezpečnostní funkce aplikují (objekty masově vyráběné, objekty malosériové či kusové), složitosti objektů (elektrárny, chemické provozy, vlaky, jednoúčelové stroje, …) a v neposlední řadě velikostí újmy, kterou mohou způsobit (mnohočetná úmrtí, zranění, ekonomické ztráty).

Z toho důvodu je třeba i k normám při jejich aplikaci v daném odvětví přistupovat s uvědoměním souvislostí a nepoužívat je jen k formálnímu naplnění požadavků funkční bezpečnosti.

Použitá literatura:

[1] FUCHS, P. Funkční bezpečnost systémově. In *Sborník z 46. semináře Odborné skupiny pro spolehlivost České společnosti pro jakost „Případové studie realizace projektů*

spolehlivosti". Česká společnost pro jakost, Praha, 2012. ISBN 978-80-02-02363-0. Dostupné na WWW: http://www.csq.cz/uskutecnene-seminare/.

[2] ZAJICEK, J., FUCHS, P. Porovnání přístupů stanovení funkční bezpečnosti. In *Sborník z 53. semináře Odborné skupiny pro spolehlivost České společnosti pro jakost „Bezpečnost a spolehlivost nových technologií"*. Česká společnost pro jakost, Praha, 2013. ISBN 978-80-02-02505-4. Dostupné na WWW: http://www.csq.cz/uskutecnene-seminare/

[3] ČSN EN 61508-1 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 1: Všeobecné požadavky.*

[4] ČSN EN 61508-2 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností*

[5] ČSN EN 61508-3 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 3: Požadavky na software.*

[6] ČSN EN 61508-4 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 4: Definice a zkratky*

[7] ČSN EN 61508-5 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Příklady metod určování úrovní integrity bezpečnosti.*

[8] 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.*

[9] ČSN EN 61508-7 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 7: Přehled technik a opatření.*

[10] ČSN EN 61511-1:2005 *Funkční bezpečnost. Bezpečnostní přístrojové systémy pro sektor průmyslových procesů bezpečností – Část 1: Požadavky na systémy hardwaru a softwaru, struktura, definice.*

[11] ČSN EN 61511-2:2005 *Funkční bezpečnost. Bezpečnostní přístrojové systémy pro sektor průmyslových procesů bezpečností – Část 2: Metodický pokyn pro používání IEC 61511-1.*

[12] ČSN EN 61511-3:2005 *Funkční bezpečnost. Bezpečnostní přístrojové systémy pro sektor průmyslových procesů bezpečností – Část 3: Pokyn pro stanovení požadované úrovně integrity bezpečnosti.*

[13] ČSN IEC 61513:2003 *Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Všeobecné požadavky na systémy.*

[14] ČSN EN 62061:2005 *Bezpečnost strojních zařízení – Funkční bezpečnost elektrických /elektronických/programovatelných elektronických systémů souvisejících s bezpečností.*

[15] ČSN EN ISO 13849-1:2008 *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Všeobecné zásady pro konstrukci.*

[16] ČSN EN ISO 1218-1:2012 *Roboty a robotická zařízení – Požadavky na bezpečnost robotů – Část 1: Roboty.*

[17] ČSN EN 50126-1:2001 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS).*

[18] ČSN EN 50128:2001 *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy pro zpracování dat – Software pro drážní řídicí a ochranné systémy.*

[19] ČSN EN 50129:2001 *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy pro zpracování dat – Elektronické zabezpečovací systémy.*

[20] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 1: Vocabulary.*

[21] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 2: Management of functional safety.*

[22] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 3: Concept phase.*

[23] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 4: Product development at the system level.*

[24] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 5: Product development at the hardware level.*

[25] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 6: Product development at the software level.*

[26] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 7: Production and operation.*

[27] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 8: Supporting processes.*

[28] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses.*

[29] ISO 26262-1:2012 *Road vehicles – Functional safety – Part 10: Guideline on ISO 26262.*

Nároky certifikace funkční bezpečnosti produktu kladené na jeho výrobce

Ing. Martin Šimonik

BD SENSORS s.r.o.

e-mail: martin.simonik@bdsensors.cz, www.bdsensors.eu

1 Úvod

Pro zajištění konkurenceschopnosti jsou v dnešní době firmy stále více nuceni inovovat své produkty, aby udrželi krok s konkurencí, který se v dnešní době neustále zrychluje. Stále modernějším trendem a jednou z podstatných vlastností výrobků nejen na českém či evropském trhu je jejich funkční bezpečnost. Firma BD SENSORS s.r.o. se zabývá výrobou snímačů tlaku a výšky hladiny již více jak 20 let a na poli tlakoměrné techniky se řadí minimálně v rámci Evropy na čelní místa. Požadavky na funkční bezpečnost a její prokázání postupně prosakují z dopravního a energetického průmyslu do dalších odvětví a měření a regulace tlaku v tom již není výjimkou. Účelem tohoto článku je přinést jeho čtenáři základní přehled o nárocích na dokumentaci funkční bezpečnosti pro certifikaci produktu v oblasti měření tlaku a jemu příbuzných odvětví.:

2 Popis snímače tlaku XMP I (XMD) a jeho vymezení

Snímač tlaku XMP i (obr. 1) vyráběný firmou BD SENSORS s.r.o. je navržený pro průmyslové procesy a to pro měření podtlaku, relativního a absolutního tlaku par, kapalin a kalů až do tlaku 600 bar. Snímač je již ve své základní verzi vybaven digitální komunikací HART (HART revize 7). Na výběr je pak dvojice pouzder, a to nerezové polní pouzdro nebo pouzdro duralové dvoukomorové. Jako vlastní senzor tlaku, zde slouží senzor s interním označením firmy DSP 411 (obr. 2) pracující na bázi polovodičového tenzometru s oddělovací membránou o průměru 18 mm. Tento senzor je vhodný pro měření plynných a kapalných médií, která jsou slučitelná s nerezovou ocelí. Technické a katalogové listy snímače tlaku XMP i tak i samotného senzoru tlaku DSP 411 jsou dostupné z webových stránek výrobce www.bdsensors.cz.

Snímač tlakové diference XMD (obr. 3) se od snímače tlaku XMP i neliší v ničem jiném než v použitém senzoru. Veškeré ostatní komponenty jsou totožné (elektronika, pouzdro atd.). Senzor tlakové diference je na obr. 4. Katalogový list snímače tlakové diference XMD je dostupný z webových stránek výrobce www.bdsensors.cz.

2.1 Popis snímače tlaku XMP i (XMD) - HW

Snímač tlaku XMP i (obr. 1) vyráběný firmou BD SENSORS s.r.o. je navržený pro průmyslové procesy a to pro měření podtlaku, relativního a absolutního tlaku par, kapalin a kalů až do tlaku 600 bar. Snímač je již ve své základní verzi vybaven digitální komunikací HART (HART revize 7). Na výběr je pak dvojice pouzder, a to nerezové polní pouzdro nebo pouzdro duralové dvoukomorové. Jako vlastní senzor tlaku, zde slouží senzor s interním označením firmy DSP 411 (obr. 2) pracující na bázi polovodičového tenzometru s oddělovací membránou o průměru 18 mm. Tento senzor je vhodný pro měření plynných a kapalných médií, která jsou slučitelná

s nerezovou ocelí. Technické a katalogové listy snímače tlaku XMP i tak i samotného senzoru tlaku DSP 411 jsou dostupné z webových stránek výrobce www.bdsensors.cz.

Snímač tlakové diference XMD (obr. 3) se od snímače tlaku XMP i neliší v ničem jiném než v použitém senzoru. Veškeré ostatní komponenty jsou totožné (elektronika, pouzdro atd.). Senzor tlakové diference je na obr. 4. Katalogový list snímače tlakové diference XMD je dostupný z webových stránek výrobce www.bdsensors.cz.

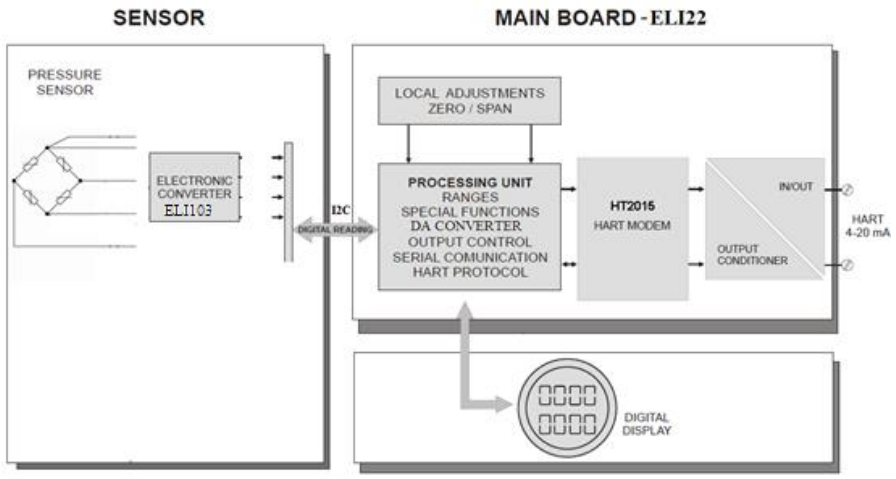
Obr. 1: Snímač tlaku XMP i firmy BD SENSORS (duralové dvoukomorové pouzdro)

Obr. 2: Senzor tlaku DSP 411

Obr. 3: Diferenční snímač tlaku XMD

Obr. 4: Senzor snímače dif. tlaku XMD

Základní blokové schéma zapojení snímačů tlaku je zobrazeno na následujícím obrázku (obr. 5).



Obr. 5: Blokové schéma snímače tlaku XMP i (XMD)

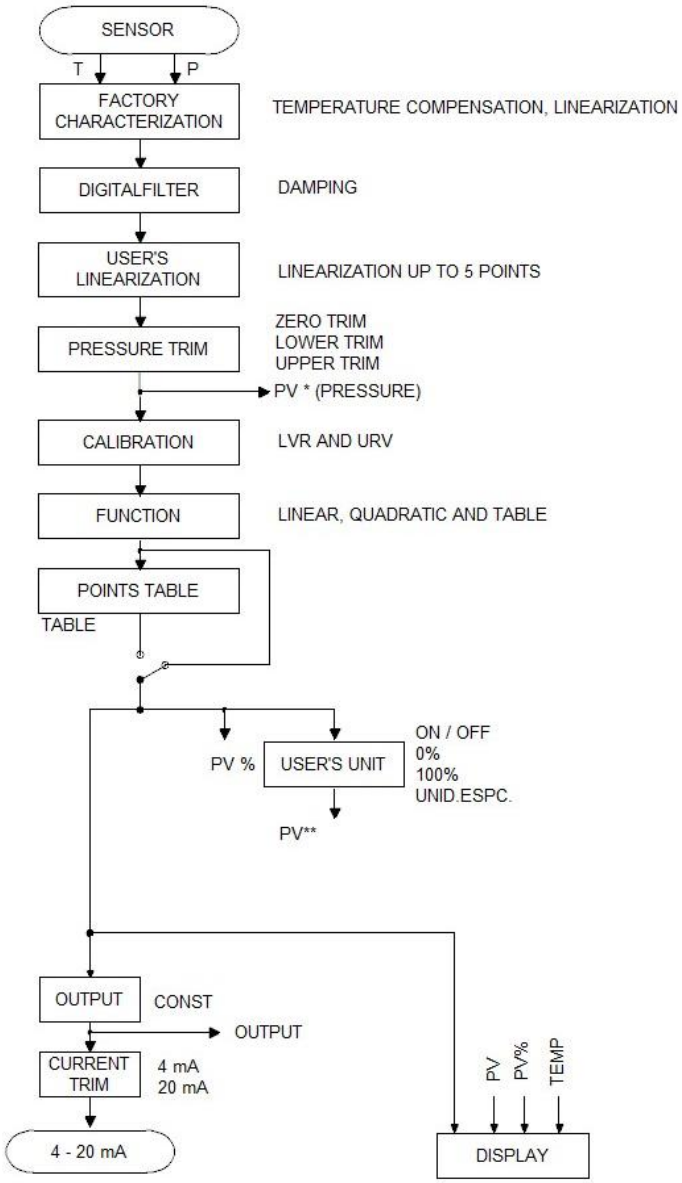
Vybrané technické parametry snímače tlaku XMP i jsou obsaženy v tab. 1. Kompletní parametry snímačů tlaku XMP i a (XMD) jsou uvedeny v katalogových listech, které jsou dostupné z webových stránek výrobce www.bdsensors.cz.

Tab. 1: Základní parametry snímače tlaku XMP i

Rozsah měřených tlaků	0,4 - 600 bar
Výstupní signál	2vodič: 4...20 mA
	jiskrově bezpečná verze s komunikací HART / U_B = 12…28 V_{DC}
	provedení Ex d - pevný závěr / U_B = 12…28 V_{DC}
Přesnost	≤ ± 0,1% FSO
Dlouhodobá stabilita	≤ ± 0,1% FSO / rok při referenčních podmínkách
Povolené teploty	bez displeje: okolí: -40…80°C
	s displejem: okolí:-20…70°C
	médium: silikonový olej -40…125°C
	médium: potravinářský olej: -10…125°C
Elektrická odolnost	odolnost proti zkratu: trvalá
	Odolnost proti přepólování: bez poškození, ale také bez funkce
	EMC: vyzařování a odolnost dle ČSN EN 61326
Mechanická odolnost	Vibrace: 5 g RMS dle DIN EN 60068-2-6
	Rázy: 100 g / 11 ms dle DIN EN 60068-2-27
Třída krytí	IP67
Hmotnost	minimálně 400g

2.2 Popis snímače tlaku XMP i (XMD) - SW

Veškerý SW použitý ve snímači XMP i (XMD) je programován za použití jazyka C. Vývojový diagram SW je znázorněn na obr. 6.



Obr.6: Vývojový diagram SW ve snímači XMP i

Funkce SW snímače XMP i (XMD):

1. Inicializace HW – inicializace všech HW částí, načtení hodnot z paměti EPROM, spuštění měření
2. Výrobní kalibrace – výpočet matematických funkcí pro určení teploty a tlaku
3. Teplotní kompenzace – korekce vlivu okolní teploty na měření tlaku
4. Linearizace – korekce převodní charakteristiky senzoru
5. Uživatelská linearizace – uživatelská korekce převodní charakteristiky senzoru
6. Přenosová funkce – nastavení přenosové funkce analogového výstupu
7. Výpočet analogového výstupu – určení hodnoty analogového výstupu
8. HART slave protokol – komunikace protokolem HART s nadřazeným systémem

9. Funkce HART protokolu – čtení hodnoty, nastavení konfigurace snímače, kalibrace snímače
10. Funkce zobrazení – zobrazení hodnoty na displeji
11. Funkce menu – lokální nastavení konfigurace snímače

2.3 Fyzické a funkční vymezení snímače

Pro analýzu objektu je nutné stanovit jeho fyzické a funkční hranice. Analyzovaným objektem byl v tomto případě snímač tlaku XMP i (XMD) firmy BD SENSORS s.r.o. a to v sestavě dané katalogovým listem snímače tlaku XMP i (XMD). Hranice systému je na jedné straně definována tlakový připojením (tlakovými přípojkami či tlakovou přírubou dle katalogového listu snímače tlaku XMP i (XMD) a na straně druhé jejich elektrickým připojením realizovaným skrz kabelovou průchodku do svorkovnice.

Podmínky činnosti snímače XMP i (XMD) jsou specifikovány v katalogovém listu snímače XMP i (XMD). Za nejdůležitější podmínky, které mohou ovlivnit funkci snímačů při překročení specifikovaných mezí, se považují:

- teplota měřeného média,
- typ měřeného média,
- teplota okolí snímače,
- tlakový rozsah měřeného média,
- tlakové rázy.

Na základě fyzického a funkčního vymezení snímače XMP i (XMD) je poté přistoupeno k popisu řešení jeho funkční bezpečnosti podle etap životního cyklu.

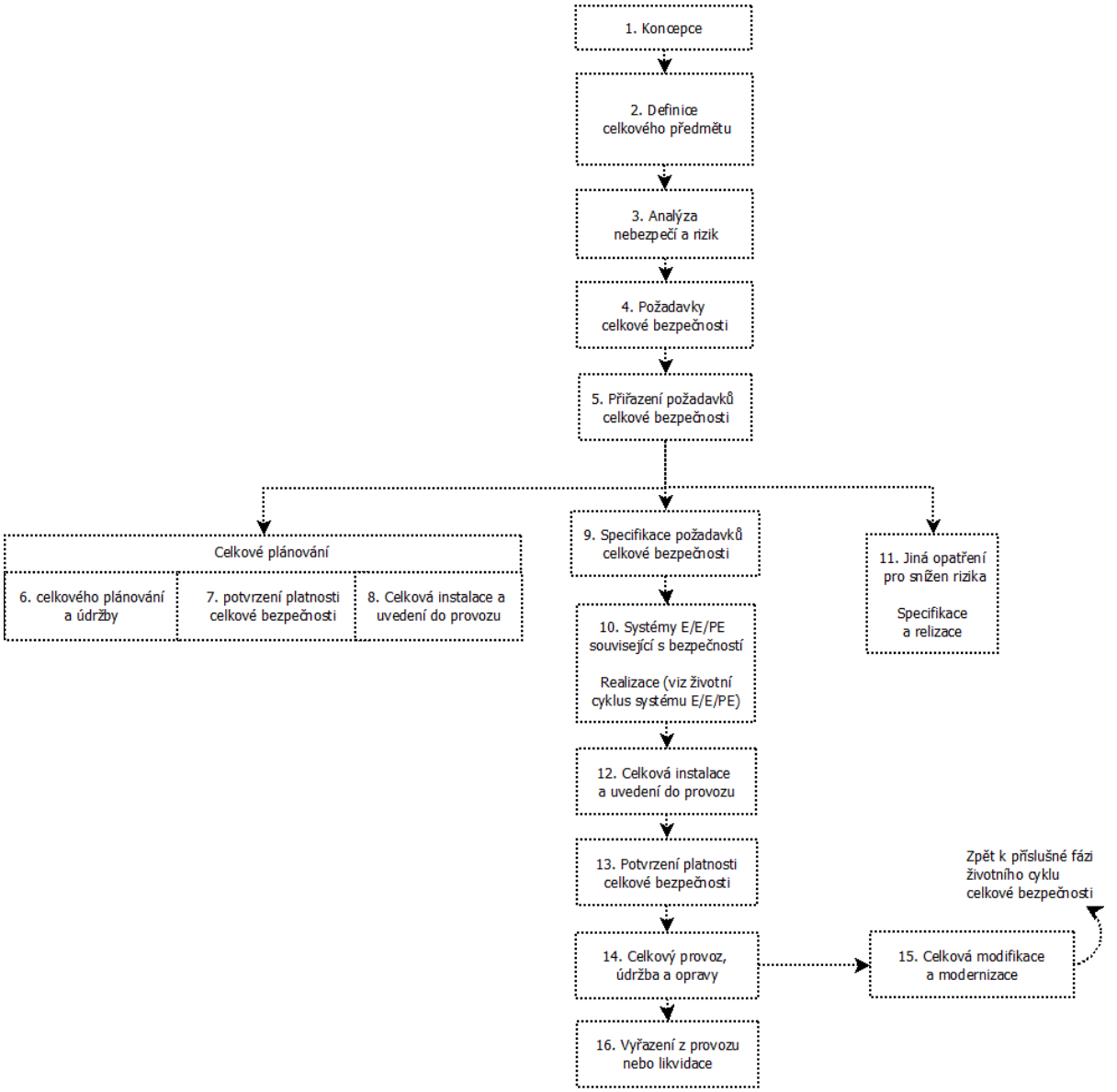
3 Důvody k podání žádosti o certifikaci u TÜV SÜD

Mezi hlavní důvody pro podání žádosti o certifikaci funkční bezpečnosti na úrovni SIL2 patřily především množící se požadavky zákazníka a rovněž ztráta možnosti účastnit se výběrových řízení, kde je certifikace výrobku minimálně na úroveň SIL2 jedním z požadavků. Mezi certifikační orgány zabývající se posuzováním funkční bezpečnosti patří, kromě vybrané TÜV SÜD například společnosti EXIDA, Risknowlogy, DEKRA ad. Sesterská společnost v Německu, firma BD SENSORS GmbH již dříve zvolila pro certifikaci analogové řady snímačů tlaku firmu Risknowlogy. Inspekční zpráva a vydané certifikáty jsou dostupné z webových stránek výrobce www.bdsensors.de.

Firma BD SENSORS s.r.o. zvolila certifikační organizaci TÜV SÜD Ostrava. A to jak z důvodů snadnější komunikace a tvorby veškeré dokumentace v českém jazyce, tak i z důvodu dobré spolupráce s touto organizací, která firmě BD SENSORS s.r.o. provádí certifikační a recertifikační audity systému managementu kvality dle ČSN EN ISO 9001:2016.

4 Požadavky na dokumentaci funkční bezpečnosti TÜV SÜD

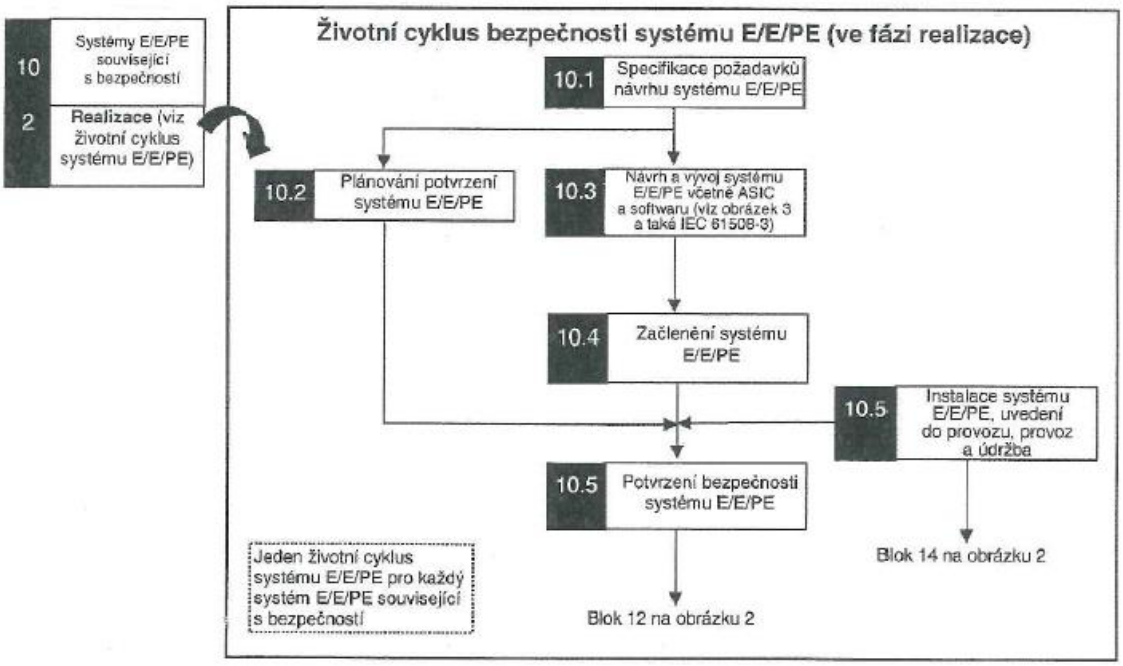
Hlavním požadavkem certifikační organizace TÜV SÜD bylo předložení kompletní dokumentace funkční bezpečnosti dle celkového životního cyklu bezpečnosti uvedeného v normě ČSN EN 61508-1 (viz obr. 7).



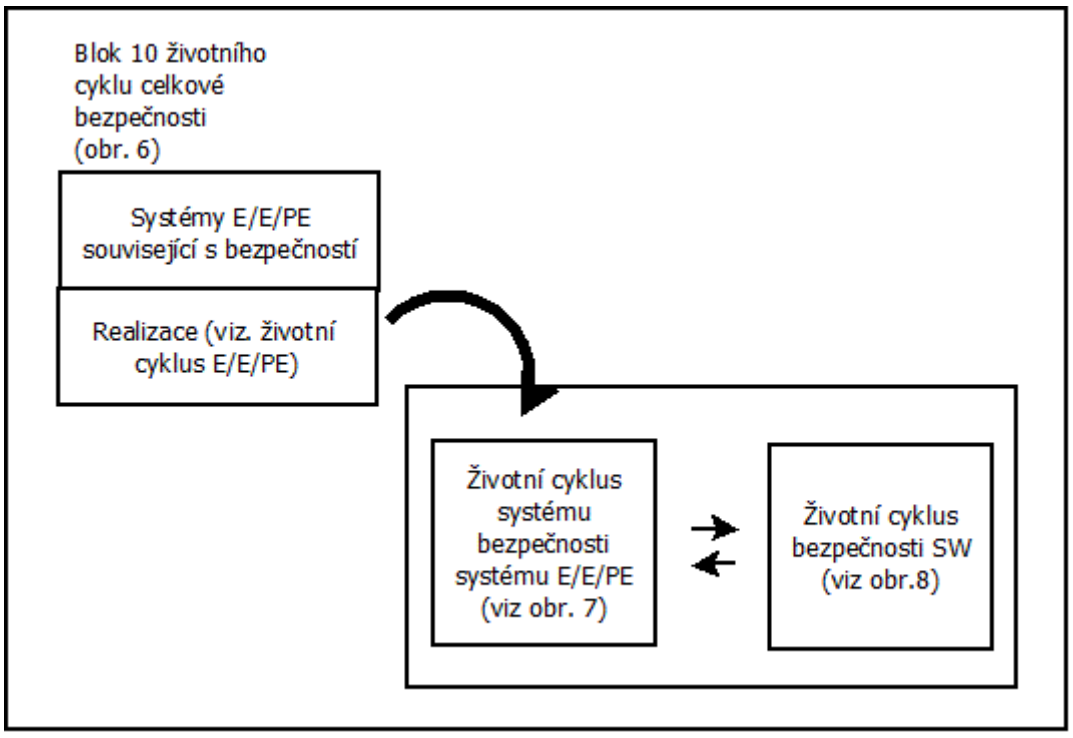
Obr.7: Životní cyklus celkové bezpečnosti dle ČSN EN 61508-1 [1]

Jelikož snímač tlaku XMP i (XMD) je v provozu vždy součásti nadřazeného systému (samotný snímač talku XMP i (XMD) není EUC), se fáze celkové bezpečnosti č. 1 až č. 9 a fáze č. 11 až č. 16 neuplatní. Tato skutečnost je v dokumentaci funkční bezpečnosti snímače tlaku XMP i náležité zdůvodněna.

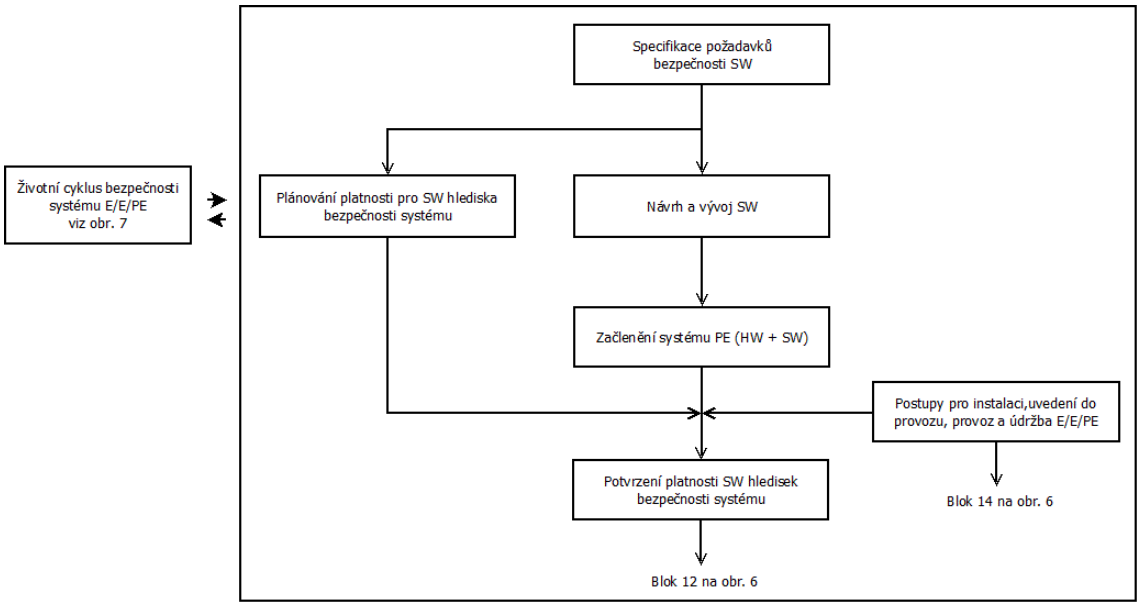
Posouzení funkční bezpečnosti E/E/PES a bezpečnosti softwaru dle požadavků ČSN EN 61508-1, ČSN EN 61508-2, ČSN EN 61508-3, za využití ČSN EN 61508-6 a ČSN EN 61508-7. bylo provedeno v rámci etapy č. 10 životního cyklu celkové bezpečnosti. Jednotlivé fáze životního cyklu E/E/PE a softwaru, včetně životního cyklu vývoje ASIC (V-model) jsou zdokumentovány na následujících obrázcích.



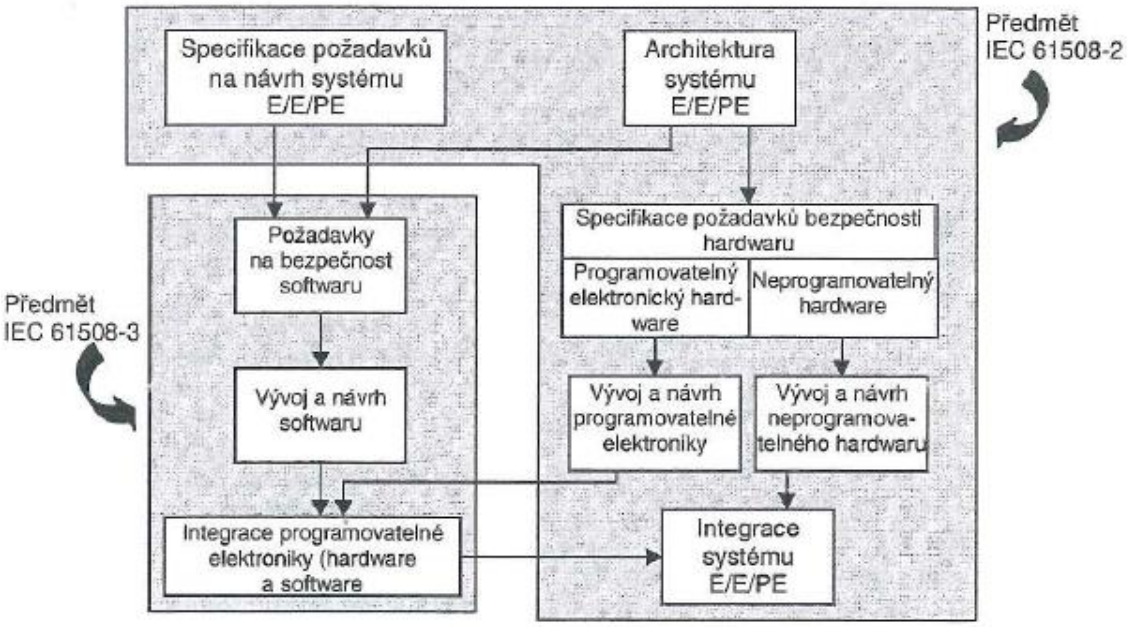
Obr. 8: Životní cyklus bezpečnosti systému E/E/PE ve fázi realizace



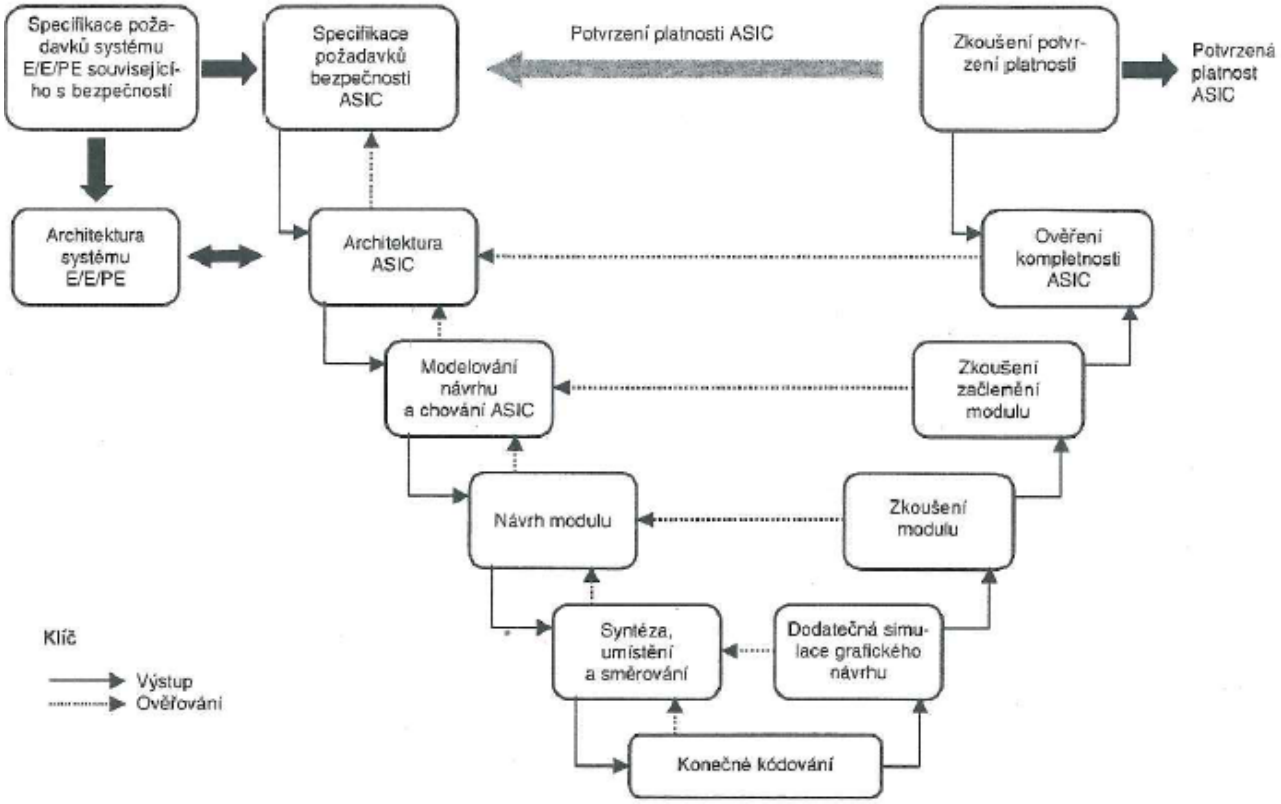
Obr. 9: Vztah mezi životním cyklem bezpečnosti systému E/E/PE a životním cyklem bezpečnosti SW



Obr. 10: Životní cyklus bezpečnosti SW (v realizační fázi)



Obr. 11: Vztah mezi předmětem ČSN EN 61508-2 a ČSN EN 61508-3



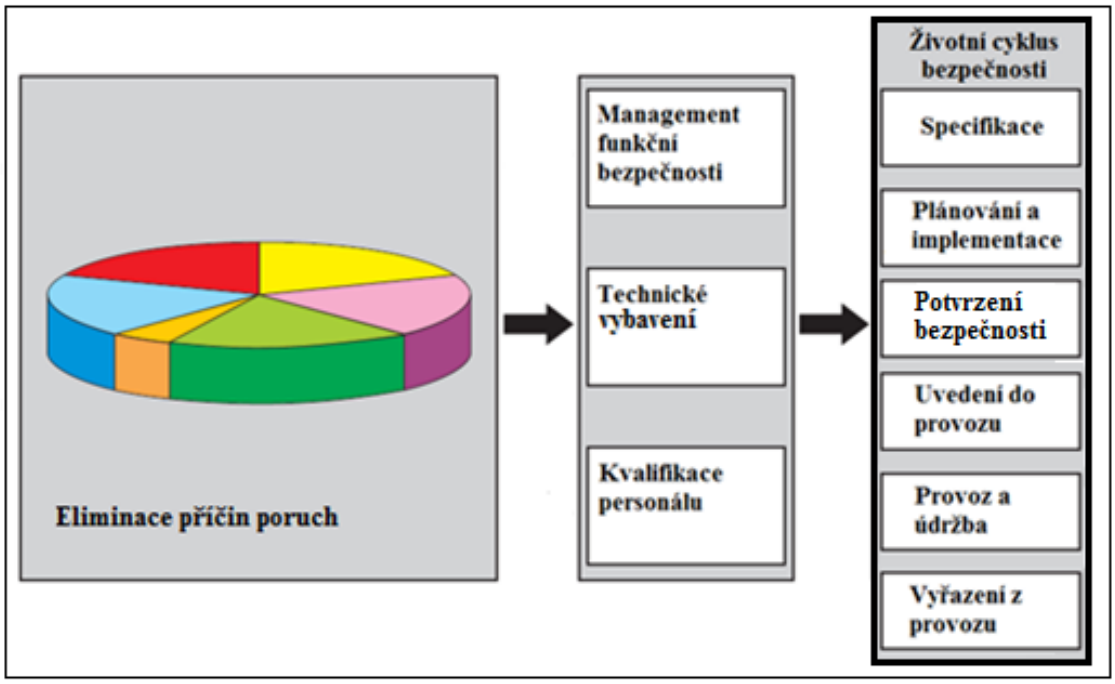
Obr. 12: Životní cyklus vývoje ASIC (Model-V)

Výše uvedené procesy životních cyklů vedou k eliminaci příčin nenáhodných poruch. Způsob jakým společnost BD SENSORS aplikuje tyto procesy je popsán v následující kapitole.

5 Řízení funkční bezpečnosti snímače tlaku XMP i (XMD)

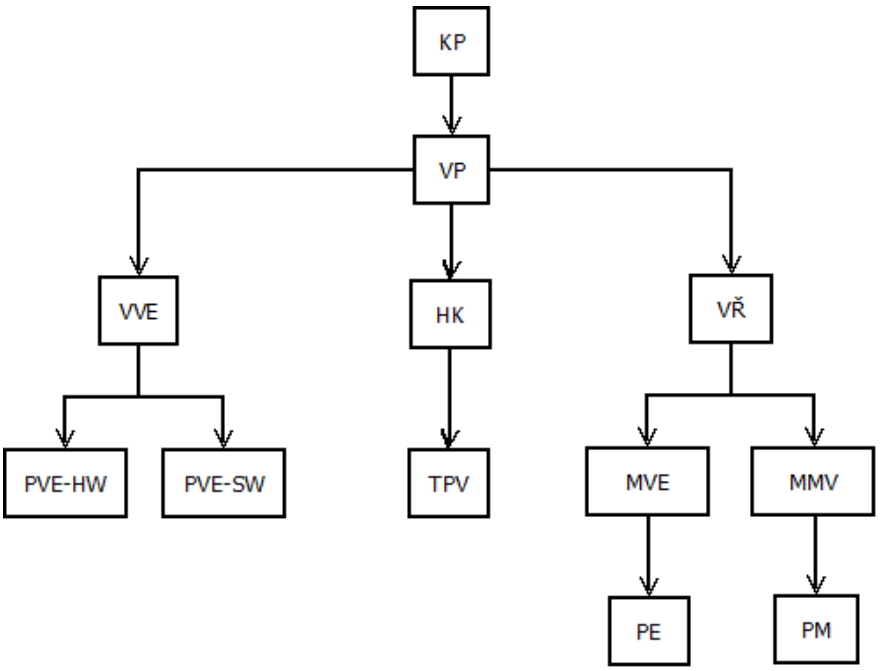
Pro řízení funkční bezpečnosti ve firmě BD SENSORS s.r.o. byla sestavena speciální směrnice, která popisuje přístup firmy k řízení funkční bezpečností. Tento přístup znázorňuje blokové schéma na obr. 13 a vychází z požadavků pro řízení funkční bezpečnosti popsanými v ČSN EN 61508-1, ČSN EN 61508-2, ČSN EN 61508-3.

Jednotlivé fáze dle obr. 13 bylo nutné v dokumentaci funkční bezpečnosti předkládané certifikačnímu orgánu TÜV SÜD náležitě zdokumentovat a doložit tak jejich naplnění.



Obr. 13: Přístup k životnímu cyklu bezpečnosti snímače XMP i (XMD) ve firmě BD SENSORS s.r.o.

Management funkční bezpečnosti - Pro jednotlivé fáze životního cyklu bezpečnosti musí být stanoveny řídící funkce. Příklad organizačního schématu managementu funkční bezpečnosti je zobrazen na obr. 14.



Obr. 14: Management funkční bezpečnosti firmy BD SENSORS s.r.o.

KP	–	Koordinátor Projektu funkční bezpečnosti
VP	–	Vedoucí Projektu funkční bezpečnosti
VVE	–	Vedoucí Vývoje Elektro
PVE-HW	–	Pracovník Vývoje Elektro HW – návrh a vývoj elektronik (ASIC)
PVE-SW	–	Pracovník Vývoje Elektro SW – návrh a vývoj SW
HK	–	Hlavní Konstruktér
TPV	–	Technická Příprava Výroby
VŘ	–	Výrobní Ředitel
MVE	–	Mistr Výroby Elektro
PE	–	Pracovník Elektro
MMV	–	Mistr Mechanické Výroby
PM	–	Pracovník Mechanické

Technické vybavení - Firma musí disponovat vybavením (pro návrh, vývoj, výrobu) svých produktů, které zaručí potřebnou bezpečnost (resp. funkční bezpečnost) výsledného produktu. Daná zařízení musí být v řádném technickém stavu a musí na nich být pravidelně prováděna údržba a kalibrace. Toto je zajištěno ve firmě BD SENSORS s.r.o. nastavením lhůt pro kalibrace a údržbu v systému SAP. Organizace TÜV SÜD požaduje zaslání kalibračních listů použitých přístrojů či záznamů o údržbě.

Kvalifikace personálu - Jednotlivé osoby (personál) podílející se na realizaci jednotlivých fázi životního cyklu bezpečnosti musí mít pro danou činnost dostatečnou kvalifikaci. Ta je zajištěna jak minimálním požadovaným vzděláním pro danou pozici, tak pravidelným školením tohoto personálu pro provádění dané činnosti. Organizace TÜV SÜD požaduje zaslání dokladů o vzdělání jednotlivých členu managementu funkční bezpečnosti.

Specifikace požadavků - V této fázi je nutné specifikovat, jakých požadavků má být v rámci požadované funkční bezpečnosti na daném produktu dosaženo. To se odvíjí především od požadované úrovně funkční bezpečnosti SIL (1-4). Konkrétní požadavky pro tyto úrovně pak předepisuje norma ČSN EN 61508 a to jak pro systém E/E/PE (HW) tak i pro integrovaný SW.

Plánování a implementace - Popis jednotlivých fází návrhu, vývoje a výroby snímače tlaku XMP i – včetně HW, SW a ASIC. Detailní popis jednotlivých fázi doplněný o validaci dané fáze. Jako příklad lze uvést návrh snímače tlaku XMP i a ověření tohoto návrhu oponentním řízením, které je předkládáno organizaci TÜV SÜD. Celkově se jedná o rozsáhlou fázi životního cyklu, kde každá dílčí fáze návrhu, vývoje a výroby musí být náležitě zdokumentována a doplněna o validační protokol. Organizace TÜV SÜD požaduje zaslání řídící dokumentace pro fáze návrhu, výroby a vývoje.

Potvrzení bezpečnosti snímače tlaku XMP i (XMD) – tato fáze dokládá splnění specifikovaných požadavků pro jednotlivé etapy životního cyklu snímače. Především je nutné doložit dostatečnou odolnost pro úroveň integrity bezpečnosti SIL2 snímače proti systematickým a náhodným chybám HW i SW. To je možné doložit například pomocí funkční analýzy a analýzy FMECA snímače a rovněž o doporučené metody normy ČSN EN 61508-7.

6 Aplikované postupy na HW a SW snímače dle ČSN EN 61508

Pro část HW snímače tlaku byly použity níže uvedené metody dle požadavků ČSN EN 61508-7.

Techniky a opatření použité pro specifikaci požadavků návrh snímače:

- Management projektu – stanovení odpovědných osob a činností
- Dokumentace – zadaní projektu na vývoj snímače SIL2 na základě požadavku trhu
- Strukturovaná specifikace
- Kontrola specifikace – oponentní řízení
- Nástroje pro specifikaci pomocí PC

Techniky a opatření pro návrh a vývoj HW:

- Dodržování technických norem
- Management projektu
- Dokumentace
- Strukturovaný návrh
- Modularizace
- Nástroje pro návrh pomocí PC
- Kontrola HW

Techniky a opatření pro návrh a vývoj SW:

- Strukturovaná metodologie
- Strukturované programování
- Programovací jazyk – programovací jazyk C/C++

Techniky a opatření během začleňování snímače HW:

- Funkční zkoušky
- Analýza důsledků chyb HW - FMECA
- Management projektu
- Dokumentace
- Provozní zkušenosti

Techniky a opatření během začleňování SW:

- Funkční testování
- Analýza důsledků chyb SW – SFMEA
- Testování výkonnosti
- Záznam analýza dat
- Modulární přístup

Techniky a opatření pro provoz a údržbu snímače

- Pokyny pro provoz a údržbu (návod)
- Management projektu
- Dokumentace
- Provoz s kvalifikovaným operátorem

Techniky a opatření během potvrzování platnosti bezpečnosti snímače

- Funkční zkoušky
- Funkční zkoušky v podmínkách okolního prostředí
- Management projektu
- Dokumentace
- Statická analýza a analýza poruch
- Provozní zkušenosti

7 Data spolehlivosti a jejich získání

Pro elektronické komponenty typu rezistor, kondenzátor apod. je možné získat data spolehlivosti (např. MTBF či intenzitu poruch λ) z katalogových listů těchto komponent. Pro součástky u kterých není možné data získat z jejich katalogových listů má pak řešitel následující možnosti:

1. Zisk spolehlivostních dat na základě typově podobné komponenty
2. Zisk (výpočet) dat na základě military standardu – MIL-HDBK-217F
3. Zisk z databáze typu EXIDA, BELLCORE, PRISM, SPIDR apod.
4. Z vlastních zkoušek spolehlivost (Data ze servisu resp. z provozu snímače)

Pro řešení funkční bezpečnosti snímače tlaku XMP i byly použity data pouze z katalogových listů vybraných komponent (př. kondenzátory firmy AVX, rezistory diody firmy Vishay), takto získaným datům byla přidělena důvěryhodnost 100%, zbylé komponenty byly odvozeny na základě servisních dat či na základě katalogového listu podobné komponenty a byla jim přidělena důvěryhodnost 75%. Získaná data byly použity pro řešení pomocí analytických metod (metoda FMECA).

8 Struktura dokumentace funkční bezpečnosti

Kompletní předložená dokumentace funkční bezpečnosti snímače organizaci TÜV SÜD obnášela tyto dokumenty:

1 Dokumentace funkční bezpečnosti - hlavní dokument
2 Metodologie řešení pomocí analytických metod a dat z provozu snímače
3 Sběr dat z provozu snímače tlaku XMP i
4 Funkční analýza a analýza FMECA snímače
5 Analýza FMEA softwaru snímače
6 Katalog s technickými parametry snímače XMP i
7 Katalog s technickými parametry snímače XMD
8 Katalog s technickými parametry senzoru tlaku DSP 411
9 Katalog s technickými parametry diferenčního senzoru tlaku

10 Návod k obsluze snímače tlaku XMP i
11 Návod k obsluze snímače tlaku XMD
12 Kompletní sestava snímače XMP i
13 Schéma zapojení elektronik snímače
14 Certifikáty a prohlášení o shodě snímače tlaku XMP i a XMD
15 Protokoly z měření přesnosti snímače a senzoru
16 Doklady o vzdělání jednotlivých členů managementu funkční bezpečnosti
17 Kalibrační listy použitých měřících přístrojů.
18 Seznam řídící dokumentace včetně směrnice o řízení funkční bezpečnosti

9 Současný stav certifikace

Firma BD SENSORS s.r.o. ke dni 11. 12. 2017 obdržela inspekční certifikát, který dokládá shodu snímače XMP i (XMD) s požadavky norem ČSN EN 61508-1 ed.2:2011, ČSN EN 61508-2 ed.2:2011, ČSN EN 61508-3 ed.2:2011, jako systém související s bezpečnosti úrovně integrity bezpečnosti SIL2. Inspekční certifikát je přílohou tohoto článku. Dále je k tomuto inspekčnímu certifikátu vydána organizací TÜV SÜD inspekční zpráva, která podrobně dokládá shodu s výše uvedenými normami na základě předložené dokumentace.

Seznam použitých norem

[1] ČSN EN 61508-1:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 1: Všeobecné požadavky.*

[2] ČSN EN 61508-2:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností*

[3] ČSN EN 61508-3:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 3: Požadavky na software.*

[4] ČSN EN 61508-4:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností – Část 4: Definice a zkratky*

[5] ČSN EN 61508-7:2011 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Přehled technik a opatření.*

[6] ČSN EN 61511:2005 *Funkční bezpečnost. Bezpečnostní přístrojové systémy pro sektor průmyslových procesů.*

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Czech

INSPEKČNÍ CERTIFIKÁT

evidenční číslo 11.412.422 rev.1

vydaný inspekčním orgánem č. 4002 akreditovaným ČIA dle ČSN EN ISO/IEC 17020:2012 organizaci:

BD SENSORS s.r.o
Hradišťská 817
687 08 Buchlovice

Na základě výsledků provedených kontrolou, hodnocením a zkouškami, které jsou uvedeny v Inspekční zprávě TÜV SÜD Czech evidenční číslo 11.359.989 z 2017-12-11 potvrzujeme shodu níže uvedeného zařízení:

Název:	**Digitální snímač tlaku**
Typ:	**XMP i**
Modifikace.	**XMP i 511-1001-AN-I-1.AKO-100-1-1-1-000**
Výrobní číslo:	**1900191**

s požadavky **ČSN EN 61508-1 ed.2:2011 (idt EN 61508-1:2010), ČSN EN 61508-2 ed.2: 2011 (idt EN 61508-2:2010), ČSN EN 61508-3 ed.2:2011 (idt EN 61508-3:2010)**
jako systém související s bezpečností úrovně integrity bezpečnosti SIL 2.

Podmínky platnosti:

uvedeny v Inspekční zprávě TÜV SÜD Czech evidenční číslo 11.359.989 z 2017-12-11.

Podrobné technické údaje uvedeny na straně 2.

V Ostravě, dne 2017-12-11

TÜV SÜD Czech s.r.o.

Za TÜV SÜD Czech s.r.o. : Ing. Michal Svrček

Zkušenosti se SW nástrojem SISTEMA pro funkční bezpečnost

Ing. Jaroslav Zajíček, Ph.D.

Technická univerzita v Liberci, Fakulta mechatroniky, informatiky a mezioborových studií

e-mail: jaroslav.zajicek@tul.cz

1 Úvod

V oblasti funkční bezpečnosti je nutné prokázat dosažené parametry navrženého (nebo v mnoha případech již realizovaného) systému. K tomu je užitečné využít softwarový nástroj, který na základě vložených parametrů jednotlivých prvků spočte výsledné parametry celého systému a především vytvoří souhrnnou strukturovanou zprávu o dosažených výsledcích. Tato zpráva je pak jednoduše kontrolovatelná a porovnatelná s analýzami jiných systémů. Takovým nástrojem je software SISTEMA, jehož funkcionality budou v tomto příspěvku prezentovány.

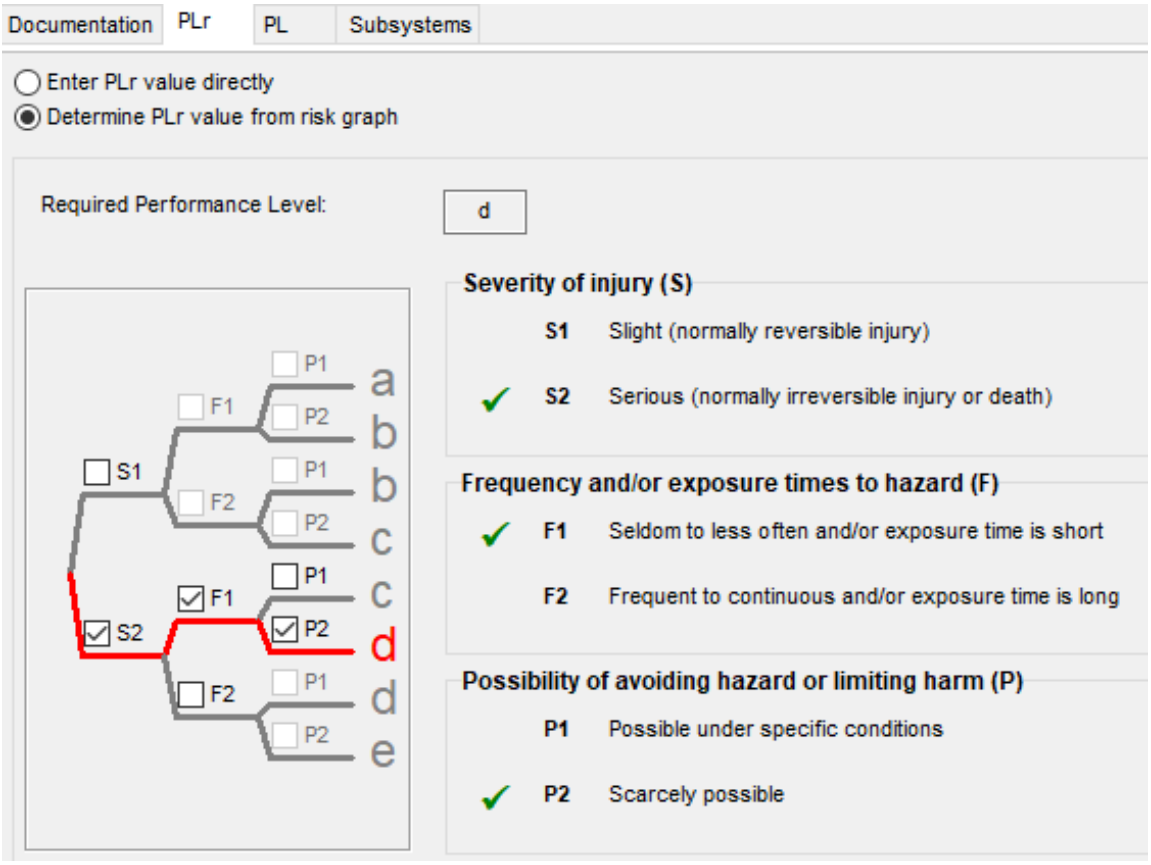
2 Software SISTEMA

Jedná se o software, který vytvořila německá organizace IFA a pomáhá při aplikaci a vyhodnocení zabezpečení strojního zařízení dle zásad funkční bezpečnosti specifikovaných v normě ČSN EN ISO 13849-1. Název SISTEMA je zkratkou z „Safety Integrity Software Tool for the Evaluation of Machine Applications“

Software je v licenci freeware a je možné ho stáhnout pomocí odkazu, který je zaslán na email zadaný na stránce IFA. Software prošel několika revizemi, které přináší nové funkcionality a zohledňují aktuální verzi normy. V době psaní tohoto příspěvku byla k dispozici verze 2.0.7 Build 2. V případě potřeby je možné mít nainstalováno více verzí tohoto software. Verze 1.x.x nejsou totiž zcela kompatibilní s verzemi 2.x.x – to se týká především používaných knihoven zařízení vytvořených výrobci těchto zařízení.

2.1 Fyzické a funkční vymezení snímače

První fází procesu zpracování projektu je jeho vytvoření, zadání identifikačních údajů a vytvoření seznamu projektovaných nebo realizovaných bezpečnostních funkcí, a to včetně požadovaných úrovní zabezpečení PLr (Required Performance Level). Úroveň zabezpečení PLr vychází z provedené analýzy rizika pomocí rozhodovacího diagramu - viz obrázek 1, nebo je možné přímo zadat úroveň PLr bez použití diagramu.



Obr. 1: Stanovení PLr rozhodovacím diagramem

V průběhu zadávání bezpečnostního systému software průběžně kontroluje, zda systém splňuje požadovanou hodnotu PLr a uživatel má tak okamžitou zpětnou vazbu o parametrech systému i korektnosti, respektive úplnosti zadávaných dat.

Software umožňuje mít otevřený větší počet projektů (1 projekt = 1 soubor na disku) a případně mezi sebou kopírovat celé bezpečnostní funkce nebo jejich dílčí části.

2.2 Sestavení bezpečnostní funkce

Každá bezpečnostní funkce má minimálně 3 hlavní subsystémy, a to vstupní část, logickou část a výstupní část (akční člen). Další subsystémy mohou být například vstupně-výstupní komunikační karty apod., které zprostředkovávají přenos dat mezi vstupní a logickou částí, nebo mezi logickou a výstupní částí. Samotné subsystémy mohou být tvořeny jedním, dvěma i více prvky. Níže jsou uvedeny příklady prvků pro jednotlivé subsystémy.

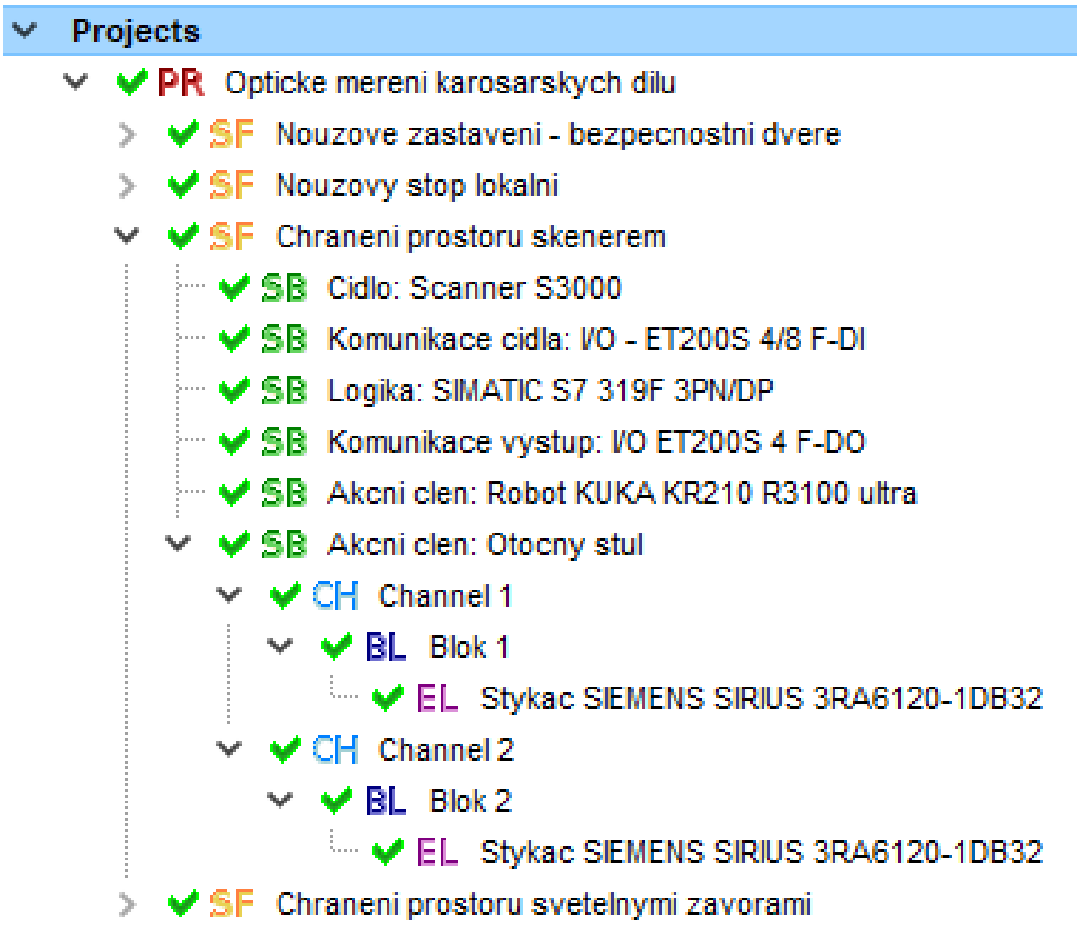
Vstupní část:

- bezpečnostní klika
- skener pohybu
- světelná závora
- spínače

Logická část:
- PLC
- bezpečnostní relé

Výstupní část:
- stykače
- ventily (hydraulické, pneumatické)
- brzdy

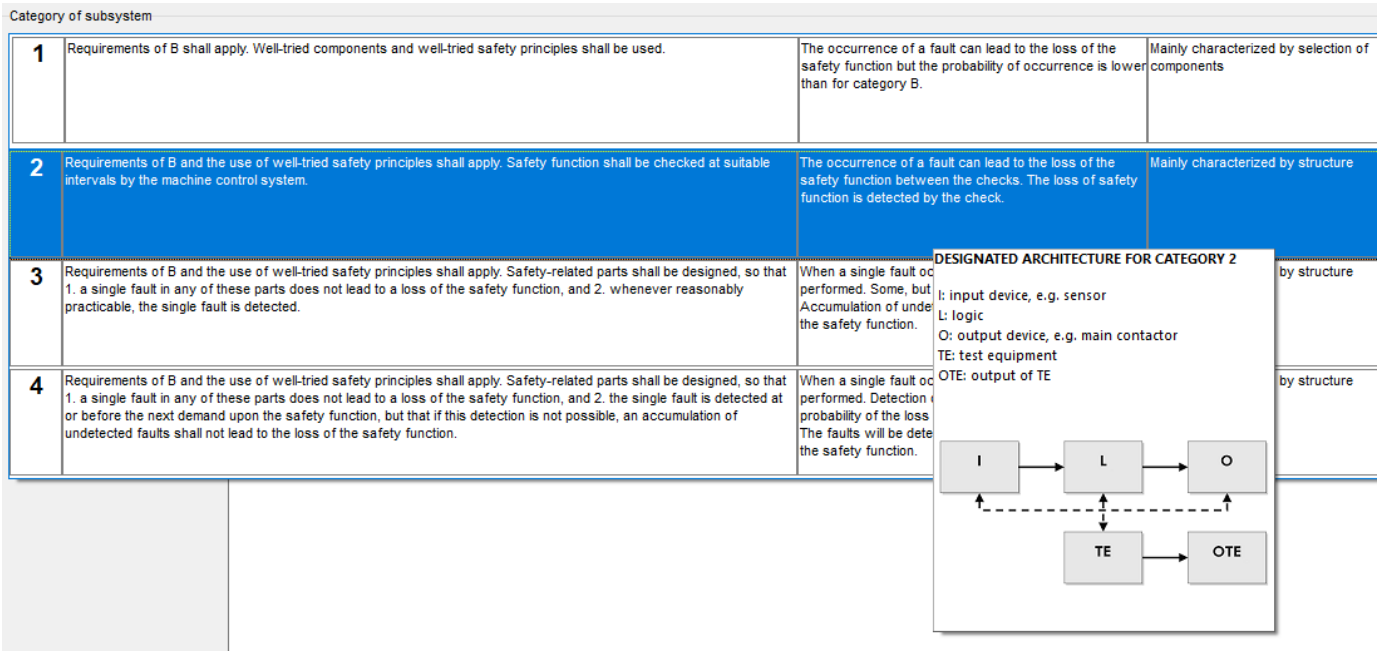
Na obrázku 2 je příklad stromové struktury jednoho projektu. Každý projekt může mít libovolný počet bezpečnostních funkcí, na obrázku jsou konkrétně 4 a jsou označeny symbolem SF (Safety Function). Bezpečnostní funkce se skládá ze subsystémů – řádky SB. Daný subsystém je tvořen buď jedním, nebo více prvky. Skener pohybu je v bezpečnostní funkci uveden jako jeden fyzický kus, ale jedná se o dvoukanálové zařízení. To, že je dvoukanálový, je obsaženo v jeho parametrech. Naopak stykačů jsou uvedeny 2 ks, pro každý kanál jeden, protože se ve skutečnosti opravdu jedná o dvě jednokanálová zařízení.



Obr. 2: Stromová struktura funkcí, subsystémů a prvků

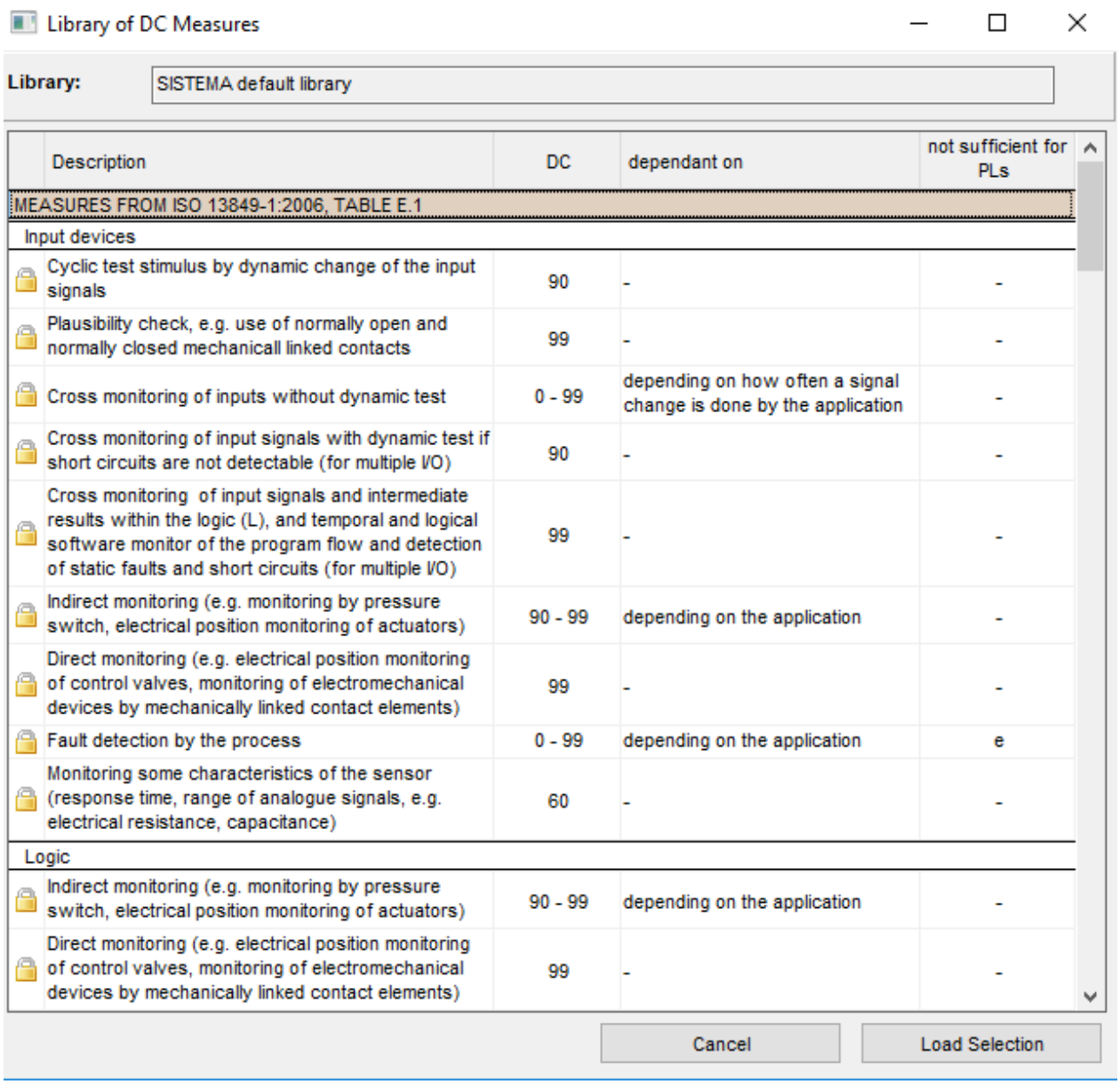
2.3 Parametry prvků

Prvky (subsystémy nebo jejich dílčí zařízení) musí být z důvodu kvantifikace bezpečnostní funkce detailně specifikovány. Nejjednodušší forma zadávání je u certifikovaných bezpečnostních zařízení, kdy výrobce buď přímo poskytuje pro software SISTEMA knihovnu svých zařízení (viz kap. 2.4), nebo jsou parametry snadno zjistitelné přes katalogové listy. V takovém případě je k prvku postačující zadat PL (nebo alternativně PFHD - Probability of Dangerous Failure per Hour) a kategorii, kterou prvek splňuje (-, B, 1, 2, 3, 4). Kategorie se stanovuje podle počtu kanálů, detekovatelnosti poruch a dalších kritérií, které jsou popsány v softwaru a přesně korespondují s požadavky v normě. Výběr kategorie je znázorněn na obrázku 3.



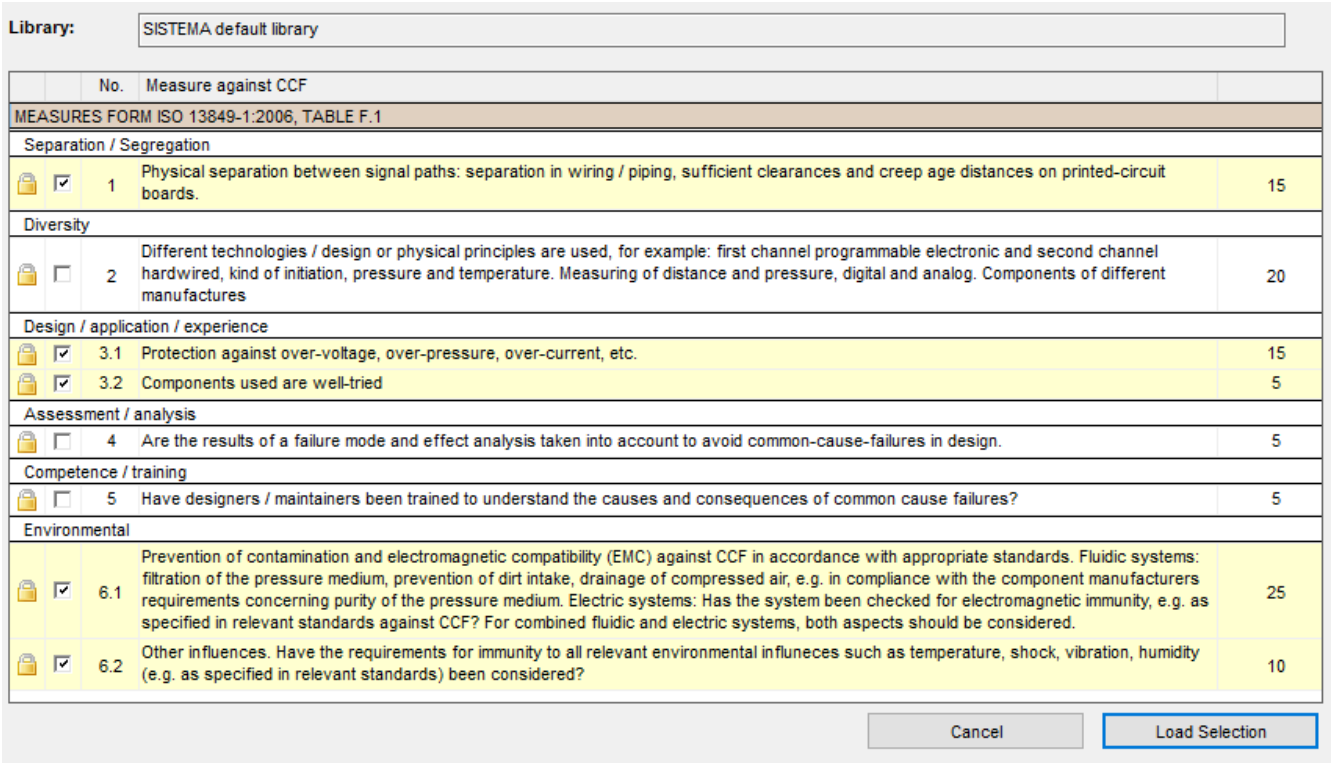
Obr. 3: Výběr kategorie subsystému

Ostatní „běžné“ prvky je třeba specifikovat detailněji, především pokud se jedná o dvoukanálové zapojení. Nezbytnou součástí je stanovení takzvaného diagnostického pokrytí DC pro každý prvek zvlášť. Diagnostické pokrytí je relativní počet poruch, který je identifikován logickým členem a může nabývat hodnot 0-99 %. Hodnotu DC je možné zadat přímo bez jakéhokoliv zdůvodnění, vhodnější je výběr z nabídky viz následující obrázek 4. Způsoby diagnostického pokrytí jsou rozděleny do kategorií podle toho, zda se týkají vstupních prvků, logických členů, nebo výstupních prvků.



Obr. 4: Knihovna pro stanovení diagnostického pokrytí

Mezi další zadávané informace o dvoukanálovém subsystému patří specifikace opatření, které jsou zajištěny z důvodu snížení výskytu poruch se společnou poruchou CCF (Common Cause Failure). Opatření jsou opět vybírána pomocí knihovny, přičemž každé opatření má nějakou bodovou hodnotu. Pro splnění požadavků je nutné v rámci každého subsystému splnit minimální bodovou hranici. Seznam opatření je součástí obrázku 5.



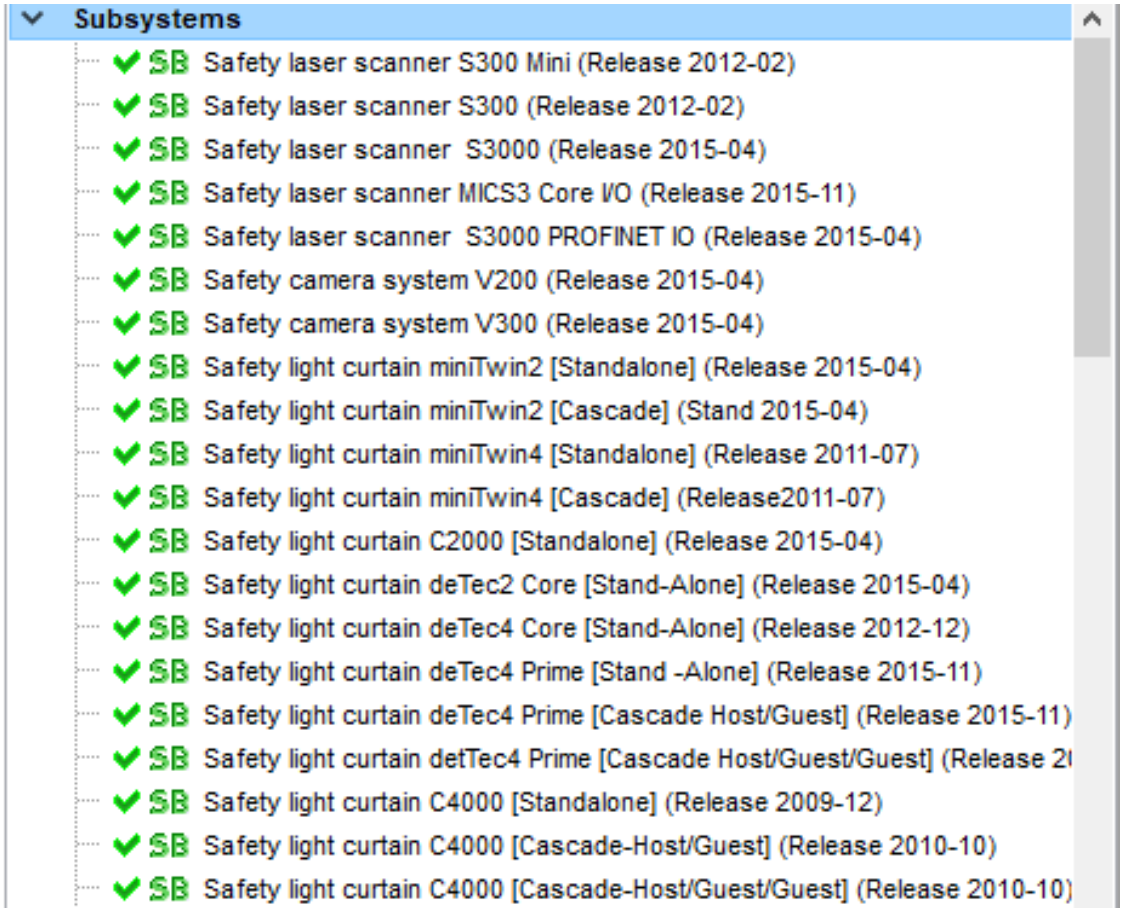
Obr. 5: Opatření pro snížení výskytu CCF

2.4 Knihovny zařízení

Certifikované bezpečnostní prvky vybraných výrobců, jako jsou Euchner, Festo, Reer, Sick a mnoho dalších, jsou k dispozici v knihovnách zařízení. Tyto knihovny vytvořili samotní výrobci zařízení a jsou k dispozici na jejich stránkách. Knihovny jsou průběžně aktualizovány s ohledem na měnící se portfolio výrobků. Co je nutné při stahování knihovny zohlednit, je verze používaného softwaru SISTEMA. Někteří výrobci zařízení zatím své knihovny nevytvořili pro verzi 2.x.x. Na druhou stranu je možné mít nainstalovanou i verzi 1.x.x, ve které se do projektu zařízení z knihovny vloží, a následně pokračovat ve vytváření projektu v aktuální verzi 2.x.x.

Pracovat s knihovnami je jednoznačně výhodné. Výrazně to zkracuje tvorbu projektu a kromě předvyplněných povinných polí pro stanovení úrovně funkční bezpečnosti jsou vyplněna i popisná pole, která podrobněji specifikují zařízení. Někteří výrobci mají knihovny ve dvou verzích – v anglickém a německém jazyce.

Část knihovny zařízení výrobce SICK je na obrázku 6. Jedná se o skenery pohybu, kamery a světelné závory.



Obr. 6: Příklad knihovny bezpečnostních zařízení

2.5 Výsledné úrovně PL bezpečnostních funkcí

Po kompletní parametrizaci všech zařízení podílejících se na bezpečnostních funkcích je možné posoudit výsledné úrovně PL pro jednotlivé bezpečnostní funkce, a to především porovnáním s požadovanými úrovněmi PLr na základě analýzy rizik – viz kapitola 2.1. Porovnání je možné jednotlivě kliknutím na danou funkci nebo hromadně vytvoření tzv. SISTEMA Reportu.

SF Chraneni prostoru skenerem	
PLr	d
PL	d
PFHD [1/h]	4,8E-7
SB Cidlo: Scanner S3000	
PL	d
PFHD [1/h]	8E-8

Obr. 7: Dosažené úrovně PL pro bezpečnostní funkci nebo zvolený subsystém

2.6 Výstupní zpráva SISTEMA Report

Posledním krokem je vytvoření samotného SISTEMA Reportu. Report je ucelenou zprávou, které obsahuje všechny podstatné informace – základní projektové údaje, seznam bezpečnostních funkcí včetně požadované a dosažené úrovně PL, seznam použitých prvků a jejich parametrizace. Bezpečnostní funkce mají na základě splnění požadavků status „green“ nebo „red“. Ve speciálních případech, například pokud některé z použitých zařízení má deklarovanou životnost nižší než je standardní výpočetní doba pro bezpečnostní funkce (20 let), má bezpečnostní funkce status „yellow“.

Detailní report mívá rozsah desítek stran. Základní shrnutí o tom, zda bezpečnostní systémy splňují požadavky, je na první straně reportu. Zpráva je generována ve formátu PDF a na konci vyžaduje podpis autora a osoby provádějící nezávislou kontrolu. Zprávu je možné generovat v anglickém nebo německém jazyce.

3 Závěr

Z pohledu autora i příjemce zprávy vytvořené v softwaru SISTEMA, která prokazuje úroveň funkční bezpečnosti dle normy ČSN EN ISO 13849-1, je tento softwarový nástroj jednoznačným přínosem z následujících důvodů:

- systematicky vede zadávání parametrů,
- kontroluje vyplněnost požadovaných údajů,
- počítá výsledné ukazatele jednotlivých prvků i celého systému,
- porovnává dosažené a požadované parametry,
- vytvoří strukturovanou zprávu.

Na druhou stranu je třeba upozornit, že samotný software není výukovou pomůckou a při jeho používání je třeba mít zažité principy a postupy funkční bezpečnosti specifikované v normě. Samozřejmostí musí také být detailní seznámení s analyzovaným systémem a jeho dokumentací.

Použitá literatura

[1] ČSN EN ISO 13849-1:2006 *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci.*

ISBN ISBN 978-80-02-02783-6

Funkční bezpečnost - Normy a řešení v praxi
Sborník přednášek
kolektiv autorů
1. vydání
rok vydání 2018, Česká společnost pro jakost
vazba brožovaná, 32 stran