VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
FACULTY OF MECHANICAL ENGINEERING

ÚSTAV VÝROBNÍCH STROJŮ, SYSTÉMŮ A ROBOTIKY
INSTITUTE OF PRODUCTION MACHINES, SYSTEMS AND ROBOTICS

METODIKA VÝVOJE A VALIDACE SOFTWARU PRO BEZPEČNOSTNÍ ČÁSTI ŘÍDICÍCH SYSTÉMŮ V DIVADELNÍ TECHNICE

METHODOLOGY DEVELOPMENT AND VALIDATION OF SOFTWARE FOR SAFETY-RELATED PARTS OF CONTROL SYSTEMS IN THEATER TECHNIQUE

DIZERTAČNÍ PRÁCE
DOCTORAL THESIS

AUTOR PRÁCE
AUTHOR

Ing. Michal Drlík

ŠKOLITEL
SUPERVISOR

doc. Ing. Petr Blecha Ph.D.

BRNO 2019

ABSTRAKT

Předložená práce nejdříve popisuje, co je to divadlo a jaké typy mechanismů se v divadle nacházejí. Následně je problematika jevištních strojně technických mechanismů uvedena do kontextu české, potažmo evropské legislativy s důrazem na použití technických norem, které jsou nutné splnit, aby bylo tohoto cíle dosaženo. V další části je proveden rozbor řídicích systémů, které se používají v jevištní technice s důrazem na funkčnost těchto systémů, neboť ta následně určuje počet a rozsah možných nebezpečí a nebezpečných událostí. Tato nebezpečí jsou poté podrobně vyjmenována a specifikována, čímž je kladen důraz na jejich existenci, závažnost a nutnost řešení. Je také nastíněno řešení, že tyto nebezpečí a nebezpečné události jsou v mnoha případech řešitelné použitím programovatelných systémů souvisejících s bezpečností, potažmo bezpečnostních funkcí realizovaných těmito funkcemi. Jednotlivé kroky jsou popsány do V-modelu s patřičnými dokumenty každého z kroků V-modelu. Výsledkem této práce bude navržený model metody vývoje a validace softwaru pro programovatelné a řídicí systémy v divadelní technologii.

KLÍČOVÁ SLOVA

software, jeviště, strojní zařízení, úroveň integrity bezpečnosti, SIL, životní cyklus bezpečnosti softwaru, validace, funkční bezpečnost, bezpečnostní funkce, nouzové zastavení, bezpečnostně instrumentovaná funkce

KEYWORDS

software, stage, machinery, safety integrity level, SIL, safety software life cycle, validation, functional safety, safety function, emergency stop, safety instrumented function

OBSAH

1 ÚVOD

Bezpečnost v divadelní technice je v posledních letech stále více diskutovanou záležitostí. Jevištní prostor je místo, kde se nepohybují pouze herci, ale také další obslužný personál, jako jsou např. strojní technici divadelní technologie, inspicient, osvětlovací technici a další.

Na jevištní scéně jsou tvořeny různé triky a vizuální efekty pomocí kulis, osvětlení a audiovizuální techniky a ke všem těmto aktivitám přispívají také mnohé strojní mechanismy. Všechna tato zařízení jsou důsledně z pohledu diváka skrývána. Všechny tyto efekty, pohyby, nástrahy pro herce a techniky jsou odehrávány ve tmě, aby efekt pro diváka byl co možná nejpůsobivější. Velký ohlas v posledních letech zaznamenává muzikálová scéna, která přivádí spousty mladých lidí do kulturního a divadelního světa. Tato skutečnost také přivádí na divadelní scénu spousty nových strojních zařízení, které se pohybují čím dál většími rychlostmi, mnohdy až 2 m/s. Hmotnosti kulis jsou od řádů kilogramů až do stovek kilogramů. Nároky scénografie a režisérů s rostoucími možnostmi také adekvátně rostou.

Obecně je snaha, aby veškeré pohyby se zařízeními byly předem definované a přednastavené v ovládacím pultu strojního technika. Řádně je celý postup po sobě jdoucích pohybů kontrolován a otestován v tak zvané „zkušební hře“, kde společně s režisérem divadla je celá hra vyzkoušena a odsouhlasena. V této fázi je vše uloženo a připraveno na dynamické pohyby při představení.

S tímto vrůstajícím technickým trendem a s narůstajícími požadavky vznikají mnohá nová, dříve neřešená nebezpečí. Současně se ovšem s tímto technickým pokrokem objevují možnosti, jak takováto nebezpečí technicky vyřešit. **V prostředí české divadelní scény vzniká čím dál větší potřeba tato nebezpečí pojmenovat, analyzovat a začít je řešit.**

Mnohá z nich jsou řešitelná částí řízení související s bezpečností, která jsou podchycena normou ČSN EN ISO 13849-1:2017. Menší část nebezpečí, nikoliv však významově, je ovšem nutné řešit celými komplexními systémy. Zde již uvedená norma není dostatečná a je nutné použít soubor norem ČSN EN 61508 ed.2:2011. [4]

Při důkladnějším rozboru evropské legislativy v oblasti strojně technických zařízení je stále větší důraz kladen na bezpečnost osob i majetku. Oblast divadelní techniky v tomto ohledu nezůstává pozadu, a i zde jsou promítnuty tyto požadavky. Tato oblast je svým využitím značně rozdílná, a i přestože je chápána jako podskupina strojně technických mechanismů, je natolik odlišná, že vyžaduje zcela osobitý přístup k řešení dané problematiky bezpečnosti.

V současné době technický pokrok v oblasti bezpečnosti natolik pokročil, že je možné řešit bezpečnostní funkce, které byly dříve technicky či ekonomicky neřešitelné. S ohledem na velký nárůst muzikálových scén je nutné provádět rekonstrukce stávajících divadelních a kulturních objektů a **je velmi důležité řešit**

bezpečnost osob, které se přímo pohybují pod zdvihanou technikou.

Vzhledem k tomu, že dodavatelé průmyslových komponentů doposud tuto problematiku přímo neřešili, **je nutné vyhledat řešení pro divadelní technologie taková, která by dostatečně řešila problematiku bezpečnosti, zejména realizací bezpečnostních funkcí pomocí programovatelných systémů souvisejících s bezpečností.** Jedním z takových řešení může být sestavení bezpečnostních funkcí s využitím standardního hardwaru a naprogramování vlastních bezpečnostních mechanismů. Tato práce bude popisovat metodiku a postupy jednotlivých kroků tak, aby bylo dosaženo maximální bezpečnosti v oblasti jevištní zdvihané techniky. Budou vytvořeny dokumenty s postupy pro bezpečnostní funkce.

Největším přínosem bude zvýšení bezpečnosti nejen na pracovištích v rámci kulturních objektů a jiné zábavní techniky, ale také přenesením do jiných odvětví strojírenství na mnoha dalších pracovištích se zcela jiným zaměřením. **Bezpečnost jako taková by měla být a je jedním z prvních faktorů, kterými se zabývají technici celého světa a žádná z technických či ekonomických kritérií by neměla být překážkou při volbě tak důležité části, jako je zabezpečení lidského života a zdraví.**

2 DIVADELNÍ PROSTOR

Hlediště určuje prostor, kde sedí diváci. Diváci zpravidla nejsou v přímém ohrožení s pohybujícím se zařízením.

V prostoru jeviště jsou instalovány pohonné mechanismy v horní i dolní části. V jevištním prostoru se pohybují pouze herci a osoby znalé tohoto prostředí a jsou v přímém ohrožení pohybujícími se zařízeními. Na Obr. 1 jsou znázorněny zařízení, se kterými se dostanou herci do kontaktu v průběhu představení.

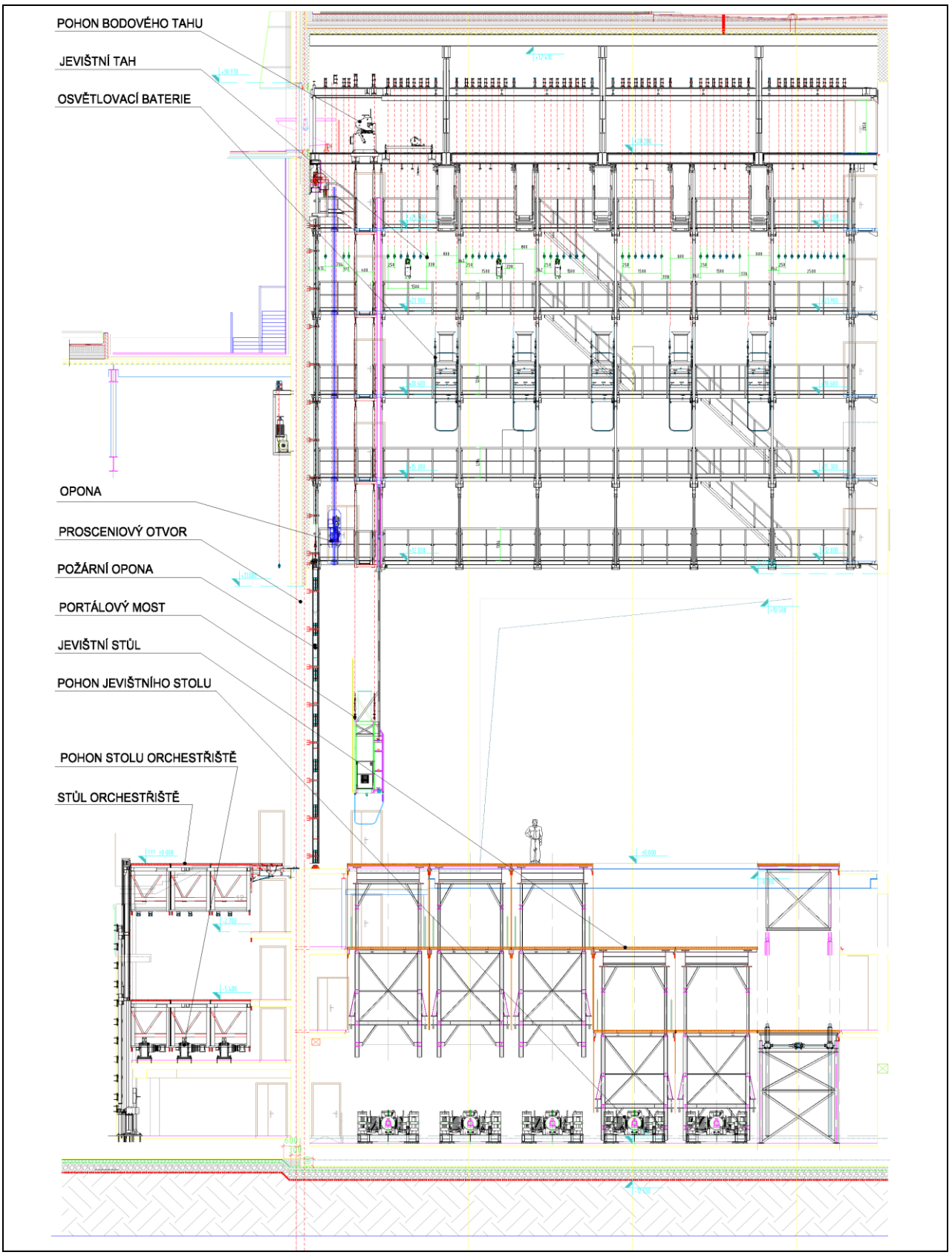
Provaziště je prostor nad herci, kde jsou instalovány pohonné mechanismy horní části jeviště.

Divadelní prostor je rozdělen do tří skupin:

- hlediště,
- jeviště,
- provaziště.

2.1 HLAVNÍ SCÉNA – JEVIŠTĚ

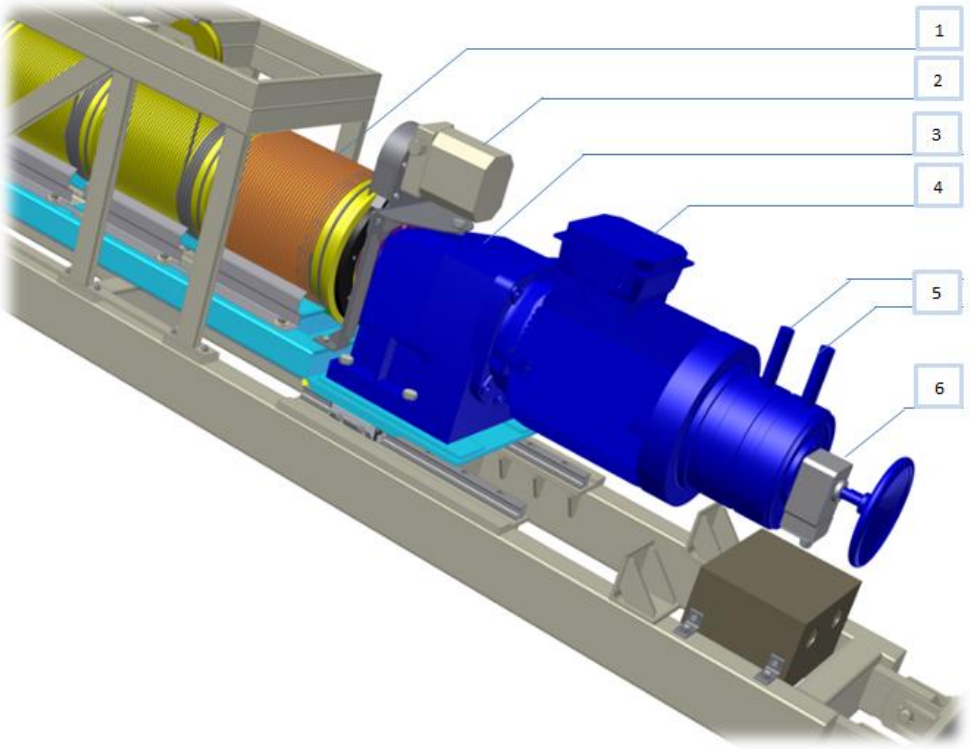
Hlavní scénu jeviště tvoří prostor, kde se pohybují výhradně herci. Z pravidla se jedná o prostor 20x20m. Jeviště je složeno z horní a dolní části. Na horní i dolní části jeviště jsou umístěny pohonné jednotky se zdvihacími mechanismy. Pohonné jednotky horní a dolní části fungují na podobném principu znázorněné na Obr. 2. Jedná se vždy o motor s elektromechanickou dvojitou brzdou, dále převodovkou, na kterou je připevněný lanový naviják. Na hřídeli motoru je připevněný hybridní absolutní snímač s inkrementální a absolutní stopou (IRC + ARC), který snímá krajní polohy zdvihu a aktuální polohu zavěšeného břemene. Hybridní snímač převádí úhel natočení na odpovídající elektrickou digitální informaci v Grayově kódu pomocí fotoelektrického snímání. Hybridní absolutní snímač je vybaven elektronikou s pamětí a díky tomu neztrácí informaci o poloze, i když je bez elektrického napájení. Většina těchto snímačů má rozlišení 4096 impulzů na otáčku a jsou schopny počítat až do 4096 otáček. Toto rozlišení 4096/4096 je dostačují pro divadelní aplikace. Krajní bezpečnostní polohy zdvihu jsou snímány vřetenovým diskrétním spínačem umístěným na hřídeli lanového bubnu. Celý pohon je umístěn na odpruženém kotevním rámu, aby byla zabráněna nežádoucí vibrace soustrojí do ocelové konstrukce jeviště. Všechna zařízení horní mechanizace, která jsou níže popsaná v podkapitolách a mají různé typy použití či vzhledu. Konstrukce jednotek a provedení se nemění.



Obr. 1: Řez divadelním prostorem

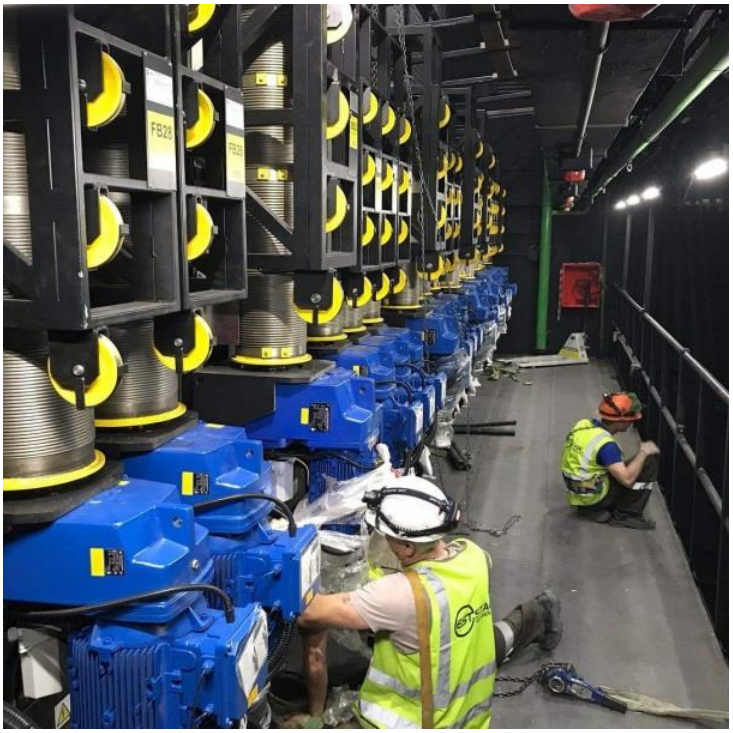
Pohonná jednotka se skládá z částí:

- lanový drážkovaný buben (1),
- elektromechanický spínač pro horní a dolní bezpečnostní polohu (2),
- převodovka (3),
- asynchronní motor (4),
- dvě elektromechanické brzdy (5),
- snímač absolutních otáček hřídele motoru (6).



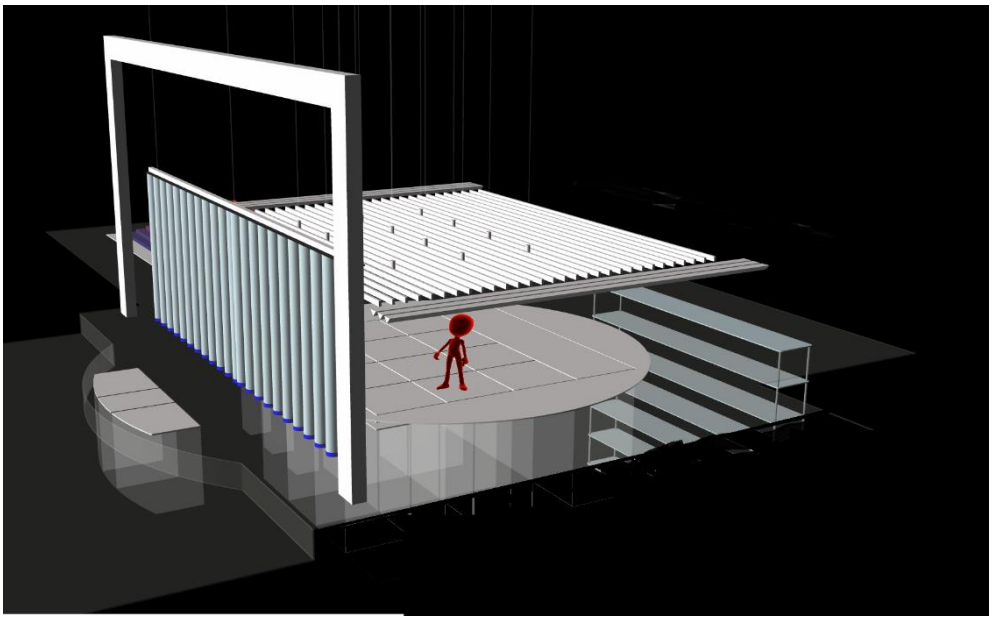
Obr. 2: Popis pohonné jednotky

V praktickém použití jsou pohonné jednotky většinou kotveny k obvodové zdi budovy, jak je znázorněno na Obr. 3. Ukotvení mechanismů do betonové konstrukce je z důvodu statického zatížení pohonných jednotek vůči stavbě. U pohonných mechanismů je umístěna obslužná lávka, pro servisní obsluhu pohonných jednotek. Veškeré zařízení v divadle prochází každý rok revizní prohlídkou, včetně zatěžkávacích zkoušek dle normy ČSN 91 8112:1993 a na základě § 4 zákona č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci a související předpisy.



Obr. 3: Pohonná jednotka divadla

Na jevišti, jak je znázorněno na Obr. 4, jsou herci vystaveni přímému nebezpečí s pohybujícími se jevištními zařízeními horní mechanizace. Zařízení pohybující se nad herci je stále kontrolováno bezpečnostními funkcemi a operátorem, který ovládá tyto zařízení.



Obr. 4: Vztah člověka a divadelní techniky

2.2 DIVADELNÍ TECHNIKA

Personál divadla tvořený herci a techniky se značnou část pracovní doby nacházejí v přímém kontaktu s technickým zařízením divadla. Zvláštní pozornost vyžadují otvory v podlaze s hloubkou přes 5 metrů, které tvoří zdvihané plošiny (stoly) Obr. 5. Na jevišti jsou zavěšené kulisy na tazích, které se pohybují během představení nad lidmi vysokou rychlostí až 1,5m/s.

Obr. 5: Jevištní stoly

Důvodem k vyřazení některých technických zařízení z oblasti působnosti strojní směrnice jsou právě se směrnicí neslučitelné podmínky provozu. Strojní směrnice má za cíl omezit právě toto vystavení nebezpečí. V divadelním prostředí toho nelze technicky dosáhnout.

2.3 OBSLUHA DIVADLA

Role strojního technika, který obsluhuje řídicí systém je klíčová. Tento člověk může pomocí ovládacích pák nebo tlačítek na ovládacím pultu spustit části zařízení do pohybů.

Strojní technik musí ovládat zařízení s opatrností, neboť:

- prostor jeviště je veliký a nepřehledný,
- v průběhu představení je na jevišti tma a není tak možné vidět na ovládané zařízení,
- počet ovládaných zařízení je velký,
- na jevišti je velký počet herců, kteří se různě pohybují pod zdvihaným zařízením,
- v průběhu představení je v jevištním prostoru velký hluk.

Bezpečný chod divadla nelze zajistit v plném rozsahu, přesto zařízení, která jsou ovládána pomocí ovládacího pultu, mají instalované bezpečnostní prvky, aby zabránily následkům úrazu či smrti. Ovládací pult je často mobilní a je možné ho umístit na okraj jevištní podlahy tak, aby bylo možné vidět na zařízení, která jsou ovládána Obr. 6.

Obr. 6: Pohled na scénu z místa obsluhy ovládacího pultu

Některé systémy ve větších divadlech umožňují připojení dvou a více pultů do jednoho řídicího systému. Při představení se na ovládání jevištních mechanismů účastní dva a více strojních techniků. Na každém z ovládacích pultů jsou povolená pouze zařízení, na která strojní technik vidí a může je bezpečně ovládat.

V divadelním prostoru budou stále hrát významnou roli zkušenosti a znalosti všech osob nacházejících se v prostoru jeviště.

3 DIVADELNÍ MECHANISMY

3.1 HORNÍ MECHANIZACE

Horní část jeviště je prostor, kde se nacházejí vlastní pohonné jednotky jednotlivých zdvihacích zařízení. Zařízení jsou zdvihána či spouštěna v tomto prostoru nad hlavami veškerého účinkujícího personálu.

3.1.1 Bodový tah

Bodový tah Obr. 7 je použit k zavěšení a zvedání dekorací v libovolném místě hlavního jeviště. Zařízení se skládá z kladek, jednoho lana, pohonné jednotky a závěsného háku.

Obr. 7: Pohonné mechanismy – bodový tah

3.1.2 **Prospektový tah**

Prospektový tah Obr. 8 je použit k zavěšení a zvedání dekorací v libovolném místě hlavního jeviště. Zařízení se skládá z kladek, lan, pohonné jednotky a závěsné tyče. Prospektová tyč je z pravidla dlouhá jako celá šířka jeviště. Jako závěs pro zdvih břemene je nejčastěji použito 5 nebo 6 lan.

Obr. 8: Pohonné mechanismy – prospektový tah

3.2 DOLNÍ MECHANIZACE

U dolní mechanizace se zařízení převážně pohybují horizontálně. U dolní části jeviště jsou od sebe typy zařízení natolik rozdílná, že při konstrukci a návrhu potřebují speciální přístup konstruktéra. V dolní části jsou odlišná nebezpečí, kde se personál a účinkující pohybují na zařízeních, a to často i za pohybu. Dolní část jeviště je tvořena podlahou, která je rozčleněna na několik segmentů. Tyto segmenty mohou být zdvihány v rozsahu většinou +/- 4 m. Celá část jeviště může být zároveň otočná. Legislativa v tomto prostředí je poměrně složitá. Zařízení jevištní technologie můžeme z části považovat jako strojní zařízení.

3.2.1 Jevištní stůl

Jevištní stoly obvykle tvoří kompletní podlahu jeviště Obr. 9. Podlaha je tak multifunkční a je možné jí tvarovat do různých schodů dle požadavků scénografů. Zpravidla tato zařízení mají vlastní hmotnost několik tun a požadavek na jejich provozní zatížení je rovněž několik tun.

Obr. 9: Pohonné mechanismy – jevištní stoly

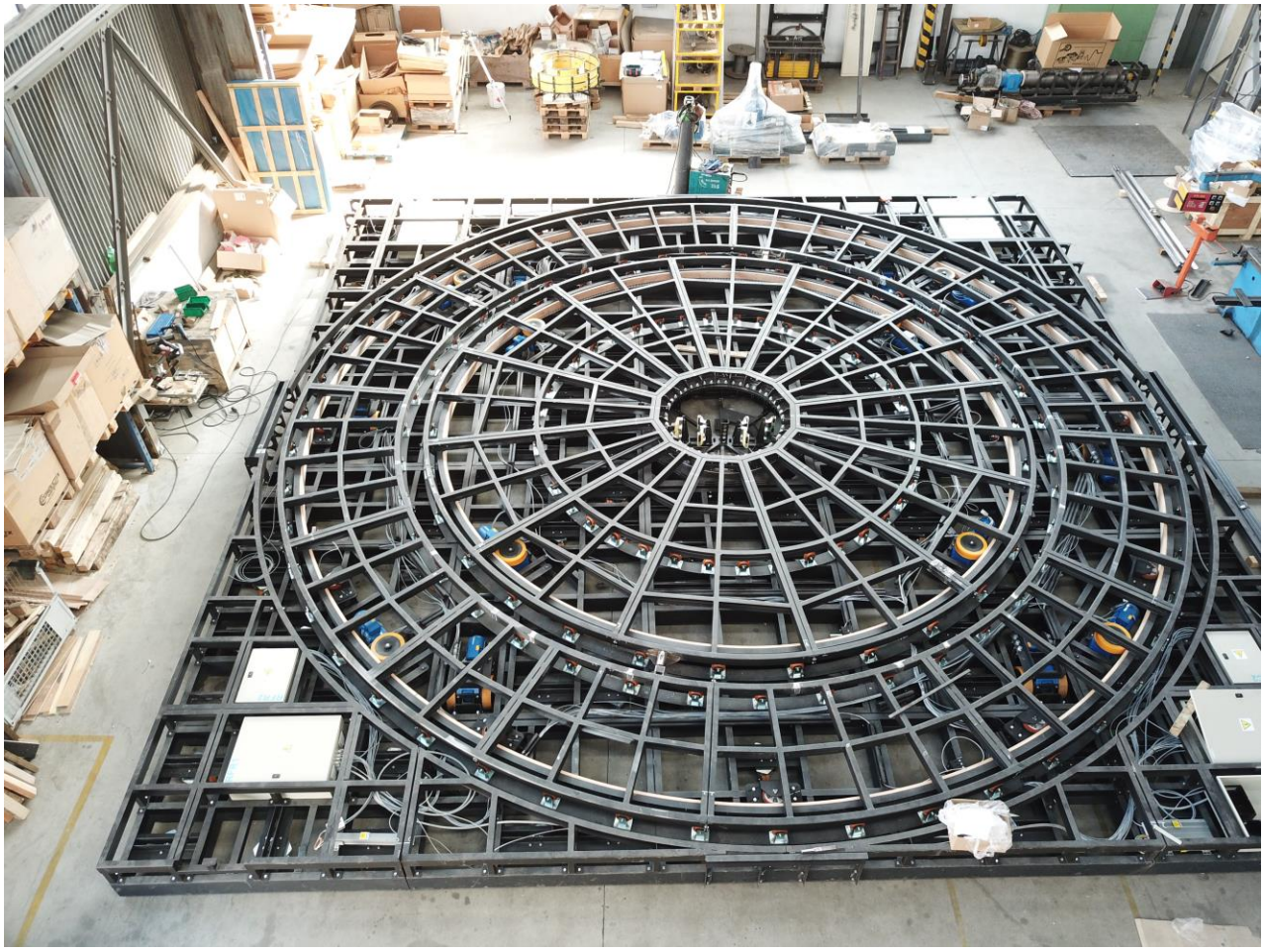
3.2.2 Nájezdový vůz

Nájezdové vozy Obr. 10 jsou určeny pro rychlou výměnu dekorací, a to i na otevřené scéně. Na vůz lze postavit kompletní dekoraci a vyvézt ji na scénu z bočního prostoru jeviště během představení. Vozy z pravého a levého bočního jeviště se mohou vzájemně střídat na scéně. S vozy lze vytvářet dynamické akce rychlostí až 0,3 m/s. Nájezdové vozy lze používat nezávisle nebo v synchronním režimu. U těchto typů zařízení je velmi složité řešení bezpečnosti, protože se jedná o velmi těžkou plošinu, která se posouvá horizontálně po jevišti a svým pohybem může srazit osoby pohybující se na jevišti.

Obr. 10: Pohonné mechanismy – nájezdové vozy

3.2.3 **Točna**

Divadelní točna Obr. 11 je tvořena kruhovým výřezem do podlahy jevištního prostoru. Kruh točny bývá z pravidla velký stejně jako prostor jeviště. V tomto mechanismu jsou také osoby pohybující se na jevišti vystavovány nebezpečí. V případě umístěné kulisy na pohyblivé části točny, může být osoba zasažena pohybujícím se předmětem. Točna má z pravidla obvodovou rychlost až 1 m/s.



Obr. 11: Pohonné mechanismy – divadelní točna

4 LEGISLATIVNÍ RÁMEC PRO DIVADLA A KULTURNÍ OBJEKTY

Oblast divadelních technologií reguluje velké množství Evropských směrnic a harmonizovaných i neharmonizovaných norem.

4.1 ZÁKON Č. 22/1997 SB. – TECHNICKÉ POŽADAVKY NA VÝROBKY

Zákon č. 22/1997 Sb. popisuje:

- způsob stanovování technických požadavků na výrobky, které by mohly ve zvýšené míře ohrozit zdraví nebo bezpečnost osob,
- práva a povinnosti osob, které uvádějí na trh, distribuují nebo uvádějí do provozu výrobky,
- práva a povinnosti osob pověřených k činnostem podle tohoto zákona, které souvisí s tvorbou a uplatňováním českých technických norem nebo se státním zkušebnictvím,
- způsob zajištění informačních povinností souvisejících s tvorbou technických předpisů a technických norem, vyplývajících z mezinárodních smluv a požadavků práva Evropských společenství. [6]

4.2 STROJNÍ SMĚRNICE 2006/42/ES PRO STROJNÍ ZAŘÍZENÍ

Tato strojní směrnice popisuje strojní zařízení v oblasti průmyslu, kam obecně spadají i divadelní mechanismy, nicméně vyjímá takové mechanismy, které jsou v přímém kontaktu s účinkujícími.

Směrnice je známá pod zkratkou MD – Machinery Directive.

Na směrnici 2006/42/ES se vztahují:

- strojní zařízení,
- vyměnitelná přídavná zařízení,
- bezpečnostní součásti,
- příslušenství pro zdvihání,
- řetězy, lana a popruhy,
- snímatelná mechanická převodová zařízení,
- neúplná strojní zařízení.

Z této směrnice jsou vyjmuty:

- strojní zařízení divadelní techniky určená k přesunu účinkujících během představení,
- zbraně a střelné zbraně,
- zařízení používaná na výstavištích,
- zábavní atrakce v zábavních parcích,
- zařízení určená pro vojenské, policejní a výzkumné účely.

Při konstruování jednotlivých zařízení v divadlech nastává komplikace při určování typu zařízení. V době, kdy byla platná směrnice 98/37/ES byly z ní vyjmuty všechny „divadelní zdviže“. S platností směrnice 2006/42/ES jsou vyjmuty pouze „strojní zařízení divadelní techniky určená k přesunu účinkujících během představení“. Dále je tedy nutné postupovat při posuzování shody podle obecné bezpečnosti. V praxi jsou všechna zařízení řízena stejným řídicím systémem. Z pravidla postupujeme dle bezpečnostních kritérií tak, jako by se jednalo o strojní zařízení s výjimkou nebezpečí, která vyplývají z divadelního prostředí. [8]

4.3 SMĚRNICE 2011/65/EU ROHS O OMEZENÍ NEBEZPEČNÝCH LÁTEK V ELEKTRONICE

Cílem směrnice 2011/65/EU je omezit používání některých nebezpečných látek při výrobě elektrických a elektronických zařízeních pro široké odborné i laické používání, a tím přispět k ochraně lidského zdraví a životního prostředí (RoHS 2). Tato směrnice nahrazuje a rozšiřuje původní směrnici 2002/95/ES, která byla zrušena v roce 2013 (RoHS). Vzhledem k tomu, že systém divadelní technologie je specifický například při výrobě ovládacích pultů, které jsou dílensky vyráběné na zakázku, je důležité myslet i na směrnici RoHS. Může se týkat i 3D tisku některých pomocných komponentů. [11]

Směrnice se vztahuje na:

- velké spotřebiče pro domácnost,
- malé spotřebiče pro domácnost,
- zařízení informačních technologií a telekomunikačních zařízení,
- spotřební elektroniku,
- osvětlovací zařízení,
- elektrické a elektronické nástroje,
- hračky, vybavení pro volný čas a sport,
- zdravotnické prostředky,
- monitorovací a kontrolní přístroje, včetně průmyslových,

4.4 SMĚRNICE 2014/30/EU ELEKTROMAGNETICKÉ KOMPATIBILITY

Tato směrnice stanoví požadavky na elektromagnetickou kompatibilitu zařízení. Jejím cílem je zajistit fungování vnitřního trhu tím, že vyžaduje, aby zařízení byla v souladu s přiměřeným stupněm elektromagnetické kompatibility. Směrnice je známá pod zkratkou EMC /Electromagnetic Compatibility/.

Směrnice elektromagnetické kompatibility hraje nedílnou roli v oblasti funkční bezpečnosti. Dopad EMC je jasně zmíněn v normách funkční bezpečnosti a normách platných pro divadelní, popřípadě strojní zařízení.

Pro prokázání shody je nutné provedení typových zkoušek EMC u typových rozvaděčů. Zkoušky jsou prováděny v oblastech vyzařování a odolnosti. Na odolnost je kladen zvláštní důraz vzhledem k výkonu a požadavkům na funkcionalitu bezpečnostního systému. Při posuzování vyzařování a odolnosti se postupuje podle požadavků, které jsou stanoveny pro průmysl, nikoliv pro domácnosti. [9]

4.5 SMĚRNICE 2014/35/EU PRO ELEKTRICKÁ ZAŘÍZENÍ NÍZKÉHO NAPĚTÍ

Tato směrnice se vztahuje na elektrická zařízení určená pro použití v rozsahu jmenovitých napětí pro střídavý proud od 50 V do 1 000 V a pro stejnosměrný proud od 75 V do 1 500 V. Směrnice je známá pod zkratkou LVD /Low Voltage Directive/.

Pokud má být elektrické zařízení uvedeno na trh, musí splnit technické požadavky. Splnění technických požadavků se prokazuje posouzením shody. Dále musí být vyrobeno v souladu se správnou praxí z hlediska technické bezpečnosti a nesmí ohrozit bezpečnost a zdraví osob, domácích zvířat ani majetku.

Postupem posouzení shody u elektrického zařízení je interní řízení výroby. Výrobce vyhotoví technickou dokumentaci, dohlíží nad výrobou, vydá prohlášení o shodě a výrobek opatří označením CE. Výrobce na vlastní odpovědnost prohlašuje a zaručuje, že elektrická zařízení splňují všechny požadavky tohoto nařízení. [10]

4.6 OSTATNÍ LEGISLATIVNÍ POŽADAVKY

4.6.1 Vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti

V oblasti divadelní techniky se nacházejí i zařízení, určená ke speciálním funkcím. Mezi taková zařízení patří požární opony a dýmové klapky. Tato zařízení omezují šíření plamene, případně regulují kouř daným směrem. V těchto případech je nutné zvažovat i legislativu vztahující se k požadavkům v případě požárů. Na tomto místě je nutné zmínit Vyhlášku č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru. Tato vyhláška mimo jiné definuje:

- požární bezpečnost,
- požární techniku,
- požárně bezpečnostní zařízení.

4.6.2 Směrnice 2009/104/ES o požadavcích na bezpečnost a ochranu zdraví

Při konstrukci divadelní techniky je bráno v úvahu, jakým způsobem dané zařízení bude provozováno. Toto nařízení vlády stanovuje základní požadavky pro bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí. Pro účely tohoto nařízení jsou definovány zejména tyto pojmy:

- používání zařízení,
- nebezpečný prostor,
- ochranné zařízení,
- obsluha,
- průvodní dokumentace,
- provozní dokumentace,
- místní provozní bezpečnostní předpis,
- normová hodnota.

Řídicí systém divadelní techniky je pro každé divadlo zpracován individuálně. V každém divadle jsou různé druhy a počty zařízení. Vždy je vypracován návod na obsluhu a údržbu. Ke každé takové realizované zakázce je zpracována průvodní dokumentace pro sestavení zařízení. Dále je vytvořena provozní dokumentace pro provozovatele technologického zařízení. Tyto náležitosti popisuje směrnice 2009/104/ES.

4.6.3 Směrnice 2012/19/EU o odpadních elektrických a elektronických zařízení

Vzhledem k rostoucí produkci a spotřebě elektrických a elektronických zařízení vzniká potřeba chránit životní prostředí před tímto druhem odpadu. Běžný způsob zpracování komunálního odpadu není dostačující při likvidaci látek obsažených v zařízeních. Elektrozařízení obsahují nevhodné, nebezpečné i vzácné látky pro životní prostředí. Druhým důvodem je tedy získání druhotných surovin.

Řešením je zavedení odděleného systému sběru elektroodpadů a vybudování recyklačních linek. Směrnice kromě tohoto řeší i cílové kvóty elektroodpadu předaného k recyklaci a problematiku kolem transportu elektroodpadu.

Nové znění z roku 2012 zásadním způsobem mění jak předepsané procento recyklovaného elektroodpadu, tak i rozsah elektrických a elektronických zařízení, na které se nejpozději od 15. 8. 2018 vztahuje. Pro velkou komplikovanost se podobně jako v původní verzi nesledují konkrétní látky, ale bere se prostá hmotnost elektropřístrojů.

Směrnice je známá pod zkratkou WEEE Directive /The Waste Electrical and Electronic Equipment Directive/. V české legislativě je používána zkratka OEEZ – odpadní elektrická a elektronická zařízení.

Namísto dosavadního cíle separovaného 4 kg elektroodpadu na obyvatele daného státu má členský stát EU od 1. 1. 2019 prokazovat splnění cílů sběrem buď 85% elektroodpadu vyprodukovaného na svém území nebo 65% hmotnosti veškerého elektrického a elektronického zařízení uvedeného v členské zemi na trh (tedy vyrobeného i dovezeného) v ročním průměru za poslední tři roky.

Na rozdíl od předchozí verze, která znamenala především vykazování elektroodpadů ze zařízení pro občanské použití se měnily nejen vykazované kategorie, ale především se zahrnuje daleko větší počet elektrozařízení pro profesionální a průmyslové použití. Například i antény a anténní kabely k nim, RFID čipy, náplně do tiskáren, pokud mají elektronické obvody a další. [12]

5 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Řídicí systém divadelní techniky je pro každé divadlo zpracován individuálně. Každá divadelní scéna obsahuje různý počet zařízení horní i dolní mechaniky. Na každý nový projekt vzniká projektová studie a design jeviště. V rámci analýzy rizik vyplynou požadavky na funkční bezpečnost a ta se dělí na jednoduché SRP/CS /Safety – related Part of a Control System/ respektující kategorie zapojení a složité SRP/CS.

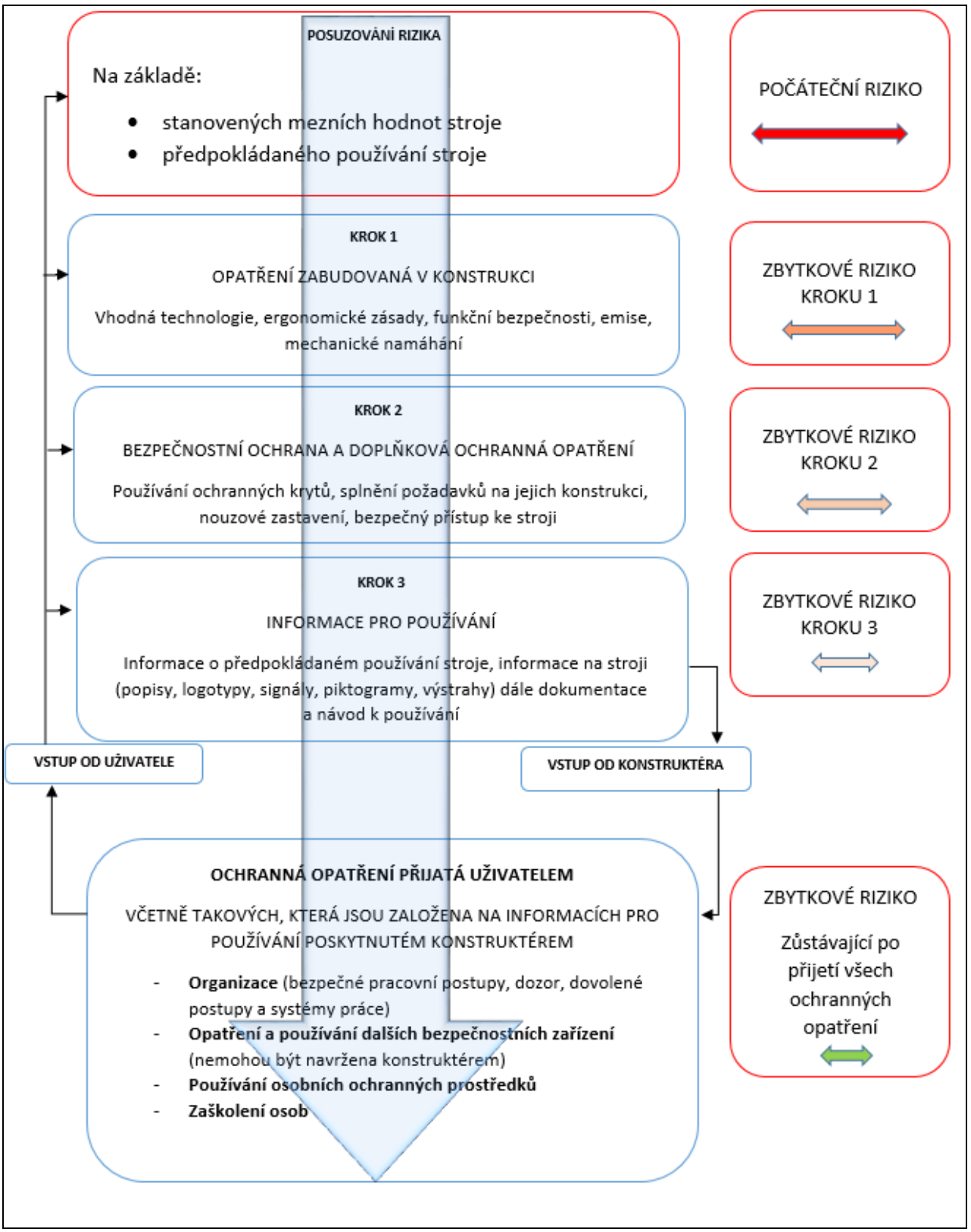
Bezpečnost divadelní techniky je posuzována jako obecné strojní zařízení. Posuzování rizik bezpečnosti strojních zařízení, potažmo samotného řídicího systému se řeší po dvou liniích. První linie aplikace normy ČSN EN 62061:2005 není použitelná pro neelektrické komponenty, jako je hydraulika, pneumatika, mechanika. Druhá linie aplikace normy ČSN EN ISO 13849-1:2017 je použitelná i na jiné oblasti včetně hydraulické, pneumatické a mechanické. Při realizaci je nutné zhodnotit obě dvě normy s ohledem na jejich vymezenou aplikovatelnost. [5]

5.1 POSUZOVÁNÍ BEZPEČNOSTI DIVADELNÍ TECHNIKY

Každý výrobce strojů je povinen provést analýzu rizik a konstrukci zařízení realizovat dle výsledků posuzování a snižování rizik dle příslušné směrnice. Popřípadě může použít harmonizovanou normu ČSN EN ISO 12100:2011. Tato norma řeší kombinaci pravděpodobnosti výskytu škody a závažnosti škody. Za škodu přitom považujeme:

- fyzické zranění,
- poškození zdraví,
- poškození majetku,
- poškození životního prostředí.

Výše uvedená norma se zabývá strategií snižování rizika Obr. 12 pomocí iterační metody, která se skládá ze tří kroků. [13]



Obr. 12: Snižování rizika podle normy ČSN EN ISO 12100:2011

5.2 FUNKČNÍ BEZPEČNOST DIVADELNÍ TECHNIKY

Vzhledem ke složitosti řídicího systému divadelní techniky je nezbytné postupovat v souladu s harmonizovanou normou ČSN EN 62061:2005, která třídí do úrovní integrity bezpečnosti SIL (Safety Integrity Level). Pro oblast strojních zařízení norma definuje tři úrovně SIL1 – SIL3, kde SIL1 představuje nejnižší a SIL3 nejvyšší úroveň. Tato norma je poměrně propracovaná a je možné ji použít do všech elektrických systémů. Norma ČSN EN 62061:2005 používá obdobné metody pro návrh jako norma ČSN EN 61508-1 ed.2:2011 až ČSN EN 61508-7 ed.2:2011, která ovšem nepodléhá harmonizaci a na management funkční bezpečnosti řídicích systémů se dívá mnohem důkladněji. Norma ČSN EN 62061:2005 je určena pro správné sestavení elektrických komponent, které jsou již certifikovány v dané integritě bezpečnosti anebo pokud nejsou, jedná se o funkční celky jako součásti daného subsystému nebo systému. Jde tedy o správné sestavení potřebné bezpečnostní funkce stroje tak, aby splňovala bezpečnostní integritu navržené úrovně. ČSN EN 61508:2011 je spíše určena pro výrobce bezpečnostních komponent, které se podle ČSN EN 62061:2005 sestavují. V předmluvě ČSN EN 62061:2005 je napsané, že patří do oblasti norem pro strojní zařízení v rámci ČSN EN 61508. Tento soubor norem s názvem „Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností“ se dělí do sedmi částí od všeobecné části, přes hardware a software požadavky až po pokyny pro použití a přehled technik a opatření k naplnění účelu normy. Mezinárodní norma je také převzata do evropské legislativy pod stejným číselným kódem se značením EN, tedy EN 61508-1 ed.2:2011 až EN 61508-7 ed.2:2011. Jednotlivé členské státy pak přejímají tyto normy se svým národním označením, např. v ČR ji najdeme jako ČSN EN 61508:2011, v Německu jako DIN EN 61508, apod.

Soubor norem popisuje životní cyklus celkové bezpečnosti. Přes počáteční kritiku, která se týkala velké dokumentační náročnosti, která z tohoto souboru vyplývá, si celý soubor postupně získal mezinárodní podporu z mnoha oblastí průmyslu a je považován za velký pokrok v technice. Důkazem je i derivát této normy v podobě funkční bezpečnosti přímo pro strojní zařízení ČSN EN 62061:2005. [15]

6 SHRNUTÍ STAVU VĚDY A TECHNIKY PRO ŘÍDICÍ SYSTÉMY DIVADELNÍ TECHNIKY

6.1 SPRÁVNÁ TECHNICKÁ PRAXE DLE DIN 56950-1:2012

Velká většina členských států Evropské unie má zpracovánu národní technickou normu pro divadelní techniku. V EU neexistuje harmonizovaná norma pro divadelní techniku. Také Česká Republika nemá obdobnou státní normu pro divadelní techniku, proto je nezbytné stanovit správnou technickou praxi pomocí národní normy jiného členského státu EU. Obecně se považuje německá národní norma za jednu z nejpropracovanějších DIN 56950-1:2012 Veranstaltungstechnik – Maschinentechnische Einrichtungen – Teil 1: Sicherheitstechnische Anforderungen und Prüfung (Divadelní technologická zařízení – Strojně technická zařízení – Část 1: Bezpečnostně technické požadavky a kontrola).

Tato německá národní technická norma je přínosná proto, že definuje potenciální nebezpečí a nebezpečné události přímo z pohledu divadelní techniky. Dalším důležitým faktorem je její striktní definice bezpečnostních funkcí, které je nutné v souvislosti s řídicími systémy divadelní techniky řešit. Pro takto definované bezpečnostní funkce, které mají být řešeny pomocí programovatelných systémů souvisejících s bezpečností, pak přímo předepisuje požadovanou úroveň integrity bezpečnosti SIL3, pokud jsou požadované funkce programovatelné. To je i důvod, proč se plnění požadavků této normy zahrnuje do kontraktačních řízení i na mimoevropských trzích. [16]

6.2 PŘEDPOKLÁDANÉ BUDOUCÍ POŽADAVKY NA DIVADELNÍ TECHNIKU

Z pohledu zajištění dlouhodobé bezpečnosti divadelní techniky je nezbytné implementovat do vývoje i aktuální stav vědy a techniky vyplývající z návrhů připravovaných norem. Aktuální technická norma, která je v současnosti připomínkována, je **pr EN 17206** „ Entertainment Technology – Lifting and Load – bearing Equipment for Stages and other Production Areas within the Entertainment Industry – Specifications for general requirements (excluding aluminum and steel trusses and towers)“.

Lze předpokládat, že tato norma se může stát účinnou již koncem roku 2019.

Tento návrh normy z velké části přebírá myšlenky a cíle stanovené německou národní normou DIN 56950-1:2012 s tím, že celou problematiku ještě podstatným způsobem rozšiřuje. Již v německé normě byla zřejmá snaha o začlenění strojních zařízení, která jsou vyjmuta z působnosti strojní směrnice. Vzhledem k nemožnosti aplikovat všechna standardní bezpečností opatření známá u strojů, která jsou vzhledem k přesunu účinkujících během představení nerealizovatelná. Klasickým případem je jevištní propadlo (výtah), které v případě zajetí zdvihací plošiny pod úroveň scény vytváří nebezpečnou jámu, která se ovšem na jevišti nemůže

ohraničovat bezpečnostním zábradlím. Toto ohraničení by bránilo hereckému výkonu a celkovému scénografickému a uměleckému záměru.

Norma DIN 56950-1:2012 ztratí svoji jedinečnost uceleného standardu z oblasti divadel, neboť připravovaná norma pr EN 17206 ji nejenom plnohodnotně nahradí, ale i sjednotí pohled na jevištní mechanismy pro všechny členské státy Evropské unie.

Připravovaná technická norma pr EN 17206 přímo uvádí: „Dokument se vztahuje na strojní zařízení používaná v zábavním průmyslu, včetně strojních zařízení vyjmutých ze strojní směrnice (2006/42/EU) specificky část 1, odstavec 2j, která vyjímá strojní zařízení divadelní techniky určená k přesunu účinkujících během představení“. [3]

Dosud není zpracován ani nikde publikován žádný metodický postup, který by specifikoval doporučený postup pro vývoj a validaci softwarových aplikací pro divadelní techniku. Tato metodika zpřehlední požadavky a povinnosti pro společnosti, které se touto problematikou zabývají.

7 CÍLE PRÁCE

Při důkladnějším rozboru evropské legislativy v oblasti strojně technických zařízení je stále větší důraz kladen na bezpečnost osob i majetku. Oblast divadelní techniky v tomto ohledu nezůstává pozadu a i zde jsou promítnuty tyto požadavky. Divadelní technika je svým využitím značně rozdílná a i přestože je chápána jako podskupina strojně technických mechanismů, je natolik odlišná, že vyžaduje zcela osobitý přístup k řešení dané problematiky bezpečnosti. V této oblasti, kde je člověk v přímém styku s řízeným strojem, může zpětně do celé skupiny strojních mechanismů přinést mnoho užitečného zejména tím, že uvede do praxe taková bezpečnostní opatření, která budou následně využitelná pro celý rámec strojních zařízení. Vzhledem k tomu, že není jednoznačně dokumentovaný postup vývoje a validace softwaru pro divadelní technologie, budou tyto dokumenty přínosné jako návod pro sestavení jednotlivých částí.

Vzhledem k výše popsanému stavu vědy a techniky byl stanoven hlavní cíl disertační práce **Metodika vývoje a validace softwaru pro bezpečnostní části řídicích systémů v divadelní technice**. Dosažení tohoto cíle bude rozděleno do následujících postupů:

- návrh metodiky vývoje a validace bezpečnostního softwaru,
- návrh dokumentace pro metodiku a validaci bezpečnostního softwaru,
- validace navržené metodiky na reálné aplikaci divadelní techniky.

8 NÁVRH METODIKY VÝVOJE A VALIDACE BEZPEČNOSTNÍHO SOFTWARU

Náklady spojené s řídicím systémem divadla, který má dosáhnout úroveň integrity bezpečnosti SIL3 jsou velmi vysoké. V tu chvíli bez velmi značných lidských, finančních a časových zdrojů nelze danou aplikaci provádět kompletně od počátku, počínaje vývojem hardwarového řešení a konče integrací softwaru a hardwaru. Bezpečnost v automatizaci je na vysoké úrovni a je možné využít komerční řešení dostupné na trhu, které poskytne následující výhody:

- certifikovaný a ověřený hardware,
- certifikovaný a ověřený komunikační protokol,
- certifikované a ověřené funkční bloky softwaru,
- certifikované softwarové (vývojové) nástroje a prostředí.

Užitím komerčního hardwaru se zjednoduší práce v určitých sekcích managementu funkční bezpečnosti, včetně verifikace vhodnosti použitých nástrojů. Budou tak splněny podmínky pro integraci softwaru na použitý hardware, testování funkčních bloků a modulů.

Softwarové nástroje jako editory bezpečnostního softwaru mají příslušnou certifikaci v oblasti funkční bezpečnosti, včetně nutných nástrojů pro řízení změn, přístupů a oprávnění.

Moderní softwarové nástroje poskytují před-certifikované funkční bloky softwaru, tyto bloky lze v daných nástrojích kombinovat za účelem tvorby sub-bloků. Pro pokročilejší aplikace je možné zvolit náročnější užití plně variabilních programovatelných jazyků jako je Safety C. Při použití plně variabilního jazyka aplikuje se celkový V-model vývoje softwaru až do spodních částí modelu v oblasti práce s kódem.

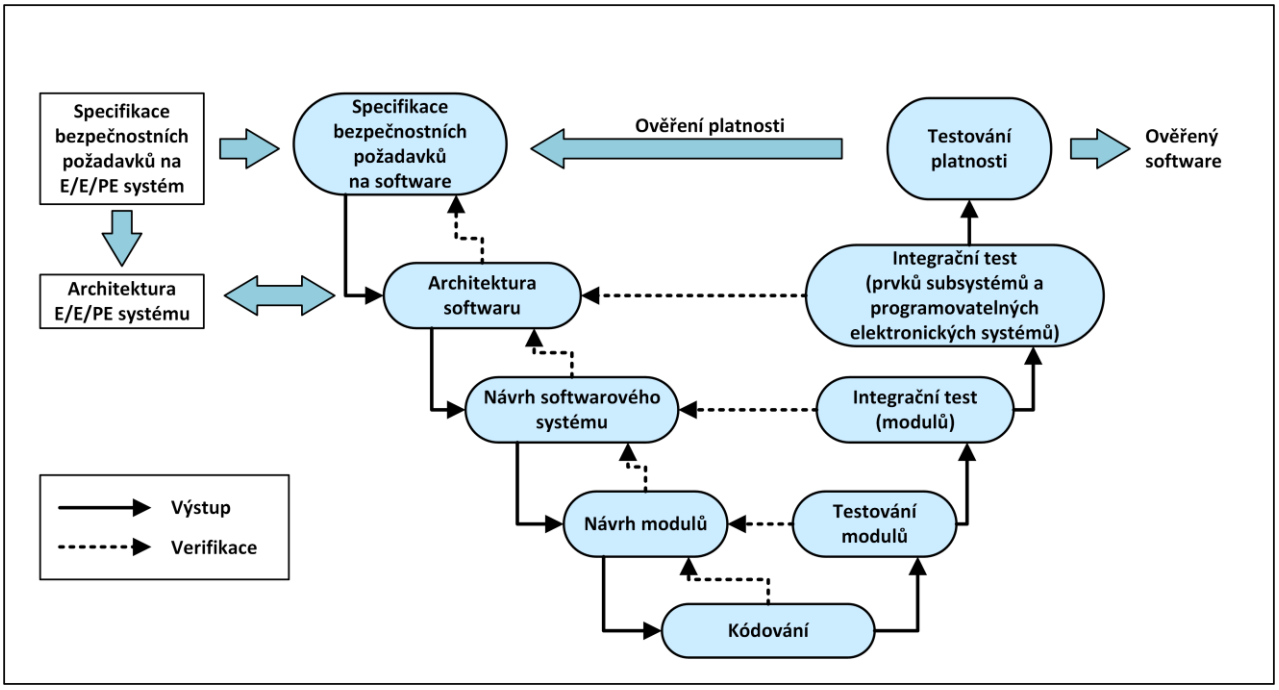
Editační softwary jsou obvykle vybaveny prostředím pro kódování s možností interaktivního odstraňování chyb a pokročilými nástroji pro simulace. Dalším nutným předpokladem jsou ověřovací mechanismy pro automatickou kontrolu shody naprogramovaného projektu s projektem exekuovaným kontrolérem.

Další velkou výhodou pro management funkční bezpečnosti a metodiku práce se softwarem jsou funkcionality pro tvorbu dokumentace a záznamů, které jsou obvyklé pro průmyslová řešení, jako řízení modifikací, přístupových práv a ověření vlastností.

8.1 V – MODEL A APLIKACE V OBLASTI DIVADEL S POUŽITÍM CERTIFIKOVANÝCH KOMPONENTŮ

V-model Obr. 13 reprezentuje standardem specifikovaný přístup k práci s funkčně bezpečným softwarem. Pro jednotlivé bloky V-modelu budou přiřazeny dokumenty.

V rámci práce s „dílčím certifikovaným průmyslovým řešením“ bude zaměřeno na horní část V-modelu Obr. 13. pro standardní aplikaci s využitím průmyslového řešení lze přístup ke kódu zcela omezit na certifikované a ověřené řešení.



Obr. 13: V-model

8.2 STRUKTURA DOKUMENTACE FUNKČNÍ BEZPEČNOSTI

Modelová struktura dokumentace funkční bezpečnosti projektu řídicího systému divadla obsahuje jak hardwarovou, tak i softwarovou část a representuje dokumentaci managementu funkční bezpečnosti divadelní technologie. Níže popsaná struktura má jednoznačné kódování, aby nedošlo k záměně jednotlivých dokumentů a jednotlivé části byly jasně identifikované pro práci ve společnosti i pro certifikační orgán.

V následujících kapitolách budou řešeny pouze ty části, které mají významný dopad na funkčně bezpečný software a jeho vývoj.

Pro přehlednost je dokumentace funkční bezpečnosti rozdělena do několika základních bloků, které jsou označeny indexem „A“. Jednotlivé bloky jsou následně číslovány od 1 s tím, že číslo bloku je formátováno na dvě číslice. V případě čísla bloku s jednou číslicí je tedy doplněna na přední pozici 0, aby tak bylo zachováno dvojčíselné označení bloku. Např. první blok je označen A.01, druhý blok A.02 a dále. Jako oddělovač mezi bloky je použitý znak tečky „.“.

Jednotlivé bloky jsou dále členěny, ale již není aplikován požadavek na dvojznakové značení. Oddělovač zůstává znak tečky. Např. blok A.02 má členění dále na A.02.1 a následující dokument bude označen například A.02.2.

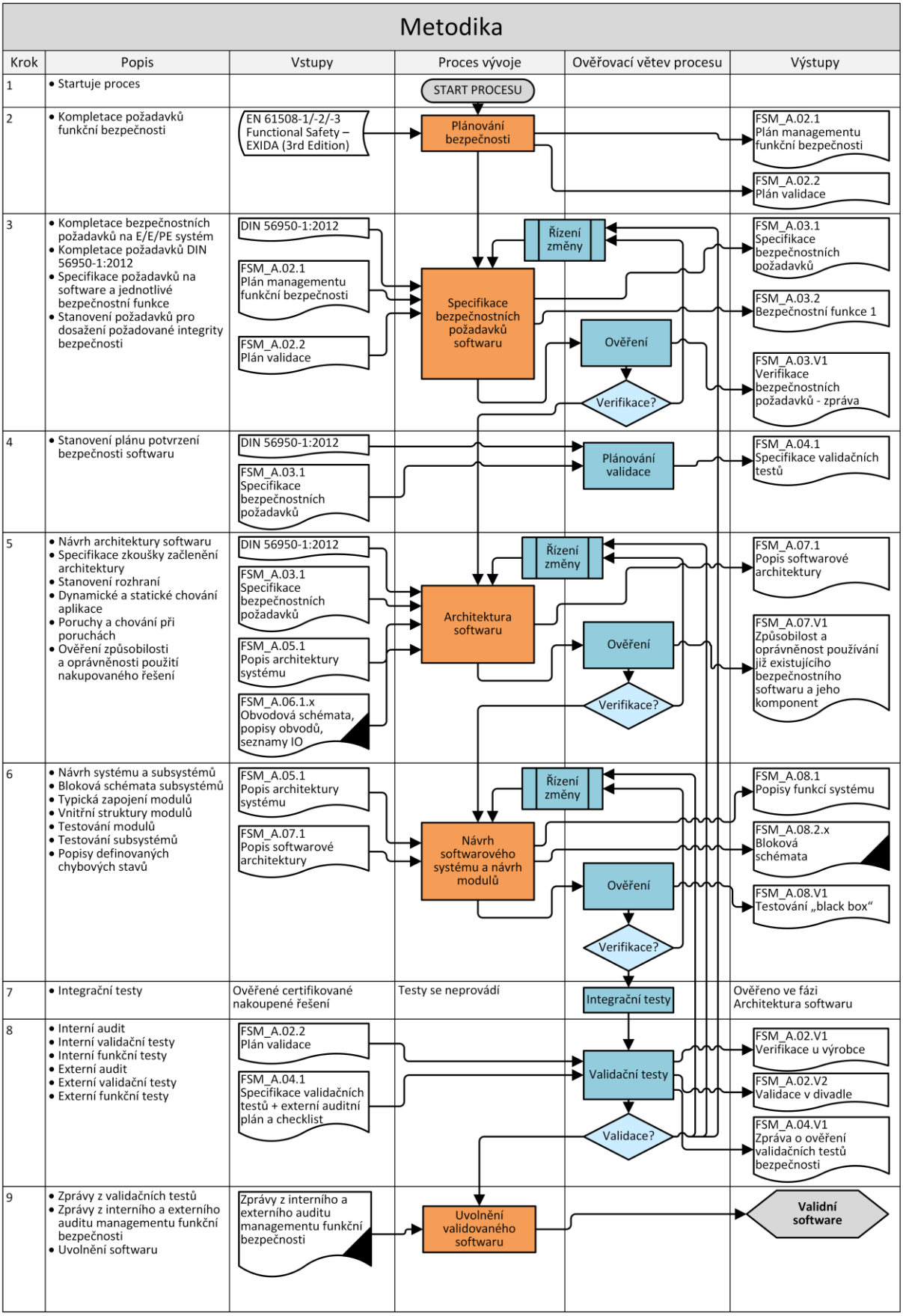
Pokud se jedná o verifikační dokument, tak je za označením daného bloku a oddělovací tečkou velké písmeno „V“ a za ním pořadové číslo. Těchto verifikačních dokumentů může být pro daný blok více. Z toho důvodu následuje za písmenem „V“ číslice s pořadím verifikačního dokumentu. Např. první verifikační dokument v bloku A.03.1 má označení A.03.1.V1 apod.

Pro celkové odlišení navržené dokumentace od vlastní práce, je před každým blokem uveden prefix „FSM“ a blok je oddělen znakem podtržítka „_“.

Dokumentace funkční bezpečnosti je do práce začleněna tak, že za číslem kapitoly dizertační práce nejdříve následuje označení bloku dokumentace funkční bezpečnosti a na dalším řádku nadpisu pak název tohoto bloku.

8.3 METODIKA VÝVOJE A VALIDACE SOFTWARU

Metodika vývoje a validace softwaru je kombinací metod vývoje softwaru se systematickým přístupem. Navržená metodika je sestavena jako seznam jednotlivých cílů a požadavků v posloupnosti, jak je definuje norma ČSN EN 61508-3 ed.2:2011. Metodický postup bude následně zpracován jako model a pro jednotlivé kroky budou vytvořeny příslušné dokumenty, popřípadě patřičné nástroje pro zrealizování. Na Obr. 14 je zobrazený postupový diagram procesu vývoje softwaru pro navrženou metodiku.



Obr. 14: Postupový diagram softwarového vývoje a validace

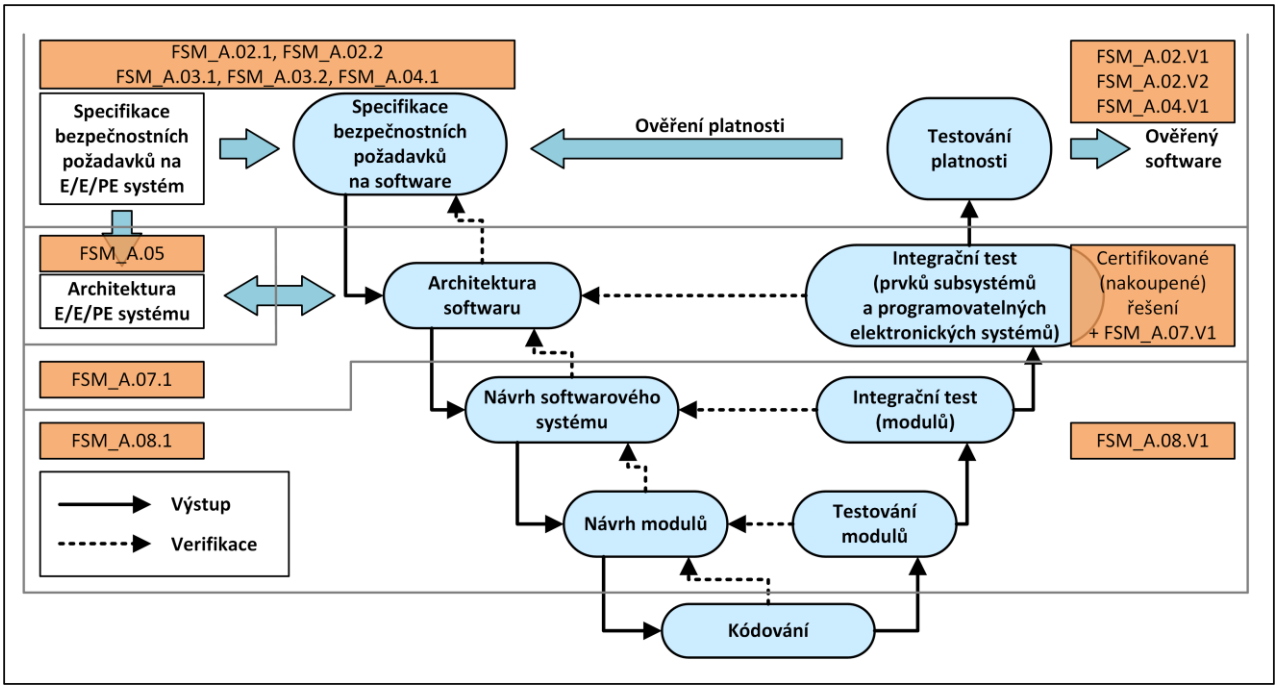
Jednotlivé kroky procesu určují posloupnost postupovým diagramem. Procesní postupový diagram se skládá z osmi následujících kroků:

- krok 1: Start procesu,
- krok 2: Kompletace požadavků funkční bezpečnosti,
- krok 3: Specifikace požadavků na software a bezpečnostní funkce,
- krok 4: Stanovení plánu potvrzení bezpečnosti softwaru,
- krok 5: Návrh architektury softwaru,
- krok 6: Návrh struktury modulů a schémat,
- krok 7: Integrační testy,
- krok 8: Interní audity, validační testy, funkční testy,
- krok 9: Zprávy z auditů, validačních testů, sestavení manuálu, uvolnění SW.

8.4 V-MODEL A VZTAH S DOKUMENTACÍ MANAGEMNTU FUNKČNÍ BEZPEČNOSTI

V-model znázorněný na Obr. 15 je doplněný o dokumenty s přímou návazností na vývoj softwaru a to plánováním, řízením požadavků a validačními testy. V-model a návaznost jednotlivých dokumentů je důležitá hlavně pro orientaci certifikačního orgánu při kontrole veškeré dokumentace.

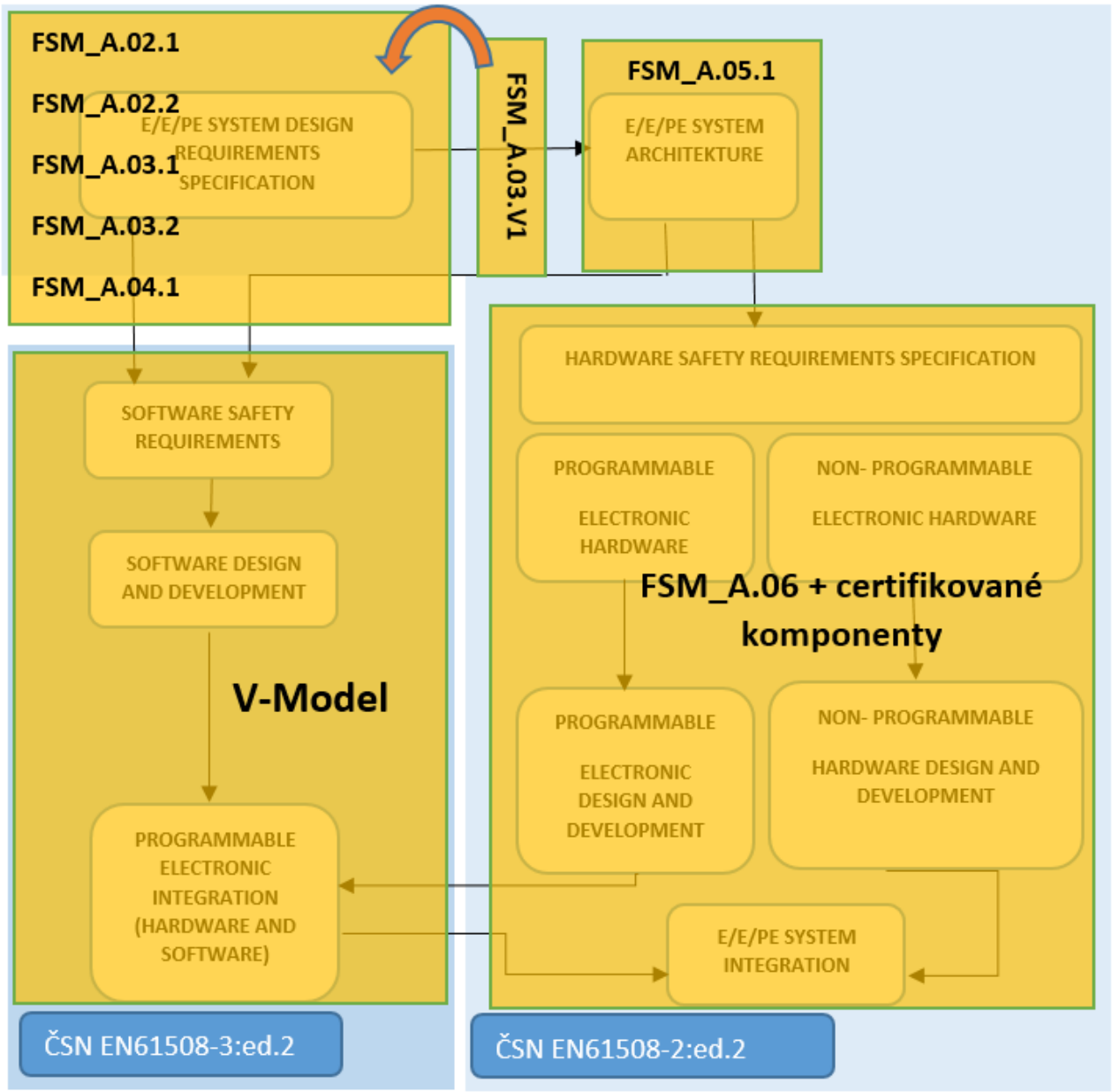
Jednotlivé dokumenty Obr. 15 reprezentují navrženou metodiku/předlohy dokumentů s doplněnými základními daty pro vývoj softwaru aplikovaného do divadelního prostředí.



Obr. 15: V-model s odkazy na jednotlivé dokumenty

Určité části jsou zastoupeny „certifikovaným řešením“. Příkladem je kódování či integrační testy softwaru na programovatelnou elektroniku, kdy již výrobce a jím dodané nástroje zajišťují správné implementace programu z připraveného prostředí na hardware, včetně jeho uložení do bezpečnostní procesorové jednotky.

Na Obr. 16 je znázorněn vztah vytvořených dokumentů a technických norem ČSN EN 61508-2 ed.2:2011 pro hardwarovou část a ČSN EN 61508-3 ed.2:2011 pro softwarovou část. Vytvořené dokumenty tak přímo navazují na jednotlivé skupiny použitých norem. [17]



Obr. 16: Vztah normy ČSN EN 61508-2 ed.2:2011 a ČSN EN 61508-3 ed.2:2011

8.4.1 Techniky a opatření softwarového vývoje

Technická norma ČSN EN 61508-3 ed.2:2011 uvádí v normativní příloze „A“ pokyny pro výběr technik a opatření při návrhu a vývoji softwaru. V jednotlivých tabulkách jsou označeny příslušné techniky jako HR, R a NR /Highly Recommended, Recommended and Positively Not Recommended/. Techniky HR jsou definovány pro danou úroveň jako velmi doporučené a jejich nepoužití je nutné zdůvodnit. Techniky R jsou označeny jako doporučené a techniky NR jsou technikami, které se pro danou úroveň integrity bezpečnosti jednoznačně nedoporučují. [18]

Tabulky jsou provedeny křížově pro jednotlivé úrovně integrity bezpečnosti, a tedy opatření, která např. nejsou nezbytná pro SIL2 jsou pro SIL3 vyžadována apod. Podle cílové úrovně integrity je tedy nutné zvolit vhodné techniky a opatření. Alternativní techniky jsou v tabulkách uvedeny pod stejným pořadovým číslem a jsou rozlišeny následným písmenem. Je to patrné z tabulky technik a opatření v položkách 1a, 1b a 1c Tab: 1. Z alternativních technik je nutné splnit jednu z požadovaných opatření. [14]

Pokyny pro výběr technik a opatření jsou rozděleny do deseti základních bloků:

- specifikace požadavků bezpečnosti softwaru,
- návrh a vývoj softwaru: architektura softwaru,
- návrh a vývoj softwaru: podpůrné prostředky a programovací jazyk,
- návrh a vývoj softwaru: podrobný návrh,
- návrh a vývoj softwaru: začlenění a zkoušení softwarových modulů,
- začlenění programovatelné elektroniky,
- potvrzení platnosti bezpečnosti softwaru,
- modifikace,
- ověření softwaru,
- odhad funkční bezpečnosti.

Z členění jednotlivých fází při vývoji softwaru od počátku až do uvolnění softwaru a z technické normy vyjmenovaných technik a opatření je zřejmá i velmi úzká provázanost mezi jednotlivými fázemi vývoje softwaru. Použitím již certifikovaného vývojového prostředí a programovacího jazyka je poměrně velké množství opatření již splněno a další nesplněná opatření jsou snadněji dostupná. Tyto opatření popisuje tabulka podrobného návrhu vývoje. V Tab: 1 jsou tři alternativní techniky, z nichž pro dosažení integrity SIL3 jsou HR pouze dvě a k těmto dvěma je v technické normě poznámka, že pokud je cílovou doménou software pro SIL3, je nutné použít 1b – polo formální metody. Certifikovaná vývojová prostředí, již mají integrovánu techniku sekvenčních diagramů a funkčních bloků, které jsou typickými zástupci polo formální metody a zbývá tedy doplnit diagramy příčin a následků a pravdivostní tabulky. [1]

Tab: 1: Návrh a vývoj softwaru: podrobný návrh [1]

Technika/opatření		Odkaz	SIL1	SIL2	SIL3	SIL4
1a	Strukturované metody	C.2.1	HR	HR	HR	HR
1b	Polo formální metody	Tab. B.7	R	HR	HR	HR
1c	Formální návrh a vylepšené metody	B.2.2, C.2.4	—	R	R	HR
2	Návrh pomocí počítače	B.3.5	R	R	HR	HR
3	Defenzivní programování	C.2.5	—	R	HR	HR
4	Modulární přístup	Tab. B.9	HR	HR	HR	HR
5	Pravidla pro návrh a kódování	C.2.6, Tab. B.1	R	HR	HR	HR
6	Strukturované programování	C.2.7	HR	HR	HR	HR
7	Použití důvěryhodných/ověřených softwarových modulů a komponent	C.2.10	R	HR	HR	HR
8	Pokročilá sledovatelnost mezi specifikací požadavků na bezpečnost softwaru a návrhem softwaru	C.2.11	R	R	HR	HR

Pozn.: Odkazy ve třetím sloupci tabulky jsou směrovány na normu ČSN EN 61508-7 ed.2:2011, která se zabývá podrobněji technikami a opatřeními

Obdobným způsobem je možné prověřit i ostatní techniky. Návrh pomocí počítače je splněn vývojovým prostředím výrobce PLC. Defenzivní programování je integrováno ve vývojovém prostředí. Pravidla pro návrh a kódování jsou výrobcem vymezena a je nutné doplnit vlastní rozšíření pro vývojový tým. Použití důvěryhodných/ověřených softwarových modulů vychází z nabídky funkčních bloků vývojového prostředí. Je nutné vytvořit sestavu nástrojů pro splnění sledování vazby mezi specifikací požadavků na bezpečnost. Dále je nutné vytvořit vlastní návrh a zavést strukturované programování, které je v tomto kontextu shodné s modulárním přístupem.

8.4.2 **Modulární přístup**

Modulární přístup je dle ČSN EN 61508-3 ed.2:2011 souborem technik a opatření, které mají vést v rámci realizace softwarového projektu k dekompozici softwarového systému do menší a lépe srozumitelných částí s cílem minimalizovat složitost systému. Modulární přístup obsahuje několik pravidel pro návrh, kódování a údržbové fáze softwarového projektu. Většina požadovaných opatření zahrnuje zejména tato pravidla (přeloženo autorem z angličtiny [2]):

- softwarový modul by měl mít jednu dobře definovanou úlohu nebo funkci, kterou bude plnit,

- propojení mezi softwarovými moduly by mělo být omezeno a jednoznačně definováno,
- měly by být vytvořeny soubory podprogramů poskytující několik úrovní softwarových modulů,
- velikost podprogramů by měla být omezena na nějakou konkrétní hodnotu, obvykle na velikost dvou až čtyř obrazovek,
- podprogramy by měly mít pouze jeden vstupní a jeden výstupní bod,
- softwarové moduly by měly komunikovat s ostatními moduly přes své interface. V případě použití globálních nebo společných proměnných, by měly být tyto proměnné dobře členěny. Přístup k nim by měl být kontrolovaný a jejich použití by mělo být odůvodněné v každé instanci,
- všechny interface softwarových modulů by měly být kompletně dokumentovány,
- každý interface softwarového modulu by měl obsahovat pouze takové parametry, které jsou nezbytné pro jeho funkci. Toto doporučení je však komplikováno možností, že programovací jazyk může povolit výchozí parametry nebo je možné použít objektově orientovaný přístup.

Podrobněji techniky a opatření pro modulární přístup popisuje tabulka B. 9 normy ČSN EN 61508-3 ed.2:2011, která je uvedena v Tab: 2.

Tab: 2: Modulární přístup [1]

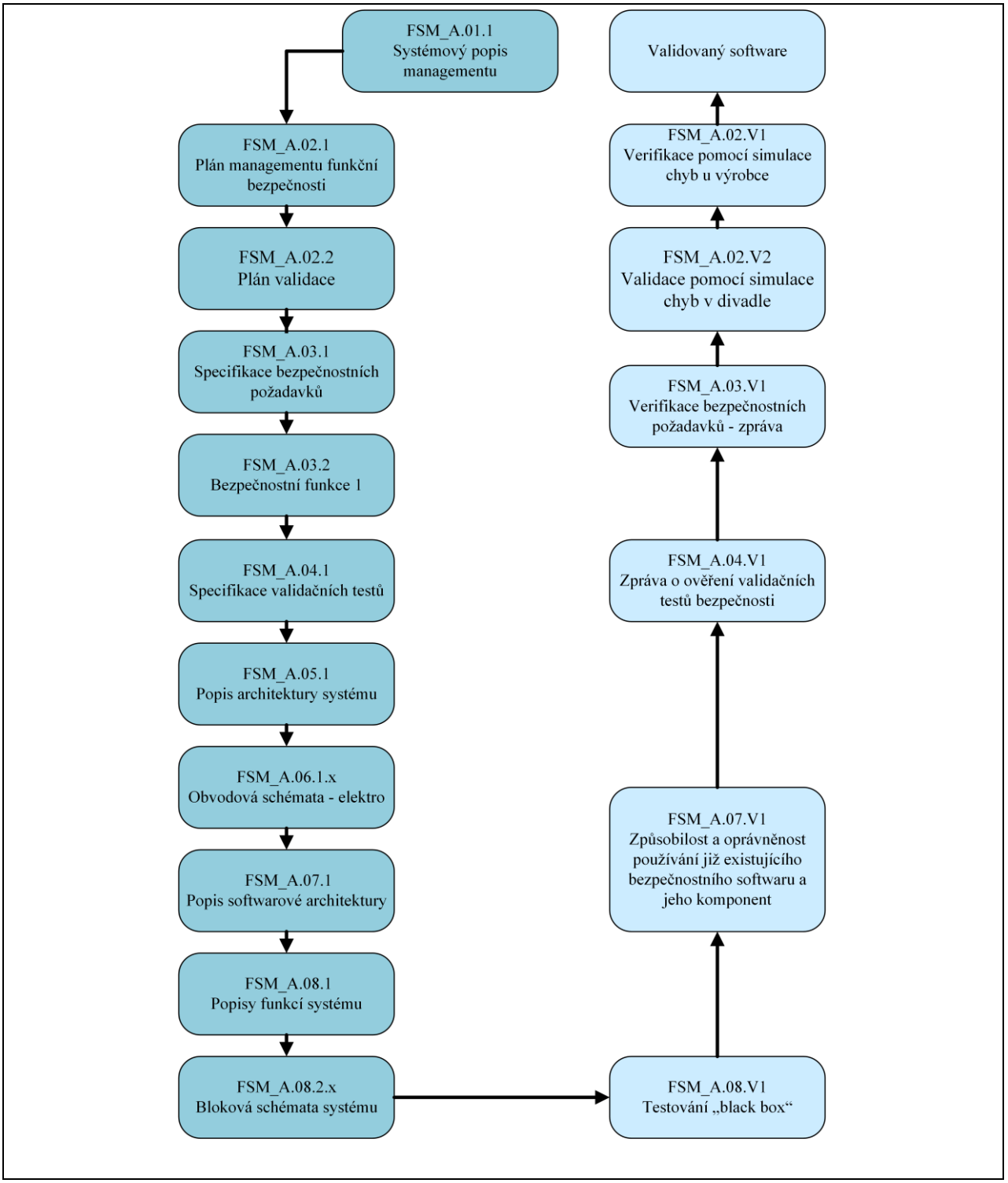
Technika/opatření		Odkaz	SIL1	SIL2	SIL3	SIL4
1	Omezení velikosti softwarových modulů	C.2.9	HR	HR	HR	HR
2	Řízení složitosti softwaru	C.5.13	R	R	HR	HR
3	Skrývání/zapouzdřování informací	C.2.8	R	HR	HR	HR
4	Omezený počet parametrů/konečný počet parametrů podprogramů	C.2.9	R	R	R	R
5	Jeden vstupní/výstupní bod u podprogramů a funkcí	C.2.9	HR	HR	HR	HR
6	Plně definovaný interface	C.2.9	HR	HR	HR	HR

Pozn.: Odkazy ve třetím sloupci tabulky jsou směrovány na normu ČSN EN 61508-7 ed.2:2011, která se zabývá podrobněji technikami a opatřeními

Při použití certifikovaného vývojového prostředí pro programování bezpečnostních aplikací lze předpokládat, že značné množství požadovaných opatření je již integrováno ve vývojovém prostředí a je tedy nutné ověřit, zda jsou požadavky integrovány a vhodným způsobem navázány na interní standardy a postupy vývojového týmu. [2]

8.5 SYSTÉMOVÝ POPIS MANAGEMENTU FUNKČNÍ BEZPEČNOSTI (FSM_A.01.1)

Systémový popis managementu funkční bezpečnosti představuje posloupný sled a návaznost jednotlivých dokumentů. Výstupem celého procesu je pak validovaný software.



Obr. 17: Systémový popis managementu funkční bezpečnosti

9 NÁVRH DOKUMENTACE PRO METODIKU A VALIDACI BEZPEČNOSTNÍHO SOFTWARU

V níže uvedených kapitolách je sestaven návrh dokumentace. Jednotlivé podnadpisy mají v závorkách název dokumentu například *(FSM_A.02.1),* vyplývající ze systémového popisu managementu funkční bezpečnosti označeného na Obr. 17.

9.1 PLÁN MANAGEMENTU FUNKČNÍ BEZPEČNOSTI (FSM_A.02.1)

Plán managementu funkční bezpečnosti je základním plánovacím dokumentem určujícím přístup k jednotlivým částem projektu, a to včetně hardwarové a softwarové části. Určuje základní požadavky a strukturu dokumentace managementu funkční bezpečnosti. Titulní list k dokumentu je v příloze pod označením Obr. 51.

Plán managementu funkční bezpečnosti popisuje proces a jednotlivé postupy používané pro návrh, verifikaci a validaci společně s údržbou řídicího systému zaměřeného na bezpečnost tak, aby tento systém řízení byl kvalifikován jako bezpečnostně orientovaný systém v souladu se souborem technických norem ČSN EN 61508 ed.2:2011. V tomto dokumentu budou specifikovány pravomoci a odpovědnosti související s managementem projektu souvisejícího s bezpečností. Tento dokument neposkytuje žádné technické požadavky nezbytné pro dosažení a udržení funkční bezpečnosti. K dosažení cíle musí být dodrženy specifikace bezpečnostních požadavků (SRS).

Tento dokument je určen výhradně pro vývojový tým v rámci projektu řídicího systému zaměřeného na bezpečnost a nepovažuje se za součást systému managementu kvality ČSN EN ISO 9001:2016, ale bude vyžívat jeho procesů a postupů. Jakékoliv použití nebo šíření mimo tento účel vyžaduje schválení vrcholovým managementem společnosti.

Plán managementu funkční bezpečnosti by měl být neustále zlepšován opakovaným přezkoumáváním a revizemi projektu po požadovaných auditech funkční bezpečnosti, což zabezpečuje:

- vedení společnosti bude objednávat audity, aby přezkoumaly plnění cílů kvality a bezpečnosti procesů,
- vývojáři a testeři budou přezkoumávat současné pracovní metody a kontext projektu a budou navrhovat jeho vylepšení,
- osoby odpovědné za management funkční bezpečnosti, budou aktualizovat dokumenty podle potřeby tak, aby odrážely nové zkušenosti.

9.1.1 Role projektu

V kapitole role projektu bude vytvořena tabulka s uvedením odpovědných pracovníků na následujícím projektu. K jednotlivým jménům bude přidělena funkce v projektu pomocí zkratek, např.:

- produktový manažer – PrM,
- technický manažer – SSA,
- finanční manažer – QM.

9.1.2 Technické normy

Tato kapitola bude obsahovat seznam harmonizovaných i neharmonizovaných norem, které se zabývají problematikou řídicích systémů divadelní technologie. Norma bude obsahovat rok vydání a přesný název technické normy.

9.1.3 Dokumenty managementu kvality

Z managementu kvality budou použita zejména integrovaná příručka kvality, proces řízení neshod a proces řízení dokumentů. Tyto dokumenty budou identifikované pod interním číslem dle normy ČSN EN ISO 9001:2016. Všechny používané dokumenty budou začleněny do příslušných bloků.

9.1.4 Dokumenty managementu funkční bezpečnosti

Níže uvedené podnadpisy jsou označeny prefixem složeným z písmene „FSM_A“ a dvojčíslím odděleným tečkou. Každá takto označená skupina je z pohledu systémového popisu managementu funkční bezpečnosti definovanou uzavřenou skupinou – blokem.

9.1.4.1. FSM_A.01: Evidence dokumentace

Všechny dokumenty použity v projektu, budou mít své identifikační číslo a bude vytvořený jejich seznam včetně zodpovědností pro schvalování a posuzování těchto dokumentů.

9.1.4.2. FSM_A.02: Plánování bezpečnosti

Plán managementu funkční bezpečnosti bude popisovat činnosti související s bezpečností u celého procesu vývoje a dokumenty, které je třeba vytvořit za tímto účelem. Uvedený postup bude splňovat požadavky na zamezení vzniku poruch podle souboru norem ČSN EN 61508 ed.2:2011 a aplikačních norem uvedených ve specifikaci bezpečnostních požadavků. V rámci modulu plánování bezpečnosti musí být navrženy formuláře pro interní a externí simulaci chyb.

Dokumenty FSM_A.02.1 – Plán managementu funkční bezpečnosti a FSM_A.02.2 – Plán validace budou sloužit jako výstupní dokumenty.

9.1.4.3. **FSM_A.03: Definice bezpečnostních požadavků**

V tomto bloku budou definovány veškeré požadavky týkající se bezpečnosti výrobku, včetně požadavků z aplikačních technických norem jako je soubor norem ČSN EN 61508 ed.2:2011. V dokumentu FSM_A.03.1 budou definovány specifikace bezpečnostních požadavků.

9.1.4.4. **FSM_A.04: Validace bezpečnosti**

Testování bude řešeno primární validační technikou, ale některé požadavky mohou vyžadovat i teoretické ověřovací techniky.

Testovací metody – prokázání požadavku na:

- funkční testování v aplikaci,
- Testování “black box”,
- zátěžové testování.

Výstupy z tohoto bloku budou zaznamenány do dokumentů:

- FSM_A.04.1 – Specifikace validačních testů bezpečnosti,
- FSM_A.04.V1 – Zprávy z ověření validačních testů.

9.1.4.5. **FSM_A.05: Návrh systému**

Architektura systému poskytuje přehled a přiděluje požadavky subsystému hardwaru a softwaru. V dokumentu FSM_A.03.1 budou specifikované bezpečnostní požadavky. V dokumentu FSM_A.05.1 bude popsána architektura systému, včetně výkresů. Budou definovány všechny rozhraní mezi komponenty, včetně seznamu materiálu.

Návrh systému zahrnuje:

- rozsah požadavků,
- detekce chyb a reakce na chyby,
- interface subsystémů.

9.1.4.6. **FSM_A.06: Hardware – architektura**

Návrh hardwaru bude popsán pomocí blokových obvodů, elektrických schémat, výpisů komponentů a seznamů vstupů/výstupů. V dokumentu FSM_A.05.1 bude popsána architektura systému. Ověřovacími dokumenty hardwaru budou systémová FMEDA a výpočty PFH, které budou v bloku FSM_A.06.x a budou sloužit jako vstupní údaje pro architekturu softwaru.

9.1.4.7. **FSM_A.07: Software – architektura**

Softwarová architektura zahrnuje:

- strukturu softwaru a jeho rozhraní,
- dynamické a statické chování aplikovaného softwaru,
- poruchy a chování.

Požadavky softwarové architektury budou specifikované v dokumentu FSM_A.03.1. Popis této architektury bude zaznamenaný v dokumentu FSM_A.05.1. Jako výstupní dokument bude naplněn dokument FSM_A.07.1, který bude popisovat softwarovou architekturu. Způsobilost a oprávnění používání existujícího bezpečnostního softwaru a jeho komponentů bude popisovat dokument FSM_A.07.V1.

9.1.4.8. **FSM_A.08: Software design**

Software design bude zahrnovat několik různých integračních testů a činností:

- SW – SW integrace,
- HW – SW integrace,
- systémová integrace.

V dokumentu FSM_A.05.1 bude doplněna architektura systému. V dokumentu FSM_A.07.1 bude doplněna architektura softwaru. Výstupními dokumenty pro software design budou:

- FSM_A.08.1 – Popisy funkcí systému,
- FSM_A.08.2.x – Bloková schémata,
- FSM_A.08.V1 – Testování „black box“.

9.1.4.9. **FSM_A.09: Funkční bezpečnostní audity/inspekce**

Zprávy managementu funkční bezpečnosti a auditu budou ověřovat, že každý tým dokončil své bezpečnostní úkoly a výstupy, tj. hardware, software a dokumentaci podle plánu řízení bezpečnosti funkcí a V&V (Verifikačního a Validačního) plánu. Inženýr, který je zodpovědný za funkční bezpečnost provádí přezkumy. Výstupním

dokumentem bude auditní plán, včetně kontrolního seznamu a auditní zpráva. Tyto dokumenty budou vytvořeny nezávislým certifikačním orgánem.

Na základě rozhodnutí produktového manažera bude systém a jeho provedení zkontrolováno nezávislou třetí stranou dle zákona „certifikačním orgánem“. Posuzovatel předloží plán, postupů a testování pro funkční bezpečnost.

9.1.5 **Kompetence jednotlivých osob**

Všechny osoby pověřené projektem budou mít technickou kvalifikaci z hlediska formálního vzdělávání, školení o konkrétním produktu, tohoto plánu FSM.

Kompetence těchto inženýrů odpovědných za návrh týkající se bezpečnosti a rozhodnutí o V&V budou dokumentovány technickými životopisy. Kompetentními osobami budou zejména:

- produktový manažer,
- vývojový manažer/specialista pro funkční bezpečnost,
- manažer kvality,
- vývojový manažer HW,
- vývojový manažer SW,
- zkušební technik,
- technik realizace/instalace.

Následující tabulka specifikuje kvalifikace požadované pro zodpovědné role projektu. Matice kompetencí testovacího týmu je popsána v Tab: 3.

Tab: 3: Matice testovacího týmu – template

Téma:	Produktový manažer	Vývojový manažer	Manažer kvality	Vývojový manažer SW	Zkušební technik	Technik realizace/instalace
Znalost systému	X	X	X	–	–	–
Znalost systematického vývoje, ověřování a validačních procesů	X	X	X	–	–	–
Funkční testy	X	X	–	X		
FMEDA; FTA; Rizikové analýzy	–	X	X	–	–	–
Požadavky managementu	X	X	–	X	–	–
Software	–	X	–	X	–	–
Řízení funkční bezpečnosti	X	X	–	–	–	–
Plánování a koordinace činností v oblasti řízení funkční bezpečnosti	X	X	–	–	–	–
Zvýšení bezpečnostních otázek	X	X	X	–	–	–
Vývoj bezpečnostních požadavků	X	X	–	–	–	–
Realizace bezpečnostních požadavků	X	X	X	X	–	–
Plánování, tvorba dokumentace, ověřování a validace	–	X	X	X	X	X
Správa konfigurace	X	X	X	X	–	–
Elektrikář – vzdělávání a požadavky místního právního zákona	X	X	–	–	X	X

9.1.6 **Požadavky přiřazení a sledování**

Účelem sledování požadavků je zajištění implementování a testování. Sledování požadavků a jejich zlepšování bude popsané v podnikové příručce QMS /Quality Management System/ dle ČSN EN ISO 9001:2016. Cílem validace je sledování požadavků na bezpečnost výrobku a bezpečnostní požadavky odvozenými od technických norem a standardů.

9.1.7 Řízení změn

Proces řízení změn verzí softwaru a hardwaru bude zařazen do podnikové příručky QMS dle ČSN EN ISO 9001:2016. Mezi hlavní sledované oblasti patří:

- Management změn a konfigurací,
- Oznámení zákazníkům,
- Zpětná vazba od zákazníka.

9.1.8 Vývojové nástroje

Tato kapitola bude specifikovat vývojové nástroje používané při vývoji systému řízení projektu. Použití jiných vývojových nástrojů nebo jiných verzí, než které jsou uvedeny v této části, vyžaduje schválení bezpečnostním týmem.

Klasifikační nástroje dělíme do tříd T1 až T3. Pro klasifikaci nástrojů můžeme použít např.: *ČSN EN 61508-4 ed.2:2011 odstavec 3.2.11 a ČSN EN 61508-3 ed.2:2011 odstavec 7.4.4:*

- T1 – Nevytváří žádné výstupy, které mohou přímo nebo nepřímo přispívat ke spustitelnému kódu (včetně dat) systému souvisejícího s bezpečností,
- T2 – Podporuje test nebo ověření návrhu nebo spustitelného kódu, kde chyby v nástroji mohou selhat při odhalení vad, ale nemohou přímo vytvářet chyby ve spustitelném softwaru,
- T3 – Generuje výstupy, které mohou přímo nebo nepřímo přispívat ke spustitelnému kódu systému souvisejících s bezpečností. [13]

U každého nástroje klasifikovaného jako T3 se musí provést kontrola spolehlivosti v provozu. Nástroje s nižší kritičností nevyžadují toto testování, neboť jejich výstup je předmětem vícenásobných překrývajících se ověřovacích činností. Verze jednotlivých softwarů budou zapsány v seznamu použitého softwaru.

Cílem této kapitoly je zdokumentovat odpovídající výběr nástrojů generujících kód. Kromě funkčního produktu pro výběr nástroje bude provedená i demonstrace kontroly spolehlivosti nástroje. Důkazem budou doložené certifikáty dodavatele. [13]

9.2 PLÁN VALIDACE (FSM_A.02.2)

Cílem plánu validace je naplánovat validaci řídicího systému, což vede k prokazatelné kontrole všech bezpečnostních požadavků.

V rámci struktury metodiky s použitím V-modelu reprezentuje plán validace požadavky na vyžadované validační testy. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 52.

Testování validace se realizuje proto, aby bylo prokazatelné, že všechny bezpečnostní požadavky byly splněny. Hlavním cílem dokumentu je informovat všechny členy plánovacího týmu. Cílovou skupinou pro tento projekt jsou všichni členové vývoje, testovací týmy a týmy zajištění kvality.

9.2.1 Plánování testování

Seznam ověřovacích testů vychází ze čtyř základních bodů:

- hardware/software, které mají být ověřeny,
- testování objektů,
- testování prostředí,
- testování logování/záznamů.

Každá část hardwaru a softwaru bude pokryta několikanásobnou validací záměrů. Každá validace záměru bude zdokonalována jedním nebo více testy případů nebo analýzou případů. Každý test záměru bude prováděn použitím testu prostředí tzv. „test bed“. Z každých zkoušek bude vyplněný formulář prováděných testů, včetně data a místa provedení. Výsledkem bude vytvoření zkušebního protokolu s výsledkem validačního testu bezpečnostních funkcí. Všechny tyto dokumenty budou číslovány pro jejich jednoznačnou identifikaci.

9.2.1.1. Testovací nástroje

Testovací případ „test bench“ bude navržen tak, aby reprezentoval jedno zařízení se vstupy a výstupy, řídicím panelem, včetně samotného pohonu vybaveného dvojitou elektromagnetickou brzdou. V dokumentu bude uvedený název bezpečnostní funkce, včetně blokového schématu, která bude aplikována a testována. Testovací případ bude proveden v každém definovaném testovacím prostředí „test bed“.

9.2.1.2. **Ověření hardwaru/softwaru**

Ověření hardwaru a softwaru se bude provádět pomocí spuštění všech bezpečnostních funkcí v simulovaných podmínkách a aktivováním bezpečnostních funkcí tak jako ve skutečných podmínkách. Následně bude sledována reakce řídicího systému, včetně reakcí všech akčních členů (relé, stykače, atd.).

Cílem této validace je ověřit zda:

- každá bezpečnostní funkce je správně implementována,
- bezpečnostní požadavek je správně proveden,
- každá bezpečnostní funkce je v požadované bezpečnostní integritě,
- specifikovaná chybová tolerance je správně implementována,
- je specifikovaná diagnostika správně implementována,
- je bezpečnostní funkce odolná proti poruše ostatních připojených systémů,
- je bezpečnostní funkce odolná proti předvídatelným poruchám,
- reakční čas řídicího systému za normálních podmínek odpovídá specifikaci,
- reakční čas řídicího systému na chybu za normálních podmínek odpovídá specifikaci,
- reakční čas řídicího systému v krizových podmínkách odpovídá specifikaci,
- reakční čas řídicího systému na chybu v krizových podmínkách odpovídá specifikaci.

Zkoušky budou zaznamenány do dokumentace o záznamu validačního testu. Data budou zaznamenána jako jednotlivé zprávy s výsledky testů.

9.3 VERIFIKACE POMOCÍ SIMULACE CHYB U VÝROBCE (FSM_A.02.V1)

Simulace chyb /Fault insertion tests/ budou prováděny jen na necertifikovaných subsystémech.

Certifikované subsystémy jsou považovány za vyhovující v případě jejich předepsaného použití. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 53. V tomto dokumentu bude vytvořena podrobná tabulka se simulacemi chyb a následným vyhodnocením všech bezpečnostních testů.

9.4 VALIDACE POMOCÍ SIMULACE CHYB V DIVADLE (FSM_A.02.V2)

Simulace chyb prováděné u zákazníka jsou obdobné, jako interní simulace chyb. Bude prokázáno, že po instalaci systému na místě určení, jsou všechna požadovaná bezpečnostní kritéria splněna a je dosaženo stejných očekávaných výsledků, jako při interních simulacích chyb.

V tomto dokumentu bude vytvořena podrobná tabulka se simulacemi chyb a následným vyhodnocením všech bezpečnostních testů.

9.5 SPECIFIKACE BEZPEČNOSTNÍCH POŽADAVKŮ (FSM_A.03.1)

Specifikace bezpečnostních požadavků SRS /Safety Requirements Specification/ vychází primárně z požadavků analýzy rizik, popřípadě ze specializované normy pro divadelní techniku. Tyto bezpečnostní požadavky jsou obvykle reprezentovány základními požadavky, včetně funkčních popisů bezpečnostních funkcí a jejich požadovaných vlastností. V rámci validačních testů jsou tyto požadované parametry validovány a testovány. Titulní list tohoto dokumentu je v příloze pod Obr. 55.

9.5.1 Požadavky nezávislé na architektuře produktu

Výrobce bude používat komponenty s bezpečnostními parametry prokazatelně garantované a certifikované. Veškeré použité EU směrnice a normy budou použité v platném znění za pomocí webového portálu *eur-lex.europa.eu*. Veškeré komponenty pro realizaci SIF budou v průmyslovém provedení.

Podmínky prostředí budou přehledně uspořádány do následující tabulky:

Tab: 4: Podmínky prostředí – template

Název	Hodnoty
Teplota – provoz	Min. – <<*doplnit hodnotu*>> °C Max. + <<*doplnit hodnotu*>> °C
Teplota – transport, skladování	Min. – <<*doplnit hodnotu*>> °C Max. + <<*doplnit hodnotu*>> °C
Vlhkost	Průměrná relativní vlhkost: <<*doplnit hodnotu*>> % Maximální relativní vlhkost:<<*doplnit hodnotu*>> % Minimální relativní vlhkost: <<*doplnit hodnotu*>> %
Tlak – provoz, transport, skladování	Od <<*doplnit hodnotu*>> hPa do <<*doplnit hodnotu*>> hPa
EMC	Minimální požadavky dle <<*doplnit normu*>>
Vibrace	Dle <<*doplnit normu*>>
Krytí	Pro venkovní instalaci min. IP <<*doplnit hodnotu*>> Pro vnitřní instalaci min. IP <<*doplnit hodnotu*>>

9.5.1.1. Doby odezvy pro systém SIF – Bezpečnostně instrumentovaná funkce

Specifické časy se můžou odlišovat v závislosti na aplikaci, dynamice řízení, časové prodlevě hardwarových komponentů a můžou se lišit v závislosti na specifické bezpečnostní funkci či požadovaných technických vlastnostech. Specifické výpočty jsou vyžadovány každým aplikačním projektem.

9.5.1.2. Alarmy a identifikace SIF v HMI

Budou rozepsány požadavky na jednotlivé úrovně alarmů a potřeby jejich odsouhlasení operátorem. Bude jasně definováno, které z alarmů jsou kritické, které závažné a které pouze informativní. Stanovené úrovně budou mít přiřazeny příslušné vlastnosti. Veškeré alarmy a informace budou logované do systému.

9.5.1.3. Funkční požadavky

V této kapitole budou specifikovány všechny požadavky na vlastní funkci SIF, jako jsou persistence chybového stavu, možnost/nemožnost bypass funkce a její způsob provedení.

9.5.2 Požadavky závislé na architektuře

Tato kapitola určuje požadavek na úroveň integrity bezpečnosti SILx pro architekturu bezpečnostního okruhu. Předpokládá se, že všechny funkce spojené s bezpečností jsou provozovány v režimu vysokého vyžádání /High Demand Mode/. Předpokládá se vyžádání bezpečnostní funkce častěji než jedenkrát ročně z důvodu intenzivního používání všech funkcí.

Obecně požadovaná architektura subsystémů je 1oo2 nebo 1oo2D. Výjimečně lze použít 1oo1 po zdůvodnění příslušnou analýzou. Pro jednotlivé SIF je nutné stanovit a striktně určit použitou architekturu.

V požadavcích na interval pro kontrolní testy T1 bude doplněna tabulka:

Tab: 5: Intervaly pro kontrolní testy – template

Test	T1
Funkční test SIF	*<<doplnit hodnotu>>/rok/*
Testování subsystému senzorů	*<<doplnit hodnotu>>/rok/*
Logický test subsystému	*<<doplnit hodnotu>>/rok/*
Test subsystému aktorů	*<<doplnit hodnotu>>/rok/*

V požadavcích pro střední dobu do obnovy MTTR bude doplněna tabulka:

Tab: 6: Odolnost hardwaru vůči vadám

HFT	MTTR
HFT = 1 (1oo2, 1oo2D architektury)	*<<doplnit hodnotu>>/hodin/*
HFT = 0 (1oo1)	*<<doplnit hodnotu>>/hodin/*

9.5.3 Požadavky odvozené od architektury jednotlivých systémů/komponent

Spolehlivost a ochrana spojená s SIF bude mít následující atributy:

- všechny logické kontroléry (programovatelná logika, atd.) budou mít certifikáty funkční bezpečnosti ze spolehlivých zdrojů,
- všechny ostatní komponenty budou mít spolehlivé bezpečnostní, pravděpodobnostní data. Spolehlivost a poruchovost bude doložena výrobcem komponentů nebo z jiného spolehlivého zdroje,
- spínací a kontrolní mechanismy spojené se SIF implementací budou v souladu s EN 60947-4-1 ed.3:2010, v platném znění,
- všechny elektromechanické stykače spojené se SIF implementací musí mít všechny kontakty ve formě nuceně vedených kontaktů – podle

- EN 60947-4-1 ed.3:2010 (viz. Dodatek “F” této normy), v platném znění,
- všechny spínací zařízení spojené se SIF implementacemi musí být vyrobeny jako /Forced – disconnect/ spínače – podle EN 60947-5-1 ed.3:2018 (viz. Dodatek “K” této normy), v platném znění,
- všechny komponenty musí být vybavené řádnými diagnostickými funkcemi.

9.5.3.1. Požadavky na diagnostické pokrytí DC

Všechny použité komponenty budou vybaveny vhodnými diagnostickými funkcemi. Pro jednotlivé SIF musí být stanoveno výsledné diagnostické pokrytí DC /Diagnostic Coverage/.

9.5.3.2. Požadavky na komunikaci

Do tabulky bude zapsán typ komunikace, rychlost komunikace, odezvu a případné další požadavky. Komunikace subsystémů mohou být použity pouze takové, které nelimitují výslednou úroveň integrity bezpečnosti dané funkce nebo souboru funkcí.

9.6 BEZPEČNOSTNÍ FUNKCE (FSM_A.03.2)

Tento dokument bude obsahovat detailní popis bezpečnostní funkce. Dokument bude zahrnovat vstupní komponenty, logické bloky, funkce a výstupní prvky.

Dokument FSM_A.03.2 bude obsahovat detailní zapojení obvodů a blokových schémat softwarových funkcí a logiky. Dále bude doplněná předpokládaná úroveň integrity bezpečnosti. Pokud je bezpečnostní funkce navázaná na jinou bezpečnostní funkci pomocí logického členu, popřípadě přes datovou komunikaci, je nutné tuto funkci zahrnout a popsat všechny provázané části. Další bezpečnostní funkce budou označeny následným číslem dokumentu FSM_A.03.3 až FSM_A.03.x. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 56.

9.7 VERIFIKACE BEZPEČNOSTNÍCH POŽADAVKŮ – ZPRÁVA (FSM_A.03.V1)

Zpráva o verifikaci požadavků vyplývá ze specifikace bezpečnostních požadavků (FSM_A.03.1) a z dokumentu bezpečnostní funkce 1 (FSM_A.03.2). Dokumentem se odsouhlasí, že byly dokumenty ověřeny a může být zahájen další blok činností.

9.8 SPECIFIKACE VALIDAČNÍCH TESTŮ BEZPEČNOSTI (FSM_A.04.1)

Obsahem dokumentu je plánování validace bezpečnostních funkcí. Specifikace validačních testů bezpečnosti vychází z plánu validace a předchozích dokumentů. V tomto dokumentu budou plánované požadavky na testy a jejich technické provedení. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 57.

Bezpečnostní funkce bude testována záměrným uvedením do činnosti – simulace bezpečnostní funkce v činnosti. Ve většině případů bude nutné aktivování vstupního zařízení. Pro zařízení jevištní techniky platí, že definovaným bezpečným stavem je uvedení zařízení do klidového bezpečného stavu s odpojením pohonu od elektrické energie.

9.9 ZPRÁVA O OVĚŘENÍ VALIDAČNÍCH TESTŮ BEZPEČNOSTI (FSM_A.04.V1)

Obsahem tohoto dokumentu bude vytvoření zprávy a výsledků provedených testů validace. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 58.

Budou zohledněna veškerá kritéria a testy bezpečnostní funkce, včetně výsledných stavů. Data budou zapsána do tabulky.

9.10 POPIS ARCHITEKTURY SYSTÉMU (FSM_A.05.1)

Cílem tohoto dokumentu je popsat bezpečnostní opatření, která je specifikovaná pro celý systém řízení. Tento dokument je určen výhradně pro použití v procesu vývoje systému řízení interně ve společnosti. Každá distribuce nebo použití mimo společnost vyžaduje schválení managementem. Bezpečnostní koncept zaznamenává bezpečnostní informace o řídicím systému a jeho softwaru. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 59.

Obsahem tohoto dokumentu bude:

- vybraná bezpečnostní architektura systému a použitých subsystémů,
- vybraná bezpečnostní architektura softwaru, včetně jedné úrovně dekompozice,
- popis auto testů a monitorovacích opatření a jejich mapování do bezpečnostní architektury,
- dosažení úrovně integrity bezpečnosti popsanými opatřeními,
- chování řídicího systému při provádění bezpečnostních funkcí, včetně zpracování definovaných chybových zpráv,
- chování řídicího systému v případě vlastní poruchy/chyby.

Cílem tohoto dokumentu bude:

- poskytnout srozumitelný popis řídicího systému a jeho architektury,
- určit vazby a způsob implementace bezpečnostních funkcí,
- specifikace implementace opatření souvisejících s bezpečností, jako jsou redundance, diverzita, self tests, monitoring a zpětné vazby,
- evidence důkazů o implementaci dalších bezpečnostních požadavků dosažených použitou systémovou a softwarovou architekturou.

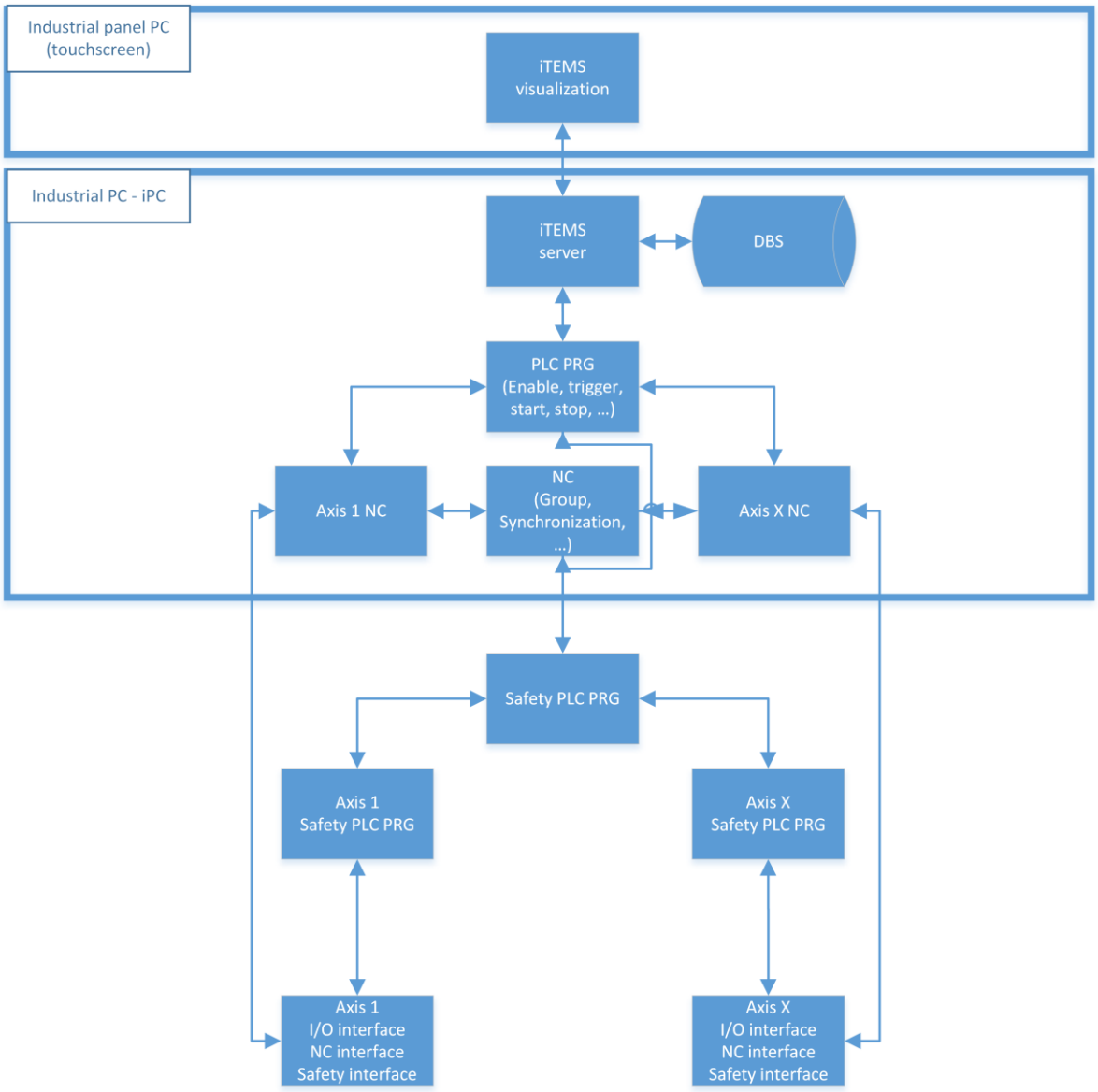
Sledování požadavků je zajištěno prostřednictvím specifikace požadavků a doložením dokladů o splnění těchto požadavků.

9.11 ARCHITEKTURA SOFTWARU (FSM_A.07.1)

Součástí řídicího systému bude kompletní softwarové vybavení například podle Obr. 18. Tento dokument bude popisovat architekturu softwaru s popisem použitých technologií a programovacích jazyků. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 60.

9.11.1 Blokové schéma softwaru systému řízení

Bude vytvořeno blokové schéma systému, včetně popisu komunikačních spojení a popsané jednotlivé bloky. Příklad je znázorněn na Obr. 18.



Obr. 18: Blokové schéma softwaru systému řízení

9.11.2 Popis architektury

V popisu architektury budou doplněny požadavky softwaru pro:

- řídicí server popřípadě PLC,
- softwarovou regulaci pokud není řešeno pomocí hardwarových komponentů,
- bezpečnostní PLC, včetně komunikačního rozhraní do standardního PLC programu,
- veškeré certifikace použitých komponent.

9.12 POUŽÍVÁNÍ JIŽ EXISTUJÍCÍHO BEZPEČNOSTNÍHO SOFTWARU (FSM_A.07.V1)

Tento Dokument je důležitý pro verifikaci správnosti a oprávněnosti použitých softwarových nástrojů, relevantních programovacích jazyků, zvolených vývojových prostředí, použitých rozhraní, předdefinovaných knihoven a dalších prostředků pro programování softwarové části dané bezpečnostní funkce. Výstupem dokumentu bude ověření zdrojů a vlastností nástrojů pro dosažení cíle – funkčně bezpečného softwaru. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 61.

Způsobilost bude ověřena formou kontroly:

Do dokumentu bude zapsáno evidenční číslo certifikace, certifikační autorita, verze softwaru, zdrojové podklady a případně i naskenovaná kopie certifikátu. Bude provedeno ověření platnosti verzí a zdrojových dat, včetně manuálů a jejich verzí. Ověření platnosti bude zapsáno do dokumentu společně se závěrem, který jednoznačně potvrdí nebo vyvrátí relevanci všech použitých softwarových nástrojů a jejich podpůrných materiálů.

9.13 NÁVRH SOFTWARU

9.13.1 Popisy funkcí softwaru (FSM_A.08.1)

V tomto dokumentu budou vložena bloková schémata bezpečného softwaru s návazností na hardwarové komponenty (FSM_A.08.2.x). Tyto logické funkce pak budou testovány pomocí funkce „black box“, který bude blíže specifikovaný v dokumentu FSM_A.08.V1. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 62.

9.13.2 Testování „black box“ (FSM_A.08.V1)

V tomto dokumentu bude zaznamenáno testování softwarových celků – bloků pro účel před – aplikačního testu. Titulní list tohoto dokumentu je vložen v příloze pod označením Obr. 63.

9.13.2.1. Specifikace testu

V tomto dokumentu bude zaznamenáno testování softwarových celků prostřednictvím simulace vstupních informací a sledování reakcí na výstupech.

9.13.2.2. Zdroje pro testování

Testovací prostředí je prostředí stejné jako pro tvorbu samotného software. Způsob definice a provedení testu je specifikováno prostředím a zvoleným nástrojem.

9.13.2.3. Zpráva o testu

Tabulka s výstupními testy bude zaznamenána v tomto dokumentu. V tabulce budou jako vstupní hodnoty kombinace jednotlivých stavů na vstupu. Dále bude sledován stav a chování funkce na výstupu funkčního bloku a zaznamenán očekávaný, popřípadě neočekávaný výsledek testu.

10 VALIDACE NAVRŽENÉ METODIKY NA REÁLNÉ APLIKACI DIVADELNÍ TECHNIKY

Vyvinutá metoda byla validována při vývoji řídicího systému pro Národní divadlo Brno – Janáčkovo divadlo Obr. 19.

Obr. 19: Janáčkovo divadlo Brno

Divadelní scéna prošla významnou rekonstrukcí z hlediska řídicího systému a mechanických částí. Jedná se o významnou budovu Národního divadla v Brně, ve které hostují divadelní soubory z celého světa. Nový systém řízení, včetně vizualizace a techniky ovládání je na vysoké úrovni. Jsou dodrženy veškeré evropské zvyklosti a standardy, jak s ohledem na bezpečnost, tak s ohledem na metodu ovládání zařízení. Celkovou rekonstrukcí prošla horní mechanika, včetně nových rozváděčů Obr. 20 a ovládacích pultů.

Obr. 20: Rozvodné skříně řídicího systému

10.1 PROVOZNÍ POŽADAVKY NA DIVADELNÍ TECHNIKU

Uživatelským požadavkem divadelního řídicího systému je synchronní chod zařízení. V hlavním řídicím systému se sestavuje posloupnost pohybů pro jednotlivé pohony. Zařízení jsou tak limitována v časové ose. Jednotlivé zařízení a skupiny zařízení mají definovány svoje startovní a cílové polohy, včetně průběhu pohybu a v rámci dané akce jsou schopny vrátit se do svých původních pozic. V rámci těchto smyček je nutné realizovat několik typů synchronizací:

- **asynchronní chod** – vytvoření skupiny současně jedoucích zařízení, kdy dosažení limitu pojezdu jednoho zařízení nebo reakce na bezpečnostní funkci daného zařízení musí vést k zastavení tohoto daného zařízení. Zbytek skupiny zůstává neovlivněn,
- **asynchronní chod se skupinovým vypnutím** – je obdobou asynchronního chodu s tím, že musí být zastavena celá skupina zařízení a musí být patrné, které ze zařízení způsobilo odstavení skupiny,
- **synchronní chod** – vytvoření skupiny zařízení, jež jsou vůči sobě ve vzájemné závislosti. Může to být např. dráhová nebo časová závislost, kdy zařízení vůči sobě udržují stejnou vzdálenost s určitou tolerancí nebo kdy zařízení musí dosáhnout cíle ve stejném čase.

Jednotlivá zařízení reagují na události jiných zařízení, např. průjezd jednoho zařízení určitou polohou odstartuje jízdu jiného zařízení nebo se např. zařízení spustí až po předem nastaveném čase. Tyto tzv. „triggery“ opět zvyšují možnosti práce se systémem. Systém také umožní přes uživatelské rozhraní kompletní diagnostiku sebe sama i jednotlivých zařízení do systému připojených.

10.2 HUMAN MACHINE INTERFACE – ROZHRANÍ ČLOVĚK – STROJ

Ovládací pult slouží pro plnou kontrolu nad automatizovanými zařízeními v rámci divadelního představení. Pult je vybavený dotykovou obrazovkou, která umožňuje nejen snadnou tvorbu divadelních scén, jejich editaci či mazání, ale také možnost odzkoušení jednotlivých zařízení při samostatné jízdě, diagnostiku jednotlivých zařízení i celého řídicího systému.

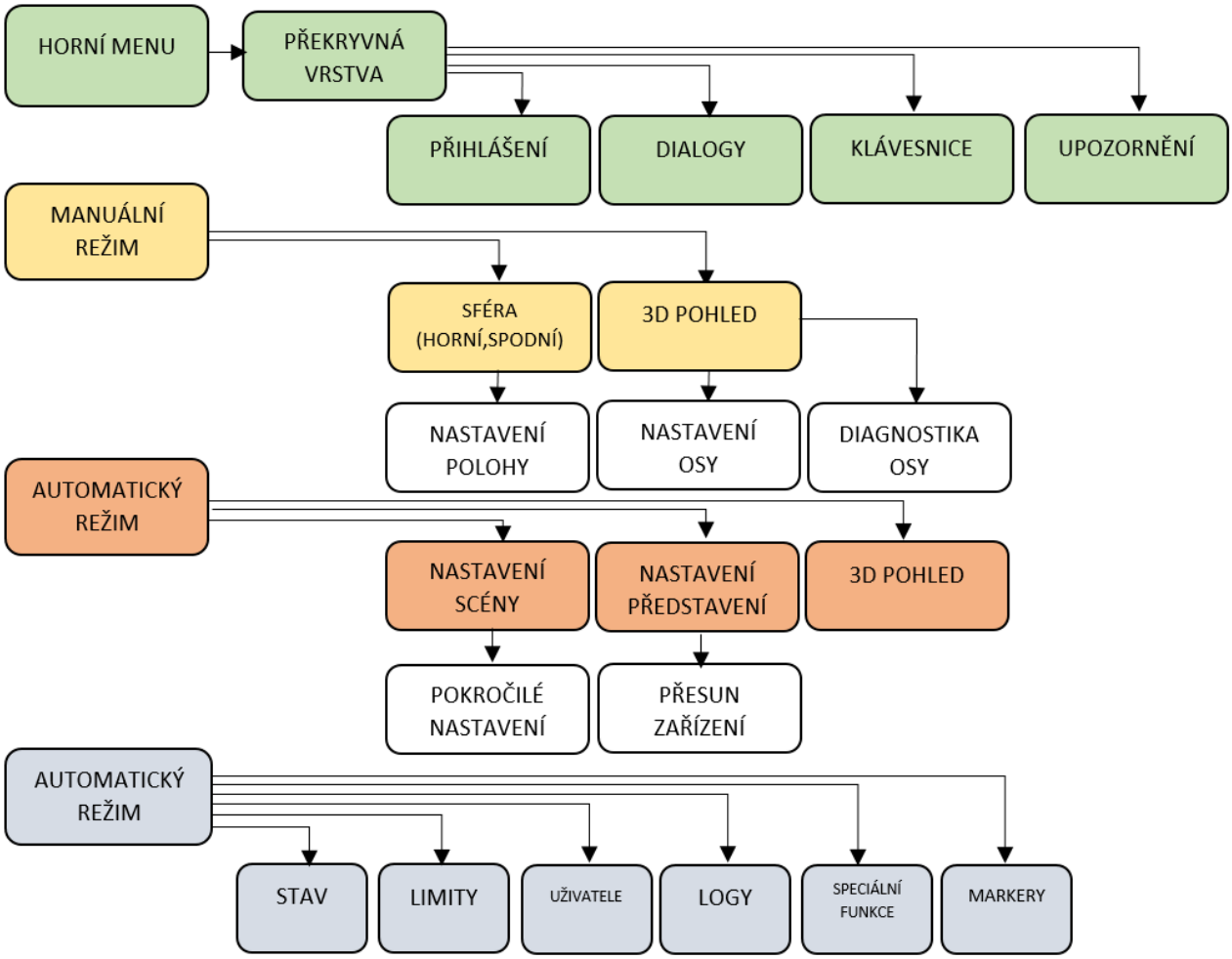
Základní požadavky na ovládací pult (Obr. 21) jsou následující:

- přehledný dotykový panel,
- ovládací páky s bezpečnostním tlačítkem „dead men“,
- tlačítko nouzového zastavení,
- tlačítko „kvitace poruchy“,
- kontrola zapnutého stavu,
- ovladač pro zapnutí ovládacího pultu.

Obr. 21: Ovládací pult Janáčkovo Divadlo

10.3 HMI – VIZUALIZACE

HMI tvoří základní a podstatnou roli v řídicích systémech pro divadla. V následujících podkapitolách jsou stručně popsány základní úkony týkající se provozu software, popis základní obrazovky, tlačítek a nástrojů, které jsou na ní zobrazeny. Stručně jsou také popsány základní režimy, jež lze v software využít k řízení divadelních představení. Na Obr. 22 je popis struktury HMI.



Obr. 22: Struktura HMI

10.3.1 Servisní režim

Servisní režim je nedílnou součástí řídicího systému a slouží primárně k diagnostice jednotlivých zařízení. Dále zobrazuje stavy bezpečnostních funkcí. Servisní režim slouží také k systémovým nastavením apod. U každého zařízení je zobrazena kompletní diagnostika bezpečnostních funkcí a stavu zařízení:

- aktuální poloha zařízení,
- stav hlavního jističe zařízení,
- bezpečnostní koncová poloha horní – bezpečnostní funkce,
- bezpečnostní koncová poloha dolní – bezpečnostní funkce,
- EDM /External Device Monitoring/ – zpětná vazba bezpečnostní funkce pro výkonové stykače a elektromechanických brzd – bezpečnostní funkce,
- stav frekvenčního měniče,
- lokální vypínač pohonu – bezpečnostní funkce,
- tenzometrický čep – vážení – stav tenzometru, bezpečnostní výsledek testu tenzometru,
- stav komunikace – odezva a CRC,
- statický test brzd – bezpečnostní funkce,
- ruční nouzové ovládání – bezpečnostní funkce,
- termo kontakt motoru a brzdného odporu,
- přeskok lana z navíjecího bubnu,
- bezpečnostní lišty /bumper/ – bezpečnostní funkce,
- kryt zařízení – bezpečnostní funkce,
- SLS /Safely Limited Speed/ – bezpečná rychlost – bezpečnostní funkce,
- stav tlačítka bezpečného zastavení – bezpečnostní funkce,
- stav diskrepance tlačítka bezpečného zastavení – bezpečnostní funkce,
- stav sběrnice PLC (odezva, chyby),
- komunikace mezi PLC a měniči,
- stav bezpečnostního PLC,
- stav primárního a sekundárního serveru,
- stav chlazení rozvaděčů.

10.3.2 Systémový log událostí

Systémový log událostí je jednou z důležitých částí bezpečnosti a také komfortu uživatele i servisního technika. V systémovém logu jsou popsány informace o stavu zařízení, jejich čas poruchy a také informace o uživateli a jeho akcích na jednotlivých zařízeních. V systémovém logu jsou dohledatelné stavy a problémy řídicího systému a jednotlivých zařízení.

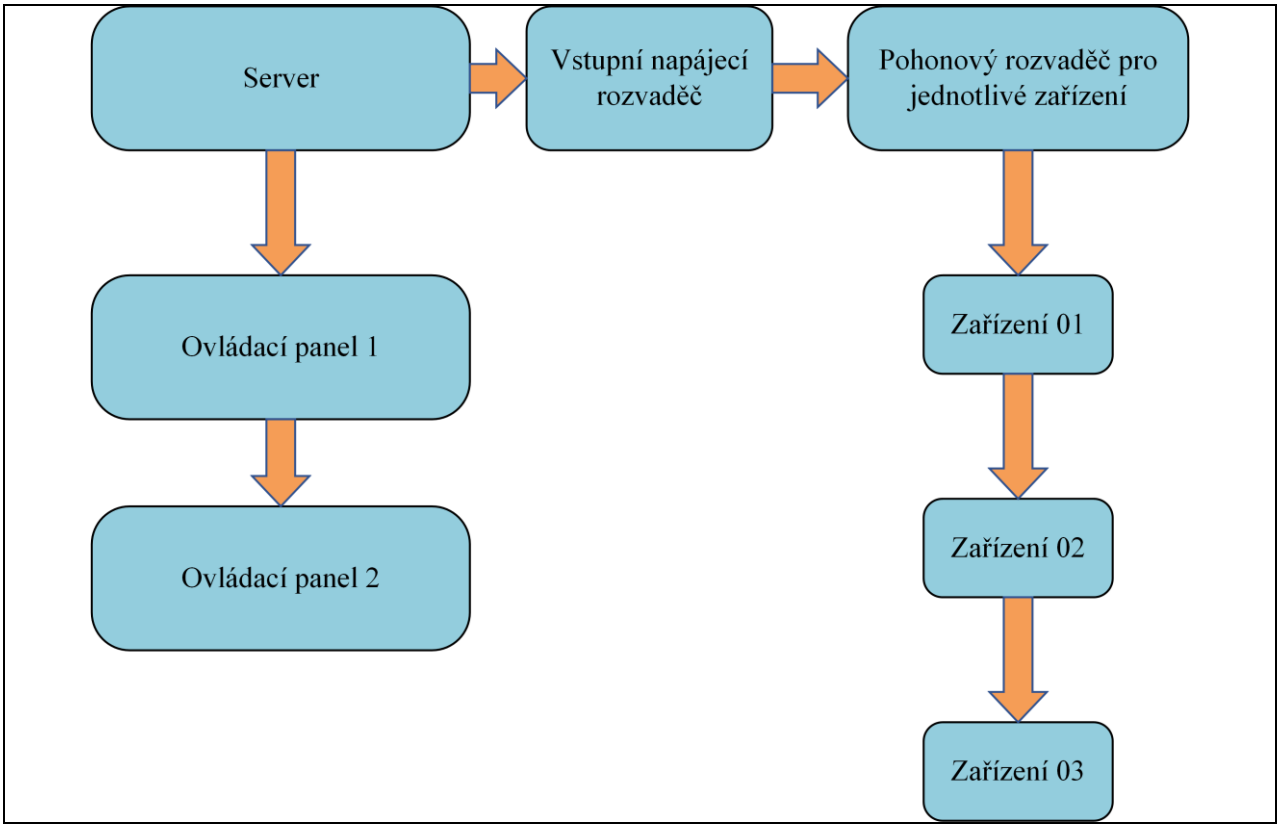
10.3.3 Speciální funkce – testování bezpečnostních funkcí

Testování bezpečnostních funkcí a jejich diagnostika je nedílnou součástí řídicího systému. Patří sem zejména:

- statický test brzd,
- dynamický test brzd,
- testování tenzometrického čepu (vážení),
- kalibrace tenzometrického čepu,
- kalibrace snímače výšky zařízení,
- obnova zálohy řídicího systému.

10.4 KONCEPCE ŘÍDICÍHO SYSTÉMU JANÁČKOVA DIVADLA

Princip řídicího systému je centralizovaným systémem, jak je znázorněno na Obr. 23. Centrální výkonová elektronika (frekvenční měniče, stykače, jističe, PLC) se nachází v rozvodně. Dále je rozvedená silová i ovládací kabeláž k jednotlivým zařízením. Řídicí počítač – server se rovněž nachází v centrální rozvodně. Ovládací pulty jsou umístěné v jevištním prostoru mimo dohled diváka, ale tak, aby bylo bezpečně vidět na ovládané zařízení.

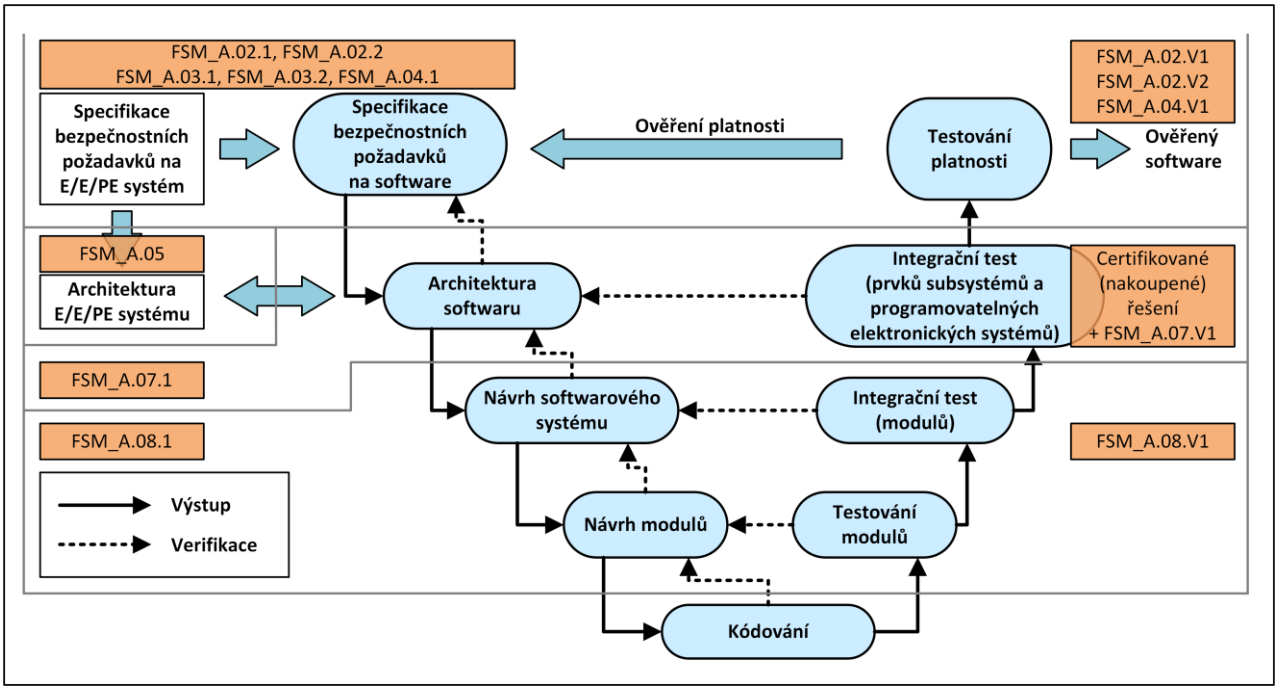


Obr. 23: Struktura řídicího systému

10.5 VÝCHOZÍ PŘEDPOKLADY

Sestavení této metodiky předpokládá její začlenění do životního cyklu celkové bezpečnosti a managementu funkční bezpečnosti společnosti či projektu. Cíle a požadavky na celkovou bezpečnost jsou definovány celým souborem norem ČSN EN 61508-1:2011 až ČSN EN 61508-7:2011. Výchozím předpokladem je předpokládaná zpracovaná metodika pro ostatní fáze životního cyklu celkové bezpečnosti.

V následujících kapitolách bude sestavena dokumentace s metodikou softwaru pro jednu bezpečnostní funkci. Dokumentovaný příklad praktické aplikace bude postupovat podle V-modelu Obr. 24. Veškeré dokumenty s prefixem FSM, které jsou propojeny na jednotlivé kroky V-modelu, budou dále prezentovány v tomto dokumentu.



Obr. 24: V-model, včetně dokumentů

10.6 PLÁN MANAGEMENTU FUNKČNÍ BEZPEČNOSTI (FSM_A.02.1)

V Tab: 7 je vytvořen seznam odpovědných pracovníků na následujícím projektu. K jednotlivým jménům je přidělena funkce v projektu pomocí zkratek:

Tab: 7: Role managementu

Role		Osoba	Kontaktní informace
Manažer společnosti a produktů	PrM	Jméno: Příjmení:	
Manažer vývoje a Architekt bezpečnostního systému	SSA	Jméno: Příjmení:	
Finanční manažer a manažer kvality	QM	Jméno: Příjmení:	

Pro aplikaci systému řízení divadelní technologie jsou použity následující technické normy uvedené v Tab: 8.

Tab: 8: Technické normy

Název normy	Popis
ČSN EN 60204-1 ed.2:2007	Bezpečnost strojních zařízení – Elektrická zařízení strojů – Část 1: Všeobecné požadavky
ČSN EN 60204-32 ed.2:2009	Bezpečnost strojních zařízení – Elektrická zařízení strojů – Část 32: Požadavky na elektrická zařízení zdvihacích strojů
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 ISO 12100:2011	Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – Posouzení rizika a snižování rizika
ČSN EN 61000-6-1 ed.2:2007	Elektromagnetická kompatibilita (EMC) – Část 6-1: Kmenové normy – Odolnost – Prostředí obytné, obchodní a lehkého průmyslu
ČSN EN 61000-6-3 ed.2:2007	Elektromagnetická kompatibilita (EMC) – Část 6-3: Kmenové normy – Emise – Prostředí obytné, obchodní a lehkého průmyslu
ČSN 33 2000-4-41 ed.2:2007	Elektrické instalace nízkého napětí – Část 4-41: Ochranná opatření pro zajištění bezpečnosti – Ochrana před úrazem elektrickým proudem
ČSN 33 2000-4-42 ed.2:2012	Elektrické instalace nízkého napětí – Část 4-42: Bezpečnost – Ochrana před účinky tepla
ČSN 33 2000-5-51 ed.3:2010	Elektrické instalace nízkého napětí – Část 5-51: Výběr a stavba elektrických zařízení – Všeobecné předpisy
ČSN 33 2000-5-54 ed.3:2012	Elektrické instalace nízkého napětí – Část 5-54: Výběr a stavba elektrických zařízení – Uzemnění a ochranné vodiče

Níže uvedené podnadpisy jsou označeny prefixem složeným z písmene „FSM_A“ a dvojčíslím odděleným tečkou. Každá takto označená skupina je z pohledu systémového popisu managementu funkční bezpečnosti definovanou uzavřenou skupinou – blokem.

10.6.1 **FSM_A.02: Plánování bezpečnosti**

Plán managementu funkční bezpečnosti vychází z normy ČSN EN 61508 ed.2:2011 a literatury Functional safety EXIDA (3rdEdition). Výstupní dokumenty jsou dokumenty uvedené v Tab: 9.

Tab: 9: Plánování bezpečnosti výstupní dokumenty

Výstupní dokumenty				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.02.1	Plán managementu funkční bezpečnosti	SSA	PrM	QM
FSM_A.02.2	Plán validace	SSA	PrM	QM

10.6.2 FSM_A.03: Definice bezpečnostních požadavků

Bezpečnostní požadavky jsou řízeny pomocí souboru norem ČSN EN 61508 ed.2:2011 a DIN 56950-1:2012.

Tab: 10: Definice bezpečnostních požadavků vstupní dokumenty

Vstupní dokumenty	
Dokument	Název
DIN 56950-1:2012	Řízené zařízení (EUC) popis podle DIN 56950-1:2012

Tab: 11: Definice bezpečnostních požadavků výstupní dokumenty

Výstupní dokumenty				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.03.1	Specifikace bezpečnostních požadavků	SSA	PrM	All

Tab: 12: Definice bezpečnostních požadavků dokumenty ověření

Dokumenty ověření				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.03.V1	Verifikace bezpečnostních požadavků – zpráva	SSA	PrM	N/A

10.6.3 FSM_A.04: Validace bezpečnosti

Testování je řešeno primární validační technikou.

Byly použité následující metody pro prokázání požadavku na:

- funkční testování v aplikaci,
- “black box” testování,
- „výkon/zátěžové“ testování.

Všechny výsledky zkoušek jsou zaznamenány v dokumentu FSM_A.04.V1.

Tab: 13: Validace bezpečnosti vstupní dokumenty

Vstupní dokumenty	
Dokument	Název
DIN 56950-1:2012	Řízené zařízení (EUC) popis podle DIN 56950-1:2012
FSM_A.03.1	Specifikace bezpečnostních požadavků

Tab: 14: Validace bezpečnosti výstupní dokumenty

Výstupní dokumenty				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.04.1	Specifikace validačních testů	Tests Team	SSA	All
FSM_A.04.V1	Zpráva o ověření validačního testů bezpečnosti	Tests Team	SSA	All

10.6.4 **FSM_A.05: Návrh řídicího systému**

Návrh systému zahrnuje:

- rozsah požadavků,
- detekce chyb a reakce na chyby,
- řídicí systém je analyzovaný v systému FMEDA.

Tab: 15: Validace bezpečnosti vstupní dokument

Vstupní dokumenty	
Dokument	Název
DIN 56950-1:2012	Řízené zařízení (EUC) popis podle DIN 56950-1:2012
FSM_A.03.1	Specifikace bezpečnostních požadavků

Tab: 16: Popis architektury systému – výstupní dokument

Výstupní dokumenty				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.05.1	Popis architektury systému	SSA	PrM	All

Tab: 17: Systémová FMEDA – dokument ověření

Dokumenty ověření				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.05.1.V1	Systémová FMEDA	SSA	PrM	N/A

10.6.5 FSM_A.06: Hardware – architektura

Návrh hardware je popsán pomocí popisů obvodů, elektrických schémat, výpisů komponentů atd.

Tab: 18: Hardware architektura vstupní dokumenty

Vstupní dokumenty	
Dokument	Název
DIN 56950-1:2012	Řízené zařízení (EUC) popis podle DIN 56950-1:2012
FSM_A.03.1	Specifikace bezpečnostních požadavků
FSM_A.05.1	Popis architektury systému

Tab: 19: Hardware architektura výstupní dokumenty

Výstupní dokumenty				
Dokument	Název	Autor	Schválení	Posouzení
Z18126-8-01-VY-000 Z18126-8-01-VY-001 Z18126-8-01-VY-002 Z18126-8-01-VY-010 Z18126-8-01-VY-050 Z18126-8-01-VY-060	Typické zapojení obvodů, popisy obvodů, seznamy	Projektant	SSA	PrM

Tab: 20: Hardware architektura dokumenty ověření

Dokumenty ověření				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.06.2.2	Systém/Komponenty FMEDA Specifikace režimu selhání pro systém	SSA	PrM	N/A
FSM_A.06.3.V2	PFH výpočty pravděpodobnosti nebezpečné poruchy za hodinu	SSA	PrM	N/A
FSM_A.06.3.V4	Simulace poruch bezpečnostních funkcí	SSA	PrM	N/A

10.6.6 FSM_A.07: Software – architektura

Softwarová architektura zahrnuje:

- strukturu softwaru a jeho rozhraní,
- dynamické a statické chování aplikovaného software,
- poruchy a chování.

Tab: 21: Software architektura vstupní dokumenty

Vstupní dokumenty	
Dokument	Název
DIN 56950-1:2012	Řízené zařízení (EUC) popis podle DIN 56950-1:2012
FSM_A.03.1	Specifikace bezpečnostních požadavků
FSM_A.05.1	Popis architektury systému

Tab: 22: Software architektura výstupní dokumenty

Výstupní dokumenty				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.07.1	Popis softwarové architektury	Vývojáři	SSA	N/A

Tab: 23: Software architektura dokumenty ověření

Dokumenty ověření				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.07.V1	Způsobilost a oprávněnost používání již existujícího bezpečnostního softwaru a jeho komponent	SSA	PrM	N/A

10.6.7 **FSM_A.08: Software Design**

V softwarovém designu se realizuje několik různých integračních testů a činností:

- SW – SW integrace,
- HW – SW integrace,
- systémová integrace.

Tab: 24: Software design – vstupní dokument

Vstupní dokumenty	
Dokument	Název
FSM_A.05.1	Popis architektury systému
FSM_A.07.1	Popis architektury softwaru
Z18126-8-01-VY-000 Z18126-8-01-VY-001 Z18126-8-01-VY-002 Z18126-8-01-VY-010 Z18126-8-01-VY-050 Z18126-8-01-VY-060	Typické zapojení obvodů, popisy obvodů a seznamy

Tab: 25: Software design – výstupní dokumenty

Výstupní dokumenty				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.08.1	Popisy funkcí systému	SSA	PrM	N/A

Tab: 26: Software design dokumenty ověření

Dokumenty ověření				
Dokument	Název	Autor	Schválení	Posouzení
FSM_A.08.V1	Testováni „black box“	SSA	PrM	N/A

10.6.8 **Kompetence jednotlivých osob**

V následující tabulce jsou zapsány jména jednotlivých kompetentních osob v realizovaném projektu.

Tab: 27: Kompetence osob

Role	Jméno	Příjmení
produktový manažer		
vývojový manažer/specialista pro funkční bezpečnost		
manažer kvality		
vývojový manažer HW		
vývojový manažer SW		
zkušební technik		
technik realizace/instalace		

Matice kompetencí testovacího týmu:

Tab: 28: Matice testovacího týmu

Téma:	produktový manažer	vývojový manažer	manažer kvality	vývojový manažer SW	zkušební technik	technik realizace/instalace
znalost systému	X	X	X	–	–	–
znalost systematického vývoje a ověřování a validačních procesů	X	X	X	–	–	–
funkční testy	X	X	–	X		
FMEDA; FTA; Rizikové analýzy;	–	X	X	–	–	–
požadavky managementu	X	X	–	X	–	–
software	–	X	–	X	–	–
řízení funkční bezpečnosti	X	X	–	–	–	–
plánování a koordinace činností v oblasti řízení funkční bezpečnosti	X	X	–	–	–	–
zvýšení bezpečnostních otázek	X	X	X	–	–	–
vývoj bezpečnostních požadavků	X	X	–	–	–	–
realizace bezpečnostních požadavků	X	X	X	X	–	–
plánování, tvorba dokumentace, ověřování a validace	–	X	X	X	X	X
správa konfigurace	X	X	X	X	–	–
elektrikář – vzdělávání a požadavky místního právního zákona	X	X	–	–	X	X

Tab: 29: Specifikace vývojových nástrojů

Název	Verze	Kl.	Certifikace
TwinCAT 2,3 (FSoE)	N/A	T3	TÜV SÜD certifikát
TwinSAFE Loader	v1.6 Build 2	T3	TÜV SÜD certifikát
TwinSAFE logic FB	v1.6 Build 2	T3	TÜV SÜD certifikát
TwinCAT System Manager	v2.11.0 (Build 2277)	T3	TÜV SÜD certifikát
TwinSAFE User	Administrator	T3	TÜV SÜD certifikát
TwinCAT PLC Control	v2.11.0 (Build 2605)	N/A	N/A

10.6.9 Klasifikační nástroje

Pro klasifikaci nástrojů jsou použity normy ČSN EN 61508-4 ed.2:2011 a EN 61508-3 ed.2:2011 odstavec 7.4.4.

10.6.10 Verze nástrojů použitých pro projekt iTEMS

Použité nástroje pro realizaci kódu.

Tab: 30: Použité softwarové nástroje

Nástroj	Výrobce	Verze	Používané od
TwinCAT 2,3	BECKHOFF	v2.11.2258	2013
EtherCAT	BECKHOFF	v2.11.2258	2013

10.7 PLÁN VALIDACE (FSM_A.02.2)

Tab: 31: Plánování testů

Popis	Místo/datum
Datum provedení testů:	2. 2. 2018
Zkušební vzorek, který bude vyroben k datu:	15. 1. 2018
Místo provedení testů:	Újezd u Brna
Vytvoření zkušebního protokolu validačního testování bezpečnostních funkcí:	FSM_A.08.V2

10.8 SPECIFIKACE BEZPEČNOSTNÍCH POŽADAVKŮ (FSM_A.03.1)

Certifikační orgán:

TÜV SÜD Czech s.r.o., Praha 4, Novodvorská 994, PSČ 14221

Požadavky nezávislé na architektuře produktu:

- EU směrnice o výrobcích: 2014/35/EU; 2014/30/EU,
- EN harmonizované normy – odvozené požadavky.

Komponenty pro realizaci SIF jsou:

- vestavěné z komponent standardní průmyslové automatizace,
- sestavené z průmyslových komponent označených CE,
- sestavené z komponentů poskytnutých třetí stranou.

10.8.1 **Podmínky prostředí**

Tab: 32: Podmínky prostředí

Název	Hodnoty
Teplota – provoz	Min. – *0,0* °C Max. + *55* °C
Teplota – transport, skladování	Min. – *40* °C Max. + *70* °C
Vlhkost	Průměrná relativní vlhkost: *68*% Maximální relativní vlhkost: *95*% Minimální relativní vlhkost: <*7*%
Tlak – provoz, transport, skladování	Od *750* hPa do *1100* hPa
EMC	Minimální požadavky dle DIN 56950-1:2012 odstavec 7.1.4.2
Vibrace	Dle souboru norem EN 60068
Krytí	Pro venkovní instalaci min. IP54 Pro vnitřní instalaci min. IP20

10.8.2 **Doby odezvy pro systém (SIF)**

Tab: 33: Doba odezvy

Sub – systém	Doba odezvy
Sensor	500 ms (zatížený, binární stav, …) 10 s (teplota, analýzy)
Logika	500 ms
Motor, regulátor, akční člen	1000 ms pro elektrické komponenty

10.8.3 **Alarmy a identifikace SIF v HMI**

Všechny alarmy jsou dostupné obsluze přes rozhraní HMI. Veškeré funkce končící ve stavu bezpečného zastavení zařízení a jeho odpojení od elektrické energie jsou obsluhou přes rozhraní HMI odsouhlaseny a v rámci bezpečnostních obvodů znovu aktivovány. V rámci bezpečnostních funkcí je zamezeno automatickým resetům. Všechny stavy jsou logovány s časovým razítkem.

Funkční požadavky

Manuální vypnutí zařízení není možné, pokud se nejedná o bezpečné vypnutí.

Bypass SF je možný pouze za podmínek:

- během systémového spuštění nebo po restartu,
- během procesu, kdy není požadavek na SF,
- během procesu testování SF nebo jednotlivých částí SF,
- bypass může být vytvořený pouze prověřenou osobou nebo prověřeným personálem,
- aktivace bypass je dvojstupňová,
- bypass je realizovaný pomocí Login PINu nebo klíče,
- bypass aktivace je viditelně označená,
- bypass aktivace je časově omezená.

10.8.4 **Požadavky závislé na architektuře**

10.8.4.1. **Požadované SIL**

SIF bezpečnostní funkce splňuje SIL3.

10.8.4.2. **Režim vyžádání**

Všechny funkce spojené s bezpečností jsou provozovány v režimu s vysokým vyžádáním /High Demand Mode/.

10.8.4.3. **Požadavky na interval pro kontrolní testy – T1**

Všeobecné požadavky pro T1:

Tab: 34: Intervaly pro kontrolní testy

Test	T1
Funkční test SIF test	1 rok
Testování senzorů	2 roky
Logický test subsystému	20 roků
Test subsystému pro pohonné jednotky	2 roky

Požadavky na střední dobu do obnovy – MTTR

Tab: 35: Požadavky na MTTR

HFT	MTTR
HFT = 1 (1oo2, 1oo2D architektury)	24 hodin
HFT = 0 (1oo1)	0

10.8.5 **Požadavky odvozené od architektury**

Spolehlivost a ochrana spojená s SIF má následující atributy:

- všechny logické kontroléry (programovatelná logika, atd.) mají certifikáty funkční bezpečnosti ze spolehlivých zdrojů (TÜV, Exida, apod.),
- všechny ostatní komponenty mají spolehlivé bezpečnostní, pravděpodobnostní data. Spolehlivost a poruchovost jsou doloženy výrobcem komponent nebo z jiného spolehlivého zdroje,
- spínací a kontrolní mechanismy spojené se SIF implementací jsou v souladu s EN 60947-4-1 ed.3:2010, v platném znění,
- všechny elektromechanické stykače spojené se SIF implementací jsou všechny kontakty ve formě nuceně vedených kontaktů – podle EN 60947-4-1 ed.3:2010 (viz. dodatek “F” této normy), v platném znění,
- všechny spínací zařízení spojené se SIF implementacemi jsou vyrobeny jako /Forced–disconnect/ spínače – podle EN 60947-5-1 ed.3:2018 (viz. dodatek “K” této normy), v platném znění,
- všechny komponenty jsou vybavené řádnými diagnostickými funkcemi.

10.8.5.1. **Požadavky na diagnostické pokrytí DC**

Všechny použité komponenty jsou vybaveny vhodnými diagnostickými funkcemi. Pro jednotlivé SIF je stanoveno výsledné diagnostické pokrytí DC /Diagnostic Coverage/.

10.8.5.2. **Komunikační spojení**

Pro komunikační spojení v rámci bezpečnostních funkcí je použit pouze protokol FSoE/Fail Safe over EtherCAT/.

10.9 BEZPEČNOSTNÍ FUNKCE 1 – NOUZOVÉ ZASTAVENÍ (FSM_A.03.2)

10.9.1 Logické uspořádání subsystémů funkce

Bezpečnostní funkce je provedena jako dvoukanálové zapojení viz Obr. 25.

Vstupní periferie

Každé použité hřibové tlačítko je vybaveno dvojicí rozpínacích kontaktů (NC). Kontakty jsou provedeny s nuceným vypnutím. Každý rozpínací kontakt se zapojuje samostatně do bezpečnostního vstupu PLC.

Kanál 1

První kontakt hřibového tlačítka je zapojen do samostatného bezpečnostního vstupu bezpečnostního PLC. Kanál je kontrolován vysíláním a přijímáním pulsů procházejících kanálem.

Kanál 2

Druhý kontakt hřibového tlačítka je zapojen do samostatného bezpečnostního vstupu bezpečnostního PLC Obr. 26. Kanál je kontrolován vysíláním a přijímáním pulsů procházejících kanálem.

Výstupní periferie

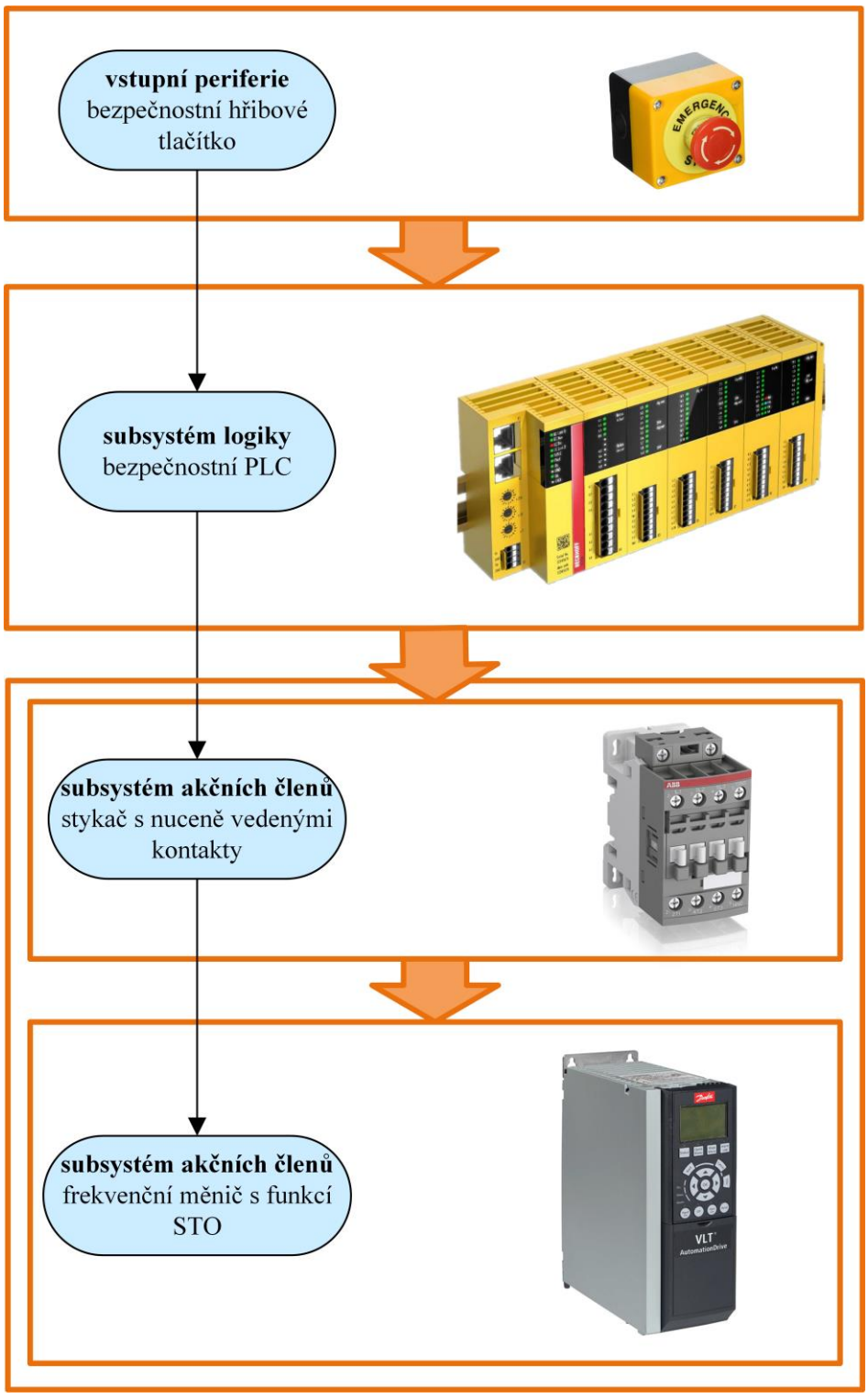
Kanál 1

V bezpečnostním výstupu DO1 je zapojen odpínací stykač umístěný před frekvenčním měničem Obr. 27. Stykač KM1 slouží k odpojení frekvenčního měniče od elektrické energie. Stykač je aktivován samostatným bezpečnostním výstupem řídicího systému. Stykač je kontrolován proti „zapečení“ zapojením rozpínacího kontaktu jako zpětné vazby (EDM), zpět do řídicího systému. Zvolený stykač odpovídá požadavkům ČSN EN 60947-1 ed.4:2008 a ČSN EN 60947-4-ed.3:2010. Bezpečnostní výstup má zapnutou kontrolu měření proudu a obvodem prochází testovací pulsy.

Kanál 2

V bezpečnostním výstupu DO2 je zapojen frekvenční měnič, který je vybaven bezpečnostním vstupem úrovně SIL2 pro zastavení v kategorii 0. Tento vstup je aktivován bezpečnostním výstupem řídicího systému. Současně je frekvenční měnič připojen přes komunikační rozhraní datovou linkou do řídicího systému. Tato komunikace slouží ke kompletní diagnostice frekvenčního měniče.

Ve většině případů dochází k odepnutí pohonu od energie až po dosažení nulových otáček, neboť časová odezva bezpečnostního systému se přibližně blíží rychlé brzdící rampě frekvenčního měniče. Dochází tak k zastavení po rampě s následným odepnutím od energie. Funkce je navržena pro bezpečnostní integritu úrovně SIL3.

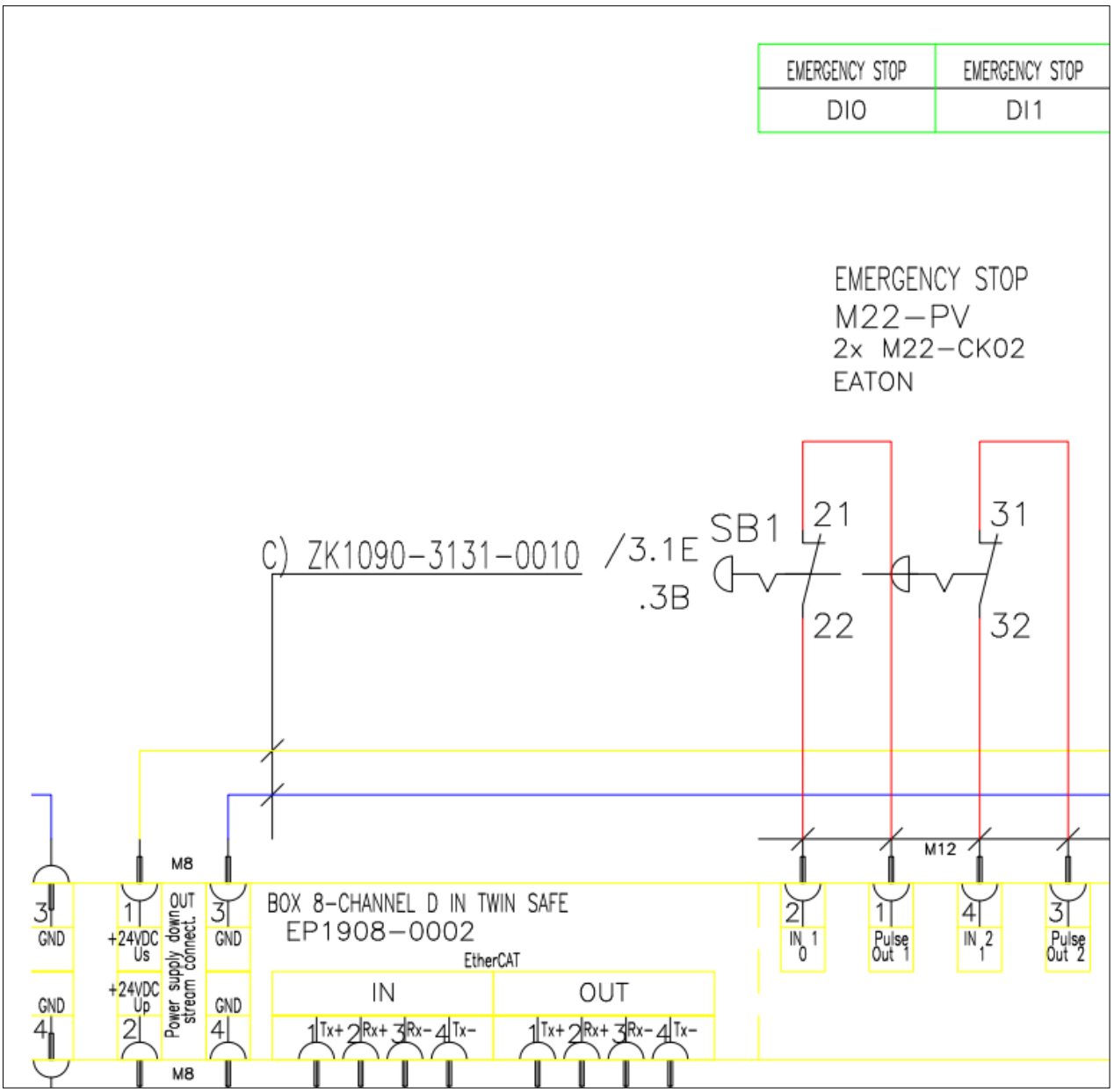


Obr. 25: Logické uspořádání bezpečnostní funkce SF1

Níže je uveden příklad, který popisuje bezpečnostní funkci v detailním zpracování s jednotlivými klíčovými částmi dokumentu.

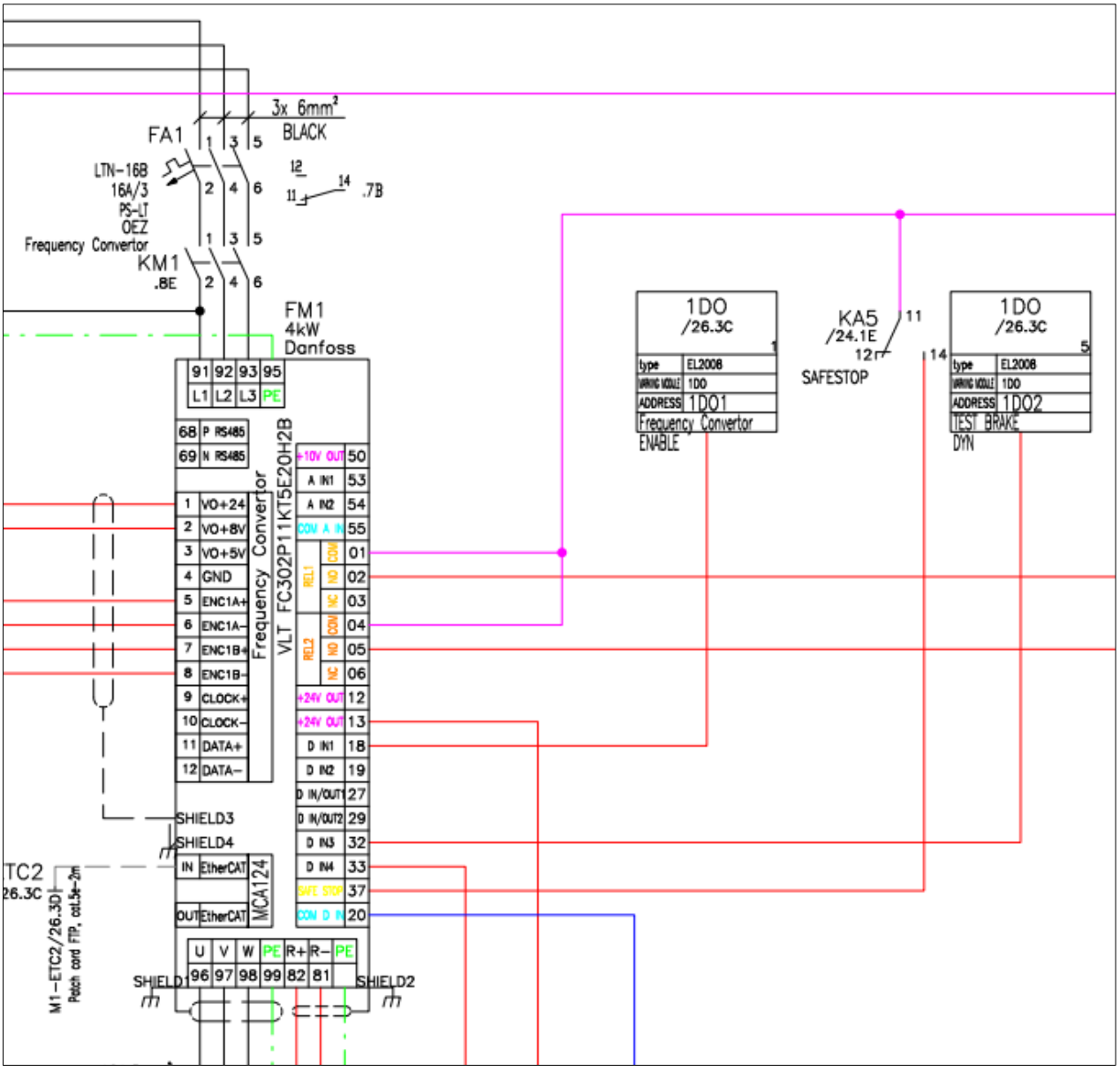
10.9.2 **Popis bezpečnostní funkce**

Bezpečnostní funkce SF1 – nouzové zastavení slouží k nouzovému zastavení pohybu jednotlivých pohonů zapojených do systému řízení. K aktivaci funkce dojde stisknutím libovolného bezpečnostního hřibového tlačítka např. SB1, které je zavedeno do bezpečnostního PLC zobrazeného na Obr. 26.



Obr. 26: Zapojení tlačítka nouzového zastavení

Výstupní funkce je realizována odpínacím stykačem KM1 a frekvenčním měničem FM1 na Obr. 27, které jsou každý jednotlivě aktivovány bezpečnostními výstupy řídicího systému 1DO1 a 1DO2. Současně dochází při aktivaci funkce k vydání povelu pro zastavení frekvenčnímu měniči přes komunikační rozhraní po datové lince – aktivace rychlé brzdící rampy.



Obr. 27: Zapojení frekvenčního měniče

Pokud by došlo k selhání tohoto povelu, paralelně jsou aktivovány povely pro odepnutí stykače KM1 a pro bezpečné zastavení STO (Safe Torque Off), svorka 37 frekvenčního měniče FM1 bezpečně odepne pohon od energie. Ke konečnému zastavení pohybu zařízení zapojeného do řídicího systému dojde aktivací dvojité elektromechanické brzdy. Pro jevištní mechanismy horní sféry je provedeno od

časování sepnutí jedné brzdy vůči druhé. Pro mechanismy dolní sféry jsou brzdy uvedeny v činnost současně. Z funkčního pohledu je možné funkci rozdělit na odpojení od energie a vlastní zastavení zařízení.

10.9.3 Požadavky na provedení

Vlastní zastavení zařízení

Pro zastavení je vyslán povel frekvenčnímu měniči, který zastavení po rychlé rampě quick-stop. Tento povel je vyslán pomocí komunikační linky a současně přes diskrétní vstup frekvenčního měniče /Enable/. Po obdržení tohoto povelu frekvenční měnič začne ukončovat pohyb snižováním rychlosti po stanovené rampě. Současně jsou vyslány povely pro zabrzdění jednotlivých brzd Obr. 29.

Povely pro realizaci rychlé rampy jdou v obou kanálech současně a ve frekvenčním měniči jsou logicky hodnoceny operandem „AND“. Tato hodnota je posílána kvůli diverzitě signálu.

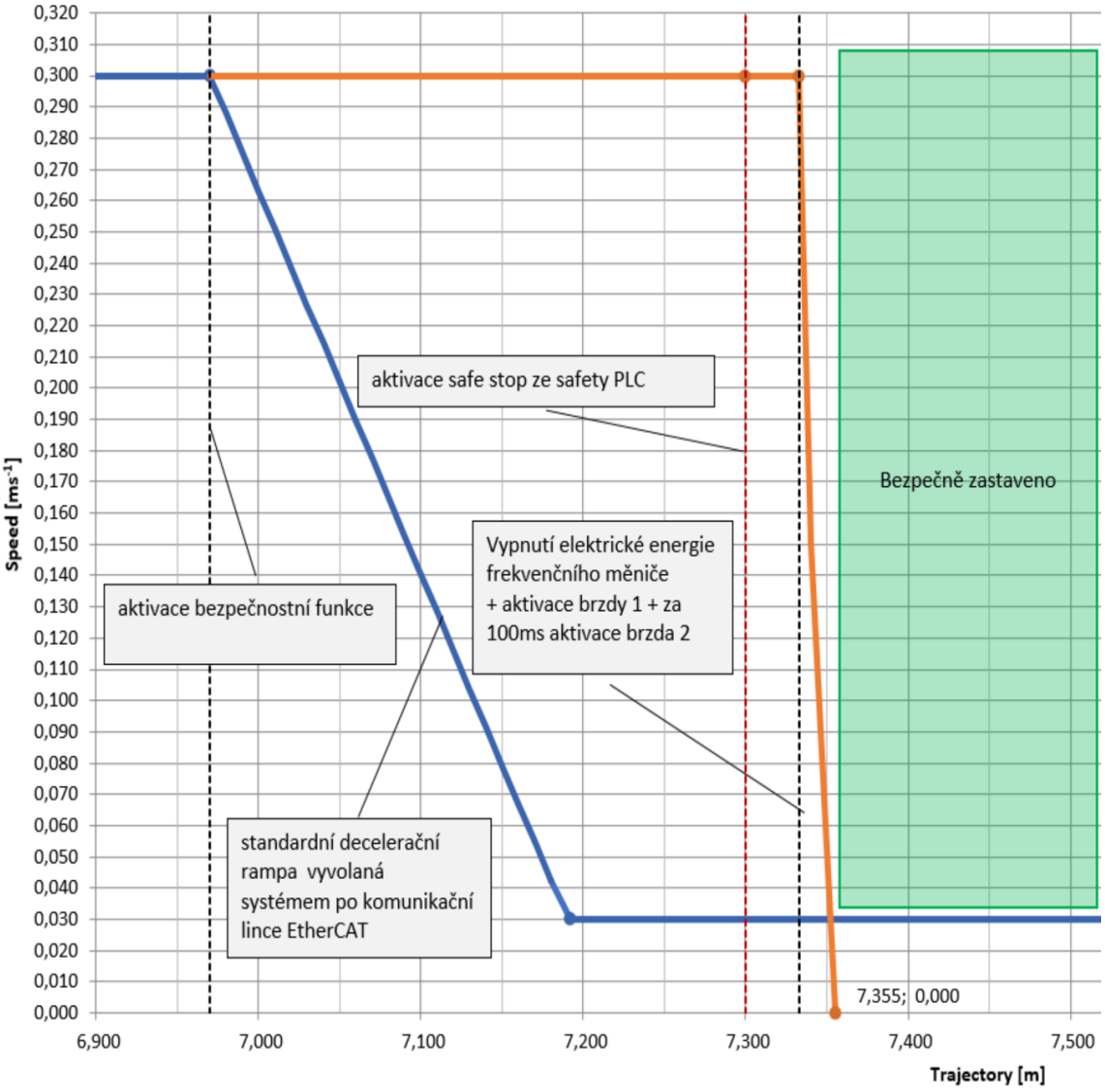
Vzhledem k rozlišnosti jevištních zařízení je před aplikací této funkce vždy proveden rozbor silových účinků brzd na dané zařízení a je zvolena správná brzdící rampa. Obecně se dá říci, že zařízení dolní sféry mohou oba dva kanály této funkce spouštět současně a to s rychlým brzděním a u zařízení horní sféry je provedeno od časování a rychlé brždění je použito pouze v jednom z kanálů.

10.9.4 Rozbor momentů na převodovce tahu

Řešení pohonů zařízení horní sféry v řídicích obvodech zajistí postupné brždění dvojice brzd na Obr. 28.

Obr. 28: Asynchronní elektromotor s dvojitou brzdou

To znamená, že v případě nouzového zastavení dojde k aktivaci zrychlené dojezdové rampy pomocí frekvenčního měniče. Současně s tímto probíhá rychlá aktivace první brzdy. S odstupem 100 ms započne aktivace druhé brzdy. V okamžiku počátku účinku první brzdy jsou již otáčky motoru podstatně snížené a frekvenční měnič, který do tohoto okamžiku brzdil, se bude snažit zachovat požadovanou dojezdovou rampu dodáním potřebného momentu k překonání brzdy zobrazené na Obr. 29.



Obr. 29: Graf bezpečného zastavení

Jednotlivé případy bezpečného zastavení:

- v případě selhání frekvenčního měniče následuje při nouzovém zastavení akce první brzdy, která sníží rychlost na nulu nebo na tak malou hodnotu, aby účinek druhé brzdy nezpůsobil na hřídeli převodovky větší přetížení než je 200% jmenovitého momentu,
- v případě selhání první brzdy následuje při nouzovém zastavení úplný dojezd pohonu po řízené rampě. Následně zapůsobí druhá brzda a měnič se vypne,
- v případě selhání druhé brzdy následuje při nouzovém zastavení dojezd jako při původním bezporuchovém zastavení s tím rozdílem, že v závěru se druhá brzda nezúčastní podržení nulové rychlosti,
- maximální moment, jehož bude dosaženo, nepřekročí hranici 200% momentu pro ustálený chod s 100% zátěží tahu.

Nouzové zastavení je koncipováno jako zastavení v kategorii 1. V případě selhání frekvenčního měniče přejde zastavení do kategorie 0 s tím, že brzdy budou aktivovány postupně, aby nebyl jednorázově překročen 200% momentu jmenovité zátěže pohonu.

10.9.5 Požadavky na ostatní profese

Dimenzování momentu každé jednotlivé brzdy tak, aby bylo možné zabrzdění zařízení z plné rychlosti s příslušným koeficientem bezpečnosti, jak je uvedeno v DIN 56950-1:2012-05, kapitola 5.2.6.1.

Provedení rozboru silových účinků brzd na zařízení – určení odstupu sepnutí jedné brzdy vůči druhé.

10.10 VERIFIKACE POMOCÍ SIMULACE CHYB U VÝROBCE (FSM_A.02.V1)

Simulace – /Fault insertion tests/ – jsou prováděny jen na necertifikovaných subsystémech.

Certifikované subsystémy jsou považovány za vyhovující v případě jejich předepsaného použití.

10.10.1 Simulace poruchy (Normal Closed Contact) – vstupy (1oo2d)

Tab: 36: Simulace poruch – vstupy

Popis	Stav	Poznámka
odpojení vodiče ze svorky bezpečnostního PLC – simulace selhání vodiče v jednom ze dvou kanálů k tlačítku	OK	Error zpráva. Aktivace brzd a zastavení pohonu.
propojení vodičů jednotlivých kanálů mezi svorkami bezpečnostního PLC – simulace křížových zkratů v přívodních vodičích	OK	Error zpráva. Aktivace brzd a zastavení pohonu.
přivedení napájecího napětí +24V = na svorku bezpečnostního PLC – simulace zkratu napájecího napětí přívodního vodiče	OK	Error zpráva. Aktivace brzd a zastavení pohonu.

Simulace poruchy tlačítka reset

Tab: 37: Simulace poruch – tlačítko reset

Popis	Stav	Poznámka
odpojení vodiče ze svorky bezpečnostního PLC (komplementární kontakty) – simulace selhání vodiče v jednom ze dvou kanálů k tlačítku	OK	Error zpráva. Aktivace brzd a zastavení pohonu.
přivedení napájecího napětí +24V = na svorku bezpečnostního PLC – simulace zkratu napájecího napětí na přívodní vodiče	OK	Error zpráva. Aktivace brzd a zastavení pohonu.

10.10.2 **Simulace poruchy relé s nuceným vedením kontaktů**

Tab: 38: Simulace poruch – porucha relé

Popis	Stav	Poznámka
přivedení napájecího napětí +24V = na cívku relé, když má být bez napětí – popř. mechanicky sepnout stykač šroubovákem – simulace selhání relé v sepnutém stavu (svaření kontaktů). Simulace zkratu přivedením cizího napětí.	OK	Nelze kvitovat. Stav je v HMI.
odpojení zpětnovazebního kontaktu – simulace upadnutí drátu	OK	Nelze kvitovat. Stav je v HMI.

10.10.3 Simulace poruchy brzdy – provádí se pomocí testů brzd

Tab: 39: Simulace poruch brzdy

Popis	Stav	Poznámka
spuštění testu v jiné než stanovené výšce – simulace chyby obsluhy	OK	Test se neprovede. Pohon je v zajištěném stavu.
sestavení testu při nedostatečné výšce – simulace chyby testu	OK	Error zpráva. Aktivace brzd a zastavení pohonu. Vyhodnocení testu jako porucha brzd.
mechanické od aretování jedné z brzd při spuštěném statickém testu – simulace chyby brzdy před statickým testem a během něho	OK	Error zpráva. Opětovná aktivace brzdy a zastavení pohonu (rychlostní diference 1mm/s). Vyhodnocení testu jako porucha brzd.
mechanické od aretování jedné z brzd při spuštěném dynamickém testu – simulace chyby brzdy před dynamickým testem a během něho	OK	Error zpráva. Aktivace brzdy a zastavení pohonu. Vyhodnocení testu jako porucha brzd.

10.10.4 Simulace výpadku komunikace s řídicím počítačem

Tab: 40: Simulace poruch komunikace řídicího systému

Popis	Stav	Poznámka
odpojení RJ45 komunikace EtherCAT – simulace poruchy spojení řídicího systému	OK	Error zpráva. Aktivace brzd a zastavení pohonu.
odpojení kabelu pultu během jízdy s pohonem – simulace ztráty řízení	OK	Error zpráva. Aktivace brzd a zastavení pohonu.

10.11 SPECIFIKACE VALIDAČNÍCH TESTŮ BEZPEČNOSTI (FSM_A.04.1)

Specifikace validačních testů bezpečnosti vychází z plánu validace a předchozích dokumentů, do detailu plánuje požadavky na testy a jejich technické provedení.

10.11.1 Specifikace testu – ověření bezpečnosti

- testy jsou prováděny na testovacích stojanech,
- testy jsou prováděny pro ověření bezpečnostních funkcí SF.

Tab: 41: Popis bezpečnostní funkce

Pořadí bezpečnostní funkce	Úplný název bezpečnostní funkce
Bezpečnostní funkce SF1	Nouzové zastavení (Emergency STOP)

Funkce je testována záměrným uvedením do činnosti – simulace bezpečnostní funkce v činnosti. Ve většině případů je nutné aktivování vstupního zařízení.

Funkce bezpečného pohybu je testována správným způsobem a správnou funkcí:

- sledování požadavků a provedení je zajištěna dokumentací,
- testovací případy jsou specifikované,
- specifikování zátěže, aby byl správně zatěžovaný motor.

Testovací kritéria jsou splněná pokud:

- funkce bezpečného zastavení má bezpečný stav – kdy je zařízení v klidu.

Testovací kritéria nejsou splněná:

- pohyb pokračuje po kvitaci bezpečnostní funkce a stisknutím „dead men“ tlačítka umístěného na ovládacím pultu.

10.11.2 Zdroje pro testování

Zdroje pro testování jsou specifikovány jako sestavy simulací pro zkoušky kompletních řetězců bezpečnostních funkcí a to jak ve spojení s hardwarem tak ve spojení se softwarem. Zodpovědnost pro zdroje a testovací stojany má SSA.

10.12 ZPRÁVA O OVĚŘENÍ VALIDAČNÍCH TESTŮ BEZPEČNOSTI (FSM_A.04.V1)

Data testu:

EDM – 3s, 1s zpoždění při vypnuté “ENABLE” (SF3), 1,5s zpoždění + 3s časový filtr (SF4), 100ms zpoždění druhé 2nd brzdy (SF9)

400ms mezi “local stop” a frekvenčním měničem STO (všechny funkce aktivují STO). V systému iTEMS je specifikovaných dalších osm bezpečnostních funkcí:

- bezpečnostní funkce SF1 – Emergency Stop,
- bezpečnostní funkce SF2 – Překročení rychlosti,
- bezpečnostní funkce SF3 – Funkce „dead men“,
- bezpečnostní funkce SF4 – Přetížení zařízení,
- bezpečnostní funkce SF5 – Ochrana proti střihu bezpečnostních lišt,
- bezpečnostní funkce SF6 – Ochrana dveří proti vniknutí do nebezpečného prostoru,
- bezpečnostní funkce SF7 – Bezpečné I/O rozhraní,
- bezpečnostní funkce SF8 – Bezpečná pozice,
- bezpečnostní funkce SF9 – Bezpečné ovládání brzdy.

Záznam výsledků testů:

Tab: 42: Záznam o testu bezpečnostní funkce

Bezpečnostní funkce	Kritéria pro splnění	Stav	Výsledek	Poznámka
SF1 – Emergency Stop	pohyb zastavený informace na HMI	OK	uspěl	Tlačítko nouzového zastavení aktivováno během pohybu zátěže dolů.

10.12.1 **Výsledky testu**

Validace testování potvrdila splnění všech základních požadavků pro FS. Testování proběhlo na rozvodnicích zapojených ve společnosti Drivecontrol.

Obr. 30: Testování bezpečnostních funkcí

10.13 POPIS ARCHITEKTURY ŘÍDICÍHO SYSTÉMU (FSM_A.05.1)

Bezpečnostní systém iTEMS je určen pro bezpečné ovládání divadelních technologií. Každý systém je jedinečný pro každý projekt divadla a požadovanou konstrukci – např. počet ovládaných motorů horní a dolní mechaniky, točny a dalších specifických pohyblivých technologií a celků.

10.13.1 Certifikační a zkušební orgány

Certifikaci provedla společnost:

TÜV SUD Czech s.r.o.

Na základě technických norem:

- ČSN EN 61508-1 ed.2:2011,
- ČSN EN 61508-2 ed.2:2011,
- ČSN EN 61508-3 ed.2:2011,
- ČSN EN 60204-1 ed.2:2007,
- ČSN EN 60204-32 ed.2:2009.

EMC : Vojenský Technický ústav, s.p.

10.13.2 Použití existujících komponentů

Všechny použité součástky související s bezpečností jsou certifikované třetími subjekty. Bezpečnostní logika je certifikována na SIL3 a vybavena softwarem odpovídajícím souboru norem ČSN EN 61508 ed.2:2011.

10.13.3 Omezení a předpoklady

Vývoj řídicího systému iTEMS je založen na určitých omezeních a předpokladech, například:

- certifikované komponenty splňují požadavky na nárokované certifikované normy,
- jako náhradní díly je třeba vždy používat tyto součásti,
- v případě výměny komponent v budoucnu je vysoká pravděpodobnost, že bude na trhu správná náhrada,
- komponenty certifikované standardy EMC splňují základní požadavky na konečnou shodu požadavků EMC,
- dodávané a certifikované komponenty třetích stran jsou pod kontrolou výrobce a certifikačního orgánu.

10.13.4 Procesní vstupy a výstupy

Systém je navržen tak, aby byl kompletní se vstupy, logikou a výstupy. Pro komunikaci s jinými divadelními systémy lze použít:

- Bezpečnostní komunikační protokol FSoE v rámci „EtherCAT“,
- Bezpečnostní digitální a analogové vstupy a výstupy na bezpečnostních PLC.

10.13.5 Bezpečnostní architektura

Položky řídicího systému jsou upřednostňovány pod pojmenovanými hardwarovými architekturami:

Architektura 1oo2D Homogenní redundantní struktura s autonomní diagnostikou.

10.13.6 Bezpečnostní funkce

Byla vybrána bezpečnostní funkce bezpečného zastavení popsaná v dokumentu: FSM_A.03.2_CS_Bezpečnostní_funkce_1

10.13.7 Bezpečnostní komunikace

Bezpečnostní funkce je navržena s protokolem FSoE. Každá jednotka je

naskenována správcem řídicího systému a tato naskenovaná konfigurace je řešena dvěma nezávislými adresami.

10.13.8 Odpovědnost koncového uživatele

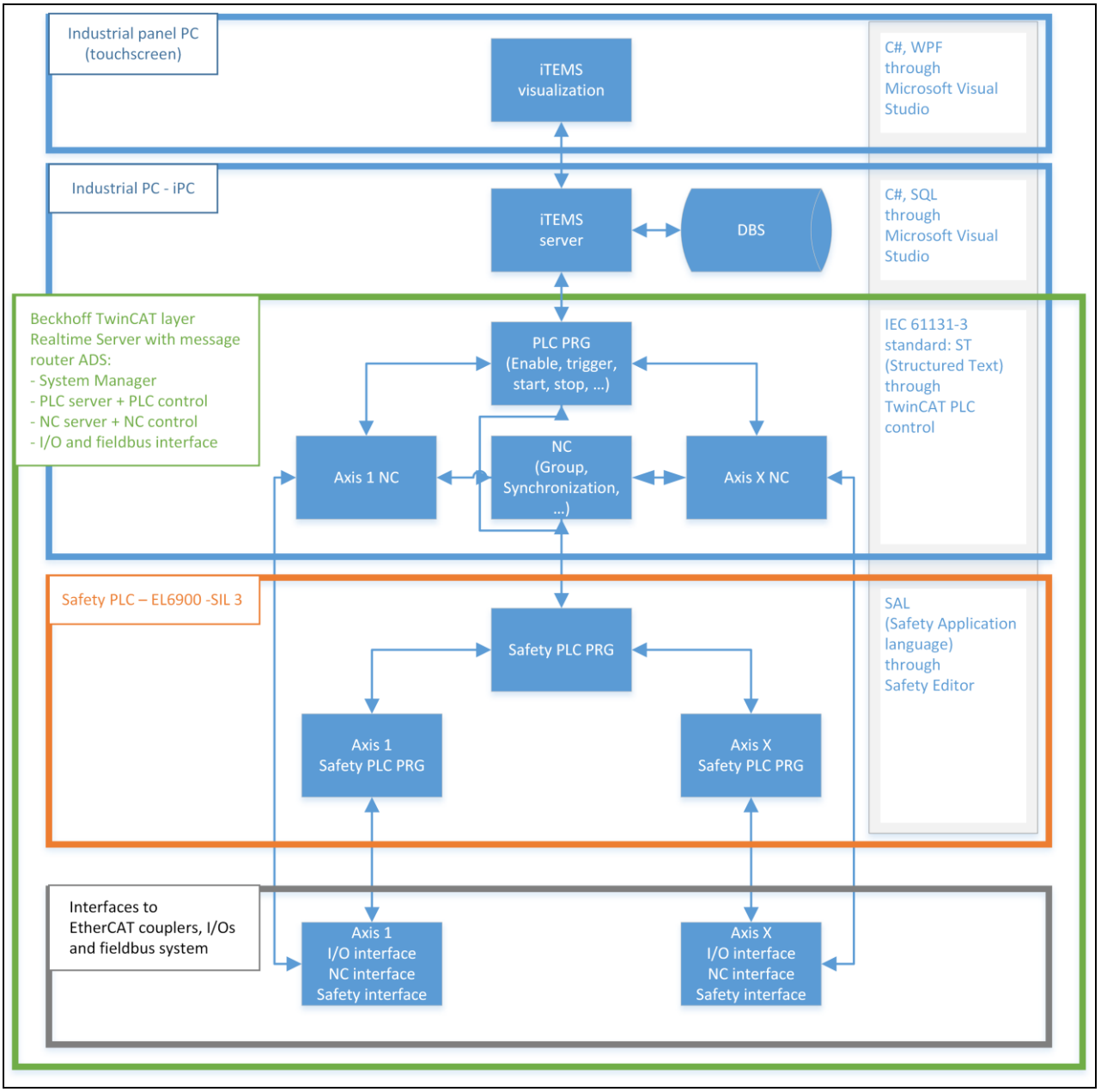
Konečný uživatel je odpovědný za:

- provoz a údržbu systému v souladu s uživatelskou dokumentací předložena výrobcem,
- provedení pravidelné funkční kontroly bezpečnostních funkcí popsaných v uživatelské dokumentaci,
- provádění pravidelné kontroly řídicího systému,
- dodržování bezpečnostní příručky řídicího systému,
- v případě problémů s bezpečnostními funkcemi kontaktuje výrobce.

10.14 ARCHITEKTURA SOFTWARU (FSM_A.07.1)

Řídicí systém společnosti Drivecontrol, s.r.o. nese společný název iTEMS. Tento dokument popisuje architekturu softwaru s popisem použitých technologií a programovacích jazyků – viz Obr. 31. Součástí řídicího systému řízení iTEMS, jsou také části, které souvisejí s bezpečností. Tyto funkce jsou hardwarově i softwarově koncipovány tak, aby splňovaly úroveň integrity bezpečnosti SIL3, dle ČSN EN 61508-1 ed.2:2011 až ČSN EN 61508-7 ed.2:2011.

10.14.1 Blokové schéma architektury softwaru



Obr. 31: Blokové schéma architektury softwaru

10.14.2 **Popis architektury**

Jádro řídicího systému řízení iTEMS je založeno na vývojovém a aplikačním prostředí TwinCAT společnosti Beckhoff Automation GmbH&Co. KG. Na obrázku Obr. 31 je tato část vyznačena zelenou barvou. V případě řídicího systému iTEMS se jedná o kompletní naprogramování PLC části, kompletní naprogramování bezpečnostního PLC a správné nastavení a propojení částí společně s částí NC /Numeric Control/, která zajišťuje regulaci všech zařízení.

Systém je naprogramován konceptem objektového přístupu k programování, kdy je k jednotlivým zařízením přistupováno jako k daným objektům. Vlastní funkčnost řídicího systému vzhledem k nastavení jednotlivých synchronizací (dráhových, časových, apod.) je fyzicky provedena prostřednictvím PLC-NC-safety PLC prostředků. Prostředí TwinCAT je real-time prostředím.

Nadstavbou nad tento real-time systém je iTEMS server, který pak provádí server-klient orientovanou interakci mezi real-time prostředím TwinCAT a mezi klientskými aplikacemi vizualizace, kterých může být libovolný počet. iTEMS vizualizace tak zprostředkovává uživateli přístup k celé funkčnosti řídicího systému, včetně jeho diagnostiky. iTEMS server současně zprostředkovává uchování všech uživatelských nastavení v připojené SQL databázi.

V následujících kapitolách jsou blíže popsány jednotlivé části řídicího systému řízení vzhledem k jeho softwarovému vybavení.

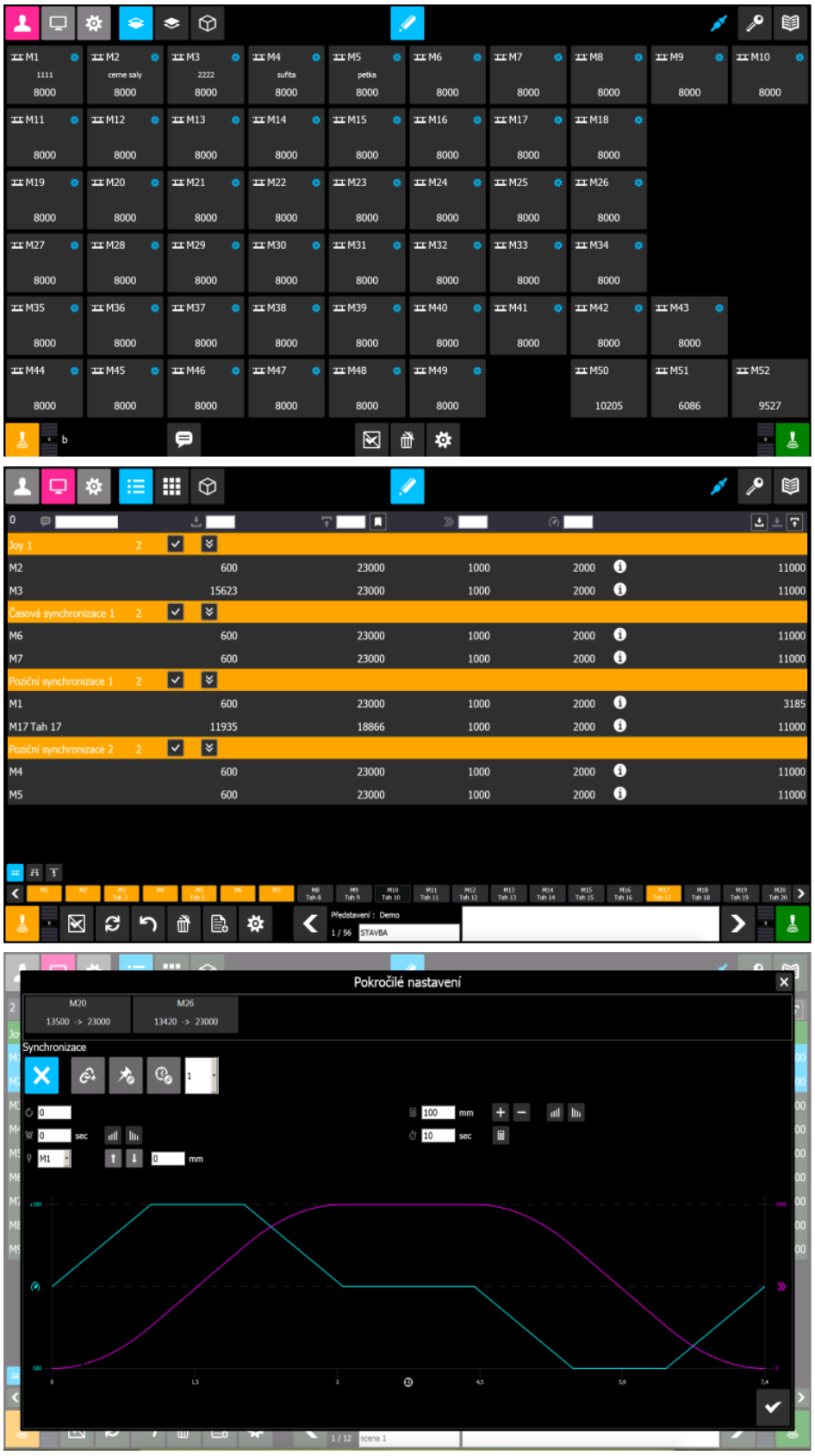
Speciální částí řídicího systému je pak část, na obrázku Obr. 31 označená oranžově, která se týká realizace bezpečnostních funkcí.

10.14.3 **iTEMS vizualizace**

Tato část řídicího systému je instalována na jednotlivé řídicí panely, včetně servisních obslužných panelů. Na Obr. 32 je zobrazen ovládací pult 24´. Na průmyslovém dotykovém /multi–touch/ panelu je instalovaný operační systém Windows 7 Embedded.

Obr. 32: Ovládací pult 24´

Software vizualizace je naprogramován ve vývojovém prostředí Microsoft Visual Studio v programovacím jazyce C#.NET s využitím framework WPF /Windows Presentation Foundation/. Ukázky zobrazení jsou na obrázku Obr. 33. Zdrojové kódy jsou spravovány systémem správy verzí GIT. Komunikace s ostatními částmi systému je prostřednictvím TCP/IP protokolu s vlastním nadstavbovým protokolem ve vyšší vrstvě. Autorem tohoto protokolu je společnosti Drivecontrol, s.r.o.



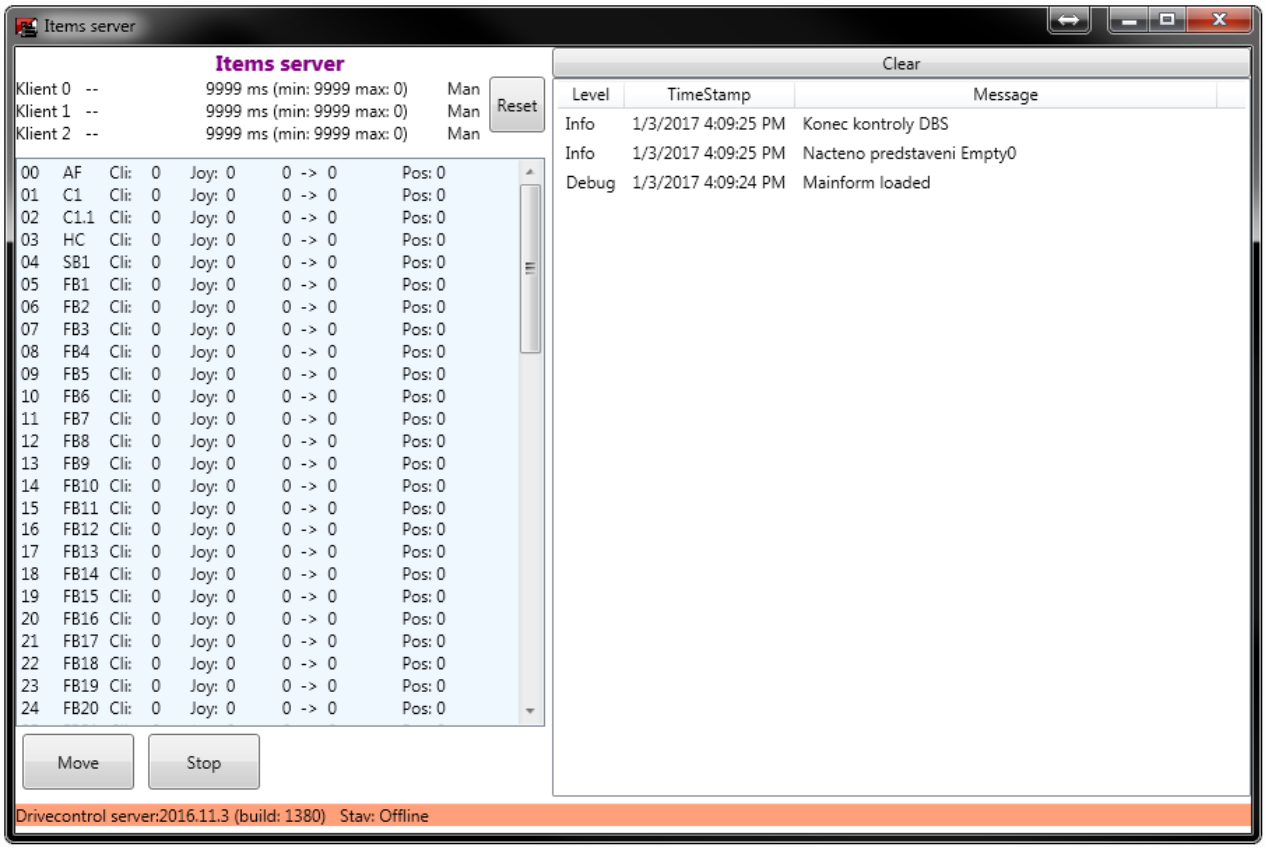
Obr. 33: Ukázky vizualizace

10.14.4 **iTEMS server**

Server pro obsluhu klientských aplikací vizualizace a komunikaci s PLC runtimem řízení je prezentovaná na Obr. 35. Server provádí rovněž přístup do databáze řídicího systému, kde jsou uchovány jednotlivá divadelní představení a další uživatelská nastavení řídicího systému. Obslužná část serverové části není přístupná uživateli. Jako server je použitý průmyslový počítač od společnosti Beckhoff, obvykle shodný s počítačem, na němž je instalováno prostředí TwinCAT. Na Obr. 34 je ukázka primárního a sekundárního serveru, včetně napájecích periferií.

Obr. 34: Server – Beckhoff

Software serveru vizualizace je kompletně naprogramován ve vývojovém prostředí Microsoft Visual Studio v programovacím jazyce C#.NET s využitím Framework WPF /Windows Presentation Foundation/. Zdrojové kódy jsou spravovány systémem správy verzí GIT. Komunikace s ostatními částmi systému je prostřednictvím TCP/IP protokolu s vlastním nadstavbovým protokolem ve vyšší vrstvě. Autorem tohoto protokolu je společnosti Drivecontrol, s.r.o. Obr. 35.

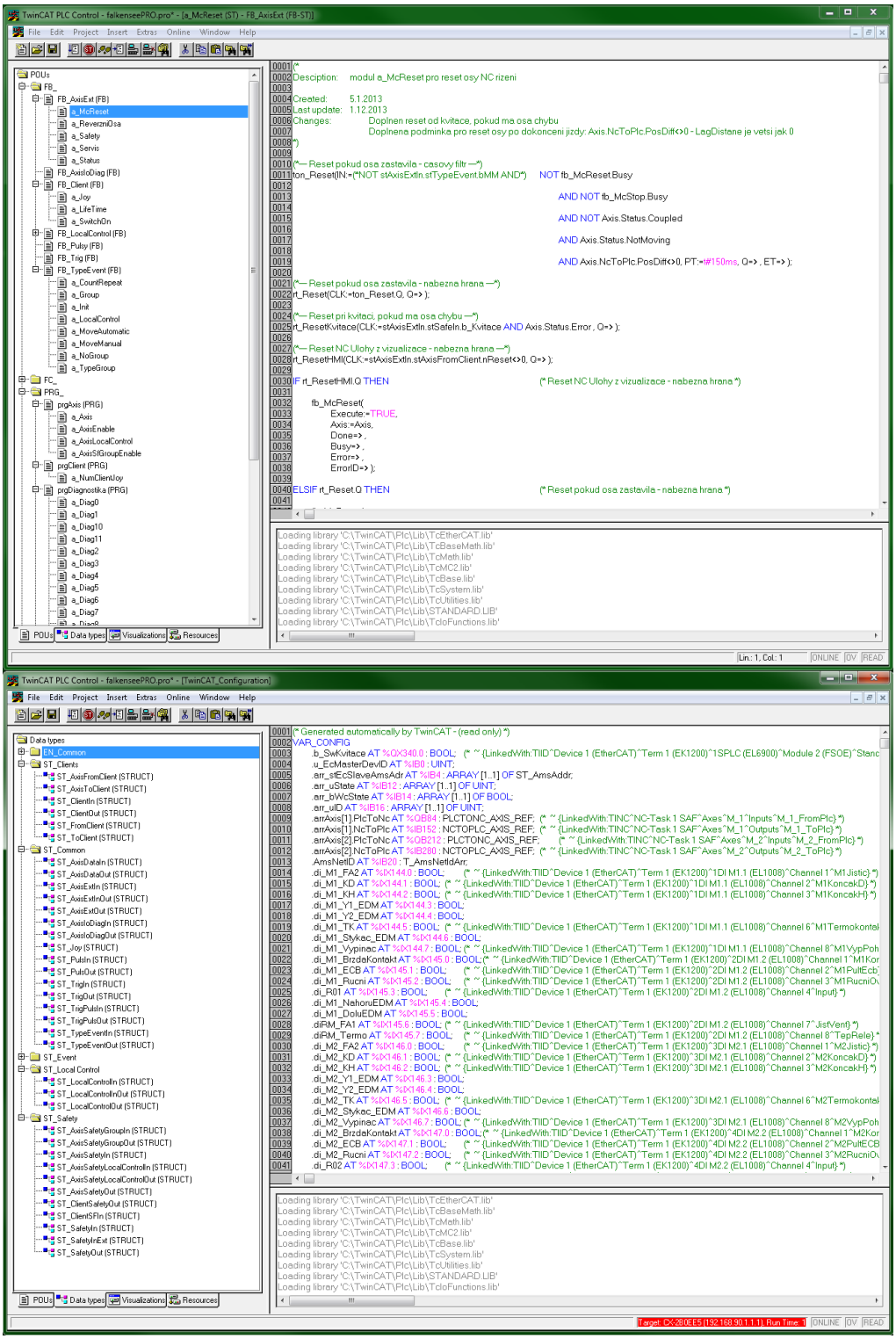


Obr. 35: iTEMS server

Program PLC

Programová část pro PLC runtime v prostředí TwinCAT PLC control. Na Obr. 36 je programová část rozdělena do dvou úloh /Task/. První FAST úloha s časováním 4ms /Cycle time/ obsluhuje volání funkčních bloků pro rychlou komunikaci mezi NC-PLC-frekvenčními měniči. Druhá úloha MAIN obsluhuje volání dalších podprogramů a funkčních bloků sloužících k vybavení požadavků vizualizace v součinnosti se stavem řídicího systému a jednotlivých os. MAIN úloha je časovaná obvykle na 8ms. V PLC PRG se nachází kompletní deklarace proměnných a konstant. Celý PLC program je převeden do binární podoby a není uživateli přístupný. Software PLC runtime je kompletně naprogramován ve vývojovém prostředí TwinCAT PLC Control v programovacím jazyce ST /Structured Text/ dle standardu EN 61131-3 ed.2:2013.

Zdrojové kódy jsou verzovány vzhledem k jednotlivým aplikacím řídicího systému. Komunikace probíhá přes protokol ADS prostřednictvím interního routeru zpráv /Message Router/ v prostředí TwinCAT Obr. 36.

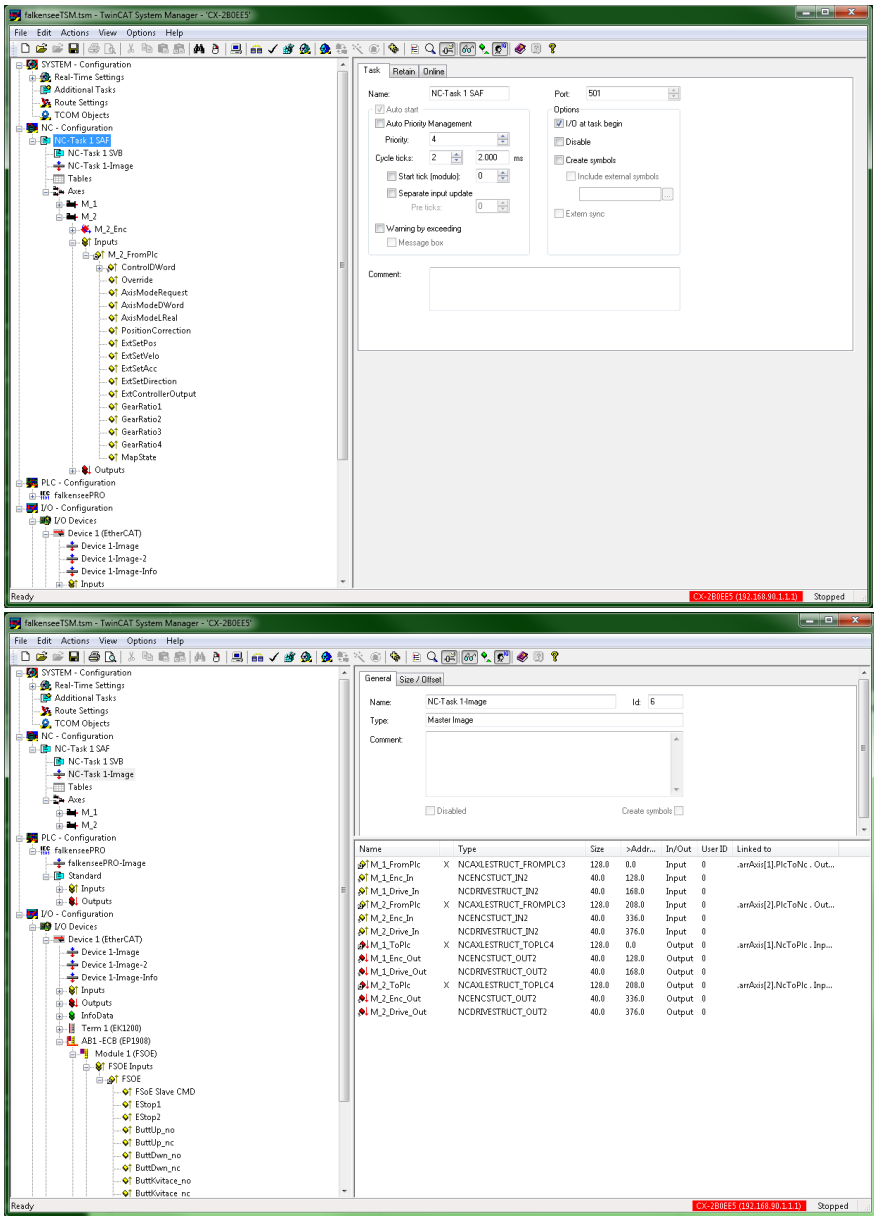


Obr. 36: Program PLC

Regulace zařízení

TwinCAT NC je numerické řízení používané pro regulaci zařízení nebo skupin zařízení, včetně synchronizací Obr. 37. NC úloha obsahuje jeden nebo více PTP /Point-to-point/ kanálů, FIFO kanálů nebo NCI kanálů a jejich dceřinných částí. Obsluha NC runtimu probíhá kompletně prostřednictvím PLC-NC interface, který je cyklický. V NC tasku se jednotlivé osy nastaví a pomocí linkování propojí na hardwarové I/O a do PLC pomocí nastaveného interface. Kompletní konfigurace je nastavena na pevno a není uživateli přístupná.

Základní nastavení NC řízení se provádí v systémovém manažeru prostředí TwinCAT a obsluha pak z PLC PRG pomocí interface Obr. 37.



Obr. 37: Motion control

Bezpečnostní PLC

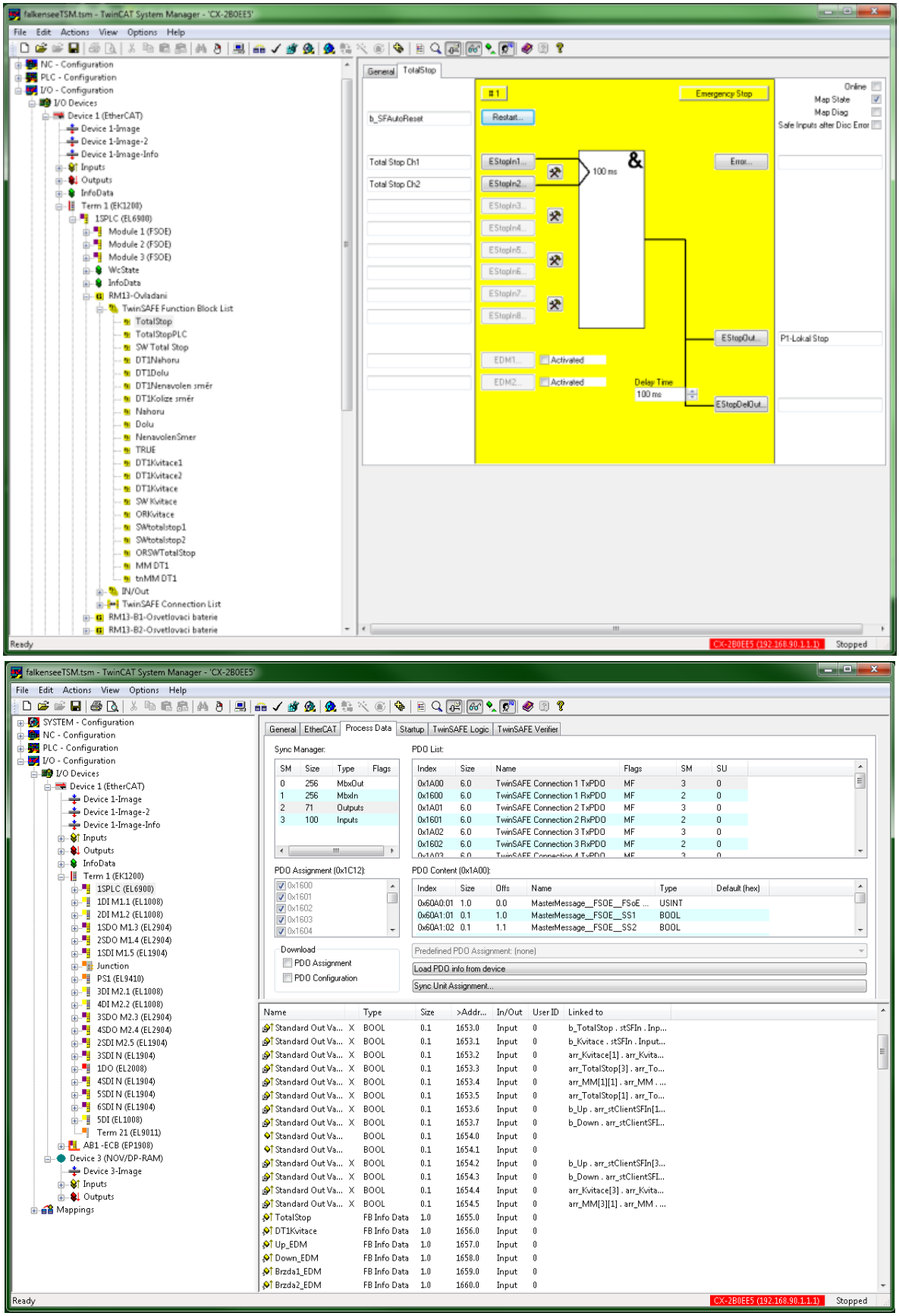
Bezpečnostní programová část PLC na Obr. 38 zajišťuje v řídicím systému definované bezpečnostní funkce. Softwarové vybavení je umístěno na bezpečnostní redundantní procesorové jednotce EL6900. Tato jednotka v řídicím systému obsluhuje až 8 zařízení podle počtu realizovaných bezpečnostních funkcí. Pro systémy s velkým počtem zařízení se v řídicím systému osadí příslušný počet těchto redundantních jednotek a jejich kooperace je zajištěna softwarovým propojením s využitím TwinSAFE komunikace prostřednictvím protokolu FSoE /Fail Safe over EtherCAT/.

Hardwarové prostředky

Redundantní procesorová jednotka CPU – EL6900.

Bezpečnostní I/O, Input: EL1904, Output: EL2904.

Programování probíhá v certifikovaném prostředí /Safety Editor/ v rámci systému TwinCAT Obr. 38. Programovací jazyk je SAL /Safety Application Language/. Bezpečnostní funkce jsou společností Drivecontrol, s.r.o. již naprogramovány. V rámci zakázky se realizuje pouze softwarová propojování jednotlivých jednotek CPU/Central Processor Unit/ (dle počtu zařízení) a jejich správné linkování do ostatních interface. Komunikace probíhá pomocí TwinSAFE/FSoE Obr. 38.



Obr. 38: Bezpečnostní PLC

10.15 POUŽÍVÁNÍ JIŽ EXISTUJÍCÍHO BEZPEČNOSTNÍHO SOFTWARU (FSM_A.07.V1)

Tento Dokument je důležitý pro správnost a verifikace použitých nástrojů. Ověření zdrojů a vlastností nástrojů pro dosažení cíle – funkčně bezpečného software.

Způsobilost ověřena formou kontroly. Ověření platnosti je předložení certifikátů funkční bezpečnosti:

- ✓ *Certifikát Z10 10 06 62386 005*

Závěr ověření:

Verze platná dle TÜV SUD Czech s.r.o. databáze.

- ✓ Parametry požadavků byly splněny.

Ověření platné verze a vlastností nástrojů:

Tab: 43: Softwarové nástroje

Název softwaru	Verze softwaru
Application Guide TwinSAFE	Version 1.9.1 (2018-02-05)
TwinSAFE loader	Version 2.1.1 (2018-01-02)
TwinSAFE logic FB /function blocks/	Version 3.1.0 (2016-11-04)
TwinSAFE user version	Version 3.1.0 (2016-11-04)

Závěr ověření:

Verze dokumentů jsou platné dle BECKHOFF dokument databáze.

- ✓ Parametry požadavků byly splněny.

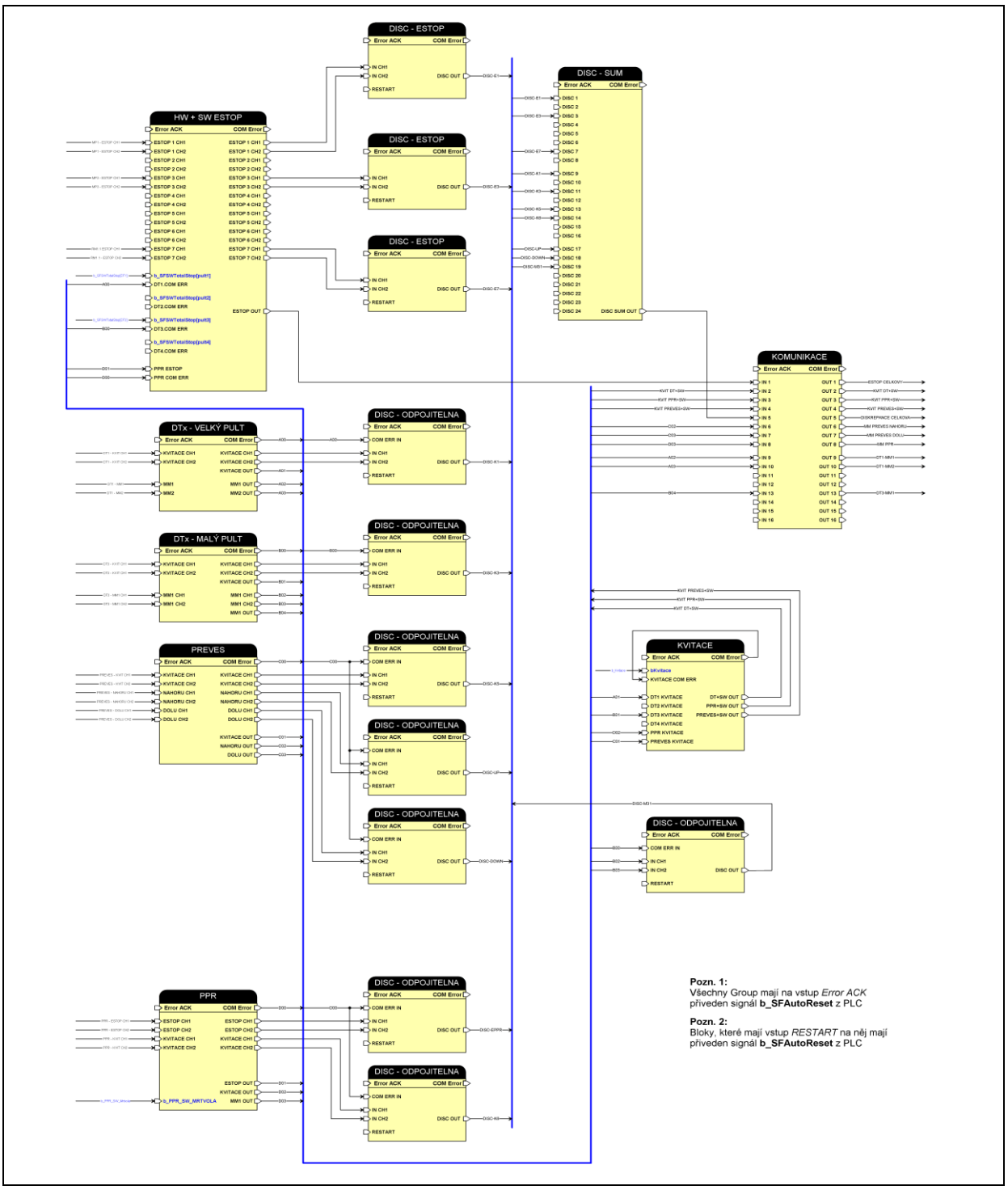
10.16 NÁVRH SOFTWARU

10.16.1 Popisy funkcí softwaru (FSM_A.08.1)

Pro architekturu softwaru je použit grafický popis s členěním na systémy a subsystémy doplněn o schémata jednotlivých bloků, které jsou na Obr. 39, Obr. 40, Obr. 41.

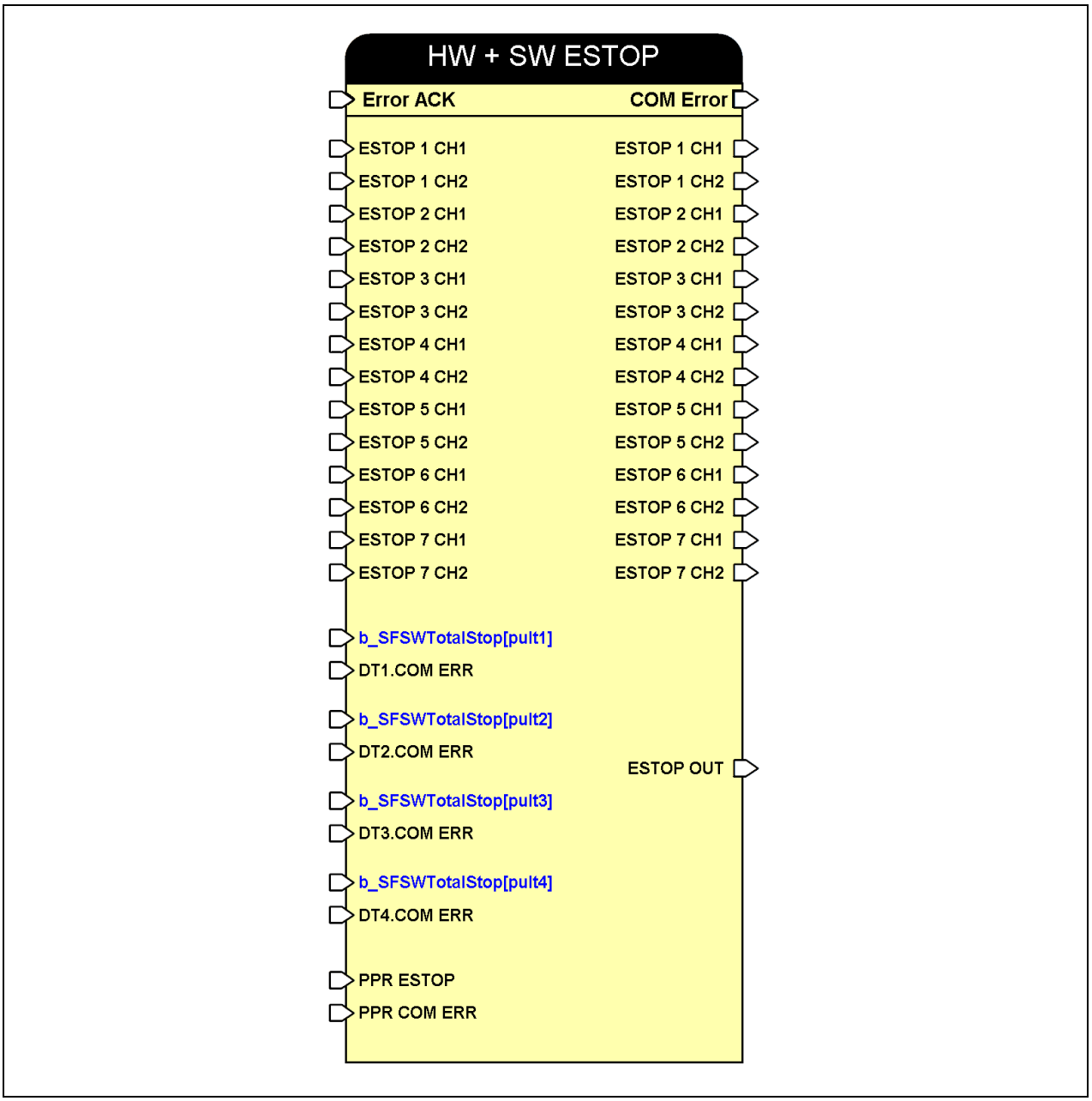
Pro ukázkovou funkci byla zvolena uvedená funkce nouzového zastavení systému iTEMS. Pro přehlednost je uvedena architektura s hlavním procesorem bezpečnostní funkce nouzové zastavení. Pro využívání v rozdílných aplikačních projektech jsou využity objektově orientované přístupy.

Na níže uvedeném obrázku, je zobrazen hlavní procesor funkce bezpečného zastavení.



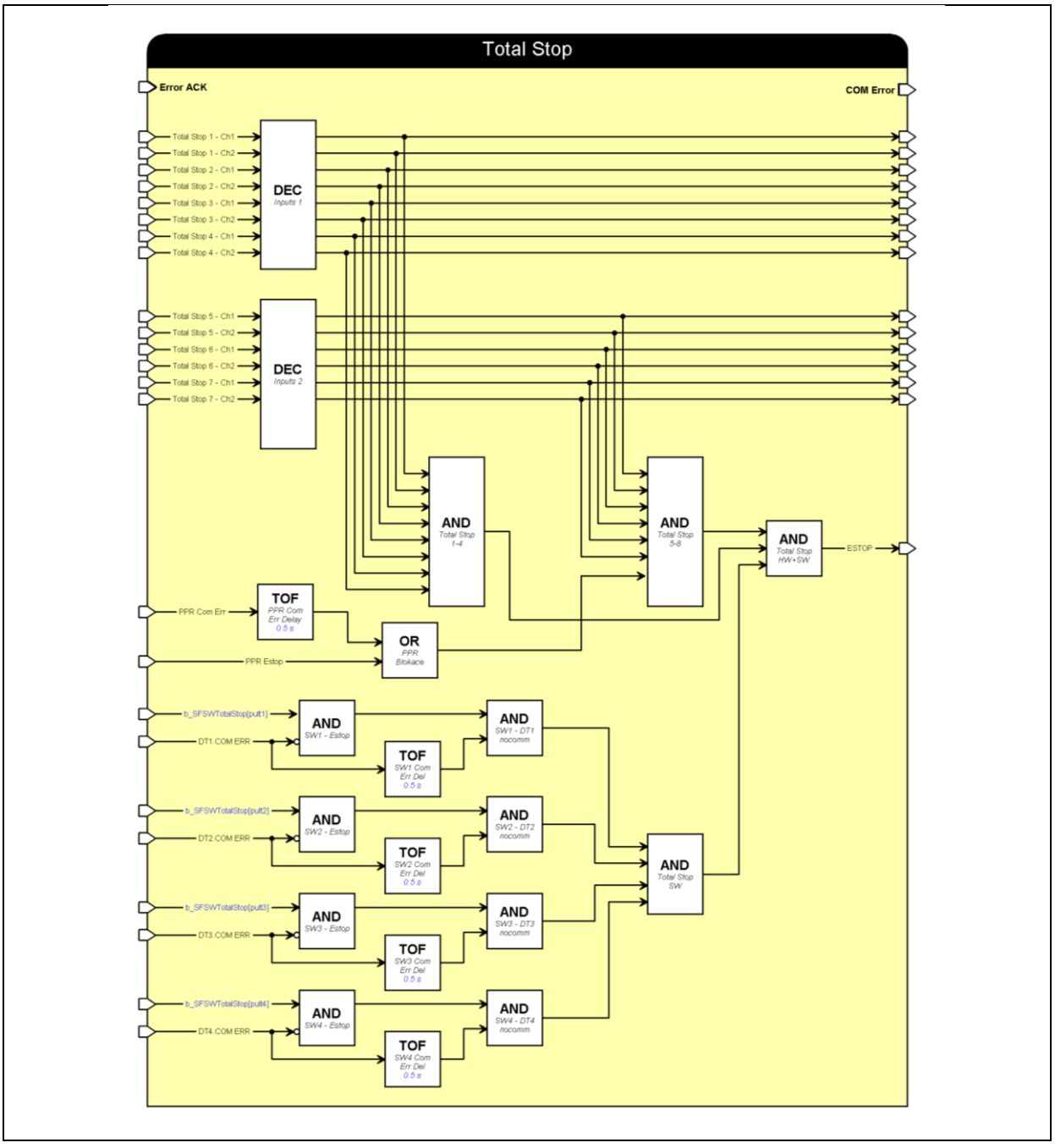
Obr. 39: Blokové schéma bezpečnostního programu

Na níže uvedeném obrázku, je zobrazen – sub blok – HW+SW ESTOP pro 7 tlačítek ve dvoukanálovém provedení.



Obr. 40: Blokové schéma bezpečnostního PRG – funkční blok

Na níže uvedeném obrázku, je zobrazeno vnitřní schéma – HW+SW ESTOP.



Obr. 41: Blokové schéma bezpečnostního PRG – Emergency Stop

10.16.2 **Testování „black box“ (FSM_A.08.V1)**

Testování softwarových celků – bloků pro účel před aplikačního testu. Testování softwarových celků prostřednictvím simulace vstupních informací a sledování reakcí na výstupech. Testovací prostředí je stejné jako pro tvorbu samotného software. Způsob definice a provedení testu je specifikováno prostředím a zvoleným nástrojem. Jednotlivé rozvaděče byly zapojeny ve společnosti Drivecontrol, s.r.o. a byly otestovány jednotlivé bezpečnostní funkce Obr. 42.

Obr. 42: Testování rozvaděčů

Za provedení a zaznamenání odpovídá:

- vývojový manažer SW,
- manažer vývoje a architekt bezpečnostního systému (SSA).

Zpráva o testu:

Tab: 44: Tabulka testů

Vstup	Stav	reakce očekávaná [ESTOP Out]	rekce zaznamenaná	výsledek (OK/Chyba)
Error ACK	0	0	0	OK
Vstup	Stav	reakce očekávaná [ESTOP Out]	rekce zaznamenaná	výsledek (OK/Chyba)
ESTOP 1 CH1	0	0	0	OK
ESTOP 2 CH1	0			
Vstup	Stav	reakce očekávaná [ESTOP Out]	rekce zaznamenaná	výsledek (OK/Chyba)
ESTOP 1 CH1	1	1	1 (Note: discrepance vstupu)	OK
ESTOP 2 CH1	0			
Vstup	Stav	reakce očekávaná [ESTOP Out]	rekce zaznamenaná	výsledek (OK/Chyba)
ESTOP 1 CH1	0	1	1 (Note: discrepance vstupu)	OK
ESTOP 2 CH1	1			

Výsledek testu:

Test funkcionality bloku je v pořádku, blok HW+SW ESTOP reaguje dle předpokladu.

10.16.3 Validace pomocí simulace chyb v divadle (FSM_A.02.V2)

Kontrolní seznam systému řízení pro FAT

DRIVE CONTROL

Výrobce:		Projekt	
Drivecontrol, s.r.o		Název:	rekonstrukce Janáčkova divadla
Control System Type:		Část:	Control System Functionality
iTEMS, typed		Rok:	2015
Datum provedení: 2.7.2015			
Prověření provedl: Ing. Michal Drlík		Podpis:	

Nr.	Položka	N/A	OK	FAULT	Proč nebo komentář
SF1	Emergency stop				
1	Test funkce - stisk hřibového tlačítka - bezpečný stav		OK		
2	Kontrola stavu ve vizualizaci - chyba je zobrazena v diagnostice		OK		
3	Logování chyby - chyba je zalogována		OK		
4	Test funkce během jízdy - rychlé zastavení zastavení - bezpečný stav		OK		
S1	Odpojení 1 kanálu ze vstupu - simulace upadnutí přívodních vodičů - bezpečný stav		OK		
S2	Propojení vodičem mezi svorkami 1, 2 (5, 6) 1SDI pro MP-A1, nebo 3, 4 (7, 8) 1SDI pro MP-A2, nebo 1, 2 (5, 6) 2SDI pro MP-A3 - simulace selhání kontaktu nebo zkratu v přívodním vodiči - bezpečný stav		OK		
S3	Propojení vodičem mezi svorkami 1, 5 (2, 6) 1SDI - simulace křížových zkratů v přívodních vodičích - bezpečný stav		OK		
S4	Přivedení napájecího napětí +24V= na svorku 1 - simulace cizího napětí na přívodních vodičích - bezpečný stav		OK		
SF2	Safety limits				
1	Test funkce - odpojení propojky ze svorkovnice - bezpečný stav		OK		
2	Kontrola stavu ve vizualizaci - chyba je zobrazena v diagnostice		OK		
3	Logování chyby - chyba je zalogována		OK		
4	Test funkce během jízdy - rychlé zastavení zastavení - bezpečný stav		OK		
S1	Odpojení 1 kanálu ze vstupu - simulace upadnutí přívodních vodičů - bezpečný stav		OK		
S2	Propojení vodičem mezi svorkami 1, 5 (2, 6) 1SDI - simulace křížových zkratů v přívodních vodičích - bezpečný stav		OK		
S3	Přivedení napájecího napětí +24V= na svorku 1 - simulace cizího napětí na přívodních vodičích - bezpečný stav		OK		
SF3	Dead man				
1	Test funkce - stisk tlačítka - odbrždění zvoleného zařízení - nulové otáčky - zařízení se nepohybuje		OK		

Stránka 1 z 6

Obr. 43: FAT – 1.strana

Kontrolní seznam systému řízení pro FAT

DRIVE CONTROL

	Výrobce:	Projekt			
	Drivecontrol, s.r.o	Název:		rekonstrukce Janáčkova divadla	
	Control System Type:	Část:		Control System Functionality	
	iTEMS, typed	Rok:		2015	
	Datum provedení: 2.7.2015				
	Prověření provedl: Ing. Michal Drlík	Podpis:			
Nr.	Položka	N/A	OK	FAULT	Proč nebo komentář
2	Test funkce - stisk tlačítka + vyhnutí páky - odbrždění - pohyb daným směrem		OK		
3	Test funkce - stisk tlačítka + vyhnutí páky - během pohybu puštění tlačítka - zařízení se uvede do nulových otáček - rychlé zastavení		OK		
S1	Odpojení 1 kanálu ze svorky tlačítka mrtvého muže v panelu - simulace upadnutí přívodních vodičů - kontrola ve vizualizaci - nelze provést jízdu + safety zůstává aktivní		OK		
S2	Propojení vodičem mezi svorkami spínací jednotky tlačítka mrtvého muže - zkrat - simulace selhání kontaktu nebo zkratu v přívodním vodiči - kontrola ve vizualizaci - nelze provést jízdu + safety zůstává aktivní		OK		
S3	Propojení vodičem mezi svorkami dvou spínacích jednotek tlačítka mrtvého muže - simulace křížových zkratů v přívodních vodičích - kontrola ve vizualizaci - nelze provést jízdu + safety zůstává aktivní		OK		
S4	Přivedení napájecího napětí +24V= na svorku některé z jednotek tlačítka mrtvého muže - simulace cizího napětí na přívodních vodičích - bezpečný stav		OK		
SF4	Load cells				
1	Test funkce - připojeny odpory místo tenzometrů - rozvážení - zobrazuje hodnotu ve vizualizaci		OK		
2	Test funkce - Kontrola stavu ve vizualizaci při rozvážení mimo rozsah - chyba je zobrazena v diagnostice		OK		
3	Logování chyby - chyba je zalogována		OK		
S1	Odpojení vodiče ze svorky 3 – simulace nedosažení min. proudu v rozsahu 4 až 20 mA - odpojení tenzometru - bezpečný stav		OK		
S2	Přivedení proudu vyššího než 20 mA na svorku 3 – simulace překročení max. proud. hodnoty rozsahu 4 až 20 mA pomocí potenciometru - bezpečný stav		OK		

Stránka 2 z 6

Obr. 44: FAT – 2.strana

Kontrolní seznam systému řízení pro FAT

DRIVE CONTROL

	Výrobce:	Projekt	
	Drivecontrol, s.r.o	Název:	rekonstrukce Janáčkova divadla
	Control System Type:	Část:	Control System Functionality
	iTEMS, typed	Rok:	2015
	Datum provedení: 2.7.2015		
	Prověření provedl: Ing. Michal Drlík	Podpis:	

Nr.	Položka	N/A	OK	FAULT	Proč nebo komentář
S3	Odpojení 1 kanálu ze vstupu - simulace upadnutí přívodních vodičů - bezpečný stav		OK		
S4	Propojení vodičem mezi svorkami 1, 2 (5, 6) 1SDI - simulace selhání kontaktu nebo zkratu v přívodním vodiči - bezpečný stav		OK		
S5	Propojení vodičem mezi svorkami 1, 5 (2, 6) 1SDI - simulace křížových zkratů v přívodních vodičích - bezpečný stav		OK		
S6	Přivedení napájecího napětí +24V= na svorku 1 - simulace cizího napětí na přívodních vodičích - bezpečný stav		OK		
SF9	Double Brakes				
1	Test funkce - odbrzděny obě brzdy po stisku Dead Man tlačítka - vizuální kontrola		OK		
MSWITCH	Maintenance switch				
1	Test funkce - bezpečný stav - kontrola ve vizualizaci		OK		
2	Test funkce během jízdy - rychlé zastavení zastavení - bezpečný stav		OK		
S1	Odpojení 1 kanálu ze svorky vypínače - simulace upadnutí přívodních vodičů - bezpečný stav		OK		
S2	Propojení vodičem mezi svorkami 1, 2 (4, 5) svorkovnice -X462 (-X662 nebo -X862) - simulace selhání kontaktu nebo zkratu v přívodním vodiči - bezpečný stav		OK		
S3	Propojení vodičem mezi svorkami 1, 4 (2, 5) svorkovnice -X462 (-X662 nebo -X862) - simulace křížových zkratů v přívodních vodičích - bezpečný stav		OK		
S4	Přivedení napájecího napětí +24V= na svorku 1 svorkovnice -X462 (-X662 nebo -X862) - simulace cizího napětí na přívodních vodičích - bezpečný stav		OK		
SFx	Common Safety Simulations				
S1	Simulace výpadku komunikace EtherCAT mezi couplery - odpojení libovolného EtherCAT kabelu - bezpečný stav		OK		

Stránka 3 z 6

Obr. 45: FAT – 3.strana

Kontrolní seznam systému řízení pro FAT

DRIVE CONTROL

	Výrobce:	Projekt	
	Drivecontrol, s.r.o	Název:	rekonstrukce Janáčkova divadla
	Control System Type:	Část:	Control System Functionality
	iTEMS, typed	Rok:	2015
	Datum provedení: 2.7.2015		
	Prověření provedl: Ing. Michal Drlík	Podpis:	

Nr.	Položka	N/A	OK	FAULT	Proč nebo komentář
S2	Simulace výpadku komunikace s pultem - odpojení komunikačního kabelu pultu - bezpečný stav - kontrola ve vizualizaci		OK		
S3	Chyba hlavního pčítače - simulace odpojením UPS od napájení - pult hlásí chybu spojení se serverem		OK		
S4	Vypnutí vizualizace během jízdy - zařízení se zastaví		OK		
S5	EDM - chyba zpětné vazby - odpojení zpětné vazby po stisku emergency stop - nelze kvitovat - kontrola ve vizualizaci - zůstává bezpečný stav		OK		
S6	Zkrat výstupní karty - chyba EDM - nutno restartovat kartu - výstup musí být aktivní		OK		
S7	Křížový zkrat výstupní karty - chyba EDM - nutno restartovat kartu - výstup musí být aktivní		OK		
FM	Frequency inverter functions				
1	Test funkce - rozběh motoru - libovolný pohon		OK		
S1	Odpojení komunikace měniče během jízdy - zastavení pohonu - chyba měniče - bezpečný stav		OK		
S2	Odpojení stykače -484 (-684, -884) - simulace FM safe stop - kontrola na frekvenčním měniči - kontrola ve vizualizaci		OK		
S3	Vypnutí měniče tlačítkem do stavu Off - kontrola stavu ve vizualizaci.		OK		
ECB	Backup system				NENÍ SOUČÁSTÍ DODÁVKY
1	Přepojení pohonu do záložního systému - ověřit funkční systém zálohy a ověřit funkční hlavní systém				
2	Kontrola parametrů na záložním pultu ECB				
3	Kontrola stavu na hlavním pultu - osa nejde navolit - hlásí stav				
4	Připojení záložního pultu s přepojenou osou - kontrola parametrů dané osy				
5	Přihlášení - záložní systém - Kontrola nemožnosti provádět testy				
6	Přihlášení - testovací systém - Kontrola možnosti provádět testy				

Stránka 4 z 6

Obr. 46: FAT – 4.strana

Kontrolní seznam systému řízení pro FAT

DRIVE CONTROL

Výrobce:		Projekt	
Drivecontrol, s.r.o		Název:	rekonstrukce Janáčkova divadla
Control System Type:		Část:	Control System Functionality
ITEMS, typed		Rok:	2015
Datum provedení: 2.7.2015			
Prověření provedl: Ing. Michal Drlík		Podpis:	

Nr.	Položka	N/A	OK	FAULT	Proč nebo komentář
7	Připojení záložního pultu bez připojené osy - kontrola nemožnosti ovládat, záložky nejsou k dispozici, pouze logování				
8	Provedení testu jízdy s připojeným motorem - korektní data na panelu - odbrzděno - motor se otáčí				
9	Test nastavení rychlosti				
10	Test nastavení polohy				
11	Kontrola diagnostiky záložního systému				
12	Logování chyb v záložním systému				
13	Provedení testů v testovacím režimu				
MCS-U	Main Control System - User Access				
1	Přihlášení uživatele - kontrola jeho pravomocí dle nastavení		OK		
2	Správa uživatelů - založit nového uživatele - kontrola funkčnosti		OK		
3	Správa uživatelů - zrušit uživatele - kontrola funkčnosti		OK		
4	Nastavení různých oprávnění - vytvořit uživatele s omezenými oprávněními		OK		
MCS-M	Main Control System - Manual				
1	Nastavení parametrů jízdy - rychlost, meze - kontrola		OK		
2	Přiřazení k joysticku - kontrola nemožnosti přiřadit osu v chybě nebo jinak zamčenou osu		OK		
3	Zobrazení parametrů osy - kontrola parametrů		OK		
4	Nemožnost navolit meze mimo rozsah fyzických mezí		OK		
5	Návrat k výchozím chodnotám mezí		OK		
4	Nastavení limitů zařízení		OK		
MCS-A	Main Control System - Automatic				
1	Přiřazení k joysticku - kontrola nemožnosti přiřadit osu v chybě nebo jinak zamčenou osu		OK		
2	Nastavení parametrů jízdy - rychlost, meze - kontrola		OK		
3	Vytvoření skupiny - vizuální kontrola		OK		
4	Parametry skupiny - testy synchronizací, triggerů, opakování a zpoždění - kontrola v simulované jízdě		OK		

Stránka 5 z 6

Obr. 47: FAT – 5.strana

Kontrolní seznam systému řízení pro FAT

DRIVE CONTROL

Výrobce:		Projekt	
Drivecontrol, s.r.o		Název:	rekonstrukce Janáčkova divadla
Control System Type:		Část:	Control System Functionality
iTEMS, typed		Rok:	2015
Datum provedení: 2.7.2015			
Prověření provedl: Ing. Michal Drlík		Podpis:	

Nr.	Položka	N/A	OK	FAULT	Proč nebo komentář
5	Vytvoření, smazání, načtení a přejmenování představení		OK		
6	Vytvoření, smazání, přepínání, kopírování a přesouvání scény		OK		
7	Režim bez uložení - kontrola funkčnosti		OK		
8	Zálohování představení, přepnutí serverů, obnova databáze		OK		
MSC-D	Main Control System - Diagnostics and Logs				

Stránka 6 z 6

Obr. 48: FAT – 6.strana

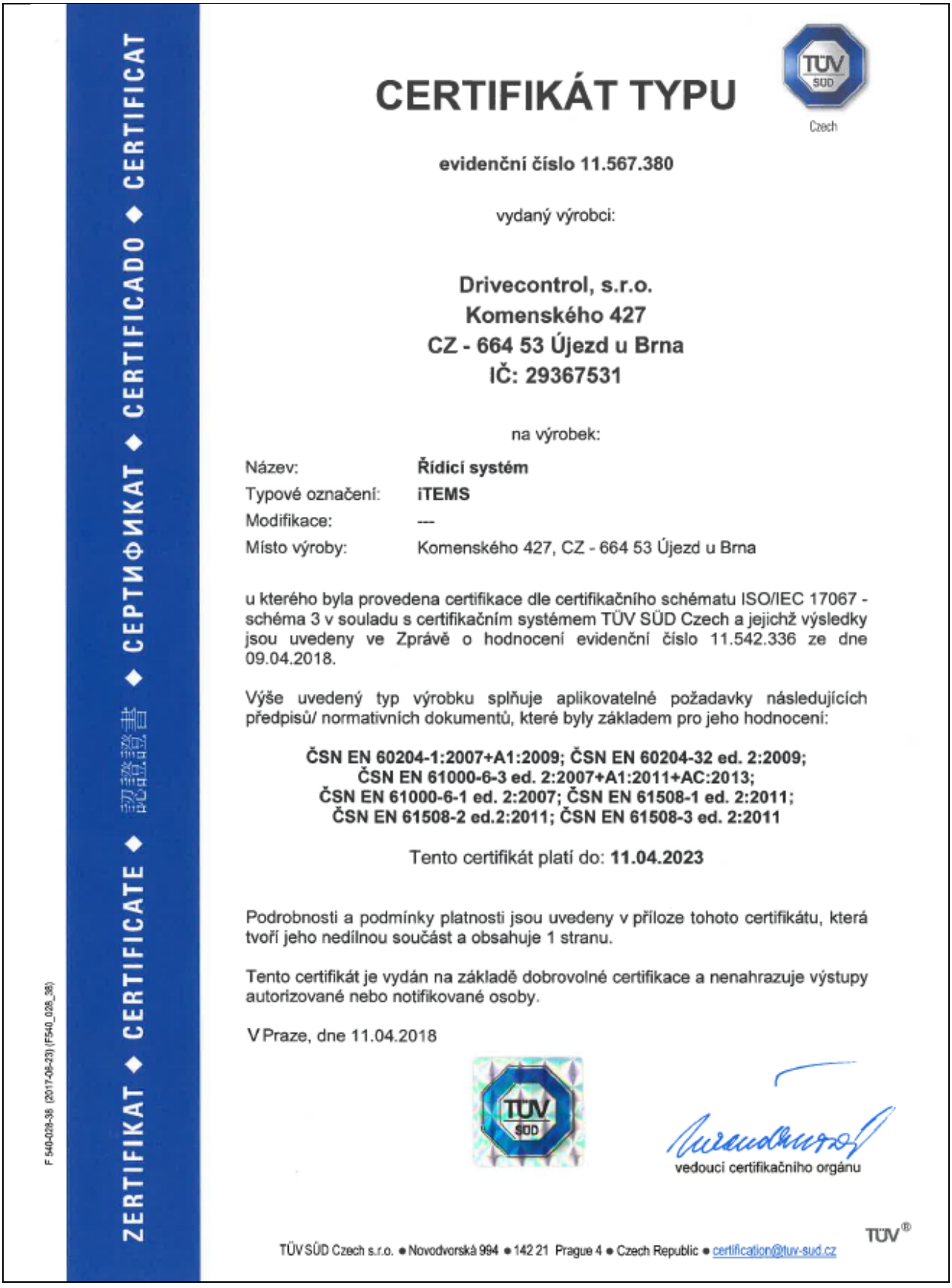
11 VÝSLEDKY DISERTAČNÍ PRÁCE

Výsledkem disertační práce je navržení metody vývoje a validace softwaru pro programovatelné řídicí systémy související s bezpečností s ohledem na bezpečnostní funkce, které je nutné řešit v divadlech a jiných kulturních objektech pro scénická zařízení a interakci s nimi.

Z celého rozsahu funkční bezpečnosti, resp. životního cyklu celkové bezpečnosti, byla řešena oblast vývoje a následné validace softwaru souvisejícího s bezpečností. S využitím poznatků z oblasti běžného programování, s požadavky a cíli souboru norem EN 61508 byla sestavena metodika pro sestavení softwaru souvisejícího s bezpečností počínaje jeho návrhem, přes vlastní vývoj, ověření až po začlenění k příslušnému hardwaru.

Během procesu jsou zohledněny modifikace, včetně postupných testů, schvalování, analýz a ověřování. Metodika zohledňuje i různé požadavky na výslednou úroveň integrity bezpečnosti až do úrovně SIL3, která je relevantní pro strojně technická zařízení. Pro lepší aplikovatelnost byl pro tuto metodiku sestaven model a byly navrženy všechny základní potřebné typy dokumentace, které jsou nutné pro fungování modelu vývoje a validace softwaru a naplnění všech fází celé metody.

Navržená metoda byla realizována na akci Národního divadlo v Brně, kde proběhla výměna řídicího systému, včetně certifikace systému iTEMS. Tato realizace byla zakončena certifikátem Obr. 49 od společnosti TÜV SÜD Czech s.r.o., Praha 4, Novodvorská 994, PSČ 14221. V kapitole Příloha – reference, jsou uvedená divadla, která byla realizována pomocí této metodiky.



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

F 540-028-38 (2017-08-23) (F540_028_38)

CERTIFIKÁT TYPU

TÜV SÜD Czech

evidenční číslo 11.567.380

vydaný výrobci:

Drivecontrol, s.r.o.
Komenského 427
CZ - 664 53 Újezd u Brna
IČ: 29367531

na výrobek:

Název:	**Řídící systém**
Typové označení:	**iTEMS**
Modifikace:	---
Místo výroby:	Komenského 427, CZ - 664 53 Újezd u Brna

u kterého byla provedena certifikace dle certifikačního schématu ISO/IEC 17067 - schéma 3 v souladu s certifikačním systémem TÜV SÜD Czech a jejichž výsledky jsou uvedeny ve Zprávě o hodnocení evidenční číslo 11.542.336 ze dne 09.04.2018.

Výše uvedený typ výrobku splňuje aplikovatelné požadavky následujících předpisů/ normativních dokumentů, které byly základem pro jeho hodnocení:

ČSN EN 60204-1:2007+A1:2009; ČSN EN 60204-32 ed. 2:2009;
ČSN EN 61000-6-3 ed. 2:2007+A1:2011+AC:2013;
ČSN EN 61000-6-1 ed. 2:2007; ČSN EN 61508-1 ed. 2:2011;
ČSN EN 61508-2 ed.2:2011; ČSN EN 61508-3 ed. 2:2011

Tento certifikát platí do: **11.04.2023**

Podrobnosti a podmínky platnosti jsou uvedeny v příloze tohoto certifikátu, která tvoří jeho nedílnou součást a obsahuje 1 stranu.

Tento certifikát je vydán na základě dobrovolné certifikace a nenahrazuje výstupy autorizované nebo notifikované osoby.

V Praze, dne 11.04.2018

TÜV SÜD

vedoucí certifikačního orgánu

TÜV®

TÜV SÜD Czech s.r.o. ● Novodvorská 994 ● 142 21 Prague 4 ● Czech Republic ● certification@tuv-sud.cz

Obr. 49: Certifikát Drivecontrol

12 ZÁVĚR

Podstatou zpracované metodiky vývoje softwaru souvisejícího s bezpečností je rozpracování jednotlivých kroků, které je nutné provést tak, aby byly splněny požadavky a cíle souboru technických norem a současně aby byly všechny fáze provedeny důsledně, a přitom co nejefektivněji a ve všech stupních celého procesu byla provedena kompletní dokumentace. Zpracovaná metodika pro vývoj a validaci softwaru pak může být použita nejen pro zpracování softwaru v oblasti divadelních technologií, ale pro celou nadřazenou skupinu strojních mechanismů a může tak zcela plnohodnotně přispět v oblasti rozvoje průmyslu nejen v České republice, ale v rámci celé Evropské Unie, potažmo celého světa.

Největším a zcela zřejmým přínosem je pak zvýšení bezpečnosti nejen na pracovištích v rámci kulturních objektů a jiné zábavní techniky, ale také přenesením do jiných odvětví strojírenství na mnoho dalších pracovišť se zcela jiným zaměřením. Bezpečnost jako taková by měla být a je jedním z prvních faktorů, kterými se zabývají technici celého světa a žádná z technických či ekonomických kritérií by neměla být překážkou při volbě tak důležité části, jako je zabezpečení lidského života a zdraví. Cíle práce byly naplněny vytvořenou metodikou i její aplikace a validace, která byla potvrzena inspekčním certifikátem certifikačního orgánu. V kapitole 18 jsou realizované referenční zakázky, které byly realizovány v Ruské federaci. Tyto divadla byly realizovány stejnou metodikou.

13 BIBLIOGRAFIE

[1] ČSN EN 61508-3 ed. 2. ČESKÁ TECHNICKÁ NORMA: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 3: Požadavky na software. Český normalizační institut, Praha 1: Český normalizační institut, 2011.

[2] ČSN EN 61508-7 ed. 2. ČESKÁ TECHNICKÁ NORMA: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 7: Přehled technik a opatření. Český normalizační institut, Praha 1: Český normalizační institut, 2011.

[3] EN 17206. Entertainment Technology – Lifting and Load–bearing Equipment for Stages and other Production Areas within the Entertainment Industry – Specifications for general requirements (excluding aluminum and steel trusses and towers). Draft. B–1000 Brussels: CEN, 2018.

[4] ČSN EN ISO 13849-1:2017. Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Obecné zásady pro konstrukci. 1. Praha 1: Český normalizační institut, 2017.

[5] ČSN EN 62061. Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností. 1. Praha 1: Český normalizační institut, 2005.

[6] ČESKÁ REPUBLIKA. Zákon o technických požadavcích na výrobky a o změně a doplnění některých zákonů. In: 22/1997 Sb. Praha: Tiskárna Ministerstva vnitra, p. o, 1997, ročník 1997, číslo 22. Dostupné také z: https://www.zakonyprolidi.cz/cs/1997–22

[7] ČESKÁ REPUBLIKA. Zákon o obecné bezpečnosti výrobků a o změně některých zákonů (zákon o obecné bezpečnosti výrobků). In: 102/2001 Sb. Praha: Tiskárna Ministerstva vnitra, p. o, 2001, ročník 2001, číslo 102. Dostupné také z: https://www.zakonyprolidi.cz/cs/2001–102

[8] ČESKÁ REPUBLIKA. Směrnice o strojních zařízeních. In: 2006/42/ES. Štrasburk: Evropská komise, 2006, 5/2006, L 157/24. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32006L0042&qid=1545390706004&from=CS

[9] ČESKÁ REPUBLIKA. O harmonizaci právních předpisů členských států týkajících se elektromagnetické kompatibility. In: 2014/30/EU. Štrasburk: Evropská komise, 2014, ročník 2014, L 96/79. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014L0030&qid=1545392298278&from=CS

[10] ČESKÁ REPUBLIKA. Harmonizaci právních předpisů členských států týkajících se dodávání elektrických zařízení určených pro používání v určitých mezích napětí na trh. In: 2014/35/EU. Štrasburk: Evropská komise, 2014, ročník 2014, L 96/357. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1545392543750&uri=CELEX:32014L0035

[11] ČESKÁ REPUBLIKA. O omezení používání některých nebezpečných látek v elektrických a elektronických zařízeních. In: 2011/65/EU. Štrasburk: Evropská komise, 2011, ročník 2011, L 174/88. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1545392633935&uri=CELEX:32011L0065

[12] ČESKÁ REPUBLIKA. O odpadních elektrických a elektronických zařízeních (OEEZ). In: 2012/19/EU. Štrasburk: Evropská komise, 2012, ročník 2012, L 197/38. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1545392713625&uri=CELEX:32012L0019

[13] BLECHA, Petr. *Ing. Petr BLECHA, Ph.D.: MANAGEMENT TECHNICKÝCH RIZIK U VÝROBNÍCH STROJŮ*. V Brně, 2009. Habilitační práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA STROJNÍHO INŽENÝRSTVÍ ÚSTAV VÝROBNÍCH STROJŮ, SYSTÉMŮ A ROBOTIKY.

[14] Metodika vývoje softwaru. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2019–04–13]. Dostupné z: https://cs.wikipedia.org/wiki/Metodika_v%C3%BDvoje_softwaru

[15] MEDOFF, Michael a Rainer FALLER. *FUNCTIONAL SAFETY: Compilant Development Process*. 3rd Edition. Sellersville, PA, USA: Exida, 2014. ISBN 978-1-934977-08-8.

[16] Uher, Jaromír. Úvod do funkční bezpečnosti I: norma ČSN EN 61508. *ATOMA: časopis pro automatizační techniku.* [Online] [Citace: 18. 2. 2016.] http://automa.cz/uvod-do-funkcni-bezpecnosti-i:-norma-csn-en-61508-32520.html.

[17] DIN 56950-1:2012-05: Veranstaltungstechnik - Maschinentechnische Einrichtungen - Teil 1: Sicherheitstechnische Anforderungen und Prüfung. Entertainment technology - Machinery installations - Part 1: Safety requirements and inspections. Deutsch: Norm_deutch, 2012.

[18] ČSN EN 61508–2 ED. 2. ČESKÁ TECHNICKÁ NORMA: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 2: Požadavky na elektrické/ elektronické/ programovatelné elektronické systémy související s bezpečností. Český normalizační institut, Praha 1: Český normalizační institut, 2011.

14 SEZNAM OBRÁZKŮ

15 SEZNAM TABULEK

16 TERMÍNY A ZKRATKY

Zkratka	Anglický název	Český název
ARC	Absolut Rotary (en)Coder	Absolutní rotační snímač
CRC	Cyclic Redundancy Check	Cyklický redundantní součet
DC	Diagnostic Coverage	Diagnostické pokrytí
EDM	External Device Monitoring	Zpětná vazba bezpečnostní funkcí
EMC	Electromagnetic Compatibility	Elektromagnetická kompatibilita
EUC	Equipment under Control	Řízené zařízení
FSM	Functional Safety Management	Management funkční bezpečnosti
FSoE	Fail Safe over EtherCAT	Bezpečná komunikace prostřednictvím linky EtherCAT
FTA	Fault Tree Analysis	Analýza stromem poruchových stavů
HFT	Hardware Fault Tolerance	Odolnost hardwaru vůči vadám
HMI	Human – Machine Interface	Rozhraní člověk – stroj
IRC	Incremental Rotary (en)Coder	Inkrementální rotační snímač
LVD	Low Voltage Directive	Směrnice o nízkém napětí
MD	Machinery Directive	Směrnice o strojních zařízeních
MTTR	Mean Time to Restoration [h]	Střední doba do obnovy [h]
NC	Numeric Control	Číslicové řízení
NC I	Numeric Control – Interpolation	Číslicové řízení s interpolací pro víceúrovňové řízení
OEEZ	The Waste Electrical and Electronic Equipment	Odpadní elektrická a elektronická zařízení (česká zkratka)
PFH	Average Frequency of Dangerous Failure – Probability of Failure per Hour	Průměrná frekvence nebezpečné poruchy – Pravděpodobnost poruchy za hodinu
PLC PRG	Programmable Logic Controller – Program	Program v programovatelném automatu
PrM	Project Manager	Produktový manažer
PTP	Point–to–Point	Řídicí proces pro jednoúrovňové poziční řízení
QM	Quality Manager	Finanční manažer
QMS	Quality Management System	Systém Managementu kvality
RFID	Radio Frequency Identification	Identifikace na základě radiové frekvence
SAL	Safety Application Language	Bezpečnostní programovací jazyk
SF	Safety Function	Bezpečnostní funkce

SIF	Safety Instrumented Function	Bezpečnostně instrumentovaná funkce
SIL	Safety Integrity Level	Úroveň integrity bezpečnosti
SLS	Safely Limited Speed	Bezpečně omezená rychlost
SRP/CS	Safety–Related Part of a Control System	Bezpečnostní část systému řízení
SRS	Safety Requirements Specification	Specifikace bezpečnostních požadavků
SSA	Technical Manager	Technický manažer
STO	Safe Torque Off	Bezpečné odpojení momentu
T1	Proof–Test Interval [h]	Interval opakování testu [h]
V&V	Verification & Validation	Verifikace a Validace
WEEE Directive	The Waste Electrical and Electronic Equipment Directive	Směrnice o odpadních elektrických a elektronických zařízeních
WPF	Windows Presentation Foundation	Grafický subsystém společnosti Microsoft pro programování uživatelského interface (zkratka se nepřekládá)

17 PŘÍLOHA – TITULNÍ LISTY K METODICE

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.01**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

EVIDENCE DOKUMENTACE PROJEKTU FUNKČNÍ BEZPEČNOSTI

VYPRACOVAL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.01**		REVIZE:	**R<<doplnit >>**	

INFORMACE O REVIZI:

Obr. 50: Titulní list evidence dokumentace

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.02**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

PLÁN MANAGEMENTU FUNKČNÍ BEZPEČNOSTI

VYPRACOVAL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.02.1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

Obr. 51: Titulní list – plán managementu funkční bezpečnosti

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.02**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

PLÁN VALIDACE

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.02.2**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 52: Titulní list – plán validace

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.02**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

Verifikace pomocí simulace chyb u výrobce

VYPRACOVAL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.02.V1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 53: Titulní list validace – simulace chyb

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.02**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

VALIDACE POMOCÍ SIMULACE CHYB V DIVADLE

VYPRACOVAL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.02.V2**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 54: Titulní list validace – simulace chyb – divadlo

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.03**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

SPECIFIKACE BEZPEČNOSTNÍCH POŽADAVKŮ

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.03.1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 55: Titulní list – specifikace bezpečnostních požadavků

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.03**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

Bezpečnostní funkce 1

VYPRACOVAL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	<< **doplnit** >>	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.03.2**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 56: Titulní list bezpečnostní funkce 1

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.04**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

SPECIFIKACE VALIDAČNÍCH TESTŮ BEZPEČNOSTI

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.04.1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 57: Titulní list – specifikace validačních testů bezpečnosti

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.04**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

ZPRÁVA O OVĚŘENÍ VALIDAČNÍCH TESTŮ BEZPEČNOSTI

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.04.V1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 58: Titulní list – zpráva o ověření validačních testů – ověření

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.05**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

Popis architektury systému

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.05.1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 59: Titulní list – popis architektury systému

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A. 07**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

ARCHITEKTURA SOFTWARU

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.07.1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 60: Titulní list – architektura software

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.07**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

Způsobilost a oprávněnost používání již existujícího bezpečnostního softwaru a jeho komponent

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.07.V1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 61: Titulní list – způsobilost a oprávněnost používání software

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**				
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**				
BLOK:	**A.08**				
URČENO SKUPINÁM:	**Společné**				
technická zpráva NÁZEV					
Popisy funkcí softwaru					
VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.08.1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 62: Titulní list – popisy funkcí software

<< logo >>

IDENTIFIKACE DOKUMENTU:

OBJEKT:	**Řídicí systém << doplnit název systému >>**
PŘEDMĚT:	**FSM – Management funkční bezpečnosti**
BLOK:	**A.08**
URČENO SKUPINÁM:	**Společné**

technická zpráva

NÁZEV

Testování „Black Box“

VYPRACOVAL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
SCHVÁLIL:	**<< doplnit >>**	DATUM:	DD. MM. YYYY	PODPIS:	
ČÍSLO:	**FSM_A.08.V1**		REVIZE:	**R<<doplnit >>**	
INFORMACE O REVIZI:					

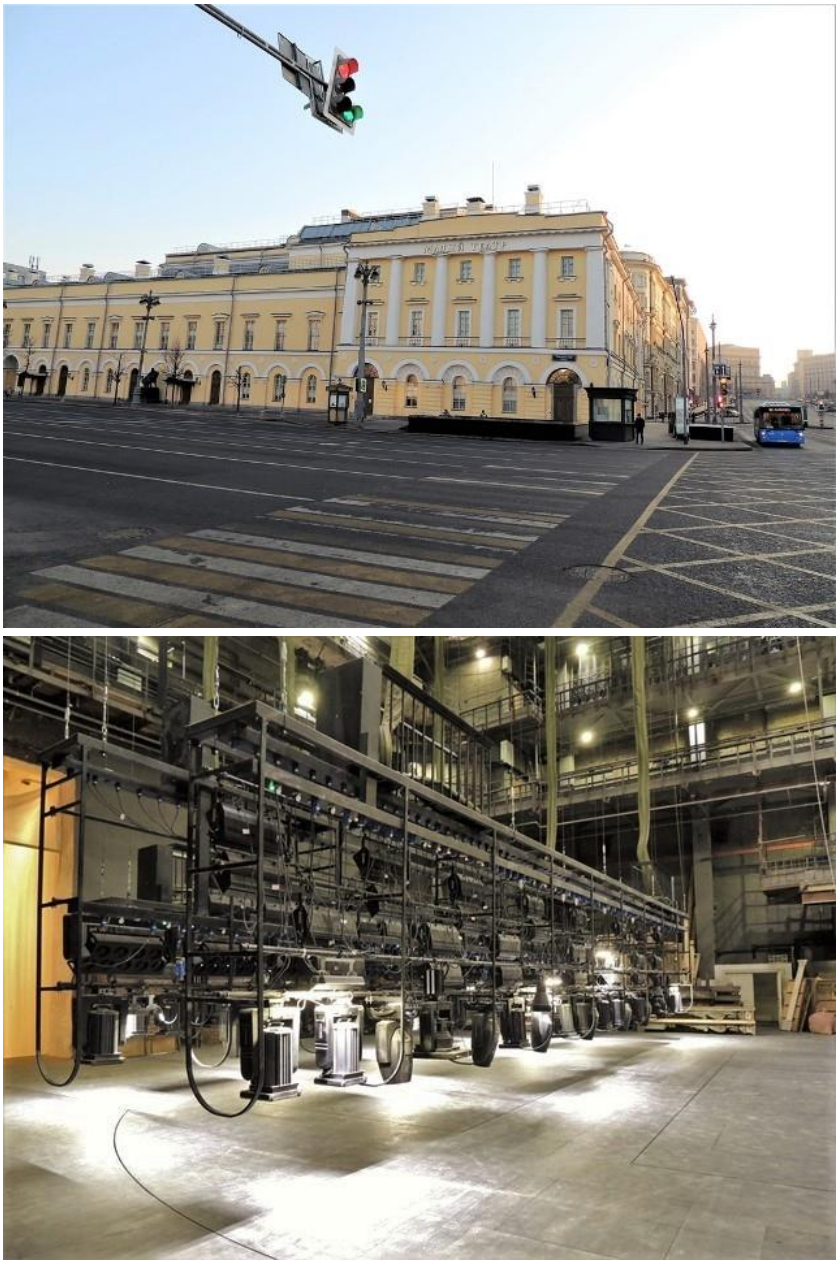
<< Doplnit společnost>>, << Doplnit adresu společnosti>>, << Doplnit stát>>
Web: << Doplnit www adresu>>
Email: << Doplnit kontaktní email>>

Obr. 63: Titulní list – testování „black box“Příloha – reference

18 REFERENČNÍ ZAKÁZKY

Další zakázky, které jsou realizovány pomocí této metodiky:

- Státní akademické Malé divadlo Ruska, Moskva, Rusko



Obr. 64: Státní akademické Malé divadlo Ruska, Moskva, Rusko

- Multifunkční sál Zarjadje – Moskva

Obr. 65: Multifunkční sál Zarjadje – Moskva

Palác umění Neftjanik, Surgut, Rusko

Obr. 66: Palác umění Neftjanik, Surgut, Rusko

19 CURRICULUM VITAE

Osobní údaje:

Jméno: Ing. Michal Drlík
Narozen: 4. 10. 1981 v Olomouci
Adresa: 9. května 806
Telefon: +420 608 730 895
Email: drlik81@gmail.com
Národnost: Česká

Vzdělání:

Základní škola: Újezd u Brna
Střední škola: Sdělovací a zabezpečovací technik SOU Spojů, zakončené maturitou

2006 – 2009

Vysoké učení technické v Brně – Fakulta strojního inženýrství - ukončení titulem Bc.

Bakalářská práce – aplikace servo – pohonu s asynchronním motorem pro řízení divadelní točny. Práce byla provedena včetně praktické aplikace

2009 – 2011

Vysoké učení technické v Brně – Fakulta strojního inženýrství – ukončení titulem Ing.

Diplomová práce – souřadnicová CNC vrtačka. Práce byla provedena včetně praktické aplikace

2011 – doposud

Vysoké učení technické v Brně – Fakulta strojního inženýrství

Doktorská práce – Metodika a validace softwaru pro bezpečnostní části řídicích systémů v divadelní technice

Zaměstnání:

2001 – 2002	technik ve společnosti Prosoton, s.r.o.
2004 – 2005	vedoucí výroby – realizace zakázek ve společnosti Prosoton, s.r.o.
2005 – 2012	vedení společnosti, obchodní činnost ve společnosti Prosoton, s.r.o.
2010 – 2012	certifikace pro divadelní technologii ve společnosti Prosoton, s.r.o.
2012 – doposud	Ředitel společnosti Drivecontrol, s.r.o.