VYSOKÉ UČENÍ
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

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 – obor aplikované informatika ve strojírenství – ukončení titulem Bc.

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

2009 – 2011

Magisterském studium – ukončení titulem Ing.

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

2011 – doposud

Doktorské studium – Fakulta strojního inženýrství ústav výrobních strojů, systémů a robotiky

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

Zaměstnání:

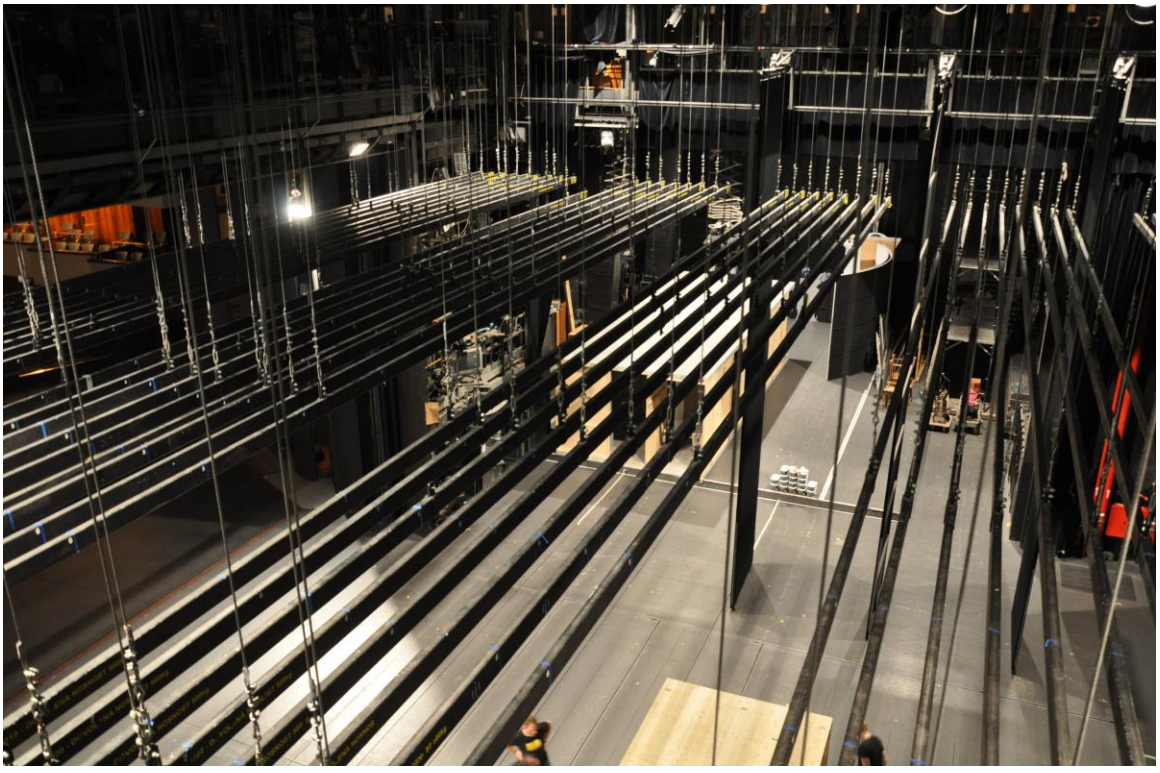
2001 – 2002	Technik ve společnosti Prosoton, s.r.o.
2004 – 2005	Vedoucí výroby – realizace zakázek ve společnosti Prosoton, s.r.o.
2005 – 2012	Vedení společnosti, obchodní činnost ve společnosti Prosoton, s.r.o.
2010 – 2012	Certifikace pro divadelní technologii ve společnosti Prosoton, s.r.o.
2012 – doposud	Ředitel společnosti Drivecontrol, s.r.o.

OBSAH

1 ÚVOD

Bezpečnost mechatronických systémů používaných v divadelní technice je v posledních letech intenzivně diskutovanou záležitostí. Na jevištní scéně jsou za přítomnosti herců tvořeny různé triky a vizuální efekty pomocí kulis, osvětlení a audiovizuální techniky. Tyto triky jsou zpravidla realizovány pomocí mechatronických prvků. Zařízení o velké hmotnosti (až několik tun), která jsou instalována na divadelní scéně, se pohybují mnohdy až rychlostí 2 m/s Obr. 1. Hmotnosti zavěšených kulis se pohybují od jednotek až do několika stovek kilogramů. Divadelní mechatronické systémy se významně liší od běžných strojních zařízení. Prostor jeviště je při aktivní scéně nepřehledný. Pohyby jednotlivých zařízení se odehrávají ve tmě, a herci nemají možnost na pohybující předměty včas bezpečně zareagovat. Počet společných pohybů jednotlivých zařízení u větších divadel lze počítat na desítky. Herci a technici se za pohybu těchto zařízení pohybují pod zdvihaným břemenem nebo v těsné blízkosti posouvaných částí nebo na nich dokonce stojí. Vzhledem k dynamice a vlastní hmotnosti mechanismů mohou mít případné úrazy v lepším případě trvalé následky. V České republice dochází ročně k desítkám zranění, které se odehrávají na scénách se zastaralou divadelní technikou bez náležitých bezpečnostních funkcí.

Významnou etapou zajišťování bezpečnosti herců nebo dalších osob pohybujících se na jevišti je návrh bezpečnostních částí řídicího systému mechatronických zařízení. Velkou roli zde má použitá metodika vývoje a validace bezpečnostního softwaru.



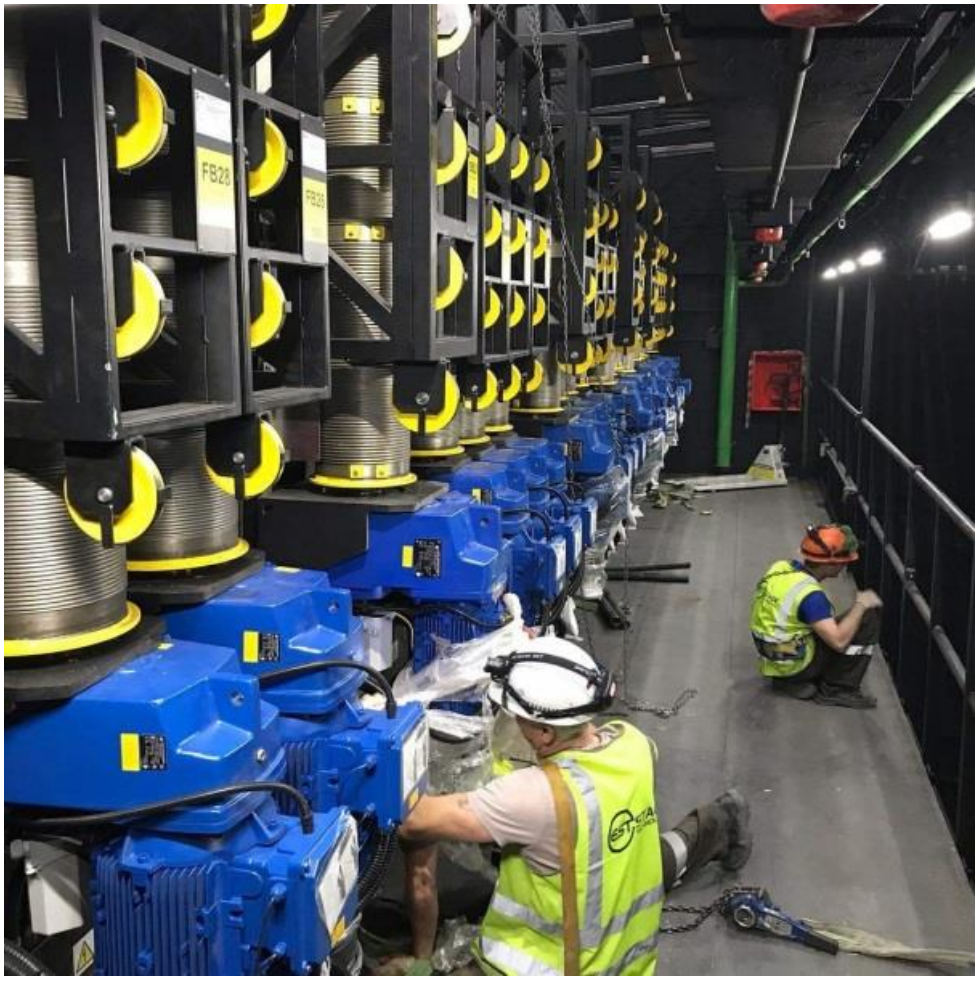
Obr. 1: Jevištní scéna

2 DIVADELNÍ PROSTOR

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. Krajní bezpečnostní polohy zdvihu jsou snímány vřetenovým diskrétním spínačem umístěným na hřídeli lanového bubnu.

V praktickém použití jsou pohonné jednotky většinou kotveny k obvodové zdi budovy, jak je znázorněno na Obr. 2. 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.

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.



Obr. 2: Pohonná jednotka divadla

3 DIVADELNÍ MECHANISMY

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.

Bodový tah Obr. 3 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. 3: Pohonné mechanismy – bodový tah

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.

Jevištní stoly obvykle tvoří kompletní podlahu jeviště Obr. 4. 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. 4: Pohonné mechanismy – jevištní stoly

4 LEGISLATIVNÍ RÁMEC PRO DIVADLA A KULTURNÍ OBJEKTY – ZÁKONY A NAŘÍZENÍ VLÁDY – LEGISLATIVA V ČR A EU

Oblast divadelních technologií reguluje velké množství Evropských směrnic a harmonizovaných i neharmonizovaných norem. Mezi významné směrnice a vyhlášky patří:

- zákon č. 22/1997 Sb. – technické požadavky na výrobky,
- strojní směrnice 2006/42/ES pro strojní zařízení,
- směrnice 2011/65/EU RoHS o omezení nebezpečných látek v elektronice,
- směrnice 2014/30/EU elektromagnetické kompatibility,
- směrnice 2014/35/EU pro elektrická zařízení nízkého napětí,
- vyhláška č. 246/2001 Sb. o stanovení podmínek požární bezpečnosti,
- směrnice 2009/104/ES o požadavcích na bezpečnost a ochranu zdraví,
- směrnice 2012/19/EU o odpadních elektrických a elektronických zařízení.

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.

V divadelní technice nelze aplikovat standardní postupy zajištění BOZP na pracovišti. 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 ani jinými výstražnými prvky nebo vybavovat herce bezpečnostními úvazy a ochrannou přilbou. Toto ohraničení nebo OOPP by bránilo hereckému výkonu a celkovému scénografickému a uměleckému záměru.

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. Česká republika tuto obdobnou normu nemá, proto je nutné vycházet ze správné technické praxe jiného členského státu EU. Obecně je považována německá národní norma DIN 56950-1:2012 (Divadelní technologická zařízení – Strojně technická zařízení – Část 1: Bezpečnostně technické požadavky a kontrola) za jednu z nejpropracovanějších, nespecifikuje však požadovaný postup vývoje bezpečného softwaru řídicího systému.

Tato německá národní technická norma je však 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.

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

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 však nebyl nikde publikován žádný ověřený metodický postup, který by specifikoval správnou technickou praxi v oblasti vývoje a validace softwarových aplikací pro bezpečnostní části řídicího systému (SRP/CS) divadelní techniky.

7 CÍLE PRÁCE

Předložená práce přispívá k řešení problematiky zajišťování bezpečnosti složitých mechatronických systémů používaných u divadelní techniky. Cílem je vyřešit problém spojený z důvodně předpokládaným nesprávným chováním osob a obsluhy těchto systémů pomocí bezpečnostních opatření respektující povahu specifických podmínek používání těchto mechanismů. Důraz je zde kladen na vývoj, verifikaci a validaci softwaru pro bezpečnostní části programovatelných elektronických systémů používaných pro ovládání jevištních mechanismů. Validace je prezentována na implementaci metodiky při vývoji systému funkční bezpečnosti jevištní techniky Národního divadla v Brně.

8 NÁVRH METODIKY VÝVOJE A VALIDACE BEZPEČNOSTNÍHO SOFTWARE

Vzhledem k rozsáhlosti a komplexnosti mechatronického systému jevištní techniky divadel vyžaduje vývoj bezpečného řídicího systému (hardware a software) značné lidské, finanční a časové zdroje. Pro dosažení integrity bezpečnosti SIL3 u hardwaru i softwaru je nezbytné používat komerčně dostupné certifikované komponenty a systémový přístup, aby nebyly překročeny mezní náklady umožňující prodejnost celého systému. Okrajové podmínky pro úspěšný vývoj řídicího systému vymezují nutnost používat pro bezpečnostní aplikace:

- certifikovaný hardware,
- certifikovaný komunikační protokol,
- certifikovaný software s omezeným programovacím jazykem.

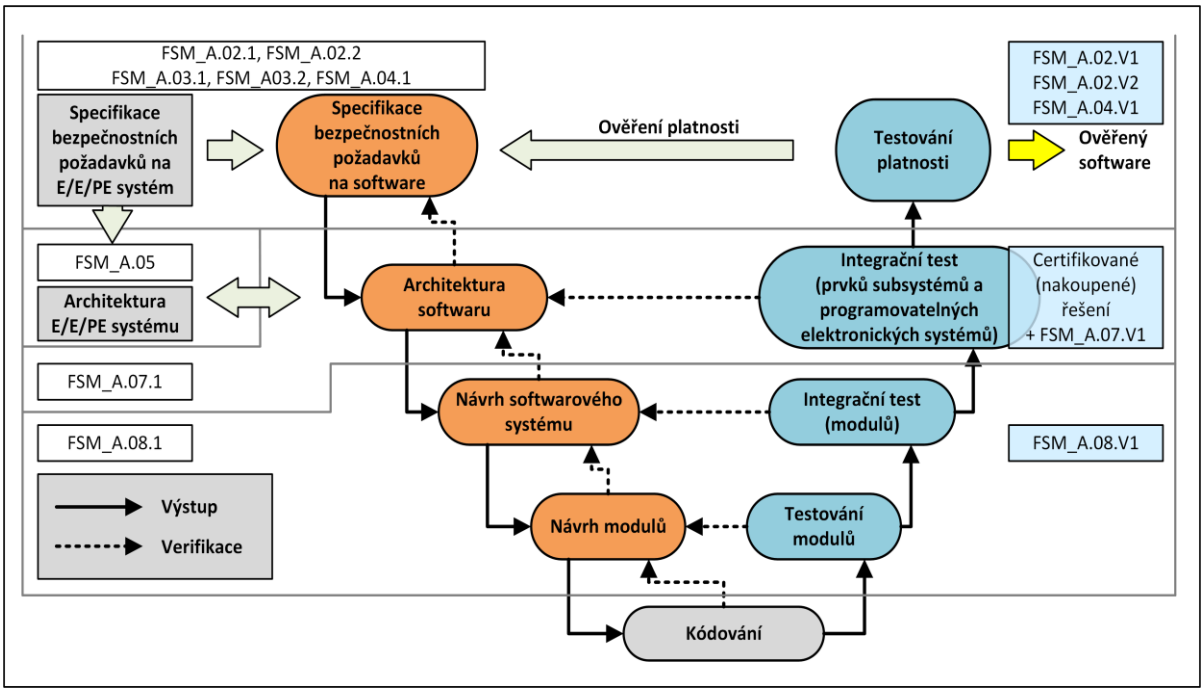
Implementace komerčně dostupného HW a SW umožní zkrátit čas nezbytný pro vývoj řídicího systému, stále však zůstává potřeba verifikovat vhodnost použitých komponent a navrženého softwaru pro vyvíjené bezpečnostní funkce.

Vývojové prostředí používané jako editor bezpečnostního softwaru musí mít příslušnou certifikaci v oblasti funkční bezpečnosti, uživatel však musí nastavit procesy umožňující specifikovat požadavky na bezpečnostní funkce, plánovat postup verifikace a validace, řídit změny vyvíjeného softwaru, nastavit přístupy a oprávnění pro programátory.

Eliminace systémových chyb při vývoji bezpečného SW v rámci managementu funkční bezpečnosti je realizovatelná výhradně pomocí systémového přístupu k návrhu dílčích procesů a dokumentování jejich realizace. Pro vývoj bezpečného SW a HW je tedy nezbytné vypracovat metodický postup a navrhnout vhodnou formu dokumentování tohoto postupu, která umožní významně redukovat potenciální systematické chyby.

8.1 METODIKA VÝVOJE A VALIDACE SOFTWARU

Sestavení této metodiky odpovídá jejímu začlenění do životního cyklu celkové bezpečnosti a managementu funkční bezpečnosti vývoje softwaru a navazuje na již zpracované metodické postupy pro ostatní fáze životního cyklu celkové bezpečnosti mechatronických systémů divadelní techniky. Základním prvkem této metodiky je osvědčený V-model vývoje mechatronických systému Obr. 5: V-model.



Obr. 5: V-model

Ve výše uvedeném obrázku představují jednotlivé bloky FSM_A.xx nezbytnou dokumentaci **F**unctional **S**afety **M**anagementu, respektive provedených vývojových činností. Osvědčilo se nám aplikovat systémový přístup jak na strukturu těchto dokumentů, tak na jejich označování, které napomáhá přehledné evidenci dokumentace. Jednotlivé dokumentační celky jsou označeny prefixem složeným z písmene „FSM_A“ a dvojčíslím odděleným tečkou. Každý takto označený blok je z pohledu systémového přístupu k managementu funkční bezpečnosti definovanou uzavřenou dokumentační skupinou. Případné další členění těchto bloků se značí další oddělovací tečkou. Např. blok A.02 má členění dále na A.02.1 a následující dokument by byl označen A.02.2 atd.

Verifikační dokumenty, mají v označení bloku navíc uvedeno velké písmeno „V“. Těchto verifikačních dokumentů může být pro každý blok více dle počtu provedených testů. Z tohoto 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.

Níže následuje vysvětlení jednotlivých kroků procesu vývoje bezpečného SW, které je dále graficky znázorněno na Obr. 6.

Krok 1 - Plánování bezpečnosti

Plán managementu funkční bezpečnosti popisuje činnosti související s bezpečností celého procesu vývoje a dokumenty, které jsou vytvořeny za tímto účelem. Tento blok je označen FSM_A.02. Uvedený postup splňuje 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 je vytvořený formulář pro interní a externí simulaci chyb.

Krok 2 - Specifikace bezpečnostních požadavků

V této části jsou definovány veškeré požadavky týkající se bezpečnosti výrobku, včetně požadavků z aplikačních technických norem ČSN EN 61508 ed.2:2011. Tento blok je označen FSM_A.03. V dokumentu FSM_A.03.1 jsou definovány specifikace bezpečnostních požadavků.

Krok 3 - Plánování validace

V tomto kroku se ze specifikací bezpečnostních požadavků FSM_A.03.1 vytvoří specifikace validačních testů FSM_A.04.1. Obsahem je soupis všech požadovaných testů, kdo je za ně odpovědný a kdy a jakým způsobem budou provedeny.

Krok 4 - Architektura softwaru

Tento blok je označen FSM_A.07 a zahrnuje:

- strukturu softwaru a jeho rozhraní,
- dynamické a statické chování aplikovaného softwaru,
- poruchy a chování,
- ověřování způsobilosti a oprávněnosti nakupovaného řešení.

Požadavky softwarové architektury jsou specifikované v dokumentu FSM_A.03.1. Popis architektury systému je zaznamenaný v dokumentu FSM_A.05.1. V popisu architektury systému jsou definovány všechny rozhraní mezi komponenty. Návrh systému zahrnuje rozsah požadavků, detekci a reakci na chyby, interface subsystému.

Jako výstupní dokument je naplněn dokument FSM_A.07.1, který popisuje softwarovou architekturu. Způsobilost a oprávnění používání existujícího bezpečnostního softwaru a jeho komponentů popisuje dokument FSM_A.07.V1.

Krok 5 - Softwarový systém a návrh modulů

Tento blok je označen FSM_A.08. V tomto kroku jsou provedeny návrhy jednotlivých softwarových subsystémů a příslušných softwarových modulů.

Software design zahrnuje několik různých integračních testů a činností:

- SW – SW integrace,
- HW – SW integrace,
- subsystémy a systémová integrace,
- návrh modulů,
- testování „black box“

Krok 6 - Integrační testy

Integrační testy na úrovni architektury softwaru se při použití nakupovaného certifikovaného vývojového prostředí software neprovádí, protože jsou již začleněny v tomto prostředí. Provádí se ovšem ověření způsobilosti použití tohoto existujícího softwaru a jeho komponent, a to už v kroku 4 při sestavování architektury softwaru.

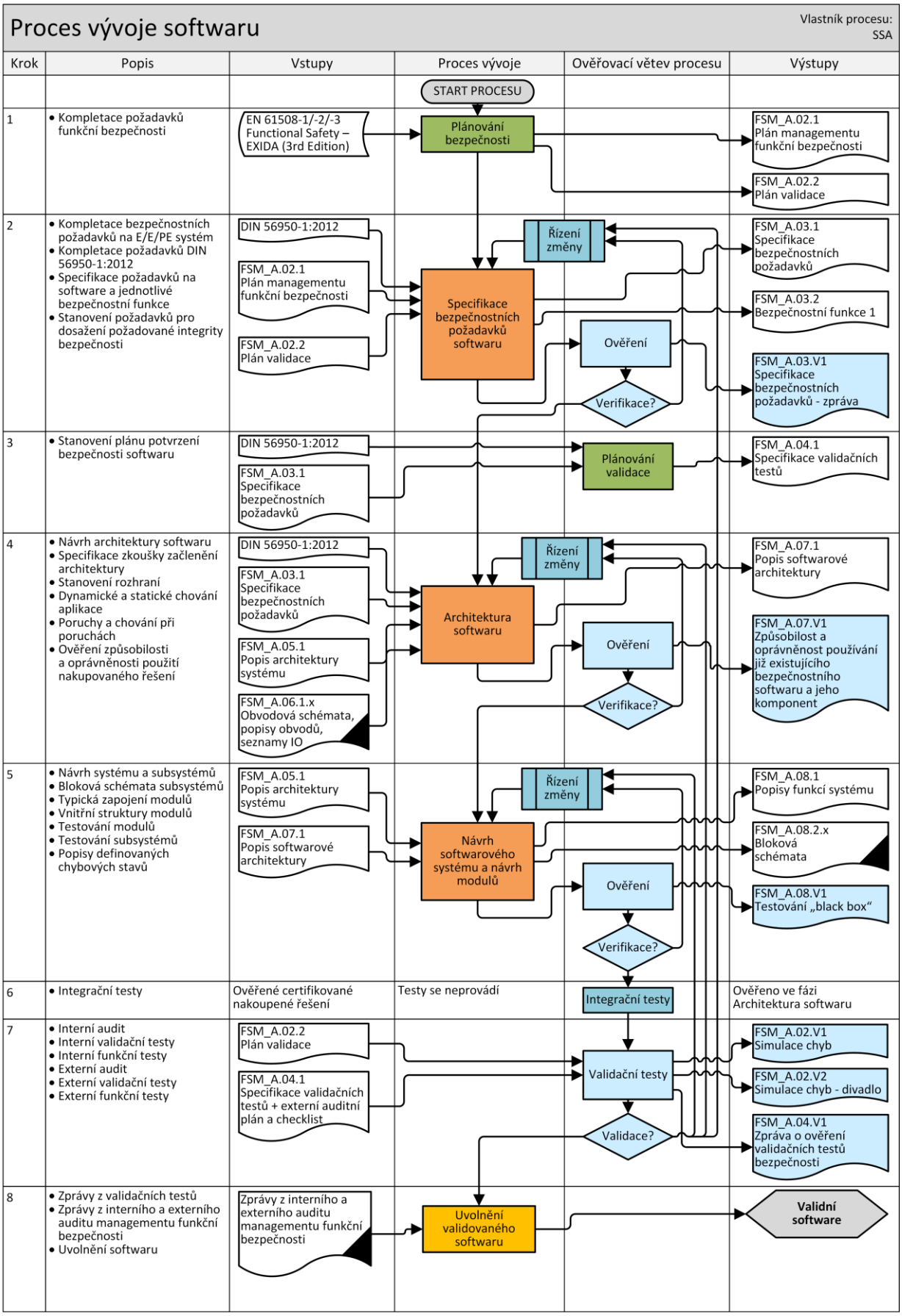
Krok 7 - Validace

Při validacích se postupuje dle specifikace validačních testů FSM_A.04. V rámci testování je prováděno např. testování „black box“ subsystémů, zátěžové testování, simulace chyb, popřípadě jiné techniky. V kroku validace jsou provedeny i specifikované interní a externí audity.

Krok 8 - Uvolnění validního softwaru

Po úspěšném dokončení validací v kroku 7 jsou zkontrolovány zprávy všech interní a externích auditů a na základně kladného závěru všech auditů může být výsledný, nyní již validní software uvolněn.

Navržená 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 je následně zpracován jako model a pro jednotlivé kroky jsou vytvořeny patřičné dokumenty, popřípadě patřičné nástroje pro zrealizování. Na Obr. 6 je zobrazený navržený postupový diagram procesu vývoje bezpečného softwaru popisující systémový a procesní přístup vyvinuté metodiky.



Obr. 6: Systémový přístup k vývoji a validaci bezpečnostního software pro jevištní techniku v divadle

8.1.1 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 tabulce 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

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 doplit 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.

8.1.2 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):

- 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. [2]

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 skutečně požadavky integrovány všechny a vhodným způsobem je navázat na interní standardy a postupy vývojového týmu. [2]

9 VALIDACE NAVRŽENÉ METODIKY NA REÁLNÉ APLIKACI DIVADELNÍ TECHNIKY

Vyvinutá metoda byla validována při vývoji řídicího systému pro Národní divadlo Brno – Janáčkovo divadlo Obr. 7.

Obr. 7: 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. 8 a ovládacích pultů.

Obr. 8: Rozvodné skříně řídicího systému

9.1 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,
- asynchronní chod se skupinovým vypnutím,
- synchronní chod.

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.

9.2 HUMAN MACHINE INTERFACE – ROZHRANÍ ČLOVĚK – STROJ

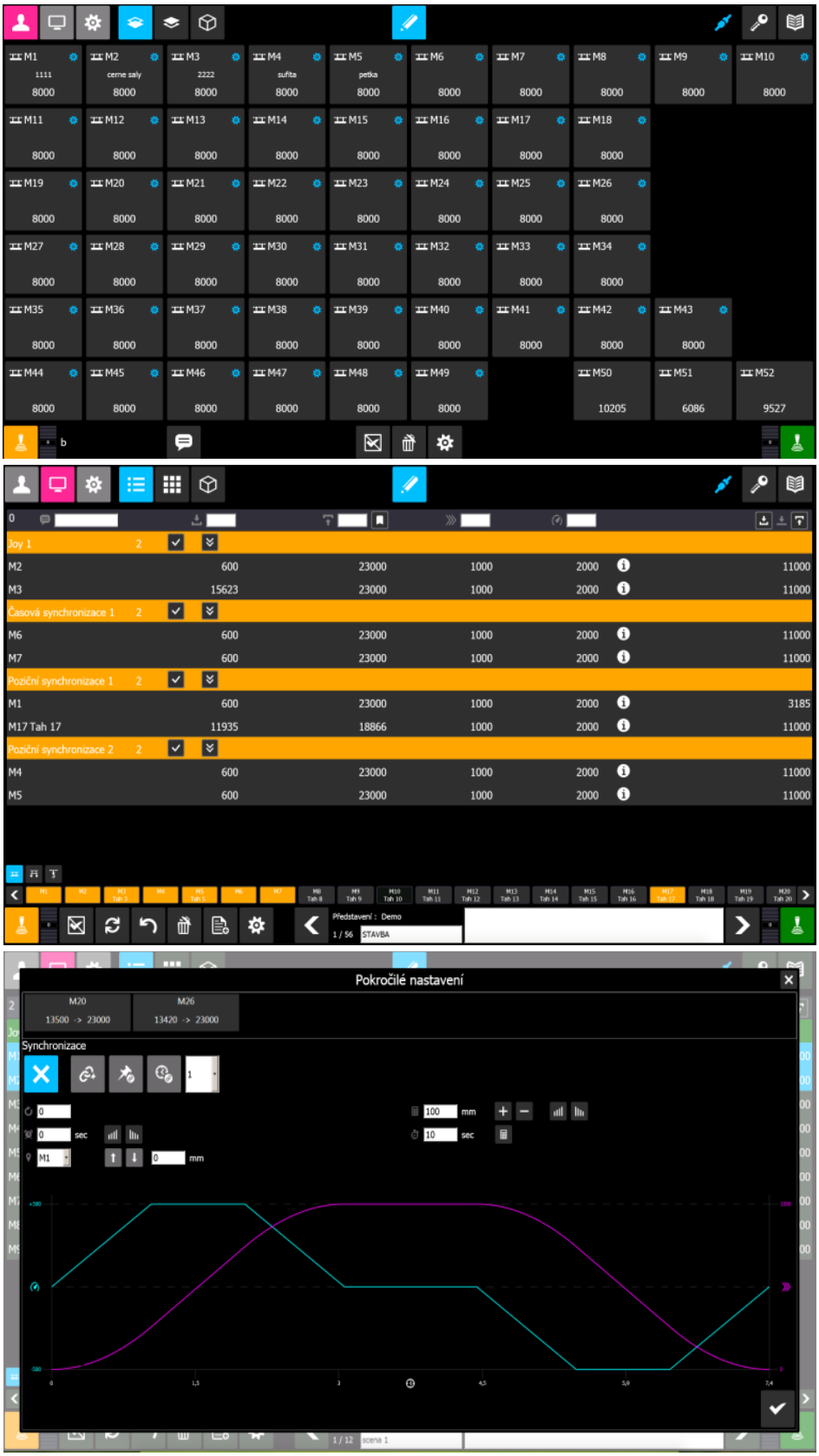
Ovládací pult slouží pro plnou kontrolu nad automatizovanými zařízeními v rámci divadelního představení. Pult je vybavený dotykovou obrazovkou, která umožňuje nejen snadnou tvorbu divadelních scén, jejich editaci či mazání, ale také možnost odzkoušení jednotlivých zařízení při samostatné jízdě, diagnostiku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

Základní požadavky na ovládací pult Obr. 9 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. 9: Ovládací pult Janáčkovo divadlo

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. 10. 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.



Obr. 10: Ukázky vizualizace iTEMS

10 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 SIL 3, 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 od společnosti TÜV SÜD Obr. 11.

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

CERTIFIKÁT TYPU

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

vedoucí certifikačního orgánu

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

TÜV®

Obr. 11: Inspekční certifikát

11 ZÁVĚR

Podstatou vyvinuté metodiky vývoje a validace softwaru souvisejícího s bezpečností je aplikace systémového a procesního přístupu specifikovaného jednotlivými kroky, které je nutné provést tak, aby byly splněny požadavky na bezpečnost jevištní techniky a současně eliminován vliv lidského faktoru na vznik vývojových, respektive programátorských chyb. Tomu významně napomáhá logicky strukturovaná dokumentace všech vývojových kroků celého procesu. Vyvinutá metodika vývoje a validaci softwaru může být použita nejen pro návrh softwaru v oblasti složitých mechatronických systémů divadelní techniky, ale obecně pro veškerá strojní zařízení, u kterých je potřeba snižovat rizika pomocí aplikace funkční bezpečnosti související s vývojem softwaru souvisejícího s bezpečností. Vyvinutá metodika může přispět nejen ke zvýšení bezpečnosti osob nacházejících se v blízkosti divadelní techniky (jevišti, hledišti i strojním zázemí) ale i v oblastech jiné zábavní techniky, nebo po přenesením do jiných odvětví strojírenství i na mnoha dalších pracovištích různorodého zaměření jak v Evropské Unii, tak i mimo ni o čemž svědčí i úspěšná implementace metodiky při vývoji řídicího systému divadelní techniky pro pobočku ruského národního divadla v Moskvě.

12 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.