ZÁPADOČESKÁ UNIVERZITA v PLZNI
FAKULTA ELEKTROTECHNICKÁ

Katedra aplikované elektroniky a telekomunikací

BAKALÁŘSKÁ PRÁCE

Automatizované víceúrovňové testování řídícího počítače kolejového vozidla

Václav Průcha **2015/2016**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Václav PRŮCHA**
Osobní číslo:	**E13B0213P**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Elektronika a telekomunikace**
Název tématu:	**Automatizované víceúrovňové testování řídicího počítače kolejového vozidla**
Zadávající katedra:	**Katedra aplikované elektroniky a telekomunikací**

Zásady pro vypracování:

1. Popište základní principy a účel testovaných funkcí v rámci kolejového vozidla.
2. Popište provozní a poruchové stavy testované skupiny funkcí.
3. Definujte metodu testování, testovací scénáře a stupeň pokrytí testy pro testovanou skupinu funkcí.
4. Určete, do jakého stavu se musí testovaná funkce dostat, aby byl zachován bezpečný stav a nedošlo k poškození zařízení anebo zařízení zůstalo v provozu s přiměřenou degradací funkce.
5. Shrňte dosažené výsledky, získané znalosti a zkušenosti.

Rozsah grafických prací: **podle doporučení vedoucího**
Rozsah kvalifikační práce: **30 - 40 stran**
Forma zpracování bakalářské práce: **tištěná/elektronická**
Seznam odborné literatury:

1. **Norma EN 50128**
2. **Dokumentace testovaného SW**

Vedoucí bakalářské práce: **Doc. Ing. Bohumil Skala, Ph.D.**
Katedra elektromechaniky a výkonové elektroniky

Datum zadání bakalářské práce: **15. října 2015**
Termín odevzdání bakalářské práce: **2. června 2016**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Dr. Ing. Vjačeslav Georgiev
vedoucí katedry

V Plzni dne 15. října 2015

Abstrakt

Předkládaná bakalářská práce je zaměřena na automatizované víceúrovňové testování řídícího počítače kolejového vozidla. Celá práce se soustřeďuje na testování stavů střídavého hlavního vypínače, který je nedílnou součástí vysokonapěťové výzbroje lokomotivy. První částí je obecný popis vysokonapěťové výzbroje lokomotivy s konkrétnějším popisem samotného hlavního vypínače pro danou lokomotivu a manuálním ovládáním. V další části se začínám zabývat algoritmy pro softwarové ovládání hlavního vypínače a jeho chování při nepožadovaných stavech. Ty souvisí s následující částí zaměřenou na bezpečnost SW a způsoby testování. Praktická část se vztahuje na automatizované testování funkcí hlavního vypínače testovacím softwarem UTS1 vytvořený společností Škoda Transportation.

Klíčová slova

Hlavní vypínač, lokomotiva, testování, V diagram, Univerzální Testovací Systém, LCC, ochrany, softwarový modul, SIL

Abstract

This bachelor thesis is focused on automated multi-level testing of the control computer of the rail vehicle. The whole work concentrates on testing the conditions of the alternating main power switch, which is an integral part of the high voltage equipment of the locomotive. The first part is a general description of the high voltage equipment with a more specific descripton of the main switches for the engine and manual control. Other parts are already starting to adress algorithms for software control of the main switch a it´s behavior when equipment not required states. Those related to the following parts of the security-oriented software and methods of testing. The practical part refers to the automated testing functions of the main power switch to test the software UTS1 created by te company Škoda Transportation.

Keywords

The main switch, locomotive, software testing, V-diagram, the Universal Testing System, LCC, protection, software module, safety integrity level

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této bakalářské práce.

Dále prohlašuji, že veškerý software, použitý při řešení této bakalářské práce, je legální.

.....

podpis

V Plzni dne 30.5.2016 Václav Průcha

Poděkování

Tímto bych rád poděkoval vedoucímu bakalářské práce doc. Ing. Bohumilovi Skalovi, Ph.D. a Ing. Jiřímu Šaškovi, Ph.D. za cenné profesionální rady, připomínky a metodické vedení práce.

Obsah

Seznam obrázků

Seznam tabulek

Seznam symbolů a zkratek

AC	Alternating Current - Střídavý proud
ADD	Automatic Drop Device – Systém, který zajišťuje automatické a rychlé stažení sběrače v případě poškození kontaktní lišty sběrače.
ATO	Automatic Train Operation – Jednotka realizující centrální regulátor vozidla zadávající tažnou a brzdnou sílu pro pohon.
CAN	Controller Area Network – Síť v oblasti řídících prvků. Je využívána díky vysokému zabezpečení dat kódu a díky symetrickému vedení i dobré odolnost vůči rušení.
ČSN	Československá norma – Chráně označení českých technických norem. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví má na starost vydávání a tvorbu.
D8206P1	Počítač nadřazeného řízení. Jednotka určena pro realizaci nadřazených řídicích systémů. Jednotka je ovládaná 16-bitovým mikrokontrolérem.
DC	Direct Current - Stejnosměrný proud
DCC	Diagnostic Computer – Diagnostický počítač.
ETH	Ethernet – Název pro souhrn technologií počítačových sítí. Používají se kabely s kroucenou dvojlinkou nebo optické kabely. Přenosové rychlosti dosahují od 10Mbit/s do 100Gbit/s. Ethernet realizuje fyzickou i linkovou vrstvu modelu ISO/OSI.
HV	Hlavní vypínač – Slouží k odpojení a připojení lokomotivy k vysokému napětí.
HW	Hardware – Soubor všech fyzicky existujících prvků. Technická výbava lokomotivy.
I/O	Input/Output – Vstupně/Výstupní moduly, zajišťují komunikaci mezi informačním systémem zpracovávající data a vnějším systémem. Vstupy jsou data přijaté systémem a výstupy jsou data odeslána do informačního systému.
LCC	Leading Command Computer - Řídicí počítač sloužící k řízení logiky vozidla a zajištění distribuce dat pro ostatní subsystémy ve správném formátu. Logika vozidla je řízena primárně na základě vstupů od obsluhy vozidla získaných prostřednictvím I/O modulů.
MBF	Modul of Base Functions – Modul základních funkcí. Programovatelná řídicí jednotka fyzickými (analogovými i binárními) vstupy a výstupy a komunikačním rozhraním. Primárním úkolem je ovládat fyzické výstupy i v případě, kdy MBF nedostává po komnikaci informaci o tom, jak mají být tyto výstupy nastaveny.
MTBF	Mean Time Beween Failures – Střední doba mezi poruchami. Statistická veličina pro ohodnocení spolehlivosti výrobků. Určuje se jen u výrobků, které se opravují.
MVB	Multifunction Vehicle Bus – Multifunkční vozidlová sběrnice. Slouží k přenosu signálů (datových souborů) pro řízení a diagnostiku v rámci lokomotivy nebo ucelené jednotky.
PDF	Portable Document Format – Formát vytvořený firmou Adobe pro nezávislé používání dokumentů. Může obsahovat text i obrázky. Hlavní výhodou je, že se na všech zařízeních zobrazí stejně.

RS232	Sériová linka – Používá se jako komunikační rozhraní. Umožňuje propojení a vzájemnou sériovou komunikaci dvou zařízení.
SIL	Safety Integrity Level – Stupeň integrity bezpečnosti. Relativní úroveň rizika zajištěného bezpečnostní funkcí.
SW	Software – Součást počítačového systému, složený z kódovaných informací nebo strojových instrukcí.
TCU	Traction control unit – Samostatný řídicí systém pro řízení trakčních měničů a jejich ochran.
THR	Tolerable hazard rate – Povolená míra rizika neboli snesitelné nebezpečí. Používá se k definování úrovně bezpečnosti integrity.
UIC	International Union of Railways – Globální společnost, která koordinuje rozvoj a fungování železniční dopravy ve všech členských státech. Řeší například vytváření nových a zachování stávajících mezinárodních spojů, unifikaci železniční techniky a dohlíží na dodržování bezpečnostních kritérií.
UTS1	Universal testing systém – Univerzální testovací software pro testování a diagnostiku. Vytvořen společností Škoda Transportation.
VCU	Vehicle control unit – Redundantní řídicí počítač lokomotivy složený ze tří procesorových karet (LCC+ATO+DCC).
VN	Vysoké napětí
4Q	Four quadrant – Měnič fungující ve všech čtyřech kvadrantech momentové charakteristiky. Využívá se pouze tehdy, kdy to umožňuje napájecí soustava.

Úvod

Tato bakalářská práce se zabývá automatizovaným víceúrovňovým testováním řídícího počítače kolejového vozidla NIM Express 109E pro Německé dráhy. Řízení softwarem je v dnešní době velmi stěžejní pro širokou škálu zařízení a k tomu neodmyslitelně patří testování. Testování se provádí pro zabezpečení správné činnosti zařízení, ochrany vozidla vůči poruchám a ochrany života cestujících.

V této práci se testuje hlavní vypínač, který je důležitou součástí vysokonapěťové výzbroje lokomotivy. Řízen je pomocí řídícího počítače LCC, který je součástí nadřazeného řízení a je jednou ze tří procesorových karet v jednotce VCU.

Úvodem jsou shrnuty základní technické parametry vysokonapěťové výzbroje lokomotivy a detailní popis testovaného hlavního vypínače. Je zde popsáno manuální ovládání hlavního vypínače strojvedoucím a algoritmy pro ovládání či ochrany hlavního vypínače. V další části je stručně vysvětlen vývojový proces software pro drážní řídicí a ochranné systémy, který je popsán normou ČSN EN 50128. V závěru se práce zabývá praktickou částí, kde je popsán průběh testování, testovací prostředí, ukázka testovacího skriptu, textový výstup zpracovatelný strojově a výsledkový protokol.

Obrázek 1 - Lokomotiva NIM 109E [2]

1. Lokomotiva NIM - 109E3

Lokomotiva NIM - 109E3 je čtyřnápravová elektrická lokomotiva pro trakční napájecí systém 15kV 16,7 Hz AC. Lokomotiva je skříňového provedení s kabinami strojvedoucího na obou koncích. Uspořádání lokomotivy je se dvěma strojovnami po stranách lokomotivy a s průchozí uličkou mezi nimi. Vstup do uličky je dveřmi v mezistěně každé kabiny.

Základní technické parametry lokomotivy jsou podrobněji popsané v následující kapitole.

1.1 Základní technické parametry lokomotivy

1.1.1 Základní údaje lokomotivy

Nejvyšší konstrukční rychlost	200 $km.h^{-1}$
Provozní hmotnost	89,1 t
Trvalý výkon trakčních motorů	6400 kW
Maximální výkon elektrodynamické brzdy	6900 kW
Rozjezdová tažná síla	274 kN
Maximální brzdná síla na obvodu kol	130 kN

Tabulka 1 - Základní údaje lokomotivy [2]

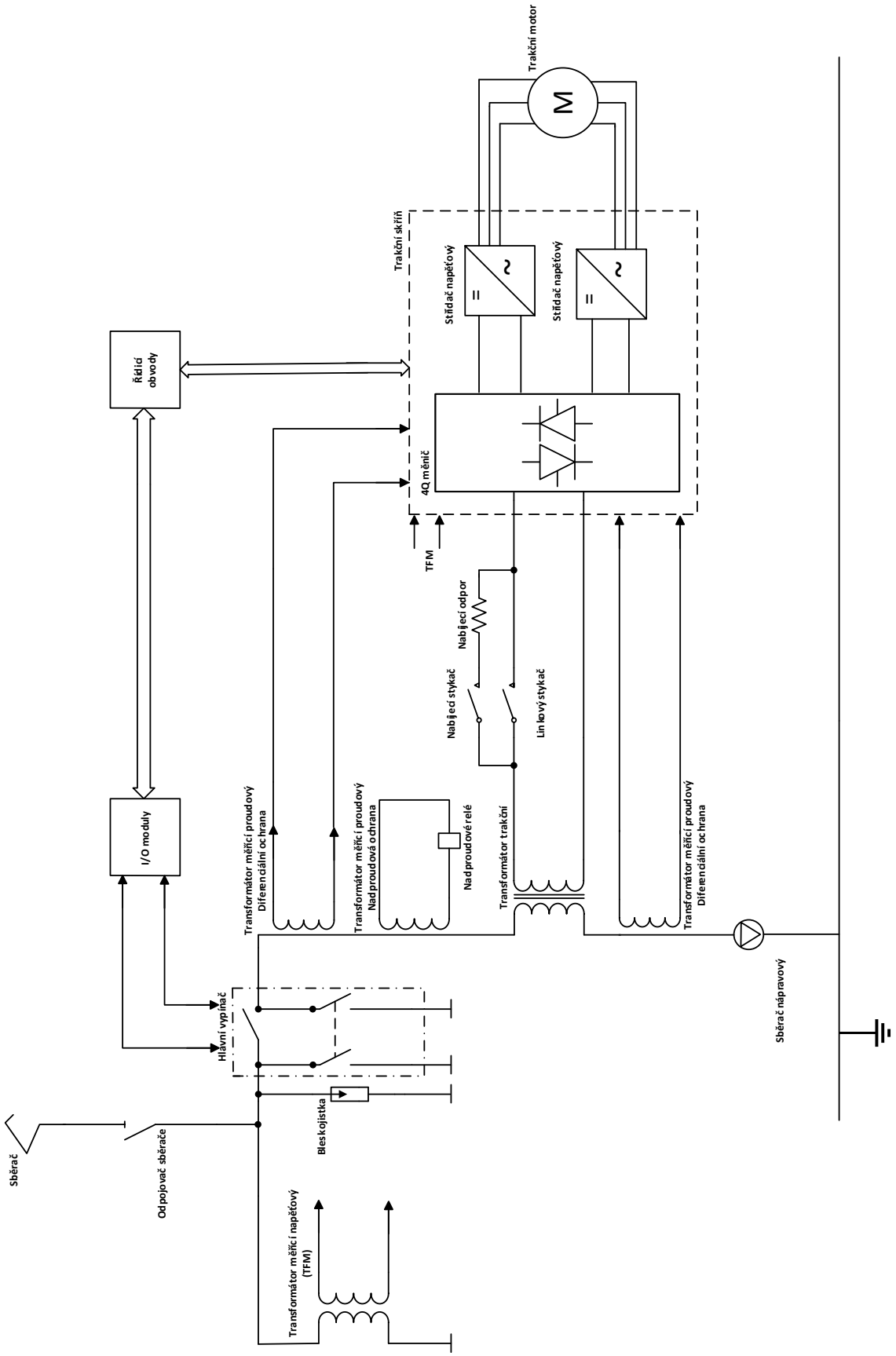
1.1.2 Základní rozměry lokomotivy

Obrys	UIC 505-1
Maximální šířka	3 080 mm
Výška lokomotivy se zaklesnutým sběračem	4 278 mm
Délka lokomotivy přes nárazníky	18 000 mm
Rozvor lokomotivy	11 200 mm
Rozvor podvozku	2 500 mm
Jmenovitý průměr nového kola	1250 mm

Tabulka 2 - Základní rozměry lokomotivy [2]

1.2 Popis schématu obvodů vysokého napětí

V dalším textu jsou stručně popsány základní komponenty lokomotivy, které souvisí s řešeným úkolem. Na obrázku číslo 2 je uvedeno zjednodušené schéma obvodů vysokého napětí. Z hlediska obsahu této práce je klíčovou komponentou hlavní vypínač, trakční pohon a řídicí systém.



Obrázek 2 - Schéma obvodů vysokého napětí

- **Trakční transformátor**

Transformátor je jednofázový lokomotivní transformátor určený k provozu na jednofázových napájecích systémech 15 kV AC / 16,7 Hz. K izolaci je použit materiál vyhovující provozu zařízení až do vysokých teplot.

Lokomotiva je prostřednictvím transformátoru schopna napájet vlak napětím 1000 v 16,7 Hz.

Chlazení soustavy transformátoru je řešeno dvěma chladiči umístěnými v prostoru nad transformátorem. Chlazení je řešeno nezávisle, tudíž při výpadku jednoho okruhu lze transformátor provozovat na 50% jmenovitého výkonu.

- **Skříň trakčních měničů**

Ve strojovnách lokomotivy jsou instalovány dvě identické měničové skříně. Každá skříň měničů tvoří mechanicky uzavřený celek, který slouží k napájení jednoho podvozku (dva trakční motory) a souvisejících pomocných pohonů.

Skříň trakčních pohonů obsahuje trakční 4Q usměrňovač, trakční střídače, pulzní měnič elektrodynamické brzdy, snižovací měnič pro napájení pomocných pohonů. Skříň měničů je vybavena samostatným řídicím systémem označeným TCU (Traction Control Unit).

TCU zajišťuje řízení jednotlivých měničů a střídačů a jejich ochrany. Současně také zajišťuje tzv. lokomotivní ochrany (nadproudová ochrana, diferenciální ochrana, ochrana zemního spojení). Elektrická zařízení pro napájení trakčních motorů jednoho podvozku, jednoho bloku elektrodynamické brzdy a pomocných pohonů lokomotivy.

- **Trakční motor**

Pohon dvojkolí zajišťuje asynchronní třífázový motor. Trakční motor je 6 pólový asynchronní motor. Jmenovitý výkon je 1600 kW a maximální provozní otáčky 3700 min^{-1}.

- **Nápravový sběrač**

Nápravový sběrač slouží k převodu elektrického proudu z lokomotivy do kolejnic. Omezuje tím na minimum nežádoucí proudy. Přechod elektrického proudu z pevné části nápravového sběrače na pohybující se sběrací kotouč je proveden pomocí uhlíkových kartáčů přitlačovaných k tomuto kotouči pružinami.

- **Sběrač trakčního proudu**

Na střeše lokomotivy jsou umístěny dva polopantografové sběrače identického typu. Sběrače jsou vybaveny zařízením ADD, které slouží k automatickému a rychlému stažení sběrače v případě poškození kontaktní lišty. Ovládání je elektropneumatické.

- **Lokomotivní ochrany**

Hardwarové lokomotivní ochrany vyhodnocují nadproud troleje na AC systému, diferenciální ochranu na AC systému či nadproud napájení vlaku, dále se hlídá přepětí na AC systému. Jsou řešeny pomocí měřících transformátorů, které ale nejsou předmětem této bakalářské práce.

- **Odpojovač sběrače**

Odpojovač je otočná hlavice, která má různé polohy a slouží k odpojení sběrače při nějaké jeho poruše. Ovladač odpojovače je ovládán pákou na stanovišti strojvedoucího.

- **Bleskojistka**

Bleskojistka je ochrana, která chrání lokomotivu před výrazným nárůstem napětí v trakčních obvodech. To se může stát třeba při špatných atmosférických podmínkách jako je například bouřka. Při vniku takového napětí do lokomotivy by se poškodila. Proto je u každého sběrače připojena bleskojistka.

- **I/O moduly**

I/O moduly jsou používány pro zpracování informace daným systémem. Do vstupů jsou přijatá data o stavu daného systému a výstupy jsou odesílány do řídícího počítače, který data dále zpracovává. Termín I/O modul se dá lehce vysvětlit z pohledu počítače – myš a klávesnice je vstup PC a například tiskárna je výstup PC.

- **Řídicí obvody – Systém nadřazeného řízení**

Lokomotiva je vybavena procesorovým distribuovaným řídícím systém. Jádrem řídicího systému je redundantní řídící počítač (VCU - Vehicle Control Unit). Redundance je pro možnost zálohování řídicího počítače. Pro případ poruchy je lokomotiva vybavena dvojicí identických a na sobě nezávislých modulů VCU. Každý modul se skládá ze tří procesorových karet:

LCC (Leading Command Computer) - Řídicí počítač LCC slouží k řízení logiky vozidla a zajištění distribuce dat pro ostatní subsystémy ve správném formátu.

Logika vozidla je řízena primárně na základě vstupů od obsluhy vozidla získaných prostřednictvím I/O modulů. Požadavky obsluhy jsou blokovány nebo povoleny na základě informací o stavu technologické části vozidla (blokády – defenzivní přístup). Na základě těchto informací jsou pomocí algoritmů LCC vytvářeny požadavky na ovládání jednotlivých zařízení. Příslušné požadavky jsou odesílány do jednotlivých zařízení předem dohodnutým způsobem a formátem.

Ochrany systému jsou realizovány na základě informace o nesplnění požadavku nebo po vyhodnocení zakázaného stavu (např. nemůže být současně zapnut spínací i rozpínací kontakt jednoho přístroje). Zásah ochran je realizován zrušením požadavku (vypnutím) nebo vytvořením požadavku na vypnutí příslušného subsystému (vysoké napětí, jízda, atd.).

Zařízení realizuje funkce do úrovně bezpečnosti SIL2.

ATO (Automatic Train Operation) - ATO zajišťuje regulaci jízdy vlaku v širším smyslu. Na základě požadavku z jízdní páky nastavuje požadavek na tažnou a brzdnou sílu trakčního pohonu na úrovni lokomotivy i vlaku (vícečlenné řízení). ATO také disponuje vyššími režimy řízení - regulátorem rychlosti.

V režimu regulátoru rychlosti ATO, nastavuje požadavek na tažnou a brzdnou sílu tak, aby bylo dosaženo požadované rychlosti. Pro snižování rychlosti může použít také pneumatickou brzdu vlaku prostřednictvím vlastního rozhraní. Zpětnou vazbu o rychlosti získává z vlastních čidel rychlosti.

Zařízení realizuje funkce do úrovně bezpečnosti SIL1.

DCC (Diagnostic Computer - zajišťuje následující činnosti:

- Distribuce diagnostického systému LCC do ethernetu;
- Uživatelský diagnostický systém (diagnostický systém nad proměnnými LCC, které lze modifikovat bez zásahu do schvalovaného SW;
- Brána do LCC pro čtení jeho proměnných po ethernetu;
- Distribuce systémového času z DPM na ethernet;
- Brána mezi ethernetem a ladící linkou MCAN.

Zařízení realizuje funkce do úrovně bezpečnosti SIL0.

Předmětem této práce je testování algoritmů řídícího počítače LCC. SW i HW řídícího počítače LCC je certifikován pro řízení bezpečnostně relevantních funkcí pro SIL2 podle EN50128. Řídící počítač komunikuje s periferiemi prostřednictvím komunikace MVB. Periferie počítače mohou být bezpečnostně relevantní (např. I/O moduly, TCU, displej, vlakový zabezpečovač) nebo bez vlivu na bezpečnost (pomocné pohony, …).

Řídící počítač zprostředkovává vazbu mezi strojvedoucím a jednotlivými subsystémy lokomotivy a rovněž mezi jednotlivými subsystémy. Provádí operace logického řízení a ovládání vozidla, poveluje jednotlivá zařízení trakčních a pomocných pohonů a zajišťuje jejich vzájemné blokování, ovládá sběrače, hlavní vypínač, zařízení v pneumatických obvodech a komunikuje se systémy pro zabezpečení jízdy vlaku.

Klíčovými komponenty distribuovaného systému nadřazeného řízení jsou I/O moduly (vzdálené vstupy a výstupů). Tyto moduly tvoří rozhraní mezi jednotlivými přístroji (stykače, přepojovače, hlavní vypínače, relé,…), které s řídicí jednotkou komunikují pomocí komunikační sběrnice.

Součástí řídicího systému je provozní diagnostika (DCC). Ten vyhodnocuje informace o provozních, poruchových a havarijních stavech všech klíčových zařízení a informuje strojvedoucího textovým i mluveným hlášením. Poruchová a diagnostická hlášení jsou tříděna do několika úrovní jednotlivých sledovaných zařízení. Diagnostika nevykonává žádné bezpečnostní funkce, z důvodu vyšší flexibility při údržbě SW a usnadnění zpracování většího množství dat. Pro přenos diagnostických informací po lokomotivě i po vlaku je lokomotiva vybavena sběrnicí Ethernet.

Uživatelské rozhraní řídicího systému je tvořeno plnobarevnými displeji s úhlopříčkou 10.4“ a s ovládáním pomocí dotykové obrazovky.

- **Hlavní vypínač**

Hlavní vypínač je podrobněji vysvětlen a popsán v následující kapitole.

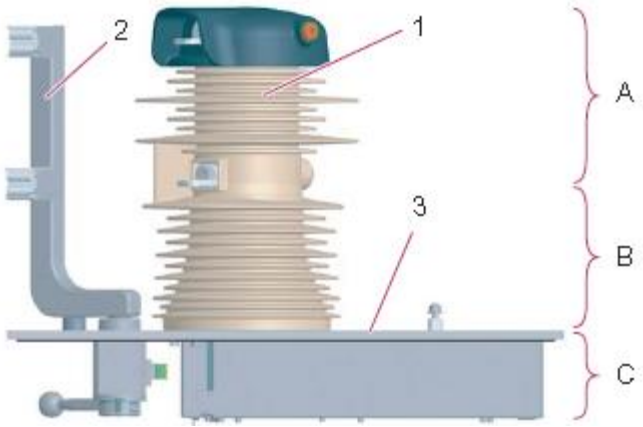
1.3 Hlavní vypínač

Střídavý hlavní vypínač je umístěn na střeše lokomotivy a slouží jako hlavní jistič lokomotivy na střídavém trakčním napájecím systému. Ovládací část vypínače je přístupná z uličky strojovny. Pohon vypínače je elektrický. Vypínač je sepnut přivedením ovládacího napětí na cívku vypínače. Cívka je napájena přes bezpečnostní smyčku, výstup řídicího systému a rozpínací výstupy ochran v měničových skříních.

Hlavním účelem hlavního vypínače je ochránit lokomotivu před vysokými zkratovými proudy co nejrychlejším rozepnutím od napájení. Další funkce je prostá, obyčejné „zapnutí“ a „vypnutí“ lokomotivy. Pokyny k rozepnutí hlavního vypínače jsou dány buďto zásahem ochran nebo povelem od obsluhy lokomotivy ze stanoviště.

1.3.1 Provedení střídavého hlavního vypínače

Hlavní vypínač Sécheron typu MACS je jednopólový rychlovypínač střídavého proudu, určený pro instalaci uvnitř nebo na střeše trakčního vozidla. Vypínač slouží pro připojování a odpojování vozidla od troleje. Uzemňovač zajišťuje bezpečnou funkci trakčního vozidla a bezpečnost personálu při provádění prohlídek údržby a oprav. Uzemňovač se ovládá zevnitř vozidla. Přestavením uzemňovače do polohy uzemněno, jsou uzemněny střešní obvody lokomotivy. Vysokonapěťová část je od nízkonapěťové části oddělena základní deskou.



Obrázek 3 - Hlavní vypínač [2]

Vypínač MACS se skládá ze tří hlavních částí:

- (A) Vysokonapěťový obvod: Hlavní kontakt (1) je umístěn ve vakuové spínací trubici (VST), která zajišťuje vedení proudu a přerušení elektrického oblouku.
- (B) Elektrická izolace: Izolační táhlo spojuje, skrz izolátor, pohyblivý kontakt s ovládacím mechanizmem (2).
- (C) Ovládací mechanismus a nízkonapěťový obvod: Ovládací mechanismus umístěný pod základní deskou (3) vypínače MASC zajišťuje zapínání a vypínaná rychlovypínače a uzemňovače.

1.3.2 Parametry hlavního vypínače

Typ	MACS
Umístění	Střecha lokomotivy
Jmenovité napětí	15 kV AC / 16,7 Hz
Jmenovitý pracovní proud	1000 a při 15 kV AC
Jmenovité ovládací napětí	24 v DC
Pracovní teplota	-40°C – 70°C
Hmotnost včetně uzemňovače a bleskojistky	122 kg ± 5%
Mechanická životnost	200 000 cyklů
Hlučnost	80 dB – 113 dB
Hodnota MTBF	$0,5 \times 10^6$ h

Tabulka 3 - Parametry hlavního vypínače [2]

2. Ovládání hlavního vypínače

Povel k zapnutí hlavního vypínače dává strojvedoucí s nutným souhlasem řídícího systému. Povel k vypnutí hlavního může dát buď strojvedoucí, nebo řídící systém. K vypnutí řídícím systémem dojde, pokud zasáhnou ochrany nebo nejsou splněny podmínky pro zapnutí.

Ovládání hlavního vypínače je řešeno pomocí software. Důvodem použití software je poměrně velká složitost ovládání s velkým množstvím vstupních podmínek a vzájemných vazeb. Pro zvýšení bezpečnosti v závažných případech je hlavní vypínač navíc ještě vypínán paralelní hardwarovou cestou. Tato paralelní hardwarová cesta je tvořena sériovým spojením kontaktů zapojených do obvodu ovládání hlavního vypínače. Vlastnosti této paralelní smyčky nejsou předmětem této práce.

2.1 Ovládání hlavního vypínače strojvedoucím

Strojvedoucí ovládá hlavní vypínač ovladačem S017 umístěným na pultu. Polohy přepínače vysokého napětí jsou následující:

- Zapnout HV (nearetovaná) 
- Výchozí poloha (aretovaná)
- Vypnout HV (nearetovaná) 

Obrázek 4 - Umístění ovladače hlavního vypínače [2]

Polohou **ZAPNOUT HV** je nastaven požadavek k uvedení lokomotivy do provozu. Tento požadavek je řídicím systémem vykonán, pouze pokud jsou splněny všechny zapínací podmínky. Poté je uvedení lokomotivy do provozu zajištěno zcela automaticky.

VÝCHOZÍ POLOHA je neutrální. Tato poloha nevyvolá žádnou akci.

Polohou **VYPNUTÍ HV** je rozepnutý hlavní vypínač, sběrač může být zvednutý.

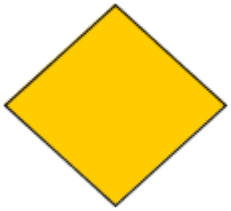
3. Algoritmy pro ovládání hlavního vypínače a ochran

Tato kapitola se zabývá algoritmy pro ovládání hlavního vypínače a ochran. Střídavý hlavní vypínač je monostabilní přístroj, který je ovládán prostřednictvím jednoho výstupu z řídicího systému. Základní poloha hlavního vypínače je poloha „vypnuto“.

Ochrany hlavního vypínače se dělí na vlastní ochrany hlavního vypínače a ochrany vedoucí k vypnutí hlavního vypínače.

Vlivem zásahu ochran hlavního vypínače může být hlavní vypínač kdykoliv vypnut a tím přerušit napájení lokomotivy. Tyto funkce jsou vytvořeny pro bezpečnost vlaku a cestujících.

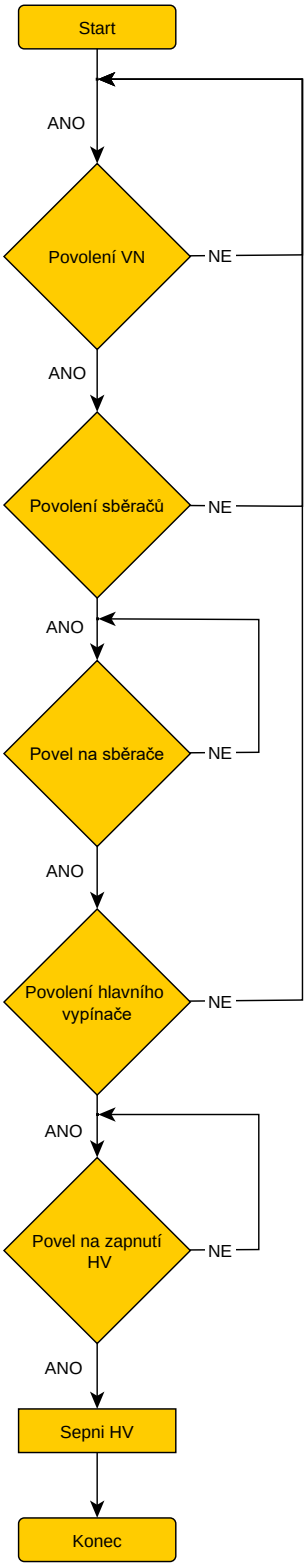
Ovládací a ochranné funkce jsou popsané v dalších kapitolách pomocí vývojových diagramů. Vývojové diagramy nám zobrazují průběh či stavbu programu. Vývojový diagram je vlastně grafické znázornění určitého algoritmu, který nám pomáhá k větší přehlednosti. Skládají se z daných grafických značek, každá značka má svůj význam. Pomocí značek se simulují různé situace a různé příkazy. K této práci jsou použity jen tři základní značky:

Začátek a konec programu	
Běžný příkaz	
Podmíněný příkaz	

Tabulka 4 - Značky vývojového diagramu

3.1 Ovládání hlavního vypínače

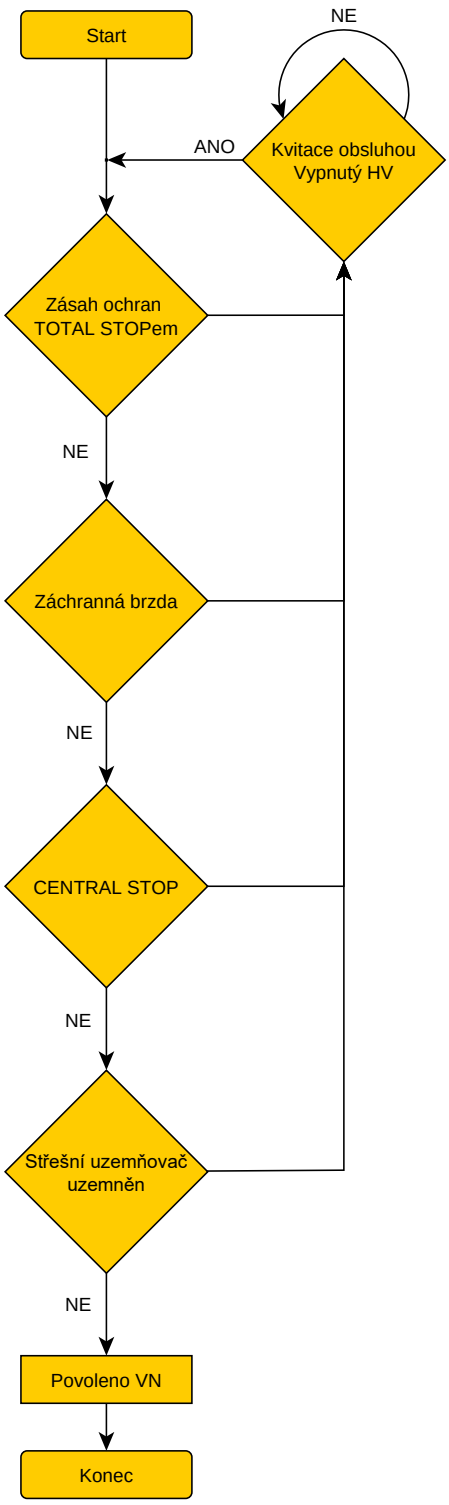
Celkový algoritmus sepnutí hlavního vypínače nám popisuje obrázek 5. Jedná se o základní podmínky, které musí být splněny pro sepnutí hlavního vypínače a připojení lokomotivy k trolejovému napětí.



Obrázek 5 - Vývojový diagram ovládání hlavního vypínače

3.1.1 Povolení vysokého napětí

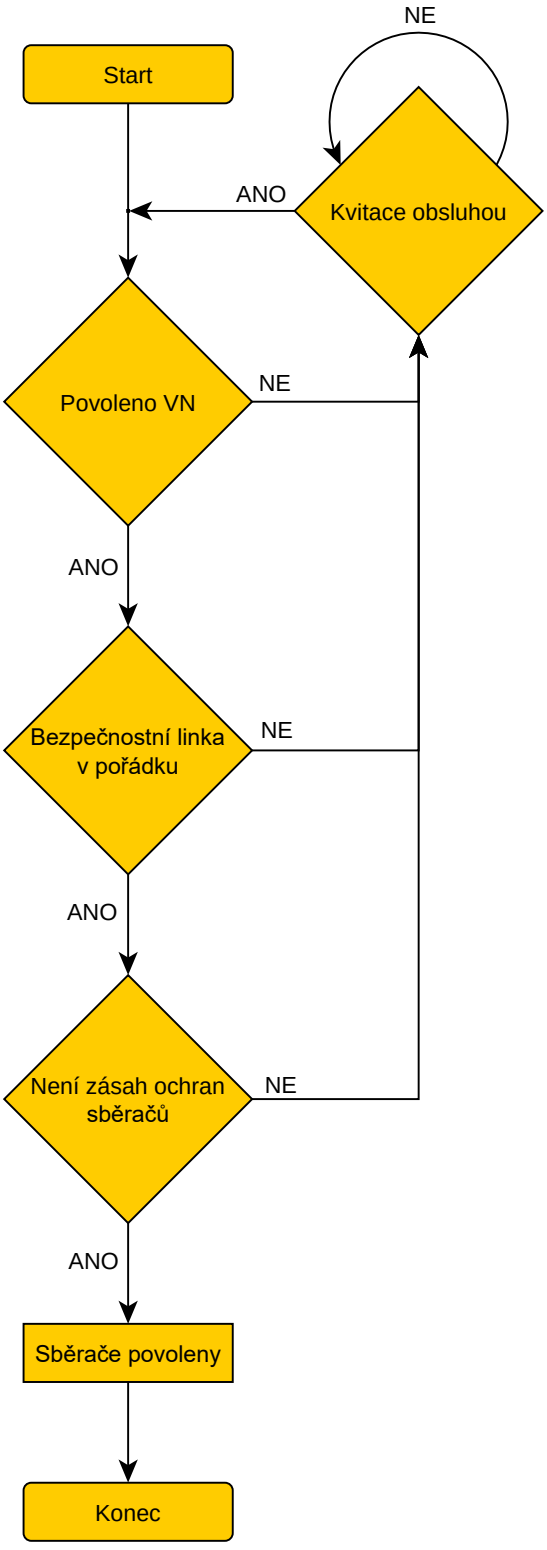
Souhrnná informace o tom, že obvody lokomotivy jsou ve stavu, kdy je možno připojit lokomotivu k vysokému napětí. Povolení vysokého napětí slouží k blokování samočinného opětovného zapnutí do poruchy.



Obrázek 6 - Povolení vysokého napětí

3.1.2 Povolení sběračů

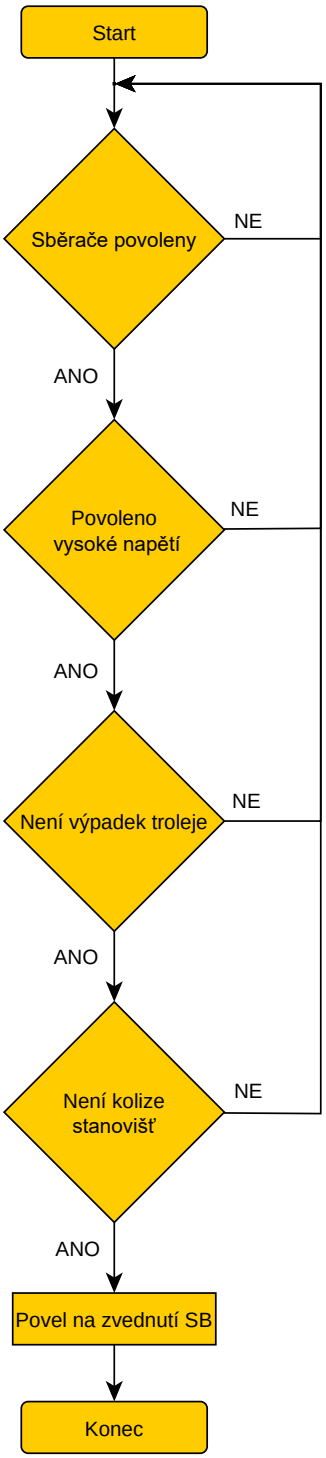
Souhrnná informace o tom, že je povoleno zvednutí sběračů. Povolení sběračů slouží buď ke zvednutí sběračů nebo ke stažení či jejich blokování ve stažené poloze. Po zásahu ochran nebo jejich deaktivaci nesmí dojít k samovolnému zvednutí sběračů.



Obrázek 7 - Povolení sběračů

3.1.3 Požadavek na ovládání sběračů

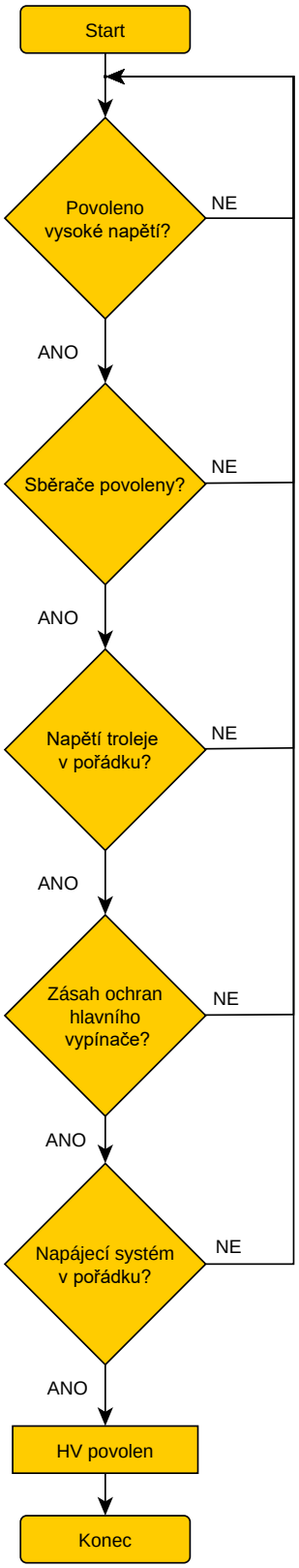
Ovládání obou sběračů je pouze jedním výstupem. Funkce bude pro každý sběrač nezávisle. Výstupem binárního signálu je cívka elektropneumatického ventilu sběrače. Pokud je cívka pod napětím, sběrač je zvednut.



Obrázek 8 - Povel na zvednutí sběračů

3.1.4 Povolení hlavního vypínače

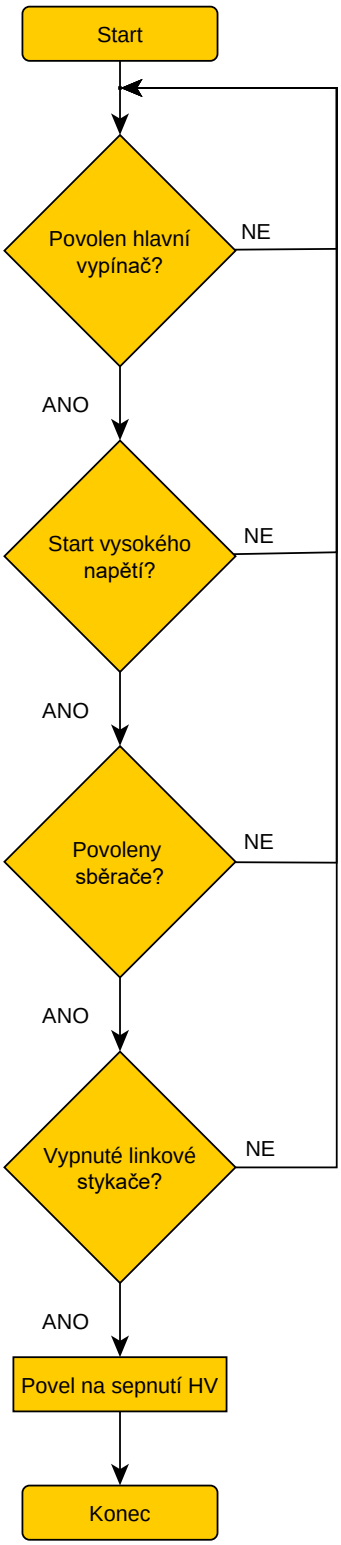
Povolení hlavního vypínače slouží k povolení ovládání hlavního vypínače. Povolení je dáno za těchto podmínek:



Obrázek 9 - Povolení hlavního vypínače

3.1.5 Povel na zapnutí hlavního vypínače

Povel na zapnutí hlavního vypínače může být vykonán, pouze když jsou splněny následující podmínky. Pokud jsou splněny, je zapnut hlavní vypínač.



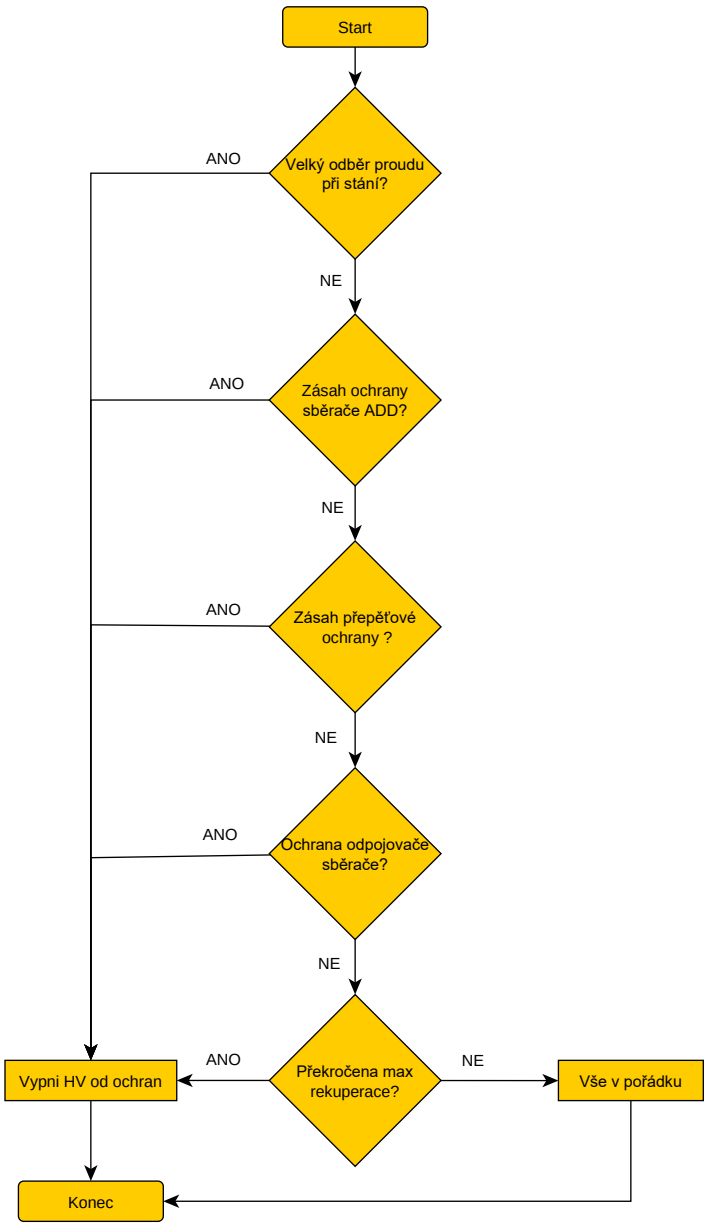
Obrázek 10 - Povel na sepnutí hlavního vypínače

3.2 Ochrany hlavního vypínače

Cílem ochran hlavního vypínače je indikovat poruchu hlavního vypínače, jeho pomocných kontaktů či poruch určitých subsystémů, které vyžadují vypnutí hlavního vypínače. V případě takové poruchy dojde k okamžitému odpojení lokomotivy od trolejového vedení kvůli bezpečnosti cestujících a pro ochranu zařízení lokomotivy.

3.2.1 Ochrany vedoucí k vypnutí hlavního vypínače

Cílem této funkce je definovat souhrnný příznak zásahu ochran vyžadující vypnutí hlavního vypínače. Příznak je aktivován, pokud je splněna jedna nebo více následujících podmínek. Zásahem této ochrany dojde k vypnutí hlavního vypínače a linkových stykačů.



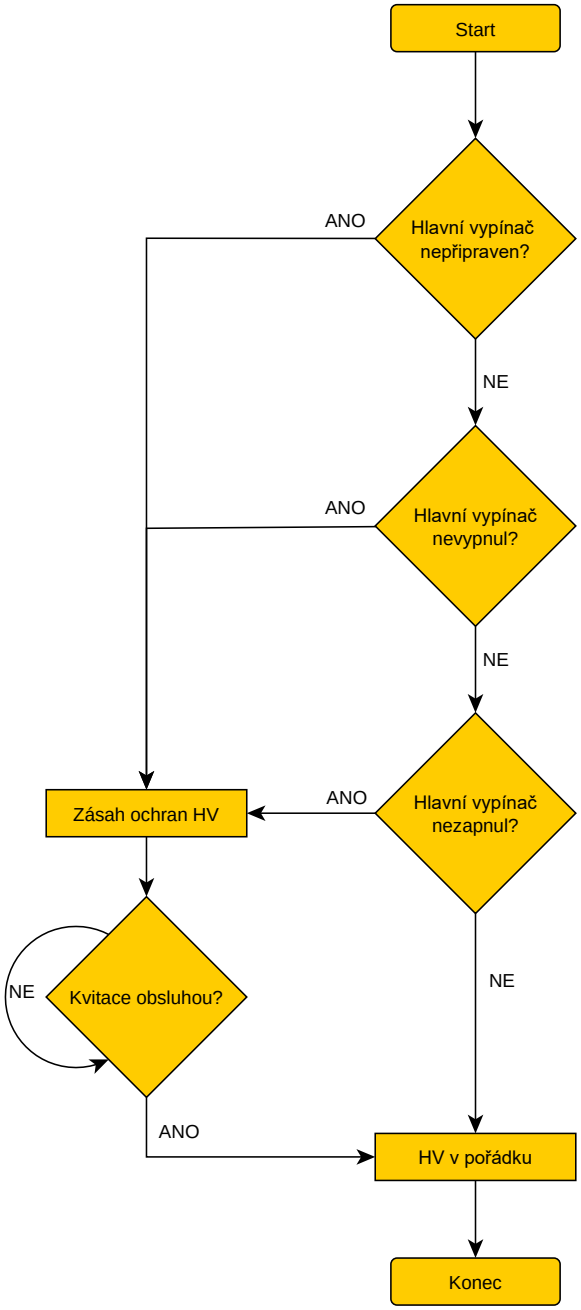
Obrázek 11 - Ochrany vedoucí k vypnutí hlavního vypínače

3.2.2 Vlastní ochrany hlavního vypínače

Vlastní ochrany hlavního vypínače slouží k opatření proti poruše či neodpovídajícímu chování. Při zásahu této ochrany dojde k Total Stopu a vypnutí hlavního vypínače. Pro odmazání ochrany musí být vypnutý hlavní vypínač, systém v pořádku a zadán povel strojvedoucím na kvitaci poruchy.

- **Souhrnná funkce pro vlastní ochrany hlavního vypínače**

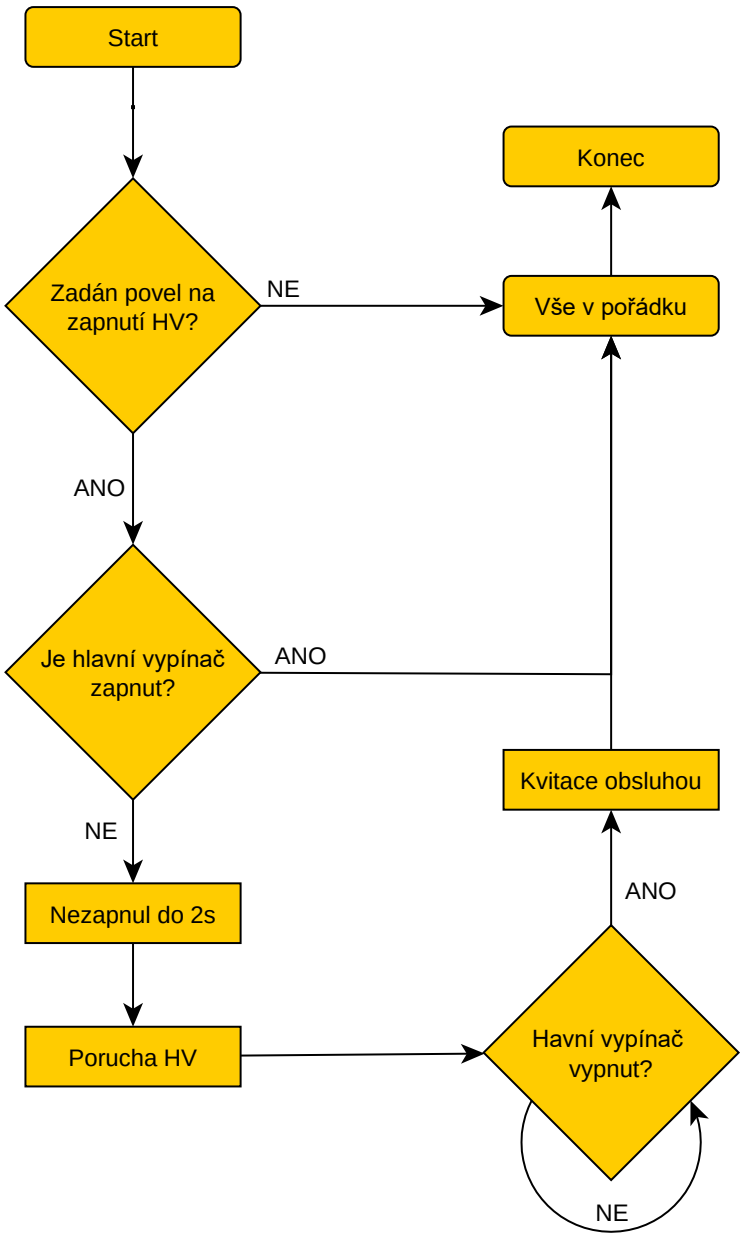
Souhrn všech vlastních ochran hlavního vypínače v jedné funkci, která má na starost při aktivaci nahodit povel pro Total Stop. Tím dojde k úplnému odpojení lokomotivy od vysokého napětí.



Obrázek 12 - Souhrnná funkce pro vlastní ochrany HV

- **Hlavní vypínač nezapnul**

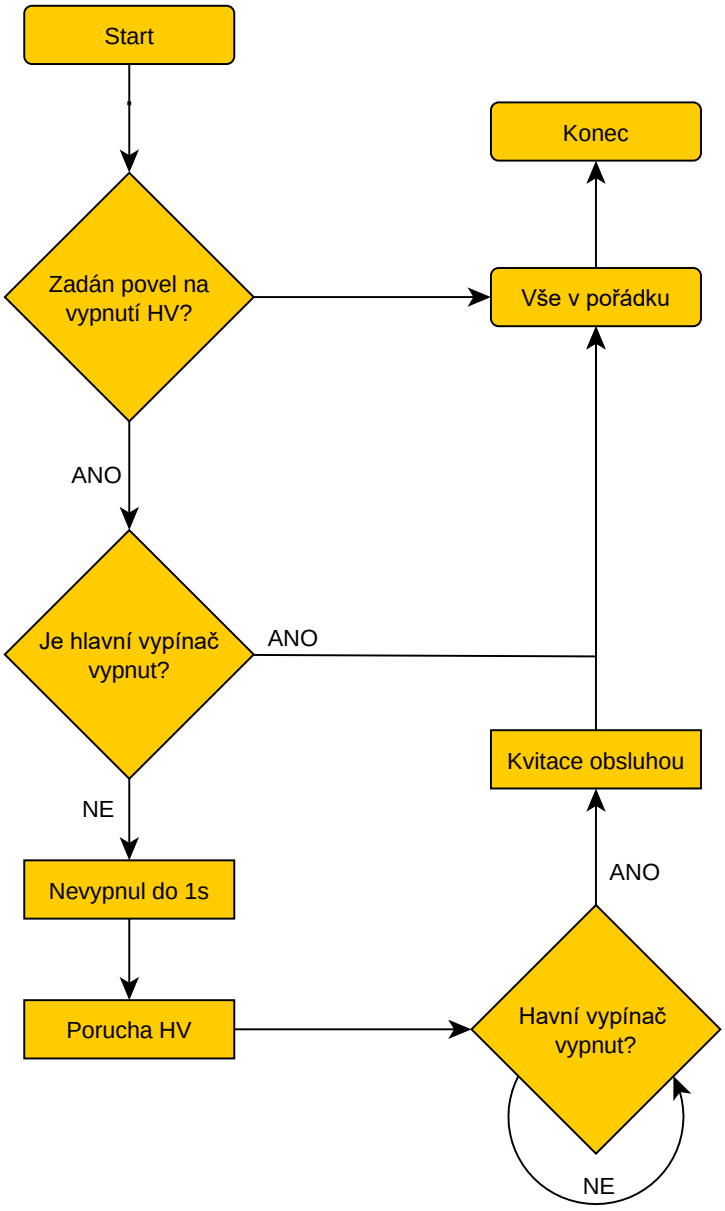
Cílem ochrany je indikovat, že hlavní vypínač při povelu na zapnutí nezapnul do 2s. Zrušení chyby se provádí povelem strojvedoucího a hlavní vypínač musí být v poloze vypnuto.



Obrázek 13 - Hlavní vypínač nezapnul

- **Hlavní vypínač nevypnul**

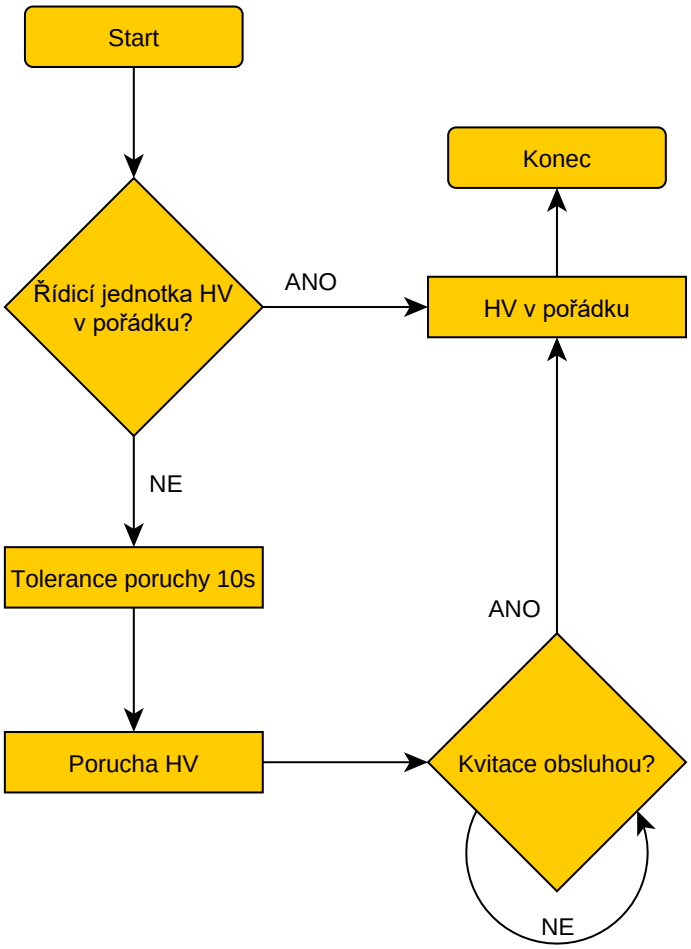
Tato ochrana má za cíl indikovat, že hlavní vypínač po povelu k vypnutí nevypnul v časovém intervalu 1s. V případě poruchy se nahodí Total Stop a odpojí se lokomotiva od trolejového vedení. Zrušení chyby se provede povelem strojvedoucího na kvitaci a vypnutím hlavního vypínače.



Obrázek 14 - Hlavní vypínač nevypnul

- **Hlavní vypínač nepřipravený**

Tato funkce indikuje, že hlavní vypínač po zapnutí nahlásil poruchu řídicího systému střídavého hlavního vypínače. Porucha je hlášena 10s od zapnutí hlavního vypínače. Zrušení chyby se provádí povelem strojvedoucího, pokud je řídicí systém v pořádku.



Obrázek 15 - Hlavní vypínač nepřipraven

- **Další funkce pro indikaci poruch hlavního vypínače**

Ochranných funkcí střídavého hlavního vypínače lokomotivy je velká řada. Pro stručnost a přehlednost práce, některé další funkce nebudou popsány pomocí vývojových diagramů, ale jen slovně.

Další důležitou vlastní ochranou hlavního vypínače je indikovat samovolné vypnutí. Tato porucha hlavního vypínače je z příčin nezávisejících na řídicím systému. V případě samovolného vypnutí je nutno synchronizovat stav řídicího systému se stavem vozidla. Samovolné vypnutí může nastat přerušením bezpečnostní smyčky nebo poruchou kabeláže. Ochrana je zpožděna o 600ms. Zpoždění je nastaveno pro případné dřívější zrušení požadavku na vypnutí hlavního vypínače.

Samovolné vypnutí hlavního vypínače bude vyhlášeno, pokud:

- Je povel pro zapnutí hlavního vypínače,
- detekován přechod vypínače ze stavu zapnuto do stavu vypnuto.

Porucha bude zrušena, pokud:

- Hlavní vypínač je vypnut,
- zásah ochrany byl potvrzen strojvedoucím.

Následující ochrana se zabývá počítáním vypnutí hlavního vypínače pod výkonem. To znamená, že pokud bude zapnutý hlavní vypínač nebo bude povel na zapnutí hlavního vypínače při proudu troleje větším než 1kA, zvýší se počet vypnutí hlavního vypínače pod výkonem o 1.

Poslední popisovanou funkcí je zpoždění zapnutí hlavního vypínače. Splnění téhle funkce je nutné k opětovnému zapnutí hlavního vypínače. Z důvodu technologie (a poruchovosti) pohonu vypínače je opětovné zapnutí povoleno:

- 3s po vypnutí hlavního vypínače a zrušení požadavku na jeho sepnutí,
- zapnutí je zpožděno o 1,5s od vzniku povolení hlavního vypínače z důvodu nevhodného omezení souběhu podmínek ochrany povolení hlavního vypínače,
- hlavní vypínač je možné sepnout 5s poté, co hlásí nabitý kondenzátor (slouží k rychlému vypnutí hlavního vypínače).

4. Bezpečnost SW

Současný stav techniky je takový, že ani používání metod zajištění jakosti (tak zvaná opatření pro vyhnutí se vadám), ani používání přístupů odolných proti vadám softwaru nemůže zaručit absolutní bezpečnost systému. Neexistuje žádný známý způsob prokázání absence vad v přiměřeně složitém softwaru vztahujícím se k bezpečnosti, zejména absence poruch specifikace a návrhu.

Principy použité ve vyvíjení softwaru s vysokou integritou zahrnují níže uvedené položky s tím, že, nejsou omezeny jen na ně:

- metody návrhu shora dolů;
- modularitu;
- ověřování každé etapy životního cyklu vývoje;
- ověřené moduly a knihovny modulů;
- jasnou dokumentaci;
- prověřitelné dokumenty;
- validační testování.

V zásadě lze bezpečnost SW shrnout do konstatování, že čím vyšší má být bezpečnost SW, tím více musí být provedeno testů a kontrol. Více testů vyžaduje podrobnější a důkladnější dokumentaci, která vyžaduje důkladnější kontroly integrity.

4.1 Úrovně integrity bezpečnosti softwaru - SIL

Integrita bezpečnosti je specifikována jako jedna ze čtyř diskrétních úrovní. Úroveň 4 má nejvyšší úroveň integrity bezpečnosti; úroveň 1 nejnižší. Úroveň 0 se používá pro informaci, že neexistují žádné požadavky na bezpečnost. SIL má být zaměřena na kvalitativní posouzení takových faktorů, jako je řízení jakosti a bezpečnosti a podmínky technické bezpečnosti.

Úroveň integrity bezpečnosti je definována tolerovaná frekvence nebezpečných poruch [1].

Tolerovatelná intenzita nebezpečí na hodinu a na funkci THR	Úroveň integrity bezpečnosti SIL
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Tabulka 5 - SIL podle tolerovatelné intenzity nebezpečí [1]

Úroveň SIL je pro jednotlivé funkce systému přiřazena v rámci analýzy rizik, kde je riziko spojené s určitým nebezpečím. Bez dalších opatření musí být úrovně SIL realizovaná pomocí software minimálně stejná jako integrity bezpečnosti systému. Existuje-li mechanismus zabraňující, aby porucha SW modulu způsobila, že systém přejde do nebezpečného stavu, může být SIL SW modulu snížena.

Rizika, která se musí brát v potaz, jsou rizika s následujícími důsledky nebezpečí:

- Ztráta lidského života;
- Zranění nebo onemocnění osob;
- Znečištění životního prostředí;
- Ztráta nebo poškození majetku.

Pro evropskou normu ČSN EN 50128 musí být integrita bezpečnosti softwaru specifikována jednou z pěti úrovní:

Úroveň integrity bezpečnosti softwaru	Popis úrovně SIL
4	Velmi vysoká
3	Vysoká
2	Střední
1	Nízká
0	Nevztahuje se k nebezpečí

Tabulka 6 - Popis úrovní SIL [1]

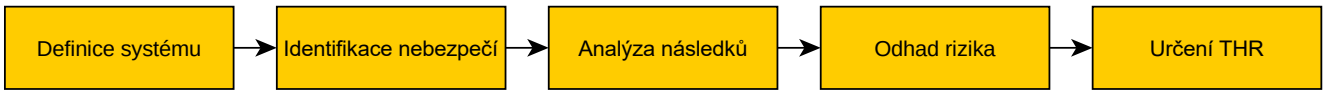
Úrovně integrity bezpečnosti softwaru musí být specifikovány ve specifikaci požadavků na software.

4.2 Analýza rizika

Ve stručnosti je v téhle kapitole popsána analýza rizika, která je důležitá pro vývoj software. Analýza rizika je proces, který udává tolerovatelné intenzity nebezpečí.

Skládá se z určitých částí:

- Definice systému – Povinnost drážní organizace definovat systém (nezávisle na technické realizaci);
- Identifikace nebezpečí – Proces, který určuje nebezpečí, ke kterému může dojít během životního cyklu;
- Analýza následků – Musí jednoznačně určit výsledné riziko;
- Odhad rizika – Kritéria odhadu rizika jsou definovány národními či evropskými požadavky;
- Přiřazení THR – Přiřazení tolerovatelných intenzit nebezpečí;

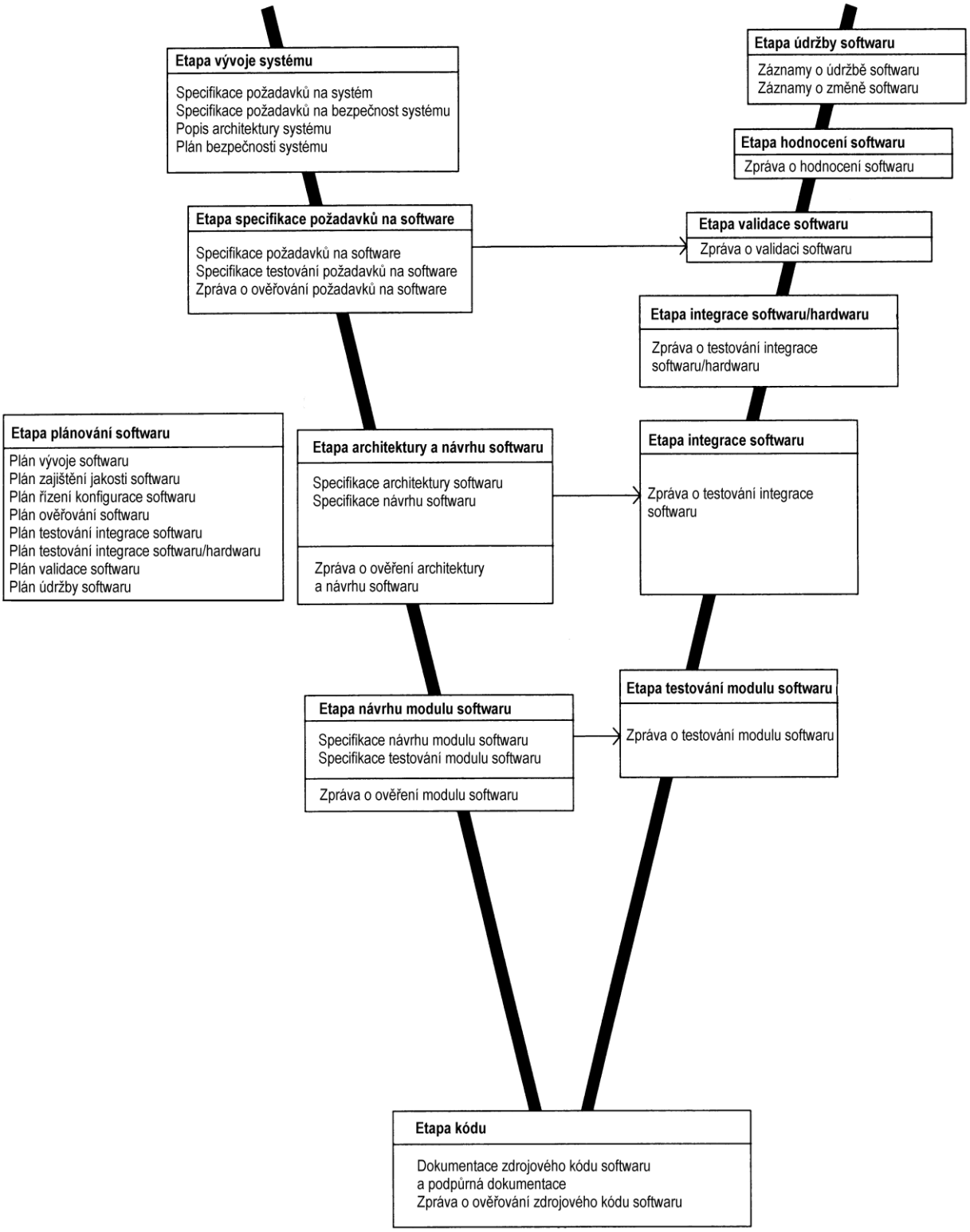


Obrázek 16 - Proces analýzy rizika

4.3 Životní cyklus software

4.3.1 V – diagram

V – diagram je systém aplikovaný na celé řadě různých modelů. Koncepční model je určený k zjednodušenému chápání složitosti výroby spojené s rozvojem systémů. Grafické znázornění vývoje systémů životního cyklu, ten shrnuje hlavní kroky, které je třeba učinit v souvislosti s odpovídajícími výstupy v rámci počítačové systémové validace. V – diagram představuje sled kroků v rozvoji projektového životního cyklu, to popisuje činnosti, které mají být provedeny a výsledky, které mají být předloženy v průběhu vývoje. Levá strana „V“ znamená rozklad požadavků a vytváření specifikace systému. Pravá strana „V“ zastupuje integraci dílů a jejich validaci. Tato práce je zaměřená na pravou stranu V – modelu.



Obrázek 17 - V – diagram [1]

5. Testování software

Funkční testování softwaru bude prováděno na cílovém hardwaru s možností využití diagnostických nástrojů SW. Testy, které se neprovádí na cílovém hardwaru, nelze považovat za součást ověřování. Jakýkoliv testovací záznam musí obsahovat podrobný popis SW a HW nástrojů, používaných k testování. Specifické zkušební metody jsou závislé na konkrétním HW a SW a mohou se lišit pro různé typy zařízení.

Veškerá simulace a testování probíhá v reálném čase a v laboratorních podmínkách. Díky tomu můžeme vlastně testovat, jak se bude hlavní vypínač chovat ve skutečné lokomotivě za běžného provozu. Laboratorní podmínky umožňují testovat i za extrémních stavů, kterých lze v lokomotivě dosáhnout jen za komplikovaných podmínek, nebo vůbec.

5.1 Testování softwarových modulů

Testování SW modulů si lze představit a interpretovat na klasickém, jednoduchém zapojení obvodu s relé a žárovkou. Pokud se testuje softwarový modul, tester se zaměřuje na samotné relé, jeho vnitřní stavy a chování. Při téhle fázi testování se nestaráme o to, jestli se při sepnutí rozsvítí žárovka či ne.

5.2 Testování integrace SW modulů

Integrace softwarových modulů se dá popsat jako spojování různých softwarových komponent či subsystému v jeden fungující celek. Hlavním úkolem je, aby celek pracoval co možná nejefektivněji. Při této fázi testování se soustředíme na společnou funkčnost a komunikaci všech subsystémů v jednom daném celku. Sepnu relé – svítí žárovka.

5.3 Validace SW

Hlavním cílem validace software je zanalyzovat a otestovat integrovaný systém, aby validátor zajistil shodu se specifikací daného požadavku na SW s daným důrazem na funkčnost a bezpečnost podle úrovně SIL. Pokud integrovaný systém nevyhoví daným požadavkům, je nutné se vrátit na začátek a opravit chybu daného integrovaného systém.

5.4 Způsoby provedení testu

5.4.1 Manuální testování

Manuální vstup ze vstupních signálů a vizuální kontroly hodnot výstupního signálu může být použita v omezené míře, kdy je třeba ověřit specifický detail testovaného softwaru. Předpokladem je podrobná dokumentace provedených testů tak, aby byla zajištěna jeho opakovatelnost. Výsledky manuálního testování musí být zahrnuta do testovacího protokolu a zaznamenáno ve zkušebním SW.

5.4.2 Automatizované testování

Vstup programově řízené simulace ze vstupních signálů a automaticky snímání a vyhodnocení výstupních signálů je preferovaný způsob pro testování softwaru. Opět platí, že podmínkou používání je zajistit opakovatelnost testů. V tomto případě je nutné archivovat testovací skripty, podpůrným softwarem a popisy pro jejich použití. Výstupem automatizovaného testování jsou testovací protokoly, ze kterých lze jednoznačně ověřit, zda software provádí požadovanou funkci. Výsledky pak musí být zaznamenány ve zprávě o testování SW.

5.5 Testovací prostředí UTS1

Tester UTS1 může číst a zapisovat data v rozhraní Ethernet, MVB, CAN, RS232 a "simulaci proměnných" v jednotkách D8206P1, MBF modulech a počítače AMIT.
Při použití testeru UTS1, specifikaci testů (např. softwarový modul) je vytvořený testovací skript. Testovací skript je poskytován s komentářem popisující test na úrovni záměrů. Součástí skriptu je kritérium vyhodnocení výsledků. V průběhu zkoušky je generován protokol. Protokol je strukturovaný textový soubor vhodný pro čtení lidskou bytostí, ale také vhodný pro strojové zpracování. Z tohoto protokolu lze automaticky vytvořit "papírovou" zprávu ve formátu PDF.

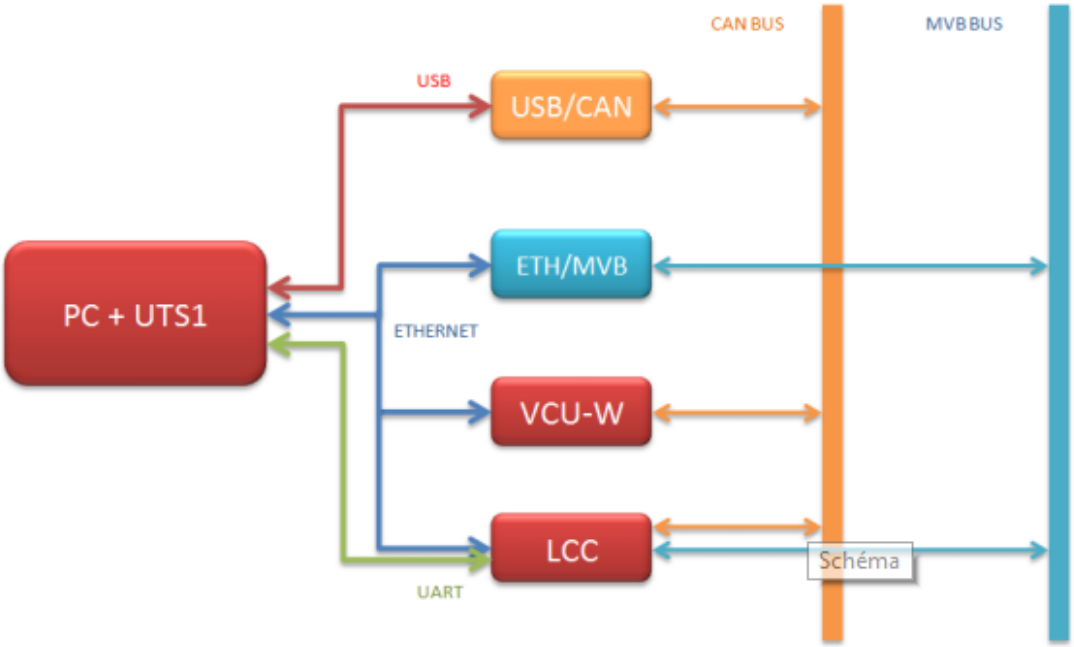
Při testování softwarových modulů jsou typicky simulované vstupy do jednotlivých softwarových modulů a UTS tester ověřuje změnu hodnoty výstupní proměnné. v případě zobrazení na obrazovce, testování, se zpětná vazba provádí pomocí testeru (člověka).

Během testování integrace SW jsou simulované výstupní proměnné na sběrnici a UTS1 ověřuje očekávané hodnoty. Vstupní signál UTS1 tester nejprve přečte a očekává změnu signálu na zkoušené sběrnici. Pak se ověří, zda došlo k očekávané změně vstupní proměnné na testovaném SW.

Během validace, UTS1 bude použito pro záznam očekávané chování systému v případech, kde je to vhodné. Simulace hodnot se provádí pouze ve výjimečných případech, kdy by testování skutečných hodnot mohlo být nebezpečné pro personál (pohyb, vysoké napětí, atd.), nebo kde vozidlo může být vážně poškozeno (např. výbuch ventilu transformátoru).

5.5.1 Komunikace UTS1

Tester UTS1 umí číst a zapisovat data na rozhraní ETH, MVB, CAN, RS232 a „simulaci proměnných“ v jednotkách D8206P1, modulech MBF a počítačů Amit.



Obrázek 18 - Komunikace UTS1

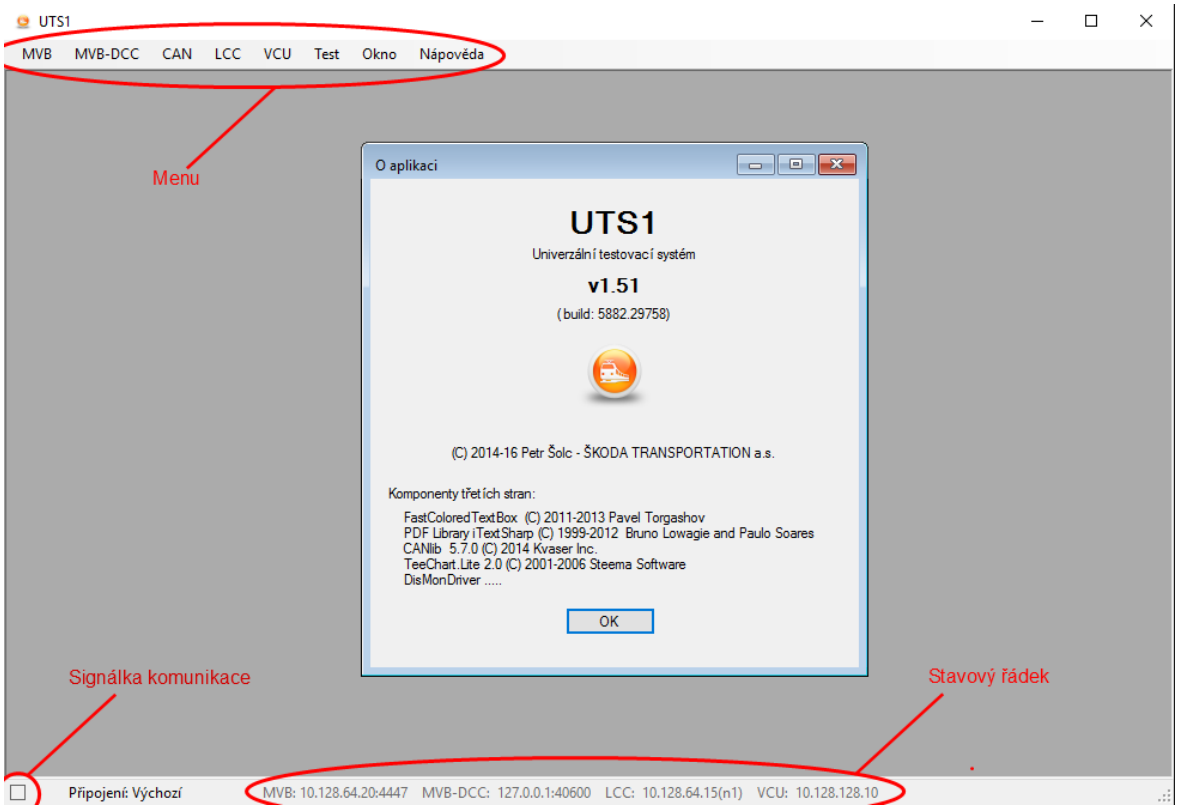
5.5.2 Hlavní okno aplikace UTS1

Hlavní okno obsahuje menu, pracovní plochu aplikace a stavový řádek. V menu je možno otevřít okno pro práci s konkrétními objekty, či okno pro tvorbu a spouštění testovacích skriptů.

Na pracovní ploše může být otevřeno libovolné množství oken. Každé pracuje nezávisle na sobě.

Stavový řádek má hlavní pracovní plocha, ale i každé otevřené okno zvlášť. Obsahuje signálku komunikace. Svítí-li modře, komunikace je aktivní, pokud červeně, je výpadek komunikace.

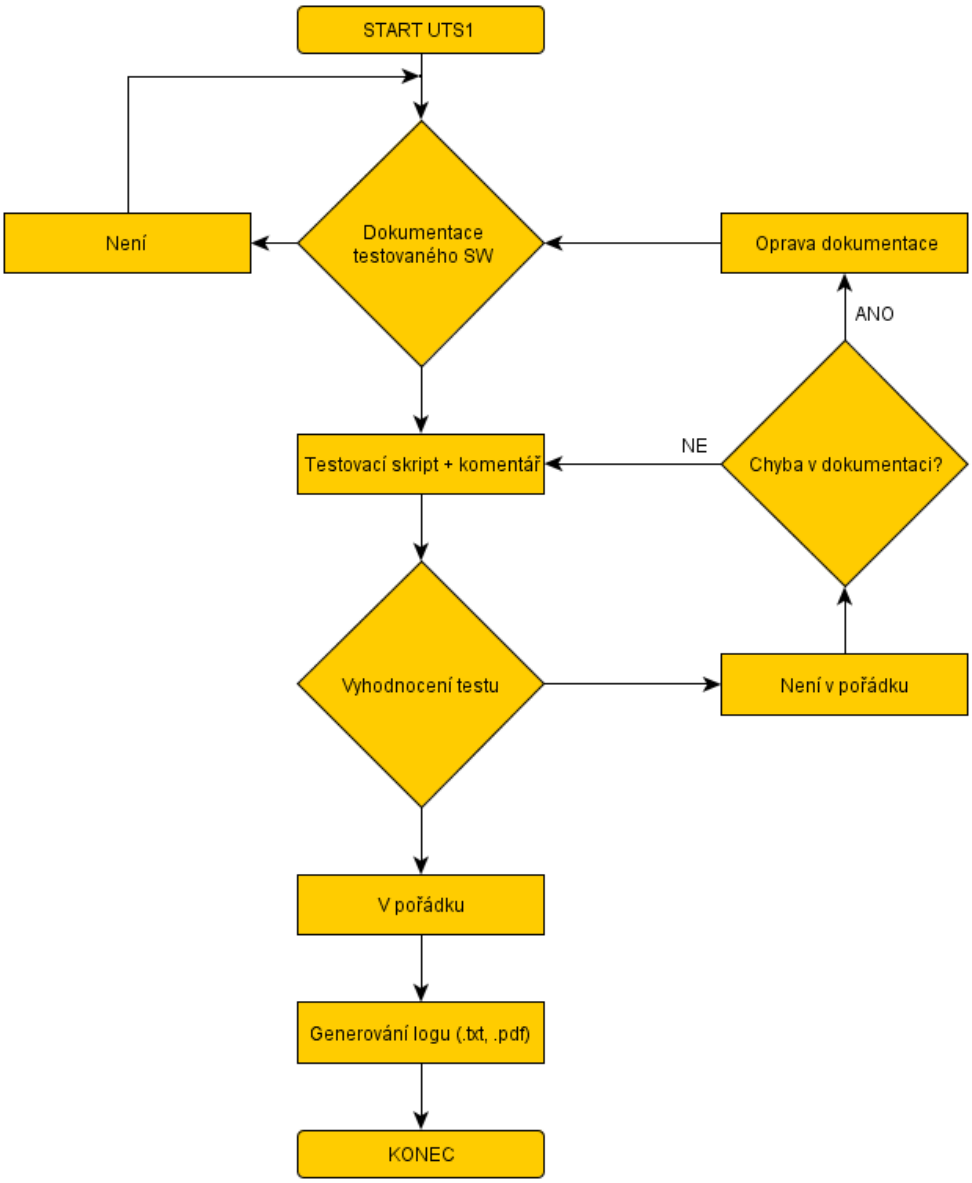
Další jsou parametry komunikace. Zobrazují aktuální nastavení IP adres a portů.



Obrázek 19 - Popis prostředí UTS1

5.5.3 Cyklus vývoje testování SW modulů

Při použití testeru UTS1, například při specifikaci zkoušek softwarového modulu je tvořen testovací skript. Testovací skript musí být opatřen komentářem popisující test na úrovni záměrů. Součástí skriptu je hodnocení výsledků. V průběhu testu je generován protokol – zkušební zpráva softwarového modulu. Protokol je strukturovaný textový soubor vhodný pro čtení lidmi, ale také vhodný pro strojové zpracování. Z tohoto protokolu lze automaticky vytvořit zprávu ve formátu PDF. Při testování SW modulů je obvyklým postupem simulovat vstupy do jednotlivých modulů a UTS1 tester ověřuje změnu hodnoty výstupní veličiny.



Obrázek 20 - Proces testování

5.5.4 Testovací skripty a jeho výstupy

Testovací model – Základní dokument pro testování software. Dokument, ve kterém je popsán daný požadavek pro testování konkrétního modulu při konkrétní situaci. V tomto dokumentu jsou popsané výchozí podmínky, které musí být při testu splněny.

Testovací skript - Vychází z určitého testovacího modelu. Může být kombinací několika testovacích modelů, které spolu musí tvořit určitý logický celek. Testovací skript obsahuje souhrn všech vstupních požadavků. Jsou to vlastně zadaná vstupní data. Dále uvádí jednotlivé testovací kroky, které jsou při testování vykonány. U každého

testovacího kroku je uveden výsledek. Tester, který daný model testuje, postupuje podle jednotlivých kroků a u jednotlivých kroků vyhodnocuje, jestli test proběhl dle požadavků. Testovací modul je úspěšně otestován, jen v tom případě, že testovací skript proběhl v pořádku a výstupy odpovídají danému požadavku.

Test - Vzor.uts

```
1  // Hlavička skriptu //
2
3  //  Porucha link. nebo nab. stykačů v M2 - SK_L8070_M2      // Název požadavku a číslo
4
5  // @src_file procs\090_Ochrany\Ochrany_Link_Stykacu.c       // Cesta ke zdrojovému kódu
6  // @requirement  SK_L8070_M2                               // Číslo požadavku
7  // @author       Václav Průcha                             // Jméno autora
8  // Created       1.10. 2015                                // Datum vytvoření
9
10 name " Porucha link. nebo nab. stykačů - SK_L8070_M2 "      // Název skriptu
11
12 use lcc                  // Používá se pro sdělení, které proměnné bude skript užívat
13     lcc.proměnná         // Deklarace proměnných z LCC
14 use end                  // Ukončení sdělení
15
16 declare variable         // Deklarace interních proměnných, či konstant
17     proměnná = hodnota   // Deklarovaná proměnná na určitou hodnotu
18 declare end              // Konec sekce deklarace
19
20 // Tělo skriptu //       // V těle skriptu se píše samotný testovací skript, pomocí
21                          // příkazů a daných proměnných konkrétního SW modulu se testují
22                          // pro zjištění jejich správné funkčnosti
23
24 setkeys 1                // U všech definovaných LCC proměnných *__val nastaví __key
25                          // na hodnotu "1"
26
27
28 // Výčet nejpoužívanějších příkazů
29
30 // Označení konkétního testu
31 TEST " Název testu "
32 // Kontrola, zda hodnota proměnné odpovídá konkrétní hodnotě
33 CHECK  Proměnná Hodnota
34 // Stejné jako check + čeká definovaný čas na splnění podmínky
35 WAITFOR Proměnná Hodnota Čas
36 // Označení řádku, kam budou směřovat podmíněné i nepodmíněné skoky
37 LABEL Návěští
38 // Volání podprogramu
39 CALL Návěští
40 // Návrat z podprogramu
41 RETURN
42 // Podmíněný skok, podmínka uvedena v příkazu
43 IFGOTO Proměnná Hodnota Návěští
44
45
46
47 setkeys 0                // U všech definovaných LCC proměnných *__val nastaví __key
48                          // na hodnotu "0"
```

Obrázek 21 - Vzorový testovací skript

Výstupní protokol - Je součástí přílohy.

Závěr

Z důvodu složitosti SW řídicího počítače kolejového vozidla nebylo možné popsat testování všech modulů, které jsou spjaty s lokomotivou NIM Express 109E. Na základě toho, byl po konzultaci s vedoucím zvolen jeden modul, a to střídavý hlavní vypínač. Ale přesto, na základě níže popsaných bodů lze konstatovat, že byly splněny všechny body zadání.

V první části byly shrnuty technické parametry kolejového vozidla, které úzce souvisí s problematikou testování střídavého hlavního vypínače. Byl popsán význam a funkcionalita jednotlivých technických parametrů a součástí vysokonapěťové výzbroje.

V druhé části práce je obecně popsáno ovládání hlavního vypínače a umístění ovladače hlavního vypínače na stanovišti strojvedoucího.

Ve třetí části jsou popsány algoritmy softwarového ovládání střídavého hlavního vypínače a jeho ochrany. Tato kapitola popisuje provozní a poruchové stavy střídavého hlavního vypínače. Bezpečnostní funkce vypínače, pro zajištění bezpečného stavu a ochrany zařízení před poškozením.

Ve čtvrté části je definována bezpečnost, kterou musí software splňovat pro určité funkce dle české technické normy ČSN EN 50128. Popsán je i stručný proces vývoje celého software pro drážní řídicí a ochranné systémy.

Pátá část definuje metody testování, testovací scénáře a popis testovacího prostředí. Na tuto část navazují přílohy, kde je konkrétně zobrazen testovací skript, log report testovacího skriptu a papírový protokol o dosažených výsledcích daného testu.

Seznam literatury a informačních zdrojů

[1] ČSN EN 50128

[2] DOKUMENTACE SWMDS

Přílohy

Příloha A – Ukázkový test Ochrany hlavního vypínače

```
// OCHRANA HLAVNÍHO VYPÍNAČE Q02
// Cílem ochrany je indikovat souhrn poruch střídavého hlavního vypínače.
// Indikátor je nastaven:
//   a) Chyba řídicí jednotky HV
//   b) Nevypnul hlavní vypínač
//   c) Nezapnul hlavni vypínač
// na základě tohoto indikátoru poruchy, bude lokomotiva vypnuta TOTAL
stopem tj. odpojena stažením sběračů a vypnutím HV.

// Ochrana hlavního vypínače Q02 - TD013644_LH_3804

// @src_file procs\090_Ochrany\Ochrany_HV.c
// @requirement  TD013162_SK_0002
// @author       Václav Průcha
// Created       24.6. 2015

name " Ochrana hlavního vypínače Q02 - TD013644_LH_3804 "

use lcc
B_HV_SYS_E__val          // Hlavní vypínač nepřipraven
B_HV_VYP_E__val          // Hlavní vypínač nevypnul
B_HV_ZAP_E__val          // Hlavní vypínač nezapnul
BI_Q02_SYS_OK__val       // Řídicí systém v pořádku
B_HV_STOP_Q__val         // Kvitace obsluhou
B_HV_EN__val             // Povolení hlavního vypínače
DI_Q02_HVAC__val         // Stav ovladače hlavního vypínače
B_Q02_OCH                // Ochrana hlavního vypínače
use end

declare variable
DK_Q0x_HVAC_V = 0x01     // HV vypnut
DK_Q0x_HVAC_Z = 0x02     // HV zapnut
declare end

setkeys 1

call Kvitace                        // Volání funkce

test " Bezporuchový stav - Není zásah ochran hlavního vypínače
"B_HV_SYS_E__val = 0              // Hlavní vypínač nepřipraven
B_HV_VYP_E__val = 0              // Hlavní vypínač nevypnul
B_HV_ZAP_E__val = 0              // Hlavní vypínač nezapnul
BI_Q02_SYS_OK__val = 1           // Řídicí systém v pořádku
B_HV_STOP_Q__val = 0             // Kvitace obsluhou
B_HV_EN__val = 1                  // Povolení hlavního vypínače
DI_Q02_HVAC__val = DK_Q0x_HVAC_Z // Stav ovladače hlavního vypínače
check B_Q02_OCH 0                // Ochrana hlavního vypínače

test " Zásah ochran HV - Hlavní vypínač nepřipraven "
B_HV_SYS_E__val = 1              // Hlavní vypínač nepřipraven
check B_Q02_OCH 1                // Zásah ochran hlavního vypínače

test " Deaktivace ochran HV - Hlavní vypínač v pořádku "
B_HV_SYS_E__val = 0              // Hlavní vypínač v pořádku
check B_Q02_OCH 1                // Zásah ochran hlavního vypínače

call Kvitace                     // Volání funkce
```

```
call ZruseniKvitace              // Volání funkce

test " Zásah ochran HV - Hlavní vypínač nevypnul "
B_HV_VYP_E__val = 1              // Hlavní vypínač nevypnul
check B_Q02_OCH 1                // Zásah ochran hlavního vypínače

test " Deaktivace ochran HV - Hlavní vypínač v pořádku "
B_HV_VYP_E__val = 0              // Hlavní vypínač v pořádku
check B_Q02_OCH 1                // Zásah ochran hlavního vypínače

call Kvitace                     // Volání funkce

call ZruseniKvitace              // Volání funkce

test " Zásah ochran HV - Hlavní vypínač nezapnul "
B_HV_ZAP_E__val = 1              // Hlavní vypínač nezapnul
check B_Q02_OCH 1                // Zásah ochran hlavního vypínače

test " Deaktivace ochran HV - Hlavní vypínač v pořádku "
B_HV_ZAP_E__val = 0              // Hlavní vypínač v pořádku
check B_Q02_OCH 1                // Zásah ochran hlavního vypínače

call Kvitace                     // Volání funkce

call ZruseniKvitace              // Volání funkce

label Kvitace                    // Návěstí funkce

test " Kvitace poruchy obsluhou "
B_HV_STOP_Q__val = 1             // Kvitace obsluhou
B_HV_EN__val = 0                 // Blokován hlavní
vypínačDI_Q02_HVAC__val = DK_Q0x_HVAC_V    // HV vypnut
check B_Q02_OCH 0               // Není zásah ochran hlavního vypínače
return

label ZruseniKvitace             // Návěstí funkce

test " Zrušení kvitace "
B_HV_STOP_Q__val = 0             // Zrušena kvitace
B_HV_EN__val = 1                 // Povolen hlavní vypínač
DI_Q02_HVAC__val = DK_Q0x_HVAC_Z    // HV zapnut
check B_Q02_OCH 0               // Není zásah ochran hlavního vypínače
return

setkeys 0
```

Příloha B – Textový report vygenerovaný pro test ochran hlavního vypínače

```
10:35:13.317  Datum      : 31.3.2016
10:35:13.317  Soubor testu: C:\Users\Administrator\Desktop\Testy pro HV\TD013644_LH_3804.uts
10:35:13.317  @requirement TD013162_SK_0002
10:35:13.317  @author   Václav Průcha
10:35:13.317
10:35:13.692  NAME      Ochrana hlavního vypínače Q02 – TD013644_LH_3804
10:35:13.693  use      lcc
10:35:13.694          B_HV_SYS_E__val
10:35:13.695          B_HV_VYP_E__val
10:35:13.696          B_HV_ZAP_E__val
10:35:13.697          BI_Q02_SYS_OK__val
10:35:13.698          B_HV_STOP_Q__val
10:35:13.699          B_HV_EN__val
10:35:13.700          DI_Q02_HVAC__val
10:35:13.701          B_Q02_OCH
10:35:13.702  use      end
10:35:13.703  declare   variable
10:35:13.704  DK_Q0x_HVAC_V = 0x01      [1]
10:35:13.705  DK_Q0x_HVAC_Z = 0x02      [2]
10:35:13.706  declare   end
10:35:13.707  SET LCC __key VARIABLES TO 1
10:35:13.727          B_HV_SYS_E__key =  1
10:35:13.754          B_HV_VYP_E__key =  1
10:35:13.768          B_HV_ZAP_E__key =  1
10:35:13.798          BI_Q02_SYS_OK__key =  1
10:35:13.893          B_HV_STOP_Q__key =  1
10:35:13.907          B_HV_EN__key =  1
10:35:13.922          DI_Q02_HVAC__key =  1
10:35:13.923  CALL     Kvitace
10:35:13.924  label    Kvitace
10:35:13.925  ------------------------------------------------------------------
10:35:13.925  TEST  1  Kvitace poruchy obsluhou
10:35:13.925  ------------------------------------------------------------------
10:35:13.948  B_HV_STOP_Q__val = 1      [1]
10:35:13.965  B_HV_EN__val = 0      [0]
10:35:13.984  DI_Q02_HVAC__val = DK_Q0x_HVAC_V  (1) [1]
10:35:14.035  DELAY    50ms
10:35:14.049  CHECK    B_Q02_OCH  (0)        0       OK
10:35:14.050  RETURN
10:35:14.051  ------------------------------------------------------------------
10:35:14.051  TEST  2  Bezporuchový stav - Není zásah ochran hlavního vypínače
10:35:14.051  ------------------------------------------------------------------
10:35:14.070  B_HV_SYS_E__val = 0      [0]
10:35:14.098  B_HV_VYP_E__val = 0      [0]
10:35:14.115  B_HV_ZAP_E__val = 0      [0]
10:35:14.302  BI_Q02_SYS_OK__val = 1      [1]
10:35:14.326  B_HV_STOP_Q__val = 0      [0]
10:35:14.348  B_HV_EN__val = 1      [1]
10:35:14.363  DI_Q02_HVAC__val = DK_Q0x_HVAC_Z  (2) [2]
10:35:14.414  DELAY    50ms
10:35:14.428  CHECK    B_Q02_OCH  (0)        0       OK
10:35:14.429  ------------------------------------------------------------------
10:35:14.429  TEST  3  Zásah ochran HV - Hlavní vypínač nepřipraven
10:35:14.429  ------------------------------------------------------------------
10:35:14.454  B_HV_SYS_E__val = 1      [1]
10:35:14.505  DELAY    50ms
10:35:14.527  CHECK    B_Q02_OCH  (1)        1       OK
10:35:14.528  ------------------------------------------------------------------
10:35:14.528  TEST  4  Deaktivace ochran HV - Hlavní vypínač v pořádku
10:35:14.528  ------------------------------------------------------------------
10:35:14.548  B_HV_SYS_E__val = 0      [0]
```

```
10:35:14.599  DELAY    50ms
10:35:14.618  CHECK    B_Q02_OCH  (1)        1        OK
10:35:14.619  CALL     Kvitace
10:35:14.620  label    Kvitace
10:35:14.621  ------------------------------------------------------------------
10:35:14.621  TEST  5  Kvitace poruchy obsluhou
10:35:14.621  ------------------------------------------------------------------
10:35:14.655  B_HV_STOP_Q__val = 1      [1]
10:35:14.669  B_HV_EN__val = 0      [0]
10:35:14.719  DI_Q02_HVAC__val = DK_Q0x_HVAC_V  (1) [1]
10:35:14.771  DELAY    50ms
10:35:14.800  CHECK    B_Q02_OCH  (0)        0        OK
10:35:14.801  RETURN
10:35:14.802  CALL     ZruseniKvitace
10:35:14.803  label    ZruseniKvitace
10:35:14.804  ------------------------------------------------------------------
10:35:14.804  TEST  6  Zrušení kvitace
10:35:14.804  ------------------------------------------------------------------
10:35:14.824  B_HV_STOP_Q__val = 0      [0]
10:35:14.852  B_HV_EN__val = 1      [1]
10:35:14.870  DI_Q02_HVAC__val = DK_Q0x_HVAC_Z  (2) [2]
10:35:14.921  DELAY    50ms
10:35:14.947  CHECK    B_Q02_OCH  (0)        0        OK
10:35:14.948  RETURN
10:35:14.949  ------------------------------------------------------------------
10:35:14.949  TEST  7  Zásah ochran HV - Hlavní vypínač nevypnul
10:35:14.949  ------------------------------------------------------------------
10:35:15.046  B_HV_VYP_E__val = 1      [1]
10:35:15.097  DELAY    50ms
10:35:15.111  CHECK    B_Q02_OCH  (1)        1        OK
10:35:15.112  ------------------------------------------------------------------
10:35:15.112  TEST  8  Deaktivace ochran HV - Hlavní vypínač v pořádku
10:35:15.112  ------------------------------------------------------------------
10:35:15.129  B_HV_VYP_E__val = 0      [0]
10:35:15.180  DELAY    50ms
10:35:15.200  CHECK    B_Q02_OCH  (1)        1        OK
10:35:15.201  CALL     Kvitace
10:35:15.202  label    Kvitace
10:35:15.203  ------------------------------------------------------------------
10:35:15.203  TEST  9  Kvitace poruchy obsluhou
10:35:15.203  ------------------------------------------------------------------
10:35:15.224  B_HV_STOP_Q__val = 1      [1]
10:35:15.248  B_HV_EN__val = 0      [0]
10:35:15.265  DI_Q02_HVAC__val = DK_Q0x_HVAC_V  (1) [1]
10:35:15.316  DELAY    50ms
10:35:15.350  CHECK    B_Q02_OCH  (0)        0        OK
10:35:15.351  RETURN
10:35:15.352  CALL     ZruseniKvitace
10:35:15.353  label    ZruseniKvitace
10:35:15.354  ------------------------------------------------------------------
10:35:15.354  TEST  10  Zrušení kvitace
10:35:15.354  ------------------------------------------------------------------
10:35:15.369  B_HV_STOP_Q__val = 0      [0]
10:35:15.398  B_HV_EN__val = 1      [1]
10:35:15.429  DI_Q02_HVAC__val = DK_Q0x_HVAC_Z  (2) [2]
10:35:15.480  DELAY    50ms
10:35:15.498  CHECK    B_Q02_OCH  (0)        0        OK
10:35:15.499  RETURN
10:35:15.500  ------------------------------------------------------------------
10:35:15.500  TEST  11  Zásah ochran HV - Hlavní vypínač nezapnul
10:35:15.500  ------------------------------------------------------------------
10:35:15.520  B_HV_ZAP_E__val = 1      [1]
10:35:15.571  DELAY    50ms
10:35:15.610  CHECK    B_Q02_OCH  (1)        1        OK
```

```
10:35:15.611  ------------------------------------------------------------
10:35:15.611  TEST  12  Deaktivace ochran HV - Hlavní vypínač v pořádku
10:35:15.611  ------------------------------------------------------------
10:35:15.628  B_HV_ZAP_E__val = 0      [0]
10:35:15.679  DELAY    50ms
10:35:15.699  CHECK    B_Q02_OCH  (1)        1        OK
10:35:15.700  CALL     Kvitace
10:35:15.701  label    Kvitace
10:35:15.702  ------------------------------------------------------------
10:35:15.702  TEST  13  Kvitace poruchy obsluhou
10:35:15.702  ------------------------------------------------------------
10:35:15.747  B_HV_STOP_Q__val = 1      [1]
10:35:15.759  B_HV_EN__val = 0      [0]
10:35:15.775  DI_Q02_HVAC__val = DK_Q0x_HVAC_V  (1) [1]
10:35:15.826  DELAY    50ms
10:35:15.847  CHECK    B_Q02_OCH  (0)        0        OK
10:35:15.848  RETURN
10:35:15.849  CALL     ZruseniKvitace
10:35:15.850  label    ZruseniKvitace
10:35:15.851  ------------------------------------------------------------
10:35:15.851  TEST  14  Zrušení kvitace
10:35:15.851  ------------------------------------------------------------
10:35:15.870  B_HV_STOP_Q__val = 0      [0]
10:35:15.899  B_HV_EN__val = 1      [1]
10:35:15.924  DI_Q02_HVAC__val = DK_Q0x_HVAC_Z  (2) [2]
10:35:15.975  DELAY    50ms
10:35:15.995  CHECK    B_Q02_OCH  (0)        0        OK
10:35:16.005  RETURN
10:35:16.015  label    Kvitace
10:35:16.025  ------------------------------------------------------------
10:35:16.025  TEST  15  Kvitace poruchy obsluhou
10:35:16.025  ------------------------------------------------------------
10:35:16.055  B_HV_STOP_Q__val = 1      [1]
10:35:16.075  B_HV_EN__val = 0      [0]
10:35:16.095  DI_Q02_HVAC__val = DK_Q0x_HVAC_V  (1) [1]
10:35:16.155  DELAY    50ms
10:35:16.396  CHECK    B_Q02_OCH  (0)        0        OK
10:35:16.406  RETURN
10:35:16.416  label    ZruseniKvitace
10:35:16.426  ------------------------------------------------------------
10:35:16.426  TEST  16  Zrušení kvitace
10:35:16.426  ------------------------------------------------------------
10:35:16.466  B_HV_STOP_Q__val = 0      [0]
10:35:16.506  B_HV_EN__val = 1      [1]
10:35:16.536  DI_Q02_HVAC__val = DK_Q0x_HVAC_Z  (2) [2]
10:35:16.596  DELAY    50ms
10:35:16.616  CHECK    B_Q02_OCH  (0)        0        OK
10:35:16.626  RETURN
10:35:16.636  SET LCC __key VARIABLES TO 0
10:35:16.646          B_HV_SYS_E__key =  0
10:35:16.666          B_HV_VYP_E__key =  0
10:35:16.696          B_HV_ZAP_E__key =  0
10:35:16.706          BI_Q02_SYS_OK__key =  0
10:35:16.746          B_HV_STOP_Q__key =  0
10:35:16.766          B_HV_EN__key =  0
10:35:16.796          DI_Q02_HVAC__key =  0
10:35:16.896
10:35:16.896  ------------------------------------------------------------
10:35:16.896  Total tests:   16
10:35:16.896  Total OK   :   16
10:35:16.896  Total NOK  :    0
10:35:16.896  Total Skip :    0
10:35:16.896  Running time: 0:00:03
10:35:16.896  Commit LCC :    0
```

Příloha C – PDF protokol k testovacímu skriptu ochrana hlavního vypínače

Test protocol

Name:	Ochrana hlavního vypínače Q02 – TD013644_LH_3804
Požadavky:	TD013162_SK_0002
Date, time:	31.3.2016 10:35:21
Autor:	Václav Průcha
Tested by:	Václav Průcha
Place:	ŠKODA Transportation - laboratory
File:	TD013644_LH_3804.uts

Tests Results				
ID	Test name	Result		
		OK	NOK	SKIP
1	Kvitace poruchy obsluhou	✓		
2	Bezporuchový stav - Není zásah ochran hlavního vypínače	✓		
3	Zásah ochran HV - Hlavní vypínač nepřipraven	✓		
4	Deaktivace ochran HV - Hlavní vypínač v pořádku	✓		
5	Kvitace poruchy obsluhou	✓		
6	Zrušení kvitace	✓		
7	Zásah ochran HV - Hlavní vypínač nevypnul	✓		
8	Deaktivace ochran HV - Hlavní vypínač v pořádku	✓		
9	Kvitace poruchy obsluhou	✓		
10	Zrušení kvitace	✓		
11	Zásah ochran HV - Hlavní vypínač nezapnul	✓		
12	Deaktivace ochran HV - Hlavní vypínač v pořádku	✓		
13	Kvitace poruchy obsluhou	✓		
14	Zrušení kvitace	✓		
15	Kvitace poruchy obsluhou	✓		
16	Zrušení kvitace	✓		

Total tests:	16
Total OK:	16
Total NOK:	0
Total SKIP:	0
MD5 of Text log:	8A7E6D2FBE18F323A958643B1C9D75F5

Signature .....