ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta elektrotechnická
Katedra řídicí techniky

DIPLOMOVÁ PRÁCE

Návrh bezpečného řízení zhlaví železničních stanic

Bernard Jaroš

Vedoucí práce: doc. Ing. Jan Bílek, CSc. květen 2003

Abstrakt

Diplomová práce se zabývá problémem bezpečného řízení železničních stanic. Úkolem tohoto řídicího systému, nazývaného zabezpečovací zařízení, je ovládat prvky v kolejišti tak, aby byla v maximální možné míře vyloučena možnost kolize kolejových vozidel i při vzniku předvídatelných poruch v systému.

Elektronická stavědla jsou poměrně novým typem zabezpečovacího zařízení (u ČD v provozu od roku 1997). Bezpečnost jejich provozu je podmíněna také jakostí softwaru. V práci jsou navrženy dva rozdílné postupy pro stavění jízdních cest. Jejich součinnost má zabránit důsledkům poruch vzniklých v elektronické části nebo chybným zadáním. Pro ověření funkčnosti byla v jazyce C++ vytvořena aplikace simulující železniční provoz a jeho řízení způsobem obvyklým u elektronických stavědel ČD.

Abstract

The diploma thesis deals with safety control of railway stations. The target of this control system, called interlocking plant, is to operate rail-yard components so that the possibility of rail vehicles collision is at the most excluded even in case of expectable failures in the system.

Electronic interlocks are relatively new type of interlocking plants (at Czech Railways operating since 1997). Safety of their operation is conditioned by software quality. In the thesis, two different ways of routing are designed. Their cooperation is to prevent effects of failures originating in electronical parts or from wrong settings. The application simulating railway traffic and its control by the technique used at Czech Railways' electronic interlocks was built up in C++ to verify their functionality.

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v přiloženém seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne . . . .

podpis

Poděkování

Na tomto místě bych rád poděkoval Dr. Ing. Ivo Myslivcovi a Dr. Ing. Jaromíru Švejdovi z AŽD Praha za úvod do problematiky zabezpečovacích zařízení a bezpečných systémů, Ing. Vladimíru Štorkovi ze STARMON Choceň za seznámení s architekturou elektronického stavědla, Zdeňku Novákovi z ČD za pomoc při vyhledávání nehodových událostí a především Ing. Zdeňku Pacholíkovi ze SUDOP Praha za vysvětlení principů zabezpečování železničních stanic.

Obsah

Úvod

Lidský faktor byl a stále je příčinou mnoha nehod. Mnohým z nich je možné zabránit vhodnými technickými prostředky, které chybu člověka vylučují. Žádné zařízení však není absolutně spolehlivé a snadno by se mohlo stát, že jeho provoz by způsoboval ještě větší množství nehod. Proto je třeba navrhnout řídicí systém tak, aby žádná předvídatelná porucha nevedla k nebezpečnému stavu. Příkladem jsou zabezpečovací zařízení v železniční dopravě, která již prošla dlouhým vývojem - od mechanických prvků přes reléová zařízení až po dnešní elektronické systémy.

Hlavním úkolem zabezpečovacího zařízení je zajištění bezpečné jízdy vlaků a dalších kolejových vozidel přes výměny a znemožnění střetnutí s jinými jedoucími či stojícími vozidly. Jízda kolejových vozidel se řídí návěstěním. Zabezpečovací zařízení musí návěstit stanovenou rychlost, kterou smí vlak jet, popřípadě určit místo, kde má vlak zastavit. Návěstěná rychlost může být přenášena na hnací vozidlo a na něm automaticky vyhodnocována a zpracovávána.

Zabezpečovací zařízení musí být řešeno především tak, aby v provozu dosahovalo stanovenou úroveň bezpečnosti. Zařízení by také mělo dosahovat požadované spolehlivosti. Elektronickým systémům se nedařilo těmto (často protichůdným) požadavkům dlouhou dobu vyhovět, jejich rozvoj lze zaznamenat až v posledním desetiletí. První kapitola se zabývá známými možnostmi dosažení bezpečnosti těchto zařízení a především popisuje současné zabezpečovací systémy.

Zatímco funkce reléových systémů byla dána vytvořenými závislostmi mezi funkčními bloky nebo i jednotlivými relé, chování elektronických zařízení určuje především jejich software. Přestože jeho návrh vychází z podobných požadavků jako návrh reléových závislostí, má dvě odlišnosti. Musí se vypořádat nejen s předpokládaným symetrickým projevem poruch v integrovaných obvodech (např. s rušením, různými chybami v pamětech), ale vzhledem ke své složitosti také s možností výskytu chyb ve vlastním návrhu. Návrhem tohoto softwaru se zabývá druhá kapitola. Nejprve shrnuje bezpečnostní a funkční požadavky na software a poté představuje návrh, který tyto požadavky zohledňuje. Kromě návrhu algoritmů pro samotné zabezpečovací zařízení popisuje i aplikaci, která umožňuje simulací železničního provozu ověřit jejich funkčnost.

Seznam použitých zkratek

AŽD	Automatizace železniční dopravy Praha, s.r.o.
ČD	České dráhy, a.s.
DN	dovolující návěst
ESA 11	elektronické stavědlo AŽD
JOP	jednotné obslužné pracoviště
K-2002	elektronické stavědlo STARMON Choceň, s.r.o.
PZZ	přejezdové zabezpečovací zařízení
SZZ	staniční zabezpečovací zařízení
TNŽ	technická norma železnic
TZZ	traťové zabezpečovací zařízení
ZTP	základní technické požadavky
ZZ	zabezpečovací zařízení

Kapitola 1

Současná zabezpečovací zařízení

V současné době tvoří převážnou většinu provozovaných zabezpečovacích zařízení reléová zabezpečovací zařízení, část hybridní zabezpečovací zařízení a část tvoří plně elektronické systémy. Pro značnou specifičnost železničních zabezpečovacích zařízení a především pro vysoké nároky na jejich bezpečnost a spolehlivost se průnik elektroniky, hlavně vyššího stupně integrace (mikroprocesory apod.), oproti jiným odvětvím zpozdil. Nicméně právě elektronické mikroprocesorové zabezpečovací systémy jsou velmi perspektivní a současný vývoj v oblasti zabezpečovací techniky je orientován právě na ně.

V této kapitole nejprve popisuji obecné možnosti dosažení bezpečnosti u zabezpečovacích systémů. Další zvláštní část je věnována relé, která jsou zatím součástí všech zabezpečovacích systémů (i elektronických). Dále následuje krátký popis reléového zabezpečovacího zařízení AŽD 71, které bylo dlouhou dobu na tratích ČD (ČSD) zaváděno a ze kterého vycházela i pozdější hybridní zařízení. Některé jeho prvky a především zkušenosti z provozu se uplatňují i v nově vytvářených elektronických systémech. Těm je věnována největší část této kapitoly.

1.1 Bezpečnost zabezpečovacích zařízení

Aby bylo možné hovořit o bezpečnosti, je třeba nejprve definovat nebezpečný stav.

Nebezpečný stav v procesu řízení železniční dopravy je situace, která umožňuje, aby se při některé z uvažovaných poruch jednotlivých prvků systému objevil na výstupu systému dovolující signál při takových datech zpracovávaných systémem, jakým by při původní bezporuchové činnosti odpovídal signál zakazující. Dovolující signál dovoluje činnost, kterou je možno vykonat, aniž by došlo k ohrožení bezpečnosti dopravy. Zakazující signál zakazuje činnost, jejíž vykonání ohrozí bezpečnost dopravy. Za ohrožení bezpečnosti dopravy je považován stav, při kterém může nehoda (bez porušení ostatních předpisů) vzniknout.

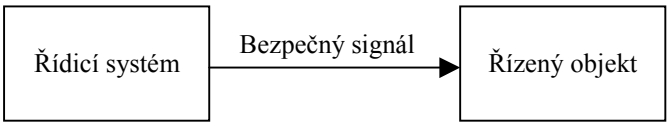
Dříve byl s reléovými zabezpečovacími zařízeními spjat pojem „fail-safe“, který byl synonymem pro absolutní bezpečnost. Při zavádění elektronických systémů se hovoří o opuštění myšlenky absolutní bezpečnosti. Mohlo by se tedy zdát, že jsou elektronická zařízení méně bezpečná. Skutečný důvod je však v něčem jiném. Poruchy se totiž dělily na uvažované a neuvažované. Mezi uvažované poruchy patřily ty, jejichž výskyt bylo možné předpokládat vzhledem k technickému provedení a struktuře zařízení. Naopak mezi neuvažované poruchy patřily takové, vůči kterým měly použité stavební prvky technologicky zajištěnou zvýšenou odolnost, poruchy způsobené násilnou obsluhou, úmyslným poškozením nebo zneužitím zařízení. Při vzniku uvažované poruchy nesmělo dojít k ohrožení železniční dopravy. A pojem absolutní bezpečnost se vztahoval jen na uvažované chyby, ty ostatní byly jednoduše ignorovány, přestože pravděpodobnost jejich výskytu nulová nebyla. U elektronických součástek s vyšším stupněm integrace je prakticky nemožné sestavit seznam uvažovaných poruch. Ještě větším problémem by bylo jejich detekování systémem samým. Proto se nově hovoří o požadované míře bezpečnosti, kterou musí systém zajišťovat. Vznik nebezpečného stavu nemusí být vyloučen, ale jen silně omezen. Funkce zabezpečovací techniky se nyní představuje tak, že musí zajišťovat takovou míru bezpečnosti, aby nebylo překročeno akceptovatelné riziko. Názorným příkladem, který opodstatňuje tuto změnu definice bezpečnosti, může být událost popisovaná v článku 1.1.4.

Zabezpečovací zařízení využívají pro dosažení požadované míry bezpečnosti následující techniky nebo jejich kombinace:

- vlastní bezpečnost při poruše,
- reakční bezpečnost při poruše,
- složenou bezpečnost při poruše.

1.1.1 Zabezpečovací systémy s vlastní bezpečností

Tyto systémy realizují požadovanou funkci jedinou funkční jednotkou. Použité stavební prvky mají takovou vlastnost, že každá jejich uvažovaná porucha způsobí přechod systému do bezpečného stavu (prvky s asymetrickým projevem poruch). Pojem „asymetrický projev poruchy“ znamená, že pravděpodobnost změny výstupního signálu v případě poruchy logického prvku z hodnoty log. „1“ na hodnotu log. „0“ je silně převažující nad pravděpodobností změnu opačné.



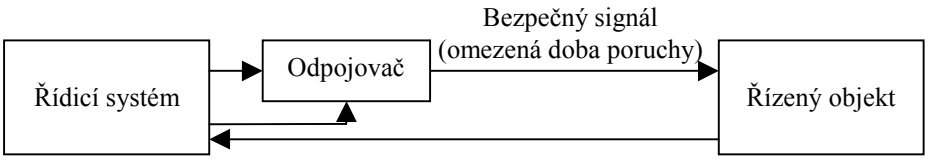
Obr. 1: Struktura zabezpečovacích systémů s vlastní bezpečností

Typickým představitelem těchto systémů jsou zařízení s mechanickými a elektromechanickými prvky pro tvorbu logických závislostí. Pro tyto typy zařízení je charakteristické, že ke zvládnutí poruchy dojde zároveň s jejím vznikem.

Standardní elektronické prvky (a tedy i komponenty počítačů) se vyznačují symetrickým projevem poruch, tedy pravděpodobnost změny výstupního signálu v případě poruchy logického prvku z hodnoty log. „1“ na hodnotu log. „0“ je přibližně stejná, jako pravděpodobnost opačné změny. Tato skutečnost značně komplikuje využití techniky vlastní bezpečnosti při poruše jako základní techniky bezpečnosti při návrhu počítačových zabezpečovacích zařízení. V těchto zařízeních bývají použity obvody s vlastní bezpečností jen jako jejich součást.

1.1.2 Zabezpečovací systémy s reakční bezpečností

Zabezpečovací systém s reakční bezpečností je tvořen jednou funkční jednotkou, ale disponuje prostředky pro detekci poruch a prostředky pro uvedení systému do bezpečného stavu (odpojovač). Funkční kontrola rozhraní mezi řídicí jednotkou a řízeným objektem se dosahuje porovnáním signálu na výstupu jednotky a zpětného signálu informujícího o stavu řízeného objektu.



Obr. 2: Struktura zabezpečovacích systémů s reakční bezpečností

Pokud se vyskytne nebezpečná porucha, musí se detekovat do určitého okamžiku a do tohoto okamžiku se hlavně musí uvést řízený objekt do bezpečného stavu. Zmiňovaný okamžik je doba od vzniku poruchy, během které se systém může nacházet v nebezpečném stavu, aniž by byla ohrožena bezpečnost řízeného procesu.

Počítačové systémy s jednokanálovou strukturou a reakční bezpečností jsou vhodné jen pro aplikace s nižší úrovní bezpečnostních požadavků, např. vnitropodniková doprava, vlečky (tedy místa s malou intenzitou dopravy, malými rychlostmi a vyloučenou přepravou osob).

1.1.3 Zabezpečovací systémy se složenou bezpečností

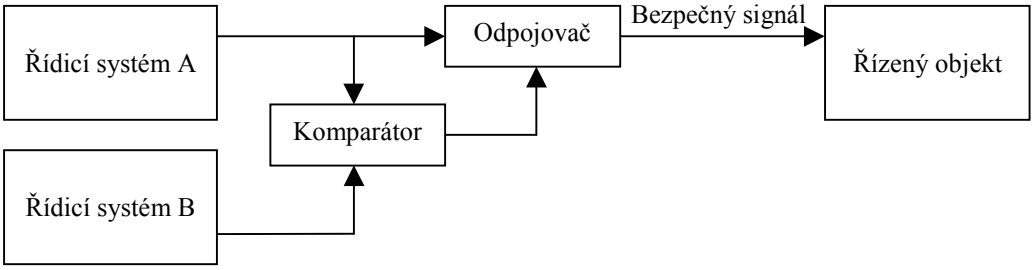
Systémy se složenou bezpečností řeší požadovanou funkci vícenásobně (alespoň ve dvou procesech). předpokladem správné a bezpečné činnosti je shoda výsledků, vzájemná nezávislost procesů, včasné zjištění poruchy a její zvládnutí.

Počítačové systémy se složenou bezpečností využívají pro dosažení požadované úrovně bezpečnosti různé formy aktivní redundance, která umožňuje vícenásobné řešení požadované úlohy. Pro aplikace v železniční dopravě jsou charakteristické systémy s:

- dvoukanálovou strukturou a komparací (označovány jako systémy 2 z 2),
- tříkanálovou strukturou a hlasováním (označovány jako systémy 2 z 3).

Systém s dvoukanálovou strukturou

Zabezpečovací systém obsahuje dvě navzájem nezávislé jednotky na vykonávání specifické funkce. Kritériem bezpečné činnosti systému jsou výsledky porovnání interních signálů a signálů na výstupech systému. Při rozdílné výstavbě kanálů je zpravidla možné porovnat jen výstupní signály nebo průběžné výsledky. Porovnání výstupních signálů obou jednotek se uskutečňuje v komparátoru a může být provedeno hardwarově, softwarově nebo kombinací těchto způsobů.



Obr. 3: Struktura dvoukanálových zabezpečovacích systémů se složenou bezpečností

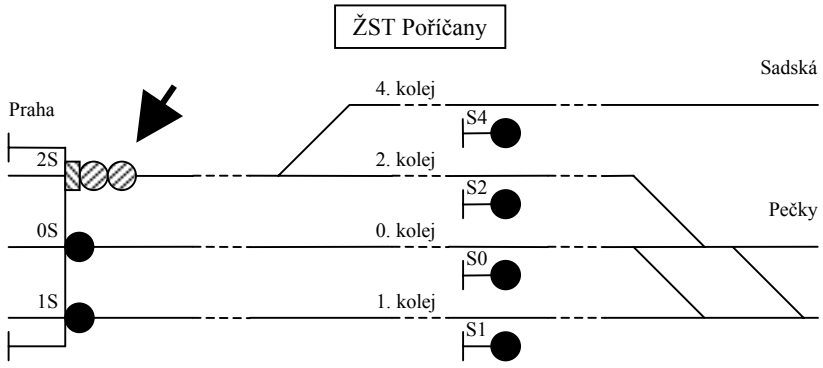
Pokud se vyskytne porucha jedné jednotky, musí systém poruchu detekovat a přejít do trvalého bezpečného stavu dřív, než se vyskytne druhá porucha, která může být v souběhu s první poruchou potencionálně nebezpečná. Doba detekce poruchy a přechodu do bezpečného stavu musí být menší než určený maximální čas, který je vypočítán na základě

informací o intenzitách poruch jednotlivých prvků. První porucha nesmí způsobit výskyt nebezpečného stavu, okamžitě po zjištění rozdílu mezi výstupními signály obou jednotek musí zaniknout i dovolující signál na výstupu celého řídicího systému.

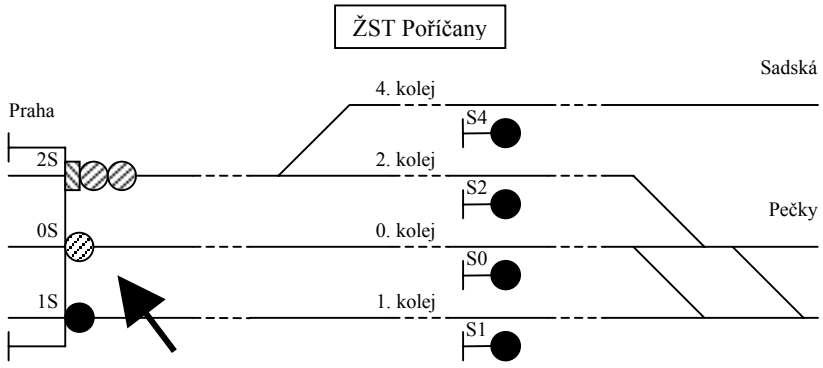
1.1.4 Nehodová událost v Poříčanech

Dne 28.6.2001 přibližně v 01:00 vjížděl vlak 65377- 1. nsl. do ŽST Poříčany po první koleji od Prahy na návěst „Očekávejte rychlost 80 km/h“ vjezdového návěstidla 1S. Téměř současně s ním vjížděl také od Prahy po nulté koleji vlak Nex 57301 rovněž na návěst „Očekávejte rychlost 80 km/h“ vjezdového návěstidla 0S. Při další jízdě vlaku 65377 - 1. nsl. po první staniční koleji však byla na odjezdovém návěstidle S1 návěst „Stůj“ a dále strojvedoucí spatřil, že za odjezdovým návěstidlem je podle polohy výhybek postavena jízdní cesta z nulté staniční koleje na první staniční kolej. Vzápětí po takto postavené jízdní cestě projel vlak Nex 57301.

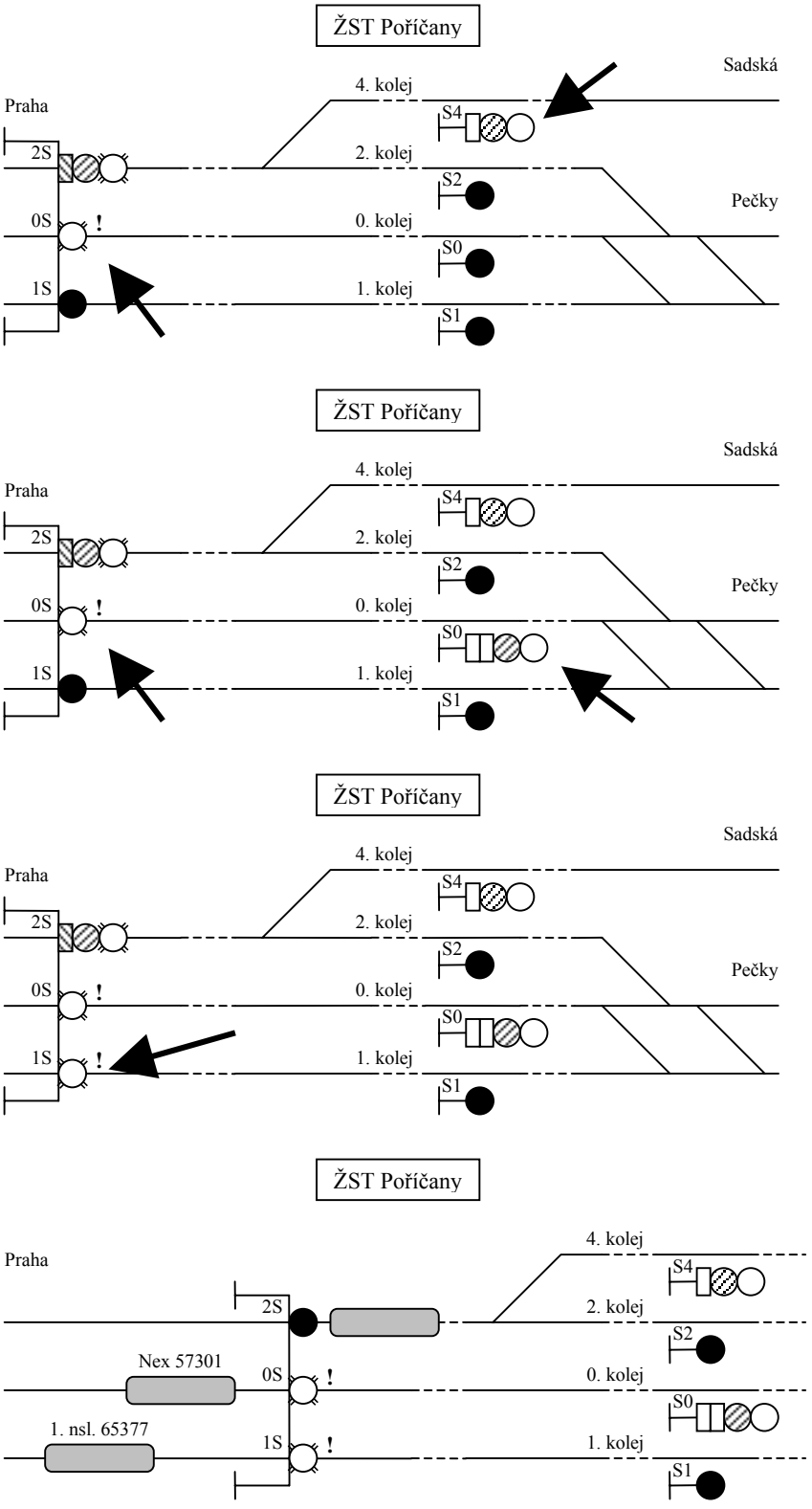
ŽST Poříčany je vybavena hybridním staničním zabezpečovacím zařízením ETB s bezpečnými povely. Záznam činnosti je v místním počítači archivován po dobu 50 až 60 hodin, takže bylo možné činnost zabezpečovacího zařízení vyhodnotit. Potvrdilo se, že oba strojvedoucí viděli na vjezdových návěstidlech 0S a 1S chybné návěsti „Očekávejte rychlost 80 km/h“ místo správných návěstí „Očekávejte rychlost 100 km/h“ na návěstidle 0S a „Výstraha“ na návěstidle 1S.



0:53:30 – postavena VC 2S – 4K a na náv. 2S svítí správný n. znak, tj. „Rychlost 60 km/h a výstraha“



0:54:50 – postavena VC 0S – 0K pro Nex 57301 a na náv. 0S svítí správný n. znak, tj. „Výstraha“



0:55:16 – postavena odjezdová VC S4 –Sadská, na náv. S4 svítí správně návěst „Rychlost 80 km/h a volno“ a na náv. 0S se rozsvěcí chybně návěst „Očekávejte rychlost 80 km/h“

1:00:12 – postavena odjezdová VC S0 – směr Pečky, na náv. S0 svítí správně návěst „Rychlost 100 km/h a volno“ a na náv. 0S stále svítí chybná návěst „Očekávejte rychlost 80 km/h“

0:01:46 – postavena VC 1S – 1K pro vlak 1. nsl. 65377 a na náv. 1S se rozsvěcí chybně návěst „Očekávejte rychlost 80 km/h“

1:01:58 – vlak do Sadské projíždí návěstidlo 2S
1:02:15 – vlak Nex 57301 vstupuje do úseku před návěstidlem 0S
1:02:18 – vlak 1. nsl. 65377 vstupuje do úseku před návěstidlem 1S

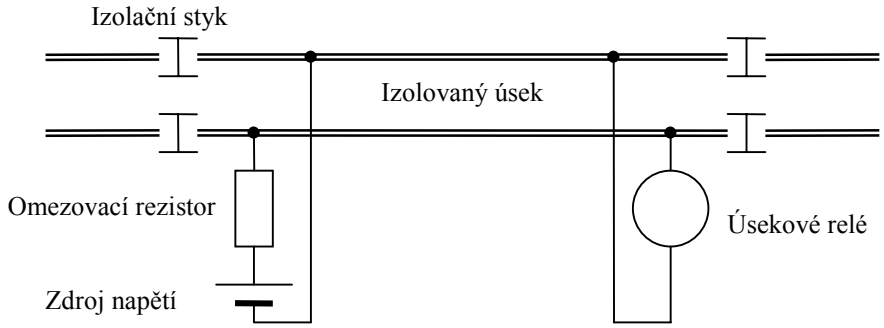
Obr. 4: Nesprávné návěstění v Poříčanech

Příčinou nesprávného návěstění byla projekční chyba této instalace ETB v zapojení obvodů průjezdových relé návěstidel 1S a 0S, která určují očekávanou rychlost při DN. Chybný výběr znaku se přenesl od návěstidla S4.

V tomto případě došlo k vážnému ohrožení bezpečnosti železniční dopravy a jen díky pozornosti strojvedoucího vlaku 65377 - 1. nsl. nedošlo k projetí odjezdového návěstidla S1 a ke srážce s vlakem Nex 57301, který projížděl za návěstidlem po kolejové spojce mezi nultou a první kolejí. Toto zabezpečovací zařízení je ve stanici Poříčany v provozu od 23.8.1996, chyba se tedy objevila až po pěti letech provozu. Popisovaná dopravní situace, při které do stanice Poříčany vjížděly od Prahy téměř najednou tři vlaky, je velmi neobvyklá, proto se chyba nemusela do té doby vůbec projevit.

1.2 Relé – základní prvek zabezpečovacích systémů

Reléové obvody nesmějí při žádné poruše (zkrat na kabelu, přerušení vodiče, proražení usměrňovače apod.) způsobit provozně méně bezpečný stav (poruchou způsobit např. změnu žlutého návěstního světla na zelené, způsobit samovolné přestavení výměny pod vozidlem apod.). Proto jsou všechna povolující kritéria vytvořena zásadně obvody na stálý proud. To znamená, že relé, které svými zapínacími kontakty hlásí dovolující stav do zabezpečovacího zařízení, je v základní poloze buzeno. Příkladem je paralelní kolejový obvod (viz obr. 5), ve kterém je vinutí úsekového relé připojeno ke zdroji přes obě kolejnice a jeho kotva je v základním stavu přitažena. Vjede-li na kolej vlak, dvojkolí šuntují kolejový obvod a přes cívku relé již neprochází téměř žádný proud, takže kotva jistě odpadne a relé hlásí do zařízení, že kolej je obsazena. Totéž se stane, dojde-li k nějaké poruše v obvodu relé (zkrat, přerušení vodiče) či lomu kolejnice. Pak relé falešně odpadne, ale z hlediska provozu nedochází k ohrožení bezpečnosti, neboť je hlášen pouze provoz omezující stav (např. falešná indikace obsazení koleje způsobí, že na tuto kolej nelze stavět jízdní cestu, což je pro plynulost provozu sice nepříjemné, ale není to nebezpečné). Při uvažovaných poruchách tedy nemůže dojít ke kolizi. Některé málo používané koleje mohou mít tak velký přechodový odpor mezi kolejnicí a kolem, že nelze zaručit správnou funkci detekce obsazení úseku. Tento stav se obvykle řeší zabezpečením administrativním, takže je v určitých případech volnost koleje potvrzována obsluhou. Tento základní obvod byl dále zdokonalován, aby nedocházelo k chybným indikacím při provozu s elektrickou trakcí, a obvod sloužil i pro přenos návěstí na vlakový zabezpečovač na místě strojvedoucího.



Obr. 5: Schéma paralelního kolejového obvodu

Spolehlivá činnost obvodu je závislá na spolehlivosti vlastního relé. Použití obvodu na stálý proud by nebylo by nic platné, kdyby kotva relé při přerušení budicího obvodu relé správně neodpadla (např. kvůli mechanické závadě ložisek kotvy apod.). Proto jsou relé pro zabezpečovací techniku robustní a mají speciální konstrukci. Podle provedení se dělí do tří skupin:

a) relé I. bezpečnostní třídy,
b) relé II. bezpečnostní třídy,
c) ostatní relé bez bezpečnostních podmínek.

Všechna relé pro zabezpečovací techniku musí mít zaručené technické parametry, například minimální tlak v kontaktech, maximální přechodové odpory kontaktů, minimální velikost mezery mezi rozevřenými kontakty, musí mít dostatečnou životnost, potřebný izolační odpor atd. Bezpečnostní relé musí mít navíc zaručený minimální poměr proudu odpadu a přítahu kotvy. Všechna jejich aktivní kontaktní péra musí být vzájemně mechanicky spojena a musí zaručovat, že při sepnutí i jediného zapínacího kontaktu jsou všechny rozpínací kontakty rozevřeny a naopak. U relé I. bezpečnostní třídy musí kotva při proudu menším než proud odpadu bezpečně odpadnout vlastní vahou (i při eventuálním spečení kontaktů), proto se zatěžuje přídavným závažím. U relé II. bezpečnostní třídy je k tomuto účelu povoleno použít síly per. Ostatní relé, která splňují jen základní požadavky, lze použít pouze v obvodech, které nemají vliv na bezpečnost dopravy.

Vyskytnou-li se jakékoli uvažované poruchy, nesmí dojít k ohrožení bezpečnosti dopravy. Za ohrožení bezpečnosti se považuje:

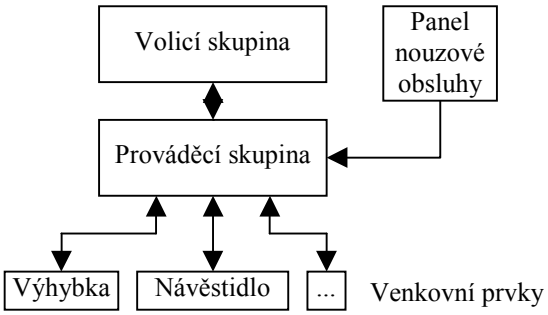
- falešná indikace volnosti koleje nebo výměny,
- samovolné nebo nedokončené či nevčasné přestavení výměny,
- nesprávná indikace polohy výměn a stavu návěstidel,
- nesprávná indikace traťových i jiných souhlasů.

Některé další požadavky kladené na zapojení v zabezpečovací technice jsou tyto: Vytažením kteréhokoli zástrčkového prvku nesmí být ohrožena bezpečnost. V obvodech, které mají vliv na bezpečnost dopravy, musí se používat relé I. třídy. Při použití relé II. třídy se musí přítah i odpad kotvy kontrolovat ve funkci další části zapojení. Indikace a příkazy obsahující pojmy z hlediska bezpečnosti dopravy povolující a důležité musí být provedeny jako obvod na stálý proud. Podpěrná relé (s mechanicky vázanými dvěma kontaktními systémy) se nesmějí používat pro kontrolní obvody. Správnou a bezpečnou činnost zabezpečovacích zařízení nesmí ovlivňovat kapacita použitých kabelů. Závada na venkovním zařízení se musí projevit okamžitě. Všechny obvody mezi zařízením v řídicí místnosti a díly v kolejišti (přestavníky, návěstidla apod.) musí být provedeny izolačně, bez uzemnění. Ztráta napětí v síti nebo krátkodobé přerušení napájení některého obvodu nesmí způsobit příznivější stav (např. vybavení postavené cesty apod.).

1.3 Reléové zabezpečovací zařízení AŽD-71

Reléové staniční zabezpečovací zařízení typu AŽD-71 je staniční zabezpečovací zařízení 2. kategorie dle TNŽ 34 2620. Zařízení má blokovém provedení, skupinově přestavované výměny a všechny jeho závislosti jsou uskutečněny elektricky. Pro kontrolu volnosti kolejí a výhybkových úseků používá kolejové obvody. Návěstidla a ústředně stavěné výměny a výkolejky s elektromotorickými přestavníky se ovládají z jednoho stavědla. V případě nutnosti (vyžadují-li to místní provozní poměry vzhledem k rozsahu kolejiště) může být stavědel i více. Při velkém místním posunu lze výměny stavět z pomocných stavědel, která jsou umístěna přímo v kolejišti.

Zařízení se ovládá z ústředního stavědla, ve kterém je na řídicím stanovišti umístěn řídicí stůl (v malých a středních stanicích) nebo ovládací stůl a kontrolní skříně, pokud by byl řídicí stůl příliš rozměrný (ve velkých stanicích s rozsáhlým kolejištěm). Všechny ovládací a indikační prvky jsou umístěny na panelu, který je na řídicím stole. Ve velkých stanicích jsou na samostatné nosné konstrukci umístěny pouze indikační prvky a ovládací prvky jsou umístěny na panelu na ovládacím stole. Nouzové ovládací prvky (tlačítka pro nouzové přestavování výměn a pro nouzové uvolnění izolovaných úseků) se obvykle umísťují mimo řídicí stůl ve skříni s pomocnými tlačítky. Podle rozsahu vlakové dopravy a kolejiště může být na jednom stanovišti více ovládacích stolů s možností přepnutí obsluhy na jeden ovládací stůl.



Obr. 6: Struktura zabezpečovacího zařízení AŽD-71

Jízdní cesty se stavějí postupným stlačením počátečního a koncového tlačítka. Tímto tzv. dvoutlačítkovým způsobem se postaví základní cesta. Má-li být postavena variantní cesta, je nutné po stisknutí počátečního tlačítka stisknout ta variantní tlačítka, která určují zamýšlenou jízdní cestu. Jako poslední se stlačí koncové tlačítko. Jsou-li splněny podmínky pro určenou jízdní cestu, rozsvítí se na příslušných návěstidlech návěst dovolující jízdu. Zrušení závěru jízdní cesty po projetí vozidlem nastává automaticky, a to postupně, jak vozidlo obsazuje a uvolňuje jednotlivé izolované úseky.

V reléovém zabezpečovacím zařízení AŽD-71 se používá celkem 12 typů normalizovaných bloků. Jednotlivé typy používaných bloků jsou uvedeny v tabulce 1.

Funkční určení bloků	Označení bloků
Závislostní bloky hlavního návěstidla	H
Doplňkový blok vjezdového návěstidla	W
Doplňkový blok odjezdového návěstidla	Q
Rychlostní blok	R
Blok seřaďovacího návěstidla mezi výhybkami	A
Blok seřaďovacího návěstidla bezvýhybkového úseku	B
Blok seřaďovacího návěstidla u kusé koleje	C
Blok bezvýhybkového izolovaného úseku	M
Blok výhybkového izolovaného úseku	S
Blok dopravní koleje	K
Dvojitý výhybkový blok	D
Blok třífázového výměnového přestavníku	Vt

Tab. 1: Typy a označení reléových bloků AŽD-71

Na toto reléové zabezpečovací zařízení navázalo několik hybridních systémů, které byly postupným přechodem k elektronickým systémům. Zadávací část byla nahrazena počítačem s rozhraním k reléové části, která nadále zajišťovala bezpečné funkce. Proto nemusela být zadávací část schvalována podle přísných norem bezpečných systémů. Později byly do zadávací části začleněny i nouzové povely, jejichž přenos již bezpečný být musel.

1.4 Elektronické stavědlo K-2002 Starmon

1.4.1 Úvod

Elektronické stavědlo K-2002 je staniční zabezpečovací zařízení 3. kategorie dle TNŽ 34 2620 v systému JOP určené pro zabezpečení jízd vlaků v malých stanicích (přibližně do 20 výhybek) a zabezpečení vlečkových kolejišť. Verzi K-2002 předcházely verze SZZK, (z r. 1996), verze SZZK-98 a verze K-2000, která byla instalována ve dvanácti železničních stanicích v průběhu let 2000 a 2001.

Zařízení umožňuje:

- zadávání povelů a zobrazení stavu staničního zabezpečovacího zařízení v kolejišti na monitoru ovládacího počítače podle JOP,
- samostatné přestavování výhybek,
- ovládání elektromagnetických zámků,
- ovládání pomocného stavědla,
- ovládání napájecího stojanu,
- stavění a rušení vlakových a posunových cest,
- ovládání a kontrolu přejezdových zabezpečovacích zařízení ve stanicích a v přilehlých mezistaničních úsecích,
- vazbu na traťové zabezpečovací zařízení přilehlých úseků,
- použití časově omezené přivolávací návěsti na hlavních návěstidlech,
- nouzové uvolnění závěrů úseků,
- nouzové přestavení výhybek,
- provedení nouzového závěru výhybek, výkolejek, elektromagnetických zámků pomocných stavědel a traťových souhlasů,
- nouzové ovládání přejezdů,
- možnost dálkového ovládání zabezpečovacího zařízení z vyššího systému,
- spolupráci se staniční diagnostikou.

V základním stavu je pomocí dvojice technologických počítačů, které jsou součástí modulu CPU, nepřetržitě sledován stav venkovního zařízení a udržována komunikace s ovládacím počítačem (OP1). Stav zařízení v kolejišti je zobrazován na obrazovce barevného monitoru podle směrnice JOP (Jednotné obslužné pracoviště). Logické algoritmy programu technologických počítačů kontrolují průběh stavění vlakové cesty, provedení závěru cesty, rozsvícení návěstního znaku, průjezd vlaku a rušení cesty.

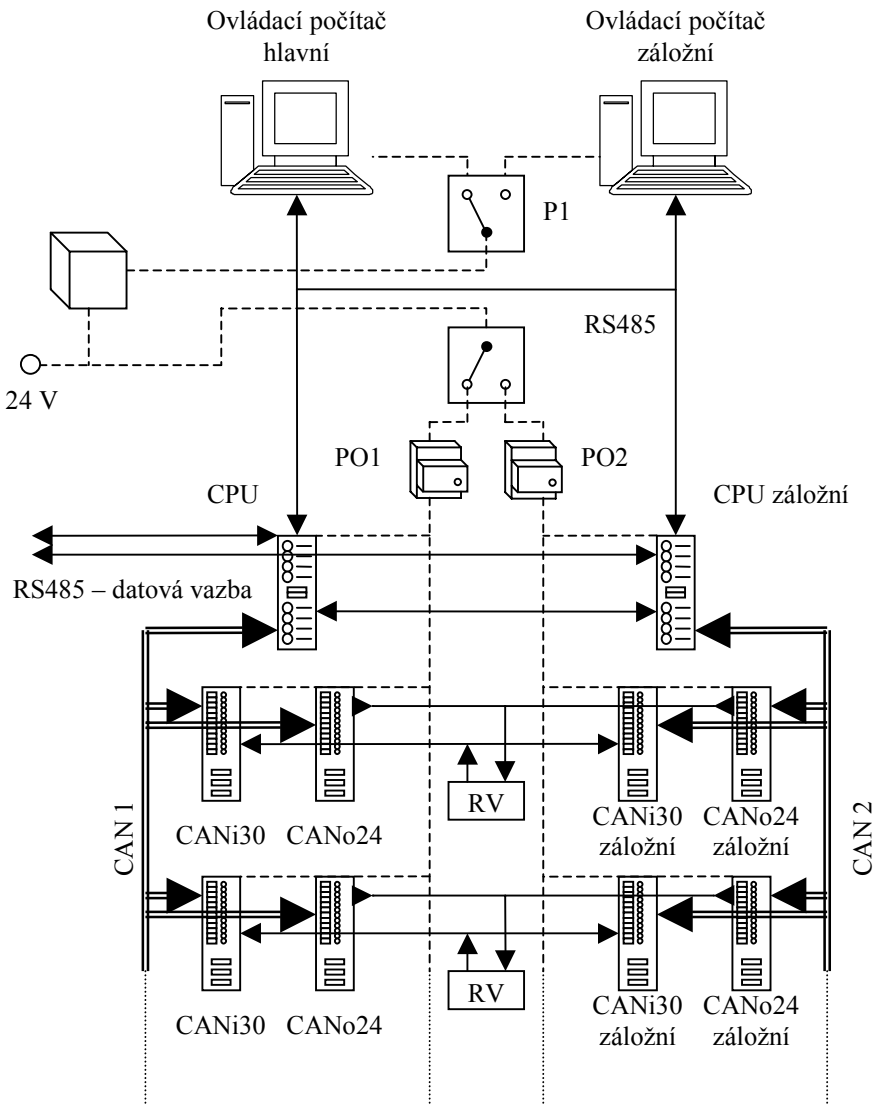
Elektronické stavědlo K-2002 lze z hlediska funkce rozdělit na čtyři úrovně (obr. 7): úroveň ovládacích počítačů, úroveň technologických počítačů, úroveň reléových obvodů a úroveň venkovních zařízení. První dvě úrovně tvoří elektronickou část, třetí a čtvrtá úroveň představuje část reléovou.

1.4.2 Úroveň ovládacích počítačů

Ovládací počítače slouží ke styku zařízení s obsluhou. Jedná se o běžná PC s procesory Pentium, která mají kromě standardních periferií navíc převodník RS232/RS485, čtečku čipových karet, mechaniku PCMCIA pro paměťové karty, případně přijímač časových značek.

Software ovládacího počítače je zpracován tak, aby jeho interpretace na monitoru a způsob komunikace „obsluha – počítač“ odpovídaly ZTP ČD pro jednotné obslužné pracoviště JOP. Programové prostředky splňující tyto požadavky jsou zpracovány modulárně pomocí vývojového prostředí DELPHI s využitím operačního systému WINDOWS 98. Na zpracování tohoto softwaru nejsou kladeny bezpečnostní požadavky, kromě zobrazení informací při nouzových obsluhách a potvrzování nouzových povelů.

Data přicházející z modulu CPU jsou zpracována v OP a cyklicky zobrazována po 0,5 s na obrazovce monitoru ovládacího počítače. V době vydávání nouzových povelů je grafické zobrazení doplněno textovým výpisem odchylek od správného stavu venkovního zabezpečovacího zařízení. Použitý princip zobrazování textového výpisu a grafiky zajišťuje bezpečné zobrazení informací nutných k vydání nouzového povelu.



Obr. 7: Blokové schéma K-2002

OP1	hlavní ovládací počítač
OP2	záložní ovládací počítač
CPU	modul bezpečného dvoukanálového počítače
CANi30	modul vstupů, obsahující 30 logických vstupů s vazbou CAN na modul CPU
CANo24	modul výstupů, obsahující 24 bezpečných výstupů s vazbou CAN na modul CPU
M	měnič pro napájení OP
PO1, PO2	přepěťové ochrany
P1	přepínání hlavního a záložního ovládacího počítače
P2	přepÍnání hlavního a záložního systému
RV	reléová vazba na venkovní zabezpečovací zařízení

1.4.3 Úroveň technologických počítačů

Modul CPU je osazen dvojicí galvanicky oddělených mikropočítačů (technologických počítačů) s procesory SAK-C167CS-LM, mezi kterými je vytvořena datová vazba pomocí optického sendviče. Oba mikropočítače obsahují obvod RTC zálohovaný baterií, 0,5 MB paměti FLASH pro program, 256 KB paměti RAM pro data a 4 až 16 MB paměti FLASH pro konfigurační data. Další výbavou jsou dvě sběrnice pro CAN BUS, komunikační linky RS485 a OPTO plus linka RS232 pro ladění software. Volitelně může být připojen i modul přijímače časových značek DCF a modul komunikace GSM. Každý mikropočítač má vlastní zdroj napájení a měniče DC-DC pro galvanické oddělení komunikačních linek. Na čelním panelu modulu CPU jsou umístěny indikační displeje a LED.

Modul CANi30 je osazen dvojicí mikropočítačů s procesory DALLAS DS80320 a zajišťuje bezpečné rozštěpení kontaktových i bezkontaktních vstupů, ošetření zákmitů, vyhodnocení vadných vstupů a komunikaci s modulem CPU po sběrnici CAN BUS. Periodicky je na krátký okamžik vypínáno napájení vstupních relé, což umožňuje zkontrolovat log. 0 na všech vstupech. Tím je zajištěna detekce proražení, zkratu a pod.

Modul CANo24 je osazen dvojicí mikropočítačů s procesory DALLAS DS80320 a zajišťuje bezpečné povelování výstupů, testování a vyhodnocení vadných výstupů a komunikaci s modulem CPU po sběrnici CAN BUS. Součástí modulu je 26 bitový bezpečný komparátor. Z toho 24 bitů je použito pro řízení výstupů, zbylé dva bity zajišťují bezpečné vypnutí výstupů v případě chyby (nesrovnalosti) v datech nebo poruchy modulu CPU. Tím dojde k odpadnutí relé 1. bezp. třídy a k přechodu všech prvků do bezpečných stavů (např. zhasnutí DN a rozsvícení červené, atd.). V každém cyklu jsou testovány výstupy jednoho modulu CANo24 tak, že výstupy jsou na krátký okamžik znegovány a přečteny v obou stavech. Tak je zjištěna závada výstupu dříve, než se projeví. Okamžik přepnutí je kratší než doba odpadnutí výstupního relé, takže v prvcích ovládaných těmito relé se přepnutí nijak neprojeví.

Programy pro druhou úroveň systému jsou zpracovány pomocí programovacího jazyka Assembler s instrukčním souborem procesoru C 166/7. Pro zajištění bezpečnosti byly vytvořeny dva různé algoritmy programů v každém kanálu. Zdrojové soubory jsou překládány do strojového kódu překladačem AXl66 firmy AMIT Praha pro přímý kanál a Al66 firmy Keil pro inverzní kanál. Vstupní informace jsou inverzní a rovněž výstupní povely (pro zabezpečení činnosti komparátoru v desce CANo24) jsou inverzní (bitově negované). Časové závislosti v řídícím programu jsou řešeny rovněž dvoukanálově, přičemž je vzájemně kontrolován chod časovačů v obou kanálech. Cyklicky je prováděna kontrola postupně celé konfigurační EPROM (FLASH) i RAM, je prováděna i kontrola CRC celého programu.

V technologických počítačích jsou použity tyto moduly:

modul inicializace,

modul komunikace s moduly CAN,

modul komunikace s OP,

modul výhybky (výkolejky, vrat),

modul elektromagnetického zámku (jednoklíčový, dvouklíčový, traťový),

modul pomocného stavědla,

modul nouzového uvolňování závěru úseků,

modul úseku (izolovaný, neizolovaný, traťový),

modul přejezdu,

modul pozitivní návěsti a uzavření PZZ při ujetí vozů,

modul výluky dopravní služby,

modul návěstidla (hlavní, seřaďovací, oddílové, vazební),

modul samostatné předvěsti,

modul traťového zařízení (RPB 71, AH88a, evidence odjezdu),

modul přípravy vlakové cesty,

modul vlakové cesty,

modul nouzové vlakové cesty,

modul posunové cesty,

modul nouzové posunové cesty,

modul označníku,

modul globálního stůj,

modul napájení ze sítě a z trakce,

modul vytvoření datagramu,

modul zpracování vstupů,

modul zpracování výstupů,

modul zpracování chyb.

Pokud stanice obsahuje více prvků stejného typu (typicky více výhybek, návěstidel, úseků, atd.), je modul použit vícekrát (s různými parametry). V každém cyklu jsou obslouženy všechny moduly, perioda cyklu je 100 ms.

1.4.4 Úroveň reléových obvodů

Ovládání venkovních zařízení je provedeno pomocí povelových relé OMRON druhé bezpečnostní třídy a kontrolních relé NMŠ první bezpečnostní třídy. Stav povelových relé je zpětně kontrolován systémem pomocí desky bezpečných vstupů CANi30.

Například u návěstidel je použito na každé světlo jedno povelové světelné relé a jedno kontrolní světelné relé.

Jiným příkladem je výhybka. Její přestavný obvod je ovládán stavěcími relé SP a SM přes desku CANo24. Poloha výhybky je dána stavem kontrolních relé KP a KM. Závěr a rozřez výhybky je proveden programově v technologickém počítači. Rozřez může odstranit udržující pracovník pomocí tlačítka v reléové místnosti.

1.4.5 Úroveň venkovních zařízení

Jako venkovní zařízení jsou použity prvky: přestavníky EP600, návěstidla AŽD, elektromagnetické zámky EMZ, pomocné stavědlo AŽD, přejezdová zařízení AŽD a VÚD, elektronický přejezd AŽD PZZ-EA, kolejové obvody 75 Hz a 275 Hz, počítače náprav Alcatel, počítače náprav Siemens (Frausher).

1.4.6 Komunikace

Komunikace mezi ovládacím počítačem a technologickými počítači v modulu CPU (a opačně) se uskutečňuje pomocí sítě s rozhraním RS485 přenosovou rychlostí 56 kBit/s. Počítač OP je řídící počítač, technologické počítače (dále TP) v CPU jsou podřízené. Druhá úroveň komunikace je mezi modulem CPU a moduly CANi30 a CANo24 pomocí sběrnice CAN přenosovou rychlostí 500 kBit/s. Každý TP řídí komunikaci ve svém kanálu CAN, oba kanály jsou fyzicky odděleny.

Komunikace RS485

Ovládací počítač během intervalu 0,5 s vysílá telegram do obou TP. Po každém vyslaném telegramu očekává telegram s daty od TP. Data z telegramu s chybnými kontrolními součty se nezobrazují. Pokud by OP třikrát za sebou vyhodnotil chybu telegramu, zobrazí se na monitoru ztráta komunikace.

Komunikace CAN

Komunikace CAN byla původně vyvinuta firmou Bosch pro použití ve vozidlech, kde měla nahradit stále složitější klasickou kabeláž. Později se stala mezinárodní normou ISO 11898 a pro své výhodné vlastnosti se rozšířila v průmyslových aplikacích. Dnes se

využívá často i v železniční dopravě. Sběrnice CAN vyniká především v jednoduchosti komunikačního protokolu, vysokém výkonu (zvláště v případě časově kritických aplikací) a dostupností levných komunikačních obvodů. Komunikační protokol v sobě obsahuje identifikační, datové a kontrolní rámce, které zabezpečují rychlý a spolehlivý přenos i v průmyslovém prostředí. Přenosové médium tvoří kroucená stíněná dvoulinka. Přenosová rychlost v případě rozvodů v rámci reléové místnosti je 500 kBit/s.

Technologické počítače v modulu CPU jsou pomocí sběrnice CAN spojeny s moduly CANi30 a CANo24 umístěnými ve skříních a tvoří distribuovaný systém, který lze vzdálit i mimo reléovou místnost.

1.4.7 Ostatní

Diagnostika

Součástí systému je diagnostika umožňující indikovat na ovládacím počítači základní informace o funkci systému. Indikace jsou na monitoru OP. Kontrolují se

AMP	proud do přestavníků:	bílý symbol znamená normální odběr
		žlutý symbol znamená zvýšený odběr
KSB	kontrola staniční baterie:	žlutý symbol znamená výpadek dobíječe
		červený symbol znamená vybitou baterii

PHN porucha hlavního napájení
PNDO porucha napájení dohlédacích obvodů
PZNP porucha základního napájení přestavníků
PZNN porucha základního napájení návěstidel
KNM kontrola návěstního měniče
IS snížený izolační stav napájení návěstidel nebo napájení přestavníků
PKP porucha kmitače - pomalého kmitání
PKR porucha kmitače - rychlého kmitání
KJ kontrola jističů
OV osvětlení výměn
EOV ohřev výměn
UN úsporné napájení
NPC porucha měniče pro napájení OP
ZTP záložní technologický počítač

Při výskytu poruchy se ještě objeví poruchové hlášení v textovém poli doprovázené akustickým signálem a porucha se zapíše do seznamu poruch. Některé poruchy nemají symbol, pouze se vypisují jako poruchová hlášení. Týká se to všech spálených žárovek, rozřezu výhybek, nepřestavení výhybky v časovém limitu a ztráty komunikace s TP. Označování poruch v seznamu poruch jako odstraněné provádí pracovník údržby po zasunutí své čipové karty do snímací skříňky. Vnitřní diagnostika umožňuje ve velké míře diagnostikovat i vlastní počítačovou část a tím je usnadněn servis zařízení v případě nepoužití 100 % zálohy. Udržující pracovník získává z diagnostiky informace o stavu komunikací v systému a o stavu desek vybavených testovacími funkcemi. Všechny vstupní a výstupní moduly jsou opatřeny indikačními prvky, které signalizují stav všech vstupů a výstupů a tím umožňují přehlednou kontrolu stavu venkovního zařízení. V případě poruchy je určení vadného obvodu usnadněno výpisem chybového hlášení na displeji modulu.

Zařízení může být doplněno o měřící ústřednu diagnostiky a diagnostický počítač pro udržující pracovníky s automatickým sledováním provozních hodnot zařízení. Výsledky diagnostiky jsou přenášeny do místa soustředěné údržby pomocí nadřazené sítě dálkového ovládání společně s ovládacími kanály. Současně jsou výsledky k dispozici také v místě nasazení pro místní údržbu.

Spolehlivost

Spolehlivostní parametry navrhovaného zařízení nejsou doposud matematicky vyjádřeny. Pro uživatele je podstatně důležitější parametr "pohotovost zařízení", který určuje schopnost zařízení nacházet se s provozuschopném stavu. Z tohoto důvodu jsou pracoviště vybavena 100% zálohou.

Archivace dat

V ovládacím počítači se data archivují na pevný disk celkem do pěti souborů. Stavový soubor, dopravní deník a historie poruch se také ukládá do paměťové karty, kterou lze vyjmout a prohlížet na jiném počítači. V dopravním deníku jsou evidovány všechny povinně dokumentované úkony, převzetí služby, textové komentáře. Druhý soubor s daty od CPU se kontroluje na počet zápisů a při dosažení 100 tisíc položek se uzavře, přejmenuje a vytvoří nový prázdný. Pracovník údržby má oprávnění prohlížet datový soubor, který se zobrazuje na jiném počítači pomocí speciálního prohlížecího programu.

Dálkové ovládání

V případě potřeby bude ovládací počítač doplněn programovým modulem, který umožní přenesení ovládacího pracoviště do vzdáleného dispečerského centra. Podle vzdálenosti se

vybere vhodný přenosový systém. Byl vytvořen HW a SW modul pro připojení zařízení K-2000 a K-2002 na dálkové ovládání AŽD.

1.5 Elektronické stavědlo ESA 11

1.5.1 Úvod

Elektronické stavědlo ESA 11 je staniční zabezpečovací zařízení 3. kategorie ve smyslu TNŽ 34 2620 s reléovým rozhraním k venkovním prvkům zabezpečovacího zařízení. Téměř všechny logické funkce stavědla jsou tedy vykonávány počítačovou částí, relé jsou použita jako spolehlivé spínače výkonového signálu k návěstním žárovkám, přestavníkům, kolejovým obvodům, pomocným stavědlům, elektromagnetickým zámkům a navazujícím reléovým zařízením. ESA 11 navázala na stavědla typu SZZ-ETS a SZZ-ETB vyvinutá dříve a uvedená do provozního ověřování v posledním desetiletí. Se stavědlem SZZ-ETB má ESA 11 shodný hardware počítačové části a využívá i stejných konstrukcí a prvků v části reléové.

Vlastnosti stavědla ESA 11 odpovídají požadavkům předpisů D1, D2 ČD, základním technickým požadavkům (ZTP) na jednotné obslužné pracoviště (JOP), ZTP na dálkové ovládání a dalším dokumentům ČD. Stavědlo rovněž respektuje existenci místních zvláštností v železničních stanicích u ČD, jako jsou například výhybky ve staničních kolejích, výhybky vybavené kolejovými obvody s nešuntující větví, jednoúsekové posunové cesty přes jediný kolejový obvod a podobně.

Jedno zařízení ESA 11 umožňuje ovládání kolejiště s přibližně 250 výhybkami. Tento údaj je však pouze orientační, maximální počet výhybek závisí například na konfiguraci kolejiště, počtu návěstěných rychlostních stupňů, počtu přejezdů v ovládané oblasti apod.) Ovládaná oblast ovšem nemusí mít nutně charakter jediné železniční stanice - může zahrnovat více stanic, odbočky, nákladiště atd. a stavědlo je schopno pojmout i funkce traťového a přejezdového zabezpečovacího zařízení.

Kolejiště s větším rozsahem lze zabezpečit prostřednictvím dvou nebo více zařízení ESA 11, případně kombinacemi zařízení ESA 11 a SZZ-ETB, přičemž obsluha může být soustředěna pomocí dálkového ovládání DOZ AŽD 1 do jednoho obslužného pracoviště, a to bez jakýchkoliv funkčních omezení. Systém ESA 11 je schopen připojení k dálkovému ovládání DOZ AŽD 1 a buď jeho prostřednictvím anebo přímo i propojení s již existujícími řídicími a informačními počítačovými aplikacemi ČD, například s ISOŘ, CEVIS, MIS atd. To je umožněno schopností systému ESA 11 zobrazovat (přenášet) čísla vlaků při jejich pohybu v kolejišti.

Diagnostika systému je nedílnou součástí každého zařízení ESA 11. Obsahuje archiv událostí, z něhož lze zpětně kontrolovat činnost zařízení i obsluhy. Využít lze i k vyhledávání příčin poruch zařízení a k lokalizaci vadných dílů. Nadstavbou diagnostiky systému je diagnostika měřicí, která není povinnou součástí systému a zřizuje se podle požadavků uživatele.

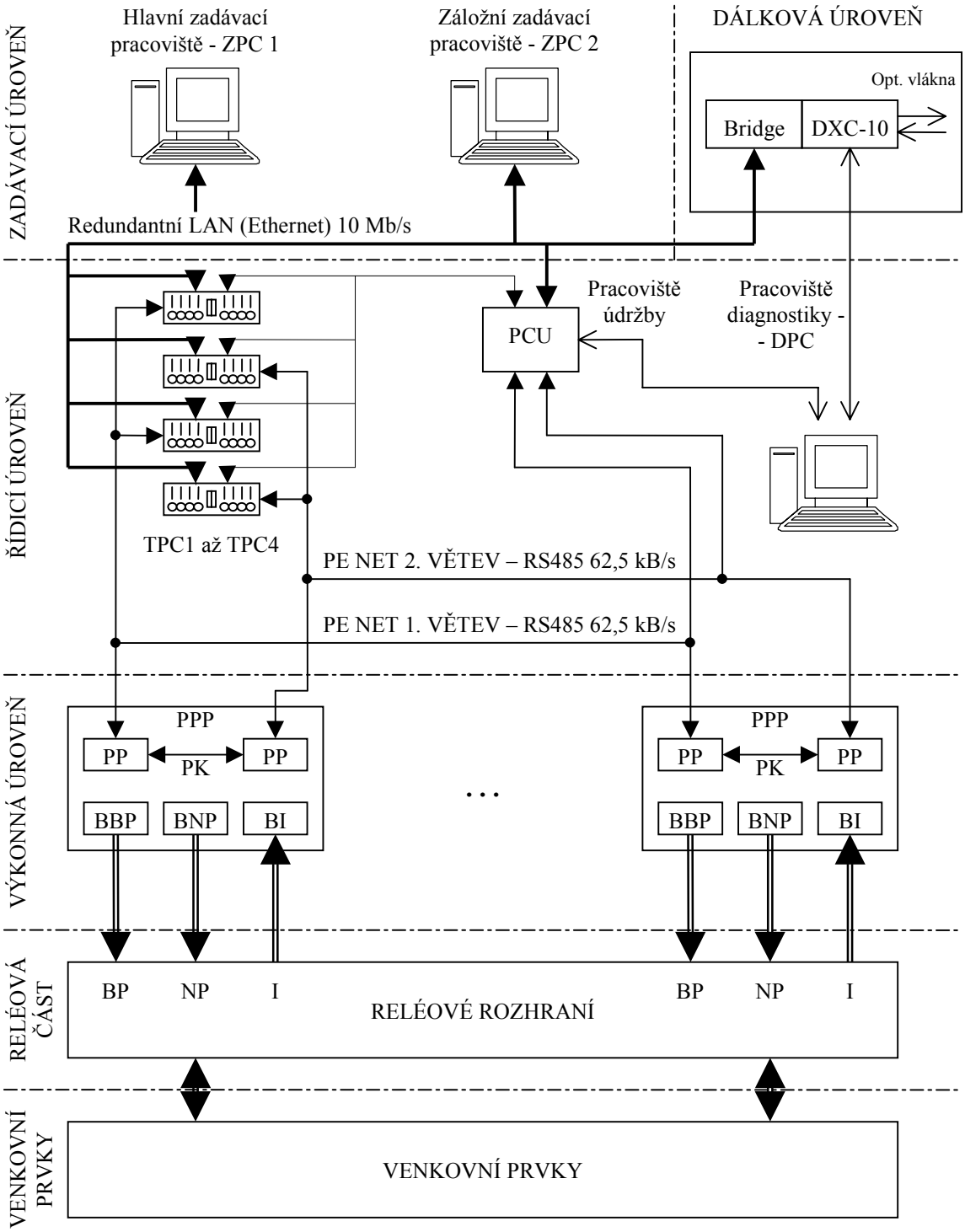
Elektronické stavědlo ESA 11 se skládá z těchto základních částí (obr. 8): z řídicí úrovně, ze zadávací úrovně, z dálkové úrovně, z výkonné úrovně, z reléového rozhraní k venkovním prvkům a k jiným reléovým zabezpečovacím zařízením a také z rozhraní k vlakovému zabezpečovači. Za součásti ESA 11 lze považovat i technickou diagnostiku a napájení.

1.5.2 Řídicí úroveň

Řídicí úroveň představuje vlastní počítačové jádro stavědla - organizuje činnost celého systému, zajišťuje komunikaci s obslužnou, dálkovou a výkonnou částí stavědla, bezpečně vykonává prakticky veškeré logické funkce stavědla (tj. nahrazuje reléové logické obvody SZZ-ETB nebo starších reléových stavědel), archivuje dohodnutá data atd. Je tvořena místní počítačovou sítí, do níž jsou zapojeny čtyři technologické počítače (TPC1 až TPC4). Počítačová síť LAN (Ethernet s komunikačním protokolem AŽD) 10 MB/s je zálohovaná a zapojena do hvězdice, jejímž středem je dvojice rozbočovačů (HUB) SH-E8/230. Technologické počítače jsou kategorie PC Pentium.

Programové vybavení se skládá ze dvou částí: tzv. úrovně ETB (převzaté ze SZZ-ETB a provádějící činnosti, které již u stavědla SZZ-ETB zajišťovala bezpečná počítačová část v řídicí úrovni) a tzv. úrovně ESA (nové části programu, která nahrazuje logické funkce reléové části). Takto byly využity již dříve vytvořené programové moduly, které zajišťují například komunikaci s obslužnými pracovišti, včetně bezpečného zadávání nouzových povelů a bezpečného zobrazování, komunikaci s výkonnou a dálkovou úrovní.

TPC1 a TPC3 jsou vybaveny operačním systémem MS-DOS, program je psán v jazyku C++ Borland. TPC2 a TPC4 jsou vybaveny WIN NT, program je psán jinou skupinou programátorů v jazyku C++ Microsoft.



Obr. 8: Blokové schéma ESA 11

V programu lze odlišit část všeobecnou, zabývající se vlastními mechanismy činností, které probíhají v počítačové síti stavědla a v jednotlivých PC, část aplikační, popisující zásady činnosti stavědla u ČD, a část adresnou, mající přímý vztah ke konfiguraci kolejiště a s ním spojeným zabezpečovacím zařízením v konkrétní ovládané oblasti. V adresné části se využívá vhodné kombinace dvou základních principů vyhledávání prvků, jichž se týká zamýšlená

operace, například stavění určité vlakové cesty. První princip je založen na vyhledávání podle tzv. stromu, tj. souboru, který popisuje konfiguraci venkovních prvků zabezpečovacího zařízení v kolejišti a umožňuje pro každou zamýšlenou operaci vždy znovu před jejím zahájením vyhledat relevantní prvky. Druhý princip je založený na tabulce, v níž je pevně uveden výčet dotčených prvků pro každou možnou operaci.

Koncepce bezpečnosti je založena na dvojnásobném zpracování dat ve dvou počítačových větvích podle dvou různých a nezávislých programů a na neustálých komparacích aktuálních dat mezi oběma aktivními TPC se zajištěným přechodem do bezpečnějšího stavu při neshodách.

Vysoká dostupnost řídicí úrovně stavědla je založena jednak na úplném zálohování všech jejích částí, jednak na výběru vysoce spolehlivých prvků. Ze čtyř TPC jsou vždy dva aktivní (například TPC1 a TPC2), tzn., že ze sítí Ethernet a PENET, do nichž jsou připojeny, nejenom data přijímají, ale též do těchto sítí svá data vysílají. Další dva TPC jsou záložní (např. TPC3 a TPC4). Tyto stroje data z připojených komunikačních sítí pouze přijímají, jsou proto neustále informovány o aktuálním stavu celého systému a připraveny v případě potřeby ihned a automaticky nahradit aktivní TPC (TPC3 je zálohou pro TPC1, TPC4 pro TPC2) Úplné zálohování se týká i vlastní LAN včetně rozbočovače HUB. Součástí řídicí úrovně stavědla je počítač pracoviště pro údržbu (PCU), který monitoruje stav sítě Ethernet. Klávesnici a monitor lze tlačítkovým přepínačem připojit ke kterémukoliv z technologických počítačů (TPC).

1.5.3 Zadávací úroveň

Zadávací úroveň slouží ke styku zařízení s obsluhou. Je tvořena jednotlivými obslužnými pracovišti, které vyhovují ZTP na JOP. Aktivních obslužných pracovišť může být k jedné řídicí úrovni stavědla připojeno nejvíce pět. Zadávací úroveň byla převzata od SZZ-ETB.

Zadávací pracoviště jsou vystavěna kolem zadávacího počítače ZPC, který je zapojen do LAN stavědla a k němuž jsou dále připojeny jeden až tři barevné grafické monitory, jeden textový monitor, klávesnice, trackball a kontrolní vstup. ZPC je stejné kategorie jako TPC a pracují pod OS DOS, program je psán v jazyku C++ Borland.

Běžné povely jsou zadávány bez potřeby prokazování bezpečnosti, protože všechny bezpečnostní aspekty požadované činnosti stavědla zajistí jeho navazující části. Bezpečnost nouzových povelů je v souladu se ZTP na JOP zajištěna potvrzením povelu obsluhou po předchozím vypsání nesplněných podmínek pro požadovanou činnost. Bezpečnost

zobrazovaní je zajištěna dvojím zobrazením (grafickým a textovým), přičemž, každé z těchto zobrazení je prováděno střídavě z jedné a z druhé větve TPC.

Dostatečné dostupnosti systému ESA 11 je dosaženo zálohováním obslužných pracovišť. Vyžaduje se, aby k systému bylo připojeno vždy o jedno obslužné pracoviště více, než je skutečná potřeba. Toto pracoviště pak plní funkci záložního obslužného stanoviště. Vysoká spolehlivost obslužného pracoviště je zajištěna výběrem spolehlivých prvků.

1.5.4 Výkonná úroveň

Výkonná úroveň je nejnižší úroveň počítačové části stavědla. Dvěma nezávislými komunikačními kanály přijímá povely od řídicí úrovně, kontroluje jejich formální správnost a převádí je (jsou-li splněny další podmínky) na vybuzení bezpečných nebo normálních výstupů. K výstupům jsou připojena relé 1. skupiny bezpečnosti funkce, relé typu NMŠ. Výkonná úroveň dále prostřednictvím bezpečných vstupů snímá polohu kontaktů v reléové části a informace o jejich poloze odesílá opět dvěma nezávislými cestami řídicí úrovni. Výkonná úroveň provádí řadu kontrol, jimiž ověřuje regulérnost a bezpečnost své činnosti. Výsledkem při zjištěných neshodách může být i nevratné odepnutí ohraničené části výkonné úrovně.

Výkonná úroveň je tvořena (stejně jako u SZZ-ETB) dvěma nezávislými sítěmi prováděcích počítačů, které ovládají jednotky vstupů a výstupů. Po konstrukční stránce je prováděcí úroveň tvořena jednotlivými panely prováděcích počítačů (PPP), PPP obsahuje (kromě mechanických dílů, Wago svorek pro připojení vodičů z reléové části a propojovacích kabelů) zásuvné elektronické jednotky uspořádané do tří pater. V nejvyšším patře jsou vedle sebe umístěny dva prováděcí počítače (PPa, PPb), obě nižší patra jsou vyhrazena pro jednotky bezpečných výstupů, normálních výstupů a jednotky bezpečných vstupů a osazují se podle projektu. Při úplném osazení má jeden PPP 24 bezpečných výstupů, 52 normálních výstupů a 120 bezpečných vstupů.

Prováděcí počítač je osazen osmibitovým procesorem fy DALLAS 80C320, 24MHz, paměťmi EPROM 32 kB, RAM 32kB, černou skříňkou 8 kB. Prováděcí počítače PPa jednotlivých panelů PPP jsou zapojeny v jedné síti PENET spolu s TPC I a TPC3. Prováděcí počítače PPb jednotlivých panelů PPP jsou zapojeny v druhé síti PENET spolu s TPC2 a TPC4. Do jedné takovéto dvojice sítí může být zapojeno nejvíce 10 PPP. K technologickým počítačům lze připojit nejvíce 8 dvojic sítí PENET. Počet PPP je tedy omezen na 80, případné větší kolejiště se zabezpečuje dvěma nebo více stavědly se společným ovládáním. Sítě

PENET (RS 485) 62,5 kbit/s se speciálním komunikačním protokolem AŽD jsou realizovány metalickým čtyřvodičovým vedením.

Programy do PPa a do PPb jsou napsány v assembleru dvěma nezávislými skupinami programátorů. Koncepce bezpečnosti PPP je založena na dvojnásobném nezávislém zpracování dat ve dvou počítačích s různým softwarem, na neustálých softwarových komparacích dat mezi PPa a PPb v rámci jednoho PPP a na hardwarové komparaci výstupů z PPa a PPb bezpečným komparátorem, který je součástí jednotek bezpečných výstupů. Koncepce bezpečnosti komunikace v PENET mezi TPC a PPP je založena na dvojnásobné komunikaci po dvou fyzicky různých vedeních a na zabezpečení telegramů cyklickým kódem s generujícím polynomem 16. stupně.

Prvky výkonné úrovně (panely PPP) nejsou zálohovány. Dostatečné dostupnosti se musí dosáhnout odpovídajícími výrobními postupy a výběrem vysoce spolehlivých komponentů.

1.5.5 Reléové rozhraní

Toto rozhraní je tvořeno povelovými relé, která jsou připojena k bezpečným výstupům PPP a svými kontakty spínají výkonové obvody zařízení v kolejišti, a dohlédacími relé, která indikují stav venkovních zařízení. Kromě toho reléová část obsahuje malé množství relé (asi 5 %), která provádějí dílčí logické funkce.

Například reléové rozhraní běžného vjezdového návěstidla je tvořeno jedenácti relé. Je zde pět povelových relé, pět dohlédacích relé a relé DS. Ovšem povelová relé jsou připojena přímo k bezpečným výstupům PPP a počítačová část stavědla svými funkcemi nahrazuje jejich složité závislostní obvody.

Jiným příkladem je reléové rozhraní k přestavníku. Toto rozhraní je tvořeno třemi relé NMŠ a dvěma stykači. Dohlédací část rozhraní tvoří dvě kontrolní relé (KP, KM), povelovou část relé OV (svolení k přestavování) a dva stykače (SP, SM), které ovšem mohou být a jsou připojeny pouze k normálním výstupům PPP. Celkově se ukazuje, že počet relé NMŠ v reléové části ESA 11 klesá asi na 1/3 ve srovnání s počtem relé u SZZ-ETB.

1.5.6 Rozhraní k vlakovému zabezpečovači

Elektronické stavědlo ESA 11 je vybaveno rozhraním k vlakovému zabezpečovači ČD. Počítačová část stavědla vybírá úsek, který má být kódován, kontakty dohlédacích relé světelných návěstidel vybírají příslušný kód. ESA 11 počítá s rozhraním pro navázání na jednotný vlakový zabezpečovač ETCS. ESA 11 je schopno poskytovat veškeré potřebné informace systému automatického vedení vlaku AVV.

1.5.7 Venkovní části zabezpečovacího zařízení

Elektronické stavědlo ESA 11 bylo vyvíjeno přednostně pro použití u ČD. Proto se dbalo na to, aby jej bylo možno bez problémů použít se všemi u ČD běžně používanými typy venkovních zařízení a současně aby zůstala otevřena možnost připojit k ESA 11 i jiné, dosud nezavedené prvky. S ESA 11 lze použít: světelná návěstidla typu AŽD70, elektromotorické přestavníky EP600, snímače polohy jazyků SPJ, jakékoli typy kolejových obvodů a počítačů náprav zavedených u ČD, a dále pomocná stavědla s cestovým stavěním a rovněž elektromagnetické zámky.

ESA 11 lze navázat na jakýkoliv typ traťových a přejezdových zabezpečovacích zařízení, která se vyskytují u ČD. Prostřednictvím ESA 11 lze řídit i části stanic vybavené jinými typy staničních zabezpečovacích zařízení. Při postupné přestavbě stanice lze například s výhodou použít ovládání závislých stavědel s elektromechanickým zabezpečovacím zařízením.

1.5.8 Ostatní

Dálková úroveň

Dálková úroveň u elektronického stavědla ESA 11 obsahuje pouze převodník místní sítě LAN do dálkové WAN (Bridge). Navazující zařízení určené k dálkovému přenosu dat již není součástí stavědla ESA 11. Bezpečnost přenášených dat je zajištěna na úrovni jejich zpracování před vstupem do (a po výstupu z) přenosového zařízení, nevyžaduje tedy žádných speciálních opatření v přenosovém zařízení.

Technická diagnostika

Stavová diagnostika systému je nedílnou součástí stavědla. Zahrnuje archivy událostí v jednotlivých PC a PP a také umožňuje uživatelsky přijatelným způsobem vyhodnotit záznamy z těchto archivů.

Měřicí diagnostika se skládá se z počítače diagnostiky DPC a sítě měřicích ústředen, které jsou rozmístěny na stojanech zabezpečovacího zařízení, v blízkosti míst, kde se nacházejí měřené soustavy (například na stojanech kolejových obvodů nebo v napájecím rozvaděči). Obvykle se měří napájecí napětí, izolační stavy či proudy v kolejovém obvodu nebo kódované smyčce.

1.6 Shrnutí

Elektronická stavědla jsou dalším článkem ve vývoji zabezpečovacích systémů. Umožňují vykonávat složitější funkce než čistě reléové systémy. Použitá diagnostika může často odhalit chybu ještě dříve, než by se projevila v provozu. Zatímco u reléových systémů bylo dosaženo bezpečnosti použitím prvků s vlastní bezpečností, u elektronických systémů je bezpečnost dosažena zdvojením programovatelných částí a neustálými kontrolami dat.

Popisované systémy ESA 11 i K-2002 mají podobnou dvoukanálovou strukturu, spolehlivost je u obou typů zajišťována zdvojením potřebných částí. Elektronické stavědlo ESA 11 je určeno pro větší stanice a patrně obsahuje složitější software, jednodušší K-2002 bylo zamýšleno pro stanice spíše menší.

V současné době je již možné vytvořit čistě elektronické stavědlo, které nebude obsahovat žádná relé. Není to však výhodné vzhledem k velmi vysoké ceně elektroniky se zaručenou vlastní bezpečností. Proto se relé a stykače stále používají pro rozhraní mezi venkovními výkonovými prvky a elektronikou, která naopak zajišťuje převážnou většinu logických funkcí.

Kapitola 2

Návrh softwaru zabezpečovacího zařízení

Nejdříve budou stručně naznačeny požadavky na software a jeho vývoj a bude proveden výběr programovacích technik. Druhá část kapitoly se věnuje seznámení s obvyklými požadavky pro řízení železničních stanic. Poslední část již bude popisovat navržené řešení řídicích algoritmů a simulačního programu.

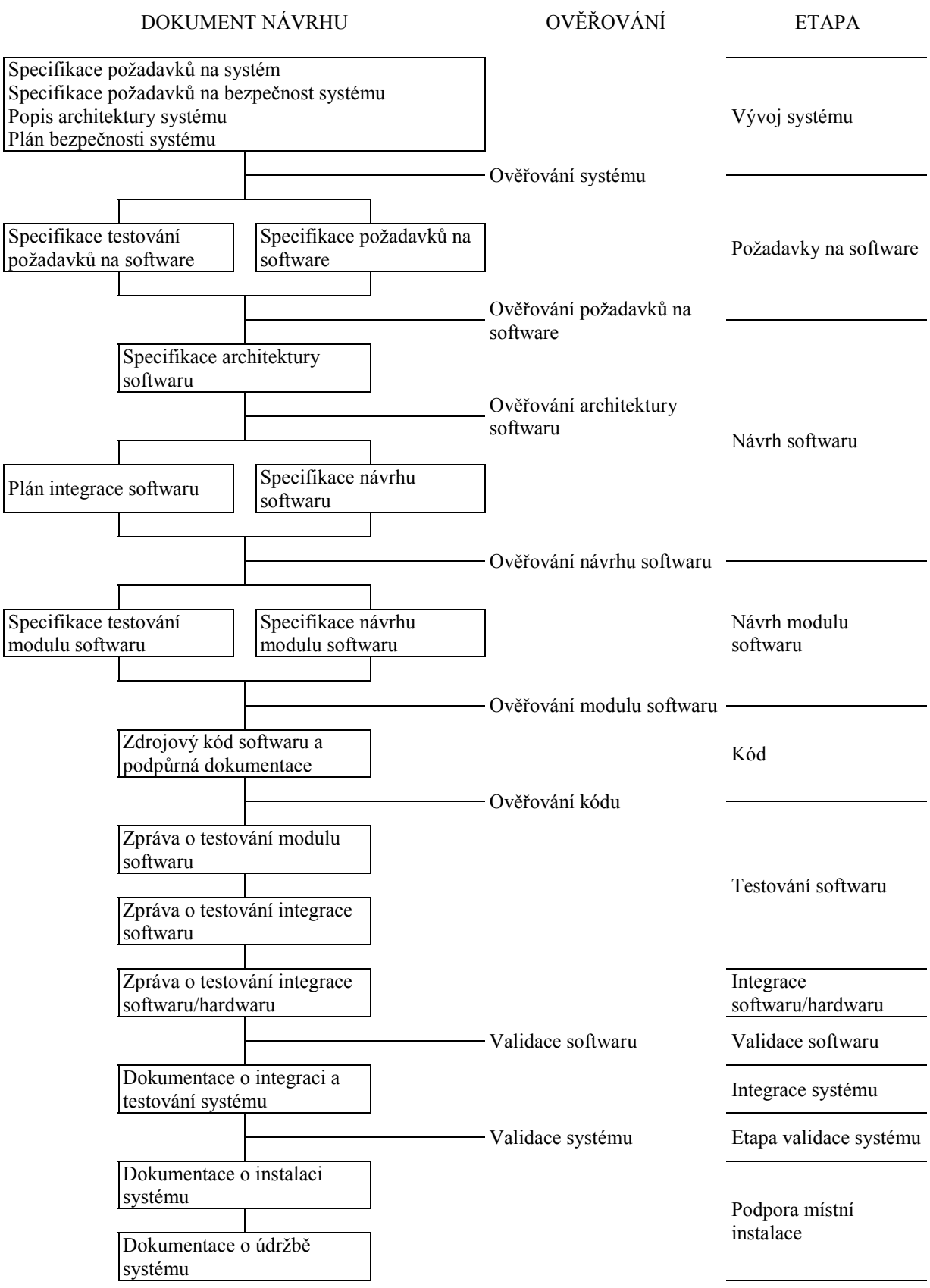
2.1 Bezpečnostní požadavky na software zabezpečovacího zařízení

Současný stav techniky je takový, že ani používání metod zajištění jakosti (tzv. opatření pro zamezení 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 chyb specifikace návrhu. Pro usnadnění návrhu softwaru a umožnění jeho schvalování byla vytvořena norma EN 50 128, která uvádí všechny požadavky na jednotlivé fáze celého životního cyklu softwaru. Tato norma pro vývoj softwaru požaduje především tyto principy:

- metody návrhu shora dolů,
- modularitu,
- ověřování každé etapy životního cyklu vývoje,
- použití ověřených modulů a knihoven,
- jasnou dokumentaci,
- prověřitelné dokumenty,
- validační testování.

Kvůli ztěžování ověřování naopak norma doporučuje se vyhnout:

- nepodmíněným skokům kromě volání podprogramů,
- rekurzi,
- ukazatelům,
- volným oblastem paměti,
- jakémukoliv typu dynamických proměnných nebo objektů,



Obr. 9: Životní cyklus vývoje bezpečného systému

- zpracování přerušení na úrovni zdrojového kódu,
- vícenásobným vstupům nebo výstupům cyklů, bloků nebo podprogramů,
- implicitní inicializaci nebo deklaraci proměnných,
- procedurám jako parametrům.

Téměř všechny bezpečnostní normy předpokládají, že bezpečnost závisí jak na vhodných opatřeních proti systematickým chybám, tak na odpovídajících opatřeních pro kontrolu náhodných poruch. Opatření zaměřená na příčiny chyb a poruch by měla být vyvážená, aby umožňovala dosažení optimální bezpečnostní výkonnosti systému. Pro tento účel byly zavedeny tzv. SILs (Safety Integrity Levels). Stupeň SIL0 nepředpokládá žádnou bezpečnostní funkci, nejvyšší stupeň SIL4 je určen pro systémy s nejpřísnějšími bezpečnostními požadavky (např. střední dobou mezi hazardními stavy přesahující 1000000 roků). Při určování SIL se vychází z analýzy rizik, navržený stupeň je obvykle konzultován se zadavatelem a schvalovatelem. Pro software jsou tyto stupně označovány SWSILs (Software Safety Integrity Levels).

2.1.1 Požadavky na programovací jazyk

Použitý programovací jazyk má v co největší míře podporovat požadavky této normy, zejména defenzivní programování, přísnou typovou kontrolu, strukturované programování a verifikační predikáty a invarianty. Na zvolený programovací jazyk jsou dále kladeny tyto požadavky:

- má vést s minimálním úsilím ke snadno ověřitelnému kódu a usnadňovat vývoj, ověřování a údržbu programu,
- má být plně a jednoznačně definovaný,
- má být spíše uživatelsky nebo problémově než strojově orientovaný,
- přednostně má být použit jazyk (nebo jeho podmnožina), který je používán v širokém měřítku, před jazykem pro speciální účely
- má zajišťovat blokovou strukturu, typovou kontrolu, kontrolu mezí v době provádění programu a kontrolu parametrů,
- má podporovat užívání malých a zvládnutelných modulů, omezení přístupu k datům v definovaných modulech, definici podrozsahů proměnných a jakýkoliv jiný typ konstrukcí omezujících chyby,
- měl by být podporován vhodným překladačem, knihovnami dříve existujících modulů, ladicím programem a nástroji jak pro řízení, tak pro vývoj verze.

Norma nejvíce doporučuje jazyky ADA, MODULA-2, PASCAL, následuje Fortran 77, Podmnožina C a C++ s kódovacími standardy a některé další, naopak nedoporučuje BASIC, PL/M a neomezené C nebo C++. Síla doporučení závisí na zvoleném SIL a roste s omezením jazyka na jeho podmnožinu.

2.1.2 Požadavky na architekturu softwaru

Pro vyšší stupně bezpečnosti jsou schválené určité kombinace vybraných technik. Je možno použít například defenzivní programování spojené s diverzním programováním a použitím detekčních kódů.

Defenzivní programování

Cílem defenzivního programování je vytvářet programy, které zjišťují anomální tok řízení, tok dat nebo hodnoty dat během jejich provádění a reagovat na ně předem stanoveným způsobem. Při programování může být použito více technik pro kontrolu anomálií. Mohou být používány systematicky během programování systému pro snižování pravděpodobnosti chybného zpracování dat. Software by měl být odolný vůči vlastním chybám, aby bylo možné odstranit nedostatky jeho návrhu. Tyto nedostatky mohou být způsobeny zřejmou chybou návrhu nebo kódování, anebo chybnými požadavky.
Mezi defenzivní techniky patří například:

- kontrola hodnot proměnných, zda jsou v požadovaném rozsahu,
- kontrola smysluplnosti hodnot, pokud je to možné,
- kontrola parametrů procedur na jejich vstupech – jejich typ, rozměr a to, zda jsou v rozsahu.

Tyto techniky pomáhají zjistit, zda jsou čísla manipulovaná programem smysluplná – jak z hlediska funkce programu, tak z hlediska fyzického významu proměnných.

Diverzní programování

Cílem programování různými postupy je maskování zbytkových vad návrhu softwaru během zpracovávání programu. To umožňuje zabránit poruchám systému kritickým z hlediska jeho bezpečnosti a pokračovat v činnostech za účelem dosažení vysoké bezpečnosti.

Specifikace daného problému je realizována N-krát rozdílnými způsoby. N verzím jsou dány stejné vstupní hodnoty a výsledky vytvořené N verzemi jsou porovnány. Je-li výsledek považován za platný, je přenesen do výstupů počítače. Těchto N verzí může probíhat

paralelně na samostatných počítačích, alternativně mohou všechny verze probíhat na tomtéž počítači a výsledky mohou být podrobeny vnitřnímu rozhodování.

Má-li systém bezpečný stav, je možné požadovat úplnou shodu všech N výsledků, jinak je použita výstupní hodnota zabezpečená proti poruchám. Tato technika neeliminuje zbytkové vady návrhu softwaru, zajišťuje však opatření pro jejich detekci a maskování dříve než ovlivní bezpečnost.

2.2 Požadavky na funkci staničního zabezpečovacího zařízení

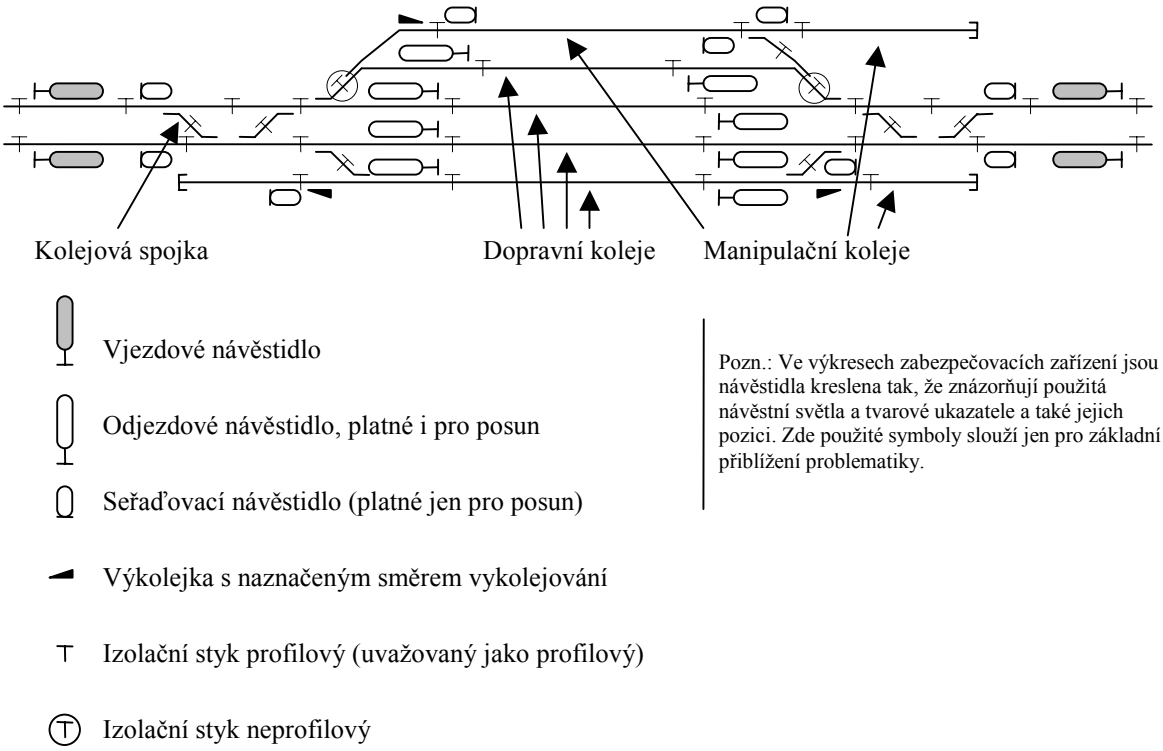
Požadavky na staniční zabezpečovací zařízení jsou uvedeny v TNŽ 34 2620. Tato norma se zabývá správným umístěním jednotlivých zabezpečovacích prvků v kolejišti, jejich funkcí i funkcí zabezpečovacího zařízení jako celku. Její znalost je klíčová pro správný návrh řídicího systému SZZ. Požadavky na uživatelské rozhraní a některé další funkce, které má řídicí systém zajišťovat, jsou uvedeny v základních technických požadavcích pro jednotné obslužné pracoviště (ZTP JOP).

Základní funkce SZZ

Na obr. 10 je zjednodušeně naznačeno SZZ smyšlené ŽST na dvoukolejné trati. Vjezd do stanice je dovolován vjezdovým návěstidlem, následuje úsek pro posun ohraničený seřaďovacím návěstidlem a dále zhlaví, na kterém se trať rozvětvuje do několika staničních kolejí. Na dopravní koleje může přijet vlak z širé trati, také z nich může odjíždět. Na manipulační kolej a z ní je povolen jen posun, nikoliv jízda.

Zabezpečený provoz se ve stanici řídí tzv. stavěním jízdních cest. Vlakové cesty začínají vždy u hlavního návěstidla (tj. vjezdového, odjezdového či cestového – to v tomto jednoduchém příkladu není použito) a končí buď na dopravní koleji, nebo na koleji širé tratě. Posunové cesty začínají u návěstidla platného pro posun (tj. seřaďovacího, obvykle také odjezdového či cestového) a končí buď na některé dopravní či manipulační koleji, anebo v úseku mezi zhlavím a vjezdovým návěstidlem. Někdy topologie zhlaví umožňuje vést cestu více způsoby – potom je jedna cesta (obvykle ta nejpřímější) považována za základní a ostatní jsou variantní. Základní cestu lze tedy jednoznačně definovat jejím typem, počátkem a koncem, variantní cestu navíc zvoleným bodem, přes který odlišně vede (případně více body, pokud je jich pro jednoznačnost třeba uvést více). Určitou vlakovou cestu lze postavit pouze tehdy, jsou-li prvky zabezpečovacího zařízení v předepsaném stavu, který je definován tzv. závěrovou tabulkou. Tato tabulka je nedílnou součástí projektu konkrétního SZZ. Závěrová

tabulka dále uvádí pro každou jízdní cestu všechny možné kombinace návěstí a současně vyloučené jízdní cesty. Pro přehlednost nejsou v závěrové tabulce uváděny požadavky zajišťované základním provedením zabezpečovacího zařízení, např. volnost všech úseků ve stavěné cestě až po následující hlavní návěstidlo, vyloučení současného postavení cest se společným výhybkovým úsekem, atd. Po splnění podmínek daných závěrovou tabulkou provede SZZ závěr jízdní cesty a teprve poté může postavit příslušné návěstidlo na dovolující návěst. Postavená jízdní cesta je postupně vybavována až projetím vlaku kontrolním místem, například uvolněním úseku po obsazení úseku sousedního.



Obr. 10: Typické zabezpečení železniční stanice, vybrané základní prvky SZZ

Provedení izolovaných úseků má umožňovat současné postavení co největšího počtu jízdních cest, který umožňuje topologie zhlaví. Často je třeba zřizovat izolované styky, jejichž poloha neodpovídá průjezdnímu průřezu (tzv. neprofilové styky). Při zjišťování volnosti úseků stavěné jízdní cesty se potom musí zjišťovat i volnost sousedních neprofilových úseků. Tyto požadavky jsou již zahrnuty v závěrové tabulce.

Výjimkou jsou styky na kolejových spojkách. Jejich poloha je sice neprofilová, ale pracuje se s nimi jako s profilovými. Obě výhybky kolejové spojky se totiž musí přestavovat současně, při přestavování nesmí být ani jedna z nich obsazená. Pokud je kolejová spojka

postavena do polohy umožňující postavení souběžných cest, nemůže dojít k bočnímu ohrožení, protože vlastní spojka nemůže být obsazena (vytváří oboustrannou přímou boční ochranu). V případě, že je přestavena do polohy umožňující jízdní cestu po spojce, jsou z podstaty kontrolovány na volnost oba izolované úseky. Kolejovou spojku tvoří vždy jen dvě závislé výhybky.

2.3 Popis navrženého řešení

Z uvedených požadavků je zřejmé, že návrh celého systému SZZ by silně přesahoval rámec této práce. Proto jsem zcela pominul návrh hardwaru a zaměřil jsem se pouze na malou část softwaru, konkrétně na vytvoření dvou odlišných algoritmů pro řízení zhlaví ŽST, algoritmů pro zlepšení možností ovládání (rozšíření ZTP JOP) a na vytvoření simulačního prostředí, ve kterém by mohla být ověřena jejich funkčnost. Aplikace si neklade za cíl být zcela bezpečnou, především má sloužit pro ověření postupů, které by mohly být v jiném, skutečně bezpečném softwaru použity.

2.3.1 Výběr techniky návrhu a programovacího jazyka

Podle mého názoru je pro tuto aplikaci velmi vhodný objektově orientovaný návrh, který umožňuje rozložit celé zabezpečovací zařízení na jednotlivé prvky s jasně popsaným chováním a umožní aplikaci snadno rozšiřovat. Objektově orientovaný způsob programování (OOP) zpřehledňuje zdrojový kód, což usnadňuje jeho kontrolu, a také umožňuje větší kontrolu přístupu k datům. Tyto a další vlastnosti OOP jsou v duchu požadavků na bezpečné systémy velmi příznivé. Další silnou stránkou OOP je dědičnost s možností vytváření virtuálních funkcí. Jejich využití úzce souvisí s používáním ukazatelů, které naopak normy doporučují omezit, především kvůli snadnější kontrole. Proto jsem s ukazateli pracoval jen tam, kde to bylo účelné. Jejich použitím se přehlednost kódu nezhoršila, spíše naopak. Použití dynamických proměnných není v řídicích algoritmech nutné, pokud je konfigurace SZZ předem pevně dána (a to v praxi je). Vzhledem k zamýšlené univerzálnosti vytvářeného programu jsou některé objekty dynamicky alokovány, ale stejné algoritmy by bylo možné použít i pro statická data.

Pro implementaci jsem zvolil jazyk C++, vývojové prostředí Microsoft Visual C++ 6.0 a jemu příslušné standardní knihovny. Kód v jazyce C++ lze napsat strukturovaným způsobem, který omezuje možnosti vzniku chyb a případně vzniklé chyby umožňuje snadněji nalézt. Může být ale také napsán ve velmi zhuštěné podobě, která naopak velmi zvyšuje

pravděpodobnost výskytu chyb a ještě navíc ztěžuje jejich hledání. Například při testování podmínky `if ((ei == 11) || si++)` nemusí vždy dojít k inkrementaci proměnné `si`, což pravděpodobně nebylo záměrem programátora. Tento způsob se nedoporučuje používat ani v jiných systémech.

Častou chybou bývá zapomenutí zdvojení „=“ v Booleovských výrazech, obecně záměna relačního operátoru za přiřazovací. Tyto a další časté chyby lze odstranit překladačem, který pracuje s jistou podmnožinou jazyka. Pokud takový překladač nalezne např. přiřazení v Booleovském výrazu, oznámí porušení pravidla kódování. Příkladem je MISRA C, který zahrnuje 127 pravidel omezujících standardní jazyk C. Zdrojový kód se potom přibližuje programovacím jazykům ADA či Pascal, což vyhovuje normě EN 50 128.

Navržené algoritmy by bylo možné implementovat i v jiném jazyku, a to bez významných změn. Dokonce by bylo výhodné mít každý z diverzních programů napsaný v jiném jazyce, aby se opět snížilo riziko chyby. Přinejmenším by měl být na každou větev použit překladač od jiných tvůrců.

2.3.2 Popis funkce aplikace

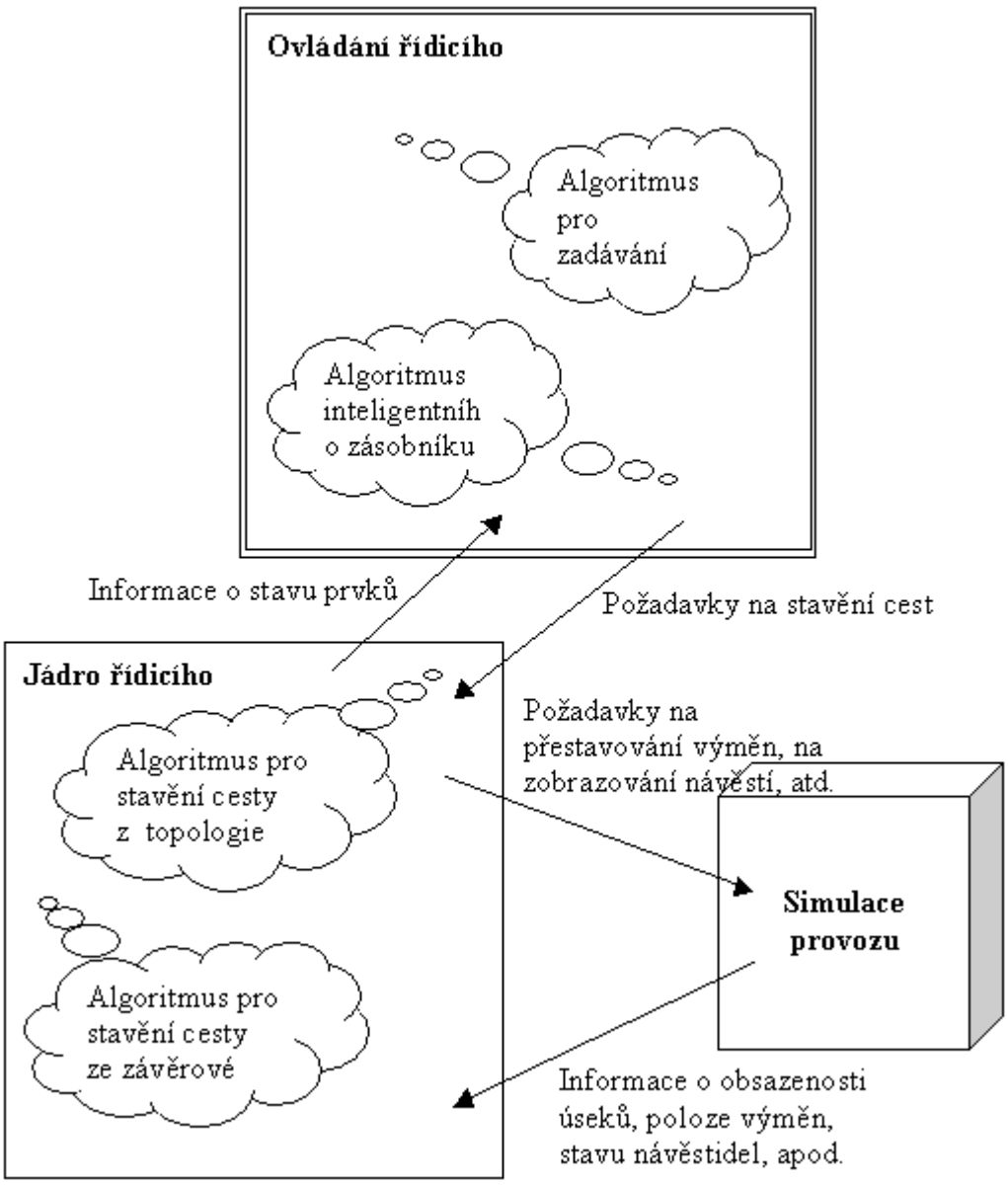
Aplikaci tvoří tři hlavní části:

- ovládání řídicího systému,
- jádro řídicího systému,
- simulace železničního provozu.

Blok „Ovládání řídicího systému“ vytváří rozhraní mezi vlastním systémem a uživatelem. Je navržen podle požadavků na JOP, navíc obsahuje dvě navržená vylepšení pro usnadnění řízení provozu. Jeho úkolem je především zobrazovat stav SZZ a převádět požadavky uživatele do formy požadované jádrem systému.

Jádro řídicího systému zajišťuje vlastní bezpečnostní funkce SZZ, k dosažení většího stupně bezpečnosti používá dva rozdílné algoritmy. Tyto algoritmy pracují s jinými konfiguračními daty, což významně zvyšuje pravděpodobnost odhalení chyby v těchto datech. První algoritmus vychází z úplné závěrové tabulky, druhý z topologie železniční stanice.

Blok simulace slouží pouze k ověření vlastností předchozích částí. Modeluje skutečný provoz na železnici, především jízdy vlaků.

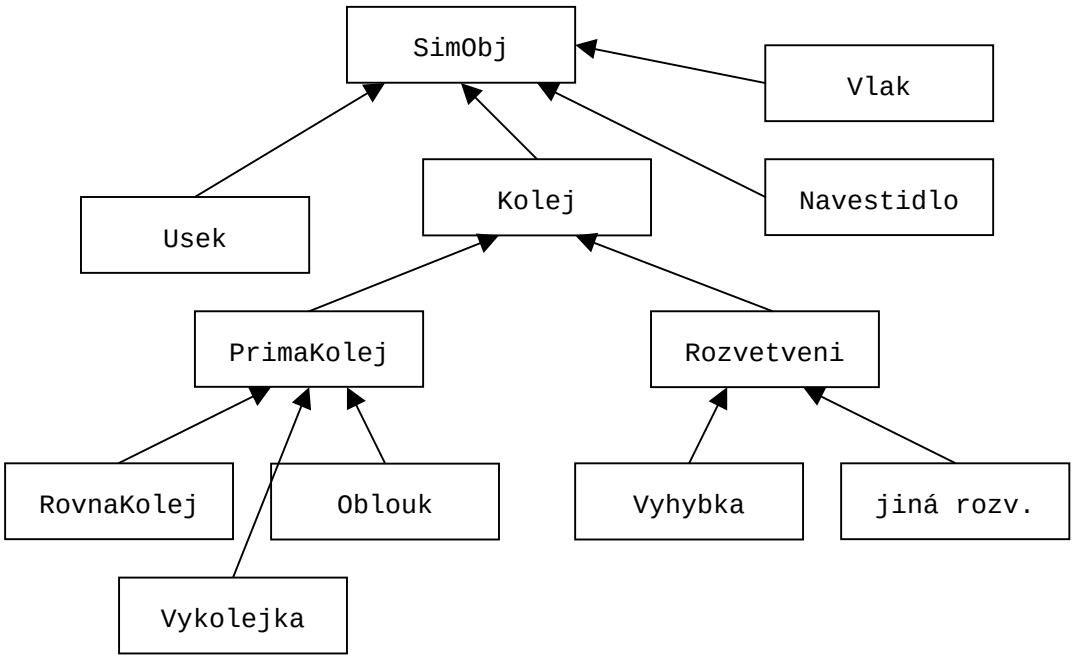


Obr. 11: Významné části aplikace a toky informací mezi nimi

2.3.3 Simulace

Simulační část má modelovat skutečný provoz. Její základ musí být dostatečně obecný, aby ji bylo možné postupem času rozšiřovat o další prvky a jinak vylepšovat. Pro snadnou kontrolu její funkce (a také funkce řídicí části) musí umožňovat reálný pohled na dopravní situaci. Pro její vytvoření se tak přímo nabízí objektově orientovaný návrh. Jeho základem je hierarchie tříd prvků skutečné železnice. Myšlenka a základní chování objektů pochází od R. Káldyho. Tento základ po některých úpravách zajišťoval pouze pohyb vlaku po trati konstantní rychlostí. Proto jsem jej dále upravil a rozšířil, především o automatické řízení

pohybu vlaků (zrychlování a zpomalování podle maximální rychlosti na trati a návěstěné rychlosti) a o grafickou reprezentaci.



Obr. 12: Hierarchie tříd simulace

Základní třídou je `SimObj`. Tato třída deklaruje virtuální metody `Krok()` a `NakresliSe()` a vlastnost `Typ` pro identifikaci. Všechny ostatní třídy jsou od ní odvozené. To umožňuje snadné vykreslování a běh simulace. Běh simulace se odehrává po diskrétních konstantních časových okamžicích, v každém kroku je vypočítán a poté vykreslen nový stav.

Železniční síť tvoří potomci třídy `Kolej`. Každý zná své sousedy na trati, například `Vyhybka` má sousedy tři. Každý potomek třídy `Kolej` má seznam vlaků, které jej obsazují (obvykle jeden nebo žádný), takže lze snadno vyhodnotit jeho volnost . Potomci dále obsahují údaj o délce a maximální rychlosti, na které se při pohybu dotazuje `Vlak`. `PrimaKolej` je kolej se dvěma konci, na kterých může být `Navestidlo`. `RovnaKolej` a `Oblouk` se liší jen ve vykreslování, `Vykolejka` má navíc metodu pro sklápění. `Rozvetveni` se liší od třídy `PrimaKolej` tím, že má jiné metody na oznamování sousedů (může mít až 4 sousedy) a také tím, že na něj (pro jednoduchost) nelze navázat žádné návěstidlo. `Vyhybka` má metody pro přestavování, ostatní druhy rozvětvení jsem zatím neuvažoval. `Navestidlo` se může vázat k přímým kolejím a slouží pro ovládání pohybu vlaků, omezuje v daném směru jejich rychlost. `Usek` je spíše pomocný objekt, který pouze indikuje obsazenost dané skupiny instancí (potomků) třídy `Kolej`.

Obr. 13: Grafická reprezentace simulovaného kolejiště

`Vlak` má seznam kolejí, které obsazuje, a údaje o tom, jaká vzdálenost mu chybí do konce koleje (čelu vlaku i konci vlaku). Při pohybu vlaku vpřed se tyto vzdálenosti zmenšují a když jsou záporné, vlak obsadil další kolej (popř. opustil poslední). V tu chvíli je třeba opravit údaje o obsazení kolejí a také o rychlosti. Vlak zjistí z obsazených kolejí maximální rychlost, kterou může jet. Dále musí nalézt místo na trati, které bude jeho rychlost při další jízdě omezovat. Pokud takové místo existuje, musí jej respektovat a začít včas zpomalovat. Vlak se snaží dosáhnout maximální dovolené rychlosti, kterou mu umožňují omezení na trati. Pro pohyb vlaku jsem zvolil nejjednodušší model s konstantním zrychlováním a zpomalováním.

2.3.4 Jádro řídicího systému

Úkolem jádra řídicího systému je monitorování stavu prvků v kolejišti, zjišťování možnosti stavění cest požadovaných zadávací částí, v případě splnění požadavků jejich stavění a následné vybavování při průjezdu vlaku. Stavění cest zahrnuje také ovládání návěstí a výměn.

Pro postavení cesty je třeba správně určit všechny dotčené prvky a jejich požadovaný stav. K tomuto účelu využívá systém dva níže popsané algoritmy. Vstupem obou algoritmů je druh, počátek, konec a případně variantní body požadované jízdní cesty, výstupem je seznam dotčených prvků s uvedeným požadovaným stavem (případně více možnými stavy, pokud to dovolují předpisy) a možnost postavení jízdní cesty při jejich aktuálním stavu. Při neshodě jejich výsledků nedojde k provedení požadované akce a systém upozorní obsluhu varovnou zprávou. Při shodě systém vybere ty prvky, které je možné v danou chvíli přestavit (není u nich proveden závěr) a pokud je možné již cestu postavit, provede závěr jízdní cesty a příslušné návěstidlo postaví na DN. Postavenou cestu si zapamatuje a vytvoří závislosti mezi prvky s touto cestou souvisejícími, aby mohl po průjezdu vlaku odstraňovat závěry, rušit DN a reagovat na neočekávané obsazení některého úseku.

Mimo to řídicí systém v každém kroku monitoruje stav návěstidel a upravuje jejich návěsti podle vzniklých závislostí. Například při postavení vjezdové cesty na přímou staniční kolej se na vjezdovém návěstidle rozsvítí návěst „Výstraha“. Po prodloužení cesty (tedy postavení pokračující přímé odjezdové cesty) se změní tato návěst na „Volno“. Systém v každém kroku také ruší projeté jízdní cesty nebo jejich části.

Algoritmus vycházející ze závěrové tabulky

Tento způsob vychází z tabulek vlakových a posunových cest, ve kterých jsou zadána data podle následujícího vzoru, který představuje jednu zadanou položku v tabulce:

Počátek cesty	Variantní bod	Konec cesty	Návěstidlo na počátku cesty	Závislost na dalším návěstidle	Prvek 1	Prvek 2	...	Prvek *N*
			návěstěná rychlost	zkrácená zábrzdná vzdálenost	role prvku 1	role prvku 2		role prvku *N*

Algoritmus pouze rozhodne, jestli se jedná o vlakovou nebo posunovou cestu, a v příslušné tabulce se pokusí cestu nalézt. Nenalezení řádku znamená nesrovnalost mezi zadanou tabulkou a schématem v bloku ovládání. Ta by měla být poté jejím tvůrcem odstraněna. Algoritmus ještě vyhodnotí možnost postavení této cesty tak, že porovná skutečný stav jednotlivých prvků 1 až *N* se stavem požadovaným. Tento výsledek spolu se seznamem prvků a jejich požadovaným stavem[1] je výstupem tohoto algoritmu. Pořadí prvků v závěru tabulky odpovídá jejich pořadí ve stavěné jízdní cestě.

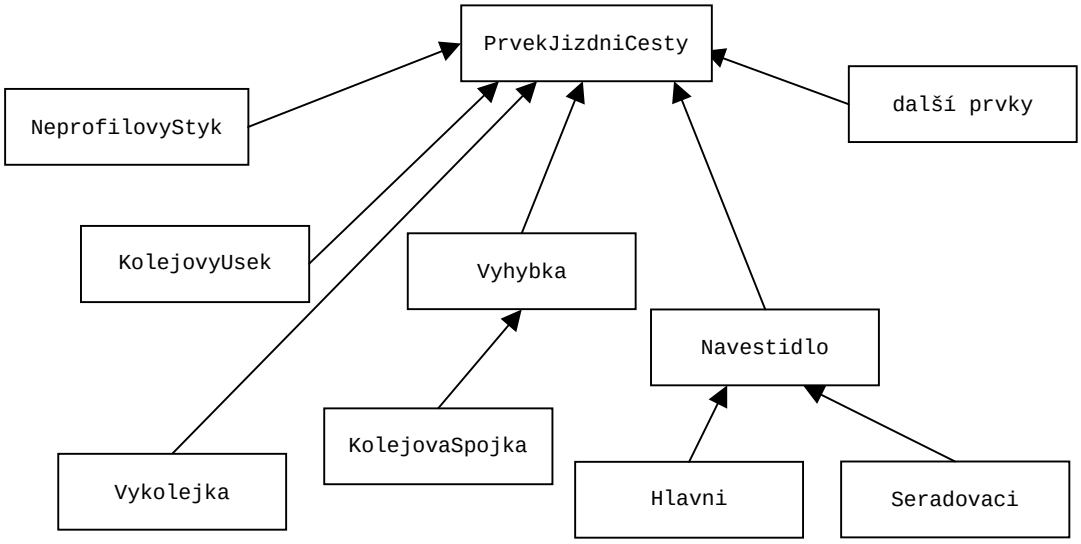
Algoritmus vycházející z topologie (schématu) stanice

Základem tohoto algoritmu je hierarchie vhodně navržených tříd objektů, z nich sestavené schéma stanice a transformace normou stanovených požadavků na stavění cest do pravidel algoritmu. Nalezení prvků dotčených cestou je založeno na prohledávání grafu.

Nejdříve nalezneme prvky v dané cestě pojížděné, a to metodou prohledávání do hloubky. Možný způsob je popsaný v následující kapitole u zadávání jízdních cest.

Cestu hledáme postupně přes variantní body až k jejímu koncovému úseku. Všechny prvky ležící na této nalezené cestě musí být volné, bez závěru jízdní cesty. Požadovaná poloha pojížděných výměn a výměn na kolejových spojkách je dána přímo směrem nalezené cesty. Výjimku tvoří koncový úsek posunové cesty, který může být obsazený nebo pod závěrem opačné posunové cesty (pokud je delší než 100 m). Z nalezené cesty lze také určit její skutečnou délku a tak rozpoznat případnou zkrácenou zábrzdnou vzdálenost.

[1] Požadovaný stav je zahrnut v položce „role prvku *i*“, kde je také uvedeno, zda se na požadovaný prvek vztahuje závěr případně postavené cesty.



Obr. 14: Hierarchie tříd používaných pro stavění jízdních cest.

Navíc je třeba zajistit boční ochranu a zkontrolovat volnost úseků sousedících přes neprofilové izolační styky. U každé samostatné výhybky ležící na jízdní cestě se prohledává její nepojížděná větev, přičemž při každém dalším rozvětvení se pokračuje v prohledávání obou větví. Prohledávání oblasti boční ochrany výhybky končí u:

- výhybky, kterou lze uzavřít v odvratné poloze (toto uzavření totiž nesmí znemožnit postavení jiné dovolené jízdní cesty),
- návěstidla platného pro opačný směr jízdy,
- výkolejky.

Pro postavení vlakových cest musí být všechny ostatní úseky v prohledávané oblasti boční ochrany volné, připouští se též jejich souvislé obsazení až na staniční kolej při současném závěru vjezdové jízdní cesty. Při stavění posunových cest na obsazenosti nezáleží.

Seznam prvků z oblasti boční ochrany je následně setříděn, jsou vypuštěny duplicitní požadavky a je zkontrolována souhlasnost všech požadavků. Výsledek je zanesen do tabulky shodné s výstupem předchozího algoritmu.

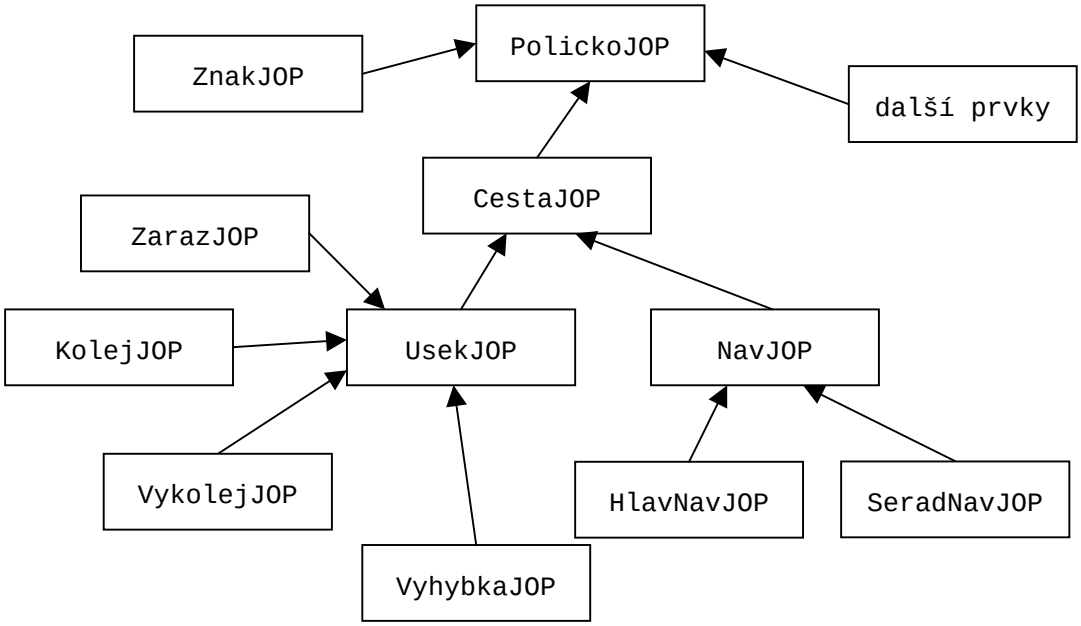
2.3.5 Blok ovládání řídicího systému

Tento blok zajišťuje komunikaci s obsluhou. Při jeho vytváření jsem se zaměřil na takový způsob zobrazení prvků kolejiště, který by umožňoval snadné zadávání jízdních cest. Zároveň jsem se snažil vyhovět požadavkům na JOP. Pro zobrazení jsem zvolil čtvercovou mřížku, která je při otáčení prvků pro vizualizaci výhodnější.

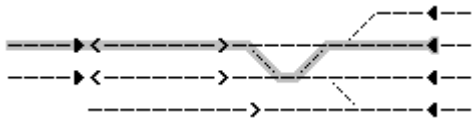
Zadávání jízdních cest

K ovládání řídicího systému stanice se používá myš se třemi aktivními tlačítky. Levé tlačítko myši slouží k vyznačení začátku vlakové cesty a konce vlakové i posunové cesty. Střední tlačítko myši slouží při jednoduchém stisknutí k vyznačení začátku posunové cesty a variantního bodu. Pravé tlačítko myši slouží k rušení posledního provedeného úkonu, druhým stiskem pravého tlačítka lze zrušit celou volbu. Postupně volené jednotky jízdní cesty jsou od okamžiku vyznačení do uplynutí 5 s od ukončení volby konce cesty zvýrazněny zeleným (u vlakových cest) nebo bílým (u cest posunových) pozadím. V případě rozsvícení návěstidla začátku cesty, zrušení povelu nebo volby další cesty je vyznačení odmazáno okamžitě. Postavená jízdní cesta musí být vyznačena příslušnou barvou souvisle v celé délce mezi návěstidly začátku a konce cesty.

Při stavění variantních cest je běžně požadováno stisknutí středního tlačítka na předem určeném variantním bodu. Celá cesta se zvýrazní až po zadání koncového bodu. Rozhodl jsem se zadávání i zobrazování vylepšit takto: středním tlačítkem může být zvolen variantní bod na kterémkoliv políčku a cesta se až k tomuto bodu zvýrazní okamžitě. Zároveň jsem upravil způsob zvýraznění tak, aby bylo opticky dokonalejší. K těmto účelům slouží hierarchie políček JOP.

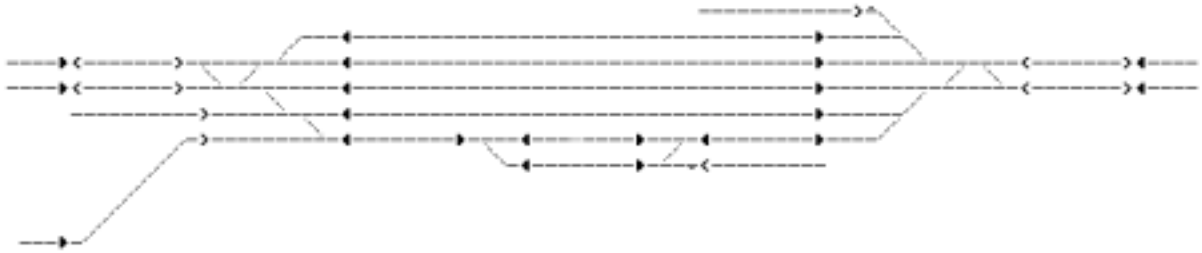


Obr. 15: Hierarchie tříd uživatelského rozhraní



Obr. 16: Vykreslení variantní cesty

`PolickoJOP` je společný předek všech tříd. Má implementovány základní metody pro zobrazování kurzoru. Jeho potomek `ZnakJOP` má předefinovanou metodu `NakresliSe()` tak, aby mohl zobrazovat grafické znaky. `CestaJOP` je abstraktní předek pro políčka, která mohou vyhledávat a zobrazovat stavěné cesty. Pro tuto funkci mají ukazatele na své sousedy v lichém a sudém směru stavěných cest. `NavJOP` je abstraktní předek pro hlavní i seřaďovací návěstidla. Zavedení této třídy umožnilo do jisté míry sjednotit práci s vlakovými a posunovými cestami. Třídy `HlavNavJOP` a `SeradNavJOP` již zajišťují kreslení značky návěstidla příslušného typu a obsluhují volby počátku cest. `UsekJOP` je abstraktní třída pro políčka, která zobrazují stav volnosti, obsazenosti nebo závěrů cest. `ZarazJOP` a `KolejJOP` se liší jen ve vykreslování, zarážedlo má (stejně jako krajní kolej širé tratě) jeden ukazatel na souseda v cestě nulový, takže u něj končí prohledávání cest. `VykolejJOP` zobrazuje stav výkolejky. `VyhybkaJOP` má navíc od ostatních prvků ještě jeden ukazatel na souseda ve směru do odbočky. Výhybka je klíčová pro vyhledávání cest.



Obr. 17: Návrh JOP pro stanici Rudoltice v Čechách

Pro vyhledávání cesty je zapotřebí znát návěstidlo na počátku cesty (tím je dán i směr cesty), koncový (popř. i variantní) bod a mít k dispozici zásobník na výhybky dostatečné velikosti a ukazatel `ZkoumanePole`, který na počátku ukazuje na počáteční návěstidlo. Začínáme s prázdným zásobníkem. Dále pokračujeme podle tohoto algoritmu:

1. pokud je `ZkoumanePole` výhybka proti hrotu, vlož ji do zásobníku
2. `ZkoumanePole` := soused od `ZkoumanePole` ve směru cesty

3. pokud je `ZkoumanePole` = `NULL`, jdi na bod 6.
4. pokud `ZkoumanePole` = koncový bod → konec, cesta nalezena
5. jdi na krok 1.
6. zásobník prázdný → konec, cesta nenalezena
7. vyjmi výhybku ze zásobníku a polož `ZkoumanePole` = soused této výhybky do odbočky
8. jdi na krok 1.

Poznámky:

- „výhybka proti hrotu“ znamená, že ve směru cesty je možné volit na výhybce jízdu rovně či odbočení
- „soused ve směru cesty“ pro výhybky proti hrotu je sousední pole směrem „rovně“
- `NULL` je hodnota pro neexistujícího souseda, například u zarážedla

Pokud algoritmus cestu nalezne, můžeme jí zrekonstruovat tak, že procházíme postupně políčka od počátečního návěstidla a když nalezneme výhybku proti hrotu, která není v zásobníku, pokračujeme po ní do odbočky. Cestou si zapamatujeme variantní body, abychom pode nich mohli určit cestu ze závěrové tabulky.

Zásobník povelů

Nalezené jízdní cesty jsou ukládány do zásobníku povelů. Zásobník povelů je v jazyku výpočetní techniky kontejner, který se chová v základním režimu (vydávání povelů ze zásobníku) jako fronta, při volbě přednostní jízdní cesty jako zásobník. Povely se odebírají ze stále stejného konce kontejneru. Dále budu pro tento kontejner používat, ve shodě s JOP, termín zásobník povelů. K požadovaným dvěma režimům jsem navrhnul vylepšení, které jsem označil jako „inteligentní stavění cest“. V zásobníku povelů jsou často blokovány některé cesty, které by bylo možné postavit ihned, aniž by to ovlivnilo stavění zbylých cest ze zásobníku povelů. Pro vyhledání těchto cest platí toto pravidlo: Pokud je možné postavit cestu současně se všemi cestami, které se před ní nacházejí v zásobníku povelů, lze ji začít stavět ihned (jsou-li splněny běžné podmínky pro její postavení). Toto navržené inteligentní stavění cest by mělo spojit méně náročné ovládání s kratšími prostoji vlaků, obzvláště při řízení náročnějších dopravních situací.

Kapitola 3

Ověření navrženého řešení

Funkčnost navrženého řešení byla ověřována při řízení provozu na počítačovém modelu skutečné železniční stanice Rudoltice v Čechách (viz obr. 17). Jde o stanici střední velikosti na hlavní dvoukolejné trati Česká Třebová – Přerov, ve které je napojena místní vedlejší trať do Lanškrouna. Stanice má 20 výhybek a 6 dopravních kolejí, z nichž jsou 2 opatřeny cestovými návěstidly. Závěrová tabulka obsahuje 60 vlakových cest a 74 cest posunových.

Nejdříve bylá správně zadána celá závěrová tabulka a vytvořena bezchybná reprezentace prvků kolejiště se zanesením jejich skutečné topologie (vzájemné návaznosti). Poté byly postupně stavěny všechny vlakové i posunové cesty. V tomto případě nedošlo k zaznamenání rozdílnosti výstupů algoritmů stavění cest a také nedošlo k postavení žádné nedovolené cesty.

Následně byly v datech záměrně vytvořeny některé chyby. V závěrové tabulce byl například pozměněn úsek kontrolovaný na volnost, zaměněn požadovaný stav výhybky atd. Všechny tyto chyby byly odhaleny a nedošlo k postavení žádné nesprávně zadané cesty.

Složitější situace nastává při zanesení chyb do dat, které zpracovává „topologický“ algoritmus. Některé chyby sice nejsou odhaleny, to však proto, že nemají žádný vliv na stavění cest. Například nesprávně zadaná větší maximální rychlost na odbočné větvi jedné z výhybek kolejové spojky se nikdy nemůže projevit na spočítané maximální rychlosti průjezdu zhlaví, protože tato rychlost zůstává při cestách po kolejové spojce omezena přinejmenším druhou z výhybek.

Pokud je stejná chyba zanesena do dat obou algoritmů, jsou jejich výstupy sice totožné, ale ve vztahu ke skutečným prvkům kolejiště nesprávné. Potom dojde k postavení cesty, přestože nejsou splněny všechny potřebné podmínky.

Správná funkce algoritmu vycházejícího z topologických dat je závislá také na správně zadané sousednosti prvků. Pokud by došlo nesprávným zadáním například k vytvoření cyklu, algoritmus skončí zaplněním zásobníku a tím je chyba v datech opět odhalena.

Testování odolnosti proti rušení a jiným chybám v elektronice nemá v této ukázkové aplikaci praktický význam. To by bylo účelné až po vytvoření dvoukanálové struktury s bezpečným komparátorem a také po implementaci detekčních kódů.

Kapitola 4

Závěr

Hlavním cílem práce byl návrh aplikace, která by demonstrovala využití některého z principů návrhu bezpečných systémů při řízení železniční stanice, a její implementace v jazyce C++.

Za tímto účelem jsem nejprve vytvořil moduly, které umožňují simulovat železniční provoz, tedy především pohyb vlaků po kolejišti. Po zadání situačního schématu části železniční trati lze simulovat jízdy vlaků, které se řídí omezenými rychlostmi na jednotlivých úsecích kolejí, návěstidly, polohou výměn, atd. Samozřejmostí je alespoň jednoduché zobrazení kolejiště, návěstidel a vlaků. Nejdůležitějším výstupem ze simulace je stav jednotlivých kolejových obvodů, tedy informace o jejich obsazenosti či volnosti.

Dále jsem navrhnul a implementoval grafické rozhraní, které umožňuje snadné stavění jízdních cest. Toto rozhraní vychází z požadavků na jednotné obslužné pracoviště (JOP), navíc představuje návrh na vylepšení postupného stavění cest a také funkci inteligentního zásobníku povelů, který by měl usnadnit a urychlit řešení některých dopravních situací, především při dálkovém ovládání více stanic na dvoukolejné trati.

Nakonec jsem se zabýval tvorbou softwaru vlastního zabezpečovacího zařízení, jejíž hlavní částí byl návrh dvou rozdílných algoritmů pro stavění jízdních cest. Zatímco první algoritmus vychází ze sestavené závěrové tabulky, druhý algoritmus zpracovává zjednodušeně zadané schéma stanice. Předností takto rozdílně zadávaných a zpracovávaných dat je možnost odhalení chyb v datech nebo algoritmech, které by jinak mohly způsobit nebezpečný stav zařízení.

Tyto algoritmy by mohly být použity v reálných elektronických stavědlech, celou aplikaci by bylo možné využít například pro zaškolení dispečerů pro libovolnou stanici. Jiný způsob využití, který již přímo nesouvisí s bezpečnými systémy, by byla automatická tvorba závěrových tabulek ze zadaného schématu železniční stanice. Obzvláště u velkých železničních uzlů jsou závěrové tabulky velmi rozsáhlé, obsahují stovky jízdních cest, což při neautomatizovaném vytváření zvyšuje možnost vzniku chyby.

Pro praktické využití by bylo vhodné vytvořit grafický editor stanic, který by umožňoval snadné zadání kolejového schéma a takto získaná data převedl do podoby modulu přímo

využitelného při kompilaci (pokud by byly vyžadovány jen statické proměnné), popřípadě datového souboru, který by sloužil pro vytvoření potřebných dynamicky alokovaných proměnných.

Další vývoj by měl být zaměřen především na zobecňování obou algoritmů, aby umožňovaly správné stavění jízdních cest i v jiných typech železničních stanic. V této práci je naznačen a uvažován jen běžný způsob zabezpečení a rozvětvení zhlaví, který je v současné době preferován při projektování většiny železničních stanic. Předpisy ČD pro zabezpečovací zařízení však povolují množství odchylek - některé se vztahují k maximální povolené rychlosti na trati, jiné podléhají jen schválení provozovatelem dráhy. Dále se při zabezpečování stanic používá množství nepsaných pravidel, která upřesňují nebo rozvíjejí normalizované požadavky, jejich respektování je však nutné pro shodu výsledků obou algoritmů. Formulace všech pravidel, přehled používaných odchylek, jejich zahrnutí do algoritmů a rozšíření celého systému o další prvky (nejen) zabezpečovacího zařízení by bylo předmětem rozsáhlejší práce.

Literatura

[1] Hanus, J., Koblasa, K. *Staniční reléové zabezpečovací zařízení typu AŽD-71*. Praha: NADAS, 1974.

[2] Kunhart, M. Elektronické stavědlo typu ESA 11 pro České dráhy. *Nová železniční technika*, 1998, č. 1, str. 21-26.

[3] Štorek, V., Hübl, F., Kovář, O. *Popis elektronického stavědla K-2002, Verze 1.0.* Firemní materiál. Choceň: Starmon Choceň, s.r.o., září 2002.

[4] *Železniční zabezpečovací zařízení. Staniční a traťové zabezpečovací zařízení.* Norma TNŽ 34 2620. Olomouc: České dráhy, s.o., 2002. Účinnost od 1.7.2002.

[5] *Software pro drážní řídicí a ochranné systémy.* Norma ČSN EN 50 128. Praha: Český normalizační institut, 2003.

[6] Švestka, J. *Jednotné obslužné pracoviště.* Základní technické požadavky. České dráhy, s.o., 2002. Vydání IV.

[7] Káldy, R. *Návrh simulátoru železniční dopravy* [online]. Cit. 17.4.2003. ⟨http://artax.karlin.mff.cuni.cz/~kaldr9am/gordikon/index.html⟩.