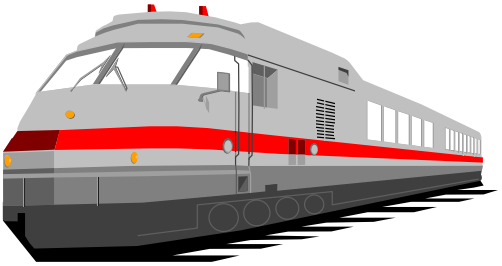
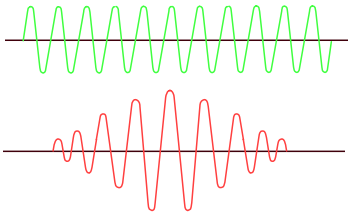
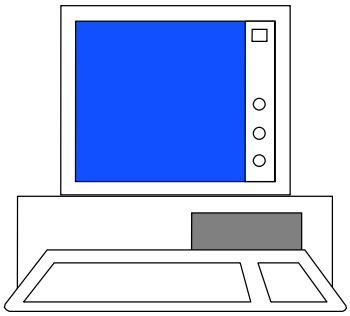
ŽELEZNIČNÍ

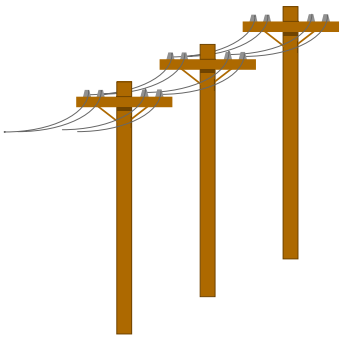




ZABEZPEČOVACÍ TECHNIKA

V. Chudáček a kol.





Praha, 2005

Předmluva

Publikace je prvotně určena zabezpečovacím inženýrům, technikům a vysokoškolským studentům tohoto oboru a poskytuje základní informace o principech železniční zabezpečovací techniky, uplatňovaných zejména při použití novějších technologií. Je zaměřena především na otázky technické bezpečnosti.

Publikace se snaží navázat na práce klasiků moderní české zabezpečovací techniky (Prof. Chudáček, Prof. Poupě, doc. Jelínek atd.) a doplnit ty části, které vývoj nově přinesl.

Podrobné informace k funkčním záležitostem zabezpečovacích zařízení je možné získat studiem příslušných norem. Doufáme, že se také znovu začnou vydávat monografie k jednotlivým konkrétním šířeji využívaným zabezpečovacím zařízením.

Publikace je přepracovaným a doplněným vydáním dvojice knížek (Železniční zabezpečovací technika a Aplikace elektrotechnických prvků) ze čtveřice knížek vydaných postupně v devadesátých letech Výzkumným ústavem železničním (VÚŽ) v Praze.

Publikace využívá práce dalších kolegů z oboru (za všechny jmenujme alespoň Ivana Konečného, Vladislava Kyjovského, Libora Lochmana, Michala Stolína a Petra Varadinova), kteří mě v té či oné míře s publikací přímo pomohli.

Chudáček

V Praze dne 21.10.2005

Obsah

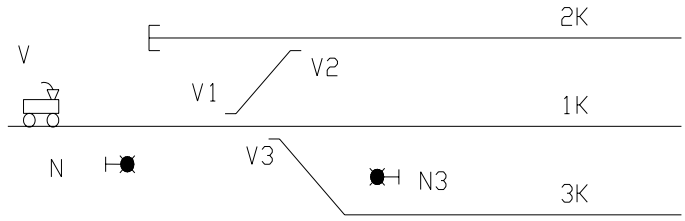
Část I. – Úvod

"… Rychlík se řítí osmdesáti- až stokilometrovou rychlostí vpřed, míjí osady a města, projíždí stanicemi, a cestující – klidně si hoví v pohodlně zařízených vozech. Zdá se, že podél dráhy postavené telegrafní tyče vždy rychleji a rychleji spějí jim vstříc, a pravidelný pohyb vlaku, jakož i šum a hluk jízdou způsobený působí konejšivě na jejich podrážděné nervy. Nikomu z nich ani z dáli nenapadne, že by mu mohlo hroziti nějaké nebezpečí. Každý ví, že jest s dostatek o to postaráno, aby rychlík při svém letu nenajel na příklad na dlouhý nákladní vlak, který silná lokomotiva těžce odfukujíc před rychlíkem na téže koleji zvolna ku předu vleče, každý ví, že tento kolos, který jako smršť prolítne stanicí, nemůže vjet na nesprávnou kolej….Ale málokomu napadne myšlenka, jaké asi duševní a tělesné činnosti bylo a jest k tomu zapotřebí, aby vlaky mohly jezditi s takovou ohromnou rychlostí a při tom s takovou jistotou …" inž. Fr. Křížek, Zabezpečování jízdy na železnici, Světem práce a vynálezů II, Praha 1907.

1 OBSAH ZABEZPEČOVACÍ TECHNIKY

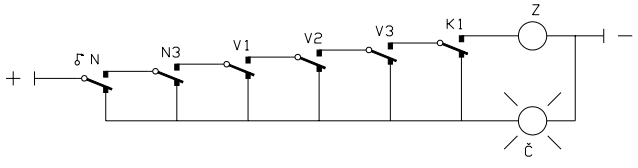
Klasická železniční zabezpečovací zařízení jsou definována jako zařízení, která prvořadě kontrolují, zda zamýšlené disposice dopravních zaměstnanců jsou bezpečné a zda jím nařízené výkony se provádějí tak, aby nebyla ohrožena bezpečnost železniční dopravy. Pro přiblížení uvažujme část stanice podle obr. 1-1 a na této situaci s určitými zjednodušeními tento obsah naznačme.

Před stanicí je umístěno návěstidlo N, které v základní poloze ukazuje návěst "stůj". Dokud návěstidlo ukazuje tuto návěst, nesmí vlak V do stanice vjet. Má-li vlak vjet bezpečně např. na kolej 1K, je třeba splnit určité podmínky. Výměny - pohyblivé části výhybek - V1 a V3 musí být v poloze umožňující řádnou jízdu na kolej 1K, tj. jeden jazyk musí vždy přiléhat k příslušné opornici, druhý musí být od své opornice náležitě vzdálen. Na koleji 1K (včetně výhybek V1 a V3) nesmí být žádná vozidla a ani nesmí být povolen příjezd jiných vozidel na tuto kolej z opačného směru. Zamýšlenou cestu nesmí ohrožovat z boku pohyby jiných vlaků nebo posunujících dílů, proto výměna V2 musí kolizní jízdu svou polohou znemožňovat a návěstidlo N3 musí kolizní jízdu zakazovat (ochrana odvratnou polohou výměny se nazývá přímou boční ochranou, ochrana návěstidlem se zakazující návěstí je nepřímou boční ochranou). Když tedy byly všechny prvky zvolené cesty správně nastaveny, přezkoušeny a shledány bez závady, může být návěstidlo N přestaveno do polohy dovolující jízdu. Po celou dobu, kdy návěstidlo dovoluje jízdu, bude dohlíženo, že všechny k tomu rozhodující podmínky jsou nadále splněny. Vlak V vjede do stanice a ihned po jeho vjezdu se návěstidlo N přestaví opět do základní polohy (návěst "stůj"), aby týž povel návěstidla nemohl být využit více vlaky a aby shora uvedený postup bylo třeba pro každý vlak znovu opakovat.



Obr. 1-1

Úkony, potřebné k tomu, aby vlak vjel do stanice bezpečně, může vykonat určený zaměstnanec. Ten se například pochůzkou přesvědčí, že kolej 1K je volná, že výměny jsou řádně postaveny atd. a po ověření všech podmínek přestaví návěstidlo N do polohy povolující jízdu. Pokud se zaměstnanec nezmýlí, nedojde k nehodě (povšimněme si, že negace této věty nemusí být pravdivá). Bezpečnost jízdy vlaku bude tedy závislá na osobních vlastnostech člověka. Aby tomu tak nebylo, vybavíme koleje technickým zařízením, které bude na jejich volnost dohlížet, výměny jinými technickými zařízeními, která budou kontrolovat jejich polohu atd. a jízdní návěst návěstidel učiníme nuceně závislou na informacích těchto technických zařízení. Primitivní schéma takového zařízení je na obr. 1-2. I když pak dopravní zaměstnanec dá návěstním řadičem N pokyn k rozsvícení jízdní (tj. jízdu povolující)



Obr. 1-2

návěsti Z, návěst se rozsvítí jen v případě, že kontakt N3 informuje svým sepnutím, že návěstidlo N3 skutečně ukazuje návěst "stůj", kontakty V1, V2 a V3 informují, že výměny jsou ve správné poloze a kontakt K1 informuje, že první kolej je volná a není na ni postavena jiná cesta. Jízdní návěst Z se tedy rozsvítí až po splnění všech předem stanovených podmínek pro bezpečný vjezd vlaku. Není-li kterákoliv podmínka splněna, na návěstidle N zůstává svítit červené světlo Č.

Přesto takové zařízení nelze považovat za zabezpečovací zařízení. Prvním důvodem je, že nebyly zřízeny vzájemné závislosti. Jízdní návěst na návěstidle N se sice rozsvítí až když jsou splněny všechny podmínky, ale výměny a návěstidla zůstala volná. Nic nebrání, aby se např. poloha výměn změnila dříve, než vlak V ukončí svou jízdu. Zhasnutí jízdního znaku Z na návěstidle N v důsledku ztráty kontroly při přestavení výměny už nemusí být nic platné, protože vlak již mohl návěstidlo minout nebo již není schopen včas zastavit. Nepostačí ale ani zřízení vzájemné závislosti tím, že by rozsvícená jízdní návěst Z uzavírala výměny a návěstidla v žádoucí poloze (např. prostřednictvím sériově řazeného relé). Vzhledem k nebezpečí přerušení sekvence postupných kroků je důležité, aby uzavření výměn a návěstidel bylo provedeno dříve, než se rozsvítí jízdní návěst. Postup stavění jízdní cesty, vyhovující požadavkům zabezpečovací techniky, bude tedy v naznačeném příkladě následující :

- nejprve se přestaví výměny do žádané polohy,
- v druhém úkonu (nazývaném závěr jízdní cesty) se při uzavírání výměn a návěstidel přezkouší jejich správná poloha a tedy, že první úkon byl řádně proveden. Pokud první úkon nebyl proveden správně, musí být znemožněn úkon druhý,
- obdobně třetí úkon, tj. rozsvícení jízdní návěsti na návěstidle N, je možný jen tehdy, byl-li druhý úkon (a tedy i první úkon) řádně proveden.

Tím jsme dosáhli požadované vzájemné závislosti, jejíž popsaná úroveň je prvním charakteristickým rysem zabezpečovacího zařízení. Zařízení z obr. 1-2 bude podmínce vyhovovat například v případě, že návěstní přepínač N bude konstrukčně upraven tak, že ho nebude možné přeložit bez provedení závěru jízdní cesty. Důsledkem zavedení závěru jízdní cesty bude potřeba po vlaku jízdní cestu vybavit, tj. závěr zrušit, aby bylo možné s jednotlivými prvky opět volně manipulovat.

Ani nyní však ještě nelze v uvedeném příkladě hovořit o zabezpečovacím zařízení. Zařízení musí být konstruováno tak, aby bezpečnost byla zachována i při jakékoliv možné poruše vlastního zařízení. Tento požadavek platí jak pro jednotlivé části, tak pro celek a je druhým charakteristickým rysem železniční zabezpečovací techniky. V uvedeném případě to znamená, že zařízení pro kontrolu volnosti koleje nesmí ani při poruše hlásit obsazenou kolej jako volnou, zařízení pro kontrolu polohy výměny nesmí ani při poruše hlásit nesprávně postavenou výměnu jako výměnu správně postavenou, ke zrušení závěru jízdní cesty nesmí ani poruchou dojít dříve než vlak dotčené prvky skutečně mine atd. Právě tak vlastní zapojení pro rozsvícení jízdní návěsti musí být konstruováno tak, aby se jízdní návěst nemohla poruchou zapojení rozsvítit, pokud všechny podmínky pro její svícení nebudou splněny. Jak patrno, vychází se ze základního železničního bezpečnostního předpokladu, že zastavení vlaku poskytuje nejvyšší bezpečnost. Tento předpoklad se zásadně liší od principů aplikovaných v letecké dopravě, kosmonautice, nukleární technice, navigaci, řízení procesů, robotice, dolování, systémech zabezpečení proti vloupání či odcizení atd., kde je prozatím obvykle hlavním cílem dosažení maximální spolehlivosti a pohotovosti systému. (Rostoucí vědomí potřeby bezpečnosti v neželezničních aplikacích může vést k užší spolupráci mezi bezpečnostními inženýry těchto oborů a železničními zabezpečovacími inženýry. Kdyby tato spolupráce vedla k použitelné standardizaci požadavků a součástí systémů tohoto typu, znamenalo by to jistě zmenšení investičních nákladů i pro železniční zabezpečovací zařízení.)

Důsledkem druhého charakteristického rysu zabezpečovací techniky, tj. převedení všech poruch bezpečnějším směrem je, že téměř každá porucha zabezpečovacího zařízení znamená omezení dopravy. To samozřejmě může vést k narušení plynulosti a vzniku provozních nepravidelností, což jsou jevy, které samy o sobě nebezpečí v dopravě výrazně zvětšují. Ve vážnějších případech je nutné zabezpečovací zařízení do skončení jeho opravy zcela vypnout, aby byl možný alespoň omezený pohyb vlaků. Pak se ovšem provoz, jehož pravidelnost je navíc narušena, děje bez jakékoliv podpory zabezpečovacího zařízení, zatížen, byť i jen na omezenou dobu, možnými lidskými omyly. Odtud tedy plyne třetí charakteristický rys zabezpečovací techniky, což je taková konstrukce zařízení, která má co nejméně poruch, tedy vysokou spolehlivost nebo - obecněji - co nejvyšší pohotovost.

Úloha zabezpečovací techniky nekončí zajištěním odpovídajícího návěstního znaku na návěstidle. Také na lokomotivě je strojvedoucí, jemuž je svěřena péče o bezpečnost vlaku a který tuto bezpečnost může ohrozit svým omylem. Působnost zabezpečovacích zařízení se tedy (prostřednictvím vlakového

zabezpečovacího zařízení) prodlužuje až na vozidlo, aby se zajistilo, že vlak také skutečně bude návěsti respektovat.

Aplikují-li se všechny výše uvedené zvláštnosti správně při vývoji zabezpečovacího systému, je třeba se postarat také o to, aby nedošlo k jejich znehodnocení při projekci, výrobě, montáži a údržbě konkrétních zařízení. Při těchto činnostech je také třeba počítat s lidskými vlastnostmi. Zařízení, sloužící primárně pro eliminaci chyb dopravních zaměstnanců konstruují, vyrábějí, montují a udržují opět lidé. Naštěstí tyto práce, na rozdíl od výkonu dopravní služby, probíhají (nebo by rozhodně měly probíhat) v lepších podmínkách a bez časové tísně. Za příznivých podmínek se nedokonalosti člověka tolik neuplatňují a práci každého pracovníka lze kontrolovat jinými s případnou pomocí dalších technických zařízení. Přesto však z toho pro projekci, výrobu, montáž a údržbu zabezpečovacích zařízení vyplývají jisté zvláštnosti.

Vedle úloh z oblasti bezpečnosti plní moderní zabezpečovací technika i úkoly další. Především jde o hlubší zásahy do vlastního provozu prostředky automatizace. Ta pak, při správném provedení, vede k zlepšenému využití technických prostředků železnic (např. zvýšení propustné výkonnosti tratí), k zhospodárnění provozu, k úspoře jiných, podstatně vyšších investičních nákladů (např. budování další koleje). Protože však zabezpečovací zařízení je zařízením v zásadě restriktivním, nelze u něj bezhlavě prosazovat zvyšování výkonnosti vždy a ve všech směrech. Později také uvidíme, že zabezpečovací technika se podílí na zvyšování bezpečnosti i v jiných oblastech: kolejové obvody alespoň částečně dohlíží na stav jízdní dráhy (celistvost kolejnic), přestavná zařízení výměn dohlíží na stav výhybek, vlakové zabezpečovače mohou do určité míry dohlížet na stav brzdové soustavy vlaku (sledováním skutečně dosaženého odrychlení při brzdění), přejezdová zabezpečovací zařízení se podílejí na eliminaci cizích vlivů na dopravu atd.

Souhrnně lze konstatovat, že prvořadým účelem zabezpečovacích zařízení na železnici je předcházet kolizím a vykolejení vlaků z důvodu chybného řízení dopravy. K tomu účelu je u zařízení třeba sledovat následující oblasti:

- funkční bezpečnost (korektnost systému), tj. řádné plnění všech požadovaných funkcí v bezporuchovém stavu a při očekávaných vlivech pracovního prostředí,
- technickou bezpečnost (bezpečnou konstrukci), tj. splnění požadavku, aby nedošlo k přímému ohrožení bezpečnosti dopravy ani při poruchách samotného zabezpečovacího zařízení,
- bezpečnou aplikaci, tj. vytvoření takových logických funkcí a vzájemných závislostí, aby pro konkrétní situaci navržené zařízení ve všech provozních stavech mohlo řádně plnit svou funkci (na jeho výstupech budou jízdu povolující informace pouze v takovém rozsahu, který odpovídá stavu informací vstupních) a zajištění, aby tyto vlastnosti zařízení mělo i po výrobě a montáži,
- bezpečný provoz a údržbu, tj. zajištění, že předchozí úrovně zůstanou v zařízení zachovány po celou dobu životnosti,
- vysokou spolehlivost, tj. omezení případů, kdy nepřímo, vyřazením zabezpečovacího zařízení a přechodem na manuální řízení, by mohlo dojít k ohrožení bezpečnosti dopravy.

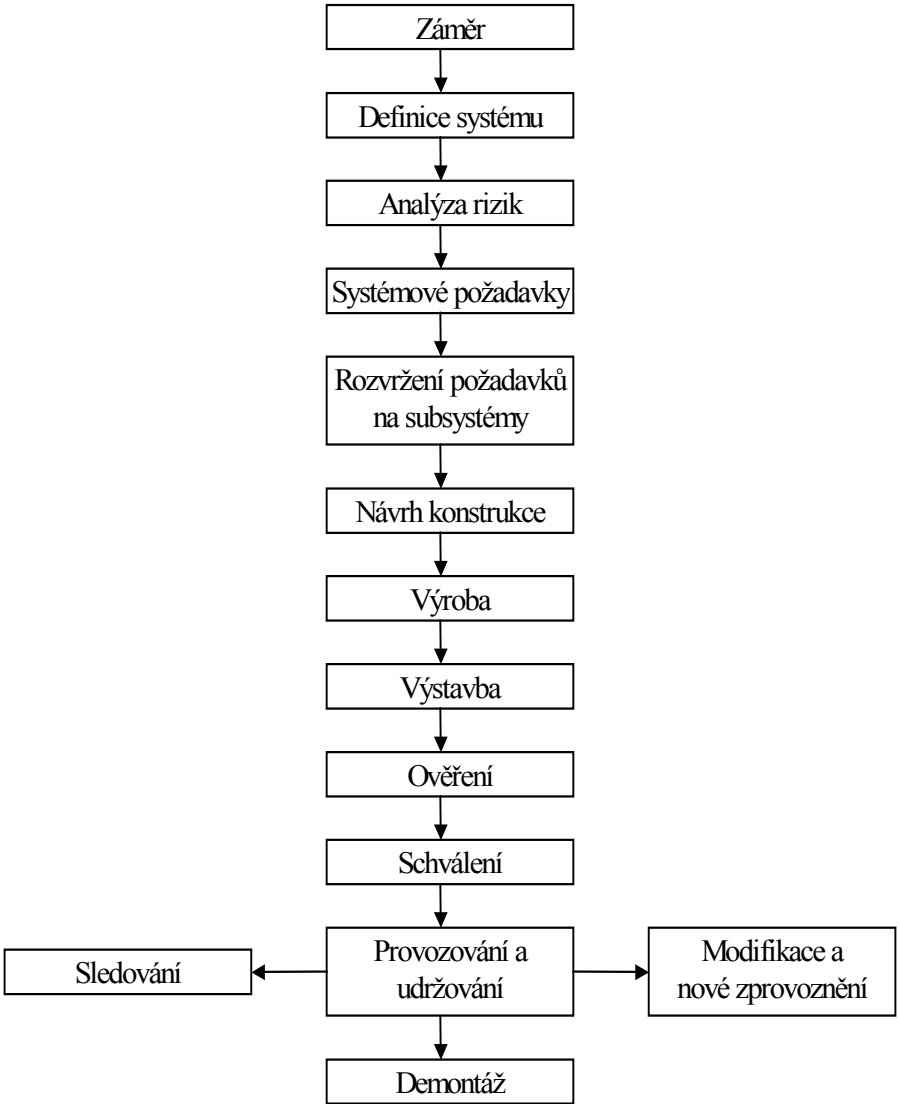
Žádnou ze zmíněných oblastí nelze preferovat, protože žádná nemůže nahradit druhou a nedostatky v kterékoliv z nich znehodnocují výsledky ostatních.

Přímým obsahem železniční zabezpečovací techniky není zajištění zdraví a bezpečnosti zaměstnanců (i když provozovaná zařízení samozřejmě musí splňovat i požadavky např. ve směru ochrany před nebezpečným dotykovým napětím, ergonomicky správně navrženého obsluhovací pracoviště atd.), zabránit nehodám ze zlého úmyslu, násilnou obsluhou, úmyslným poškozením nebo zneužitím zařízení. V poslední době se však jeví jako nezbytné dokonaleji zajišťovat zabezpečovací zařízení proti vandalům a lapkům všeho druhu a neoprávněným zásahům do zařízení v případě, že používají jiných než speciálně drážních zařízení (viz dále např. ochrana dat v otevřených sítích).

2 ŽIVOTNÍ CYKLUS

Požadavky na bezpečnost pokrývají tak celé období životnosti zařízení (life-cycle). Významné fáze života zabezpečovacího zařízení jsou znázorněny na obr. 2-1 a lze je v krátkosti charakterizovat následovně:

- **záměr -** stanovení obecných cílů a účelu nového projektu včetně bezpečnostních a spolehlivostních aspektů ale i aspektů sociálních, politických a legislativních; obsahem by měla být i analýza stávajícího stavu,
- **definice systému** - obsahem je popis systému, stanovení výkonnostních požadavků, provozních podmínek, aplikačních podmínek, celkové strategie obsluhy a údržby, omezení plynoucí z existující infrastruktury, prvotní analýzy bezpečnosti a spolehlivosti, předpokládané rámcové náklady na celou dobu životnosti zařízení,
- **analýza rizik** - předmětem této fáze je identifikace hazardů ve směru bezpečnosti a spolehlivosti zařízení, určení událostí vedoucích k hazardu, určení závažnosti rizika. Tato a předchozí fáze bývají součástí studie dráhy nebo nabídky výrobce k danému problému,



Obr. 2-1

- s**ystémové požadavky** - tato fáze, na základě výše zmíněné studie, shrnuje požadavky na systém a to jak z hledisek funkčních tak i bezpečnostních a spolehlivostních, specifikuje provozní prostředí, definuje všeobecně kritéria pro ověřování a schvalování systému,
- **rozvržení požadavků na subsystémy** - přiřazení funkčních, bezpečnostních a spolehlivostních požadavků k jednotlivým subsystémům, definice obdobných kritérií jako v předchozím pro jednotlivé subsystémy,
- **návrh konstrukce** - vytvoření subsystémů a dílů odpovídajících požadavkům, demonstrace splnění požadavků, příprava plánů řízení bezpečnosti a jakosti v budoucích etapách života zařízení, zpracování podkladů pro projekci, montáž, obsluhu a údržbu, příprava podkladů pro schvalovací řízení. Tato a předchozí etapa plně probíhá v rámci vývoje zařízení u dodavatele,
- **výroba** - zavedení výroby produkující subsystémy a díly odpovídající schváleným, zavedení systému řízení a zabezpečování jakosti ve výrobě,
- **výstavba** - příprava a instalace zařízení v konkrétní adresné aplikaci (zaškolení obsluhy a údržby, zajištění náhradních dílů, zajištění dalších podpůrných procedur, vlastní instalace),
- **ověření** - přezkoušení zařízení a ověřovací provoz, doplnění podkladů pro schvalovací řízení,
- **schválení** - schválení zařízení do provozu,
- **provozování a udržování** - zavedení a sledování obslužných a údržbových procedur, zajištění dlouhodobého souladu s požadavky na bezpečnost a spolehlivost (náhradní díly, periodické školení obsluhy a údržby, kalibrace nástrojů),
- **sledování** - smyslem této fáze je udržet důvěru, že zařízení nadále odpovídá požadavkům na bezpečnost a provozuschopnost. Obsahuje sběr provozních údajů o zařízení, jejich analyzování a sledování vývoje tak, aby bylo možné zlepšovat obsluhu a údržbové procedury,
- **modifikace** - v případě nutné změny na zařízení je v podstatě třeba odstartovat nový životní cyklus zařízení od začátku a projít všemi jeho fázemi pro modifikované zařízení znovu. Podrobnost a důkladnost jednotlivých opakovaných fází bude záviset na velikosti a závažnosti změny,
- **demontáž** - v této fázi je třeba zajistit, aby rušením určitého systému (nebo jeho části) nebyly ohroženy jiné stávající systémy a aby celý proces probíhal plánovitě. Při této příležitosti je vhodné také provést závěrečné zhodnocení výkonnostních parametrů a investičních a provozních nákladů.

Mluvíme-li v souvislosti se zabezpečovacími zařízeními o bezpečnosti, jde nám vždy o takovou funkci zabezpečovacího zařízení, která zajišťuje bezpečnou jízdu vlaku (popřípadě zabezpečeného posunu) a to v rozsahu, který zabezpečovací zařízení může ovlivnit a máme přitom na mysli dosažení stavu s přijatelně nízkým rizikem nehody. Dosažení nulového rizika nehody je ideálním, ale nedostižným cílem; tímto problémem se budeme zabývat podrobněji později.

3 TŘÍDĚNÍ

K železničním zabezpečovacím zařízením se obvykle řadí i zabezpečovací zařízení používaná na podzemních drahách (metro, doly), na pouličních drahách (tramvaje - zejména městské rychlodráhy) a na vlečkách, protože využívají obdobných principů, často i obdobná nebo jen poněkud upravená zařízení. Při třídění zařízení lze použít řadu třídících hledisek; téměř vždy se však vyskytnou zařízení přechodová (smíšená) nebo podle užitého třídění obtížně definovatelná. Přesto je dále několik třídění uvedeno, protože poskytují obrázek o pestrosti a mnohotvárnosti pojednávaného zařízení.

Nejpřirozenějším a klasickým tříděním zabezpečovacích zařízení je třídění podle účelu zařízení. Podle tohoto hlediska lze zabezpečovací zařízení dělit na zařízení:

- staniční,
- traťové,
- vlakové,
- přejezdové.

Účel je patrný již z názvu. Staniční zabezpečovací zařízení zajišťuje bezpečný pohyb vlaků ve stanici, traťové zařízení zabezpečuje jízdu vlaku na trati mezi stanicemi, vlakové zařízení zabraňuje vlaku pohybovat se nad rámec, který povoluje zařízení staniční a traťové (s případným zahrnutím i dalších omezení), přejezdové zařízení přispívá k zajištění bezpečnosti na úrovňovém křížení silnice a železnice informováním uživatelů silnice, že se k přejezdu blíží vlak s předností v jízdě. Nad všemi těmito zařízeními pak může být budováno zařízení pro dálkové ovládání většího úseku tratě z jednoho místa.

Podle místa ovládání zařízení mluvíme o zařízení s obsluhou :

- místní,
- ústřední (centralizovanou v oblasti jedné stanice),
- dálkovou (mimo vlastní stanici).

Další třídění je odvozeno od způsobu ovládání periferií (výměn, návěstidel atd.) a tak vlastně zahrnuje celou historii železniční zabezpečovací techniky. Rozeznáváme zařízení:

- mechanická (využívající výhradně lidské síly),
- elektrická,
- pneumatická,
- hydraulická.

Obdobně, v následujícím třídění je rozhodující způsob, jímž se v zařízení potřebné závislosti realizují. Zde rozeznáváme zařízení se závislostmi:

- mechanickými,
- mechanickými i elektrickými (tzv. elektromechanická a elektrodynamická zařízení),
- elektrickými, která lze dále dělit podle rozhodujících stavebních prvků, jimiž jsou závislosti realizovány, na zařízení:
    - reléová,
    - hybridní (rozhodující část bezpečné logiky je realizována reléově, zbytek elektronicky),
    - elektronická (mikroprocesorová).

U traťových zabezpečovacích zařízení je kladen důraz na rozsah spolupůsobení vlaku. Zařízení se pak dělí na:

- poloautomatická (poloautobloky),
- automatická (autobloky).

Podle rozmístění traťových zařízení podél trati lze automatická zařízení dále dělit na:

- decentralizovaná (funkční bloky jsou umístěny v každém návěstním bodě),
- částečně centralizovaná (funkční bloky jsou umístěny pouze ve vybraných bodech na trati),
- centralizovaná (zařízení je koncentrováno do stanic).

Vlaková zabezpečovací zařízení se dělí podle způsobu přenosu informací mezi tratí a hnacím vozidlem na zařízení:

- bodová,
- semiliniová,
- liniová.

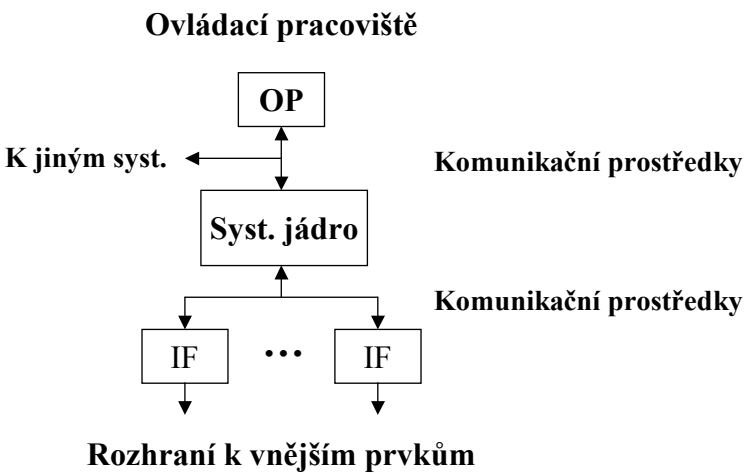
Podle způsobu kontroly souladu jízdy vlaku s přenášenými informacemi se vlaková zařízení dále dělí na zařízení s kontrolou:

- bdělosti strojvedoucího,
- rychlosti vlaku.

Zařízení přejezdová se dělí podle způsobu výstrahy na přejezdová zařízení:

- mechanická,
- světelná bez závor,
- světelná se závorami.

U moderních systémů dělení zabezpečovacích zařízení na zařízení staniční, traťová, vlaková a přejezdová ztrácí smysl, protože systémy jsou komplexní, se společným jádrem řídícím jednotlivé periférie a tyto celky pak tvoří nanejvýš podsystémy. Na obr. 3-1 je základní blokové schéma takového systému.



Obr. 3-1

Obdobně jako zabezpečovací zařízení je nutné posuzovat také nově vznikající a rychle se rozšiřující kategorii počítačově orientovaných pomůcek pro projekci, přípravu dat a testování konkrétních aplikací počítačově orientovaných zabezpečovacích zařízení. Také u nich je nutné přiměřeně uplatnit požadavky zabezpečovací techniky.

Část II. - Základy zabezpečovací techniky

4 PRINCIPY ZAJIŠŤUJÍCÍ TECHNICKOU BEZPEČNOST

Zvláštnosti zabezpečovacích systémů se ve velké míře odvíjejí od požadavku na technickou bezpečnost, tj. na předepsané chování zařízení při poruchách. Při výchozím předpokladu zabezpečovací techniky, že v zařízení může v jednom okamžiku vzniknout pouze jedna nezávislá porucha, lze požadavek na bezpečnou konstrukci vyjádřit (*zabezpečovací šesterka*):

1. žádnou poruchou nesmí dojít k ohrožení bezpečnosti jízdy vlaků. K ohrožení nedojde, pokud výstupy zařízení nebudou ani při poruše povolovat vlakům větší volnost než odpovídá stavu vstupů,
2. každá porucha se musí vhodně a dostatečně rychle (s přihlédnutím k četnosti poruch) projevit, aby bylo možné vyloučit, že se objeví jakákoliv další porucha, která by v kombinaci s poruchou první mohla ohrozit bezpečnost. Riziko je zde funkcí velikosti časového intervalu a četnosti poruch. Proto by detekce chyb měla být nezávislá na toku informací. U klasických zařízení (bez mikroprocesorů) se za přijatelnou ale obvykle považuje i detekce až při následné činnosti či obsluze zařízení,
3. není-li některá porucha detekována ve smyslu předchozího odstavce, je nutné předpokládat vznik jakékoliv další poruchy, přičemž současné působení obou těchto poruch se musí projevit ve smyslu předchozích odstavců,
4. pokud by vlivem jedné poruchy mohlo dojít ke vzniku následných (závislých) poruch, je nutné uvažovat také všechny kombinace těchto poruch jako poruchu jednu,
5. po detekci poruchy by mělo bezprostředně samočinně dojít k odstavení vadného zařízení nebo vadné části zařízení. Podle povahy zařízení lze ale za vhodný projev poruchy považovat i zastavení nebo podstatné (a tedy nepřehlédnutelné) omezení železničního provozu. V každém případě však výstupy vadného zařízení (vadné části) musí zůstat nebo neprodleně přejít do stavu, který neohrožuje bezpečnost dopravy (negace poruchy),
6. po odstavení zařízení pro poruchu nesmí ani další poruchou dojít k samovolnému obnovení funkce. K obnovení funkce zařízení odstaveného pro poruchu může dojít až za účasti udržujícího pracovníka nebo po jiném bezpečném zjištění, že zařízení je bez chyb.

Splnit požadavky na bezpečnou konstrukci je možné různými způsoby. V zásadě lze rozlišit tři dále uvedené základní principy, reagující na skutečnost, zda u rozhodujících použitých stavebních prvků lze některé poruchové stavy vyloučit či nikoliv. Reálná zařízení ovšem nebývají "jednobarevná", ale obvykle v různých částech základní principy vhodně kombinují - skutečná realizace pak má řadu odlišných podob.

Při konstrukci nových systémů, je třeba si uvědomovat, že plně automatizovaný systém sice vylučuje nejméně spolehlivou část poloautomatického systému, tj. člověka s jeho omyly, ale na druhé straně plně automatizovaný zabezpečovací systém pak nemůže těžit ze spolupráce s obsluhou (a tedy ani z kontroly obsluhou) a proto nutně musí být dokonalejší. Dále je nezbytné si uvědomovat, že poruchy, byť bezpečné (tj. nevyvolávající hazardní stavy), budou v provozu u plně automatizovaných systémů pociťovány podstatně závažněji než u systémů s lidskou obsluhou, protože v dosahu nemusí být žádná oprávněná osoba, která by alespoň nouzově automatický systém zastoupila.

Pozn.: České názvosloví se u jednotlivých systémů, jak již to u novinek bývá, tvořilo postupně na různých zainteresovaných pracovištích poněkud odlišně. Dnes je normalizováno zejména evropskými normami EN 50126, 50129, 50128, 50159. Při překladu těchto norem do češtiny se ale až příliš dbalo na doslovný překlad a nebral se dostatečně v potaz již zavedený stav a skutečnost, že některé takto přeložené výrazy mají v češtině již tradičně poněkud jiný význam. V dalším textu v takových případech používáme termíny z vlastní praxe a v závorce uvádíme jednak původní anglický výraz, jednak výraz uváděný v přeložených normách, aniž bychom si tím troufali vlastní výrazy protěžovat. Rozhodnutí o nejvhodnějším termínu ponecháváme na

obecném ustálení, přičemž výhodu co nejbližšího tvaru angličtině sice uznáváme, ale občas je nám proti srsti.

4.1 Systémy s vnitřní bezpečností

V prvním případě, kdy stavební prvky mají využitelné, poruchami nedotčené vlastnosti, lze zařízení řešit obvody s vnitřní bezpečností (inherent fail-safety – systémy s inherentní bezpečností). U typických představitelů této konstrukce jsou funkce zpracování informace a zabezpečení před poruchami řešeny v jedné rovině - jsou navzájem neoddělitelné. Tento přístup znamená, že žádná z uvažovaných poruch nevyvolá hazardní stav systému a systém může být realizován jediným zařízením (hardware i software). Jde tedy o přístup, který je notoricky znám z konstrukce reléových schémat s relé typu N nebo C (I. a II. bezpečnostní skupina relé).

Tento přístup je použitelný také pro realizaci zabezpečovacích systémů s elektronickými prvky, ale elektronických součástek s vlastnostmi vhodnými pro konstrukci obvodů s vnitřní bezpečností není mezi běžně průmyslově vyráběnými součástkami příliš mnoho. Teoreticky je samozřejmě možný vývoj nových speciálních prvků či bloků s vhodnými vlastnostmi (a vývoj zabezpečovací techniky se skutečně nějaký čas ubíral tímto směrem), ale nyní se všeobecně soudí, že zabezpečovací zařízení by se měla pokud možno používání speciálních prvků vyhýbat. Důvody jsou především ekonomické: připojení se na prvky masově vyráběné se za současného stavu technologií jeví výhodnějším. Proto zejména u komplikovaných elektronických zabezpečovacích systémů se tento princip využívá obvykle jen u některých specifických částí (ověřování vstupů, komparace, obvody odpojení atd.).

Určitý problém u tohoto, v klasické technice téměř výhradně používaného, principu představuje plné vyhovění druhému a pátému z uvedených požadavků na bezpečnou konstrukci, tj. dostatečně rychlá detekce poruchy a odstavení vadného zařízení. Je zřejmé, že se při poruše zařízení chová stejně jako zařízení neporouchané při nesplnění některé podmínky funkce (např. pro postavení vlakové cesty není volný kolejový úsek) a zařízení není obvykle schopno poskytnout informaci proč není požadovaná funkce realizována. Tato skutečnost není příliš na závadu u systémů s obsluhou. Obsluha je do značné míry, na základě zkušeností, schopna nadbytečná poruchová omezení rozpoznat (a tak vlastně poruchu detekovat) a následně přijmout příslušná opatření, daná například předpisy. Podstatně nepříznivější situace je u systémů, které pracují bez obsluhy.

Pro účely analýz důsledků náhodných poruch HW je v takto orientovaném systému nezbytné identifikovat možné poruchové stavy každé součástky. S přihlédnutím k dlouhodobým a stále doplňovaným zkušenostem železničních správ a výrobců zabezpečovacích zařízení byly postupně vytvářeny různé katalogy poruch široké škály stavebních prvků, které určují uvažované a popřípadě též nepravděpodobné poruchy (včetně případných technologických předpokladů) pro aplikaci těchto prvků v zabezpečovacích obvodech. U ČD byl dříve zcela neformálně akceptován přístup, který v zásadě odpovídal Katalogu poruch pro elektronické součástky, řadu let tvořenému v UIC a posléze vydanému v dubnu 1988 jako Report RP 12 výboru A155. Následně pak byl přístup normalizován TNŽ 34 2606. V roce 1998 byl, jako poslední z materiálů tohoto druhu, na mezinárodní úrovni kodifikován materiál „Identifikace poruchových stavů HW součástek“ (normativní příloha C normy CENELEC EN 50129). Tato příloha obsahuje procedury a informace pro identifikaci věrohodných poruchových stavů hardwarových součástek. Na rozdíl od předchozích katalogů se zde žádné poruchové stavy nepovažují za apriori nepravděpodobné, pouze se zvlášť vyznačují poruchové stavy, které více přicházejí v úvahu k rozhodnutí, že skutečně nepravděpodobné jsou. Rozhodnutí, že některý poruchový stav je pro konkrétní typ součástky skutečně nepravděpodobný, závisí na uživateli, který ovšem k tomuto rozhodnutí musí použít uvedených postupů. Předpokládá se přitom, že jednou předložené důkazy budou zahrnuty do firemního (drážního atd.) katalogu a nebude je nutné dále opakovat. (Překlad materiálu „Identifikace poruchových stavů HW součástek“ je v příloze.)

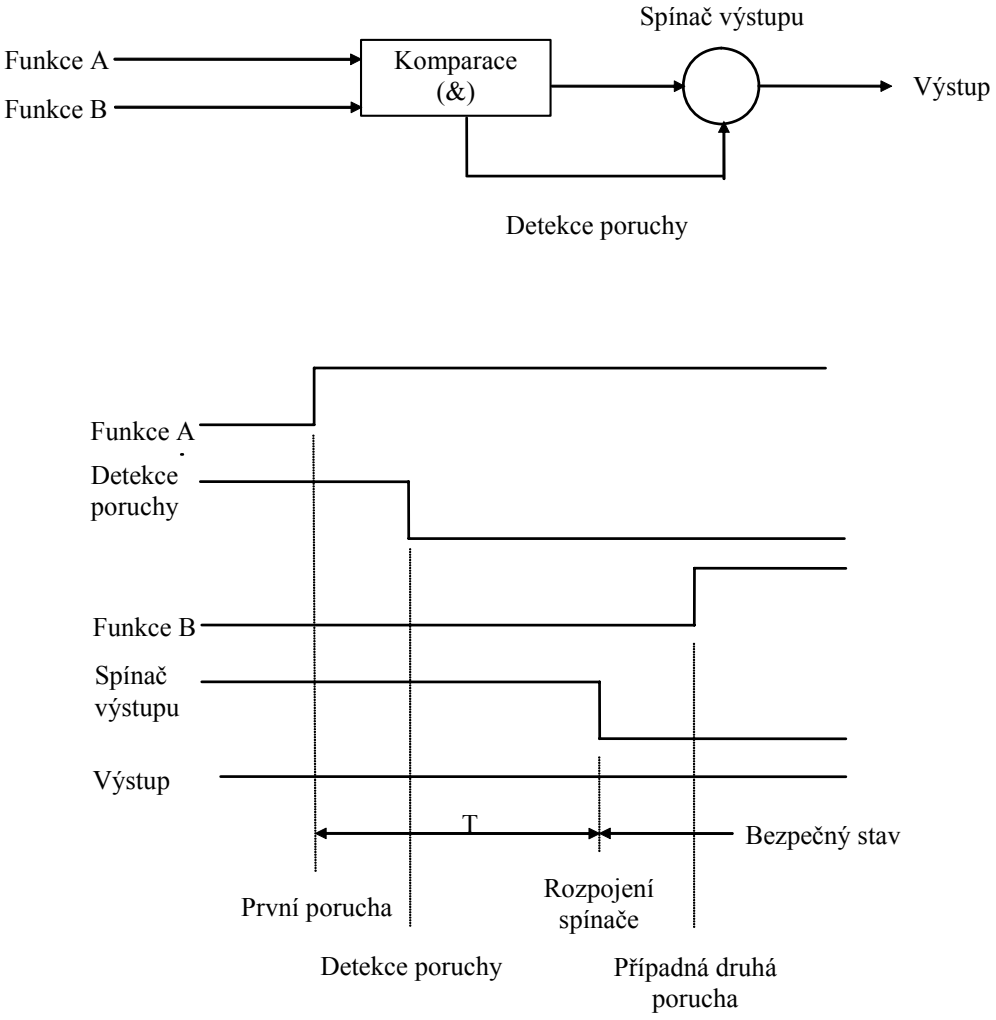
4.2 Redundantní systémy

V případě, že rozhodující stavební prvky nemají využitelné, poruchami nedotčené vlastnosti, spočívá jedno z možných řešení ve využití některé z mnoha forem redundance, doprovázené následnou

komparací (composite fail-safety – systémy se složenou bezpečností). Zpracování informace a zabezpečení před poruchami jsou v tomto případě dvě zjevně oddělené funkce. Zpracování informace se uskutečňuje vícenásobně, obvykle obvody nesplňujícími požadavky na bezpečnou konstrukci, ale vzájemně nezávisle. Zabezpečení před poruchami pak zajišťuje nezávislost vícenásobného zpracování spolu s komparací, porovnávající výsledek (popřípadě i průběh) vícenásobného zpracování informací (odtud někdy používané nepřesné označování jako vícekanálový princip).

Tento princip je založen na předpokladech, že jakákoliv porucha při jednom zpracování informace způsobí odlišný výsledek (případně mezivýsledek) od druhého (případně dalšího) zpracování informace a že komparace chybu neprodleně odhalí a vyvodí patřičné důsledky. Při dvojnásobném zpracování informace půjde o přestavení výstupů systému do stavu, který neohrožuje bezpečnost dopravy a izolování (znemožnění další činnosti) celého systému až do opravy, respektive bezpečného zjištění, že systém je bezchybný. Při více než dvojnásobném zpracování informace je možné na základě majority rozhodnout o tom, která část je vadná a vyřadit z činnosti pouze ji. I v tomto případě je nutná izolace vadné části až do opravy. Dosahuje se tak bezpečného chování celého systému i při poruše (tzv. chování fail-safe), ačkoliv některé použité části systému samy o sobě požadavky na bezpečnou konstrukci nesplňují.

Schematické znázornění jednoho z možných využití uvedeného principu je na obr. 4-1. Výsledek



Obr. 4-1

funkce postoupí na výstup za předpokladu, že výsledky identických funkcí jsou shodné. Pokud však bude identifikován rozdíl, tj. lze předpokládat poruchu, dojde k nevratnému odstavení systému rozpojením spínače výstupu. Žádná další porucha nesmí již takto získaný bezpečný stav ohrozit. Návrat do základního stavu

bude možný až bude bezpečným způsobem ověřeno, že systém není porouchán. Kritická doba, kdy případná druhá porucha by mohla systém uvést do hazardního stavu, je doba T. Její přípustná délka je závislá na pravděpodobnosti druhé poruchy a lze ji limitovat kvantitativními požadavky na bezpečnost, jak bude uvedeno dále.

Redundantní struktury mohou využívat redundanci technického vybavení (hardware), redundanci programového vybavení (software), redundanci datovou, informační atd. Redundantní části přitom mohou být identické nebo diverzifikované a opět je běžné, že se v jednom systému vyskytují různé kombinace.

Komparace může být hardwarová nebo softwarová. V případě hardwarové realizace se komparátor sám konstruuje obvykle s využitím principu vnitřní bezpečnosti. Při softwarové realizaci je nutné použít takové struktury a programovací techniky, které zajistí stejný stupeň bezpečnosti. V obou případech nemusí jít jen o prostou komparaci, ale při třech a více paralelních kanálech může jít o hlasování, obecně "n z m" (obvykle "2 ze 3"). Zcela obecně lze u redundantních systémů pro řešení bezpečné konstrukce využít architektury konjunktivní, pro které platí $n = m \geq 2$ nebo architektury majoritní, kde $n > m/2 \geq 2$. Architektury minoritní se v zabezpečovacích zařízeních využívají zřídka a to výhradně pro řešení problémů spolehlivosti, nikoliv bezpečnosti.

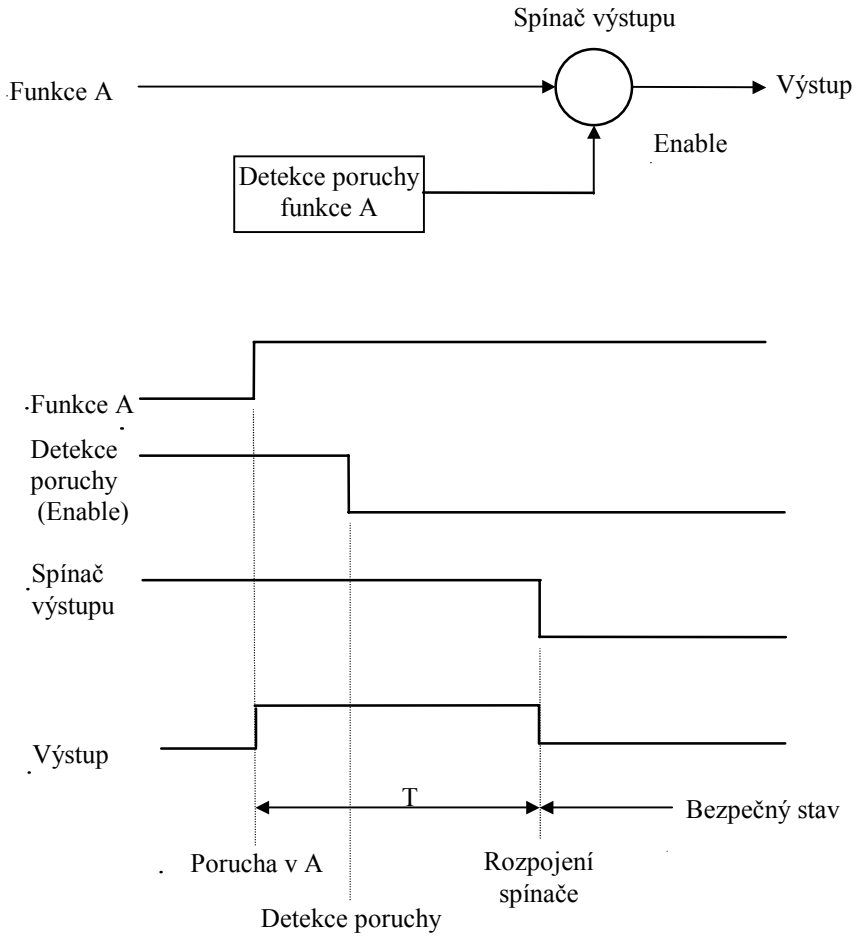
4.3 Reakční systémy

Jako třetí princip je možné uvést přístup, který umožňuje aby bezpečnostně relevantní funkce byly prováděny pouze jedním zařízením a bezpečnost konstrukce se zajišťuje rychlou detekcí hazardního stavu a následným převedení výstupů do bezpečného stavu (reactive fail-safety). Prostředkem pro detekci hazardního stavu mohou být různé způsoby kódování nebo kontinuální testování zařízení.

Funkce je opět zpracována zařízením, které samo o sobě neplní požadavky na bezpečnou konstrukci, tzn. že v něm mohou vlivem poruch vzniknout hazardní stavy, ale ty budou odhaleny detekčním zařízením jiným způsobem než komparací vícenásobného paralelního zpracování funkce (např. kódováním, opakovaným výpočtem a komparací, spojitým testováním). Využití tohoto principu v širším měřítku při konstrukci zařízení je možné až díky vysoce výkonným mikroprocesorům.

Schematické znázornění je na obr. 4-2. Z něj je patrné, že na dobu T se na výstupu zařízení může objevit hazardní stav. Trvání tohoto přechodového stavu nesmí překročit jistý limit. Ten musí být natolik krátký, aby, s ohledem na celý systém, nemohlo dojít k ohrožení bezpečnosti.

Je evidentní, že v některých aplikacích lze detekční funkci do jisté míry také považovat za diverzifikovanou funkci funkce A a tedy i takovéto řešení považovat za řešení redundantní, které však vzhledem k zcela jiné koncepci poskytuje vyšší ochranu proti společným chybám a dokonce i proti systematickým chybám. V některých jiných aplikacích lze naopak funkci detekce poruchy považovat za pouhé rozšíření souboru poruchových stavů, které v systému nemohou navodit hazardní stav a tedy zařízení považovat za zařízení s vnitřní bezpečností.


Spínač výstupu
Funkce A
Výstup
Enable
Detekce poruchy funkce A
Funkce A
Detekce poruchy (Enable)
Spínač výstupu
Výstup
T
Bezpečný stav
Porucha v A
Rozpojení spínače
Detekce poruchy

Obr. 4-2

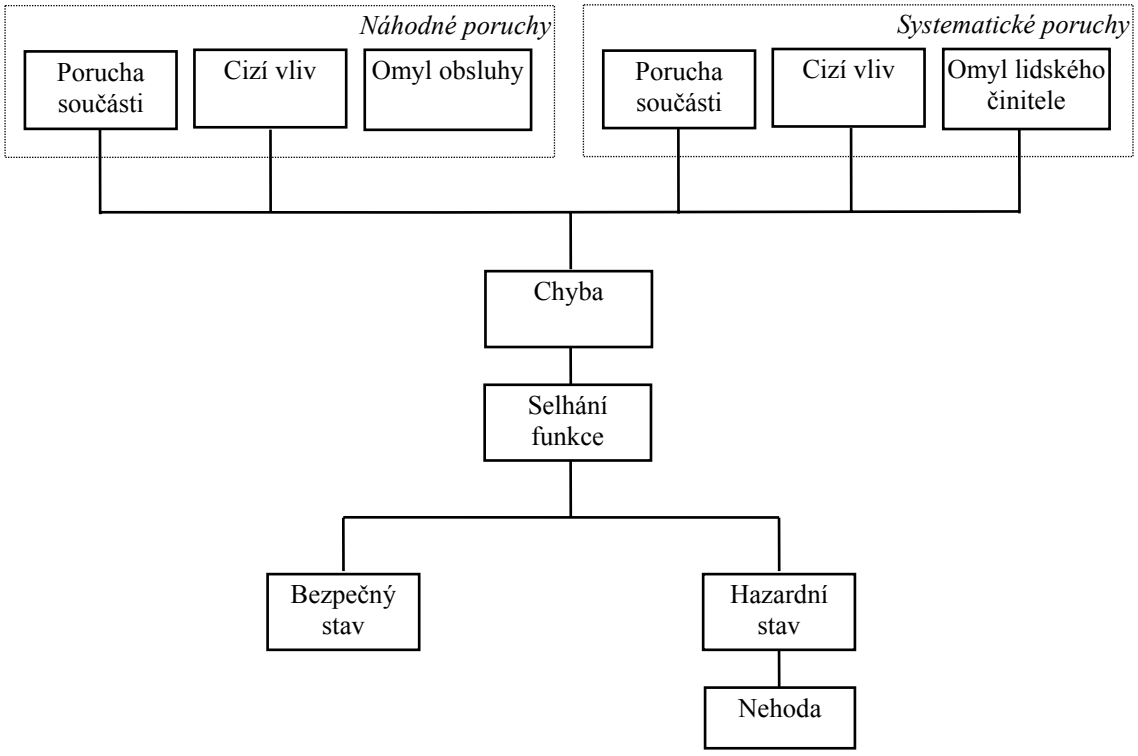
5 PORUCHY

Chyba je rozdíl mezi správnou a skutečnou hodnotou nějaké veličiny. V zařízení se chyby mohou obecně objevit jako důsledek (projev) poruchy některé jeho součásti, působením nějakého cizího vlivu nebo selháním lidského činitele. Za poruchy hardware se považují všechna vybočení z předpokládaných vlastností stavebního prvku (součástky, dílu) zařízení. Předpokládanými vlastnostmi prvků přitom jsou vlastnosti odpovídající příslušným technickým podmínkám popisujícím jeho vlastnosti. Jako omyl lze označit každou lidskou činnost, která může vést k nezamýšlenému chování zařízení. V širším slova smyslu se jako porucha označují souhrnně všechny příčiny vedoucí k chybě, tj. porucha součásti, cizí vliv i omyl.

Chyby se mohou v zařízení vyskytnout náhodně jako projev náhodné poruchy (např. jako výsledek náhodných degradačních procesů v hardware) nebo systematicky jako projev systematické poruchy (např. vždy při určité kombinaci vstupů nebo vlivem určitých podmínek prostředí).

Chyby mohou vést k selhání některých funkcí systému. Za selhání se považuje každé odchýlení poskytnuté funkce od funkce projektované. Selhání funkce, které by mohlo vést k nehodě, se označuje jako hazardní (nebezpečný) stav. Za nehodu se (pro tento účel) považuje každé selhání, které vede k úmrtí, zranění, velké materiální ztrátě nebo poškození životního prostředí.

Vztah mezi uvedenými pojmy je schematicky zachycen na obr. 5-1. Ovšem, ne každá porucha (vliv, omyl) musí způsobit chybu, ne každá chyba musí způsobit selhání, ne každé selhání musí vést k hazardnímu stavu, ne každý hazardní stav musí vést k nehodě.



Obr. 5-1

5.1 Náhodné poruchy

V kategorii náhodných poruch má pro zajištění technické bezpečnosti systémů s vnitřní bezpečností význam následující klasifikace:

- poruchy uvažované:
  - nahodilé poruchy součástí a dílů, které nejsou technicky vyloučené (viz katalog poruch),
  - ohrožující účinky možných cizích vlivů - zejména vlivy energetických a trakčních a dalších silových zařízení,
  - nesprávná obsluha volných ovládačů (s výjimkou ovládačů opatřených plombou nebo počitadlem),
- poruchy neuvažované:
  - poruchy nepravděpodobné - poruchy z fyzikálních nebo technologických důvodů nebo předepsanou údržbou vyloučené. Technologické předpoklady opravňující považovat určitou poruchu prvku za nepravděpodobnou se udávají v katalogu poruch a jejich splnění musí být zakotveno v technických podmínkách příslušného výrobku,
  - nesprávná manipulace s ovládacími prvky opatřenými plombou nebo počitadlem (u těchto prvků je před použitím předepsáno splnění administrativních opatření, což nelze zařízením kontrolovat),
  - poruchy způsobené násilnou obsluhou (pokud zařízení není určeno pro nehlídané prostory), úmyslným poškozením nebo zneužitím zařízení,
  - poruchy nepředvídatelné.

Jak patrno, uvažované poruchy jsou všechny poruchy, které lze technicky předpokládat. Přitom nesprávná manipulace s volnými ovládacími prvky zabezpečovacích zařízení a možný výskyt ohrožujících cizích vlivů na zařízení se posuzuje v podstatě stejně jako náhodná porucha hardware. Pokud by vlivem jedné poruchy mohlo dojít ke vzniku následných - závislých - poruch (např. poruchou jednoho prvku dojde k přetížení a tím k poškození jiných prvků), je nutné uvažovat také všechny kombinace těchto poruch.

Poruchy se mohou vyskytovat přechodně (např. vlivem pouze určitých vnějších podmínek) nebo trvale (nevratná změna parametru). Poruchy mohou mít značně rozdílnou četnost výskytu. Četnost výskytu poruchy nezávisí obvykle pouze na typu stavebního prvku, ale i na zvolené technologii jeho výroby, výrobní kázni, výrobních kontrolách, způsobu jeho použití, jeho pracovním prostředí atd. Lze tedy poruchám předcházet opatřeními při návrhu (konstrukci), ve výrobě i v provozu. Metody předcházení poruch mají však své meze, protože od určité úrovně u každého prvku bude další snižování poruch doprovázeno neúměrně vysokými náklady.

Kategorie nepravděpodobných poruch umožňuje zařadit mezi neuvažované ty poruchy, jejichž vznik se vyloučí technologickými opatřeními. Tímto postupem je možné rozšířit poruchami nedotčené fyzikální vlastnosti stavebních prvků, pokud se vychází z dlouhodobých zkušeností, které oprávněnost takového postupu ověřily. (Typickým příkladem je nepravděpodobnost sepnutí pracovních kontaktů u speciálních zabezpečovacích relé v případě, že cívka není buzena.) I tak ovšem pravděpodobnost výskytu nepravděpodobné poruchy není nulová, ale závisí na skutečném provedení příslušného technologického opatření, tj. technologické úrovni, technologické kázni a kontrole. Ty musí zajistit, že pravděpodobnost výskytu bude tak malá, že ji lze oprávněně zanedbat.

Problematická je otázka vzájemné závislosti působení různých zdrojů chyb. Tak například se může poruchou součástky zvýšit citlivost systému na cizí vlivy. Také existence kategorie nepředvídatelných poruch (tj. poruch jejichž výskyt nelze za daného stavu poznání v oboru vyloučit) znamená, že zabezpečovací zařízení nevylučuje vznik nebezpečných stavů absolutně.

Všechny tyto otázky je nutné zvažovat individuálně na základě konkrétní znalosti zdrojů poruch a jejich rozložení. Úplnou a všeobecnou charakteristiku třeba jen elektromagnetického prostředí nelze jednoduše stanovit vzhledem k velké variabilitě. Nicméně z existující literatury lze získat užitečné informace nebo lze provést zvláštní měření pro určení hodnot parametrů pro určitý prvek nebo druh prvků. Nezbytné je ale vždy porozumět fyzikální podstatě zdrojů chyb, protože některé druhy chyb nemusí být detekovány ani statistickými vzorkovacími metodami. S přihlédnutím k dlouhodobým, stále doplňovaným zkušenostem všech železničních správ, jsou dnes k disposici katalogy poruch široké škály stavebních prvků, které určují uvažované i nepravděpodobné poruchy včetně případných technologických předpokladů.

5.2 Systematické poruchy

Kategorie systematických poruch je svým způsobem největší hrozbou pro tvorbu bezpečných systémů, protože účinná ochrana před systematickými chybami nespočívá jen v opatřeních technické povahy.

Při využívání složitých stavebních prvků vzrůstá pravděpodobnost generace složitých chybových struktur, které mohou znehodnotit i taková ochranná opatření jako je kódování. U těchto prvků (např. integrované obvody s vysokou hustotou integrace) je možné očekávat, že se (vlivem vývoje nebo výroby) vyskytnou systematické chyby vlastní všem prvkům stejného typu nebo alespoň stejné série. Pravděpodobně půjde o složité chyby, které se mohou vyskytovat například pouze za určité teploty, při určité kombinaci dat nebo při určitém použití součástky. Obdobně některé druhy cizích vlivů mohou mít tendenci produkovat například periodicky rozložené chyby.

K zavlečení systematické chyby do zařízení však může dojít i vlivem špatného návrhu, projektu, konstrukce, výroby nebo při údržbě. Ve většině případů tedy půjde o tzv. selhání lidského činitele, lidskou chybu, omyl. Jistou obranu v těchto případech představuje vhodná organizace práce, soustavná a plánovitá kontrola v určitých etapách práce a soustavná péče o kvalitu personálu (výběr, pravidelná školení, přezkušování, kontroly atd.). Uvedené se plně týká i chyb software. Při přechodu na systémy s procesory vzniká celá nová kategorie chyb, a to chyby v programovém vybavení. Koncepční chyby programů jsou způsobeny většinou tím, že programátor nevzal v úvahu všechny možné okolnosti a kombinace stavů zařízení. Z oblasti výpočetní techniky je dostatečně osvědčeným poznatkem, že ani dlouhodobě provozovaný a opravovaný program nedává záruku, že bude prostý chyb. Určitou ochranu představuje pečlivé zadání, podrobné a přehledné zpracování programové dokumentace, strukturované programování, systematická kontrola atd.

Chyby software ovšem mohou nastat i při převodu systémových požadavků do kódu strojových instrukcí. Při použití vyšších programovacích jazyků se snáze prověřuje program z hlediska koncepčních chyb, ale tento program musí být do strojového kódu převeden pomocí kompilátoru. Bylo by tedy třeba buď zkoumat, že kompilátor je bezchybný, nebo zkoumat chyby ve strojovém kódu. Ve složitějších případech není ani jedno řešení bez problémů. uplatňují se proto v některých případech speciální kompilátory, které pracují s omezeným souborem instrukcí a jejich funkce je ověřována postupy blízkými obvyklým postupům při ověřování zabezpečovacích zařízení.

Konečně chyby programového vybavení mohou vzniknout i při přepisu strojových instrukcí do paměti ROM systému. Za dostatečnou kontrolu se dnes považuje úplný test funkce zařízení, který zajišťuje, že během testu bude každá větev programu nejméně jednou provedena. K těmto chybám, vzniklým při procesu tvorby a vkládání programu, je třeba přičíst i chyby plynoucí z možného poškození programu později, během provozu. Právě tak je třeba zařízení chránit proti omylem vloženému jinému programu.

V dalším bude patrno, že existují i technická opatření která vliv systematických chyb mohou výrazně potlačit, v některých případech snad i vyloučit. Závažnost těchto chyb může být zvýrazněna nebo potlačena při volbě koncepce bezpečné konstrukce zařízení. Přihlédnout k tomuto typu chyb je nutné rovněž při určování rozsahu testů, prováděných u všech vyrobených zařízení. Z existence této kategorie chyb pak mohou vyplynout i některé přídavné požadavky na zabezpečovací zařízení. Příkladem může být požadavek, aby zabezpečovací systémy pokud možno nevyžadovaly žádnou periodickou regulaci - evidentně se tak omezí možnost vzniku systematické chyby v údržbě.

5.3 Společné chyby

Při konstrukci redundantních systémů je třeba věnovat zvláštní pozornost chybám, které jsou způsobeny jednou příčinou, ale mohou působit současně na obě (či více) redundantní oblasti. Současný výskyt stejné chyby v redundantních systémech není možné vyhodnotit komparací a tak by vzniklá chyba zůstala neodhalena. Dále jsou uvedeny nejčastější příčiny společných chyb.

Elektrická interference
Největším zdrojem tohoto typu chyb jsou interference způsobené přechodovými jevy při energeticky náročných spínacích procesech, které mohou zasáhnout různé části zabezpečovacího systému současně. Ochrana proti nim může být vedena řadou promyšlených a periodicky prověřovaných pasivních ochran jako je stínění, bleskojistky, optické vazby atp. Zásadnějším řešením je však pouze použití takového zabezpečovacího systému, u něhož bude vznik vícenásobných účinků principiálně vyloučen nebo jinak zajištěno, že nemůže dojít k jejich falešné kompenzaci.
Obdobná situace nastává i u ostatních rušeních s tím rozdílem, že doba působení může být podstatně delší při pravděpodobně nižších úrovních ovlivnění.

Společné obvody
Pokud bude napájecí napětí mimo relativně úzkou toleranci, může se i bezchybný složitější stavební prvek chovat zcela nepředvídaně. Poklesne-li např. napětí napájecí sítě, může být způsobena stejná chyba v různých částech zabezpečovacího systému, i když každý obvod bude napájen ze samostatného stabilizátoru. Obdobně je třeba i uvažovat ztrátu a následné obnovení napájení.
Obdobně mohou chyby vznikat i vlivem jiných společných obvodů, jako jsou obvody vstupů, hodinových impulsů, atd.

Programové vybavení
Použití identicky chybného programového vybavení pro redundantní zařízení může způsobit identicky chybné chování zařízení.

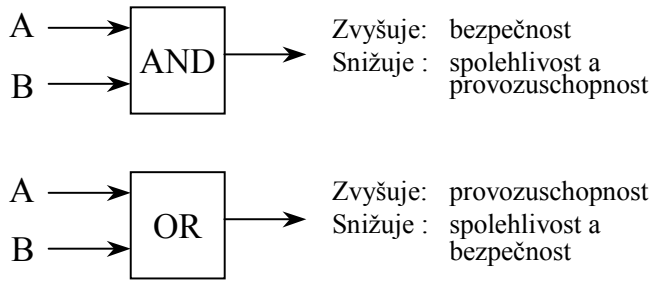
6 FORMY REDUNDANCE

U klasických zařízení se konstrukce využívající redundantního hardware vyskytují jen zřídka – tam se obvykle postupovalo cestou systémů s vnitřní bezpečností, které využívají specifické vnitřní fyzikální vlastnosti určitých vhodných prvků – zejména relé a diskrétních elektronických prvků. Přechod k programovatelným systémům s vysokou hustotou integrace byl v zabezpečovací technice vyvolán stejnými důvody jako v jiných odvětvích – snahou využít vynikajících vlastností těchto systémů, tj. především extrémní flexibilitu, umožňující relativně levně konstruovat systémy s nesrovnatelně lepšími funkčními vlastnostmi, než které bylo možné požadovat od klasických systémů. Redundance je zde pak obvyklým nástrojem, umožňujícím i v těchto systémech splnit bezpečnostní požadavky, které musí i v těchto systémech zůstat absolutní prioritou.

Hned úvodem je ale třeba konstatovat, že vyplnění bezpečnostních požadavků zavedením redundance zdaleka není tak jednoduchou záležitostí, jak se na první pohled zdá. Neexistuje žádná jediná jednoduchá snadno proveditelná cesta k dosažení odpovídající úrovně technické bezpečnosti. Existuje pouze řada opatření a postupů, které, aplikovány v míře odpovídající individuální povaze věci, společně mohou snížit nebezpečí hazardních stavů pod přijatelnou mez. V následujících částech této kapitoly jsou naznačeny možné architektury systémů využívajících redundanci a dále je věnována pozornost některým kritickým bodům těchto systémů.

Je třeba ještě upozornit na to, že ze systémového pohledu jde při aplikaci redundance v otázkách technické bezpečnosti o první využití redundance podle obr. 6-1. Existují zabezpečovací systémy, které aplikují redundanci také druhým způsobem, ale pouze s cílem zvýšení provozuschopnosti (bezpečnost je v takovém případě zajištěna jiným způsobem). Existují také systémy, které s pomocí první aplikace vytvoří systém bezpečný a dva takové bezpečné systémy pak jako celek zapojí ještě redundantně druhým způsobem pro zvýšení provozuschopnosti. To je samozřejmě třeba při posuzování neznámých systémů přesně rozlišovat.

(Na obr. 6-1 je zachycen případ, kdy výstupy obou zařízení jsou trvale připojeny k ovládaným prvkům. Pokud budou v druhém případě připojeny exkluzivně, tj. připíná se záložní systém až v době, kdy hlavní systém je odpojen, nebude bezpečnost ovlivněna.)



Obr. 6-1

6.1 Možné struktury

Existuje řada způsobů a forem, kterými lze redundanci zavést; pět následujících způsobů není vyčerpávajícím výčtem, ale pouze ilustrací :

1. totožný program na nejméně dvou procesorech s bezpečnou komparací - redundantní hardware, což lze v praxi realizovat rozdílnými způsoby, např. jako:
   - vícenásobné procesory v těsném sdružení. Takové systémy obvykle vedou k použití identických procesorů se synchronizovanými hodinami, zpracovávající identický software s porovnáním na úrovni sběrnice,
   - vícenásobné procesory v méně těsném sdružení. Tato technika obvykle vede k použití identických podsystémů, s porovnáním stavů na úrovni paměti a výstupu, a k synchronizaci pomocí příznaků, vyměňovaných mezi redundantními kanály,
2. dva rozdílné programy na jednom procesoru s bezpečnou komparací - dva nezávislé logické kanály na jednom HW,
3. rozdílné programy na nejméně dvou procesorech s bezpečnou komparací - diverzifikovaný software na redundantním HW,
4. jediný program, vykonávající bezpečnostně relevantní funkce, doplněný nezávislou kontrolou za účelem detekce jakékoliv nebezpečné poruchy,
5. datová a/nebo informační redundance.

V bodech, v nichž jsou uvažovány nejméně dva procesory, vzniknou použitím více než dvou procesorů.redundantní majoritní systémy "n z m" (např. 2 ze 3), přičemž zvyšování m nemá přímý pozitivní bezpečnostní význam - podrobnosti viz část 6.2 a 7.3.

Příklad uvedený pod prvním bodem (tedy totožný SW na dvou procesorech) vychází z víry, že je možné konstruovat bezchybný SW. Zajištění, že SW je opravdu bezchybný, je pak věnována významná část vývojových (a posléze i schvalovacích) činností. Výhoda toho řešení je spatřována v sice náročné práci, ale pouze na jediném, pro oba kanály shodném, SW a HW a v příznivých okolnostech pro komparaci. Těsné sdružení (tj. naprosto synchronní chod) obou redundantních systémů je naopak považováno za nevýhodné z hlediska možných společných chyb. Bude-li totiž takový systém vystaven např. rušení nebo systematické chybě HW, je vysoká pravděpodobnost, že oba systémy budou reagovat stejně chybně, což ovšem komparace není schopna jako poruchu detekovat. Tyto námitky vedly k myšlence nesdružovat oba systémy pevně, ale synchronizovat je jen v určitých předem stanovených bodech nebo zajistit jejich sice synchronní, ale z hlediska taktování obou procesorů konstantně fázově posunutou činnost. Obě řešení s volnějším sdružením HW však omezují a komplikují významně možnost komparace – nelze již komparovat cokoliv a v reálném čase jako u systémů pevně sdružených (např. trvalé porovnávání stavu sběrnice). Komparace je třeba například omezit na místa synchronizace a navíc se situace komplikuje problémy vyplývajícími ze skutečnosti, že je obtížnější zajistit, aby oba systémy v rámci jednoho komparačního cyklu pracovaly se stejnými vstupními daty. Pokud nebudou za všech okolností pracovat se stejnými vstupními daty, komparátor musí umožnit podmíněné zachování funkce i v případě, že oba systémy nedospějí ke stejnému výsledku. Tato podmíněnost – tolerantnost komparátoru přinese další komplikaci do bezpečné konstrukce komparátoru a může představovat větší nebezpečí hazardních stavů, než vzniká v těsně sdružených systémech vlivem společných chyb.

Druhý příklad – tedy dva diverzitní SW na jednom procesoru – vychází z názoru, že neexistuje způsob jak vytvořit bezchybný SW. Možným systematickým chybám v programu se brání diverzifikací tvorby SW, přičemž se předpokládá, že každá porucha HW se při zpracování funkce v obou diverzitních SW projeví různými výsledky či mezivýsledky, bude tedy možné komparátorem poruchu detekovat a proto je možný provoz na jediném HW. Tento přístup nepochybně pravděpodobnost hazardních stavů vlivem systematických chyb snižuje, problémem je však věrohodně doložit, že předpoklad detekce všech poruch pomocí komparací diverzitních SW je u konkrétního zařízení naplněn.

Třetí příklad – tedy diverzitní SW na redundantním HW se snaží sloučit výhody obou předchozích řešení. Z povahy je však zřejmé, že se tento systém musí vyrovnat s obdobnými problémy v oblasti komparace, jako systém s méně těsným sdružením z bodu prvního – vlivem diverzifikovaného SW jsou možnosti komparace opět omezeny a oba procesy dospívají k porovnatelným výsledkům v rozdílných okamžicích a neobejdou se bez harmonizace vstupů nebo tolerantních komparátorů.

Čtvrtý příklad při realizaci vede na tzv. reakční systémy (při vnější kontrole vznikne konstrukce s dvěmi procesory, kdy jeden procesor vykonává požadované funkce a druhý jej ověřuje, což ovšem lze také zařadit pod předchozí bod). Je řešením, jehož předpokladem je použití výkonných procesorů a rozsah

nezbytných testů je stále ve stádiu bádání. Není nám v současné době znám systém, který by byl jednoznačně orientován tímto směrem. Na druhé straně určité prvky takového řešení lze vysledovat i v jiných typech zařízení principiálně založených na redundanci.
Určitou dobu byla zkoumána i možnost provozování jednoho SW na jednom HW (tedy architektura běžných procesorových systémů). K tomu účelu byl například konstruován tzv. ultrabezpečný procesor VIPER ve Švédsku. Program skončil neúspěchem, protože se nepodařilo bezpečnost doložit ve smyslu zabezpečovací techniky.

Pátý příklad se týká hlavně specifického dílčího problému - přenosu bezpečnostně relevantních informací, ale také zabezpečení a zpracování dat uvnitř systému a tedy se vyskytuje ve všech dříve zmíněných příkladech. Zde se plně využívají poznatky ze sdělovací techniky přenosu dat – vybrané způsoby kódování, zabezpečení dat, atd., které prokázaly vysokou účinnost již ve sdělovacím provozu.
Takzvaný kódovaný procesor (jemuž byla po určitou dobu věnována pozornost zejména ve Francii) je založen právě na adaptaci principů zabezpečení přenášených dat i do dalších funkcí procesoru. Vstupní data jsou ve vstupních HW obvodech (konstruovaných jako obvody s vnitřní bezpečností) zakódovaná a stejný princip je (místo redundantního HW nebo SW) adaptován i pro zpracování dat. Každý element bezpečných dat je složen z funkční části a redundantní části. Platnost funkční části je ověřována redundantní částí. Tato redundance zajišťuje, že informace byla získána z platných vstupních dat a podrobena očekávané funkci. Redundantní část je pak analyzována vnějším obvodem, tzv. dynamickým řadičem s vnitřní bezpečností, který ověřuje platnost výstupních dat a odepíná výstup v případě, že ověření neproběhlo bez závad. Z hlediska detekce poruch jde tedy opět o reakční systém. Bližší podrobnosti nám nejsou známy.

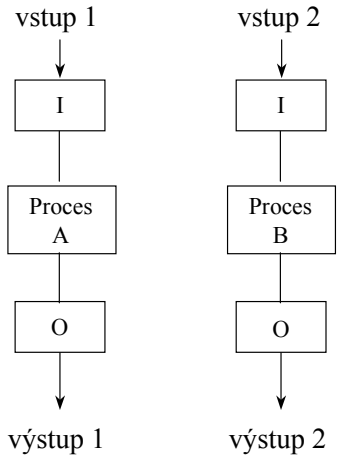
6.2 Příklady aplikací

Obecně je třeba mít na zřeteli, že samotné zavedení redundance problém technické bezpečnosti neřeší. Aby bylo možné hovořit o bezpečné konstrukci, musí být minimálně ještě zaručeno, že:

- redundantní části jsou nezávislé,
- komparace je provedena způsobem vyhovujícím zásadám zabezpečovací techniky,
- každá případná porucha je dostatečně včas detekována,
- po detekci poruchy jsou výstupy zařízení dostatečně rychle převedeny do bezpečného stavu,
- vadné zařízení je neprodleně odstaveno způsobem, který zajistí, že se nebude moci vrátit k funkci dříve, než bude dostatečně zkontrolována jeho bezchybnost.

Každá z uvedených podmínek má řadu řešení. V následujícím jsou uvedeny některé příklady možných řešení a rozhodující okolnosti pro hodnocení, zda jde o přijatelné řešení. Je třeba zopakovat, že žádný ze skutečně provozovaných systémů není zcela jednobarevný, tj. obvykle používá v různých částech různých shora uvedených principů, vhodně je kombinuje nebo přidává některý z význaků jednoho systému do druhého atd.

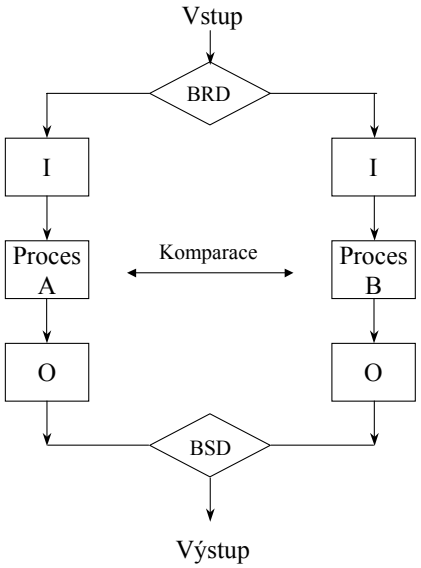
Nejjednodušší řešení zabezpečovacího systému pomocí redundance je naznačeno na obr. 6-2 a pochází z diluviálního období aplikací mikroprocesorů do zabezpečovací techniky. Systém je tvořen dvěma kanály, které samostatně zpracovávají tutéž úlohu. Výstup systému tvoří logický součin výstupů obou kanálů. Lze zde dokumentovat, že i když systém budou tvořit dva skutečně nezávislé kanály a obvod logického součinu (=komparátor) bude bezpečný, nebude možné takové řešení, snad s výjimkou velmi jednoduché funkce, považovat za vyhovující. Nebude totiž pravděpodobně možné prokázat, že každá jednotlivá chyba v systému se projeví, ani že zařízení s poruchovým stavem bude nevratně odstaveno.



Výstup = (výstup 1) AND (výstup 2)

Obr. 6-2

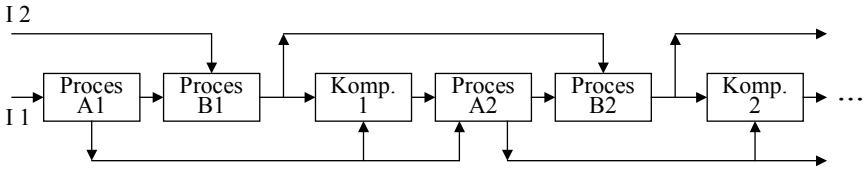
Na obr. 6-3 je uvedeno obecné blokové schéma vyhovujícího systému s redundantním HW. Na tomto obrázku část označená jako bezpečné rozvětvení dat (BRD) musí zajistit, že k redundantním systémům přivedená vstupní data (mající původ ve společném zdroji) nebudou nebezpečně falzifikována (co do hodnoty, ale ani záměnou s jiným vstupem) ani případnou poruchou druhého vstupu, ani možnou společnou



Obr. 6-3

poruchou (napájení, zkrat vedení atd.). V průběhu zpracování bude ve vhodných místech procesu A a procesu B docházet k výměně a porovnání ekvivalentních dat, aby případná porucha byla odhalena co nejdříve a s co nejpřesnějším určením příčiny. Jaké všechny problémy musí komparace řešit, je uvedeno podrobněji dále. Mají-li být výstupy obou procesů sloučeny do jediného bezpečného výstupu, např. pro ovládání jednoduchých prvků bez vlastní zabezpečovací inteligence, musí se tak dít obvodem bezpečného sloučení dat (BSD), který kromě komparace výstupů zajistí i zaujetí bezpečného stavu výstupu při detekci poruchy a to nevratně do doby, než bude zjištěno, že systém je bezchybný.

V případě systému s redundantním SW na jednom HW bude skutečnosti bližší zobrazení procesu na obr. 6-4. Logicky paralelní procesy A a B probíhají reálně, v časové oblasti, sériově. Dílčí sériově prováděné procesy budou střídány dílčími komparacemi, přičemž k dalšímu dílu bude možné přistoupit pouze v případě úspěšného ukončení dílu předchozího.

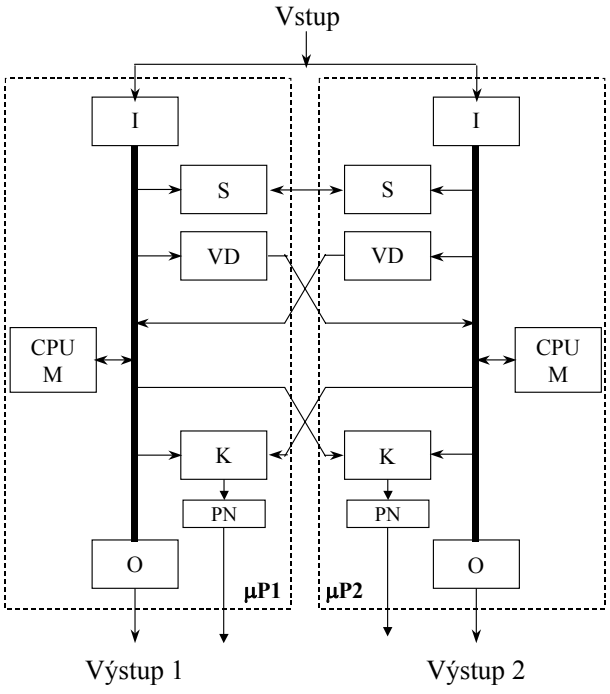


Obr. 6-4

Na obr. 6-5 je znázorněn blokově princip systému SIMIS fy Siemens, využívající identický SW na redundantním HW. Každý procesorový systém má na sběrnici připojen blok vstupů (I), procesor (CPU), paměť (M) a blok výstupů (O). Kromě toho jsou zde další tři funkční bloky :

- blok S, zajišťující synchronizaci obou redundantních systémů,
- blok VD, zajišťující distribuci dat mezi oběma procesorovými systémy,
- blok K, zajišťující komparaci výsledků obou procesů redundantního systému.

Jednotlivé výstupy O jsou pak z obou procesorů vyvedeny samostatně pomocí relé. Také na výstupu každého komparátoru je relé. To je přitaženo pokud komparátor hlásí shodu výsledků a odpadá v případě, že komparátor vyhodnotí neshodu, přičemž paměť nesouladu (PN) nedovolí opětovné přitažení relé dokud není paměť nesouladu vymazána vnějším zásahem (protiopakovací funkce). Komparátory navíc hlásí nesoulad procesorům a tím je uvádí do neaktivního stavu. Výstup k ovládaným prvkům je vytvořen sériovým řazením kontaktů obou výstupních relé (= oba kanály dospěly v konečné podobě ke stejnému výsledku) a obou relé komparátorů (= nebyly zjištěny žádné neshody komparovaných veličin). Všechna výstupní data jsou znovu načtena do systému a jsou porovnána s daty pro výstup požadovanými.



Obr. 6-5

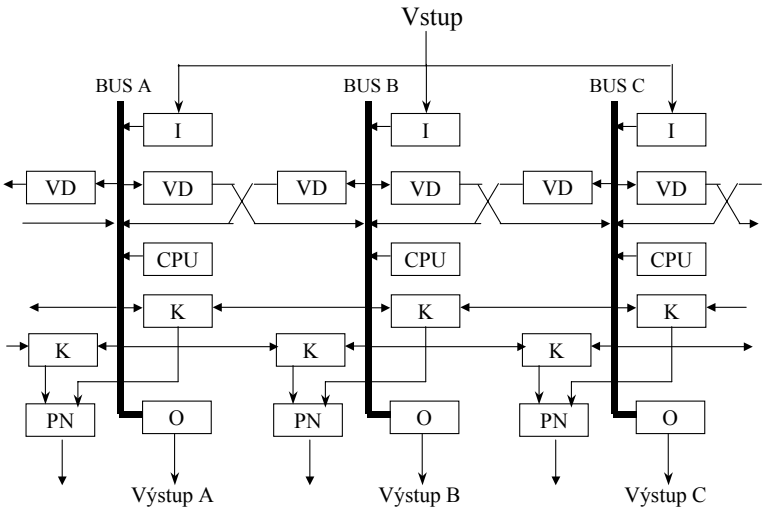
Důležité z hlediska bezpečnosti je, že bloky S, VD a K (a tedy jejich funkce) jsou odděleny (i konstrukčně) od CPU a není proto nutné například uvažovat současnou chybu ve zpracování procesu a v komparaci. Blok VD pouze zprostředkovává přenos vlastním systémem načtených vstupních informací do systému redundantního; funkce komparace vstupních informací a případné harmonizace provádí jednotky CPU. Blok komparátoru K pracuje nezávisle na CPU a provádí komparace výstupních hodnot CPU na úrovni sběrnice. Jedná se o poměrně jednoduchou HW strukturu s vnitřní bezpečností, tj. všechny její případné poruchy vedou k negativnímu výsledku komparace. Na výstupu každého povelu je pak ještě provedena jakási konečná HW komparace řazením relé odpovídajících výstupů obou kanálů a výstupních relé komparátorů do série (viz obr. 6-7).

Každý CPU je řízen vlastními hodinami, blok S zajišťuje, že přibližně po každé desáté instrukci jsou procesory synchronizovány (výkonnost procesoru je tím omezena maximálně o 5%). Touto synchronizací je dosaženo zjednodušení procedur vykonávaných bloky K a VD. Kromě základní činnosti pro synchronní chod obou systémů, vykonává blok S také určitý dozor nad sledem funkcí obou CPU a nezávisle na komparátoru rozpozná rozpad koordinace obou procesů.

Systém je dále opatřen cyklickými testovacími programy, které prováděním kontrolních operací na pozadí ověřují funkčnost CPU a paměti. Aritmetická jednotka procesoru je testována sčítáním dvou 8-mi bitových operandů, výsledek se zapisuje na nepoužitou adresu a je komparován s výsledkem druhé větve. Tento dílčí test se provádí pro všechny možné kombinace hodnot operandů. Dále se testuje paměť RAM srovnáním obsahu, zápisem a zpětným čtením všech buněk paměti RAM dvanácti vybranými kombinacemi bitů a dvanácti kvazináhodnými kombinacemi. Testuje se obsah paměti EPROM, adresování a další funkce sběrnice. Testy probíhají s minimální prioritou (např. v čekacích smyčkách) a tedy nezatěžují propustnost systému. Testování se periodicky opakuje obvykle v průměru každých 10 minut, je však zajištěno, že celá kontrola proběhne nejméně každých 30 minut. Účelem je odhalit i chyby, které ještě nemají negativní vliv na zpracovávané funkce.

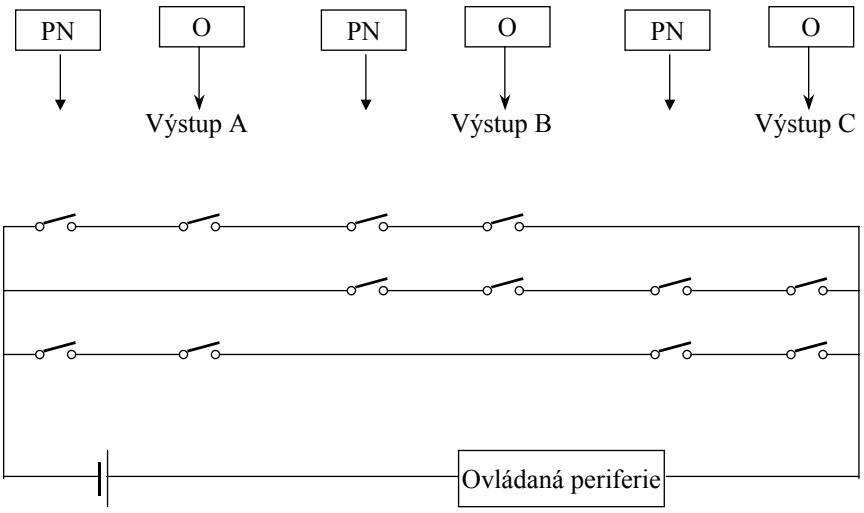
Z hlediska programování se dvoukanálový systém SIMIS jeví velmi podobně jako běžný jednoprocesorový systém. Pro základní ladění programu je možné redukovat systém na jednokanálový, což umožňuje použít běžné testovací nástroje (emulace atp.). Pro systém je vytvořen vlastní operační systém (real-time multitasking OS) COSPAS, napsaný v jazyce PASCAL.

Přidáním dalšího kanálu a změnou zapojení vnějších obvodů lze systém převést na systém dva ze tří (obr. 6-6). Struktura systému je poněkud komplikovanější – každý procesor má dva komparátory. Celkem je tedy v systému 6 komparátorů, stejně jako 6 bloků VD. Tak např. komparátory procesoru B uprostřed obrázku porovnávají data ze své vlastní sběrnice B s daty ze sběrnice A a daty se sběrnice C. Podobně dva distributory dat VD přenáší data na sběrnici A a C. K odpojení výstupu komparátorů na sběrnici B dojde pouze v případě, že je hlášen jak nesoulad se sběrnicí A, tak se sběrnicí B. Informace o zneplatnění výstupů procesoru B jsou v takovém případě přeneseny procesorům A a C a ty pak nadále neakceptují informace posílané z kanálu B prostřednictvím VD. Konfigurace si nadále zachová činnost jako systém dva ze dvou.



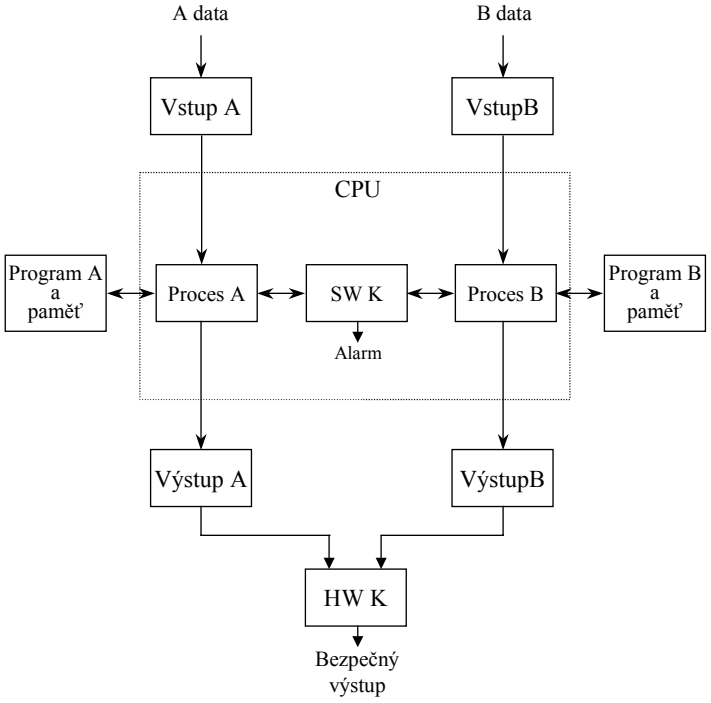
Obr. 6-6

Zapojení výstupních obvodů do navazující technologie je znázorněno na obr. 6-7. Jak patrno, hlasovací obvod nemusí vždy znamenat velkou komplikaci. Provozuschopnost systému dva ze tří záleží pak zejména na střední době opravy případně odstaveného kanálu. Hrubé odhady dovozují, že střední doba mezi poruchami, které způsobí výpadek funkce systému, se takovým řešením dá prodloužit někam mezi 50 až 500 let.



Obr. 6-7

Na obr. 6-8 je znázorněn blokově princip systému EBILOC 850 fy ABB, reprezentující řešení s dvěmi nezávislými SW, provozovanými na jediném procesoru (HW). Do systému vstupují dva rozdílné soubory dat (A, B), které diverzifikovaně popisují stejný stav. Data jsou v obou souborech odlišně kódována a odlišně strukturovaná v jednotlivých paměťových souborech. V procesoru běží dva rozdílné programy A a B, zpracovávající stejnou úlohu odlišnými softwarovými prostředky, vytvořenými dvěma nezávislými



Obr. 6-8

skupinami programátorů na základě odlišného souboru dat. V průběhu programů jsou, opět softwarovými prostředky (SW K) na témž procesoru, porovnávány mezivýsledky (což ovšem nezávislost programů poněkud omezuje) i výsledky probíhajících funkcí. Pro bezpečný výstup jsou výsledky obou procesů ještě znovu porovnány v hardwarovém komparátoru (HW K). Pokud má být informace bezpečného charakteru odeslána k vzdálené periferii (viz dále), je odeslána v podobě oddělených zpráv A a B, produkovaných programy A a B, přičemž každá zpráva má své vlastní kódování.

Rozdílné kódována dat způsobí, že instrukce, které s nimi nakládají, budou různé, což snižuje riziko nebezpečné poruchy v dekódování instrukcí. Rozdílná struktura (poloha) dat v paměti redukuje riziko nebezpečných poruch adresování. Ve speciálních případech, kdy tyto zásady nelze dodržet, jsou použity zvláštní metody, které ověří, že data nejsou falzifikována a že instrukce pracují řádně. Zvláštní opatření jsou zavedena proti možné záměně výstupů (poruchy adresace). Pro bezpečnost významná data mají časově omezenou platnost. K tomu účelu jsou data doplněna časovou značkou, která odpovídá době vzniku a tím určuje i platnost. Zdroj času (např. doba cyklu) musí pak být samozřejmě také bezpečný. Pro ujištění, že program běží řádně a že jsou skutečně prováděny všechny části programu a v předem určené posloupnosti, předává se mezi nimi určitý příznak. Každý blok programu v řetězci nejdříve ověřuje, že příznak má očekávanou hodnotu, při provádění programu hodnotu modifikuje a předá dalšímu bloku. Obsah pamětí (ROM i RAM) je neustále kontrolován pomocí redundantních bitů ke každému slovu. Neustále jsou testovány nejdůležitější instrukce a navíc na pozadí probíhají podrobnější testy instrukcí.

EBILOC 850 je jedním z mála skutečně budovaných plně elektronických stavědel. Každé venkovní zařízení (návěstidlo, přestavník atd.) má svůj vlastní procesorový řadič (tzv. object controller) umístěný obvykle v blízkosti zařízení. Jde tedy o do značné míry decentralizovaný systém, který výrazně omezuje kabelizaci ve stanici. V takovém případě pak postupují obě výstupní informace (výstupy A i B) z centrálního procesoru až do řadiče periférie (ve formě telegramu prostřednictvím komunikační smyčky s modemy a koncentrátory), kde jsou popřípadě ještě dále zpracovávány s využitím stejných bezpečnostních principů, jaké byly uvedeny u centrálního procesoru a teprve před vlastním výstupem do venkovního prvku jsou bezpečným způsobem, pomocí hardwarového komparátoru HWK převedeny na jednoduchý povel (ve většině případů je výstup elektronický a pro zachování bezpečnosti dynamický).

Není bez zajímavosti, že navazující vývojový stupeň - EBILOC 950 - zachoval téměř všechny bezpečnostně relevantní principy ze systému 850, ale programy A a B běží nyní na různých procesorech.

6.3 Nezávislost

U systémů založených na redundanci HW nebo SW (a podobně i u systémů reakčních), jejichž současná porucha může vést k hazardnímu stavu, je nezbytné zajistit nezávislost redundantních částí. Pokud by nebyly nezávislé, existovaly by společné chyby, které by v obou (nebo více) redundantních systémech mohly současně způsobit tutéž chybu, která by pak samozřejmě nemohla být detekována komparací. Opatření, podniknutá k zajištění nezávislosti, musí být účinná po celou dobu životnosti zařízení.

Existuje řada typů vlivů, jejichž působením může ke ztrátě nezávislosti dojít. Obecně jsou to vlivy:

- vnitřní:
  - fyzikální - galvanické spojení, elektromagnetická vazba atd. uvnitř zabezpečovacího systému,
  - funkční – např. zavlečení falešné informace z jednoho redundantního systému do druhého,
- vnější:
  - fyzikální - elektromagnetická interference, elektrostatický výboj a další působení okolního prostředí (teplota, vibrace atd.) ; napájení; vstupy a výstupy,
  - funkční - zavlečení falešné informace z vnějšího zdroje informací.

6.3.1 Dosažení vnitřní fyzikální nezávislosti

Opatření proti nezamýšleným galvanickým spojením

Proti nechtěným galvanickým spojením vodičů na téže vrstvě DPS se za dostatečnou ochranu považuje použití izolačních vzdáleností přinejmenším podle požadavků na zesílenou izolaci podle EN

50124-1. Proti nechtěným galvanickým spojením vodičů na různých vrstvách DPS nebo v témž kabelu musí být izolace dimenzována minimálně v souladu s EN 50124-3. Proti nechtěným spojením v transformátorech musí být různá vinutí v témž transformátoru izolována minimálně v souladu s EN 50124-3 a musí být limitována maximální teplota uvnitř transformátoru (včetně poruchových stavů), aby se předešlo karbonizaci. Proti nechtěným spojením v optočlenech musí být izolace dimenzována minimálně v souladu s EN 50124-3 a musí být limitována maximální teplota uvnitř optočlenu (včetně poruchových stavů), aby se předešlo karbonizaci.

V zabezpečovacích systémech je obvykle praktické aplikovat tyto zásady při konstrukci bez výjimky u všech HW dílů majících vliv na bezpečnost, bez dalšího zkoumání, zda ten který spoj, vodič, součástka atd. je skutečně v uvedených souvislostech relevantní. To ovšem samo o sobě nestačí. Je nutné také ověřit, že z výroby odchází skutečně zařízení, které taková nechtěná galvanická spojení neobsahuje. To lze zajistit jen pečlivým kusovým opakovaným a velmi podrobným testováním dílů ve vhodných místech výrobního procesu.

Opatření proti nezamýšlenému působení přes úmyslná spojení

Zejména z důvodů komparace, synchronizace redundantních částí, nebo harmonizace vstupních dat je často nutné zřídit fyzické spojení mezi oběma redundantními částmi. Aby ani v takovém případě nebyla ohrožena nezávislost, je nutné podniknout opatření proti nebezpečnému ovlivnění jednoho procesu druhým. Tato opatření mohou být obecně založena na vhodných vlastnostech stykových obvodů (konstruovaných pak jako obvody s vnitřní bezpečností) či na vhodné proceduře výměny dat atd.

Opatření proti nezamýšleným vlivům prostřednictvím elektromagnetické vazby

Proti přeslechům mezi dvěma systémy na téže DPS by mělo být použito dvou rozdílných napájecích sítí. Pokud ne, pak musí být dostatečně nízká impedance zemní sítě (i při poruchách), aby se přeslechu předešlo. Při souběhu dvou vodičů, které potřebují ochranu proti vzájemnému přeslechu, je nutné podle použité technologie upravit jejich vzdálenost, délku a mechanizmus vazby tak, aby bylo možné doložit (výpočtem nebo měřením), že k ovlivnění nemůže dojít. Pokud je nutné předejít vazbě v případě poruchy, musí se provést přídavná opatření (např. stínění, zvětšení vzdálenosti). Účinnost je třeba doložit teoreticky nebo praktickým měřením.

6.3.2 Dosažení vnější fyzikální nezávislosti

Pro dosažení odolnosti proti externím fyzikálním vlivům je třeba zejména :

- respektovat opatření podle EN 50121-4 (EMC),
- respektovat specifikované vlivy prostředí (EN 50125-1 a EN 50125-3),
- chránit zařízení proti nepovoleným úrovním napájecího napětí (monitorování napájecího napětí a při vybočení z povolených mezí zajistit přechod do bezpečného stavu. Přitom monitorování napájecího napětí musí být v činnosti po celou dobu života zařízení a pokud nelze vyloučit jeho poruchu může být nezbytná i jeho redundance,
- zavést důkladná opatření proti rušení na vstupních a výstupních bránách systému (ochrana vnějších interface). Musí se přitom předpokládat nejhorší možné případy EMI a jim musí odpovídat vzdušné i povrchové vzdálenosti podle EN 50124-1. Zvlášť velká pozornost musí být u železničních systémů věnována možnému působení přeslechu, blesku a obecně přeskoku vysokého napětí,
- věnovat zvláštní pozornost problémům spojeným s chybným zemním spojením.

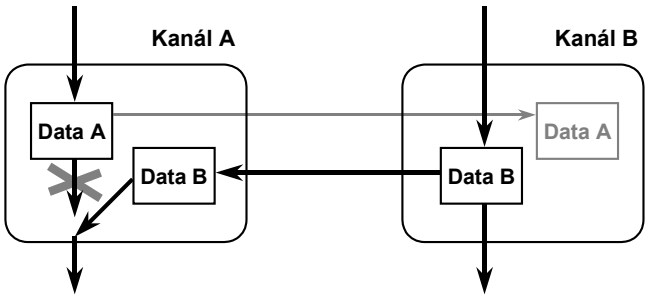
6.3.3 Funkční nezávislost

Nezávislost v redundantních systémech může být principiálně ohrožena skutečností, že pro komparaci musí být výsledky i mezivýsledky procesů v jednotlivých částech porovnatelné (v čase, formou i obsahem). Pro dosažení tohoto cíle je nutná :

- určitá synchronizace obou procesů,
- určitá forma harmonizace vstupních hodnot pro oba procesy,

- určitá forma výměny dat obou procesů a konečně
- určitá forma sdružení dat z obou procesů.

Ve všech případech je třeba postupovat se zvláštní obezřetností a obvykle i používat speciálních postupů, aby nedošlo k ovlivnění činnosti jednoho procesu druhým a tedy aby nebyla ohrožena nezávislost obou redundantních částí. Jako příklad poslouží situace na obr. 6-9, kde vlivem poruchy, např. v bloku komparace, by došlo k nepřijatelné záměně dat A za data B. Pokud formát dat A i B bude stejný, nemůže být v následujících krocích odhalena situace, kdy proces A dává jiné výsledky než proces B.



Obr. 6-9

6.3.4 Nezávislost programů

Jako významné opatření proti systematickým programovým chybám (kromě jiného) se často doporučuje využívat diverzitního programování. I při tvorbě diverzitních programů je však třeba zachovávat jistá pravidla, která co nejlépe zajistí nezávislost programů. Absolutní nezávislost je ovšem mýtus. Více či méně ji vylučují problémy uvedené v předchozím odstavci, tj. nutnost koordinovat činnost obou programů a skutečnost, že konkrétní činnost jednotlivých programátorů do jisté míry ovlivňují stejné základy, získané např. už ve škole atd.

Kromě obecných zásad inteligentního, ukázněného strukturovaného programování je při tvorbě diverzitních programů třeba dbát na následující :

- diverzitní programy tvoří dva rozdílné týmy programátorů, jejichž spolupráce při tvorbě (ale i odlaďování a opravování) programů je striktně omezena pouze na nezbytnou míru, aby se snížila pravděpodobnost stejného přístupu k řešení problému,
- oba týmy samostatně převádějí volnou řečí vyjádřené funkční (popř. speciální bezpečnostní) požadavky do rovnic, algoritmů atp., aby se omezilo nebezpečí stejně špatně pochopených specifikací,
- oba týmy užívají pokud možno rozdílné programovací jazyky, případně rozdílný soubor instrukcí,
- oba týmy užívají rozdílné soubory vstupních dat (např. invertované, zrcadlově řazené),
- při práci je striktně zakázáno používání knihoven programů jiných, než vytvořených při práci týmu, aby se snížilo nebezpečí, že oba týmy budou vycházet ze stejných řešení,
- oba týmy užívají rozdílnou posloupnost ukládání souborů dat (zdola nahoru, shora dolu),
- programy jsou překládány rozdílnými ale vždy speciálně ověřenými kompilátory.

Určitý problém představují právě specifikace – budou-li totiž příliš podrobné, povedou na velmi blízká nebo totožná řešení; budou-li příliš nekonkrétní, povedou na tak odlišná řešení, že bude obtížné hledat styčné body pro komparace mezivýsledků. Dále, v některých případech, kdy problém má evidentně více rozdílných nezávislých řešení, není vhodné spoléhat na nahodilý výběr rozdílných řešení oběma týmy, ale může být lepší záměrné vynucení rozdílných řešení.

6.4 Komparace

Prvotním účelem komparace je ověřit, že redundantní procesy dospěly ke shodnému výsledku. Výsledkem v tomto smyslu ovšem nemusí být vždy pouze výstupy z procesorového systému, ale výsledkem mohou být i do paměti ukládané vnitřní stavy systému, které budou dále použity později nebo v jiném procesu. Tuto záležitost nepodchytí vnější komparátor, komparující pouze výstupy ze systému.

Druhotným smyslem komparace je co nejrychlejší odhalení jakékoliv poruchy v průběhu kteréhokoliv redundantního procesu. Tyto úvahy vedou k porovnání nejen výsledků procesu, ale i vhodných mezivýsledků, protože některé poruchy mohou být při pouhé komparaci výsledků zamaskovány.

Dalšími úlohami, které by komparátor měl plnit, je určení pravděpodobné příčiny neshody a její závažnost pro bezpečnost systému. První záležitost má význam i pro určení části systému, kde k problému došlo - tedy pro kvalitní diagnostickou informaci. Druhá je důležitá pro rozhodnutí jaká opatření je třeba následně po detekci poruchy přijmout. Je zřejmé, že tyto úkoly v jemněji odstupňované škále může být snazší splnit SW komparátorem než HW komparátorem.

Komparace je jednou z klíčových úloh v redundantním systému. Pozitivní výsledek porovnání dvou redundantních procesů má být známkou, že oba procesy probíhají bez poruchy. Naopak se předpokládá, že negativní výsledek komparace je známkou poruchy systému. Z mnoha důvodů však nelze vždy koncipovat komparaci tak striktně. Tak například nebude-li zajištěno, že do redundantních systémů vstupují za všech okolností stejné vstupní informace, není možné očekávat za všech okolností stejné výsledky. Tyto problémy se zdůrazní zejména při přechodových stavech, kdy dochází ke změně vstupních hodnot, popřípadě k rozkolísání vstupních hodnot po určitou dobu (např. zakmitání relé, z nichž jsou vstupní hodnoty odvozeny). Řešení tohoto problému je možné obecně dvěma způsoby:

- harmonizací vstupních hodnot před zavedením do procesu. Takový postup však v sobě nese nebezpečí ohrožení nezávislosti redundantních částí systému. Konkrétní provedení musí takové nebezpečí bezpečným způsobem vyloučit nebo alespoň velmi přísně a bezpečně omezit (např. časově - přiměřeně k deklarované reakční době systému). Harmonizace může být provedena různými způsoby :
  - sledováním a bezpečně omezenou filtrací dočasných neshod,
  - vydáním varování, popř. omezením činnosti,
  - dočasným použitím více omezujících předdefinovaných hodnot,
  - pozastavení činnosti systému.

  Rozhodnutí o nejvhodnějším řešení závisí na požadovaných funkčních vlastnostech systému, časových parametrech atd.,
- dočasným tolerováním negativního výsledku komparace. Musí být provedeno opět bezpečným způsobem a umožněno pouze v odůvodněných situacích a to jen na nezbytně nutnou dobu (opět přiměřeně k deklarované reakční době systému). Komparátor musí tedy v takovém případě rozlišit, zda jde o očekávanou (plánovanou) neshodu nebo zda jde o neshodu vlivem poruchy, což ovšem je z hlediska bezpečné činnosti komparátoru velmi obtížný úkol. V prvém případě proces může dále pokračovat obdobnými způsoby jaké jsou uvedeny v případě harmonizace. V druhém případě, při detekci poruchy, musí systém reagovat jednoznačně nevratným ukončením činnosti systému, jak bude popsáno dále.

Myšlenka komparátoru jako prostředku pro zjištění nesouladu dvou procesů má ještě jednu významnou slabinu. Uvažme zjednodušeně, že výstupem komparátoru je po celou dobu provozního stavu redundantního zařízení výstup „shoda“ a že k výstupu „neshoda“ dojde pouze v případě poruchy HW systému, která způsobí nestejné výsledky obou redundantních procesů. Za provozního stavu pak ovšem může dojít k poruše toho druhu, že komparátor poskytuje poruchou výstup „shoda“ bez ohledu na skutečný stav vstupů do komparátoru. Výstup komparátoru je tedy za takové situace svou hodnotou správný, ale není odvozen z regulérního procesu komparace. Tento problém není relevantní u HW komparátorů, realizovaných jako vnější HW obvod s vnitřní bezpečností, který při všech nebezpečných poruchách bez výjimky zaujme stav "neshoda". V ostatních případech není tento typ poruchy principiálně odhalitelný a může tedy v systému přetrvávat neomezeně dlouhou dobu. Ani řešení formou testování kritických částí nebude pravděpodobně dokonalé.

Jak je tedy patrné, realizace komparátoru je v zásadě možná externím HW obvodem (obvykle obvodem s vnitřní bezpečností – dodnes často komparace prostřednictvím reléových výstupů) nebo

redundantní SW komparací. Obě řešení mají své výhody i své nedostatky a proto je v úspěšných realizacích častá kombinace obou způsobů.

6.5 Působení náhodných poruch

První porucha

Každá porucha, která může být nebezpečná sama o sobě nebo v kombinaci z druhou poruchou, musí být detekována a negována (tj. zařízení musí být vnucen bezpečný stav) v době dostatečně krátké pro splnění kvantitativních bezpečnostních cílů.

Reakce po detekci

Po detekci poruchy musí systém přejít do bezpečného stavu, nebo musí v bezpečném stavu setrvat. Tohoto bezpečného stavu musí být dosaženo v přiměřeně krátkém čase, který zahrnuje jak dobu detekce, tak dobu vynuceného přechodu do bezpečného stavu (negace poruchy). Důvodem pro takto striktní definici chování systému je ochrana před další poruchou, která by se mohla objevit v druhé části redundantního systému a projevit se stejným způsobem jako porucha v první části. Tyto dvě poruchy společně by pak znemožnily komparátoru plnit svůj účel.

Přiměřeně krátká doba detekce poruchy plus doba negace poruchy je závislá na celkové poruchovosti systému a na kvantitativních bezpečnostních cílech pro systém. Orientačně lze tuto limitní dobu určit například výpočtem podle vztahu [EN 50129]

$$\mathbf{t_{sf} = \frac{k}{1000 \cdot a}}$$

kde a = četnost poruch zařízení, jejichž současná porucha může být nebezpečná,
k = 1 pro systém dva ze dvou,
k = 0,5 pro systém dva ze tří.

Při určování četnosti poruch je třeba vzít v úvahu vliv prostředí, ve kterém zařízení pracuje. Pokud je pro detekci poruch použito testování, musí být cyklus úplných testů kratší nebo roven době t_{sf}.
Z této hodnoty lze i odvodit, jaká opatření je třeba podniknout, bude-li zařízení, které bylo vypnuto v bezporuchovém stavu, po určité době znovu uváděno do provozu. Předpokládejme např., že pro zařízení bude doloženo, že je 20 krát méně poruchové v době, kdy je bez napájení. Pak systém dva ze dvou nebo dva ze tří musí být před opětovným zapnutím prověřován na vícenásobné chyby, pokud od jeho vypnutí uplynula doba větší než 400 násobek hodnoty t_{sf}.

Po detekci a vynucení bezpečného stavu nesmí ani další porucha(y) způsobit zrušení bezpečného stavu. Ukončení takto vynuceného bezpečného stavu je možné pouze řízeným způsobem v rámci opravné procedury. Ta může zahrnout účast pracovníka údržby na obnovení činnosti, kterou potvrdí, že zařízení je v pořádku (po alespoň částečném funkčním přezkoušení, s přihlédnutím k okolnostem za kterých k poruše došlo) a může se do činnosti vrátit. Právě tak je možné automatické navrácení do činnosti například po automaticky provedených testech. Při použití této metody je však třeba prokázat, že testovací procedura je dostatečná pro bezpečné zjištění, že zařízení je bezchybné a že bez absolvování celé testovací procedury se zařízení do činnosti nemůže navrátit.

Druhá porucha

Jestliže doba detekce poruchy plus doba negace poruchy je v jednom z redundantních systémů příliš dlouhá, je nutné vzít v úvahu možnost výskytu další poruchy v druhém systému. Tyto dvě současné poruchy nesmí vyvolat nebezpečný stav. To znamená, že je v takovém případě nezbytné použít tři nezávislé systémy zapojené tak, že teprve třetí porucha by mohla vést k nebezpečnému stavu (systém tři ze tří). Detekční doba plus doba negace poruch pro dvojnásobnou poruchu pak nesmí být větší než doba t_{df}

$$\mathbf{t_{df} = \frac{2}{a}}.$$

Třetí porucha

Jestliže doba detekce poruchy plus doba negace dvojnásobné poruchy je příliš dlouhá, je nutné vzít v úvahu možnost výskytu další poruchy v třetím systému. Tyto tři současné poruchy nesmí vyvolat nebezpečný stav. To znamená, že je v takovém případě nezbytné použít nejméně čtyři nezávislé systémy zapojené tak, že teprve čtvrtá porucha by mohla vést k nebezpečnému stavu (systém čtyři ze čtyř). Opatření pro detekci trojnásobné poruchy se nepožadují pokud četnost poruch nepřevýší hodnotu

$$\mathbf{a \leq 2 \cdot 10^{-4}\,h^{-1}}$$

kde **a** je suma četností poruch těch zařízení, jejichž současná chyba může být hazardní (čtyřnásobná porucha).

„Nedetekované" poruchy

I přes veškerou snahu a správnou volbu architektury se mohou vyskytnout dílčí části, kde detekce poruchy ve smyslu předchozích odstavců není možná. Typickými případy jsou např.:

- porucha bezpečného výstupu, která způsobuje jeho aktivaci nezávisle na regulérních podmínkách, v době, kdy tyto podmínky jsou splněny. Na první pohled se zdá, že tato porucha není nebezpečná – podmínky jsou splněny, výstup je aktivován. Problém ale nastane u výstupů, které mohou být aktivovány dlouhodobě (např. závěrné relé na výhybce vedlejší koleje do výjimečně pojížděného šturcu je přitažené prakticky po celou dobu životnosti zařízení), tedy porucha tohoto typu může trvat řádově léta, aniž byla odhalena nesouladem s redundantním výstupem. Pravděpodobnost výskytu obdobné chyby v redundantním kanálu pak může být nepřijatelně velká,
- porucha v té části zařízení, které je jen výjimečně aktivované – např. v některých částech pro ovládání nouzových povelů, obvodech (částech systému) zajišťujících odstavení systému po detekci nebezpečné poruchy atd. – takové poruchy samy o sobě také nejsou nebezpečné, ale nepřijatelná je pravděpodobnost výskytu obdobné chyby v redundantním kanálu.

K problémům tohoto typu je sice třeba přistupovat uvážlivě, ale na druhou stranu je určitě nelze odbýt odkazem na redundanci. Účelným řešením prvního problému může být taková úprava systému, že nebude dlouhodobě (z hlediska potřebných detekčních dob – viz předchozí odstavce) buzené bezpečné výstupy vůbec potřebovat, řešení druhého problému může spočívat v nalezení vhodnější architektury systému nebo v použití vhodných testovacích metod (pokud možno automatických).

6.6 Působení systematických poruch

Systematickým poruchám se předchází zejména vhodnými postupy v rámci procesu řízení kvality a bezpečnosti systémů (viz kap. 18.2). Pokud by přesto hrozilo nebezpečí hazardních systematických poruch, je nutné v dosažitelné míře podniknout i opatření technického rázu. Jimi jsou zejména vhodná architektura systému a řešení na základě diverzifikace (SW, HW).

6.7 Software v redundantních systémech

6.7.1 Dvouprocesorové systémy

Jak již bylo uvedeno, tyto systémy využívají HW redundance, tzn. pokud v důsledku HW poruchy dojde k chybnému vykonávání programu v jednom kanále, předpokládá se, že druhý kanál neudělá stejnou chybu. Nepředpokládá se tedy vznik stejné poruchy ve stejném okamžiku i v druhém kanále.

Tento předpoklad může být ale narušen chybami, které se vyskytují systematicky v obou kanálech. Tím je narušena jejich nezávislost, jedna ze základních podmínek. Takové chyby mohou být snadno do systému zavlečeny právě softwarem. Úroveň, na které dochází k narušení nezávislosti, může být přitom různá. Příčinou zavlečení systematických chyb mohou být:

- stejné programy
- stejné podprogramy, moduly, knihovny
- stejné překladače, linkery (od stejné firmy)
- stejný operační systém
- stejný BIOS, firmware atp.
- stejní autoři programů

Možnou ochranou proti takovým chybám je diversifikace software. Problematikou diversifikovaného programování se zabývala kap. 6.3.4. Podobně jako u příčin narušení nezávislosti lze i u diversifikace software jít do různé hloubky. Míra diversifikace by měla být taková, aby porucha vedla na možná chybné, ale odlišné výsledky. Tato situace musí být dále detekována a bezpečně zvládnuta, jak bylo popsáno v kap. 6.4 o komparacích.

Stejně jako v ostatních fázích vývoje, i v těchto případech lze diversitu doplnit či částečně nahradit zpětnou kontrolou, verifikací. Dekompilací výsledného strojového kódu a porovnáním s původním zadáním lze např. ověřit korektnost překladu.

6.7.2 Jednoprocesorové systémy

U těchto systémů je redundance HW nahrazena redundancí SW. Programové vybavení je tvořeno vícenásobnými moduly či algoritmy, které opět tvoří dva logicky nezávislé kanály, ale fakticky se jedná o jeden program prováděný jedním procesorem, vytvořený jedním překladačem, atp. Systematické chyby jsou zde proto z principu přítomny. Navíc již neplatí, že porucha HW ovlivní v jednom okamžiku pouze jeden logický kanál programu.

Diversita se zde proto stává nutností. Musí být zajištěno, aby jedna porucha procesoru nevedla na stejné chybné výsledky v obou logických kanálech. I když tato porucha postihne oba kanály, musí být jejich algoritmy natolik odlišné, aby se dalo předpokládat, že se jejich výsledky budou lišit. Pro zajištění včasné detekce takového stavu je pak žádoucí, aby program byl členěn na dílčí výpočty a mezivýsledky byly porovnávány (viz příklad na obr. 6-4 v kap. 6.2). I zde platí, že komparace a detekce nesouladu musí být bezpečná.

Zatímco u dvouprocesorových systémů byla diversita ochranou zejména proti systematickým chybám již obsažených v software, u jednoprocesorových systémů musí chránit i před chybným vykonáváním programu v důsledku poruch hardware. Kromě opatření uvedených v kapitole o dvouprocesorových systémech je proto nutné použít v programu takové konstrukce, které umožní detekci poruchy procesoru nebo souvisejících obvodů, především těch, které mohou způsobit narušení nezávislosti obou logických větví. Záludnost problému je v tom, že porucha procesoru může postihnout i tyto konstrukce samotné. Ochranou je opět diversita, redundance a také testování (viz kap. 6.8). Univerzální způsob, jak program zabezpečit, ale neexistuje. Vhodnou kombinací různých ochran lze však dosáhnout stavu, kdy pravděpodobnost jejich nedetekovaného selhání je dostatečně malá.

Poznámka: Právě obtížnost prokázání bezpečnosti jednoprocesorových systémů vedla některé výrobce k tomu, že raději přešli na dvouprocesorový systém, aby prokázání bezpečnosti bylo jednodušší. Viz např. popis systému EBILOC v kap. 6.2.

Základní typy poruch procesoru uvažované při tvorbě diverzitních SW

V následujícím textu jsou shrnuty skupiny poruch, které je třeba vzít v úvahu, a základní ochranné mechanismy. Jedná se především o poruchy procesoru, ale i souvisejících obvodů jako je sběrnice, adresové dekodéry, paměti atp. Pod pojmem procesor budou proto dále zahrnuty i tyto obvody. Do úvahy naopak nejsou zahrnuty vstupní a výstupní obvody, protože jejich bezpečnost je většinou řešena samostatně. Úvaha pro jednoduchý jednočipový mikroprocesor (např. I 8051):

1. Chyby v uložených datech
2. Chyby přístupu k datům
3. Chyby instrukcí při výpočtu
4. Chyby rozhodovacích instrukcí (chyby podmíněného skoku)
5. Chyby sledu vykonávání programu
6. Úplné seběhnutí programu

1. Chyby v uložených datech

Chyba se může projevit
- změnou jednoho či více bitů na daném paměťovém místě
- stejnou změnou jednoho či více bitů na množině pam. míst (např. v pam. stránce)
- náhodnými změnami na množině pam. míst

Příčinou může být
- porucha paměti
- porucha datové sběrnice
- porucha registru nebo sběrnice procesoru
- náhodné rušení

Ochrana dat může být založena na
- kódování uložených dat (a kontrole kódu)
- použití různých formátů pro data a jejich kopie
- použití nezávislých pam. prostorů pro uložení dat a jejich kopií
- testování paměťových míst a práce s nimi
- testování neporušenosti paměti dat

2. Chyby přístupu k datům

Chyba se může projevit
- načtením dat z jiného než požadovaného pam. místa
- zápisem dat na jiné než požadované pam. místo
- použitím jiné než požadované vst.-výst. brány

Příčinou může být
- porucha adr. dekodéru paměti
- porucha adresové sběrnice
- porucha registru nebo sběrnice procesoru
- porucha instrukce procesoru
- náhodné rušení

Ochrana může být založena na
- použití nezávislých pam. prostorů pro uložení dat a jejich kopií
- použití diversifikovaných adres pro uložení dat a jejich kopií
- použití odlišných dat. struktur pro uložení kopií tabulek, polí atp.
- testování adresové sběrnice a přístupu k pam. místům
- použití kódovaných adres

3. Chyby instrukcí při výpočtu

Chyba se může projevit
- nesprávným výsledkem logické či aritmetické instrukce

Příčinou může být
- porucha instrukce procesoru

- porucha paměti programu

Ochrana může být založena na
- použití dvojího různého zpracování dat a porovnání výsledků
- použití různých instrukcí pro stejný výpočet a porovnání výsledků
- zpětná kontrola výsledku provedením „zkoušky“ jinou instrukcí
- testování instrukce
- testování neporušenosti paměti programu

4. Chyby rozhodovacích instrukcí (chyby podmíněného skoku)

Chyba se může projevit
- odskokem programu i při nesplněné podmínce
- neprovedením skoku při splněné podmínce

Příčinou může být
- porucha příznaku
- porucha instrukce procesoru
- porucha paměti programu

Ochrana může být založena na
- použití dvou různých instrukcí pro jedno větvení programu
- testování instrukce
- testování neporušenosti paměti programu

5. Chyby sledu vykonávání programu

Chyba se může projevit
- neprovedením (přeskočením) jedné nebo více instrukcí
- odskočením na jinou než požadovanou adresu
- návratem z podprogramu na jinou než návratovou adresu

Příčinou může být
- porucha registru nebo instrukce procesoru
- porucha sběrnice
- porucha zásobníku
- porucha paměti programu

Ochrana může být založena na
- kontrolu průchodu programu klíčovými body
- testování neporušenosti paměti programu

6. Úplné seběhnutí programu

Porucha se projevuje chaotickým prováděním libovolných instrukcí, často i takových, které se v programu vůbec nevyskytují. Nelze určit vztah mezi původním programem a činností procesoru. Během této pseudonáhodné činnosti může procesor vykonávat i části původního programu, což je obzvlášť nebezpečné (např. provádí-li sekvence, které ovládají výstupy systému). Tato porucha je specifická tím, že ji nelze programově nijak ošetřit, protože příslušný kód nemusí být vůbec vykonáván.

Příčinou může být
- porucha paměti programu
- porucha sběrnice
- porucha vlastního procesoru
- silné rušení

Ochrana proti této poruše musí být vázána na použité hardwarové prostředky (zejména výstupní). Obecně lze říci, že k aktivaci bezpečných výstupů musí být nutná dostatečně složitá posloupnost signálů na výstupech procesoru, aby nemohla být vygenerována náhodnou činností procesoru ani plněním částí kódu původního programu, resp. aby pravděpodobnost takového vygenerování byla dostatečně nízká. Dále lze aktivaci výstupů podmínit nějakým dalším signálem indikujícím bezchybný chod procesoru (obdoba watch-

dogu), pokud je HW k tomu navržen tak, aby to bezpečně umožňoval. Tyto úvahy jsou však již nad rámec kapitoly o softwarových prostředcích ochrany.

Shrnutí

Logické programové kanály v jednoprocesorovém systému musí být silně diversifikované. Nelze nahradit diversifikaci verifikací kódu, protože ta neposkytuje ochranu před chybným prováděním programu při HW poruše procesoru. Hlavním problémem je dostatečná hloubka diversity a zajištění bezpečné komparace a detekce nesouladu. Kromě redundance a diversity je důležitým prvkem cyklické vnitřní testování. I při úspěšném návrhu může být obtížné bezpečnost prokázat. Jednoprocesorová koncepce je proto vhodná spíše pro jednodušší systémy. To je dáno také tím, že při použití výkonnějšího a složitějšího procesoru se množina uvažovaných poruch procesoru začne rozrůstat o problémy, které již není reálné popsaným způsobem řešit (vyrovnávací paměti, pipe-lining, ...).

6.8 Testování

Testy tvoří důležitou součást zabezpečovacích zařízení. Používají se v následujících formách :

- **testy pro detekci poruch v redundantních systémech** - týkají se jak SW, tak HW a jsou součástí standardního vybavení všech konkrétních aplikací daného systému. Používají se zejména ze dvou různých důvodů:
  - **testy při startu zařízení -** pro ověření výchozího bezporuchového stavu zařízení,
  - **cyklické testy** - pro ověření bezporuchovosti systému (nebo jeho části) za běhu programu zejména v případech, které nepokryje princip redundance (např. pro vyloučení jinak nedetekovatelených poruch) nebo pro detekci poruch nezávislou na toku dat a tedy pro zkrácení doby detekce poruchy.

  V obou těchto případech jsou (nebo by alespoň měly být) na jejich funkci kladeny stejné bezpečnostní požadavky, jako na jiné části SW a HW a tedy se také zde uplatňují obecné principy redundance, včetně následné komparace,

- **diagnostické testy** - kromě bezpečnostně relevantních testů obsahuje obvykle zařízení i testy pouze diagnostické povahy, tj. testy orientované na usnadnění opravných procesů v případě poruchy. Tyto testy sice nepodléhají bezpečnostním požadavkům, ale nesmí svou činností nijak ohrozit bezpečnou činnost celého systému. Zato jsou obvykle tyto testy spojeny s ukládáním dat i pro případné pozdější kontroly činnosti zařízení (korektního chodu zařízení, správnosti obsluhy, monitorování funkce atd.).

V dalším jsou uvedeny příklady vhodných testovacích postupů pro detekci poruch v jednotlivých částech procesorového systému, jak je uvádí norma EN 50129. Využití takových postupů přichází v úvahu zejména u jednodušších procesorových systémů; u složitějších systémů bude třeba volit sofistikovanější postupy. Tyto záležitosti jsou v současné době předmětem

CPU - registr
možné poruchy: jakékoliv, např. i v závislosti na kombinaci datových bitů
opatření:

- testy všech registrů (s výjimkou inicializačních registrů) při všech možných kombinacích datových bitů,
- po inicializaci testovat korektnost inicializační funkce,
- registry větší než 8 bitů mohou být testovány za použití všech následujících kombinací datových bitů v každém testovacím cyklu (hexadecimálně):
  5555..
  AAAA...
  3333..
  9999...
  CCCC...
  6666...
  0000...
  FFFF...
  F0F0...

0F0F...
Navíc jsou nezbytné testy všech kombinací datových bitů, rozložené např. do více testovacích cyklů.

CPU – instrukce – dekódování a vykonání
možné poruchy: jakékoliv, např. špatné dekódování nebo špatné provedení působících registrů nebo pamětí, v závislosti na kombinacích datových bitů zdroje nebo cíle,
opatření:

- využívání jediné instrukce z každého typu a její testování při výše uvedených kombinacích dat,
- testování zda všechny použitelné systémové instrukce jsou proveditelné za všech podmínek, zdrojů, cílů a hodnot adresových bitů,
- testování zda všechny použitelné systémové instrukce přerušení jsou proveditelné v závislosti na přerušeních nebo podmínkách přerušení,
- pro testování všech použitelných systémových instrukcí je povoleno generovat je v paměti RAM a odskakovat do nich. Po provedení změn obsahu alespoň jednoho registru se doporučuje testovat nejen obsah dotčeného registru ale i obsah ostatních registrů,

CPU – hodiny
možné poruchy: chybná frekvence,
opatření:

- pokud jsou použity nezávislé hodinové generátory v každém kanále, pak chybná frekvence v jednom kanálu může být odhalena komparací,
- v případě závislosti nebo vícenásobné poruchy může být nezbytné přídavné sledování frekvence

CPU – reset
možné poruchy: další (dodatečný) reset nebo nefunkční reset,
opatření:

- pokud jsou použity nezávislé zdroje resetu v každém kanále, pak chybný reset v jednom kanálu může být odhalena komparací,
- v případě závislosti nebo vícenásobné poruchy může být nezbytné přídavné sledování resetů

CPU – napájecí zdroj
možné poruchy: chybné napájecí napětí,
opatření:

- pokud jsou použity nezávislé zdroje v každém kanále, pak chybné napájení v jednom kanálu může být odhaleno komparací,
- v případě závislosti nebo vícenásobné poruchy může být nezbytné přídavné sledování napětí

Paměť – ROM
možné poruchy: jakýkoliv chybný obsah nebo chybné dekódování adresy nebo řídících signálů,
opatření:

- čtení a porovnání celého obsahu,

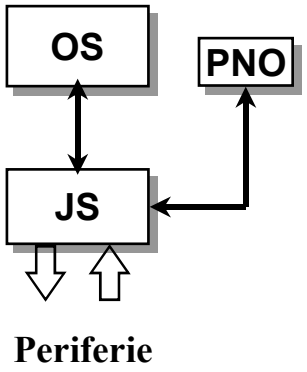
Paměť – RAM
možné poruchy: chybný obsah po čtení nebo zápisu nebo chybné dekódování adresy nebo řídících signálů,
opatření:

- čtení a porovnání celého obsahu,
- test zápis-čtení-komparace pro všechny kombinace data, uvedených u CPU – registr,
- test zda všechny buňky jsou adresovatelné (např. vkládáním zvláštních kombinací datových bitů do jedné buňky a čtení a porovnávání všech ostatních buněk na čipu), stejné znovu při invertované kombinaci datových bitů a to celé opakovat pro všechny buňky. Tento test současně detekuje vliv každého bitu na každý bit čipu RAM.

6.9 Procedury

Při řešení problémů technické bezpečnosti lze také použít různých specifických postupů, známých z jiných odvětví elektrotechniky - jako zpětná vazba, kontrola toku dat, funkce watch-dog atd. Samozřejmě musí být uplatněny způsobem vhodným pro zabezpečovací techniku, tj. zejména s uvážením jejich možných vnitřních poruch.

Principy redundance nelze obvykle plně aplikovat výše uvedenými způsoby při ovládání zabezpečovacího systému. Za běžných provozních podmínek zajišťuje jádro moderního zabezpečovacího systém (JS) plně bezpečnost pohybu vlaku a nedovoluje obsluze nařídit akce, při nichž by bezpečnost byla ohrožena. Předpokládejme systém blokově naznačený na obr. 6-10. Část OS zprostředkovává styk mezi bezpečným zařízením JS a obsluhou (pro tento případ je lhostejné, zda obsluhou je výpravčí nebo např. počítačově orientovaný manažerský systém). Část JS je jádro systému, v němž probíhají všechny bezpečnostně relevantní funkce a který vyhovuje z hlediska technické bezpečnosti (např. je konstruován jako bezpečný systém 2 ze 2). V takovém případě je dostačující, když informace poskytované obsluze a ovládání budou pouze spolehlivé. Není tedy nezbytné, aby ovládací systém byl konstruován jako bezpečný - i když obsluha vydá povel, který je v rozporu s bezpečností nebo zařízení OS poruchou povel obsluhy zkomolí nebo dokonce poruchou vydá povel samo, jádro systému nedovolí vykonat povel, který by byl v přímém rozporu s bezpečností.



Obr. 6-10

Za zvláštních podmínek se ale vyskytují situace, kdy obsluha musí sama provést akce, které jsou bezpečnostně relevantní. Příkladem takových činností (obvykle označovaných jako nouzové povely) jsou:

- rozsvícení přivolávací návěsti,
- přestavení výměny náležející k obsazenému kolejovému úseku,
- zadání výluky (nebo omezení rychlosti) do systému,
- odvolání výluky
- nouzové zrušení závěru.

Pokud má tuto činnost obsluha provádět prostřednictvím zabezpečovacího systému, musí mít prostředky k tomu, aby ji mohla provést zodpovědně - potřebuje bezpečné informace o stavu zařízení a bezpečný prostředek, kterým jádru systému nezaměnitelně sdělí svůj úmysl vynechat obvyklé kontroly. Pro takové případy pak musí být ovládací systém konstruován jako bezpečný.

V této souvislosti je třeba uvést, že existují dráhy, které nepožadují, aby zabezpečovací systémy plnily nouzové operace na dálku s odůvodněním, že již pouhá nepřítomnost obsluhy na místě vylučuje možnost zodpovědného řízení. V takovém případě tedy i do neobsluhované stanice nastupuje „nouzový“ výpravčí. Existují dokonce tak rozumné dráhy, které vůbec kategorii nouzových povelů na zabezpečovacích zařízeních nevyžadují s inteligentním uvážením skutečnosti, že nouzová situace a zabezpečovací systém je protimluv, z něhož nemůže nic rozumného vzejít. Nouzové situace pak řeší výhradně administrativními opatřeními - telefonickou resp. radiofonickou výměnou informací mezi dispečerem nebo výpravčím a jízdním personálem, naprosto jasnou, administrativně danou odpovědností za další jízdu vlaku. Obdobně, s velmi dobrými zkušenostmi, je řešena doprava i na naší první dálkově řízené trati Plzeň – Cheb. Na druhé straně je nutné připustit, že snahou nových zabezpečovacích systémů by mělo být zachování alespoň částečné funkce i při poruchách (backup). Oba způsoby obsluhy, pravidelné i nouzové, lze sice provádět na odlišných zařízeních - i JOP pro ČD takový způsob připouští (viz panel nouzové obsluhy, PNO na obr. 6-10) - ale to má praktický význam jen pro případ místní obsluhy. Vzhledem k zásadním snahám o soustředěné řízení (z obou důvodů : jak pro snížení nákladů na vedlejších tratích, tak pro dostatečně předvídavé řízení na hlavních tratích) je tedy toto řešení nepraktické. Svou váhu při výběru některého z těchto postojů má také dosahovaná spolehlivost zabezpečovacích systémů.

Vystavět část OS na podobných principech jako JS (tj. s respektováním zásad pro technickou bezpečnost) je obtížné, vzhledem k tomu, že minimálně obrazovka, videokarta a klávesnice jsou takové povahy, že neposkytují dobré možnosti pro jednoduché zavedení některé formy redundance s následnou bezpečnou komparací, vhodnou činnost po detekci poruchy atd. Většina zařízení se proto v těchto místech odchyluje od obvyklých řešení a vypomáhá si jiným způsobem. Přitom se nepředpokládá, že obsluhy charakteru nouzových povelů by vykonával nadřazený počítačový systém, ale že vždy na tomto procesu bude účasten člověk, jehož vlastností lze specificky využít.

Poruchou ovládacího systému - jeho informační, zobrazovací části - by obecně mohlo dojít k situaci, kdy by se obsluha rozhodovala na základě falešných informací, protože poruchou mohou být:

- zobrazená data závislá pouze na jednom zpracování dat,
- přijatá data z jádra nesprávně interpretována,
- zobrazeny neaktuální (zastaralé) informace,
- aktualizována data pouze v části obrazovky.

Jako opatření proti těmto poruchám byla úspěšně použita následující řešení (pomineme-li vyloučení nouzových obsluh):

- taková architektura systému, která posune redundantní princip řešení co nejdále k zobrazení, až tam, kde zobrazení probíhá již poměrně transparentním způsobem (tj. nemůže již být vlivem zařízení pro zobrazení modifikováno nebezpečným způsobem - vytvořením jiné smysluplné informace než je informace původní) a zde se použije HW přepínač, který na principu obvodu s vnitřní bezpečností zajistí bezpečně střídavé zobrazování z obou kanálů. Takovému řešení v zásadě vyhoví (za splnění určitých dalších předpokladů) řešení s dvěmi přepínanými obrazovými kartami (videoRAM). Vnitřně bezpečný přepínač zajistí, že zobrazovány jsou informace z obou logických kanálů a jejich stejnost je vyhodnocována obsluhou - při přenášení nestejných informací bude obrazovka "mrkat". Nevýhodou tohoto řešení je nutnost konstrukčního zásahu do běžného HW počítačů, zde obvykle třídy PC,
- procedura, při níž je na obrazovku přenášen střídavě dvojnásob redundantní obraz, jehož originál je vytvořen v bezpečných (redundantních) částech JS. Střídání kanálů musí mít možnost obsluha zkontrolovat (např. pomocí měnícího se grafického symbolu, který je také vytvořen, jako součást bezpečné informace, v části JS). Jako ochrana před špatnou interpretací bezpečných informací slouží dvě kvalitativně různá vyjádření téže informace (např. grafický symbol a textové vyjádření obsahu). Obdobná opatření jsou pak použita i pro ochranu před neaktuálními nebo částečně neaktuálními informacemi,
- zpětná vazba, která zpětně informuje bezpečné jádro systému z nejzazšího možného místa přenosu o skutečné informaci předané na obrazovku.

Obdobně poruchou ovládacího systému - jeho povelovací, zadávací části - by mohlo dojít k situaci, kdy by povel k nouzové obsluze byl vydán:

- samovolně ovládacím počítačem,
- sice obsluhou, ale nechtěně (nevědomky).

Jako opatření proti těmto poruchám se používá:

- zavedení zvláštního potvrzovacího tlačítka, které technikou obvodu s vnitřní bezpečností předává u kritických nouzových povelů jinou cestou bezpečnému jádru systému JS ještě potvrzení, že v dané chvíli je skutečně vyžadováno splnění nouzového povelu,
- vyslání zvláštní sekvence povelů do bezpečného jádra systému JS, která potvrzuje zadání nouzového povelu (u ČD zvolena sekvence znaků a-s-d-f-enter, které musí být v limitovaném čase a bez narušení posloupnosti předány do JS).

V obou případech je zadání nouzového povelu chápáno systémem jako předběžný povel. Místo vykonání povelu se systém na jeho vykonání pouze připraví a informuje obsluhu, jaký povel je připraveno vykonat (popř. o nesplnění běžně uvažovaných bezpečnostních podmínek pro danou funkci) a po limitovanou dobu čeká na příchod potvrzení. Veškeré tyto funkce jsou zařízením registrovány a spolu s údajem o času a stavu zařízení dohodnutým způsobem archivovány pro případnou pozdější potřebu.

7 BEZPEČNOST A SPOLEHLIVOST

Smyslem železnice je poskytovat bezpečné a kvalitní dopravní služby. Spolehlivost, s níž je služba poskytována, má na výslednou kvalitu služby výrazný vliv, i když kvalitu samozřejmě ovlivňují i další faktory (frekvence služby, struktura atd.). Z tohoto základu musí vycházet všechny železniční systémy a tedy i zabezpečovací zařízení. Hodnotit celkové naplnění provozních požadavků jednotlivých systémů pak znamená sledovat celý soubor vlastností: bezporuchovost, pohotovost, udržovatelnost a bezpečnost (v anglické literatuře označováno jako RAMS - Reliability, Availability, Maintainability, Safety).

V následujících odstavcích je naznačeno, jak lze (bez nároků na úplnost) využít poznatků teorie pravděpodobnosti v zabezpečovací technice.

7.1 Bezpečnost

Jak již bylo uvedeno, v řádně navrženém zabezpečovacím systému musí být, kromě jiného, zabudována i schopnost systému omezit důsledky poruch zařízení tak, že i při jejich výskytu bude vyvolána výstupní informace, která není méně omezující než ta, která by byla výsledkem funkce neporouchaného systému v téže situaci. Tato schopnost představuje kvalitativní stránku bezpečnosti. V případě systémů s vnitřní bezpečností by bylo takto dosaženo absolutní bezpečnosti, pokud by absolutně platilo roztřídění poruchových stavů, tj. nevyskytl by se nikdy žádný případ, kdy by došlo k nepravděpodobné nebo neuvažované poruše. Pokud k takové neuvažované poruše dojde, nelze nebezpečnou situaci vyloučit. Podobně při správné aplikaci redundantního systému se zajistí, že žádný hazardní stav nebude mít negativní vliv na bezpečnost, pokud v době T po výskytu první chyby nedojde k druhé poruše, která by zabránila komparací zjistit nesoulad. Toho ale také lze dosáhnout jen s jistou pravděpodobností a to tím větší, čím kratší bude doba T a čím větší bude obecná spolehlivost systému. U reakčních systémů je tato složka bezpečnosti dána schopností detekčního zařízení absolutně podchytit všechny možné hazardní stavy a také je negovat v dostatečně krátké době.

V zabezpečovacím systému tedy mohou existovat určité poruchové stavy, s pravděpodobností výskytu ležící pod požadovanou úrovní (a o nichž se pak zjednodušeně předpokládá, že jsou nepravděpodobné), při kterých zabezpečovací zařízení nebude reagovat správně. Bezpečnost zabezpečovacího zařízení lze tedy také kvantifikovat a to jako pravděpodobnost nepřítomnosti hazardního stavu v zařízení po jistou dobu jeho využívání a za určitých podmínek provozu a údržby.

Při hodnocení bezpečnosti zabezpečovacího systému je nutné vždy pamatovat na obě hlediska - kvalitativní i kvantitativní. Pro minimalizaci rizika se u zabezpečovacích zařízení musí postupy, ovlivňující kvantitativní i kvalitativní stránku bezpečnosti, navzájem doplňovat. Přesto úplné eliminaci rizika brání jak technické tak ekonomické ohledy. Problémem je, jak určit mez, kdy riziko je přijatelné a kdy ne. V klasické zabezpečovací technice se obvykle prosazoval názor, že zařízení je nutno konstruovat tak bezpečně, jak to umožňuje stav techniky, tj. pohybovat se na hranici technicky dosažitelné bezpečnosti. Se stupňující se složitostí zabezpečovacích zařízení se stalo zjevné, že existuje jistá vazba mezi bezpečností, spolehlivostí a cenou zařízení. Sebebezpečnější zabezpečovací zařízení nezvýší bezpečnost železniční dopravy, bude-li tak složité (nebo postaveno z tak nekvalitních prvků), že bude nespolehlivé, protože provoz se nakonec bude odehrávat s jeho vyloučením. Podobně sebebezpečnější zařízení bezpečnost nezvýší, bude-li z cenových důvodů pro železnici v širším měřítku nedostupné. Tato konstatování ovšem nelze zneužívat jako výmluvy.

V současné době dochází mezi železnicemi k jisté shodě v metodice hodnocení bezpečnosti všech na železnici používaných systémů (nejen zabezpečovacích). Prostředkem je analýza rizik. Pro ni je třeba klasifikovat četnost a závažnost výskytu hazardních stavů. Následující tabulky jsou převzaty z normy EN 50 126. V tabulce 7-1 jsou uvedeny kvalitativní definice pravděpodobnostních úrovní výskytu hazardního stavu. Obdobné definice úrovně závažnosti hazardního stavu jsou v tabulce 7-2. Kombinací úrovně pravděpodobnosti a úrovně závažnosti lze získat matici (tabulka 7-3), v níž lze vyznačit a klasifikovat oblasti různého rizika. Definice těchto rizikových oblastí obsahuje tabulka 7-4. Pokud by se kvalitativní ukazatele

doplnily o kvantitativní (což je v tabulce 7-3 naznačeno) získal by se praktičtější návod pro určení přijatelnosti rizika. Tak daleko ovšem zatím zmiňovaná shoda nesahá, což je patrno z toho, že kvantitativní ukazatele jsou doplněny faktory x a y, které mohou nabývat hodnot ...0,1; 1; 10 ... a které si mohou jednotlivé železnice určit ve vlastní zodpovědnosti podle celkových bezpečnostních cílů o které usilují. Přesto tento postup uvádíme jako jistý trend a metodu, kterou lze v určité míře aplikovat i na zabezpečovací zařízení a to jako doplněk pro tu oblast zabezpečovacího zařízení, kterou, při splnění všech kvalitativních požadavků, lze jednoznačně kvantifikovat.

Úroveň	Definice	Kvantifikace
Vysoce nepravděpodobný	Extrémně nepravděpodobný výskyt; lze předpokládat, že se riziko neobjeví	$x.10^{-7}$
Nepravděpodobný	Nepravděpodobný ale možný výskyt; lze předpokládat, že se riziko objeví výjimečně	$x.10^{-6}$
Vzdálený	Možná se objeví několikrát za dobu životnosti zařízení; bude rozumné riziko očekávat	$x.10^{-5}$
Nahodilý	Možná se několikrát objeví; riziko lze očekávat několikrát	$x.10^{-4}$
Pravděpodobný	Několikrát se objeví; riziko lze očekávat často	$x.10^{-3}$
Častý	Pravděpodobnost výskytu častá; riziko lze očekávat trvale	$x.10^{-2}$

Tab. 7-1 Klasifikace pravděpodobnosti výskytu hazardních stavů

Úroveň	Definice	
	Důsledek pro osoby	Důsledek pro službu
Katastrofická	Vícenásobné úmrtí a/nebo těžká zranění	
Kritická	Jednotlivé úmrtí nebo těžké zranění	Rozpad systému
Okrajová	Drobnější zranění	Hrubé narušení systému
Nevýznamná	Možnost ojedinělého drobného poranění	Narušení systému

Tab. 7-2 Klasifikace následků nehod, které mohou z hazardních stavů plynout

	Úroveň pravděpodobnosti výskytu hazardu	Klasifikace rizika			
$y.10^{-2}$	Častý		Nepřípustné		Nežádoucí
y.10-3	Pravděpodobný				Přípustné
y.10-4	Nahodilý		Nežádoucí		
y.10-5	Vzdálený			Přípustné	
y.10-6	Nepravděpodobný	Přípustné			
y.10-7	Vys. nepravděp.			Zanedbatelné	
		Katastrofická	Kritická	Okrajová	Nevýznamná
		Úroveň závažnosti hazardu			
		$x.10^{-1}$	x.10-2	x.10-3	x.10-4

Tab. 7-3 Princip matice rizik

Úroveň	Definice
Nepřípustné	Musí být vyloučeno
Nežádoucí	Může být připuštěno pouze se souhlasem schvalovatele pokud je redukce rizika neproveditelná
Přípustné	Lze připustit s odpovídající kontrolou a souhlasem schvalovatele
Zanedbatelné	Přijatelné se souhlasem schvalovatele

Tab. 7-4 Klasifikace rizik

Pro srovnání uveďme následující spekulaci, která kvantifikuje tolerovatelné hazardní poruchové stavy u zabezpečovacích zařízení:

- předpokládejme, že tolerovatelná četnost velkých železničních nehod vlivem hazardních poruch technických zařízení na všech evropských železnicích je jedna za rok, tj. $10^{-4}\,h^{-1}$,
- předpokládejme, že k nehodě vede zhruba každá desátá hazardní porucha technických zařízení. Pak tolerovatelná četnost hazardních poruch všech technických zařízení na železnicích v Evropě je $10^{-3}\,h^{-1}$,
- předpokládejme, že z tohoto počtu 10 % poruch se týká zabezpečovacích zařízení. Pak tolerovatelná četnost hazardních poruch všech zabezpečovacích zařízení na železnicích v Evropě je $10^{-4}\,h^{-1}$,
- ponecháme-li pro další úvahy rezervu jednoho řádu (např. na chybu dvou posledních odhadů), můžeme dále uvažovat s hodnotou $10^{-5}\,h^{-1}$,
- odhadněme dále, že v Evropě se může vyskytovat 1000 komplexních zabezpečovacích systémů (např. hlavní trať, uzel). Pak tolerovatelná četnost hazardních poruch na jeden komplexní zabezpečovací systém je $10^{-8}\,h^{-1}$,
- předpokládejme, že komplexní zabezpečovací systém se skládá z 10ti subsystémů (např. staničních zařízení). Pak tolerovatelná četnost hazardních poruch jednoho subsystému je $10^{-9}\,h^{-1}$,
- předpokládejme, že jeden subsystém se skládá ze 100 elementů (např. k.o., výhybková jednotka, návěstní jednotka). Pak tolerovatelná četnost hazardních poruch jednoho elementu je $10^{-11}\,h^{-1}$,
- předpokládejme, že jeden element se skládá ze 100 elementárních stavebních prvků (např. relé, přepínač přestavníku, kontrolní tyč, spojka, vedení, usměrňovač). Pak průměrná tolerovatelná četnost hazardních poruch jednoho elementu je $10^{-13}\,h^{-1}$.

Samozřejmě, že rozdělení četnosti hazardních poruch na jednotlivé prvky by bylo nutné provést individuálně, s respektováním všech zvláštností, tedy s rozdíly přesahujícími i několik řádů. Přesto tento hrubý odhad dává představu o tom, že např. relé s četností výskytu nebezpečné poruchy větší než $10^{-13}\,h^{-1}$ je pro splnění shora uvedených cílů jistě nepoužitelné. Podobně zjednodušeně je možné konstatovat, že zabezpečovací technik by neměl být spokojen se subsystémy u nichž pravděpodobná četnost hazardní události je větší než $10^{-9}\ h^{-1}$ i když byly dodrženy veškeré kvalitativní bezpečnostní požadavky (10^9 h = 114155 let)[1].

Bezpečnost zabezpečovacího systému mohou přímo či nepřímo ovlivnit spolehlivostní parametry zařízení. Lze očekávat, že vzrůstající poruchovost zařízení bude doprovázena také vzrůstem obecné četnosti výskytu hazardních stavů ale také četností výskytu hazardního stavu v uvažovaném časovém okně (druhá porucha). V druhém případě, pokud zabezpečovací zařízení bude z jakéhokoliv důvodu provozu neschopné, budou vlaky pokračovat v jízdě řízeny náhradním způsobem, pravděpodobně s výhradně lidským rozhodováním. Protože četnost lidských chyb bývá až o několik řádů vyšší než četnost nebezpečných poruch zabezpečovacích technických systémů, dojde nepřímo k redukci celkové bezpečnosti systému.

[1] Problémem je, že neumíme ze spolehlivostních parametrů určitého zařízení dedukovat četnost jeho hazardních stavů - ne každá porucha vyvolá přímo hazardní stav.

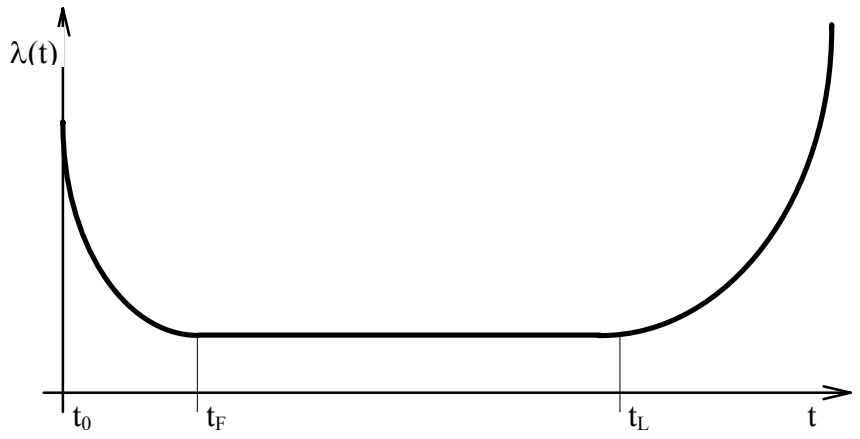
7.2 Spolehlivost

Pod termínem spolehlivost rozumíme souhrnný termín popisující pohotovost včetně všech činitelů, které ji ovlivňují, tj. bezporuchovost, udržovatelnost a zajištěnost údržby. Pro dosažení požadovaných cílů je třeba vždy posuzovat celý komplex a nikoliv jen bezhlavě usilovat o dosažení co nejlepšího dílčího parametru. Jen tak lze předejít neúčelně vynaloženým nákladům.

Výpočty spolehlivostních parametrů lze vztahovat na všechny typy poruch (bez ohledu na příčinu, projev i následek) nebo na vybrané druhy (např. na poruchy bezpečné a nebezpečné).

7.2.1 Bezporuchovost

Bezporuchovost je definována jako schopnost objektu plnit v daných podmínkách a daném časovém intervalu požadovanou funkci. Ukazatelem bezporuchovosti jsou (kromě jiných) četnost (intenzita) poruch λ [h^{-1}] nebo střední doba provozu mezi poruchami MTBF[h], pravděpodobnost bezporuchového provozu v čase t - R(t)[-] nebo pravděpodobná doba mezi poruchami t_p [h].



Obr. 7-1

Rozložení poruch elektronických systémů se obvykle vyjadřuje vanovou křivkou (viz obr. 7-1). V časovém intervalu < t_F ; t_L >, tj. při omezení zleva ukončeným zahořování zařízení (během něhož proud poruch výrazně klesá) a zprava pak uplynutím doby životnosti zařízení (kdy proud poruch výrazně stoupá), lze považovat všechny výše uvedené parametry za konstantní. Pro popis rozložení pravděpodobnosti poruch v tomto intervalu se používá Weibullovo, nebo zjednodušeně exponenciální rozdělení. Pak lze definovat :

kumulovanou (celkovou) pravděpodobnost, že v době < 0 ; t > dojde k výskytu poruchy

$$\mathbf{p_t = 1 - e^{-\lambda t}},$$

pravděpodobnou dobu mezi poruchami jako

$$\mathbf{t_p = \frac{k_D}{\lambda}},$$

kde k_D je dolní mez konfidenčního intervalu zohledňujícího konfidenci (důvěryhodnost) ukazatele t_p,

pravděpodobnost bezporuchového provozu za dobu t

$$\mathbf{R(t) = 1 - p = e^{-\lambda t}}$$

a pravděpodobnost poruchy v době $< t, t+\Delta t >$

$$\mathbf{p_{\Delta t} = p_{t+\Delta t} - p_t = e^{-\lambda t} - e^{-\lambda(t+\Delta t)}}.$$

7.2.2 Pohotovost

Pohotovostí zařízení je schopnost zařízení nacházet se, v daném časovém okamžiku a v daných podmínkách, v provozuschopném stavu. Pro dosažení vyšší pohotovosti zařízení (což je pro uživatele obvykle rozhodující spolehlivostní parametr) lze ovlivňovat bezporuchovost zařízení (či jeho části) vhodnějším výběrem součástek a jejich vhodným konkrétním zapojením na základě znalosti spolehlivostních parametrů jednotlivých součástí. Celkovou pohotovost systému ale ovlivňují další aspekty : vhodná architektura systému (modularita, zálohování), vhodná údržba (např. automatická diagnostika) a vhodná organizace údržby (která např. zajistí, že v potřebnou dobu je na potřebném místě jak vhodný materiál, tak vhodný personál). Hlavním problémem je posoudit přínos jednotlivých složek, vyhodnotit různé kombinace a nalézt nejlepší a přitom ekonomické řešení. Pohotovost zařízení se hodnotí součinitelem technického využití K_{tv}:

$$\mathbf{K_{tv} = \frac{\sum t}{\sum t + \sum t_{oo} + \sum t_{ou}}}$$

kde Σ t je celková doba úplné provozuschopnosti,
Σ t_{oo} je celková doba detekce poruch + celková doba oprav
Σ t_{ou} je celková doba technických prostojů (preventivní údržby atd.).

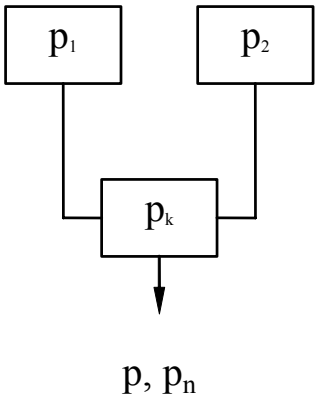
7.2.3 Udržovatelnost

Pro zmíněný vliv na pohotovost a bezpečnost musí být pro zabezpečovací systém definována údržba a to jak po technické, tak i organizační stránce. Ukazatelem náročnosti zařízení na údržbu může být např. doba opravy (doba potřebná k lokalizaci poruchy, k jejímu odstranění a ke kontrole správnosti funkce po opravě) a náročnost na preventivní údržbu (doba preventivní údržby a její četnost). Souhrnným ukazatelem pro kvalitu údržby může být doba poruchového prostoje, tj. doba organizačního prostoje (doba oznámení poruchy, čekání na opraváře, náhradní díly atd.) a doba opravy. Vliv na tyto ukazatele mají technická opatření na straně výrobku (modularita, diagnostika atd.), ale neméně důležitou okolností je organizace údržby (rozmístění údržbářů, jejich proškolení, vybavení odpovídajícími přístroji a nástroji atd.). Existuje také jistá závislost mezi požadavky na kvalitu údržbářů a kvalitu pomůcek. Kvalitnější pomůcky obvykle umožňují správné provedení práce i méně kvalifikovanému personálu.

Obvyklými parametry udržovatelnosti jsou střední doba údržby $t_{oú}$, a střední doba opravy t_{oo}.

7.3 Pravděpodobnost

Uvažujme pravděpodobnost nebezpečné poruchy p_n jako kumulovanou pravděpodobnost výskytu nebezpečné poruchy za dobu t. Dále uvažujme mezní hodnotu pravděpodobnosti nebezpečné poruchy p_N jako maximální pravděpodobnost výskytu nebezpečné poruchy určitého zařízení, požadovanou např. závaznými předpisy nebo normami. V každém zabezpečovacím systému musí vždy platit $p_n < p_N$.



Obr. 7-2

U systému s vnitřní bezpečností by bylo třeba výpočty prokázat, že sérioparalelní kombinace prvků (s určitou konkrétní pravděpodobností nebezpečných poruch) z níž se systém skládá, nevede k překročení stanoveného limitu. Reakční struktury se vyznačují obvykle jedinou větví, která zpracovává všechny bezpečnostně relevantní funkce. Pravděpodobnost výskytu nebezpečné poruchy na dobu delší, než povolenou je zde proto dána kombinací pravděpodobnosti výskytu hazardního stavu na výstupu a pravděpodobnosti nebezpečného selhání zařízení detekujícího poruchy. U redundantních struktur 2 ze 2 nebo 2 ze 3 je výsledná hodnota pravděpodobnosti nebezpečné poruchy dána kombinací pravděpodobnosti vzniku nebezpečných poruch se shodným projevem ve dvou větvích systému, pravděpodobnosti postupného vzniku dvou nezávislých nebezpečných poruch v čase kratším, než je detekční rychlost komparátoru a pravděpodobností nebezpečné poruchy komparátoru. Přes známé problémy se získáním věrohodných výchozích hodnot je v následujícím takový rozbor naznačen, protože poskytuje řadu poznatků i bez konkrétních čísel.

Na obr. 7-2 je blokové schéma redundantní konjunktivní struktury se dvěma větvemi (s pravděpodobností poruchy p_1 a p_2) a komparátorem (s pravděpodobností poruchy p_k). Pravděpodobnost jakékoliv poruchy této struktury je dána součtem pravděpodobnosti poruch jednotlivých částí p_1, p_2, p_k (za předpokladu, že p_1, p_2, $p_k \ll 1$), protože každá z nich musí být funkční, aby byl funkční celek

$$\mathbf{p = p_1 + p_2 + p_k \cong 2p_1 + p_k}.$$

Pravděpodobnost nebezpečné poruchy vlivem výskytu nebezpečných poruch se shodným projevem v obou větvích je

$$\mathbf{p_{n1} = p_1 p_2 \frac{x_{12}}{x_1 x_2} q \cong p_1^2 \frac{x_{12}}{x_1^2} q},$$

kde x_1, x_2 jsou množiny poruchových stavů v jednotlivých větvích,
x_{12} je množina poruchových stavů společných oběma větvím,
q je míra ohrožení, tj. pravděpodobnost, že porucha bude nebezpečná a
přibližný výraz platí pro případ, že obě větve jsou shodné.

Pravděpodobnost nebezpečné poruchy vzniklé u redundantního systému tím, že po nebezpečné poruše jedné větve dojde (v časovém okně Δt od vzniku této první poruchy do jejího vyhodnocení komparátorem) k obdobné poruše v druhé větvi je

$$\mathbf{p_{n2} = \left(p_1 \cdot p_{2\Delta t} + p_2 \cdot p_{1\Delta t}\right) \cdot q \cong 2p_1 \cdot p_{1\Delta t} \cdot q}$$

a pravděpodobnost nebezpečné poruchy komparátoru je

$$\mathbf{p_{n3} = p_k \cdot q}.$$

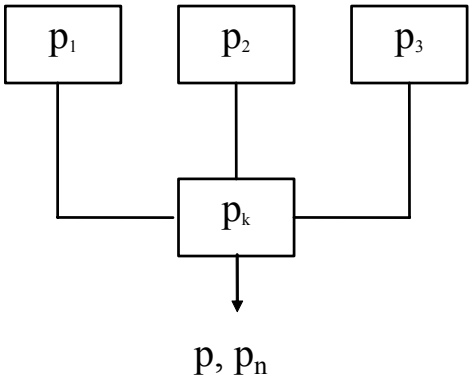
Použijeme-li přibližné výrazy, platné pro případ, že obě větve jsou shodné, dostaneme z předchozího výraz pro pravděpodobnost nebezpečné poruchy celé struktury

$$p_n = p_{n1} + p_{n2} + p_{n3} \cong \left(p_1^2 \frac{x_{12}}{x_1^2} + 2p_1 \cdot p_{1\Delta t} + p_k \right) \cdot q$$

Jednotlivé členy mnohočlenu naznačují cestu, jak lze danou strukturu učinit bezpečnější. První člen lze například zmenšit zmenšením x_{12}, tedy diverzifikací obou větví. Druhý člen ukazuje příznivý vliv zkracování doby Δt, nutné pro detekci poruchy a odstavení zařízení. Dominantní však pravděpodobně zůstane člen třetí (v prvních dvou se pravděpodobnost vyskytuje v druhé mocnině), což dokládá mimořádně vysoké nároky na spolehlivost komparátoru, pro níž by mělo vždy platit, že

$$p_k < p_1^2 .$$

I to je důvod pro přetrvávající používání reléových komparátorů u některých jinak plně elektronických systémů.



Obr. 7-3

Pro majoritní strukturu z obr. 7-3 bude obdobně pravděpodobnost poruch způsobujících výpadek systému:

$$p = p_1 p_2 + p_2 p_3 + p_1 p_3 + p_k \cong 3p_1^2 + p_k ,$$

pravděpodobnost nebezpečné poruchy vlivem výskytu nebezpečných poruch se shodným projevem v obou větvích

$$p_{n1} = p_1 p_2 \frac{x_{12}}{x_1 x_2} q_1 + p_2 p_3 \frac{x_{23}}{x_2 x_3} q_2 + p_1 p_3 \frac{x_{13}}{x_1 x_3} q_3 \cong 3p_1^2 \frac{x_{12}}{x_1^2} q ,$$

pravděpodobnost nebezpečné poruchy vzniklé tím, že po nebezpečné poruše jedné větve dojde (v časovém okně od vzniku první poruchy do jejího vyhodnocení komparátorem) k obdobné poruše v další větvi bude

$$p_{n2} \cong 6p_1 \cdot p_{1\Delta t} \cdot q$$

Jak patrno, ve srovnání s konjunktivní strukturou mohou majoritní systémy 2 ze 3 v praktických případech nabídnout vyšší spolehlivost, ale nikoliv bezpečnost. Navíc požadavek na vysokou spolehlivost komparátoru se tentokrát týká složitějšího hlasovače.

8 OVĚŘOVÁNÍ BEZPEČNOSTI

Při návrhu zabezpečovacích zařízení je nutné ověřovat, že jsou řádným způsobem plněny jak funkční požadavky, tak požadavky na technickou bezpečnost. To se děje tzv. rozborem bezpečnosti. Ten je vždy, byť ve zjednodušené podobě a třeba pouze intuitivně, opakovaně zahrnut ve všech úvahách zkušeného návrháře v průběhu práce na zabezpečovacím zařízení. Na závěr určitých etap práce je však nezbytné vypracovat rozbor bezpečnosti se všemi formálními náležitostmi pro definitivní provedení výrobku. Tento rozbor pak tvoří součást průkazu bezpečnosti a jeho pozitivní závěry jsou jedním z nepominutelných podkladů pro schválení a uvedení zařízení do provozu.

Rozbor bezpečnosti obecně dokládá ověření:

- řádné funkce při bezporuchovém stavu,
- důsledků náhodných poruch, cizích vlivů a chybné obsluhy,
- nezávislosti redundantních částí a jejich odolnosti proti společným chybám,
- detekce jednotlivých poruch a funkcí po detekci (zachování bezpečného stavu),
- ochran proti systematickým chybám.

První položka se týká ověření funkční bezpečnosti, další čtyři uvedené položky se týkají ověření technické bezpečnosti.

8.1 Rozbor bezpečnosti

Charakter rozboru bezpečnosti závisí ve značné míře na použitém principu zajištění technické bezpečnosti. U zařízení koncipovaných na principu vnitřní bezpečnosti se zjišťuje, že žádná z uvažovaných chyb (stanovených s přihlédnutím k normalizovanému katalogu poruch) nevede k hazardnímu stavu. U zařízení založených na redundanci je nutné doložit nezávislost redundantních systémů, schopnost vypořádat se se společnými chybami, bezpečnou detekci chyb a dostatečnost akcí, následujících po detekci. U zařízení reakčních je předmětem rozboru bezpečnosti mechanizmus detekce poruchy a opět dostatečnost následujících akcí. Jak patrno, u obou posledních principů je podstatou prokázat, že všechny poruchy, které mohou vést k hazardním stavům, budou v odpovídajícím čase detekovány a jejich vliv zneškodněn. Rozbor bezpečnosti se samozřejmě týká celého zařízení - jak hardware, tak software.

Vlastnímu rozboru bezpečnosti určitého zařízení musí předcházet:

- určení konkrétních zařízení (částí), pro které je třeba rozbor provést – určení částí ovlivňujících bezpečnost,
- určení povahy zařízení (částí) - vnitřní bezpečnost, redundance, reaktivnost - z které pak vyplyne zaměření rozboru bezpečnosti,
- rozdělení rozsáhlejšího zařízení do menších funkčních celků, u kterých ale lze jednoznačně definovat vstupy a výstupy a na kterých lze snáze rozbory provádět postupně,
- určení normálních a případných mimořádných provozních stavů zařízení. Klasicky se za normální provozní stavy považují všechny bezporuchové stavy, v kterém se zařízení může nalézat v souvislosti s obvyklým cyklem zabezpečovacích zařízení, tj. příprava vlakové cesty, příjezd (průjezd) vlaku, odjezd vlaku, návrat zařízení do základního stavu a za mimořádné provozní stavy se považují ty stavy, ve kterých se zabezpečovací zařízení může nacházet vlivem dopravních nepravidelností nebo poruchy některé vnější části zařízení. Tento postup ovšem zahrnuje možnost, že se opomine pro některý stav vstupů definovat výstup, což může vést (a často vede) k nemilým překvapením. Je tedy lépe určit stav všech výstupních signálů zařízení v bezporuchovém stavu pro všechny možné kombinace vstupních veličin podle kritérií odvozených z požadovaných funkčních vlastností,
- určení stavů, které jsou z hlediska zařízení a jeho předpokládaného použití nepřípustné, tj. které by ohrožovaly bezpečnost, nebo naopak určení bezpečného stavu, do kterého zařízení musí přejít vždy, když není z jakéhokoli důvodu nadále schopno dodržet předpokládaný program funkce.

8.1.1 Ověření důsledků náhodných poruch

Ať je použita kterákoliv z technik nebo jejich kombinace, je nutné prokázat odpovídající analytickou metodou, že žádná jednotlivá porucha hardware, vnější vliv nebo omyl obsluhy nezpůsobí nekontrolovaný hazardní stav. Analýza musí být kvalitativní a pokud možno by měla být doplněna i analýzou kvantitativní pro náhodné poruchy hardware. Kvantitativní analýza by pak měla být založena na reálných pravděpodobnostních údajích.

U **zařízení s vnitřní bezpečností** vůbec nesmí k hazardnímu stavu dojít. Porucha může zařízení obecně uvést do stavu, který se z hlediska bezpečnosti dopravy:

- projeví:
  - příznivým způsobem, tj. když v jejím důsledku dojde k nadměrnému omezení, popř. zastavení pohybu kolejových vozidel nebo k omezení, popř. znemožnění další obsluhy zařízení (pokud ovšem nejde o obsluhu vedoucí k omezení nebo zastavení pohybu vozidel),
  - nepříznivým způsobem, tj. když v jejím důsledku dojde ke stavu ohrožujícímu bezpečnost jízdy vlaků nebo zabezpečeného posunu,
- neprojeví.

Za vyhovující se považují zařízení, u nichž je projev každé uvažované poruchy příznivý alespoň v jednom normálním provozním stavu; přitom při ostatních provozních stavech se nesmí žádná z uvažovaných poruch projevit nepříznivým způsobem. U obvodů, které jsou v činnosti pouze při mimořádných provozních stavech, postačuje příznivý projev poruchy při mimořádných provozních stavech.

Neprojeví-li se porucha v žádném provozním stavu, ve smyslu předchozího odstavce, je nutné tuto poruchu postupně uvažovat v kombinaci se všemi ostatními jednotlivými poruchami. Výsledek se pak posuzuje jako u jiné jednotlivé poruchy.

Mimořádně lze v případě, kdy se porucha s malou četností projevila nepříznivým způsobem a nelze ji jiným řešením odstranit, uvážit možnost nebezpečný stav eliminovat přídavným technickým nebo administrativním opatřením. Celá situace a navržené opatření musí být podrobně dokumentována a výslovně předložena schvalovacímu orgánu v závěrech průkazu bezpečnosti poruch. Při posuzování takových mimořádných případů je pak třeba zejména zkoumat přijatelnost, dostatečnost, realisovatelnost a účinnost administrativních a technologických opatření v provozu, výrobě či údržbě a to vše konfrontovat se skutečností, že usilování o vysokou bezpečnost má také své ekonomické hranice.

Ve všech ostatních případech je obvod shledán nevyhovujícím a nelze jej v zabezpečovacím zařízení použít.

U **zařízení redundantních** se ověřování náhodných poruch obvykle týká pouze detekčních (komparačních, hlasovacích) částí a částí zajišťujících požadované funkce po detekci.

U **zařízení reakčních** je nutné zejména prokázat, že všechny poruchy, které by mohly vést k hazardnímu stavu, mohou být a také budou za všech okolností řádně detekovány a že řádně budou zajištěny také všechny požadované funkce po detekci.

8.1.2 Ověření nezávislosti a odolnosti proti společným chybám

U systémů využívajících redundantních částí, u nichž by současná chyba vyvolaná jednou poruchou mohla vést k hazardním stavům, je nutné prokázat vzájemnou nezávislost redundantních částí. Opatření zajišťující nezávislost musí být efektivní po celou dobu životnosti zařízení.

8.1.3 Ověření detekce a funkcí po detekci

Každá porucha, která by sama o sobě nebo v kombinaci s druhou poruchou mohla vést k hazardnímu stavu, musí být v dostatečně krátkém čase detekována a po detekci musí být provedena odpovídající opatření, která bezpečný stav vynutí. V případě redundantních řešení to znamená, že první porucha musí být detekována a k vynucení bezpečného stavu musí dojít v čase natolik krátkém, aby riziko, že druhá porucha (vzniklá během doby detekce a vynucení bezpečného stavu) vyvolá hazardní stav, bylo menší než požadované (obr. 6-1). Tato část musí být kvantifikována s využitím nejpřesnějších dostupných

dat a s přihlédnutím k údajům v kapitole 7 musí být uvedena podrobná diskuse dosažených výsledků. V případě reaktivních řešení to znamená, že maximální doba, kterou zabere detekce a vynucení bezpečného stavu, tj. doba trvání přechodového a tedy potenciálně hazardního stavu, nepřekročí požadovanou hodnotu, kterou je třeba stanovit na základě funkce celého systému a, opět jako v předchozím případě, s ohledem na kvantitativní analýzu rizik (obr. 6-2).

8.1.4 Ověření ochrany proti systematickým chybám

Navíc k opatřením daným programy řízení kvality a bezpečnosti, které mají minimalizovat vliv lidských chyb, je vhodné přijmout také dostupná technická řešení, která by předcházela nepřijatelným rizikům i v případě technických systematických chyb. Toho lze dosáhnout například volbou vhodné architektury systému, která sníží pravděpodobnost výskytu nehody v případě, že se objeví systematická porucha, potenciálně schopná hazardní stav vyvolat. Použité řešení musí být v rozboru podrobeno diskusi.

8.2 Metody

Nejběžnějšími metodami rozboru bezpečnosti jsou analýza důsledků poruch, analýza nezávislosti a důsledků společných chyb (pro redundantní systémy), modelování poruch za použití výpočetní techniky, laboratorní ověřování poruch na skutečném zařízení (nebo dostatečně věrném modelu), simulace, nezávislá kontrola programů a především různé kombinace těchto metod.

V dalším je uveden výčet metod, které jsou, obvykle v různých kombinacích, používány při rozborech bezpečnosti. Volba vhodné metody nebo jejich kombinace závisí na povaze zkoumaného zařízení. V některých případech je při rozboru účelné analyzovat nejprve důsledky poruch s vyšší četností, pak ohrožujících účinků cizích vlivů a nakonec poruch s malou četností. Za vysoce efektivní se při vývoji zařízení považuje doplnění těchto metod, použitých autorem řešení, ještě ověřením funkce zařízení a posouzením rozborů bezpečnosti a programů se zabezpečovacími funkcemi experty, nepodílejícími se přímo na vývoji a konstrukci zařízení a to jednak během vývoje, jako vnitřní opatření firmy (tzv. validace), jednak během schvalovacího procesu experty na firmě zcela nezávislými (tzv. hodnocení neboli technické schválení).

8.2.1 Analýza rizika

Metoda spočívá v analýze rizik, vyplývajících z použitého technického řešení, aby se odhalily slabiny a určila ochranná opatření. Existují-li dostatečně věrohodné podklady, je vhodné analýzu doplnit kvantitativním oceněním jednotlivých rizik.

Analýza se obvykle provádí pro celý systém ještě před detailním návrhem zařízení a na základě pravděpodobnosti výskytu jednotlivých poruch. Výsledky analýzy a z ní plynoucí doporučení se pak berou v úvahu při vlastním návrhu. Obdobně ji však lze použít i pro orientační stanovení problémových míst již hotového zařízení.

8.2.2 Analýza důsledků poruch

Analýza poruchových stavů a jejich důsledků (FMEA - Failure Modes and Effects Analysis) se využívá zejména u řešení využívajících principu vnitřní bezpečnosti. Je systematickou analýzou vlivu všech poruchových stavů u každého prvku zabezpečovacího obvodu na činnost obvodu pro všechny možné provozní podmínky. Jde tedy v zásadě o kvalitativní metodu, označovanou jako postup „zdola-nahoru (bottom-up)“. Možné poruchové stavy jednotlivých stavebních prvků se odvozují z mezinárodně uznávaného katalogu poruch (nyní příloha C „Identifikace poruchových stavů HW součástek“ normy EN 50129). Pokud se mimořádně provádí rozbor obvodu s prvkem, který se v katalogu nenachází, je třeba nejprve analogicky ke katalogu poruchové stavy stanovit.

Metoda umožňuje zjistit potenciální nebezpečí, která z poruchy vyplývají. Následně je pak možné navrhnout opatření, která buď vliv eliminují nebo sníží pravděpodobnost jeho výskytu pod přijatelnou mez. Metodu lze obdobně použít i pro vyšetřování software.

Metodu lze doplnit kvantitativními úvahami o pravděpodobnosti výskytu poruchových stavů a uspořádání podle stupně jejich závažnosti – pokud jsou ovšem k disposici věrohodné údaje. Pak se metoda označuje jako analýza druhů, důsledků a kritičnosti poruchových stavů (FMECA - Failure Modes, Effects and Criticality Analysis).

Obě metody se využívají i v jiných oblastech a existuje pro ně mezinárodní norma IEC 60812, kterou lze rámcově využít i pro zabezpečovací techniku.

8.2.3 Analýza poruchového stromu

Za opak analýzy důsledků poruch lze považovat analýzu poruchového stromu (FTA - Fault Tree Analysis). Jde o deduktivní metodu, která umožňuje, vycházeje z nežádoucí události, určit všechny možné příčiny jejího vzniku, s případným doplňkem určujícím pravděpodobnost jejího výskytu. K této metodě také existuje mezinárodní norma - IEC 61025.

8.2.4 Analýza nezávislosti a důsledků společných chyb

Tato metoda se používá u redundantních systémů. Jde o systematickou analýzu vlivů, které by mohly způsobit společné chyby v redundantních částech systému a ověření skutečné nezávislosti redundantních částí.

U systémů obsahujících redundantní části (hardware nebo software), jejichž současná porucha může vést k hazardnímu stavu, je nezbytné ověřovat nezávislost. Je třeba prokázat, že nedojde ke ztrátě nezávislosti vlivy:

- vnitřními:
    - fyzikálními (galvanické spojení, elektromagnetická vazba),
    - funkčními (zavlečení falešné informace vlivem poruchy druhého systému),
- vnějšími:
    - fyzikálními (elektromagnetická interference, elektrostatický výboj a další působení prostředí; napájení; vstupy a výstupy),
    - funkčními (zavlečení falešné informace z vnějšího zdroje informace vlivem poruchy systému).

8.2.5 Testování funkce

Testování funkce se používá zejména pro ověření shody funkce zkoušeného systému a požadavků (ZTP). Funkční testy se provádějí na kompletním systému, při normálních i mezních okolních podmínkách anebo na jednotlivých dílech, pokud ovšem lze pro ně jednoznačně určit všechny hodnoty výstupů pro všechny kombinace vstupů. Je možné i spojitě porovnávat výsledky testů s očekávanými výsledky.

Úplné testování

Při úplném testování se generují a testují jednotlivé případy systematicky a všechny. Při testování programů tato metoda znamená minimálně jeden průchod každé větve programu. Užívá se vždy, když jde o závěrečné ověření nějaké fáze prací.

Nahodilé testování

Nahodilé testování je metodou, kdy se testovací případy generují nahodile. Tuto metodu lze použít pro zkrácené ověření, že při systematickém testování se skutečně braly v úvahu všechny možné varianty. Podobně lze metodu použít pro předběžné orientační ověření.

8.2.6 Modely a simulace

Při použití matematických modelů, elektrických náhradních schémat nebo simulací, je třeba pamatovat na to, že výsledek bude nesprávný, pokud je založen na nesprávných předpokladech nebo nesprávných numerických hodnotách. Proto je absolutně nezbytné předem potvrdit transformační hypotézy alespoň částečnými zkouškami.

8.2.7 Laboratorní ověřování

Laboratorní ověřování poruch na skutečném zařízení nebo dostatečně věrném modelu umožňují prozkoumat skutečné chování zařízení při poruchách. Toto ověření je naprosto nezbytné provést na klíčových obvodech zařízení s vnitřní bezpečností a pro ujištění, že zvolená náhradní metoda odpovídá skutečnosti.

Část III. - Hlavní subsystémy

9 ZABEZPEČENÍ VÝMĚN

Významnou součástí železničního svršku, s kterou zabezpečovací zařízení aktivně spolupracuje, jsou výhybky. Výhybkové konstrukce se podle konstrukčního uspořádání dělí na jednoduché výhybky, oboustranné výhybky, obloukové výhybky, celé křižovatkové výhybky, poloviční křižovatkové výhybky, jednoduché kolejové spojky, dvojité kolejové spojky a kolejové křižovatky. Výhybky se nově zřizují v soustavách svršku UIC 60 a S 49 a označují se jako výhybky sjednocené soustavy, charakterizované úhlem odbočení (vyjádřeným poměrem) a poloměrem oblouku v odbočné větvi výhybky. V provozu ovšem existují a až do vyčerpání životnosti budou existovat starší konstrukce, odvozené od starších soustav (např. T, R 65) a charakterizované obvykle úhlem odbočení ve stupních.

Pojížděnou část výhybky tvoří opornice, jazyky a srdcovka. Opornice se pořizují z normální kolejnice a v oblasti přiléhání jazyka jsou opatřeny opornicovými opěrkami. Jazyky výhybek sjednocené soustavy se konstruují jako jazyky pérové, tečné, se zkoseným hrotem. Srdcovky se konstruují jednoduché a dvojité a často mají všechny části pevné. Při požadavku na vytvoření nepřerušené pojížděné hrany (zejména pro vysoké rychlosti, ale také pro malá kola) musí mít ovšem srdcovka hrot pohyblivý (používá se zkratka PHS). Pokud má být nepřerušená cesta vytvořena jen v jednom směru, používají se přestavitelné srdcovky s tzv. pohyblivou křídlovou kolejnicí, pro oba směry pak srdcovka s pohyblivým klínem. Dvojité srdcovky se použijí vedle jednoduchých srdcovek v dvojitých kolejových spojkách, křižovatkových výhybkách a kolejových křižovatkách.

Pohyblivé části výhybky se souhrnně nazývají výměna**.** Patří k ní oba jazyky, výměnový závěr(y) včetně spojovacích tyčí a spřáhel. Přiléhání jazyka k opornici a pohyblivých částí dvojitých a jednoduchých srdcovek ke kolenovým nebo křídlovým kolejnicím zajišťuje hákový, rybinový nebo čelisťový závěr (u jazyků dlouhých 14 m a více jsou dva nebo více závěrů, které mohou být navzájem spojeny táhlem a tak ovládány jediným přestavníkem). Konstrukce výměnových závěrů eliminuje přímé silové účinky jedoucího vozidla po jazyku a zamezuje jejich přenosu do stavěcích zařízení. Velikost rozevření a zdvihu stavěcího zařízení je stanovena ve vzorových listech. Závěry se kloubově spojují spojovací tyčí a umožňují postupný pohyb jazyků při přestavování. Spojovací tyč je dále spojena s táhlem výměníku. Zdvih spojovací tyče u ČD musí činit 245 mm, u výhybek na spádovišti s rychloběžnými přestavníky a u srdcovek s pohyblivými hroty 155 mm. Pro jednotlivé typy výměn jsou stanoveny maximálně dovolené hodnoty přestavných sil.

Postupný chod jazyků při přestavování umožňuje řešit výhybky jako rozřezné - tzn. že při jízdě omezenou rychlostí (např. posun s rychlostí do 40 km/h) po hrotu ze směru, pro který není výměna přestavena, kolejové vozidlo průjezdem výhybkou samo přestaví jazyky do polohy nutné pro projetí z tohoto směru, aniž by došlo k poškození výhybky. Výhybkové konstrukce u nichž nelze tuto vlastnost zajistit jsou nerozřezné a při jejich průjezdu z nesprávného směru by mohlo dojít k jejich poškození.

Výměnový závěr se podle předpisů ČD nesmí dát uzavřít, je-li u výhybek pojížděných rychlostí 60 km/h a vyšší mezera mezi jazykem a opornicí 4 mm a větší a u výhybek pojížděných rychlostí menší než 60 km/h mezera 6 mm a větší. Splnění tohoto požadavku se pravidelně kontroluje tzv. západkovou zkouškou.

Součástí výhybek bývá zpravidla i výměník spojený výměníkovým táhlem se spojovací tyčí výměnového závěru. Výměník je opatřen výměnovým závažím na páce, které svým silovým účinkem přidržuje výměnový závěr v požadované poloze. Umožňuje ruční přestavování výměny a současně nese výhybkové návěstidlo.

K zajištění správné funkce kolejových obvodů a zpětného vedení trakčních nebo topných proudů musí být ve výhybkách, kolejových spojkách a křižovatkách provedena izolace příslušných částí výhybek včetně spojovacích tyčí a současně vodivé propojení těch částí výhybky jejichž způsob montáže nezajišťuje elektrickou vodivost.

9.1 Stupně zabezpečení výhybek

Platná norma pro ČD (TNŽ 34 2620) předpisuje požadavky na zabezpečení výhybek ve čtyřech stupních podle rychlosti pojíždění:

a) při I. stupni zabezpečení výhybek (proti hrotu nejvýše 60 km/h) musí být aspoň přilehlý jazyk a přestavitelná srdcovka zapevněny ve správné poloze,

b) při II. stupni zabezpečení výhybek (proti hrotu nejvýše 80 km/h) musí být přilehlý i odlehlý jazyk a přestavitelná srdcovka ve správné poloze buď elektricky uzavřeny a současně elektricky kontrolovány v obvodu povolujícího návěstního znaku nebo mechanicky zapevněny,

c) při III. stupni zabezpečení výhybek (proti hrotu nejvýše 120 km/h) musí být přilehlý i odlehlý jazyk a přestavitelná srdcovka buď elektricky uzavřeny a současně elektricky kontrolovány v obvodu povolujícího návěstního znaku ve správné poloze, která odpovídá uzavřeným hákovým závěrům nebo musí být mechanicky zapevněny tak, aby bylo znemožněno otevření hákových závěrů,

d) při IV. stupni zabezpečení výhybek (nejvýše 160 km/h) musí být přilehlý i odlehlý jazyk a přestavitelná srdcovka mechanicky zapevněny ve správné poloze tak, aby bylo znemožněno otevření hákových závěrů a správná poloha výhybky musí být elektricky kontrolována v obvodu povolujícího návěstního znaku.

Pro jízdu po hrotu dovolují výhybky zabezpečené I., II. nebo III. stupněm rychlost až 120 km/h.

Předpis ČD T 100 uvádí jakými prostředky lze jednotlivé stupně zabezpečení výhybek dosáhnout, tj. uvádí použitelná zabezpečovací zařízení či jejich kombinace:

- pro I. stupeň:
  a) výměnový zámek,
  b) mechanický přestavník nebo
  c) elektromagnetický zámek s kontrolou polohy výhybky,
- pro II. stupeň:
  a) mechanický závorník,
  b) elektromotorický přestavník s kontrolou jazyků nebo
  c) uzamykatelný závorník,
- pro III. stupeň:
  a) výměnový a odtlačný zámek,
  b) mechanický závorník a stojanový zámek,
  c) mechanický závorník a odtlačný zámek nebo
  d) mechanický přestavník a mechanický závorník,
- pro IV. stupeň:
  a) elektromotorický přestavník s kontrolou jazyků a elektromagnetický závorník (u elektromotorických přestavníků typu EP 600 se elektromagnetický závorník nepoužívá).

Výše uvedená normativní a předpisová ustanovení zasluhují podrobnější diskusi. Mezi základní nedostatky patří chybějící definice mechanického zapevnění (kvalitativní či kvantitativní) a nedostatečnost i přímé kontroly polohy jazyků. Zejména pro vyšší rychlosti bude pravděpodobně nezbytné uvažovat o kontrole tvaru pojížděné hrany výměny a kontrole šířky žlábku.

Při I. stupni zabezpečení výhybek (60 km/h) musí být aspoň přilehlý jazyk a přestavitelná srdcovka zapevněny ve správné poloze. Pro jednotlivé použitelné technické prostředky platí:

- závěrný hák výměnového zámku kontroluje přiléhání jazyka v předepsané toleranci. Tento způsob zabezpečení je možno používat pouze u výhybek, které jsou pod dohledem dopravního pracovníka, neboť je nutno vyloučit zásah nepovolané osoby vedoucí k přeložení výměníkového závaží do polohy neodpovídající poloze uzamčené výhybky. Došlo by tak k vyklesnutí závěrného ústrojí výhybky a veškeré silové účinky by při pojíždění výhybky zachycoval pouze závěrný hák výměnového zámku, který pro tento účel není konstruován,
- u mechanického přestavníku (MP) se v mezích předepsaných provozních podmínek (délka drátovodných táhel, velikost přestavných odporů výhybky, počty odbočných bodů ap.) zaklesnutím západky výměnové stavěcí páky kontroluje, že byl vykonán celý předepsaný pohyb stavěcího (závěrného) ústrojí nutný pro řádné přestavení výhybky. Poloha přilehlého i odlehlého jazyka je kontrolována nepřímo a vychází z předpokladu celistvosti a neporušenosti závěrného ústrojí a jeho spojení s přestavníkem, které se kontroluje při denních prohlídkách výhybek dopravními pracovníky. Předepsaná tolerance přiléhání jazyka je kontrolována rovněž nepřímo

tím, že dojde k zaklesnutí výměnového závěru, jehož správnost seřízení se periodicky kontroluje tzv. západkovou zkouškou. Vykonáním celého předepsaného chodu výměnového závěrného ústrojí je (rovněž za předpokladu jeho neporušené celistvosti) zajištěna správná poloha odlehlého jazyka. Soustava mechanického přestavníku spolu s rozřeznou spojkou výměnové stavěcí páky (za předpokladu celistvosti drátových táhel) zajišťuje při současném silovém působení výměníkového závaží v horní poloze dostatečnou přídržnou silou zapevnění výměnového závěrného ústrojí v uzavřené poloze za všech provozních režimů výhybky, tím je současně zapevněn i přilehlý jazyk.

- u elektromotorického přestavníku (EMP) je situace analogická jako v případě MP. Při použití EMP bez kontroly polohy hrotnic je mechanická kontrola koncové polohy u MP nahrazena elektrickou kontrolou koncové polohy stavěcího ústrojí. Zapevnění závěrného ustrojí výměny pak zajišťuje s mnohonásobnou rezervou rozřezná spojka tohoto přestavníku při současném spolupůsobení silového účinku výměnového závaží v horní poloze. Vyšší technická kvalita, spolehlivost a nezávislost provedení elektrické kontroly na způsobu obsluhy a proměnných provozních podmínkách (přestavné odpory, předpětí drátových táhel ap.) u EMP bez kontroly polohy hrotnic proto dovoluje zajistit tento stupeň zabezpečení výhybek s mnohonásobnou rezervou.

K I. stupni zabezpečení výhybek lze poznamenat, že užití pouze odtlačného zámku k zabezpečení výhybky (za předpokladu správně seřízeného výměnového závaží tak, aby se neudrželo v nesprávné poloze a vlastní vahou se vrátilo do správné polohy) zabezpečí výhybku mnohem lépe (nelze vyklesnout závěr výměny) i při pouze nepřímé kontrole polohy přilehlého jazyka než samotný výměnový zámek. Současně je tak řešena i otázka střežení výhybky. Možnost použít EMP bez kontroly polohy hrotnic by měla být do předpisu T100 doplněna, protože s jeho pomocí lze dostatečně zabezpečit výměny na většině vedlejších kolejí ve stanici.

Při II. stupni zabezpečení výhybek (80 km/h) musí být přilehlý i odlehlý jazyk a přestavitelná srdcovka ve správné poloze buď elektricky uzavřeny a současně elektricky kontrolovány v obvodu povolujícího návěstního znaku nebo mechanicky zapevněny. V tomto místě je nezbytné upozornit, že definice tohoto stupně zabezpečení výhybek je poněkud nepřesná, neboť pouze elektrické uzavření kontrolovaných částí by minimálně vyžadovalo výhybku střežit před zásahem nepovolané osoby a vyžadovalo by silové působení výměnového závaží ve spodní poloze. Ve skutečnosti vždy spolupůsobí přídržná síla rozřezné spojky EMP. Pro nejběžněji používané technické prostředky platí:

- mechanický závorník (MZ) kontroluje správnou polohu přilehlého jazyka v předepsané toleranci, dále kontroluje, že se odlehlý jazyk nepřiblížil k opornici více než na dovolenou minimální vzdálenost (90 mm), která není "provozní tolerancí" výhybkové konstrukce, ale dokáže ještě zajistit průjezd vozidla výhybkou požadovaným směrem. Současně zapevňuje výše uvedené části výhybky. Toto snížení nároků na kontrolu polohy odlehlého jazyka vyplývá ze snahy zachovat rozřeznost výhybky i při použití z principu nerozřezného závorníku. To umožňuje při nesprávném pojíždění výhybky vyklesnutí závěrného ústrojí výměny a po poškození mechanického závorníku dojde již běžným způsobem k dokonaní rozřezu zpravidla bez poškození součástí výhybky. Není kontrolováno vykonání celého přestavného chodu závěrného ústrojí a toto není zapevněno jinak než silovým působením výměnového závaží ve spodní poloze; z toho plyne, že takto zabezpečená výhybka musí být pod dohledem dopravního pracovníka - viz podmínky pro výměnový zámek. Analogická je situace pro uzamykatelný závorník.
- EMP s kontrolou hrotnic kontroluje polohu obou jazyků, vykonání celého chodu přestavného ústrojí a zapevňuje přestavné ústrojí v koncové poloze přídržnou silou rozřezné spojky a spolupůsobením silového účinku výměnového závaží v horní poloze.

Při III. stupni zabezpečení výhybek (120 km/h) musí být přilehlý i odlehlý jazyk a přestavitelná srdcovka buď elektricky uzavřeny a současně elektricky kontrolovány v obvodu povolujícího návěstního znaku ve správné poloze, která odpovídá uzavřeným výměnovým závěrům nebo musí být mechanicky zapevněny tak, aby bylo znemožněno otevření výměnových závěrů. V tomto místě je opět nezbytné upozornit, že i definice tohoto stupně zabezpečení výhybek je poněkud nepřesná, neboť pouze elektrické uzavření kontrolovaných částí by minimálně vyžadovalo výhybku střežit před zásahem nepovolané osoby a vyžadovalo by silové působení výměnového závaží ve spodní poloze. Ve skutečnosti vždy spolupůsobí přídržná síla rozřezné spojky EMP. Pro nejběžněji používané technické prostředky platí:

- výměnový a odtlačný zámek - závěrný hák výměnového zámku kontroluje přiléhání jazyka a závěrný hák odtlačného zámku kontroluje správnou polohu odlehlého jazyka v předepsané toleranci. Odtlačný zámek současně zapevňuje závěrné ústrojí vyhybky tak, aby bylo

znemožněno otevření výhybkového závěru. Veškeré silové účinky vyvolané jízdou železničních vozidel působí na závěrné ústrojí výhybky, které je kromě mechanického zapevnění odtlačným zámkem proti nežádoucí manipulaci přidržováno ve správné poloze silovým působením výměníkového závaží ve spodní poloze. Závěrné háky zámků jsou sice opatřeny vrubem, který má usnadnit jejich ulomení při nesprávném pojíždění výhybky a tak umožnit vyklesnutí výměnového závěru pro předejití poškození výhybky, ale skutečný průběh a výsledek celého procesu řezání výhybky, který je závislý na mnoha faktorech, nelze vždy zaručit.

- mechanický závorník a stojanový zámek - mechanický závorník kontroluje požadovanou polohu přilehlého i odlehlého jazyka, stojanový zámek uzavírá výměník a tím i výměníkové závaží ve spodní poloze a tím znemožňuje vyklesnutí výměnového závěru. Rozřez výhybky se neobejde bez destrukce některých součástí výhybky i zabezpečovacího zařízení.
- mechanický závorník a odtlačný zámek - platí obdobné podmínky jako v předešlém bodě, stojanový zámek je nahrazen zámkem odtlačným, který kromě zajištění uzavřeného výměnového závěru ještě zpřísňuje kontrolu polohy odlehlého jazyka. Při rozřezu dochází rovněž k destrukci součástí výhybky i zabezpečovacího zařízení.
- mechanický přestavník a mechanický závorník - mechanický přestavník kontroluje vykonání celého chodu přestavného ústrojí a zapevňuje silou rozřezné spojky výměnové stavěcí páky spolu se silovým působením výměníkového závaží v horní poloze výměnový závěr v uzavřené poloze. Současně mechanický závorník kontroluje a zapevňuje přilehlý jazyk v předepsané poloze a nedovolí odlehlému jazyku přiblížit se k opornici na méně než předepsanou vzdálenost (90 mm), což ovšem umožňuje vyklesnutí výměnového závěru. Tato skutečnost má za následek, že při řezání výhybky dojde většinou pouze k destrukci mechanického závorníku, pokud je použito rozřezného mechanického přestavníku.

Při IV. stupni zabezpečení výhybek (160 km/h) musí být přilehlý i odlehlý jazyk a přestavitelná srdcovka mechanicky zapevněny ve správné poloze tak, aby bylo znemožněno otevření výměnových závěrů a správná poloha výhybky musí být elektricky kontrolována v obvodu povolujícího návěstního znaku. K této definici nutno poznamenat, že v budoucnu bude nutno pro konkrétní typ výhybky tento způsob zabezpečení vyjádřit vzorovým výkresem zabezpečení výhybky, neboť přibývají požadavky na kontrolu polohy jazyka v dalších místech mimo hrot a protože výhybky pro větší rychlosti se zpravidla vyznačují i více závěry, u nichž již není možno zaručit rozřeznost výhybky, je nutno je vybavovat i prvky pro kontrolu najetí do výhybky z nesprávného směru. Pro tyto případy se uplatňují následující zásady:

1) Výhybka s více závěry (s přídavným, s pomocným, nebo přídavným i pomocným závěrem) musí být vybavena zařízením pro vyhodnocení najetí z nesprávného směru podle bodu 3. Není-li přes takovou výhybku realizován nezabezpečený posun, smí být vybavena nerozřezným přestavníkem.
2) Výhybka s PHS musí být vybavena zařízením pro vyhodnocení najetí z nesprávného směru do PHS a smí být vybavena nerozřezným přestavníkem, i když je přes ni veden nezabezpečený posun.
3) Výhybky, které musí být vybaveny zařízením pro vyhodnocení najetí z nesprávného směru, se vybavují takto:
    - výhybka, která není sdružena ve spojce musí být vybavena zařízením pro vyhodnocení najetí z nesprávného směru z obou větví,
    - sdružené výhybky, mezi které je dovoleno odstavovat kolejová vozidla, musí být vybaveny zařízením pro vyhodnocení najetí z nesprávného směru z obou větví,
    - sdružené výhybky, mezi které není dovoleno odstavovat kolejová vozidla, musí být vybaveny zařízením pro vyhodnocení najetí z nesprávného směru jen z větve, která nesměřuje ke sdružené výhybce.
4) Přilehlá poloha jazyka pojížděného rychlostí větší než 120 km/h musí být vícebodově kontrolována.
5) Výhybka jednozávěrová bez PHS se nevybavuje ani nerozřezným přestavníkem, ani zařízením pro vyhodnocení najetí z nesprávného směru.

Termín "zapevnění" pohyblivé součásti výhybky vyjadřuje technickými prostředky zajištěnou fixaci výhybkové součásti v požadované poloze tak, aby bylo znemožněno její přestavení. Tyto technické prostředky zpravidla s výše uvedeným zapevněním slučují i kontrolní funkci (kontrolují v předepsaných tolerancích správnou polohu příslušných součástí výhybky) a současně poskytují možnost vytvořit závislost výhybky na zabezpečovacím zařízení. Výraz "mechanické zapevnění" nelze chápat jako absolutní pojem, ale je třeba je charakterizovat v silovém vyjádření. Veškeré silové účinky vyvolané jízdou železničních vozidel, případně způsobené vlastnostmi výhybkové konstrukce (např. pružení jazyků ap.) zachycuje závěrné ústrojí

výhybky (závěrný hák, čelist). Výjimku tvoří přestavníky s vnitřním závěrem, které přebírají funkci závěrného ústrojí výhybky. Každý typ výhybky je navržen tak, aby při všech režimech pojíždění výhybky bylo závěrné ústrojí výhybky spolehlivě přidržováno v požadované poloze silou vyvolanou výměníkovým závažím ve spodní poloze (bez "gatí").

U výhybek zabezpečených pouze výměnovými zámky se plně uplatňuje tento účinek výměnového závaží a z toho plyne, že výměnové zámky mají pouze charakter kontrolní a "vazební" (včetně ochrany před nechtěným přestavením do nežádoucí polohy omylem obsluhy). Tento způsob zabezpečení lze uplatnit pouze u výhybek, které jsou pod přímým dohledem dopravního zaměstnance, neboť podmínkou pro bezpečný provoz je správná poloha výměníkového závaží, které zajišťuje přidržení závěrného ústrojí výhybky v uzavřené poloze. Proto výhybky nestřežené je nutno opatřit, bez ohledu na rychlost pojíždění, navíc stojanovým nebo odtlačným zámkem, který znemožní otevření závěrného ústrojí výhybky a dále zajišťuje i správnou polohu výměníkového závaží. Analogická situace je v případě zabezpečení výhybky mechanickým nebo uzamykatelným závorníkem.

U výhybek zabezpečených přestavníky, ať již mechanickými či elektromotorickými se na přidržování závěrného ústrojí výhybky ve správné poloze současně podílí síla vyvolaná výměníkovým závažím v horní poloze (s "gatěmi") a přídržná síla přestavníku. U současně používaného mechanického přestavníku je tato síla dána především vlastnostmi rozřezné spojky výměnové stavěcí páky. U elektromotorického přestavníku je tato přídržná síla dána vlastnostmi rozřezné spojky elektromotorického přestavníku (např. u přestavníků typové řady EP 600 dosahuje hodnot až 800 kN). Dostatečná rezerva přídržné síly přestavníku umožňuje žádoucí provoz soustavy výhybka - přestavník bez výměnového závaží. Tato skutečnost musí být uvedena ve vzorovém výkresu zabezpečení daného typu výhybky.

Jak patrno, je zabezpečení výměn velmi speciálním a komplexním problémem, který zejména při požadavcích na zvyšování rychlosti potřebuje úzkou spolupráci znalců zabezpečovací problematiky s odborníky z odvětví traťového hospodářství.

9.2 Samovratné výhybky

Výhybky použité v samovratném režimu se vybavují samopřestavitelným přestavníkem. Samovratná výhybka uzamknutá v poloze, ve které je v činnosti samopřestavitelný přestavník, který v této aplikaci výhybky nahrazuje spojovací tyč k výměníku, má uzamčený výměník, s výměníkovým závažím ve spodní poloze. Silový účinek samopřestavitelného přestavníku v koncové poloze převyšuje silový účinek výměníkového závaží. V této situaci se výhybka nachází v tzv. preferované poloze a její závěr je přidržován silou pružiny samopřestavitelného přestavníku (cca 2 kN). Výhybku je možno v preferované poloze pojíždět proti hrotu i po hrotu. Po hrotu je možno výhybku v preferované poloze pojíždět i z opačného směru než představuje preferovaná poloha. V takovém případě první dvojkolí železničního vozidla přestaví jazyky výměny do polohy pro jízdu vozidla jako při řezání výhybky. Přitom se stlačí pružina samopřestavitelného přestavníku a její energie se využívá ke zpětnému přestavení výměny do preferované polohy. Aby se jazyky výměny nevracely mezi jednotlivými dvojkolími zpátky do preferované polohy a proces řezání výhybky se tak neopakoval pro každou nápravu, je samopřestavitelný přestavník opatřen hydraulickým tlumičem, který dovolí návrat jazyků do preferované polohy až po nastaveném čase (zpravidla více než 10 s). Vzhledem ke značnému namáhání výměnové části při jízdě železničních vozidel po hrotu z opačného směru než představuje preferovaná poloha je rychlost omezena zpravidla na 40 km/h nebo méně.

Pro pojíždění samovratných výhybek vlaky je rovněž nutno posuzovat tento režim výhybky z pohledu zabezpečení. Z tohoto pohledu lze samovratnou výhybku, která je doplněna elektrickou kontrolou koncové polohy pro zajištění závislosti na návěstidlech povolujících jízdu proti hrotu samovratné výhybky, považovat za výhybku zabezpečenou I. stupněm zabezpečení.

Použití tohoto typu výměn v zabezpečovacích systémech je věnována pozornost v kap. 17.3.

10 PROSTŘEDKY SPOLUPŮSOBENÍ VLAKU

Nezbytností pro poloautomatické a automatické zabezpečovací systémy je detekce vlaku; jen tak lze v systémech realizovat funkce, které jsou závislé na skutečné poloze a pohybu vlaku. Různé zabezpečovací systémy vyžadují různou kvalitu a přesnost detekční informace. Ta v souhrnu obsahuje údaje o poloze vlaku, směru pohybu, rychlosti pohybu (popř. i o aktuálním zrychlení) a to pro všechny vlaky v celé řízené oblasti (tab. 10-1). Výběr vhodné metody detekce vlaku není jednoduchou záležitostí. Metoda musí odpovídat použitému systému, musí splňovat bezpečnostní kritéria podle analýzy možných hazardních stavů a musí být kompatibilní s ostatními provozovanými železničními systémy (např. elektrickou trakcí).

Tab. 10-1

Detekční informace

Poloha	• detekce volnosti • detekce přítomnosti • detekce vyklizení • měření polohy čela vlaku • měření polohy konce vlaku
Směr pohybu	• detekce směru • detekce orientace
Rychlost pohybu	• měření rychlosti

U jednotlivých zařízení lze rozlišit až osm detekčních funkcí (viz také obr. 10-1, 10-2):

Detekce volnosti
Funkce: indikuje se, že v úseku trati nejsou železniční vozidla.
Výstup: dva stavy
- "volno",
- "obsazeno".

Typická aplikace: ověření, že vymezený úsek trati je před vydáním povolení k pohybu vlaku nebo posunujícího dílu volný.
Bezpečnost: nebezpečnou poruchou by byl falešný výstup "volno".

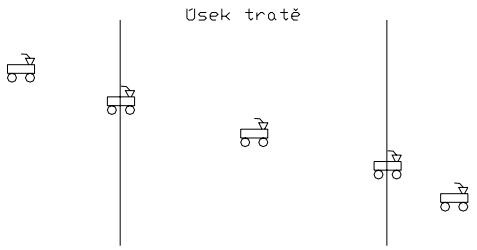
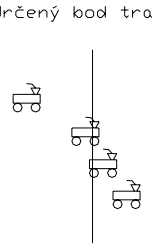
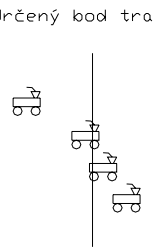
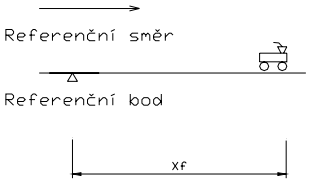
Detekce přítomnosti
Funkce: indikuje se, že čelo vlaku minulo určený bod na trati.
Výstup: dva stavy
- "přítomen" - čelo vlaku je detekováno v daném bodě nebo čelo vlaku minulo daný bod a je nadále detekována přítomnost vlaku,
- "nepřítomen".

Typická aplikace: spuštění výstrahy na přejezdu.
Bezpečnost: nebezpečnou poruchou by obvykle byl chybějící výstup "přítomen".

Detekce vyklizení
Funkce: indikuje se, že celý vlak minul určený bod na trati.
Výstup: dva stavy
- "vlak minul", konec vlaku je detekován v daném bodě,
- "vlak ještě neminul".

Typická aplikace: vybavení cesty; uvolnění přejezdu.
Bezpečnost: nebezpečnou poruchou by obvykle bylo falešné hlášení "vlak minul".

Měření polohy čela vlaku
Funkce: indikuje se poloha čela vlaku.
Výstup: proměnná, specifikující polohu čela vlaku (např. měření dráhy v určeném směru od známého referenčního bodu).
Typická aplikace: vlakové zabezpečovací systémy, traťové systémy s pohyblivým blokem.
Bezpečnost: nebezpečnou poruchou by obvykle byl výstup indikující, že čelo vlaku nedojelo tak daleko, jak skutečně dojelo.

Detekce volnosti		Volno Obsazeno Obsazeno Obsazeno Volno
Detekce přítomnosti		Nepřítomen Přítomen Přítomen *) Nepřítomen
Detekce vyklizení		Vlak ještě neminul Vlak ještě neminul Vlak ještě neminul Vlak minul **)
Měření polohy čela vlaku		Xf

*) v některých aplikacích může být indikováno "nepřítomen"

**) pro návrat do stavu "vlak ještě neminul" je obvykle třeba jiný vnější podnět

Obr. 10-1

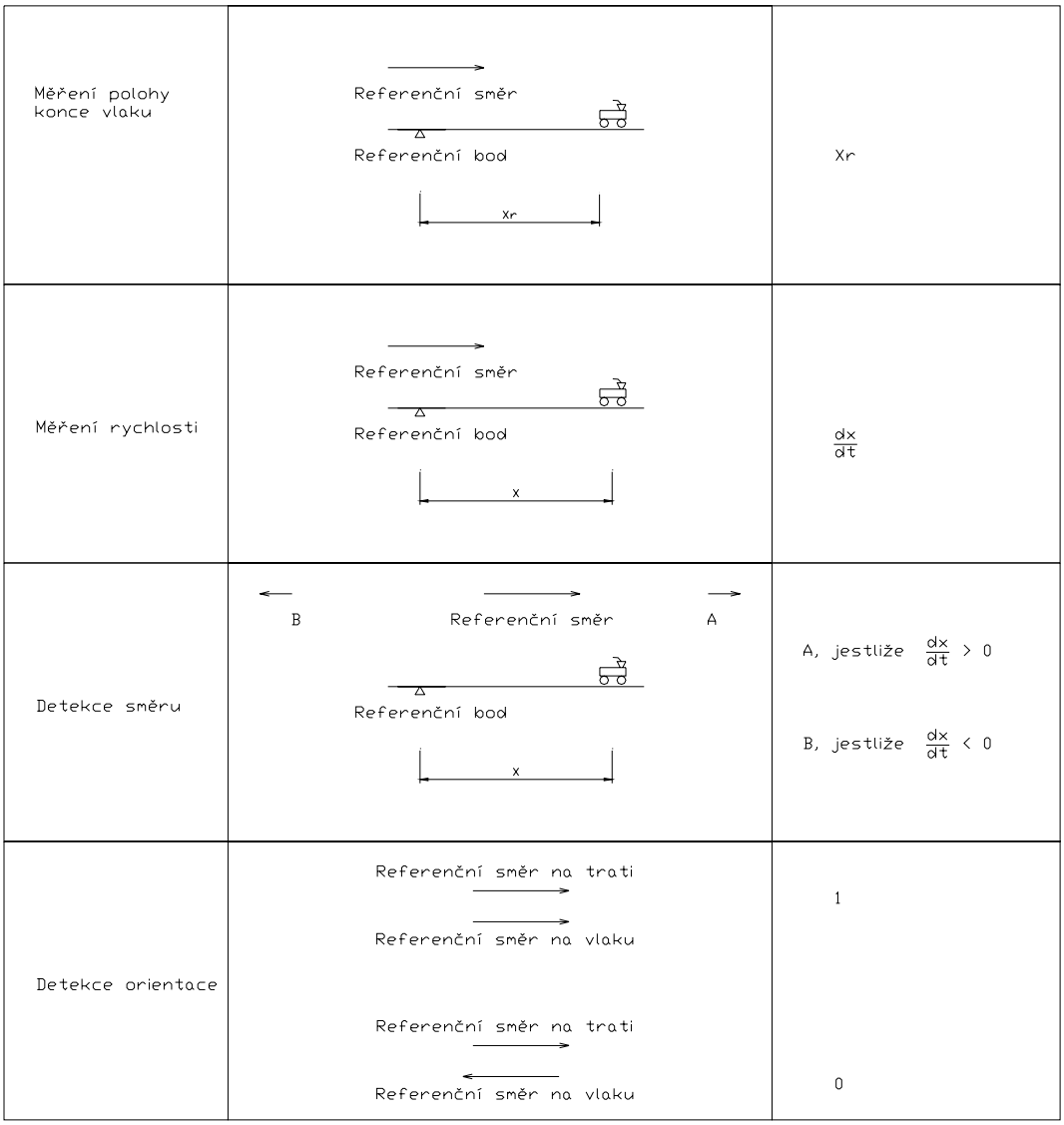
Měření polohy konce vlaku

Funkce: indikuje se poloha konce vlaku.

Výstup: proměnná, specifikující polohu konce vlaku (např. měření dráhy v určeném směru od známého referenčního bodu).

Typická aplikace: vlakové zabezpečovací systémy, traťové systémy s pohyblivým blokem.

Bezpečnost: nebezpečnou poruchou by obvykle byl výstup indikující, že konec vlaku dojel dále, než skutečně dojel.



Obr. 10-2

Měření rychlosti
Funkce: indikuje se rychlost, kterou se vlak pohybuje.
Výstup: proměnná specifikující rychlost vlaku.
Typická aplikace: vlakové zabezpečovací systémy, traťové systémy s pohyblivým blokem, nastavení okamžiku spuštění výstrahy na přejezdu.
Bezpečnost: nebezpečnou poruchou by obvykle byl výstup indikující nižší rychlost než je skutečná. (V případě pohyblivého bloku by to ale mohla být i vyšší rychlost.)
Detekce směru
Funkce: indikuje se směr pohybu vlaku s ohledem na referenční směr podél tratě.
Výstup: tři stavy

- "A", pohyb vlaku ve směru A, např. v lichém směru,
- "B", pohyb vlaku ve směru B, např. v sudém směru,
- "nedefinován".

Typická aplikace: vlakové zabezpečovací systémy, traťové systémy s pohyblivým blokem.
Bezpečnost: nebezpečnou poruchou by byl výstup indikující opačný směr než je skutečný.

Detekce orientace
Funkce: indikuje se zda referenční směr podél vlaku souhlasí nebo je opačný k referenčnímu směru podél tratě.
Výstup: tři stavy

- "1", referenční směr podél vlaku souhlasí s referenčním směrem podél tratě,
- "0", referenční směr podél vlaku je opačný k referenčnímu směru podél tratě,
- "nedefinován".

Typická aplikace: vlakové zabezpečovací systémy, traťové systémy s pohyblivým blokem.
Bezpečnost: nebezpečnou poruchou by byl výstup indikující opačný směr než je skutečný.

První tři uvedené detekční funkce se běžně vyskytují u většiny klasických zařízení, zatímco zbývající jsou typické pro inteligentní vlaková zařízení či komplexní řídící a zabezpečovací systémy. Prvních pět detekčních funkcí lze využít k určení části tratě, která je obsazena vlakem. U první funkce, detekce volnosti, je to evidentní. Obdobně lze ale využít i kombinaci detekce přítomnosti (na vstupu do úseku tratě) s detekcí vyklizení (na konci úseku tratě) a ekvivalentně kombinaci měření polohy čela vlaku s měřením polohy konce vlaku. Zejména posledně jmenované systémy jsou schopné poskytovat údaje o poloze a pohybu s vysokou přesností, bez množství doplňujícího zařízení na trati, ale přímou informaci obvykle mají pouze o poloze čela vlaku a informaci o poloze konce vlaku odvozují nepřímo (např. z délky a orientace vlaku). Při konstrukci zabezpečovacích zařízení je však nezbytné, aby obecně poskytovaly dostatečnou ochranu i v případě neočekávaného rozdělení vlaku. V takovém případě se obvykle předpokládá, že neřízená zadní část vlaku brzdí až do zastavení (např. působením průběžné brzdy) a nadále se nepohybuje. I když je pravděpodobné, že se přední (řízená) část vlaku zastaví stejně, není u nových systémů obvyklé na to spoléhat a předpokládá se, že přední část v jízdě pokračuje. Aby bylo možné výše zmíněná zařízení využít, je nezbytné dříve uvedené detekční funkce doplnit o detekci celistvosti vlaku:

Detekce celistvosti vlaku
Funkce: indikuje rozdělení vlaku.
Výstup: dva stavy

- "vlak nerozdělen",
- " vlak rozdělen".

Typická aplikace: zabezpečovací systémy, které nemají přímou informaci o poloze konce vlaku.
Bezpečnost: nebezpečnou poruchou by byl falešný výstup "vlak nerozdělen".
Při zániku signálu „vlak nerozdělen“ je pak třeba „zmrazit“ posledně známou polohu konce vlaku a nadále sledovat jen polohu čela vlaku a řízenou část vlaku (opatrně?) zastavit.

Kromě detekčních funkcí vyžadují některé automatizační procesy další informace o vlaku, nákladu, vozidlech ve vlaku atd. Tyto další informace nemají obvykle bezpečnostní charakter, ale často je u nich vyžadována vysoká spolehlivost, protože poruchovost může vést k závažným problémům v řízení dopravního procesu. (K těmto otázkám blíže v navazující publikaci „Vlakové zabezpečovací systémy“.)

Pro účely spolupůsobení vlaku je dnes k disposici celá řada prostředků, z nichž nejvýznamnější jsou:

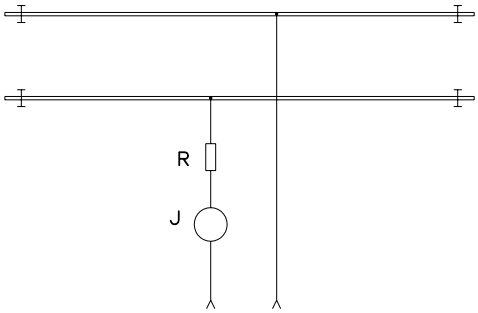
- sériové a paralelní kolejové obvody, reagující na propojení kolejnic elektricky vodivou nápravou,
- detektory kol, reagující na přítomnost kola v určitém místě kolejnice,
- počítače náprav, spolupracující s detektory kol,
- detektory vozidel, reagující na přítomnost masy vozidla,
- paprskové detektory, jejichž paprsek je přerušován vozidlem,
- reflektometry s odrazem od vlaku, emitující energii a registrující její odraz od vlaku,
- detektory zdrojů z vozidel, reagující na zdroj energie na vlaku,
- přijímač na vlaku, přijímající zprávy z vysílače umístěného v určitém bodě tratě,
- radiový zaměřovač polohy vlaku (čela nebo konce),
- inerciální navigátor na vozidle, založený na registraci snímače akcelerace,
- pantografový kontakt, ovlivňovaný pantografem projíždějícího vlaku.

Uvedené prostředky poskytují různou úroveň bezpečnosti a spolehlivosti pro jednotlivé detekční funkce; nároky jsou dány strukturou navazujících systémů. Některé z těchto prostředků mohou působit liniově (tj. spojitě v určité délce trati) nebo semiliniově (tj. přerušovaně v určité délce trati), jiné mohou působit bodově, tj. pouze v určitém předem stanoveném místě, další mohou vytvářet požadovaný efekt zvláštní kombinací stejných či různých prostředků. V klasických zabezpečovacích systémech doznala

všeobecného využití jen malá část z uvedených prostředků, větší část je uplatnitelná pouze v souvislosti s inteligentními vlakovými zabezpečovacími systémy. V dalším jsou uvedeny základní informace k některým všeobecněji používaným prostředkům. Podrobnější informace jsou v navazující publikaci „Prostředky detekce vlaku“.

10.1 Kolejové obvody

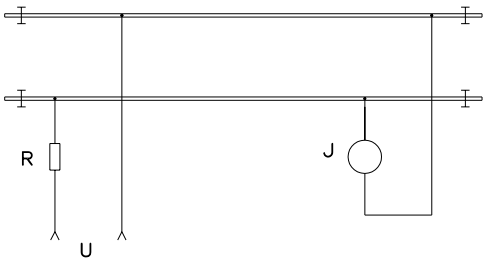
Na obr. 10-3 a 10-4 jsou zapojení dvou základních typů klasických kolejových obvodů. Každý kolejový obvod se skládá z kolejového vedení a k němu připojené výstroje. Kolejové vedení je tvořeno úsekem železničního svršku, u kterého kolejnicové pásy představují vodiče a izolaci nahrazují pražce a štěrk. Kolejnicové pásy jsou složeny z jednotlivých kolejnic (podle typu o délce většinou 15 - 25 m), které jsou spojeny buď svárem nebo kolejnicovými spojkami. Kolejnicové spojky (styky) jsou z hlediska elektrického odporu značně neurčité, protože jejich hlavní účel je pevné mechanické spojení sousedících kolejnic. Uvnitř kolejových obvodů se proto styky obvykle přemosťují vodivými stykovými propojkami. Na koncích klasického kolejového obvodu se běžné kolejnicové spojky nahrazují izolačními spojkami - izolovanými styky. Ty sice tvoří pevné mechanické spojení kolejnic kolejového obvodu s kolejnicemi sousedícími, ale elektricky je od nich izolují. Když kolejové vozidlo vjede do kolejového obvodu, spojí oba kolejnicové pásy svými elektricky vodivými dvojkolími. Elektrický odpor dvojkolí a zejména přechodové odpory mezi koly a kolejnicemi nemusí být zanedbatelné vzhledem k ostatním odporům v kolejovém obvodu a proto se nehovoří o zkratování kolejnicových pasů, ale o jejich šuntování. Výsledný elektrický odpor všech dvojkolí (včetně přechodových odporů kolo-kolejnice) vlaku v kolejovém obvodu se nazývá vlakový šunt.



Obr. 10-3

V kolejovém obvodu podle obr. 10-3 protéká kolejovým relé J pouze malý proud vlivem svodu mezi kolejnicovými pásy a relé nepřitahuje. Při šuntování kolejového obvodu vlakem proud v kolejovém relé stoupne a relé přitáhne. Při uvolnění kolejového obvodu, po výjezdu vlaku, proud v relé opět poklesne a relé odpadne. Tento typ kolejového obvodu se nazývá sériový kolejový obvod, protože jeho hlavní části - zdroj, přijímač (relé) a kolejové vedení (resp. vlakový šunt) - jsou řazeny v sérii. V kolejovém obvodu podle obr. 10-4 protéká proud ze zdroje kolejnicovými pásy do kolejového relé J a relé je přitažené. Když vlak kolejový obvod šuntuje, proud do relé se zmenší a relé odpadne. Tento typ kolejového obvodu se, analogicky k předchozímu, nazývá paralelní kolejový obvod.

Pro získání bezpečné informace o volnosti koleje je třeba, aby byl kolejový obvod konstruován tak, že ani při své poruše nebude obsazenou kolej hlásit jako volnou. Bude-li naopak při poruše volnou kolej hlásit jako obsazenou, může sice dojít k narušení provozu, ale nedojde k přímému ohrožení bezpečnosti, protože zabezpečovací zařízení cestu nepovolí. Rozborem poruch podle obvyklých zásad zabezpečovací techniky lze dovodit, že tomuto účelu v zásadě vyhovuje paralelní kolejový obvod podle obr. 10-4. Kolejový obvod přitom poskytuje informaci o volnosti kontinuálně, bez potřeby paměťového prvku a bez ohledu na způsob, jímž k obsazení či uvolnění koleje došlo (včetně například nasazení či sejmutí vozidla v kterémkoli místě).

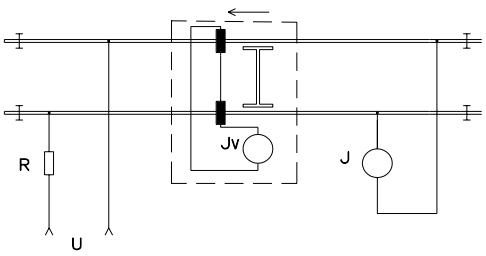


Obr. 10-4

Při vybavení vlakové cesty (a obdobně i při anulaci u přejezdového zařízení, tj. potlačení účinku šuntování vzdalovacího kolejového obvodu) je důležitá volba vhodného okamžiku, kdy k vybavení smí dojít.

Předčasné zrušení závěru může vést k nehodě, protože důležité části vlakové cesty, např. výměny, přestanou být chráněny proti mylnému přestavení v době, kdy jízda vlaku ještě neskončila. Proto kolejový obvod použitý pro tento účel nesmí neoprávněně hlásit příjezd vlaku - obsazení kolejového obvodu - a tedy musí být konstruován tak, že ani při poruše nebude volnou kolej hlásit jako obsazenou. Bude-li naopak při poruše obsazenou kolej hlásit jako volnou, nedojde k ohrožení bezpečnosti jízdy vlaku, ale po jízdě nebude možné např. přestavovat výměny. Opět lze dokázat, že tomuto účelu v zásadě lépe vyhovuje sériový kolejový obvod podle obr. 10-3.

U modernějších zabezpečovacích zařízení by se kolejové úseky pro zjišťování volnosti a kolejové úseky pro vybavování vlakové cesty překrývaly. Pro takové případy má zabezpečovací technika hned tři použitelná řešení. První řešení spočívá ve využití navazujících kolejových obvodů. Dvojicí nebo i trojicí obvodů určených pro zjišťování volnosti lze nahradit kolejový obvod, určený speciálně pro vybavení vlakové cesty resp. anulaci přejezdového zařízení. Je ovšem také možné konstruovat kolejový obvod, který bude na témže kolejovém vedení a při jednom napájení mít jeden výstup s vlastnostmi sériového obvodu a druhý výstup s vlastnostmi paralelního kolejového obvodu. Třetí řešení využívá možnosti superponovat druhý kolejový obvod na téže kolejové vedení při frekvenčním oddělení.



Obr. 10-5

Jinou oblastí uplatnění kolejových obvodů je přenos informace z tratě na vozidlo prostřednictvím signálního proudu kolejového obvodu. V takovém případě v kolejovém obvodu po vstupu vlaku přibývá další přijímač, přijímač vlakového zabezpečovače na vozidle, který je se signálním proudem kolejového obvodu vázán indukčně pomocí vozidlových snímačů (obr. 10-5). Přijímač vlakového zabezpečovače se v kolejovém obvodu pohybuje (spolu s vlakem) směrem k napájecímu konci. Jeho parametry musí být s parametry kolejového obvodu sladěny. Pro rozmnožení přenášených informací musí být signální proud kolejového obvodu vhodně kódován.

Kromě uvedených ryze zabezpečovacích úloh lze kolejových obvodů s výhodou využít i v dalších, z hlediska bezpečnosti méně závažných, automatizačních procesech (např. spádoviště).

Paralelní kolejové obvody jsou z principu své činnosti, za určitých podmínek a s jistým omezením, schopny nejen detekce volnosti, ale i detekce mechanické celistvosti jízdní dráhy. Paralelní kolejový obvod lze totiž navrhnout tak, aby v případě přerušení elektrické vodivosti kolejnic nebyl schopen poskytnout výstup „volno“. Tato vlastnost, byť ne zcela dokonalá (může dojít k mechanickému poškození pojížděné hrany kolejnice bez podstatné změny elektrické vodivosti kolejnice), může pak být cenným příspěvkem kolejového obvodu k celkové bezpečnosti provozu na železnici. Ze všech typů detekčních prostředků je paralelní kolejový obvod také jediným prostředkem, který poskytuje bezpečnou informaci o volnosti ihned po startu (restartu) funkce.

Postupem let byla z obou základních typů kolejových obvodů odvozena celá škála kolejových obvodů, které akcentují tu či onu jejich stránku a přizpůsobují je určitému účelu. Pozornost je přitom zaměřena zejména na:

- dosažení co nejlepších provozních parametrů kolejových obvodů,
- použití kolejového obvodu na elektrifikovaných tratích,
- ochranu před vlivem sousedních kolejových obvodů,
- ochranu před ostatními cizími vlivy,
- odstranění izolovaných styků,
- získání specifických vlastností pro zvláštní použití.

10.2 Detektory kol

Základní vlastností zařízení této kategorie je schopnost detekovat přítomnost/nepřítomnost kola v určitém předem stanoveném místě. Realizace této schopnosti je založena na principu snímání mechanických účinků nebo feromagnetických vlastností kola železničního dvojkolí.

Nejjednodušším typem nápravového snímače je tzv. „pedál“, tj. zařízení, připevněné ke kolejnici, jehož vysunutá část je „sešlapávána“ nákolkem železničních dvojkolí. Změna polohy vysunuté části je využita k rozepínání a spínání kontaktů připojených elektrických obvodů. Přestože jde napohled o velmi primitivní zařízení, je v zabezpečovací technice některých železnic široce využíváno právě pro svou jednoduchost, a také schopnost detekovat jednotlivé projíždějící nápravy i při rychlostech přesahujících 200 km/h.

Detektory, využívající elektromagnetických účinků kola na snímač umístěný na kolejnici, jsou podstatně složitějšími zařízeními, ale na rozdíl od mechanických nemají pohyblivé části a při určité konstrukci a uspořádání lze některé jejich funkce považovat za bezpečné ve smyslu zabezpečovací techniky. Způsobů, jakým je snímána přítomnost železničního kola je několik, podstatou je vždy schopnost snímače reagovat na přítomnost magneticky nebo elektricky vodivého materiálu kola v elektromagnetickém poli, které snímač produkuje. Změny, které jsou takto průjezdem kola ve snímači vyvolávány, jsou transformovány připojenými elektrickými obvody do podoby signálu vhodného k přenesení do místa, kde je vyhodnocení průjezdu vozidla vyžadováno.

10.3 Počítače náprav

Počítač náprav je zařízení, využívající bodových prvků ke kontrole volnosti/obsazení uceleného úseku. Nejčastěji se využívá detektorů kol, umístěných na hranicích takového úseku. Ty zaznamenávají kola - nápravy, které do úseku vstupují nebo z úseku vystupují. Počet vstupujících náprav je v počítači náprav připočítáván, počet náprav z úseku vystupujících je odečítán. Pokud je počet náprav zaznamenaný v počítači náprav nulový, je úsek hlášen jako volný. Pro tuto funkci na nerozvětveném kolejovém úseku jsou potřeba alespoň dva páry detektorů kol, jeden na každém konci kolejového úseku. Pár a nikoliv jen jeden detektor zde musí být umístěn proto, aby počítač náprav mohl vyhodnotit směr pohybu vlaku, pohybujícího se na hranici úseku, a tak správným způsobem nápravy přičítat nebo odečítat. Celý počítač náprav tedy tvoří soustava detektorů kol, vyhodnocovací jednotka a vedení k detektorům kol.

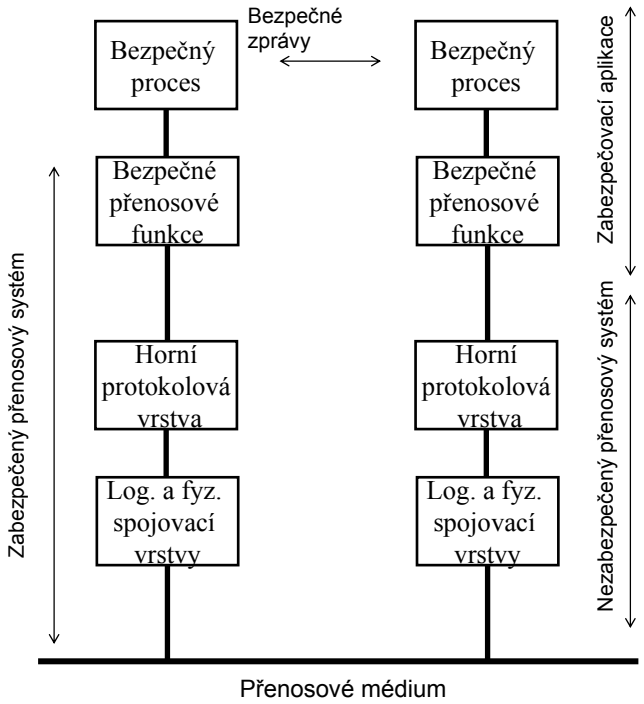
10.4 Detektory vozidel

Zařízení tohoto typu pracuje v principu obdobně jako detektor kol, ale tentokrát reaguje na přítomnost masy železničního vozidla. Snímačem je obvykle indukční smyčka přiložená k vnitřní patě kolejnic a tvořící uvnitř koleje osmičku. Tento tvar je nutný pro eliminaci rušivých napětí vyvolaných ve smyčce indukcí z okolního prostředí, zejména z kolejnic (např. topné proudy, zpětné trakční proudy). Vlivem přítomnosti vozidla dojde ke změně indukčnosti elektricky vodivé smyčky v kolejišti, což je využito k formování příslušného elektrického signálu. Napájecí a vyhodnocovací část tvoří elektronická výstroj, která napájí vlastní smyčku a snímá změny elektrických veličin, související s ovlivněním elektromagnetického pole smyčky magneticky nebo elektricky vodivým materiálem železničního vozidla (snímač musí reagovat nejen na přítomnost feromagnetické hmoty, ale také na nejrůznější lehké slitiny využívané v moderních konstrukcích železničních vozidel). Tyto změny jsou příslušným způsobem vyhodnocovány a vysílány v požadovaném formátu do navazujícího zabezpečovacího zařízení. Detektory vozidel se zatím nejčastěji využívají pro detekci přítomnosti při ovládání přejezdových zabezpečovacích zařízení.

11 PŘENOS A OCHRANA DAT

Podstatnou část činnosti zabezpečovacích zařízení tvoří přenos, zpracování a úschova dat. Všechny tyto operace musí být prováděny způsobem vyhovujícím zabezpečovací technice. Data je třeba chránit proti falzifikaci během přenosu a úschovy, ale také je třeba zajistit, aby systém pracoval s aktuálními, tj. v daném okamžiku ještě platnými daty. V případě chyby je pak nutné chybu detekovat a vyvolat náležitou bezpečnou reakci.

Přenos informací probíhá mezi systémy, uvnitř systému mezi jádrem a periferiemi, uvnitř jádra systému mezi jednotlivými funkčními bloky. U klasických (reléových) zabezpečovacích systémů je základem informace obvykle bitová struktura popisující v podstatě stav relé a pro přenos informací se používají obvykle nekomplikované způsoby (jedno vedení pro každý bit informace). U počítačově orientovaných zabezpečovacích systémů převažují informace ve formě složitějších datových struktur. Z hlediska zabezpečovací techniky je pak třeba při přenosu řešit dva základní problémy: možnost falzifikace zprávy v přenosovém kanálu a možnost chybného zformování zprávy na vysílací straně nebo chybného dekódování zprávy na straně přijímací (vlivem poruchy v koncových zařízeních). Významnou z hlediska bezpečnosti může být i volba cyklicky opakovaného přenosu, přenosu řízeného událostmi, potvrzovaného přenosu atd.



Obr. 11-1

Od obecných datových přenosových systémů není zvykem (s malými výjimkami) vyžadovat plnění specifických zabezpečovacích funkcí (ve smyslu železniční zabezpečovací techniky). Zabezpečovací systémy se však bez bezpečných informací, tj. informací, které nejsou ani chybné (chybné ve zdroji, typu nebo obsahu dat), ani zastaralé (časově příliš opožděné nebo přijaté v chybné posloupnosti), neobejdou. Obvyklým řešením tohoto rozporu je využití obecného přenosového systému a doplnění zabezpečovacích funkcí v aplikační vrstvě přenosového systému. Při správném provedení pak je přenos informací jako celek bezpečný - zajistí, že přijatá informace nebude nebezpečně zkreslena ani vlivem možných rušení v průběhu

přenosové cesty, ani vlivem možných poruch zařízení na přenosu zúčastněných a to včetně poruch v koncových zařízeních.

Zásadní ochranou proti cizímu rušení přenášené zprávy je použití vhodného kódování informace. Kódování musí poskytnout dostatečnou úroveň bezpečnosti zpráv s ohledem na kvalitu přenosových tras (zejména úroveň a charakter rušení). Ta by se ovšem mohla (např. poruchou) časem zhoršit tak, že zvolené kódování již nebude poskytovat dostatečnou bezpečnost. Proto musí být úroveň rušení trvale dohlížena (bezpečně) a v případě nadměrného rušení musí být systém odstaven. Obdobně zásadní ochranou proti poruchám koncových zařízení je použití některého z obvyklých principů konstrukce zabezpečovacích systémů : redundantních obvodů nebo obvodů s vnitřní bezpečností. Z toho ovšem plyne, že tvorba zprávy (včetně adresace, kódování, znaků aktuálnosti zpráv atd.) a obdobně dekódování zprávy musí být provedeno v aplikační zabezpečovací vrstvě, bez ohledu na to, že se některé činnosti opakují i v nižších vrstvách přenosového systému (tentokrát ovšem nezabezpečeně z hlediska pojetí železniční zabezpečovací techniky) v rámci přenosového protokolu (obr. 11-1).

Poněkud odlišné požadavky na rozsah bezpečné přenosové funkce lze uplatnit při přenosu ve vlastních sítích (tzv. uzavřené sítě), kde je možné kalkulovat s předvídaným chováním jednotlivých účastníků, podrobnou znalostí přenosového kanálu atd. a neměnností takovýchto parametrů. Rozsáhlejší pak budou požadavky při využití tzv. otevřených přenosových systémů (typicky GSM a Internet), u nichž nebudou detailně a s jistotou známy přenosové vlastnosti, počet účastníků a jejich chování, citlivost k cizím vlivům, způsob řízení provozu atd. Nezbytnou se zde stane i ochrana před nepovolenou manipulací se zabezpečovacími daty od nepovolaných účastníků přenosu, což je kategorie, s níž zabezpečovací technika doposud pracovala jen velmi omezeně. Vynikne tak význam zpráv se zpětnou vazbou nebo použití kryptografických metod.

11.1 Ochrana přenosu v uzavřených sítích

Ochranu proti poruchám v detailně známém přenosovém kanálu je možné v zásadě aplikovat na úrovni:

- fyzikálního signálu; zvažují se analogové charakteristiky (úroveň, frekvence, fáze) a vylučují se signály nepatřičné. I když se tyto operace provedou způsobem vyhovujícím zabezpečovací technice, nebudou postiženy případy, kdy rušivé signály mají stejný charakter jako signály přenášející zprávu,
- dat; opatření se zaměřují na bitovou kombinaci. Podchyceny nebudou případy, kdy se význam informace změní způsobem, při kterém bitová kombinace bude z hlediska ochranných opatření dodržena,
- procedur; obdoba předchozího, ale na úrovni bytů,
- obsahu informací; při zkoumání správnosti přenosu se bere v úvahu význam přenášené informace.

Ochranná opatření na první a čtvrté úrovni (fyzikální signál a obsah informace) jsou využívána i v klasické zabezpečovací technice. Ochranná opatření ve druhé a třetí úrovni (data a procedury) jsou plně založena na redundanci informace - množství přenášených informací je větší než to, které vychází ze zdroje. Přídavná informace je tím, co poskytuje schopnost chyby detekovat. K tomu účelu existuje celá škála kódů, které dovolují v dané zprávě detekci určitého počtu individuálních chyb, popřípadě i jednoho nebo několika shluků chyb. Problematice kódů je věnována řada publikací, zaměřených na obecnou sdělovací techniku a většinu těchto poznatků lze samozřejmě aplikovat i v zabezpečovací technice. Proto lze plně odkázat na tuto literaturu a zde se omezit pouze na zvláštnosti aplikace.

Obecně je třeba při výběru metody přenosu a jeho ochrany brát v úvahu následující faktory:

- požadovaná informační kapacita - jde jak o požadovaný objem přenosu informací, tak o potřebnou dobu odezvy a to včetně omezení kanálové kapacity v důsledku nutné informační redundance,
- vlastnosti přenosového média - zejména je nutný důkladný rozbor charakteristiky sítě, jejích řídících procedur, kvalitativní i kvantitativní rozbor rušivých zdrojů. Při použití kanálů, které obsahují paměť, se musí použít procedury detekující nepřípustná časová prodlení,
- vlastnosti přenosové metody - metody modulace, detekce, demodulace, synchronizace atd. mohou výrazně ovlivnit citlivost systému na chyby,
- normy - je nutné vyhovět normám, doporučením ITU-T atd., týkajícím se např. omezení úrovně signálu nebo šířky pásma. To může některé ochranné metody vyloučit,

- bezpečnost - z hlediska bezpečnosti systému se za zvlášť účinné považuje, kromě odpovídající redundance, použití kombinace různých ochranných technik na různých úrovních. Vždy musí být dodržen princip, že chyby zavedené a nedetekované na dané úrovni musí být detekovány na vyšší úrovni. Příkladem takové kombinací může být:
    - kódování jako ochrana před interferencemi, adresování jako ochrana před přeslechy a časové značkování jako ochrana proti nadměrným časovým zpožděním,
    - kódování jako ochrana před interferencemi, rozlišení nosné frekvence na ochranu proti přeslechu, adresování pro ochranu proti falešnému spojení nebo přeslechu.

Některé kódy umožňují, aby dekodér opravil zprávu obsahující malý počet chyb a tak zlepšil schopnost přenosu. Tyto korekční postupy musí být v zabezpečovacích systémech používány s maximální opatrností, protože se zvyšuje pravděpodobnost nedetekované chyby. Kromě toho použití samoopravných kódů může zamaskovat zhoršení přenosové linky a tak značně redukovat úroveň bezpečnosti. Protože u přenosu jde o redundanci informací, volí se míra redundance s ohledem na četnost výskytu rušení v přenosovém kanálu. Je pak ale nutné dohlížet, že výchozí předpoklad je skutečně plněn a v případě výskytu vyšší četnosti rušení spojení přerušit. Korekce chyb lze dosáhnout bezpečněji při plném využití Hammingovy vzdálenosti detekčních kódů např. žádostí o opakování zprávy v případě detekce chyby.

Z výše uvedeného lze pro bezpečný přenos prostřednictvím uzavřené přenosové sítě definovat následující požadavky (EN 50159-1) :

1. pro generování dat k přenosu a pro detekci příchozích informací musí být aplikovány obecně platné principy zabezpečovací techniky, které zajistí i bezpečnou reakci v případě poruchy,
2. musí být zajištěna funkční nezávislost mezi bezpečnými přenosovými funkcemi a funkcemi použitými ve vrstvách nezabezpečeného přenosového systému (tedy zjednodušeně řečeno : nezabezpečený přenosový systém nesmí být např. schopen imitovat funkce zabezpečeného systému a ty pak „podstrčit“ systému zabezpečenému),
3. zbytková chybovost dat pro každou výměnu informací mezi zdrojem a příjemcem dat musí být menší než předdefinovaná hodnota. Musí odpovídat zvolené úrovni integrity (SIL) přijímače,
4. SIL bezpečného přenosového systému musí odpovídat nejvyšší úrovni SIL navazujícího bezpečného procesu,
5. pokud zdroj není v přenosovém systému unikátně identifikovatelný, musí být jeho autenticita zajištěna přidáním identifikátoru zdroje k uživatelským datům,
6. neporušenost dat musí být zajištěna bezpečným kódováním uživatelských dat (bezpečný proces nesmí být založen na kódování a dekódování dat v nezabezpečené části přenosového systému),
7. aktuálnost uživatelských dat musí být zajištěna přídavnou časovou informací (časové razítko, sekvenční číslo atd.). Dovolené časové zpoždění záleží na aplikaci,
8. v případě potřeby musí být bezpečným procesem ověřována posloupnost zpráv,
9. bezpečné procedury musí být funkčně nezávislé na procedurách použitých v nezabezpečené části přenosového systému. Pokud například obě procedury používají stejný kódovací mechanizmus, musí pracovat s odlišnými parametry (např. generující polynom cyklického kódu),
10. pokud se kvalita přenosu sníží pod předdefinovanou úroveň, musí dojít k odpovídající bezpečné reakci,
11. pokud jsou současně přenášeny bezpečné a nikoliv bezpečné zprávy, musí mít odlišnou strukturu. Kódování musí být voleno tak, aby nikoliv bezpečná zpráva nemohla emulovat zprávu bezpečnou, procedury bezpečných částí zařízení musí být funkčně nezávislé na procedurách nikoliv bezpečných zařízení,
12. pro splnění požadované úrovně SIL je nezbytné detekovat a reagovat na typické poruchy nezabezpečené části přenosového systému. Uvažovat je třeba nejméně:
    - přerušení přenosové linky,
    - všechny bity jsou logická 0,
    - všechny bity jsou logická 1,
    - inverze zprávy,
    - synchronizační posun (při sériovém přenosu),

13. pro splnění požadované úrovně SIL je nezbytné detekovat a reagovat na typické přenosové chyby. Uvažovat je třeba nejméně :
    - náhodné chyby,
    - shluky chyb,
    - systematické chyby, např. poruchové opakování posloupnosti dat,
    - kombinace výše uvedeného,
14. bezpečný kód musí být funkčně nezávislý na přenosovém kódu,
15. bezpečné kódování musí garantovat, že nezabezpečený přenosový systém nebude schopen generovat bezpečné kódové slovo. Splnění tohoto požadavku lze prokazovat pravděpodobnostním přístupem, s respektováním otázek bezpečnosti. Přijatelný je ale i předpoklad, že požadavek je splněn pro složité kódy (např. CRC).
16. je třeba zajistit, aby délka (úroveň) bezpečného kódu byla kompatibilní s bezpečnostními cíly přenosového systému. Konzervativní přístup velí neuvažovat vnitřní zabezpečení v nezabezpečené (obecné) části přenosového systému a kódování v aplikační úrovni volit pouze s ohledem na četnost výskytu EMI (přičemž systém musí nepřekročení této četnosti bezpečně monitorovat). Norma EN 50159-1 poskytuje jistý návod, jak do kvantitativního posouzení bezpečných vlastností přenosového systému zahrnout i zabezpečení z obecné části a na základě toho redukovat úroveň zabezpečení v aplikační vrstvě. To je možné na základě znalosti četnosti výskytu hazardních stavů v ne zabezpečeném systému.

11.2 Ochrana přenosu v otevřených sítích

Obecně lze při přenosu předpokládat, že dojde k následujícím poruchám:

- opakování zprávy - chybě, při níž jedna zpráva bude přijata vícekrát,
- odstranění zprávy - chybnému vypuštění zprávy z toku dat,
- vložení zprávy - chybě, při níž bude do toku dat zpráva vložena,
- změna posloupnosti zpráv - změna pořadí zpráv v toku dat,
- zkomolení zprávy - náhodně pozměněná zpráva,
- zpoždění zprávy - zpráva bude přijata později než se očekávalo,
- změně zprávy - záměrné vložení neautentické zprávy neautorizovaným účastníkem přenosu.

Stejně obecně lze uvést soubor ochranných prostředků:

- číslo sekvence, kdy každá zpráva je při formování doplněna číslem sekvence zprávy a přijímací straně tak umožňuje ověřit posloupnost zpráv,
- časová značka, která umožní zjistit, že data, s kterými systém pracuje, jsou v daném okamžiku ještě platná, tj. aktuální. Toto opatření je nutné použít v případě, že nebylo použito jiných systémových opatření, která zcela jednoznačně vylučují, že by se v zařízení pohybovala zastaralá data, obvykle na místě číslování sekvencí. Tento údaj pak umožňuje při zpracování dat posoudit, zda zpracovávaná data jsou ještě aktuální,
- time-out, kdy přijímač sleduje čas mezi dvěma sekvencemi (cyklického přenosu). Při překročení maximálně povoleného zpoždění předpokládá přenosovou chybu,
- zpětnovazební zprávy, kdy přijímač vysílá původci zprávy zpět původní nebo pozměněnou zprávu. Pak buď čeká na potvrzení, že správně rozuměl, nebo je proces zabezpečen jinak u původce zprávy,
- identifikace původce a/nebo příjemce, což umožňuje zjistit, že původce zprávy souhlasí s očekávaným a že zpráva je skutečně určena příjemci,
- identifikační procedura, která zdokonaluje v předchozí odrážce uvedenou identifikaci pro případ, že existuje riziko záměrné zprávy od zdroje předstírajícího, že je originálním zdrojem,
- bezpečné kódování, které bude použito i v případě, že otevřená síť má vlastní kódovou ochranu proti náhodným poruchám přenosu, protože té nelze plně věřit,
- kryptografické techniky, používané zejména v případě využití otevřených veřejných sítí, radiových sítí atd. V zásadě jde o kódovací techniku, která umožňuje udržet klíč použitého kódu v tajnosti před nepovolanými osobami.

V tabulce 11-1 jsou přehledně uvedeny poruchy a možné ochranné prostředky tak, jak je uvádí norma EN 50159-2.

Tab. 11-1

	Ochrana							
Porucha	Číslo sekvence	Časová značka	Time-out	Zpětnovazební zpráva	Identifikace původce a příjemce	Identifikační procedura	Bezpečné kódování	Kryptografie
Opakování	X	X						
Odstranění	X							
Vložení	X			X 1)	X 2)	X 1)		
Změna posloupnosti	X	X						
Zkomolení							X	X
Zpoždění		X	X					
Změna zprávy				X 1)		X 1)		X

Pozn.: 1) Závisí na aplikaci
2) Bude detekovat pouze vložení z nesprávného zdroje

11.3 Ochrana uložených dat

I tato ochrana musí být v zásadě založena na datové nebo informační redundanci. V podstatě je možné ukládat data zakódovaná nebo v několika kopiích. V prvním případě je důkazem neporušenosti dat jejich příslušnost k patřičnému kódu. V druhém případě je nutná komparace a jistota, že data nemohla být falzifikována společnou chybou. Proto se většinou současně uplatňuje i diversifikace, obvykle v nejjednodušších formách - uložení v hardwarově nezávislých datových prostorech, popřípadě v inverzní nebo zrcadlové podobě.

Mezi ochranu uložených dat patří i kontrola správnosti a neporušenosti vložených programů. Je třeba bránit tomu, aby do zařízení nebyl omylem vložen nepatřičný program a aby patřičný program nebyl (omylem nebo poruchou) poškozen.

12 NÁVĚSTĚNÍ

Dopravní proces vyžaduje předávání informací jedoucímu dopravnímu prostředku o stavu dopravní cesty před vozidlem. Část těchto informací je trvalého charakteru (např. spád, rychlostní omezení daná stavebními důvody) nebo dočasného charakteru (např. přechodná omezení rychlosti z důvodu poruchy na jízdní dráze), část informací je proměnná v závislosti na okamžité dopravní situaci. Některé informace mají povahu rozkazu, jiné pak povahu obecnější zprávy.

Nejstarším způsobem, avšak nadále široce užívaným, je předávání informací pomocí různých optických nebo akustických návěstí. Návěst je viditelné nebo slyšitelné vyjádření informace. Obsahem (podrobným významem) návěsti je návěstní pojem, vyjádření návěstního pojmu je návěstní znak. Zařízení, jímž se návěst dává je návěstidlo nebo návěstní pomůcka. Výhodou akustických návěstí je jejich vnímání v jakékoliv poloze - zdroj nemusí být vidět. Nevýhodou je jejich rušení okolním hlukem (také nepříznivým větrem), ale hlavně jejich neadresnost, která může způsobit problémy v případě, že bude informace vyhodnocena někým, komu nebyla určena. Zvuk se vytváří píšťalou, píšťalkou, trubkou, zvoncem, houkačkou nebo také třaskavkou. V poslední době se tyto návěsti stále více nahrazují radiovým spojením. Optické návěsti působí na pozorovatele buď tvarem, světlem nebo kombinací obou.

12.1 Návěstní systémy

Výstupem staničního a traťového zabezpečovacího zařízení jsou obecně informace (s povahou rozkazu) pro vozidlo. Tyto informace se předávají nepřenosnými návěstidly umístěnými podél tratě strojvedoucímu nebo se prostřednictvím vlakového zabezpečovacího zařízení dopravují až na hnací vozidlo, kde jsou dále využity pro zajištění bezpečného pohybu vlaků. Nejběžnější je dnes použití kombinace obou způsobů, přičemž gradace způsobu druhého musí dříve či později vést k útlumu způsobu prvního.

Návěstění na železnicích je ovlivněno zejména skutečností, že vlak od počátku brzdění až do úplného zastavení projede značnou vzdálenost. Tato dráha je výrazně proměnná v závislosti na rychlosti jízdy, konstrukci brzd, sestavě soupravy, na stavu trati, počasí atd. Vzdálenost, na níž vlak s nejhoršími uvažovanými vlastnostmi zastaví i za nejnepříznivějších okolností, se nazývá zábrzdná vzdálenost a je určována základním železničním předpisem. U ČD je pro tratě s traťovou rychlostí do 60 km/h stanovena zábrzdná vzdálenost 400 m, pro rychlost do 100 km/h 700 m, pro rychlost do 120 km/h 1000 m a pro rychlost větší než 120 km/h zábrzdná vzdálenost 2000 m. Nejméně v této vzdálenosti před určeným místem zastavení musí být vlaku informace předána, má-li spolehlivě zastavit. Současně, z důvodu nejmenších provozních ztrát v případě zastavení, musí ale být návěstidlo umístěno co nejblíže překážce. Z kapitoly věnované optice bude patrné, že problémy s viditelností návěstidel (jak tvarových, tak světelných) neumožňují, zejména za špatného počasí, zajistit spolehlivě přenos návěsti opticky ani na kratší vzdálenosti. Řešením uvedeného rozporu je umisťování návěstidla v blízkosti překážky a zavedení předvěsti, umístěné na zábrzdnou vzdálenost před návěstidlem. Předvěst již svou polohou upozorňuje strojvedoucího, že návěstidlo je vzdáleno minimálně na zábrzdnou vzdálenost a zároveň (aby nemusel snižovat vždy rychlost v očekávání návěsti "stůj" na návěstidle) návěstí (před-návěstí) stav návěstidla. Takový způsob návěstění umožňuje železnici bezpečný provoz i za nepříznivých povětrnostních podmínek, kdy provoz ostatních druhů doprav je výrazně omezen, ne-li ochromen.

Základním pravidlem všech železničních návěstních systémů je zásada, že jízda vlaku je vždy zakázána, když není povolena. Tato zásad je právě opačná než např. u dopravy silniční (jízda je vždy povolena, není-li zakázána). Dále se pak železniční návěstní systémy zásadně dělí na systémy směrové a systémy rychlostní. U starších směrových systémů se v obvodu stanice (odbočky) v podstatě návěstí směr jízdy a z něj si strojvedoucí sám, se znalostí místní situace, odvozuje rychlost, kterou smí jet. Nověji však většina železnic přešla na systém rychlostní, kde se strojvedoucímu návěstí přímo rychlost. Impulsem pro to byla konstrukce celé škály výhybek, dovolujících vyšší, ale různé, rychlosti do odboček než výhybky původní. Toto řešení má řadu nedostatků. Prvním je, že rychlost jízdy vlaku je ovlivňována řadou jiných faktorů a konstrukce výhybky je jen jednou z mnoha záležitostí. Takto určená rychlost tedy platí jen v

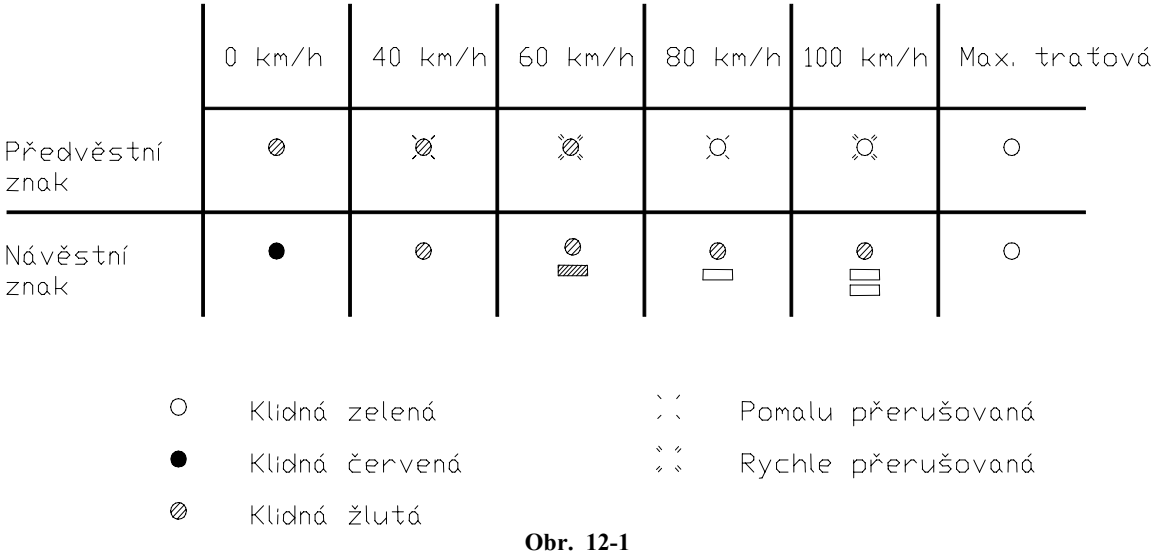
omezené (a navíc velmi vágně ohraničené) oblasti výhybek, přilehlých k návěstidlu. Druhým problémem je, že velikost omezení rychlosti je často závislá na vlastnostech vlaku, který informaci přijímá (viz kap. 16) Třetím problémem je skutečnost, že při některých činnostech potřebuje strojvedoucí i informaci o směru jízdy, což v několika případech vedlo až k tvorbě návěstního systému, který oba základní principy kombinuje a je tedy jak rychlostní, tak směrový (SNCB). Dalším problémem je realizace potřebného počtu rychlostních informací prostřednictvím optického návěstění. V této otázce přistupuje i problém unifikace návěstních systémů evropských železnic, protože jejich různorodost představuje podstatnou překážku při integračních snahách evropských železnic. Pokud by návěstní systém měl být základním informačním systémem pro řízení vlaků, musel by v každém případě vyhovovat jistým, všeobecně platným zásadám :

- systém musí umožnit bezpečné vedení vlaku v celém rozsahu použitých rychlostí; musí proto včas návěstit kde a na jakou úroveň je třeba dovolenou rychlost snížit a v odůvodněném rozsahu i směr jízdy,
- zvolené návěstní znaky musí být jednoznačné; musí tedy mít vždy stejný význam ať jsou použity kdekoliv a pro všechny druhy vlaku,
- zvolené návěstní znaky musí být nezaměnitelné; jejich podoba se nesmí tedy blížit jinému znaku, aby je ani za ztížených podmínek nebylo možné zaměnit zejména za návěst více povolující,
- zvolené návěstní znaky musí být za všech okolností stále stejné (ve dne i v noci, při různém počasí),
- zvolený návěstní znak nesmí mít více omezující význam, než měl v předchozí návěstní soustavě, barvy musí být použity ve shodě s jejich vžitým významem (červená pro "stůj", zelená pro "volno", žlutá pro "pomalu", modrá a bílá pro posun),
- zvolené návěstní znaky musí být jednoduché aby se jejich vjem v značně rušeném přenosovém optickém kanálu co nejvíce usnadnil,
- znaky návěstního systému musí tvořit lehce zapamatovatelnou logickou řadu, aby se jejich význam co nejsnáze vybavoval a tak umožňoval rychlou reakci,
- jemnost odstupňování rychlostních stupňů by měla vyloučit nadbytečné omezování rychlosti z titulu návěstní soustavy; to je však po překročení určité meze v rozporu s požadavky bezpečnostního rázu (jednoduchost, logičnost atd.), - složitost návěstních znaků ovlivní konstrukci návěstidel i návěstní schematiky, protože ani žádná porucha návěstidla nesmí vést ke svícení návěsti více povolující.

Tyto požadavky ve svém souhrnu neponechávají příliš mnoho možných řešení.

Veškeré návěsti používané u ČD, jsou uvedeny v Návěstním předpise (D1); velmi podobné návěstní systémy užívají i ostatní dráhy dříve sdružené v OSŽD. Zjednodušená tabulka návěstních a předvěstních znaků ČD je v tab. 12-1. Pokud je hlavní návěstidlo sloučeno s předvěstí následujícího návěstidla, zobrazují se předvěstní znaky v horní části návěstidla, návěstní znaky v dolní tak, jak je uvedeno v tabulce, s dvěma výjimkami:

- je-li návěstní znak "červená", samozřejmě se nezobrazuje žádný předvěstní znak následujícího návěstidla,
- je-li návěstní znak "zelená", svítí pouze jedno zelené světlo.



Obr. 12-1

Lze si i povšimnout, že systém pro rychlosti nad 100 km/h má k disposici pouze jeden znak, totožný pro maximální traťovou rychlost. Po pravdě řečeno nelze předpokládat, že by bylo možné povolit rychlost jízdy vlaku, řídícího se návěstidly, nad 120 km/h vzhledem k množství a omezené době pozorování návěstidel. Účelnost návěstění vyšších rychlostí venkovním návěstidlem je více než sporná.

Byla již zmíněna druhá možnost - návěstění pomocí lokomotivního návěstidla při přenosu informace na vozidlo. Touto problematikou se podrobněji zabývají vlaková zabezpečovací zařízení. Připomeňme zde jen jeden podstatný rozdíl: při sledování návěstidla dostává strojvedoucí, jaksi mimoděk, poměrně přesnou informaci o cílové vzdálenosti, tj. o místě, od kterého dovolená rychlost platí. Převede-li se tedy návěstidlo do kabiny strojvedoucího a venkovní návěstidla se zruší, je třeba zároveň zajišťovat i údaj o cílové vzdálenosti. Současný trend rozšiřujícího se přenosu návěstidla do kabiny strojvedoucího nepovede ani v budoucnosti k úplnému potlačení venkovních návěstidel. Ta zůstanou zachována v nejdůležitějších místech dopravní cesty minimálně jako záložní systém pro náhradní řízení dopravy při poruchách a přechodných stavech. S tímto pojetím je ale možné upustit od snah přenášet návěstidly úplnou informaci a to pro celou škálu používaných traťových rychlostí a tyto ambice ponechat pouze vlakovému zařízení. Návěstidly, chápanými jako záložní systém, by se pak přenášely pouze informace „stůj“, „volno“ (plná traťová rychlost = max. 100 km/h), „pomalu“ (v podmínkách ČD např. 40 km/h) a „výstraha“. (Informace vlakového zařízení by pak samozřejmě musely mít před informacemi na návěstidle přednost.) Dopad na snížení investičních i provozních nákladů u pevných zařízení na trati je evidentní.

Největší problém v dopravě je spojen s nejjednodušší návěstí, s návěstí "stůj". Tato návěst je nejzávažnější a proto na jejím respektování je třeba důsledně trvat. Návěst "stůj" se však na návěstidle může objevit nejen z důvodů nepříznivé dopravní situace, ale i z důvodu dopravní nepravidelnosti nebo poruchy zabezpečovacího zařízení, a tehdy je nutné průjezd vlaku okolo ní umožnit. U zařízení obsluhovaných dopravním zaměstnancem je na tuto situaci pamatováno přivolávací návěstí. Tuto návěst rozsvěcí zvláštním úkonem dopravní zaměstnanec, když se přesvědčil, že vlaku žádné nebezpečí nehrozí. Celá situace je doprovázena různými administrativními opatřeními. Větší potíže působí neobsluhované návěstidlo automatického nebo dálkově řízeného zařízení. Pro případ automatického traťového návěstidla přijaly některé dráhy zavedení zvláštního druhu návěstního pojmu "stůj", tzv. permisivní "stůj". U takové návěsti vlak sice musí zastavit, ale pak smí omezenou rychlostí a po splnění určitých opatření pokračovat v jízdě. Benevolencí těchto opatření se ČD řadí k nebezpečným optimistům. Problém dálkově ovládaných návěstidel je diskutován v kap. 17.1.

12.2 Návěstidla

Rozvoj dopravních cest je doposud stále ještě doprovázen zvětšováním hustoty návěstidel, nyní většinou světelných; v okolí tratí přibývá světelných zdrojů, které pozorování návěstidel mohou ovlivnit; při rychlosti 120 km/h na tratích s automatickým blokem míjí strojvedoucí návěstidlo téměř každých 30 s. Za těchto okolností je nutné využít pro zkvalitnění toku informací předávaných návěstidly všech možností nabízených současným stavem poznání v oblasti světelné techniky. Při konstrukci nebo hodnocení návěstidla se v oblasti optiky věnuje pozornost zejména

- vytvoření barevného světla zdrojem s co nejvyšším měrným výkonem (nebo měrnou svítivostí) a životností při co nejmenších rozměrech, s možností velmi častého rozsvěcování a zhasínání bez pozorovatelného samovolného zakmitání,
- soustředění výstupního světelného toku do požadovaného tělesa dohlednosti tak, aby pokud možno mimo těleso světlo vůbec nesvítilo a uvnitř tělesa byly hodnoty osvětlení vhodně upraveny podle pozorovací vzdálenosti,
- vytvoření kontrastního neutrálního okolí pro pozorování znaku,
- ochraně před rušivými světelnými jevy.

V návěstidlech se jako světelných zdrojů využívá téměř výhradně tepelných zářičů s "bílým" světlem, žhavených Joulovým teplem, a filtrů. Tepelné zdroje žhavené plamenem patří minulosti, barevné výbojové zdroje jsou zatím nepoužitelné zejména pro zakmitávání při rozsvícení. Pro praktické využití v dnešních železničních návěstidlech tak zůstávají v podstatě k disposici pouze žárovky (novější i halogenové). Současný technologický pokrok v oblasti svítivých diod však může vbrzku počet vhodných světelných zdrojů rozšířit.

Účinnost světelných zdrojů se hodnotí měrným výkonem [lm/W] (poměr světelného toku a příkonu) a měrnou svítivostí [cd/W] (poměr svítivosti a příkonu). Pro návěstní žárovky obecně platí, že jejich měrný výkon a měrná svítivost s rostoucí teplotou vlákna rostou. Při zvyšování teploty vlákna však rychle klesá životnost. Příčinou jsou zejména drobná zeslabení vlákna vlivem výrobních nepřesností; v těchto místech dochází k lokálním přehřátí, vlákno se nejvíce odpařuje a navíc rekrystalizací dochází k jeho křehnutí. Relativně nejmenších výrobních nepřesností se dosahuje u silnějších vláken, tedy u žárovek pro nižší napětí. S ohledem na požadovanou dlouhou životnost se proto v železničním návěstění užívá snížených napětí obvykle v rozsahu 12-48 V (u ČD 12 V). Zvýšení životnosti žárovky snížením napětí na žárovce pod nominální hodnotu je v rozporu s požadavkem velkého měrného výkonu (např. s ohledem na potřebné náhradní zdroje pro napájení návěstidel) a způsobuje změnu barvy světla směrem k červené. Proto je třeba zde postupovat obezřetně a uvažovat i snížené napětí pro noční znak. Někdy používaná přídavná stabilizace (napětí návěstního zdroje nebo proudu žárovkou) zajišťuje udržení zvoleného kompromisu mezi optickou výkonností a životností zdroje. Využívání dvouvláknových žárovek pro zvýšení spolehlivosti optického zdroje přináší problémy v návěstní optice vzhledem k různosti geometrické polohy obou zdrojů a kromě toho nezajišťuje, že po poruše prvního vlákna bude žárovka nadále dostatečným zdrojem, protože při přehoření prvního vlákna mohlo dojít k zakalení baňky.

Oko strojvedoucího se při jízdě pohybuje. Množina všech bodů, v kterých se může oko strojvedoucího ocitnout s ohledem na různou polohu v různých vlacích a uspořádání tratě, tvoří plochu dohlednosti. Spojnice bodů obvodu plochy dohlednosti s návěstní svítilnou vymezuje těleso dohlednosti. V celém tomto prostoru pak nemají být žádné pevné překážky a do celého prostoru má návěstní svítilna vyzařovat světlo požadované úrovně. Požadovanými tělesy dohlednosti se zabývají příslušné normy.

U tvarových návěstidel, návěstních desek ale i u světelných návěstidel složených z více světel je nutné pro správné rozlišení zajistit takové rozměry, aby rozhodující díly byly viděny z požadované vzdálenosti pod úhlem minimálně 1'. Ze vzdálenosti 100 m je pod zorným úhlem 1' pozorována délka 2,9 cm, ze vzdálenosti 400 m délka 11,6 cm, ze vzdálenosti 1000 m délka 29 cm.

V návěstidle je optické zařízení, tzv. optika návěstidla, která má světelný tok svítivého zdroje usměrnit do žádaného směru a dodat světlu předepsanou barvu. K usměrnění toku do svazku paralelních paprsků, blízkých podobě válce, lze použít buď parabolický reflektor nebo spojnou čočku. Optimálního soustředění se dosáhne v případě, kdy bude zdroj světla blízký zdroji bodovému a bude umístěn v ohnisku. Čočky se užívají buď asférické nebo, častěji, Fresnelovy. Návěstní svítilny s parabolickým reflektorem se u železničních návěstidel využívají pouze výjimečně s ohledem na možnost vzniku tzv. fantomní návěsti, tj. falešné návěsti vzniklé obecně odrazem cizího (vnějšího) světla od částí optiky návěstní svítilny. Skutečná nebezpečnost fantomní návěsti závisí na konkrétním návěstním systému.

Pokrytí celého tělesa dohlednosti jedním soustředěným světelným tokem je zpravidla nemožné při pozorování návěstního znaku v oblouku nebo z blízkosti paty návěstidla. Pro zlepšení situace v oblouku se využívají rozptylná skla, která záměrně zvyšují vodorovnou divergenci návěstní svítilny. Pro lepší pozorování návěstního znaku v blízkosti návěstidla se ve svítilně záměrně vytváří vedlejší světelný tok a to buď samostatným vychylovacím prvkem nebo speciálně upraveným rozptylným sklem.

Konstrukčně odlišná jsou tzv. reléová návěstidla. Žárovka je umístěna v jednom ohnisku eliptického reflektoru, který soustředí veškerý tok (za předpokladu bodového zdroje) do druhého ohniska, kde je umístěn rámeček se třemi filtry. Polohu rámečku a tedy umístění jednoho ze tří filtrů do ohniska ovládá polarizované relé. Další čočkový konvergentní systém zajistí konvergenci paprsků. Je zřejmé, že u tohoto systému nemůže vzniknout nebezpečná fantomní návěst - cizí zdroj může jen posílit správný znak. Pro stejnou svítivost postačí, vzhledem k reflektoru, zhruba žárovka s poloviční příkonem. Obdobná svítilna s dvěmi neutrálními ovládacími relé může zajistit přestavování čtyř filtrů.

Kontrast pozorovaného návěstidla vůči okolí pomáhá zajistit svítilnová deska. Obdobnou funkci při pozorování návěstní svítilny z menší vzdálenosti má i svítilnové stínítko, které však současně slouží i jako mechanická a protifantomní ochrana.

Konstrukce návěstidla musí umožnit pokud možno snadné seřízení návěstní svítilny do požadovaného směru.

12.3 Návěstní obvody

Logika zabezpečovací techniky vede k tomu, aby se po splnění podmínek pro zamýšlenou jízdní cestu nejprve rozsvítil na návěstidle povolující znak, zkontrolovala se jeho správnost a teprve potom se odpojila návěst zakazující. Sleduje se tím, aby se ani při poruše (např. spálená žárovka) ani na přechodnou dobu neobjevila falešná návěst, případně aby návěstidlo nezůstalo neosvětlené. Dále by dohlédací obvody návěstidla v případě poruchy (např. přepálení žárovky) měly, ve spolupráci s řídícími obvody, zajistit rozsvícení takového povolujícího znaku, který sice není více povolující než ten, který rozsvícen být má, ale je pokud možno co nejméně omezující.

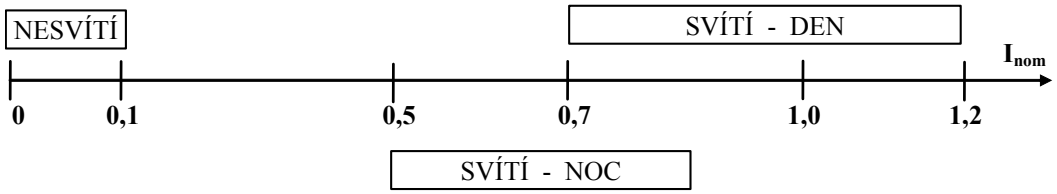
Dohlédací obvody tedy musí prvotně získat informaci o tom, zda a které žárovky na návěstidle svítí. Vycházet přitom mohou z výsledného efektu na žárovce, tj. jejího světelného toku nebo z proudu žárovkou. První řešení, ač správnější, se zatím uplatňuje jen omezeně vzhledem k problému dostatečně selektivního zpětného převodu světla na elektrickou veličinu a potřebě dalšího vedení mezi žárovkou a řídícím systémem pro tuto informaci. Posuzování výsledného efektu na návěstidle z proudu žárovkami má také svá úskalí. Pokud se do úvah zahrne možnost svodů na vedení k žárovce (např. kapacitních při střídavém napájení), bylo by nutné umístit proudové čidlo co nejblíže k žárovce. Ani to však nebude dostatečné, pokud bude jako možný uvažován svod přímo v žárovce a navíc opět bude nutné informaci o stavu dohledu dopravit zpět k řídícím obvodům. Ze všech těchto důvodů v praxi dohlédací obvody vychází z proudu žárovkou (včetně vedení a případných transformačních prvků) a umisťují se do stejného místa jako řídící obvody. Dohled žárovek je pak přímo nebo zprostředkovaně využit ke kontrole správnosti návěstěného znaku a k následnému odpojení zakazujících znaků popř. k přepnutí na náhradní světlo. Přitom je nutno uvažovat s tím, že svítivost žárovky (a tedy i proud) musí být jiná ve dne a v noci.

Pro určení nebezpečných stavů v dohlédacích obvodech je nutná konfrontace s použitým návěstním předpisem. V návěstní soustavě ČD by, kromě falešného hlášení dohlédacího obvodu o svícení žárovky, byly nebezpečné i stavy, kdy se poruchou změní:

- pomalu nebo rychle přerušované zelené světlo na trvale svítící zelené světlo,
- pomalu přerušované světlo na rychle přerušované světlo,
- trvale svítící žluté světlo na cyklicky přerušované světlo,
- opakovací návěstidlo na hlavní návěstidlo (zhasnutím bílého světla).

Teoreticky vzato (a prakticky realizovatelné s mikroprocesorovým interface k návěstidlu) by dohled všech žárovek měl rozlišovat následující oblasti (obr. 12-4):

- žárovka svítí, jejíž hranice jsou :
  - I = 0,7 I nom (- 10 % na kolísání sítě, - 20 % na regulaci žárovky),
    až
  - I = 1,2 I nom (+ 10 % na kolísání sítě, + 10 % na klidový proud),
- žárovka nesvítí : I < 0,1 I nom ,
- porucha obvodu : vše ostatní.



Obr. 12-2

Je třeba vzít v úvahu, že nominální proud žárovkou může být v noci ještě o 30 % snížen vzhledem k regulací den/noc. Tím se buď rozšíří oblast "svítí" směrem k nižším hodnotám proudů nebo je třeba limity modifikovat v závislosti na regulaci den/noc. Žárovky žlutého a zeleného světla na vjezdových a odjezdových návěstidlech a jejich předvěstí (opakovacích předvěstí) by měly být navíc dohlíženy, zda svítí přerušovaným světlem (a případně i rozlišit, zda pomalu či rychle). Dalšími výstupními stavy dohledu žárovek pak budou:

- žárovka svítí pomalu přerušovaným světlem - při impulsním spínání s kmitočtem 0,9 Hz ± 10 %, kdy v impulsu velikost proudu odpovídá výše uvedenému stavu "žárovka svítí" a v mezeře výše uvedenému stavu "žárovka nesvítí",
- žárovka svítí rychle přerušovaným světlem - při impulsním spínání s kmitočtem 1,8 Hz ± 10 %, kdy v impulsu velikost proudu odpovídá stavu "žárovka svítí" a v mezeře stavu "žárovka nesvítí".

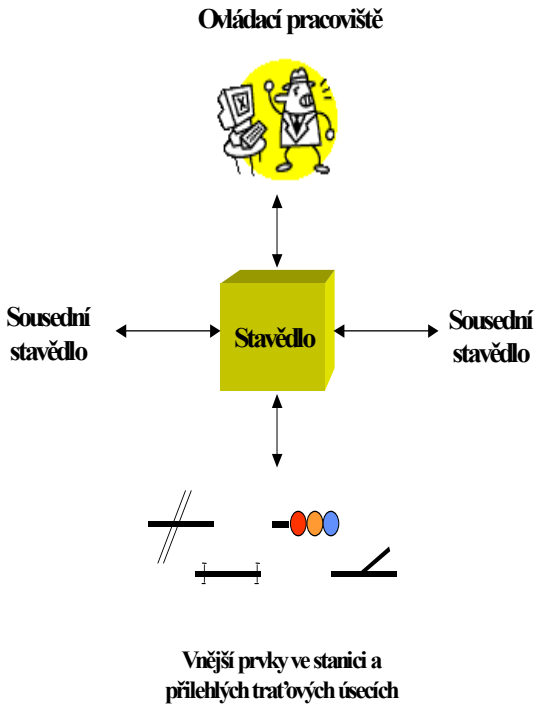
Je nasnadě (a také se často využívá) možnost nedohlížet přímo na impulsní svícení žárovky, ale dohlížet v daném okamžiku impulsní charakter napájecího zdroje. Zdroj impulsního proudu pro žárovky by měl mít parametry:

- pomalé kmitání : 0,9 Hz ± 10%, trvání impulsu 40 - 60 %,
- rychlé kmitání : 1,8 Hz ± 10%, trvání impulsu 30 - 60 %.

13 ZABEZPEČENÍ DOPRAVY VE STANICI

"... zařízení má být takové, aby se dalo lehce obsluhovati, aby i slabší zřízenci mohli každý jednotlivý úkon bez zvláštní námahy vykonati ..." Theodor Nechvátal, vrchní inspektor ministerstva železnic, Telegrafní, telefonní, návěstní a zabezpečovací zařízení u státních drah, Praha 1923.

Pro zabezpečení dopravy ve stanicích se používají zařízení pod souhrnným označením stavědla. Název stavědlo je odvozen od jeho základní funkce - „stavění“ jízdních cest pro vlaky a posunové díly. V současné době lze ovšem pod označením „stavědlo“ nalézt i takové zařízení, které kromě své základní funkce plní úkoly, připadající jiným druhům zabezpečovacích zařízení (přejezdovým, traťovým), popř. také funkce, které samy o sobě vliv na bezpečnost nemají, ale podílejí se významně na efektivním řízení dopravy (práce s číslem vlaku, automatické stavění jízdních cest,...).



Obr. 13-1

Stavědlo, jako technické zařízení, lze vymezit určením jeho rozhraní k okolnímu prostředí (obr. 13-1). Činnost stavědla je řízena, usměrňována z hierarchicky vyšší úrovně, která v tom nejjednodušším případě může být představována obslužným pracovištěm operátora stavědla (výpravčím). Stavědlo předává pracovišti informace o stavu svém i řízeného dopravního procesu. V opačném směru je stavědlo pracovištěm povelováno. Hierarchicky nižší úroveň představují vnější jednotky zabezpečovacích zařízení, tvořící jízdní cestu. Těmito jednotkami jsou například kolejové úseky, výhybky, křižovatky, ap. Stavědlo vnější jednotky poveluje se záměrem dosáhnout jejich požadované polohy. V opačném směru se stavědlu dostávají informace o skutečném stavu těchto jednotek.

Důležitým rozhraním je pro stavědlo styk s prostředky pro předávání oprávnění k jízdě ať už vlaku nebo posunovému dílu. Nejrozšířenějším typem tohoto zařízení jsou dnes optická návěstidla. Jejich technickým následníkem, umožňujícím zprostředkování mnohem podrobnější informace o oprávnění k jízdě, je vlakový zabezpečovač. Ať už se jedná o kterýkoliv výše jmenovaný typ zařízení, platí i pro něj, že je

stavědlem povelován s cílem předat vlaku (posunu) takový stupeň oprávnění k jízdě, který byl stavědlem vyhodnocen, a v opačném směru informuje stavědlo o svém stavu.

Pokud stavědlo netvoří ostrůvek v oblasti zcela nevybavené zabezpečovacími zařízeními, pak jeho nezbytnou součástí je bezpečná komunikace s navazujícími systémy. Těmito systémy mohou být jak druhově odlišná zabezpečovací zařízení (přejezdová, traťová), tak sousedící zařízení staniční (stavědla). Všechny tyto systémy jsou hierarchicky rovnocenné, navzájem spolupracující, ale také navzájem svou činnost podmiňující (blokující). Pro moderní stavědla mohou být vnější prvky jak traťového, tak přejezdového zařízení pojata stejně jako jakékoliv prvky ve stanici, protože mohou integrovat i veškerá zařízení z přilehlých úseků.

Hlavním posláním stavědla je připravit a zajistit cestu pro bezpečnou jízdu vlaku nebo posunového dílu. K tomu musí stavědlo vykonat minimálně následující sekvenci úkonů:

- kontrola dostupnosti jízdní cesty,
- vyhrazení jednotek jízdní cesty,
- přestavení jednotek s pohyblivými částmi do požadované polohy,
- zapevnění jízdní cesty,
- výběr a vyslání odpovídajícího oprávnění k jízdě,
- vybavení jízdní cesty.

Stavědlo, jako zařízení zabezpečující pohyb vlaků v obvodu stanice, neplní jen úlohy související s řádným stavěním a vybavováním jízdních cest. Tato jeho funkce je samozřejmě primární, ale pro její podporu, pro řešení nouzových situací a též pro řízení posunové práce ve stanici, je nezbytně nutný soubor dalších funkcí, jakými jsou např.:

- změna polohy jednotky,
- zavedení nouzového závěru,
- nouzové uvolnění závěru jednotky,
- vyloučení jednotky,
- zablokování jednotky,
- předání části obvodu stavědla na místní obsluhu.

Výčet funkcí, uvedených jako základní pro stavění jízdních cest, jakož i funkcí podpůrných, není v žádném případě úplný; představuje jen základní soubor, který musí staniční zařízení umožňovat a bezpečným způsobem realizovat.

Kontrola dostupnosti jízdní cesty
Po přijetí povelu z obslužného pracoviště k postavení jízdní cesty z místa A do místa B je zapotřebí prověřit, zda je povel proveditelný, tj. především zda je kolejově možné takové spojení realizovat. Poté následuje výběr a kontrola dostupnosti jednotlivých jednotek, které mají být na jízdní cestě zúčastněny. Zjišťuje se, zda kolejové úseky jsou volné, zda výhybky je možné přestavit a zda se žádná z jednotek nenachází v nějaké dříve postavené jízdní cestě. Jestliže od místa B není postavena navazující jízdní cesta, může být součástí kontroly taktéž správné označení konce jízdní cesty v místě B. Pokud je toto prověření pozitivní, může následovat další krok.

Vyhrazení jednotek jízdní cesty
Úlohou této funkce stavědla je všechny jednotky zvolené jízdní cesty pro tuto cestu rezervovat, aby jakýkoliv další přijatý povel, který by některou z jednotek vyžadoval, nemohl celý proces stavění jízdní cesty narušit.

Přestavení jednotek s pohyblivými částmi do požadované polohy
Jakmile jsou všechny potřebné jednotky rezervovány, je možné přistoupit k vytváření skutečně sjízdné dráhy mezi místy A a B, tj. k přestavování jednotek s pohyblivými částmi do požadované polohy. Těmito jednotkami jsou zpravidla výhybky a výkolejky, mohou jimi však též být pohyblivé hroty srdcovek kolejových křižovatek nebo např. zvedací mosty.

Zapevnění jízdní cesty
Jsou-li všechny jednotky jízdní cesty v poloze, umožňující požadovanou jízdu, je potřebné je v této poloze zapevnit. Toto zapevnění je možné provést uzamčením za použití zámku nebo elektricky, bezpečným odpojením napájecího napětí přestavných motorů, popř. provedením logického uzavření jednotky v cestě, nemá-li tato pohyblivé komponenty (např. závěr kolejového úseku pro zablokování protisměrných jízdních cest).

Výběr a vyslání odpovídajícího oprávnění k jízdě
Na základě informací, které stavědlo získá o připravené jízdní cestě, je možné vybírat odpovídající stupeň oprávnění k jízdě. Při výběru jsou rozhodujícími faktory omezení rychlosti pro jízdu odbočnými větvemi výhybek a vzdálenost k cíli jízdní cesty (vzdálenost |AB|), pokud je v cíli cesty nařízeno zastavení nebo omezení rychlosti. U mnoha železničních správ je důležitým faktorem při výběru stupně oprávnění k jízdě taktéž délka pojistné (prokluzové) vzdálenosti za cílem jízdní cesty, pokud je další jízda zakázána. U systémů,, využívajících spolupráce s vlakovým zabezpečovačem je možné přizpůsobit výběr oprávnění i znalostem o nejvyšších dovolených rychlostech v jednotlivých úsecích jízdní cesty.
Vybrané oprávnění se přenáší určenému vlaku nebo posunovému dílu dostupnými prostředky, které již byly zmíněny výše.

Vybavení jízdní cesty
Jakmile vlak či posunový díl obdrží oprávnění k jízdě, smí vstoupit za bod začátku postavené jízdní cesty. Tímto bodem je zpravidla optické návěstidlo, u jednodušších dopravních poměrů však může být určen i jiným způsobem; u systémů využívajících vlakového zabezpečovače je tímto místem aktuální pozice vlaku.
Vlak (posunový díl) který postupně jízdní cestu projíždí, připravuje zároveň podmínky pro její vybavení tak, aby bylo zajištěno její bezpečné trvání po dobu jízdy toho vlaku, pro který byla cesta postavena, a současně aby jízdní cesta nesetrvávala zapevněna nad dobu nezbytně nutnou. Nejjednodušším řešením tohoto problému je zkontrolovat, zda vlak opustil celý úsek mezi místy A a B, nebo před místem B zastavil.
Pokud je potřebné zvětšit intenzitu dopravy, je takový přístup z důvodu dlouhého času, nutného k projetí dráhy mezi A a B, nedostatečné. Řešením je tzv. postupné vybavování jízdní cesty. Princip postupného vybavování jízdní cesty tkví v plynulém bezpečném sledování pohybu vlaku jízdní cestou, na základě kterého je možné vyvodit, že konec vlaku bezpečně opustil část jízdní cesty. Zapevnění vlakem uvolněné části jízdní cesty pak smí být zrušeno a jednotky této části mohou být použity v jiné, následně požadované cestě.

Změna polohy jednotky
Tato funkce je použita u jednotek s pohyblivými částmi (výhybky, výkolejky, ap.) a slouží dopravním i servisním potřebám. Z dopravních důvodů je nutno tuto funkci použít v případech, kdy jednotka nereaguje na povel, vydaný stavědlem v rámci stavění jízdní cesty, nebo je- li stavěna jízdní cesta nouzovým způsobem. Servisním důvodem je zpravidla mazání třecích ploch a kontrola chodu pohyblivých částí.

Zavedení nouzového závěru
Pokud není možné jízdní cestu postavit řádným způsobem, není samozřejmě přípustné zastavit dopravu. Z toho důvodu je zajištěn přístup k jednotlivým jednotkám pro změnu jejich polohy - viz předchozí odstavec - a také možnost tyto jednotky v jejich koncových polohách zapevnit, aby při jízdě vozidel nedošlo k jejich náhodnému přestavení. Každou jednotku musí být proto možné kromě jejího uzavření v řádné jízdní cestě zapevnit též náhradním způsobem, kterým je obvykle přímý přístup k bezpečnému odpojení napájecího napětí přestavných motorů.

Nouzové uvolnění závěru jednotky jízdní cesty
Sledování pohybu vlaku jízdní cestou musí být bezpečné, to již bylo uvedeno výše. Pokud tedy v tomto sledování nastane porucha, musí být jejím důsledkem, že ta část jízdní cesty, o které není možné hodnověrně prohlásit, že byla opuštěna koncem vlaku (posunu), musí zůstat zapevněna. Taková situace ovšem pochopitelně vede ke znemožnění stavění dalších jízdních cest, které ty zapevněné jednotky vyžadují. Z toho důvodu musí stavědlo disponovat funkcí, která umožní operátoru poté, co na vlastní zodpovědnost prohlásil cestu (nebo její část) za projetou, nouzovým způsobem zrušit její zapevnění (uvolnit závěr).

Vyloučení jednotky
V některých případech je potřebné vyloučit možnost použití jednotky v jízdní cestě. Obvykle tomu bývá tehdy, jestliže se na dotyčné jednotce provádí údržba či oprava takového rozsahu, která si vyžaduje přijetí nouzových opatření. V těchto situacích je k dispozici možnost takovou jednotku označit a zabránit stavědlu, aby ji v řádné jízdní cestě používala.

Zablokování jednotky
Užití této funkce je obdobně jako v předchozím případě předpokládané při servisní činnosti. Důsledkem je ovšem nikoliv zabránění jejího použití v jízdní cestě, nýbrž zablokování možnosti jejího přeložení do jiné polohy (např. zablokování možnosti přestavit výhybku).

Předání části obvodu stavědla na místní obsluhu
Pokud technologie práce ve stanici předpokládá větší rozsah posunu, zřizují se obvykle pomocná stavědla, jakožto podřízené buňky, vybavené možností ovládat jednotky, nezbytné k realizaci posunové práce na vymezených kolejích.

14 ZABEZPEČENÍ DOPRAVY NA ŠIRÉ TRATI

"Zabezpečovacím zařízením na tratích nutno ... nejen dohonění, nýbrž i setkání se vlaků opačných směrů zameziti ..." M. Boda, em. hon. docent při c.k. Vysoké škole technické v Praze, Zabezpečování dopravy vlakové na železnicích, Praha 1905.

Pro bezpečnou jízdu vlaků na širé trati je třeba zajistit, že :

- na tutéž traťovou kolej nebudou vypraveny proti sobě jedoucí vlaky a že
- následné vlaky jedoucí po téže traťové koleji budou řízeny tak, aby se k sobě nepřiblížily více než je bezpečné.

Splnění první podmínky musí být zajištěno takovou spoluprací stanic na hranicích širé trati, která dovolí odjezdovou vlakovou cestu jen tehdy, když na traťové koleji není vlak směřující proti a když v protější stanici není vlak již směřující na tuto traťovou kolej a jsou znemožněny všechny odjezdové vlakové cesty na tuto kolej. Realizace je možná tzv. souhlasem, který může být :

- udělovací, což znamená, že žádná ze stanic nemá v základní poloze souhlas a souhlas k jízdě je udělován stanicí vlak přijímající, při splnění určitých podmínek, pro každý vlak samostatně,
- kyvadlový, kdy v základní poloze má souhlas jedna stanice a ta vypravuje vlaky tak dlouho, dokud neobdrží žádost o souhlas ze sousední stanice. Pak, za splnění určitých podmínek, udělí sousední stanici souhlas k jízdě a ta bude vypravovat vlaky tak dlouho, dokud nedojde opět k žádosti o změnu směru,
- nezadaný, kdy při pokusu o postavení odjezdového návěstidla ve vlastní stanici dojde prostřednictvím žádosti o souhlas nejprve k zablokování odjezdu v sousední stanici (za předpokladu, že trať je volná a v sousední stanici není připravována odjezdová cesta) a v důsledku toho k udělení souhlasu, což umožní dokončit postavení odjezdové vlakové cesty.

Oba posledně uvedené způsoby se v praktické realizaci liší jen málo a jsou v podstatě vhodné i pro automatická zařízení, kdežto prvně uvedený způsob je určen pro poloautomatické řízení se striktním zachováním rovnoprávnosti obou výpravčích.

Řízení následných vlaků lze v zásadě řešit třemi způsoby:

- soustavou časovou,
- soustavou pevných prostorových oddílů a
- soustavou pohyblivého bloku (moving block, dříve označováno také jako jízda na elektrický dohled).

Při časové soustavě se následné vlaky na trať vypravují za vlakem předchozím po uplynutí stanoveného času. Tento systém nepředstavuje žádné nároky na přenos informací a jeho nebezpečnost v případě, že se vpředu jedoucí vlak omeškal, není třeba rozebírat, využíván byl v počátcích železnice.

Prostorová soustava (podobně jako soustava časová) dělí trať na prostorové úseky, oddíly, pro něž však platí, že se uvnitř oddílu smí nacházet pouze jeden vlak. Proto podmínkou pro vpuštění následného vlaku do oddílu (tzv. základní blokovou podmínkou) je tentokrát skutečně informace o jeho úplném vyklizení vlakem předchozím, což ve svém důsledku znamená potřebu přenosu informace z konce oddílu na jeho začátek. Základní bloková podmínka se u většiny traťových zařízení doplňuje na tzv. úplnou blokovou podmínku, která vyžaduje, aby před uvolněním návěstidla na vstupu do oddílu došlo nejen k jeho úplnému vyklizení předchozím vlakem, ale také k přestavení následujícího návěstidla do polohy "stůj". Jde v podstatě o zavedení doplňkové kontroly sledu funkce. Ta sice většinou znamená zvýšení bezpečnosti obvodového řešení, ale zařízení jako celek bude náchylnější na zablokování funkce v případě jakékoliv provozní nepravidelnosti, což v souhrnu poskytnutou úroveň bezpečnosti naopak snižuje. Tento častý paradox je nutné v zabezpečovací technice řešit individuálně, vždy s přihlédnutím k celému komplexu provozních a technických požadavků.

Ohraničením pevného oddílu návěstidly se pouze nemotorně nahrazuje návěstidlo, které by správně mělo být umístěno v jisté vzdálenosti za vlakem a s ním se plynule pohybovat. Vznikla by tak soustava s pohyblivým blokem, která byla realizována až mnohem později a to ve spolupráci s vlakovým zabezpečovačem, který problém pohybující se „návěsti“ je schopen v některých aplikacích vyřešit při existenci kontinuálního nebo kvasikontinuálního spojení hnacího vozidla s traťovým systémem.

Druh a způsob aplikace traťového zabezpečovacího zařízení určují hustotu a počet vlaků, které je možné po trati přepravit. Proto při projekci traťového zařízení je nutné kromě bezpečnostních aspektů sledovat i aspekty dopravní, vyjadřované takovými termíny jako je propustnost či následné mezidobí. Na obr. 14-1 je zachycena situace u klasického traťového zařízení se samostatnými předvěstmi. Každý oddíl (o

délce Lpo) je kryt oddílovým návěstidlem a před ním umístěnou předvěstí. Obrázek zachycuje situaci, kdy na návěstidle Lo1 právě došlo ke změně z "červené" na "zelenou", protože vlak 1 vyklidil oddíl mezi návěstidly Lo1 a Lo3 a uplynula doba obsluhy (reakce) zařízení t_o, za kterou vlak ujel dráhu L_o. V tomto okamžiku se 2. vlak může nacházet nejdále v takovém místě, kde ještě spolehlivě dostane informaci o tom,

Obr. 14-1

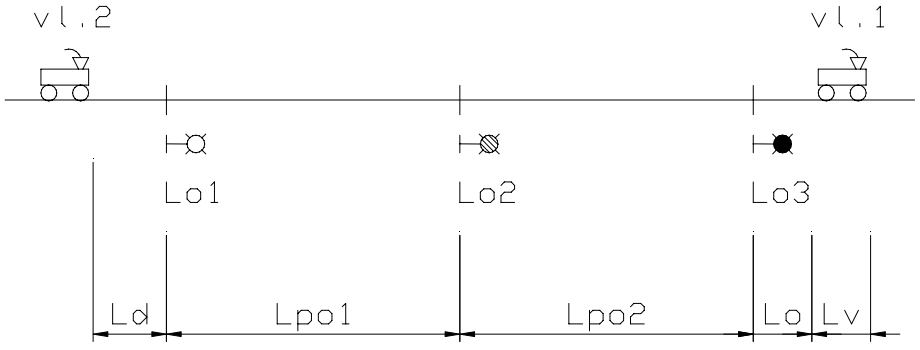
že nemusí rychlost jízdy z titulu přiblížení se k 1. vlaku snižovat, tj. ve vzdálenosti předepsané dohlednosti předvěsti PřLo3 - L_d. Předvěst je umístěna minimálně na zábrzdnou vzdálenost L_z před hlavním návěstidlem a vlak je dlouhý L_v. Pak vzdálenost následných vlaků nemůže být kratší než

$$l_{min} = L_d + L_z + L_{po} + L_o + L_v$$

a interval následné jízdy τ_{nj} (nejmenší časový odstup mezi dvěmi stejným směrem jedoucími vlaky, při kterém je zajištěna bezpečnost a plynulost provozu) nemůže být pro vlaky pohybující se rychlostí **v** kratší než

$$\tau_{nj} = 3600 \frac{l_{min}}{v} \qquad [s; km, km/h]$$

Je zřejmé, že pro výpočet vzdálenosti následných vlaků je nezbytné uvažovat nejhorší případ, který se ve sledovaném úseku vyskytuje. Zkracování délky L_{po} povede ke zkrácení následného mezidobí, ale také ke zvýšení investičních a provozních nákladů na traťové zabezpečovací zařízení. Zkracování je samozřejmě



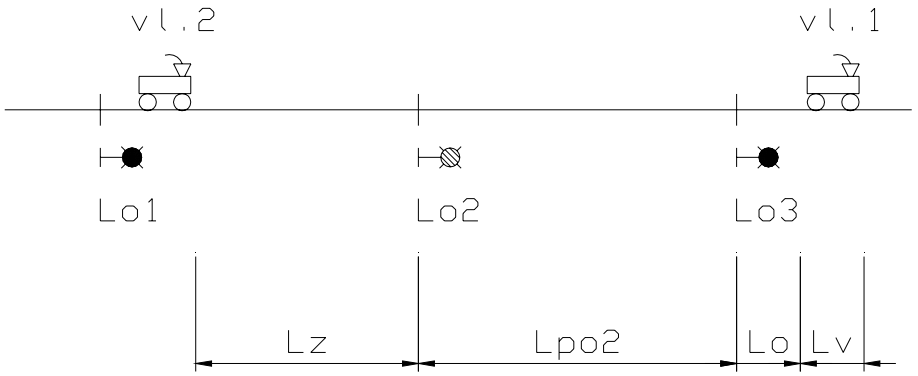
Obr. 14-2

limitováno zábrzdnou vzdáleností L_z. V takovém případě by předvěsti byly umístěny v úrovni předchozího oddílového návěstidla, což odpovídá obvyklému rozmístění zařízení při automatickém bloku, kde každé oddílové návěstidlo je současně předvěstí následujícího návěstidla (předvěst je sloučená s předchozím oddílovým návěstidlem). Pokud se strojvedoucí bude řídit optickými návěstidly, bude minimální vzdálenost následných vlaků na tříznakém automatickém bloku (obr. 14-2):

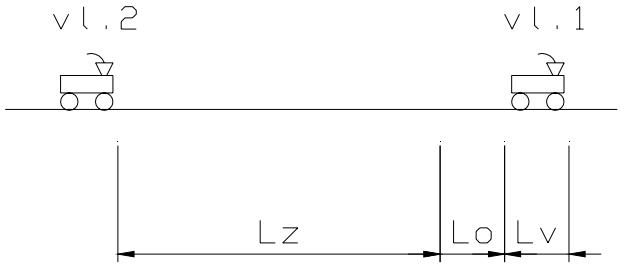
$$l_{min} = L_d + 2 \cdot L_{po} + L_o + L_v$$

přičemž délka oddílu L_{po} bývá jen o málo větší než zábrzdná vzdálenost L_z . V případě, že vlaky budou vybaveny inteligentním vlakovým zabezpečovacím zařízením, které určuje individuální brzdnou křivku vlaku pro každé návěstidlo se znalostí jeho skutečné polohy, bude postačující, aby ke změně návěstidla došlo nejpozději v okamžiku, kdy se vlak nachází právě na zábrzdnou vzdálenost před návěstidlem (viz obr. 14-3). Minimální vzdálenost následných vlaků se tak může snížit až na

$$l_{min} = L_z + L_{po} + L_o + L_v .$$



Obr. 14-3



Obr. 14-4

V případě pohyblivého bloku je konec vlakové cesty následujícího vlaku dán poslední známou polohou konce předchozího vlaku (obr. 14-4). Minimální přípustná vzdálenost následných vlaků by pak byla

$$\mathbf{l}_{min} = L_z + L_o + L_v$$

(Teoreticky by bylo možné uvažovat ještě další přiblížení vlaků a to až na vzdálenost

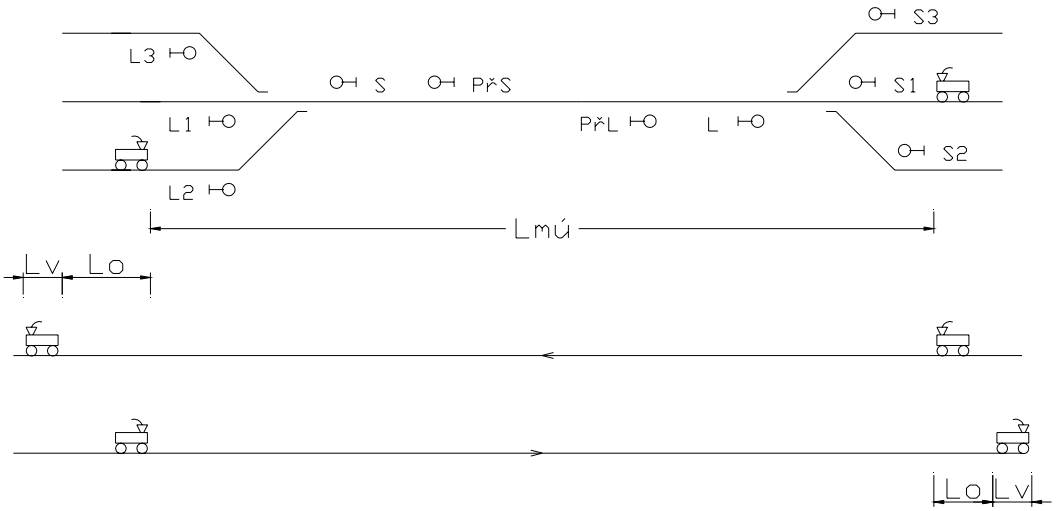
$$\mathbf{l}_{min} = L_o + L_v$$

v případě, že bude zajištěno, že první vlak nebude schopen většího odrychlení než druhý vlak a že okamžitá rychlost 2. vlaku nebude vyšší než okamžitá rychlost 1. vlaku. Druhý vlak by tedy musel mít informaci nejen o poloze konce 1. vlaku, ale i o jeho okamžité rychlosti a odrychlení.)

Při jízdě následných vlaků je zkracování délky prostorového oddílu prostředkem pro dosažení kratšího následného mezidobí. Při střídavé jízdě vlaků opačných směrů musí vlaky celou vzdálenost mezi stanicemi skutečně postupně ujet a pak teprve je možné vyslat následný vlak. Zjednodušeně je tato situace zachycena na obr. 14-5. Vzdálenost, kterou musí vlaky postupně ujet je

$$\mathbf{I}_{min} = 2 \cdot L_{mú} + 2 \cdot L_o + 2 \cdot L_v ,$$

přičemž je nutné počítat až se dvěmi rozjezdy a dvěmi brzděními. Z údajů na obrázku lze stanovit, jaká doba uplyne mezi odjezdem vlaku v jednom směru a příjezdem vlaku z opačného směru. Výsledek ukazuje na význam konstrukce tzv. svazkového grafikonu, kdy určitý počet vlaků jede ve svazku v jednom směru a potom se změní směr provozu a určitý počet vlaků jede opět ve svazku v opačném směru. Lze tak provést podstatně více vlaků než by bylo možné při změně směru po každém vlaku. Patrný je i důsledek rozdílných rychlostí vlaků na propustnou výkonnost trati. Plně svazkový lze grafikon konstruovat na dvoukolejné trati, kde je každá kolej pravidelně využívána pouze v jednom směru (opačný směr se využije pouze výjimečně při kolejových výlukách a jiných plánovaných nebo neplánovaných nepravidelnostech). To je důvod, proč dvoukolejná trať je více než dvojnásobně výkonná v porovnání s tratí jednokolejnou.

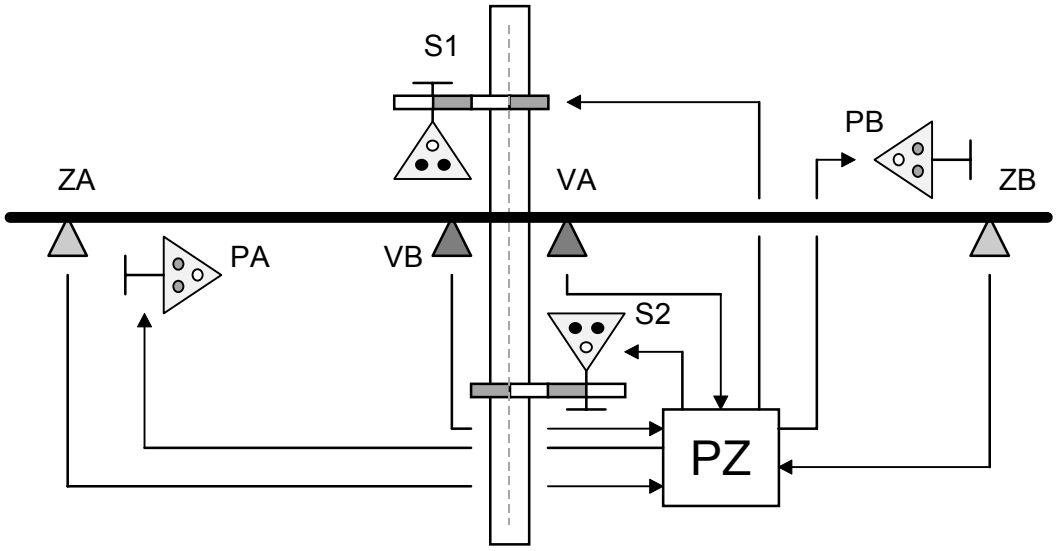


Obr. 14-5

15 ZABEZPEČENÍ PŘEJEZDŮ

I když železnice má ze zákona při křížení se silniční dopravou přednost, je v jejím zájmu, aby pro respektování této přednosti uživateli silnic vytvořila co nejlepší podmínky, protože střety se silničním vozidlem, byť neprávem se na přejezdu vyskytujícím, mají na bezpečnost a spolehlivost železniční dopravy katastrofální dopad. Riziko nehody stoupá s rostoucím provozem na přejezdu (tzv. dopravní moment přejezdu), následky pro železniční provoz stoupají s hmotností silničního vozidla a rychlostí vlaku. I když na nejzatíženějších přejezdech je jediným dostatečným opatřením zřízení mimoúrovňového křížení, v ostatních případech se (zejména vzhledem k vysokým investičním nákladům mimoúrovňového křížení) zřizují a nadále budou zřizovat automatická přejezdová zabezpečovací zařízení. Tato zařízení musí:

- v dostatečném předstihu před příjezdem vlaku informovat uživatele silnic, že se k přejezdu blíží vlak (spustit výstrahu),
- poté setrvat ve výstraze tak dlouho, dokud vlak svou jízdu (k přejezdu a přes přejezd) neukončí,
- při vzdalování vlaku od přejezdu zajistit, aby zařízení nepovažovalo další jízdu vlaku za přibližování druhého vlaku z opačného směru,
- předávat, přímo či zprostředkovaně, potřebné informace vlaku.



Obr. 15-1

Na obr. 15-1 je nakreslena základní sestava přejezdového zabezpečovacího zařízení. Přejezdové zařízení PZ je informováno o blížícím se vlaku zapínacími body ZA a ZB. Zapínací body musí reagovat na čelo vlaku (tedy vycházet z detekce přítomnosti a směru) a musí být umístěny na takovou vzdálenost od vlastního křížení, aby poté, co přejezdové zařízení zaregistruje blížící se vlak a vyvolá výstrahu na výstražnících S1 a S2, do příjezdu vlaku uplynula doba dostatečná k vyklizení přejezdu silničním vozidlem, popř. chodcem. Vyklizovací doba je závislá na délce přejezdu (počtu kolejí, úhlu křížení, šířce vozovky atd.). Vzdálenost zapínacích bodů od křížení se pak určí na základě potřebné vyklizovací doby, rychlosti vlaku v úseku před přejezdem, doby reakce zařízení, bezpečnostní rezervy atd. Při další jízdě vlaku je ovlivněn vypínací bod VA (VB). Úlohou tohoto bodu je poskytnout do PZ informaci, že vlak skutečně dospěl do prostoru (případně za prostor) křížení a že PZ může výstrahu ukončit.

Zařízení musí předávat uživatelům silnice prostřednictvím výstražníku tři informace:

- výstraha - k přejezdu se blíží vlak,
- klidový stav - k přejezdu se neblíží vlak,
- porucha zařízení - přejezd je nechráněn.

Informace musí být předány způsobem, který vylučuje omyl. Pro výstrahu se obvykle volí dvě kmitavá červená světla, protože se tato kombinace považuje za nejsnáze rozpoznatelnou a nehrozí záměna tak, jak by tomu bylo při použití jinak na železnici všeobecně přijatého klidného červeného světla (např. koncové světlo vpředu jedoucího auta). Tato základní výstraha se obvykle doplňuje akustickou návěstí a v některých případech závorami. Pro klidový stav byla dříve obvykle volena energeticky co nejméně náročná návěst, což u optických návěstidel je jistě zhaslý výstražník. To však znemožňuje odlišit třetí informaci - poruchový stav, která by měla být předána i v případě úplné ztráty napájení. Z toho důvodu je pro klidový stav nyní volena aktivní (tzv. pozitivní) návěst, obvykle lunobílé kmitavé světlo a při poruše zařízení je výstražník zhaslý. Výše uvedené základní přiřazení návěstí na výstražnících je dnes u ČD porušováno tím, že v případě, kdy se na spouštění přejezdu podílí lidský činitel (např. přejezd ovládaný z jedné strany výpravčím) je pozitivní návěst trvale zhasnuta. Uživatel silnice pak ovšem ví, že řada přejezdových zařízení se zhaslými výstražníky je schopna hlásit příjezd vlaku ale nemůže rozeznat přejezd s chybějící pozitivní návěstí od přejezdu s poruchou. Důsledkem pak je, že se u neosvětleného výstražníku nechová tak, jak bylo zamýšleno, tj. jako na nechráněném přejezdu, ale naopak tak, že každý přejezd s výstražníkem bez výstrahy považuje za potvrzení skutečnosti, že se vlak neblíží.
Původní pojetí přejezdových zařízení vycházelo z názoru, že vlak má vždy přednost, tedy uživatel silnice je vždy povinen mu přednost dát a dráha jaksi navíc zajišťuje, že přibližující se vlak spustí výstrahu (pokud je zařízení v pořádku). Logika tohoto postupu by byla obhajitelná jen pokud by železnice za všech okolností zajistila na přejezdech dostatečné rozhledové poměry pro uživatele silnice, což je však dnes na řadě přejezdů prakticky vyloučeno. Neorganické zavedení pozitivní návěsti, na základě mezinárodních dohod, spolu s všeobecnou nekázni uživatelů silnic vytváří mimořádně nepříznivé situace v bezpečnosti na přejezdech, i když jsou sem vkládány nemalé prostředky. Představa, že by se za této situace měla rychlost vlaků také na přejezdech zvýšit na 160 km/h je alarmující. Existující rozpory je nezbytné urychleně a jednoznačně vyřešit zákonnými úpravami.

Přejezdové zařízení dále musí v jistém rozsahu informovat o svém stavu, přímo či zprostředkovaně, vlak, což je na obr. 15-1 naznačeno zařízením PA (PB). Potřebná úroveň této stavové informace je závislá na bezpečnostních parametrech jednotlivých subsystémů přejezdového zařízení a na požadované úrovni poskytované bezpečnosti a lze ji zásadně dělit do tří úrovní:

1. přejezdové zařízení se nachází v pohotovostním stavu a není známa žádná okolnost, která by momentálně bránila zařízení, po jeho ovlivnění, dávat řádně výstrahu,
2. výstraha na přejezdovém zařízení již byla aktivována,
3. na přejezdu po zahájení výstrahy již uplynula celá vyklizovací doba (a případně přídavným zařízením pro detekci překážek na křížení je hlášeno, že průjezdný profil je volný).

První úrovní je v současnosti v České republice vybavena většina automatických přejezdových zařízení. Používá se přejezdových zařízení s přenosem informace o pohotovosti k výstražnému stavu výpravčímu. Nedostatkem je skutečnost, že takový způsob informování dopravního personálu nepokrývá případy, kdy k poruše na přejezdovém zařízení dojde po odjezdu vlaku ze stanice. Při centralizaci řízení dopravního procesu pak vzniká nutnost přenášet tuto informaci na značné vzdálenosti a při absenci prostředku radiové komunikace výpravčí - strojvedoucí se značně prodlužuje dobu, po kterou nelze na poruchu zařízení reagovat. (Na druhé straně je ovšem přejezdové zařízení konstruováno tak, aby při většině vnitřních poruch přešlo do výstrahy. To však nelze na přejezdu zajistit plně, protože například při totální ztrátě napájení, nelze samozřejmě zajistit svícení výstrahy.) Přes tyto nedostatky je použití takového typu zařízení opodstatněné na tratích s velkou hustotou dopravy, protože je nejefektivnější z hlediska neomezování silniční dopravy. Určité zlepšení by přinesl přenos stavových informací o přejezdu přímo na vlak nebo zařazení příslušné stavové informace do posledního návěstidla kryjícího přejezd, což bývá většinou odjezdové návěstidlo v poslední stanici před přejezdem nebo oddílové návěstidlo. Ve všech těchto případech by odpadla aktivní úloha dopravního personálu na zprostředkování informace, bylo by však nutné zároveň předpisem upravit reakci dopravních zaměstnanců a strojvedoucího. Jistou nevýhodou je pak podmíněnost funkce jednoho systému funkcí jiného systému.

Při druhé úrovni je možné použít pro aktivaci výstrahy na přejezdu prvků, které nemají význak prvků bezpečných. Nevýhodou je obvykle prodloužení doby výstrahy na přejezdovém zařízení v důsledku nutnosti předávat informaci o spuštění výstrahy vlaku tak, aby v případě, že k vyvolání výstrahy pro poruchu zařízení nedojde, vlak stačil před nechráněným přejezdem zastavit. K tomu účelu je i nutné instalovat zvláštní návěstidla - přejezdníky, které jsou investičně i provozně značně náročné. Toto řešení se obvykle využívá pouze na tratích s menší hustotou dopravy a kratšími zábrzdnými vzdálenostmi. Alternativou je opět využití systémů pro přenos informací přímo na vlak.

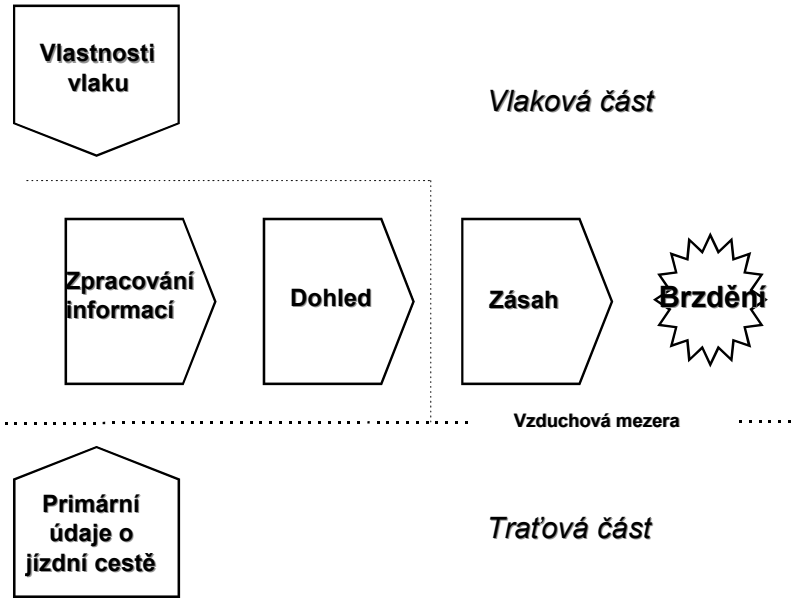
Třetí úroveň poskytuje maximální míru bezpečnosti pro oba účastníky křížení dvou druhů doprav. Zajišťuje totiž obvykle nejen varování řidičů silničních vozidel, ale také volnost jízdního profilu pro vlak a možnost zastavit vlak v případě, že prostor křížení se nepodařilo včas uvolnit. Nevýhodou jsou opět vysoké investiční náklady a extrémně dlouhá výstražná doba, v jejímž průběhu musí proběhnout uzavření a vyklizení přejezdu a informace o vyklizení přejezdu musí být vlaku předána tak včas, aby byl v případě potřeby schopen před přejezdem zastavit. To jsou také důvody, proč se zařízení tohoto typu u nás (a u řady dalších železničních správ) nebudují. Význam by však mohly mít zejména na tratích s vyššími rychlostmi v těch případech, kdy není možné budovat mimoúrovňové křížení.

16 ZABEZPEČENÍ HNACÍCH VOZIDEL

Hlavním úkolem vlakového zabezpečovacího zařízení je zajistit, že nedojde k ohrožení vlaků při omylu nebo indispozici strojvedoucího. K tomu účelu zařízení obecně musí:

- shromáždit potřebné informace,
- informace zpracovat, tj. stanovit limity bezpečného pohybu vlaku,
- trvale dohlížet, že limit není překračován a
- zasáhnout do jízdy vlaku v případě, že překročen je.

Tyto své základní činnosti může zařízení plnit v různém rozsahu a s různou úrovní, v závislosti na požadavcích železniční správy (příklad je na obr. 16-1). Rozsah jednotlivých činností je funkcí dostupných informací a má značný vliv na celkové náklady na pořízení a provoz systému. Pokud jsou informace dostatečné (a to jak obsahem, tak kvalitou), je možné za normálních provozních podmínek zcela vyloučit případ nerespektování návěstidel a rychlostních omezení vlakem.



Obr. 16-1

Kromě tohoto svého primárního úkolu je ale vlakové zabezpečovací zařízení, při využití nových technologií, přímo předurčeno podílet se mnohem výrazněji než doposud na celkovém řízení dopravy. Vlakové zabezpečovací zařízení může za určitých podmínek poskytovat řídícímu dopravnímu systému některé mimořádně důležité základní informace, které jsou dnes získávány pomocí fixních zařízení na trati. Tak například informace o poloze vlaku je u klasických zařízení získávána kolejovými obvody nebo počítači náprav a to s nejistotou délky překlenovaného úseku. Inteligentní vlakový zabezpečovač je schopen tuto informaci řídícímu systému poskytnout (opět za určitých předpokladů) dokonce přesněji, jako produkt své běžné činnosti a za celkově významně nižší investiční náklady.

Protože se jedná o zabezpečovací zařízení, musí konstrukce zařízení plně vyhovovat zásadám zabezpečovací techniky. Vlakové zabezpečovací zařízení může však plnit i další funkce, které již nemají přímý vliv na bezpečnost dopravy ve smyslu zabezpečovací techniky (např. otvírání/zavírání dveří, stahování pantografu atd.). Jako integrální součást nebo jako nástavba mohou být k vlakovému zabezpečovači připojeny také jednotlivé prvky nebo celý systém automatického řízení vlaku. Jejich účelem je buď pomáhat strojvedoucímu v řízení (např. zobrazením průběhu skutečné a doporučené rychlosti), nebo skutečně automaticky ovlivňovat rychlost vlaku (např. prostřednictvím regulátoru rychlosti nebo cílového brzdění). Jako další nástavba pak může být dále připojeno zařízení pro automatickou úpravu jízdy vlaku na základě přídavných optimalizačních procesů (např. podle výsledků časové nebo energetické optimalizace). V zásadě

je možné, aby veškeré tyto nástavby vlakového zabezpečovače byly budovány jako samostatné celky. Dohromady ale musí tvořit hierarchickou strukturu, ve které jsou základní funkce vlakového zabezpečovače nadřazeny ostatním. Domyslíme-li bezpečnostní aspekty, lze dokonce říci, že žádné z těchto nástavbových zařízení nelze přímo provozovat bez vlakového zabezpečovače. Vlakový zabezpečovač potom ale musí být uspořádán tak, aby řízení vlaku zbytečně neomezoval a zasahoval pouze v případech skutečného ohrožení bezpečnosti jízdy.

16.1 Informace

Informacemi, potřebnými pro vlaková zabezpečovací zařízení, jsou obecně údaje o:

- vlaku:
  - charakteristika (max. dovolená rychlost, brzdové schopnosti, délka vlaku atp.),
  - okamžitá rychlost a zrychlení,
  - poloha,
- aktuální dopravní situaci (povolení k jízdě),
- charakteristice tratě:
  - dovolená traťová rychlost,
  - trvalá a přechodná omezení traťové rychlosti ze stavebních důvodů,
  - sklon,
- ostatní.

Veškeré informace lze charakterizovat proměnností (v závislosti na dopravní situaci, trati a čase) a místem původu.

16.1.1 Proměnnost

Časově proměnné jsou informace o aktuální dopravní situaci a o skutečné rychlosti vlaku. Všechny další informace o vlastnostech vlaku jsou spojeny s jeho sestavením a nemění se, pokud se nemění sestava.

Zbývající informace jsou pak pevně spojeny s tratí a jako časově proměnné se pro vlak jeví pouze před místy, od kterých vlak může v další jízdě pokračovat po různých tratích (či různých kolejích ve stanici) s odlišnými parametry. Jinak je proměnnost informací o trati s časem, s výjimkou přechodných omezení traťové rychlosti, velmi malá, protože souvisí s konstrukcí tratě. I u informací pro přechodná omezení traťové rychlosti je nutné spíše než o častých změnách uvažovat o operativnosti jejich zavedení a rušení.

Poněkud zvláštní postavení mohou mít informace o dovolené traťové rychlosti a o jejím omezení, protože nemusí být vždy primárními informacemi. Tyto rychlosti mohou být za určitých okolností určeny až na základě podrobnějších informací o trati a vlastnostech vlaku (např. rozdílné stanovení rychlosti pro daný úsek trati pro klasický vlak a vlak s naklápěcími skříněmi, nebo u ČD zavedený obdélníkový a kruhový rychlostník). Obecně se vlakové parametry mající vliv na omezení rychlosti vztahují k složení vlaku - kvalitě podvozků, tlaku na nápravu, zavěšení skříně atd.

Informace o velikosti omezení rychlosti vlivem polohy výměn, tak jak ji známe z vjezdových a odjezdových návěstidel, je jen zjednodušenou náhražkou za úplnou informaci o povolení k jízdě a stavebních vlastnostech aktuálně zvolené dopravní cesty v místech možného větvení. Ve složitějších stanicích je počet takových možných cest dán nejen počtem dopravních kolejí, ale je ještě zvýšen o variantní cesty.

Řidčeji se mohou vyskytovat i jiné druhy proměnných informací - např. stupeň omezení rychlosti jízdy v určitém tunelu může být na vysokorychlostních tratích závislý nejen na typu soupravy, ale i na přítomnosti nebo nepřítomnosti dalšího vlaku ve vícekolejném tunelu, nebo dovolená rychlost jízdy vlaku na mostě může být podmíněna silou větru.

16.1.2 Dostupnost

Informace o vlastnostech vlaku a skutečné rychlosti vlaku jsou spojeny s vlakem a obvykle se získávají snáze na hnacím vozidle než na trati (ve stanici).

Informace o existenci překážky nebo aktuálně zvolené dopravní cestě jsou odvozeny z traťového nebo staničního zabezpečovacího zařízení a jsou tedy přístupné v příslušných bodech na trati, ve stanici či centrále zabezpečovacího zařízení tratě. U klasických zabezpečovacích zařízení je tato informace spojena s diskrétními body tratě (je dána polohou návěstidla nebo hranicí oddílu), u pohyblivého bloku nebo radiobloku se poloha této informace může spojitě měnit například na základě posledně centrále oznámené polohy konce předchozího vlaku téhož směru.

Ostatní informace, tj. údaje o stavu dopravních cest v místech větvení, dovolené traťové rychlosti, trvalých nebo přechodných omezení traťové rychlosti a spádech jsou pro určitou traťovou nebo staniční kolej (cestu) fixní a lze je tedy podle potřeby jako fixní informace umístit jak na trať, tak na hnací vozidlo. V předchozím odstavci jsme již zmínili skutečnost, že tyto informace musí být pro správné dešifrování kombinovány s informacemi o vlastnostech vlaku a proto oba soubory musí být dostupné současně ve stejném místě - buď na vlaku nebo na trati - má-li být jejich využití optimální.

16.1.3 Místo zpracování

Informace mohou být v zásadě zpracovány a dohledové funkce provedeny jak ve vlaku, tak na trati. Výsledné pokyny pro funkci brzdy musí být samozřejmě k disposici na vlaku. Budou-li tedy informace zpracovávány na vlaku, je třeba na vlak přenést informace o překážce nebo aktuálně zvolené dopravní cestě zabezpečeným přenosem ve směru trať - vlak. Budou-li informace zpracovávány na trati, je třeba na trati zajistit informace o vlastnostech vlaku a skutečné rychlosti vlaku a na vlaku zajistit výsledné pokyny pro funkci brzdy. Musí tedy v tomto případě být zřízen obousměrný přenos: vlak - trať i trať - vlak. Ostatní fixní informace není nezbytné přenášet, lze je prostě přímo umístit do místa zpracování na vhodném médiu.

Volbu té či oné varianty ovlivňují vlastnosti dostupných přenosových kanálů, vlastnosti traťového zařízení a některých dalších technických prostředků. Velmi úzké sepětí zabezpečovacího zařízení na trati a na vozidle vyniká u systémů s jízdou na elektrický dohled a u nově uvažovaných radiobloků. Tyto systémy se nemohou obejít bez informací z vlakové soupravy a tedy kanál vlak - trať je předpokladem již pro samotnou funkci traťového zařízení.

16.1.4 Místo přenosu

Důležitou otázkou je umístění informace ve vztahu k místu počátku platnosti. Aby bylo zajištěno, že v žádném případě nedojde k překročení rychlostního limitu pro bezpečný pohyb vlaku, je třeba přenos uskutečnit nejpozději v takové vzdálenosti, aby vlak s nejhoršími uvažovanými vlastnostmi ani za nejnepříznivější situace nepřekročil dovolenou rychlost. (V řadě případů se pro jednoduchost uvažuje zábrzdná vzdálenost.) Má-li být ale táž informace využita pro prvky automatizovaného řízení vozidla, je nutné ji mít s určitým předstihem, aby byl vždy dostatek času nejen na nouzové zabrzdění, ale i na plynulé přechody např. z vyšší rychlosti na rychlost nižší. Má-li táž informace sloužit pro optimalizaci jízdy vlaku (z hlediska času, spotřeby energie atp.) je informace tím užitečnější, čím je včasnější. I zde ale existuje limit, daný okamžikem pravidelné přípravy vlakové cesty, protože jinak by byla běžně přenášena omezující informace, která se následně změní na více povolující.

Důsledkem prodlužování vzdálenosti přenosu informace před počátkem platnosti je zvětšení počtu souběhů různých omezení rychlosti, které musí být pro každý vlak nejen současně propočítávány, aby se zjistil individuální limitní rychlostní profil, ale také současně přenášeny.

16.1.5 Druh přenosu

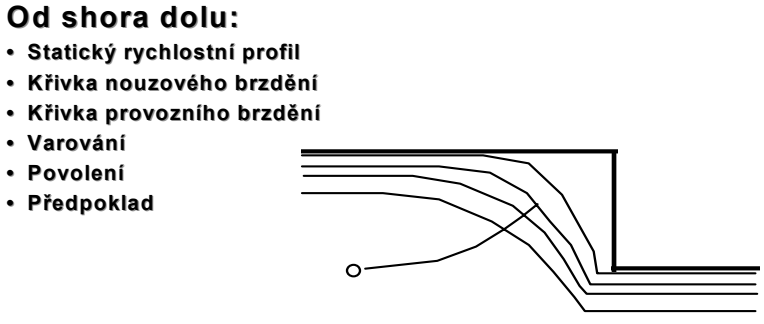
Specifické problémy přenosu zabezpečovací informace spočívají zejména v zajištění dat před falzifikací během přenosu a zajištění aktuálnosti (trvající platnosti) přenesených dat.

Informace mohou být přenášeny bodově (přerušovaně) pomocí lokálních majáků (balíz, krátkých smyček) nebo liniově (spojitě) pomocí kolejových obvodů, rádia nebo speciálně zřízených přenosových liniových kanálů (dlouhé smyčky). V zásadě je možná i kombinace různých přenosových prostředků. Přenos dále může být pouze jednosměrný z trati na vozidlo nebo může být obousměrný, přičemž je opět možné přenosové prostředky kombinovat. Kromě výše uvedených informací může být výhodné současně přenášet i některé pomocné informace pro řízení vozidla, optimalizaci jízdy atd.

Zásadní nevýhodou bodových (přerušovaných) přenosů zůstala, po doplnění informace o místu následujícího přenosu, nepružnost systému z hlediska aktualizace proměnných informací. Z tohoto důvodu je nutné přenášet dvě řady rychlostí: např. rychlost platnou u právě míjeného informačního bodu a rychlost očekávanou u následujícího informačního bodu. Specifický problém vznikne při zastavení vlaku před návěstidlem na „stůj“, ale i v zastávce, stanici nebo z technických důvodů. V prvém případě byl vlak informován o konci své cesty (u návěstidla) a po zastavení před ním, až do přejetí následného místa bodového přenosu, nedostane informaci o změně návěstidla na znak povolující jízdu. V druhém případě, po zastavení, je třeba vzít v úvahu, že by veškeré přenesené proměnné informace měly mít po uskutečněném přenosu přísně omezenou dobu platnosti (v podstatě na dobu, po kterou pozemní zabezpečovací zařízení může platnost garantovat). Při zastavení pak prakticky nezbývá, než dříve přijaté informace ze zařízení odstranit a zařízení pak bude opět minimálně do přejetí dalšího informačního bodu bez relevantních informací. Problém je technicky řešitelný přídavným přenosem (tzv. infill informace) prostřednictvím opakovaného bodového přenosu nebo přídavným liniovým přenosem (krátká, nebo střední smyčka, rádio atd.) před návěstidly. Současně je třeba také zvážit, které informace (a v jakém intervalu) je nutné aktualizovat z hlediska bezpečnosti, které informace (a v jakém rozsahu) je vhodné aktualizovat z hlediska operativnosti a které není nutné aktualizovat vůbec. Některé problémy lze omezit využitím prokluzových vzdáleností za návěstidly. Naopak předností bodových systémů je pevné a přesné přiřazení bodového zdroje k pevné infrastruktuře.

Liniové systémy jsou z principu schopné zajistit nepřetržitou aktualizaci přenášených informací bez přídavných instalací. Také volba vhodného místa přenosu nemá tak velký význam. Na druhé straně u liniových přenosů přesahujících délku prostorového oddílu je nutné dokonale řešit problém adresace jek zdroje, tak příjemce informace.

Kromě těchto specifických hledisek je třeba při výběru respektovat i všeobecně platná kritéria týkající se zajištění dostatečné kapacity přenosu, odolnosti proti rušení, vysoké spolehlivosti, mechanické odolnosti, minimalizace nároků na montáž traťové části, náročnosti na napájení, ceny atd.



Obr. 16-2

16.2 Zpracování informací

Na základě informací o trati a aktuální dopravní situaci lze pro určitou oblast stanovit tzv. křivku statického rychlostního profilu, kterou vlak nesmí překročit. V tomto rychlostním profilu se vyskytují skokové změny rychlosti (obr. 16-2). V místech skokové změny rychlosti z vyšší hodnoty na hodnotu nižší (z hlediska zabezpečovací techniky je zajímavý pouze tento přechod) je třeba vzít v úvahu brzdové vlastnosti vlaku, které reálně určují schopnost vlaku přejít z vyšší hladiny rychlosti na hladinu nižší. V závislosti na podrobnosti informací o této schopnosti vlaku (individuálně pro každý vlak, skupinově pro typ vlaků, jednotně pro vlak s nejhoršími přípustnými vlastnostmi) lze konstruovat křivku dynamického rychlostního profilu, která zahrnuje i přechodové fáze při poklesu dovolené rychlosti. Tato křivka by již reálněji určila, jakou rychlost nesmí vlak překročit. Vzhledem k nelineárnímu průběhu účinku brzd a obvyklé prodlevě mezi vydáním povelu a skutečným zahájením brzdění, je ale významnější křivka, která určuje místo, kde nejpozději musí být aplikována příslušná brzda, aby vlak dodržel předepsaný statický rychlostní profil, tzv. křivka intervence brzdy. Vzhledem k různým vlastnostem brzd se obecně konstruuje křivka nouzového brzdění a křivka provozního brzdění. Pod ní se dále konstruuje křivka, tzv. varovná křivka, která upozorňuje strojvedoucího, který skutečně vlak řídí, na okamžik, kdy je třeba zahájit brzdění, pokud se chce vyhnout intervenci zařízení do řízení vlaku. Teprve pod touto křivkou leží křivka nejvhodnější rychlosti jízdy vlaku s ohledem na známé informace, tzv. křivka povolení. Na obrázku je naznačena ještě tzv. předpovědní křivka, která predikuje jak se bude další jízda vyvíjet, pokud nastavení jízdních stupňů, brzdy atd. zůstane ve stávající poloze.

Z významu jednotlivých křivek je zřejmé, že postačí, když pouze křivka nouzového brzdění bude konstruována způsobem odpovídajícím požadavkům zabezpečovací technika. Z hlediska bezpečnosti jsou všechny ostatní křivky pouze pomocné. Na druhé straně by bylo nebezpečné, kdyby pro řízení vlaku byly poskytnuty tyto pomocné křivky vypočtené způsobem neodpovídajícím zabezpečovací technice, aniž by byla zřízena bezpečná křivka nouzového brzdění (a návazný dohled a zásah do jízdy vlaku), protože by v případě poruchy mohly působit na strojvedoucího zavádějícím způsobem.

Dále je zřejmé, že předpovědní křivka musí být počítána cyklicky v čase, zatímco ostatní křivky mohou být spočteny jen jednou a to po změně vstupních informací.

16.3 Dohled

Kontrolní funkci souladu přenášených informací s režimem jízdy lze realizovat v zásadě dvěma způsoby, i když konkrétní aplikace se od sebe budou v podrobnostech výrazně lišit:

- zařízením s kontrolou bdělosti, kde se z obsluhy tlačítka bdělosti vyvozuje, že strojvedoucí je schopný reagovat a tudíž také bude správně vykonávat všechny ostatní potřebné úkony na vozidle,
- zařízením s kontrolou rychlosti, kde se ze vstupních informací stanovený rychlostní limit nepřetržitě porovnává se skutečnou rychlostí vlaku.

Při aplikaci systému s kontrolou bdělosti jsou nároky na technické řešení nesporně nejmenší. Přenášené informace jsou zpravidla určeny pro strojvedoucího, který je porovnává s informacemi získanými z přímého sledování tratě a tak upřesňuje a doplňuje jejich význam. Může tedy i zpětně kontrolovat správnou funkci vlakového zabezpečovače. Krátkodobá přerušení přenosového kanálu nebo krátkodobé poruchy v přenosovém kanálu (vznikající např. vlivem elektrické trakce) nejsou na závadu, jsou eliminovány zkušeností strojvedoucího, takže nedochází k rušivým zásahům do řízení vozidla. Zařízení nevyžadují velký rozsah přenášených informací. Rozhodující pro přijatelnost takového systému je zda se podaří zajistit, že strojvedoucí skutečně bude obsluhovat tlačítko bdělosti předpokládaným způsobem. Relativně chudší (a tedy podstatně levnější) technické vybavení musí být doplněno promyšlenou soustavou netechnických opatření, zabraňujících vzniku stereotypu při obsluze tlačítka bdělosti a zajišťujících vysokou zodpovědnost strojvedoucích (výběr, školení a kontrola).

Systém s úplnou kontrolou rychlosti vyžaduje rozšíření technického vybavení o zařízení pro měření rychlosti a ujeté dráhy a pro generaci bezpečnostní křivky. Závažnější je pak skutečnost, že nemá-li systém pracovat s nadbytečnými rezervami, musí pracovat s daleko větším obsahem informací, na kvalitativně vyšší

úrovni. Logický požadavek na zpracování nejen informací časově proměnných (odvozených od hlavních návěstidel), ale i informací o omezeních rychlostí z důvodů stavebních a požadavek na respektování specifických vlastností každého vlaku, vede k podstatnému zvýšení složitosti celého systému. U moderních vlakových zabezpečovacích systémů. může být diskutabilní pouze úroveň a kvalita kontroly rychlosti; zařízení s kontrolou bdělosti se již neuvažují. Základem konstrukce je pak mikroprocesorový nebo přesněji multiprocesorový systém.

16.4 Zásahy do jízdy vlaku

Výstupem dohledu je pokyn k zásahu do jízdy vlaku. Zásahy jsou možné obecně ve třech úrovních:

- optické a akustické varování strojvedoucího, že skutečná rychlost vlaku se blíží limitní dovolené rychlosti,
- zavedení (provozního) brzdění při dalším přiblížení skutečné rychlosti vlaku k limitní dovolené rychlosti; brzdění lze po snížení rychlosti pod požadovanou hodnotu na žádost strojvedoucího přerušit,
- zavedení (nouzového) brzdění při překročení limitní dovolené rychlosti způsobem, který vede k co nejrychlejšímu snížení rychlosti vlaku pod dovolenou mez (a obvykle i k zastavení vlaku).

Je patrné, že druhou úroveň může zajišťovat strojvedoucí sám nebo nějaké jiné zařízení, určené pro úpravu rychlosti vlaku a tedy tato úroveň nemusí být součástí VZ a nemusí na ni být uplatňovány zabezpečovací požadavky. Vlakové zařízení by však v takovém případě mělo alespoň poskytnout příslušné informace pro strojvedoucího. Uvážit je třeba i nutnost stejného měření rychlosti, dráhy atd. jak pro zařízení VZ, tak pro strojvedoucího, aby nedocházelo k nesouladu.

Rozhodující úroveň, zdánlivě jednoduchá úroveň třetí, bohužel není bez problémů. Podrobnosti budou uvedeny v navazující publikaci Vlakové zabezpečovací systémy.

16.5 Činnost zařízení při mimořádných stavech

Všechny vlakové zabezpečovací systémy se mohou dostat do situace, kdy informace, které mají k disposici, další jízdu vlaku nedovolují, ale informace strojvedoucího (fónické předání rozkazu, písemný rozkaz atd.) další jízdu umožňují. Obecně je možné, aby některé nebo všechny kontrolní funkce zařízení byly přenosem zvláštní informace a/nebo zásahem strojvedoucího dočasně vyloučeny a zařízení se samo uvádělo do plné činnosti po obnovení informací. Výluka kterékoliv činnosti zařízení sebou ovšem nese nebezpečí, že strojvedoucí na výluku zařízení pozapomene (automatické obnovení plné činnosti po mimořádných případech nelze obvykle zajistit samotným zařízením bezpečně). Prakticky použitelná je proto pouze výluka zařízení doprovázená výrazným omezením jízdy (co do rychlosti a/nebo délky) a případná obsluha tlačítka bdělosti po dobu chybějících informací. Tato omezení budou provozně nepřijatelná, pokud četnost mimořádných případů bude příliš vysoká. Je vždy důležité provést všechna možná opatření, která umožní zachovat funkci zařízení alespoň v degradované podobě.

17 KOMPLEXNÍ ZABEZPEČOVACÍ SYSTÉMY

17.1 Centralizace řízení a zabezpečení

V předešlém již byly zmíněny přídavné úlohy, které zabezpečovací technika může pomáhat řešit v oblasti řízení vlakové dopravy. Teoreticky by pro řízení dopravy měl vystačit seriózně zpracovaný grafikon vlakové dopravy (GVD), na jehož základě by jednotlivé stanice včas připravovaly potřebné jízdní cesty. K tomu účelu lze ovšem GVD využít pouze v případě, že se vlaky skutečně podle něj pohybují. Objeví-li se odchylky, je nutné na ně reagovat včas a správně.

Při tvorbě centralizovaných řídících a zabezpečovacích systémů je nutné respektovat základní odlišnosti, plynoucí z funkčních požadavků na zařízení pro hlavní a vedlejší tratě :

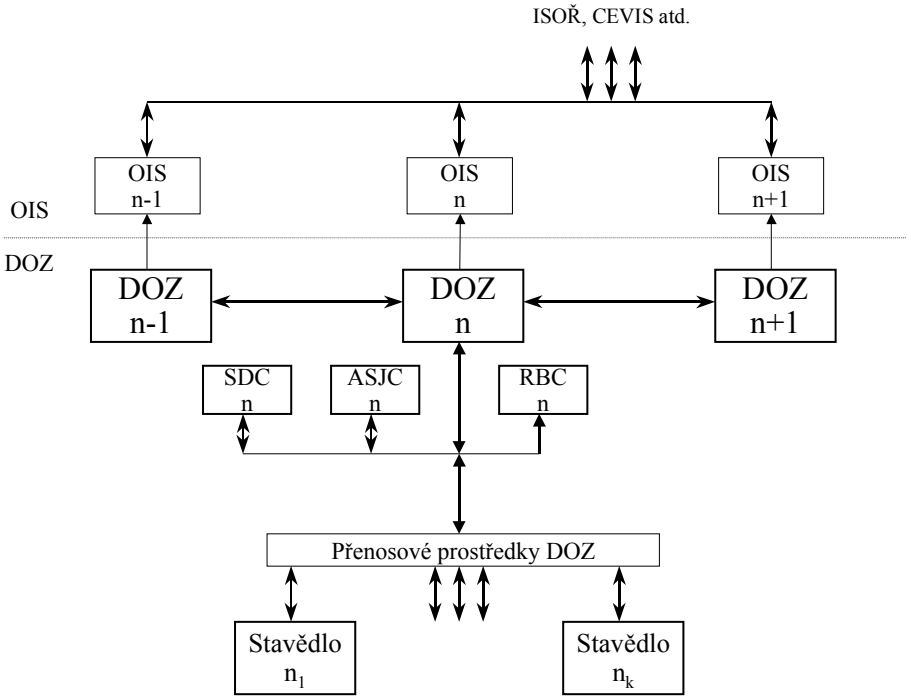
- na hlavních tratích je prvotním důvodem pro zavedení takového systému nemožnost racionálně řídit dopravu z jednotlivých stavědel v dopravnách, vzhledem k tomu, že v jednotlivých dopravnách nejsou dostupné přímé informace o dopravním procesu ve vzdálenější lokalitách tratě (ramene) a zprostředkované informace pro nedostatečnou přesnost neumožňují správné rozhodování. Situace se výrazně zhoršuje se stoupající rychlostí vlaků, zvyšující se intenzitou provozu a smíšeným provozem vlaků různých tříd rychlosti. Až druhotným důvodem je na těchto tratích snaha o úsporu trvale aktivních dopravních zaměstnanců, která nesmí být v rozporu s požadovanou vysokou operabilitou za všech (tedy i poruchových) stavů zařízení,
- na vedlejších tratích s nižší intenzitou provozu je evidentní nevyužití kapacity dopravních zaměstnanců ve stanicích i při sdružování funkcí a tedy úspora zaměstnanců je důvodem primárním, přičemž požadavek na operabilitu za poruchových stavů (zejména vzhledem k rezervám v propustné výkonnosti tratě) není tak kategorický.

Ovšem neexistence dopravních zaměstnanců ve stanicích bude mít zásadní dopad pro dopravní řešení situací při poruchách zařízení. To je třeba vzít v úvahu při návrhu jak technických zařízení, tak dobře promyšlených organizačních opatření.

17.1.1 Dálkové ovládání pro hlavní tratě

Pro kvalitnější řízení provozu je tedy nutné zřídit pracoviště, které poskytuje dostatek kvalitních informací z přiměřeně velké oblasti a dovoluje provoz ovládat kvalifikovaně. Takové zařízení se obvykle označuje jako dálkové ovládání zabezpečovacích zařízení (DOZ). Dochází tak k vytvoření centrálního obslužného pracoviště několika do té doby samostatných staničních, traťových a přejezdových zařízení. Logika, vytvářející bezpečné závislosti zabezpečovacích zařízení zůstává místní, avšak její ovládání je pro ucelenou oblast soustředěno do jediného místa, disponujícího vymezenými nebo úplnými možnostmi obsluhy podřízené oblasti. Úroveň bezpečnosti zpracování dat na centrálním ovládacím pracovišti a bezpečnosti přenosu dat mezi ovládacím pracovištěm a podřízenými subsystémy je závislá na požadovaných možnostech obsluhy. V nejjednodušším případě je možno centrální obslužné pracoviště a související komunikaci považovat za vyšší stupeň automatizace řízení bez zvláštních požadavků na bezpečnost, neboť záruku bezpečnosti nesou jednotlivé řízené subsystémy ve stanicích. Pokud je ovšem vyžadována možnost ovládat subsystémy i při nouzových situacích, kdy je nutno ignorovat částečně či úplně bezpečné závislosti, realizované těmito subsystémy, pak musí být tomu odpovídající aktivity realizovány striktně bezpečným způsobem. Základní struktura takto pojatého systému dálkového ovládání je na obr. 17-1. Z obr. 17-2 je podrobněji patrno celkové uspořádání jednotlivých komponent řídícího a zabezpečovacího systému (stavědla, DOZ, IRI, RBC, GSM-R), včetně dodatečně budovaného vlakového zabezpečovacího zařízení ETCS druhé úrovně. RBC je zde radiová centrála, sloužící v systému ETCS pro předávání informací za stavědel na vozidlo a IRI je interface mezi stavědly a RBC. Tato architektura by potom měla být realizována na všech tratích národních koridorů, kde již byla modernizována klasická stavědla a autobloky.

Určitou alternativou k předešlému pojetí je pouhé zřízení informačního systému, který soustředí informace o průběhu dopravního procesu z jednotlivých stavědel celého ramene a poskytne je obsluze jednotlivých stavědel. Tím se odstraní v úvodu zmiňovaný nedostatek informací ve stanicích a řízení provozu je možné ponechat na výpravčích. Možná je i varianta, kdy do tohoto informačního systému je zapojen také dispečer. Dispečer pak vlastní zabezpečovací zařízení neobsluhuje, ale pouze v určitém rozsahu, vhodným způsobem, prostřednictvím informačního systému, poveluje místní obsluhu. Takovým řešením se dosáhne toho, že informační systém může být pojat jako jakékoliv jiné automatizační zařízení a nemusí být konstruován s uplatněním zabezpečovacích principů. Proto i náklady na jeho zřízení mohou být podstatně nižší. Obecně je ale toto řešení méně pružné, méně pohotové, neumožňuje úsporu pracovníků ani v mezilehlých stanicích a nebere ohled na RBC vlakového zabezpečovacího zařízení ETCS druhé úrovně.

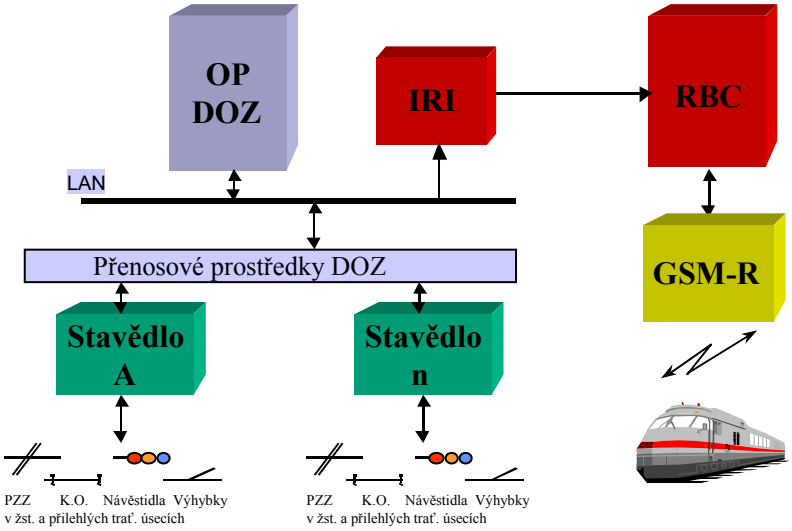


Obr. 17-1

Z obrázku 17-1 je patrné propojení sousedních oblastí DOZ a připojení jednotlivých prvků v oblasti: terminálu pro údržbu (SDC), prostředku pro automatické stavění jízdních cest (ASJC), RBC. Veškerá tato zařízení musí být koncipována tak, aby nenarušila integritu systému DOZ a stavědel v úrovni SIL4. Jednosměrně je systém DOZ spojen s případnými oblastními informačními systémy pro dispečera (OIS), které již přímo nesouvisí s ovládáním zabezpečovacích zařízení, ale mohou s výhodou využívat informace o skutečné dopravní situaci. Obousměrné propojení by bylo možné pouze za předpokladu, že budou existovat technické prostředky vylučující napadení systému DOZ (který je při dnes používané technologii u ČD koncipován jako uzavřený přenosový systém) z vnějšku.

Základní funkcí dálkového ovládání je přenos a zobrazení informací z jednotlivých stavědel (nutných k řízení provozu v dané oblasti) na ovládací pracoviště DOZ a přenos povelů zadaných na ovládacím pracovišti DOZ do jednotlivých stavědel. V omezeném nebo plném rozsahu lze tak prostřednictvím dálkového ovládání vykonávat funkci obslužných pracovišť všech stavědel v dané oblasti. Systém DOZ musí být schopen dálkově ovládat všechny typy stavědel v daném úseku a to včetně příslušných traťových a přejezdových zařízení. Pokud se při výstavbě zařízení postupuje koncepčně, je výhodné již při instalaci zařízení v jednotlivých stanicích neoddělovat jednotlivé subsystémy pro zabezpečení stanic, tratí a přejezdů, ale budovat zabezpečovací systémy komplexní - např. integrovat logiku traťového a přejezdového zařízení do zařízení staničního, nevytvářet úplné místní obslužné pracoviště ve stanici, atp.

Zobrazování a ovládání na ovládacím pracovišti DOZ by v zásadě mělo být shodné se zobrazováním a ovládáním na ovládacích pracovištích jednotlivých stavědel. To je u ČD dáno ZTP pro Jednotné ovládací pracoviště (JOP). Rozdílný stupeň vybavení stavědel nesmí mít na základní způsob obsluhy žádný vliv; přípustné je pouze omezení možností obsluhy v souvislosti s technickou úrovní a možnostmi ovládaného zařízení.



Obr. 17-2

Hlavní funkční otázky, kterými je nutné se při návrhu dálkového ovládání dále podrobněji zabývat, pak jsou:

- potřeba a způsob uplatnění nouzových obsluh ze zařízení DOZ na různých kategoriích tratí,
- rozsah oblasti, jíž je schopen jeden dispečer obsloužit (počet současně jedoucích vlaků, počet přestavitelných prvků, rozsah dopravní práce s vlaky atd.) a proměnnost obsluhovatelné oblasti v závislosti na různých denních obdobích (např. denní směna - noční směna),
- možnost dělby ovládání stavědla na dálkovou (průjezdy) a místní (posuny) část.

Pod pojmem nouzové obsluhy se zde rozumí veškeré obsluhy, které jsou bezpečnostně relevantní a přitom není možná jejich kontrola (buď momentálně nebo trvale, částečně nebo úplně) technickými prostředky zabezpečovacího zařízení. Pokud obsluha k takovému kroku přistoupí, musí mít k jejich provedení jiné spolehlivé informace (např. administrativně zjištěné), že tato obsluha není v rozporu s bezpečností. Povely takového charakteru (podle JOP jak nouzové, tak potvrzovací) a jim předcházející informace (bezpečné) je nutné v počítači zadávacího pracoviště DOZ technicky a procedurálně ošetřit na stejné úrovni jako u zadávacího pracoviště stavědla. Obecně je nutné potřebu nouzových obsluh dobře uvážit, protože významným způsobem zvyšuje náročnost technického řešení systému DOZ a projeví se tedy i v ceně zařízení (existují významné dráhy, které nouzové obsluhy ani na místní úrovni vůbec nezřizují a problémy řeší jen dobře propracovanými organizačními opatřeními).

S přihlédnutím k DOZ je možné zavedené nouzové povely u ČD podle JOP rozdělit do tří skupin :

- nouzové povely, které může/musí provádět dispečer stejně jako výpravčí (NUZ>, NOT>, OBSL>, jízdní cesty s potvrzením, rušení výluk atd.),
- nouzové povely vyžadující spolupráci se strojvedoucím - chybí pouze informace o volnosti některého úseku nebo některých úseků cesty, přičemž dispečer nemá informaci, že by se v daném úseku měl nacházet vlak nebo vozidlo (stejně jako obvykle výpravčí při místní obsluze). Zde je oprávněné okamžité použití přivolávací návěsti dispečerem (jízda je pak, pod zodpovědností strojvedoucího,

provedena způsobem, zajišťujícím zastavení před případnou překážkou), ale dohovor dispečera se strojvedoucím pomocí rádia je účelnější - lze lépe definovat strojvedoucímu problém, pro který není možná řádná jízdní cesta,

- nouzové povely vyžadující účast informovaného pracovníka na místě (všechny ostatní případy) - jsou podmíněny informací, kterou lze získat pouze na místě (např. od místního pracovníka nebo strojvedoucího), popř. je nutné na místě provést nějaké opatření (např. zajištění výměny ambulantním zámkem). Na základě této informace (a tedy nutné komunikace místního pracovníka nebo strojvedoucího s dispečerem) může pak dispečer jízdu povolit operativněji než místní pracovník z místního ovládacího pracoviště (např. místní pracovník dává ambulantní zámek na zhlaví na výhybku, ale musí jít zpět do dopravy než může vydat povel vlaku pomocí PN).

Již z tohoto hrubého přehledu existence první skupiny nouzových povelů napovídá, že pro koridorové i další hlavní tratě bude (při respektování dnešních provozních zvyklostí) vhodné, aby zařízení DOZ bylo nadáno schopností vydávat nouzové povely. Existence třetí skupiny ovšem napovídá, že současně bude nutné ve stanicích na hlavních tratích držet personál, schopný určitých dopravních úkonů pod vedením dispečera. Současně, při nezbytném mobilním rádiovém spojení (včetně přenosných osobních přístrojů), lze zpochybnit účelnost dnešního provozování přivolávacích návěstí - kromě jiného má přivolávací návěst jiný význam v druhém a třetím případě předchozího odstavce. Při nasazení ETCS se předpokládá, že datovým kanálem bude možné vydat z RBC povel "Jízda podle rozhledu" s kontrolou dodržení výrazně omezené rychlosti (např. 30 km/h). Záleží ovšem na schopnosti použitého stavědla a stanovených pravidlech pro tento povel.

Se zavedením dálkového ovládání je nutné rozhodnout a předpisově ošetřit kdo a jakým způsobem (pro různé kategorie tratí a konkrétní podmínky) bude jednotlivé činnosti při nouzových obsluhách provádět. Současně musí být zaveden systém školení, ale zejména cyklického obnovování praktických znalostí této nouzové obsluhy. Evidentní je tedy nutnost zavedení jakési, pravděpodobně sdružené, funkce pomocného (pohotovostního) výpravčího, který bude trvale, nebo jen v období silného provozu a plánovaných výluk zařízení, přítomen v jednotlivých žst. hlavních tratí.

Oblast dálkového ovládání by měla zahrnovat souvislou část tratě, ne menší než ta, kterou je v dopravním sedle schopen běžně ovládat jediný dispečer. Dispečerské pracoviště pak bude vybaveno více zadávacími pracovišti (ovládacími pracovišti dispečera v téže místnosti), která budou obsazena dalšími dispečery v době vyššího provozu až do počtu nutného pro řízení v době provozní špičky. Tato jednotlivá pracoviště jsou rovnocenná a z každého lze ovládat celou oblast v rozsahu daném JOP a dělba dopravní práce jednotlivých dispečerů v oblasti závisí pouze na administrativním uspořádání, tedy dohodě. Činnost každého dispečera je zaznamenávána zvlášť. Jak patrno, takové uspořádání je z hlediska obsluhy maximálně flexibilní a nepřináší uvnitř oblasti žádné problémy. Omezení rozsahu oblasti shora je dáno technickými možnostmi systému DOZ, popř. dalších návazných zařízení. Oblasti DOZ a RBC by měly mít stejné hranice.

Pracoviště dálkového ovládání vybavené podle předchozího odstavce umožňuje jakoukoliv dělbu práce mezi jednotlivými dispečery téhož DOZ. Je tedy také možné, aby se např. jeden (či více) dispečer věnoval "dálkovému" provozu a jiný(í) místní práci v jedné či více stanicích. Přitom je možná vzájemná zastupitelnost, změna oblasti podle momentálních potřeb dopravní práce atd. To vše je závislé pouze na organizačních pravidlech, které rozdělují práci mezi jednotlivé dispečery na tomtéž pracovišti. Pokud se místní a dálková práce vzájemně ovlivňují (např. přesun posunu přes průjezdné koleje) je k tomu k disposici dostatek informací a možnost přímé komunikace mezi dispečery na pracovišti.

Kromě tohoto způsobu ovládání je dostupné z DOZ trvalé nebo dočasné předání celé stanice nebo pomocného stavědla ve stanici na místní obsluhu. Rozsah pomocného stavědla je ovšem dán pevně již projektem stavědla.

Žádné stávající stavědlo u ČD neumožňuje současné ovládání z úrovně dálkové a úrovně místní. Požadavek na takový způsob ovládání vyvolává jak technické, tak provozní komplikace a v současné době vhodné řešení neexistuje. Pro zvláštní případy (situace, kdy jedno stavědlo pokrývá dvě do značné míry separátní a separátně řiditelná kolejiště) je možné uvažovat o elektronických pomocných stavědlech, která by takové rozdělení obsluhy umožňovala (pevně podle projektu) a kdy cesty z jedné oblasti do druhé by byly řešeny složením dílčích cest, z nichž žádná nepřesahuje vlastní oblast.

Velkoplošné přehledové obrazovky nejsou pro samotného dispečera (tj. člověka ovládajícího DOZ) nezbytné. Jiná je situace, kdy stejný prostor s dispečerem sdílí i jiní pracovníci (např. dispečer sousedního DOZ, provozní dispečer, operátorka atd.), kteří informace z DOZ pro svou práci potřebují, ale nejsou oprávněni k přímému řízení DOZ. Pak velkoplošné zobrazení slouží více méně jako náhrada bezobslužných pracovišť BOP, známých ze systému ESA 11. Také v případě, že se na obsluze podílí více dispečerů, může být velkoplošné přehledové zobrazení pro jejich práci užitečné. K jednoznačnému rozhodnutí o přehledových velkoplošných zobrazení (účelnosti jejich použití, tvaru zobrazení, jeho podrobnosti) chybí dnes u ČD provozní zkušenosti. V zahraničí se sice často používají, nejsou ale pravidlem. Je také třeba si uvědomit jejich zatím mimořádnou nákladnost a to jak investiční, tak provozní.

Možnost ovládat zařízení DOZ z přehledové obrazovky je omezena v případě více ovládacích pracovišť, kdy by bylo nutné předem pevně vymezit, které pracoviště do které oblasti má přístup (vždy jen jedno), což je v rozporu se shora požadovanou pružností systému.

Kromě stavění vlakových a posunových cest a individuálního ovládání jejich jednotlivých prvků v intencích JOP, je třeba rozhodnout, co z dalších vymožeností je nezbytnou součástí DOZ, co je volitelnou součástí a co do DOZ již nepatří. Jde o následující celky:

1. veškeré informace kontrolních prvků zabezpečovacích zařízení, umístěných ve stanicích a při místním ovládání kontrolovaných obsluhou, musí být přeneseny na pracoviště dálkového ovládání (týká se zejména kontrol přejezdů nezapojených do místního ovládacího pracoviště stavědla) - tento požadavek bude automaticky splněn, pokud jsou tyto prvky soustředěny na místním ovládacím pracovišti a na dálkové ovládací pracoviště bude přenesen úplný soubor informací stavědla,
2. vedení dopravní dokumentace,
3. splněný grafikon,
4. automatické stavění vlakových cest (z plánovaného nebo aktualizovaného GVD),
5. ovládání jiných než zabezpečovacích zařízení (trakce, osvětlení, ohřev výměn atd.),
6. návaznost na další informační systémy:
   - jednosměrné poskytování zabezpečených informací ze systému ven,
   - jednosměrné poskytování nezabezpečených informací ze systému ven,
   - obousměrná výměna informací s nadřazeným řídícím systémem (není možné u žádného dnešního stavědla ČD),
   - obousměrná výměna informací s cizími systémy (není možné u žádného dnešního stavědla ČD).

Ve všech těchto případech jde vlastně o dělbu požadavků mezi DOZ, OIS a diagnostiku.

Za logické lze považovat, aby body 1,4 a 5 plnilo zařízení DOZ. Přitom:

- ad 1 - preferuje se provedení, kdy informace této povahy budou zásadně zavedena do stavědla a odtud dopravena na ovládací pracoviště DOZ stejně jako ostatní bezpečnostně relevantní informace stavědel,
- ad 4 - tento systém bude připojen do sítě DOZ do stejného místa jako zadávací počítač DOZ, přičemž nesmí narušit uzavřenost sítě a splnění dalších požadavků pro přenos bezpečných informací. Může být součástí zadávacího pracoviště DOZ nebo specializovaným zařízením připojeným k síti DOZ. Nepředpokládá se, že by byl zdrojem nouzových povelů. V prvém případě zařízení nemůže přímo spolupracovat s jiným informačním systémem a tedy jeho funkce by byla omezena pouze na generování vlakových cest podle GVD. Ve druhém případě lze (při jeho plně zabezpečovací redundantní konstrukci) uvažovat o možnosti jeho propojení s OIS, odkud by mohl získávat aktualizovaný GVD,
- ad 5 - tyto informace a povely stavědla již obsahují (viz JOP) a lze je bez problému posunout i na úroveň DOZ.

Právě tak je zřejmé, že body 2, 3 a 6 je schopen plnit systém OIS, protože neobsahují bezpečnostně relevantní řešení.

Systém DOZ musí být podporován dvěma dalšími prostředky:

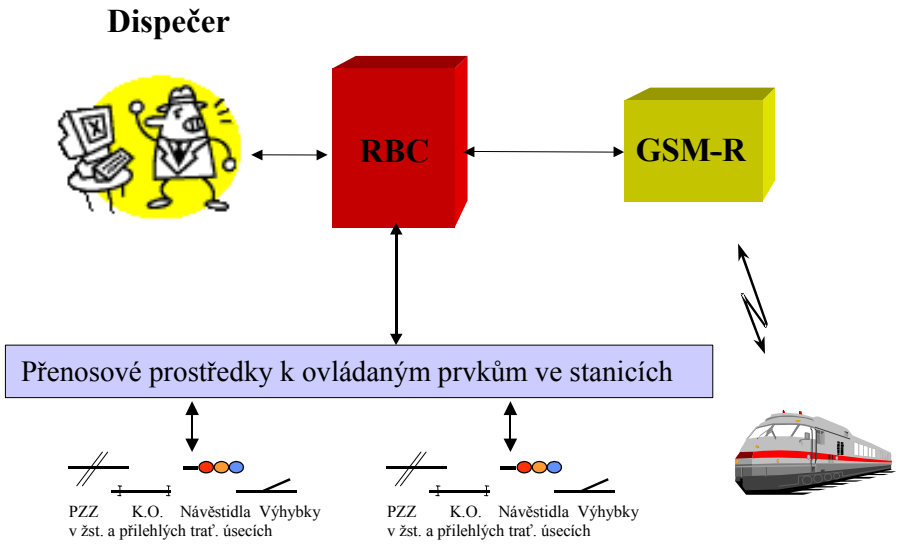
- kvalitním sdělovacím zařízením, které musí v každém případě obsahovat:
  - digitální traťové rádio s datovým kanálem pro ETCS a další uvažované datové přenosy. Tento radiový systém musí zajistit fónickou komunikaci dispečera se všemi vlaky v oblasti a pracovními skupinami pohybujícími se na infrastruktuře oblasti (posuny, pohotovostní výpravčí, údržba atd.),

- dispečerský telefonní okruh pro spojení dispečera se všemi stanicemi a případnými telefony u vjezdových návěstidel. Systém musí umožňovat jak selektivní, tak skupinovou volbu,
- spojení dispečera s obsluhou sousedních stanic oblasti DOZ (včetně odbočných tratí),
- vstupy do staničních rozhlasů a informačních zařízení. I když se předpokládá, že pravidelné vstupy budou předmětem navazujících informačních systémů, musí mít dispečer možnost vstupu pro akutní případy,
- jak traťové rádio, tak dispečerský telefonní okruh musí být doplněny záznamovým zařízením hovorů,

- soustředěnou diagnostiku zabezpečovacích zařízení z celé oblasti DOZ, která musí dále umožnit také centrální stažení archivů z jednotlivých stavědel a trvalé monitorování zabezpečovacích zařízení pro statistické a další účely.

17.2 Radiobloky

Jako radioblok se označují souhrnné řídící a zabezpečovací systémy, které (na rozdíl od pouhého dálkového ovládání) dokonaleji integrují staniční, traťová, přejezdová a vlaková zabezpečovací zařízení a z jejich těsnější spolupráce těží. Výsledkem by pak mělo být zařízení ve svém celku pružnější i lacinější, umožňující v porovnání s klasickými systémy lepší využití všech informací v systému obsažených. Typický příklad takového zařízení je na obr. 17-3.



Obr. 17-3

Jak patrno, podstatná část logiky systému, u klasických zařízení soustředěna ve stavědlech, je přesunuta do radioblokové ústředny (Radio Block Centre – RBC), která ovládá prvky v kolejišti a prostřednictvím radiového spojení komunikuje obousměrně s vlaky (posunujícími díly)[2]. Radiobloková ústředna je pak zodpovědná jak za korektní vyhrazování jízdní cesty (po vhodných úsecích) pro vlaky i posun (včetně zajištění protisměrných a následných jízd), tak za vybavování již projeté vlakové či posunové cesty (a to na základě informací vlaků o jejich poloze) a popřípadě i za návrat zařízení do základní polohy po ukončení jízdy vlaku.

Tyto základní funkce může radiobloková ústředna provádět sama (v případě, že všechny vlaky jsou příslušně vybaveny, včetně zařízení pro sledování celistvosti vlaku) nebo za větší či menší spolupráce s dalšími podsystémy a s úrovní odpovídající potřebám provozu. Radioblokové systémy jsou tak zaměřené

[2] Nezaměňovat s RBC u ETCS, úroveň 2, kde RBC pouze zprostředkovává přenos informací ze stavědla na hnací vozidlo.

buď na řídký provoz na vedlejších tratích, kde jejich hlavní úlohou je s co nejnižšími investičními a provozními náklady řídit a zabezpečovat jízdu vlaků, nebo jsou naopak orientovány na extrémně zatížené tratě, kde jejich hlavním účelem je ekonomicky přístupnými prostředky zajistit vysokou propustnost infrastruktury.

V případě nové výstavby je nasnadě, že mohou odpadnout nebo se alespoň významně redukovat podstatné části klasických zabezpečovacích zařízení. Z klasických stavědel v jednotlivých stanicích zůstanou pouze výkonné prostředky k ovládaným prvkům v kolejišti, které budou nadány pouze lokální inteligencí, nutnou pro řízení příslušného prvku a informace o jeho stavu budou postupovat RBC. Prostředky pro zjišťování volnosti kolejí budou v podstatné míře nahrazeny informacemi o poloze vlaků, které RBC získá prostřednictvím rádia z hnacích vozidel a vlaky budou touž cestou povelovány z RBC, bez nutnosti použít návěstidel. Traťové zařízení bude nadbytečné, protože RBC bude mít dostatek informací pro řízení sledu vlaků a výluk jízdních cest. Samozřejmým předpokladem pro aplikaci radiobloku je inteligentní vlakové zabezpečovací zařízení na vozidle, v jednoduchých případech (např. pro provoz na vedlejších tratích) postačí pouhý terminál, schopný spolupracovat s brzdovým systémem vlaku. Dále je evidentní, že předpokladem pro to, aby se mohl zredukovat nákladný klasický systém detekce vlaku (kolejové obvody, počítače náprav), musí být na vozidle k disposici informace o celistvosti (integritě) vlaku. Typickým příkladem takových zařízení je úroveň 3 v systému ETCS, ale lze vytvořit celou škálu různě modifikovaných zařízení mezi úrovní 2 a úrovní 3 zmíněného systému ETCS, která vyhoví skutečným potřebám provozu u jednotlivých drah.

Právě tak budou existovat systémy radiobloku využívající již vybudované části klasické sdělovací a zabezpečovací infrastruktury. Jak patrno, pro existující systém dálkového ovládání klasických staničních zabezpečovacích zařízení (DOZ) a rádio GSM-R postačí pouze zajistit nově vstupy do RBC a jeho výstup do rádiové sítě a RBC pak může zastávat funkci prostředníka mezi již vybudovaným zařízením a vlaky (viz předchozí kapitola), přičemž optický kanál přenosu informací - návěstidla - se stává nadbytečným a bude sloužit (v redukované míře) jen jako záložní systém pro případ poruchy nebo pro jízdu vlaků nevybavených inteligentním mobilním vlakovým zařízením. Přísně takto orientované zařízení nelze označit jako radioblokové zařízení podle shora uvedené definice – jde stále jen o klasické zařízení, doplněné vlakovým zabezpečovačem ETCS v úrovni 2 a tak právem patří do předchozí kapitoly o dálkovém ovládání. Ale při určitých modifikacích - „polepšení“ úrovně 2 systému ETCS, zařízení může být schopno poskytovat i služby, které jdou daleko za rámec možností původního systému, bez podstatných zásahů do již existujícího klasického zařízení (např. zkrácení následného mezidobí prostřednictvím zavedení pohyblivého bloku v RBC, nebo zavedení obousměrné komunikace mezi stavědly a RBC pro využití informací o poloze vlaků z ETCS).

17.3 Zařízení pro méně zatížené tratě

Problematika zachování provozu na vedlejších tratích je obvykle zužována na problém snížení provozních nákladů. Úspory jsou pak přednostně hledány v úspoře pracovní síly, kterou zde představují zejména dopravní zaměstnanci (vzhledem k malému provozu ne vždy plně vytížení), ale také pracovníci údržby technických zařízení. Úspora v jedné skupině a stejný nárůst v druhé skupině problém neřeší. Zásadní chybou by ovšem bylo snižování provozních nákladů na úkor bezpečnosti dopravy. V podmínkách ČD, kde vedlejší tratě jsou mimořádně zanedbané, je naopak třeba hledat taková řešení, která současně podstatně přiblíží bezpečnost provozu standardním podmínkám.

Paralelně s tím se objevují úvahy, které naznačují, že v některých případech by bylo výhodné, aby železniční a tramvajová doprava sdílela některé části infrastruktury. Bohužel oba systémy nejsou zatím příliš kompatibilní - problémy jsou v oblasti kolo-kolejnice, trakčního napájení, sběrače, výšky nástupiště atd., ale také v nestejné úrovni pasivní bezpečnosti (např. nestejná podélná pevnost vozidel). Většinu problémů musí řešit odborníci z oblasti kolejových vozidel, ale problém s nižšími parametry pasivní bezpečnosti tramvaje může vyřešit vhodný řídící a zabezpečovací systém, který bezpečně zajistí, že minimálně při běžném provozu (s cestujícími) k žádnému střetu vozidel nedojde.

Již v minulosti bylo ve VÚŽ navrženo zjednodušené zabezpečovací zařízení pro vedlejší tratě, z kterého byl později odvozen i systém pro tramvaje na samostatném tělese. Oba systémy byly založeny na principu vlakového hradla (trať bez návěstidel), kdy přenosový kanál mezi tratí a vlakem byl tvořen

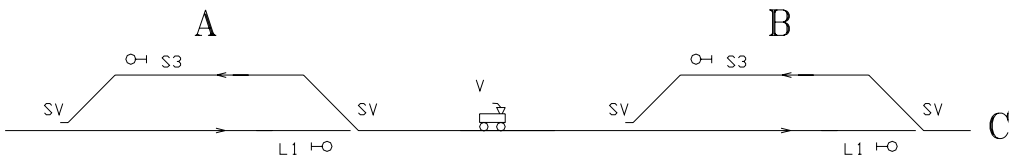
neohraničenými kolejovými obvody. V prvním případě byla jako přijímač přenášených informací použita mobilní část VZ-ČD (což zajišťovalo funkčnost systému i na hlavních tratích), v druhém případě bylo použito jednoduššího, plně elektronického speciálního přijímače. Obě zařízení (první v úseku Bohuňovice - Šternberk z první poloviny 60. let, druhé Most - Litvínov z přelomu 60. a 70. let) byla plně v provozu s velmi dobrým výsledkem ověřena, byly získány cenné zkušenosti s provozem systémů bez vnějších návěstidel, vyřešeny problémy s kompatibilitou, jízdou nevybavených vozidel, jízdou při poruše traťové části atd. K rozšíření pro malý zájem provozovatele však nedošlo. Při současném stavu technologie by již nebylo účelné tato řešení oživovat, lze však využít tehdy získaných provozních zkušeností.

Od roku 1999 probíhá v rámci UIC, také za aktivní účasti VÚŽ, projekt ETCS-LC, zaměřený na zabezpečení vedlejších tratí. Přívlastek LC (Low-Cost) značí snahu o dosažení vyšší efektivnosti celého systému ETCS, zejména s ohledem na vedlejší tratě. Úspory by měly být dosaženy především omezováním zařízení na trati, dále pak použitím standardní, hromadně vyráběné technologie, zjednodušením dopravy, případně úlevou z kvantitativních parametrů zařízení (spolehlivost, dostupnost). Podobné snahy se objevují také v dalších projektech dodavatelů zabezpečovacích zařízení (např. Lokoprol v 5. rámcovém programu), popř. v návrzích na využití nových prvků k těmto účelům (Galileo, ...).

V dalším je uveden systematický pohled na zabezpečovací zařízení, která mohou oba shora uvedené problémy vyřešit stejnými prostředky a podrobněji jsou popsány jejich vlastnosti.

Klasickým řešením úspory dopravních zaměstnanců je, stejně jako u hlavních tratí, v prvním kroku centralizace obsluhy na úrovni stanice, v druhém kroku centralizace na úrovni celého traťového ramene. Vzniknou tak systémy s ústředními stavědly ve stanicích a s dálkovým ovládáním zabezpečovacích zařízení DOZ, bez dopravních zaměstnanců ve stanicích, s řízením provozu z pracoviště DOZ. Logickým krokem je tedy využití zařízení dálkového ovládání z hlavních tratí a jejich zjednodušení pro jednodušší dopravní poměry. Rozbory a praktické zkušenosti ale prokázaly, že pouhým zjednodušováním zařízení se nedosahuje úměrného snížení investičních nákladů na tratích s extrémně nízkým provozem a to zejména proto, že se zjednodušováním neklesá úměrně náročnost zařízení na kabelová vedení a pozemní stavby, což jsou dvě rozhodující položky celkových investičních nákladů na zabezpečovací zařízení. Proto tento postup není obecně vhodný pro tvorbu levného systému, může však být vhodným doplňkem, např. pro vybranou stanici či část tratě se speciálními požadavky.

Kvalitativně odlišný přístup v zabezpečení takových tratí pak umožňuje striktní přizpůsobení stanic a jejich provozu řídké dopravě. Tím je i konstrukce stanice se dvěmi jednosměrně pojížděnými kolejemi, spojenými s tratí dvěmi samovratnými mechanickými výměnami (viz obr. 17-4). Vlaky při příjezdu najíždějí na staniční kolej proti hrotu výměny s preferenční polohou a při odjezdu druhou výměnu (s opačnou preferenční polohou) jízdou po hrotu přestaví. Po skončení jízdy se tato výměna přestaví sama opět do preferenční polohy. Ostatní výměny ve stanici (pokud nějaké jsou) jsou přestavitelné místně a při běžném provozu jsou uzamčené. Je patrné, že při vjezdu a odjezdu vlaku nebo při křižování vlaků není ve stanici třeba žádné přípravné manipulace ani s výměnami ani s vlaky. Snížená rychlost při pojíždění výměn (u samovratných výměn obvykle na 40 km/h) není na překážku, pokud stanice nejsou rozlehlé a všechny vlaky ve stanici zastavují.



Obr. 17-4

Popsaná jednoduchá stanice předurčuje do jisté míry i způsob řízení jízdy vlaku na trati, přičemž není nutné ani zachovat ve stanici konvenci vjezd - odjezd. Vzhledem k minimalizaci zařízení ve stanici lze jízdu vlaku řídit v prostorových oddílech, vymezených dvěmi za sebou následujícími odjezdovými návěstidly. Takto vzniklý oddíl, na rozdíl od dosavadních zvyklostí, není přesně stejný pro oba směry. Oddíl

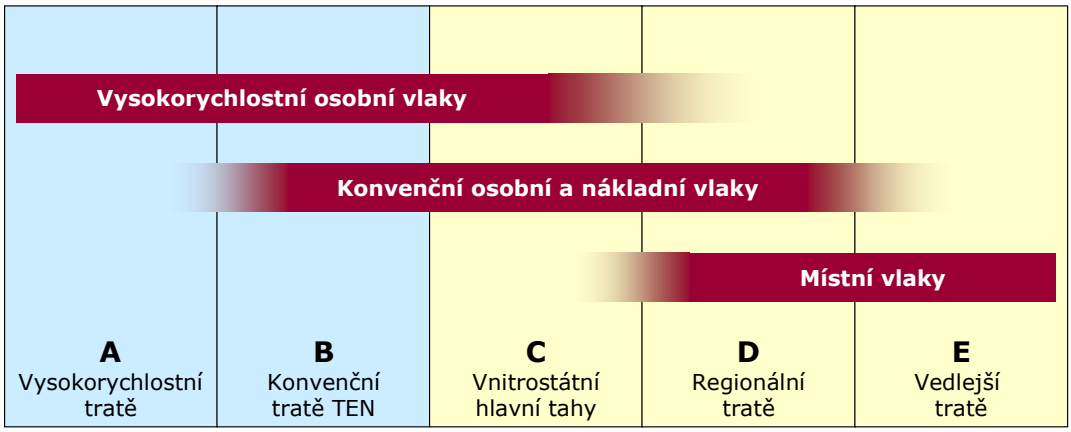
se skládá ze dvou částí. První část tvoří mezistaniční úsek, včetně přilehlých samovratných výhybek SV, druhou část tvoří samotná staniční kolej. Pro jízdu ze stanice A do stanice B je nutné, aby byl volný mezistaniční úsek a pravá kolej stanice B. Pro jízdu ze stanice B do stanice A musí být volný mezistaniční úsek a pravá kolej stanice A. Připustíme-li ještě, že není nutná jízda ze stanice A do stanice B dříve, než vlak dorazí do stanice C (tj. následný vlak ob jeden traťový oddíl), technické zařízení lze dále zjednodušit.

Řídící a zabezpečovací systém může být budován jako decentralizovaný systém s obsluhou vlakovým personálem nebo jako tzv. radioblokový systém. Radioblokové systémy navíc k výše uvedenému sledují další snížení nákladů (investičních i provozních) redukcí zařízení ve stanici a podél trati. Základním prostředkem pro dorozumívání mezi dispečerem a strojvedoucím je radiové spojení. Na radiovém spoji lze vytvořit kromě fónického spoje i datový kanál pro přenos zabezpečovacích informací. Jeho prostřednictvím pak lze na hnací vozidlo přenést i „návěstidlo“, podobně jako tomu je v případě inteligentních vlakových zabezpečovačů a klasická návěstidla mohou zcela odpadnout. Výhodou proti decentralizovaným systémům je tak i principiální zahrnutí hnacího vozidla do zabezpečovacího systému a tím vytvoření předpokladu pro účinné vlakové zabezpečovací zařízení s případným návazným automatickým řídícím systémem hnacího vozidla. Všechny důležité informace (povolení k jízdě, poloha vlaků) jsou zabezpečeně přenášeny mezi vozidly a radioblokovou centrálou. Centrála soustřeďuje všechny informace, zpracovává je a na vozidlo odesílá výsledná povolení žádané činnosti. Vozidlové zařízení pak dohlíží na soulad chování vozidla (strojvedoucího) s obdrženými povoleními. Kromě toho centrála může ovládat a dohlížet i případná zařízení na trati. Systém splní svůj účel tím lépe, čím méně zůstane na trati zařízení zapojených do centra.

Oba uvedené systémy umožňují také provoz s běžnými elektrickými přestavníky, s preferenční polohou nebo s dálkovým řízením, s menším dopadem na omezení rychlosti než u samovratných výhybek, samozřejmě však s odpovídajícím zvýšením investičních nákladů. Do radioblokových systémů pak lze bez problémů začlenit i stanice již vybavené klasicky nebo i nově vybavit stanice se složitějším dopravním programem klasickým stavědlem s dálkovým ovládáním. Radioblokové systémy si i v případě, že většina stanic je vybavena klasicky (bez samovratných výhybek), uchovávají část úspornosti. I tato vlastnost je mimořádně důležitá při konfiguracích tratí u ČD. ČD nemají typicky vedlejší tratě ve formě dlouhých končících větví (100 i více km) odbočujících z hlavní tratě, jak je tomu u některých jiných železnic. Typičtější jsou tratě tvořící zahušťující síť mezi dvěmi hlavními tratěmi, s délkou cca 20 - 30 km a často s křížením s další vedlejší tratí. Potenciálně je radioblokový systém schopen rádiem ovládat i další zabezpečovací zařízení (stavědlo, přejezdy) a to buď prostřednictvím centrály nebo přímo z vlaku.

Nejzávažnějším a obecným problémem všech zabezpečovacích systémů bez dopravních zaměstnanců ve stanicích, je získání informace o vyklizení celého traťového úseku nebo staniční koleje s dostatečnou věrohodností a za přijatelnou cenu. V zásadě je možné volit mezi prostředky pro přímé zjišťování volnosti nebo prostředky nepřímými, přičemž je třeba přihlédnout k tomu, kde má být informace primárně k disposici (na trati či na vozidle). Z přímých prostředků se nabízí klasická řešení s kolejovými obvody nebo počítači náprav, s případným doplněním pro přenos informace na vozidlo. Z nepřímých prostředků připadají v úvahu vybavovací obvody nebo polohovací systémy, doplněné některou formou kontroly celistvosti vlaku. Zde je ale nutné se nejprve zásadním způsobem vypořádat s rizikem jak "ztracených" vagónů na trati, tak "zapomenutých" vagónů ve stanicích (způsob, využívaný u většiny poloautomatických zařízení, tj. vybavovací obvody v kombinaci s vizuální kontrolou koncových návěstí vlaku dopravním zaměstnancem, je přímo nepoužitelný vzhledem k chybějícím zaměstnancům ve stanicích). Nahradit je může za určitých okolností vlakový personál nebo samočinná indikace konce vlaku. Dokonalejší alternativou pak jsou technické prostředky na vlaku, detekující jeho celistvost. Jsou zahraniční správy, které pravděpodobnost těchto jevů považují na tratích s malým provozem za tak nepatrnou, že odpovědnost ponechávají zcela na vlakovém personálu, bez technického zajištění bezpečnosti. Zda jde o tu pravou situaci, pro kterou platí "optimální bezpečnost za minimální náklady", je třeba posoudit spolu s odborníky dopravy adresně pro každou konkrétní aplikaci a podle toho pak zvolit vhodné technické řešení.

Druhým závažným problémem je, do jaké míry může být použité zařízení unikátní pro daný traťový úsek a zda lze očekávat, že se na něm bude pohybovat pouze vymezený okruh hnacích vozidel, která lze speciálně vybavit. Přehnaná touha po univerzálnosti jistě přináší zbytečné výdaje, ale požadavek co největší přechodnosti nelze bez diskuse pominout (obr.17-5). Protože naprostá většina drah vyžaduje přechodnost mezi různými kategoriemi tratí, předpokládá se obecně jistá forma uplatnění systému ETCS na vozidle. Jen pro vedlejší tratě, u kterých není požadována přechodnost na tratě vybavené ETCS, se dále uvažuje alternativní levné zařízení VT, nekompatibilní s ETCS.



Obr. 17-5

Výše uvedené principy zabezpečení jednoduchých tratí se od 80tých let, v různých obdobách, objevily u řady železnic. Jisté je, že zcela primitivní řešení, která s využitím samovratných výhybek a hovorového kanálu rádia zachovávají nezabezpečený provoz (obdobný dnešnímu řízení podle D3 u ČD), nelze považovat za přijatelná ani odůvodnitelná snahou po minimálních nákladech. Takový provoz je zcela závislý na lidském faktoru a ze strany železnice je v podstatě nezodpovědný.

Je třeba zdůraznit, že vytváření investičně a provozně nenáročných zabezpečovacích systémů pro vedlejší tratě musí být doprovázeno minimalizací provozních požadavků, omezením záložních systémů a zásadní aktivní účastí strojvedoucího na řešení mimořádných stavů. Nezbytný je také adekvátní příspěvek ostatních složek infrastruktury a vozby, která však nesmí vyústit v omezení rychlosti dopravy, protože taková doprava není schopná konkurovat dopravě silniční (minimální potřebná traťová rychlost je 80–100 km/h).

Základním předpokladem jakýchkoliv řešení na vedlejších tratích samozřejmě zůstává rozumná státní dopravní politika, která vrátí dopravu ze silnic na železnici. Úvahy o privatizaci tohoto typu tratí nejsou z technického hlediska relevantní a i obecně jsou jen zástupným problémem při neexistenci přijatelné dopravní politiky státu.

17.3.1 Klasické řešení s obsluhou vlakovým personálem

Charakteristickým rysem je minimalizace a decentralizace zabezpečovacího zařízení a jeho obsluha vlakovým personálem. Dispečer zasahuje do provozu pouze fónickými pokyny či souhlasy k jízdě (po telefonním nebo rádiovém spoji), vlastní zabezpečovací zařízení obsluhuje, pokud je to vůbec třeba, vlakový personál, zabezpečené povely jsou strojvedoucímu sdělovány návěstidlem. Vybavení stanice a tratě je znázorněno na obr. 17-4. Světelná, dvousvětlová návěstidla (červená, zelená) jsou osazena pouze na koncích obou jednosměrně pojížděných staničních kolejí. Vjezdové výměny jsou buď mechanické, samovratné s elektrickou kontrolou jazyků nebo elektromotorické, ovládané automaticky při stavění jízdní cesty. V celém obvodu stanice je rychlost jízdy s ohledem na samovratné výměny, chybějící předvěsti a jednoduché dvouznakové návěštění omezena rychlostníky na 40 km/h. Volnost traťových úseků, staničních kolejí a vjezdových výhybek je zjišťována vhodně rozmístěnými počítači náprav nebo kolejovými obvody. Traťové zabezpečovací zařízení může být tvořeno upraveným elektronickým blokem (který byl vyvinut začátkem 90tých let ve VÚŽ), je připojeno k vedení traťového telefonu a pracuje nad hovorovým pásmem. Také vazba detektorů kol a počítače náprav musí být pro úsporu vedení možná v jiném nadhovorovém kanálu téhož telefonního vedení.

Při odjezdu vlaku ze stanice je třeba rozsvícením zeleného světla potvrdit, že jsou splněny všechny podmínky pro bezpečnou jízdu až k dalšímu návěstidlu, na konci staniční koleje sousední stanice. V tomto

případě to bude volnost traťového úseku včetně přilehlých výhybek, volnost staniční koleje v následující stanici, zablokování odjezdového návěstidla v protisměru a základní poloha vjezdové výhybky v sousední stanici. V případě elektromotorických výhybek je nutné také vydat pokyn pro přestavení vjezdové výměny v sousední stanici a odjezdové výměny ve vlastní stanici, jejich polohu zkontrolovat a uzavřít je. Žádost o uvolnění odjezdového návěstidla (a tím v případě potřeby i o změnu směru) může vyslat jedině strojvedoucí, např. obsluhou tlačítka na odjezdovém návěstidle, u kterého bude vždy zastavovat. Traťový souhlas musí tedy pracovat pouze na základě takto vyjádřené žádosti o souhlas.

Pro jízdu ze stanice A do stanice B stiskne strojvedoucí tlačítko na odjezdovém návěstidle L1. (Variantně je možné přenést obsluhu tlačítka na vozidlo pomocí jednoduchého dálkového ovládání z kabiny strojvedoucího - rádio, infra atd. Přenos nemusí být zabezpečován způsobem obvyklým v zabezpečovací technice, protože zabezpečovací funkce plní teprve návazné obvody, rozsvěcující povolující znak na odjezdovém návěstidle. Průjezdy by pak bylo možné v případě účelnosti uskutečnit za předpokladu dostatečného dosahu dálkového ovládání odjezdových návěstidel z kabiny hnacího vozidla.) Jsou-li splněny podmínky pro bezpečnou jízdu, na odjezdovém návěstidle se rozsvítí zelené světlo. Obsazením výhybkového kolejového obvodu za návěstidlem se povolující znak zhasne. Po ukončení cesty celého vlaku na staniční koleji v sousední stanici se vybaví traťové zabezpečovací zařízení a je možné stejným způsobem uskutečnit jízdu v opačném směru z B do A. Po vyklizení staniční koleje je možné uskutečnit jízdu následujícího vlaku.

O povolení posunu ve stanici se žádá tlačítkem, umístěným ve vhodném objektu ve stanici, přístupném vlakové četě. Na žádost o posun se souhlasy obou přilehlých traťových úseků obrátí jako pro odjezd ze stanice a zablokují se. Tím je znemožněna jízda ze sousedních stanic do stanice žádající o posun. Dále se uvolní výměnový klíč. Vyjmutí výměnového klíče znamená souhlas k posunu a klíč je zároveň i prostředkem pro odemknutí uzamykaných výměn ve stanici. Rozhodující výměny a výkolejky ve stanici jsou uzamykány kontrolními zámky tak, aby vrácení výměnového klíče do zařízení zajišťovalo základní polohu zařízení ve stanici. V případě elektromotorických výměn v dopravních kolejích je nutno zřídit jejich místní ovládání pro posun. Uzamčení výměnového klíče zpět do objektu vrátí traťové zařízení do základní polohy, takže bude možné znovu obsluhovat odjezdová návěstidla ve vlastní stanici i ve stanicích sousedních. Umožňují-li to místní podmínky, lze vlak při posunu na kolejích mimo koleje dopravní uzavřít a výměnový klíč vrátit do objektu. Tak lze dopravní koleje využít pro jízdu jiných vlaků, zatímco mimo dopravní koleje probíhá posun. Pro návrat posunujícího vlaku na dopravní koleje bude nutné znovu požádat o povolení posunu.

Jak je z popisu patrné, na takto pojatých tratích bude bez problémů jízda vlaků od stanice ke stanici, křižování dvou vlaků i posun. Předjíždění lze sice uskutečnit (tak, že předjížděný vlak posunem uvolní staniční kolej příslušného směru a po předjetí se opět posunem přestaví zpět; zpětný posun by bylo možné ušetřit, ovšem za cenu rozšíření zařízení o odjezdová návěstidla ze staničních kolejí opačného směru) ale není příliš praktické. Systém umožňuje, aby v případě potřeby pružnějšího zajištění průjezdů, předjíždění či dalších operací v některé stanici tratě, byla tato stanice vybavena jednoduchým dálkovým ovládáním. Stavění jízdních cest by pak zajišťoval traťový dispečer způsobem obvyklým na dispečerizovaných tratích, za bezproblémové spolupráce zařízení na zbytku tratě. Vlastní prováděcí zařízení, s vlastnostmi zařízení zabezpečovacích, zůstanou přitom ve stanicích.

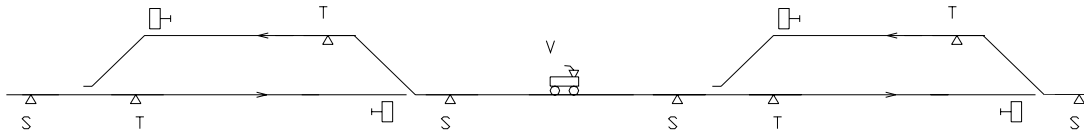
Zvláštní pozornost vyžadují kontrolní linky přejezdových zařízení. Stav kontrol by bylo třeba sdělovat vlakové četě (např. při obsluze odjezdu), ale za úvahu stojí i možnost náhradního řešení pomocí přejezdníku, umístěného v blízkosti přejezdu.

17.3.2 Radioblok pro vedlejší tratě

Informace, jdoucí z vozidla do centra, informují o vyklizení úseku tratě nebo staniční koleje. Protože jde o informace zásadní důležitosti, měly by být vázány na skutečně projetý úsek. Postupy, použité u dnešních zařízení poskytují takovou informaci na trati, nikoliv na vozidle. Na vozidlo ale lze relativně jednoduchým prostředkem přenést informaci o poloze vlaku, např. přenosem identifikačního čísla z vhodně umístěného bodového majáku. Informace o vyklizení úseku tratě lze pak vázat na uskutečnění přenosu z odpovídajícího bodu tratě. Zřejmým dalším předpokladem oprávněnosti takové informace je zjištění celistvosti vlaku.

Vybavení stanice a tratě je schematicky znázorněno na obr. 17-6. Balízy T jsou umístěny vždy na konci traťového úseku (včetně přilehlých výhybek), balízy S bezprostředně za stanicí. Balízy T slouží k

identifikaci polohy pro hlášení volnosti traťového úseku, balízy S k identifikaci polohy pro hlášení volnosti staniční koleje. Ve stanici se dvěma jednosměrně pojížděnými staničními kolejemi jsou samovratné výhybky s ukazatelem polohy do směru jízdy proti hrotu. Na konci staniční koleje, v místě odjezdového návěstidla, je umístěna tabule, která označuje místo jež nesmí vlak minout bez příslušného povolení. Rychlost jízdy v celém obvodu stanice je omezena rychlostníky na 40 km/h. Polohu výměny při vjezdu do stanice kontroluje (s pomocí ukazatele polohy výměny) strojvedoucí, výměny nejsou dohlíženy obvyklým zabezpečovacím zařízením.



Obr. 17-6

Informační body - pasivní nepřepínatelné balízy - při průjezdu hnacího vozidla přenesou na vozidlo číslo informačního bodu. Po příjmu čísla (a ujetí vzdálenosti, odpovídající délce vlaku) vyšle vlak (po kontrole integrity vlaku) prostřednictvím datového kanálu rádia telegram, s povahou odhlášky, do radioblokové centrály. Telegram se skládá z čísla vlaku, čísla informačního bodu a kódu předcházejícího povolení k jízdě. Balíza typu S v opačném směru může být využita jako spouštěcí bod jednoduchého VZ před místem zastavení (tabulí na konci vjezdové koleje).

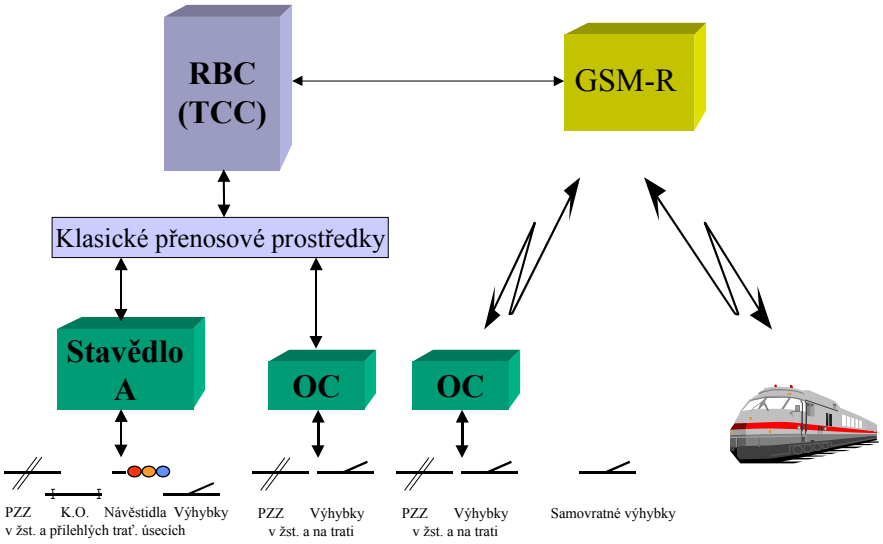
Obsluha zařízení je kombinací fónického spojení strojvedoucího s dispečerem a automatického spojení centra s vozidlem prostřednictvím radiového datového kanálu. Strojvedoucí ze stanice A požádá fónií dispečera o odjezd do stanice B. Dispečer zapíše požadavek na terminálu centrálního zařízení. Není-li požadavek v rozporu s provozními okolnostmi, objeví se na terminálu centrálního zařízení souhlas. Ten dispečer fónií oznámí strojvedoucímu. Paralelně je souhlas automaticky přenesen na vozidlo po datovém kanálu a je zobrazen na vozidlovém terminálu v podobě nahrazující odjezdové návěstidlo (např. nápis na obrazovce "Povolení jízdy z žst. A do žst. B"). Při přejetí balízy S (příslušného směru) se datovým kanálem pošle automaticky zpráva centrále o vyklizení staniční koleje. Po přejetí balízy T v sousední stanici se zruší na lokomotivním zařízení dosavadní indikace povolující jízdu a automaticky se vyšle informace o vyklizení traťového úseku. Tato informace je důležitá při křižování, pro následné nemá význam. Je možné povolit jízdu i v delším úseku, přes několik stanic. Projetá část se pak uvolňuje automaticky. Obdobným způsobem probíhá obsluha při posunu. Strojvedoucí fónií požádá, dispečer přenese požadavek do zařízení a oznámí strojvedoucímu výsledek. Povolení k posunu se paralelně přenese i po datovém kanálu, čímž se uvolní univerzální klíč na vozidle pro místní obsluhu výměn. Zpráva o ukončení posunu musí obsahovat i hlášení o volnosti koleje, na které vlak po skončení posunu nestojí a potvrzení návratu univerzálního klíče. Žádosti o povolení jízdy či posunu by bylo možné také přenášet pouze datovým kanálem. Naznačený způsob však má své výhody ve větší informovanosti dispečera, což usnadňuje jeho rozhodování za mimořádných stavů.

V zahraničí jsou v provozu nyní i jednodušší varianty, bez vazby na trať, se zvýšenou odpovědností strojvedoucích. Místo balíz jsou umístěny tabule s identifikačním číslem, které strojvedoucí použije pro formování zprávy o své poloze do centra. Odesláním zprávy také strojvedoucí, bez dalších technických pomůcek, potvrzuje, že vlak je celý. Naopak dokonalejší varianta by vznikla, kdyby balízy navíc přenášely traťovou rychlost a vzdálenost bodu zastavení, popřípadě i kompletní statický rychlostní profil pro celý úsek tratě. Přenosem dalšího povolení k jízdě z centra na vozidlo by cílová rychlost 0 byla upravena na příslušnou dovolenou rychlost, odpovídající okamžité dopravní situaci. Pohyb vlaku by tak byl plně pod kontrolou VZ.

Realizace radiobloku vyžaduje zabezpečený řídící počítač v centru a zabezpečený terminál na vozidle s funkcí jednoduchého VZ, obojí připojeno k datovému kanálu mnohabodového radiového spoje (viz obr. 17-7). Dále je třeba trať vybavit pasivními balízami. Trať musí být pokryta radiovým signálem pouze v místech přenosu, tj. zejména v okolí stanic. Ani jízda nevybaveného vlaku, nebo vlaku s poruchou terminálu na vozidle nezpůsobí neřešitelné problémy, protože rozhodující informace do systému radiobloku může zavést také dispečer na základě ústních zpráv strojvedoucího, předaných radiofonií nebo telefonem. V tom případě pak budou také povolení k jízdě vydána dispečerem ústně, na základě zpráv zobrazených na

terminálu dispečera. Chování vlaku je ovšem v takovém případě pouze pod výhradní kontrolou strojvedoucího – zařízení zabraňuje jen omylům dispečera.

Přejezdová zařízení mohou být v tomto systému provozována jako autonomní nebo mohou být zahrnuta do funkcí radiobloku. V případě rozšíření přenosu na datový spoj mezi přejezdem a radioblokovou



ústřednou (popř. vozidlem) se nabízí kontrola funkce nebo i řízení přejezdu vlakem (viz dále).

Obr. 17-7

Je třeba podtrhnout, že předpokladem pro výše uvedené omezení klasických zařízení ve stanici a na trati je pojímání vlakové soupravy jako poruchou nedělitelné – buď proto, že souprava je konstruována jako nedělitelná, nebo je vybavena zařízením integritu (nerozdělenost) vlaku kontrolujícím, nebo je povinnost kontroly celistvosti vlaku přenesena na strojvedoucího - a pominutí nebezpečí "zapomenutých" vagónů. V opačném případě zůstane mnoho klasických zařízení po trati a dosažené úspory budou nevýznamné.

V dalším jsou naznačeny možnosti jednotlivých úrovní systému při modulární výstavbě zařízení. Předpokládá se, že podle místních, velmi diferencovaných, podmínek se systém může uplatnit v následujících úrovních (provedení), která na sebe budou modulární výstavbou navazovat (i dodatečně bude možné bez překážek úroveň zvýšit) a budou navzájem kompatibilní (úroveň vlaku se projeví při přihlášení). Předpokládáme, že provozní ověření ukáže, které z úrovní budou vhodné pro zavedení do trvalého provozu u ČD.

Zabezpečený expertní systém u dispečera (VT, úroveň 0)

Pro tento způsob provozu postačuje vybavení stanic dvěmi samovratnými výměnami, fónické rádiové spojení strojvedoucího s dispečerem v oblasti stanic a zabezpečený terminál u dispečera (RBC pro VT). Výměna informací a příkazů mezi dispečerem a strojvedoucím probíhá na fónickém spojení. Formalizované žádosti a hlášení strojvedoucího ale dispečer vkládá do terminálu RBC a povolení k bezpečnostně relevantním činnostem vydává strojvedoucímu až na základě odpovídajícího výstupu na terminálu. Tím je zajištěno, že veškeré, pro bezpečnost relevantní, údaje budou u dispečera uloženy a před vydáním povelů budou správně vyhodnoceny, aniž by mohly být opomenuty.

RBC dispečerovi poskytuje přehlednou grafickou informaci o současné dopravní situaci na řízeném úseku. Navíc může ovládat případné řízené venkovní prvky infrastruktury.

Hnací vozidlo není vybaveno žádným zabezpečovacím zařízením. Strojvedoucí přijímá povely dispečera fónií a vozidlo je pouze pod dohledem strojvedoucího. Strojvedoucí informuje dispečera o příjezdu

do další stanice a o ukončení posunu fónií formou odhlášek. Odhlášku nesmí podat bez ověření, že souprava je kompletní a smí tak učinit pouze v místech k tomu určených.
Požadavky na fónický kanál:

- Vlak-Dispečer alespoň v oblasti žst. (cca 2 km od budovy žst.) a pokud možno (není nezbytné) i v oblasti přejezdu (cca 1 km před a za),
- Přejezd-Dispečer jako případná náhrada traťového a nehodového telefonu (ovládání přejezdu viz dále),
- možnost vstupu dalších přenosných stanic do fónie (údržba i provoz).

Doplnění o polohové lokátory GPS (VT, úroveň 0+)

Pokud budou vozidla vybavena komerčními nezabezpečenými polohovými lokátory GPS a informace o poloze všech vlaků v oblasti budou přeneseny k dispečerovi, mohou být využity pro kontrolní účely v expertním systému. Protože tyto informace nepochází z bezpečného systému (není u nich zajištěna bezpečnost informace ve smyslu zabezpečovací techniky), nelze je využívat přímo (např. ani zobrazením dispečerovi), protože by mohly maskovat skutečné bezpečné výchozí informace (byť zatížené chybou lidského činitele). Jsou tedy využity jako informace kontrolní. V případě, že systém GPS bude hlásit vlak kolidující s připravovaným povelem dispečera, nebude připravovaný povel vydán a dispečer bude nucen znovu ověřit polohu vlaku a tedy nezávadnost zamýšleného povelu. Tímto řešením se nikterak nesejme výlučná odpovědnost dopravního personálu za správnost vstupních informací do expertního systému, ale dále se sníží pravděpodobnost jejich, jinak včas neidentifikovatelných, omylů.

Radiové spojení musí být v takovém případě zřízeno již podél celé trati a doplněno o datový kanál pro přenos nezabezpečených informací z jednotlivých vozidel o poloze vlaků, popřípadě i pro přenos korekčních signálů pro systém GPS (DGPS). Je totiž třeba počítat s tím, že údaje polohového lokátoru (i když nezabezpečené a přímo dispečerovi nezobrazované) bude nutno přenášet kvaziliniově, aby bylo možné v RBC alespoň do jisté míry vyhodnocovat důvěryhodnost informace.

Úrovně 0 a 0+ jsou předpokládány pouze jako dočasné předstupně pro budování vyšších úrovní – pro rychlejší opuštění systému dopravy podle D3.

Doplnění o datový kanál zabezpečovacích informací (VT, úroveň 1)

Fónické dorozumívání je doplněno datovým kanálem, který zajistí přenosy ve směru:

- dispečer - vlak pro přenosy povolení k jízdě na zabezpečovací terminál vozidla,
- strojvedoucí - dispečer pro přenosy odhlášek od strojvedoucího do RBC u dispečera,

Strojvedoucí na terminálu vozidla při odhlášce udává polohu vlaku a pokud vozidlo není vybaveno technickou kontrolou celistvosti soupravy, potvrzuje i celistvost vlaku. Proces odhlášky je tedy poloautomatický. Mobilní zařízení znemožňuje pohyb vlaku (nad určitý limit) bez povolení k jízdě.

Požadavky na rádiové pokrytí jsou stejné jako v úrovni 0, ale týkají se jak fónického, tak datového spojení.

Doplnění o datový kanál zabezpečovacích informací a GPS (VT, úroveň 1+)

Zařízení úrovně 1 je doplněno nezabezpečenými polohovými lokátory GPS (jako v úrovni 0+). Informace o poloze vlaku je ale nejen přenesena k dispečerovi, ale může být využita i v mobilním zařízení jako kontrola, že strojvedoucí odesílá odhlášku v místě k tomu určeném (resp. že ji neodesílá před dosažením tohoto místa).

Požadavky na rádiové pokrytí musí vyhovět požadavkům jak úrovně 1 i 0+.

Doplnění o datový kanál zabezpečovacích informací a balízy (VT, úroveň 2)

Fónické dorozumívání je doplněno datovým kanálem, jako v úrovni 1, ale navíc je trať vybavena nepřepínatelnými balízami a vozidlo jejich snímačem. Na základě příjmu z odpovídající balízy je mobilním zařízením automaticky připravena odhláška a pokud je vozidlo vybaveno technickou kontrolou celistvosti soupravy, jsou odhlášky vysílány automaticky. Pokud toto zařízení chybí, nahrazuje jejich funkci strojvedoucí potvrzením celistvosti soupravy na terminálu vozidla. Systém tak pracuje se zabezpečenou informací o poloze vlaku.

Požadavky na rádiové pokrytí jsou stejné jako v úrovni 1.

Doplnění o kontrolu rychlosti (VT, úroveň 3)

Předávaná povolení k jízdě radiovým datovým kanálem a informace o poloze z balíz vytváří předpoklady pro podrobnější dohled nad jízdou vlaku. Budou-li tyto informace doplněny o SSP (radiem, balízou, mapou tratě), je možná komplexní kontrola rychlosti vlaku. Využití traťové mapy, uložené v paměti počítače na vozidle, sníží objem předávaných zpráv. Je otázkou, zda toto doplnění již není v podstatě ETCS a zda je možné je vytvořit významně levněji než ETCS. Evidentně bude účelné, aby systém této úrovně byl navržen jako systém ETCS kompatibilní.

Část V. - Technickoorganizační opatření

18 INTEGRITA BEZPEČNOSTI

Norma EN 50126, zabývající se specifikací parametrů RAMS (spolehlivost, pohotovost, udržovatelnost a bezpečnost) obecně pro všechny železniční systémy, reaguje na skutečnost, že naléhavost požadavků na bezpečnost funkce jednotlivých železničních systémů je různá a lze je tedy splňovat s různou pravděpodobností jejich selhání. Zavádí nový pojem **integrita bezpečnosti** (safety integrity - celistvost, úplnost, neporušenost bezpečnosti), který definuje jako pravděpodobnost, s níž systém uspokojivě splní požadované bezpečné funkce, za všech stanovených podmínek a ve stanoveném časovém období. Jde o to, do jaké míry může být pro bezpečnost relevantní funkce narušena např. poruchami vlastního zařízení, omyly obsluhy, vnějším rušením atd.

Modifikovaně byl tento pojem přenesen i do normy ENV 50129 (příloha A) pro železniční elektronické zabezpečovací systémy. I klasická zabezpečovací technika bez velkého zdůrazňování respektovala, že ne na všechna zařízení jsou stejně důrazné bezpečnostní požadavky (kategorizace zařízení, vedlejší tratě/hlavní tratě, zařízení pro ČD/zařízení pro vlečky, staniční zařízení/spádoviště atd.). Uvidíme dále, že v pojmu integrita bezpečnosti je pro zabezpečovací zařízení dominantně obsažena oblast, kterou běžně v této technice označujeme (a také norma ENV 50129 ji tak označuje ve své základní části) termínem **technická bezpečnost**. Úvahy okolo integrity bezpečnosti zde sledujeme odděleně od úvah o technické bezpečnosti (přes jejich podobnost) pro jejich výhodnost zejména v úvodních fázích projektu nového systému (zařízení, výrobku atd.) – viz kap. 2, obr. 2-1. Úvahy o technické bezpečnosti jsou naproti tomu praktičtější pro etapy vlastního technického řešení nového zařízení (návrh, kontrola, schvalování). Tak například při konečných bezpečnostních rozborech navrženého zařízení v rámci materiálů pro schvalovací řízení se část úvah sice opakuje, ale v jiné úrovni - s podrobnou znalostí technické realizace.

18.1 Požadavky na integritu

S předchozím vysvětlením lze tedy obecně bezpečnostní požadavky na zabezpečovací zařízení uvažovat ve dvou částech :

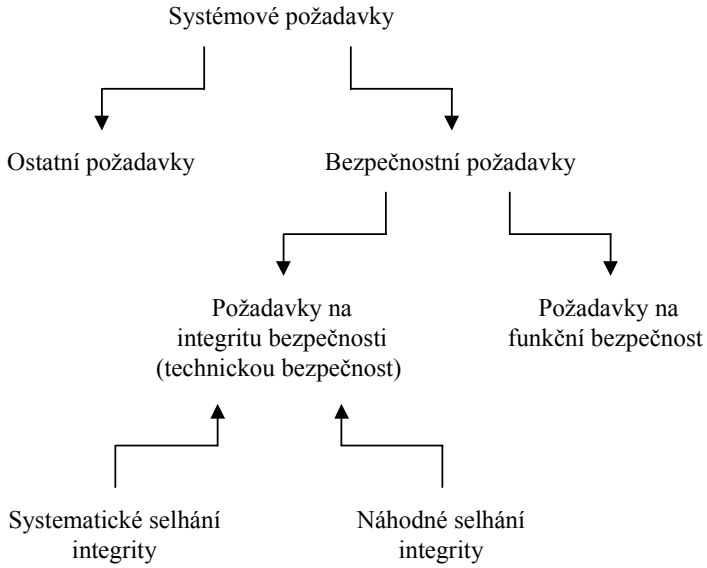
- požadavky na funkční bezpečnost,
- požadavky na integritu bezpečnosti.

Požadavky na funkční bezpečnost zahrnují skutečné, pro bezpečnost relevantní funkce požadované od systému, tj. jsou předpisem za jakých podmínek smí být ta která funkce vykonána. Funkční požadavky jsou pro jednotlivá zařízení dány různými materiály (normy, základní požadavky - ZTP, závěrová tabulka atd.). Ty často obsahují i funkce, které nejsou pro bezpečnost významné a proto se jimi dále nezabýváme – viz Ostatní požadavky na obr.18-1.

Požadavky na integritu definují úroveň bezpečnosti, která je pro tyto funkce požadována a vztahují se k pravděpodobnosti, s kterou bezpečný systém dosahuje své bezpečné funkce. Čím vyšší integrita zařízení, tím menší pravděpodobnost, že zařízení při vykonávání bezpečnostně relevantních funkcí selže. Požadavky na integritu plynou ze dvou částí (viz obr. 18-1):

- systematických selhání integrity,
- náhodných selhání integrity.

Pro dosažení adekvátní úrovně bezpečnosti (integrity) je nutné splnit požadavky z obou větví a to i s ohledem na okolí (EMI, teplota, vibrace atd.).



Obr. 18-1

Systematická selhání integrity jsou nekvantifikovatelná a týkají se hazardních systematických poruch HW i SW (hazardem přitom rozumíme takový stav či okolnosti systému - zařízení, které za určitých dalších podmínek vedou k nehodě). Jsou důsledkem **lidských chyb** v různých etapách života zařízení – chyby specifikací, chyby konstrukční, některé nedokonalosti součástek, výrobní chyby, montážní chyby, chyby obsluhy, chyby údržby, chyby při dodatečných úpravách zařízení atd. Předchází se jim zejména organizačními opatřeními v rámci procesů řízení kvality a bezpečnosti – existují pro to určité nástroje, které při efektivní aplikaci poskytují přijatelný výsledek. Jen do jisté míry jim lze předcházet i technickými opatřeními – např. vhodnou volbou architektury systému.

Náhodná selhání integrity se převážně týkají hazardních náhodných poruch, konkrétně náhodných poruch HW, které vyplývají z konečné **spolehlivosti součástek** (patří sem ale také – viz kap. 5 – omyly obsluhy, rušení atd.). Předchází se jim plněním podmínek zaručujících technickou bezpečnost. Navíc je nezbytné provést kvantitativní zhodnocení pomocí pravděpodobnostních výpočtů. Tyto výpočty jsou založeny na údajích o četnosti poruch součástek a době odhalení poruchy. Pro součástky s definovanými vnitřními fyzikálními vlastnostmi se četnost hazardních poruch zpravidla uvažuje jako nulová, i když i zde existuje jisté zbytkové riziko hazardních poruch.

Pro určení požadované úrovně integrity zabezpečovacího zařízení je nutné brát v úvahu :

- provozní podmínky železnice a
- architekturu zabezpečovacího systému.

Úkolem pak je na základě těchto vstupů stanovit odpovídající kvalitativní (a pokud možno i kvantitativní) požadavky na integritu. Pro různá zabezpečovací zařízení (systémy, podsystémy, elementy), či dokonce pro jejich jednotlivé funkce, lze uplatňovat, v závislosti na účelu zařízení a bezpečnostních cílech provozovatele, i různou úroveň bezpečnosti. Vychází-li se z jednotlivých funkcí, pak při požadavcích na zařízení či jeho část je samozřejmě nutné, podle toho na kterých funkcích se podílí, požadovat úroveň integrity bezpečnosti zařízení vyhovující nejpřísněji sledované funkci.

Celý proces určení požadavků na úroveň integrity sestává z analýzy rizika a analýzy hazardů. Analýza rizika zkoumá důsledky možných hazardních stavů a poskytne tolerovatelnou četnost hazardů (THR – Tolerable Hazard Rate) - nezbytnou součást systémových požadavků. THR je pak jedním ze vstupů pro následující analýzu hazardů. Analýza hazardů, nebo přesněji analýza hazardů systémového návrhu, určí možné příčiny hazardů, požadavky na integritu bezpečnosti jednotlivých částí systému a určí spolehlivostní požadavky na zařízení. Analýza hazardů může vést ke změně navrhovaného systému např. proto, že prokáže, že navrženým systémem nelze efektivně dosáhnout požadovaných bezpečnostních vlastností. V tom případě nejsou obě analýzy nezávislé, ale celý proces je iterativní – je třeba podle změn upravit analýzu rizika a

pokračovat s novou analýzou hazardů. Aby celá práce měla smysl, musí být obě analýzy odsouhlaseny provozovatelem (orgánem zodpovědným za bezpečnost železnice) jako jeden z klíčových výchozích materiálů pro vlastní vývojové práce na novém systému. Celý proces spojený s určováním požadavků na integritu je přehledně znázorněn na obr. 18-2.

18.1.1 Analýza rizika

Analýza rizik je v první řadě věcí uživatele. Při ní se :

- definují požadavky na systém,
- identifikují jeho hazardní stavy,
- analyzují se možné **důsledky** hazardních stavů,
- definují se kritéria pro tolerovatelná rizika,
- odvozuje se tolerovatelná četnost rizik,
- ověřuje se, že výsledná rizika jsou skutečně tolerovatelná.

Nezávisle na technickém řešení se definuje systém (výrobek, proces, jeho funkce) a identifikují nepříznivé stavy (hazardy), které se mohou vyskytnout v průběhu celé životnosti zařízení a jsou potenciálně nebezpečné (zranění, poškození životního prostředí, ekonomické ztráty). Hazardy se identifikují systematickou analýzou na rozhraní mezi provozním prostředím a sledovaným zabezpečovacím zařízením - proto postačí povšechná definice systému, bez znalosti podrobností o jeho budoucí realizaci, ale nutná je podrobná znalost operačního prostředí a jasná definice rozhraní mezi novým systémem a prostředím.

Identifikace hazardů vychází jednak z předchozích zkušeností, jednak z rozborů typu „co - když“, tedy prognóz. Aby výsledky byly použitelné, je třeba se vyhnout definování nadměrného množství triviálních hazardních stavů. V každém případě musí být sestaven seznam uvažovaných hazardních stavů. Analýza hazardních stavů pak pro každý jednotlivý hazardní stav identifikuje možné důsledky hazardů.

Tolerovatelná četnost rizika musí být odvozena s uvážením určitých kritérií, která nejsou stanovena normou ENV 50129, ale obecnými požadavky legislativy na národní nebo evropské úrovni a bezpečnostními cíli, které si železnice klade. Tolerovatelnost rizika je tedy v zásadě problém sociální a legislativní - nikoliv technický - a vyžaduje proto přístup na základě konsensu a všeobecně akceptovaných principů. Obecně lze vycházet ze statistických údajů o nehodovosti na stávajících zařízeních nebo z analýzy četnosti hazardních stavů na stávajících zařízeních. Jak patrno, do těchto úvah se mohou pouštět snáze ty železnice, které disponují dlouhodobými a věrohodnými statistikami bezpečnosti.

Jako určitý návod může také sloužit to, co je shrnuto v část 7.1. V zahraniční praxi se v těchto směrech prosazují, vedle snah po explicitním určení rizika, také zjednodušené přístupy známé jako :

- ALARP (As Low As Reasonably Practicable) - princip uvažovaný v UK - zařízení musí poskytnout takovou úroveň bezpečnosti, jaká je za rozumných podmínek dosažitelná. Vychází se z toho, že vždy existuje jistá všeobecně akceptovaná míra rizika. Pokud se nepřekračuje, není o čem diskutovat. Právě tak existuje jistá hranice, nad níž je riziko absolutně nepřijatelné (s výjimkou zvláštních okolností - např. nouzové stavy zařízení). Mezi oběma těmito hranicemi je oblast ALARP, kde je možné se pohybovat v případě, že náklady na další redukci rizika by převýšily zisk z dosaženého zlepšení nebo je zlepšení přímo nemožné. Pro demonstraci, že riziko je ALARP, lze dokladovat, že zařízení aplikuje nejlepší stávající normy a zkušenosti. Pokud jsou ale pochyby o adekvátnosti norem či zkušeností, nebo se jedná o zcela nové zařízení, musí být provedena analýza nákladů a přínosů.
- GAMAB (Globalement Au Moins Aussi Bon) - princip uvažovaný ve Francii - nový systém musí poskytnout globálně přinejmenším stejnou úroveň bezpečnosti jakou poskytoval ekvivalentní existující systém. Jak patrno, tento princip vychází ze statistik bezpečnosti existujících zařízení a umožňuje „přerozdělení“ rizik, protože se bere v úvahu globálně.
- MEM (Minimum Endogenous Mortality) - princip uvažovaný v Německu - minimální endogenní úmrtnost (úmrtnost nezahrnující úmrtí vlivem nemocí). Vychází se z obecné statistiky úmrtnosti populace ve státě. Tam pro nejméně ohroženou věkovou skupinu (5-15 let) platí $R_m = 2.10^{-4}$ úmrtí/osobu*rok a požaduje se, aby vlivem nového systému nedošlo k znatelnému zvýšení. Odtud byla stanovena rizika, kterým mohou být cestující vystaveni vlivem zařízení:
  - $R_1 \leq 10^{-5}$ úmrtí/osobu*rok,
  - $R_2 \leq 10^{-4}$ těžké zranění/osobu*rok,

- $R_3 \leq 10^{-3}$ lehké zranění/osobu*rok,

(pro případy, že může být ohroženo více než 100 osob najednou se dovolené riziko o jeden řád snižuje na každý další řád ohrožených osob).

Pro domácí praxi neexistuje žádná všeobecně přijatá definice. V nezbytných případech postupujeme obvykle obdobně k přístupu ALARP. Všechny tyto přístupy však vyžadují velký nadhled a ucelenost pohledu. Jakékoliv dogmatické uplatňování dílčích pohledů může vést ke zcela nesprávným závěrům a to v obou směrech.

Metodicky vzato, lze tedy při určování tolerovatelné četnosti hazardů postupovat více méně kvalitativní analýzou nebo čistě kvantitativní analýzou. Náznak kvantitativní analýzy rizik je uveden v příkladu v části 18.1.3.

Ještě je třeba zdůraznit, že při zavádění nových technologií do zabezpečovací techniky mohou vznikat nové hazardní stavy, protože :

- chybí zkušenosti,
- mohou se projevit hazardy, které u stávající technologie zůstaly skryty,
- mohou vzniknout nové hazardy při vývoji vzhledem k nedostatečnosti nových specifikací,
- nové provozní vlastnosti či způsoby obsluhy mohou nevyhovovat obsluze, údržbě, cestujícím atd. a tedy mohou vzniknout nové hazardní stavy.

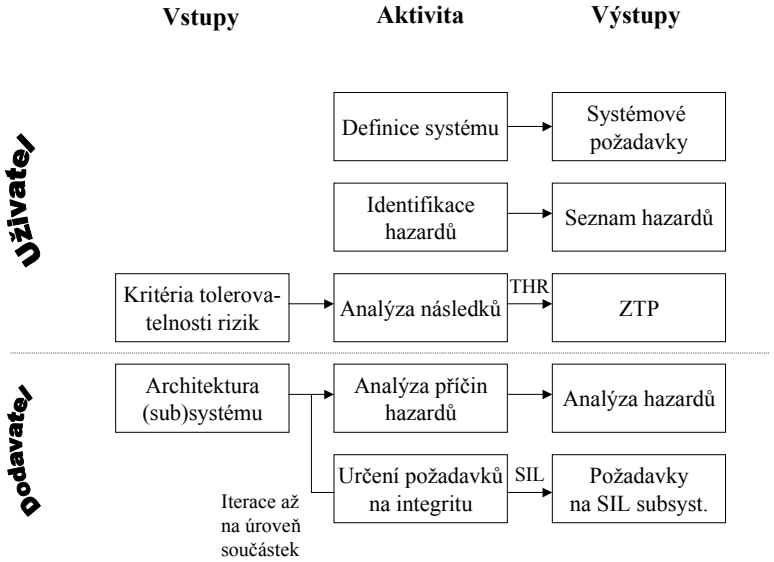
Všem těmto záležitostem je třeba věnovat zvýšenou pozornost a řešit je na základě kvalitní kooperace mezi dodavatelem nové technologie a provozovatelem a analýzy doplňovat postupně podle nových poznatků.

18.1.2 Analýza hazardů

Analýzu hazardů musí zpracovat dodavatel zařízení. Obsahuje :

- definici funkcí a architekturu (technické řešení) systému,
- analýzu **příčin** vedoucích k hazardním stavům,
- určení požadavků na integritu bezpečnosti (SIL a četnost hazardů) pro jednotlivé podsystémy,
- určení spolehlivostních požadavků na zařízení.

Analýza příčin hazardních stavů určí, na úrovni fyzického zařízení, která zařízení (či jeho části) se na příčinách hazardů podílí a tedy jaké úrovně integrity bezpečnosti musí to které zařízení dosahovat.



Obr. 18-2

18.1.3 Příklad

Jako příklad uvádíme nástin analýz, provedených pro přejezdové zabezpečovací zařízení (PZZ). Vybíráme z celkové množiny jen jednu funkci, jeden hazardní stav, jen některé příčiny jeho vzniku atd.

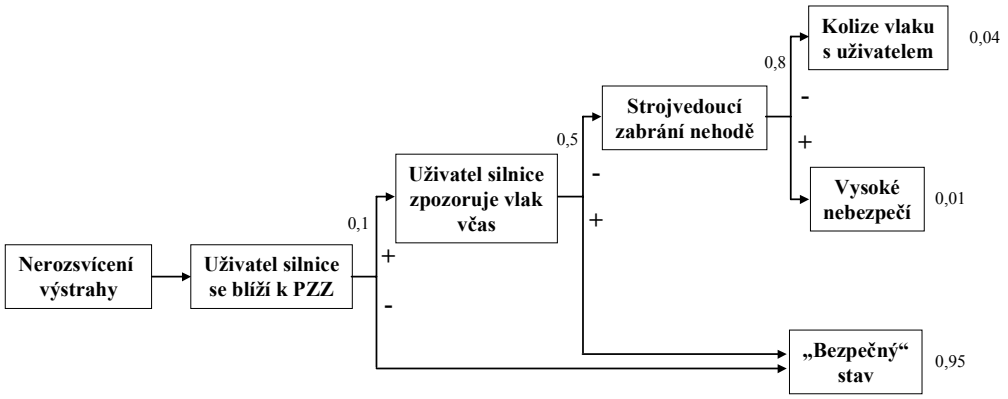
Systém:
PZZ

Interface :
1. PZZ → uživatel silnice
2. PZZ → strojvedoucí

Funkce :
1. spuštění výstrahy
2. ...
3. ....

Identifikace hazardních stavů (seznam):
1. nerozsvícení výstrahy na výstražníku
2. ....
3. ....

Analýza následku hazardního stavu ad 1.:
Redukční faktory a pravděpodobnost fatální nehody je pouze odhadnuta, ale teoreticky, u solidní dráhy, je možné ji určit ze statistik. Jak patrno z obr. 18-3, lze do úvah zahrnout i takové faktory jako je frekvence na přejezdu (0,1), rozhledové poměry (0,5) atd.



Obr. 18-3

Číslo (k)	Nehoda (A_k)	Redukční faktor rizika (C_1^k)	Pravděpodobnost fatální nehody (F_1^k)
1	Kolize vlaku s uživatelem	0,04	0,2
2	Vysoké nebezpečí	0,01	0,01

Tab. 18-1

Analýza příčin hazardního stavu ad 1:

1. pozdní nebo zcela chybějící detekce přiblížení vlaku,
2. ...
3. porucha vstupu řadiče logických funkcí,
4. porucha řadiče logických funkcí,
5. porucha výstupu z řadiče,
6. ....
7. porucha napájení,
8. ...
9. přejezdník neukazuje návěst „Otevřený přejezd“,
10. ...
11. vlak nerespektoval přejezdník s návěstí „Otevřený přejezd“.

Tolerovatelná četnost hazardního stavu :
Předpokládáme, že je stanoven bezpečnostní cíl, že z titulu poruchy automatického přejezdového zařízení může na přejezdu být fatálně ohrožen jeden ze 100 000 uživatelů za rok (převzato z Railtrack´s Railway Group Safety Plan - 1997/1998).
Abychom se dostali na „široce akceptovatelné hodnoty“, vezmeme v úvahu ještě bezpečnostní faktor 10, takže cílové individuální riziko pro uživatele (TIR – target individual risk) musí být menší než 10^{-6} za rok.
Předpokládejme dále, že uživatel silnice přejíždí přejezd 1000x za rok. Předpokládáme, že hazardní stav – pokud se vyskytne – trvá 10h, tj. výrazně déle než je expoziční doba uživatele na přejezdu a proto expoziční dobu zanedbáme.
Individuální riziko fatální nehody (IRF), vyplývající ze zkoumaných hazardů, musí být menší než cílové individuální riziko (TIR):

$$\mathbf{IRF} \leq \mathbf{TIR}$$

Individuální riziko, jemuž bude uživatel silnice na přejezdu vystaven vlivem hazardního stavu přejezdového zařízení ad 1., lze vyjádřit:

$$\mathbf{IRF_1} = \mathbf{N_1}\left[\mathbf{HR_1} \times \left(\mathbf{D_1} + \mathbf{E_1}\right) \sum_{\mathbf{nehody A_k}} \mathbf{C_1^k} \times \mathbf{F_1^k}\right]$$

kde N_1 ..... počet vystavení uživatele riziku za jednotku času (např. za rok),
HR_1..... četnost hazardního stavu za tutéž jednotku času,
D_1..... délka trvání hazardu za tutéž jednotku času,
E_1 ..... expoziční doba pro uživatele za tutéž jednotku času,
ostatní viz tab. 1. .... ke každému typu nehody A_k lze přiřadit postupem naznačeným na obr. 2 určitou pravděpodobnost, že k ní dojde (C_j^k) a určitou pravděpodobnost (F_j^k), že při ní dojde k fatálním následkům (totéž jde ovšem udělat s rozdělením např. na úmrtí, těžké ublížení na zdraví, lehké ublížení na zdraví).

Pro respektování většího počtu hazardních stavů je třeba ještě úprava výše uvedeného vztahu sumací:

$$\mathbf{IRF_j} = \sum_{\mathbf{hazardy H_j}} \mathbf{N_j}\left[\mathbf{HR_j} \times \left(\mathbf{D_j} + \mathbf{E_j}\right) \sum_{\mathbf{nehody A_k}} \mathbf{C_j^k} \times \mathbf{F_j^k}\right]$$

Po dosazení konkrétních hodnot (doba exposice účastníka byla zanedbána, protože doba trvání hazardního stavu je o několik řádů delší) dostaneme vztah, z něhož je možné určit limitní hodnotu četnosti hazardního stavu HR_1, při níž bude ještě dosaženo v předu uvedených cílů.

$$\mathbf{IRF_1} = \mathbf{N_1}\left[\mathbf{HR_1} \times \mathbf{D_1} \times \left(\mathbf{C_1^k} \times \mathbf{F_1^k}\right)\right] = \mathbf{1000} \times \mathbf{HR_1} \times \mathbf{10} \times \left(\mathbf{0{,}04} \times \mathbf{0{,}2} + \mathbf{0{,}01} \times \mathbf{0{,}01}\right) \leq \mathbf{10^{-6}}$$

$$\mathbf{HR_1} \leq \mathbf{1{,}25} \cdot \mathbf{10^{-8}\,h^{-1}}$$

Odtud tedy plyne, že tolerovatelná četnost hazardního stavu THR (za předpokladu, že žádné jiné hazardní stavy k fatálnímu ohrožení účastníka již nevedou) může pro splnění výše uvedeného cíle být až

$$\mathbf{THR = HR_1 \approx 1{,}25 \cdot 10^{-8} h^{-1}}$$

což by odpovídalo jednomu tolerovatelnému hazardu na jednom PZZ za 9000 let. Po stránce kvantitativního ukazatele by pro realizaci této funkce vyhovělo (za předpokladu, že neexistuje jiný než v příkladu zpracovaný hazard) zařízení SIL3 (viz dále).

Alokace požadavků na integritu pro systém / subsystém / element:
Z rozboru příčin hazardů se určí, jakým dílem se na hazardu v té které funkci ta která část zařízení podílí a jakou úroveň bezpečnosti musí zajišťovat, aby bylo dosaženo v předu uvedeného cíle.

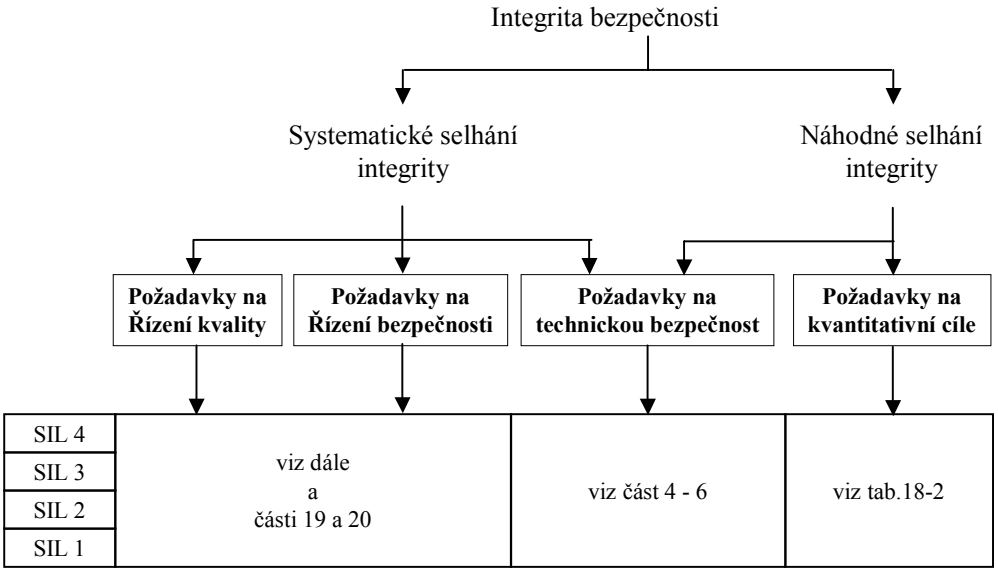
18.2 Úroveň integrity bezpečnosti

Úroveň integrity bezpečnosti (Safety Integrity Levels – SIL) se dělí podle normy ENV 50129 do čtyř kategorií – úroveň 4 (SIL 4) je nejvyšší, úroveň 1 (SIL 1) je nejnižší. Pokud se objevuje úroveň SIL 0, značí to, že se jedná o zařízení na které nejsou kladeny žádné bezpečnostní požadavky (ve smyslu zabezpečovací techniky).

Proto, aby jisté zařízení mohlo být zařazeno do odpovídající úrovně bezpečnosti SIL, musí vyhovovat všem faktorům, kterými jsou:

- naplnění podmínek řízené kvality,
- naplnění podmínek řízené bezpečnosti,
- splnění požadavků na technickou bezpečnost,
- dosažení kvantitativního bezpečnostního cíle.

Jak patrno, splnění kvantitativního ukazatele samo o sobě neznamená, že bylo dosaženo odpovídající úrovně bezpečnosti. To platí ovšem i naopak – splnění tří předchozích podmínek (řízení kvality, řízení bezpečnosti a technické bezpečnosti) nezaručuje, že bylo dosaženo kvantitativních cílů a nelze tedy tvrdit, že zařízení lze zařadit do odpovídající skupiny SIL (viz obr. 18-4).



Obr. 18-4

Žádná z norem CENELEC nepředepisuje, které zařízení musí být jaké úrovně. Toto určení je ponecháno na provozovateli, resp. regulátorovi, vyplyne ale také z dříve uvedených analýz rizik a hazardů. Nelze vyloučit, že v budoucnu bude předepsáno předpisy pro interoperabilitu mezi jednotlivými dráhami (TSI) či normami pro jednotlivé typy zařízení (pokud nějaké budou).

18.2.1 Řízení kvality

Požadavky na Řízení kvality jsou shrnuty v normách řady ISO 9000 a je nezbytné jim věnovat pozornost ve všech fázích vzniku a životnosti zařízení – týkají se jak vývoje, projekce, výroby, montáže tak i údržby. Zabezpečovací zařízení se v těchto otázkách neliší od jiných automatizačních zařízení metodikou, leč naléhavostí jejich pečlivé aplikace.

18.2.2 Řízení bezpečnosti

Požadavky na Řízení bezpečnosti (viz též části 19 a 20) představují souhrn převážně administrativních opatření a to opět jak v průběhu vývoje, tak ve všech dalších etapách životnosti zařízení. Mají umožnit vyhnout se (pokud možno) určitému druhu systematických poruch resp. včas odhalit nepředpokládaný výskyt jak systematických, tak náhodných poruch. Opatření se liší pro různé úrovně požadované bezpečnosti SIL, pro různé fáze vzniku a životnosti zařízení a jsou velmi závislá na konkrétních podmínkách aplikace. Nejdůležitější a všeobecně platná pro zařízení SIL3 a SIL4 jsou uvedená dále, pro zařízení SIL1 a SIL2 jsou tato opatření jen poněkud mírnější (v současné době nám není známa dráha, která by pro hlavní zabezpečovací systémy a jeho běžné části požadovala zařízení jiné úrovně než úrovně SIL3 a SIL4).

Plánování bezpečnosti

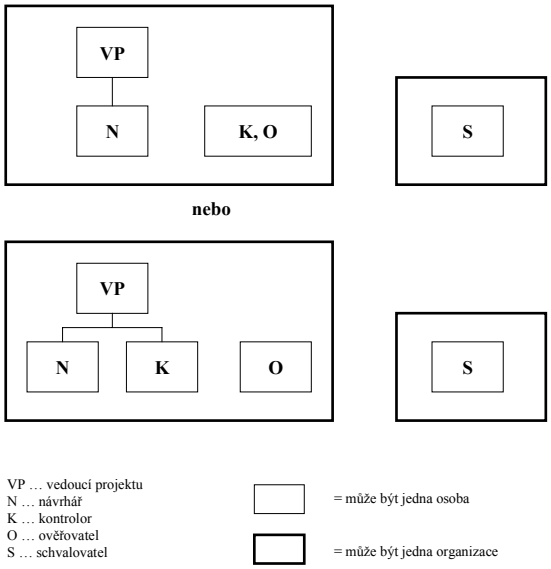
Toto základní opatření zavádí do projektu elementární pořádek a zajišťuje, že žádná aktivita důležitá z hlediska bezpečnosti systému nebude opominuta. Zahrnuje zejména :

- seznam aktivit pro zajištění bezpečnosti zařízení, které je třeba v rámci vývoje nového zařízení provést,
- plán kontrol dílčích úkolů,
- průběžnou kontrolu veškeré dokumentace,
- určení postupu a kontroly veškerých změn, ke kterým v průběhu prací dochází, tak, aby bylo zajištěno, že změny budou promítnuty do všech částí, na které mohou mít vliv,
- založení záznamníku hazardních stavů, který bude udržován po celou dobu vývoje a životnosti zařízení,
- revizi plánu bezpečnosti po každé etapě prací.

Organizace

Během přípravy plánu bezpečnosti musí být určena odpovídající organizace řízení bezpečnosti. Zde je nutno pamatovat zejména na:

- určení kompetentních (tj. osobní kompetence, technické znalosti, kvalifikace, zkušenosti) osob pro jednotlivé úlohy,
- zajištění příslušného výcviku personálu (vývojového, servisního i provozního – u prvně jmenovaných se týká zejména osob, nemajících vlastní zkušenosti se zabezpečovacími aplikacemi popř. s novým typem zařízení, u posledně jmenovaných jde zejména o opakovaný výcvik nebo opakované přezkušování znalostí jako podmínky kvalifikace pro výkon dopravní či údržbářské služby),
- zajištění příslušného stupně nezávislosti návrhářů, ověřovatelů, schvalovatelů (viz obr. 18-5).



Obr. 18-5

Specifikace systémových požadavků

Výsledkem úvodních etap vývoje (definice systému, analýza rizik, koncepce, aplikační podmínky atd.) je vypracování základních technických požadavků na systém, kde se při jejich tvorbě důrazně doporučuje (viz také [12], část 18.1):

- separace bezpečnostně relevantních systémů od ostatních, dobře definovaný interface mezi nimi,
- podrobná analýza interface,
- grafický popis systému včetně např. blokových diagramů,
- strukturovaná specifikace, s hierarchickým uspořádáním, pokud možno za použití formálních nebo počítačově podporovaných specifikačních nástrojů s automatickou prověrkou konzistence,
- postupné zpřesňování směrem k funkční úrovni, popis všech objektů a jejich vztahu ke společné databázi a opět pokud možno automatické prověrky konzistence,
- důkladná prověrka specifikací.

Vývoj

V průběhu vývoje jsou základními opatřeními této povahy :

- systematické, hierarchisticky strukturované vedení vývoje. Vyžaduje-li to povaha úkolu, musí být rozdělen do příslušných dílčích částí (modularizace), s přesně definovanými (psanými) vnitřními specifikacemi, definovanými testy atd.,
- pro každou část i celek musí být v průběhu vývoje vedena jasná a srozumitelná dokumentace, popisující funkční vlastnosti, působení poruch, průběh zkoušek, nutná opatření (technologická i jiná) pro výrobu, aplikaci, údržbu atd., k nimž se během vývoje došlo,
- již od počátku vývoje musí být vedena dokumentace, popisující systém (případně subsystémy a včetně grafického vyjádření), rozhraní, prostředí, změny, dokumentaci pro výrobu, aplikaci (projekční), údržbu. Tato dokumentace je v průběhu vývoje zpřesňována a doplňována,
- soustavná kontrola, ověřování a testování systému (subsystému) v každé etapě. Pro dílčí etapy vývoje je důležité kontrolovat a testovat, že jsou splněny požadavky (funkční a bezpečnostní) podrobně definované v předchozí etapě. Pro zařízení jako celek je důležité ověřovat a testovat, že zařízení splňuje ZTP (opět jak funkční, tak bezpečnostní požadavky). K tomu se provádí :
  - simulace,
  - funkční testy – úplné testy lze provést pouze na základě předem přesně definovaných případů pro demonstraci požadovaných charakteristických vlastností (funkčních, bezpečnostních),

- funkční testy pod vlivem prostředí (teplota, EMC, chvění, napájení atd.) – měly by se provádět i orientované na bezpečnostní požadavky a v širších rozmezích než se vyskytují ve skutečném provozním prostředí,
- výpočty četnosti poruch – pro tento účel by měly být provedeny pro nejhorší možné případy,
- kontrola veškeré průvodní dokumentace,
- ověření, že skutečná výroba, montáž, přezkušování, provoz a údržba probíhá (nebo bude probíhat) za splnění případných předpokladů z etapy vývoje a že tedy nedojde k narušení bezpečných vlastností zařízení vlivem pozdějších etap,
- pokud budou navrhovány testovací systémy, měl by být návrhář takových systémů nezávislý na návrháři zařízení,
- spolehlivá demonstrace vhodnosti zařízení pro použití by měla probíhat v reálných provozních podmínkách, měla by představovat cca 1 milion provozních hodin, přinejmenším však dvouletou zkušenost s více zařízeními, při minimu změn v průběhu ověřovacích provozů [7].

Následné etapy

Pro etapy výroby, aplikace (projektování), montáže, přezkušování, provozu a údržby jsou důležitým opatřením perfektně zpracovaná dokumentace (návody) s přihlédnutím k minimalizaci možnosti vzniku chyb z nesprávného pochopení, chybějících údajů atd.

18.2.3 Technická bezpečnost

Při vlastním vývoji a během další životnosti zařízení je samozřejmě třeba plně respektovat všechny požadavky na zajištění technické bezpečnosti. Základní principy jsou uvedeny v části 4 a 6.

Jmenovitě je normou EN 50129 vyloučeno použít v zařízeních SIL3 a SIL4 jednoduchých (jednokanálových) elektronických struktur, které nejsou orientovány na vnitřní bezpečnost nebo nemají význaky reaktivních systémů a dále primitivní duální systémy bez patřičné komparace a následných funkcí – tedy struktur nevyhovujících na první pohled požadavkům na technickou bezpečnost.

I při splnění všech požadavků na technickou bezpečnost je však důležité nezapomínat na další technická opatření, která dostatečně respektují zejména :

- provozní prostředí :
  - přizpůsobení podmínkám (teplota, EMC, chvění atd.), přičemž by mělo být i ověřeno, zda nejsou nutná zvláštní opatření - např. bezpečné odepnutí při přehřátí atd.,
- rozhraní mezi vlastním zařízením a okolím :
  - směrem k obsluze – obsluha by měla být tak jednoduchá, jak je možné, aby se omezilo riziko chyb,
  - k údržbě – údržbě by zařízení mělo poskytovat jednoduché ale dostatečné informace pro opravy a nemělo by vyžadovat cyklické bezpečnostně relevantní úkony,
  - k napájení - opatření proti ztrátě, kolísání (podpětí i přepětí), možnému zvlnění napájecího napětí atd.,
  - k řízeným prvkům – zejména naléhavá jsou opatření proti zavlečenému přepětí v případě vnějších prvků,
  - k jiným zařízením – zejména spolupráce s jiným zařízením při bezpečnostně relevantních funkcích může být značně komplikovaná, protože vedle funkčního přizpůsobení mohou vznikat problémy v oblasti poruchových stavů, detekce poruchy, reakce při poruše atd.,
- a další vedlejší, ale důležité okolnosti :
  - modularizace – používání snadno pochopitelných modulů limitovaných rozměrů, funkčně izolovaných (HW i SW),
  - dostatečná registrace stavu zařízení pro případ nehodových událostí, ale i komplikovaných poruch,
  - využívání možností on-line dynamického testování pro ověřování řádné funkčnosti zařízení a automatické odepínání porouchaných částí,

- monitorování časové a logické posloupnosti běhu programu v řadě kontrolních bodů programu a opět automatické odepínaní při poruše,
- specifikování případných požadavků na výrobu, montáž, přezkoušení, provoz, údržbu – tedy požadavků na následné etapy života zařízení

18.2.4 Kvantitativní ukazatel

Kvantitativní ukazatele jsou shrnuty v následující tabulce :

Tab. 18-2

Úroveň integrity bezpečnosti SIL	**Tolerovatelná četnost hazardu THR [za hodinu a funkci]**
4	$10^{-9} \leq THR < 10^{-8}$
3	$10^{-8} \leq THR < 10^{-7}$
2	$10^{-7} \leq THR < 10^{-6}$
1	$10^{-6} \leq THR < 10^{-5}$

(Funkce, jejichž kvantitativní požadavky by převyšovaly hranici 10^{-9} - která se zdánlivě nelogicky objevuje u SIL4, vyžadují podle normy EN 50129 zvláštní technická nebo provozní opatření pro dosažení tak mimořádného bezpečnostního cíle.)

19 VÝVOJ

Již několikrát bylo zdůrazněno, že problémy zabezpečovacích zařízení je nezbytné vidět vždy ve všech souvislostech. To plně platí pro vývoj nového systému, kde již od úvodních rozvah je třeba pamatovat na to, že kromě samozřejmých funkčních požadavků a požadavků na bezpečnost a spolehlivost, musí systém vyhovovat i z hlediska výroby, aplikovatelnosti v různých specifických situacích, obsluhy, údržby - systém musí vyhovovat ve všech fázích své životnosti. Aby se žádné aspekty neopomenuly, je důležité zajistit řádné vedení jeho vývoje. Vedení projektu bezpečných systémů se podstatně neliší od vedení jiných složitých projektů a mohou se použít obdobné nástroje řízení. Při řešení je však třeba počítat s vyšším stupněm opakování prací (neúspěšná dílčí řešení), s určitým zvětšením experimentálních prací, případně větším počtem prototypů a zejména s důkladnou odbornou kontrolou kritických činností. Důležité je vyhradit dostatečný čas pro zpracování rozborů bezpečnosti a závěrečnou revizi bezpečnosti, protože může zabrat podstatnou část celé doby řešení. V průběhu celého vývoje je nutné pamatovat na potřebné podklady pro schvalovací řízení a shromažďovat všechny výsledky prací, využitelné i pro tuto konečnou etapu. Pokud se řádné, až puntičkářské vedení vývoje zanedbá, zvyšuje se pravděpodobnost, že i při sebepečlivějším dodatečném ověřování bezpečnosti systému po ukončení vývoje dojde k opomenutí nějaké významné okolnosti. Je proto důležité, aby se v klíčových místech vývoje prováděly i formální revize a aby se v každé etapě vývoje přezkušovala shoda návrhu se zadáním. Každá etapa vývoje musí být řádně dokumentovaná a podepsaná osobou odpovědnou za přípravu dokumentu a osobou odpovědnou za její ověření. Totéž platí o všech změnách. Je nezbytné, aby všechny změny byly uvedeny ve všech dotčených dokumentech, aby se zajistilo, že byl vyšetřen jejich vliv na systém jako celek a že navrhovaný systém i nadále plně odpovídá zadání.

Otázkám zajištění bezpečnosti a vysoké pohotovosti (spolehlivosti) nového systému je třeba věnovat vysokou pozornost již od úvodních etap vývoje. K tomu je u většiny projektů účelné zpracovat programy řízení jakosti (quality management) a programy řízení bezpečnosti (safety management). Oba je třeba rozpracovat hned na počátku řešení a postupně je v následujících etapách prohlubovat. Musí brát v úvahu celý cyklus životnosti zařízení a musí se zabývat koordinovaně všemi aspekty zařízení (hardware i software). Hlavním smyslem obou je zajistit minimalizaci lidských chyb a tak vlastně redukovat riziko systematických chyb.

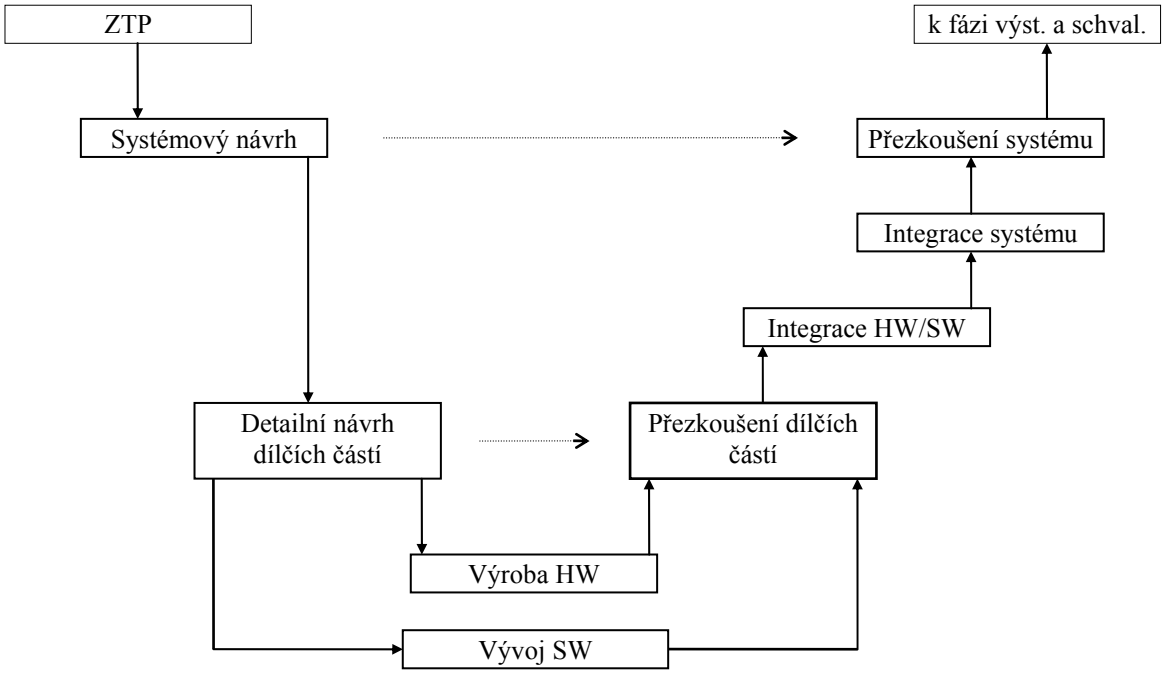
Program řízení jakosti koresponduje s problematikou řešenou v normách ISO série 9000. Program řízení bezpečnosti má obdobnou strukturu a zabývá se zejména :

- organizací vývojového procesu z hlediska zajištění koncepční bezpečnosti a bezpečnosti konstrukce, tj. určením jednotlivých úkolů a pro ně kompetentních osob,
- bezpečnostními požadavky na celý systém, jednotlivé podsystémy a funkční celky, které vyplynou z analýz a identifikací rizikových stavů,
- postupným zpřesňováním a konkretizací obecných požadavků na bezpečnost,
- zajištěním vazby mezi hardware a software při návrhu systému, jednotlivých podsystémů a funkčních celků,
- vedením Záznamníku hazardů (hazard log, safety log), kde jsou obsaženy všechny aktivity řízení bezpečnosti, identifikované hazardní stavy, provedená rozhodnutí, přijatá řešení atd.,
- zajištěním dílčího prověření bezpečnostních aspektů v určitých fázích vývoje a to včetně ověření jinou osobou než autorem řešení,
- zajištěním prověření bezpečnostních aspektů při jakýchkoliv změnách v zařízení ať již během vývoje nebo v pozdějších etapách životnosti zařízení,
- programem přezkušování, testování a bezpečnostních analýz (podle dříve určených bezpečnostních požadavků) funkčních celků, podsystémů a nakonec celého systému v příslušných etapách vývoje,
- zajištěním bezpečnosti v provozu a při údržbě, tj. zajištěním případných podpůrných systémů (diagnostika, sledování bezpečnosti atd.) pro provoz a údržbu tak, aby nebyla ohrožena bezpečnost ani v pozdějších etapách životnosti zařízení.

Protože zodpovědnost za provozování zabezpečovacího systému leží také na provozovateli (v našem případě ČD), je logické jeho významné postavení při schvalování zařízení do provozu. Cena vývoje dnešních zařízení, podstatně sofistikovanějších než v minulosti, je velmi vysoká, a proto je nutné přijmout taková opatření, která by minimalizovala riziko, že zařízení nebude v koncové etapě vývoje schváleno. Proto

se dnes i u renomovaných světových výrobců uplatňuje podstatně užší spolupráce výrobce a provozovatele a to již od úvodních etap vývoje nového zabezpečovacího systému. Zvláště důležitý je takový postup v případech, kdy se použije nových technologií nebo se výrazně bude měnit obsluha, provoz nebo údržba zařízení. Je proto třeba dbát na dostatečnou komunikaci v patřičných etapách vývoje.

V následujícím jsou uvedeny klíčové vývojové etapy tak, jak po sobě logicky následují (obr. 19-1). Před vlastním rozhodnutím o zahájení vývoje nového systému může ještě předcházet (a u zásadních projektů obvykle předchází) studie proveditelnosti (feasibility study). Jejím obsahem by měla být i analýza, která by dokládala kde a jak může nové zařízení redukovat bezpečnostní rizika a kvantifikace nákladů a přínosů.



Obr. 19-1

19.1 Základní technické požadavky

Definování základních technických požadavků (ZTP) je počáteční etapou návrhu a vývoje systému. Musí tvořit základ, z kterého se celý vývoj odvozuje. Musí obsahovat přesný popis požadovaných funkcí, prostředí a všech softwarových a hardwarových požadavků. V zásadě musí ZTP důkladně a jednoznačně popisovat co se musí udělat, ale ne jak se to udělá. Způsob provedení se uvádí pouze v případě, že určité provedení je závazné nebo naopak nepřijatelné. Chování systému by mělo být specifikováno pro všechny okolnosti - musí se brát ohled na všechny možné kombinace vstupních proměnných, na poruchy zařízení a poruchy napájení. Musí definovat dovolený rozsah kolísání parametrů a vstupních a výstupních proměnných. Zpracování ZTP, zejména částí týkajících se funkčních a bezpečnostních požadavků, je třeba věnovat maximální pozornost. Jejich struktura a vyjádření musí být takové, aby umožnily odpovědné prověřování správnosti a úplnosti. Důležité je volit pro ZTP formu dostupnou i pro laiky v oboru zabezpečovací techniky a elektrotechniky, protože k některým částem se musí vyjadřovat také pracovníci jiných odvětví (doprava, lokomotivní hospodářství atd.).

ZTP pro zabezpečovací systémy může přímo zpracovat budoucí odběratel jako technickou objednávku na vývoj nového zařízení. Je však obvyklé, že odběratel zpracuje nanejvýš základní požadavky a podrobné ZTP navrhne dodavatel. V každém případě by se v počáteční etapě vývoje nového zařízení mělo dospět k oboustranně odsouhlasenému návrhu ZTP. Při schvalování ZTP by měla být pozornost zaměřena především na správnost, kompletnost, přesnost a konzistenci požadavků, se zvláštním zaměřením na bezpečnostní aspekty. U zcela nových systémů (např. založených na nové technologii) je také obvyklé, že se ZTP i v pozdějších stadiích vývoje rozsáhle upřesňují a odběratelem (i dodavatelem) znovu schvalují. Na tento postup je nutné již v počátcích pamatovat a zahrnout ho do příslušných smluv.

Obsah ZTP

Úvod

Tato část by měla poskytnout ve všeobecných termínech popis celého systému, do kterého musí konkrétní specifikovaný systém zapadnout a důvody pro předložení navrhovaného systému.

Všeobecný popis

Tato část by měla poskytnout popis funkce zamýšleného systému, všeobecný způsob činnosti a vnější interface.

Způsob činnosti

Smyslem této části je poskytnout detailnější popis jak systém funguje v normálním stavu a při poruše.

Aplikace systému

Tato část by měla zahrnovat zamýšlené způsoby a postupy, které budou používány pro úpravu HW, přípravu dat a jejich ověření, postup instalace systému a vložení software pro adresnou aplikaci.

Bezpečnostní principy a požadavky

Tato část by měla zahrnovat základní bezpečnostní principy, které provozovatel musí zajistit při normálním provozu, právě tak jako činnosti, které je nutné provést v případě, že jsou detekovány nebo se objeví chyby, včetně činností pro obnovení normální funkce systému po přerušení.

Rozhraní

Tato část by měla popsat všechny okolnosti týkající se interface mezi částmi systému, vnějškem a obsluhou.

Fyzikální prostředí

Tato část by měla definovat podmínky okolního prostředí (např. rozsahy teplot a vlhkostí, vibrace, elektromagnetické prostředí), napájení (kolísání napětí a frekvence, interferenční úrovně atd.), normy ochran před nebezpečným dotykem, dovolený vliv systému na okolní prostředí, požadavky na uzemnění a ukolejnění.

Údržba a spolehlivost

Tato část by měla určit způsoby údržby, požadovanou životnost systému a dobu, po kterou budou výměnné části dostupné.

Jestliže budou zabudovány diagnostické a záznamové prostředky, mělo by být společně s chybovými hlášeními specifikováno, které budou určeny obsluze a které údržbě. Kromě textu zpráv by měly být určeny události, které je budou generovat.

Požadavky na údržbu software sahají od pravidelných změn dat nedotýkajících se bezpečnosti (např. změny jízdního řádu) po modifikace týkající se bezpečnosti. Musí být jasně popsány metody pro modifikaci dat a software. Je nezbytné rozlišit změny, které tvoří součást normálních provozních podmínek a nesmí tedy mít vliv na bezpečnost, od změn, které mají vliv na integritu bezpečné databáze (např. implementace změny rozmístění zabezpečovacích zařízení v systémem řízené oblasti) a proto vyžadují nové ověření a schválení správnosti všech dat.

Požadavky na údržbu hardware sahají od potřeby náhrady vadné součástky až po změnu stávajícího systému hardware, vyplývající z přidání nebo odstranění kolejí, výhybek a návěstidel ze zabezpečovacího zařízení. Měl by být uveden jasný popis postupu náhrady a opravy součásti s vědomím, že průkaz bezpečnosti může

být založen na nějakých (fyzikálních) vlastnostech těchto součástí. Popis by měl zahrnovat i testy, které je třeba po opravě nebo náhradě provést, aby se neznehodnotil průkaz bezpečnosti.

Dále by měly být uvedeny údaje o úrovni výcviku udržovacího personálu a doby zákroku. Tyto okolnosti mohou mít vliv na návrh prostředků pro údržbu, dobu opravy a pohotovost systému.

Dokument by také měl stanovovat minimální provozní spolehlivost částí systému, včetně střední doby mezi poruchami, střední dobu opravy a očekávanou pohotovost systému.

Software omezení

Tato část by měla zahrnovat seznam norem, které mají být aplikovány na software, pokrývající specifikaci, dokumentaci, kódování a testování. Mělo by být požadováno, aby software byl připraven řádným strukturovaným způsobem a aby se dokumentace přizpůsobila vnitřní, národní nebo mezinárodní normě.

Hardware omezení

Dodavateli mohou být uložena jistá omezení pro zajištění kompatibility s existujícím systémem (např. provedení jednotné nákupní politiky pro zařízení zpracovávající informace). Jestliže je třeba zkonstruovat a vyrobit zařízení, je možné, aby byl dodán seznam součástek známých jako spolehlivé (doporučené) nebo nevyhovující (vyloučené).

Měly by být specifikovány rozměry, váha, upevnění a způsoby spojení různých článků zařízení.

V bezpečném systému musí být analyzována funkce každého subsystému a měl by být předem určen jeho příspěvek k celkové bezpečnosti systému.

Pro výrobce může být předepsáno splnění norem z oblasti řízení kvality, aby se zajistilo, že osoby zaměstnané při výrobě jsou vhodně kvalifikované, s ohledem na spolehlivost. Ale toto řešení má možné nevýhody v omezení počtu dodavatelů schopných splnit specifikaci.

Vývoj systému

Tato část by měla popsat způsoby a nástroje, které budou použity při vývoji systému.

Dokumentace

Je nezbytné definovat požadovanou dokumentaci, obsah a formu každého dokumentu, způsob jakým se připravuje a údaje, které je třeba připravit a doložit pro schválení. Jasnou a úplnou dokumentaci je nutné zpracovávat současně s návrhem systému. Je prostředkem, kterým různí účastníci v průběhu návrhu komunikují a kterým se předává zodpovědnost z jedné etapy do druhé, umožňuje kontrolu průběžných etap.

Program práce

Program práce by měl jasně formulovat různé etapy vývoje, výroby a dodávky systému, včetně cílů, určit postup schvalování, časový program a zodpovědnost. Tato část by také měla definovat zamýšlené pracovní vztahy s dodavatelem (např. pravidelná setkání, školení personálu, dodávky součástek).

19.2 Systémový návrh

Smyslem systémového návrhu je převedení ZTP do technických řešení, tedy odpověď na otázku jak. U složitějších systémů je obvykle účelné rozdělení celé funkce na řadu funkcí dílčích. Smysl má i separace funkcí podílejících se na bezpečnosti od funkcí obecných, bez zvláštních požadavků na bezpečnost. Předejde se tak použití zbytečně složitých postupů pro funkce, které to nevyžadují. Dále se systémově řeší rozvržení funkcí mezi hardware a software, rozdělení do funkčních bloků, definují se jejich rozhraní a stanoví se vzájemné informační toky. Také tato rozhodnutí budou mít vliv na cenu, spolehlivost, udržovatelnost i prokazatelnost splnění bezpečnostních aspektů. Proto se jako součást etapy dále prohlubují programy řízení bezpečnosti a kvality.

Nezbytné je zajistit stejný přístup a stejné posuzování problémů bezpečnosti a spolehlivosti jak na straně dodavatele tak na straně provozovatele, resp. příštího schvalovatele vhodnosti zařízení k provozu na železnici. Protože názory na tyto otázky při použití nových technologií nemohou být ani zdaleka ustáleny (natož aby byly normovány), musí dodavatel v této fázi komunikovat s budoucím provozovatelem

(schvalovatelem) tak, aby bylo dosaženo shody. I k tomu účelu slouží rozpracovávané programy řízení kvality a bezpečnosti. Pokud je to potřebné, zpracovává se zvláštní materiál věnovaný koncepci bezpečnosti. Je zaměřen speciálně na řešení technických aspektů funkční a technické bezpečnosti systému. Projednání těchto materiálů a dosažení konsensu mezi dodavatelem a provozovatelem (schvalovatelem) je u nových technologií zatím jediný způsob, kterým je možné minimalizovat riziko vysokých ztrát, vzniklých z pokračování vývoje vlivem nedorozumění směrem, který by byl pro provozovatele nepřijatelný.

Při návrhu je třeba dbát na průhlednost celého řešení. Praxí je plně ověřeno, že jednodušší řešení bývají bezpečnější. V každém případě lze u jednoduššího systému snáze prokázat bezpečnost. Příliš složité systémy, s neprůhlednými vazbami pro bezpečnost, je nutné striktně odmítat.

Souhrnně lze říci, že výsledkem této etapy by měla být schválená architektura systému a koncepce bezpečnosti systému.

19.3 Detailní návrh

V dalších etapách následuje stále podrobnější propracovávání návrhu dílčích částí systému, včetně zpracování dílčích rozborů bezpečnosti. Práce na jednotlivých částech mohou probíhat do značné míry paralelně. Musí být však uplatněno velmi přísné řízení celého projektu, aby bylo dosaženo potřebné koordinace prací. I k tomu slouží programy řízení kvality a bezpečnosti.

19.4 Integrace

Po dokončení detailních návrhů jednotlivých částí následuje integrační etapa, v níž se z jednotlivých dokončených částí sestavují větší celky, ověřují se návaznosti, provádí se funkční zkoušky stále větších celků a doplňují se rozbory bezpečnosti až je dokončena integrace celého systému (viz obr. 18-1). Pokud některá ze zkoušek nebyla úspěšná, je třeba se skokem vrátit do etapy návrhu.

19.5 Přezkoušení

V různých etapách vývoje nového zařízení se na jednotlivých modulech zařízení provádí důkladné testy. Jedná se obvykle o řadu testů, orientovaných obvykle samostatně na :

- testy technické bezpečnosti a
- testy funkční bezpečnosti.

Po úspěšném ukončení integrační etapy následuje etapa podrobného zkoušení celého systému. Jejím výsledkem je komplexní zkouška systému (zjišťující soulad specifikace a skutečného provedení, včetně vlivu prostředí) a definitivní průkaz bezpečnosti systému. V této etapě je zvláště důležité, aby přezkoušení autorem návrhu bylo doplněno pokud možno nezávislou kontrolou. I to by mělo být náplní programu řízení bezpečnosti a kvality.

19.6 Aplikace

Přizpůsobení obecného systému adresné aplikaci musí být řešeno tak, aby nebylo třeba opakovat celý schvalovací proces pro každou aplikaci. Je vhodné zařízení rozdělit na část neměnnou (hardware i software), která by mohla být schvalována pouze jednou, a část (pokud možno jen soubor dat), která adaptuje zařízení pro určitý typ aplikace. Projektování pak bude spočívat jen v definici struktury aplikačně

závislých dat, s použitím vhodného formálního zápisu. Musí být také zajištěno, že adresná aplikace nemůže pracovat s neodpovídajícími aplikačními daty.

Projektování takového systému se neobejde bez adekvátních prostředků, pravděpodobně založených opět na výpočetní technice. Tyto projekční systémy však musí odpovídat podobným bezpečnostním požadavkům, jako samotný zabezpečovací systém a také musí být stejnou procedurou schváleny (nejlépe již jako součást schvalovacího procesu nového systému). Výrobce by měl být schopen projekční systém na objednávku dodat.

Po naprojektování a výrobě zařízení pro konkrétní aplikaci by měl ještě ve výrobním závodě následovat tzv. factory test. Jde o testy vnitřní části zařízení, prováděné před dodávkou zařízení k montáži pro ověření shody konkrétní aplikace se schváleným typem a pro ověření specifických projektovaných vlastností konkrétní aplikace. Vnější zařízení je při zkouškách simulováno, přičemž je nutné věnovat pozornost věrohodnosti simulace (reálnost časování reakcí vnějších zařízení, možné poruchy a odchylky od normální činnosti atd.).

Smyslem těchto testů je co nejdůkladněji ověřit v relativně klidných podmínkách (nezatížených vlivy železničního provozu), že vlastnosti zařízení odpovídají projektu (a tedy i požadavkům odběratele - proto je vhodné, aby se jich, alespoň při závěrečném testování, po odstranění všech chyb, zúčastnili odpovědní zástupci odběratele) a to zejména z hlediska funkční bezpečnosti. Testy se zásadně provádějí úplné v pozitivním smyslu (tj. zjištění, že určitou činnost je možné vykonat při splnění všech požadovaných podmínek), tak negativním smyslu (tj. zjištění, že určitou činnost není možné vykonat při nesplnění kterékoliv z požadovaných podmínek) a také zjišťují, že v zařízení nejsou zabudována nadbytečná omezení.

Celkové pojetí této kategorie testů musí být zaměřeno tak, aby umožnilo minimalizovat zkoušky po instalaci zařízení do reálných podmínek.

19.7 Software

Za současného stavu žádná technika programování nezajišťuje absolutně bezpečnost. Není známa cesta, jak ve složitých programech zajistit, aby byly s jistotou bezchybné. Problémy jsou zejména v oblasti systematických chyb. Aby se minimalizovaly, je při návrhu programů, které mohou mít vliv na bezpečnost, nezbytné využívat následující principy (kromě jiného):

- systematický přístup shora-dolů,
- modularitu,
- verifikaci v každé fázi vývoje programu,
- verifikaci modulů a modulových knihoven,
- jasnou prověřitelnou dokumentaci,
- validační zkoušky.

Při tvorbě architektury software je třeba vzít v úvahu následující možnosti:

1. defensivní programování, což umožňuje detekovat neobvyklé toky dat a neobvyklá data,
2. detekci chyb a diagnostiku, tj. postupy založené na redundanci, diverzitě a komparaci nebo na detailním diagnostikování,
3. detekční kódy pro detekci chyb u zvláště závažných informací (Hammingovy kódy, cyklické kódy, polynomiální kódy),
4. asertivní programování, což je založeno na ověřování podmínek před provedením určité sekvence a po jejím provedení,
5. diverzitní programování, kdy je funkce provedena n-krát odlišným způsobem výsledky jsou porovnány. N-verzí může běžet paralelně na zvláštním hardware nebo postupně na témže hardware,
6. memorování (memorising executed cases), kdy je předem pořízen záznam povolených běhů programu a běžném provozu je prováděná operace porovnána se souborem možných běhů,
7. analýza působení chyb software, analýza poruchového stromu, obdoby analýz hardware pro určení hazardních stavů a jejich následků.

Ověřenými a tedy doporučenými jsou kombinace metod 1, 5 a jedna z 3, 4, 6; 1, 3 a 4; 1, 3 a 6; 1, 2 a 3;1, 3 a jedna ze 6, 7.

Při návrhu a vývoji software je třeba vzít v úvahu následující techniky (opatření):

1. formální metody (např. CCS, CSP, HOL, LOTOS, OBJ, Temporal Logic, VDM a Z), tj. vývoj software způsobem, který je založen na matematice a může pak být podroben matematickým analýzám konzistence a nesprávností (CCS a CSP - prostředky pro popis chování systému v konkurenčním komunikačním procesu; HOL, LOTOS, OBJ - formální jazyky pro specifikaci a ověřování systémů; Temporal Logic - přímé vyjádření bezpečnostních a provozních požadavků a formální demonstrace, že tyto náležitosti jsou obsaženy v určitém vývojovém kroku; VDM, Z - matematicky orientované techniky pro etapu specifikací s využitím v etapě návrhu a implementace),
2. semi-formální metody (logické diagramy, sekvenční diagramy, diagramy toku dat, finite state machines, state transition diagramy, časové Petriho sítě, rozhodovací a pravdivostní tabulky,
3. strukturované metodologie (JSD, MASCOT, SADT, SDL, SSADM a Yourdon), jde v zásadě o pomůcky v myšlení - chápání a rozdělení problému,
4. modulární přístup, tj. dělba systému na menší srozumitelné celky, zahrnuje několik pravidel: modul musí mít jednoduchou a dobře definovatelnou funkci, spojení mezi moduly musí být přesně definováno a vymezeno, podprogramy musí mít pouze jeden vstup a jeden výstup (s omezeným počtem parametrů - obvykle max. 5), moduly musí komunikovat s ostatními moduly přes interface, globální a společné proměnné musí být zvlášť dobře organizovány s řízeným přístupem atd.,
5. normy návrhu a kódování, pro zajištění jednotnosti dokumentace a převedení programů do strojového kódu musí obdobné práce na systému dodržovat stejná pravidla, stejný jazyk, vyloučení některých jazykových konstrukcí atd. To je důležité i z hlediska ověřování, schvalování a údržby,
6. analyzovatelné programy, tj. striktní vyloučení všech „krkolomností“ v programech, jednoduchá větvení a rozhodování ve smyčkách na základě jednoznačně stanovených parametrů atd.,
7. vhodné programovací jazyky, které se vyznačují přísně organizovanou strukturou (ADA, MODULA-2, PASCAL, FORTRAN 77). Za současného stavu techniky se zejména nedoporučují jazyky typu C, PL/M, BASIC,
8. jazykové podsoubory, tj. stanovení omezených jazykových prostředků - vyloučí se ty prostředky, které jsou náchylné k chybám, nebo které jsou obtížně analyzovatelné a pracuje se pouze s omezeným podsouborem,
9. certifikované nástroje a kompilátory, tj. používání jen jazykových verzí, které mají certifikované (nezávisle ověřené) i nástroje (tools) a kompilátory a jsou ověřeny v mnoha jiných projektech. Je to důležité i když je v současné době známo, že ne všechny části mohou být ověřeny tak, aby bylo možné vyloučit bezchybnost
10. knihovna ověřených modulů a částí.

Při ověřování a zkouškách software je třeba vzít v úvahu následující techniky:

1. formalizovaný průkaz, tj. použití teoretických a matematických modelů pro prokázání korektnosti programu bez jeho provádění. Prokazuje se, že program prochází vstupními a výstupními podmínkami v souladu s požadovanými logickými funkcemi a že vždy regulérně skončí. Opět lze využít formálních metod CCS, CSP, HOL, LOTOS, OBJ, Temporal Logic, VDM a Z,
2. statickou analýzu, která zahrnuje analýzu hraničních hodnot (kdy se ověřuje funkce při extrémních hodnotách, které mohou vstupy nabývat; zvláštní pozornost vyžaduje nula, prázdný ASCII znak, prázdný zásobník, nebo chybějící položka v seznamu, nulová matice, nulový vstup tabulky atd.), analýzu řídících toků, analýzu toku dat, formální audit dokumentace, symbolické provedení atd.,
3. dynamickou analýzu a testování, která zahrnuje skutečné provedení analýzy hraničních hodnot, modelování výkonnosti (tj. provádějí se testy zaměřené na potvrzení dostatečnosti systému - např. rychlosti odezvy - pro nejhorší případ), kompletní simulaci (ověřování za všech stavů vstupů a porovnání výstupů s očekávanými), simulace s omezeným počtem variant atd.

Ověřenými a tedy doporučenými jsou kombinace metod 1 a 3; 2 a 3.

19.8 Vedení dokumentace

Dokumentace je nejen nejdůležitějším prostředkem komunikace mezi týmy během vývoje, ale i prostředkem komunikace směrem ven - k provozovateli, schvalovateli atd. Proto celý návrh zabezpečovacího systému musí být neustále doprovázen kvalitní, řádně vedenou dokumentací. Většinou ji tvoří pět hlavních skupin dokumentů, zabývajících se:

- strukturou systému (systémový návrh a koncepce bezpečnosti),
- hardwarem (podrobná dokumentace technických prostředků),

- softwarem (podrobná dokumentace programových prostředků),
- testy (dokumentace provedených zkoušek),
- projekcí, obsluhou a údržbou (podrobné pokyny, návody).

Dokumentace se při vývoji ve všech částech postupně doplňuje řadou technických dokumentů s přibývajícími podrobnostmi. Měla by uchovávat důvody všech klíčových rozhodnutí v etapě návrhu a podklady pro všechny předávané dokumenty.

Dokumentace principů a struktury systému

Tyto dokumenty jsou vlastně další úrovní vnitřních specifikací. Obsahují schéma systému, ukazující dělení do podsystémů a logické spojení mezi funkčními moduly. Určují dělení mezi software a hardware. Doporučuje se, aby dokumenty popisující logiku zpracování byly vyjádřeny přísně matematickými vzorci (formální specifikace). Ověření kompletnosti této interní specifikace a její konzistence se ZTP je jedním z hlavních kroků etapy přezkoušení.

Dokumentace týkající se hardware

První úroveň hardwarové dokumentace se skládá z hardwarové specifikace, která uvádí funkce zajišťované hardwarem a požadovanou úroveň provedení.

Podrobnější dokumentace popisuje vybranou hardwarovou strukturu a jak jsou splněny podmínky prostředí. Zahrnuje obvodová schémata, nákresy mechanické konstrukce, výsledky obvodových výpočtů, použité normy a prostředky řízení kvality.

Dokumentace týkající se software

Tato dokumentace zahrnuje :
- softwarovou specifikaci, makroskopický překlad funkční specifikace do softwarových termínů,
- strukturální softwarovou specifikaci, která musí poskytnout úplné detaily :
    - rozběhu a inicializace,
    - synchronizace redundantních modulů,
    - způsobu, který zajišťuje, že redundantní moduly pracují se stejnými daty,
    - řízení přerušení, pokud je nezbytné,
    - dobu zpracování,
    - problémy zpracování v reálném čase a saturace,
    - mechanizmus zotavení po poruše,
    - řízení interface,
    - aktualizaci proměnných a dat,
- výpis zdrojových programů,
- slovník proměnných, dat a adresových způsobů,
- detaily použitého jazyku.

Dokumentace testů

Dokumentace musí zahrnovat výsledky a metody analýz, prováděných pro ohodnocení spolehlivosti, pohotovosti a bezpečnosti systému, právě tak jako výsledky funkčních testů.

Dokumentace pro obsluhu a údržbu

Tato dokumentace se skládá z instrukcí pro provoz a údržbu a zahrnuje:
- návody k obsluze,
- význam výstrah a diagnostiky,
- postupy při opravě systému zejména za provozu,
- nominální hodnoty a tolerance pro měření prováděná v různých testovacích bodech atd.

20 UZNÁNÍ A SCHVÁLENÍ BEZPEČNOSTI

Žádné zabezpečovací zařízení nelze použít v železničním provozu na místě, kde by mohlo nepříznivě ovlivnit bezpečnost dopravy, pokud nebylo příslušnými orgány schváleno jako zařízení odpovídajícím způsobem bezpečné pro zamýšlenou aplikaci. Smyslem schvalovacího procesu je tedy souhrnně ověřit a potvrdit odpovídající úroveň bezpečnosti, provozuschopnosti, kompatibility a interoperability zabezpečovacího zařízení ve vztahu k evropským a národním standardům (normy, doporučení UIC atd.).

Pro evropský prostor upravuje požadavky na uznání a schválení železničních zabezpečovacích zařízení norma CENELEC EN 50129 (v české verzi ČSN EN 50129) a normy související (zejména EN 50126, EN 50128, EN 50159-1, EN 50159-2). Normy ale nestanovují kdo má provádět práci v jednotlivých etapách schvalovacího procesu, ani se nezabývá otázkami zodpovědnosti.

Rozsah zodpovědnosti státu, provozovatele zařízení a dodavatele zařízení za bezpečný provoz (a tedy i za bezpečnost zabezpečovacích systémů) je dán (nebo by měl být jasně dán) zákonnými úpravami, z nichž by mělo být možné jednoznačně odvodit i rozdělení úloh, zodpovědnost a tedy i hloubku jednotlivých kroků schvalovacího procesu. V České republice tyto záležitosti v současné době upravuje zákon č. 266/1994 Sb. o drahách a prováděcí předpisy (zejména vyhláška č. 100/1995 Sb. „Řád určených technických zařízení“, vyhláška č. 101/1995 Sb. „Řád pro zdravotní a odbornou způsobilost osob při provozování dráhy a drážní dopravy“ a výnos MD „Podmínky pro určování právnických osob k provádění technických prohlídek a zkoušek UTZ podle §47, odst.4 zákona č. 266/1994 Sb., o drahách“ včetně přílohy 1), ale bohužel nikoliv dostatečně.

Jestliže má schvalovatel udělit souhlas k provozu nového zabezpečovacího zařízení (systému), musí být přesvědčen o tom, že zadané požadavky pro vývoj zařízení byly správné, že vývoj zařízení probíhal organizovaně a kvalifikovaně, že navrhovaný systém je z hlediska funkční a technické bezpečnosti na požadované úrovni, že příslušné testy na zařízení prokázaly vhodnost zařízení pro navržené použití a že byly vytvořeny předpoklady pro to, aby požadovaná bezpečnost byla zajištěna po celou dobu životního cyklu zařízení (systému). Vzhledem k významu zabezpečovacího zařízení pro bezpečnost železniční dopravy, nelze ke schvalování přistupovat jen jako k ryze správnímu (administrativnímu) úkonu, při kterém se pouze ověří existence a kladné závěry dokumentů předkládaných výrobcem. Mezi nepominutelné podmínky pro schválení zabezpečovacích systémů proto patří nezávislé hodnocení bezpečnosti systému (tzv. technické schválení) kompetentním a pro tuto problematiku kvalifikovaným schvalovatelem a ověření systému v provozních podmínkách.

Na schvalovacím procesu železničních zabezpečovacích zařízení se v různé míře a se specifickými úkoly podílí dodavatel, technický schvalovatel, provozovatel a státní správa. Pokud je to praktické, schvalují se nejen konkrétní adresné aplikace, ale odpovídajícím způsobem se schvalování aplikuje i na menší celky (funkční jednotky, prvky), které se opakovaně vyskytují v různých systémech a na celé typové systémy, které jsou pak opakovaně použity v konkrétních aplikacích. Schvalovací proces se pak může týkat tří odlišných případů:

- schválení typového výrobku (nezávisle na aplikaci), který bude používán v různých aplikacích,
- schválení typové aplikace, která bude opakovaně použita,
- schválení konkrétní adresné aplikace.

Je zřejmé, že schvalování typové aplikace se pak může (v případě, že se nezměnily podmínky) pouze odvolat na schválení typového výrobku a obdobně schválení adresné aplikace se odvolá na schválení typové aplikace. Pokud ovšem došlo při konkrétní aplikaci ke změně podmínek, předpokládaných při schválení typového výrobku, nebo k aplikaci nad rámec schválené typové aplikace, je nutné nové schválení, které nové okolnosti bude reflektovat.

Schvalování nového zařízení by ale mělo jen omezený účinek, pokud by se návazně u takto již schválených zařízení neověřovalo, že zařízení je skutečně provozováno ve stavu v jakém bylo schváleno a v souladu se všemi stanovenými podmínkami. Proto je ke shora uvedeným případům nutno obecně přidat

- ověření způsobilosti provozovaného zařízení.

20.1 Průvodní dokumentace

Pro celkové schválení zabezpečovacího systému (zařízení) musí být předloženy následující dokumenty:

- specifikace požadavků na systém (System Requirements Specification) včetně požadavků na bezpečnost (Safety Requirements Specification),
- důkaz bezpečnosti systému (Safety Case),
- zpráva o nezávislém hodnocení bezpečnosti (technické schválení) (Independent Safety Assessment),
- zpráva o výsledku provozního ověření (Safety Qualification Tests).

Tyto dokumenty předkládá ke schválení dodavatel (výrobce, dovozce) a jejich účelem je schvalovatelům doložit, že vývoj, výroba, instalace, provoz a údržba zařízení proběhly nebo budou moci probíhat organizovaně a kvalitně, že zařízení splňuje veškeré jím uvedené požadavky a že má pro všechny etapy života zamýšlené aplikace za všech okolností odpovídajícím způsobem bezpečné chování.

Obsah dokumentace podrobně určuje EN 50129. Specifikace požadavků deklaruje, kterým požadavkům platných norem a případných dalších ujednání zařízení vyhovuje. Důkaz bezpečnosti (Safety Case) systému tvoří přísně strukturovaný, závazný, systematicky zpracovaný materiál, který v podstatě postupně vzniká během vývoje systému, jako nedílná součást technického řešení. Jeho hlavními částmi jsou :

- definice systému - definuje systém na který se důkaz vztahuje, včetně čísel verzí či modifikací,
- zpráva o řízení jakosti (Quality Management Report) - dokladuje řízení jakosti po celou dobu života zařízení,
- zpráva o řízení bezpečnosti (Safety Management Report) - dokladuje konzistentnost procesu řízení bezpečnosti po celou dobu života zařízení s procesem řízení RAMS v EN 50126,
- technická zpráva o bezpečnosti (Technical Safety Report) - doklady k funkční a technické bezpečnosti systému,
- související důkazy bezpečnosti - odkazy na důkazy bezpečnosti již schválených subsystémů nebo zařízení, přičemž dokladuje, splnění tam uvedených podmínek nebo zahrnutí do systémových podmínek,
- závěr - shrnutí předchozího a hlavní argumenty dokládající, že systém je pro specifikované podmínky odpovídajícím způsobem bezpečný.

Skutečný obsah všech uváděných dokumentů se řídí podle konkrétního výrobku, jeho závažnosti pro bezpečnost provozu, složitosti, podmínek použití atd. Části všech dokumentů mohou být nahrazeny přesnými odkazy na přesně určené, jinde uvedené a dostupné závazné podklady.

20.2 Technické schválení

Smyslem technického schválení je odborně posoudit, zda předložené zařízení odpovídá požadovaným a výrobcem deklarovaným vlastnostem zejména v oblasti funkční bezpečnosti, technické bezpečnosti a provozuschopnosti a zda tyto vlastnosti nejsou v rozporu s jinými platnými závaznými dokumenty (normy, mezinárodní ujednání atd.). Technické schválení proto musí provádět na výrobci nezávislý specializovaný technický orgán, s vlastní znalostí aplikace příslušné technologie v železniční zabezpečovací technice, s odpovídající železniční zkušeností a znalostí režimu práce systému v provozu. Dále by měl mít pracovní kontakty s více dodavateli, s obdobnými schvalovacími orgány v zahraničí a možnost trvale sledovat vývoj nových technologií doma i ve světě. Jeho nálezy musí být obecně uznávané jak dodavatelem, tak státní správou a budoucím provozovatelem. Organizací, pracovními procedurami a zodpovědností musí tento orgán dále vyhovovat všeobecným požadavkům EN 45 001, 45 011, 45 012 a po náběhu evropského železničního akreditačního systému bude muset být schváleným železničním certifikačním orgánem a notifikovanou osobou. Pokud by touto prací byly pověřovány i organizace nesplňující tyto požadavky, vedlo by to obecně k devalvaci úrovně této činnosti. Problémem je kdo a na základě čeho posoudí kompetentnost schvalovatele a jak se zajistí odolnost schvalovatele proti "cizím"

vlivům. „Tržní“ mechanizmy zde způsobí evidentně více škody než užitku. (V současné době v ČR poměrně dobře vyhovuje pouze pracoviště ZL 7 VÚŽ.)

Kromě dokumentace uvedené v odstavci 20.1 k technickému schválení dodavatel předkládá navíc :

- podrobnou dokumentaci HW a SW,
- vlastní zařízení nebo umožní k němu přístup pro zkoušení,
- se zařízením případně vyvinuté nástroje pro projekci a testování.

Při technickém schvalování je nezbytné posoudit úplnost a správnost dodavatelem předložených dokumentů a to jednak jejich analýzou a jednak vlastními testy zařízení. Ověřují se zejména (s přihlédnutím k EN 50129, EN 50128, EN 50159 a dalším normám):

- správnost, kompletnost, přesnost a konzistence specifikace požadavků se zvláštním zaměřením na funkční bezpečnost,
- systémový návrh (hardware i software - tzv. koncept bezpečnosti) - vhodnost zvolených principů s ohledem zejména na technickou bezpečnost a spolehlivost - zejména oddíl 1 a 2 technické zprávy o bezpečnosti,
- doklady prokazující bezpečné chování za bezporuchového i poruchového stavu (tzv. průkaz bezpečnosti) - zejména oddíly 3 a 5 technické zprávy o bezpečnosti,
- zkoušky systému provedené výrobcem během vývoje zařízení - dostatečnost zkoušek pro zajištění souladu specifikace a skutečného provedení a ověření vhodnosti pro použití (tj. schopnosti výrobku poskytovat dobré chování a výkon během životnosti výrobku, za specifikovaných provozních podmínek - prostředí, EMC atd.) - zejména oddíl 4 a 5 technické zprávy o bezpečnosti,
- systém jakosti - zejména část 2 důkazů bezpečnosti,
- systém bezpečnosti - zejména část 3 důkazů bezpečnosti,
- provedení a průběh provozního ověření.

Při obecně akceptovatelných časových a finančních nárocích na technické schválení není možné se při schvalování zabývat všemi detaily zařízení. Hlavní pozornost je třeba věnovat ověření metod práce dodavatele při vývoji systému a úplnosti dokladů bezpečnosti a detailně je možné posuzovat pouze některá vybraná kritická místa systému (jak z hlediska bezpečnosti, tak i spolehlivosti, resp. dostupnosti). Pokud v těchto případech nebudou zjištěny podstatné nedostatky, je možné technické schvalování uzavřít s pozitivním výsledkem. V opačném případě je nutné požadovat doplnění dokumentace, popř. změny v zařízení a posuzování prohloubit nebo schválení systému ve stávající podobě přímo odmítnout.

Kritickými a často opomíjenými místy jsou vazby mezi různými subsystémy (rozhraní), vazba mezi HW a SW, funkční a technická bezpečnost. Zejména u složitých projektů je vhodné (a často i nezbytné), když se na technickém schválení podílí více osob, případně i specializovaných na určité problémy (HW, SW, přenosový systém, MMI, funkční vlastnosti atd.), ale je nutné zajistit jejich dokonalou souhru prostřednictvím zodpovědného zpracovatele technického schválení.

Významná může být i volba okamžiku, kdy schvalovací proces začíná. Je možné, aby se schvalovatel zúčastňoval od začátku všech hlavních etap vývoje, práce sledoval a v rozhodujících místech se k nim vyjadřoval, či je přímo schvaloval. Vzhledem k možným změnám v průběhu procesu ovšem musí nakonec stejně provést zevrubnou celkovou revizi. Takový postup může být na objem práce schvalovatele náročnější, ale může zvýšit kvalitu vývojového procesu, redukovat potřebu dodatečných úprav a významně zkrátit dobu mezi dokončením vývojových prací a vydáním technického schválení. Schvalovatel si ovšem po celou dobu musí udržet od projektu odstup, nepodlehnout směru myšlení, jímž se projekt ubírá a nesmí se na vlastním vývoji přímo podílet. Nesmí problémy projektu řešit, ale musí se omezit na vyhledávání a prověřování kritických míst, upozorňování na to, co by mohlo být špatně, co bylo opomenuto atd. Jeho účast v projektu nesmí být důvodem pro omezení činností verifikátora či validátora.

Pokud se k technickému schválení přistupuje až po ukončení projektu, vyžaduje značný čas, než se schvalovatel s projektem seznámí natolik, aby mu dokonale porozuměl. I k tomu potřebuje úzkou spolupráci s pracovníky vývoje a to v ovzduší vzájemné důvěry a otevřenosti. Dodatečné odstraňování nedostatků je opět časově náročné a obvykle se obtížně hledají optimální řešení.

20.2.1 Ověření specifikace funkčních požadavků

V prvním kroku jde o ověření správnosti, kompletnosti, přesnosti a konzistence funkčních požadavků, na jejichž základě vývoj zařízení probíhal. Specifikace požadavků musí brát v úvahu zejména veškeré požadavky platných norem a dalších ujednání (mezinárodní pro zajištění interoperability systémů, specifické požadavky provozovatele atd.) a měla by být odsouhlasena provozovatelem, pokud jím přímo není vytvořena. Pokud pro danou kategorii zařízení existuje jiná schválená specifikace, posuzuje se, zda ve srovnání s ní nebyla některá část opomenuta, zda případná doplnění a změny nepříznivě nenarušily nebo neovlivnily původní smysl atd.

V druhém kroku jde o ověření způsobu převodu výše uvedených požadavků (obvykle záměrně zpracovaných volným jazykem, bez odborných údajů) na formální zápis, který byl výchozím technickým podkladem pro detailní návrh HW a SW (principiální schémata, algoritmy, rovnice, vývojové diagramy atd.).

Schvalovatel při této práci musí mít odpovídající železniční zkušenosti, zkušenosti z řešení dosavadních zařízení, dobré znalosti režimu práce výrobku v provozu atd. Nemusí mít podrobné znalosti o případně použitých nových technologií výrobku, ale při posuzování bere přiměřeně v úvahu veškeré existující schválené nebo připravované mezinárodní normy, národní normy, ZTP nebo jiné relevantní specifikace.

Tato ověření by neměla zůstat jen u ověřování intuitivního, ale měla by být prováděna za pomoci :

- formálních metod založených na matematice a matematických analýzách konzistence a nesprávností,
- semi-formálních metod (logické diagramy, sekvenční diagramy, diagramy toku dat, finite state machines, state transition diagramy, časové Petriho sítě, rozhodovací a pravdivostní tabulky atd.),
- strukturované metodologie - jde v zásadě o pomůcky v myšlení, chápání a rozdělení problému.

20.2.2 Ověření konceptu bezpečnosti

Jde o ověření systémového návrhu (hardware, software, spolupráce obou) a vhodnosti zvolených principů pro zajištění technické bezpečnosti. Důraz se, kromě bezpečnosti klade i na spolehlivost. Dále se ověřuje správnost určení rozsahu zařízení, které se podílí na zajištění bezpečnosti. Tato etapa schvalování je klíčovou prací a účastní se jí společně specialisté na HW i SW pod vedením zodpovědného zpracovatele technického schválení, který musí mít dobré znalosti s aplikací dané technologie v zabezpečovací technice. Pozornost se věnuje styku mezi HW a SW. Na závěr se stanoví rozsah prací a zodpovědnost při následném posuzování HW a SW, které již může probíhat odděleně.

20.2.3 Ověření průkazu bezpečnosti

Předmětem není ověření pravdivosti údajů v průkazu bezpečnosti - za ty plně zodpovídá dodavatel. Předmětem je především posouzení vhodnosti zvolené metody průkazu bezpečnosti a namátkové ověření úplnosti průkazu bezpečnosti, adekvátnosti opatření přijatých při jiných než pozitivních reakcích atd. Práce se zaměřuje spíše na celek než detail, protože to by znamenalo plně průkaz bezpečnosti zopakovat. Budou-li však zjištěny globální nedostatky, je třeba průkaz bezpečnosti (a tedy i zařízení) odmítnout jako celek.

20.2.4 Ověření zkoušek systému

Ověřuje se vhodnost, dostatečnost a průkaznost zkoušek, které dodavatel na systému provedl (včetně vlivu prostředí - teplota, EMC atd.). V případě potřeby je možné vyžadovat doplňující zkoušky. Namátkově, pro potvrzení uváděných zjištění, provádí schvalovatel zkoušky vlastní. Nezbytné jsou dokonalé znalosti o funkci obdobných zabezpečovacích zařízení a režimu jejich práce v provozu.

Kromě toho se podle konkrétního případu a možností provede vlastní ověření HW a SW.

20.2.4.1 Ověření HW

V případě HW se ověřuje konkrétní realizace konceptu bezpečnosti v klíčových místech zařízení a namátkově v dalších místech, která se na bezpečnosti podílí. K tomu jsou nezbytné dobré znalosti a vlastní zkušenosti s aplikací elektronických komponent v zabezpečovací technice.

20.2.4.2 Ověření SW

Tato část je nejkontroverznější částí technického schvalování. Lze ji provádět do úplných detailů a i pro konkrétní aplikace, nebo naopak spoléhat pouze na systémová opatření a komplexní funkční ověření - v tomto směru není u jednotlivých evropských železnic soulad. Minimálně se však ověřuje uplatnění následujících pravidel (EN 50128):

- modulární přístup, tj. dělba systému na menší srozumitelné celky. Tento přístup zahrnuje několik pravidel:
  - modul musí mít jednoduchou a dobře definovatelnou funkci,
  - spojení mezi moduly musí být přesně definováno a vymezeno,
  - podprogramy musí mít pouze jeden vstup a jeden výstup (s omezeným počtem parametrů - obvykle max. 5),
  - moduly musí komunikovat s ostatními moduly přes interface,
  - globální a společné proměnné musí být zvlášť dobře organizovány s řízeným přístupem atd.,
- logická dělba programů, včetně dělby na část:
  - obecnou (opakovaně a beze změny použitou u všech zařízení daného druhu),
  - typovou (opakovaně a beze změny použitou u všech zařízení daného typu),
  - aplikační (proměnnou s konkrétní aplikací),
- normy návrhu a kódování - pro zajištění jednotnosti dokumentace a převedení programů do strojového kódu musí obdobné práce na systému dodržovat stejná pravidla, stejný jazyk, vyloučení některých jazykových konstrukcí atd.,
- analyzovatelné programy, tj. striktní vyloučení všech „krkolomností“ v programech, jednoduchá větvení a rozhodování ve smyčkách na základě jednoznačně stanovených parametrů atd.,
- použití vhodných programovacích jazyků, které se vyznačují přísně organizovanou strukturou,
- jazykové podsoubory, tj. stanovení omezených jazykových prostředků - vyloučí se ty prostředky, které jsou náchylné k chybám, nebo které jsou obtížně analyzovatelné a pracuje se pouze s omezeným podsouborem,
- certifikované nástroje a kompilátory, tj. používání jen jazykových verzí, které mají certifikované (nezávisle ověřené) i nástroje (tools) a kompilátory a jsou ověřeny v mnoha jiných projektech. Je to důležité i když je v současné době známo, že ne všechny části mohou být ověřeny tak, aby bylo možné vyloučit bezchybnost,
- knihovna ověřených modulů a částí.

Pokud systémová opatření u SW (např. dva nezávislé programy) nevylučují vznik nebezpečné chyby při převodu ZTP do strojového kódu, bylo by nejsprávnější, ale také technicky nejnáročnější, zpětně převést pomocí nezávislých pracovníků konkrétní obsah pamětí do formy podobné vývojovému diagramu, kterou by bylo možné porovnat se zadanými ZTP. Tato oblast by zřejmě vyžadovala použití řady pomocných počítačových prostředků. Jejich vývoj, nezávislý na dodavatelích zabezpečovacích zařízení, by měl být předmětem seriozního výzkumu. Výhodou tohoto postupu bude, že pak převahu práce na hodnocení SW může vykonávat specialista v oblasti software, bez podrobných znalostí zabezpečovací techniky. Obecně se pro ověřování a zkoušky software doporučuje (EN 50 128) vzít v úvahu následující techniky:

1. formalizovaný průkaz, tj. použití teoretických a matematických modelů pro prokázání korektnosti programu bez jeho provádění. Prokazuje se, že program prochází vstupními a výstupními podmínkami v souladu s požadovanými logickými funkcemi a že vždy regulérně skončí. Opět lze využít formálních metod,
2. statickou analýzu, která zahrnuje analýzu hraničních hodnot (kdy se ověřuje funkce při extrémních hodnotách, které mohou vstupy nabývat; zvláštní pozornost vyžaduje nula, prázdný ASCII znak, prázdný zásobník, nebo chybějící položka v seznamu, nulová matice, nulový vstup tabulky atd.), analýzu řídících toků, analýzu toku dat, formální audit dokumentace, symbolické provedení atd.,
3. dynamickou analýzu a testování, která zahrnuje skutečné provedení analýzy hraničních hodnot, modelování výkonnosti (tj. provádějí se testy zaměřené na potvrzení dostatečnosti systému - např.

rychlosti odezvy - pro nejhorší případ), kompletní simulaci (ověřování za všech stavů vstupů a porovnání výstupů s očekávanými), simulace s omezeným počtem variant atd.

Ověřenými a tedy doporučenými jsou kombinace metod 1 a 3; 2 a 3.

20.2.5 Ověření dokladů o řízení jakosti a bezpečnosti

Ověřuje se kvalita průběhu vývojových etap a dostatečnost dokumentace pro zajištění systému jakosti a bezpečnosti v etapách života zařízení následujících po vývojové fázi, tj. zejména dokumentace pro projekci, montáž, zkoušení, sledování a údržbu zařízení.

20.2.6 Vyhodnocení provozního ověření

Hodnotí se průběh a dostatečnost provozního ověření a vyjádření budoucího provozovatele zařízení (obsluha i údržba) nejen k vlastnímu zařízení, ale i k dokumentaci předávané se zařízením.

20.2.7 Závěry technického schválení

Technické schválení probíhá obvykle ve dvou hlavních etapách - předběžné technické schválení a (konečné) technické schválení. Důvodem je nutnost zahrnout do celkového schválení i výsledky provozního ověření.

Dokument „Předběžné technické schválení“ slouží jako podklad pro zahájení provozního ověřování. V závislosti na postupu prací na technickém schválení a konkrétních okolnostech daného případu se do předběžného technického schválení formulují požadavky na přídavná opatření a omezení pro zajištění bezpečnosti a plynulosti provozu během provozního ověřování. Obvykle je účelné navrhnout provozní ověření rozdělené do několika etap, u kterých se postupně, na základě příznivého průběhu detailních ověřovacích prací a poznatků z ověřovacího provozu, zmírňují dočasná omezení či přídavná opatření. Pak je ovšem třeba také navrhnout předpoklady, za kterých se může přechod z jedné etapy provozního ověření do další uskutečnit. Na základě předběžného technického schválení a smlouvy s dodavatelem (nebo jeho žádosti o provozní ověření) vydá provozovatel souhlas k zahájení provozního ověření, ve kterém je stanoven rozsah, místo, doba trvání a případné jeho další podmínky pro ověřovací provoz.

Předběžné technické schválení nelze vydat, pokud v procesu technického schvalování nebyla úspěšně zakončeny alespoň etapy uvedené výše pod body 20.2.1 a 20.2.2 (ověření funkčních vlastností a konceptu bezpečnosti) a provedeny laboratorní a tovární testy nového zařízení.

Je nezbytné uvažovat s reálnými termíny pro konečné vyhodnocení provozního ověření, následné zpracování definitivního technického schválení a vydání průkazu způsobilosti pro trvalý provoz a pamatovat tak i na tuto část provozního ověřování.

Dokument „Technické schválení“ se vydává po úspěšném ukončení všech výše uvedených prací na technickém schválení, včetně úspěšného ukončení provozního ověření. Dokument slouží jako podklad pro schválení zařízení do trvalého provozu. Jasně definuje předmět schválení a rozsah, pro který schválení platí. Může obsahovat i trvalá omezení v užívání zařízení.

20.3 Provozní ověření

Před schválením musí být nově vyvinuté zařízení ověřeno ve skutečných provozních podmínkách, aby se ověřilo, že zařízení je skutečně schopné plnit provozní požadavky, v reálném provozním prostředí, s patřičnou úrovní bezporuchovosti a bezpečnosti. Kromě toho je to prakticky jediná příležitost pro ověření udržovatelnosti systému. Tyto zkoušky samozřejmě nemohou prokázat splnění všech uvedených vlastností absolutně - jsou také jen jednou částí schvalovacího procesu - ale mohou poskytnout určitý obraz o chování zařízení a napomoci ke zvýšení důvěry schvalovatele a provozovatele v nové zařízení. Kromě toho je institut provozního ověření prostředkem, jak umožnit uvedení nového zařízení do skutečného provozu před

konečným schválením (schvalovací paradox: zařízení nelze uvést do provozu bez schválení a schválit jej nelze bez provozního ověření).

Vzhledem k tomu, že při provozním ověření není ještě zařízení definitivně schváleno, není jeho bezpečné chování plně zajištěno a musí být tedy pro jeho provoz provedena určitá dodatečná bezpečnostní opatření. Ta, stejně jako doba a rozsah provozního ověření, se volí s ohledem na stupeň novosti a komplikovanosti systému. Způsob provozního ověření je, obvykle na návrh dodavatele, uveden v podmínkách předběžného technického schválení - viz dále - a vlastní povolení ověřovacího provozu (tj. souhlas s jejich dostatečností) musí vydat provozovatel.

20.4 Schválení typového výrobku, typové aplikace

Výrobky a systémy pro zabezpečovací zařízení se obvykle využívají v řadě konkrétních aplikací při zachování stejného jádra. Tedy typové výrobky a typové aplikace se přizpůsobují jen konkrétním podmínkám - např. kolejišti. Je proto výhodné schválit jednu typovou aplikaci a toto schválení využít v konkrétních aplikacích. Pokud je typová aplikace vhodně navržena, je možné její přizpůsobení konkrétním podmínkám např. pouze změnou aplikačního SW, bez zásahu do základních funkcí. Správnost aplikačního SW je pak možné poměrně jednoduše přezkoušet ověřením funkčních vlastností a není třeba opakovat ověření technické bezpečnosti, což je nejnáročnější část schvalovacího procesu. Z tohoto poznání se odvíjí způsob schvalování nových systémů pro kolejovou dopravu v ČR.

Schvalování typového výrobku (nezávisle na aplikaci), který bude používán v různých aplikacích, nebo schválení typové aplikace, která bude opakovaně použita, se obvykle odehrává v souvislosti s první stavbou, kde je nové zařízení použito. Má tři základní části:

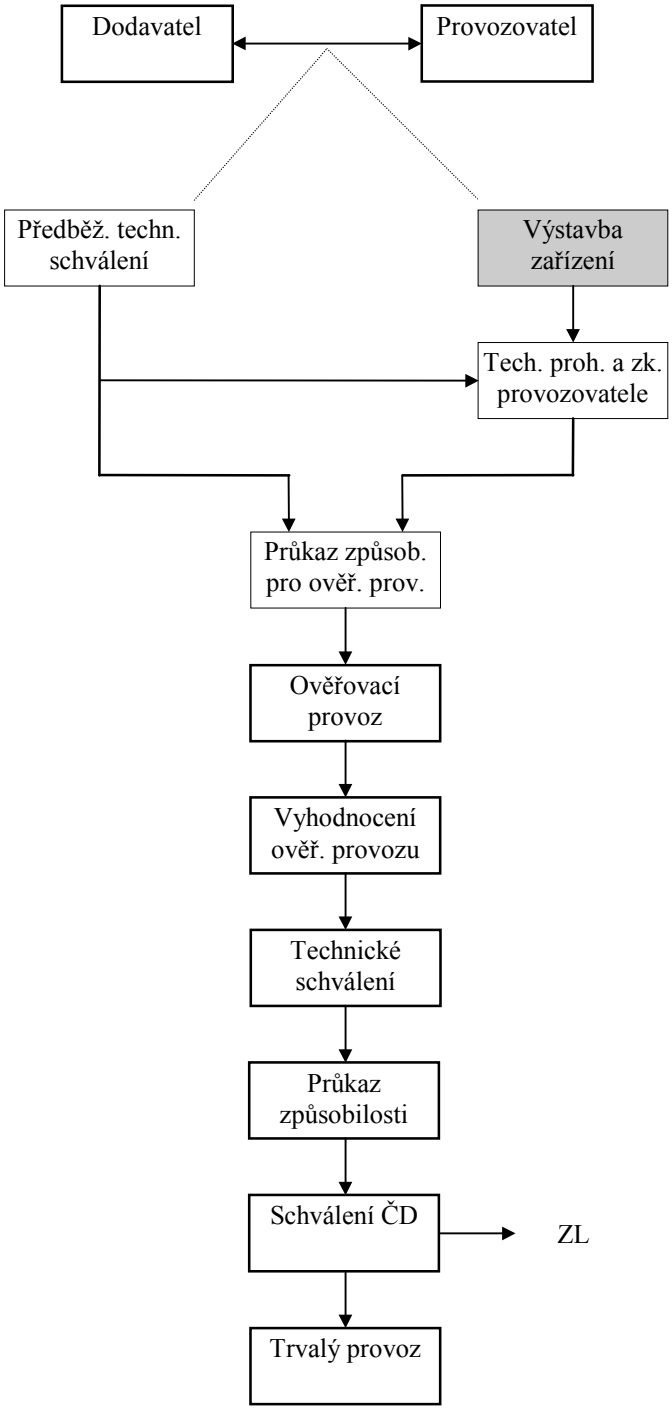
- technické schválení (safety assessment),
- schválení státní správou (safety approval),
- uznání bezpečnosti (schválení provozovatele - safety acceptance).

Smyslem schválení státní správou je výsledně potvrdit, na základě předložené dokumentace, technického schválení a provozního ověření, že výrobek či systém je možné, jako dostatečně bezpečný pro dané použití, převzít. Schválení může být závislé na splnění doplňujících podmínek, plynoucích z technického schválení. Státní správa (dnes reprezentována pro tuto záležitost v ČR Drážním úřadem) na základě tohoto procesu vydává průkazy způsobilosti - časově omezený průkaz způsobilosti na dobu ověřovacího provozu (na základě předběžného technického schválení) a po kladném závěrečném hodnocení provozního ověření (a na základě technického schválení) průkaz způsobilosti pro trvalý provoz na určenou dobu.

Smyslem schválení provozovatele je z typů schválených státní správou vybrat typy (všechny nebo jen některé) a potvrdit, že splňují požadavky provozovatele, které sice nemohou být méně přísné než požadavky státní správy, ale mohou být v některých směrech přísnější (např. provozní spolehlivost, vhodnost pro zavedený systém údržby, náklady na údržbu) nebo zohledňovat další hlediska (kompatibilita zařízení, jednotnost zařízení, harmonizace v rámci UIC atd.). Toto schválení vydává drážní orgán (railway authority), zodpovídající státní správě za bezpečný provoz zařízení. V podmínkách ČD schvalování provádí určený odborný útvar (ČD, O14) na základě technického schválení, průběhu provozního ověření a případných dalších doplňujících zkoušek o nichž si sám rozhodne. O kladném ukončení schvalovacího procesu provozovatel informuje zaváděcím listem. Schválit pro provoz u ČD může ve své vlastní kompetenci i ta zařízení, která schválení státní správou nepodléhají (nemají vliv na bezpečnost provozu).

Schválení nového výrobku obvykle iniciuje dodavatel (výrobce), který chce svůj výrobek u provozovatele uplatnit. Vhodným prostředkem pro dohodnutí všech potřebných náležitostí je obchodní smlouva mezi dodavatelem a provozovatelem pro dodávku a realizaci 1. stavby nového systému. Zjednodušené organizační schéma procesu schválení první stavby nového systému je na obr.20-1.

Provozovatel, tj. železniční podnik, může sám s časovým odstupem vyvolat opakování schvalovacího řízení. Smyslem může být ověření, zda rozhodující vlastnosti výrobku zůstávají zachovány po celou dobu životnosti zařízení, ověření kvality výroby v dalších sériích, vyjasnění pochybností při odhalení nových závažných poruch či náhlém nárůstu poruch atd.

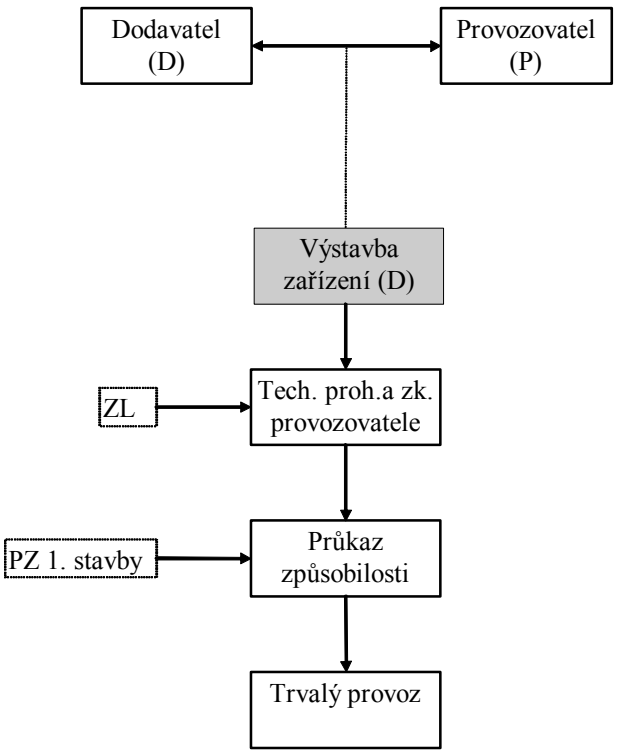

Dodavatel
Provozovatel
Předběž. techn. schválení
Výstavba zařízení
Tech. proh. a zk. provozovatele
Průkaz způsob. pro ověř. prov.
Ověřovací provoz
Vyhodnocení ověř. provozu
Technické schválení
Průkaz způsobilosti
Schválení ČD
ZL
Trvalý provoz

Obr. 20-1

20.5 Schválení adresné aplikace

Pokud konkrétní aplikace vychází ze schválené typové aplikace, nepřekračuje rozsah schváleného typu, ani se nemění požadavky na systém, je možné schvalovací proces výrazně zjednodušit. Zjednodušené organizační schéma schvalovacího procesu při opakované stavbě je na obr.20-2. Při uvádění nové stavby do provozu vystaví DÚ průkaz způsobilosti pro zařízení když:

- půjde o zařízení schváleného typu (tj. při některé z předchozích staveb již úspěšně proběhl schvalovací proces)
- je deklarována shodnost zařízení se schváleným typem a
- u zařízení byla s kladným výsledkem provedena technická prohlídka a zkouška právnickou osobou určenou MD.



Obr. 20-2

20.6 Zkoušky zařízení před uvedením do provozu

U těchto zkoušek nejde v zásadě o rozdílný postup, ať jde o zkoušky nového systému nebo zkoušku opakovaně nasazovaného adresného systému. Rozdíl je však v hloubce a důkladnosti zkoušek, což může mít vliv na jejich trvání. Teoreticky zde lze odlišit :

- testy dodavatele po instalaci zařízení do provozních podmínek - jde o testy dodavatele na závěr montáže zařízení do skutečného prostředí. Pokud byl zodpovědně proveden factory test a nebyly prováděny změny při stavbě, je nejdůležitější částí tohoto testu nastavení všech periferií a kontrola správnosti jejich připojení (možnost záměny periferií!),
- technickou prohlídku a zkoušku právnickou osobou - pro vydání Průkazu způsobilosti státní správou,
- zkoušky provozovatele.

Protože jsou však tyto testy a zkoušky obvykle spojeny s přepínáním starého zařízení na zařízení nové (jen mimořádně probíhá stavba „na zelené louce“), je minimálně v závěrečné etapě nutné je všechny sloučit do jediné a provádět je společně, s ohledem i na další úkoly spojené s kolaudačním procesem a to vše ještě s ohledem na bezpečnost probíhající dopravy. To vyžaduje mimořádně náročnou spolupráci všech zúčastněných. Proto je důležitá přesná a podrobná příprava, která bere v potaz jak příslušné návody dodavatele, tak příslušné předpisy provozovatele.

20.7 Ověřování způsobilosti provozovaného zařízení

Zabezpečovací zařízení nelze provozovat bez platného průkazu způsobilosti. Průkaz způsobilosti, vydávaný státní správou, je platný u zabezpečovacích zařízení obvykle 5 let. Po této době je třeba průkaz způsobilosti prodloužit. K tomu je nutné provést příslušné prohlídky a zkoušky, předepsané státní správou. Další závazné prohlídky a zkoušky určují předpisy ČD a pokyny pro údržbu zařízení, které dodává výrobce.

20.8 Vzájemné uznání schválení

Náklady na vývoj a schválení bezpečnosti nových zabezpečovacích systémů vedou ke snaze jak výrobců tak provozovatelů o vývoj kompatibilních systémů na základě společných norem. Norma EN 50 129 vytvořila předpoklady pro stejné posuzování bezpečnosti zabezpečovacích systémů a za předpokladu nadnárodního dohledu nad kvalitou schvalovacího procesu v jednotlivých státech by bylo možné přebírat výsledky schvalovacího procesu i z jiného státu (cross-acceptance). Problémem zůstaly doposud nesjednocené požadavky funkční. To vyvolává potřebu přizpůsobení každého zařízení místním podmínkám a tedy zásah do systému, který nálezy původního schválení může negovat.

Přesto, pokud má být schvalován již u jiného provozovatele do provozu zavedený systém (výrobek) schválený věrohodným orgánem, může se v určitém rozsahu k původnímu schválení přihlédnout a zjednodušit tak proces vlastního schválení. Pro uznání však musí být k dispozici kromě shora uvedených podkladů pro technické schválení ještě:

- doklad o původním schválení,
- závěry původního technického schválení,
- definice výchozích bezpečnostních požadavků uvažovaných při schvalovacím řízení, popřípadě jen jejich odlišností od mezinárodně normalizovaných principů,
- definice pole působnosti, pro které původní schválení výrobku platí (podmínky použití),
- reference o původním technickém schvalovateli,
- seznam změn, k nimž při aplikaci do nového prostředí došlo,
- doplňující důkaz bezpečnosti, podchycující změny na zařízení a vztah k původnímu důkazu bezpečnosti.

Na základě těchto údajů rozhodne zpracovatel technického schválení (po případné konzultaci s původním a budoucím provozovatelem) o rozsahu převzetí předchozího technického schválení, o doplňujících zkouškách nebo o plném opakování technického schvalování. Provozní ověření musí proběhnout vždy.

20.9 Po schválení bezpečnosti

Po schválení zařízení a uvedení do trvalého provozu, musí provozovatel použít postupy, podpůrné systémy a monitorování funkce v souladu s oddílem 5 technické zprávy o bezpečnosti systému. Jen tak bude zachována bezpečnost systému i v následujících etapách života zařízení.

Jakákoliv zamýšlená změna (SW i HW) ve schváleném systému (zařízení) podléhá v zásadě novému schvalovacímu řízení. Veškerá příslušná dokumentace, včetně důkazu bezpečnosti musí být aktualizována nebo doplněna přídavnou dokumentací a předložena technickému schvalovateli k posouzení, v

jakém rozsahu a jakým postupem bude třeba zařízení znovu schválit. V případě drobných změn ve funkčních vlastnostech zařízení, které nemohou mít negativní vliv na bezpečnost ani způsobilost zařízení pro dané použití, může schvalovatel potvrdit platnost původního technického schválení a navrhne podmínky provozního ověření. Po kladném vyhodnocení provozního ověření se nová verze doplní do existujícího schválení. V ostatních případech bude po teoretickém (popř. i laboratorním) prozkoumání změn vydáno nové PTS s určením místa, délky a ochranných opatření provozního ověření. Po kladném ukončení provozního ověření bude vydáno nové TS.

21 LITERATURA

Průřezové knihy

[1] Boda M.: Zabezpečování dopravy vlakové na železnicích. Česká matice technická, Praha 1905.

[2] Nechvátal Th.: Telegrafní, telefonní, návěstní a zabezpečovací zařízení u státních drah, Praha 1923.

[3] Machytka V.: Zabezpečování vlakové dopravy na československých drahách. Kober, Praha 1938.

[4] Hlásný L.: Zabezpečování vlakové dopravy na železnicích. Technický průvodce X. Česká matice technická, Praha 1948.

[5] Chudáček V., Poupě O.: Zabezpečovací technika v železniční dopravě I. díl. NADAS, Praha 1970.

[6] Chudáček V., Poupě O.: Zabezpečovací technika v železniční dopravě II. díl. NADAS, Praha 1972.

[7] Poupě O. a kol.: Zabezpečovací technika v železniční dopravě II. díl. NADAS, Praha 1990.

Významné monografie

[11] Halavanja P.: Elektrická stavědla ČSD. Knihovna železničních příruček, 1949.

[12] Chudáček V.: Zabezpečení přejezdů. SNTL, Praha 1953.

[13] Poupě O.: Automatický blok a liniový vlakový zabezpečovač (autostop). Dopravní nakladatelství, Praha 1960.

[14] Suchánek J.: Vlakové bodové zabezpečovače (autostopy) pro ČSD. Dopravní nakladatelství, Praha 1960.

[15] Viktorin J.: Ochrana úložných kabelů před korozí způsobovanou elektrickou trakcí. Dopravní nakladatelství, Praha 1960.

[16] Matis B., Uhlík A., Vedral V.: Reléový poloautomatický blok. NADAS, Praha 1963.

[17] Koblasa K.: Reléové staniční zabezpečovací zařízení. Část I. Konstrukce a díly. NADAS, Praha 1963.

[18] Pešťál M., Petřík V.: Výstražná světelná zařízení typu VÚD. NADAS, Praha 1964.

[19] Koblasa K., Kulle K.: Reléové staniční zabezpečovací zařízení. Část II. Funkce a zapojení. NADAS, Praha 1965

[20] Poupě O.: Liniový vlakový zabezpečovač. NADAS, Praha 1965.

[21] Macoun Z., Nádvorník B.: Liniový vlakový zabezpečovač LS II, LS III, LS IV. NADAS, Praha 1971.

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

[23] Nádvorník B. a kol.: Měřící přístroje a měření v zabezpečovací technice. NADAS, Praha 1975.

[24] Volf J., Jakl J.: Výstražná světelná zařízení typu AŽD 71. NADAS, Praha 1975.

[25] Stoll K., Bečka J., Nádvorník B.: Vlivy tyristorové regulace hnacích vozidel na železniční zabezpečovací zařízení. NADAS, Praha 1984.

[26] Kadeřávková L. a kol.: Dopravní světelná návěstidla. NADAS, Praha 1986.

Předpisy

[31] Zákon č. 266/94 Sb. o drahách a prováděcí předpisy.

[32] Zákon č. 173/95 Sb. Dopravní řád – v platném znění dle vyhl. Sb.

[33] Zákon č. 177/95 Sb. Stavební a technický řád - v platném znění dle vyhl. Sb.

[34] ČSD D1: Návěstní předpisy (včetně všech změn)

[35] ČSD D2: Dopravní předpisy (včetně všech změn)

Normy (s mimořádným dopadem na odvětví)

[41] ČSN EN 50126

[42] ČSN EN 50128

[43] ČSN EN 50129

[44] ČSN EN 50159-1

[45] ČSN EN 50159-2

[46] TNŽ 28 1020 Zkoušky hnacích vozidel z hlediska rušení železničních zabezpečovacích zařízení.

[47] ČSN 34 2613 Železniční zabezpečovací zařízení. Kolejové obvody.

[48] TNŽ 34 2614 Železniční zabezpečovací zařízení. Kolejové obvody. Projektování kolejových obvodů.

[49] ČSN 34 2617 Určování a ověřování ukazatelů spolehlivosti železničních zabezpečovacích zařízení.

[50] TNŽ 34 2620 Železniční zabezpečovací zařízení. Staniční a traťové zabezpečovací zařízení.

[51] ČSN 34 2650 Předpisy pro železniční přejezdová zabezpečovací zařízení.

Časopisy (s relativně kvalitními články i z našeho odvětví)

[61] Sborník prací ČD

[62] International Railway Journal (GB)

[63] Revue Générale des Chemins de fer (F)

[64] Signal und Draht (D)

Internet (mohutný zdroj relevantních informací, zahlcený ale také nejhoršími škváry a pověrami. Obtížně selektovatelné.)

22 … A SLOVO ZÁVĚREM

Při dokončování této publikace se nám přihodilo krátce po sobě několik událostí. Začalo to dopisem, které jsme s kolegou Konečným poslali ředitelům VÚŽ, O14 a DÚ, když případy evidentních pochybení v zabezpečovací technice se začaly rozšiřovat. Pro jednoduchost jsme si vybrali případ Pendolina:

Rozhodování o zabezpečovacích zařízeních

V poslední době se čím dál tím více setkáváme v oblasti železniční zabezpečovací techniky s případy, kdy rozhodování ovlivňují netechnické argumenty podstatně více, než argumenty technické. Tato situace je částečně pochopitelná a pravděpodobně i správná - je třeba brát např. v úvahu více ekonomické aspekty atd., než jak jsme byli zvyklí dříve - ale existují jisté meze, které jsou dány zejména zvláštností zabezpečovací techniky, tj. přednostním zaměřením na bezpečnost provozu. Proto by se místo rozhodování ad hoc měly dodržovat jisté postupy tak, jak k tomu nabádá například norma ČSN EN 50129 (zejména v příloze A) nebo norma ČSN EN 50126 (zejména v příloze D). Podobnými problémy se zabývají i naše publikace Železniční zabezpečovací technika a Aplikace elektronických prvků v železniční zabezpečovací technice, vydané ve VÚŽ Praha.

Zvlášť varovný případ byl rozehrán okolo problému s ohrožujícími vlivy na kolejové obvody jednotky řady 680. Je evidentní, že všechny netechnické aspekty hovoří pro to, aby jednotka byla uvedena do provozu co nejdříve a bez zbytečných průtahů. Náš ústav, VÚŽ, již v minulém roce předložil jasný, schůdný (časově i finančně) a bezpečný plán, kterým je možné dosáhnout zvýšení limitů pro ohrožující vlivy na kolejové obvody infrastruktury SŽDC a tak i do budoucna vyhovět i nově očekávaným požadavkům TSI. Místo toho byla zvolena následující posloupnost kroků k tzv. kompenzátoru ohrožujících proudů dodatečně dosazenému na jednotky řady 680:

- *nejprve byl VÚŽ, který problém při měření EMC jednotky 680 detekoval (stejně jako měřil všechny ostatní hnací vozidla schvalovaná pro provoz na ČD a je jediným na dodavateli nezávislým pracovištěm schopným důsledky ohrožujících vlivů na kolejové obvody analyzovat), z další činnosti vyřazen a v následujících krocích obejit,*
- *dodavatelem kompenzátoru (AŽD) byla navržena a podivuhodně rychle schválena „oprava“ ČSN 34 2613, která technicky neodůvodněně a chybně ve svém důsledku zvýšila stávající úroveň dovolených vlivů až na pětinásobek (v závislosti na typu kolejového obvodu) původního limitu, přičemž doba trvání vlivů se dovoluje dvojnásobná. Původní limity přitom byly určeny na základě podrobné technické analýzy, s přihlédnutím k vlastnostem na ČD provozovaných kolejových obvodů,*
- *byla navržena – opět z iniciativy dodavatele – a schválena nová norma TNŽ 34 2613-1, která zahrnuje „opravu“ ČSN 34 2613, ale dobu trvání vlivu zvyšuje na pětinásobek. Dále se (většinou chybně) mění i řada dalších parametrů stávající ČSN normy a prohlašuje se za normu normě ČSN nadřazenou (k tomu a předchozímu bodu podrobněji v dopisu VÚŽ ing. Thunovi z 9.9.05 – bez odpovědi – a proto zveřejněn na internetových stránkách VÚŽ),*
- *bylo zadáno měření upravené jednotky řady 680 s kompenzátorem jinému subjektu (Zkušební laboratoř drážních vozidel Škoda Transportation), s metodikou připravenou dodavatelem zkoušeného zařízení (AŽD), kterou nikdo nezainteresovaný ani neposoudil, přestože by měla při schvalovacím procesu podléhat i akreditaci ČIA. Důsledkem je, že nelze tvrdit, že měření provedená podle této metodiky skutečně zachycují kritické případy,*
- *ihned po měření byla dodavatelem na všech možných místech vypouštěna falešná informace, že měření plně vyhovělo původním limitům,*
- *nahlédnutím do výsledků měření lze zjistit, že výsledky nevyhovují ani nově v normách stanoveným limitům (byly naměřeny hodnoty srovnatelné s původním měřením bez kompenzátoru, v některých případech i vyšší),*
- *dodavatel na základě tohoto měření zpracoval „Bezpečnostní rozbor o zajištění bezpečnosti kolejových obvodů SŽDC s.o.“, který i přes sofistikovanou manipulaci s naměřenými daty dochází k tomu, že výsledky měření nevyhovují „opravené“ normě ČSN 34 2613 ani nově navržené normě TNŽ 34 2613-1. S odvoláním na jeden vytržený článek normy ČSN EN 50 238 a metodikou, která neodpovídá žádné ze zmíněných norem (je jejich nelogickou kompilací) „dokládá“, že to nevadí. Implicitně stanovuje nové limity, tentokrát více než 10ti násobné ve srovnání s limity původními (a zcela bez časového omezení). S těmito novými (v žádné výše zmíněné normě neuvedenými) limity pak porovnává naměřené výsledky,*

- *s odvoláním na tento irelevantní bezpečnostní rozbor vydal schvalovatel (ČVUT-FD) „Technické schválení analýzy kompatibility elektrické jednotky řady 680 ve vztahu k zajištění bezpečné funkce kolejových obvodu SŽDC s.o.“ s odkazem na ČSN EN 50238 přesto, že tato norma žádné limity neudává. Zcela pominuty přitom byly i další důležité body schvalovacího procesu podle ČSN EN 50129.*

Tímto postupem došlo k takovému zkreslení technických závěrů, jaké jsme v našem odvětví doposud nezažili. Zařízení nebylo hodnoceno podle stanovených limitů, ale limity byly zcela účelově postupně „opravovány“ tak, aby zkoušené zařízení - kompenzátor - vyhovělo. Úplným paradoxem pak je skutečnost, že „opraveným“ limitům by s největší pravděpodobností vyhověla jednotka 680 i bez kompenzátoru a skutečnost, že tento postup „řeší“ problém kompatibility soupravy 680, ale neřeší obecný problém kompatibility ve smyslu TSI.

V popsané situaci si počínala správně akreditovaná zkušební laboratoř drážních vozidel Škoda Transportation, jejímuž protokolu nelze nic podstatného vytknout - nekonstatoval nic než fakta, neautorizoval nedostatky, které se mu pokusil podsunout dodavatel (metodiku) a dráha („oprava“ normy). Dodavatel (AŽD) manipuloval s výsledky tak, aby za každou cenu prosadil jím preferovaný kompenzátor i když měření jasně prokázalo, že nebylo dosaženo proklamované a potřebné účinnosti. Na takový přístup dodavatelů jsme sice nebyli doposud zvyklí, ale tento postoj má být zachycen a odmítnut procesem schvalování - nezávislým schvalovatelem i dráhou, s prioritními zájmy na dodržení bezpečnosti. To se však nestalo: schvalovatel (ČVUT-FD) ani dráha (ČD-O14) své povinnosti nedostály a není rozhodující, zda se tak stalo z důvodu nekompetence nebo pro neúměrný tlak a nadhodnocení netechnických důvodů.

My jako osoby, ani VÚŽ jako instituce, nemá a ani nemůže mít ambice stanovovat technické limity nebo trvat na limitech, které jsme po technických analýzách doporučili – to je věcí konsensu mezi železnicí (v tomto případě železnicí stanovenými bezpečnostními cíli) a státem (který z titulu garanta bezpečnosti musí tyto cíle potvrdit). Nebylo by však nezajímavé znát, kdo z aktérů si skutečně uvědomil, že tímto plíživým postupem, bez řádného technického zhodnocení a mimo normy, došlo k řádové změně (na více než 10ti násobek) jednoho z parametrů, který může mít na bezpečnost celého železničního systému výrazný vliv, kdo má zájem na budování neúčinného zařízení, kdo je zodpovědný za nekoncepčnost celého postupu a proč nefungují mechanizmy schvalovacího procesu.

Zdá se, že přehlížení technických argumentů a ne zcela solidní technická práce se v posledních letech stává stále častějším a obecnějším problémem zabezpečovací techniky (a asi nejen té). Jediným, kdo má za této situace možnost tento zpackaný a i potencionálně nebezpečný „schvalovací“ proces zastavit, je dnes DÚ.

V Praze dne 26.10.2005
Chudáček, Konečný

PS.: Nejsme tak naivní, abychom si neuvědomovali, že oficiální místa mají dostatek možností, jak nás“zamést“. Toto fakta zveřejňujeme jako soukromé osoby, protože se na podobné nehoráznosti nehodláme podílet ani mlčením, které si v této věci, logicky po výše zmíněném vyřazení, uložila naše instituce.

Následovalo propuštění našeho ředitele a jeho zástupce a dosazení dvou ke všemu ochotných „podržtašků“ na jejich místa. Reagovali jsme následujícím dopisem:

Rozhodování o zabezpečovacích zařízeních II.

Když jsme na konci října zveřejnili svůj názor na situaci v zabezpečovací technice, zejména v souvislosti s řešením EMC u jednotek řady 680, měli jsme na mysli prvotně nápravu nepřijatelného technického stavu. Poukázali jsme na to, že existují jiná, reálná a technicky odůvodnitelná opatření, jak se s daným problémem vypořádat na úrovni.

S politováním konstatujeme, že jediné čeho jsme takto věcným jednáním dosáhli, bylo odvolání ředitele naší instituce jako pomsty za to, že nám nezabránil (?!) náš vlastní názor, tj. názor soukromých osob neschovávajících se za instituci, zveřejnit. Vlastním obsahem a smyslem našeho prohlášení (z něhož je doložitelná každá věta, ba každé slovo) se nikdo z vedoucích pracovníků ČD neunavoval - další promeškaná příležitost jak navrátit odvětví k seriozní technické práci.

Skutečnost, že v souvislosti se zveřejněním našeho názoru byl odvolán jeden z mála kompetentních vedoucích, ředitel VÚŽ ing. L. Lochman Ph.D, s širokým a kvalifikovaným záběrem na domácím i mezinárodním poli, se v budoucnosti negativně projeví v řadě oblastí a je jen potvrzením toho, že vedení ČD nejde o věc. I když nás tento výsledek našeho snažení velmi mrzí, trváme na tom, že povinností všech techniků je seriozně sloužit technickému rozvoji odvětví a nikoliv posluhovat. Po vyčerpání všech obvyklých možností (zprávy, informace, publikace, semináře) jsme byli donuceni sáhnout k tomuto kroku.

Dnes se tedy již nedomníváme, že by stačila technická opatření. Evidentně budou muset předcházet opatření proti těm, kdo brání (proč asi?) řešit technické problémy technicky, na úrovni a bez trapných výmluv. Ostatně z průběhu soudíme, že „těmi" jsou zejména ředitel O14 ing. Zdeněk Thun a jeho nadřízení. Zvláště líto je nám to v případě prvně jmenovaného, kterého jsme dříve znali jako slušného člověka.

V Praze dne 11.11.2005
Chudáček, Konečný

Následovala naše expelace z VÚŽ jeho novým vedením, opět bez jakékoliv odpovědi na naše argumenty. Nevěřili jsme svým smyslům a tak jsme informovali GŘ ČD:

Pendolino a VÚŽ

Výzkumný ústav železniční, a.s. (VÚŽ) je od letošního roku dceřinou společností ČD. Tento ústav disponuje v určitých oblastech pracovníky nejvyšší úrovně znalostí u ČD. Jeho náplní práce je mezi jiným i provozování zkušební laboratoře, která se zabývá také, v různých formách, schvalováním typů vozidel a zabezpečovacích zařízení. Provozování zkušební laboratoře podléhá mimořádně přísným pravidlům, daných dnes i evropskými normami (ČSN EN 17025, 45011 atd.). V těchto normách se, kromě jiného, velmi pečlivě dbá na to, aby tyto zkušebny byly chráněny před netechnickými tlaky (korupce, lobistické zájmy, neodborné zásahy nadřízených), které by mohly ovlivnit zjištění a závěry laboratoří. Realizace tohoto záměru ovšem v ČR podléhá velmi zvláštním zákonitostem.

Příkladem může být proces schvalování jednotky řady 680 (Pendolino). Při schvalování této jednotky se vyskytla celá řada potíží, jak je to konec konců běžné při dokončovacích pracích každého nového rozsáhlejšího technického díla. Obvyklé množství problémů bylo v tomto případě doplněno problémy plynoucími ze skutečnosti, že adaptováno bylo zařízení morálně staré cca 20 let, firmou bez zkušeností s prostředím ČD/SŽDC. Jednotka musí navíc vyhovovat i normám okolních států (kam má zajíždět) a normám nově v posledních letech připraveným pro zajištění interoperability v rámci EU. Řadu těchto problémů se díky značnému úsilí dodavatelské firmy, ale také pracovníků VÚŽ a dalších odborníků z ČD, dařilo postupně řešit. Samozřejmě tím ale docházelo ke zpožděním proti původním předpokladům.

Zásadní problém vznikl v okamžiku, kdy vedení ČD a MD ČR ztratilo trpělivost (což je pochopitelné, ale šíře problematiky byla evidentní již při mimořádných okolnostech spojených s objednáním vozidla) a rozhodli o pevném datu, kdy vozidla vyjedou. Od té doby (a to je již nepochopitelné) všechny technické problémy byly označeny za snahu nepřátelskou vedení ČD a MD ČR a bylo dáno na vědomí, že nebude-li schvalovací proces ukončen do nového jízdního řádu 2005/2006 s kladným výsledkem, budou zodpovědní pracovníci (zejména VÚŽ a DÚ) odvoláni. Tak je v ČR prakticky realizována výše zmíněná ochrana technických schvalovatelů před netechnickými vlivy.

Na podzim letošního roku, kromě některých drobnějších problémů v oblasti mechanické a elektrické výzbroje vlastního vozidla (technických i administrativních), zůstala nejpodstatnějším problémem, zato ale přímo ohrožujícím bezpečnost železničního provozu, možnost ovlivnění kolejových obvodů infrastruktury ČD/SŽDC jednotkou řady 680. V této věci se ČD spolu s dodavatelem (Alstom) a jeho subdodavatelem (AŽD), přes navržené jiné možnosti, jednoznačně orientovalo na zcela nekoncepční řešení pomocí tzv. kompenzátoru, který měl tyto ohrožující vlivy potlačit. Účinnost tohoto zařízení se prokázala jako nedostatečná a proto se ČD na popud AŽD, opět nekoncepčně, rozhodlo změnit stávající limity dovolených vlivů v narychlo vydaných nových normách. Protože zařízení nevyhovělo ani těmto nově (a podle našeho názoru nezodpovědně) určeným limitům, byla rozehrána nebezpečná hra na slepou bábu mezi AŽD, FD ČVUT a O14.

Tuto absurdní situaci jsme se rozhodli veřejně kritizovat otevřeným dopisem, zaslaným ředitelům VÚŽ, O14 a DÚ (viz 1. dopis), když jsme bez odezvy vyčerpali všechny tradiční prostředky informování o technické podstatě problému (oficiální zprávy VÚŽ, články v odborném tisku, na internetu, seminář atd.). Klamání v zabezpečovací technice není totiž jen prohřeškem morálním. Znamená zahrávat si přímo

s bezpečností železničního provozu. Pokud by se takové metody práce v zabezpečovací technice prosadily, bylo by to přímé popření smyslu a účelu zabezpečovací techniky. Této technice se věnujeme již nemalou dobu a takovému vývoji nemůžeme mlčky přihlížet. (Podsouvat nám jiné motivy je nesmysl. Těm, kdo nás a naši práci znají, to není třeba zdůrazňovat, vyvracet to ostatním je neproveditelné - z toho konec konců žije pomluva.)

Očekávali jsme, že, po pojmenování problému pravými jmény, odvětví přehodnotí svůj postoj a přikloní se ke koncepčnímu řešení, tj. např. k úpravě infrastruktury (není to jediné řešení) a k následné odpovídající změně limitů. K tomu má ČD/SŽDC od loňského roku všechny potřebné technické prostředky. Okamžité náklady tohoto řešení jsou, třeba jen v porovnání s kompenzátorem, nepatrné a k obecné úpravě infrastruktury dříve či později (s ohledem na existující i připravované změny TSI) stejně musí dojít. Existují, nebo v té době ještě existovala i řešení, která by dovolila dodržet i stanovený termín zahájení provozu, byť s určitými omezeními.

Vedení ČD ale reagovalo nepochopitelným odvoláním generálního ředitele VÚŽ a technického ředitele a vedoucího zkušebny VÚŽ (se špatně zakrývaným důvodem, že nezajistili bezproblémové schválení jednotky 680, která je v tomto stavu pro zodpovědné lidi evidentně neschvalitelná), podstatou problému se vůbec nezabývalo a podpořilo tak klam. Důsledky tohoto kroku již mnohonásobně přesahují, v porovnání s tím nyní již „drobný" problém schválení jednotky řady 680, :

1. *vedení dráhy dalo na vědomí všem technickým pracovníkům, že okamžikem rozhodnutí šéfů přestávají platit fyzikální zákony a snaha nadále je uplatňovat přímo ohrožuje nejen postavení oněch techniků,*
2. *vedení dráhy dalo na vědomí, že se neštítí akceptovat technicky neudržitelný a nezodpovědný schvalovací proces a klidně pomine výsledky solidní technické práce, pokud to odpovídá jeho „zájmu",*
3. *vedení dráhy znevěrohodnilo další činnost VÚŽ, protože nelze pochybovat, že pod novým vedením bude přání vedení ČD na prvním místě, bez ohledu na zjištěná technická fakta,*
4. *vedení dráhy dalo na vědomí, že mu na koncepční tvořivé práci nezáleží. Škrtem pera zrušilo několikaleté úsilí dosavadního vedení VÚŽ získat kvalitní technickou prací, i v mezinárodním prostředí dobré postavení nejen pro VÚŽ, ale i pro ČD/SŽDC a další instituce ČR. Jak dosavadní ředitel VÚŽ – ing. Lochman, Ph.D., tak dosavadní vedoucí laboratoře Ing. Opava, CSc. v této oblasti vykonali velký kus práce. Dosavadní ředitel je například respektovaným odborníkem v mezinárodní železniční komunitě, člen i vedoucí řady mezinárodních projektů, pracovních a řídících skupin, často vyzývaným přednášejícím na zásadní mezinárodní konference atd. Z toho jsme všichni – nejen ve VÚŽ - těžili jak přísunem, jinak nedostupných, přesných, aktuálních a kompetentních informací o tom, co se ve stále více globalizovaném železničním technickém prostředí Evropy děje, tak přísunem zahraničních zakázek. Výsledkem bylo, že VÚŽ, jako jedna z mála institucí spojených s dráhou, technickou prací vysoké kvality, přes letité macešské chování ČD, na svou činnost bez dotací vydělávalo,*
5. *vedení dráhy je jedno, že nové vedení VÚŽ nebude schopno tyto mimořádně obtížné úkoly plnit a je tedy vážně ohroženo i dokončení přerodu VÚŽ do podoby skutečně (a nejen formálně) mezinárodně uznávané schvalovací instituce (Notified Body). Přitom je dnes zřejmé, že pokud v ČR taková instituce vbrzku nebude, bude řešení všech záležitostí infrastruktury, které mají mezinárodní dopad (což je dnes s ohledem na požadavky interoperability v rámci EU téměř všechno), dříve či později přesunuto k zahraničním schvalovatelům. Není těžké odhadnout, že pak ČD/SŽDC jako národní instituce rychle skončí a v důsledku toho pak také skončí i domácí dodavatelé.*

Je nám z toho trapně. Kdo a proč tohle všechno chce, komu to slouží ? Jak se sníží ohrožení bezpečnosti železničního provozu vyhozením několika pracovníků VÚŽ ? Chtělo vedení skutečně toto, nebo jde o zkratové chování při nekvalitních informacích, ve vypjaté situaci ?
PS.: Zkratky ČD/SŽDC používáme proto, že ČR dodnes neprovedlo skutečné oddělení infrastruktury od provozovatele dráhy (oddělení se provedlo, jak je u nás již zvykem, jen „jako") a je obtížné zodpovědnost za tristní stav infrastruktury jednoznačně přiřadit.

V Praze dne 17.11.2005
Chudáček, Konečný
Odkazy na některé publikace autorů dopisu z poslední doby k výše uvedené problematice :

[1] Chudáček, Kyjovský, Lochman : Detekce kolejových vozidel. ČD-VÚŽ, Praha 1997
[2] Konečný a kol.: Přínos VÚŽ pro rozvoj železniční dopravy v odvětví sdělovací a zabezpečovací techniky. Sborník ČD č. 9, VÚŽ, Praha 2000

[3] *Chudáček, Konečný, Stoll : Problémy elektrické kompatibility kolejových obvodů. Sborník ČD č. 14, VÚŽ, Praha 2002*
[4] *Chudáček, Kyjovský : Analýza limitů ovlivnění kolejových obvodů. Zpráva VÚŽ pro ČD, Praha duben 2004*
[5] *Chudáček : Nová regulace KO 3100 a 3200. Zpráva VÚŽ pro ČD, Praha září 2004*
[6] *Konečný, Hloušek : Vybrané problémy EMC hnacích vozidel a kolejových obvodů č.17/2004. Sborník ČD č. 17, VÚŽ, Praha 2004*
[7] *Chudáček : Předběžná analýza kolejových obvodů při použití přijímače FCP. Zpráva VÚŽ pro ČD, 2004*
[8] *Studie SUDOP, VÚŽ a AŽD pro SŽDC, 2004*
[9] *Chudáček : Problémy kompatibility kolejových obvodů u ČD. Sborník ČD č. 19, ČD, Praha 2005*
[10] *Chudáček : Elektromagnetická kompatibilita kolejových obvodů. Seminář „Problematika elektromagnetické kompatibility kolejových obvodů a elektronické přijímače kolejových obvodů“, ZČU Plzeň, květen 2005*
[11] *Konečný : Elektronický fázově citlivý přijímač KO. Seminář „Problematika elektromagnetické kompatibility kolejových obvodů a elektronické přijímače kolejových obvodů“, ZČU Plzeň, květen 2005*
[12] *http://www.cdvuz.cz/cz/o7/index.html*

Nebyli jsme ani tak shledáni hodnými odpovědi zabývající se meritem věci. Dočkali jsme se jen pomluv, vyslovovaných jak oficiály ČD, tak novým vedením VÚŽ a vedením AŽD, ovšem za našimi zády. Až po několika dalších dnech jsem v hromadě svých starých papírů objevil starý varovný štítek, s nakreslenými blesky a textem „Nedotýkejte se ani drátů spadlých na zem - elektrika pálí, tluče a zabíjí!“. Ten jsem kdysi v 60tých letech přinesl domů a táta k tomu připsal několik veršů, které končí slovy: „...a k tomu se podotýká, nechť vedení se nikdo nedotýká!“. Jak ti naši otcové byli prozíraví : konečně máme odpověď na své dopisy a to napsanou 40 let před událostí !

Důvodem, proč tuto záležitost znovu přetřásáme na těchto stránkách, není podat odstrašující či zastrašující případ pro čtenáře. Je to upozornění na další rovinu, s níž se zabezpečovací inženýr může setkat a tak o ni tuto publikaci doplňujeme. Nestačí totiž být na výši jen v technických otázkách zabezpečovací techniky tak, jak jsme se je v předchozích kapitolách snažili probrat. V dopisech kritizované metody práce jsou v přímém rozporu se smysluplnou prací v zabezpečovací technice a přímo ohrožují její podstatu. Zabezpečovací inženýr musí při své práci respektovat řadu norem i nepsaných morálních (promiňte to zastaralé slovo) pravidel a podle svých sil pak v praxi sloužit technickému rozvoji odvětví a nikoliv posluhovat vašnostům. Aby to mohl plnit, musí se ovšem každý také starat o to, aby mu nevládli lidé nekompetentní, lidé s pochybnými cíly a pochybným žebříčkem hodnot. Jak liché je žvanění těchto lidí o loajalitě k firmě, když tím myslí loajalitu k sobě!

Zde zřejmě chybí ještě mnoho vykonat, ale v tomu vám, jak je z našeho případu patrno, již poradit neumíme.

Chudáček

V Praze dne 28.11.2005