Petr Hloušek

Úvod do problematiky návrhu a schvalování elektronických zabezpečovacích zařízení dle nových evropských norem

Klíčová slova: *návrh a schvalování elektronických zabezpečovacích zařízení, normy EN 50 12x, SILs, Cross-acceptance, Interoperability.*

1. Současný stav elektronických zabezpečovacích zařízení

V současné době je většina používaných zabezpečovacích zařízení s elektrickými závislostmi a z toho převážnou část tvoří reléová zabezpečovací zařízení, část hybridní zabezpečovací zařízení a menší část tvoří plně elektronické (mikroprocesorové) systémy. Pro značnou specifičnost železničních zabezpečovacích zařízení a především pro vysoké nároky na jejich bezpečnost a spolehlivost se průnik elektroniky, hlavně vyššího stupně integrace (mikroprocesory apod.), zpozdil oproti jiným odvětvím a v současnosti k němu dochází ve stále větší míře. Nicméně právě elektronické mikroprocesorové zabezpečovací systémy jsou do budoucnosti nejperspektivnější a současný vývoj v oblasti zabezpečovací techniky je orientován právě na ně.
Pro tyto nové zabezpečovací systémy však donedávna neexistovaly normy v nichž by byly definovány obecné metody a postupy jak návrhu tak i ověřování bezpečnosti těchto zařízení. Díky jejich velké odlišnosti od všech dosavadních zařízení se ukázalo, že na ně nelze aplikovat stávající normy.

Ing. Petr Hloušek, nar. 1973. Západočeská univerzita v roce 1996, obor Dopravní elektroinženýrství. V současnosti pokračuje v postgraduálním doktorandském studiu. Od roku 1999 asistentem na katedře aplikované elektroniky na Elektrotechnické fakultě, ZČU, Plzeň. Vědecká a odborná činnost: železniční zabezpečovací technika, HW i SW. Využití výpočetní techniky v této oblasti - počítačové simulace elektronických obvodů, počítačová podpora návrhu systémů (CASE).

Druhým důvodem pro potřebu nových norem se stal politicko-ekonomický vývoj v Evropě probíhající od konce 80. a v průběhu 90. let.

Sjednocování Evropy do Evropské Unie vedoucí k rozšiřování trhu nastoluje nový trend ve vývoji evropských železnic, který je hlavní hybnou silou při vývoji těchto norem. Zrušení hraničních bariér mezi státy má za následek rostoucí výměnu zboží a osob, což klade samozřejmě nové nároky na veškerou dopravu, železniční nevyjímaje. Rostoucí tlak na ekologii v dopravě spolu s trvale rostoucí cenou ropy je dalším z hlavních faktorů stojícím na pozadí za obnoveným zájmem v Evropě o železniční dopravu.

1.1 Interoperabilita a vzájemné uznávání

Historicky se bohužel železnice každého státu vyvíjela téměř zcela samostatně, nezávisle na sousedních zemích . Většinu technických zařízení a systémů, ale i předpisů a norem si každá železnice vyvíjela vlastní, a tudíž odlišně od ostatních. Částečně je to dáno také tím, že železnice patří mezi strategická odvětví každého státu a tudíž není žádoucí závislost na jiném státu. Toto sebou ovšem přináší vyšší náklady na vývoj a provoz zařízení, které samozřejmě souvisejí s velikostí trhu.

V posledních několika letech se stále výrazněji projevují problémy, které tato nekompatibilita způsobuje, díky vrůstající celkové globalizaci a zvyšování hustoty železniční dopravy v rámci Evropy a především Evropské Unie. V reakci na tyto problémy byl vznesen požadavek na tzv. *Interoperabilitu (Interoperability)*, nejprve u projektu mezinárodního vysokorychlostního vlakového spojení. Tento požadavek byl definován v direktivě Evropské Unie: “High-Speed Train Interoperability Directive 96/48” v červenci 1996. Posléze bylo konstatováno, že tento požadavek je prospěšný pro všechna zabezpečovací zařízení (ale i ostatní technická zařízení) na železnici.

Tato direktiva byla impulsem k vypracování nových norem, podle nichž se mají vyvíjet standardní systémy, u kterých bude snadné uplatnit tzv. *vzájemné uznávání (cross-acceptance)*, což by mělo přinést výrazné snížení nákladů na vývoj a schvalování, a v konečném důsledku i ceny zabezpečovacích zařízení. Termín *Cross-acceptance* znamená, že při předložení rovnocenných podkladů musí být homologovaný produkt, který se shoduje s normou, akceptován nejenom v mateřské zemi, kde byl povolen, nýbrž i v ostatních členských zemích CENELEC.

1.2 Schvalování nezávislým orgánem

V době monopolního postavení státního železničního operátora (přepravce) se vždy zdálo normální, že státem vlastněná firma by měla předem připravit, nebo přinejmenším doporučovat administrativě ke schválení všechny technické normy, předpisy a nařízení týkající se železnice. Jelikož státní technické prostředky a zdroje nikdy nebyly příliš rozsáhlé, vždy to byli železniční operátoři, jež prováděli jejich vlastní ověřování zařízení. Z tohoto plynulo, že tito operátoři byli pokládáni odpovědnými za bezpečnost provozu, takže přenesení ověřovacích procedur na třetí stranu postrádalo smysl.

Teprve nedávno se toto zavedené schéma začalo v Evropě měnit. Některé železniční sítě přestaly být vlastněné a řízené státem. Firmy ztratily část svých výsadních práv, ačkoli fundamentální role státu při definici bezpečnostních pravidel a přidělování práv uživatelům zůstává.Vzhledem k těmto změnám, jež nastaly během posledních patnácti let v právním řádu dříve Evropského společenství nyní Evropské Unie se stalo evidentním, že musí být změněny základní principy certifikace železničních zařízení a systémů. Vyvstala potřeba certifikace třetí nezávislou, kompetentní stranou, tzv. *notified body*. Tento schvalovací orgán musí splňovat několik základních požadavků: nestrannost, nezávislost a odbornost. V rámci vstupu České Republiky do Evropské Unie bude nutné vytvoření tohoto orgánu například dle francouzského vzoru, kde byl založen národním výzkumným ústavem pro bezpečnost dopravy (INRETS), asociací francouzského železničního průmyslu (FIF) a francouzskými státními dráhami (SNCF) v roce 1997.

Tyto nové normy reagují na tuto potřebu, když definují schvalovací proces a složky účastnící se ho včetně jejich rolí a vzájemných vztahů (závislosti či nezávislosti). V závislosti na úrovni bezpečnosti SIL je nutné splnit různé (stupňující se s rostoucí úrovní bezpečnosti) požadavky na nezávislost mezi vedoucím projektu, návrhářem, ověřovatelem splnění požadavků kladených na systém, ověřovatelem splnění požadavků managementu kvality a bezpečnosti a schvalovatelem. Viz. norma EN 50 129 str. 38-40 (obr.6).

Tabulka E.9 v informativní příloze E normy ENV 50 129 uvádí vhodné ověřovací techniky a opatření pro různé úrovně bezpečnosti SIL.

2. Elektronická zabezpečovací zařízení – problémy při vývoji a schvalování

Důvodů proč železniční zabezpečovací technika odolávala a do značné míry odolává používání plně elektronických zabezpečovacích zařízení i dnes je více.
Jedním z dnes již podružných problémů při použití elektroniky byla její nižší spolehlivost a odolnost vůči nepříznivým okolním vlivům; ovšem v současnosti je již technologie na dostatečné úrovni, dovolující nasazení elektronických systémů i v náročných provozních podmínkách.
Větším problémem je i v současnosti relativně vyšší cena těchto systémů oproti klasickým, jejíž nikoli nepodstatnou složku tvoří náklady na vývoj a schválení zařízení, neboť vše co platí pro vývoj a schvalování zabezpečovacích zařízení obecně , platí pro elektronická zařízení ještě ve větší míře a je třeba klást maximální požadavky na vývojový a schvalovací proces u těchto zařízení. Důvodem je jejich novost (velká odlišnost od stávajících) a složitost - viz. další odstavce.

2.1 Elektronické systémy s vnitřní bezpečností

Jedním z hlavních důvodů je ovšem velká obtížnost konstrukce elektronických zabezpečovacích zařízení na principu vnitřní bezpečnosti (*inherent fail-safety*), která jsou obecně z hlediska rozsáhlosti systému (= ceny) a snadnosti ověření bezpečnosti, a tudíž schválení, nejméně náročná. Z tohoto důvodu se značně rozšířila kategorie hybridních zabezpečovacích zařízení, u nichž se převážná část systému skládá z elektronických prvků, nicméně bezpečnost je zajišťována klasickými prvky, především relé.Systémy založené na tomto principu využívají stavební prvky, jež mají poruchami nedotčené vlastnosti a na využití těchto vlastností je postavena bezpečnost systému. V těchto systémech jsou většinou funkce zpracování informace a zabezpečení před poruchami navzájem neoddělitelné, tj. ta funkce jež zpracovává nějakou informaci to dělá bezpečně. Tento přístup znamená, že žádná z uvažovaných poruch nevyvolá nebezpečný stav a systém může být realizován jediným zařízením (jednokanálově) jak hardware tak software. Tento princip se hojně využívá u reléových a hybridních zabezpečovacích zařízení, kde tím stavebním prvkem na který se spoléhá je zabezpečovací relé I. či II. bezpečnostní skupiny.
U elektronických zabezpečovacích systémů tento princip naráží na nedostatek běžně vyráběných elektronických prvků s vhodnými vlastnostmi a především ekonomické důvody nastolily trend

nepoužívat nebo dokonce vyvíjet speciální prvky (vyskytují se určité výjimky), který se v současnosti jeví jako výhodnější.
Další problém tohoto principu u elektronických zařízení jsou požadavky na dostatečně rychlou detekci poruchy a odstavení systému. Při poruše některé funkce se zařízení chová stejně jako neporouchané zařízení, u něhož nebyla splněna některá podmínka nutná pro vykonání té funkce a obvykle není poskytnuta informace proč není daná funkce provedena. U systémů s obsluhou je tato většinou, na základě zkušeností, schopna detekovat poruchu a učinit příslušná opatření, daná například předpisy. Je však zřejmé, že u systémů bez obsluhy je situace podstatně horší. Z výše uvedených důvodů se zatím tento princip u elektronických systémů příliš nerozšířil.
Proto se v současnosti jeví jako nejschůdnější cesta vývoj elektronických zabezpečovacích systémů na principu redundance (composite fail-safety) nebo jako reakční systémy (reactive fail-safety). Tyto dva principy zajištění technické bezpečnosti však zvyšují složitost systému a tím i obtížnost prokazování bezpečnosti, což má samozřejmě negativní vliv na cenu zařízení.

2.2 Bezpečnost softwaru

Dalším velmi významným, ne-li nejvýznamnějším, problémem je, že nedílnou součástí těchto systémů je programové vybavení - software. Do konzervativnosti zabezpečovací techniky se plně promítá softwarová krize trvající již od 80. let více méně do současnosti, ačkoliv se objevily některé trendy a nástroje pro zlepšení situace. Softwarová krize je pojem znamenající, že na rozdíl od hardwaru, kde s růstem složitosti a komplexnosti systémů rostla i vnitřní, tj. pro návrháře systému skrytá, složitost základních stavebních prvků (diskrétní součástky např. tranzistor - integrované obvody se vzrůstající hustotou integrace) a tudíž celý systém se stále skládá z relativně malého počtu prvků, jež jsou samy o sobě s vysokou pravděpodobností bezchybné (prověřené v mnoha aplikacích), tak u softwaru musel programátor(ři), i přes rychle vzrůstající složitost a rozsáhlost programů, vytvářet téměř vše v každém projektu znovu pomocí téměř nejzákladnějších programových prvků. To má samozřejmě za následek pomalý a nákladný vývoj software s velkým množstvím systematických chyb, což je situace pro zabezpečovací zařízení naprosto nepřípustná. Jisté zlepšení této neutěšené situace přinesly v nedávné době systémy pro rychlý návrh aplikací (Rapid Application Development Tools) usnadňující vývoj programů pro operační systémy Windows. Hlavní kvalitativní skok by však měla znamenat nová generace CASE systémů, které se již dlouhou dobu snaží řešit automatizaci vývoje softwaru

(Computer Aided Software Engineering). Postupně se však tyto systémy přeorientovaly na podporu návrhu celých systémů, jejichž součástí je software, což se projevilo ve změně názvu – Computer Aided System Engineering. Bude-li se ubírat jejich vývoj správným směrem, mohly by v budoucnosti výrazně zvýšit efektivitu vývoje a kvalitu systémů, a to i v oblasti železniční zabezpečovací techniky.

2.3 Hodnocení bezpečnosti elektronických systémů

Nikoli nevýznamným problémem je nutnost změny přístupu k hodnocení bezpečnosti elektronických zabezpečovacích zařízení, a jejímu ověření, z výše uvedeného důvodu jejich složitosti. Dříve se klasické zabezpečovací zařízení konstruovaly tak bezpečně, jak to umožňoval soudobý stav technického poznání. Při zvyšující se složitosti zabezpečovacích zařízení se začalo ukazovat, že existuje určitý vztah mezi bezpečností, spolehlivostí a cenou zařízení, který si vynucuje přijmout určitý kompromis mezi těmito protichůdnými požadavky při návrhu zařízení, obzvláště pak elektronických. Problémem právě je určení tohoto kompromisu z hlediska přijatelné míry rizika ohrožení bezpečnosti dopravy. Více také v následující kapitole.

3. Normalizace elektronických zabezpečovacích zařízení

Ačkoli se v posledních letech začínají ve větší míře objevovat elektronická (či alespoň převážně elektronická) zabezpečovací zařízení neexistují ještě obecné prověřené metody a postupy jak návrhu tak ověřování bezpečnosti těchto zařízení. Teprve nedávno vstoupily v platnost první mezinárodní (evropské) standardy týkající se elektronických železničních zabezpečovacích systémů s vysokými požadavky na bezpečnost.

3.1 Zaměření nových evropských norem

Především jsou to normy EN 50 126, ENV 50 129 a EN 50 128. Norma EN 50 126 je základní a týká se obecně *provozní spolehlivosti - dependability (RAMS)* komplexních železničních systémů, tj. nejen zabezpečovacích systémů. Norma ENV 50 129 se týká obecně procesu zajištění bezpečnosti elektronických zabezpečovacích systémů, především procesu vývoje systému a hardwarového vybavení, a norma EN 50 128 se týká bezpečnosti jejich softwarových částí. Základem těchto norem je myšlenka - že proces definovaný z hlediska kvality a z hlediska zabezpečovací techniky vede k produktu a k zařízení, které pak mají tyto stejné vlastnosti. Do

této míry lze tyto předlohy srovnávat s normou DIN EN ISO 9001, podle které má být kvalita produktu dosahována prostřednictvím kvality procesu.
Souběžně s činnostmi CENELEC v oblasti železnice vznikl návrh mezinárodní normy IEC 61 508: "Functional Safety of Safety Related Systems" jako obecná technická norma pro systémy a procesy, která stanovuje obecné požadavky a dokonce je považována za základní bezpečnostní normu, z níž mají vycházet normy specifické pro jednotlivé sektory, ale taktéž ji lze použít jako samostatnou normu. V normě EN 50 126, kterou lze považovat za normu, specifickou pro procesy v železniční dopravě a tudíž mající vyšší prioritu - je uveden odkaz na IEC 61 508, která je zde také považována za základní bezpečnostní standard. Doposud nebylo provedeno sladění mezi některými relevantními částmi dokumentů IEC a normy ENV 50129 (viz. kap. 4). Speciální norma sice stojí výše než základní norma, ovšem není žádoucí, aby mezi příbuznými normami existovaly např. rozdílné definice nebo dokonce obsahy.
Norma EN 50126 je vlastně základní normou, která je specificky určena pro železniční dopravu - ovšem lze ji použít jako samostatnou normu. Pro bezpečné aplikace v železniční technice, které nejsou zařazeny do zabezpečovací techniky (například řízení pohonu a brždění vozidel) se používá norma EN 50126 jako samostatná norma. Pro zařízení bezpečná z hlediska zabezpečovací techniky platí jako základní norma ENV 50129, ovšem i pro tuto normu je základem norma EN 50126.
Je třeba říci, že norma ENV 50 129 je především zaměřena na vysoce komplexní (složité) systémy (např. zabezpečení hlavních tratí nebo vlakové zabezpečovací systémy) nikoli na nezabezpečovací (bez vztahu k bezpečnosti) a jednoduché či středně složité zabezpečovací systémy, používané na vedlejších tratích. Ve všech případech (u všech systémů) je ovšem nutné provést analýzu hazardních stavů (hazard analysis) a vyhodnocení rizika (risk assessment) definované v EN 50 126 pro identifikaci bezpečnostních požadavků (safety requirements)pro každou jednotlivou situaci. Pokud tato analýza odhalí, že neexistují žádné požadavky systému na bezpečnost, pak se tato norma na systém nevztahuje. Nevztahuje se také na současné systémy, ale pouze na nově vyvíjené.

3.2 Nové požadavky plynoucí z normy ENV 50129

Dříve byla bezpečnost absolutně definována z hlediska zabezpečovací techniky - tj. buď byla bezpečnost zajištěna nebo nebyla – současná obecná mezinárodní definice bezpečnosti říká: "Být

prost /zbaven/ neakceptovatelných rizik". To v sobě zahrnuje, že akceptovatelná rizika existují, a že je nutné je rozpoznávat a též je podrobně a jednoznačně prokazovat. Míra bezpečnosti musí být určována tímto předpokladem, jehož základem je riziko. Tedy již neplatí dřívější kvalitativní definice bezpečnosti; a tedy v podstatě dosloužily též pojmy jako "fail-safe", které většinou platily jako synonyma pro absolutní bezpečnost. Nový předpoklad tedy představuje obsah funkce zabezpečovací techniky tak, že existuje taková míra bezpečnosti, jaká je nutná pro to, aby nebylo překročeno akceptovatelné riziko. Lze tedy doufat, že budou existovat cenově přístupné systémy - ovšem nejdříve je nutné nalézt tu správnou míru bezpečnosti.

Žádná z norem CENELEC pro použití v železniční dopravě však nedefinuje, jaká je vlastně potřebná míra celkové bezpečnosti. Tento úkol musí zpravidla splnit provozovatel železničního systému. Určování výšky akceptovatelného rizika pro technický systém může být dosti složité a náročné. Norma ENV 50129 předpokládá, že jsou k dispozici takové rozbory rizika, jejichž cílem musí být, že v případě selhání sledovaných funkcí budou poskytovat procentuální poměr technického ohrožení.

Všechny tyto moderní aktivity podle normy ENV 50129 náleží k tzv. *managementu bezpečnosti*. Norma jasně požaduje, že kompletní management bezpečnosti není nutné pouze zrealizovat, nýbrž že je nutné aby management bezpečnosti bylo možné dostatečným způsobem prokázat - tj. musí být dostatečně zdokumentován. V normě je podrobně popsána, jak má vypadat dokumentace zabezpečovacího zařízení – vývojového i schvalovacího procesu: tzv. *Safety Case*.

4. Úrovně celistvosti bezpečnosti (SILs)

Jako téměř všechny ostatní bezpečnostní normy, normy CENELEC předpokládají, že bezpečnost závisí jak na vhodných opatřeních proti systematickým chybám tak na odpovídajících opatřeních pro kontrolu náhodných poruch. Opatření zaměřená na příčiny chyb a poruch by měla být vyvážená, aby umožňovala dosažení optimální bezpečnostní výkonnosti systému. Pro tento účel byly zavedeny tzv. *Safety Integrity Levels (SIL)*,viz. [1].. Jejich přiřazení je navrženo, aby poskytovalo prostředky pro vyvážení mezi opatřeními proti systematickým chybám a prostředky pro kontrolu náhodných poruch, jelikož z pohledu výboru CENELEC není přijatelné kvantifikovat odolnost proti systematickým poruchám (systematic integrity) (přinejmenším ne pro komplexní aplikace). Je třeba poznamenat, že nejpřísnější bezpečnostní požadavky (např.

střední doba mezi hazardními stavy přesahující 1000000 roků je někdy požadována) mohou být zřídkakdy předvedeny (jejich splnění) pomocí testování či provozem. Proto úrovně bezpečnosti musí také zahrnovat opatření proti chybám v uvažovaných předpokladech a výpočtech obsažených v *Safety Case*.
SILs jsou jedna z nejdiskutovanějších novinek v této normě.Pro tzv. safety-related (tj. s vlivem na bezpečnost) systémy jsou definovány SIL 1-4, přičemž SIL 4 vyjadřuje nejvyšší úroveň bezpečnosti. Je také definována úroveň SIL 0, do níž patří systémy nemající vztah či vliv na bezpečnost – tj. nezabezpečovací systémy. A tato norma (ENV 50 129) se na ně nevztahuje.

4.1 Určování a přiřazování SILs

Při určování SIL se vychází z analýzy rizik, pomocí níž se získají tzv. míry akceptovatelného rizika - *Tolerable Hazard Rates (THR)*, jinak také nazývané *Safety Targets*, a z nich se stanoví příslušná SIL pomocí tabulky v ENV 50 129 [1]. Tato tabulka (tj. hranice mezi jednotlivými úrovněmi bezpečnosti) nebyla v prestandardu preENV 50 129 z roku 1997 ještě zcela upřesněná. Byly v ní obsaženy dva různé provozní režimy, v kterých může systém pracovat a podle toho jsou zde různé kvantitativní meze pro přiřazení příslušné úrovně SIL systému. Výběr režimu (sloupce tabulky) je dán zaměřením systému (úkolem, který má plnit). Výrobce systému a drážní provozovatel by se vždy měli dohodnout na sloupci nejvíce odpovídajícím systému. Problémem interpretace této tabulky bylo kromě dvou režimů provozu systému a neurčitosti mezí také odlišnost od tabulky přiřazení SIL systému uvedené v normě IEC 61 508.
Dalším nedostatkem tohoto prestandardu bylo to, že zatímco poskytuje srozumitelné vedení týkající se dosažení příslušné SIL, nedefinuje přesně metodu a pravidla pro odvozování úrovní bezpečnosti SIL pro prvky systému ze systémových bezpečnostních cílů (systém safety targets) nebo akceptovatelného systémového rizika. Na jeho základě nelze provádět *cross-acceptance* ani u obecného výrobku ani u konkrétní aplikace.

4.2 Návrh metodiky přiřazování SILs

Proto po jeho vydání byla vytvořena pracovní skupina A10, která měla za úkol vypracovat metodiku postupu odvozování úrovní bezpečnosti (SIL) pro prvky systému ze systémových bezpečnostních cílů nebo akceptovatelného systémového rizika (viz. [2]).

Jádrem navrženého postupu je dobře definované rozhraní mezi provozními požadavky, včetně okolního prostředí, a zabezpečovacím systémem. Z hlediska bezpečnosti je toto rozhraní určeno seznamem rizikových stavů spjatých s bezpečností, které pravděpodobně vedou k nehodě. Analýzou rizika jsou získávány akceptovatelné míry rizika pro systém. Odpovědností železniční správy je provést analýzu rizik zahrnující následující aktivity:

definice funkčních požadavků systému (nezávisle na technické implementaci) takových jako provozní režim (zabezpečovací principy), provozní parametry (rychlost a hustota dopravy), rozhraní systému atd.

určení rizikových stavů systému

odhad míry rizik

analýza následků rizik vedoucích nakonec k nehodám, téměř vedoucím k nehodám *(near misses)* a bezpečnému stavu

odvození akceptovatelných mír rizik (THR)

ujištění se, že výsledné riziko je akceptovatelné (na základě vhodného kritéria akceptovatelnosti rizika užitím prostředků redukce rizika).

Zásadní důležitost zde má odvození akceptovatelných mír rizik, které bere v úvahu kritéria akceptovatelnosti rizika. Tyto kritéria nejsou definovány v normách CENELEC, ale závisí na národních či evropských legislativních požadavcích. Bylo navrženo, že pro interoperabilní aplikace bude aplikován MEM princip pro získání cílových individuálních rizik. Celkově pro železniční dopravu může být předpokládáno individuální riziko Ri < 10^{-5} nehod (smrtelných) / (osoba * rok). Akceptovatelná individuální rizika (TIR) pro části zabezpečovacího systému musí být odvozena a vyšetřena ve zbytku procesu.

Kritéria akceptovatelnosti rizika mohou být buď explicitní nebo implicitní. Explicitní kritéria vyžadují odhad (individuálního) rizika, kdežto implicitní kritéria vyžadují např. důkaz, že nový systém je přinejmenším tak bezpečný jako schválený referenční systém. V druhém případě akceptovatelné míry rizika mohou být odvozeny ze srovnání s výkonností referenčního systému, použitím buď statistických nebo analytických metod.

Povinností dodavatele je provést analýzu návrhu systému, jež zahrnuje následující:

definice systémové architektury beroucí v úvahu THR pro každý rizikový stav

analýza příčin každého rizikového stavu

určení požadavků úrovně bezpečnosti (SILs a míry rizika) pro subsystémy

určení požadavků spolehlivosti (míry poruch) pro vybavení

Analýza příčin je prováděna ve dvou etapách. V první je přiřazena akceptovatelná míra rizika systémové funkční úrovni. Úrovně integrity bezpečnosti jsou definovány na této úrovni pro subsystémy implementující funkčnost. Míra rizika pro subsystém je poté přeměněna na úroveň integrity bezpečnosti použitím SIL tabulky. Tato skupina navrhla novou zjednodušenou tabulku přiřazení úrovní SIL - viz. následující tabulka 1. Bylo provedeno sjednocení provozních režimů systému, neboť se dospělo k názoru, že není nutné železniční zabezpečovací zařízení rozlišovat původní dva režimy – požadavkový a nepřetržitý (Low Demand and High Demand /Continuous Mode of Operation), a že nepřetržitý režim provozu je dostatečný, poněvadž pro elektronické zabezpečovací systémy pravděpodobnost poruch pro systémy v požadavkovém režimu a četnost poruch pro systémy v nepřetržitém režimu těsně spjaty, takže tyto systémy (požadavkový režim) mohou být modelovány také jako systémy v nepřetržitém režimu provozu.Také byly upraveny hodnoty mezí mezi jednotlivými úrovněmi. Tato nová tabulka odpovídá tabulce uvedené v již zmiňované normě IEC 61 508, která již získala široké přijetí v mnoha zemích.

Úroveň bezpečnosti (SIL)	Míra akceptovatelného rizika (THR) vztažená na hodinu a funkci systému
4	$10^{-9} < THR < 10^{-8}$
3	$10^{-8} < THR < 10^{-7}$
2	$10^{-7} < THR < 10^{-6}$
1	$10^{-6} < THR < 10^{-5}$

Tab. 1: Nově navržená tabulka přiřazení úrovní SIL

V současnosti platí zatím stále experimentální norma ENV 50 129, poněkud inovovaná v roce 1999, jejíž součástí je i tato nová tabulka SIL.

Během druhé etapy jsou přiděleny míry rizika subsystémům, čímž se získají četnosti poruch pro vybavení. Úrovně bezpečnosti se nezmění na této fyzické implementační úrovni. Přiřazení lze udělat použitím jakékoli metody dovolující vhodnou reprezentaci kombinační logiky, např. spolehlivostní blokové diagramy, chybové stromy, binární rozhodovací diagramy, Markovovy modely atd. Zvláštní péči je třeba věnovat, jestliže je požadována nezávislost subsytémů. Zatímco v první etapě analýzy příčin je požadována funkční nezávislost, ve druhé je dostatečná

fyzická nezávislost. Předpoklady udělané při této analýze musí být ověřeny a mohou vést k vytvoření aplikačních pravidel vztažených k bezpečnosti pro implementaci zařízení. Analýza rizika a analýza návrhu systému musí být schváleny schvalovacím úřadem.
Toto je stručný nástin metodiky přiřazování úrovní bezpečnosti – SILs, navržené CENELEC pracovní skupinou A10, jež se v současnosti ověřuje v praxi (viz. [3]).

1. Závěr

Vzhledem k tomu, že Česká republika se připravuje na vstup do Evropské Unie, je nezbytné již nyní přijmout Evropské normy a začít se jimi řídit. To platí i v tomto případě a vývojáři nových elektronických zabezpečovacích zařízení pro železnici by měli začít implementovat metody a postupy zaváděné těmito standardy. Tento přechod není jednoduchý, ale odměnou může být i výrazný průnik na Evropský trh, jež se zde vytváří díky vzájemnému uznávání zařízení a na něm stavících celoevropských výběrových řízeních.

Literatura:

[1] CENELEC European Standard ENV 50 129 : Safety Related Electronic Systems For Signalling. 1999

[2] Peters, Harald: Erfahrungen mit der Anwendung der ENV 50129 im Fernbahnsektor in: Signal + Draht, č. 6, s. 35 - 39, 1999.

[3] Braband, J.; Lennartz, K.: A Systematic Process for the Definition of Safety Targets in: Signal + Draht, č. 9, s. 53 - 57, 1999.

[4] Taillé, Jean-Yves: The Role of Notified Bodies – French View in: Signal + Draht, č. 9, s. 48 - 50, 1999.

[5] Chudáček, Václav a kol.: Železniční zabezpečovací technika ČD - VÚŽ Praha, 1996

V Plzni, červenec 2000

Lektoroval: Ing. Václav Chudáček, CSc.
VÚŽ Praha