INFORMAČNÝ PRÍSTUP K ANALÝZE BEZPEČNOSTI ZABEZPEČOVACÍCH SYSTÉMOV

INFORMATION APPROACH TO SAFETY ANALYSIS OF SIGNALLING SYSTEMS

Nadežda Hanusová, Jiří Zahradník

Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina

Abstrakt V článku je na konkrétnom príklade vysvetlená podstata informačného prístupu k analýze bezpečnosti zabezpečovacích systémov. Vhodným nástrojom, ktorý možno použiť pre analýzu bezpečnosti, a ktorý podporuje informačný prístup k analýze bezpečnosti sú bayesovské siete. Ďalej budú opísané výhody plynúce z použitia bayesovských sietí na analýzu bezpečnosti zabezpečovacích systémov.

Summary The paper describes foundamentals of information approach to safety analysis of signalling systems on a particular example. Bayesian network is applicable apparatus for safety analysis by using information approach. Advantages of using bayesian networks to safety analysis of signalling systems are described further.

1. ÚVOD

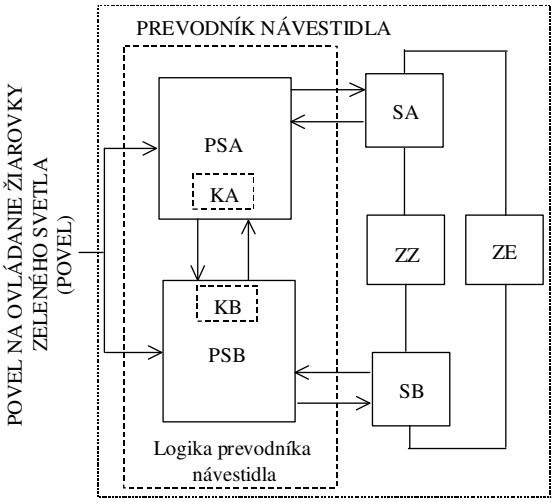
Pri posudzovaní bezpečnosti železničných zabezpečovacích systémov (ďalej len systémov) sa musí predpísaným spôsobom preukázať, že systém dosahuje požadovanú úroveň integrity bezpečnosti.

Preukázanie požadovanej úrovne integrity bezpečnosti systému si vyžaduje vykonanie analýzy bezpečnosti, ktorej súčasťou je aj posúdenie dôsledkov porúch na činnosť systému [1].

V článku je ako príklad vykonané posúdenie dôsledkov porúch pre zjednodušené zapojenie prevodníka návestidla zeleného svetla. Na posúdenie dôsledkov porúch je použitá bayesovská sieť a softvérový produkt Netica 1.12 od Norsys Software Corp.

2. OPIS ALGORITMU ČINNOSTI SYSTÉMU

Bloková schéma zjednodušeného zapojenia prevodníka návestidla zeleného svetla je na obr. 1.



Kde: PSA je procesná stanica A, PSB je procesná stanica B, KA je softvérový komparátor A, KB je softvérový komparátor B, SA je spínač A, SB je spínač B, ZZ je žiarovka zeleného svetla a ZE je zdroj energie.

Obr. 1 Bloková schéma prevodníka návestidla pre zapojenie zeleného svetla

Fig. 1 Block scheme of a signal converter for a green light lamp

Inicializačnou udalosťou je povel na ovládanie žiarovky zeleného svetla (*POVEL*), ktorý má dva stavy: povel na rozsvietenie zeleného svetla (*rozsvZZ*) a povel na zhasnutie zeleného svetla (*zhasZZ*). Inicializačná udalosť *POVEL* sa prenesie k procesným staniciam *PSA* aj *PSB*. Prenos je realizovaný dvoma kanálmi, pričom sa pre zjednodušenie predpokladá, že prenos prebieha bezchybne. Na základe preneseného povelu sa v *PSA* a v *PSB* formuje povel na ovládanie žiarovky zeleného svetla (*rozsv_PSA*, *zhas_PSA*, *rozsv_PSB*, *zhas_PSB*). Medzi *PSA* a *PSB* dochádza k výmene týchto povelových dát, k ich komparácii s dátami príslušnej stanice a len v prípade, že dáta od obidvoch procesných staníc vyjadrujú povel na rozsvietenie zeleného svetla, vydá procesná stanica *PSA* aj *PSB* povel na rozsvietenie žiarovky zeleného svetla. (*rozsv_KA*, *rozsv_KB*) a zopnú sa spínače *SA* a *SB*. V opačnom prípade vydá procesná stanica povel na rozopnutie príslušného spínača (*zhas_KA*, *zhas_KB*). Spínače *SA* a *SB* sú zapojené do série so žiarovkou zeleného svetla. Žiarovkou preteká prúd a žiarovka svieti len vtedy, keď sú zopnuté obidva spínače *SA* aj *SB*. V opačnom prípade je žiarovka zhasnutá.

Analýza bezpečnosti bude z dôvodu zjednodušenia vykonaná len pre logiku prevodníka návestidla, teda pre tú jeho časť, ktorá vytvára povely pre výkonové prvky – spínače.

3. BAYESOVSKÁ SIEŤ ANALYZOVANEJ ČASTI SYSTÉMU

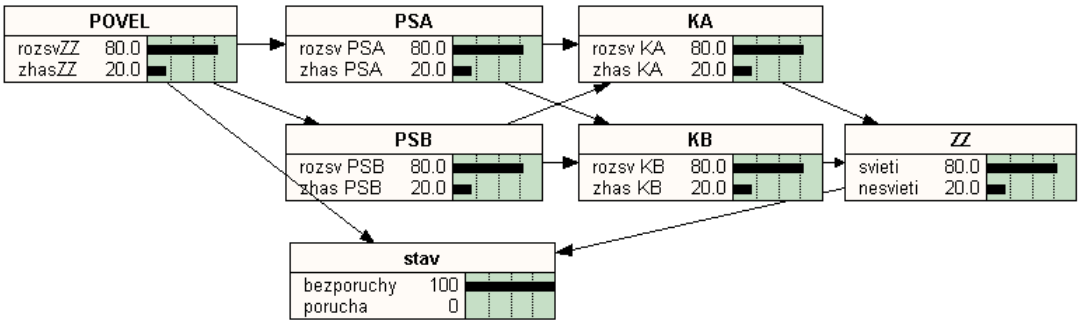
Informačný prístup k analýze bezpečnosti systému predpokladá rozdelenie systému na jednotlivé bloky manipulácie s informáciou a sledovanie vzniku chýb v informácii prenášanej zo vstupu systému na jeho výstup. Príčinami takýchto chýb sú poruchy jednotlivých blokov na manipuláciu s informáciou v systéme. Väzby medzi blokmi zodpovedajú kauzálnym závislostiam, ktoré sú dané algoritmom činnosti systému.

Predpokladá sa, že analyzovaný systém pracuje v prevádzkovom zaťažení, ktoré vyžaduje svietenie žiarovky zeleného svetla v osemdesiatich percentách a nesvietenie žiarovky zeleného svetla v dvadsiatich percentách času, počas ktorého je systém sledovaný.

Pravdepodobnosti výskytu stavov inicializačnej udalosti *POVEL* potom sú: *P(POVEL=rozsvZZ)=0,8* a *P(POVEL=zhasZZ)=0,2*.

Pri bezporuchovej činnosti (výstupná informácia každého bloku manipulácie s informáciou zodpovedá jeho vstupnej informácii) časti prevodníka návestidla pre zapojenie zeleného svetla možno algoritmus jeho činnosti zobraziť pomocou bayesovskej siete na obr. 2.

Problémom, ktorý treba riešiť je naplnenie modelu na analýzu bezpečnosti systému dátami. Pri podmienených pravdepodobnostiach typu *P(výstupná_inf | vstupná_inf)* ide o vyčíslenie pravdepodobnosti správnej alebo nesprávnej činnosti bloku pre manipuláciu s informáciou (*výstupná_inf*) za podmienky, že je k nemu privedený konkrétny vstup (*vstupná_inf*). Keďže v praxi nie sú k dispozícii údaje o intenzite vzniku



Obr. 2 Zobrazenie algoritmu činnosti analyzovanej časti systému pomocou bayesovskej siete

Fig. 2 The algorithm of analyzed system part made by bayesian network

Tab. 1 Zadanie pravdepodobnostných tabuliek uzlov Bayesovskej siete pre bezporuchovú činnosť systému

Table 1 The settings of nodes probability tables of bayesian network for reliable system operation

PSA:				***PSB:***			
rozsv_PSA	**zhas_PSA**	**POVEL**		**rozsv_PSB**	**zhas_PSB**	**POVEL**	
1	0	rozsvZZ		1	0	rozsvZZ	
0	1	zhasZZ		0	1	zhasZZ	
KA:				***KB:***			
rozsv_KA	**zhas_KA**	**PSA**	**PSB**	**rozsv_KB**	**zhas_KB**	**PSA**	**PSB**
1	0	rozsv_PSA	rozsv_PSB	1	0	rozsv_PSA	rozsv_PSB
0	1	rozsv_PSA	zhas_PSB	0	1	rozsv_PSA	zhas_PSB
0	1	zhas_PSA	rozsv_PSB	0	1	zhas_PSA	rozsv_PSB
0	1	zhas_PSA	zhas_PSB	0	1	zhas_PSA	zhas_PSB
ZZ:				***stav:***			
svieti	**nesvieti**	**KA**	**KB**	**bez poruchy**	**porucha**	**POVEL**	**ZZ**
1	0	rozsv_KA	rozsv_KB	1	0	rozsvZZ	svieti
0	1	rozsv_KA	zhas_KB	0	1	rozsvZZ	nesvieti
0	1	zhas_KA	rozsv_KB	0	1	zhasZZ	svieti
0	1	zhas_KA	zhas_KB	1	0	zhasZZ	nesvieti

Blok *stav* je informatívnym blokom a obsahuje percentuálne vyjadrenie výskytu dvoch navzájom doplnkových javov systému: *porucha* a *bez poruchy*.

Pre uvedený algoritmus činnosti časti prevodníka návestidla pre zapojenie zeleného svetla sú jednotlivé uzly siete definované pomocou tabuliek podmienených pravdepodobností uvedených v tab. 1.

V tab. 2 sú uvedené intenzity porúch, pravdepodobností vzniku poruchy a pravdepodobnosti bezporuchovej činnosti pre funkčné bloky analyzovanej časti prevodníka návestidla počas 100 000 hodín prevádzky.

bezpečných a nebezpečných porúch jednotlivých blokov v systéme, pri analýze bezpečnosti systémov budeme predpokladať, že každá porucha systému je nebezpečnou poruchou. Takýto prístup k analýze bezpečnosti nazveme *konvenčným* prístupom. V takomto prípade treba vytvoriť model, ktorý považuje všetky poruchy jednotlivých blokov systému za nebezpečné. To znamená, že ide o najprísnejšie ohodnotenie systému z hľadiska analýzy výskytu jeho nebezpečného stavu. Pravdepodobnostné hodnoty porúch treba zadať do pravdepodobnostných tabuliek jednotlivých uzlov (blokov systému) bayesovskej siete podľa nasledujúceho vzoru, ktorý označíme ako *vzor 1*:

$$p_{zakaz\_\inf} = P(zakaz\_\inf \mid zakaz\_\inf) = p,$$

$$q_N = P(povoľ\_\inf \mid zakaz\_\inf) = q,$$

$$p_{povoľ\_\inf} = P(povoľ\_\inf \mid povoľ\_\inf) = 1,$$

$$q_B = P(zakaz\_\inf \mid povoľ\_\inf) = 0,$$

kde jav *zakaz_inf* vyjadruje informáciu, ktorá vyžaduje zhasnutie žiarovky zeleného svetla a jav *povoľ_inf* vyjadruje informáciu, ktorá vyžaduje rozsvietenie žiarovky zeleného svetla. Pravdepodobnosť q_N je pravdepodobnosť vzniku nebezpečnej poruchy bloku a pravdepodobnosť q_B je pravdepodobnosť vzniku bezpečnej poruchy bloku. Pravdepodobnosť bezporuchovej činnosti bloku pri výskyte zakazujúcej informácie $p_{zakaz\_\inf}$ resp. povoľujúcej $p_{povoľ\_\inf}$ na vstupe bloku je doplnkom ku q_N resp. q_B.

4. ANALÝZA BAYESOVSKEJ SIETE

Za predpokladu *konvenčného* prístupu k analýze dôsledkov porúch systému a použitím bayesovskej siete možno vytvoriť model pre analýzu vzniku nebezpečného stavu systému, ktorý je ekvivalentný napr. s modelom analýzy stromu poruchových stavov. Podmienkou pre vytvorenie takéhoto modelu (ktorý považuje všetky poruchy za nebezpečné) je použitie spôsobu zadania hodnôt podmienených pravdepodobností pre uzly siete, ktoré zodpovedá *vzoru 1*. Zodpovedajúca bayesovská sieť je zobrazená na obr. 3. Zo siete, za predpokladu uvedeného prevádzkového zaťaženia systému, možno odčítať nasledujúce pravdepodobnosti výskytu javov uzla *stav*:

bez poruchy *0,98707* … $1- Q_N'$,

neb_porucha *0,012932* … Q_N',

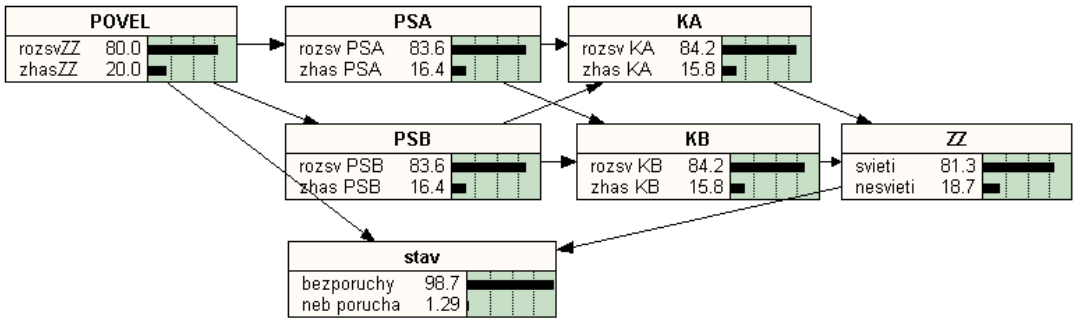
kde Q_N' je pravdepodobnosť výskytu nebezpečného stavu systému pri uvedenom prevádzkovom zaťažení. V sieti na obr. 3. zodpovedá tejto pravdepodobnosti hodnota *1,29*, čo je percentuálne vyjadrenie (použitý softvér zobrazuje len prvé štyri znaky) výskytu konkrétneho javu v uzle siete. Súčet percentuálnych hodnôt všetkých javov v každom uzle siete je *100%*. Pravdepodobnostné údaje zodpovedajúce percentuálnym údajom možno pre požadované uzly siete získať výpisom [2].

Tab. 2 Štatistické údaje pre jednotlivé bloky manipulácie s informáciou v systéme

Table 2 Statistical data for particular blocks of information manipulation in the system

činnosť	**označenie**	**intenzita porúch [h^{-1}]**	**pravdepodobnosť poruchy $q=1-e^{-\lambda t}$**	**pravdepodobnosť bezporuchovej činnosti $p=e^{-\lambda t}$**
formovanie povelu v procesnej stanici	PSA, PSB	$2{,}000.10^{-6}$	$q^{PSA}=q^{PSB}=0{,}1813$	$p^{PSA}=p^{PSB}=0{,}8187$
komparácia dát v procesnej stanici a vydanie povelu	KA, KB	$2{,}000.10^{-6}$	$q^{KA}=q^{KB}=0{,}1813$	$p^{KA}=p^{KB}=0{,}8187$

Predpokladajme, že existuje pozorovanie, že je vyslaný povel na zhasnutie žiarovky zeleného svetla, *POVEL=zhasZZ=100%*, t. j. pre pravdepodobnosť platí *P(POVEL=zhasZZ)=1*. Bayesovská sieť, ktorá zodpovedá uvedenému pozorovaniu je na obr. 4. a získame ju úpravou siete z obr. 3. Za predpokladu existencie uvedeného pozorovania sa automaticky zväčší hodnota pravdepodobnosti výskytu nebezpečného stavu v systéme. Pre výskyt javov uzla



Obr. 3 Bayesovská sieť systému zodpovedajúca konvenčnému prístupu k analýze bezpečnosti systému

Fig. 3 The bayesian network of conventional approach to system safety analysis

stav možno výpisom získať nasledujúce pravdepodobnosti:

bez poruchy *0,93534* … $1-q_N^{sys'}$,

neb_ porucha *0,064659* … $q_N^{sys'}$,

kde $q_N^{sys'}$ je pravdepodobnosť výskytu nebezpečného stavu za predpokladu existencie pozorovania *POVEL=zhasZZ=100%*, a je zhodná s hodnotou, ktorú by sme získali analýzou stromu poruchových stavov uvažovaného systému. Z toho vyplýva, že *vzor 1* pre zadanie hodnôt do pravdepodobnostných tabuliek uzlov bayesovskej siete predstavuje model analýzy dôsledkov porúch, ktorý je ekvivalentný so štandardnými modelmi používanými za týmto účelom, napr. modelom stromu poruchových stavov.

Rovnako by sa postupovalo pri analýze pravdepodobnosti vzniku iba bezpečných porúch systému. V tomto prípade by sa všetky poruchy považovali za bezpečné, t. j. uvažovali by sa len zmeny povoľujúcej informácie na zakazujúcu.

5. VÝHODY BAYESOVSKÝCH SIETÍ

Výhodou bayesovských sietí je možnosť odčítať z bayesovskej siete pravdepodobnosť výskytu povoľujúcej a zakazujúcej informácie na výstupe každého bloku systému.

Najdôležitejšou vlastnosťou bayesovskej siete je schopnosť aktualizovať model po získaní nových pozorovaní [3]. Napríklad predpokladajme, že sme pre uvažovanú časť prevodníka návestidla pre zapojenie zeleného svetla uskutočnili pozorovanie *PSA=rozsvPSA=100%*. Zodpovedajúca bayesovská sieť je zobrazená na obr. 5. Z výpisu zo siete odčítame pravdepodobnosť, s akou bol na vstup *PSA* privedený povel na zhasnutie *ZZ*, ak sa v *PSA* vytvoril povel na rozsvietenie žiarovky zeleného svetla, čo zodpovedá pravdepodobnosti výskytu nebezpečnému stavu systému pri zistení uvedeného pozorovania. Táto hodnota je:

P(POVEL=zhasZZ|PSA=rozsvPSA)= 0,04336.

Ak je získané pozorovanie, že v obidvoch procesných staniciach bol vytvorený povel na rozsvietenie *ZZ*, zmení sa sieť podľa obr. 6. Zo siete možno odčítať pravdepodobnosť výskytu nebezpečného stavu:

POVEL=zhasZZ|PSA=rozsvPSA∩PSB=rozsvPSB,

ktorá je *0,0081504*. Táto hodnota je podľa očakávania menšia, než hodnota odčítaná zo siete na obr. 5, pretože pravdepodobnosť vzniku súčasnej poruchy v obidvoch procesných staniciach je menšia, než pravdepodobnosť poruchy v jednej z nich. Ak je teda k dispozícii pozorovanie vytvorenia povelu na rozsvietenie žiarovky zeleného svetla v obidvoch procesných staniciach, bol k nim s najväčšou pravdepodobnosťou takýto povel vyslaný.

Nech je zistené pozorovanie *ZZ=svieti=100%*. Pre tento prípad možno rovnako ako v predchádzajúcich prípadoch na obr. 5. a obr. 6. nastaviť v sieti príslušné pozorovanie a z výpisu zo siete získať hodnotu pravdepodobnosti výskytu nesprávneho stavu. Nesprávnym stavom je stav, že bol vydaný povel na zhasnutie *ZZ*, ak *ZZ* svieti a pravdepodobnosť výskytu tohto stavu je *0,015908*.

6. ANALÝZA BEZPEČNOSTI SYSTÉMU PRE ZNÁME HODNOTY λ_B A λ_N

Ďalšou výhodou modelu je, že ak sú k dispozícii hodnoty intenzít bezpečných λ_B a nebezpečných λ_N porúch blokov systému, možno z jednej siete vytvorenej pre daný systém odčítať pravdepodobnosť výskytu bezpečnej aj nebezpečnej chyby na výstupe systému.

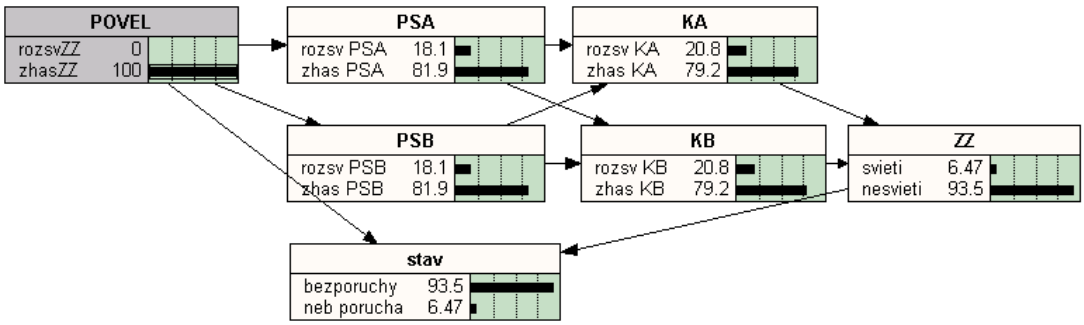
Predpokladá sa, že sú známe nasledujúce hodnoty intenzít bezpečných a nebezpečných porúch blokov analyzovanej časti prevodníka návestidla z obr. 1.

$\lambda_B^{PSA} = 1{,}99.10^{-6}$ h^{-1}, $\lambda_N^{PSA} = 1.10^{-8}$ h^{-1},

$\lambda_B^{PSB} = 1{,}99.10^{-6}$ h^{-1}, $\lambda_N^{PSB} = 1.10^{-8}$ h^{-1},

$\lambda_B^{KA} = 1{,}99.10^{-6}$ h^{-1}, $\lambda_N^{KA} = 1.10^{-8}$ h^{-1},

$\lambda_B^{KB} = 1{,}99.10^{-6}$ h^{-1}, $\lambda_N^{KB} = 1.10^{-8}$ h^{-1},



Obr. 4 Bayesovská sieť systému pre pozorovanie POVEL = zhasZZ=100%

Fig. 4 The bayesian network of the system for the evidence POVEL=zhasZZ=100%

kde λ_B^{PSA} je intenzita bezpečných porúch *PSA*, λ_N^{PSA} je intenzita nebezpečných porúch *PSA*, λ_B^{PSB} je intenzita bezpečných porúch *PSB*, λ_N^{PSB} je intenzita nebezpečných porúch *PSB*, λ_B^{KA} je intenzita bezpečných porúch komparácie *KA*, λ_N^{KA} je intenzita nebezpečných porúch komparácie *KA*, λ_B^{KB} je intenzita bezpečných porúch komparácie *KB*, λ_N^{KB} je intenzita nebezpečných porúch komparácie *KB*.

Pre výsledné intenzity porúch platí (pozri tab. 2.):

$$\lambda^{PSA} = \lambda_B^{PSA} + \lambda_N^{PSA} = 2.10^{-6} \quad \text{h}^{-1},$$

$$\lambda^{PSB} = \lambda_B^{PSB} + \lambda_N^{PSB} = 2.10^{-6} \quad \text{h}^{-1},$$

$$\lambda^{KA} = \lambda_B^{PK} + \lambda_N^{KA} = 2.10^{-6} \quad \text{h}^{-1},$$

$$\lambda^{KB} = \lambda_B^{KB} + \lambda_N^{KB} = 2.10^{-6} \quad \text{h}^{-1}.$$

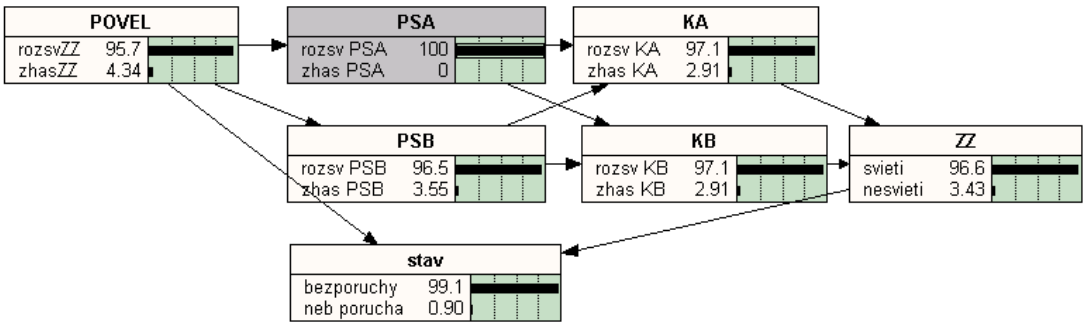
Do pravdepodobnostných tabuliek jednotlivých uzlov siete sa zadajú hodnoty podľa nasledujúceho vzoru, ktorý označíme ako *vzor 2:*

$$p_{zakaz\_\text{inf}} = P(zakaz\_\text{inf} \mid zakaz\_\text{inf}) = 1 - q_N,$$

$$q_N = P(povol'\_\text{inf} \mid zakaz\_\text{inf}),$$

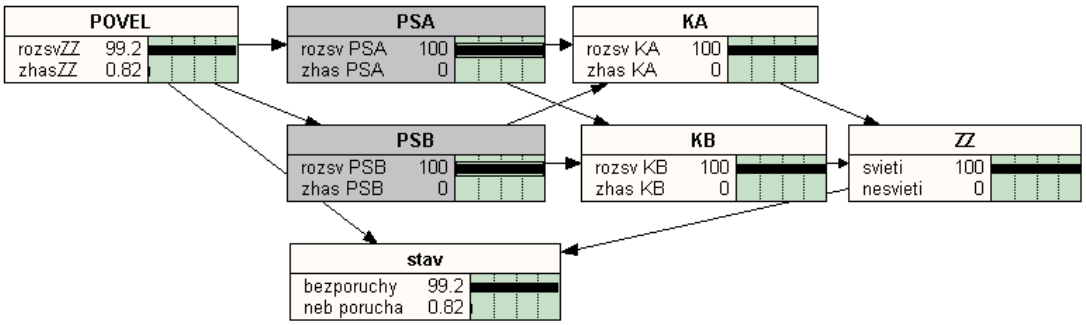
$$p_{povol'\_\text{inf}} = P(povol'\_\text{inf} \mid povol'\_\text{inf}) = 1 - q_B,$$

$$q_B = P(zakaz\_\text{inf} \mid povol'\_\text{inf}).$$



Obr. 5 Bayesovská sieť pre analýzu vzniku nebezpečného stavu pri pozorovaní PSA = rozsvPSA=100%

Fig. 5 The bayesian network for analysis of unsafe state occurrence for the evidence PSA = rozsvPSA=100%



Obr. 6 Bayesovská sieť pre analýzu vzniku nebezpečného stavu pri pozorovaniach PSA = rozsvPSA=100% a PSB = rozsvPSB=100%

Fig. 6 The bayesian network for analysis of unsafe state occurrence for the evidence PSA = rozsvPSA=100% and PSB = rozsvPSB=100%

Zodpovedajúca bayesovská sieť pre dané prevádzkové zaťaženie je na obr. 7. Zo siete možno odčítať hodnotu pravdepodobnosti vzniku poruchy do času 100 000 hodín *Q= 0,4391* pri danom prevádzkovom zaťažení systému.

Predpokladajme, že je vyslaný povel k zhasnutiu *ZZ*. Nastavením pozorovania *POVEL=zhasZZ=100%* v sieti na obr. 7. získame pravdepodobnosť výskytu nebezpečného stavu systému:

$$q_N^{sys} = P(stav=porucha|POVEL=zhasZZ=100\%) =$$

$$= 1{,}67.10^{-6}.$$

Pre výpočet hodnoty tejto pravdepodobnosti platí vzťah:

$$q_N^{sys} = \left(1 - q_N^{PSA}.q_N^{PSB}\right).q_N^{KA}.q_N^{KB} +$$
$$+ q_N^{PSA}.q_N^{PSB}.\left(1 - q_B^{KA}\right).\left(1 - q_B^{KB}\right) =$$
$$= q_N^{KA}.q_N^{KB} + q_N^{PSA}.q_N^{PSB} - q_N^{PSA}.q_N^{PSB}.\left(q_B^{KA} + q_B^{KB}\right) -$$
$$- q_N^{PSA}.q_N^{PSB}.\left(q_N^{KA}.q_N^{KB} - q_B^{KA}.q_B^{KB}\right).$$

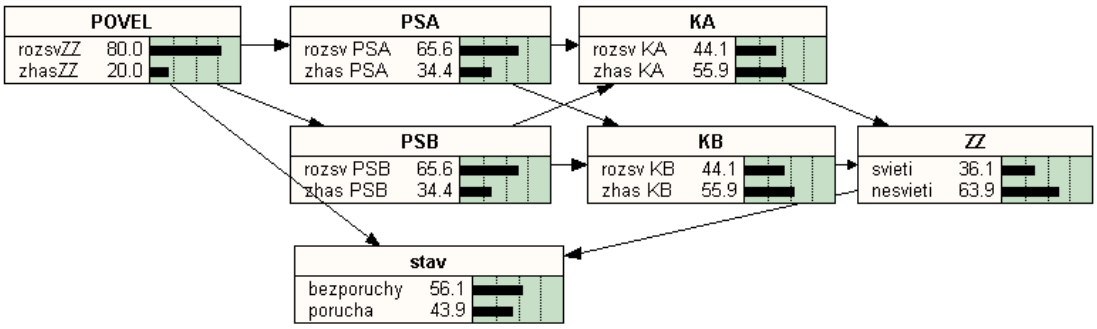
Tento vzťah vychádza z použitia informačného prístupu k analýze bezpečnosti. Nebezpečný stav systému vzniká vtedy, keď vznikne nebezpečná porucha buď na výstupe bezpečná porucha pri komparácii, nevznikne nebezpečná porucha systému ako celku.

Pre porovnanie uvedieme vzťah a hodnotu pravdepodobnosti výskytu nebezpečného stavu systému získanú z analýzy stromu poruchových stavov [4]:

$$q_{N_{FTA}}^{sys} = q^{PSA}.q^{PSB} + q^{KA}.q^{KB} - q^{PSA}.q^{PSB}.q^{KA}.q^{KB},$$

$$q_{N_{FTA}}^{sys} = 0{,}064659.$$

Táto hodnota sa líši od hodnoty q_N^{sys} vypočítanej



Obr. 7 Bayesovská sieť pre známe hodnoty λ_B a λ_N a dané prevádzkové zaťaženie systému

Fig. 7 The Bayesian network presentation of system if values of λ_B, λ_N are known and for given system operating conditions

Tab 3 Porovnanie pravdepodobností výskytu nebezpečného stavu systému pre uvažované prístupy k analýze bezpečnosti systému

Table 3 The probabilities of system unsafe state comparison for considered approaches to system safety analysis

PSA	***PSB***	***KA***	***KB***	***PSA***	***PSB***	***KA***	***KB***	***výstup***	q_N^{sys}	$q_{N_{FTA}}^{sys}$
p	p	p	p	zhas	zhas	zhas	zhas	zhas		
p	p	p	q	zhas	zhas	zhas	rozsv	zhas		
p	p	q	p	zhas	zhas	rozsv	zhas	zhas		
p	p	q	q	zhas	zhas	rozsv	rozsv	rozsv	x	x
p	q	p	p	zhas	rozsv	zhas	zhas	zhas		
p	q	p	q	zhas	rozsv	zhas	rozsv	zhas		
p	q	q	p	zhas	rozsv	rozsv	zhas	zhas		
p	q	q	q	zhas	rozsv	rozsv	rozsv	rozsv	x	x
q	p	p	p	rozsv	zhas	zhas	zhas	zhas		
q	p	p	q	rozsv	zhas	zhas	rozsv	zhas		
q	p	q	p	rozsv	zhas	rozsv	zhas	zhas		
q	p	q	q	rozsv	zhas	rozsv	rozsv	rozsv	x	x
q	q	p	p	rozsv	rozsv	rozsv	rozsv	rozsv	x	x
q	q	p	q	rozsv	rozsv	rozsv	zhas	zhas		x
q	q	q	p	rozsv	rozsv	zhas	rozsv	zhas		x
q	q	q	q	rozsv	rozsv	zhas	zhas	zhas		x

komparácií povelov, pri súčasnej bezporuchovej činnosti aspoň jednej z procesných staníc alebo na výstupe procesných staníc, pri súčasnej bezporuchovej činnosti komparácií povelov. Ak vznikne nebezpečná porucha na výstupe procesných staníc a súčasne vznikne z bayesovskej siete. Pravdepodobnosť vzniku nebezpečného stavu určená metódou stromu poruchových stavov je väčšia než hodnota získaná z bayesovskej siete.

Pre zistenie príčiny rozdielu treba vychádzať zo všeobecných vzťahov pre výpočet pravdepodobnosti vzniku nebezpečného stavu, ak je vydaný povel na zhasnutie žiarovky zeleného svetla. Možné stavy systému z hľadiska poruchovosti blokov sú uvedené v prvých štyroch stĺpcoch tab. 3. Piaty až ôsmy stĺpec tab. 3 vyjadrujú význam informácie na výstupe jednotlivých blokov pre jednotlivé stavy systému. V deviatom stĺpci je význam výstupnej informácie systému. Posledné dva stĺpce obsahujú symbol *x* v každom takom riadku tabuľky, ktorý prispieva k nebezpečnému stavu systému podľa vzťahov pre výpočet q_N^{sys} a $q_{N_{FTA}}^{sys}$. Z tab. 3. vidno, že pri analýze stromu poruchových stavov sa k pravdepodobnosti vzniku nebezpečného stavu systému pripočítajú aj niektoré „nie nebezpečné“ stavy (v tab. 3 sú zvýraznené).

Za predpokladu zadania pravdepodobnostných tabuliek uzlov podľa *vzoru 2* možno zistiť zo siete na obr. 7 aj hodnotu pravdepodobnosti výskytu bezpečnej poruchy q_B^{sys} a to nastavením pozorovania *POVEL = rozsvZZ =100%*. Táto hodnota je *0,0075704*.

7. ZÁVER

Jednou z metód analýzy bezpečnosti systému je analýza bayesovskej siete. Pre prípad, keď sa predpokladá len znalosť výslednej intenzity porúch jednotlivých blokov v systéme bolo treba prispôsobiť model bayesovskej siete tak, aby zodpovedal *konvenčnému* prístupu k analýze bezpečnosti, ktorý je charakterizovaný prijatím predpokladu, že každá porucha systému je nebezpečná. Toto prispôsobenie bolo realizované návrhom spôsobu, akým treba do pravdepodobnostných tabuliek uzlov siete zadávať hodnoty jednotlivých podmienených pravdepodobností. Je to spôsob zadania podľa *vzoru 1*.

Pre analýzu bezpečnosti, ktorá je založená na informačnom prístupe je nutná znalosť intenzít bezpečných aj nebezpečných porúch blokov systému (*vzor 2*). Pri tomto prístupe k analýze bezpečnosti sa uvažuje s možnosťou viacnásobnej zmeny informácie v systéme. Napríklad ak je vznikne inicializačná udalosť *POVEL=zhasZZ*, a v procesných staniciach sa vyhodnotí ako *rozsvPSA* a *rozsvPSB* je možné, že následne, prechodom informácie procesom komparácie, opäť dôjde k zmene informácie na *zhasKA* alebo *zhasKB* a výsledkom je zhasnutie žiarovky *ZZ*. To znamená, že v systéme sa môže s určitou pravdepodobnosťou objaviť správna informácia na výstupe aj v prípade výskytu porúch v systéme. Táto pravdepodobnosť sa s násobnosťou porúch zmenšuje, čo zodpovedá skutočnosti, že násobením pravdepodobností sa získa hodnota menšia než je každá z pravdepodobností, ktoré do súčinu vstupujú. Tento prístup zohľadňuje „vlastnú korekciu“ chýb v systéme. Výhodou použitia informačného prístupu a modelu bayesovských sietí je aj to, že z jedného modelu možno zistiť pravdepodobnosť výskytu bezpečných aj nebezpečných chýb na výstupe systému.

Okrem toho bolo v článku poukázané na niektoré výhody, ktoré poskytujú bayesovské siete pri získavaní rôznych pravdepodobnostných údajov o javoch v systéme.

LITERATÚRA

[1] STN EN 50 129: Železnice. Pevné inštalácie. Elektronické signalizačné systémy súvisiace s bezpečnosťou. 2003.

[2] Manuál k softvérovému produktu Netica 1.12; www.norsys.com.

[3] Vose, D.: Risk analysis. A quantitative guide. Second edition. John Wiley & sons, Ltd. New York, 2002. ISBN 0-471-99765-X.

[4] STN IEC 1025: Analýza stromu poruchových stavov. 1995.