komunikácie
COMMUNICATIONS

Karol Rástočný – Jiří Zahradník – Aleš Janota *

OBJEKTOVO ORIENTOVANÝ MODEL ŽELEZNIČNÉHO ZABEZPEČOVACIEHO SYSTÉMU

AN OBJECT ORIENTED MODEL OF A RAILWAY SAFETY-RELATED CONTROL SYSTEM

Existuje rad metód a foriem použiteľných na tvorbu špecifikácií železničných zabezpečovacích systémov alebo ich podsystémov. Napísať vyhovujúcu technickú špecifikáciu znamená vytvoriť model s požadovanou úrovňou presnosti, jasný a úsporne vyjadrený, ktorý neobsahuje biele miesta a/alebo rozpory. Jednom z možných foriem vhodných na tvorbu takýchto modelov je unifikovaný modelovací jazyk UML' (obchodná značka spoločnosti OMG). V článku sú prezentované skúsenosti a poznatky autorov, ktorí pracujú nad prepisom neformálnej špecifikácie nového železničného zabezpečovacieho systému do objektovo orientovaného modelu založeného na UML. Hlavná pozornosť je venovaná fázam analýzy a návrhu. Výsledkom prvej fázy sú diagramy prípadov použitia a sekvenčné diagramy, výsledkom druhej fázy diagramy tried/objektov a stavové diagramy. Syntax uvádzaných diagramov je v súlade so štandardom UML ver. 1.2, v po-dobe použitej SW nástrojom Rhapsody' ver. 2.2 (obchodná značka spoločnosti I-Logix). Na záver sú zhrnuté skúsenosti a výhody prezentovaného prístupu.

Kľúčové slová: *UML, špecifikácia, objektovo orientovaný, model, železnica*

There is a variety of methods and formalisms usable for writing specifications of railway interlocking and signalling systems or their subsystems. To write a consistent technical specification means to make a model with a required level of precision, clarity and economy of expression that is free of unknown spots and/or conflicts. One of possible formalisms suitable for making such models seems to be the Unified Modeling Language' (trademark of OMG). The paper presents experience and knowledge of authors who have worked over transcription of informal specification of a new railway interlocking and signalling system into the UML based object-oriented model. The main attention is paid to analysis and design phases. The former phase results in use case diagrams and sequential diagrams, the latter in class/object diagrams and statechart diagrams. The syntax of the discussed diagrams is in accordance with the UML ver. 1.2 as given by the software tool Rhapsody' ver. 2.2 (a trademark of I-Logix). Experiences and advantages resulting from the presented approach are summarised within conclusions.

Key words: *UML, Specification, Object-oriented, Model, Railway*

1. Úvod

Proces riadenia bezpečnosti pozostáva z množstva fáz a činností, ktoré spolu vytvárajú životný cyklus bezpečnosti. V procese vývoja systému je potrebné vytvoriť model, ktorý umožní preskúšať komplexnosť a bezchybnosť špecifikácie a umožní odstrániť prípadné biele miesta alebo protirečenia v neformálnej špecifikácii. Všeobecne platí, že prirodzený jazyk alebo iné neformálne zápisy majú veľa nevýhod, ak sú použité na technické opisy. Model systému realizovaný na báze poloformálnych a formálnych metód napomáha ku tvorbe jednoznačných a logických opisov najmä funkčných vlastností systému [1]. Jedným z nástrojov vhodných na tvorbu takéhoto modelu je UML [2]. UML reprezentuje sústavu techník modelovania [3], ktoré sa osvedčili pri tvorbe rozsiahlych systémov a stáva sa obľúbeným, pretože výrazne zefektívňuje a skvalitňuje proces návrhu, vývoja a schvaľovania nových zabezpečovacích systémov. Takýto prístup k vývoju systému je v plnej zhode s požiadavkami európskych noriem pre železničné aplikácie, napr. [4]. Diagramy prezentované ďalej v texte boli prekreslené z pôvod-

1. Introduction

The safety management process consists of a number of phases and activities that are linked to form the safety life cycle. During the system development process there is necessity to make a model that enables testing of complexity and soundness of specification and that allows removing possible unknown spots or conflicts included in an informal specification. Generally, natural languages and similar informal notations are said to have many disadvantages when used for technical descriptions. The system model realised on the basis of semiformal or formal methods helps to develop unambiguous and logical descriptions of mainly functional properties of the system [1]. One of the formalisms suitable for making such a model is the UML [2]. The UML represents a set of modelling techniques [3] approved in development of complex and large-scale systems and becomes popular since it makes the process of analysis, design, safety approval and acceptance more effective and qualitative. This approach to system development fully complies with requirements defined in the European Standards applicable to railway applications, e.g. [4]. Diagrams presented later in the paper

* **doc. Ing. Karol Rástočný, PhD., doc. Ing. Jiří Zahradník, PhD., Ing. Aleš Janota, PhD.**
Department of Information and Safety Systems, Faculty of Electrical Engineering, University of Žilina, Veľký diel, 010 26 Žilina, Slovak Republic
Tel.: +421-41-5655559, Fax: +421-41-5252241, E-mail: zahra@fel.utc.sk, rastoc@fel.utc.sk, janot@fel.utc.sk

ného SW nástroja pomocou textového procesora kvôli lepšej čitateľnosti. V článku je prezentovaný objektovo orientovaný prístup pri modelovaní činnosti traťového zabezpečovacieho zariadenia.

2. Zjednodušená neformálna špecifikácia funkčných požiadaviek

Spôsob technického riešenia daného problému závisí do značnej miery od maximálnych požiadaviek na konfiguráciu koľajiska (maximálny počet traťových koľají, maximálny počet traťových oddielov, umiestnenie vlečiek a odbočujúcich miest na trati atď.) a od prevádzkových požiadaviek zákazníka. Tie sú spravidla definované národnými predpismi a normami.

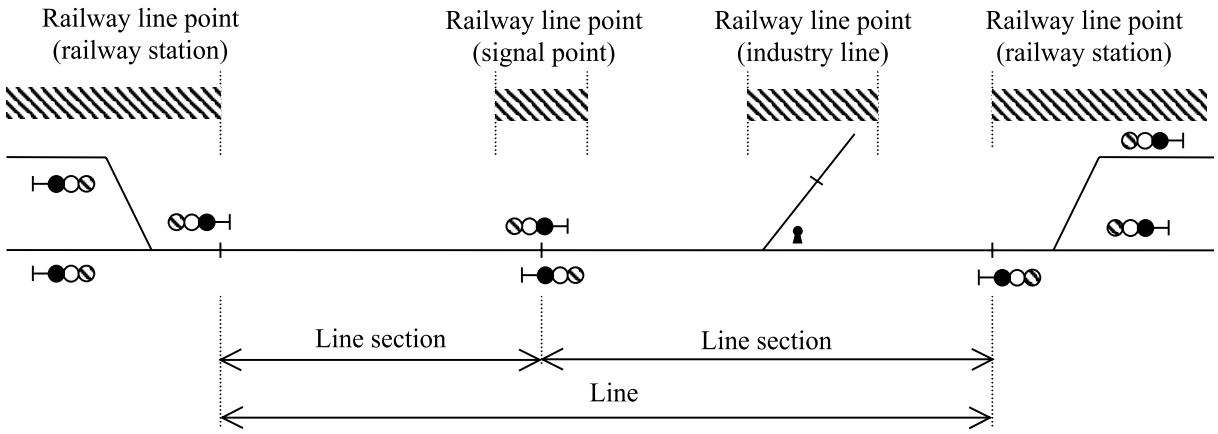
Model je vyvinutý pre jednokoľajnú konvenčnú trať, bez priecestných zabezpečovacích zariadení, ktorá je rozdelená na pevné traťové oddiely (obr. 1). Na hraniciach traťových oddielov sa nachádzajú trojsvetlové návestidlá. Dĺžka traťových oddielov je taká, aby oddielové návestidlo mohlo byť zlúčené s predzvesťami pre nasledujúce oddielové návestidlo. V základnom stave svieti na oddielových návestidlách pre zadaný smer dopravy zelené svetlo, s výnimkou posledného návestidla, ktoré plní funkciu predzvesti a kde svieti žlté svetlo. Na oddielových návestidlách pre nezadaný smer nesvieti žiadne svetlo. Voľnosť traťových oddielov môže byť zisťovaná koľajovými obvodmi alebo počítačmi osí.

were redrawn from the original SW tool using the word processor to get better readability. The paper deals with an object oriented approach applied to modelling of operation of the safety-related section blocking system.

2. A simplified informal specification of functional requirements

The way of technical solution of the given problem considerably depends on maximum requirements for tracks configuration (maximum number of line tracks, maximum number of line sections, location of industry tracks and branching-off points, etc.) and on a customer's operational requirements. They are usually defined by national standards and regulations.

The model is designed for a conventional single line without level crossing installations that is sectioned to fixed line sections (Fig. 1). At the boundaries of line sections there are three-aspect signals installed. The length of each line section is determined in such a way that the function of each block signal can be integrated with the function of a distant signal for the subsequent block signal. By default, there is a "proceed" aspect at every block signal (green light on) for the given direction of traffic, except for the last block signal performing the function of an entry distant signal (yellow light on). There are no signal aspects given (lights off) at the block signals for the undefined direction of traffic. Vacancy of line sections can be monitored by track circuits or axle counters.



Obr. 1. Príklad konfigurácie trate
Fig. 1. Example of the railway line configuration

Na trati môže byť situovaných niekoľko vlečiek. Vlaky na vlečku môžu byť vypravované z obidvoch staníc, taktiež vlaky z vlečky môžu odchádzať do obidvoch staníc. Treba uvažovať aj situáciu, že vlak je na vlečku vypravený z jednej stanice a z vlečky odchádza do druhej stanice alebo na inú vlečku. V každom prípade však ide o riešenie s uvoľnením traťovej koľaje.

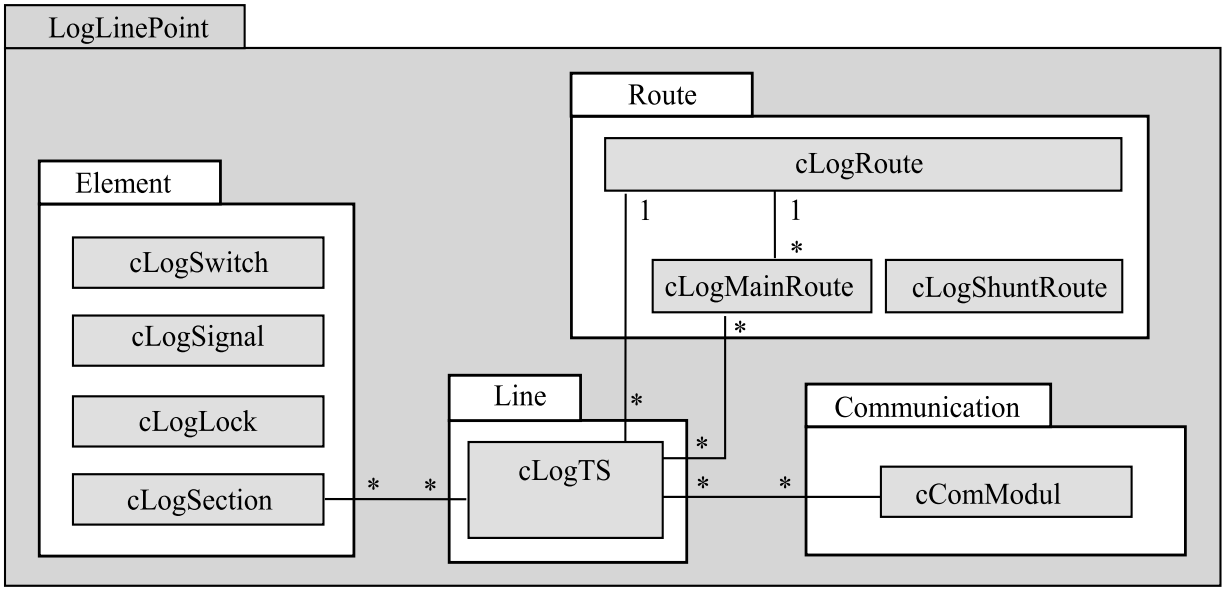
Several industry lines may be connected to the (main) line. Trains directed at industry lines may be dispatched from each of the indicated railway stations and the other way round. The situation when a train is dispatched from one station to the industry line and from there further on to the next railway station or industry line has also to be considered. Anyway, each solution assumes making the line vacated.

3. Formálny opis statickej štruktúry

Pri tvorbe objektovo orientovaného modelu uvažovaného systému je základnou požiadavkou použitie jedného modelu pre ktorýkoľvek druh traťového bodu. Tento predpoklad ústi do generického diagramu tried, ktorý znázorňuje zjednodušenú statickú štruktúru modelovaného systému (obr. 2). Štruktúra zariadenia v každom traťovom bode je potom taká istá, pričom počet jednotlivých objektov závisí od typu traťového bodu, topológie jeho koľajiska a technológie dopravných prác. Package *Trat* obsahuje triedu *cLogTS*. Z tejto triedy je generovaný taký počet objektov *oLogTS*, ktorý zodpovedá počtu traťových koľají spolupracujúcich s traťovým bodom. Objekt oLogTS vytvára logické závislosti súvisiace so spoluprácou traťových bodov pri jazde vlakov v traťových úsekoch, okrem väzby medzi návestidlami (väzba hlavné návestidlo a jeho predzvesť). Package *Cesta* obsahuje triedu *cLogCesta* generujúcu jeden objekt *oLogCesta* a triedu *cLogVlakCesta* generujúcu objekt *oLogVlakCesta* pre každú možnú vlakovú cestu na traťovom bode. Analogicky je triedou *cLogPosun* generovaný počet objektov zodpovedajúci počtu posunových ciest. Objekty package *Cesta* vytvárajú logické väzby medzi prvkami koľajiska tak, aby bol zaistený bezpečný pohyb vlaku v rámci príslušného traťového bodu či už pri posunových prácach alebo pri vlakových cestách. Package *Prvok* obsahuje logické väzby na riadenie a kontrolu jednotlivých prvkov v koľajisku (návestidlá, prestavníky výhybiek, technické prostriedky na zisťovanie voľnosti koľajových úsekov, elektromagnetické zámky atď.) a tiež rieši problematiku väzby medzi návestidlami. Package *Komunikácia* umožňuje prenos informácií medzi zariadeniami jednotlivých traťových bodov. V diagrame sú z dôvodu prehľadnosti zobrazené len tie relácie, ktoré sa využívajú pri činnostiach opísaných ďalej v článku.

3. Formal description of the static structure

Creating an object-oriented model of the considered system, the fundamental requirement is to use one model for any kind of the line point. This precondition results in a generic class diagram showing a simplified static structure of the modelled system (Fig. 2). The structure of the equipment in each line point is then the same whilst a number of particular objects depends on a kind of the line point, tracks topology and technology of shunting work. The package *Line* contains the class *cLogSLP*. This class generates such a number of objects *oLogSLP* that is equal to a number of line tracks co-operating with the line point. The class *cLogSLP* creates logical dependencies related to cooperation of line points when trains are running along the line sections, except for signal-to-signal relation (relation between a block signal and its distant signal). The package *Route* contains the class *cLogRoute* generating one object *oLogRoute* and the class *cLogVlakCesta* generating one object *oLogMainRoute* for each possible main route at the line point. By analogy, corresponding number of objects *oLogShuntRoute* is generated by the class *cLogShuntRoute* for shunting routes. Objects of the package *Route* make logical dependencies among track area elements in order to ensure safe train running within a relevant line point – both for shunting and main routes. The package *Element* contains logical dependencies for control and monitoring of individual elements installed in the track area (signals, point operating devices, technical means used to monitor vacancy of track sections, electromagnetic locks, etc.) and also solves the problem of signal-to-signal relation. The package *Communication* makes information transmission between equipment of particular line points possible. For the sake of comprehensibility only those relations are shown that are necessary for activities discussed later in the paper.

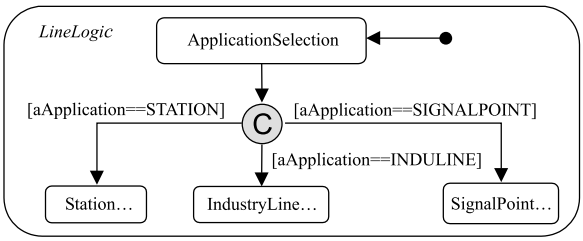


Obr. 2. Statická štruktúra modelu (výsek z diagramu tried)
Fig. 2. Static structure of the model (extract from the class diagram)

4. Spolupráca traťových bodov pri zmene traťového súhlasu

Riadenie dopravy v traťovom úseku si vyžaduje výmenu informácií medzi jednotlivými zariadeniami umiestnenými na traťových bodoch. V základnom stave jedna stanica môže stavať odchodové cesty (t. j. vysielať vlaky na trať, lebo má udelený traťový súhlas (TS)) a druhá spolupracujúca stanica môže stavať len vchodové cesty (prijímať vlaky z trate, lebo nemá udelený TS a má blokované odchodové návestidlá pre danú trať). Stanica s udeleným TS smie vysielať vlaky na trať bez toho, aby pre každý vlak opätovne žiadala TS. Spolupracujúca stanica, s blokovanými odchodovými návestidlami, požiada o TS automaticky pri pokuse o postavenie odchodovej cesty. Pri stavaní odchodovej cesty sa kontroluje prítomnosť TS (udalosť *evStKontrolaTS*). Ak TS nie je udelený, automaticky sa žiada o zmenu smeru jazdy vlakov v traťovom úseku (udalosť *evStZiadanieTS*). Podmienkou pre vyslanie žiadosti o udelenie traťového súhlasu sú zablokované odchodové návestidlá pre danú trať (na návestidle sa dáva návesť zakazujúca jazdu) v stanici, ktorá žiada o TS a voľný traťový úsek medzi spolupracujúcimi stanicami. Žiadosť o udelenie TS sa prenáša postupne z jednej stanice cez jednotlivé traťové body až od druhej stanice. V stanici, ktorá prijala žiadosť o TS, sa zablokujú odchodové návestidlá pre danú trať v polohe zakazujúcej jazdu vlaku a vydá sa povel na udelenie TS pre stanicu, ktorá oň žiadala. Informácia o udelení TS sa opäť prenáša postupne od jedného traťového bodu k druhému traťovému bodu späť do spolupracujúcej stanice. Pri jazde vlaku v traťovom úseku sa vysiela z jedného traťového bodu (alebo stanice) informácia o jazde vlaku (tzv. odhláška) do predchádzajúceho traťového bodu (alebo stanice) za predpokladu, že bol zaznamenaný vjazd vlaku na traťový bod, že traťový oddiel medzi týmito dvoma traťovými bodmi je voľný a návestidle pre daný smer jazdy sa dáva návesť zakazujúca jazdu vlaku. Okrem týchto základných informácií treba prenášať medzi susednými traťovými bodmi informácie o stave traťového oddielu (voľný, obsadený) a informácie o stave návestidiel (väzba medzi hlavným návestidlom a jeho predzvesťou).

Na základe tejto jednoduchej neformálnej špecifikácie možno vytvoriť sekvenčný diagram (obr. 3), ktorý znázorňuje interakcie medzi objektmi (*oLogSLP, oLogRoute, oLogMainRoute, oKomModul*) pre model traťového bodu – stanica. Každá sekvencia ukazuje, ako zúčastnené objekty komunikujú odovzdávaním si správ jeden druhému v čase ako reakciu na menený TS. Zobrazené sú iba štyri scenáre, hoci by bolo možné pridať mnohé ďalšie. Na obrázkoch 4 a 5 sú zobrazené stavové diagramy opisujúce správanie sa triedy *cLogSLP* na traťovom bode „stanica" (príslušné objekty dedia stavové diagramy po svojich triedach). Výber traťového bodu závisí od hodnoty atribútu aAplikácia (obr. 4). Tento výber je nevyhnutný, pretože existujú niektoré jedinečné vlastnosti konkrétneho traťového bodu, ktoré nie je možné zovšeobecniť pre všetky traťové body.

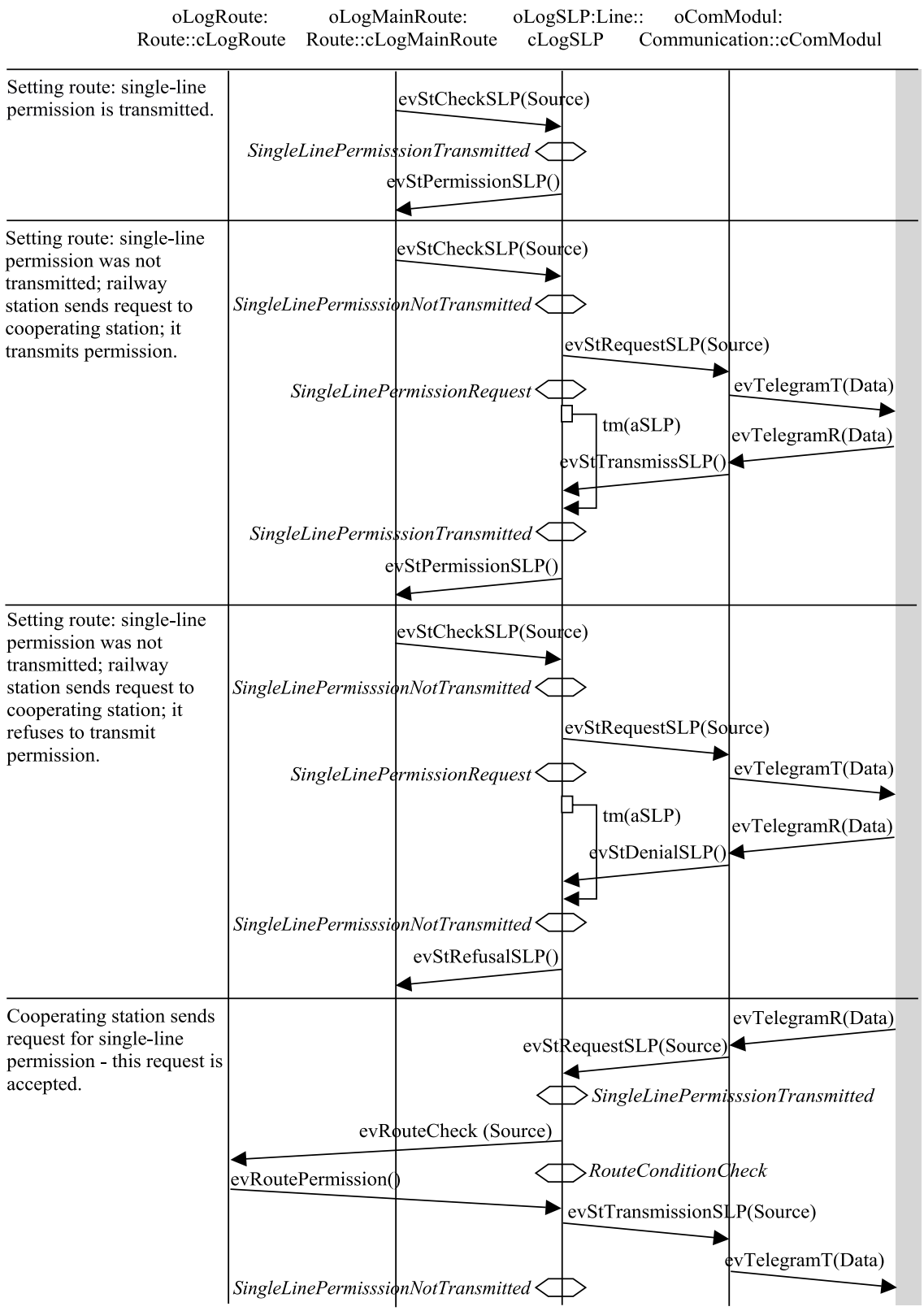


Obr. 4. Stavový diagram triedy cLogTS
Fig. 4. Statechart of the class cLogSLP

4. Co-operation of line points when changing single line permission

Traffic control within the line section needs information exchange between individual equipment installed at line points. By default one railway station may set outgoing routes (i.e. dispatch trains to the line because of having single-line permission (SLP)), while the other co-operating railway station may set only entry routes (i.e. accept trains from the line because of having no SLP and due to blocked departure signals). The railway station having SLP may dispatch trains to the line without any re-asking for the permission if once granted. The co-operating station with blocked departure signals asks for SLP automatically when attempting to set a departure route. In the process of setting a departure route existence of SLP is tested (event *evStCheckSLP*). If SLP is not granted, request for change of traffic direction is automatically generated (event *evStRequestSLP*). Request can successfully be transmitted provided that the relevant departure signals in the requesting station are blocked (having stop aspect) and the line between both co-operating stations is vacated. Request for SLP is then transmitted from the requesting station through the line points successively as far as to the other station. The station, that has accepted the request, blocks its departure signals (having stop aspects) and transmits SLP to the requesting station. This information is again transmitted through line points back to the other co-operating station. When a train runs inside the line section, information called "return indication" is transmitted from one line point to the previous one provided that occupation of the block section was detected, the section between these two points has become vacated and the relevant signal (signal for a given traffic direction) is at stop. In addition, information on the state of line sections (vacated, occupied) and the state of block signals (resulting from "distant signal - signal" relationship) also has to be transmitted.

On the base of such a simple informal specification the sequential diagram can be designed (Fig. 3) showing interactions between objects (*oLogSLP, oLogRoute, oLogMainRoute, oComModul*) for the model of the line point – railway station. Each sequence shows how the participating objects communicate by passing messages to each other over time as reaction to changing SLP. Only four possible scenarios are shown, however, many others could be added. Figures 4 and 5 show statechart diagrams describing behaviour of the class *cLogSLP* at the line point "station" (relevant objects inherit statechart diagrams from their classes). Selection of the kind of line point depends on the value of the attribute aApplication (Fig. 4). This selection is necessary because there are some unique properties of a particular line point that can't be generalised for all kinds of line points.



Obr. 3. Sekvenčný diagram – realizácia funkcie traťového súhlasu (TS)
Fig. 3. Sequential diagram – performing the function of single-line permission

Po inicializácii (proces inicializácie nie je podrobne znázornený) objekt *oLogTS.Stanica* prejde do stavu *UdelenyTratovySuhlas* (v stanici, ktorá prvá požiadala o TS za predpokladu, že sú splnené podmienky na udelenie TS) alebo do stavu *NeudelenyTratovySuhlas* (v stanici, ktorá bola požiadaná o TS a na žiadosť odpovedala kladne). Obdobná činnosť prebehne aj na ostatných traťových bodoch a tým sa zadefinuje smer dopravy. Stav *UdelenyTratovySuhlas obsahuje substavy Necinnost, BlokovanieStanica, BlokovanieVlecka*. Objekt sa nachádza v substave BlokovanieStanica, ak „používa" TS pre odchodovú cestu. Tento substav môže objekt opustiť až po príjme odhlášky (*evStOdhlaska*) od susedného traťového bodu v smere jazdy vlaku. V substave BlokovanieVlecka sa objekt nachádza vtedy, ak sa uskutočňuje odchod vlaku z vlečky, ku ktorému dala stanica súhlas (*evVlSuhlasTS*). Po odchode vlaku z vlečky a uvoľnení traťového úseku (v ktorom sa vlečka nachádza), sa z vlečky vysiela signál odhláška (*evVlOdhlaska*). Po príjme tejto správy môže byť TS použitý pre inú vlakovú cestu. Ak operátor vydá príkaz na postavenie odchodovej cesty a stanica nemá udelený TS (objekt *oLogTS.Stanica* je v stave *NeudelenyTratovySuhlas*), tak po príjme správy *evStKontrolaTS* objekt zisťuje voľnosť k nemu prislúchajúceho traťového úseku (relácia itsUsek a správa *jeVolny*). Ak je úsek voľný, žiada spolupracujúcu stanicu o udelenie TS (vysiela správu *evStZiadanieTS* k susednému traťovému bodu v smere predpokladanej jazdy vlaku; od tohto traťového bodu je požiadavka na TS vysielaná k nasledujúcemu traťovému bodu, až sa dostane do susednej stanice) a prechádza do stavu *ZiadanieOTratovySuhlas*. Ak je úsek obsadený, vracia objektu *oLogVlakCesta* správu *evStNesuhlasTS* a stavanie cesty sa ukončí. V prípade kladnej odpovede od susednej stanice vracia objektu *oLogVlakCesta* správu *evStSuhlasTS* a prechádza do stavu *UdelenyTratovySuhlas*. Ak je odpoveď na žiadosť negatívna (*evStOdmietnutieTS*) alebo neprišla v stanovenom čase žiadna odpoveď (*tm(aTS)*), prechádza objekt naspäť do stavu *NeudelenyTratovySuhlas*. Ak je stanica požiadaná o udelenie TS (prijala správu *evStZiadanieTS*) a TS sa „nepoužíva" ani pre odchodovú cestu a ani pre odchod vlaku z vlečky, potom objekt *oLogTS* vysiela objektu *oLogCesta* správu *evKontrolaCesta* a prechádza do stavu *KontrolaPodmienokCesta*.

Ak na odchodových návestidlách pre danú trať svieti zakazujúci návestný znak a nie je v stanici postavená (ani sa neuskutočňuje) žiadna cesta, ktorá by zasahovala na trať, dá objekt *oLogCesta* súhlas na odovzdanie TS (*evSuhlasCesta*). Ak objekt *oLogTS* prijal správu *evSuhlasCesta* a traťový úsek je voľný, vyšle správu *evStOdovzdanieTS* a prejde do stavu *NeudelenyTratovySuhlas*. Ak niektorá z uvedených podmienok nie je splnená, tak objekt žiadosť o súhlas zamietne (*evStOdmietnutieTS*) a vráti sa do stavu *UdelenyTratovySuhlas*.

5. Záver

Za hlavný prínos vyplývajúci z použitia objektovo orientovaného modelovania na návrh železničných bezpečnostne relevantných systémov možno považovať nasledovné:

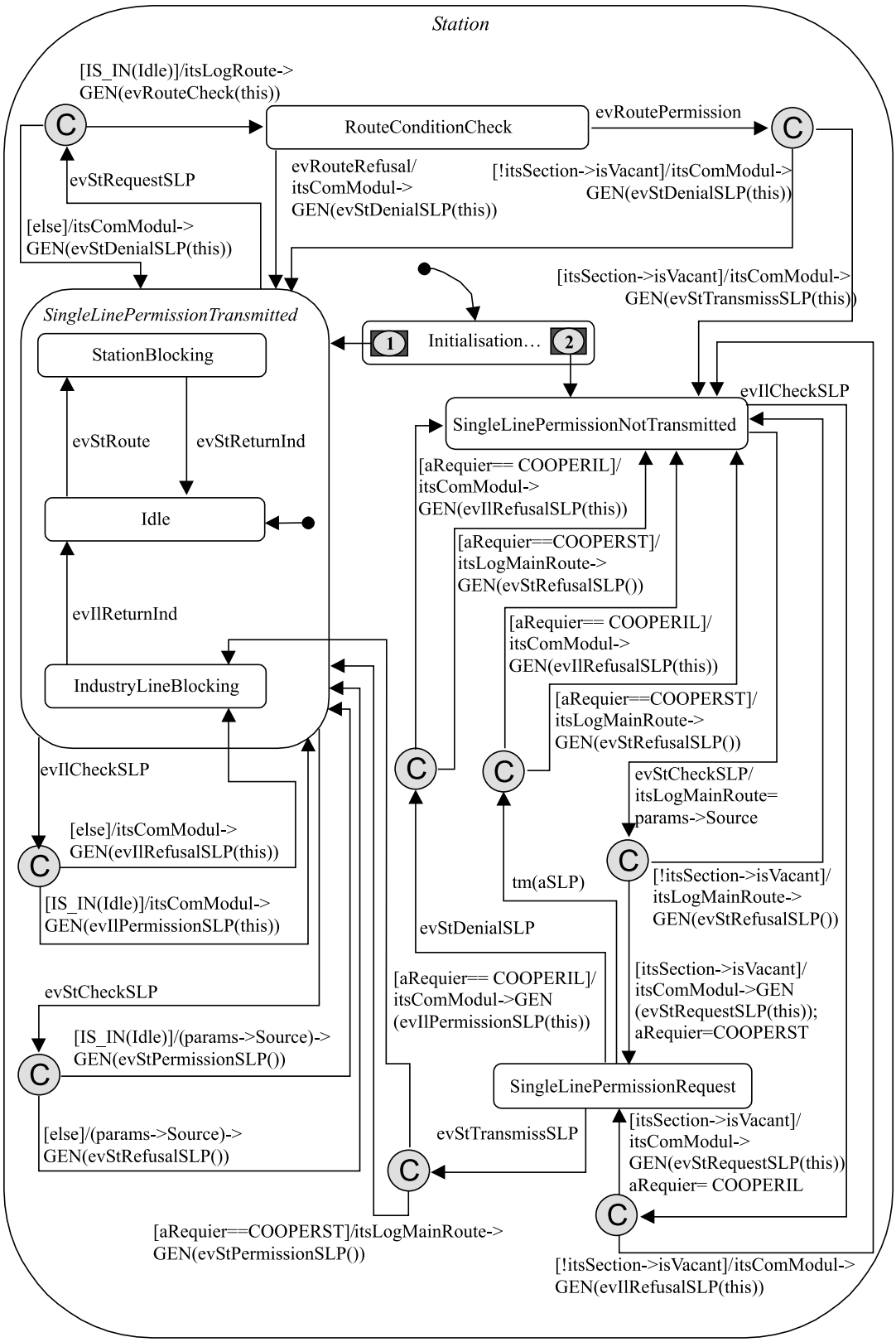
- vytvára vhodné a účinné prostredie pre komunikáciu členov tímu, ktorí pracujú nad projektom (modularita)

After initialisation (the process of initialisation is not depicted here in details) the object *oLogSLP.Station* gets to the state *SingleLinePermissionTransmitted* (in the station that first asked for SLP and that satisfied conditions for transmitting it) or to the state *SingleLinePermissionNotTransmitted* (in the station that was asked for SLP and replied in the affirmative). Similar activity will also take place at other line points and thus the traffic direction becomes defined. The state *SingleLinePermissionTransmitted* includes the states *Idle, StationBlocking* and *IndustryLineBlocking*. The object gets to the sub-state *StationBlocking* if SLP is "used" for a departure route. This sub-state may be left only when return indication was received (*evStReturnInd*) from the adjacent line point in the direction of train running. The object is in the sub-state *IndustryLineBlocking* when a train is to leave the industry line and the station has given permission for this operation (*evIlPermissionSLP*). After the train left the industry line and the line section (containing connected industry line) became vacated, return indication is sent from the industry line (*evIlReturnInd*). Having received this event SLP may be used for another main route. If an operator gives order to set a departure route and the station has no SLP (object *oLogSLP.Station* is in the state *SingleLinePermissionNotTransmitted*) then having received the event *evStCheckSLP* the object tests vacancy of the relevant line section (relation *itsSection* and message *isVacant*). In case the section is vacated, it sends request to the co-operating railway station for transmission of SLP (message *evStRequestSLP* is sent to the adjacent line point in direction of planned train running; from this line point the request is forwarded to the next line point as far as it reaches the co-operating station) and gets to the state *SingleLinePermissionRequest*. In case the section is occupied, it returns the message *evStRefusalSLP* to the object *oLogMainRoute* and the attempt to set the route is over. In case of positive answer from the co-operating station the event *evStPermissionSLP* comes back to the object *oLogMainRoute* and the class gets to the state *SingleLinePermissionTransmitted*. In case of a negative answer (*evStDenialSLP*) or no answer received within an expected time (*tm(aSLP)*) the object gets back to the state *SingleLinePermissionNotTransmitted*.

If the station is asked to transmit SLP (message *evStRequestSLP* was received) and SLP is "used" neither for a departure route nor for departure of a train from the industry line then the object *oLogSLP* sends a message *evRouteCheck* to the object *oLogRoute* and gets to the state *RouteConditionCheck*. If the relevant departure signals are at stop and there is no route set which could have effect on the line (and no setting is under process) the object *oLogRoute* permits transmission of SLP (*evRoutePermission*). If the object *oLogSLP* received the message *evRoutePermission* and the line section is vacated it sends message *evStTransmissSLP* and gets to the state *SingleLinePermissionNotTransmitted*. If some of the given conditions is not fulfilled the object denies the request for SLP (*evStDenialSLP*) and gets back to the state *SingleLinePermissionTransmitted*.

5. Conclusions

The main contribution resulting from applying an object-oriented modelling to the design of railway safety-related systems can be seen as follows:



Obr. 5. Stavový diagram triedy cLogTS.Stanica
Fig. 5. Statechart of cLogSLP.Station

- zjednodušuje proces návrhu softvéru (vývojový proces redukuje celkový vývojový čas určený pre softvérové inžinierstvo)
- podporuje špecifikácie, ktoré sú nezávislé od konkrétnych programovacích jazykov a vývojových procesov
- špecifikácie sú čitateľné a zrozumiteľné pre ostatné subjekty začlenené do procesu posudzovania a schvaľovania bezpečnosti aplikácie
- unifikuje princípy a postupy použité na vytváranie dokumentácie pre elektronické bezpečnostne relevantné systémy (s možnosťou automatického generovania dokumentov)
- údržba modelov pri napredovaní projektu je oveľa ľahšia ako v prípade jednoduchých nákresov.

Nástroje založené na UML majú často implementované kontrolné mechanizmy, ktoré dovoľujú vybrať, na ktoré vlastnosti má byť model alebo jeho časť zamerané. Verifikácia funkčnej správnosti tiež môže byť testovaná animáciou vytvoreného modelu. Platnosť všetkých uvedených predností bola potvrdená praktickou realizáciou modelu funkcií, ktorý bol vytvorený pre nový železničný zabezpečovací systém vyvíjaný nemeckou firmou Scheidt&Bachmann.

- Creates a sound and efficient environment for communication of team members working over the project (modularity)
- Simplifies the design process of SW (the development process reduces the overall software engineering development time)
- Supports specifications that are independent on particular programming languages and development processes
- Specifications are readable and understandable for other subjects involved in the process of safety assessment and approval
- Unifies principles and procedures used to create documentation for electronic safety-related systems (with possibility of automatic document generation)
- Maintenance of models as the project progresses is far easier than in the case of simple drawings.

The UML based tools have often checking mechanisms implemented that allow to select checks to be performed on the model or a part of it. Verification of the functional correctness can also be tested by animation of the created model. All declared merits have been validated by practical realisation of a function model that has been designed for a new railway safety-related system being under development by the German company Scheidt&Bachmann.

Literatúra – References

[1] BOWEN, J. P., STAVRIDOU, V.: *Safety-critical systems, formal methods and standards*. Programming Research Group Technical Report PRG-TR-5-92, Oxford University Computing Laboratory, 1992.
[2] *OMG Unified Modeling Language Specification*, ver. 1.3, 1999. http://www.omg.org
[3] BOOCH, G., RUMBAUGH, J., JACOBSON, I.: *The Unified Modeling Language*. User Guide, Addison – Wesley, 1999, 482 pp.
[4] EN 50128: Railway applications: Software for railway control systems and protection systems. CENELEC, Brussels, 2000