اولین کنفرانس ملی تصادفات وسوانح جاده ای و ریلی
ایران- زنجان، دانشگاه آزاد اسلامی –واحد زنجان، آذر ۱۳۸۸

مدلسازی و درستنمایی سیستم اینترلاکینگ راه آهن به روش رسمی و با استفاده از متدB

احمد میر آبادی[۱] و محسن پیکرستان[۲]
[1]mirabadi@iust.ac.ir
[2]mpeykar@yahoo.com

دانشگاه علم و صنعت ایران – دانشکده مهندسی راه آهن

چکیده

ابهامات سیستمها منشاء بروز خطا بوده و خطا در سیستمهای کنترلی مانند سیستمهای کنترل ریلی از علل و عوامل حوادثی مانند تصادفات ریلی و یا خروج از خط میباشد. یکی از راهکار های رفع ابهامات استفاده از روشهای رسمی بوده بطوریکه در بسیار از قراردهای توسعه نرم افزار های ایمنی محور استفاده از روش مذکور در مجموعه الزامات قراردادی گنجانده میشود. روش رسمی با استفاده از اثبات کننده های اتوماتیک، در زمینه توسعه نرم افزارهای ایمنی محور که هزینه خطای بالایی دارند بسیار مورد توجه میباشد. درحوزه مهندسی را ه آهن بکار گیری روش مذکور در کشورهای پیشرفته بسیار متداول بوده ویک نمونه از چگونگی استفاده آن در این تحقیق بررسی شده است. در بحث اینترلاکینگ ایستگاهها تعامل بین اجزا، مدلی پیچیده می سازد که فهم آن بسیار مشکل خواهد بود. وازاین دید بیان رسمی مشخصات با استفاده از روشی رسمی مانند روش رسمی B بسیار کارا میباشد. در این مقاله سعی شده است یک نمونه از اینترلاکینگ متمرکز ارایه شود که اکثر فرآیندها مانند رزرو نمودن مسیر، قفل مسیر، مسیر شانت، مسیر معکوس و مسیر فراخوان را در بر داشته باشد.

کلمات کلیدی

ایمنی محور[۱]، روش رسمی[۲]، مشخصات رسمی[۳]، درستنمایی، متد B[۴]

مقدمه

سیستمهای کامپیوتری با ترکیبی از سخت افزار و نرم افزار، بعنوان سیستمهای Embedded شناخته میشوند که امروزه جز< جدا نشدنی و بعضا محوری از اغلب سیستمهای مهندسی محسوب میشوند.

این سیستمها اغلب بعنوان بخش کنترل و/یا مدیریت سیستمها عمل مینمایند. در سیستمهای ایمنی محور (safety Critical)، سیستمهای کامپیوتری مزبور از حساسیت و اهمیت ویژه ای برخوردارند چرا که عملکرد این سیستم و عدم وقوع سانحا و خسارت بر عوامل انسانی و یا تجهیزات را بر عهده دارند.

سیستمهای اینترلاکینگ راه آهن از جمله سیستمهای ایمنی-محور محسوب میگردند که عملکرد و سیر و حرکت ایمن سیستم را تضمین مینمایند.

مدلسازی و درست نمایی سیستمهای ایمنی-محور، از مراحل مهم در فرایند طراحی و ساخت آنها میباشد. تاکنون محققین روشها و

[1] Safety critical
[2] Formal method
[3] Formal specification
[4] B method

ابزارهای متنوعی را برای این منظور وعرفی نموده و مورد بررسی قرار داده اند. روشهای رسمی(Formal methods) ، روشهایی جهت مدلسازی و و درستنمایی آن میباشد که بر پایه اصول و مفاهیم ریاضیات عمل مینماید. هم نرم افزار و هم سخت افزار با این روش میتواند مدل و چک مدل شوند. تکنیک های ریاضی با استفاه از نمادگزاری ویژه خود، میتوانند سازگاری و یا ناسازگاری مدل را، با توجه به مشخصات آن اثبات کنند. [1]

با توجه به هزینه های قابل توجه بکار گیری روشهای فرمال، استفاده از این روشها در سیستمهای مهندسی معمول فاقد توجیه اقتصادی میباشد و کاربرد آنها در حال حاضر به سیستمهای ایمنی-محور محدود میگردد. نیاز به صرف هزینه و وقت زیاد از عدم امتیازات روش مذکور و همین موضوع استفاده آنرا تنها در سیستمهای ایمنی محورقابل توجیه میکند.[2]

هدف اصلی در اینترلاکینگ راه آهن ایجاد ایمنی حرکت قطار در یک ناحیه مشخص از خطوط ریلی بوده و وظیفه دارد انسانهاو تجهیزات را از آسیب مصون بدارد. از این جهت سیستم نرم افزاری اینترلاکینگ دارای مرحله درستنمایی بسیار جدی میباشد. از سوی دیگر تعاملات لازم بین اجزاء کنار خط از جمله سوزنها، سیگنالها و سیستمهای تشخیص قطار، با توجه به حالات ممکن و متصور برای هر یک از آنها، طراحی و تحلیل سیستمهای اینترلاکینگ را پیچیده مینماید. این نکته که برای هر یک از اجزاء حالتهای متعددی قابل تصور میباشد و تشکیل و اختصاص هر مسیر به یک قطار، فقط در یکی از ترکیب حالتهای اجزاء مرتبط باآن مسیر امکانپذیر است، مدل را پیچیده مینماید. بطور عمومی حتی برای یک اینترلاکنیگ با سایزمتوسط و فرآیند های معمول آن، اجزاء زیادی باید بررسی و صحت حالت آن درستنمایی گردد.[3]

آزمایشگاه کنترل و سیگنالینگ دانشکده مهندسی راه آهن، دانشگاه علم و صنعت ایران، فعالیتهای تحقیقاتی متمرکزی را به بکارگیری روشهای فرمال در طراحی و توسعه سیستمهای سیگنالینگ اختصاص داده است که از آن جمله میتوان به مطالعات انجام شده در زمینه استفاده از NuSMV در تدوین و درست نمایی جداول کنترل اینترلاکینگ اشاره نمود.[4] ولی در این کار تحقیقاتی سعی شده است با بکار گیری روش رسمی کامل[1] به مدلسازی و اثبات مدل پرداخته شود. برای ارایه نمونه، از ماکت موجود در آزمایشگاه دانشکده راه آهن استفاده شده است و روش B برای مدلسازی آن استفاده شده است. ارایه یک نمونه واقعی میتواند بسیار از ابهامات را از بین بر دارد و چگونگی بکار گیری روش مذکور را به خوبی نشان دهد. البته بعضی از مدلهای در این رابطه ارایه شده است که برای نمونه میتوان به مدل آقای آبریل[2] اشاره نمود[5]. مدل مذکور تنها برای ایستگاه های منفرد ایجاد گردید است و لی در این کار تحقیقاتی، منطق مدل، برای بیش از دو ایستگاه نیز صادق است . قابل توجه است که منطق مدل یک ایستگاه منفرد که در آن قطار وارد و خارج میگردد با منطق مجموعه از ایستگاهها که دارای مسیر بسته ایی هستند بسیار متفاوت است. از این دید میتوان بیان نمود که این کار تحقیقاتی برای کنترل همزمان چند ایستگاه مرتبط با مسیر بسته، کاری جدید محسوب میگردد.

روش B مورد استفاده دراین تحقیق، دارای نماد گزاری ریاضی به نام AMN[3] میباشد و با کمک ابزارهای خود میتواند در توسعه نرم افزاری بسیار سود مند باشد. ریشه این روش مرتبط با نماد گزاری Z بوده و توسعه نرم افزار تا مرحله کد را برپایه مشخصات بنا مینماید. کاربرد روش مذکور در سیستمهای ایمنی محور متداول بوده و خط۱۴ مترو پاریس را میتوان نمونه ای از کاربرد آن نام برد. کاربرد این روش در صنعت رو به افزایش است و بیشتر از پیش مورد توجه قرارگرفته است. برای تمام مراحل بیان مشخصات رسمی، طراحی، اثبات و ایجاد کد این روش ابزارمنداست.[6]

زبانهایی که پایه ریاضی دارند مثل زبان B با استفاده از نمادهای ریاضی کارا در این نوع سیستم میتوانند بسیاری از مشکلات و

[1] Full formalization
[2] Abrial
[3] Abstract machine notation

پیچیدگی موجـود در بیـان مشخـصات سیـستم و مدلـسازی آنـرا بکاهند. به عنوان مثال کد ارائـه شـده در زیـر، بیـانگر ملاحظـات موجود پیرامون جزء مسیر مشترک بین دو مسیر ممکن است کـه در هر لحظه صرفا امکان تنظیم یکی از مسیرها وجود دارد:

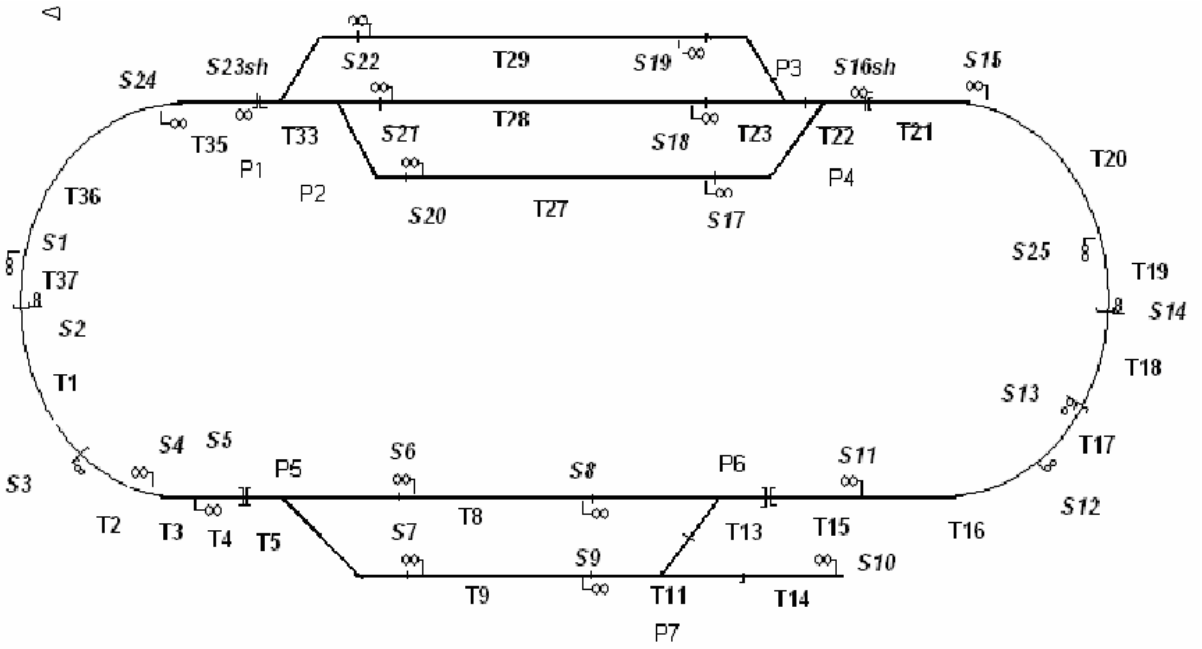
```
ovl={xx,yy|xx:nei & yy:TS &
!(uu,vv).(uu:RR & vv:RR &uu|->vv=xx
=>yy:rtbl~[{vv}]/\rtbl~[{uu}])}&
```

چه بسا دستور دوخطی فوق در یک زبان معمولی برنامـه نویـسی نیاز به نوشتن برنامه چندین سطری برای عملکرد مشابه دارد کـه با حجیم شدن آن ابهامات و اشکالات نیز افزایش مـی یابـد. بیـان مشخصات سیستم که شامل دو ایستگاه میباشد و بیش از بیست و هشت قانون سـطح بـالای ایمنـی در آن وجـود دارد (تعـداد ایـن قوانین در سطوح پایین تر بیشتر میگردند) با استفاده از این نمـاد ها بیان شد و سعی شده است آنچه که در دنیای واقعی اتفاق مـی افتد در این مدل نیز دیده شـود. مـدل اسـتفاده شـده دارای دو ایستگاه میباشد و میتواند نمونه ای سـاده از منطـق اینترلاکینـگ متمرکزایستگاهها باشد.

مدل

شکل شماره یک عکس و شکل شماره دو شماتیک ماکت ایـستگاه موجود در آزمایشگاه دانشکده راه آهـن میباشـد. همـانطور کـه در شکل مشخص میباشد در ماکت دو ایستگاه وجود دارد که توسـط یک مسیر بسته به یکدیگر مرتبط شده اند. جانمایی اجزاء ایستگاه مطابق با قوانین ودستورالعملهای جاری در راه آهن ایران میباشـد. این جانمایی شامل ۳۸ جـزء مـسیر، ۷ سـوزن، ۲۵ سـیگنال، کـه شامل سیگنال اصـلی ،شـانت و سـیگنال فاصـله میباشـد. در ایـن چیدمان ۲۹ مسیر ممکن دیده شده اسـت کـه شـامل مـسیرهای اصلی، مسیر شـانت و مـسیر فراخـوان میباشـد. مقـرر اسـت ایـن مجموعه تحت کنترل یک اینترلاکینگ متمرکز باشد.

شکل شماره ۱:عکس ماکت موجود در آزمایشگاه دانشکده مهندسی راه آهن

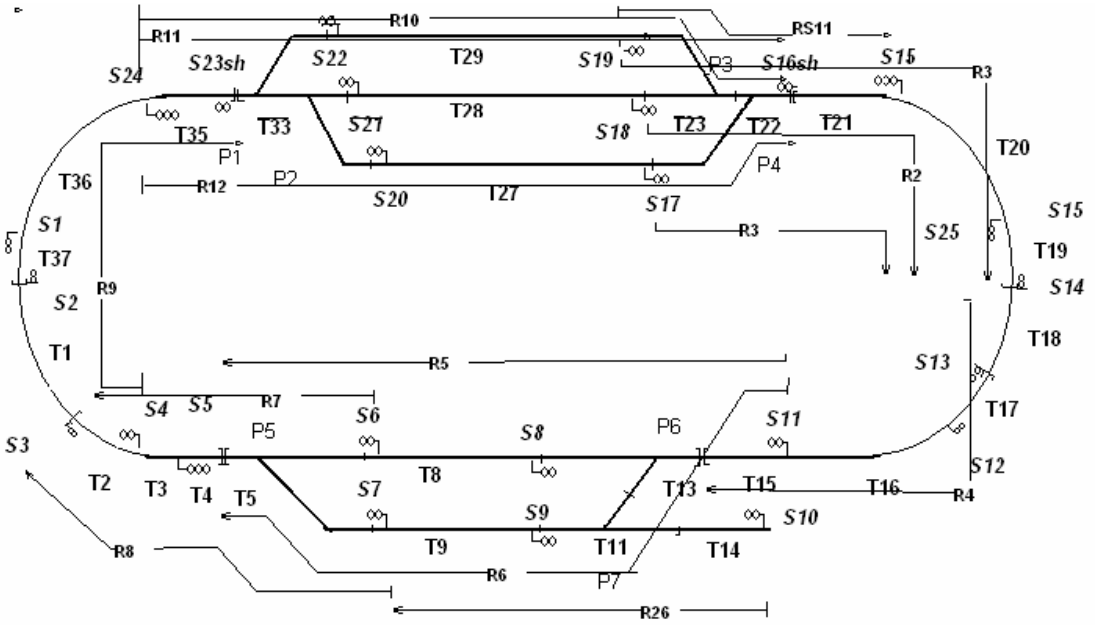


شکل شماره ۲: شماتیک اجزاء مدل برای ماکت آزمایشگاه

البته سعی شده است عمومیت مدل حفظ شود و قابل استفاه با اندکی تغییر برای چیدمانهای دیگر نیز باشد. شکل سه و چهار قسمتی از مسیرهای جهت عقربه های ساعت و خلاف جهت عقربه های ساعت را نشان میدهد.لازم به ذکر است به منظور خوانا بودن شکل، تمام مسیر ها در شکل مشخص نگردیده است . همانطور که از شکل ها مشخص میباشد مسیرهای اصلی دارای جزء مسیر مشترک[1] میباشد. همچنین مسیرهای شانت دارای جزء مسیر مشترک نمی باشد.

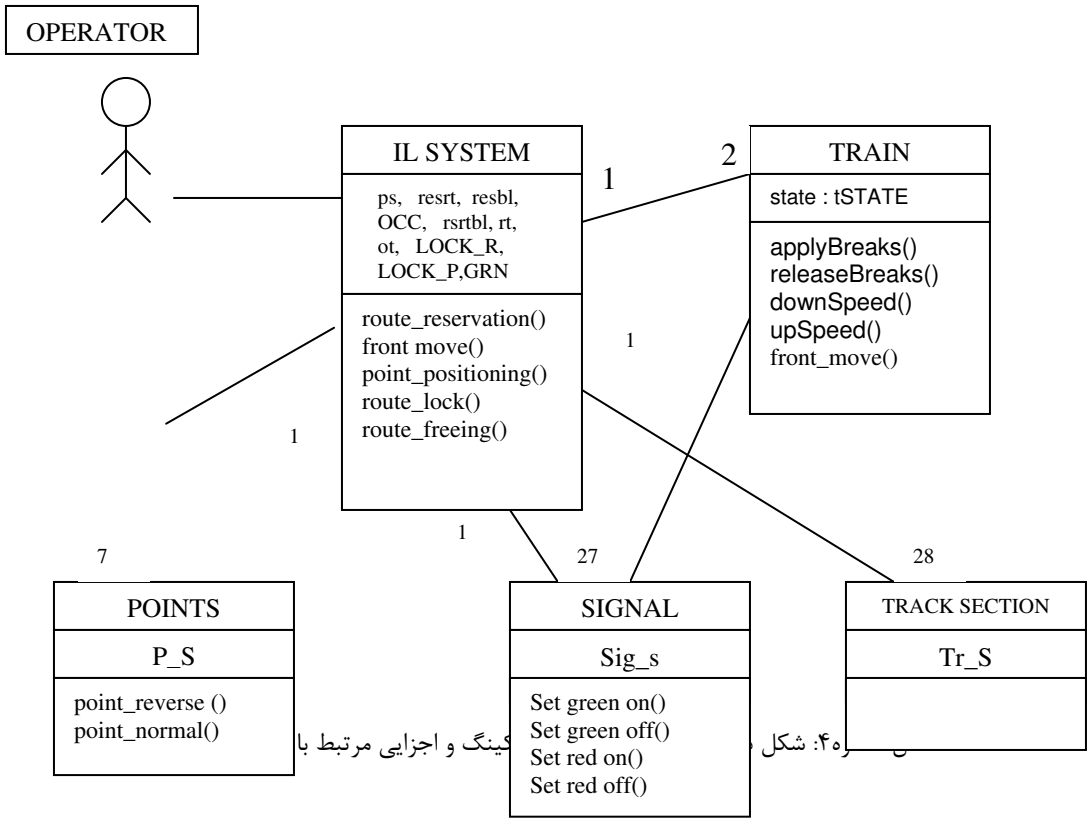
برای رزو نمودن هر مسیر برای قطاری مشخص، لازم است قطار در پیشنیاز آن مسیر باشد. مجموعه پیش نیازهای یک مسیر ممکن است شامل مسیرهای مستقیم و معکوس(همجهت یا خلاف جهت عقربه های ساعت) باشد.

[1] overlap

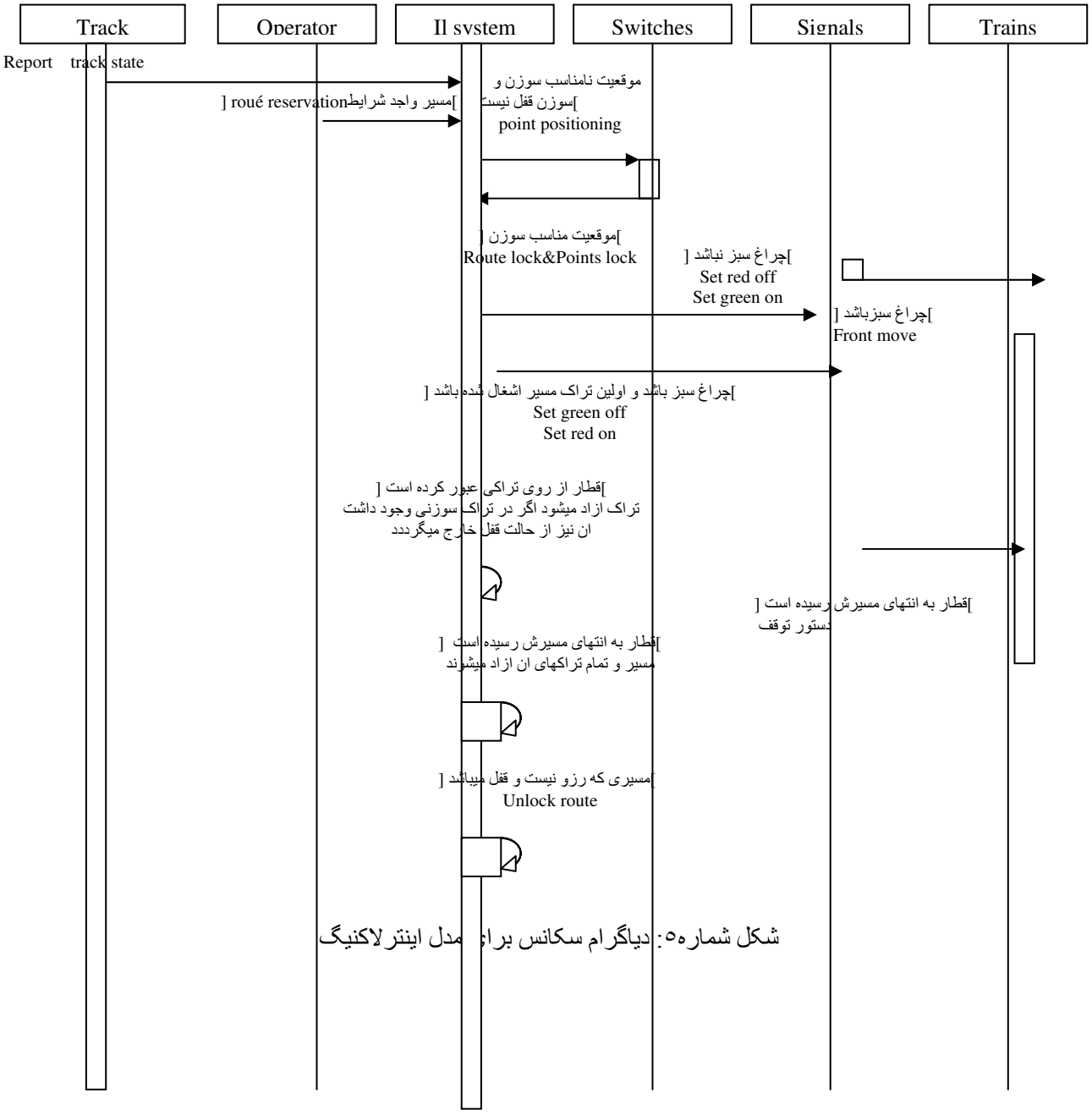


شکل شماره۳: مسیرهای جهت عقربه های ساعت در شکل ماکت ایستگاهها

خلاصه سیستم در نمودار کلاس شکل ۴ مشخص گردیده است. شکل برای یک قطار تنظیم شده است هرچندکه تعداد بیشتر قطار فقط سایز مسئله را بزرگ مینماید و چیزی به پیچیدگی مسئله اضافه نمیکند. سناریو اتفاقات ممکن در مدل در شکل ۵ که یک نمودار سکانس(Sequence) میباشد، بیان گردیده است.



ه۴: شکل کینگ و اجزایی مرتبط با



شکل شماره۵: دیاگرام سکانس برای مدل اینترلاکنیگ

ماشین مجرد [1]

موضوعات اصلی که بدنه مدل را تشکیل میدهند در اولین گام ایجاد مدل یعنی در ماشین مجرد مطرح میگردند. در مراحل بعد جزییات طی کامل نمودن عملیاتها [2] و یا طرح عملیات جدید به مرور اضافه شده و مدل را کامل تر مینمایند که به آن پالاش گوییم .پالایش میتواند یا ماشین مجرد را کامل نماید ویا پالایش مرحله قبلی خود را کامل تر کند. در اینجا ماشین مجرد (M0)درخصوص تعریف جزء مسیر ورزرو نمودن مسیر میباشد. برخی از عملگر ها مانند رزرو نمودن، حرکت، و آزاد سازی جزء مسیر در این سطح ایجاد شده است.

پالایشها [3]

اولین پالایش r1 مربوط سوزنها، تنظیم مسیر، قفل مسیر و رهاسازی ها می باشد. عملگرها شامل تنظیم موقعیت سوزن، قفل مسیر، آزاد سازی مسیرو رها سازی آن بوده و پالایش مرحله دوم در خصوص سیگنالها میباشد. در این قسمت برخی توضیخات راجع به ماشین مجرد، پالایش و جدول توصیف متغیرها بیان شده است. برخی از پیش شرطهای مهم تر در قسمت بعد توضیح داده شده است.

[1] Abstract machine
[2] Operation
[3] Refinement

جدول ۱ توصیف متغیرها و مجموعه ها

توضیحات	نام متغیر و یا مجموعه	توضیحات	نام متغیر و یا مجموعه
مجموعه جزمسیر- مسیر	rsrtbl	مسیر	R
مجموعه مسیر های پیشین(مستقیم)	nei	مجموعه جزمسیر- قطار	ot
مجموعه جزءمسیرها	TS	مجموعه مسیر های پیشین(معکوس)	rv
مجموعه قطار ها	TRAINS	مجموعه مسیر ها	RR
توالی اجزاء مسیر	nxt	جدول مسیر ها	rtbl
آخرین جزء مسیر	lst	اولین جزء مسیر	fst
جزء مشترک انتهایی- مسیر	r_ovl	جزء مسیر مشترک	ovl
مجموعه جزء مسیرهای اشغال شده	occ	مجموعه مسیر رزرو شده	resrt
وصعیت سوزن	ps	مجموعه مسیر_قطار	rt
مجموعه سیگنالهای	SIGNAL	وصعیت صحییح سوزن برای مسیر	prcs
		مجموعه سیگنالهای سبز	GRN

در این قسمت چند پیش شرط مربوط به رزرو نمودن مسیر آمده است .

rtbl~[{r}]/\OCC={}
rtbl~[{r}]/\resbl={}
rsrtbl[ot~[{t}]]/\LOCK_R={}

این پیش شرایط تضمین مینماید که مسیری که مقرر است رزرو شود میبایست دارای اجزای خالی، غیر رزرو و غیر قفل باشد.

r:nei~[{rsrtbl(ot~(t))}]\/
rv~[{rsrtbl(ot~(t))}]&

همچنین این شرط تضمین میکند برای هر مسیر که مقرر است رزرو شود قطار مسیر پیشین را اشغال نموده باشد. برای تنظیم سوزن جفت، از شرط زیر استفاده مینماییم که تضمین میکند سوزنهای جفت دارای یک وضعیت میباشد وهنگامیکه سوزنهای مسیر در وضعیت صحیح میباشند، مسیر میتواند رزرو شود.

!(r_,p_).(r_:resrt-LOCK_R & p_:PP & p_|->r_:pr =>ps(p_)=prcs(p_|->r_))&
!(p_).(p_:dom(p_pair)=>ps(p_)=ps(p_pair(p_)))

آنالیز و اثبات مدل

اثبات مدل در روش رسمی به دوصورت امکان پذیر میباشد که شامل روش استنتاجی و آزمون مدل میباشد. در روش اول با ابزار های خودکار موجود برای روشهای رسمی میتوان به تولید قضایای موجود اقدام نمود[1]. درمرحله بعدی با کمک اثبات کننده های خودکار اقدام به درستنمایی مدل مینماییم. مرحله اثبات دو دسته قضیه را مشخص میسازند. قضایایی که در این مرحله اثبات میشوند و قضایای که در ای مرحله اثبات نمی شوند. برای قضایای اثبات نشده میبایست با روشها تجزیه تحلیلی و با تغییرات لازم سعی در اثبات قضایا نمود ودر صورتی که قضیه ایی ثابت نشد

[1] Automated theorem prover(ATP)

نشانگر خطـا در مـدل میباشـد. در مقابـل روش اسـتنتاجی روش آزمون مدل قرار دارد. در این نـوع اثبـات بـا اسـتفاده از ابزارهـای آزمون مدل میتوان به کاوش کل فضای حالـت موجـود پرداخـت. بدین ترتیب میتوان اطمینان کسب کرد کـه در تمـام سـناریوهای ممکن که میتواند در سیستم رخ دهد، مدل فاقد خطا میباشد

اثبات قـضایا بـرای سیـستمهای کـامپیوتری همیـشه کـار آسـانی نمیباشد و نیاز با صرف وقت و هزینـه فراوانـی دارد همـانطور کـه کاوش تمام فضای حالـت در روش دوم نیـز همیـشه امکـان پـذیر نیست. ابزار استفاده شده برای روش اسـتنتاجی Atelier Bبـوده و برای روش آزمون مدل از ابزار ProB استفاده شده است. نتایج چک مدل نشان میدهد کـه۴۰ - PO [1] در سـطح ماشـین وجـود دارد و همچنین ۴۶ PO در اولـین پـالایش و ۴۸ PO در دومـین پالایش قرار دارد. تمامی PO ها در با بکار گیری ابزار AtelierB اثبات گردید همچنین با ابزار تـست آزمـون ProB تمـام حـالات مدل کاوش و چک گردید. شرح قضایای مراحـل ماشـین مجـرد و دوپالایش متوالی آن در جدل شماه دو آمده اسـت و هـر عـدد در جدول تعداد قضایای هر عملیات در پالایـشهای متخلـف را نـشان میدهد.

[1] proof obligations

جدول شماره ۲: تعداد POهر عملگر در پالایشهای مختلف

	Abstarct Machine	Refine (r1)	Refine (r2)
Initialisation	8	7	3
Route_reservation1	4	1	0
Route_reservation 2	4	1	0
Point_positioning	-	3	1
Point_positioning 2	-	3	1
Front_move_1	3	1	5
Route_lock	-	3	7
Route_freeing	-	3	3
Back_move 1	6	12	13
Back_move_2	6	10	11
Front _move_2	9	2	4
	40	46	48

نتیجه گیری

همانطور که اشاره گردید مدل با یکصد هزار گره [1] کاوش شد که این کاوش حدودا هشت ساعت به طول انجامید. حال این سوال مطرح میگردد که اگر مقرر بود در عمل این یکصد هزار حالت، با چک برنامه توسط اپراتوری صورت گیرد چه میزان وقت لازم بود. در حالت خوشبینانه اگه در عمل دویست حالت سیستم در روز قابل کاوش باشد برای کاوش این تعداد حالت به پانصد روز زمان نیاز هست. که در واقع کاری غیر ممکن به نظر میرسد ودر نهایت میتوان گفت :

درست است که استفاده از متد رسمی روشی زمانبر میباشد ولی این تجربه نشان داد که چگونه مشخصات پیچیده با این روش به خوبی بیان میشود و نیز خطاهای که یافتن آنها درعمل بسیار مشکل میباشد توسط این روش به راحتی و روشنی قابل کشف و رفع میباشد و در نهایت با کاوش تمام سناریوهای ممکن و اثبات قضایا اطمینان از عملکرد صحیح سیستم حاصل میشود.

مقاله حاضر اولین تلاش در جهت بکارگیری متد B در مدلسازی و درست نمای سیستمهای اینترلاکینگ میباشد. بدین جهت مفروضات زیر بعنوان فرضهای ساده کننده لحاظ شده است که امید است در تحقیقات آتی مد نظر قرار گیرد:

- همانطور که در قوانین سطح دو بیان شد، اپراتور مجاز به رزرو نمودن چند مسیر برای ترن بطور همزمان نمیباشد.
- در عملیات شانت به هم پیوستن واگن و ایجاد یک قطار گنجانده نشده است.
- در عملیات شانت جدا شدن چند واگن و پیوستن به قطار دیگر لحاظ نشده است.
- ایزوله نمودن مسیر در مدل گنجانده نشده است .
- امکان پیوستن قطارها و ایجاد قطاری جدید و یا جدا شدن و پیوستن به قطار لحاظ نگردیده است.

مراجع

[1] Wikipedia encyclopedia www.wikipedia.org

[1] node

[2] L.-H. Eriksson, K. Johansson" Using formal methods for quality
assurance of interlocking systems "Swedish National Rail Administration,

[3]Marcano, S. Colin , G. Mariano " A Formal Framework for UML Modelling with Timed Constraints: Application to Railway Control Systems" National Institute for Transport and Safety Research INRETS-ESTAS ,2003

[4] Mirabadi A., Yazdi M. B., “Automatic generation and verification of railway interlocking control tables using FSM and NuSMV”, Transport Problems, Vol 4, No. 1, 2009

[5]J.R Abrial "Formal method-train system" sld. lecture 9 ,January 2006

[6]Thierry Lecomte 1, Thierry Servat 1, Guilhem Pouzancre"Formal Methods in Safety-Critical Railway Systems" ClearSy, Aix en Provence, France.