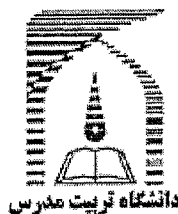


بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

٩٣٢٥٩



دانشگاه تربیت مدرس

دانشکده فنی و مهندسی

پایان‌نامه‌ی دوره کارشناسی ارشد مهندسی کامپیوتر - نرم‌افزار

راستی آزمایی حین اجرای برنامه‌های واکنشی بی‌درنگ با رویکرد منطق بی‌درنگ

مهدی میرزاآقایی

استاد راهنما :

دکتر سعید جلیلی

زمستان ۱۳۸۵

۱۳۸۷ / ۱۲ / ۲۵

۹۳۲۵۹

وزارت معارف و اوقاف و صنایع مستظرفه
تربیت مدرس



بسمه تعالی

تاییدیه هیات داوران

آقای مهدی میرزاآقایی پایان نامه ۹ واحدی خود را با عنوان راستی آزمایی حین اجرای برنامه های واکنشی بی درنگ بارویکرد منطق بی درنگ در تاریخ ۱۳۸۵/۱۱/۸ ارائه کردند. اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده و پذیرش آنرا برای تکمیل درجه کارشناسی ارشد مهندسی برق - مهندسی کامپیوتر نرم افزار پیشنهاد می کنند.

اعضای هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر سعید جلیلی	استادیار	
استاد ناظر	دکتر نصراله مقدم چرکری	استادیار	
استاد ناظر	دکتر محمدتقی حمیدی بهشتی	استادیار	
استاد ناظر	دکتر - میریان		
مدیر گروه (یا نماینده گروه تخصصی)	دکتر نصراله مقدم چرکری	استادیار	

این نسخه به شماره ثبت نهایی پایان نامه مورخه ۱۳۸۵/۱۱/۸ تایید است.
اعضای هیات داوران

دستور العمل حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقامه: با عنایت به سیاست های پژوهشی دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران لازم است اعضای هیات علمی دانشجویان دانش آموختگان و دیگر همکاران طرح در مورد نتایج پژوهشهای علمی که تحت عناوین پایان نامه رساله و طرحهای تحقیقاتی با هماهنگی دانشگاه انجام شده است موارد ذیل را رعایت نمایند:

ماده ۱: حقوق مادی و معنوی پایان نامه ها / رساله های مصوب دانشگاه متعلق به دانشگاه است و هر گونه بهره برداری از آن باید با ذکر نام دانشگاه و رعایت آیین نامه ها و دستورالعمل های مصوب دانشگاه باشد.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان نامه / رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی می باید به نام دانشگاه بوده و استاد راهنما نویسنده مسئول مقاله باشند.

تبصره: در مقالاتی که پس از دانش آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان نامه / رساله نیز منتشر می شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب حاصل از نتایج پایان نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آیین نامه های مصوب انجام می شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه در جشنواره های ملی، منطقه ای و بین المللی که حاصل نتایج مستخرج از پایان نامه / رساله و تمامی طرح های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق حوزه پژوهشی دانشگاه انجام گیرد.

ماده ۵- این دستورالعمل در ۵ ماده و یک تبصره در تاریخ ۱۳۸۴/۴/۲۵ در شورای پژوهشی دانشگاه به تصویب رسیده و از تاریخ تصویب لازم الاجرا است و هر گونه تخلف از مفاد این دستورالعمل، از طریق مراجع قانونی قابل پیگیری خواهد بود.

تقدیم به دیدگانم

به حامیان بزرگ زندگی‌ام

آنان که عاشقانه دوستشان دارم

تقدیم به پدر و مادر عزیزم

و خواهران مهربانم

تشکر و قدردانی

سپاس خداوند منان را که بار دیگر دری از درهای رحمت خود را بر من گشود و به من توفیق کسب علم، در راستای افزایش درک خویش از عظمت باری تعالی و شکوه جهان هستی مرحمت نمود. زیرا هر آنچه که بر انسان اتفاق می‌افتد بهانه‌ای است برای شناخت بهتر از جهان هستی و نزدیکی بیشتر با باری تعالی؛ این پژوهش نیز از این قاعده مستثنی نیست هر چند که در نگاه اول موضوع پژوهش چنین حسی را تداعی نمی‌کند.

در فرایند انجام این پژوهش از استاد گرانقدر جناب آقای دکتر سعید جلیلی درس‌های علمی و اخلاقی بی‌شماری را آموختم. از ایشان به دلیل این‌که طی مدت زمان انجام این پژوهش تجربیات ارزنده و چندین ساله‌ی خود را در اختیار اینجانب قرار دادند، نهایت تشکر را دارم.

حضور و نقش کلیدی پدر، مادر و خواهران عزیزم غیر قابل چشم‌پوشی است؛ زیرا اگر نبود زحمات و پشتیبانی‌های عاطفی آنها، انجام این پژوهش یا میسر نمی‌شد و یا با مشقت‌های فراوان انجام می‌شد. قدردان تمام حمایت‌های ایشان هستم.

از جناب آقای دکتر نصراله مقدم، به دلیل حمایت‌های بی‌دریغشان و اعضای محترم هیات داوران به دلیل صرف وقت برای ارزیابی این پژوهش، نهایت تشکر را دارم.

آخرین و نه کمترین سپاس من از آقایان غلامرضا شاه‌محمدی، مهدی آبادی، محرم منصوری‌زاده و سید مرتضی بابامیر به دلیل صرف وقت و راهنمایی‌هایشان است.

امید است، این پژوهش دریچه‌ای برای گام‌های وسیع‌تر باشد.

مهدی میرزاآقایی

۸۵/۱۱/۲

چکیده

رویکردهای متداول واریسی و اعتبارسنجی نرم‌افزار برای برنامه‌های واکنشی بی‌درنگ به اندازه کافی قابل اعتماد نیستند. با توجه به پیچیدگی زیاد رویکرد واریسی رسمی و کامل نبودن رویکرد آزمون، رویکرد راستی‌آزمایی حین اجرا پیشنهاد شده است. این رویکرد، به علت این که در محیط واقعی اجرا می‌گردد، قادر به کشف خطاهایی است که تاکنون آشکار نشده‌اند. به عبارت دیگر، مکملی برای دو رویکرد فوق محسوب می‌شود.

در این پایان‌نامه، چارچوبی جهت راستی‌آزمایی حین اجرای برنامه‌های واکنشی بی‌درنگ ارائه شده است که علاوه بر مستقل بودن از زبان بیان ویژگی‌ها، توانایی اجرای همراه با برنامه تحت پایش را دارد و می‌تواند برنامه را در هنگام بروز وضعیت ناهنجار به حالت ایمنی ببرد. همچنین از رویکرد جنبه‌گرا برای ابزارآزمایی ویژگی‌های ایمنی استفاده شده است. این چارچوب در سه فاز، عمل راستی‌آزمایی ویژگی‌ها را انجام می‌دهد. در فاز اول، ویژگی‌های ایمنی پس از استخراج از مسئولیت‌های برنامه با یک منطق‌زمانی بیان گردیده و رفتار تحمل‌پذیری برنامه در برابر نقض این ویژگی‌ها به آن اضافه می‌شود. راستی‌آزمای رفتار برنامه در حین اجرا که توسط جنبه‌های زمانی، عملیاتی و ضرب‌الاجل تحقق می‌یابد، به کد برنامه بافته می‌شود و در محیط به همراه کد برنامه اجرا می‌گردد. راستی‌آزمای رفتار برنامه را در نقاط اتصال با توجه به ویژگی‌های ایمنی مربوطه، مورد بررسی قرار داده و در صورت تشخیص نقض ویژگی، رفتار مشخصی (تحمل‌پذیری در برابر نقض ویژگی) را از خود نشان داده و برنامه را به وضعیت ایمنی می‌برد که روش‌های متداول قادر به انجام این کار نیستند و تنها به رویدادنگاری بسنده می‌کنند.

این چارچوب با دو روش بیان ویژگی‌های RTL و ERL مدل‌سازی و اجرا گردید. RTL به علت این که توانایی بیان ویژگی‌های بی‌درنگ نظیر تأخیر، ضرب‌الاجل و چندین وقوع یک رخداد خاص را دارد، به راحتی می‌تواند در بیان ویژگی‌های زمانی برنامه‌های واکنشی بی‌درنگ بکار گرفته شود. ERL نیز به علت این که مختص برنامه‌های بی‌درنگ طراحی شده است و دارای بیان ساده و روانی می‌باشد، برای راستی‌آزمایی حین اجرا بکار گرفته شده است.

آزمایشات نشان می‌دهد که چارچوب پیشنهادی، نقض تمام ویژگی‌های تحت راستی‌آزمایی را تشخیص می‌دهد. سربار چارچوب پیشنهادی از ۴٪ تا ۳۳٪ می‌باشد که با توجه به تعداد و نوع ویژگی‌های مورد پایش و زبان بیان ویژگی‌ها تعیین می‌گردد. در ضمن مشخص شد که سربار چارچوب پیشنهادی با افزایش تعداد ویژگی‌ها بصورت خطی افزایش می‌یابد.

کلمات کلیدی: راستی‌آزمایی حین اجرا، برنامه واکنشی بی‌درنگ، منطق‌زمانی بی‌درنگ، منطق بی‌درنگ رویدادگرا، برنامه‌نویسی جنبه‌گرا.

فهرست مطالب

عنوان.....	صفحه.....
۱- کلیات.....	۱
۱-۱- مقدمه.....	۱
۲-۱- صورت مسئله.....	۱
۳-۱- اهداف و نتایج حاصل از پژوهش.....	۴
۴-۱- مروری بر فصول پایان نامه.....	۵
۲- مفاهیم پایه.....	۸
۱-۲- مقدمه.....	۸
۲-۲- منطق زمانی.....	۸
۳-۲- منطق بی درنگ.....	۱۰
۱-۳-۲- مدل رخداد-عمل.....	۱۱
۲-۳-۲- ابعاد منطق بی درنگ.....	۱۲
۳-۳-۲- زبان RTL.....	۱۳
۴-۳-۲- معنی فرمول‌های RTL.....	۱۵
۵-۳-۲- مسندهای وضعیت.....	۱۶
۶-۳-۲- منطق بی درنگ محدود شده.....	۱۸
۴-۲- منطق بی درنگ رویدادگرا.....	۱۹
۱-۴-۲- مفاهیم.....	۱۹
۲-۴-۲- مسندهای پایه‌ای ERL.....	۲۱
۵-۲- رویکرد جنبه‌گرایی.....	۲۲
۱-۵-۲- نگاه به نرم‌افزار به عنوان مجموعه‌ای از دغدغه‌ها.....	۲۳
۲-۵-۲- دغدغه‌های برش عرضی در یک نرم‌افزار.....	۲۴
۳-۵-۲- مشکلات دغدغه‌های برش عرضی.....	۲۵
۴-۵-۲- مفاهیم AOP.....	۲۶
۵-۵-۲- فوائد AOP.....	۲۸
۶-۵-۲- جنبه.....	۲۸
۷-۵-۲- بافتن.....	۳۰
۸-۵-۲- AspectJ: یک پیاده‌سازی AOP برای جاوا.....	۳۱

۳۱	۶-۲- سیستم گذرگاه راه آهن
۳۲	۱-۶-۲- تاریخچه
۳۳	۲-۶-۲- تعریف مسئله
۳۳	۳-۶-۲- بیان مسئله
۳۴	۷-۲- نتیجه گیری
۳۶	۳- چالش های واری و اعتبارسنجی نرم افزار
۳۶	۱-۳- مقدمه
۳۷	۲-۳- واری و اعتبارسنجی
۴۰	۳-۳- واری رسمی
۴۰	۱-۳-۳- رویکرد بازبینی مدل
۴۱	۲-۳-۳- رویکرد اثبات قضیه
۴۱	۳-۳-۳- مقایسه رویکردها
۴۲	۴-۳- آزمون
۴۳	۱-۴-۳- رویکرد آزمون جعبه سیاه
۴۴	۲-۴-۳- رویکرد آزمون جعبه سفید
۴۵	۳-۴-۳- مقایسه روش ها
۴۵	۴-۴-۳- دسته بندی کلی آزمون نرم افزار
۴۷	۵-۴-۳- اوراکل آزمون
۴۷	۶-۴-۳- کفایت آزمون
۴۸	۵-۳- مقایسه رویکردهای واری رسمی و آزمون
۴۹	۶-۳- راستی آزمایی حین اجرا
۵۱	۷-۳- نتیجه گیری
۵۲	۴- تاریخچه پژوهش
۵۲	۱-۴- مقدمه
۵۲	۲-۴- روش های مبتنی بر منطق
۵۲	۱-۲-۴- روش جهانیان و همکاران
۵۴	۲-۲-۴- روش Barringer و همکاران
۵۵	۳-۲-۴- روش LOLA
۵۶	۴-۲-۴- روش Kristoffersen و همکاران
۵۸	۳-۴- روش های مبتنی بر آتاماتا

۵۸MCM روش ۱-۳-۴
۵۹ روش Stolz و همکارش ۲-۳-۴
۶۰ روش‌های مبتنی بر زبان ۴-۴
۶۰ روش MaCS ۱-۴-۴
۶۲ روش Klose و همکارش ۲-۴-۴
۶۲ نتیجه‌گیری ۵-۴
۶۳ روش پیشنهادی برای راستی‌آزمایی حین اجرای برنامه‌های واکنشی بی‌درنگ ۵-۴
۶۳ مقدمه ۱-۵
۶۳ چارچوب پیشنهادی ۲-۵
۶۴ استخراج و آماده‌سازی ویژگی‌های ایمنی ۱-۲-۵
۶۷ ابزارآمایی ۲-۲-۵
۷۱ راستی‌آزمایی حین اجرای برنامه‌ها ۳-۲-۵
۷۲ چارچوب پیشنهادی با زبان بیان RTL ۳-۵
۷۲ استخراج و آماده‌سازی ویژگی‌های ایمنی ۱-۳-۵
۷۳ ابزارآمایی ۲-۳-۵
۷۵ چارچوب پیشنهادی با زبان بیان ERL ۴-۵
۷۶ استخراج و آماده‌سازی ویژگی‌های ایمنی ۱-۴-۵
۷۶ ابزارآمایی ۲-۴-۵
۸۰ نتیجه‌گیری ۵-۵
۸۱ ارزیابی روش پیشنهادی ۶-۵
۸۱ مقدمه ۱-۶
۸۱ پیاده‌سازی سیستم گذرگاه راه‌آهن ۲-۶
۸۳ مزایای ASPECTJ ۳-۶
۸۴ ارزیابی چارچوب پیشنهادی با زبان بیان RTL ۴-۶
۸۴ استخراج و آماده‌سازی ویژگی‌های ایمنی ۱-۴-۶
۸۶ ابزارآمایی ۲-۴-۶
۸۸ تحلیل نتایج ۳-۴-۶
۹۲ ارزیابی چارچوب پیشنهادی با زبان بیان ERL ۵-۶
۹۲ استخراج و آماده‌سازی ویژگی‌های ایمنی ۱-۵-۶
۹۳ ابزارآمایی ۲-۵-۶

۹۴ ۶-۵-۳- تحلیل نتایج
۹۸ ۶-۶- مقایسه دو روش بیان ویژگی ها
۹۹ ۶-۷- مقایسه روش های راستی آزمایی حین اجرا
۱۰۱ ۶-۷-۱- زبان توصیف
۱۰۳ ۶-۷-۲- راستی آزما
۱۰۵ ۶-۷-۳- عمل بعد از تشخیص نقض ویژگی ها
۱۰۸ ۶-۷-۴- سایر عوامل
۱۰۹ ۶-۸- نتیجه گیری
۱۱۰ ۷- نتیجه گیری و پژوهش های آتی
۱۱۰ ۷-۱- مقدمه
۱۱۱ ۷-۲- نتایج حاصل از پژوهش
۱۱۳ ۷-۳- پژوهش های آتی
۱۱۴ مراجع و منابع
۱۱۸ واژه نامه انگلیسی به فارسی
۱۲۳ واژه نامه فارسی به انگلیسی

فهرست جداول

عنوان.....	صفحه.....
جدول ۱-۲: مسندها و تعریف آن‌ها در ERL.....	۲۱
جدول ۱-۳: مقایسه رویکردهای راستی‌آزمایی و اعتبارسنجی نرم‌افزار.....	۵۰
جدول ۱-۵: نحوه انتخاب مسندهای منطقی برای درج در جدول زمانی برای زبان بیان ERL.....	۷۷
جدول ۱-۶: نتایج بدست آمده در حالتی که جدول رخداد در حافظه اصلی قرار دارد.....	۸۹
جدول ۲-۶: نتایج بدست آمده در حالتی که جدول رخداد در دیسک قرار دارد (RTL).....	۹۰
جدول ۳-۶: نتایج بدست آمده در حالتی که جدول رخداد در حافظه اصلی قرار دارد (ERL).....	۹۵
جدول ۴-۶: نتایج بدست آمده در حالتی که جدول رخداد در دیسک قرار دارد (ERL).....	۹۶
جدول ۵-۶: مقایسه رویکردهای راستی‌آزمایی حین اجرا از نظر زبان توصیف.....	۱۰۳
جدول ۶-۶: مقایسه روش‌های راستی‌آزمایی حین اجرا از نظر راستی‌آزما.....	۱۰۶
جدول ۷-۶: مقایسه روش‌های راستی‌آزمایی حین اجرا از نظر عمل بعد از تشخیص نقض ویژگی‌ها.....	۱۰۷
جدول ۸-۶: مقایسه روش‌های راستی‌آزمایی حین اجرا از نظر سایر عوامل.....	۱۰۹

فهرست اشکال

عنوان.....	صفحه.....
شکل ۱-۲: پیاده‌سازی پیمانها به صورت مجموعه‌ای از دغدغه‌ها [۲۹].....	۲۳
شکل ۲-۲: جداسازی دغدغه‌ها: قیاس منشور [۲۹].....	۲۴
شکل ۳-۲: یک کلاس که منطقی را پیاده‌سازی می‌کند [۲۹].....	۲۵
شکل ۴-۲: مراحل توسعه نرم‌افزار با رویکرد AOP [۲۹].....	۲۷
شکل ۵-۲: نمونه‌ای از جنبه.....	۲۹
شکل ۶-۲: نمایی از سیستم گذرگاه راه‌آهن.....	۳۴
شکل ۱-۳: جایگاه راستی‌آزمایی رسمی و آزمون در نرم‌افزار.....	۳۷
شکل ۲-۳: بررسی زمانی مدل.....	۴۱
شکل ۳-۳: دسته‌بندی روش‌های آزمون بر حسب اجرا.....	۴۳
شکل ۴-۳: فرایند آزمون جعبه سیاه [۵۵].....	۴۴
شکل ۵-۳: فرایند آزمون جعبه سفید [۵۵].....	۴۵
شکل ۶-۳: سه دیدگاه مختلف از آزمون نرم‌افزار [۵۵].....	۴۶
شکل ۱-۴: چارچوب روش MACS [۷۰].....	۶۱
شکل ۱-۵: چارچوب پیشنهادی.....	۶۴
شکل ۲-۵: فرایند استخراج ویژگی‌ها.....	۶۵
شکل ۳-۵: فرایند ابزارآزمایی.....	۶۸
شکل ۴-۵: ضوابط تولیدکننده جنبه ضرب‌الاجل.....	۷۰
شکل ۵-۵: جنبه ضرب‌الاجل.....	۷۱
شکل ۶-۵: راستی‌آزمایی حین اجرا.....	۷۲
شکل ۷-۵: ساختار جدول رخداد (EVENTTABLE) برای زبان بیان RTL.....	۷۳
شکل ۸-۵: ضوابط تولیدکننده جدول رخداد (EVENTTABLE) برای زبان بیان RTL.....	۷۴

- شکل ۵-۹: ضوابط تولیدکننده جنبه زمانی ۷۵
- شکل ۵-۱۰: تولیدکننده جنبه عملیاتی ۷۵
- شکل ۵-۱۱: ساختار داده جدول رخدادهای در ERL ۷۷
- شکل ۵-۱۲: ضوابط تولیدکننده جنبه زمانی برای زبان بیان ERL ۷۸
- شکل ۵-۱۳: ضوابط تولیدکننده جنبه عملیاتی برای زبان بیان ERL ۷۹
- شکل ۶-۱: نمایی از APPLETT پیاده‌سازی شده سیستم گذرگاه راه‌آهن ۸۱
- شکل ۶-۲: نمودار کلاس سیستم گذرگاه راه‌آهن ۸۲
- شکل ۶-۳: نمودار توالی اجرای برنامه ۸۳
- شکل ۶-۴: مشخصات خواسته‌های سیستم گذرگاه راه‌آهن ۸۵
- شکل ۶-۵: بیان ویژگی‌ها ایمنی سیستم گذرگاه راه‌آهن به RTL ۸۶
- شکل ۶-۶: بخشی از نمودار کلاس سیستم گذرگاه راه‌آهن ۸۶
- شکل ۶-۷: جنبه زمانی ویژگی ایمنی (۳) ۸۷
- شکل ۶-۸: سربار ناشی از راستی‌آزمایی حین اجرا با RTL (جدول رخداد در حافظه اصلی) ۸۹
- شکل ۶-۹: سربار ناشی از راستی‌آزمایی حین اجرا با RTL (جدول رخداد در دیسک) ۹۰
- شکل ۶-۱۰: روند کاهش سربار با توجه به افزایش تعداد ویژگی‌ها ۹۲
- شکل ۶-۱۱: بیان ویژگی‌ها ایمنی سیستم گذرگاه راه‌آهن به ERL ۹۳
- شکل ۶-۱۲: جنبه زمانی ویژگی ایمنی (۶) ۹۴
- شکل ۶-۱۳: سربار ناشی از راستی‌آزمایی حین اجرا با ERL (جدول رخداد در حافظه اصلی) ۹۶
- شکل ۶-۱۴: سربار ناشی از راستی‌آزمایی حین اجرا با ERL (جدول رخداد در دیسک) ۹۷
- شکل ۶-۱۵: روند کاهش سربار نسبت به افزایش تعداد ویژگی‌ها در ERL ۹۸
- شکل ۶-۱۶: رده‌بندی معیارهای ارزیابی روش‌های راستی‌آزمایی حین اجرای برنامه‌ها [۴] ۱۰۰

فصل اول

کلیات

فصل اول

کلیات

۱-۱- مقدمه

امروزه نرم افزارها کاربردهای گسترده‌ای پیدا کرده‌اند که این گستردگی و دامنه استفاده، باعث افزایش پیچیدگی آن شده است. در کاربردهای خاصی مانند کنترل قطارها، کاربردهای پزشکی، فضاپیماها و غیره در صورتی که شکستی در نرم افزار بوجود بیاید هزینه‌های جبران ناپذیری مثل صدمات جانی و هزینه‌های مالی عظیمی خواهد داشت. بنابراین مقوله اعتبارسنجی نرم افزارها از اهمیت فوق‌العاده‌ای برخوردار است.

۱-۲- صورت مسئله

در دو دهه اخیر تلاش‌های زیادی برای تحلیل و اعتبارسنجی^۱ برنامه‌های واکنشی بی‌درنگ انجام شده است. به علت ماهیت این گونه برنامه‌ها که معمولاً حیاتی و حساس هستند، از روش‌های متداول برای اعتبارسنجی آنها استفاده نمی‌شود، چراکه زبان‌های برنامه نویسی رایج قابل اعتماد نیستند و اعتبارسنجی آنها به طور کامل قابل انجام نیست [۱].

روش متداولی که برای آشکارسازی خطا در برنامه‌ها بکاربرده می‌شود، آزمون پیاده‌سازی برنامه توسط مجموعه ورودی‌های مشخص است. این رویکرد نمی‌تواند درستی پیاده‌سازی را برای تمام توالی‌های ورودی برنامه (که یک مجموعه نامحدود است) تضمین کند. بنابراین تضمینی برای عملکرد درست برنامه هنگام اعمال ورودی‌های داده نشده نمی‌دهد [۲، ۳]. بنابراین هیچگاه از طریق این رویکرد نمی‌توان بطور کامل به رفتار برنامه اطمینان پیدا کرد. علاوه بر آن تولید مجموعه ورودی‌ها برای برنامه‌های واکنشی بی‌درنگ بسیار مشکل‌تر از برنامه‌های عادی است [۴]. در سال

^۱ Validation

۲۰۰۲ گزارش RTI^۱ به انستیتو ملی استاندارد و فناوری آمریکا مشخص ساخت که آزمون نرم افزار ۳۰٪-۹۰٪ از تلاش را برای تولید یک برنامه عملیاتی تشکیل می‌دهد. با این وجود، ۵٪ از تمام خطاهای پیداشده طی حیات نرم‌افزار، پس از انتشار نرم‌افزار کشف می‌شود. در سال ۱۹۹۹ هزینه تخمینی خطاهای نرم‌افزار تنها در صنعت هوانوردی ۶ میلیارد دلار بوده است [۵].

روش دیگری که برای حل مشکلات برنامه بکار می‌رود، شیوه‌های رسمی هستند که اجازه مدل‌سازی ریاضی و اثبات ویژگی‌های برنامه را می‌دهند. این روش‌ها که اثبات قضیه^۲ و بازیابی مدل^۳ نام دارند، باعث افزایش ضریب اطمینان رفتار برنامه می‌شوند. با این وجود، واری رسمی برنامه بطور کامل قابل انجام نیست. وجود شاخه‌های نامحدود در فرایند اثبات، در روش اثبات قضیه و مشکل انفجار فضای حالات^۴ در روش بازیابی مدل، باعث غیرعملی شدن واری کامل برنامه‌های واکنشی بی‌درنگ می‌شود [۶]. در ضمن واری تمام حالات برنامه باعث پیچیدگی واری این‌گونه برنامه‌ها می‌شود. علاوه بر این، واری برنامه تنها به مدل‌های رسمی این برنامه‌ها اعمال می‌گردد و هنوز درستی پیاده‌سازی و عوامل محیطی زمان اجرای آن‌ها بررسی نمی‌شود. بنابراین حتی اگر برنامه به صورت رسمی، قبل از پیاده‌سازی آن، واری گردد، با توجه به جزئی‌تر بودن پیاده‌سازی، هنوز اطمینان کاملی به درستی پیاده‌سازی عملی آن وجود ندارد [۷].

با توجه به مطالب بالا، زمانی که برنامه در حال اجرا است، تضمین این‌که برنامه بدون هیچ‌گونه خطایی به درستی اجرا شود، با بهره‌گیری از رویکرد آزمون و در صورت نیاز واری رسمی برنامه امکان‌پذیر نمی‌باشد. در اینجا است که رویکرد راستی‌آزمایی حین اجرای برنامه به منظور جبران کمبودهای این دو رویکرد می‌تواند بکار گرفته شود و مکملی برای این دو روش باشد [۷، ۸]. بنابراین پیشنهاد ما در این پژوهش استفاده از رویکرد آزمون و/یا واری رسمی است، اما از آنجا که نمی‌توان به رفتار برنامه بطور کامل اطمینان داشت، در نتیجه باقیمانده خطاهای موجود در برنامه از طریق رویکرد راستی‌آزمایی حین اجرا، شناسایی و از رفتار سوء برنامه پیش‌گیری شود.

هدف روش راستی‌آزمایی حین اجرای برنامه، مشاهده رفتار برنامه برای بررسی رفتار درست برنامه در حین اجرای آن می‌باشد. در حقیقت بررسی این‌که اجرای برنامه خصوصیات مشخصی را حفظ

^۱ Research Triangle Institute

^۲ Theorem Proving

^۳ Model checking

^۴ State Space Explosion

می‌کند یا خیر. تعاریف متفاوتی در متون علمی برای راستی‌آزمایی خطای حین اجرای برنامه ارائه شده است [۴]. تعریفی که در بین اکثر آن‌ها مشترک می‌باشد، عبارت است از:

"یک راستی‌آزمایی برنامه‌ای است که رفتار برنامه را در حین اجرای آن راستی‌آزمایی کرده و تعیین می‌نماید آیا برنامه با ویژگی‌های داده شده همخوانی دارد؟" [۴].

برای راستی‌آزمایی رفتار برنامه در حین اجرای آن با هدف اطمینان از اجرای درست آن با توجه به مسئولیت‌های بیان شده برنامه، ابتدا می‌بایست انواع ویژگی‌های قابل راستی‌آزمایی را مورد بررسی قرار داد. ویژگی‌های برنامه شامل دو نوع سلامت^۲ و ایمنی^۳ هستند که ویژگی‌های سلامت اتفاق خوبی که باید در برنامه رخ دهد را مشخص می‌کنند و با توجه به این‌که این نوع ویژگی‌ها خطرات جدی ندارند و تلاش می‌شود در روش‌های رسمی و آزمون نرم‌افزار این ویژگی‌ها حتی الامکان بررسی شوند و راستی‌آزمایی حین اجرای آن‌ها هزینه سربار بالایی دارد، لازم نیست که در زمان اجرا راستی‌آزمایی شوند [۹، ۱۰].

ویژگی‌های ایمنی نیز که در صورت نقض، باعث ناهنجاری رفتار برنامه می‌شوند از اهمیت فوق‌العاده‌ای در تمام برنامه‌های حساس به ایمنی برخوردارند. بنابراین در این پژوهش تنها ویژگی‌های ایمنی در زمان اجرا راستی‌آزمایی می‌شوند. البته اگر در برنامه‌ای سربار ناشی از راستی‌آزمایی حین اجرای ویژگی‌های سلامت قابل تحمل باشد، می‌توان تمامی یا تعدادی از ویژگی‌های سلامت را نیز حین اجرا راستی‌آزمایی نمود. ویژگی‌های ایمنی می‌تواند به روش‌های مختلفی مانند جبر، آتاماتا و منطق [۱۱] بیان شود که با توجه به نوع برنامه مورد راستی‌آزمایی تعیین می‌گردد [۴، ۱۲].

با توجه به این‌که برنامه‌های واکنشی بی‌درنگ، معمولاً حیاتی هستند، در نتیجه در بیان این‌گونه برنامه‌ها نباید ابهام وجود داشته باشد. به همین دلیل از روش‌های رسمی برای بیان خصوصیات و رفتار این‌گونه برنامه‌ها استفاده می‌شود [۷]. روش بکارگرفته شده در این پژوهش، منطق بی‌درنگ^۴ و منطق بی‌درنگ رویدادگرا^۵ می‌باشد که به صورت رسمی ویژگی‌های ایمنی برنامه را بیان نموده و با

^۱ Monitor

^۲ Liveness

^۳ Safety

^۴ Real-Time Logic (RTL)

^۵ Event-based Real-time Logic (ERL)

توجه به این که در زمان اجرا راستی آزمایی می‌شوند و تمامی پارامترهای ویژگی‌های ایمنی مقادیر ثابت است، قابل تصمیم‌گیری می‌باشند.

۱-۳- اهداف و نتایج حاصل از پژوهش

هدف از انجام این پژوهش فائق آمدن بر مشکلاتی است که روش‌های معمول واری و اعتبارسنجی برنامه‌ها دارند. این روش‌ها که شامل آزمون برنامه و واری رسمی (بازبینی مدل و اثبات قضیه) هستند، نمی‌توانند درستی اجرای برنامه را بطور کامل تضمین کنند. بنابراین برای این که اجرای درست برنامه بطور کامل تضمین شود، روشی برای راستی آزمایی حین اجرای برنامه‌های واکنشی بی‌درنگ تدوین و طراحی می‌گردد و با دو منطق زمانی RTL و ERL درستی این روش بررسی می‌شود. در این پژوهش، از رویکرد جنبه‌گرا^۱ در بخش ابزارآزمایی^۲ برنامه‌های واکنشی بی‌درنگ برای راستی آزمایی حین اجرای این دسته از برنامه‌ها استفاده می‌شود.

چارچوبی برای راستی آزمایی حین اجرای برنامه‌های واکنشی بی‌درنگ ارائه شده است، که کار راستی آزمایی حین اجرا را در سه فاز انجام می‌دهد. دو فاز اول قبل از زمان اجرا انجام می‌شوند، اما فاز سوم در حین اجرای برنامه انجام می‌گردد. فاز اول، ویژگی‌های ایمنی^۳ را از مشخصات خواسته‌های برنامه استخراج می‌نماید و پس از استانداردسازی، به ازای هر ویژگی، رفتار تحمل پذیری^۴ در برابر نقض آن تعیین می‌گردد. در فاز بعد، عمل ابزارآزمایی ویژگی‌ها داخل کد برنامه انجام می‌شود. در این فاز، جنبه‌های عملیاتی، زمانی و ضرب‌الاجل تولید شده و توسط بافنده به کد برنامه افزوده می‌شوند. کد ابزارآزمایی شده پس از ترجمه^۵ در محیط اجرا می‌شود. در فاز سوم نیز راستی آزمایی حین اجرای برنامه در محیط انجام می‌گیرد.

نتایج حاصل از این پژوهش عبارتند از:

- چارچوب پیشنهادی، مستقل از زبان بیان ویژگی، زبان برنامه‌نویسی یا سیستم عامل می‌باشد. البته زبان بیان ویژگی‌ها باید نوعی از منطق زمانی باشد. این چارچوب با دو روش بیان ویژگی RTL و ERL بررسی شده است. RTL توانایی بیان قیدهای زمانی نظیر تاخیر و ضرب‌الاجل و

^۱ Aspect Oriented Programming

^۲ Instrumentation

^۳ Safety Property

^۴ Fault Tolerant

^۵ Compile

مشخص سازی دفعات وقوع یک رخداد را دارد. علاوه بر این، RTL دارای قدرت تشریح بالا و سادگی فرمول نویسی است. از طرفی ERL دارای بیانی سطح بالا است به طوری که قیدهای منطق زمانی به راحتی با ERL بیان می شوند. این سادگی بیان، باعث شده است که فرمول های ERL به صورت کوتاه نوشته شوند. به عبارت دیگر، فرمول های ERL دارای قدرت خوانایی بسیار زیادی است.

- در چارچوب پیشنهادی، راستی آزما با برنامه تحت راستی آزمایی جمع شده و به صورت یک برنامه واحد اجرا می شود و در صورت نقض هر کدام از ویژگی های ایمنی، اجرای برنامه متوقف شده و برنامه به وضعیت امنی هدایت می شود.

- مشکل اصلی روش های جاری راستی آزمایی برنامه های واکنشی بی درنگ، به علت حیاتی و حساس بودن آنها، عدم راهبری و هدایت به یک وضعیت امن بعد از تشخیص نقض ویژگی است، اما در چارچوب پیشنهادی علاوه بر تشخیص نقض ویژگی ها، عمل تحمل پذیری در برابر نقض ویژگی نیز انجام می شود.

- استفاده از رویکرد جنبه گرایی باعث کاهش پیچیدگی راستی آزمایی حین اجرای برنامه شده، در نتیجه تولید راستی آزما و نگهداری آن آسانتر شده است.

برای نشان دادن عملکرد درست روش ارائه شده، برنامه گذرگاه راه آهن پیاده سازی شد و روش ارائه شده روی آن اعمال شد. آزمایشاتی روی نمونه مدل سازی شده انجام گردید و با رویکردهای مشابه مقایسه شد. در آزمایشات که به صورت جداگانه انجام گرفته است، مشخص گردید که چارچوب ارائه شده سرپار ۴٪ تا ۳۳٪ را به برنامه اضافه می کند که به راحتی با افزایش توان سخت افزاری قابل جبران است.

۱-۴- مروری بر فصول پایان نامه

این پایان نامه مشتمل بر هفت فصل است که در فصل اول به بیان کلیاتی از پژوهش پرداختیم. مقدمه فصل ضرورت این پژوهش و کاربردهای آن را متذکر می شود. بخش بعد به بیان مسئله و مشکلات پیش روی اختصاص دارد. در این بخش روش های متداول اعتبارسنجی برنامه های واکنشی بی درنگ مورد بحث قرار گرفتند. سپس اهداف پژوهش مطرح شد. نتایج پژوهش نیز که شامل روش ارائه شده و ویژگی های این روش است، شرح داده شد.