ارائه یک روش رسمی جهت اعتبارسنجی ماشین قلب-ریه

رضا رافع[1*]، فاطمه یوسفی فرد[2]، سیده زینب حسینی کب[1]

۱) گروه مهندسی کامپیوتر، دانشگاه اراک، اراک، ایران

۲) گروه کامپیوتر، دانشگاه آزاد اسلامی، واحد اراک، اراک، ایران

تاریخ دریافت: ۹۳/۲/۸ **تاریخ پذیرش: ۹۳/٤/۳۰**

چکیده

مقدمه: رخداد خطا در سیستم های کامپیوتری، مخصوصاً سیستم هایی که در پزشکی استفاده می شوند، می تواند منجر به صدمات جبران ناپذیری شود. بنا بر این وارسی چنین سیستم هایی اهمیت زیادی دارد. چک کردن مدل یکی از روش هایی است که برای اطمینان از عدم وجود خطا در یک مدل استفاده می شود. ماشین قلب-ریه ماشینی است که در جراحی هایی که نیاز است قلب ساکن باشد به کار می رود و وظایف قلب و ریه را به عهده می گیرد. هدف از این مطالعه ارایه روش رسمی برای اعتبارسنجی ماشین قلب- ریه است.

مواد و روش ها: عملکرد ماشین قلب-ریه با استفاده از ابزار UPPAAL که از ماشین خودکار زمانی پشتیبانی می کند مدل شده است. چون در این ماشین سه مجموعه کار به طور موازی انجام می شود، که در سه زیرسیستم ماشین عملکرد کلی سیستم، ماشین تزریق دارو و ماشین تحویل محلول کاردیوپلژیا مدل شده است.

یافته های پژوهش: پس از مدل سازی، با جستجوی جامع روی فضای حالت مدل، خصوصیات مهم سیستم وارسی شد. وضعیت هایی که موجب ورود سیستم به حالت های ناامن می شود شناسایی شدند. دسترس پذیری تمام حالات مهم سیستم بررسی شد. در نهایت از بد عمل نکردن سیستم و صحت خصوصیات آن اطمینان لازم کسب گردید.

بحث و نتیجه گیری: مدل سازی یک روش کم هزینه برای مطالعه یک سیستم و ارزیابی واکنش آن به تغییرات محیطی قبل از ساخت آن است. نظر به اهمیت ماشین قلب-ریه در جراحی ها در این مقاله یک مدل رسمی برای وارسی عملکرد این ماشین ارائه شده است.

واژه های کلیدی: وارسی مدل، ماشین قلب-ریه، ماشین خودکار زمانی، UPPAAL، اعتبارسنجی سیستم

* **نویسنده مسئول:** گروه مهندسی کامپیوتر، دانشگاه اراک، اراک، ایران

Email:r-rafeh@araku.ac.ir

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

مقدمه

به کار گیری دستگاه های مبتنی بر نرم افزار در بسیاری از فعالیت های پزشکی به سرعت در حال افزایش است. علی رغم تاثیر مهم این دستگاه ها بر زندگی بشر، استفاده از آن ها با چالش های امنیتی شدیدی همراه است. در میان همه چالش های امنیتی ناشی از دستگاه های پزشکی، مسائل مربوط به نرم افزار از بیشترین اهمیت برخوردار است(۱). از این رو لزوم استفاده از روش های اعتبارسنجی برای اطمینان از برآورده شدن شرایط ایمنی در آن ها لازم می باشد. اعتبارسنجی با فراهم کردن یک الگوریتم تعیین می کند که آیا یک مدل، مشخصات بیان شده برای هدف مشخصی را برآورده می کند یا نه؟ در واقع، مجموعه متفاوتی از فعالیت ها که تضمین می کند نرم افزار ساخته شده با خواسته های مورد نظر مطابقت دارد(۲). یکی از راه های رسمی اعتبارسنجی نرم افزار، وارسی مدل است. با استفاده از وارسی مدل تمام حالات سیستم به طور کامل بررسی می شوند و اگر حالتی مشاهده شود که یکی از خصوصیات سیستم را نقض کند، یک مثال نقض تولید می شود.

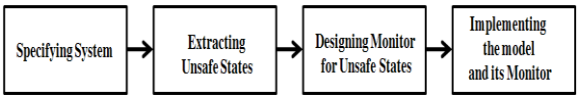
پژوهش های مختلفی در مورد اعتبارسنجی ماشین های پزشکی انجام شده است. در(۳) کاربرد وارسی مدل برای تحلیل قابلیت اعتماد خودکار دستگاه های پزشکی بلادرنگ و قابل برنامه ریزی ارائه شده است. این روش ماشین خودکار زمانی و ترکیبی را برای مدل سازی عملیات بلادرنگ دستگاه و تعامل آن با بیمار و پرستار به کار می برد. در(۴) یک روش اعتبارسنجی رسمی برای تشخیص مسائل مربوط به طراحی مربوط به تعامل با کاربر، با تمرکز بر واسط کاربری در دستگاه های پزشکی ارائه شده است. مطالعه موردی نشان می دهد که این روش می تواند موارد طراحی مربوط به تعامل در پیاده سازی واقعی که ممکن است منجر به مشکلات امنیتی شود را تشخیص دهد.

مقاله(۵) یک متدولوژی اعتبارسنجی نرم افزار دستگاه پزشکی ارائه نموده است. این متدولوژی با استفاده از نرم افزار دستگاه تنظیم کننده ضربان قلب شرح داده شده است. در(۶) یک روش مدیریت ایمنی در نرم افزارهای پزشکی ارائه شده است که در آن با تکیه بر چرخه حیات ایمنی نرم افزار، پارامترهای اندازه گیری برای کیفیت ایمنی موجود در سیستم پیشنهاد شده است تا به کمک آن بتوان ایمنی نرم افزار را در سیستم های ایمنی–حیاتی و بالاخص سیستم هایی که در پزشکی کاربرد دارند، ارزیابی نمود و آن را بهبود داد.

سیستم های فیزیکی سایبری پزشکی MCPS و طراحی این سیستم ها به گونه ای که هم ایمن باشند و هم مواردی از جمله دستیابی به اطمینان بالا در نرم افزار سیستم، قابلیت همکاری، هوشمندی و استقلال را ارائه کنند در(۷) بحث شده است.

در(۸) از شبکه های پتری به منظور مدل کردن و اعتبارسنجی پمپ انسولین CIIP استفاده شده است. سپس محدودیت های سیستم با زبان Z توصیف شده، با زبان برنامه نویسی C# پیاده سازی شده است. سیستم CIIP یک سیستم بلادرنگ متناوب و سیستم ایمنی حیاتی است که مسئول نرمال کردن قندخون بیماران مبتلا به دیابت نوع یک می باشد. این تحقیق به شبیه سازی اعتبارسنجی رفتار سیستم در برابر نیازهای ایمنی دیابتی پرداخته است. با استفاده از شبکه پتری رفتار سیستم در ارتباط با بیمار مدل شده است. سپس گراف دسترس پذیری از مدل برای تعیین حالات خطرناک سیستم به دست آمده است. از نمودار دسترس پذیری محدودیت های متنی دیابتی در زبان خصوصیات Z به دست آمده و در نهایت، مدل شبکه پتری و محدودیت ها در زبان C# پیاده سازی شده است(شکل شماره ۱).

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]



شکل شماره ۱. روش ٤ مرحله ای برای اعتبارسنجی سیستم CIIP در(۸)

مقاله(۹) اعتبارسنجی نرم افزار را وقتی به صورت تعبیه شده در دستگاه های پزشکی که کار می رود بررسی می کند. محققان هم چنین حملات احتمالی علیه دستگاه های خاص پزشکی مانند پمپ انسولین(۱۰) و دستگاه تنظیم کننده ضربان قلب را نشان دادند(۱۱).

بیماری های قلبی-عروقی یکی از علت های اصلی مرگ در کشورهای در حال توسعه است(۱۲). یکی از بزرگ ترین پیشرفت ها در معالجات این بیماری ها، ماشین قلب-ریه می باشد(۱۳). ماشین قلب-ریه ماشینی است که وظایف قلب و ریه را در جراحی قلب به عهده می گیرد. این ماشین همواره باید در یک وضعیت امن باشد به گونه ای که هیچ خطری برای سلامت و ایمنی بیماران و کاربران نداشته باشد و هر گونه خطا هرگز نباید دستگاه را به یک حالت غیرقابل کنترل ببرد. ماشین قلب ریه باید با تاکید بر ایمنی مطلوب طراحی، ساخته و تولید شود(۱۴). اگر این ماشین درست عمل نکند آسیب های جدی به بیمار وارد می شود.

توسعه بای پس قلب-ریه در(۱۵) توضیح داده شده است. یک تزریق کننده ماهر باید به طور پیوسته بر متغیرهای ضروری ماشین قلب-ریه نظارت داشته باشد و آن ها را تنظیم نماید. در این تحقیق ماشین قلب-ریه شبیه سازی شده و سعی شده سیستم به طور خودکار کنترل شود.

ماشین قلب-ریه یک سیستم واکنشی می باشد که در تعامل با محیط اطراف خود بوده و به طور همروند با محیط اطراف خود اجرا می شود. در این مقاله برای مدل کردن این ماشین از ابزار UPPAAL استفاده شده است. UPPAAL ابزاری برای ارزیابی سیستم های بلادرنگ است و از ماشین خودکار زمانی پشتیبانی می کند(۱۶).

با توجه به نقش حیاتی عملکرد ماشین قلب-ریه در سلامتی بیمار، ارزیابی عملکرد سیستم برای جلوگیری از ورود آن به حالاتی که برای بیمار ایجاد خطر می کند موضوع مهمی است. از این رو در این مطالعه سعی شده یک روشی رسمی برای اعتبارسنجی عملکرد این ماشین ارائه شود.

مواد و روش ها

وارسی مدل: در علم کامپیوتر وارسی مدل به مسائل زیر اشاره دارد: به دست آوردن مدلی از سیستم، تست خودکار این که آیا این مدل با خصوصیات تعیین شده مواجه می شود و تشخیص دارا بودن نیازهای امنیتی از قبیل عدم بن بست و حالت های بحرانی مشابهی که سیستم را به شکست می رساند. تعیین خصوصیات سیستم مشخص می کند که سیستم چه کارهایی باید انجام دهد و چه کارهایی نباید انجام دهد. وارسی کننده مدل تمام حالت های سیستم را امتحان می کند تا بررسی کند آیا خصوصیت مورد نظر برقرار می شود یا نه. یک ویژگی مهم وارسی مدل، توانایی آن در فراهم کردن مثال نقض است که نشان می دهد چگونه حالت غیرمنتظره ایجاد می شود. این اطلاعات خیلی مهمی است که به طراح کمک می کند تا خطا را در سیستم تصحیح کند(۱۷).

برای حل الگوریتمی این قبیل مسائل، مدل سیستم و خصوصیات آن با برخی زبان های ریاضی دقیق فرموله می شوند. وارسی مدل به این معنی است که آیا یک فرمول خاص در منطق گزاره ای در یک ساختار خاص صدق می کند. روش های رسمی می تواند به عنوان «کاربرد ریاضیات در مدل سازی و تحلیل سیستم های ICT» مطرح شود. هدف آن صحت سنجی سیستم با رویکرد ریاضی است. گذشته از این روش های رسمی تنها روش ارزیابی «موکداً توصیه شده» برای توسعه نرم افزاری سیستم های

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

ایمنی-حیاتی مطابق بهترین استاندارد IEC و استانداردهای ESA می باشد(۱۸).

طی دو دهه گذشته تحقیقات در روش های رسمی منجر به پیشرفت روش های ارزیابی شده که کشف کاستی ها را سریع تر کرده است. این روش ها با ابزارهای قوی نرم افزاری همراه می شوند که می توانند برای ارزیابی خودکار استفاده شوند.

ماشین های خودکار زمانی رفتار سیستم هایی که در آن ها نقش زمان حیاتی است را مدل می کنند. یک ماشین خودکار زمانی در حقیقت یک گراف برنامه است که با مجموعه متناهی از متغیرهای حقیقی زمان سنج برای همگام کردن فعالیت ها مجهز شده اند. زمان سنج ها از متغیرهای معمولی متمایزند چون دسترسی به آن ها محدود است؛ ممکن است فقط مقدار آن ها بررسی شود و یا به صفر تغییر کنند ولی نمی توان سایر عملیات تخصیص را روی آن ها اعمال کرد. تمام زمان سنج ها با یک سرعت حرکت می کنند؛ با گذشت d واحد زمانی تمام زمان سنج ها به اندازه d پیشرفت می کنند. شرایط مقادیر زمان سنج ها به عنوان شرایط فعال سازی جریان به کار برده می شوند. فقط اگر شرط برقرار باشد جریان می تواند فعال شود و توانایی اجرا را دارد؛ در غیر این صورت جریان غیرفعال است(۱۸).

همان طور که ماشین خودکار برای توصیف جزئیات رفتار سیستم اختصاص داده شده، منطق ها برای توصیف مجزایی از خصوصیات مورد نیاز سیستم اختصاص داده می شوند. فرمول های منطق گزاره ای شامل متغیرها و عملگرهای منطقی هستند. مدل سازی منطق گزاره ای یک تخصیص مقدار «درست» یا «نادرست» به متغیرها است به طوری که روابط و محدودیت های روی متغیرها ارضاء شود. منطق گزاره ای برای بیان برخی خصوصیات مناسب است. در حالی که با توجه به با بسط فرمول های منطق زمانی عملگرهای زمانی، مدل فقط یک تخصیص ساده در مدل سازی منطق گزاره ای نیست بلکه مجموعه ای از مدل های وابسته زمانی می باشد. منطق های زمانی برای بیان رابطه خصوصیات با فعالیت سیستم های بلادرنگ اختصاص داده شده اند. دو نوع منطق زمانی بر طبق روش رفتارشان با انشعاب زمان متمایز می شود. انشعاب زمان در حقیقت به معنی شاخه بندی مسیرها در سیستم انتقال حالت است: منطق زمانی خطی(LTL) و منطق محاسبات درختی(CTL)(۱۷).

منطق زمانی خطی برای تشخیص و ارزیابی سیستم های واکنشی ارائه شده است(۱۹). به این دلیل این منطق خطی نامیده می شود چون زمان مبنی بر مسیر است و به طور خطی دیده می شود: در هر لحظه از زمان فقط یک حالت جانشین ممکن وجود دارد و بنا بر این هر زمان یک حالت بعدی شدنی منحصر به فرد دارد(۱۸).

مدل سازی منطق انشعاب زمانی، مدل سازی تولید درخت است. در طول این انشعاب زمان، این رده از منطق «منطق انشعاب زمانی» نامیده می شود. اساس این منطق تشکیل درختی از حالت ها است. انواع گوناگونی از منطق انشعاب زمانی پیشنهاد شده است. در این جا منطق محاسبات درختی(CTL) را بررسی می کنیم. CTL بین فرمول مسیر و فرمول حالت تمایز قایل شده است. به طور مستقیم فرمول حالت یک ویژگی از یک حالت را بیان می کند و فرمول مسیر یک ویژگی از یک مسیر(یک توالی از حالت های نامتناهی) را بیان می کند(۱۸).

از آن جایی که ابزار وارسی مدلی که در این مقاله استفاده شده است، UPPAAL می باشد، در ادامه به طور مختصر به معرفی این ابزار می پردازیم.

UPPAAL: در این مقاله برای نمایش گرافیکی ماشین های خودکار زمانی از ابزار UPPAAL استفاده می شود. UPPAAL ابزاری برای ارزیابی سیستم های بلادرنگ است که به طور مشترک توسط دانشگاه های «Uppsala» و «Aalborg» طراحی شده است. این ابزار با موفقیت در مطالعاتی پیرامون پروتکل های ارتباطی برای برنامه های چند رسانه ای به کار برده شد. UPPAAL برای ارزیابی سیستم هایی طراحی شده است که قابل مدل سازی با متغیرهای صحیح، انواع ساختار داده ای و کانال های هم زمانی هستند. وارسی کننده مدل UPPAAL از تئوری ماشین خودکار زمانی پشتیبانی می کند. زبان پرس و جوی آن برای مشخص کردن خصوصیات مورد بررسی زیرمجموعه ای از CTL است(۱۶). در UPPAAL

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

یک سیستم به عنوان شبکه ای از چندین ماشین خودکار زمانی موازی مدل می شود. زبان مدل سازی آن ترکیبات اضافی مثل متغیرهای صحیح کران دار و فوریت را ارائه می دهد.

در UPPAAL کانال های نرمال و فوری متمایز وجود دارد. لبه های همگام شده توسط کانال نرمال وقتی که با گارد فعال شده باشند می توانند در زمان اختیاری گرفته شوند، اما لبه های همگام شده با کانال فوری باید به محض ممکن شدن گرفته شوند(وقتی که یک لبه فوری فعال شود اجازه هیچ توقفی در هیچ زمانی وجود ندارد). مدل به کار رفته در UPPAAL شبکه ای از ماشین های خودکار زمانی همگام شده با کانال ها می باشد(۱۶).

بیان ویژگی ها در UPPAAL: هدف اصلی وارسی کننده مدل، ارزیابی مدل در نیازمندی های مشخص شده است. نیازمندی ها باید به طور رسمی با یک زبان مشخص بیان شود. زبان پرس و جو مشابه CTL شامل فرمول مسیر و فرمول حالت است. فرمول حالت، حالت های منحصر به فردی را توصیف می کند در حالی که فرمول مسیر بر روی مسیرها یا تعقیب های مدل بیان می شود. فرمول مسیر می تواند در دسترس پذیری، امنیت و زنده ماندن رده بندی شود.

در UPPAAL بن بست با یک فرمول حالت مخصوص بیان می شود. فرمول شامل لغت deadlock بوده و برای تمام حالت های بن بست برقرار می شود. یک حالت بن بست است اگر هیچ انتقال فعال خروجی از آن وجود نداشته باشد.

دسترس پذیری: ویژگی دسترس پذیری ویژگی ساده ای است که سوال می کند: آیا با شروع از حالت اولیه مسیری وجود دارد که سرانجام φ در طول مسیر برقرار شود. به عنوان نمونه وقتی مدلی از پروتکل های ارتباطی شامل یک فرستنده و گیرنده باشد، این ویژگی سوال می کند که آیا برای یک فرستنده امکان ارسال و یا برای دریافت کننده امکان دریافت وجود دارد. در UPPAAL این ویژگی را با استفاده از نحو E<>φ می نویسیم.

امنیت: ویژگی امنیت به این معنی است که بعضی اتفاقات بد هرگز رخ ندهد. در UPPAAL این ویژگی فرمول بندی شده است. بعضی اتفاقات خوب به طور ثابت درست است. φ را یک فرمول حالت در نظر می گیریم. بیان می کنیم که φ باید در تمام حالت های دسترس پذیر با فرمول مسیر A□φ درست باشد، در حالیکه E◊φ می گوید باید یک مسیر حداکثری وجود داشته باشد که φ همیشه درست باشد. در UPPAAL به ترتیب می نویسیم A[]φ و E [] φ.

زنده ماندن: منظور از ویژگی زنده ماندن این است که بعضی اتفاقات سرانجام رخ می دهد. زنده ماندن در شکل ساده خود با فرمول مسیر A◊φ بیان می شود به این معنا که φ عاقبت برقرار می شود. شکل کاربردی تر آن ویژگی نتیجه گرفتن یا پاسخ است با نوشتن φ → ω که خوانده می شود هر وقت φ برقرار شود پس عاقبت ω برقرار خواهد شد. در UPPAAL این ویژگی ها به ترتیب به این صورت نوشته می شوند :

A<>φ، φ−−→ ω . هم چنین بیان این که در صورت برقرار بودن شرط خاصی φ برقرار است با استفاده از "imply" تعریف می شود(۱۶).

ماشین قلب-ریه

ماشین قلب-ریه ماشینی است که وظایف قلب و ریه را به عهده می گیرد و امکان جراحی با قلب ساکن را برای جراح فراهم می کند. در تاریخ ۶ مه ۱۹۵۳، گیبون با استفاده از ماشین قلب-ریه اولین عمل موفق قلب باز در جهان را بر روی یک زن ۱۸ ساله انجام داد(۲۰). اهداف اصلی بای پس قلبی ریوی(CPB) عبارتند از:

تنفس: فراهم کردن CO2 و اکسیژن کافی و کنترل شده خون، مطابق با تقاضای بدن.

گردش خون: حفظ فشار مطلوب با حداقل آسیب به عناصر خونی.

تنظیم درجه حرارت: کاهش شدید متابولیسم بدن با هیپوترمی عمیق.

علی رغم تنوع تکنولوژی، معمولاً اجزای اصلی و ضروری CPB یکسان باقی مانده است. این اجزا که شامل پمپ خون، اکسیژن دهنده، مبدل دما، مخزن سیاهرگی، خط کاردیوپلژیا برای حفظ ماهیچه قلب و

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

فیلترهای شریانی و لوله های سیستم می باشند در شکل شماره ۲ نمایش داده شده است.

مدار CPB همیشه یک خط اصلی برای انتقال خون دارد. خط اصلی قبل از اکسیژن دهنده خط بازگشت سیاهرگی و بعد از اکسیژن دهنده خط شریانی نامیده می شود. ساختار HLM این کار که در شکل شماره ۲ نشان داده شده است برای بیمارستان دانشگاه روهر بوچام وفق داده شده است. خط اصلی خون حاوی دی اکسیدکربن را از سمت سیاهرگ سیستم بدن بیرون می کشد، در یک مخزن کوچک سیاهرگی ذخیره می کند و خون را درون اکسیژن دهنده پمپاژ می کند. در اکسیژن دهنده دی اکسیدکربن از خون حذف شده اکسیژن به آن اضافه می شود و قبل از ورود به سیستم مجرادار خون تصفیه می شود(۲۱). برای کسب اطلاعات بیشتر در رابطه با ساختار و عملکرد اجزا ماشین قلب–ریه به(۱۴) و(۲۱) رجوع شود.

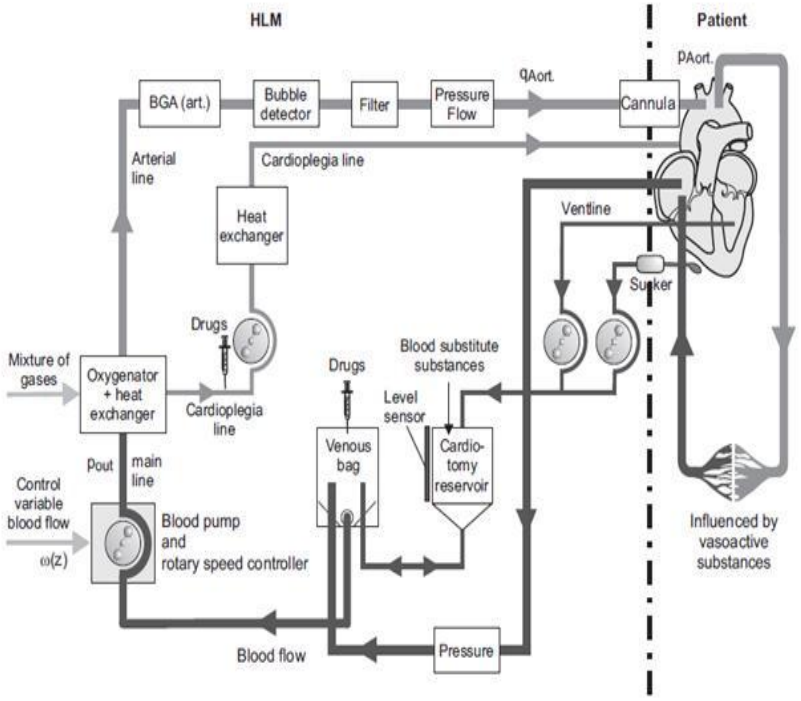
مدل سازی ماشین قلب–ریه با استفاده از ابزار UPPAAL: در ابتدا روش کار ماشین قلب–ریه را به طور خلاصه بیان می کنیم. ابتدا خون از بدن بیمار به داخل مخزن سیاهرگی کشیده می شود تا درون اکسیژن دهنده پمپاژ شود. در اکسیژن دهنده به خون سیاهرگی اکسیژن داده می شود و دمای خون کاهش می یابد. بعد از اکسیژن دهنده مقداری از خون به خط کاردیوپلژیا رفته و باقی آن به خط شریانی می رود. در ادامه خط شریانی خون فیلتر می شود و به بدن بر می گردد. در خط کاردیوپلژیا محلول پتاسیمی به خون تزریق می شود و مجدداً دما و فشار آن کنترل می شود و وارد قلب می شود. این محلول باعث می شود تا از آسیب و مرگ نسوج قلب جلوگیری شود. در گردش مصنوعی خون برای جلوگیری از لخته شدن خون به آن هپارین تزریق می شود. در هر ۳۰ دقیقه زمان فعالیت انعقاد(ACT) اندازه گیری می شود و با توجه به مقدار آن، مقدار تزریق هپارین مشخص می شود. این روند به صورت چرخشی تکرار می شود. با توجه به توضیحات بالا در ماشین قلب–ریه سه مجموعه کار به طور موازی انجام می شود. بنا بر این ماشین در ۳ زیر سیستم مدل شد. عملکرد کلی سیستم، تزریق دارو و تحویل محلول کاردیوپلژیا. در ادامه هریک از این قسمت ها شرح داده می شوند.

تزریق دارو: این ماشین هر ۳۰ دقیقه Act را اندازه گیری می کند. اگر از حد نرمال پایین تر باشد تزریق هپارین انجام می شود. در غیر این صورت تا ۳۰ دقیقه دیگر منتظر مانده مجدداً Act را اندازه گیری می کند. اگر Act اندازه گیری شده کمتر از حد نرمال باشد هپارین اضافه کرده و حتی اگر در حد نرمال باشد به اندازه یک سوم از هپارین اولیه تزریق می شود. مدل سازی این زیرسیستم در شکل شماره ۳ نشان داده شده است.

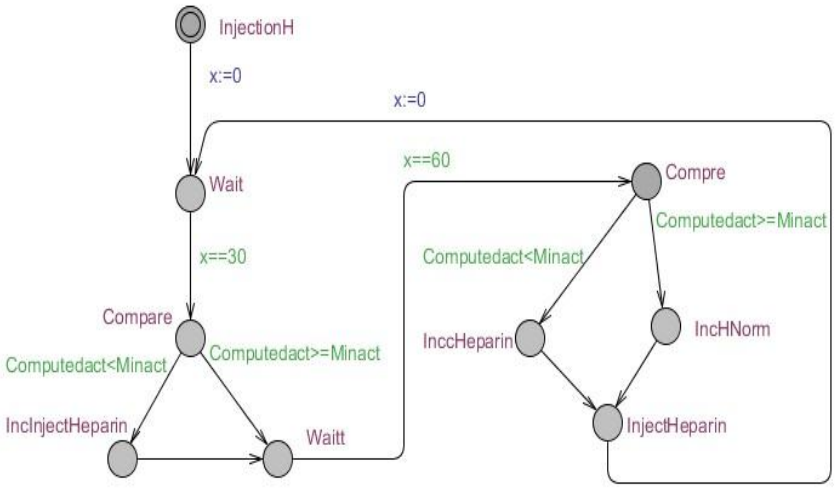
مکان اولیه InjectionH تزریق اولیه دارو را نشان می دهد. سپس در مکان Wait منتظر می ماند. گارد ''x==30'' باعث می شود تا زمانی که مقدار متغیر زمان سنج x برابر ۳۰ نیست ماشین نتواند از آن عبور کند، در نتیجه تا ۳۰ واحد زمانی در مکان Wait می ماند. سپس مقدار ACT محاسبه شده، متغیر Computedact را با مقدار کمینه مجاز Minact مقایسه می کند اگر از حد مجاز کمتر باشد به حالت IncInjectHeparin رفته و تزریق را انجام می دهد، سپس به حالت wait می رود و در غیر این صورت بدون تزریق به حالت wait می رود. مجدداً ۳۰ واحد زمانی صبر می کند، یعنی تا زمانی که مقدار x به ۶۰ برسد منتظر می ماند. مقدار محاسبه شده با مقادیر مجاز مقایسه می شود. اگر در حد مجاز باشد به حالت IncHNorm رفته و به اندازه یک سوم از هپارین اولیه برای تزریق در نظر گرفته می شود. اگر از حد مجاز پایین تر باشد به حالت IncHeparin رفته و مقدار بیشتری برای تزریق در نظر گرفته می شود. بعد از تعیین مقدار تزریق به حالت InjectHeparin رفته و تزریق انجام می شود. سپس مقدار متغیر زمان سنج x را صفر کرده و این چرخه تکرار می شود.

ماشین عملکرد کلی سیستم: ماشین خودکار زمانی عملکرد کلی سیستم در شکل شماره ۴ نشان داده شده است. در این ماشین مراحل کلی ماشین قلب–ریه مدل شده است.

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

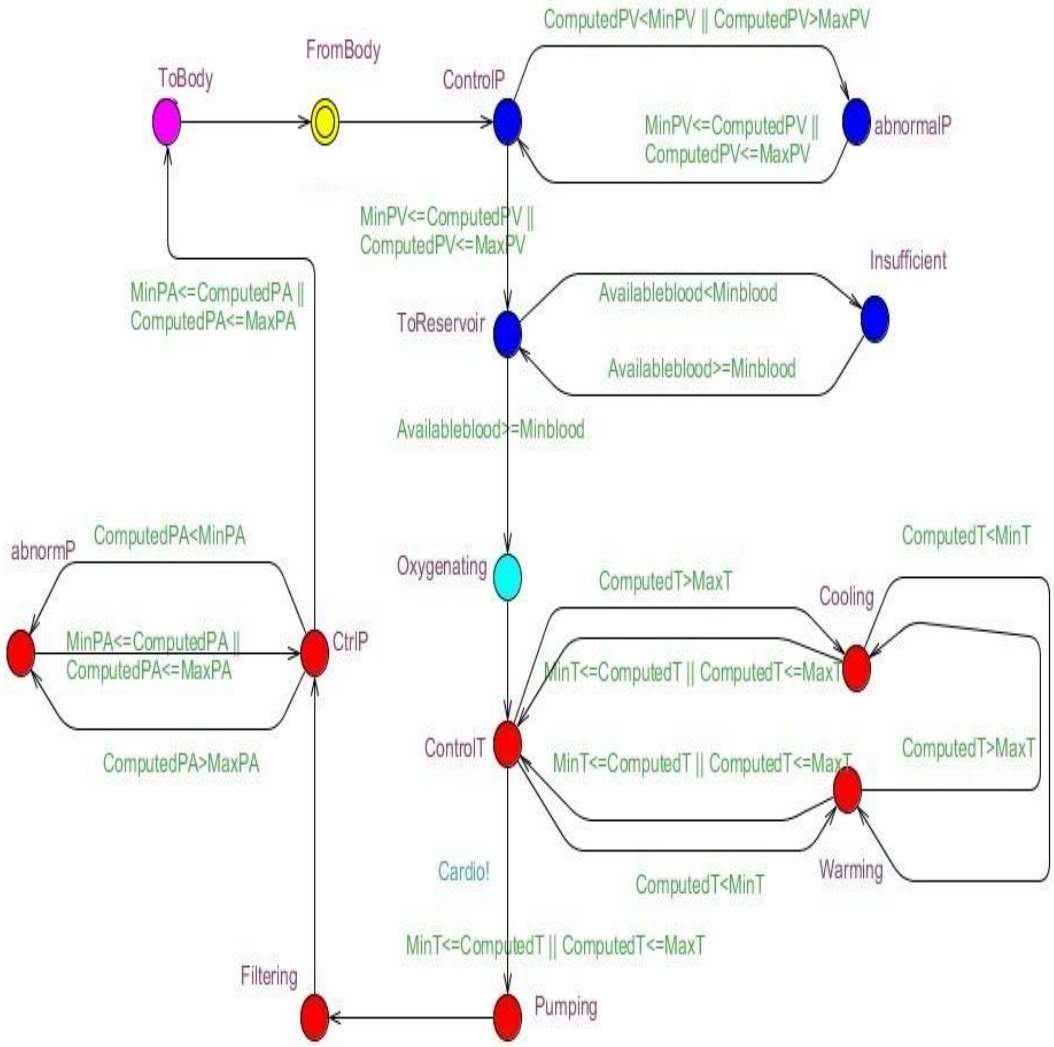


شکل شماره ۱. اجزا مدار بای پس قلبی ریوی همراه با HLM در سمت چپ و سیستم بدن بیمار در سمت راست(۲۰)



شکل شماره ۳. ماشین خودکار زمانی تزریق دارو در ماشین قلب-ریه

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]



شکل شماره ٤. ماشین خودکار زمانی عملکرد کلی سیستم

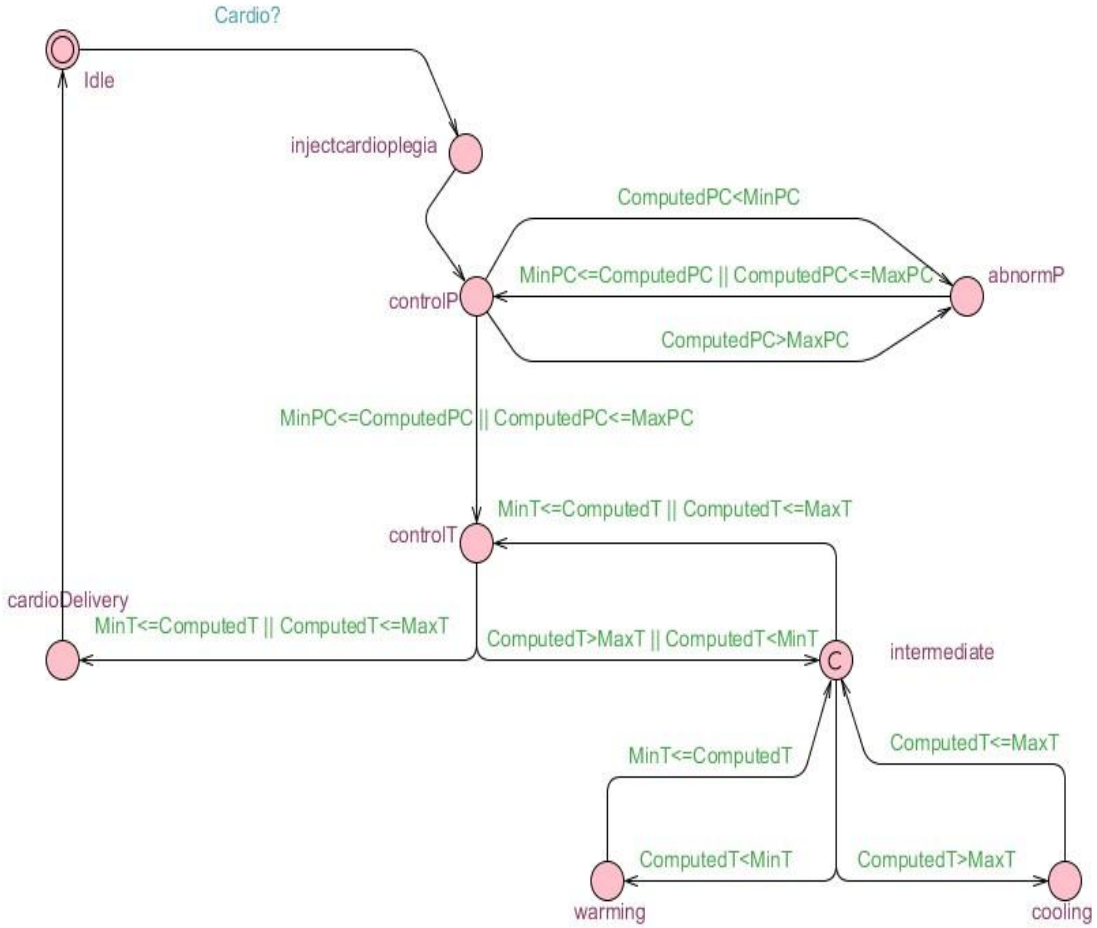
ابتدا خون بدون اکسیژن از بدن خارج می شود. باید فشار این خون قبل از ورود به مخزن کنترل شود. این کنترل در مکان ControlP با مقایسه فشار اندازه گیری شده با مقدار کمینه و بیشینه مجاز فشار سیاهرگی انجام می شود. در صورتی که فشار در این محدوده باشد به مکان ToReservoir می رود. ورود به این مکان نشان دهنده ورود خون سیاهرگی به مخزن می باشد. خون از مخزن باید به اکسیژن دهنده وارد شود. برای این کار باید حجم مخزن کافی باشد. بنا بر این شرط خروج از مکان ToReservoir به سمت مکان Oxygenating کافی بودن حجم مخزن است که با مقایسه حجم موجود مخزن با مقدار کمینه مجاز انجام می شود. بعد از اکسیژن دهی باید خنک سازی و کنترل دما انجام شود. بنا بر این در مکان ControlT دمای خون با مقدار کمینه و بیشینه مجاز دما مقایسه می شود. اگر دمای خون از حد کمینه کمتر باشد به مکان Warming رفته و گرما می گیرد و اگر از حد بیشینه بیشتر باشد به مکان Cooling رفته و خنک می شود.

وقتی دمای خون در محدوده مجاز قرار گرفت، بخشی از آن باید در خط کاردیوپلژیا به سمت قلب برود و بخشی دیگر در خط شریانی برای بازگشت به بدن

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

پمپاژ شود. تحویل خون به قلب در خط کاردیوپلژیا در ماشین cardioplegia مدل می شود. در ماشین عملکرد کلی سیستم بعد از کنترل دما به ماشین cardioplegia سیگنال همگامی !cardio را می فرستد. سپس ماشین به مکان Pumping رفته پمپاژ انجام می شود. در مکان Filtering خون فیلتر می شود. این خون اکسیژن دار باید به بدن برگردد. اما قبل از آن باید فشار آن کنترل شود. این کنترل در مکان CtrlP انجام می شود و فشار شریانی خون با مقدار کمینه و بیشینه مجاز آن MinPA و MaxPA مقایسه می شود. وقتی فشار شریانی در محدوده مجاز قرار گرفت خون به بدن بر می گردد و وارد مکان ToBody می شود. با ورود خون شریانی به بدن، خون سیاهرگی از بدن خارج شده وارد ماشین می شود و این مراحل تکرار می شود.

ماشین کاردیوپلژیا: این ماشین برای تحویل محلول کاردیوپلژیا به قلب طراحی شده است و در شکل شماره ۵ نمایش داده شده است.



شکل شماره ۵. ماشین خودکار زمانی کاردیوپلژیا که با ابزار UPPAAL مدل شده است.

در ابتدا ماشین منتظر دریافت سیگنال همگامی از ماشین عملکرد کلی سیستم می ماند تا خون اکسیژن دار به آن برسد. دریافت این سیگنال با عبارت "cardio?" بیان می شود. بعد از دریافت سیگنال، محلول کاردیوپلژیا به خون تزریق می شود. برای تحویل این خون حاوی محلول به قلب باید فشار و دمای آن کنترل شود. کنترل فشار در مکان controlP انجام می شود. به این صورت که فشار خون نمونه برداری شده با مقدار کمینه و بیشینه مجاز فشار مقایسه می شود. سپس در مکان controlT دما کنترل

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

می شود. دمای اندازه گیری شده ComputedT با مقدار کمینه و بیشینه مجاز دما مقایسه می شود. اگر از حد کمینه کمتر باشد به مکان warming رفته و گرما می گیرد و اگر از حد بیشینه بیشتر باشد به مکان cooling وارد می شود و خنک سازی انجام می گیرد. وقتی دمای خون در محدوده مجاز قرار گرفت تحویل خون حاوی محلول کاردیوپلژیا به قلب در مکان cardioDelivery انجام می شود. سپس ماشین به مکان Idle رفته و منتظر سیگنال همگامی بعدی می ماند.

یافته های پژوهش

بررسی خصوصیات سیستم

با مدل کردن سیستم می توانیم ویژگی های مهم آن را بررسی کنیم. در این مقاله مهم ترین خصوصیات ماشین قلب–ریه بررسی و در مدل اعمال شد. در ادامه چند نمونه از این موارد که با استفاده از زبان پرسش UPPAAL بررسی شدند بیان می شوند:

یکی از این ویژگی ها ایمنی می باشد. در مورد ماشین قلب–ریه ایمنی به این معناست که سیستم در فراهم کردن انتشار فوق جسمی تداوم داشته باشد و تحت هیچ شرایطی متوقف نشود. این همان ویژگی عدم وجود بن بست در مدل است که به صورت زیر بیان می شود:

"A[] not deadlock"

در ماشین عملکرد کلی سیستم برای ورود خون به مکان ToBody باید فشار شریانی در محدوده مجاز باشد، هم چنین در مراحل قبل از آن باید دمای خون در محدوده مجاز قرار بگیرد. این نیاز سیستم به این صورت بیان می شود: «خون قبل از بازگشت به بدن باید در محدوده مجاز فشار و دما باشد» که در زبان پرس و جوی UPPAAL به صورت زیر بیان می شود:

"A[] CBM.ToBody imply ((MinPA<=ComputedPA) || (ComputedPA<=MaxPA)) && ((MinT<=ComputedT) || (ComputedT<=MaxT))"

قبل از تحویل محلول کاردیوپلژیا به قلب باید فشار و دما کنترل شود. این نیاز را به این صورت بیان می کنیم: «قبل از تحویل خون حاوی محلول کاردیوپلژیا به قلب باید فشار خون در محدوده مجاز فشار و هم چنین دمای آن در محدوده مجاز دما باشد» که در UPPAAL به شکل زیر بیان می شود:

"A[] Cardioplegia.cardioDelivery imply ((MinPC<=ComputedPC) || (ComputedPC<=MaxPC)) && ((MinT<=ComputedT) || (ComputedT<=MaxT))"

در ماشین تزریق دارو همان طور که گفتیم هر ۳۰ دقیقه زمان انعقاد اندازه گیری می شود. اگر از حد مجاز کمتر باشد دارو تزریق می شود اگر کمتر نباشد ۳۰ دقیقه بعد بسته به زمان انعقاد، دارو تزریق می شود. در نتیجه هر یک ساعت باید تزریق داروی ضدانعقاد خون انجام شود. تزریق در مکان InjectHeparin انجام می شود. این نیاز سیستم در UPPAAL به صورت زیر بیان می شود:

"A[] ACT.InjectHeparin imply x>=60 "

خون سیاهرگی که وارد اکسیژن دهنده می شود باید در محدوده مجاز فشار باشد و هم چنین برای ورود خون به اکسیژن دهنده باید حجم مخزن کافی باشد. در ماشین عملکرد کلی سیستم اکسیژن دهی در مکان Oxygenating انجام می شود و محدوده مجاز فشار سیاهرگی با متغیرهای MinPV و MaxPV و حجم کمینه مجاز مخزن با Minblood بیان می شود. این نیاز سیستم را در UPPAAL به صورت زیر بیان می کنیم:

"A[] CBM.Oxygenating imply ((MinPV<=ComputedPV) || (ComputedPV<=MaxPV)) && Availableblood>=Minblood "

طبق تعریف ویژگی ها در UPPAAL خصوصیات فوق در قالب ویژگی زنده ماندن و بن بست بیان شدند. در ادامه خصوصیاتی در قالب ویژگی دسترس پذیری بیان می شوند:

بررسی این که «آیا مسیری وجود دارد که داروی ضد انعقاد خون تزریق شود.» در ماشین تزریق دارو تزریق در مکان InjectHeparin انجام می شود. این ویژگی در UPPAAL به صورت زیر بیان می شود:

"E<> ACT.InjectHeparin "

بررسی این که «آیا در خط کاردیوپلژیا تحویل محلول به قلب دسترس پذیر است.» تحویل کاردیوپلژیا در ماشین Cardioplegia در مکان

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

cardioDelivery انجام می شود. این ویژگی در UPPAAL به صورت زیر بیان می شود:

"E<> Cardioplegia.cardioDelivery "

بررسی این که «آیا خون در انتهای مسیر به بدن بر می گردد.» بازگشت خون به بدن در ماشین عملکرد کلی سیستم و در مکان ToBody انجام می شود. این ویژگی در UPPAAL به صورت زیر بیان می شود:

"E<> CBM.ToBody "

بحث و نتیجه گیری

با مدل سازی و شبیه سازی می توان یک سیستم صنعتی را قبل از ساخت مورد مطالعه قرار داد که از نظر اقتصادی و زمانی بسیار مقرون به صرفه تر است. با توجه به اهمیت ماشین قلب–ریه، ما روشی رسمی برای نظارت روند خون رسانی و اکسیژن رسانی در این ماشین ارائه کردیم.

با مطالعه رفتار سیستم دریافتیم که در عملکرد این سیستم زمان نقش مهمی دارد. از این رو تصمیم گرفتیم از ابزاری استفاده کنیم که ماشین های خودکار زمانی را پشتیبانی کند. در این ابزار سیستم به صورت شبکه ای از ماشین های خودکار زمانی مدل می شود. در نهایت ماشین قلب–ریه را با استفاده از UPPAAL مدل سازی کرده و نیازمندی های آن را با استفاده از زبان پرس و جوی آن که زیرمجموعه ای از CTL است بیان کردیم. بعد از مدل کردن سیستم خصوصیات مهم سیستم که باید برقرار باشند را با استفاده از زبان پرس و جوی UPPAAL نوشتیم. UPPAAL اعتبار این خصوصیات در مدل را با جستجوی جامع روی فضای حالت سیستم بررسی می کند. با اعتبار سنجی سیستم نتیجه گرفتیم که تمام حالات مهم سیستم دسترس پذیر است. سیستم دچار توقف و بن بست نمی شود و خصوصیات مهم مورد نیاز در سیستم مشکلی نداشته و در آن برقرار هستند.

البته باید توجه نمود که در مورد سیستم های ایمنی حیاتی از جمله سیستم های پزشکی با توجه به اهمیت اطمینان از صحت عملکرد سیستم، مدل های کامپیوتری جهت سهولت و پایین آوردن هزینه بررسی سیستم استفاده می شوند ولی خبره های انسانی هم باید به طور مستمر بر عملکرد سیستم نظارت داشته باشند. هم چنین روش ارائه شده در این مقاله را می توان در مورد سیستم های پزشکی دیگر به کار برد.

References

1.Hahn RW, Klovers KB, Singer HJ. The need for greater price transparency in the medical device industry an economic analysis. Health Aff 2008;27:1554-9.

2.Clarke EM, Emerson EA, Sifakis J. Model checking algorithmic verification and debugging. Commun ACM2009;52:74-84.

3.Jiang Z, Pajic M, and Mangharam R. Cyber physical modeling of implantable cardiac medical devices. Proce IEEE 2012;100:122-37.

4. Majma N, Babamir SM. Specification and verification of medical monitoring system using petri nets. J Med Sign Sen2014;4:181-93.

5.Chunxiao L, Raghunathan A, Jha NK. Improving the trustworthiness of medical device software with formal verification methods. Emb Sys Letter IEEE2013;5:50-3.

6.Rafeh R. A proposed approach for safety management in medical software design. J Med Syst2013;37:1-5.

7.Silva LC, Perkusich M, Almeida HO, Perkusich A, Lima MA, Gorgonio KC. A baseline patient model to support testing of medical cyber physical systems. Stud Health Technol Inform 2015;216:549-53

8.Babamir SM, Borhani M. Formal verification of medical monitoring software using z language: a representative sample. J Med Syst 2012;36:2633-48.

9.Daw Z, Cleaveland R, Vetter M. Formal verification of software based medical devices considering medical guidelines. Int J Comput Assist Radiol Surg2014;9:145-53.

10.Das UN. Hypothesis: Intensive insulin therapy-induced mortality is due to excessive serotonin autoinhibition and autonomic dysregulation. World J Diabetes 2010 15;1:101-8.

11.Brambatti M, Mathew R, Strang B, Dean J, Goyal A, Hayward JE, rt al. Management of patients with implantable cardioverter defibrillators and pacemakers

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

who require radiation therapy. Heart Rhythm 2015 ; 5271:1547.
12.Sohrabnejad A, Veisani Y, Afkhamzadeh A, Rezaeian S. Family Physicians attitudes and practice toward prevention and treatment of cardiovascular disease. J Ilam Uni Med Sci 2013;21:268-75.
13.Wang Z. The blossom of the rose of surgery the birth of heart lung machine. J Med Colle PLA2013;28:11-9.
14.Hurkmans CW, Scheepers E, Springorum BG, Uiterwaal H. Influence of radiotherapy on the latest generation of implantable cardioverter defibrillators. Int J Radiat Oncol Biol Phys2005;63:282–9.
15.Birnbaum D, Philipp A, Kaluza M, Detterbeck M. On the way to an automatic heart-lung machine a control system for oxygen tension in the oxygenator. Biomed Tech1997;42 :313-4.
16.Kang K, Ryu J, Hur J, Sha L. Design and qos of a wireless system for real time remote electrocardiography. IEEE J Biomed Health Inform2013;17:745-55.
17.Waszniowski L, Hanzalek Z. Formal verification of multitasking applications based on timed automata model. Real time Syst2008;38:39-65.
18.Mishra B. Intelligently deciphering unintelligible designs algorithmic algebraic model checking in systems biology. J R Soc Interface2009;6:575-97.
19. Blom JA. Temporal logics and real time expert systems. Comput Method Program Biomed1996;51:35-49.
20. Konstantinov IE, Aleximeskishvili VV. Sergei S. Brukhonenko the development of the first heart lung machine for total body perfusion. Annal Thorac Surger2000;69:962-6.
21. Passaroni AC, Silva MA, Yoshida WB. Cardiopulmonary bypass development of John Gibbons heart-lung machine. Rev Bras Cir Cardiovasc2015;30:235-45.

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]

Proposing a Formal Approach for Verification of Heart-Lung Machine

*Rafeh R[1 *], Yousefifard F[2], Hosseinikob Z[1]*

(Received: April 28, 2014 Accepted: July 21, 2014)

Abstract

Introduction: error occurrence in computer systems, can lead to irreparable damage, especially those used in medical systems. As a result, verification of such systems is important. Model checking as a method is used to ensure the absence of errors in the model. The heart-lung machine is used in surgeries in which heart must stop working and assumes the heart and lungs duties. In this article, a formal approach is to verify the operation of the heart-lung machine.

Materials & methods: The heart-lung machine has been modeled by using the UPPAAL tool which supports time automatic machine, since, this machine do three sets operations in parallel which has been modeled in three subsystems: system overall performance machine, heparin injection machine and cardioplegia solution delivery machine.

Findings: After modeling by a complete search on state space of model, the most important characteristics of system were verified. Situations were identified which cause entering the system to unsecure states. The reachability of all important states of the system was investigated. Finally, we ensured about system accuracy features and the system operates correctly.

Discussion & Conclusion: Modelling is a cheap way to study a system and evaluate its reaction to environmental changes before implementation of the system. Considering to importance of heart-lung machine in surgeries, in this research a formal model has been presented to verify the operation of this machine.

Keywords: Model checking, Heart-lung machine, Time automatic machine, UPPAAL, System verification

1. Dept of Computer Engineering, faculty of Engineering, Arak University, Arak, Iran
2. Dept of Computer, Islamic Azad University, Arak Branch, Arak, Iran
**Corresponding author Email: r-rafeh@araku.ac.ir*

[Downloaded from sjimu.medilam.ac.ir on 2026-11-13]