ارائه پلتفرم الکترونیکی مناسب برای افزایش ایمنی عملکرد تجهیزات پزشکی

حسین سلیمی[۱]، ولی طالب‌زاده [۲]
[۱]پژوهشکده سامانه‌های ماهواره، پژوهشگاه فضایی ایران، تهران، ایران، h.salimi@isrc.ac.ir
[۲] پژوهشکده سامانه‌های ماهواره، پژوهشگاه فضایی ایران، تهران، ایران v.talebzadeh@isrc.ac.ir

چکیده - ایمنی عملکرد، بخشی از امنیت کلی یک سیستم یا دستگاه است و به طور کلی بر روی الکترونیک و نرم‌افزار مربوطه تمرکز دارد و به جنبه‌های ایمنی می‌پردازد که به عملکرد یک دستگاه یا سیستم، به عنوان نمونه یک دستگاه پزشکی، مربوط می شود و تضمین می‌کند که در پاسخ به دستورات دریافتی آن درست کار کند. در این مقاله ابتدا یک سیستم الکترونیکی امن تعریف و استانداردهای مختلف ایمنی عملکرد معرفی شده است. پس از تعریف سطوح مختلف ایمنی، چگونگی دستیابی به آن سطوح با استفاده از ابزارهای تجاری موجود در بازار مطرح و در این مسیر، نقش سخت‌افزار و نرم‌افزار مشخص شده است. به منظور کاهش خطر در طراحی یک سیستم امن، روشی سیستماتیک ارائه و چالش‌های ادغام سخت‌افزار و نرم‌افزار بررسی شده است. علاوه بر این، پلتفرم‌های سخت‌افزاری/نرم‌افزاری مناسب جهت طراحی یک سیستم الکترونیکی و پزشکی ایمن معرفی و تجزیه و تحلیل شده است. با توجه به این که در ارائه مطالب، سعی بر توجه نکات عملی در کنار لحاظ شدن استانداردهای مربوط بوده است، این مقاله می‌تواند برای دست‌اندرکاران ایمنی تجهیزات پزشکی بسیار مفید باشد.

کلید واژه– ایمنی عملکرد، استاندارد، تجهیزات پزشکی، الکترونیک، سطوح ایمنی.

۱- مقدمه

یک سیستم الکترونیکی زمانی دارای کارکردی ایمن است که برای تمام ورودی‌های ممکن، پاسخ مناسب داشته باشد. سیستم‌هایی با کارکرد ایمن، بسته به استانداردهای ایمنی عملکردی[۱] که در حوزه خاص تعریف شده‌اند، توسعه و اعتبارسنجی می‌شوند. در الکترونیک، استاندارد IEC61508 به عنوان استاندارد ایمنی عملکردی معرفی شده است. این استاندارد به طور خاص به ایمنی سیستم‌های الکترونیکی برقی و سیستم‌های الکترونیکی قابل برنامه‌ریزی اشاره دارد. بسیاری از استانداردهای ایمنی و دستورالعمل خاص بازار، مانند استانداردهای زیر از IEC61508 گرفته شده است:

- ISO 2626 برای خودروهای سواری خودرو
- IEC61511 برای صنایع فرایند و ابزارهای مرتبط
- IEC62061 و ISO 13849 برای سیستم‌های کنترل الکتریکی ماشین آلات
- IEC62304 برای سیستم‌های پزشکی

اکثر نرم‌افزارهای موجود در بازار (COTS[۲])، مانند سیستم عامل‌های زمان حقیقی (RTOS[۳])، که براساس استاندارد IEC61508 توسعه یافته‌اند، می‌توانند به عنوان یک مبنای معتبر برای توسعه دهندگان نرم‌افزارهای ایمن باشند. با این حال، توسعه‌دهندگان باید تلاش کنند تا رضایت مشتری‌های

[۱] Functional Safety

[۲] Commercial-Off-The-Shelf

[۳] Real Time Operation System

خود را در مورد الزامات ایمنی اضافی و خاص، مربوط به بخش بازار هدف، را به دست آورند.

به عنوان مثال، استاندارد DO-178B برای سیستم‌های هوافضا و استاندارد IEC62304 برای سیستم‌های پزشکی، از بسیاری از اصول توسعه نرم‌افزار ایمنی کاربردی در استاندارد IEC61508 استفاده می‌کنند، اما از این استاندارد فراتر رفته و سطح بالاتری از گواهینامه ایمنی ارائه می‌دهند. بنابراین، محصولات شرکت‌هایی که گواهی IEC61508 را دریافت کرده‌اند، نقطه آغاز خوبی برای توسعه نرم‌افزار ایمنی عملکردی بر اساس استانداردهای DO-178B و IEC62304 هستند.

ارزیابی اینکه سیستم ارائه شده دارای ایمنی عملکردی استاندارد خاص است باید مستقل از شرکت ارائه دهنده باشد و بخش مهمی از توسعه سیستم ایمنی عملکردی است. در برخی از بخش‌های بازار، ارزیابی و صدور گواهینامه مستقیما توسط موسسات معتبر (مانند اداره غذا و داروی ایالات متحده) انجام می‌شود و در بسیاری از موارد، ارزیابی این موسسات، مستقل از توسعه دهنده انجام می‌شود. این مراکز اغلب شرکت‌های خصوصی هستند که اعتبار خود را برای صلاحیت‌های فنی، کیفیت پایدار و اجرای دقیق ارزیابی‌های خود توسعه داده‌اند. شرکت‌هایی نظیر TÜV و Exida دارای شهرت جهانی هستند، به طوری که استفاده از نام آنها در رابطه با ادعای گواهینامه ایمنی عملکردی می‌تواند یک مزیت عمده بازاریابی برای توسعه دهنده باشد.

۲- سطوح مختلف ایمنی (SIL)

در مراحل اولیه توسعه ایمنی عملکردی، با توجه به کاربرد مورد نظر، ریسک‌ها شناسایی و ارزیابی می‌شوند. این فرایند به منظور تعیین سطح خطر قابل قبول برای کاربرد استفاده می‌شود. سطوح مشابهی از ریسک قابل قبول، با استفاده از سطوح ایمنی یا SIL ها محاسبه می‌شود. استاندارد IEC61508، سطح SIL ها را از ۱ تا ۴ ارائه می‌دهد (۴ برای بالاترین و ۱ برای پایین‌ترین سطح ایمنی). به طور کلی هدف، ریسک قابل قبول پایین‌تر و رسیدن به سطح SIL بالاتر است که بالطبع در الزامات توسعه محصول، چالش‌برانگیزتر خواهد بود. سطوح مختلف ایمنی در واقع نوعی سنجش است که درجه (حفاظت) سیستم‌های ایمنی یک دستگاه را نشان داده و اساس کار آن، احتمال شکست در دستورات (PFD) و فاکتور کاهش خطر (RRF) می‌باشد. در جدول شماره ۱ سطوح مختلف SIL و میزان احتمال شکست هر سطح نشان داده شده است.

SIL	احتمال شکست دستورات (PFD) در سال	فاکتور کاهش خطر (RRF)
1	0.1 – 0.01	10-100
2	0.01 – 0.001	100-1000
3	0.001 – 0.0001	1000-10000
4	0.0001 – 0.00001	10000-100000

جدول ۱. سطوح مختلف SIL با میزان احتمال شکست و فاکتور کاهش خطر

سخت‌افزار، نرم‌افزار و سیستم می‌تواند براساس استاندارد IEC61508 طراحی شده و یک SIL خاص را هدف قرار دهد.

معمولا، سخت‌افزار و سیستم‌ها با استفاده از معیارهای کمی جهت ارزیابی احتمال رخداد خطا در بازه‌های زمانی مشخص و همچنین در کل بازه کارکردی (تا پایان مدت عملکرد)، ارزیابی می‌شوند. اما برخلاف سخت‌افزارها و سیستم‌ها، نرم‌افزار دارای نرخ شکست ذاتی نیست و تنها به صورت سیستماتیک ارزیابی می‌شود. باید دقت داشت که محاسبه شاخص SIL نمی‌تواند بدون ارزیابی سیستم کامل و مشخص، انجام شود. در انتخاب اجزای سیستم می‌توان از اجزایی با سطح SIL مشخص که توسط توسعه دهنده ارائه شده است استفاده کرد

علاوه بر این، شاخص SIL که برای یک سیستم به دست می‌آید، به ضعیف‌ترین پیوند آن محدود می‌شود. به عنوان مثال، یک عنصر با سطح SIL1 در طراحی یک محصول می‌تواند سطح مربوط به یک سیستم را محدود کرد، حتی در صورتی که خود سیستم به صورت مستقل دارای سطح SIL3 باشد.

در مورد یک محصول COTS که کاربرد نهایی آن مشخص نیست، باید فرضیات در سطح طراحی سیستم و الزامات ایمنی در نظر گرفته شود. به همین دلیل توسعه دهنده COTS به الزامات بالاترین SIL پیش‌بینی شده در پیاده‌سازی مقید می‌شود. از طرف دیگر، لازم است تجمیع‌گر سیستم قبل از انتخاب یک محصولات COTS، اسناد ایمنی آن اجزاء را دقیقا بررسی کند.

در قسمت سوم استاندارد IEC61508 الزامات نرم‌افزار آورده شده است و باید لحاظ شود و این مساله یکی از جنبه‌های اجباری استاندارد است که باید به منظور دستیابی به یک سیستم برای رتبه بندی SIL مورد توجه قرار گیرد. برخلاف سخت‌افزار، نرم‌افزار پتانسیل از کار افتادن ندارد و هیچ حالت خرابی تصادفی در آن رخ نمی‌دهد. در واقع، می‌توان استدلال کرد که نرم‌افزار کامل شده هرگز شکست نخواهد خورد [1]! در واقع، این سطح تست سیستماتیک و فرآیند توسعه تست (که همراه با فرآیند توسعه نرم‌افزار دیده می‌شود) است که سطح SIL قابل دسترسی را تعیین می‌کند. هرچه روند توسعه دقیق‌تر و منظم‌تر باشد،

امتیاز SIL بالاتری می‌تواند به دست آید. سطح SIL3 در عمل بالاترین سطحی است که طیف وسیعی از سیستم‌ها توسعه یافته را شامل می‌شود. سطح SIL4 اهداف ایمنی فوق العاده بالا و پیچیده‌ای دارد و برای توسعه دهندگان سیستم از لحاظ اقتصادی بصرفه نیست [۲] ، زیرا بدون استفاده از مسیرهای چندگانه (مانند دو یا چند نرم‌افزارهای ناهمسان که یک کار مشترک انجام می دهند و یک سیستم که نتایج را داوری می کند) رسیدن به سطح SIL4 از لحاظ فنی غیرممکن است، بنابراین یک مولفه واحد مانند یک RTOS با قابلیت عملکرد سطح SIL3 نمی‌تواند به خودی خود مبنایی برای راه حل رسیدن به هدف سطح SIL4 ارائه دهد. با این حال، دو یا چند RTOSکه از تامین کنندگان جداگانه تهیه شده‌اند و هر کدام قادر به عملکرد SIL3 می‌باشند، می توانند در یک سیستم واحد برای دستیابی به امتیاز سیستم SIL4 طراحی شوند [۳].

با استفاده از نرم‌افزار COTS که قادر به عملکرد SIL3 است، تضمین نمی‌شود که سیستم مربوط، گواهینامه SIL3 را به دست آورد، با این وجود، نرم‌افزار COTS برای ایمنی عملکردی باید با تمام فرآیندهای مستندسازی توسعه و تست همراه باشد.

اسناد اصولی و قاعده‌دار مربوط به روند توسعه نرم‌افزار، یک راهنمای بسیار مفید برای فرایند توسعه نرم‌افزار کاربردی محسوب می‌شود. توسعه دهنده نرم‌افزار می‌تواند از این دستورالعمل‌های توسعه استفاده کنند.

در واقع زمانی که طراحی سیستم با سخت‌افزار و نرم‌افزار استاندارد انجام می‌شود با احتمال بیشتری سیستم معیارهای ارزیابی ایمنی عملکردی را خواهد داشت.

۳- نقش سخت‌افزار و نرم‌افزار در سطوح ایمنی

هدف نهایی هر سیستم توسعه یافته برای رسیدن به استانداردهای ایمنی، گذراندن همه آزمون‌های ارزیابی نیست. بلکه هدف، دستیابی به سیستمی است که به طور عملی ایمن باشد. این بدان معنی است که اگر (به دلیل اینکه همیشه احتمال وقوع خطا وجود دارد) خطایی در سیستم رخ دهد، باعث قراردادن افراد در معرض خطر غیر قابل قبول، نشود.

با این حال، خطای انسانی در مراحل مختلف توسعه و کاربری وجود دارد و غیر قابل تصور است که بتوان یک سیستم کاملا ایمن با خطر صفر ایجاد کرد. بنابراین هدف نهایی طراحان و سازندگان سیستم‌های ایمن، دفاع از محصول خود در صورت بروز خرابی‌های پیش بینی نشده است.

بهترین راه اثبات ایمن بودن سیستم داشتن یک مدرک سیستماتیک است که نشان دهد سیستم به گونه‌ای طراحی و ساخته شده است که اکثر احتمالات خرابی پیش‌بینی شده و اثرات آن جبران و یا تاحد ممکن کاهش داده شده است.

مکانیزم‌های ایمنی که برای هر ریسک شناسایی شده انتخاب می‌شوند، می‌تواند بسیارمتنوع باشد. صرفا به دلیل استفاده از تراشه‌های قابل‌برنامه‌ریزی در طراحی یک سیستم، نمی‌توان هر ریسک را با کمی نرم‌افزار هوشمند و مهندسی حل کرد. به عنوان مثال، اگر سیستمی یک برش لیزری را کنترل می‌کند و این احتمال وجود دارد که کنترل کننده مرکزی به گونه‌ای عمل کند که زندگی کاربر آن را در معرض خطر قرار دهد، لزوماً نیازی به توسعه نرم‌افزار هوشمند برای شناسایی و رفع این خطر نیست. یک راه حل برتر ممکن است قرار دادن یک مانع محافظ فیزیکی در اطراف لیزر باشد. حتی اگر این راه حل جزء الزامات ایمنی عملکردی استاندارد IEC6150 نباشد.

به همین دلیل است که استانداردهای ایمنی عملکردی مختلفی با معیارهای خاص بازار هدف وجود دارد که هر یک با درکی از خطرات و چالش‌های پیش رو، به ارزیابی فرآیند ایمنی می‌پردازند. به عنوان مثال، این سوال مطرح است که «آیا انتخاب زبان برنامه‌نویسی C برای استفاده از نرم‌افزارهای توسعه‌ای می‌تواند مناسب باشد؟». به نظر برخی متخصصان، پاسخ منفی است و توسعه‌دهندگان باید به سوی زبان‌های ایمن مثل ADA حرکت کنند. با این حال، گذر زمان نشان داده است که این استدلال خیلی درست نیست. در واقع، بسیاری از محصولات نرم‌افزاری COTS با قابلیت پشتیبانی ازSIL3، مانند برخی RTOSها، در زبان برنامه‌نویسی C توسعه یافته‌اند. نکته مهم این است که باید در استفاده از زبان C از فرایندهای سیستماتیک جهت کاهش خطرات مرتبط با آن استفاده کرد. در حقیقت بسیاری از جنبه‌های ناامن بودن برنامه‌نویسی در C را می‌توان به طور مستقیم با استفاده از یک RTOS و قابلیت‌های اساسی آن مورد استفاده قرار داد.

با این حال، یک نوع چالش برای توسعه دهنده RTOS این است که کاربر در توسعه سیستم خود (با عملکرد کاربردی ایمن)، ممکن است مجبور به انتخاب یک کامپایلر خاص به غیر از پیشنهاد توسعه دهنده شود. سوال اینجاست که آیا استفاده از یک کامپایلر متفاوت با آنچه توسعه دهنده پیشنهاد می‌دهد، باعث ازبین رفتن قابلیت اطمینان آن RTOS می‌شود؟ پاسخ این است که بستگی دارد. اگر فروشنده فرایند صدور گواهینامه خود را با یک دیدگاه مستقل از ابزار توسعه دهد، می‌توان هر

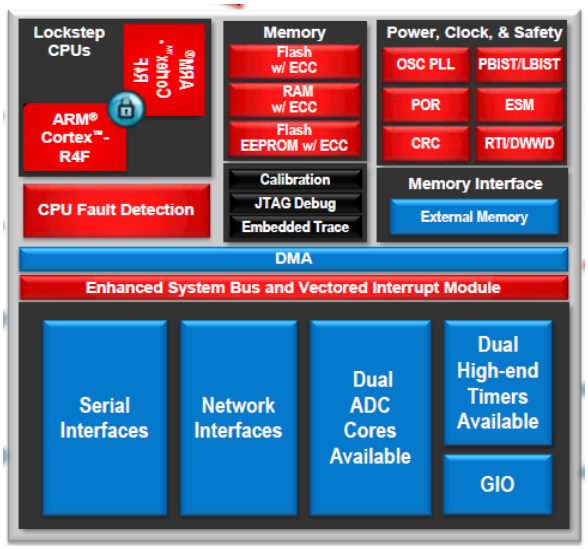
کامپایلری را انتخاب کرد. این مرحله فقط نیاز به تجزیه و تحلیل تاثیر تغییر کامپایلر برروی قابلیت اطمینان RTOS دارد.
پیش‌بینی این مسئله، همراه با دانش عمیق و درک چالش‌های نرم‌افزاری در طراحی سیستم ایمن می‌تواند ارزش بزرگی برای کار با هر تامین کننده سخت‌افزار و نرم‌افزاری که محصولات خود را بر اساس استاندارد ایمنی طراحی کرده است، به وجود آورد.

۴- روش سیستماتیک برای کاهش خطر

یکپارچه‌سازی نرم‌افزار بر روی یک پردازشگر خاص و محیط سخت‌افزاری، یکی از چالش برانگیزترین بخش‌های سیستم در توسعه و ارزیابی الزامات ایمنی استاندارد است. به عنوان نمونه، تخصیص حافظه برای پردازنده مرکزی، ورودی و خروجی‌ها، واحدهای جانبی و همچنین توانایی ارزیابی ایمنی به طور سیستماتیک برای آن، به یک چالش بزرگ در روند توسعه سیستم است. این موارد از دلایل اصلی استفاده از یک RTOS مطمئن و از قبل تایید شده، در سیستم‌هایی است که دارای بخش قابل توجهی از نرم‌افزار هستند. در این سیستم‌ها مدیریت منابع به گونه‌ای خواهد بود که بتوانند پاسخگوی معیارهای ارزیابی دقیق آزمایش شده باشد.
انتخاب یک میکروکنترلر، به جای انتخاب یک پردازنده و ادغام واحدهای جانبی، خود نیز یک تصمیم کلیدی است. وقتی یک میکروکنترلر انتخاب می‌شود، نحوه مدیریت حافظه و ورودی/خروجی‌های آن مشخص شده است. بنابراین می‌توان بطور سیستماتیک سطح SIL سخت‌افزار را در مرحله طراحی ارزیابی کرد.

۵- معرفی یک پلتفرم مناسب براساس استاندارد IEC62304

همان‌گونه که بیان شد جهت رسیدن به یک سیستم توسعه‌یافته با استانداردهای ایمنی می‌توان از سیستم‌عامل‌هایی استفاده کرد که دارای سطح ایمنی عملکردی مورد نظر باشند. همچنین لازم است سخت‌افزاری که جهت اجرای نرم‌افزار و RTOS استفاده می‌شود دارای شرایط سطح استاندارد مورد نظر باشد.
پردازنده‌های Hercules شرکت TI، Power Architecture شرکت NXP، STM32F4 شرکت ST، Znq-7000 شرکت Xilinx نمونه‌های پیشنهادی جهت رسیدن به سطح استانداردهای صنعتی و پزشکی می‌باشند.
پردازنده‌های Power Architecture شرکت NXP دارای گواهینامه استاندارد نیستند [۴]. پردازنده‌های STM32F4 شرکتST مطابق ادعای سازنده، دارای گواهینامه ISO26262 است، ولی سندی برای آن ارائه نداده است [۵]. پردازنده Znq-7000 دارای گواهینامه IEC61508 است اما قیمت آن بالاست و ابزار توسعه پیچیده‌ای دارد [۶]. پردازنده‌های Hercules شرکت TI، که پرچمدار پردازنده‌های ایمنی شرکت TIمی‌باشد، گزینه مناسبی جهت استانداردهای فوق است. این پردازنده‌ها به طور مستقل برای استفاده در برنامه های IEC 61508 SIL3 توسط موسسه Exida مورد ارزیابی قرار گرفته است [۷]. این پردازنده‌ها از پایه طوری طراحی شده‌اند تا خطرات سیستماتیک مرتبط با توسعه میکروکنترلر و همچنین مدیریت اتفاق‌های تصادفی در طول عملیات را بررسی کنند. ویژگی بارز این خانواده‌ها، دو هسته‌ای بودن آنها با آرایش قفل مرحله‌ای است، به این معنی که هر دو پردازنده همزمان جریان کد و داده را پردازش می‌کنند و یک مدار تشخیص خرابی امن با مقایسه نتایج در آنها طراحی شده است (شکل ۱).
شرکت TI در طراحی میکروکنترلرهایی با کارکرد ایمن و یکپارچه سازی حافظه و ورودی/خروجی‌ها تمهیدات بیشتری نسبت به دیگر میکروکنترها انجام داده است. آنها می‌توانند با استفاده از ECC به صورت خودکار خطاهای یک بیتی را در حافظه در زمان اجرا اصلاح کنند و خطاهای دو بیتی در حافظه‌های SRAM، FLASH و حافظه‌های ارتباطی را شناسایی کنند. حتی صف و بافرهای واحدهای جانبی میکروکنترلر دارای بیت پریتی در زمان اجرا هستند. همچنین این میکروکنترها دارای چک کننده CRC سخت‌افزاری در حافظه می‌باشند.



شکل ۱. ساختار میکروکنترلر Hercules شرکت TI

در حوزه نرم‌افزار، سیستم عامل SAFERTOS® که دارای

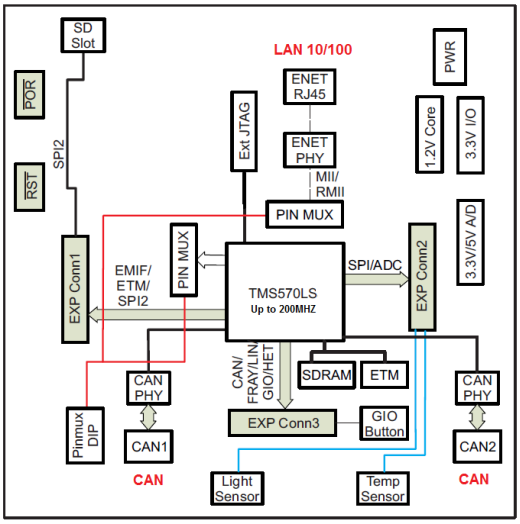
تاییدیه از قبل می‌باشد، برای استفاده در برنامه های IEC61508 SIL3 مناسب است. اگر SAFERTOS® در یک سیستم با ایمنی عملکردی بالا استفاده می‌شود باید آن را مطابق راهنمای ایمنی شرکت ارائه دهنده استفاده کرد.

بسته نرم افزاری WITTENSTEIN Design Assurance Pack (DAP) که همراه با این سیستم عامل عرضه شده، در زمینه استفاده از حافظه و یکپارچه سازی ورودی/خروجی تراشه‌های Hercules شرکت TI مورد آزمایش قرار گرفته است، که به طور قابل توجهی زمانهای توسعه و دریافت گواهینامه ایمنی عملکردی سیستم را کاهش می‌دهد.

برای کاربردهای پزشکی SAFERTOS با بسته نرم افزاری WITTENSTEIN Design History File (DHF) عرضه می‌شود. DHF به طور مستقل برای انطباق با استانداردهای دستگاه‌های پزشکی کلاس III FDA510 (k) و EN62304 تایید شده است.

بنابراین SAFERTOS® که بر روی تراشه‌های Hercules شرکت TI پیاده سازی شده است، یک پلتفرم ایده‌آل برای توسعه سیستم‌های ایمنی در پزشکی مانند پمپ‌های دیابتی، سیستم‌های تزریق و سیستم‌های کنترل فشار خون، است. این پلتفرم علاوه بر کاربردهای پزشکی در صنایع حمل و نقل، راه‌آهن و هوا فضا نیز قابل استفاده است.

جهت استفاده از پردازنده Hercules شرکت TI و نرم‌افزار SAFERTOS لازم است که یک پلتفرم و برد سخت‌افزاری طراحی شود. این طراح باید بر اساس استانداردهای طراحی برد انجام شود و تمام بخش‌ها در این طراحی دیده شود. در شکل (۲) بلوک دیاگرام پلتفرم طراحی شده نشان داده شده است. در این پلتفرم از پردازنده مرکزی TMS570LS شرکت TI که از خانواده Hercules می‌باشد استفاده شده است. به غیر از پردازنده مرکزی در طراحی دیگر بخش‌ها مانند بخش توان و بخش ارتباطات مانند ارتباط LAN و CAN از استاندارد ایمنی استفاده شده است. در این پلتفرم تمام ارتباطات دیجیتال و آنالوگ لازم برای اغلب کاربردها دیده شده است و همچنین ارتباط با کامپوتر از طریق ارتباط USB میسر شده است و می‌توان در یک شبکه LAN یا CAN با دیگر دستگاه ها ارتباط برقرار کرد.



شکل ۲. بلوک دیاگرام پلتفرم طراحی شده

۶- نتیجه‌گیری

در این مقاله استانداردهای مختلف ایمنی بررسی شده و استاندارد EN62304 به عنوان استاندارد هدف در تجهیزات پزشکی مبنا قرار گرفته است. ازآنجا که استاندار فوق از استاندارد IEC61508 استفاده کرده است، لذا تحلیل سطوح مختلف ایمنی براساس آن انجام شده است. انتخاب RTOS مطمئن و یک میکروکنترلر به جای پردازنده، می‌تواند در کاهش خطر و بالابردن سطوح ایمنی یک سیستم الکترونیکی موثر باشد. پس از بررسی سخت‌افزارهای مختلف، استفاده از پردازنده‌های Hercules شرکت TI به همراه برنامه SAFERTOS® برای طراحی و ساخت سیستم‌های با سطوح ایمنی بالا توصیه می‌شود. این پردازنده‌ها در سیستم‌های مختلف صنعتی، خودرویی، پزشکی و حتی نظامی استفاده شده‌اند و اسناد سطوح ایمنی آنها توسط سازنده انتشار داده شده است.

پلتفرم معرفی شده در این مقاله بر اساس پردازنده TMS570LS شرکت TI از خانواده Hercules طراحی شده است. این پلتفرم اکثر گذرگاه‌های استاندارد (ماند LAN) را پشتیبانی می‌کند و برای استفاده در تجهیزات پزشکی توصیه می‌شود.

مراجع

[1] Software Safety Standard , NASA-STD-8719.13C, Approved:05-07-2013

[2] Eric Verhulst, Jose de la Vara ,"From Safety Integrity Level to Assured Reliability and Resilience Level for Compositional Safety Critical Systems",ICSSEA 2013-4,

[3] Gianpiero Negri, challenges and Approaches in Ethical Machines Development - Conference Paper ·

Opportunities and Challenges in Regulating Robotics and Artificial Intelligence. 2018

[4] https://www.nxp.com/products/processors-and microcontrollers/power-architecture-processors/mpc5xxx-55xx-32-bit-mcus/ultra-reliable-mpc57xx-32-bit-automotive-and-industrial-microcontrollers-mcus/

[5] https://www.st.com/en/automotive-microcontrollers/spc5-mcus-for-safety-critical-applications-and-motor-control.html?querycriteria=productId=SS1534

[6] https://www.xilinx.com/news/press/2017/xilinx-single-chip-solution-with-on-chip-redundancy-for-functional-safety-speeds-up-iec-61508-certification-and-reduces-systems-development-cost.html

[7] http://www.ti.com/ww/en/functional_safety/safeti/SafeTI-61508.html.