طراحی و تحلیل ایمنی واحد کنترل درب در سیستم درب‌های جدا کننده سکو منطبق بر متروی تهران

امید خان‌فرخانی، دانشجوی کارشناسی ارشد، دانشکدهٔ مهندسی راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران

محمدعلی صندیدزاده*، دانشیار، دانشکدهٔ مهندسی راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران

*پست الکترونیکی نویسنده مسئول: sandidzadeh@iust.ac.ir

دریافت: ۹۶/۱۲/۰۵- پذیرش: ۹۷/۰۴/۱۸

صفحه ۲۷۰-۲۵۹

چکیده

واحد کنترل درب یکی از اجزای کنترلی در سیستم درب‌های جدا کننده سکو می‌باشد که عملکرد صحیح و ایمن آن نقش بسزایی بر ایمنی مسافرین بر روی سکو و جلوگیری از تاخیر قطارها در ایستگاه دارد. در سیستم کنترل درب‌ها، بیشترین نرخ خطا مربوط به واحد کنترل درب است، بنابراین تحلیل خطاها و بررسی قابلیت اطمینان آن از اهمیت ویژه‌ای برخوردار می‌باشد. بدین منظور، در این مقاله ابتدا اجزای یک واحد کنترل درب برای سیستم درب‌های جدا کننده سکو و منطبق بر متروی تهران مشخص می‌گردند. سپس خطاهای احتمالی در این اجزا به روش تحلیل مقدماتی خطر مورد بررسی قرار گرفته و اصلاحات مورد نیاز انجام شده است. در گام بعد با استفاده از اجزای انتخاب شده و نتایج تحلیل خطا، واحد کنترل درب بصورت بلوکی ارائه می‌شود. در نهایت جهت بررسی درجه ایمنی مدار، قابلیت اطمینان به روش بلوک دیاگرام و سطح ایمنی طبق استاندارد IEC61508 محاسبه شده که منتهی به سطح ایمنی ۳ گردید.

واژه‌های کلیدی: درب‌های جدا کننده سکو، واحد کنترل درب، تحلیل خطا و قابلیت اطمینان

۱- مقدمه

در سیستم‌های حمل و نقل ریلی درون شهری، به‌منظور تامین سلامتی مسافران و افزایش ضریب ایمنی سکو در حرکت‌های مسافری، یکی از تجهیزات مرسوم که بخصوص در سیستم‌های بدون راهبر بعنوان جزء ثابت لحاظ می‌شود، سیستم درب‌های جدا کننده سکو (PSD)[1] است. PSD به‌عنوان یک ابزار کنترلی، ضمن ممانعت از سقوط مسافران به روی ریل، وظایف امنیتی را تا توقف کامل قطار بر روی سکو و پیاده و سوار شدن مسافران و ترک ایستگاه به‌وسیله قطار، بصورتی کاملا خودکار انجام می‌دهد (اصفهانی، صالحی و فتحنائی، ۱۳۹۱). سیستم PSD دارای درب‌های خودکار به تعداد درب‌های قطار است که پس از توقف قطار در ایستگاه، همزمان با درب‌های قطار باز می‌شوند و پس از اتمام جابجایی مسافرین، همزمان با درب‌های قطار بسته می‌شوند (Connor, 2011; Luo, Zhaoyong and Jin, 2012). در PSD جهت جابجایی ایمن مسافرین و همچنین جلوگیری از تاخیر قطار، سیستم‌های کنترلی مختلفی وجود دارد که یکی از آن‌ها واحد کنترل درب (DCU)[2] است (Luo, Zhaoyong and Jin, 2012; Dubai Municipality, 2004; Pintsch Bamag, 2011). DCU بخش اصلی سیستم محرک درب‌ها است که کلیه وظایف مربوط به درب‌های خودکار اعم از باز و بسته کردن آن‌ها، تشخیص مانع و ارسال گزارش وضعیت درب‌ها به

سیستم نظارت را بر عهده دارد (Dubai Municipality, 2004; Pintsch Bamag, 2011). در مورد سیستم محرک درب‌های PSD و مترو پژوهش‌هایی نیز انجام گرفته است. لو و همکاران (۲۰۱۲)، مطالعاتی بر روی استراتژی کنترل سیستم PSD برای دستیابی به ایمنی انجام داده‌اند. در پژوهش مذکور، بعد از بررسی خطاهای سیستم PSD، استراتژی کنترل سلسله مراتبی برای آن معرفی شده که شامل سه سطح کنترل خودکار، کنترل نیمه خودکار و کنترل دستی است. سپس سطوح ایمنی بر روی مدارات سیگنال ایمنی و تشخیص مانع در یک سیستم PSD محاسبه شده‌اند (Luo, Zhaoyong and Jin, 2012). هی و کیم (۲۰۱۱)، به تشریح DCU در سیستم PSD پرداخته‌اند. در این پژوهش، ابتدا اجزای یک سیستم PSD و سپس DCU آن، معرفی شده‌اند. سپس یک بلوک دیاگرام کنترلی، برای کنترل سرعت موتور بدون جاروبک جریان مستقیم (BLDC)[3] استفاده شده در درب‌های متحرک پیشنهاد شده است (Hee and Kim, 2011). چنگ و همکاران (۲۰۱۳)، به تحلیل قابلیت اطمینان در سیستم درب مترو به روش FMECA پرداخته‌اند. در پژوهش مذکور ابتدا اجزای محرک درب معرفی شده و خطاهای مهم در این اجزا مشخص شده است. سپس این خطاها دسته‌بندی شده و مدهای خطا محاسبه شده‌اند. در نهایت، روش FMECA برای تحلیل قابلیت اطمینان پیاده سازی شده است (Cheng (et.al), 2013). در سیستم محرک درب‌های PSD، بیشترین نرخ خطا مربوط به DCU است و عملکرد صحیح سیستم PSD در نقطه آخر به عملکرد صحیح DCU وابسته است (Cheng (et.al), 2013). بنابراین تحلیل خطاها و بررسی قابلیت اطمینان DCU از اهمیت ویژه‌ای برخوردار است که تاکنون مطالعاتی بر روی آن انجام نشده است. اما لازمه تجزیه و تحلیل یک سیستم داشتن اطلاعات دقیق از ساختار و عملکرد آن است. در این مقاله ابتدا اجزای یک واحد کنترل درب برای سیستم درب‌های جدا کننده سکو منطبق بر متروی تهران مشخص می‌گردند. سپس خطاهای احتمالی در این اجزا به روش تحلیل مقدماتی خطر (PHA)[4] مورد بررسی قرار گرفته و اصلاحات مورد نیاز انجام شده است. در گام بعد با استفاده از اجزای انتخاب شده و نتایج تحلیل خطا، واحد کنترل درب بصورت بلوکی ارائه می‌شود. در نهایت جهت بررسی درجه ایمنی مدار، قابلیت اطمینان به روش بلوک دیاگرام (RBD)[5] و سطح ایمنی طبق استاندارد IEC61508 محاسبه می‌شود.

۲- واحد کنترل درب

سیستم PSD دارای مجموعه‌ای از درب‌ها شامل درب‌های ثابت (FD)[6]، درب‌های کشویی خودکار (ASD)[7]، درب‌های اضطراری (ED)[8] و درب انتهای سکو (PED)[9] می‌باشد که این درب‌ها در یک چهار چوب فلزی قرار دارند. FD ثابت و همیشه بسته هستند. ASD شامل یک جفت درب کشویی است که هماهنگ با درب‌های قطار باز و بسته می‌شوند که تعدادشان به تعداد درب‌های قطار است. ED ها می‌توانند در موارد بروز حادثه و در صورت نیاز به صورت دستی باز شوند. این درب‌ها به تعداد مورد نیاز بین درب‌های ASD قرار می‌گیرند. PED نیز در آخر ایستگاه قرار دارد و می‌تواند به صورت دستی کنترل (باز و بسته) شود. از این درب برای دسترسی کارکنان ایستگاه به تونل و تخلیه اضطراری مسافرین استفاده می‌شود (Luo, Zhaoyong and Jin, 2012; Dubai Municipality, 2004; Pintsch Bamag, 2011; NRT group, 2010).

سیستم کنترل PSD از دو بخش تشکیل می‌شود. بخش اول واحد کنترل عملکرد است که برای عملکرد ایمن سیستم PSD در شرایط مختلف، استراتژی کنترل سلسله مراتبی برای آن اتخاذ می‌گردد. در شرایط عادی، سیستم PSD به طور کاملا خودکار کنترل می‌شود. در موارد خاص، کنترل نیمه خودکار و کنترل دستی مطرح می‌شوند. بخش دوم، DCU است که بر روی هر درب خودکار نصب می‌شود (Luo, Zhaoyong and Jin, 2012). DCU وظیفه انجام تمامی عملیات مربوط به درب‌ها را بر عهده دارد. پس از توقف کامل قطار در موقعیت مناسب، دستور «باز» یا «بسته» شدن درب‌ها از سیستم کنترل PSD به واحد کنترل درب ارسال می‌شود. درب‌های ED و PED، DCU ندارند، اما اگر یکی از این درب‌ها باز شوند، سیگنالی به نزدیک‌ترین DCU برای گزارش باز شدن درب فرستاده می‌شود. همچنین، هر DCU می‌بایست وضعیتش را به سیستم کنترل ارسال نماید. اگر هر DCU وضعیتش را به سیستم کنترل ارسال نکرد، می‌بایست درب مورد نظر باز

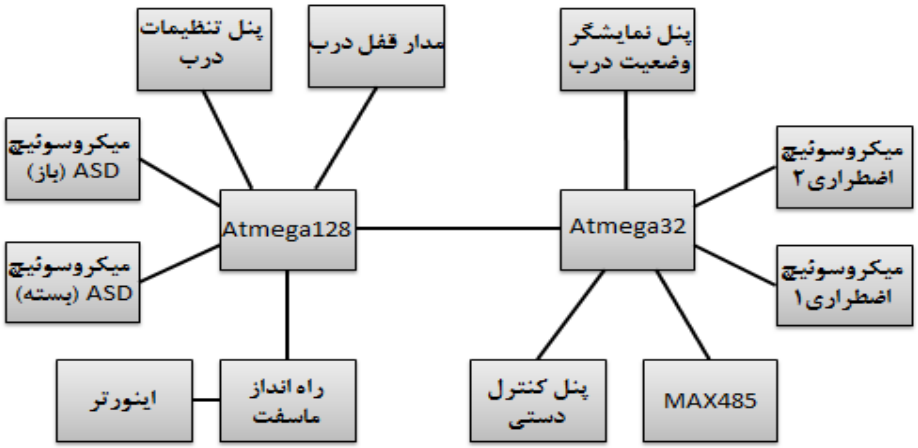
تلقی شود (Pintsch Bamag, 2011; Ashby, 2010). بنابراین یک DCU باید در تمامی زمان‌ها آماده به‌کار و منتظر دریافت فرامین باشد. یک DCU در حالت کلی دارای اجزای مدار کنترل موتور، تغذیه، حسگر یا مکانیزم تشخیص موانع، حسگر درب‌های اضطراری، حسگرهای تایید باز یا بسته بودن درب‌ها، سوئیچ‌ها، مدار قفل درب‌ها، سیستم تعیین وضعیت هر درب، درگاه‌های ارتباطی و ریز پردازنده می‌باشد (Pintsch Bamag, 2011; Hee and Kim, 2011; NRT group, 2010). درب‌های سیستم PSD می‌بایست همزمان با درب‌های قطار باز یا بسته شوند تا سوار و پیاده شدن مسافرین با تاخیر صورت نگیرد. بنابراین باید به نحوی فرمان‌های باز یا بسته شدن درب‌های خودکار از قطار به کنار خط و PCU منتقل شوند. در سیستم سیگنالینگ متروی تهران، ارتباط بین قطار و کنار خط در ایستگاه از طریق آنتن ارتباط با کنار خط قطار (TWC)[10] صورت می‌گیرد. به این ترتیب، با ایجاد تغییراتی در سیستم کنترل روی قطار و ارتقای آنتن TWC می‌توان فرمان باز یا بسته شدن درب‌های خودکار سکو را به PCU ارسال کرد. در قطارهای متروی تهران، باز و بسته شدن درب قطار برعهده راهبر است. بنابراین با فشردن دکمه باز شدن درب‌های قطار، درب‌های PSD باز و با فشردن دکمه بسته شدن درب‌های قطار، درب‌های PSD بسته می‌شوند (Bombardier Inc, 2016). سیستم کنترل PSD این فرمان‌ها را به تمام DCUها ارسال می‌کند. بنابراین کافی است تمام DCU ها از طریق یک کانال ارتباطی به سیستم کنترل PSD وصل شوند (Dubai Municipality, 2004; Pintsch Bamag, 2011). حال که وظایف و اجزای کلی DCU مشخص شد، لازم است این اجزا به صورت قطعات الکترونیکی، الکترومکانیکی و یا مکانیکی انتخاب شده تا بتوان خطاها و قابلیت اطمینان آن را ارزیابی کرد. در جدول (۱) این انتخاب‌ها صورت گرفته است، بطوری که ضمن حفظ کیفیت، تمام قطعات در بازار ایران به راحتی نیز قابل دسترسی هستند.

۳- تحلیل ایمنی واحد کنترل درب

۳-۱- تحلیل خطا به روش PHA

روش PHA ابزاری برای شناسایی خطرات، عوامل مسبب، اثرات، شدت خطا و تعیین برخی نکات طراحی است. هدف PHA، تحلیل کیفی خطراتی است که در مراحل اولیه طراحی سیستم شناسایی شده‌اند. شاید اجرای PHA یکی از مهم‌ترین تحلیل‌ها در جریان ارزیابی ایمنی سیستم‌ها باشد چرا که این مطالعه اولین تلاش جدی برای تشخیص و رفع خطرات سیستم است. مشخص بودن تمام وظایف، حالت‌ها و اجزای سیستم و زیر سیستم‌ها پیش‌نیاز انجام تحلیل PHA است (Rausand, 2004). جدول (۲) نحوه کدبندی خطاها در تحلیل PHA و جدول (۳)، تحلیل PHA را بر روی اجزای DCU نشان می‌دهند.

هم‌اکنون می‌توانیم با توجه وظایف DCU، اجزای انتخاب شده و تحلیل خطای صورت گرفته، ساختار بلوکی شکل (۱) را برای DCU ارائه نماییم.



شکل ۱. ساختار بلوکی DCU

جدول ۱. اجزا و قطعات داخلی DCU

قطعات داخلی انتخابی	وظایف	اجزا
مقاومت و میکروسوئیچ	تشخیص باز یا بسته بودن درب اتوماتیک و اضطراری	حسگرهای تایید باز یا بسته بودن درب‌ها
مقاومت، ترانزیستور BD139، دیود، رله ۵ ولت	قفل کردن درب اتوماتیک پس از بسته شدن، باز کردن قفل قبل از باز شدن درب	مدار قفل الکتریکی درب
ترانزیستور ماسفت IRF540 برای اینورتر ۳ فاز ٦ سوئیچه، دیود، مقاومت، خازن، TC4427 برای تحریک ماسفت‌ها	تحریک موتور BLDC درب	مدار تحریک موتور (اینورتر و راه انداز اینورتر)
Atmega128	فرمان به مدار تحریک موتور برای چرخش راستگرد و ساعتگرد، تشخیص مانع، کنترل مدار قفل درب، تشخیص باز یا بسته بودن درب اتوماتیک	کنترل کننده موتور
MAX485 برای ارتباط سریال با استاندارد RS485 و پروتکل Profibus DP	کانال ارتباطی بین تمام DCU ها و سیستم کنترل PSD	رابط کنترلی
Atmega32	ارتباط با سیستم کنترل PSD از طریق رابط کنترلی جهت دریافت فرمان‌ها و ارسال وضعیت، ارتباط با کنترل کننده موتور، ارتباط با پنل کنترل دستی، ارتباط با نمایشگر وضعیت درب	کنترل کننده اصلی
کلید فشاری، مقاومت، الس‌ی‌دی کاراکتری	تنظیم شماره DCU، سرعت حرکت درب و زمان افت سرعت	پنل تنظیمات
	برای اتصال موتور، منابع تغذیه، سنسورها، کابل شبکه، قفل، نمایشگر وضعیت درب و پنل کنترل دستی به DCU	پورت ها

جدول ۲. کدبندی خطاها در PHA (Rausand, 2004)

کد	شدت	توضیحات
٤	فاجعه بار	خطایی که منجر به آسیب‌های شدید یا مرگ افراد شود
۳	بحرانی	خطایی که منجر به آسیب‌دیدگی کوچک در افراد شود
۲	بزرگ	خطایی که منجر به شکست در سیستم شود
۱	کوچک	خطایی که باعث ایجاد مشکلات کوچک در سیستم شود

جدول ۳. تحلیل PHA برای DCU

شماره	خطا	علت	اثرات	شدت	اقدامات پیشگیرانه
۱	یکسره شدن میکروسوئیچ درب اضطراری	قطع ارتباط با DCU، خرابی یا گرفتگی میکروسوئیچ، سوختن مقاومت	عدم نمایش صحیح وضعیت درب اضطراری، تاخیر در سرویس‌دهی، آسیب دیدن مسافرین، تلفات	٤	تحلیل وضعیت میکروسوئیچ توسط پردازنده اصلی، اضافه کردن یک میکروسوئیچ دیگر و اجاد ترکیب 2oo2 برای آن‌ها
۲	یکسره شدن میکروسوئیچ‌های ASD	قطع ارتباط با DCU، خرابی یا گرفتگی میکروسوئیچ‌ها، سوختن مقاومت	عدم کنترل صحیح درب، عدم نمایش صحیح وضعیت درب، تاخیر در سرویس‌دهی	۲	تحلیل وضعیت میکروسوئیچ‌ها توسط پردازنده موتور
۳	عمل نکردن قفل	خرابی قفل، قطع ارتباط با DCU، خرابی رله، سوختن ترانزیستور، سوختن دیود، سوختن مقاومت	عدم تشخیص صحیح قفل بودن یا نبودن درب، باز نشدن یا قفل نشدن درب، عمل نکردن حالت کنترل دستی، تاخیر در سرویس‌دهی، آسیب دیدن مسافرین، تلفات	٤	ایجاد وضعیت 2oo2 با گرفتن فیدبک از پایه قفل که به رله متصل شده (با استفاده از رگولاتور ۷۸۰۵)
٤	مشکل در پنل کنترل دستی	قطع ارتباط با DCU ، خرابی یا گیر کردن کلیدها، سوختن مقاومت	عدم کنترل صحیح درب، عدم عملکرد درب در حالت کنترل دستی، تاخیر در سرویس‌دهی	۲	تشخیص وضعیت کلیدها توسط پردازنده اصلی
۵	خرابی نمایشگر درب بر روی سکو	قطع ارتباط پورت نمایشگر با DCU، سوختن نمایشگر، مشکل در پنل کنترل دستی	عدم اطلاع صحیح از وضعیت کنترل درب بر روی سکو	۱	-
٦	مشکل در ارتباط با شبکه	قطع شدن کابل شبکه، جدا شدن کابل شبکه از پورت DCU، خرابی آی‌سی رابط (MAX485)	عدم اطلاع از وضعیت درب در اتاق نظارت، عدم اجرای فرمان‌های صادر شده به درب، تاخیر در سرویس‌دهی	۱	-
۷	مشکل در پنل تنظیمات	سوختن ال‌سی‌دی، خرابی یا گیرکردن کلیدها، سوختن مقاومت	عدم اطلاع از شماره DCU در هنگام تنظیم، ناتوانی در تنظیم پارامترها، درست کار نکردن درب، عدم اجرای فرمان‌ها	۱	-

اضافه کردن فیوز به لینک DC اینورتر	۲	کار نکردن درب، تاخیر در سرویس‌دهی و آسیب دیدن موتور	سوختن آی‌سی‌های راه‌انداز ماسفت، خرابی خازن یا مقاومت راه‌انداز ماسفت، سوختن دیودها یا ترانزیستورهای اینورتر و قطع شدن تغذیه	مشکل در مدار راه‌انداز (اینورتر و راه‌انداز ماسفت)	۸
انتخاب پردازنده با کیفیت، جدا کردن تغذیه قسمت‌های دیجیتال از بخش‌های جریان‌کش	۲	کار نکردن درب، درست کار نکردن درب، کار نکردن پنل تنظیمات، مشخص نبودن وضعیت درب ، تاخیر در سرویس‌دهی	خرابی پردازنده	مشکل در پردازنده موتور	۹
انتخاب پردازنده با کیفیت، جدا کردن تغذیه قسمت‌های دیجیتال از بخش‌های جریان‌کش	۲	از کار افتادن کلیه عملیات درب‌های متصل به این واحد، تاخیر در سرویس‌دهی	خرابی پردازنده، قطع شدن تغذیه	مشکل در پردازنده اصلی	۱۰

۳-۲- ارزیابی قابلیت اطمینان DCU به روش RBD

روش RBD یک توصیف بلوکی از چگونگی ارتباط اجزای سیستم است که در آن هر جزء به صورت یک بلوک نمایش داده می‌شود. سپس با توجه به نحوه عملکرد سیستم، بلوک‌های موثر در شکست به‌صورت سری، موازی و یا ترکیبات خاص از چپ به راست به یکدیگر وصل شده و خروجی را می‌سازند. درنهایت با استفاده از روابط قابلیت اطمینان مربوط به هر چیدمان، قابلیت اطمینان کلی سیستم محاسبه می‌گردد. بلوک دیاگرام قابلیت اطمینان یکی از ساده‌ترین روش‌های نمایش و محاسبه قابلیت اطمینان در سیستم‌های پیچیده است. همچنین در این روش، میزان حساسیت خرابی سیستم به نرخ خرابی هر جزء به وضوح نمایان‌گر می‌گردد (بیلیتون و آلن، ۱۳۹۳ ,Distefano Salvatore and Puliafito, 2007).

برای محاسبه قابلیت اطمینان به روش RBD، می‌بایست اقدامات زیر انجام شود (Distefano, Salvatore and Puliafito, 2007).

–تعیین وظایف سیستم

–تعیین ارتباط بین حداقل اجزای سیستم جهت دستیابی به اهداف

–ترسیم بلوک دیاگرام RBD

–استخراج نرخ خرابی بلوک‌ها و ساده سازی

–محاسبه قابلیت اطمینان سیستم

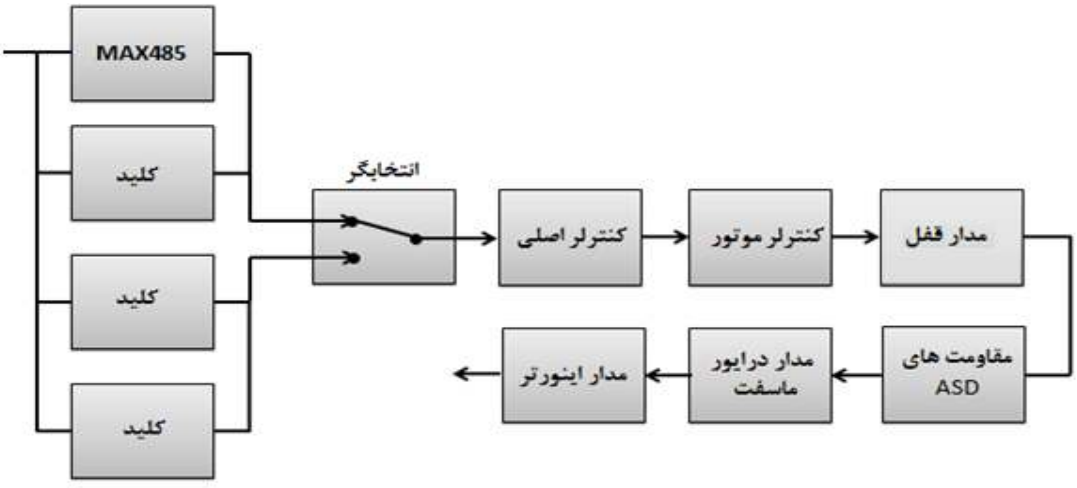
DCU، دارای دو ماموریت است؛ اینکه بتواند فرمان‌های رسیده به درب را اجرا کند و همچنین وضعیت صحیح درب‌های خودکار را به سیستم نظارت ارسال کند. عدم اجرای هر یک از این وظایف منجر به تحت الشعاع قرار گرفتن عملکرد رضایت بخش سیستم می‌گردد.

در DCU ارائه شده، خرابی برخی اجزا فقط بر روی اجرای فرامین اثر می‌گذارد، خرابی برخی فقط بر روی اعلام وضعیت صحیح تاثیر گذار است و خرابی برخی اجزا روی هر دو وظیفه تاثیر می‌گذارد. بنابراین در اینجا مفهوم «وقوع حداقل یکی از دو حادثه» مطرح می‌شود که در آن حادثه‌ها مستقل ولی سازگارند. به این ترتیب، از دو مدل برای سیستم استفاده می‌کنیم. در مدل اول، زیرسیستم‌هایی آورده می‌شود که خرابی آن‌ها بر روی اجرای فرامین اثر گذار است و در مدل دوم زیر سیستم‌هایی آورده می‌شود که خرابی آن‌ها بر اعلام وضعیت صحیح درب‌ها تاثیر گذار است. سپس قابلیت اطمینان دو مدل بطور جداگانه محاسبه شده و در نهایت باتوجه به رابطه (۱) قابلیت اطمینان کل سیستم بدست آورده می‌شود (بیلیتون و آلن، ۱۳۹۳).

$$P_{final} = P(A \cup B) = P(A) + P(B) - P(A).P(B) \quad (۱)$$

در رابطه (۱)، $P(A)$ احتمال وقوع حادثه A و $P(B)$ احتمال وقوع حادثه B است. برای اجرای وظیفه اول، می‌بایست فرمان باز یا بسته شدن به طریقی به کنترل کننده اصلی برسد. این فرمان در حالت کنترل خودکار از طریق آی‌سی شبکه یا کلید سمت تونل (در پنل کنترل دستی) به کنترل کننده اصلی می‌رود. بنابراین این دو المان بصورت موازی با یکدیگر هستند و تشکیل یک زیر سیستم می‌دهند.

در حالت کنترل دستی فرمان از کلید سمت تونل یا سمت ایستگاه به کنترل کننده اصلی می‌رسد. بنابراین این دو المان نیز با یکدیگر موازی هستند و تشکیل یک زیر سیستم دیگر می‌دهند. اما درب در یک زمان یا در حالت کنترل خودکار است یا دستی و این حالت با استفاده از انتخابگر تعیین می‌شود. بنابراین، در ابتدا دو زیر سیستم داریم که یکی از آن‌ها در حال کار و دیگری آماده بکار است. این گونه ارتباط، سیستم با عضو مازاد آماده بکار نامیده می‌شود. سپس کنترل کننده اصلی، دستورات را به کنترل کننده موتور می‌رساند. کنترل کننده موتور نیز پس از چک کردن وضعیت قفل و میکروسوئیچ‌های ASD، از طریق راه اندازهای ماسفت به اینورتر فرمان داده و در نهایت موتور به چرخش در می‌آید. میکروسوئیچ‌های ASD از اجزای داخلی DCU نیستند اما سالم بودن مقاومت‌های در نظر گرفته شده برای آن بر کنترل صحیح درب اثر گذار است. بنابراین، مدار قفل، مقاومت‌های میکروسوئیچ‌های ASD، کنترل کننده اصلی، کنترل کننده موتور، مدار راه‌انداز ماسفت و اینورتر به صورت سری عمل می‌کنند. در نتیجه، مدل سیستم بصورت شکل (۲) خواهد گردید.



شکل ۲. مدل سیستم DCU برای اجرای وظیفه اول

شکل ۳. مدل سیستم DCU برای اجرای وظیفه دوم

اما برای اجرای وظیفه دوم، وضعیت صحیح درب به عملکرد صحیح کنترل کننده موتور، کنترل کننده اصلی، مدار قفل، آی‌سی شبکه و سالم بودن مقاومت‌های میکروسوئیچ‌های ASD وابسته است و نقص در هریک منجر به تشخیص اشتباه می‌گردد. به این ترتیب، مدل سیستم در این حالت همانند شکل (۳) می‌شود. در هر بلوک کلید، یک کلید فشاری و یک مقاومت سری با یکدیگر هستند. در بلوک انتخابگر، یک کلید انتخابگر و یک مقاومت با یکدیگر سری هستند. در بلوک مقاومت‌های ASD، چهار مقاومت با یکدیگر سری هستند. در بلوک مدار قفل، مقاومت، ترانزیستور BD139، دیود، رله، رگولاتور ۷۸۰۵ و دو خازن با یکدیگر سری هستند. در بلوک راه‌انداز ماسفت، ۸ خازن، ٦ مقاومت و ۳ آی‌سی TC4427 سری هستند. در نهایت، در بلوک اینورتر، دو عدد فیوز، ٦ دیود و ٦ ترانزیستور IRF540 سری با یکدیگر می‌باشند.

بنابراین در مدل‌های سیستم و بلوک‌ها، قطعات بصورت سری، موازی و مازاد آماده به‌کار قرار دارند که قابلیت اطمینان آن‌ها از روابط (۲-٤) محاسبه می‌شود.

$$R_s = \prod_{i=1}^{n} R_i \qquad (۲)$$

$$R_p = 1 - \prod_{i=1}^{n} Q_i \qquad (۳)$$

$$R_t = e^{-\lambda_A} + \frac{Ps\lambda_A}{\lambda_B - \lambda_A}(e^{-\lambda_A} - e^{-\lambda_B}) \qquad (٤)$$

در رابطه (۲)، n تعداد سیستم‌های سری و R_i قابلیت اطمینان هرکدام از آن‌هاست. در رابطه (۳)، n تعداد سیستم‌های موازی و Q_i احتمال خرابی هر کدام از آن‌هاست. در رابطه (٤)، λ_A نرخ خرابی عضو اصلی، λ_B نرخ خرابی عضو مازاد و P_s احتمال سالم بودن انتخابگر می‌باشند.

میزان نرخ خرابی و قابلیت اطمینان قطعات موثر در ارزیابی قابلیت اطمینان در جدول (٤) لیست شده است که در آن، قابلیت اطمینان از رابطه (۵) محاسبه شده است (بیلیتون و آلن، ۱۳۹۳).

$$R(t) = e^{-\lambda t} \qquad (۵)$$

در رابطه (۵)، λ نرخ خرابی بر حسب خطا بر ساعت می‌باشد. با استفاده از جدول (٤)، روابط (۲-٤) و شکل‌های (۲) و (۳) داریم:

$$R_{Auto} = (R_{C3}R_{C13}) + R_{C1} - R_{C1}R_{C3}R_{C13} \qquad (٦)$$

$$\lambda_{Auto} = -\ln(R_{Auto}) \qquad (۷)$$

$$R_{Manual} = 2(R_{C3}R_{C13}) - (R_{C3}R_{C13})^2 \qquad (۸)$$

$$\lambda_{Manual} = -\ln(R_{Manual}) \qquad (۹)$$

که در آن، R_{Auto} و λ_{Auto} به ترتیب قابلیت اطمینان و نرخ خرابی بلوک‌های موازی MAX485 و دکمه در مدل ۱ هستند. R_{Manual} و λ_{Manual} به ترتیب قابلیت اطمینان و نرخ خرابی ۲ بلوک موازی دکمه در مدل ۱ می‌باشند.

$$R_{Model1} = \left(R_{Auto} + \frac{R_{C2}R_{C13}\lambda_{Auto}}{\lambda_{Manual} - \lambda_{Auto}}(R_{Auto} - R_{Manual})\right) (R_{C3})^2 \left(R_{C13}R_{C4}R_{C5}R_{C6}R_{C7}(R_{C12})^2\right)(R_{C13})^4 \left((R_{C12})^2\left(R_{C9}(R_{C13})^2(R_{C12})^2\right)^3\right) \left((R_{C11})^2(R_{C10})^6(R_{C3})^6\right) \qquad (۱۰)$$

$$Q_{Model1} = 1 - R_{Model1} = 1.21 \times 10^{-6} \qquad (۱۱)$$

$$R_{Model2} = (R_{C13})^4(R_{C13}R_{C4}R_{C5}R_{C6}R_{C7})(R_{C12})^2(R_{C3})^2R_{C1} \qquad (۱۲)$$

$$Q_{Model2} = 1 - R_{Model2} = 7.688 \times 10^{-7} \qquad (۱۳)$$

از معادلات (۱)، (۵)، (۱۱) و (۱۳) داریم:

$$R_{DCU} = 1 - (Q_{Model1} + Q_{Model2} - (Q_{Model1}Q_{Model2})) = 0.99999802 \qquad (۱٤)$$

$$\lambda_{DCU} = -\ln(R_{DCU}) = 1.98 \times 10^{-6} \quad (۱۵)$$

حال لازم است بدانیم که این میزان نرخ خرابی برای مدار DCU مناسب است یا نه. یک معیار مناسب برای سنجش درجه ایمنی یک سیستم، سطوح ایمنی (SIL)[۱۱] است. در استاندارد IEC61508 چهار سطح ایمنی تعریف شده است. SIL1 کمترین میزان در کاهش خطرات را داراست و SIL4 بیشترین سطح کاهش خطرات را نشان می‌دهد (Exida, 2006). سطوح ایمنی برای دو حالت، کم تقاضا و پر تقاضا یا حالت پیوسته تعریف شده است. در حالت کم تقاضا، احتمال خطا روی تقاضا (PFD)[۱۲] و در حالت پرتقاضا احتمال خطای خطرناک بر ساعت (PFH)[۱۳] مطرح می‌شوند که مقادیر آن‌ها مطابق استاندار IEC61508 در جدول (۵) آورده شده است (Exida, 2006; Börcsök).

باید توجه کرد که واحد حالت پرتقاضا بر ساعت است در حالیکه حالت کم تقاضا برای یک سال تعریف می‌شود. از آنجا که یک سال ۸۷۶۰ ساعت است (تقریبا ۱۰۰۰۰)، بنابراین هر دو حالت از نظر اندازه گیری ایمنی تقریبا یکسان هستند (Exida, 2006).

جدول ٤. نرخ خرابی و قابلیت اطمینان قطعات موثر در ارزیابی قابلیت اطمینان DCU

شماره	نام قطعه	نرخ خرابی (خطا بر ساعت)	قابلیت اطمینان	توضیحات	مرجع
C1	MAX485	0.8×10^{-9}	0.9999999992	-	(Pedicord, 2002)
C2	Selector	0.2×10^{-6}	0.9999978	-	(Electroswitch Corp, 1994)
C3	Push Button	0.1×10^{-6}	0.9999999	-	(HSE, 2002)
C4	BD139	1.15×10^{-9}	0.99999999885	-	(ON Semicoductor, 2016)
C5	Diode	0.056×10^{-9}	0.999999999944	-	(ROHM, 2013)
C6	Relay	0.1×10^{-6}	0.9999999	-	(OMRON)
C7	LM7805	6.08×10^{-7}	0.9999994	-	(Lee, 2009)
C8	AVR	27.8×10^{-9}	0.9999999722	Mega , Tiny	(Atmel Corp, 2005)
C9	TC4427	2.17×10^{-9}	0.99999999783	Similar	(Linear Technology, 2016)
C10	IRF540	54×10^{-9}	0.99999994	-	(International Rectifier, 2004)
C11	Fuse	2×10^{-8}	0.99999998	-	(HSE, 2002)
C12	Capacitor	4×10^{-9}	0.999999996	-	(Kyu and Kim, 2012)
C13	Resistor	0.6×10^{-9}	0.9999999994	–	(Kyu and Kim, 2012)

جدول ۵. سطوح ایمنی در استاندارد IEC61508 (Exida, 2006)

SIL	PFD	PFH
4	$\geq10^{-5}$ to $<10^{-4}$	$\geq10^{-9}$ to $<10^{-8}$
3	$\geq10^{-4}$ to $<10^{-3}$	$\geq10^{-8}$ to $<10^{-7}$
2	$\geq10^{-3}$ to $<10^{-2}$	$\geq10^{-7}$ to $<10^{-6}$
1	$\geq10^{-2}$ to $<10^{-1}$	$\geq10^{-6}$ to $<10^{-5}$

برای محاسبه سطح ایمنی در حالت کم تقاضا و برای سیستم با معماری یک از یک داریم:

$$PFD = (\lambda_{DU} + \lambda_{DD})t_{CE} = \lambda_D t_{CE} \quad (۱۶)$$

در رابطه (۱۶)، λ_D نرخ خرابی خطرناک، λ_{DD} نرخ خرابی خطرناک قابل رویت، λ_{DU} نرخ خرابی خطرناک غیرقابل رویت و t_{CE} زمان از کارافتادگی معادل هستند.

اگر نرخ خرابی یک سیستم λ باشد، ۵۰٪ آن بعنوان نرخ خرابی ایمن (λ_S) و ۵۰٪ دیگر بعنوان نرخ خرابی خطرناک درنظر گرفته می‌شود. برای تعیین λ_{DU} و λ_{DD} از فاکتور پوشش تشخیصی (DC)[14] استفاده می‌شود. این فاکتور میزان تشخیص خطای خطرناک در سیستم را تعیین می‌کند که برای مشخص کردن آن از تست‌های تشخیصی خودکار استفاده می‌شود (Börcsök; Aschenbrenner, 2007). این میزان بخاطر تشخیص راحت خطا در DCU ، ۰/۹ در نظر گرفته شده است (Luo, Zhaoyong and Jin, 2012) که باتوجه به ساختار تقریبا ساده آن منطقی به نظر می‌آید. بنابراین، داریم:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \quad (۱۷)$$

$$If\ DC= 0.9\ then\ \lambda_{DD}= 0.9\lambda_D\ ,\ \lambda_{DU}= 0.1\lambda_D \quad (۱۸)$$

همچنین مقدار t_{CE} از رابطه (۱۹) تعیین می‌شود.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (۱۹)$$

که در آن T_1 فاصله زمانی اثبات تست (برحسب ساعت) و MTTR[15] میانگین زمان تعمیر (برحسب ساعت) می‌باشند (Aschenbrenner, 2007). باتوجه به اینکه PFD برای دوره زمانی یکساله تعریف شده است بنابراین T_1 برابر ۸۷۶۰ درنظر گرفته می‌شود. همچنین مقدار MTTR برابر ۰/۵ ساعت در نظر گرفته شده است (Luo, Zhaoyong and Jin, 2012). به این ترتیب از روابط (۱۵-۱۹) داریم:

$$PFD_{DCU} = 438.5 \times 0.99 \times 10^{-6} = 4.34 \times 10^{-4} \quad (۲۰)$$

مطابق جدول (۵)، DCU پیشنهادی دارای SIL3 می‌باشد.

٤- نتیجه‌گیری

در این مقاله، هدف طراحی و تحلیل ایمنی واحد کنترل درب در سیستم درب‌های جدا کننده سکو بود. برای این منظور ابتدا اجزای واحد کنترل درب برای سیستم درب‌های جدا کننده سکو منطبق بر متروی تهران مشخص شدند و تحلیل خطا به روش PHA بر روی آن‌ها انجام شد. سپس مدار DCU به‌صورت بلوکی ارائه گردید تا ارزیابی قابلیت اطمینان بر روی آن انجام شود. درنهایت، قابلیت اطمینان به روش RBD بر روی سخت افزار مدار ارزیابی گردید و برای سنجش درجه ایمنی مطابق استاندارد IEC61508، سطح ایمنی محاسبه شد، که با بدست آمدن SIL3، میزان ایمنی آن مورد تایید قرار گرفت.

٥- پی‌نوشت‌ها

1. Platform Screen Door
2. Door Control Unit
3. Brushless Direct Current
4. Preliminary hazard analysis
5. Reliability Block Diagram
6. Fixed Door
7. Automatic Sliding Door
8. Emergency Door
9. Platform End Door
10. Train-to-Wayside Communications
11. Safety Integrity Level
12. Probability of Failure on Damage
13. Probability of dangerous Failure per Hour
14. Diagnostic Coverage
15. Mean Time to Repair

٦- مراجع

- اصفهانی، م.، صالحی، پ.، فتحنائی، ف.، (۱۳۹۱)، "تحلیلی بر نقش مدیریت و تکنولوژی در استقرار سیستم‌های متروی بدون راننده"، دوازدهمین کنفرانس

بین‌المللی مهندسی حمل و نقل و ترافیک، تهران، ایران، ۱-۲ اسفند، ۱۳۹۱.

- بیلینتون، ر.، و آلن، ر.، (۱۳۹۳)، "ارزیابی قابلیت اطمینان سیستم‌های مهندسی"، ترجمه دکتر محسن رضائیان، ویرایش دوم، انتشارات دانشگاه صنعتی امیرکبیر، ص. ۱- ۱۵۰.

-Aschenbrenner, S. (2007), "IEC 61508- Where do the lambda values originate?", Hannover Messe.

-Ashby, D. (2010), "Sydney Metro Network Stage 2: Section 19 - Platform Screen Doors Reference Design Report", Pre-Final Reference Design.

Atmel Corporation (2005), "Microcontroller/AVR Reliability Data Package".

-Bombardier Inc (2016), "Tehran Psd Technical Proposal", Revision: 0.3.

-Börcsök, Josef, H. "Comparison of PFD Calculation", HIMA Paul Hildebrandt GmbH.

-Cheng, Xiaoqing, et al (2013), "Reliability Analysis of Metro Door System Based on FMECA", Journal of Intelligent Learning Systems and Applications.

-Connor, P. (2011), "Platform Protection Systems, A review of platform/train interface protection systems on railway", Railway Technical Web Pages, Info paper No.1.

-Distefano, Salvatore, and Antonio Puliafito (2007), "Dynamic reliability block diagrams vs dynamic fault trees", Annual Reliability and Maintainability Symposium, IEEE.

-Dubai Municipality (2004), "Dubai Light Rail Transit Project Final Design and Construction, PART 3 - Rail System Specific Technical Documents Platform Screen Door Particular Specification".

-Electroswitch Corp (1994), "Rotary Switches for Military Applications", Technical Publication, MIL-1.

-Exida (2006), "IEC 61508 Overview Report", Version.2.

-HSE (2002), "Proposal for requirements for low complexity safety related systems", RM Consultants Limited for the Health and Safety Executive.

-International Rectifier (2004), "Switch, I/O and IC Reliability Report".

-Kim, Sung Kyu, and Yong Soo Kim (2012) "A Study on FMEDA Process for SIL Certification: A Case Study of a Flame Scanner", IE interfaces, pp. 422-430.

-Lee, D. (2009), "Reliability and Safety Analysis: Report Number 11", Digital Senior Design Project.

-Linear Technology (2016), "Reliability Data Report Product Family R419".

-Min, Luo, Cai Zhaoyong, and Zhang Jin (2012), "Study on PSD system control strategy for safety", System Science, Engineering Design and Manufacturing Informatization (ICSEM), 3rd International Conference on, Vol.1, IEEE, pp. 154-159.

-NRT group (2010), "Creating New Era of Platform Screen Door System". OMRON "G5V-1: PCB Relay".

-ON Semiconductor (2016), "BD139G Reliability Data", Website: http://www.onsemi.com /Power Solutions /Reliability, 30th August.

-ROHM Semiconductor (2013), “Field Failure Rate of Diode”.

-Woo, Chun-Hee, and Jin-Sik Kim (2011), "The Development of DCU for the Platform Screen Door", The Transactions of the Korean Institute of Electrical Engineers, pp. 68-71.

-Pedicord, J. (2002), “Reliability Report for MAX485 Plastic Encapsulated Devices”, Maxim Integrated Products.

-Pintsch Bamag (2011), "Platform Screen Doors: Short Form Description".

-Rausand, M. (2004), “Preliminary Hazard Analysis”, System Reliability Theory, 2nd edition, Wiley.