

# تحلیل قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال در سیستم علائم راه آهن با استفاده از روش بلاک دیاگرام و افزونگی سخت افزاری

علیرضا تویکی، دانش آموخته کارشناسی ارشد کنترل و علائم، دانشکده راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران

محمدعلی صدیدزاده (مسئول مکاتبات)، دانشیار دانشکده راه‌آهن دانشگاه علم و صنعت ایران، تهران، ایران

Email: sandidzadeh@iust.ac.ir

پذیرش: ۱۳۹۹/۰۴/۱۱

دریافت: ۱۳۹۸/۰۲/۰۴

## چکیده

در سیستم علائم راه آهن، ایمنی سیستم به حفاظت از تلفات خطرناک و زیان‌های اقتصادی اشاره دارد. ارتباط سیستم اینترلاکینگ با تجهیزات کنار خط از قبیل سیگنال، ماشین سوزن، مدارات راه و ... از طریق سیستم کنترل‌کننده‌ی تجهیزات انجام می‌شود. از آنجاکه ارسال و دریافت دیتا از تجهیزات کنار خط از طریق این سیستم که به عنوان واسطی حیاتی بین سیستم اینترلاکینگ و تجهیزات کنار خط عمل می‌کند است؛ لذا بررسی وضعیت و صحت کارکرد هرکدام باید بصورت لحظه‌ای انجام پذیرد؛ بنابراین بررسی ایمنی و قابلیت اطمینان این سیستم تحت تمامی شرایط بسیار حائز اهمیت است. معمولاً این بردها از جمله برد کنترل‌کننده‌ی سیگنال در برابر خرابی تحمل‌پذیر ساخته می‌شوند. با توجه به اینکه محاسبات قابلیت اطمینان و ایمنی در عمل نیازمند تست‌های آزمایشگاهی و میدانی است و هزینه‌ی بسیار بالایی را شامل می‌شود بنابراین باید این کار با مدل‌سازی، شبیه‌سازی و استفاده از روش‌های عددی و تحلیلی انجام پذیرد. در این مقاله در ابتدا به معرفی سیستم OCS و سپس برد کنترل‌کننده‌ی سیگنال پرداخته می‌شود. در ادامه به معرفی قابلیت اطمینان پرداخته شده و کمیت‌های مربوط به آن معرفی می‌گردد. سپس قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال را با استفاده از بلاک دیاگرام سیستم و شبیه‌سازی با نرم افزار MATLAB بدست آورده و در ادامه با استفاده از افزونگی سخت افزاری به بررسی دقیق‌تر قابلیت اطمینان پرداخته می‌شود؛ در انتها نیز به نتیجه‌گیری و ارائه‌ی پیشنهادات در زمینه‌ی مربوطه پرداخته خواهد شد. نوآوری اصلی در این مقاله استفاده از روش بلاک دیاگرام و افزونگی ساختاری در محاسبه قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال و شبیه‌سازی با نرم افزار MATLAB است.

واژه‌های کلیدی: قابلیت اطمینان، کنترل‌کننده‌ی سیگنال، OCS950

## ۱. مقدمه

در اجرای سیستم سیگنالینگ خطوط مترو مدرن دنیا، سیستم کنترل کننده‌ی تجهیزات از جمله سیستم‌های ضروری و بسیار مهم در انتقال فرامین کنترلی از ایترلاکینگ به تجهیزات کنار خط و بالعکس می‌باشد. این سیستم با هدف اصلی انتقال دیتای کنترلی و وضعیتی تجهیزات کنار خط، از مهم ترین زیرسیستم‌های سیستم سیگنالینگ است؛ لذا اطمینان از عملکرد صحیح آن امری اجتناب ناپذیر است. سیستم سیگنالینگ مورد استفاده در برخی از خطوط مترو تهران ساخت شرکت بمباردیه بوده که در کنترل تجهیزات کنار خط از سیستم OCS950 استفاده شده است. یک مجموعه‌ی کنترلی می‌باشد که یک زیر سیستم CBI را برای کنترل و مانیتورینگ تجهیزات کنار خط سیگنالینگ فراهم می‌سازد. این سیستم بر اساس توسعه و کاربرد عمومی در راه آهن‌های مختلف استفاده شده است که به عنوان یک سیستم انطباقی شناخته شده و فرایند انطباق دستورات بین سیستم ایترلاکینگ و تجهیزات کنار خط را انجام می‌دهد.

مهمترین بخش سیستم که باعث ایجاد تردد ایمن قطار و پردازش صحیح اطلاعات دریافتی و ارسالی می‌گردد بخش نرم افزاری می‌باشد که این سیستم با توجه به اطلاعات دریافتی از سیستم ایترلاکینگ و از طریق سیستم کنترل تجهیزات کنار خط تردد ایمن قطارها در طول خط را امکان پذیر می‌سازد. سیستم OCS950 از چهار کنترل کننده‌ی تجهیزات که به عنوان واحدهای ارتباطی شناخته می‌شوند، تشکیل شده است که این واحدها از طریق قاب‌های کنترلی به منابع تغذیه‌ی موجود در کابینت OCS950 متصل می‌باشند. کنترل کننده‌های تجهیزات که در این سیستم موجود هستند می‌توانند به صورت مرکزی، متمرکز و از طریق سیستم کامپیوتری کنترل شده و یا دارای قابلیت نصب به صورت غیر متمرکز برای کنترل کردن تجهیزات کنار خط هستند. این سیستم در یک کابینت مجزا قرار می‌گیرد که در آن منبع تغذیه، کابل کشی و بردهای مخصوص برای کنترل

تجهیزات مختلف کنار خط قرار می‌گیرد. این کابینت برای نصب ۸ کنترل کننده تجهیزات و یک متمرکز کننده و یک منبع تغذیه‌ی ضروری به کار می‌رود. با توجه به تعداد تجهیزاتی که در کنار خط قرار می‌گیرند این کابینت می‌تواند برای نمایش و کنترل نواحی و تجهیزات مختلف همان ایستگاه و ایستگاه‌های مجاور مورد استفاده قرار بگیرد.

ساختار این مقاله به این صورت است که در بخش دوم به معرفی و ساختار کلی سیستم OCS950 و کنترل کننده‌ی سیگنال پرداخته شده و مدار الکتریکی مربوطه نشان داده خواهد شد. در بخش سوم با هدف ارزیابی ایمنی سیستم، قابلیت اطمینان آن مورد بررسی قرار گرفته و نتایج مربوطه ارائه خواهد شد. در بخش پایانی هم به جمع‌بندی و ارائه‌ی نتایج و پیشنهادات پرداخته خواهد شد.

## ۲. معرفی و مدل سازی سیستم مورد مطالعه

سیستم مورد مطالعه سیستم کنترل کننده‌ی تجهیزات کنار خط OCS950 و مورد استفاده در خطوط ۱،۲،۷ مترو تهران است که از این سیستم برد کنترل کننده‌ی سیگنال به طور خاص مورد بررسی قرار می‌گیرد.

این سیستم یک قسمت داخلی از پردازنده‌های سیستم EBILOCK مبتنی بر سیستم ایترلاکینگ برای بهبود کیفیت سیستم سیگنالینگ مورد استفاده در راه آهن می‌باشد که حالات گوناگون تجهیزات کنار خط را با ویژگی‌های خراب ایمن و غیر خراب ایمن کنترل کرده و نمایش می‌دهد. سیستم ایترلاکینگ مرکزی (CIS) که منطق ایترلاکینگ را کنترل می‌کند، در یک کامپیوتر مرکزی قرار داده شده است که به دلیل افزایش دسترس پذیری کامپیوتر مرکزی با افزودنی آماده بکار در نوع میکروپروسسوری فراهم می‌شود که تجهیزات کنار خط برای تبادل اطلاعات با تعدادی حلقه یا لوپ به کامپیوتر مرکزی متصل می‌شوند. هر لوپ به عنوان یک خط انتقال در نظر گرفته می‌شود که می‌تواند ۱۵ متمرکز کننده را دربرگیرد. حلقه‌ی متمرکز کننده فصلنامه مهندسی حمل و نقل / سال چهاردهم / شماره سوم (۵۶) / بهار ۱۴۰۲

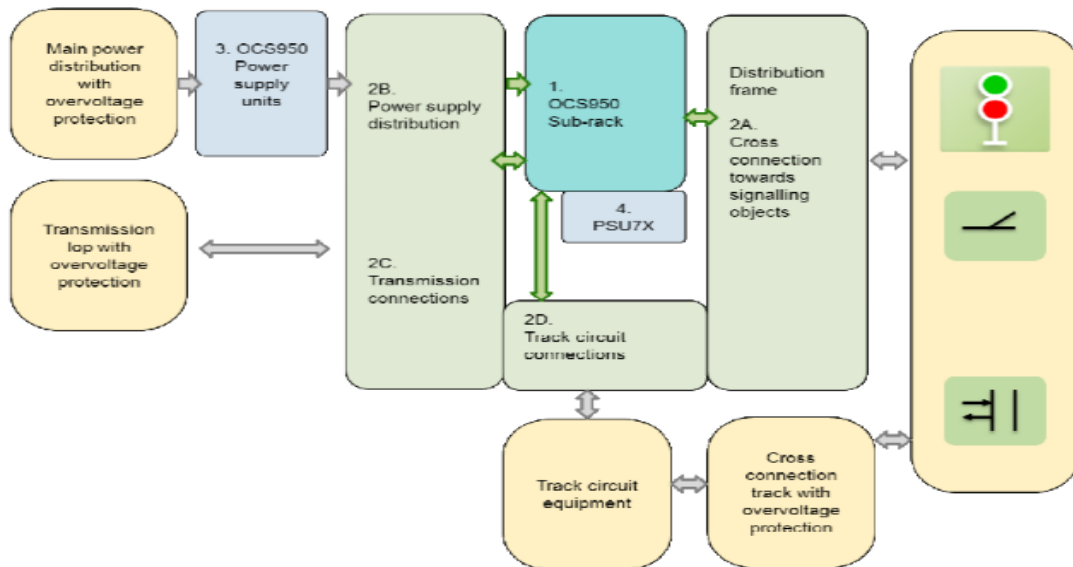
- دسترس پذیری بالا
  - قابلیت انتقال اطلاعات بالا
  - زمان پاسخ‌دهی کوتاه
  - قابلیت پیشرفته تشخیص خرابی
  - ارتباط با ورودی خروجی‌های حیاتی و غیرحیاتی
  - راحتی و سرعت تغییرات و رابط جدید تجهیزات کنار خط
  - مهندسی سایت ساده شده
  - ساینز فیزیکی اصلاح شده
  - طراحی ماژولار برای نصب و تعمیرپذیری راحت
  - کاهش هزینه‌های تامین تجهیزات و نصب و راه اندازی
- تجهیزات اساسی سیستم شامل حلقه‌ی متمرکز کننده، متمرکزکننده، لینک کنترل کنترل کننده، کنترل کننده‌ی تجهیزات و کابل تجهیزات می‌باشد. پورت حلقه که بخش باز CIS بوده و به کامپیوتر مرکزی متصل می‌باشد که با تغییر فریم اطلاعات مانند تنظیم پیام‌ها و تمامی متمرکزکننده‌ها در یک حلقه‌ی خاص سروکار دارد. این پورت هم چنین به ماژول‌های ورودی/خروجی وابسته می‌باشد.
- اشیاء کنار خط توسط تعدادی حلقه به کامپیوتر مرکزی متصل می‌شوند. هر حلقه یک خط انتقال است که می‌تواند ۱۵ متمرکزکننده را پوشش دهد. هر حلقه قابلیت انتقال رادر دو خط فراهم می‌سازد تا قابلیت دسترس‌پذیری حتی با قطع یک کابل حفظ شود. لازم به ذکر است که این خطوط به این دلیل به صورت حلقه در می‌آیند که در صورت قطع شدن کابل بتوان از طرف دیگر ارتباط را برقرار کرد. شکل ۳ نحوه‌ی ارتباط سیستم ایترلاکینگ مرکزی با تجهیزات کنار خط را نشان می‌دهد. [Hagelin,2018], [Johansson,2016]

قابلیت برقراری ارتباط دوجتهه با خط را برای اطمینان از اینکه در صورت خرابی یکی از کابل‌ها دیگری عمل نماید، برقرار می‌کند. هر متمرکز کننده به ۸ کنترلر تجهیز متصل می‌شود که هر کنترل کننده‌ی تجهیز در حالت روشن یک یا تعداد بیشتری از تجهیزات کنار خط را با استفاده از میکروپروسورهای برنامه ریزی شده خاص کنترل می‌نماید. شکل ۱ سیستم OCS950 را نشان می‌دهد [Murphy,2018]:

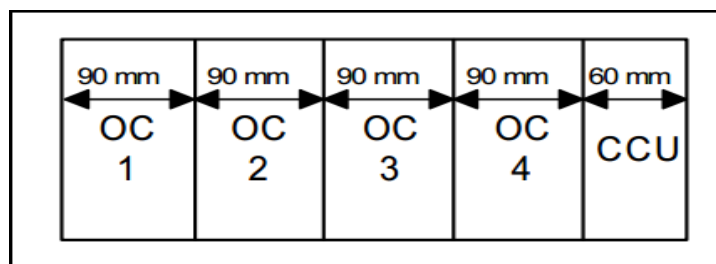
معماری توزیعی این سیستم به گونه‌ای است که اجازه می‌دهد OCها یا در نزدیکی اتاقی که کامپیوتر مرکزی در آن واقع شده قرار بگیرند و یا اینکه در فاصله‌ی نزدیک به تجهیزات کنار خط واقع شوند. در صورتی که OCها در فاصله‌ی نزدیک به تجهیزات کنار خط واقع شوند میزان کابل چند رشته سیگنالینگ به طور محسوسی کاهش خواهد یافت. با توجه به پیچیدگی سایت، هر OC می‌تواند برای کنترل و نمایش بخشی از نواحی ایستگاه، یک ایستگاه کامل و یا بیش از یک ایستگاه مورد استفاده قرار بگیرد.

برای پیاده سازی این سیستم در اتاق فنی ایستگاه‌ها از یک رک یا کابینت مخصوص استفاده می‌شود که تمامی تجهیزات سیستم اعم از کلیه‌ی بردها و منابع تغذیه و فیوزها و غیره در این کابینت پیاده‌سازی و نصب می‌شوند. رک یا کابینتی که در آن سیستم OCS950 پیاده سازی می‌شود به چهار قسمت برای نصب کنترل کننده‌های تجهیزات (OC) و یک قسمت برای نصب واحد کنترل کننده‌ی ارتباطات (CCU) تقسیم می‌شود. ضخامت و عرض هر یک از OCها برابر ۹۰ میلیمتر بوده و عرض برد CCU برابر ۶۰ میلیمتر می‌باشد. شکل ۲ وضعیت پیاده‌سازی OCها و CCU را نشان می‌دهد [Hagelin,2018], [Johansson,2016]:

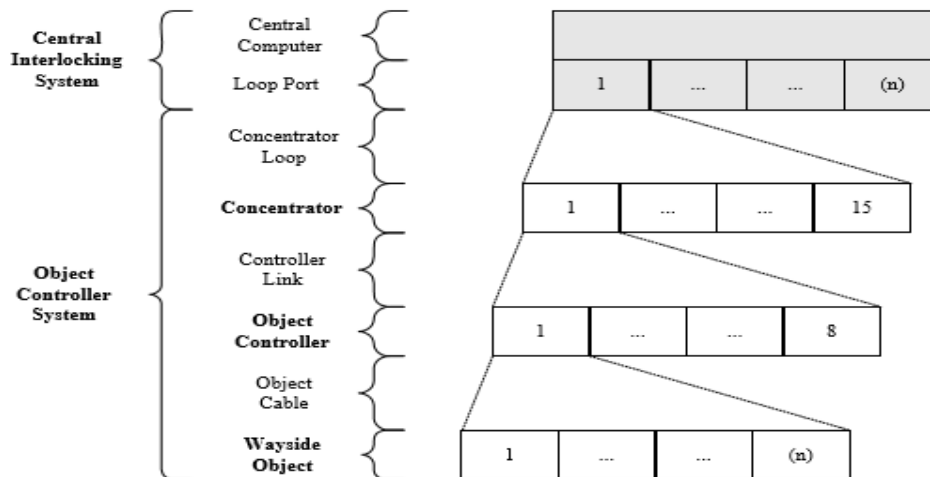
سیستم OCS950 دارای ویژگی‌ها و مزایایی بوده که به صورت زیر است:



شکل ۱. ساختار سیستم OCS950



شکل ۲. وضعیت قرارگیری OCها و CCU



شکل ۳. نحوه‌ی ارتباط اینترلاکینگ با تجهیزات کنار خط

- مرتب کردن قطعات و تجهیزات OC
- بررسی ملاحظات مربوط به تطابق الکترومغناطیسی EMC
- ملاحظات ویژه برای حفاظت روشنایی
- فاصله تا تجهیزات کنار خط

- برای نصب تجهیزات سیستم OCS950 لازم است که قبل از نصب موارد زیر مورد توجه مهندسین سایت قرار گیرند:
- بررسی نیازها و الزامات مربوط به تغییرات ولتاژ و فرکانس منبع تغذیه

برد روشنایی سیستم ایترلاکینگ یا رله، نمای سیگنال را مشخص می‌کنند. واحد روشنایی سیگنال از یک ترانسفورماتور و یک رله‌ی تغییر فیلامان تشکیل شده است که ترانسفورماتور وظیفه‌ی تبدیل ولتاژ ۲۲۰ ولت به ۱۲ ولت را دارد. رله‌ی تغییر فیلامان برای نظارت بر عملکرد فیلامان اصلی مورد استفاده قرار گرفته است؛ اگر فیلامان اصلی سیگنال خراب شود، رله‌ی تغییر فیلامان در سیستم روشنایی از فیلامان دوم استفاده می‌کند تا عملکرد سیگنال با اختلال مواجه نشود. این کار در حالی انجام می‌شود که این رله به طور همزمان مدار هشدار خرابی را در برد کنترل کننده‌ی سیگنال فعال می‌کند. سیگنال‌های حبایی دارای دو نوع تک فیلامان و دو فیلامان می‌باشند که سیگنال دارای دو فیلامان دارای ایمنی و کارایی بهتری نسبت به سیگنال تک فیلامان می‌باشد [Hagelin,2018].

## ۲-۲ برد کنترل‌کننده‌ی سیگنال

این برد وظیفه‌ی ارسال اطلاعات دریافتی از CCU به سیگنال‌ها و وضعیت سیگنال‌ها به ایترلاکینگ را دارد. لامپ در سیگنال‌ها به یک ترانسفورماتور متصل می‌شود که ترانسفورماتور نیز به کنترل‌کننده‌ی سیگنال متصل است. لامپ‌های حرکت و توقف به خروجی‌های برد متصل می‌شوند که حداکثر می‌توانند دو حالت توقف و چهار حالت حرکت را کنترل نمایند. در صورتی که تعداد نماهای چراغ سیگنال‌ها از مقدار اشاره شده بیشتر باشد، باید از دو برد کنترل کننده‌ی سیگنال جهت کنترل نمای سیگنال‌ها استفاده نماییم. لامپ‌های توقف با نمای قرمز در خروجی به صورتی برنامه‌ریزی شده‌اند که در صورتی که کنترل کننده‌ی تجهیزات خارج از کنترل باشد، به صورت خودکار در حالت روشن قرار بگیرند؛ این در حالی است که نماهای سبز و زرد که مربوط به حرکت قطار می‌باشند به گونه‌ای برنامه‌ریزی شده‌اند که در صورت خارج از کنترل بودن سیستم OCS به صورت خودکار در حالت خاموش قرار بگیرند. به دلیل افزایش سطح ایمنی و بالابردن دقت سیستم سیم برگشتی مربوط به نماهای

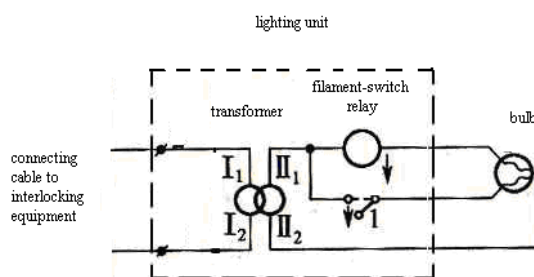
مورد آخر به این دلیل با اهمیت است که در اکثر سیستم‌های سیگنالینگ معتبر دنیا، حداکثر فاصله‌ی تجهیز کنار خط از سیستم کنترل کننده در حدود ۲ کیلومتر می‌باشد که این فاصله به دلیل جلوگیری از افت ولتاژ و یا جریان نشتی در نظر گرفته می‌شود. تغییرات فرکانس و ولتاژ منبع تغذیه در دقت اندازه‌گیری جریان سوزن و چراغ سیگنال موثر خواهد بود. بنابراین باید الزامات زیر برای منبع ولتاژ حتما در نظر گرفته شوند [Johansson,2016]:

(الف) ولتاژ ورودی به واحد منبع تغذیه نباید بیشتر از  $\pm 10\%$  درصد تلورانس داشته باشد.

(ب) تلورانس فرکانس ولتاژ نباید خیلی بیشتر از  $\pm 2\%$  درصد باشد.

## ۱-۲ ساختار سیگنال

ساختار سیگنال‌های مورد استفاده در مترو تهران از نوع ماژولار با مواد آلیاژ آلومینیوم می‌باشد. در این مکانیزم حباب چراغ سیگنال می‌تواند در بسیاری از جهات منطبق شود. فاصله‌ی بین دو لنز قابل تنظیم بوده که امکان تحقق بخشیدن به نور کاملا موازی را ایجاد می‌کند. پوشش پشت چراغ سیگنال ضد گرد و غبار بوده که دارای یک حفاظت خوب در برابر گرد و غبار و نفوذ آب می‌باشد. باز و بسته شدن درب سیگنال‌ها از طریق اپراتورهای تعمیر و نگه‌داری سیگنالینگ می‌باشد. معمولاً در خطوط مترو از سیگنال‌های کوتاه که در دیواره‌ی تونل نصب می‌شوند استفاده می‌شود. شکل ۴ مدار و واحد روشنایی سیگنال را نشان می‌دهد [Johansson,2016]:



شکل ۴. مدار واحد روشنایی سیگنال

احتمال با یک عدد بیان می‌شود که همان شاخص ارزیابی قابلیت اطمینان است. در سه بخش دیگر که تماماً جزء پارامترهای مهندسی هستند، تئوری احتمال هیچ‌گونه کمکی نمی‌کند. آهنگ از کارافتادگی وابستگی زیادی به شرایط کار و هم‌چنین سطح یا میزان تنش‌ها دارد [Flammini, et al,2005].

بدیهی است که قابلیت اطمینان به عبارتی مبین تداوم عملکرد سیستم بدون وقوع از کار افتادن است و لذا قابلیت اطمینان عبارت خواهد بود از احتمال باقی ماندن سیستم و یا یکی از تجهیزات سیستم در شرایط عملکرد بدون وقوع از کار افتادگی. برای سیستم کنترل کننده‌ی برد سیگنال از کارافتادگی تجهیزات مانند رله‌ها، مقاومت‌ها و ... قابل پذیرش است که در این حالت از مفهوم دیگری به نام دسترس پذیری استفاده می‌شود که عبارت است از:

احتمال عملکرد صحیح سیستم و در دسترس بودن آن در لحظه‌ی  $t$ . سیستمی که تازه از مدار خارج شده باشد دسترس پذیری صددرد دارد.

این دو مفهوم نشان می‌دهد که نمی‌توان صرفاً یک مقیاس فراگیر برای بیان کیفیت عملکرد به کار برد. در این صورت شاخص‌های دیگری نیز علاوه بر این دو مطرح است که هر یک جایگاه کاربردی خاص خود را دارد که از توضیحات اضافه در این مورد صرف نظر می‌شود [Morant, 2016].

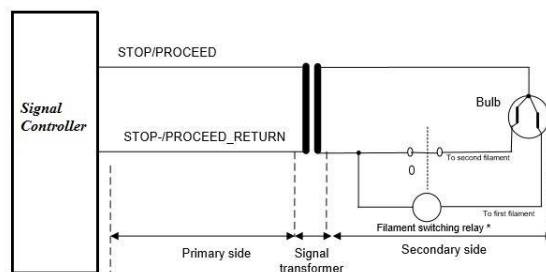
### ۲-۳ شاخص‌های قابلیت اطمینان

در محاسبه‌ی قابلیت اطمینان سیستم از شاخص‌های نرخ خرابی، میانگین زمان تا خرابی، میانگین زمان تا تعمیرات، زمان متوسط بین خرابی‌ها استفاده می‌شود که در ادامه به معرفی هر یک پرداخته شده و با استفاده از آن‌ها قابلیت اطمینان برد کنترل کننده‌ی سیگنال را بدست خواهیم آورد [Flammini, et al,2005].

#### ۱-۲-۳ نرخ خرابی $\lambda$

نرخ خرابی تابعی از زمان است. به تعداد خرابی که مورد انتظار است که در زمان مشخصی رخ دهد نرخ خرابی گفته می‌شود،

توقف و حرکت را نمی‌توان به یکدیگر متصل نمود. نحوه‌ی اتصال لامپ به برد کنترل کننده به صورت شکل ۵ خواهد بود:



شکل ۵. ارتباط برد کنترلی با سیگنال

همانطور که از شکل پیداست برای چراغ سیگنال یک رله‌ی تغییر فیلامان قرار داده می‌شود که در صورتی که انرژی دار باشد لامپ روشن شده و در غیر این صورت چراغ سیگنال روشن نخواهد شد. لازم به ذکر است که دو برد کنترل کننده‌ی سیگنال را نمی‌توان با یک سیم به شبکه متصل کرد زیرا در این صورت جریان‌های برگشتی در عملکرد بردها تاثیرگذار خواهند بود.

لامپ‌های چراغ سیگنال‌ها می‌توانند در سه حالت روشن، خاموش و یا چشمک‌زن قرار بگیرند. سیگنال تک نما که DWELL نامیده می‌شوند به دلیل تک فیلامانه بودن دارای رله‌ی تغییر فیلامان نیست.

کابل‌های تجهیزات بین کنترل کننده‌ی تجهیزات و تجهیزات نصب شده در کنار خط باید از آسیب‌های فیزیکی محفوظ باشند. به منظور بالاتر بردن سطح ایمنی سیستم کنترل کننده‌ی تجهیز از تشخیص‌گر خرابی اتصال به زمین استفاده می‌کنند [Johansson,2016].

### ۳. محاسبه و بررسی قابلیت اطمینان برد

#### کنترل کننده‌ی سیگنال

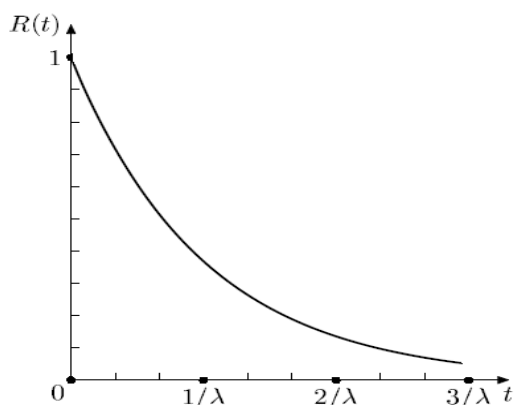
##### ۱-۳ تعریف قابلیت اطمینان

عبارت است از احتمال عملکرد رضایت بخش آن سیستم تحت شرایط کار مشخص که برای مدت زمان معینی در نظر گرفته می‌شود. تعریف فوق شامل چهار بخش اصلی احتمال، عملکرد رضایت‌بخش، زمان و شرایط کار معین است.

به دلیل اینکه در زمان عمر مفید سیستم نرخ خرابی مقداری ثابت می‌باشد می‌توان گفت که قابلیت اطمینان سیستم به صورت نمایی تغییر خواهد کرد که رابطه‌ی آن در زیر نشان داده شده است:

$$R(t) = e^{-\lambda t} \quad (2)$$

حال با توجه به رابطه‌ی بالا در زمان عمر مفید سیستم نمودار قابلیت اطمینان به صورت زیر بدست خواهد آمد:



شکل ۷. قابلیت اطمینان سیستم در زمان عمر مفید

### ۲-۲-۳ زمان متوسط تا وقوع خرابی (MTTF)

به زمان مورد انتظار تا وقوع اولین خرابی سیستم زمان متوسط تا وقوع خرابی گفته می‌شود که دارای رابطه‌ی زیر است:

$$MTTF = \frac{1}{\lambda} \quad (3)$$

$\lambda$  نرخ خرابی سیستم است. هرچه نرخ خرابی کمتر باشد، مدت زمان تا وقوع اولین خرابی بیشتر است. می‌توان گفت که در حالت کلی، MTTF برای سیستم‌هایی که تا زمان وقوع اولین خرابی تعمیر نمی‌شوند، استفاده می‌شود [Bardos,1989].

### ۳-۲-۳ زمان متوسط وقوع تعمیرات (MTTR)

در یک سیستم به میانگین مدت زمان مورد نیاز برای تعمیر زمان متوسط تا تعمیرات گفته می‌شود.

MTTR بر حسب نرخ تعمیرات بیان می‌شود که  $\mu$  تعداد تعمیرات مورد انتظار در واحد زمان است. هرچه MTTR کمتری مورد نیاز باشد، هزینه بهره‌برداری سیستم بالاتر می‌رود [Bardos,1989].

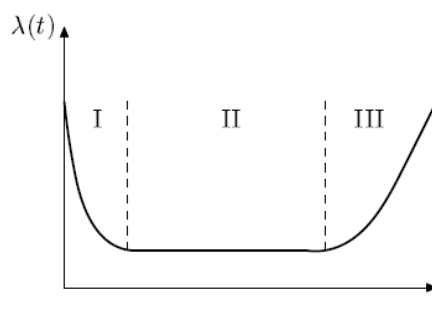
مثلاً اگر یک میکروکنترلر Atmega32 به طور میانگین در هر ۱۰۰۰۰ ساعت یک بار خراب شود، نرخ خرابی آن  $1/10000$  خواهد بود.

معمولاً در سطوح عملیاتی اطلاعات نرخ خرابی در سطح اجزا و قطعات سیستم موجود است، این در حالی است که شرکت‌های سازنده نرخ خرابی کل سیستم را در اختیار مصرف‌کننده قرار نمی‌دهند.

در مواردی که نرخ خرابی اجزاء مانند برد کنترل‌کننده‌ی سیگنال در دسترس باشد، یک تخمین کاربردی از نرخ خرابی سیستم بدون افزونگی، با استفاده از تجمیع نرخ‌های خرابی هر یک از اجزاء ( $\lambda_i$ ) به دست می‌آید [Power,2009]:

$$\lambda = \sum_{i=1}^n \lambda_i \quad (1)$$

برای سخت‌افزار، از یک چرخه‌ی عمر برای نمایش طول عمر سیستم استفاده می‌شود که شامل دوره‌های طراحی و ساخت اولیه (I)، طول عمر مفید (II) و دوره فرسودگی (III) که اصطلاحاً دوره‌ی پیری سیستم نامیده می‌شود، است. چرخه‌ی حیات سیستم را به صورت نمودار U شکل نشان می‌دهند که در زیر به آن اشاره شده است. مطابق با این نمودار، به دلیل خرابی‌های محتمل در قطعات ضعیف سیستم که نقوص آن را سازنده در طول آزمایش پیدا نکرده است، با گذشت زمان نرخ خرابی کاهش پیدا خواهد کرد. سپس بعد از یک مدت زمان مشخص تثبیت می‌شود و بعد از آن در هنگامی که تجهیزات الکترونیکی برد به پایان طول عمر خود نزدیک شوند، نرخ خرابی افزایش خواهد یافت [Bardos,1989].



شکل ۶. نمودار U شکل چرخه‌ی حیات سیستم

### ۲-۴-۳ زمان متوسط بین خرابی‌ها (MTBF)

به زمان متوسط زمان بین وقوع خرابی‌ها MTBF گفته می‌شود. اگر فرض کنیم هر تعمیر، سیستم را کاملاً بی‌عیب و نقص کند، در این صورت رابطه بین MTTF و MTBF به صورت زیر خواهد بود [Bardos,1989]:

$$MTBF = MTTF + MTTR \quad (۴)$$

### ۳-۳-۳ بلاک دیاگرام برد کنترل‌کننده‌ی سیگنال

مدل‌های ترکیبی قابلیت اطمینان شامل بلاک‌های دیاگرام قابلیت اطمینان، درخت‌های خطا، درخت‌های موفقیت می‌شود. در این فصل برای قابلیت اطمینان از بلاک دیاگرام استفاده خواهیم کرد. بلاک دیاگرام قابلیت اطمینان یک طرح مختصر و مفید از سیستم ارائه می‌دهد. اجزاء به شکل بلاک‌ها نمایش داده می‌شوند که اتصالات بین بلاک‌ها وابستگی عملی بین اجزاء را نشان می‌دهد. اگر برای کارکرد سیستم همه آن‌ها ضروری باشند، بلوک‌ها به صورت سری متصل می‌شوند. بلوک‌ها به صورت موازی متصل می‌شوند اگر تنها یکی از آن‌ها برای عملکرد صحیح سیستم کافی باشد. در برد کنترل‌کننده‌ی سیگنال برای کارکرد صحیح تمام برد لازم است که تمامی بلاک‌ها به صورت صحیح کار کنند در نتیجه بلاک دیاگرام مربوط به برد کنترل‌کننده‌ی سیگنال طراحی شده از نوع سری است.

بلاک‌های دیاگرام قابلیت اطمینان به دلیل درک ساده‌تر و هم‌چنین راحت بودن مدل کردن سیستم‌های دارای افزونگی مدل بسیار رایجی است؛ این در حالی است که بلاک‌های دیاگرام قابلیت اطمینان همانند دیگر مدل‌های ترکیبی قابلیت اعتماد، محدودیت‌هایی جدی دارند.

اولاً در بلاک‌های دیاگرام قابلیت اطمینان فرض می‌شود که اجزای سیستم به دو حالت معیوب و سالم محدود هستند و هم‌چنین در آن‌ها ساختار سیستم در طول کارکرد سیستم تغییر نمی‌کند، ثانیاً خرابی هر یک از اجزاء به صورت مستقل فرض می‌شود. بنابراین حالتی که در آن توالی از خرابی‌های اجزاء،

قابلیت اطمینان سیستم را تحت تاثیر قرار می‌دهد، به صورت مناسب نشان داده نخواهد شد [Bardos,1989]. با توجه به اینکه برد کنترل‌کننده‌ی سیگنال می‌تواند حداکثر ۶ نمای خروجی را کنترل نماید که ۲ خروجی آن حتماً مربوط به حالت توقف و نمای قرمز رنگ است، لذا در طراحی این برد از ۶ بلاک مشابه استفاده شده است. هر کدام از این بلاک‌ها مربوط به یک خروجی بوده و وظیفه‌ی ارسال و دریافت دیتا به نمای سیگنال و بلعکس را بر عهده دارند. هر بلاک از یک پردازنده‌ی اصلی که مدل Atmega32 است به همراه اطمینان مربوطه مجموع این مقاومت و خازن‌ها به عنوان تجهیزات الکترونیکی در نظر گرفته شده است.

تجهیزات مورد استفاده در هر بلاک با یکدیگر به صورت سری قرار دارند به طوری که در صورتی که یکی از تجهیزات نامبرده در هر بلاک از کار افتاده و یا معیوب شوند در عملکرد آن بلاک تاثیر گذاشته و آن بلاک معیوب خواهد شد. حال با توجه به اینکه ورودی برد کنترل‌کننده‌ی سیگنال برق ۲۲۰ ولت AC بوده و تجهیزات و قطعات الکترونیکی مربوطه حداکثر با برق ۲۴ ولت DC تغذیه می‌شوند از یک مبدل AC/DC که قابلیت تبدیل ۲۲۰ ولت AC به ۲۴ ولت DC را دارا باشد استفاده شده است. خروجی برد کنترل‌کننده‌ی سیگنال برعکس ورودی آن بوده و باید ۲۲۰ ولت AC را به دو سر ترانس فورماتور موجود در چراغ سیگنال که قبل از هر نمای سیگنال و در داخل درب چراغ سیگنال نصب می‌شود ارسال نماید. به همین منظور و برای دسترسی به مقدار ولتاژ نامبرده شده از یک مبدل DC/AC که بلعکس مبدل ورودی می‌باشد استفاده شده است.

حال با توجه به اینکه مبدل‌های AC/DC، DC/AC و بلاک‌های معرفی شده با یکدیگر سری هستند عملکرد هر یک بر عملکرد تمام برد تاثیر گذاشته و بروز خرابی در هر یک باعث ایجاد اختلال در عملکرد نهایی برد کنترل‌کننده‌ی سیگنال خواهد شد. حال برای بررسی قابلیت اطمینان مربوطه در ابتدا مقدار قابلیت اطمینان یکی از بلاک‌های مشابه را بدست آورده و سپس



## تحلیل قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال در سیستم علائم راه آهن با استفاده از روش بلاک دیاگرام و افزونگی سخت افزاری

برای تجهیزات الکترونیکی به کار رفته فرض شده که متوسط زمان رسیدن به خرابی ۶۳۰۰۰۰ ساعت باشد با این وجود داریم [Power,2009]:

$$MTTF = Year * Days * Hour = 630000$$

$$\lambda_{Electronic-Equipment} = \frac{1}{MTTF} = \frac{1}{630000} = 1.58 * 10^{-6} \quad (V)$$

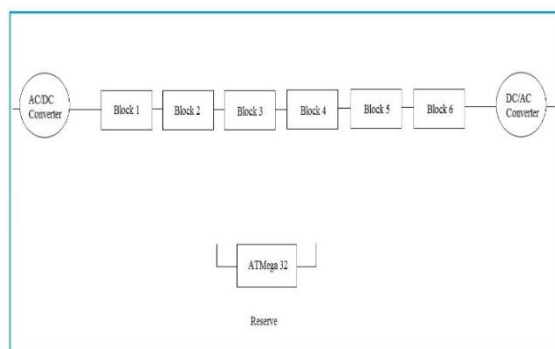
$$R_{Electronic-Equipment} = e^{-\lambda t} = e^{-(1.58 * 10^{-6})t}$$

با توجه به اینکه تجهیزات هر بلاک بایکدیگر به صورت سری هستند قابلیت اطمینان هر بلاک به صورت زیر محاسبه می‌گردد:

$$R_{Block} = R_{ATmega32} * R_{Coil} * R_{Electronic-Equipment} = \quad (A)$$

$$e^{-1.9 * 10^{-6}t} * e^{-1.88 * 10^{-6}t} * e^{-1.58 * 10^{-6}t} = e^{-5.36 * 10^{-6}t}$$

در محاسبه‌ی قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال از روش بلاک دیاگرام استفاده می‌شود. در ساختار واقعی برد کنترل‌کننده‌ی سیگنال علاوه بر ۶ پردازنده‌ی Atmega32 از یک پردازنده‌ی Atmega32 به عنوان پردازنده‌ی آماده به کار استفاده می‌شود. عملکرد این پردازنده به گونه‌ای است که در صورتی که هر یک از ۶ پردازنده‌ی دیگر به هر دلیلی دچار خرابی شده و معیوب گردد، این پردازنده جایگزین آن شده و وارد مدار می‌گردد تا عملکرد برد با معیوب شدن یک پردازنده دچار اختلال نشود. این چیدمان تجهیزات در برد باعث بالا رفتن ایمنی برد می‌شود. شکل زیر بلاک دیاگرام برد کنترل‌کننده‌ی سیگنال را که در آن از یک پردازنده‌ی آماده به کار نیز استفاده شده است نشان می‌دهد:



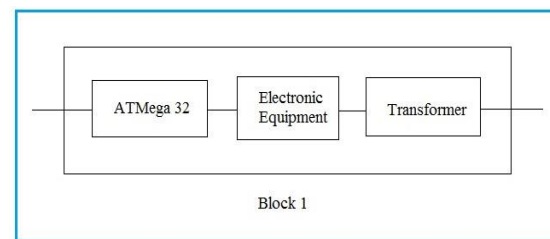
شکل ۹. بلاک دیاگرام برد کنترل‌کننده‌ی سیگنال با استفاده از

پردازنده‌ی آماده به کار

مقدار بدست آمده را برای ۵ بلاک دیگر تعمیم خواهیم داد. لازم به ذکر است در محاسبه‌ی قابلیت اطمینان سعی شده از مقادیر واقعی و فرضی مربوط به نرخ خرابی تجهیزات نامبرده شده استفاده شود زیرا برخی از تجهیزات دارای نرخ خرابی مشخص و برخی دیگر دارای نرخ خرابی نامشخص هستند. با این تفاسیر خواهیم داشت:

### ۳-۱-۳ قابلیت اطمینان هر بلاک

هر بلاک از یک پردازنده‌ی مرکزی به همراه سیم پیچ القایی و تجهیزات و قطعات الکترونیکی تشکیل شده که با یکدیگر به صورت سری کار می‌کنند. شکل زیر بلاک و تجهیزات مورد نظر را نشان می‌دهد:



شکل ۸. بلاک مربوط به خروجی سیگنال

از آنجا که متوسط خرابی هر پردازنده‌ی Atmega32 در دمای ۲۵ درجه‌ی سانتی‌گراد ۱۰۰ سال و در دمای ۸۵ درجه‌ی سانتی‌گراد ۲۰ سال است در اینجا فرض شده که به طور متوسط میزان خرابی هر Atmega32 در دمای ۷۰ درجه‌ی سانتی‌گراد ۶۰ سال باشد با این تفاسیر برای محاسبه‌ی نرخ خرابی خواهیم داشت [Power,2009]:

$$MTTF = Year * Days * Hour = 60 * 365 * 24 = 525600$$

$$\lambda_{ATmega32} = \frac{1}{MTTF} = \frac{1}{525600} = 1.9 * 10^{-6} \quad (5)$$

$$R_{ATmega32} = e^{-\lambda t} = e^{-(1.9 * 10^{-6})t}$$

برای سیم پیچ‌های به کار رفته در هر بلاک فرض می‌شود که متوسط زمان رسیدن به خرابی ۵۳۰۰۰۰ ساعت باشد با این وجود نرخ خرابی به صورت زیر بدست خواهد آمد [Power,2009]:

$$MTTF = Year * Days * Hour = 530000$$

$$\lambda_{Coil} = \frac{1}{MTTF} = \frac{1}{530000} = 1.88 * 10^{-6} \quad (6)$$

$$R_{Coil} = e^{-\lambda t} = e^{-(1.88 * 10^{-6})t}$$

زمان متوسط رسیدن به خرابی در مبدل‌های تغذیه‌ی DC/AC برابر ۲۰۰۰۰۰ ساعت است. با توجه به این مقدار برای محاسبه‌ی نرخ خرابی و قابلیت اطمینان مربوطه داریم [Bardos,1989]:

$$MTTF = Year * Day * Hour = 200000$$

$$\lambda_{DC/AC} = \frac{1}{MTTF} = \frac{1}{200000} = 5 * 10^{-6} \quad (13)$$

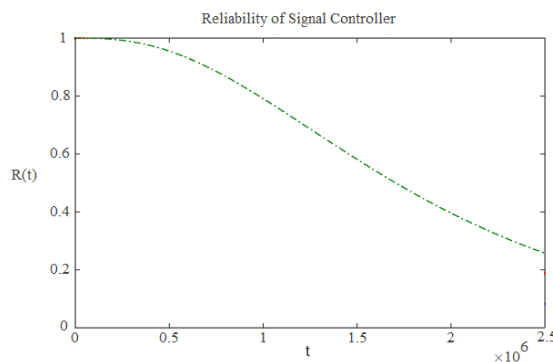
$$R_{DC/AC} = e^{-\lambda t} = e^{-(5*10^{-6})t}$$

با توجه به شکل ۹ مشاهده می‌شود که تجهیزات موجود در این برد به صورت سری با یکدیگر کار می‌کنند زیرا عدم عملکرد صحیح هر یک در کارایی تمام برد اختلال ایجاد خواهد کرد. با این وجود قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال و نمودار نمایی مربوطه به صورت زیر بدست است:

$$R_{Signal-Controller} = R_{Block} * R_{AC/DC} * R_{DC/AC} \quad (14)$$

$$= \left(\frac{7}{6} (e^{-(5.36*10^{-6})t})^6 - \frac{1}{6} (e^{-(5.36*10^{-6})t})^7\right) * (e^{-10^{-5}t}) * (e^{-5*10^{-6}t})$$

با توجه به رابطه‌ی بدست آمده نمودار قابلیت اطمینان مربوط به برد کنترل‌کننده‌ی سیگنال به صورت زیر نشان داده شده است:



شکل ۱۰. نمودار قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال

همانطور که از نمودار فوق پیداست با توجه به اینکه در ساختار برد کنترل‌کننده‌ی سیگنال از یک پردازنده‌ی آماده به کار استفاده شده تا در موارد ضروری عملکرد برد با اختلال مواجه نشود؛ قابلیت اطمینان برد مقدار یک بوده که با گذشت زمان بسیار زیادی به تدریج و با توجه به طول عمر قطعات الکترونیکی کاهش یافته و به مقدار مشخصی خواهد رسید.

با توجه به اینکه بلاک‌های اشاره شده با یکدیگر به صورت سری در ارتباط هستند لذا در صورتی که عضو آماده به کار در نظر گرفته نشود، قابلیت اطمینان ۶ بلاک به صورت زیر بدست می‌آید:

$$R_{Block} = R_{Block 1} * R_{Block 2} * R_{Block 3} * R_{Block 4} * R_{Block 5} * R_{Block 6} =$$

$$e^{-5.36*10^{-6}t} * e^{-5.36*10^{-6}t} * e^{-5.36*10^{-6}t} * e^{-5.36*10^{-6}t} * e^{-5.36*10^{-6}t} * e^{-5.36*10^{-6}t}$$

$$= e^{-32.16*10^{-6}t}$$

عدم قابلیت اطمینان سیستم را با Q نشان می‌دهند که نمایانگر عدم کارکرد سیستم با وجود خرابی است. عدم قابلیت اطمینان با قابلیت اطمینان رابطه‌ی مستقیمی داشته که عبارت است از:

$$Q_{system} = 1 - R_{system} \quad (10)$$

همانطور که از شکل بالا پیداست پردازنده‌ی Atmega32 به عنوان عضو آماده به کار و رزرو در نظر گرفته شده است در صورت خرابی آماده‌ی جایگزینی با هر یک از پردازنده‌های موجود در ۶ بلاک را دارد. به همین منظور برای بدست آوردن قابلیت اطمینان مربوط به بلاک‌ها با توجه به وجود این عضو آماده به کار خواهیم داشت:

$$R_{Blocks} = R_{Block}^6 + \frac{1}{6} Q_{Block} * R_{Block}^5 = R_{Block}^6 + \frac{1}{6} (1 - R_{Block}) R_{Block}^5 \quad (11)$$

$$= \frac{7}{6} R_{Block}^6 - \frac{1}{6} R_{Block}^7 = \frac{7}{6} (e^{-(5.36*10^{-6})t})^6 - \frac{1}{6} (e^{-(5.36*10^{-6})t})^7$$

حال با توجه به مقادیر بدست آمده مقادیر قابلیت اطمینان را برای مبدل‌های مورد استفاده بدست می‌آوریم؛

زمان متوسط رسیدن به خرابی در مبدل‌های تغذیه AC/DC برابر ۱۰۰۰۰۰ ساعت است. با این وجود در محاسبه‌ی قابلیت

اطمینان مربوطه خواهیم داشت [Bardos,1989]:

$$MTTF = Year * Day * Hour = 100000$$

$$\lambda_{AC/DC} = \frac{1}{MTTF} = \frac{1}{100000} = 10^{-5} \quad (12)$$

$$R_{AC/DC} = e^{-\lambda t} = e^{-10^{-5}t}$$

### ۳-۴ مکانیزم تشخیص پردازنده خراب از سالم

راه حل تشخیص پردازنده خراب از سالم در نوع نمای سیگنال خروجی و زمان روشن-خاموش شدن نماهای چراغ سیگنال در حالت دریافت دستورات از ایترلاکینگ است. زمانی که اپراتور مرکز فرمان مسیریابی ناحیه سوزن را انجام می‌دهد دستور مسیریابی بلافاصله از ایترلاکینگ به OBC انتقال یافته و سپس نرمال یا ریورس شدن سوزن انجام می‌شود. همزمان با تغییر وضعیت سوزن، نمای سیگنال‌های موجود در ناحیه سوزن تغییر می‌کند. در صورتیکه سوزن تغییر وضعیت داده و نمای چراغ سیگنال ثابت بماند مشکل از پردازنده‌ی برد و خروجی سیگنال مربوطه است که باید اپراتور تعمیر و نگهداری به سرعت وارد عمل شده و پردازنده خراب را با استفاده از پین‌کش از داخل برد معیوب برداشته و پردازنده سالم را جایگزین نماید. البته ساختار برد به گونه‌ای است که عملکرد برد با پردازنده ثانویه انجام می‌شود تا اپراتور پردازنده معیوب را با پردازنده سالم یدکی جایگزین کرده و سپس از پردازنده معیوب رفع عیب نماید.

### ۳-۵ تئوری شرایط ایمن

طبق تعریف یک سیستم ایمن است اگر تحت تمامی شرایط کاری خود، شرایط خطرآفرین که منجر به حادثه گردد را نداشته باشد. این شرایط کاری شامل سلامت کامل سیستم، عیب جزئی یا عیب کلی سیستم (خرابی) می‌باشد. در واقع در صورتی که سیستم در حالت عادی خود در حال کار باشد هرگونه عیب جزئی یا کلی سیستم باید موجب انتقال سیستم به حالت خراب-ایمن گردد. سیستم خراب ایمن سیستمی است که با وقوع عیب یا خرابی هیچ گونه خطری ایجاد نکند و با توقف کامل سیستم ایمنی آن تضمین گردد. برای مثال طراحی مدارراه باید به نحوی باشد که در صورت وقوع عیب کلی و خرابی آن، حالت اشغال را نشان دهد. در این صورت احتمال وقوع حادثه خطرآفرین به علت این خرابی به حداقل می‌رسد.

به طور کلی اگر در هر لحظه عیب جزئی یا کلی سیستم شناسایی شود می‌توان با طراحی مناسب، آن را به یک سیستم خراب-

ایمن مطلق تبدیل نمود. شرایط خطرآفرین شرایطی است که تحت آن عیب جزئی در سیستم پدید آید اما سیستم از کشف آن ناتوان باشد. در این صورت سیستم به صورت معیوب ادامه کار داده و در هر لحظه ممکن است منجر به بروز حادثه گردد.

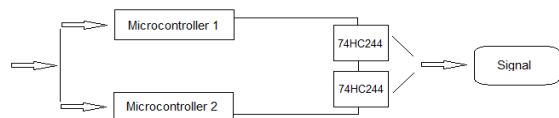
### ۳-۵-۱ ضریب عیب یابی

برای تمامی اجزای سیستم یک فاکتور به نام ضریب عیب یابی (Coverage Factor) تعریف می‌شود و مقداری بین صفر و یک دارد. در صورتی که سیستم قادر به کشف تمامی عیوب خود به صورت مطلق باشد آنگاه این فاکتور برابر با یک شده و سیستم نیز مطلقاً ایمن می‌گردد. در سیستم های ایمن واقعی، این مقدار به عدد یک بسیار نزدیک می‌باشد.

### ۴. محاسبه‌ی قابلیت اطمینان با استفاده از

#### افزونگی ساختاری

برای بررسی و محاسبه‌ی قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال این برد را به عنوان سیستم دو عضو با یک عضو آماده به کار در نظر می‌گیریم. در شبیه‌سازی انجام شده از دو میکروکنترلر برای ارسال و دریافت دستورات به کنار خط و از ایترلاکینگ استفاده شده که میکروکنترلر اول در حالت آنلاین بوده و میکروکنترلر دوم در حالت آماده به کار مورد استفاده قرار گرفته است. نحوه کارکرد و خروجی هر دو میکروکنترلر یکسان بوده و در صورتی خرابی میکروکنترلر آنلاین از میکروکنترلر آماده به کار استفاده می‌شود که در این صورت انتظار می‌رود که قابلیت اطمینان سیستم افزایش یافته و ایمنی سیستم بالاتر برود. برد کنترل‌کننده‌ی سیگنال با یک عضو آماده به کار به صورت زیر شکل زیر نمایش داده شده که از این پس این برد با نام اختصاری LMP.RE شناخته می‌شود.



شکل ۱۱. شماتیک سیستم کنترل‌کننده‌ی سیگنال LMP.RE با

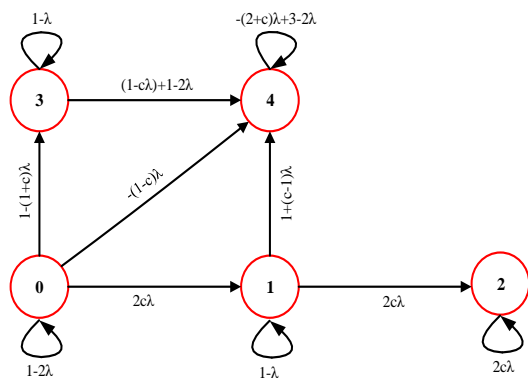
پردازنده‌ی دارای افزونگی

دارای واحد عیب‌یابی غیرایده‌آل هستند، لذا حالت‌های کاری برد کنترل‌کننده‌ی سیگنال در این حالت به صورت زیر خواهند بود: در حالت ابتدایی هر دو پردازنده سالم هستند. ممکن است یک پردازنده سالم و پردازنده دیگر معیوب با عیب قابل کشف باشد. حالت دیگر این است که هر دو پردازنده معیوب با عیب قابل کشف باشند. در حالت دیگر پردازنده اصلی سالم و پردازنده آماده به کار معیوب با عیب غیرقابل کشف است. حالت پایانی این است که پردازنده اصلی معیوب با عیب غیر قابل کشف است. کلیه حالت‌ها در جدول زیر خلاصه شده‌اند.

جدول ۱. حالت‌های کاری سیستم LMP.RE

حالت	توصیف حالت سیستم در زمان $t$	$R$	$S$
0	سیستم سالم و بی‌عیب	✓	✓
1	یک عضو معیوب است و عیب آن قابل کشف است	✓	✓
2	هر دو عضو معیوب هستند با عیب قابل کشف	X	✓
3	عضو اصلی سالم و عضو آماده‌به‌کار معیوب با عیب غیر قابل کشف	X	✓
4	عضو اصلی معیوب است با عیب غیرقابل کشف	X	X

با توجه به اطلاعات موجود در جدول بالا می‌توان نمودار حالت گذار سیستم را برای بدست آوردن روابط مختلف سیستم در حالات گوناگون به صورت زیر ترسیم کرد. داریم:



شکل ۱۲. نمودار حالت گذار سیستم در حالت استفاده از دو

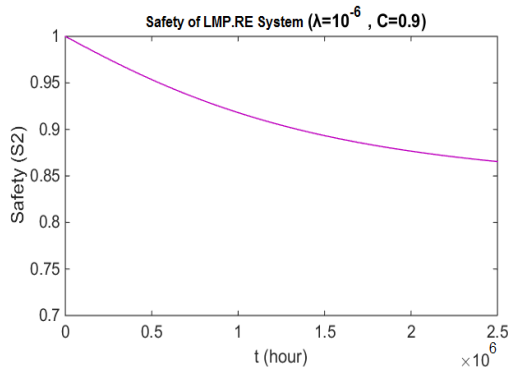
پردازنده همزمان

این افزونگی از نوع فعال است و براساس جایگزینی عضو معیوب کار می‌کند. در این نوع از معماری سیستم دارای ۲ واحد پردازنده‌ی مستقل است. این دو واحد سخت‌افزار یکسانی دارند و می‌توانند یک برنامه نرم‌افزاری مشابه را اجرا کنند، همچنین در مواردی ممکن است نرم‌افزار آن‌ها نیز تفاوت داشته باشد. تحت شرایط متعارف، هر دو واحد با هم مرتبط هستند و ورودی دریافت می‌کنند در حالی که سوئیچ تنها به پردازنده‌ی اصلی (۱) اجازه می‌دهد در مدار باشد و خروجی خود را به عنوان خروجی نهایی برد کنترل کننده‌ی سیگنال ارائه نماید. در این شرایط واحد دیگر به عنوان پردازنده‌ی آماده به کار به حساب می‌آید. این واحد تنها زمانی وارد مدار می‌شود که در پردازنده‌ی اصلی خرابی اتفاق افتاده و یا دچار عیب شود که تشخیص این کار از طریق واحد عیب‌یاب انجام می‌شود. در واقع واحد عیب‌یابی، با دادن یک سیگنال به سوئیچ باعث می‌شود واحد فعال از واحد اصلی به واحد کمکی توسط سوئیچ تغییر کند. البته در انتها ذکر این نکته حائز اهمیت است که واحد عیب‌یابی ایده‌آل نبوده و ممکن است برخی از عیوب را نیز کشف نکند. کارکرد سوئیچ و واحد عیب‌یابی در این ساختار بسیار مهم است. طیف وسیعی از خطاها و عیوب سیستم پس از شناسایی توسط واحد عیب‌یابی توسط سوئیچ از خروجی قطع شده و در واقع سیستم خراب-ایمن می‌شود. یعنی اگر عیوب خطرناکی در سیستم رخ دهد توسط این واحد از عبور آن و قرار گرفتن روی خروجی جلوگیری می‌شود. چالشی که برای این واحد وجود دارد همگام کردن دو واحد و نیز قطع خروجی در موارد خطر می‌باشد. از طرفی سوئیچ با واحد پردازنده آنلاین یا اصلی به صورت سری قرار گرفته است، لذا خرابی آن مانع تغییر پردازنده‌ی اصلی مدار می‌شود. به همین دلیل قابلیت اعتماد و ایمنی سوئیچ باید به شکل قابل ملاحظه‌ای بالا باشد. در بسیاری از مقالات و مدل‌سازی‌ها قابلیت اعتماد این واحد را بین صفر و یک در نظر می‌گیرند. برای محاسبه‌ی قابلیت اطمینان این بخش باید از روش سیستم با یک عضو آماده به کار استفاده کرد. مطابق فرضیات پردازنده‌ها

حالت‌های ایمن سیستم شامل تمامی حالت‌هایی می‌شود که یا کنترل‌کننده در آن کار می‌کند و یا اینکه در صورت خرابی و وقوع عیب، عیب مورد نظر پیدا شده و کشف شود. لذا به جز حالت ۴ سایر حالت‌ها ایمن بوده و بنابراین ایمنی سیستم طبق رابطه زیر به دست می‌آید.

$$S_2(t) = 1 - P_4 = c^2 + 2c(1-c)e^{-\lambda t} + \frac{1-c}{1+c}e^{-\lambda(1-c)t} - c^2 \frac{1-c}{1+c}e^{-2\lambda t} \quad (19)$$

با فرض اینکه نرخ خرابی سیستم باشد و ضریب عیب‌یابی واحد پردازنده برابر با ۰,۹ در نظر گرفته شود؛ منحنی ایمنی برد کنترل‌کننده سیگنال با استفاده از یک پردازنده‌ی آماده به کار را مطابق شکل زیر با نرم‌افزار MATLAB می‌توان ترسیم نمود.



شکل ۱۴. منحنی ایمنی برد کنترل‌کننده سیگنال با استفاده از یک پردازنده‌ی آماده به کار LMP.RE

همانطور که از نمودار بالا پیداست ایمنی سیستم در ابتدا مقدار ۱ بوده و در بالاترین حد خود قرار می‌گیرد که این مقدار به مرور زمان و با افزایش مدت استفاده از سیستم کاهش پیدا خواهد کرد.

## ۵. نتیجه‌گیری

در این مقاله در ابتدا به معرفی سیستم OCS950 و سپس برد کنترل‌کننده سیگنال در خطوط مترو تهران اشاره شده و در ادامه مفاهیم قابلیت اطمینان سیستم مورد بررسی قرار گرفت. سپس به معرفی چرخه‌ی حیات سیستم پرداخته شد و نرخ خرابی، زمان متوسط بین خرابی‌ها، زمان متوسط تا خرابی و زمان متوسط تا تعمیر معرفی و بررسی گردید. در ادامه به معرفی قابلیت اطمینان پرداخته شد و قابلیت اطمینان برد کنترل‌کننده سیگنال مورد ارزیابی قرار گرفت که مشخص شد برد طراحی

با استفاده از نمودار بالا ماتریس حالت گذار سیستم با استفاده از یک پردازنده آماده به کار به صورت زیر بدست می‌آید:

$$M_2 = \begin{bmatrix} 1-2\lambda & 2c\lambda & 0 & 1-(1+c)\lambda & -(1+c)\lambda \\ 0 & 1-\lambda & 2c\lambda & 0 & 1+(c-1)\lambda \\ 0 & 0 & 2c\lambda & 0 & 0 \\ 0 & 0 & 0 & 1-\lambda & (1-c\lambda)+1-2\lambda \\ 0 & 0 & 0 & 0 & -(2+c)\lambda+3-2\lambda \end{bmatrix} \quad (15)$$

حال با استفاده از معادله‌ی دیفرانسیل زیر معادلات حالت پیوسته زمان به صورت زیر بدست خواهد آمد:

$$\frac{d}{dt}P(t) = P(t).M_2 \quad (16)$$

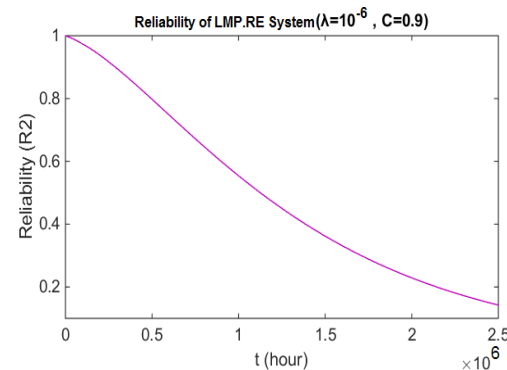
حال با استفاده از نرم‌افزار Matlab احتمال هر یک از حالت‌ها به صورت زیر بدست می‌آید:

$$\begin{cases} P_0 = e^{-2\lambda t} \\ P_1 = 2c(e^{-\lambda t} - e^{-2\lambda t}) \\ P_2 = c^2(e^{-2\lambda t} - 2e^{-\lambda t} + 1) \\ P_3 = \frac{1-c}{1+c}(e^{-\lambda(1-c)t} - e^{-2\lambda t}) \\ P_4 = 1 - c^2 - 2c(1-c)e^{-\lambda t} - \frac{1-c}{1+c}e^{-\lambda(1-c)t} - c^2 \frac{1-c}{1+c}e^{-2\lambda t} \end{cases} \quad (17)$$

با توجه به ماهیت حالات می‌توان گفت که دو حالت اول جزء حالت‌های قابلیت اعتماد هستند، لذا داریم:

$$R_2(t) = P_0 + P_1 = e^{-2\lambda t} + 2c(e^{-\lambda t} - e^{-2\lambda t}) = e^{-2\lambda t}(1-2c) + 2ce^{-\lambda t} \quad (18)$$

با فرض اینکه نرخ خرابی سیستم مورد نظر باشد و ضریب عیب‌یابی واحد پردازنده برابر با ۰,۹ باشد منحنی قابلیت اعتماد این سیستم با یک عضو آماده به کار (LMP.RE) را با استفاده از نرم‌افزار Matlab به شکل زیر ترسیم نمود:



شکل ۱۳. منحنی قابلیت اطمینان برد کنترل‌کننده سیگنال با یک پردازنده آماده به کار نسبت به زمان

2. Computer Base Interlocking
3. Central interlocking system
4. Concentrator
5. Object Controller
6. Communication Control Unit
7. Electro Magnetic Compatibility

## ۷. پیشنهادات

با توجه با اینکه در ساختار صنعتی این بردها از برخی قطعات همانند پردازنده‌ها به تعداد بالا استفاده شده، برای سهولت کار و کاهش هزینه‌های تولید می‌توان از یک پردازنده‌ی قوی‌تر به عنوان پردازنده‌ی اصلی و پردازنده‌ی دوم به عنوان رزرو در جهت بالابردن قابلیت اطمینان کنترل‌کننده‌ی سیگنال استفاده کرد. می‌توان ساختار برد را به گونه‌ای طراحی کرد که برای هر دو نوع سیگنال LED و حبابی به طور همزمان قابل استفاده بوده و فیدبک مناسب را از سیگنال به کنترل‌کننده‌ی تجهیزات ارسال نماید.

جهت عیب‌یابی سریع‌تر تجهیزات می‌توان از درخت خرابی تجهیزات در تحلیل خرابی قطعات الکترونیکی برد کنترل‌کننده‌ی سیگنال استفاده کرد.

## ۸. علائم و اختصارات

علائم و اختصاراتی که در این مقاله مورد استفاده قرار گرفته است به شرح زیر است:

جدول ۲. علائم و اختصارات

Explanation	Abbreviation
Object Controller System	OCS
Computer Base Interlocking	CBI
Centralized Interlocking System	CIS
Object Controller	OC
Communication & Control Unit	CCU
Electromagnetic Compatibility	EMC
Mean Time To Repair	MTTR
Mean Time To Failure	MTTF
Mean Time Between Failure	MTBF
Reliability	R
Safety	S
Coverage Factor	C
Unreliability	Q

شده دارای قابلیت اطمینان نسبتاً بالایی است که جهت افزایش آن می‌توان از افزودن در طراحی برد استفاده کرد که هم باعث کاهش هزینه‌های تحمیلی شده و هم کارایی و ایمنی سیستم را در شرایط گوناگون بالاتر ببرد.

در تحقیقات پیشین، موضوع کنترل‌کننده‌های تجهیزات به دلیل کاربردهای صنعتی و انحصاری بودن اسناد مربوطه شرکت‌های سازنده‌ی سیگنالینگ، به طور کامل و جامع و با تمامی تجهیزات مورد بررسی قرار نگرفته است. از این رو از دیدگاه‌های سخت-افزاری، نرم‌افزاری، تبادل اطلاعات و زمانی همچنان زمینه تحقیقات زیادی وجود دارد. در این پروژه در بحث قابلیت اطمینان برخی فرضیات در مقادیر نرخ خرابی و هم‌چنین ایده‌آل بودن کارکرد پردازنده‌های Atmega32 در نظر گرفته شد. در این مقاله آنالیز مورد نظر برای طرح ساختاری برد کنترل‌کننده‌ی سیگنال که جزئی از سیستم ocs950 است انجام شده است و باتوجه به اینکه شرکت سازنده با فروش این تجهیزات درآمد کسب می‌کند جهت جلوگیری از کپی برداری اطلاعات دقیقی از MTTF قطعات ساختاری برد در اختیار مشتری قرار نمی‌دهد، لذا مقادیر MTTF فرضی بوده که البته مقادیر مورد نظر با مقادیر واقعی در نمونه‌های مشابه مطابقت دارد. از روابط و محاسباتی که در این مقاله بدست آمد می‌توان نتیجه گرفت که برد کنترل‌کننده‌ی سیگنال یا یک عضو تعمیرپذیر و دارای افزودنی ساختاری از لحاظ قابلیت اطمینان در شرایط نرمال قرار می‌گیرد و ایمنی مسافران و سیرو حرکت در قطارها را تامین خواهد کرد. بحث قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال مورد بررسی قرار گرفت در حالی که این برد از لحاظ دسترس پذیری، تعمیرپذیری و درخت خطا مورد بررسی قرار نگرفت زیرا این مقاله صرفاً به معرفی و بررسی قابلیت اطمینان برد کنترل‌کننده‌ی سیگنال پرداخته است که موارد دیگر که اشاره شد می‌تواند موضوعات مناسبی در زمینه تحقیقات محققان و دانشجویان عزیز باشد.

## ۶. پی‌نوشت‌ها

1. Object Controller System (OCS)

## ۹. مراجع

- IGO, Frank Hagelin (2018) "General Application Information for OCS 950 Object Controller System" Bombardier Transportation, vol. 1, no. 31, pp. 1-31.
- Min-Seok Kim, Min-Kyu Kim, Jong-Woo Lee (2011) "Reliability Analysis for Train Control System by Hardware Redundancy Architecture in Fault Tolerance System" Journal of International Council on Electrical Engineering, Vol. 1, No. 2, pp. 140-144.
- Mikael Johansson, RIU (2016) "Basic Signaling Works OC application Works" ABB Daimler-Benz Transportation, pp. 1-31.
- Mikael Johansson, RIU and Johansson, Martin (2017) "Application Information for Signal Object Controller" Tehran Metro Line 7 Design, vol. 1, no. 34, pp. 1-34.
- Morant, Amparo (2016) "Safety and Availability Evaluation of Railway Signaling Systems" Railway Signaling, pp. 303-316.
- Murphy, Erik (2018) "System Description Tehran Line 7" Tehran Metro Line 7 Project, pp. 1-61.
- Power, Expert (2009) "Reliability in Electronics" Technical Article, pp. 1-11.
- Thulin, Michael (2018) "Technical Description Ebilock, Computerized Interlocking" Bombardier Transportation.
- Vinod Chandra, K. Vijaya Kumar (1997) "Reliability and safety analysis of tolerant-fault and safe-fail node for use in a railway signaling system" Reliability Engineering and System Safety, no.57, pp.177-183.
- Wei-Chih Hsu, Yen-Ta Chiu (2012) "An Application of Reliability Analysis on the Signaling System of the Kaohsiung Metro

- توبکی، علیرضا (۱۳۹۶) " طراحی، شبیه‌سازی و بررسی قابلیت برد کنترل‌کننده‌ی سیگنال در مترو"، پایان نامه‌ی کارشناسی ارشد، استاد راهنما: محمدعلی صندیدزاده، تهران: دانشکده راه‌آهن - گروه مهندسی کنترل و علائم، دانشگاه علم و صنعت ایران.

- جعفری، هستی و صندید زاده، محمدعلی و قیصری، کیوان و قوی بازو، امیر (۱۳۹۵) " آنالیز سطوح تمامیت ایمنی با استفاده از درخت خطای فازی (مطالعه‌ی موردی در صنعت ریلی)" فصلنامه مهندسی حمل و نقل، سال هشتم، دوره دوم، ص. ۳۸۷-۳۷۱.

- Singh, Pankaj, Singh, Rupali, Sharma, Rohit, Agrawal, Pankaj (2016) "Reliability measures for switched-mode power supplies (SMPS) with redundant fly back transformer" International Conference on Micro-Electronics and Telecommunication Engineering.

- Ramakrishnan, Arun, Syrus, Toby and Michael Pecht (2000) "Electronic Hardware Reliability" The RF and Microwave Handbook.

- Cadwallader, Lee C, and Peter I. Petersen (2005) "Reliability estimates for power supplies" In 21st IEEE/NPS Symposium on Fusion Engineering SOFE 05, pp. 1-4.

- Flammioni, Fabio, Mazzocca, Nicola, Iacono, Mikel and Marrone, Samuel (2005) "Using repairable fault trees for the evaluation of design choices for critical repairable systems" IEEE International High Assurance System.

- Geunhong Min (2008) "A Study on a Safety Activity on Safety Critical Related Software in Train Control System" The Korean Society of Automotive Engineers, vol.2, pp.1077-1083.

"International Symposium on Computer, Consumer and Control, pp.564-567.

- Xiaoqing Cheng<sup>1</sup>, Zongyi Xing, Yong Qin, Yuan Zhang<sup>1</sup>, Shaohuang Pang, Jun Xia (2013) "Reliability Analysis of Metro Door System Based on FMECA "Journal of Intelligent Learning Systems and Applications, no.5, pp.216-220.



علیرضا تویکی، درجه کارشناسی در رشته مهندسی برق قدرت را در سال ۱۳۹۲ از اصفهان اخذ نمود. ایشان در سال ۱۳۹۷ موفق به کسب درجه کارشناسی ارشد در رشته مهندسی کنترل و علائم از دانشگاه علم و صنعت ایران گردید. زمینه های پژوهشی مورد علاقه ایشان، سیستم‌های کنترل و سیگنالینگ ریلی، ایمنی و کنترل ترافیک، شبکه‌های تولید و توزیع برق است.



محمدعلی صدیدزاده، درجه کارشناسی را در رشته مهندسی برق الکترونیک در سال ۱۳۷۰ از دانشگاه تهران و درجه کارشناسی ارشد را در رشته مهندسی برق کنترل در سال ۱۳۷۲ از همان دانشگاه اخذ نمود. در سال ۱۳۷۹ موفق به اخذ درجه دکتری در رشته مهندسی برق کنترل، از دانشگاه صنعتی امیرکبیر گردید. زمینه های پژوهشی مورد علاقه ایشان کنترل و سیگنالینگ راه آهن و قطار بوده و در حال حاضر عضو هیات علمی با مرتبه دانشیار در دانشگاه علم و صنعت ایران است.

