تحلیل و مقایسه ایمنی و قابلیت اعتماد سیستم‌های اینترلاکینگ کامپیوتری با افزونگی‌های مختلف به روش زنجیره‌های پیوسته زمان مارکوف

مقاله علمی – پژوهشی

محمدعلی صندیدزاده*، دانشیار، دانشکده راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران
مسعود محمدکریمی، دانش‌آموخته کارشناسی ارشد، دانشکده راه‌آهن، دانشگاه علم و صنعت ایران، تهران، ایران
*پست الکترونیکی نویسنده مسئول: Sandidzadeh@iust.ac.ir

دریافت: ۱۴۰۲/۰۹/۲۸– پذیرش: ۱۴۰۳/۰۱/۲۵
صفحه ۱۶۳-۱۵۱

چکیده

اینترلاکینگ به عنوان قلب سیستم سیگنالینگ ریلی، مهم‌ترین بخش این سیستم و یک بخش ایمنی-محور محسوب می‌شود. با نگاهی به وظایف سیستم اینترلاکینگ از جمله مسیرسازی صحیح، قفل کردن مسیر و آزاد سازی به موقع آن و فرمان دادن به تجهیزات کنار خط از جمله سیگنال، ماشین سوزن و مدار راه، آشکار خواهد شد که به دلیل حیاتی بودن این وظایف، این بخش الزاماً باید تحمل‌پذیری بالایی در برابر وقوع عیوب مختلف داشته باشد. مهم‌ترین راه تحمل‌پذیر کردن سیستم، استفاده از افزونگی در سخت افزار پردازنده‌های اینترلاکینگ می‌باشد. ساختارهای دو عضوه (با یک عضو آماده به کار)، سه عضوه (با رأی‌گیری ۲ از ۳) و چهار عضوه (۲ از ۲ مضاعف) از جمله مهم‌ترین افزونگی‌های سخت‌افزاری پیاده‌سازی شده در طراحی پردازنده‌های سیستم اینترلاکینگ توسط سازنده‌های معتبر دنیا می‌باشد که سیستم را در مقابل عیوب، تحمل‌پذیر کرده و ایمنی و قابلیت اعتماد آن را افزایش می‌دهد. در این پایان‌نامه با استفاده از روش مارکوف تحلیل ایمنی و قابلیت اعتماد سیستم‌های اینترلاکینگ ِدارای افزونگی‌های مذکور انجام شده و این معماری‌ها از دیدگاه ایمنی و قابلیت اعتماد مقایسه شده‌اند. در روش مارکوف با در نظرگیری حالت‌های مختلف کار پردازنده‌های تحت افزونگی، با درنظرگرفتن نرخ خرابی، دیاگرام حالت سیستم به دست می‌آید. سپس گذارهای سیستم بین حالت‌های مختلف کاری با یک ماتریس بیان می‌شود. بدین ترتیب با تشکیل معادلات گذار حالت می‌توان رفتار سیستم را به طور کامل ارزیابی کرد و ایمنی، قابلیت اعتماد و میانگین زمان تا خرابی سیستم اینترلاکینگ را به صورت کمّی به دست آورد. در این پایان‌نامه همچنین تأثیر ضریب عیب‌یابی و نرخ خرابی بر ایمنی و قابلیت اعتماد سیستم اینترلاکینگ دارای افزونگی بررسی شده و اثبات شده است که بهبود این شاخص‌ها در اتکاپذیر کردن سیستم تأثیر بسزایی دارد.

واژه‌های کلیدی: افزونگی، ایمنی، تحمل‌پذیری، سیستم اینترلاکینگ، قابلیت اعتماد

۱- مقدمه

در کنترل عبور و مرور قطارها، تعداد زیادی از فرمان‌ها و پردازش‌های سیستم سیگنالینگ توسط سیستم اینترلاکینگ انجام می‌شود. عملیات مسیرسازی، قفل کردن و آزادسازی مسیر و ایجاد همانگی بین تمامی تجهیزات کنار خط اعم از سیگنال، ماشین سوزن و مدار راه به عهده این سیستم می‌باشد. از طرفی راهبر به صورت بلادرنگ و لحظه‌ای قطار را کنترل می‌کند لذا چک کردن وضعیت تجهیزات کنار خط و بررسی صحت آن‌ها باید بصورت لحظه‌ای انجام شود بنابراین ایمنی و قابلیت اعتماد این سیستم تحت تمامی شرایط بسیار حائز اهمیت است. از دهه ۱۹۸۰ با ظهور سیستم اینترلاکینگ کامپیوتری است تا کنون ساختارهای گوناگونی در معماری این سیستم به کار رفته است. به دلیل حیاتی بودن این سیستم و حساسیت آن، همواره سعی

سازندگان بر این بوده است که ساختارهایی در معماری پردازنده‌ها استفاده شود که ایمنی و قابلیت اعتماد قابل قبولی را ارائه دهند و تا حد امکان در برابر عیوب احتمالی تحمل‌پذیر باشد. تحمل‌پذیری بدین معناست که با وجود امکان و احتمال وقوع عیب در اجزای سیستم، روشی به کار گرفته شود تا عیوب اجزا بر عملکرد سیستم کلی تا حد امکان اثر نگذارد و سیستم به انجام وظایف خود ادامه دهد. یکی از راهکارهای مهم برای افزایش قابلیت اعتماد و تحمل‌پذیری سیستم، استفاده از افزونگی سخت‌افزاری در پردازنده‌های سیستم اینترلاکینگ است. تاکنون ساختارهای افزون چندعضوه توسط سازندگان مختلف مورد استفاده بوده است. ساختارهای Dual Hot Spare، 2-Vote-3 و 2-Vote-2 Double از متداول‌ترین ساختارها بوده که در معماری پردازنده‌های اینترلاکینگ استفاده شده است. برای نمونه به ترتیب در سیستم های Siemens SIMIS ، SSI Alstom و Bombardier Adtranz از ساختارهای فوق استفاده شده است [Nesi, 2013 و Theeg , 2009]. انتخاب روش مناسب جهت ارزیابی ایمنی و و قابلیت اعتماد سیستم مساله مهمی است، سیستم اینترلاکینگ باید ایمنی، قابلیت اعتماد و دسترس پذیری قابل قبولی داشته باید. لذا ابزاری نیاز است که قادر به ارزیابی و تحلیل دقیق عددی این فاکتورها باشد. مهمترین روش‌هایی که برای این منظور استفاده میشود عبارتند از درخت خرابی (FTA) درخت دینامیکی خرابی (DFT)، بلوک دیاگرام قابلیت اعتماد (RBD)، شبکه عصبی و مدل‌سازی مارکوف (Markov). استفاده از درخت خرابی دینامیکی برای سیستم‌های دینامیکی دارای محدودیت‌هایی میباشد. روش شبکه عصبی می تواند پارامترهای طراحی مربوط به قابلیت اعتماد را با بهینه کند و بدین ترتیب انتخاب پارامترها را آسان‌تر می‌کند.

روش مارکوف اما مدل سازی ساده‌تری دارد و همچنین اساس روش درخت دینامیکی خرابی و شبکه عصبی است. روش مارکوف می‌تواند با مدل سازی حالت‌های کاری سیستم و در نظر گرفتن گذار بین آن‌ها تمامی اتفاقات سیستم نظیر خرابی و تعمیرات را مدل کند. برای مثال فرایند تعمیرات که گذار از حالت معیوب به حالت سالم است یک رخداد دینامیکی است که باید بخوبی مدل‌سازی شود، از طرفی مدل‌سازی مربوطه باید طبیعت متغیر با زمان سیستم را بتواند بخوبی بیان کند، مثلا اگر نرخ خرابی سیستم متغیر با زمان بود باید بتوان این ویژگی در مدل سازی لحاظ شود [Rástočný, 2000]. روش مارکوف به عنوان یک روش تحلیلی مدرن امروزه برای ارزیابی قابلیت اعتماد سیستم‌های دارای افزونگی مورد استفاده قرار می‌گیرد. نمونه آن مراجع [Zhou , 2018] ، [Morant, 2016]، [Yuc, 2004] و [Bindal, 2013] هستند.

سیستم اینترلاکینگ یک سیستم تعمیرپذیر با رفتار دینامیکی است. مدل‌سازی‌های ساده عملاً نمی‌تواند تاثیر زمان تعمیرات را در تحلیل قابلیت اعتماد و دسترس‌پذیری وارد کنند روش‌های FTA و DFT قادر به مدل‌سازی این ویژگی با تقریب هستند. این تقریب البته زمانی معقول است که نرخ خرابی سیستم کم و زمان تعمیرات هم اندک باشد، از آن‌جایی که گاهی ممکن است خرابی‌های بزرگ در سیستم رخ دهد. لذا برای مدل‌سازی سیستم دینامیکی تعمیرپذیر بهترین انتخاب، روش مارکوف می‌باشد[Kuang, 2008].

۲- معرفی روش مارکوف

برخلاف روش های معمول روش مارکوف با درگیر کردن خرابی اجزای سیستم قابلیت تحلیل سیستم‌های پیچیده را دارد. نظریه فرآیندهای مارکوف نام خود را از ریاضیدان روسی به همین اسم گرفته‌است. وی برای اولین بار ارزیابی آماری فرایندهای تصادفی را بصورت سیستماتیک انجام داد. فرآیندهای مارکوف یک دسته ویژه از فرآیندهای آماری هستند. در فرآیندهای آماری اگر احتمال گذار از یک حالت به حالت دیگر صرفاً به شرایط کنونی بستگی داشته باشد و از از حالت قبلی مستقل باشد آن فرآیند از نوع مارکوفی خواهد بود. قبل از اینکه یک تغییر یا گذار رخ دهد رفتار هر حالت از تابع نمایی پیروی می‌کند. در آنالیز قابلیت اعتماد این فرض زمانی صحیح است که تمامی رفتار سیستم از قبیل خرابی و تعمیرات با نرخ‌های ثابتی انجام شوند. فرآیندهای مارکوف براساس فضای حالت و نیز فضای زمان، طبقه‌بندی می‌شوند. مطابق جدول ۱ [Dubrova, 2013].

جدول ۱. انواع فرایندهای مارکوف از لحاظ فضای زمانی و حالت

فضای حالت	فضای زمانی	نام مدل‌سازی
گسسته	گسسته	زنجیره‌های گسسته زمان مارکوف
گسسته	*پیوسته*	*زنجیره‌های پیوسته زمان مارکوف*
پیوسته	گسسته	فرآیندهای پیوسته‌ی زمان گسسته
پیوسته	پیوسته	فرآیندهای پیوسته‌ی زمان پیوسته

در اغلب مدل‌سازی های قابلیت اعتماد، فضای حالت سیستم گسسته است. برای مثال سیستم ممکن است دو حالت داشته باشد؛ حالت سالم و حالت معیوب. فضای زمانی سیستم معمولا پیوسته است، که بدین معناست که خرابی و تعمیرات سیستم متغیرهای تصادفی هستند. لذا زنجیره‌های پیوسته مارکوف متداول‌ترین مدل‌سازی در قابلیت اعتماد سیستم می‌باشد. با این وجود از زنجیره‌های گسسته مارکوف نیز کاربردهایی در ارزیابی قابلیت اعتماد سیستم وجود دارد. زنجیره‌های زمان پیوسته مارکوف به عنوان پرکاربردترین روش ارزیابی قابلیت اعتماد شناخته می‌شود بنابراین مدل‌سازی در این مقاله بر همین اساس انجام می‌شود.

۳- محاسبات ایمنی و قابلیت اعتماد به روش مارکوف

روش مارکوف دو مفهوم پایه ای دارد: حالت سیستم و گذار سیستم. زمانی که از لحاظ کمی و کیفی سیستم در یک شرایط معلوم قرار داشته باشد آن شرایط را یک حالت منحصر به فرد در نظر می‌گیرند در صورتی که این شرایط دستخوش تغییر شود و سیستم به حالت ثانویه‌ای وارد شود این تغییر حالت را گذار سیستم می‌گویند. در واقع حالت سیستم آن را در هرلحظه ای از زمان تعریف می‌کند و گذار سیستم تغییر حالت را در هر لحظه‌ای از زمان ممکن و محتمل می‌نماید [Pukite , 1998] و [Zhou, 2012].

یکی از روش‌های متداول تقسیم بندی حالت‌های کاری سیستم به سه حالت سالم، معیوب و کاهش یافته است همانطور که در مرجع [Morant, 2016] این کار برای سیستم سیگنالینگ به طور کامل انجام شده است. برای مدل‌سازی هر حالت کاری مبین ترکیبی از واحدهای معیوب و سالم سیستم می‌باشد و گذارها احتمال تغییر حالت هرواحد بین سالم و معیوب را نشان می‌دهند. هدف روش مارکوف محاسبه $P_i(t)$ است، یعنی احتمال اینکه سیستم در زمان t در حالت i قرار داشته باشد. زمانی که این مقادیر مشخص شود قابلیت اعتماد، دسترس‌پذیری و ایمنی سیستم را با جمع زدن حالت‌های مطلوب می‌توان به دست آورد. اگر حالت صفر را به عنوان حالت سالم و بی‌عیب سیستم در نظر گرفته شود، با فرض اینکه در زمان صفر سیستم در حالت سالم باشد:

$$P_0(0)=1 \qquad (۱)$$

از آنجایی که در هر لحظه سیستم تنها می‌تواند در یک حالت باشد:

$$\sum_{i\in O\cup F} P_i(t)=1 \quad ; \quad P_i(0)=0, \forall i\neq 0 \qquad (۲)$$

برای تعیین کردن $P_i(t)$ یک مجموعه معادله دیفرانسیل باید به دست آورد، برای هر حالت یک معادله دیفرانسیل. این معادلات را معادلات گذار حالت سیستم می‌گویند که چگونگی تغییر حالت سیستم بین دو حالت را بیان می‌کند. مجموعه تمامی معادلات یک فرم ماتریسی را تشکیل می‌دهند که ماتریس مذکور را M می‌نامند که در آن نرخ تغییرات بین دو حالت i و j را بیان می‌کند که i نشان دنده سطر و j نشان‌دهنده ستون است.

$$M=\begin{bmatrix} m_{00} & m_{01} & \dots & m_{0(k-1)} \\ m_{11} & m_{12} & \dots & m_{1(k-1)} \\ \vdots & \vdots & \vdots & \vdots \\ m_{(k-1)1} & m_{k2} & \dots & m_{(k-1)(k-1)} \end{bmatrix} \qquad (۳)$$

و با در نظر گرفتن حالات سیستم با ماتریس سطری P آن‌گاه معادلات دیفرانسیل فضای پیوسته مارکوف نیز بصورت رابطه ٤ نوشته می‌شوند.

$$P(t)=[P_0(t), P_1(t) \quad \dots \quad P_k(t)]$$

$$\frac{d}{dt}P(t)=P(t).M \qquad (٤)$$

۳-۱-ضریب عیب‌یابی

در تمامی سیستم هایی که ایمنی محور هستند معمولا واحدهایی نرم‌افزاری یا سخت‌افزاری تحت عنوان واحد عیب‌یابی تعبیه می‌شود. این واحد امکان یافتن عیب و خرابی واحدهای پردازنده یا سایر واحدهای سخت افزاری را فراهم می‌کند. مثل تمامی واحدهای دیگر این واحد نیز ایده‌آل نیست و ممکن است برخی از عیوب را نیز کشف نکند. اصولاً یافتن عیب گام اول در اقدام سیستم تحمل‌پذیر در برابر عیب سیستم می‌باشد لذا اگر عیوب واحدها و زیر سیستم‌ها پیدا نشوند تحمل‌پذیری سیستم نیز می‌تواند با اشکال مواجه شود. طبق تعریف ضریب عیب‌یابی برابر است با یک احتمال شرطی. احتمال اینکه عیب یک واحد توسط واحد عیب‌یابی کشف شود، به شرطی که عیب در سیستم رخ داده باشد تعریف این ضریب است. البته تعاریف دیگری از جمله مکان یابی عیب یا محدودکردن عیب و نیز بهبودی سیستم به شرط وقوع عیب در سیستم نیز در برخی مراجع به عنوان ضرایب مشابهی تعریف شده اند[Dubrova, 2013] ، اما در این مقاله تنها تعریف متداول، مطابق رابطه (۵) را به کار خواهیم‌بست:

$$C = P(\mathit{fault\ \ detection} \mid \mathit{fault\ \ existence}) \qquad (۵)$$

طبق این تعریف عیوب به دو دسته قابل کشف (با ضریب C) و عیوب غیر قابل کشف (با ضریب $(1\text{-}C)$) تقسیم می‌شوند. در این مقاله فرض شده که تمامی واحدهای پردازنده دارای واحد عیب‌یابی هستند و به صورت مستقیم این ضریب در محاسبات ایمنی و قابلیت اعتماد وارد شده است. ضریب عیب-یابی به طور مستقیم بر ایمنی سیستم تاثیر می‌گذارد. [Dubrova, 2013] این موضوع در ادامه بررسی خواهد شد.

۳-۲-محاسبات ایمنی و قابلیت اعتماد

در حالت کلی قابلیت اعتماد سیستم برابر خواهد بود با جمع احتمال تمامی حالت‌هایی که سیستم کلی در آن سالم است و می‌تواند وظایف خود را انجام دهد[Dubrova, 2013]، [Iserman, 2005] و [Koren, 2007].

$$R(t) = \sum_{i \in O} P_i(\mathrm{t}) \qquad (۶)$$

جمع فوق روی تمامی حالت‌های کاری سیستم (O) انجام می‌شود. بصورت مکمل می‌توان قابلیت اعتماد را از رابطه ۷ نیز محاسبه نمود.

$$R(t) = 1 - \sum_{i \in F} P_i(\mathrm{t}) \qquad (۷)$$

که جمع فوق روی تمامی حالت‌های خراب سیستم (F) انجام می‌شود.

در حالت کلی ایمنی سیستم برابر خواهد بود با جمع احتمال تمامی حالت‌های ایمن. چه سیستم در آن‌ها سالم باشد و چه خراب. حالت دوم را خراب-ایمن می‌گویند [Dubrova, 2013]، [Iserman, 2005] و [Koren, 2007].

$$S(t) = \sum_{i \in S} P_i(\mathrm{t}) \qquad (۸)$$

که جمع فوق روی تمامی حالت‌های ایمن بسته شده‌است.

بصورت مکمل می‌توان ایمنی را از رابطه ۹ نیز به دست آورد.

$$S(t) = 1 - \sum_{i \in U} P_i(\mathrm{t}) \qquad (۹)$$

جمع فوق روی حالت‌های ناایمن بسته شده‌است

٤-مدل‌سازی سیستم اینترلاکینگ به روش مارکوف

در این مقاله به طور کلی چند فرض برای انجام مدل‌سازی و ارزیابی رفتار سیستم اینترلاکینگ در نظر گرفته شده‌است. این فرض‌ها از طرفی کار مدل‌سازی را اندکی آسان‌تر کرده و از سوی دیگر واقعیت سیستم را نیز حفظ می‌کند و از دقت مدل‌سازی تحت شرایط یکسان نمی‌کاهد. فرض‌ها به صورت زیر در نظر گرفته شده‌اند:

- همه واحدهای پردازنده یک اینترلاکینگ مشابه هستند و تابع چگالی خرابی هریک تابع نمایی است. در کنار این‌ها نرخ خرابی واحدها نیز ثابت و مشابه می‌باشد.

-احتمال وقوع عیب در بیش از یک واحد، در یک لحظه از زمان بسیار اندک می‌باشد. بنابراین در هر زمان تنها وقوع عیب در یک واحد امکان‌پذیر در نظر گرفته شده‌است. به بیان دیگر خرابی سبب مشترک در این تحلیل در نظر گرفته نشده‌است. البته می‌توان گفت که با توجه به مدل‌سازی وقوع دو یا چند عیب به صورت متوالی و بدون فاصله زمانی از لحاظ تئوری وجود داشته و در مدل‌سازی‌های این مقاله نیز خرابی سبب مشترک نه به صورت آشکار بلکه به صورت پنهان، در نظر گرفته شده‌است.

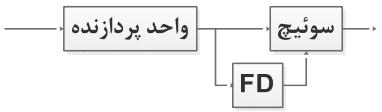
-تمامی واحدهای فرعی از جمله واحدهای مقایسه، واحدهای رأی‌گیری و سوئیچ‌ها کاملاً قابل اعتماد در نظر گرفته شده‌اند. این فرض تا حد بسیار زیادی مورد قبول است. دلیل آن را می‌توان با توجه به ساختار ساده این واحدها و نیز بالا بودن کیفیت ساخت و مرغوبیت آن‌ها توضیح داد.

- در شروع کار هر سیستم، تمامی واحدهای آن سالم و بدون هیچ عیبی شروع به کار می‌کنند. هر عیبی با گذر زمان برای زمان‌های بیشتر از صفر امکان و احتمال وقوع دارد.

-واحدهای پردازنده اینترلاکینگ در این پایان‌نامه، همگی دارای واحد عیب‌یابی سخت‌افزاری هستند، این واحد ایده‌آل نبوده و بازدهی آن معادل ضریب عیب‌یابی می‌باشد. به بیان دیگر این واحد ممکن است برخی از عیوب واحد تحت نظارت خود را نتواند بیابد و عیب مورد نظر عملاً شناسایی نشود.

٤-١- مدل‌سازی ایمنی و قابلیت اعتماد سیستم تک عضوه (Simplex)

سیستم اینترلاکینگ دارای تک عضو پردازنده مطابق شکل ۱ می‌باشد. واحد عیب‌یابی با FD در این ساختار نمایش داده شده است. نقش سوئیچ نیز قطع خروجی در صورت اعلام عیب توسط واحد عیب‌یابی می‌باشد. در تمامی ساختارهای معرفی شده در این مقاله عملکرد به همین صورت خواهد بود. توصیف حالت‌های کاری سیستم مذکور به صورت جدول ۲ خواهد بود[Dubrova, 2013] .

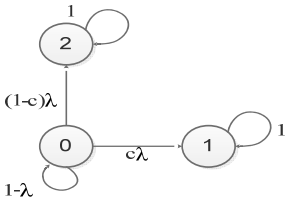


شکل ۱. شماتیک اینترلاکینگ با پردازنده تک عضو

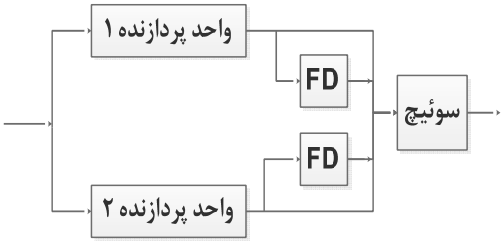
جدول۲. حالت‌های کاری سیستم اینترلاکینگ تک عضو

حالت	توصیف حالت در زمان t	R	S
0	سیستم سالم و بی‌عیب	✓	✓
1	سیستم معیوب است و عیب آن قابل کشف است	✗	✓
2	سیستم معیوب است و عیب غیرقابل کشف است	✗	✗

لذا مطابق شکل ۲ دیاگرام گذار حالت سیستم با تک عضو پردازنده به دست می‌آید.



شکل ۲. دیاگرام مارکوف سیستم تک عضوه



شکل ۳. شماتیک سیستم اینترلاکینگ DHS

در این صورت ماتریس گذار حالت مارکوف بصورت زیر به دست می‌آید و طبق رابطه (۳) با حل معادله دیفرانسیل احتمال وقوع هر حالت به دست می‌آید و از آن‌جا با توجه به تعریف حالت‌ها می‌توان هر دو شاخص قابلیت اعتماد و نیز ایمنی سیستم را به دست‌آورد. واضح است که حالت صفر تنها حالت عملیاتی سیستم است پس در محاسبه قابلیت اعتماد استفاده می‌شود. تنها حالت غیر ایمن سیستم نیز حالت ۲ است که در آن عیب کشف نشده‌ای در سیستم اتفاق می‌افتد. ایمنی و قابلیت اعتماد این سیستم در رابطه ۱۰ محاسبه شده است.

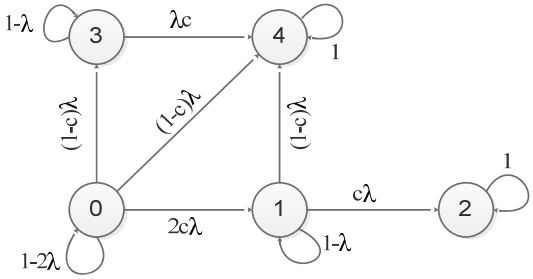
$$M_1=\begin{bmatrix}-\lambda & c\lambda & (1-c)\lambda\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}\overset{\dot{P}=P.M}{\Rightarrow}\begin{cases}P_0=e^{-\lambda t}\\ P_1=c(1-e^{-\lambda t})\\ P_2=e^{-\lambda t}(c-1)-c+1\end{cases}\Rightarrow\begin{cases}R_1(t)=P_0\\ S_1(t)=1-P_2\end{cases}\qquad(۱۰)$$

٤-٢-مدل‌سازی ایمنی و قابلیت اعتماد سیستم افزونه با یک عضو آماده به‌کار (Dual Hot Stand-By)

در این ساختار که آن را DHS می‌نامیم، در هر لحظه تنها واحد پردازنده ۱ در مدار است و در صورت وقوع عیب و سپس کشف شدن آن سیستم با پردازنده کمکی (شماره ۲) به کار خود ادامه خواهد داد. با توجه به اصول کاری این سیستم مطابق جدول ۳ تمامی حالت‌های کاری سیستم از هم تفکیک شده‌اند و وضعیت هر حالت از دید ایمنی و قابلیت اعتماد مشخص شده است با توجه به جدول ۳، در شکل ٤ دیاگرام مارکوف سیستم DHS آورده شده است. نقش واحدهای عیب‌یاب و سوئیچ همانند پردازنده تک عضو توصیف شده در بخش ٤-١ می‌باشد.

جدول ۳. حالت‌های کاری سیستم DHS

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	✗	✓
3	عضو اصلی سالم و عضو آماده‌به‌کار معیوب با عیب غیر قابل کشف	✗	✓
4	عضو اصلی معیوب است با عیب غیرقابل کشف	✗	✗



شکل ٤. دیاگرام مارکوف سیستم DHS

لذا ماتریس‌گذار حالت مارکوف به صورت زیر (M_2) به دست می‌آید و از آنجا می‌توان با نرم افزار *matlab* معادلات را حل کرد. با توجه به ماهیت حالات که در جدول ۳ مشخص شده است، می‌توان ایمنی و قابلیت اعتماد سیستم را به دست آورد. طبق رابطه ۱۱.

$$M_2=\begin{bmatrix} -2\lambda & 2c\lambda & 0 & (1-c)\lambda & (1-c)\lambda \\ 0 & -\lambda & c\lambda & 0 & (1-c)\lambda \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -(1-c)\lambda & (1-c)\lambda \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow[Matlab]{\dot{P}=P.M} \Rightarrow$$

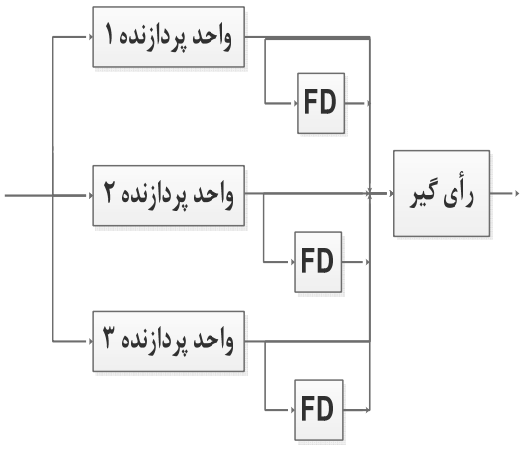
$$\begin{cases} P_0 = e^{-2\lambda t} \\ P_1 = 2c(e^{-\lambda t} - e^{-2\lambda t}) \\ P_2 = c^2(e^{-2\lambda t} - 2e^{-\lambda t} + 1) \\ P_3 = \dfrac{1-c}{1+c}(e^{-\lambda(1-c)t} - e^{-2\lambda t}) \\ P_4 = 1 - c^2 - 2c(1-c)e^{-\lambda t} - \dfrac{1-c}{1+c}e^{-\lambda(1-c)t} - c^2\dfrac{1-c}{1+c}e^{-2\lambda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

$$\Rightarrow \begin{cases} R_2(t) = P_0 + P_1 \\ S_2(t) = 1 - P_4 \end{cases} \qquad (۱۱)$$

٤-۳-مدل‌سازی ایمنی و قابلیت اعتماد سیستم با افزونگی ۲ از ۳ (2-Vote-3)

یکی از ساختارهای رایج که بصورت گسترده در سیستم‌های اینترلاکینگ استفاده شده است افزونگی 2-Vote-3 یا افزونگی با رای‌گیری ۲ از ۳ می‌باشد، که با رأی‌گیر و سوئیچ عمل می‌کند. این ساختار افزونه را با نام TMR نیز می‌شناسند. با درنظرگیری تمامی فرض‌های گفته شده می‌توان حالت‌های کاری سیستم را مطابق جدول ٤ از یکدیگر تفکیک نمود. باید توجه داشت که حالت‌ها بر اساس استراتژی طراح سیستم به قابل اعتماد و ایمن و یا متضاد این‌ها تقسیم می‌شود. حالت‌هایی که سیستم در آن‌ها کار می‌کند اما چند عضو از سیستم معیوب هستند در واقع حالت‌های کاهش‌یافته محسوب می‌شوند، پذیرش عملکرد سیستم در این حالت‌ها به طراحی سیستم برمی‌گردد.

در این مقاله تمامی حالت‌های کاهش یافته به عنوان حالت کاری در نظر گرفته شده اند. با توجه به جدول ٤ حالت‌های صفر تا ۳ به عنوان حالت‌های قابل اعتماد درنظر گرفته‌شده، حالت‌های ایمن نیز شامل تمام حالت‌ها به جز ٦ می‌شود. حالت ۵ حالت خراب-ایمن است که در آن تمامی واحدها معیوب هستند[Wang, 2011].

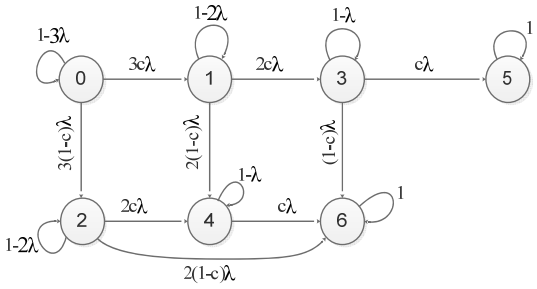


شکل ۵. شماتیک سیستم اینترلاکینگ 3V2

جدول ٤. حالت‌های کاری سیستم 3V2

حالت	توصیف حالت سیستم در زمان t	R	S
0	هر سه عضو سیستم سالم و بی عیب هستند	✓	✓
1	یک عضو معیوب است و عیب آن قابل کشف و رفع	✓	✓
2	یک عضو معیوب است و عیب آن غیر قابل کشف و رفع	✓	✓
3	دو عضو معیوب در سیستم وجود دارد که عیب هردوی آنها قابل کشف و رفع است، تحت این شرایط سیستم قابلیت تحمل سومین خرابی را نیز دارد	✓	✓
4	دو عضو معیوب در سیستم وجود دارد عیب عضو اول قابل کشف و رفع است ولی عیب دومی غیر قابل کشف است سیستم در این حالت کار می‌کند اما تحمل‌پذیری ندارد	✗	✓
5	هر سه عضو معیوب هستند و عیب انها قابل کشف است سیستم خروجی ندارد و در حالت خراب–ایمن است	✗	✓
6	حداقل دو عضو با عیب غیر قابل کشف در سیستم وجود دارد، سیستم خراب–ناایمن است	✗	✗

با استفاده از جدول فوق دیاگرام مارکوف سیستم 3-Vote-2 طبق شکل ٦ به دست می‌آید. سپس ماتریس گذار حالات سیستم (M_3) نوشته می‌شود.



شکل ٦. دیاگرام مارکوف 3-Vote-2

با حل دستگاه معادلات $P = P.M$ با استفاده از نرم‌افزار متلب می‌توان احتمال حالت‌ها را به دست آورد.

$$M_3 = \begin{bmatrix} -3\lambda & 3c\lambda & 3(1-c)\lambda & 0 & 0 & 0 & 0 \\ 0 & -2\lambda & 0 & 2c\lambda & 2(1-c)\lambda & 0 & 0 \\ 0 & 0 & -2\lambda & 2c\lambda & 0 & 2(1-c)\lambda & 0 \\ 0 & 0 & 0 & -\lambda & (1-c)\lambda & c\lambda & 0 \\ 0 & 0 & 0 & 0 & -c\lambda & 0 & c\lambda \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

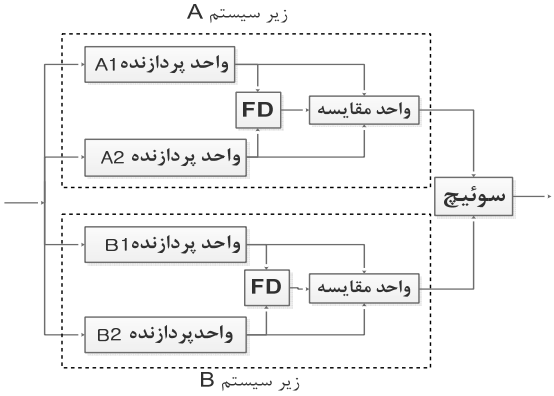
ایمنی و قابلیت اعتماد سیستم طبق رابطه ۱۲ با توجه به تعریف حالات در جدول ٤ محاسبه شده است.

$$\xrightarrow{Matlab} \begin{cases} P_0 = e^{-3\lambda t} \\ P_1 = 3c(e^{-2\lambda t} - e^{-3\lambda t}) \\ P_2 = 3(1-c)(e^{-2\lambda t} - e^{-3\lambda t}) \\ P_3 = 3c(e^{-\lambda t} - 2e^{-2\lambda t} + e^{-3\lambda t}) \\ P_4 = \dfrac{2c(1-c)}{c^2+3c+2}(e^{-\lambda t(1-c)} - 2e^{-2\lambda t} - ce^{-2\lambda t} + ce^{-3\lambda t} + 1) \\ P_5 = c^3 e^{-3\lambda t}(e^{\lambda t} - 1)^3 \\ P_6 = \dfrac{c^4 - c^3 + 6c^2 - 10c + 4}{c+1} e^{-3\lambda t} + (1-c^3) + 3c^2(1-c)e^{-\lambda t} \\ \qquad + \dfrac{3(1-c)(c^3+2c-1)}{c+1} e^{-2\lambda t} - \dfrac{12c(1-c)}{(c+1)(c+2)} e^{-\lambda t(1-c)} \end{cases}$$

$$\Rightarrow \begin{cases} R_3(t) = P_0 + P_1 + P_2 + P_3 \\ S_3(t) = 1 - P_6 \end{cases} \qquad (۱۲)$$

٤–٤–مدل‌سازی ایمنی و قابلیت اعتماد سیستم با افزونگی ۲ از ۲ مضاعف (Double 2-Vote-2)

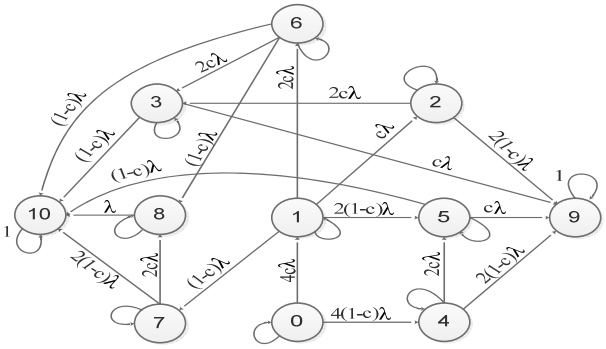
از مهم‌ترین ساختارهای افزونگی Double 2-Vote-2 یا افزونگی ۲ از ۲ مضاعف است که از نوع Hot Stand-By می‌باشد. به اختصار این سیستم را با D2V2 نمایش می‌دهیم. تحمل‌پریری در این ساختار بر مقایسه استوار است و از رأی‌گیری در آن استفاده نمی‌شود. در این ساختار به دلیل وجود ٤ واحد پردازنده حالت‌های کاهش یافته تعداد بیشتری دارند و به همین دلیل این ساختار پتانسیل بیشتری برای قابلیت اعتماد دارد. در هنگام وقوع عیب در هر عضو از این سیستم فرض می‌شود که سایر عضوها به کار خود ادامه می‌دهند. تا جایی که آخرین عضو نیز دچار اشکال شود (که تحت عنوان استراتژی عملکرد سوئیچ شناخته می‌شود). وقوع عیب در هر عضو توسط واحد عیب‌یابی می‌تواند کشف شود که همانطور که گفته شد با ضریب عیب‌یابی در شبیه‌سازی لحاظ می‌شود و در تمام این موارد سیستم قابل اعتماد است. تمامی حالت‌های کاری سیستم D2V2 در جدول ٥ آمده است و بر این اساس در شکل ٧ دیاگرام مارکوف آن ترسیم شده‌است. حالت‌های صفر تا ٨ قابل اعتماد هستند و تنها حالت ١٠ خراب–ناایمن است.



شکل٦. شماتیک سیستم اینترلاکینگ D2V2

جدول ۵. حالت‌های کاری سیستم D2V2

حالت	توصیف حالت سیستم در زمان t	R	S
0	هر چهار عضو سیستم سالم و بی‌عیب هستند و سیستم در حالت نرمال کار می‌کند	✓	✓
1	یک عضو از زیرسیستم کمکی معیوب شده، عیب مورد نظر قابل کشف است.	✓	✓
2	هر دو عضو زیر سیستم کمکی معیوب شده، عیب قابل کشف و رفع است.	✓	✓
3	سه عضو سیستم معیوب شده اند با عیوب قابل کشف، تنها یک عضو در حال کار است.	✓	✓
4	یک عضو از زیرسیستم کمکی معیوب شده و غیرقابل کشف است.	✓	✓
5	یک عضو از زیرسیستم اصلی معیوب شده، یک عضو از زیر سیستم کمکی هم معیوب شده و غیر قابل کشف است.	✓	✓
6	یک عضو از زیرسیستم اصلی و کمکی معیوب هستند و عیب قابل کشف و رفع است.	✓	✓
7	زیرسیستم اصلی سالم است، یک عضو از زیرسیستم کمکی معیوب و قابل کشف و دیگری معیوب با عیب غیرقابل کشف است.	✓	✓
8	یکی عضو از زیرسیستم اصلی معیوب است و عیب آن قابل کشف است، هر دو عضو زیرسیستم کمکی معیوب هستند، یکی قابل کشف و دیگری غیرقابل کشف	✓	✓
9	هر چهار عضو سیستم معیوب است، تمامی عیوب قابل کشف هستند، سیستم تحت این شرایط خراب-ایمن است	✗	✓
10	هر چهار عضو سیستم معیوب هستند، دست کم یک عضو عیب غیر قابل کشف دارد، خروجی سیستم خراب-ناایمن است	✗	✗



شکل ۷. دیاگرام مارکوف سیستم D2V2

طبق روندی که برای سیستم‌های قبلی طی شد ماتریس تغییرحالت مارکوف (M_4) به دست می‌آید و سپس با حل معادلات احتمال هر حالت محاسبه می‌شود. ایمنی و قابلیت اعتماد این سیستم نیز در رابطه ۱۳ محاسبه شده است.

$$M_4=\begin{bmatrix}
-4\lambda & 4c\lambda & 0 & 0 & 4(1-c)\lambda & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -3\lambda & c\lambda & 0 & 0 & 2(1-c)\lambda & 2c\lambda & (1-c)\lambda & 0 & 0 & 0\\
0 & 0 & -2\lambda & 2c\lambda & 0 & 0 & 0 & 0 & 0 & 2(1-c)\lambda & 0\\
0 & 0 & 0 & -\lambda & 0 & 0 & 0 & 0 & 0 & c\lambda & (1-c)\lambda\\
0 & 0 & 0 & 0 & -2\lambda & 2c\lambda & 0 & 0 & 0 & 2(1-c)\lambda & 0\\
0 & 0 & 0 & 0 & 0 & -\lambda & 0 & 0 & 0 & c\lambda & (1-c)\lambda\\
0 & 0 & 0 & 2c\lambda & 0 & 0 & -2\lambda & 0 & (1-c)\lambda & 0 & (1-c)\lambda\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -2\lambda & 2c\lambda & 0 & 2(1-c)\lambda\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & 0 & \lambda\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}\overset{\dot{P}=P.M}{\Rightarrow}$$

$$\overset{Matlab}{\Rightarrow}\begin{cases}
P_0=e^{-4\lambda t}\\
P_1=4c(e^{-3\lambda t}-e^{-4\lambda t})\\
P_2=2c^2(e^{-2\lambda t}-2e^{-3\lambda t}+e^{-4\lambda t})\\
P_3=4c^3(e^{-4\lambda t})(e^{\lambda t}-1)^3\\
P_4=2(1-c)(e^{-2\lambda t}-e^{-4\lambda t})\\
P_5=4c(1-c)(e^{-\lambda t}-e^{-2\lambda t}-e^{-3\lambda t}+e^{-4\lambda t})\\
P_6=4c^2(e^{-2\lambda t}-2e^{-3\lambda t}+e^{-4\lambda t})\\
P_7=2c(1-c)(e^{-2\lambda t}-2e^{-3\lambda t}+e^{-4\lambda t})\\
P_8=\dfrac{8}{3}c^2(1-c)(e^{-4\lambda t})(e^{\lambda t}-1)^3\\
P_9=(e^{-\lambda t}-e^{-2\lambda t})^2(c^2+c-1-e^{\lambda t}(c^2-c+1))^2\\
P_{10}=\dfrac{1}{3}(1-c)(e^{-4\lambda t})(1-e^{\lambda t})^3\\
\qquad\times(3c^2+5c-6-e^{\lambda t}(3c^2-3c+6))
\end{cases}$$

$$\Rightarrow\begin{cases}R_4(t)=\sum_{i=0}^{8}P_i\\ S_4(t)=1-P_{10}\end{cases}\qquad(۱۳)$$

۵-نتایج شبیه‌سازی قابلیت اعتماد و ایمنی سیستم‌های اینترلاکینگ افزون

۵-۱- محاسبات MTTF سیستم‌ها

شاخص میانگین زمان تا خرابی (MTTF) به عنوان یک معیار برای ارزیابی قابلیت اعتماد سیستم اینترلاکینگ مورد استفاده قرار می‌گیرد، این شاخص با رابطه ۱۴ قابل محاسبه است. در این مقاله با فرض $C=1$ برای تمامی سیستم‌های معرفی شده این شاخص محاسبه شده است.

$$MTTF=\int_0^\infty R(t)dt\qquad(۱۴)$$

$$MTTF_1=\int_0^\infty R_1(t)dt=\frac{1}{\lambda}\qquad(۱۵)$$

$$MTTF_2=\int_0^\infty R_2(t)dt=\frac{3}{2\lambda}\qquad(۱۶)$$

$$MTTF_3=\int_0^\infty R_3(t)dt=\frac{11}{6\lambda}\qquad(۱۷)$$

$$MTTF_4=\int_0^\infty R_4(t)dt=\frac{25}{12\lambda}\qquad(۱۸)$$

ملاحظه می‌شود که قابلیت اعتماد سیستم D2V2 از 3V2 بالاتر بوده و 3V2 نیز از DHS عملکرد بهتری دارد:

$$MTTF_4>MTTF_3>MTTF_2>MTTF_1\qquad(۱۹)$$

نرخ خرابی برابر با $10^{-5}(1/\mathrm{h})$ در نظر گرفته می‌شود. این مقدار امروزه برای یک سیستم اینترلاکینگ تک پردازنده منطقی و متداول است (Su & Wen, 2014). در این صورت به شکل عددی مقادیر زیر برای میانگین زمان تا خرابی به دست می‌آید.

$$MTTF_4=23.8years>MTTF_3=20.9years>\\ MTTF_2=17.2years>MTTF_1=11.4years\qquad(۲۰)$$

۵-۲-مقایسه ایمنی و قابلیت اعتماد سیستم‌ها

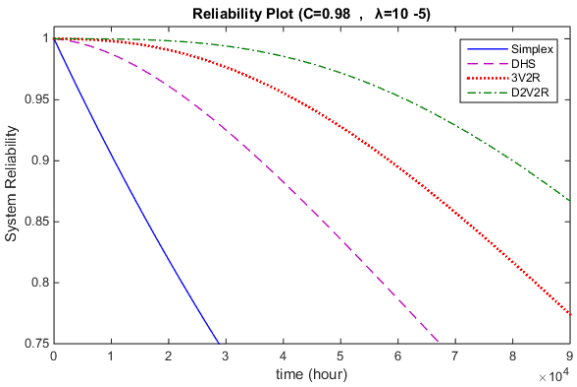
با توجه به مقادیر تحلیلی R_1 تا R_4 و نیز S_1 تا S_4 که برای هر چهار سیستم بصورت پارامتری محاسبه شد، می‌توان قابلیت اعتماد و ایمنی هر چهار سیستم را با هم مقایسه نمود. در این ارزیابی مقدار نرخ خرابی برابر با 10^{-5} و مقدار ضریب عیب‌یابی برابر با 0.98 در نظر گرفته شده است. بر این اساس با توجه به شکل ۸ می‌توان دریافت که برای قابلیت اعتماد سیستم D2V2 بالاترین سطح را دارد و پس از آن سیستم 3V2 و سپس

سیستم DHS قرار دارد. بدین ترتیب واضح است که هرچه تعداد عضوهای سیستم بیشتر شود قابلیت اعتماد آن نیز به همان نسبت افزایش می‌یابد. این نتیجه گیری با مقایسه شاخص‌های MTTF در رابطه (۱۹) نیز کاملاً هماهنگ است.

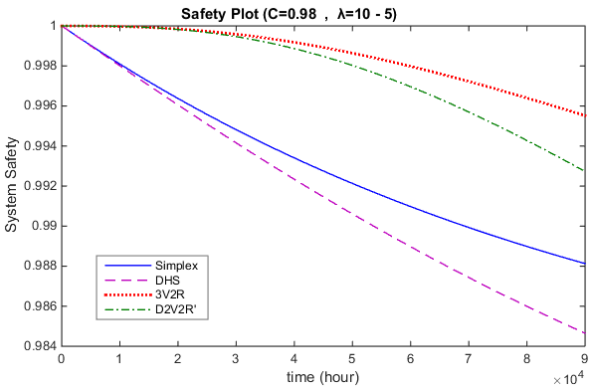
$$R_4 > R_3 > R_2 > R_1 \qquad (۲۱)$$

با توجه به شکل ۹ نیز مشخص است که از لحاظ ایمنی سیستم 3V2 بالاترین سطح ایمنی را داراست و سپس D2V2 و بعد از آن سیستم تک عضو قرار دارد. تمامی این نتایج براساس استراتژی تعریف عملکرد سوئیچ و حالت‌های کاهش یافته می‌باشد و می‌تواند با توجه با استراتژی دستخوش تغییرات شود.

$$S_3 > S_4 > S_1 > S_2 \qquad (۲۲)$$



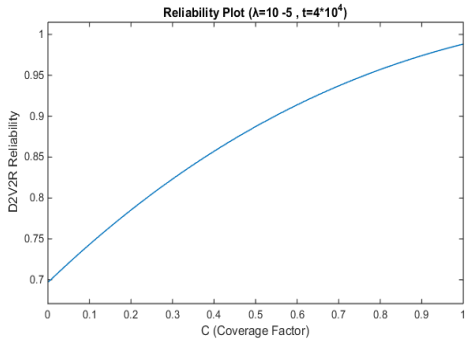
شکل ۸. مقایسه قابلیت اعتماد هر ۳ نوع Redundancy



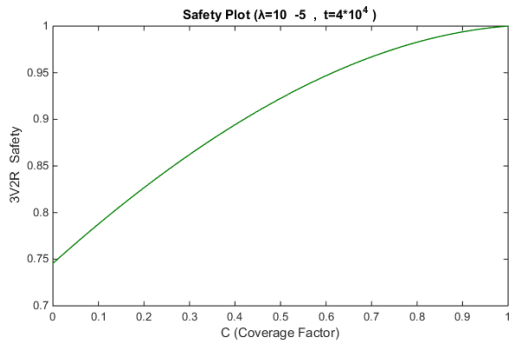
شکل ۹. مقایسه ایمنی هر ۳ نوع Redundancy

۵-۳-بررسی تأثیر ضریب عیب‌یابی بر ایمنی و قابلیت اعتماد سیستم اینترلاکینگ

همانطور که اشاره شد هر پردازنده دارای یک واحد عیب‌یابی است که همواره بر صحت عملکرد آن پردازنده نظارت دارد. این واحد در شماتیک‌ها با **FD** نشان داده شد. چگونگی عملکرد این واحد در میزان ایمنی و قابلیت اعتماد سیستم بسیار تاثیرگذار است. در شکل‌های ۱۰ و ۱۱ تاثیر پارامتر ضریب عیب‌یابی بر این دو شاخص بررسی شده است. با بررسی این منحنی‌ها می‌توان نتیجه گرفت که هرچه ضریب عیب‌یابی به مقدار ایده‌آل یک نزدیک‌تر شود ایمنی و قابلیت اعتماد نیز به حد ماکزیمم خود بیشتر نزدیک می‌شوند. همچنین مشخص است که در صورتی که ضریب عیب‌یابی برابر با یک شود آن‌گاه سیستم مطلقاً ایمن خواهد شد ($S=1$).



شکل ۱۰. تغییرات قابلیت اعتماد نسبت به ضریب عیب‌یابی



شکل ۱۱. تغییرات ایمنی نسبت به ضریب عیب‌یابی

٦- نتیجه‌گیری

در این مقاله با استفاده از زنجیره‌های پیوسته زمان مارکوف ایمنی و قابلیت اعتماد سیستم اینترلاکینگ با سه نوع افزونگی مختلف بررسی و شبیه‌سازی شد. در روش مارکوف کلیه حالت‌های کاری سیستم درنظر گرفته شده و رخداد خرابی سیستم تحت تمامی شرایط مدل‌سازی شده است. سیستم اینترلاکینگ در ٤ ساختار یک، دو، سه و چهار پردازنده تحت عنوان تک عضوه، Dual Hot Stand-by ، 3-Vote-2 و

Double 2-Vote-2 در این مقاله مورد بررسی قرار گرفت و در نتایج شبیه‌سازی مشخص شد که قابلیت اعتماد سیستم D2V2 نسبت به تمامی سیستم‌ها بالاتر بوده و ایمنی سیستم 3V2 نسبت به سایر سیستم‌ها بهتر می‌باشد. در این مقاله علاوه بر موارد مذکور، تاثیر ضریب عیب‌یابی در میزان قابلیت اعتماد و ایمنی سیستم نیز شبیه‌سازی و بررسی شد و مشخص شد که برای افزایش ایمنی و قابلیت اعتماد سیستم اینترلاکینگ می‌توان واحد عیب‌یابی هریک از پردازنده‌های سیستم اینترلاکینگ را بهبود بخشید تا سیستمی ایمن‌تر و قابل اعتمادتر به دست آید.

فهرست علائم

علائم و کمیت‌ها

قابلیت اعتماد	R
ایمنی	S
ضریب عیب‌یابی	C
نرخ خرابی (1/h)	λ
زمان (h)	t
احتمال وقوع یک حالت	P_i
ماتریس گذار حالت مارکوف	M

اختصارات و اصطلاحات

سیستم تک عضوه بدون افزونگی	Simplex
سیستم ۲ عضوه با یک عضو آماده به کار	DHS
سیستم ۳ عضوه با اعمال رأی‌گیری	3V2
سیستم ٤ عضوه با ۲ عضو آماده به کار	D2V2

۷-مراجع

-Bindal, Divya. (2013) "A Review of Markov Model for Estimating Software Reliability." *International Journal of Advanced Research in Computer Science and Software Engineering* 3(6): 426–33.

-Dubrova, Elena. (2013) *Fault Tolerant Design : An Introduction*. 1st ed.

-Isermann, Rolf. (2005) *Fault-Diagnosis Systems*.

-Koren, Israel, and C. Mani Krishna. (2007) *FAULT TOLERANT SYSTEMS*. Denise Penrose.

Kuang, Changhong, Hongxia Song, Yusong Wang, and Lifeng Wang. (2008) "System, -Analysis of Reliability and Security of a Type of VC of the ATP. *Industrial control computer* 21(1). [Chinese Language]

-Morant, Amparo and Gustafson, Anna and Söderholm, Peter and Larsson-Kråik, Per-Olof and Kumar, Uday (2016). Safety and Availability Evaluation of Railway Operation Based on the State of Signalling Systems. Proceedings of the Institution of Mechanical Engineers, Part F: *Journal of Rail and Rapid Transit*.

-Nesi, Paolo. (2013). Report of Comparative Analysis of Interlocking Systems. *Rapporto Di Analisi Comparata Di Sistemi Di Report of Comparative Analysis of Interlocking Systems*. 0–59.

-Pukite, Jan, and Paul. Pukite. (1998). *Modeling for Reliability Analysis : Markov Modeling for Reliability, Maintainability, Safety, and Supportability Analyses of Complex Computer Systems*. IEEE Press.

-Yuc, Qiang & and Xu, Hongze. (2004). Computer-Interlocking System of 2 out of 2 Multiplying 2 Redundancy and Its Security Analysis. 5292–96.

-Rástočný, Karol, Jiří Zahradník, and Aleš Janota. (2000). Quantitative Approach to Safety Assessment of the Railway Interlocking System. *2nd International Workshop on Computer Science and Information Technologies CSIT'2000*. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.22.7027.

-Su, H., and J. Wen (2014). Reliability and Safety Analysis on Railway Signal Regional Computer Interlocking System. *International Journal of Safety and Security Engineering* 4(4): 315–28.

-Theeg, Gregor, and Sergej Vlasenko (2009). *Railway Signaling and Interlocking*. Eurail press.

-Wang, Wei. (2011). Rail Transit Computer Platform Reliability and Availability Analysis. *Modern Urban Rail Transit* 4, 93–95. [Chinese Language]

-Zhou, Chen, and Ni Ming. (2012). Reliability and Security Analysis of 3-Module Redundancy System Based on Common Mode Fault. 21–27.

-Zhou, Yaoming, Chenghao Lin, Yaolong Liu, and Hongzhe Xu. (2018). Analytical Study on the Reliability of Redundancy Architecture for Flight Control Computer Based on Homogeneous Markov Process. *IEEE Access* 6: 18290–98.

Analysis & Comparative Study of Reliability & Safety for Various Redundant Computerized Interlocking Systems Based on Continues-time Markov Chains Approach

Mohammad Ali Sandidzadeh, Associate Professor, School of Railway Engineering, Iran University of Science & Technology (IUST), Tehran, Iran.

Masoud Mohammad Karimi, M.Sc., Grad., School of Railway Engineering, Iran University of Science & Technology (IUST), Tehran, Iran.

E-mail: sandidzadeh@iust.ac.ir

Received: February 2024- Accepted: June 2024

ABSTRACT

Interlocking as a heart of railway signaling system is an important part of this safety-critical system. Looking at the interlocking tasks including correct routing, locking the routes and releasing them timely and commanding to wayside equipment, including signals, point machines and track circuits, will be revealed due to the critical nature of these tasks, interlocking necessarily must have a high tolerance against different probable faults. The best way to design a fault tolerant system is redundancy in processors. Structures with 2 processor units (dual hot stand-by), 3 processor units (3-vote-2 redundancy) and 4 processor units (double 2-vote-2 redundancy) are the most practical techniques which manufacturers have used in the interlocking systems. These redundancies improve reliability, safety and fault tolerancy of system. Each structure has its own advantage. In the Markov method by considering the different states of processors and failure rate, system state diagram is obtained. Then the system transitions between the various operating modes can be expressed by a matrix. The state transition equations formed the behavior of the system to fully assess the safety, reliability and mean time to failure of interlocking system to quantify these indexes. In this article we evaluate and compare the reliability and safety of mentioned structures and study the impact of system parameters (such as failure rate and coverage factor) on the dependability property. We showed that the increasing of coverage factor can straightly improve the safety and also reliability of the system, in addition the control strategy of switch in the hardware of redundant interlocking system is very important in the dependability of this system.

Keywords: Redundancy, Safety, Reliability, Fault-tolerant, Interlocking