

# بررسی سطوح تمامیت ایمنی با استفاده از درخت خطای فازی (مطالعه موردی در صنعت ریلی)

هستی جعفری ، دانش آموخته کارشناسی ارشد، دانشکده مهندسی راه آهن، دانشگاه علم و صنعت، تهران، ایران

محمدعلی صندیدزاده (مسئول مکاتبات)، دانشیار، دانشکده مهندسی راه آهن، دانشگاه علم و صنعت، تهران، ایران

کیوان قصیری، استادیار، دانشکده مهندسی راه آهن، دانشگاه علم و صنعت، تهران، ایران

امیر قوی بازو، دانش آموخته کارشناسی ارشد، دانشکده مهندسی راه آهن، دانشگاه علم و صنعت، تهران، ایران

E-mail: jafarihasti@yahoo.com

دریافت: ۱۳۹۴/۰۷/۲۰ پذیرش: ۱۳۹۵/۰۴/۲۰

## چکیده

مسئله ایمنی در همه محیط های کاری امری بسیار مهم و ضروری است. صنعت همیشه با این معضل روبروست که چگونه سطح تمامیت ایمنی مورد نیاز برای سیستم های ایمنی خود را تعیین نماید. هدف از انجام این مطالعه تعیین سطح تمامیت ایمنی در شرایط عدم قطعیت با استفاده از استاندارد IEC 61508 است. در ابتدا به بررسی مفهوم شاخص سطوح تمامیت ایمنی با استفاده از دیدگاه استاندارد IEC 61508 پرداخته می شود و باتوجه به وجود عدم قطعیت در مراحل مختلف فرآیند اندازه گیری، به در نظر گرفتن عدم قطعیت در پارامترهای ورودی مساله و به محاسبه کمی شاخص در شرایط عدم قطعیت پرداخته ایم. جهت تعیین خطای سیستم از درخت خطای فازی استفاده شده است و با تعیین میزان تعلق سیستم ایمنی به هر یک از سطوح تمامیت ایمنی در محیط فازی، سطح تمامیت ایمنی سیستم تعیین می شود. استفاده از رویکرد فازی باعث می شود که بتوان میزان تعلق سیستم را به هر یک از سطوح ایمنی با دقت بیشتری تعیین نمود. در این مقاله، سیستم ترمز قطار به عنوان مطالعه موردی بررسی شده است و نتایج، نشان دهنده دقت بیشتر در تعیین سطوح تمامیت ایمنی سیستم است.

واژه های کلیدی: استاندارد IEC 61508، تئوری فازی، درخت خطا، سطح تمامیت ایمنی، سیستم های ایمنی.

## ۱. مقدمه

ریسک، ماتریس شدت خطرات و بررسی عواقب به عنوان روش‌هایی جهت تعیین سطح ریسک هدف برای سیستم‌های ایمنی (SIS) معرفی شد [Summers, 1998].

در سال ۲۰۰۳ در دو مطالعه مجزا از روش مارکوف جهت تعیین SIL سیستم‌های ایمنی تعمیرپذیر، استفاده شد و بیان گردید که استفاده از این متدولوژی برای ارزیابی این‌گونه از سیستم‌ها، باعث بروز خطا در محاسبات و در نتیجه اشتباه در نتایج خواهد شد [Simpson, 2003]. این مسئله در مطالعه دیگری مورد نقد قرار گرفت و رد شد [Bukowski, 2005]. در سال ۲۰۰۴ تجارت پیاده‌سازی استاندارد IEC61508 در کتابی منتشر شد. [Smith and Simpson, 2004] در مطالعه‌ای به تعیین SIL سیستم‌های ایمنی در حالتی که زمان تعمیرات دارای توزیع احتمالی‌نمایی نیست، پرداخته شده است [Bukowski, 2006]. در مطالعه‌ای توسط [Guo and Yang, 2007] با استفاده از متدولوژی بلوک دیاگرام قابلیت اطمینان (RBD) به تحلیل سطح ایمنی سیستم‌های ایمنی پرداخته شده است.

در مطالعه‌ای ضمن معرفی روش مارکوف به عنوان روشی مناسب در تحلیل و اندازه‌گیری سطح تمامیت ایمنی یک سیستم اقدام به معرفی روش‌های تشخیص سیستم‌های پرتقاضا و کم تقاضا با استفاده از مقایسه نرخ خرابی و مدت زمان آن در سیستم‌های ایمنی پرداخته شده است [Sato, 2007]. در مطالعه دیگری به ارائه ماتریس ریسک فازی پرداخته شده است [Markowski Mannan and, 2008].

همچنین در این سال مطالب بسیاری در مورد استفاده از تئوری فازی در آنالیز ریسک نیز مطرح گردید که از آن جمله می‌توان به [Lee and Chen, 2008] اشاره نمود.

پیشرفت‌های اخیر در عرصه تکنولوژی و پیچیده‌تر شدن سیستم‌ها، باعث می‌شود تا شناخت و تحلیل سیستم‌ها و تعیین ایمنی آنها امری دشوار و حتی در برخی شرایط غیرممکن باشد. از طرفی گسترش بیش از پیش استفاده از این سیستم‌ها باعث می‌شود تا حصول اطمینان از ایمنی آنها امری الزامی گردد.

موارد فوق به همراه حوادث و فجایع صنعتی رخ داده در طول سالهای اخیر در سراسر جهان باعث ایجاد تغییرات شگرفی در رویکرد متخصصین به ایمنی شده است. مانند تغییر از این عقیده که سیستم‌ها فقط می‌توانند ایمن و یا نا ایمن باشند (نگاه به ایمنی سیستم‌ها به صورت صفر و یک)، به این عقیده که سطح ایمنی به صورت یک طیف بوده که سیستم‌های مختلف می‌توانند در قسمت‌های مختلف این طیف قرار گیرند [Redmill, 2000]. در این راستا در سالهای اخیر اقدامات بسیار گسترده‌ای صورت گرفته و استانداردهای مختلفی در این زمینه طراحی و تدوین شده است. از جمله این استانداردها می‌توان به استاندارد بین‌المللی ۶۱۵۰۸ IEC و دیگر استانداردها که از این استاندارد مشتق شده‌اند، اشاره نمود. در سال ۱۹۹۴ با ترکیب تئوری فازی و آنالیز درخت خطا سعی شده تا عدم قطعیت مربوط به پارامترهای مسئله در مدل در نظر گرفته شوند [Weber, 1994]. در سال ۱۹۹۵ از روش مارکوف جهت ارزیابی قابلیت اطمینان سیستم‌های ایمنی به عنوان معیاری جهت سنجش سطح ایمنی این سیستم‌ها استفاده نمودند و مفهوم جدیدی با عنوان احتمال بروز خطا در هنگام تقاضا را معرفی کردند. این مفهوم در دو استاندارد IEC ۶۱۵۰۸ و ISAS ۸۴،۰۱ نیز مطرح گردید و مورد استفاده قرار گرفت [Bukowski and Gobl, 1995] و در مطالعه‌ای با توجه به پیش‌نویس استاندارد IEC ۶۱۵۰۸ اقدام به تشریح روش‌های کلی تعیین SIL هدف برای یک سیستم ایمنی (SIS) شد. در این مطالعه روش‌های گراف

و ضروری به نظر می‌رسد. از سویی با توجه به اینکه خسارات جانی و مالی ناشی از بروز سوانح ریلی بسیار قابل توجه است، بنابراین طراحی دقیق تجهیزات مورد استفاده در بخش های مختلف و بویژه قطارها امری ضروری است. در این مطالعه ابتدا به بررسی SIL سیستمها از دیدگاه استاندارد IEC61508 پرداخته شده است و سپس با توجه به وجود عدم قطعیت در مراحل مختلف فرآیند اندازه‌گیری این شاخص، به محاسبه آن در شرایط عدم قطعیت پرداخته ایم. وجود عدم قطعیت در فرآیند اندازه‌گیری، باعث افزایش ریسک در محاسبات خواهد شد و این عامل پژوهشگران را وادار به طراحی سیستم‌های ایمنی با ضریب ایمنی بسیار بالاتر از سطح مورد نیاز واقعی خواهد نمود که این مسئله باعث افزایش قابل توجه هزینه‌ها در پیاده سازی سیستم ایمنی می‌گردد. بنابراین محاسبه شاخص SIL به صورت فازی لازم و ضروری است. بنابراین با استفاده از مطالعه موردی در سیستم مخزن فشار به اندازه‌گیری کمی شاخص SIL در شرایطی که پارامترهای ورودی مدل غیرقطعی است، پرداخته شده است. همچنین این امکان ایجاد شده است که شاخص SIL در استاندارد IEC 61508 به صورت فازی بیان شود و میزان تعلق یک سیستم ایمنی به هر سطح از SIL تعیین گردد.

## ۲. مفهوم SIL

به طور کلی شاخص SIL به دو روش زیر تعریف می‌گردد [Redmill, 2000]

با استفاده از میزان کاهش در احتمال بروز خطر یک سیستم/فرآیند که در نتیجه استفاده از یک سیستم ایمنی (SIS) رخ می‌دهد می‌توان شاخص SIL را محاسبه نمود.

تعیین احتمال شکست یک سیستم ایمنی (SIS) در انجام موفقیت آمیز فعالیت/فرآیند مربوطه در هنگام وجود تقاضا روش دیگری

[Wenjin, 2012] با استفاده تکنولوژی تشخیص سطح تمامیت ایمنی به تعیین درجه IL مورد نیاز در قطارهای پرسرعت پرداخت. در مطالعه ای توسط [Shu and Zhao, 2014] رویکرد ساده شده ای از روش مارکوف بروی سیستم های ایمنی ارائه شده است. در سالهای اخیر مطالعات بسیاری در خصوص استفاده از روش درخت خطای فازی در سیستم های ایمنی انجام شده است که از آن جمله میتوان به [Komal, 2015] و [Liu, et al. 2015] و [Lavasani, et. al, 2015]. [Purba, et al. 2015]. [Rezvan and Jafarian, 2012], اشاره نمود. در مطالعه‌ای با استفاده از روش درخت خطا به بررسی عوامل و اثرات خروج از خط قطارهای مسافری پرداخته شد و به دلیل عدم قطعیت در داده ها از رویکرد فازی استفاده گردید [Rezvani and Jafarian, 2012].

Komal در سال ۲۰۱۵ به ارائه مدل ریسک در مراقبتهای بهداشتی پرداخته است و با استفاده از درخت خطای فازی، اعداد فازی دوزنقه‌ای، برش  $\alpha$  و کوچک‌ترین نرم T به محاسبه تقریبی احتمال خطای نهایی در درخت خطای فازی پرداخت [Komal, 2015].

در مطالعه [Liu, et al. 2015] با استفاده از ترکیب روشهای تحلیل درخت خطا و تحلیل کمی به بررسی تصادفات در حمل و نقل ریلی سریع السیر پرداخته شده است و با توجه به عدم دسترسی به اطلاعات و پیچیدگی محیط تصمیم‌گیری از رویکرد تئوری فازی استفاده شده است. در همین سال Lavasani به ارائه آنالیز درخت خطای فازی به منظور تحلیل ریسک چاه های نفت و گاز طبیعی پرداخت.

با توجه به کلیه مطالب فوق، اهمیت مفهوم ایمنی و تحلیل وقایع با استفاده از روشهایی مانند درخت خطا با گذشت زمان بیشتر شده و بنابراین توجه بیشتری به این زمینه نشان می‌دهند. بنابراین انجام مطالعات بیشتر در کشور و تلاش برای بومی سازی این مفهوم لازم

-ایجاد مدلی ریاضی از وجوه شناخته شده و ناشناخته سیستم برای تشریح نحوه ارتباط پارامترهای سیستم به صورت کمی و ریاضی تبدیل اطلاعات و داده‌های واقعی به پارامترها و اطلاعات ورودی سیستم

-حل مدل ریاضی برای به دست آوردن نتایج مورد نظر با استفاده از پارامترهای ورودی

تمامی این مراحل می‌توانند باعث ایجاد عدم قطعیت در نتیجه نهایی گردند، بنابراین نیازمند مدلسازی عدم قطعیت است. در ادامه به ضرورت ارائه مدل در محیط فازی پرداخته می‌شود.

#### ۴. لزوم استفاده از تئوری فازی

همان‌گونه که در بخش‌های قبلی بیان شد، داده‌های ورودی آنالیز قابلیت اطمینان در سیستم‌ها به دو روش کلی زیر جمع‌آوری می‌شود:

جمع‌آوری داده‌های شکست و خرابی زیر مجموعه‌ها در هنگام فعالیت سیستم.

جمع‌آوری اطلاعات مربوط به نرخ خرابی اجزاء از طریق بانک‌های اطلاعاتی جامعی که در این زمینه ایجاد شده و نرخ خرابی انواع اجزاء استاندارد به کار برده شده در سیستم‌ها را (غالباً) به صورت مقدار متوسط و حد بالا و پایین ارائه می‌کند. در برخی دیگر از این بانک‌های اطلاعاتی نیز داده‌ها به همراه نرخ خطای آنها ارائه می‌شود.

استفاده از هر یک از روش‌های فوق برای جمع‌آوری داده‌های ورودی مدل همراه با عدم قطعیت است.

برای محاسبه‌ی شاخص SIL است. در استاندارد IEC61508. شاخص SIL به چهار سطح تقسیم شده و به هر سطح از این شاخص بازه‌ای از احتمالات تخصیص داده شده است. این احتمالات بیانگر میانگین احتمال بروز خطا در سیستم ایمنی (SIS) در هنگام وجود تقاضا برای انجام فعالیت/فرآیند تخصیص داده شده به آن است که به آن میانگین نرخ خطای احتمالی در زمان تقاضا (PFD) نیز گفته می‌شود. [IEC61508 Standard, 1999]. در این استاندارد سیستم‌های ایمنی به دو دسته کم تقاضا و پرتقاضا تقسیم‌بندی شده است.

سیستم‌های کم تقاضا: سیستم‌هایی که فرکانس تقاضای آنها کمتر از یک بار در سال و همچنین کمتر از دو برابر فرکانس انجام تست اطمینان آنها نباشد. برای مثال می‌توان به سیستم کیسه هوای خودرو و یا ترمز اضطراری قطار اشاره نمود. [IEC61508 Standard, 1999].

سیستم‌های پرتقاضا: سیستم‌هایی که فرکانس تقاضای آنها بیش از یکبار در سال و یا کمتر از دو برابر فرکانس تست اطمینان آنها باشد. برای مثال می‌توان به سیستم ترمز معمولی و یا اینترلاکینگ اشاره کرد [IEC61508 Standard, 1999].

سطح بندی و احتمالات تخصیص داده شده به شاخص SIL در هنگام بروز خطا در جدول زیر که برگرفته از استاندارد IEC61508 است، نمایش داده ایم:

#### ۳. عدم قطعیت در محاسبات مربوط به شاخص SIL

به طوری کلی برای کمی کردن مفاهیمی همچون شاخص SIL لازم است گام‌های زیر برداشته شود:

جدول ۱. احتمال بروز خطا به تفکیک سیستم های کم تقاضا و پرتقاضا متناظر با سطوح SIL

سطح تمامیت ایمنی	سیستم پر تقاضا (خرابی خطرناک در هر ساعت)	سیستم کم تقاضا (احتمال بروز خطا در هنگام تقاضا)
۴	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
۳	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
۲	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
۱	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

ترکیب تئوری فازی با روش های سنتی آنالیز SIL مانند آنالیز گراف ریسک فازی.

لیکن روش اول که با استفاده از شبیه سازی به آنالیز عدم قطعیت های موجود در مدل می پردازد توسط برخی بنابراین همچون Sallak et al. [2008] زیر سوال برده شده است. زیرا که برای استفاده از این روش نیاز به اطلاعات کافی در مورد تابع احتمال خرابی هر یک از اجزاء است که با توجه به موارد بیان شده این امر امکان پذیر نیست. این مسئله باعث شده تا در سال های اخیر پژوهشگران به استفاده از روش دوم یعنی استفاده از تئوری فازی در مطالعات خود روی آورند. به صورت سنتی و در مدل های قدیمی با کلیه عدم قطعیت های موجود در سیستم به صورت محافظه کارانه برخورد می گردید. به این صورت که کلیه پارامتر هایی که امکان تعیین مقادیر آنها به صورت قطعی وجود نداشت در بدترین حالت اندازه گیری و استفاده می شدند. این مسئله باعث گردیده تا هزینه های مربوط به طراحی و پیاده سازی سیستم های ایمنی به شدت افزایش یابد. با توجه به این مسئله، به کارگیری مدل هایی که قابلیت در نظر گرفتن عدم قطعیت های موجود در مراحل مختلف مدل سازی سیستم را دارا باشد، الزامی به نظر می رسد.

برخی بانکهای اطلاعاتی اقدام به ارائه نرخ شکست اجزاء به همراه میزان خطای احتمالی آنها و یا حد بالا و پایین آنها نموده اند. این

در روش اول با توجه به اینکه نرخ خرابی سیستم ها به ویژه سیستم های ایمنی بسیار کوچک است ( $< 10^{-4}$ ) و همچنین تعداد ساعات کاربرد آنها نیز کمتر از باقی سیستم های کاربردی موجود در شبکه بوده و فقط در موارد وجود تقاضا وارد عمل می شوند، بنابراین امکان جمع آوری اطلاعات کافی در مورد نرخ شکست آنها (به مقداری که بتوان از قاعده اعداد بزرگ در علم احتمال استفاده نمود) بسیار کم و تاحدی غیرممکن است و محاسبه نرخ خطا یک جزء از سیستم با توجه به اطلاعات جمع آوری شده از عملکرد سیستم قطعیت دقت بسیار کمی خواهد داشت [Sallak et al. 2008].

در روش دوم نیز با توجه به اینکه اعداد ارائه شده در شرایط آزمایشگاهی به دست آمده اند بنابراین استفاده از سیستم در محیط های مختلف موجب انحراف نرخ واقعی خرابی از نرخ خرابی ارائه شده در این بانکهای اطلاعاتی خواهد شد. بنابراین تهیه کنندگان این بانکهای اطلاعاتی، اقدام به ارائه حدود بالا و پایین نرخ خرابی اجزاء نموده اند [Sallak et al. 2008].

با توجه به موارد فوق استفاده از روشی که بتواند عدم قطعیت های موجود در این پارامترها را در نظر بگیرد الزامی به نظر می رسد. پژوهشگران برای انجام این امر از دو روش مختلف استفاده نموده اند. ترکیب شبیه سازی با روش های سنتی آنالیز SIL مانند روش آنالیز پیشرفته مارکوف.

می‌کند، مشخص می‌شود و آنرا می‌توان با یک مجموعه از زوج‌های مرتب  $X$  و مقدار تعلق آن همانگونه که در فرمول ۱ نشان داده شده، نمایش داد.

$$A = \{(x, u_A(x)) | x \in U\} \quad (1)$$

### ۲-۵ برش آلفا

برش آلفای یک مجموعه فازی  $A$  یک مجموعه غیر فازی  $A_\alpha$  است که شامل تمامی عضوهای  $U$  است که مقادیر تعلق بزرگ‌تر از  $\alpha$  دارند.

$$A_\alpha = \{x \in U | u_A(x) \geq \alpha\} \quad (2)$$

### ۳-۵ جمع و تفریق و ضرب اعداد فازی

#### روش برش آلفا

فرض کنید  $A$  و  $B$  دو عدد فازی بوده و برشهای آلفا آنها به صورت  $A_\alpha = [a_\alpha^-, a_\alpha^+]$  و  $B_\alpha = [b_\alpha^-, b_\alpha^+]$  باشند. آنگاه جمع  $A$  و  $B$ ،  $A+B$  یک عدد فازی است که برشهای آلفای آن به صورت زیر تعریف می‌شود.

$$(A+B)_\alpha = [a_\alpha^- + b_\alpha^-, a_\alpha^+ + b_\alpha^+] | \alpha \in [0,1] \quad (3)$$

از آنجائی که یک مجموعه فازی کاملاً توسط برشهای آلفا خود تعیین می‌شود، بنابراین عدد فازی  $A+B$  نیز در فرمول ۳ به خوبی تعریف شده است.

به طور مشابه تفاضل  $A$  و  $B$ ،  $A-b$ ، یک عدد فازی است که برش آلفا آن توسط رابطه زیر تعریف می‌گردد:

مسئله فرصت بسیار خوبی در اختیار قرار می‌دهد تا با ترکیب مدل‌های قطعی کمی رویکرد احتمال فازی اقدام به ارائه مدلی نمود که علاوه بر تعیین احتمال خطای سیستم ایمنی، در هنگام تقاضا، میزان قطعیت آن را نیز تعیین نماید.

در این پروژه سعی شده تا با ارائه مدلی در محیط فازی، عدم قطعیت‌های موجود در انتخاب و تعیین پارامترهای ورودی در نظر گرفته شود.

با استفاده از روش فازی می‌توان از اتلاف هزینه مربوط به طراحی سیستم‌های ایمنی (به دلیلی بیش از حد ایمن بودن آنها) بر اساس نتایج روش‌های آنالیز قطعی به صورت گسترده‌ای جلوگیری نمود زیرا که در روش‌های سنتی دیدگاه بنابراین بر این اساس بود که وجود عدم قطعیت در پارامترها و مدل باعث افزایش ریسک خواهد شد و بنابراین اقدام به طراحی سیستم‌های ایمنی با ضریب ایمنی بسیار بالاتر از سطح مورد نیاز واقعی می‌نمودند که این مسئله باعث افزایش قابل توجه هزینه‌ها در پیاده سازی سیستم ایمنی می‌گردید.

به این سبب در این مطالعه به ارائه مدلی جدید از آنالیز درخت خطا در محیط فازی با استفاده از مطالعه موردی پرداخته شده است تا بتوان علاوه بر به دست آوردن نرخ خطای سیستم به صورت کمی به همراه میزان قطعیت آن، میزان تعلق سیستم به هر یک از سطوح SIL را تعیین نماییم. در ادامه به بیان برخی از مفاهیم فازی می‌پردازیم.

## ۵. مفاهیم فازی

### ۱-۵ مجموعه‌های فازی

یک مجموعه فازی  $A$  در فضای جهانی  $U$  به وسیله یک تابع  $u_A(X)$  که تابع تعلق نام داشته و مقادیری در بازه  $[0,1]$  اختیار

$$(A - B)_\alpha = [\min(a_\alpha^- - b_\alpha^-, a_\alpha^+ - b_\alpha^+), \max(a_\alpha^- - b_\alpha^-, a_\alpha^+ - b_\alpha^+)] \mid \alpha \in [0,1] \quad (4)$$

$$(A.B)_\alpha = [\min(a_\alpha^- . b_\alpha^-, a_\alpha^+ . b_\alpha^+), \max(a_\alpha^- . b_\alpha^-, a_\alpha^+ . b_\alpha^+)] \mid \alpha \in [0,1] \quad (6)$$

i. هرگاه نماد منطقی مربوط به حادثه ای از نوع OR باشد فهرست جداگانه ای از ورودی‌ها شامل حادثه‌های مبنا و نمادها تنظیم می‌شود.

ii. هرگاه نماد منطقی مربوط به حادثه از نوع AND باشد، فهرست مشترکی از ورودی‌ها شامل حادثه‌های مبنا و نمادها تنظیم می‌شود.

iii. عملیات فوق تا حصول فهرستی که صرفا شامل حادثه‌های مبنا باشد، ادامه می‌یابد. همه ردیفهایی که غیرتکراری نیست حذف می‌شود و به این ترتیب مجموعه‌های انقطاع به دست می‌آید.

با به دست آوردن مجموعه‌های انقطاع و جمع احتمال رخداد هریک از آنها می‌توان احتمال رخداد حادثه نهایی را محاسبه نمود.

#### ۱-۶ آنالیز SIL با استفاده از درخت خطای فازی:

در این روش گامهای زیر برای به دست آوردن نرخ خطای سیستم از طریق درخت خطای فازی طی خواهد شد:

- I. تهیه درخت خطای سیستم
- II. تهیه تابع تعلق مربوط به نرخ خطای هر یک از اجزاء سیستم.
- III. تهیه کوچکترین مجموعه‌های انقطاع غیر تکراری برای درخت خطای به دست آمده
- IV. انجام محاسبات بر روی اعداد فازی مربوط به هر یک از اجزاء موجود در مجموعه‌های انقطاع غیر تکراری

هر مجموعه فازی می‌تواند به صورت منحصر به فرد با برش آلفا خود به شکل زیر نشان داده شود.

$$A_\alpha = [A_\alpha^-, A_\alpha^+] \quad (5)$$

فرض کنید  $A$  و  $B$  دو عدد فازی بوده و برشهای آلفا آنها به صورت  $A_\alpha = [a_\alpha^-, a_\alpha^+]$  و  $B_\alpha = [b_\alpha^-, b_\alpha^+]$  باشند. آنگاه ضرب  $A$  و  $B$ ، یک عدد فازی است که برشهای آلفای آن به وسیله فرمول (۶) تعریف می‌شود.

#### ۳-۵ عدد فازی مثلثی

عدد فازی مثلثی یک مجموعه فازی در  $R$  با تابع تعلق مثلثی است که به شکل زیر نمایش داده می‌شود:

(۷)

$$u_A(x) = u_A(x; a, b, c) = \begin{cases} (x-a)/(b-a) : a \leq x < b \\ (c-x)/(c-b) : b \leq x \leq c \\ 0 : x > c \end{cases}$$

#### ۶. آنالیز درخت خطا

شیوه درخت خطا از اولین شیوه‌های ارزیابی قابلیت اطمینان است که به ویژه برای تحلیل سیستم با عضوهای آماده به کار، سیستم ایمنی و سیستم‌های ویژه ماموریت مورد استفاده قرار می‌گیرد.

بررسی کمی احتمال حادثه نهایی در درخت خطا با استفاده از روش کوچکترین مجموعه‌های انقطاع غیر تکراری انجام می‌شود. در این شیوه از حادثه نهایی در درخت معایب شروع کرده و گام‌های زیر طی می‌شود.

در این مثال منبع تغذیه صرفاً می‌تواند در مُد ایمن (قطع شدن تغذیه) خراب شود. برای هر یک از اجزاء نرخ خرابی به تفکیک مُد ایمن و خطرناک داده شده است و به شکل فرمول ۸ نمایش داده می‌شود:

مد خراب  
 $\lambda$   
جز

(۸)

در قسمت نام اجزاء از اسامی مخفف مربوط به هر یک از اجزاء استفاده می‌شود و به جای مد خرابی از مخفف اسم هر یک از مدها (برای مثال: S برای مُد ایمن، D برای مُد خطرناک و CC برای مُد خرابی مشترک) استفاده می‌گردد. کلیه خرابی‌ها به غیر از خرابی دو عضو موازی به دلیل وجود مُد خرابی مشترک، مستقل از هم تصور شده‌اند.

#### ۷-۱ فرضیات مدل ارائه شده

در این مطالعه تابع تعلق مربوط به نرخ خطای هر یک از اجزاء به صورت یک عدد فازی مثلثی در نظر گرفته می‌شود. با توجه به موارد بیان شده در مورد نرخ خطای ارائه شده در بانک‌های اطلاعاتی استاندارد و اینکه نرخ خطای هر یک از اجزاء به صورت یک عدد میانگین و حد بالا و پایین ارائه شده است از اعداد فازی مثلثی استفاده می‌کنیم.

در این مدل برای انجام محاسبات بر روی اعداد فازی از روش برش آلفا استفاده شده است.

#### ۷-۲ نحوه پیاده سازی مدل

برای پیاده سازی مدل ابتدا به ترسیم درخت خطای سیستم می‌پردازیم.

V. برای به دست آوردن تابع تعلق نرخ خطای سیستم در هنگام تقاضا

VI. تعیین تابع تعلق هر یک از سطوح تمامیت ایمنی

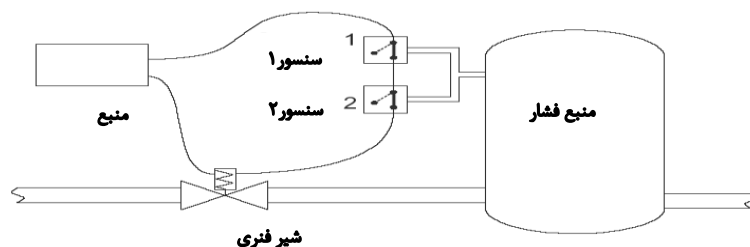
VII. محاسبه سطح تمامیت ایمنی سیستم و میزان قطعیت آن

#### ۷. مطالعه موردی

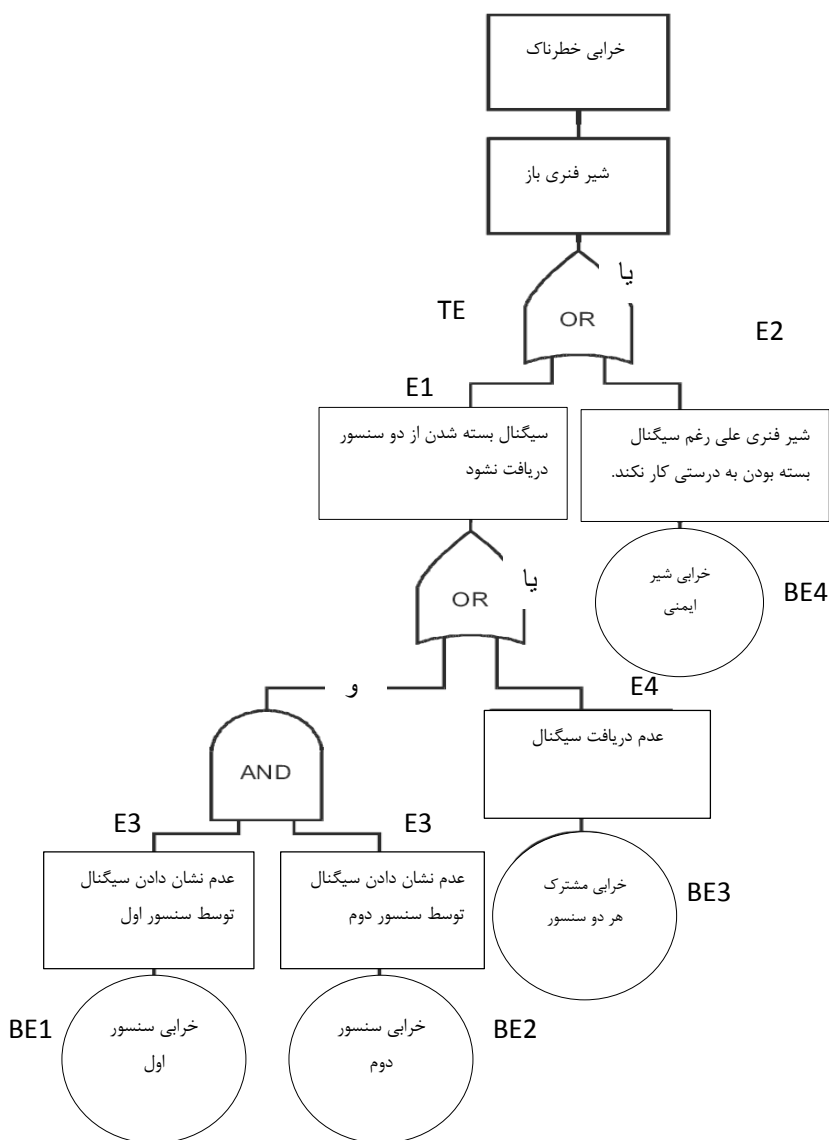
در مطالعه موردی حاضر سطوح تمامیت ایمنی در محیط فازی برای مخزن فشاری که در سیستم ترمز قطار مورد استفاده قرار می‌گیرد، تعیین می‌شود. در ابتدا با استفاده از تعریف نرخ خطاهای سیستم در محیط فازی و با استفاده از درخت خطا به تعیین نرخ خطای نهایی سیستم پرداخته می‌شود. در ادامه به تشریح سیستم مخزن فشار پرداخته شده است. [Bukowski, 2005]

یک مخزن فشار (PV) توسط یک سیستم ایمنی (SIS) در مقابل افزایش بیش از حد فشار محافظت می‌گردد. این سیستم ایمنی (SIS) از یک عدد منبع تغذیه (PS)، دو عدد سنسور فشار کاملاً مشابه (S1 و S2) که در موقع افزایش بیش از حد فشار، منبع تغذیه را قطع می‌نمایند و یک عدد شیر فتری (SV) که در صورت قطع شدن منبع تغذیه، از تغذیه مخزن فشار جلوگیری می‌کند، تشکیل شده است. سنسورها به صورت موازی به یکدیگر متصل شده‌اند، بنابراین در صورت قطع شدن منبع تغذیه توسط حداقل یکی از آنها شیر فتری بسته شده و جلوی تغذیه مخزن فشار را خواهد گرفت. برای انجام بررسی‌ها فرض خواهیم کرد که کلیه اجزاء به غیر از منبع تغذیه دارای دو مُد خرابی هستند: خرابی ایمن و خرابی خطرناک. در صورتی مُد خرابی یک جزء از سیستم خطرناک است که با وجود تقاضا (برای مثال افزایش بیش از حد فشار)، وظیفه خود را انجام ندهد و در صورتی که وظیفه ایمنی خود را انجام داده باشد در حالی که هیچگونه تقاضایی از طرف فرآیند ارسال نشده باشد به آن مُد خرابی ایمن گفته می‌شود.





شکل ۱. سیستم ایمنی کنترل مخزن فشار



شکل ۲. درخت خطای سیستم ایمنی مخزن فشار [Bukowski, 2005]

## بررسی سطوح تمامیت ایمنی با استفاده از درخت خطای فازی (مطالعه موردی در صنعت ریلی)

بنابر تعریف کوچکترین مجموعه‌های انقطاع، با از کار افتادن حداقل یکی از این مجموعه‌ها کل سیستم ایمنی از کار خواهد افتاد، بنابراین برای محاسبه احتمال حادثه نهایی (عدم موفقیت سیستم در انجام فعالیت ایمنی (SF)) از فرمول ۱۰ استفاده می‌شود. از آنجاکه احتمالات به دست آمده برای هر یک از مجموعه‌های انقطاع از نوع اعداد فازی هستند، بنابراین برای محاسبه حادثه نهایی روابط ۱۱ تا ۱۳ را خواهیم داشت. با توجه به فرمول‌های فوق برای برش آلفا نرخ رخداد حادثه نهایی (TE) رابطه ۱۴ را خواهیم داشت. که با قرار دادن اعداد صفر و یک به جای پارامتر آلفا در رابطه ۱۴ می‌توان حد بالا، پایین و مقدار میانگین نرخ رخداد حادثه نهایی و یا همان خطا در زمان وقوع تقاضا (PFDavg) را محاسبه نمود که در جدول ۵ نشان داده شده است.

نرخ خطای هر یک از اجزا در مطالعه ی Bukowski در سال ۲۰۰۵ ارائه شده است که بر این اساس لیست اجزا و نرخ خطای هر یک از آنها در جدول ۲ نشان داده شده است. با توجه به اطلاعات داده شده در مورد نرخ خرابی اجزاء در جدول ۲ و با توجه به اعداد فازی مثلثی برای نمایش نرخ خطای اجزاء، می‌توان با استفاده از فرمول زیر برش آلفا هر یک از اجزاء را به صورت پارامتریک محاسبه کرد. بنابراین با توجه به فرمول فوق برای هر جز از سیستم ایمنی، برش آلفای آن در جدول ۳ نمایش داده شده است. با توجه به درخت خطای سیستم، کوچکترین مجموعه‌های غیر تکراری سیستم ایمنی تعیین و در جدول ۴ مشخص شده است. همچنین احتمال رخ داد آنها با استفاده از روش‌های جمع و ضرب فازی به روش برش آلفا محاسبه و در جدول فوق نشان داده شده است.

جدول ۲. لیست اجزاء سیستم و نرخ خطای هر یک از آنها [Bukowski, 2005]

نام اجزاء سیستم ایمنی	بیشترین نرخ خطای احتمالی $\times 10^{-6}$	میانگین نرخ خطا $\times 10^{-6}$	کمترین نرخ خطای احتمالی $\times 10^{-6}$
خرابی سنسور اول (BE1)	۵۵	۵۰	۴۸
خرابی سنسور دوم (BE2)	۵۵	۵۰	۴۸
خرابی مشترک هر دو سنسور (BE3)	۶,۶	۶	۵,۷
خرابی شیر ایمنی (BE4)	۱۱۰	۱۰۰	۷۰

$$u_A(x) = u_A(x; LL, m, UL) = \begin{cases} (x - LL)/(m - LL) : LL \leq x < m \\ (UL - x)/(UL - m) : m \leq x \leq UL \\ 0 : x > UL, x < LL \end{cases} \quad (9)$$

جدول ۳. برش آلفای اعضا

نام اجزاء سیستم ایمنی	$A^+_{\alpha \times 10^{-6}}$	$A^-_{\alpha \times 10^{-6}}$
خرابی سنسور اول	۵۵-۵۵	۴۸+۲,۵۵
خرابی سنسور دوم	۵۵-۵۵	۴۸+۲,۵۵

جدول ۴. برش آلفای کوچکترین مجموعه های انقطاع غیر تکراری

$A^- \alpha \times 10^{-6}$	$A^+ \alpha \times 10^{-6}$	فرمول احتمال	کوچکترین مجموعه انقطاع
$(\varepsilon 8 + 2, 5 \alpha)^2$	$(55 - 5 \alpha)^2$	$P_{BE1}(t) \times P_{BE2}(t)$	خرابی سنسور اول و سنسور دوم
$5, 7 + 0, 3 \alpha$	$6, 6 - 0, 6 \alpha$	$P_{BE3}(t)$	خرابی مشترک هر دو سنسور
$70 + 30 \alpha$	$110 - 10 \alpha$	$P_{BE4}(t)$	خرابی شیر ایمنی
$5, 7 + 0, 3 \alpha$	$6, 6 - 0, 6 \alpha$		خرابی مشترک هر دو سنسور
$70 + 30 \alpha$	$110 - 10 \alpha$		خرابی شیر ایمنی

$$P_{TE}^D(t) = P_{BE3}^D(t) + P_{BE1}^D(t)P_{BE2}^D(t) + P_{BE4}^D(t) \quad (10)$$

$$(P_{TE}^D(t))_{\alpha}^+ = (P_{BE3}^D(t))_{\alpha}^+ + (P_{BE1BE2}^D(t))_{\alpha}^+ + (P_{BE4}^D(t))_{\alpha}^+ \quad (11)$$

$$(P_{TE}^D(t))_{\alpha}^- = (P_{BE3}^D(t))_{\alpha}^- + (P_{BE1BE2}^D(t))_{\alpha}^- + (P_{BE4}^D(t))_{\alpha}^- \quad (12)$$

$$(P_{TE}^D(t))_{\alpha} = [(P_{TE}^D(t))_{\alpha}^-, (P_{TE}^D(t))_{\alpha}^+] \quad (13)$$

$$(P_{TE}^D(t))_{\alpha} = [7.6 \times 10^{-4} + 1.1 \times 10^{-4} \alpha + 6.3 \times 10^{-10} \alpha^2, 1.2 \times 10^{-3} - 1.1 \times 10^{-4} \alpha + 2.5 \times 10^{-9} \alpha^2] \quad \alpha \in [0, 1] \quad (14)$$

جدول ۵. حدود بالا و پایین و میانگین نرخ خطای سیستم

کمترین نرخ خطای احتمالی (LL) $\times 10^{-6}$	میانگین نرخ خطا (m) $\times 10^{-6}$	بیشترین نرخ خطای احتمالی (UL) $\times 10^{-6}$
۷۵	۱۰۶	۱۱۶

نرخ رخداد حادثه نهایی (خرابی سیستم ایمنی)

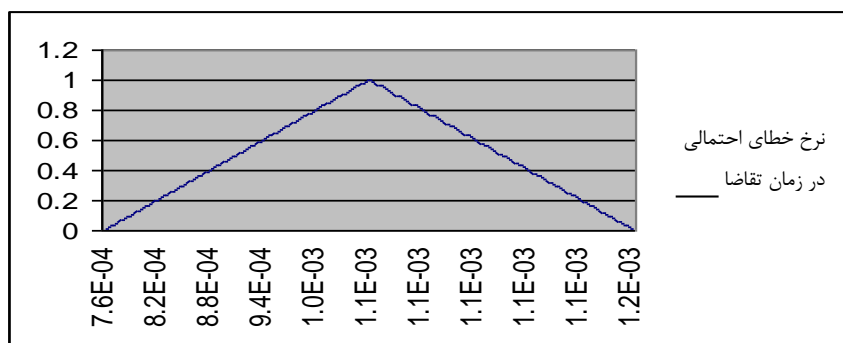
### ۳-۷ تعریف شاخص SIL در محیط فازی

برای اینکه بتوان اعداد فازی به دست آمده از آنالیز درخت خطای فازی را با بازه‌های مربوط به SIL مقایسه نمود لازم است تا این بازه‌ها را در محیط فازی تعریف نمود. برای انجام این کار هر سطوح آن به صورت یک عدد فازی دوزنقه ای نرمال که دارای تابع تعلق زیر است تعریف می شود.

تابع تعلق نرخ خطای سیستم به صورت زیر محاسبه می شود. همچنین شکل تابع تعلق به دست آمده برای نرخ خطای سیستم ایمنی در زمان وقوع تقاضا در نمودار ۳ نشان داده شده است. همانگونه که مشاهده می شود نرخ خطای سیستم از  $75 \times 10^{-6}$  تا  $116 \times 10^{-6}$  در حال تغییر است که با مقایسه اعداد به دست آمده با بازه‌های SIL مشخص می شود که این سیستم به طور همزمان به دو بازه سطح ۲ و ۳ تعلق دارد. در قسمت بعد میزان تعلق این سیستم به هر یک از این دو بازه را محاسبه خواهیم نمود.

بررسی سطوح تمامیت ایمنی با استفاده از درخت خطای فازی (مطالعه موردی در صنعت ریلی)

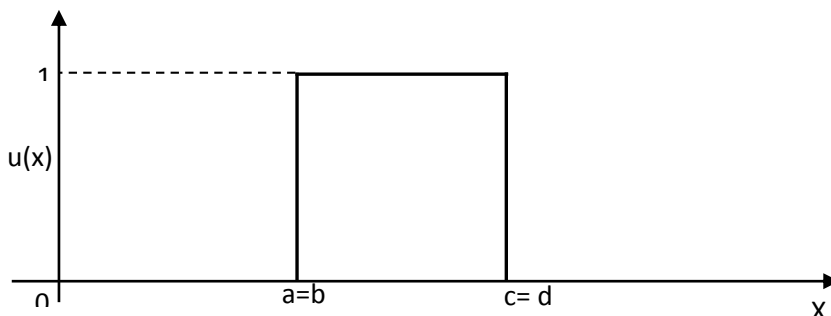
$$u_{p(TE)}(x) = \begin{cases} \frac{-1.1 \times 10^{-4} + \sqrt{1.21 \times 10^{-8} - 2.52 \times 10^{-10}(7.6 \times 10^{-4} - y)}}{14 \times 10^{-16}} & 75 \times 10^{-5} < x \leq 106 \times 10^{-5} \\ \frac{1.1 \times 10^{-4} - \sqrt{1.21 \times 10^{-8} - 1 \times 10^{-8}(1.2 \times 10^{-3} - y)}}{4 \times 10^{-16}} & 106 \times 10^{-5} < x \leq 116 \times 10^{-5} \\ 0, & x < 75 \times 10^{-5}, x > 116 \times 10^{-5} \end{cases} \quad (15)$$



شکل ۳. تابع تعلق نرخ خطای کل سیستم

$$u_{SIL}(x) = u_{SIL}(x; a, b, c, d) = \begin{cases} 0: a \leq x < b \\ 1: b \leq x \leq c \\ 0: c < x \leq d \\ 0: x > d, \quad x < a \end{cases} \quad (16)$$

$$a = b, \quad c = d$$



شکل ۴. نمودار تابع تعلق سطوح سیل

همانگونه که در تابع تعلق مشخص شده است این تابع تعلق، یک تابع تعلق خاص بوده که همه اجزاء آن دارای مقادیر تعلق ۰ یا ۱ هستند. بنابراین با استفاده از این تابع تعلق، برای شاخص SIL برش‌های آلفا آنها در جدول ۶ تخصیص داده شده است.

دست آمده از این روش این مسئله فاصله زیادی از واقعیت خواهد داشت.

## ۸. نتیجه گیری

با توجه به پیشرفتهای اخیر در صنعت، تعیین سطح ایمنی سیستم ها امری بسیار مهم و پیچیده است. وجود عدم قطعیت در داده های ورودی هر مساله باعث شده است که محاسبه سطح تمامیت ایمنی در سیستمها همراه با عدم قطعیت همراه شود. وجود عدم قطعیت در پارامترها و مدل باعث افزایش ریسک در محاسبه ی شاخص تمامیت ایمنی می شود، از این رو طراحی سیستم های ایمنی با ضریب ایمنی بسیار بالاتر از سطح مورد نیاز واقعی باعث افزایش قابل توجه هزینه های طراحی می گردد. از این رو استفاده از تئوری فازی در محاسبه سطوح تمامیت ایمنی امری ضروری است و باعث کاهش هزینه های طراحی سیستم های ایمنی می شود. در این مطالعه، به محاسبه ی کمی شاخص سطوح تمامیت ایمنی در یک سیستم ایمنی با استفاده از استاندارد IEC61508 پرداخته شده است و با در نظر گرفتن عدم قطعیت موجود در پارامترهای ورودی، به آنالیز سیستم پرداخته ایم و میانگین احتمال خطا در هنگام تقاضای سیستم به همراه میزان قطعیت آن (تابع تعلق در فضای فازی) محاسبه شد. علاوه بر این هر یک از سطوح شاخص SIL (ارائه شده در استاندارد آی ای سی ۶۱۵۰۸) به صورت عدد فازی دوزنقه ای در نظر گرفته شد و در نهایت شاخصی جهت مقایسه نرخ خطای سیستم با محدوده خطای هر یک از سطوح تمامیت ایمنی ارائه گردید تا میزان تعلق سیستم ایمنی به هر یک از سطوح این شاخص مشخص گردد.

جهت انجام مطالعات آتی می توان با بکارگیری سایر روش های موجود (مانند ماتریس شدت خطرات، گراف ریسک و ...) به محاسبه شاخص SIL سیستم های ایمنی پرداخت و نتایج حاصل از آن را با روش ارائه شده در این مقاله مقایسه نمود.

همان گونه که مشاهده می شود برش آلفا تعیین شده برای شاخص SIL مستقل از میزان آلفاست که به دلیل شکل خاص تابع تعلق آن است. حال با استفاده از این تابع تعلق و همچنین تابع تعلق به دست آمده برای نرخ خطای سیستم در هنگام تقاضا اقدام به تعیین میزان تعلق سیستم به هر یک از سطوح این شاخص می نمایم.

## ۷-۴ تعیین میزان تعلق سیستم ایمنی به هر یک از سطوح تمامیت ایمنی در محیط فازی

در این قسمت برای تعیین میزان تعلق سیستم ایمنی به هر یک از سطوح SIL، از شاخص مساحت استفاده می کنیم. به این ترتیب که تابع تعلق نرخ خطای سیستم ایمنی در زمان تقاضا را با تابع تعلق شاخص برخورد داده و مساحت زیر منحنی محاسبه می شود. این مرحله در شکل ۵ به صورت تصویری نمایش داده شده و محاسبه آن با استفاده از فرمول ۱۷ انجام می شود.

همان گونه که در تصویر فوق نشان داده شده است، حاصل تقاطع تابع تعلق نرخ خطا سیستم با تابع تعلق شاخص SIL، سطحی است (از Cp1 تا Cp2) که نسبت آن به کل مساحت زیر منحنی برابر با میزان تعلق سیستم ایمنی به آن شاخص است. بنابراین برای محاسبه آن از فرمول ۱۷ استفاده می شود.

با مقایسه میانگین، حد بالا و پایین نرخ خطای سیستم در هنگام تقاضا با حد بالا و پایین بازه های مربوط به شاخص SIL می توان دریافت که این سیستم به طور همزمان به سطح ۲ و ۳ این شاخص تعلق دارد. با استفاده از فرمول ۱۷ میزان تعلق این سیستم به شاخص مورد نظر متناسب در جدول ۷ ارائه شده است.

این در حالیست که در صورت محاسبه سطح شاخص SIL سیستم، با استفاده از روش درخت خطای سنتی (در محیط قطعی) سطح تمامیت ایمنی سیستم برابر با ۳ خواهد بود که با توجه به نتایج به

بررسی سطوح تمامیت ایمنی با استفاده از درخت خطای فازی (مطالعه موردی در صنعت ریلی)

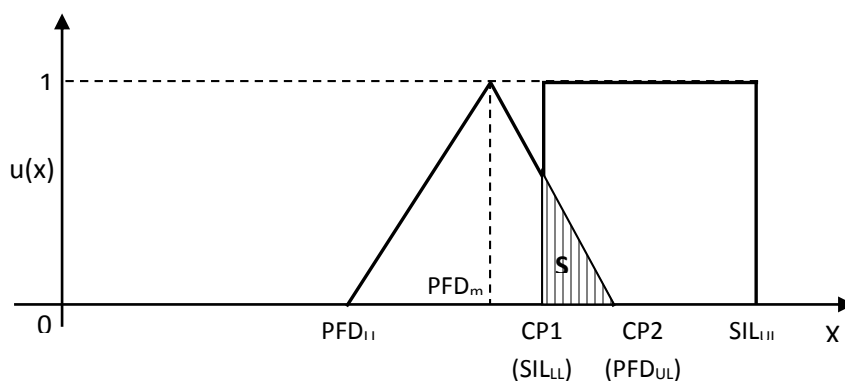
جدول ۶. برش آلفای شاخص SIL برای سیستم های کم تقاضا و پر تقاضا

سیستم کم تقاضا		سیستم پر تقاضا		نوع سیستم
$A_{\alpha}^{-}$	$A_{\alpha}^{+}$	$A_{\alpha}^{-}$	$A_{\alpha}^{+}$	سطوح تمامیت ایمنی
$10^{-9}$	$10^{-4}$	$10^{-9}$	$10^{-8}$	SIL4
$10^{-4}$	$10^{-3}$	$10^{-8}$	$10^{-7}$	SIL3
$10^{-3}$	$10^{-2}$	$10^{-7}$	$10^{-6}$	SIL2
$10^{-2}$	$10^{-1}$	$10^{-6}$	$10^{-5}$	SIL1

جدول ۷. میزان تعلق سیستم به سطوح شاخص SIL

SIL3	SIL2	
%۴۹	%۵۱	میزان تعلق سیستم

$$Dp = \begin{cases} 0, & pfd_{UL} < SIL_{ll} \text{ or } pfd_{LL} > SIL_{UL} \\ \frac{\int_{pfd_{UL}}^{pfd_{UL1}} u_{pdf_{avg}}(x) dx}{cp1 \int_{pfd_{UL}}^{pfd_{UL}} u_{pdf_{avg}}(x) dx}, & SIL_{ll} < pfd_{UL} \leq SIL_{UL}, pfd_{LL} < SIL_{LL} \\ \frac{\int_{pfd_{UL}}^{pfd_{UL1}} u_{pdf_{avg}}(x) dx}{cp1 \int_{pfd_{UL}}^{pfd_{UL}} u_{pdf_{avg}}(x) dx}, & pfd_{UL} > SIL_{UL}, pfd_{LL} < SIL_{LL} \\ \frac{\int_{pfd_{UL}}^{pfd_{UL1}} u_{pdf_{avg}}(x) dx}{cp2 \int_{pfd_{UL}}^{pfd_{UL}} u_{pdf_{avg}}(x) dx}, & pfd_{UL} > SIL_{UL}, pfd_{LL} \geq SIL_{LL} \\ 1, & pfd_{UL} \leq SIL_{UL}, pfd_{LL} \geq SIL_{LL} \end{cases} \quad (17)$$



شکل ۵. تقاطع دو نمودار تعلق مربوط به سطوح سیل و تابع تعلق نرخ خطای سیستم

Minimal Cut Sets	کوچکترین مجموعه‌های انقطاع غیر تکراری		۸. پی نوشت ها
PV (Pressure vessel)	مخزن فشار	SIL ( safety integrity level)	سطوح تمامیت ایمنی
PS (Power Supply)	منبع تغذیه	Fault tree analysis	آنالیز درخت خطا
Identical	کاملاً مشابه	Safety Instrument System (SIS)	قابلیت اطمینان سیستم‌های ایمنی
SV(Safety valve)	شیر فنی	Probability of Failure on Demand	احتمال خطارد در هنگام تقاضا
Component name	نام اجزاء	Risk Graph	گراف ریسک
Failure mode	مد خرابی	Hazardous event severity matrix	ماتریس شدت خطرات
Common cause failure	مد خرابی مشترک	Consequence only	بررسی عواقب
SF ( Safety Function)	فعالیت ایمنی	Reliability Block Diagram	بلوک دیاگرام قابلیت اطمینان
TE (Top Event)	حادثه نهایی	PFD( Average probability of failure on demand)	میانگین نرخ خطای احتمالی در زمان تقاضا
Cp (Cross point)	نقطه ی تلاقی	Proof test	تست اطمینان
Worst case scenario	بدترین حالت	Triangular fuzzy number	عدد فازی مثلثی
Fuzzy Probabilistic Approach	رویکرد احتمال فازی	Enhanced Markov Analysis	آنالیز پیشرفته مارکوف

## ۹. مراجع

- Lavasani, S. M., Ramzali, Nahid, Sabzalipour, Farinaz and Akyuz, Emre (2015) "Utilisation of fuzzy fault tree analysis (FFTA) for quantified risk analysis of leakage in abandoned oil and natural-gas wells", Ocean -Engineering, Vol. 108, No. 1, pp. 729-737.
- Lee, L.W. and Chen, S. M. (2008) "Fuzzy risk analysis based on fuzzy numbers with different shapes and different deviations", Expert Systems with Applications, Vol. 34, No. 4, pp. 2763–2771.
- Liu, P., Yang, L. Gao, Z. Li, S. and Gao, Y. (2015) "Fault tree analysis combined with quantitative analysis for high-speed railway accidents", Safety Science, Vol. 79, No 1, pp. 344-357.
- Markowski, A. S. and Mannanb, M. S. (2008) "Fuzzy risk matrix", Journal of Hazardous Materials, Vol. 159, No.1, pp. 152–157.
- Sallak, M., Simon,C. and Aubry,J. F. (2008) "A fuzzy probabilistic approach for determining safety integrity level", IEEE Transactions on Fuzzy Systems, Vol. 16, No. 1, pp. 239 – 248.
- Purba, J. H., Tjahyani, D.T.S. Ekariansyah, A.S. and Tjahjono, H. (2015) "Fuzzy probability based fault tree analysis to propagate and quantify epistemic uncertainty", Annals of Nuclear Energy, Vol. 58, No.1, pp. 1189-1199.
- Redmill, F. (2000) "Understanding the use, misuse and abuse of safety integrity levels", Eighth Safety-critical Systems Symposium, Southampton, UK, Springer.
- رضوانی، محمد علی و جعفریان، احسان (۱۳۹۱) " توسعه یک مدل تحلیلی از علل و پیامدهای ناشی از خروج از خط قطار مسافری در راه آهن جمهوری اسلامی ایران"، فصلنامه مهندسی حمل و نقل، سال دوم، شماره چهارم، تابستان ۱۳۹۰، ص. ۳۱۷-۳۳۳.
- IEC61508 Standard (1999) "Functional safety of electrical/ electronic/ programmable electronic safety-related systems", International Electro Technical Commission.
- Bukowski, J.V. and Goble, W. M. (1995) "Using Markov models for safety analysis of programmable electronic systems", ISA Transactions, Vol. 34, No. 2, pp. 193\_198.
- Bukowski, J. V. (2005) "A comparison of techniques for computing PFD average", Annual Reliability and Maintainability Symposium, Proceedings, pp. 590-595.
- Bukowski, J. V. (2006)" Using Markov models to compute probability of failed dangerous when repair times are not exponentially distributed", Reliability Engineering and System Safety, Vol. 71, No. 1, pp. 201-208.
- Guo, H., Yang, X. (2007)" A simple reliability block diagram method for safety integrity verification", Reliability Engineering and System Safety, Vol. 92, No. 1, pp. 1267–1273.
- Komal. (2015) "Fuzzy fault tree analysis for patient safety risk modeling in healthcare under uncertainty", Applied Soft Computing, Applied Soft Computing, Vol. 37, No. 1, pp. 942\_951.



-Smith, D. J. and Simpson, K. G. L. (2004) "Functional safety-A straightforward guide to applying IEC 61508 and related standards", Elsevier, Second Edition.

-Summers, A. E. (1998) "Techniques for assigning a target safety integrity level", ISA Transactions, Vol. 37, pp. 95\_104.

-Wenjin, Z. Nan, L. and Xinwei, L. (2012) "Estimating technology of safety integrity level of safety-related systems in high-speed train." IERI Procedia, Vol. 1, No. 1, pp. 172-177.

-Weber, D. P. (1994) "Fuzzy fault tree analysis", IEEE, Vol. 3, No. 1, pp. 1899-1904

-Sato, Y. (2007) "Throwing a bridge between risk assessment and functional safety", SICE Annual Conference, Kagawa University, Japan, pp. 17-20.

-Shu, Y. and Zhao, J. (2014) "A simplified Markov-based approach for safety integrity level verification", Journal of Loss Prevention in the Process Industries, Vol. 29, No.1, pp. 262-266.

-Simpson, K. G. L. and Kelly, M. (2003) "Reliability assessments of repairable systems – Is Markov Modeling -correct?", Safety and Reliability, Vol. 22, No. 2, pp. 19-39.

محمدعلی صندیدزاده، درجه کارشناسی در رشته مهندسی برق الکترونیک. را در سال ۱۳۷۰ از دانشگاه تهران و درجه کارشناسی ارشد در رشته مهندسی برق کنترل در سال ۱۳۷۲ را از دانشگاه تهران اخذ نمود. در سال ۱۳۷۹ موفق به کسب 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.



هستی جعفری، درجه کارشناسی خود را در رشته مهندسی حمل و نقل ریلی در سال ۱۳۹۰ از دانشگاه علم و صنعت تهران اخذ نمود و به عنوان استعداد درخشان در همان سال وارد مقطع کارشناسی ارشد شد و در سال ۱۳۹۲ مدرک کارشناسی ارشد خود را در رشته مهندسی حمل و نقل ریلی از دانشگاه علم و صنعت تهران اخذ نمود. زمینه های پژوهشی مورد علاقه ایشان بهینه سازی و ایمنی راه آهن و قطار است.

