تجزیه و تحلیل خطرات با استفاده از روش تجزیه و تحلیل فرایند تئوری سیستم (STPA): مطالعه موردی در سیستم های خاموش کننده اضطراری یک نیروگاه حرارتی تولید برق

اسماعیل کرمی[1] - زهرا گودرزی[2] - طاهر حسین زاده[2]- غلامعباس شیرالی[3*]

shirali@ajums.ac.ir

تاریخ دریافت: ۹۳/۸/۱۰ *تاریخ پذیرش: ۹۳/۱۲/۲۵*

چکیده

مقدمه: روش های سنتی تجزیه و تحلیل خطر به دلیل ضعفهای آن برای سیستم های فنی- اجتماعی امروزی از کارایی لازم برخوردار نمی باشند. روش تجزیه و تحلیل فرایند تئوری سیستم (STPA) که جزء روش‌های سیستماتیک تجزیه و تحلیل می‌باشد به عنوان یک روش جایگزین مناسب، از یک منطق قدرتمند برای شناسایی خطرات در چنین سیستم هایی سود می برد. هدف این مطالعه، تجزیه و تحلیل خطرات با استفاده از روش STPA در سیستم های خاموش کننده واحد بخار یک نیروگاه برق می باشد.

روش کار: مطالعه حاضر یک پژوهش موردی از نوع کیفی است. با استفاده از روش STPA، خطرات مرتبط تعریف، دیاگرام ساختار کنترلی ایمنی در بخش های مختلف فرایند ترسیم و اقدامات کنترلی ناکافی و عوامل سببی آن شناسایی شد.

یافته ها: برای واحد بخار نیروگاه، فاجعه بارترین حوادث مربوط به آسیب ها و خطرات دستگاه توربین (تغییر دور توربین) تشخیص داده شد. سپس با ترسیم دیاگرام ساختار کنترل ایمنی سیستم های خاموش کننده مرتبط با تغییر دور توربین، دستگاه PLC به عنوان مهم ترین بخش سیستم کنترلی و اپراتور به عنوان بخش استراتژیک و تأثیر گذار بر روی سیستم کنترلی تشخیص داده شدند. در ادامه با تجزیه و تحلیل خطرات برای توربین، بیش از 54 عامل سببی با جزییات مربوطه شناسایی گردید.

نتیجه گیری: روش STPA با توجه به ساختار مدون و سیستماتیک خود می‌تواند در شناسایی کامل تر خطرات و عوامل سببی ایجاد کننده ی خطرات در سیستم‌های خاموش کننده اضطراری مؤثر باشد. بنابراین توسعه چنین ابزارهایی برای افراد مرتبط با سیستم‌های حساس از نظر ایمنی مفید خواهد بود.

کلمات کلیدی: *تجزیه و تحلیل خطر، نیروگاه حرارتی برق، سیستم های خاموش کننده اضطراری، STPA*

1- مربی، گروه مهندسی بهداشت حرفه‌ای، دانشکده بهداشت واحد دامغان ،دانشگاه علوم پزشکی سمنان

2- کارشناسی ارشد مهندسی بهداشت حرفه‌ای، دانشکده بهداشت، دانشگاه علوم پزشکی جندی شاپور اهواز

3- استادیار مهندسی بهداشت حرفه‌ای، دانشکده بهداشت ،دانشگاه علوم پزشکی جندی شاپور اهواز

مقدمه

روش های سنتی تجزیه و تحلیل خطرات در مهندسی ایمنی برای یافتن متغیرهای سببی خطر و تأثیر آنها بر روی سطوح سیستم و نقص یک قسمت از سیستم بنا نهاده شده‌اند. با این حال، همیشه سناریوهایی وجود دارد که ممکن است باعث ایجاد خطرهایی شوند و این خطرات به وسیله ی روش‌های سنتی تجزیه و تحلیل خطر به طور کامل در کل سیستم قابل پیش بینی نباشند. این حالت در سیستم های خودکار صنایع ممکن است بسیار شدیدتر باشد (Parnas, 1990)، زیرا سیستم های خودکار که اغلب در برنامه های ایمنی با حساسیت بالا مورد استفاده قرار می گیرند یک بازخورد اطلاعاتی از فرمان اپراتور تحت عنوان پاسخ فراهم می کنند. بنابراین، در هنگام تجزیه و تحلیل مسایل مربوط به ایمنی سیستم، تمام اجزاء عملیاتی که می توانند به طور مستقیم یا غیرمستقیم بر روی ایمنی سیستم اثر داشته باشند باید بررسی شوند و خطرات مربوط به آنها حذف یا کاهش داده شوند (Leveson, 1995).

نیروگاه حرارتی برق یکی از حوزه هایی است که در آن اکثر سیستم های کنترل کننده به طور خودکار عمل می کنند و یک حادثه در این حوزه می تواند باعث یک فاجعه وحشتناک گردد. بنابراین تجزیه و تحلیل خطر در این سیستم ها امری حیاتی محسوب می شود. امروزه برای شناسایی خطرات و ارزیابی ریسک در نیروگاه های برق روش های بسیار زیادی معرفی شده اند که هر کدام از آنها دارای نقاط قوت و ضعف خاص خود می باشند. در حال حاضر تمام روش های به کار گرفته شده در کشور ما برای شناسایی خطرات سیستم های خودکار نیروگاه های تولید برق جزء روش های سنتی تجزیه و تحلیل خطر می باشند.

روش های سنتی تجزیه و تحلیل، خطر را به عنوان مجموعه ای از وقایع که به صورت خطی در یک ظظم خاص اتفاق می‌افتد توصیف می کنند (Holl-nagel, 2004) و برای بسیاری از حالت های نقص و علت نقص طراحی شده‌اند. لذا اکثر این مدل ها مدت طولانی است که در سیستم های نیروگاهی اجرا می شوند. با وجود این، اکثر این روش ها به تنهایی جوابگوی نیاز تکنولوژی و صنایع پیچیده نیستند، زیرا روش های سنتی با فرض استاتیک سیستم یا سازمان، اقدام به تجزیه و تحلیل خطر می نمایند. در حالی که وقوع حوادث شدید در صنایع نشان داده است که سیستم ها دارای حالت پویا هستند. در نتیجه مرتب در حال تغییر و تحول می باشند. بنابراین، روش های سنتی در زمان ارزیابی ریسک و تجزیه و تحلیل خطر دید جامع نگر ندارند و هر جزء از سیستم را به طور جداگانه بررسی می کنند. بنابراین، با استفاده از روش های سیستماتیک جدید نظیر STAMP, FRAM و غیره می توان برای رفع این مشکلات راه حلی اندیشید (Shirali, 2011).

این روش‌ها بر خلاف روش‌های سنتی ارزیابی ریسک، ماهیت غیرخطی دارند و ریسک را به عنوان مجموعه ی غیرخطی از تعاملات بین انسان- ماشین- تکنولوژی در نظر می گیرند. به عنوان نمونه روش STAMP که مبتنی بر تئوری سیستم ها می باشد، شامل روابط غیرمستقیم و غیرخطی و بازخوردها می باشد که می تواند سطح پیچیدگی و تغییر تکنولوژی را در سیستم های امروزی بهتر از مدل های سنتی و علیتی حادثه، تشریح و بیان نماید. در این روش مثل روش های سنتی، نقص اجزاء و اصل علیت گنجانده و بررسی می گردد، اما مفهوم از علیت که شامل اختلالات جزء می‌باشد، به دیگر اجزاء سیستم نیز بسط داده شده و ایمنی به عنوان یک مشکل

کنترلی به جای قابلیت اطمینان فرمول‌بندی می‌شود. این روش مبتنی بر رویکرد جدید ذهنی پیرامون حادثه می‌باشد (Leveson, 2004) که همه جنبه های ریسک از جمله جنبه های اجتماعی و سازمانی را شامل می شود (Misra, 2008). در مطالعه ای که توسط کنستانتین کازاراز (Konstantinos Kazaras) و همکارانش در سال ۲۰۱۲ با عنوان معرفی روش STAMP در ارزیابی ایمنی تونل ها انجام گرفت، مشخص شد که این روش برای رفع محدودیت های رفتار سازمانی، نرم افزار و سازگاری سیستم در طول زمان مناسب است (Kazaras et al., 2012).

این شیوه را می توان به عنوان پایه‌ای برای روش های اصلاح شده و جدید نظیر (STPA) برای تجزیه و تحلیل خطر و پیشگیری از حادثه، بررسی و تحلیل حادثه، ارزیابی و مدیریت ریسک، تدوین ماتریس های ریسک و پایش عملکرد به کار برد.

STPA یک روش آنالیز خطر جدید مشتق شده از روش STAMP می باشد که در هر مرحله از چرخه عمر سیستم، قبل از طراحی تا بعد از اجرا، باعث افزایش توانایی سازمان در پایش عملکرد سیستم ها می شود و از اضمحلال ایمنی و افزایش ریسک قبل از بروز یک فاجعه جلوگیری مینماید. این روش برای طراحی فنی در سیستم نیز به‌کار می‌رود (Pentti and Atte, 2002). در خصوص تحقیقات انجام شده با استفاده از روش STPA، می‌توان به مطالعه "روش تجزیه و تحلیل نرم افزاری خطر بر پایه STPA" توسط سان هی لی (Sun Hwi Lee) و همکارانش در سال ۲۰۱۲ اشاره نمود که به عنوان یک روش تجزیه و تحلیل خطر مؤثر برای سیستم های پیچیده معرفی گردید. هدف از انجام این تحقیق، اجرای روش STPA بر روی سیستم های خاموش کننده اضطراری توربین یک نیروگاه حرارتی تولید برق به منظور تجزیه و تحلیل خطرات به صورت سیستماتیک می باشد. حال با توجه به عدم اثربخشی مؤثر روش‌های سنتی در تجزیه و تحلیل خطرات، و اهمیت نقش روش STPA در تجزیه و تحلیل خطرات، بر ضرورت انجام این تحقیق تأکید می شود.

روش کار

مطالعه حاضر یک مورد پژوهی از نوع کیفی می‌باشد که به منظور تجزیه و تحلیل خطرات در سیستم های خاموش کننده یک نیروگاه حرارتی تولید برق اجرا گردید، زیرا با توجه به مطالعات خطرات و وقوع حوادث از اهمیت ویژه ای برخوردار و بسیار حائز اهمیت است. برای اجرای این مطالعه ابتدا یک بازدید کلی جهت آشنایی با فرایند صورت گرفت، سپس با توجه به اطلاعات به‌دست آمده از حساسیت واحدهای مختلف عملیاتی و کنترل قدرت نیروگاه و تمامی تجهیزات و تکنولوژی و سنسورهای مهم، واحد بخار نیروگاه به دلیل اهمیت آن نسبت به بقیه واحدها (به دلیل عملیاتی بودن در طول شبانه روز و هم چنین تولید بالا و دارای بخش های حساس) جهت انجام پروژه ارزیابی خطر در نظر گرفته شد. لذا سیستم های خاموش کننده بخش واحد بخار به عنوان بخش مورد مطالعه انتخاب گردید.

روش انجام مطالعه

انجام مطالعه به روش STPA شامل چهار مرحله به شرح زیر می‌باشد:

۱- تعریف خطرات واحد بخار نیروگاه و محدودیت های ایمنی مرتبط با آنها

در این مرحله با شناسایی حوادث گذشته شغلی، خطراتی که سیستم را تهدید می کند باید تعریف

شوند. حوادث در اینجا به عنوان وقایع برنامه ریزی نشده و ناخواسته منجر به صدمه از جمله صدمه جسمی و مالی، آلودگی زیست محیطی، از دست دادن اهداف و غیره تعریف می‌شوند. خطرات نیز به عنوان حالت های سیستم یا مجموعه ای از شرایط که همراه با مجموعه ی خاصی از شرایط خطرناک منجر به حادثه می‌گردند تعریف می‌شوند. بعد از تعریف و تعیین خطرات سیستم، محدودیت های ایمنی مربوطه تفسیر می شوند که چگونه محدودیت های اعمال شده بر روی سیستم می‌تواند به اهداف خود برسد و از وقوع حوادث جلوگیری شود.

۲- تعیین ساختار کنترلی ایمنی

پس از این که خطرات و محدودیت های مرتبط با آن تعریف گردید، ساختار سلسله مراتبی فنی- اجتماعی مربوط به فرآیند کنترل ایمنی که ساختار کنترلی سلسله مراتبی ایمنی نامیده می شود ترسیم خواهد شد. روش کار به این صورت است که پس از شناسایی اولیه سیستم، مشاهده مستقیم فعالیت، بررسی اسناد و برگزاری میزگردهای تخصصی، ساختار کنترلی ایمنی سیستم ترسیم می شود. استفاده اصلی از تعریف این ساختار کنترلی شامل شناسایی مسوولیت و وظیفه هر جزء یا زیر سیستم و همچنین تمام روابط بین آنها است که آن تابع طراحی خاص سیستم می‌باشد. همچنین هیچ نوع استانداردی برای ترسیم ساختار کنترلی وجود ندارد و آن بستگی به این دارد که چقدر اطلاعات را دقیق در نظر بگیریم. ساختار سلسله مراتبی کنترل ایمنی می‌تواند بسیار پیچیده باشد، بنابراین هنگام تجزیه و تحلیل خطرات مختلف، تنها بخشی از ساختارهای کلی به عنوان هدف در نظر گرفته می شود و بقیه تحت عنوان عوامل محیطی دسته‌بندی می‌گردد.

۳- شناسایی اقدام های کنترلی ناکافی

پس از تعریف ساختار کنترلی سیستم، گام بعدی شناسایی اقدام های کنترلی ناکافی است که ممکن است سیستم را به سمت حالت خطرناک سطح پایین تر سوق دهد. برای اکثر سیستم های پیچیده، خطرات سطح پایین تر باید با توجه به طراحی خاص سیستم شناسایی شوند. حالت خطرناک، حالتی است که محدودیت های ایمنی که قبلاً برای سیستم تعریف شده، نقض شوند (Leveson, 2011). حالت خطرناک (حالتی که اختلال در محدودیت های ایمنی ایجاد می شود) در روش STPA به علت کنترل نامؤثر و ناکافی ایجاد می‌گردد. کنترل ناکافی می تواند به یکی از دلایل زیر رخ دهد (Pentti and Atte, 2002):

۱. اقدام کنترلی مورد نیاز فراهم نیست (اقدام لازم برای ایمنی ارایه نشده و یا دنبال نشده است)

۲. اقدام کنترلی به صورت ناامن فراهم شده، در نتیجه منجر به ایجاد خطر می شود. اقدام کنترلی نا امن یا غلط ممکن است به علت رفتار یا تعاملات ناکارامد در بین اجزاء باشد (Ishimatsu *et al.*, 2010).

۳. اقدام کنترلی امن یا صحیح فراهم شده ولی خیلی دیر یا خیلی زود (در زمان اشتباه) اجرا می شود.

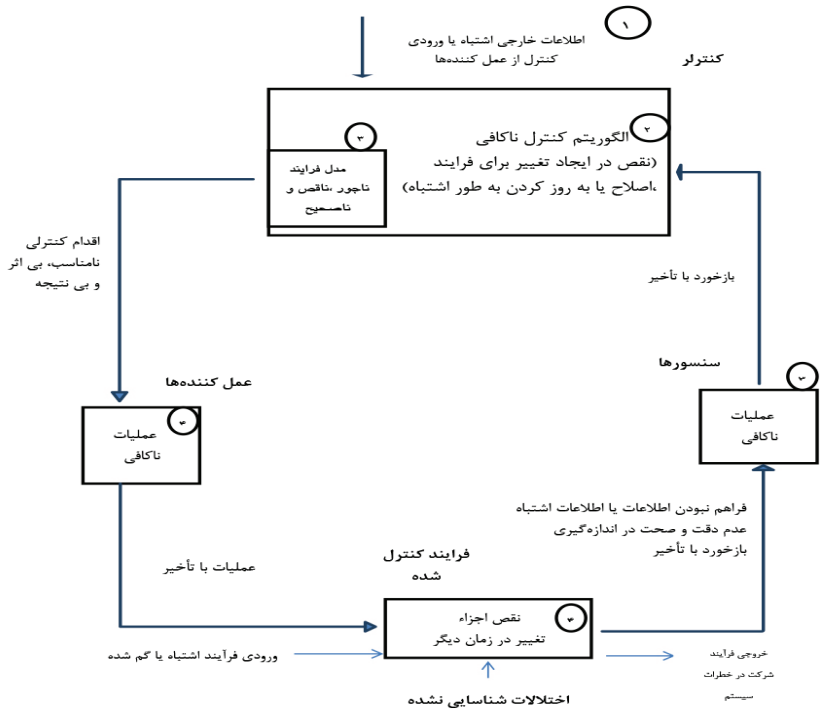
۴. اقدام کنترلی صحیح خیلی زود متوقف می شود (برای اقدام کنترلی مداوم و پیوسته).

برای هر عملکرد چندین اقدام کنترلی مرتبط وجود دارد که با توجه به نوع درخواست کنترل کننده از فرایند کنترل شده/ یا هدف مرتبط با عملکرد انتخاب شده، می‌توان آنها را شناسایی کرد. برای اطمینان از یک ارزیابی کامل، هر اقدام کنترلی باید یک به یک در مسیر خود بررسی شود.

۴- شناسایی چگونگی وقوع اقدام کنترلی ناکافی

خطرات، ناشی از کنترل ناکافی و عدم اجرای محدودیت‌های ایمنی می‌باشد. بعد از شناسایی خطرات، در ادامه باید عوامل سببی که یک ویژگی بسیار مفید برای کاهش خطرات هستند مشخص شوند. در این مرحله نمودارهای کنترل عملکرد مورد واکاوی قرار گرفته و نقص هایی که در حلقه های کنترلی آنها وجود دارد شناسایی خواهد شد. نقص های کنترلی اشاره به هرگونه نقص یا کاستی در طول کنترل فرایند دارد. عوامل سببی در ارتباط با نقص های کنترلی قابل فهم می‌باشد. با استفاده از طبقه بندی نقص‌های کنترلی، ساختار کنترلی ایمنی ارزیابی می‌شود. در ضمن باید به این نکته توجه شود که همه نقص‌های کنترلی جزء عوامل سببی نخواهد بود و به موارد مختلفی بستگی دارد. شکل ۱ (Lee *et al.*, 2012) یک دسته بندی از نقص های کنترلی منجر به خطا را نشان می‌دهد. همان طور که در شکل ۱ مشاهده می شود ۴ نوع نقص کنترلی قابل شناسایی می‌باشد.

نقص نوع اول (مربوط به اطلاعات ورودی کنترل یا اطلاعات خارجی اشتباه یا از بین رفته)؛ هر کنترل کننده در ساختار سلسله مراتبی کنترل توسط کنترل کننده سطوح بالاتر بررسی می شود. نقص نوع دوم (مربوط به الگوریتم کنترل ناکافی)؛ الگوریتم در اینجا به دستورالعمل ها، هم برای کنترل کننده‌های سخت افزاری و هم کنترل کننده‌های انسانی اشاره می کند. این الگوریتم ها ممکن است ناکافی باشند زیرا که آن ها در اصل و به طور پایه ای ممکن است به طور ناکافی طراحی شده باشند. نقص نوع سوم (مربوط به مدل فرایند و حس گرها)؛ مدل فرایند می تواند از همان ابتدا اشتباه باشد بدان معنی



شکل ۱. طبقه بندی نقص های کنترلی منجر به خطرات (Leveson, 1995)

که مدل با روند فرآیند فعلی ناسازگار است. یک مدل فرآیند نیز ممکن است به دلیل گم شدن بازخورد، یا تأخیر یا اشتباه در اندازه گیری ایجاد شود. نقص نوع چهارم (مربوط به فرآیند کنترل شده و عمل کننده ها)؛ حتی اگر فرض شود که دستورات کنترلی با حفظ محدودیت های ایمنی کافی باشند، باز ممکن است فرایند کنترل شده با این دستورات اجراء و پیاده سازی نشود. دلایل آن می تواند ایجاد خطا در کانال انتقال یا عمل کننده و یا خطا در هدف کنترل باشد.

علاوه بر چهار نوع نقص بالا، اگر چندین کنترل کننده وجود داشته باشد، نقص های ارتباطی در بین این کنترل کننده‌ها نیز می تواند قابل ملاحظه باشد. این عوامل کلی و عمومی شبیه به هم در هر سطح از ساختار کنترل ایمنی فنی – اجتماعی به کار گرفته می شود. اما، در برنامه های کاربردی، عوامل در هر سطح ممکن است متفاوت باشند (Weber *et al.*, 2003). علاوه بر این، اگر انسان یا سازمان نیز درگیر باشد ضروری است که محیط و فضا نیز ارزیابی شود. از آن جا که عوامل محیطی و زمینه ای در دسته بندی سخت و مشکل هستند بنابراین در این جا مورد بحث قرار نمی‌گیرند (Leveson, 2011).

یافته ها

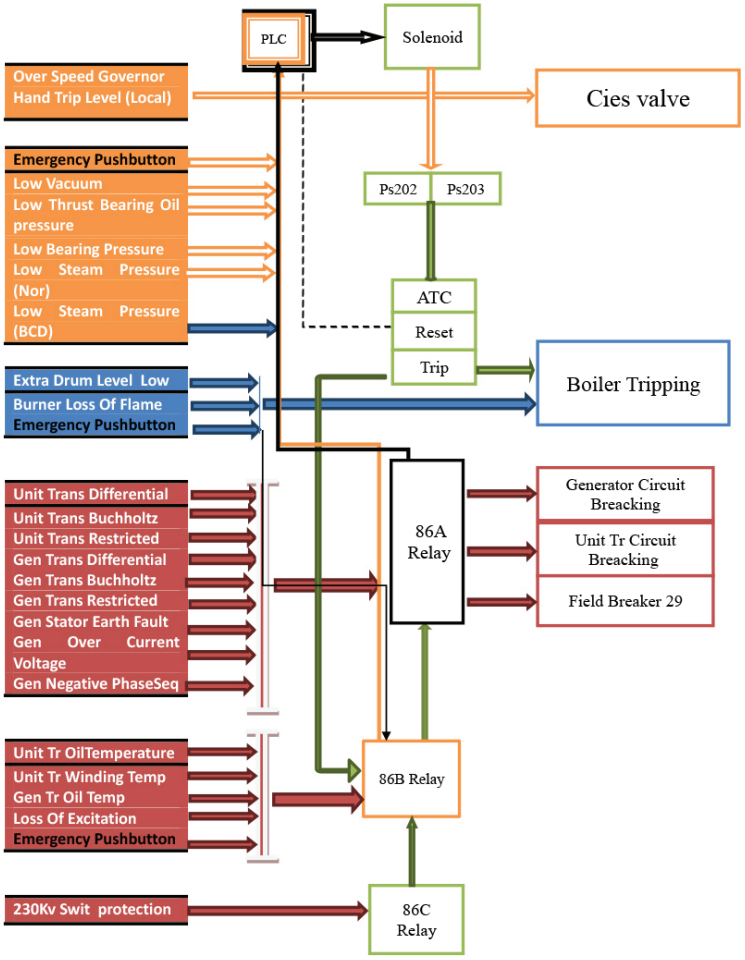
طبق مراحل روش STPA، یافته های این تحقیق را می‌توان در چهار بخش به شرح زیر دسته بندی نمود:

۱- خطرات سیستم و محدودیت های مرتبط با آنها

در این پژوهش برای واحد بخار نیروگاه حوادث زیادی شناسایی شد، ولی فاجعه بارترین حوادث مربوط به آسیب ها و خطرات دستگاه توربین (افزایش دور بیش از حد توربین) تشخیص داده شد که منجر به آسیب های اقتصادی، انسانی و زیست محیطی فراوانی می شود. با تفسیر خطرات سطح سیستم برای توربین، اینکه نتواند در زمان مورد نظر تریپ شود، برای سیستم های خاموش کننده در چنین شرایطی حداقل دوکانال تریپ باید اتفاق بیفتد (توربین از طریق دو مسیر تریپ شود). بنابراین محدودیت های ایمنی موجود و مرتبط با افزایش دور بیش از حد توربین، گاورنر و PLC تعیین گردید که در زمان بروز مشکل برای توربین، سیستم را خاموش می‌کند.

۲- ساختار کنترلی ایمنی

دیاگرام ساختار کنترل ایمنی سیستم های خاموش کننده در سطح سیستم در شکل ۲ ارایه شده است. کل سیستم را میتوان به عنوان یک فرایند کنترلی مشاهده کرد. همانطور که ملاحظه می‌گردد اجزاء شامل توربین، ژنراتور، بویلر، دی الکتریک، اپراتور، عمل کننده، PLC و سنسور می‌باشد. ما در اینجا از مبدل های سیگنال های آنالوگ به دیجیتالی، فرستنده ها و آمپلی فایرها صرفنظر کردیم. سنسورها گروهی جداگانه هستند که در چندین بخش به چهار کانال اصلی PLC و 86A و 86B و 86C وصل می شوند و کار آن ها گرفتن اطلاعات از بخش های مختلف توربین، ژنراتور و بویلر می باشد. سنسورهای مختلف مسوول گرفتن اطلاعات از بخش های متفاوت مثل دور غیر مجاز توربین، کاهش خلاء، بالا بودن درجه حرارت یاتاقان ها و غیره می باشد. آمپلی فایرها و فرستنده ها در تقویت و انتقال سیگنال های آنالوگ از سنسورها مورد استفاده قرار می گیرد. دستگاه PLC به عنوان کنترل کننده، مهم ترین بخش سیستم کنترلی می‌باشد. اپراتور نیز به عنوان بخشی از کنترل کننده، یک استراتژی برای



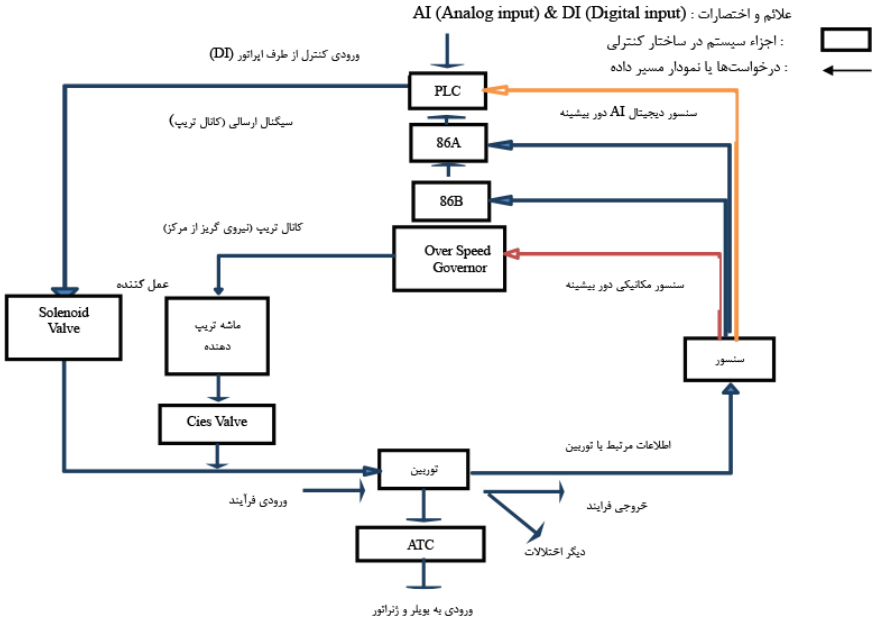
شکل ۲. ساختار کلی کنترلی مربوط به تریپ توربین، بویلر، ژنراتور

بررسی تریپ سیستم تهیه می‌کند. عمل کننده جزء اجرا کننده عملیات برای هدف در حال کنترل است. توربین هدفی است که ما قصد داریم کنترل شود. در سیستم خاموش کننده توربین، دو نوع عمل کننده به صورت جداگانه وجود دارد که هر یک از آنها دارای ولوی اختصاصی (Cies Valve و Solenoid Valve) می باشند و اقدام به خاموش کردن توربین می کنند.

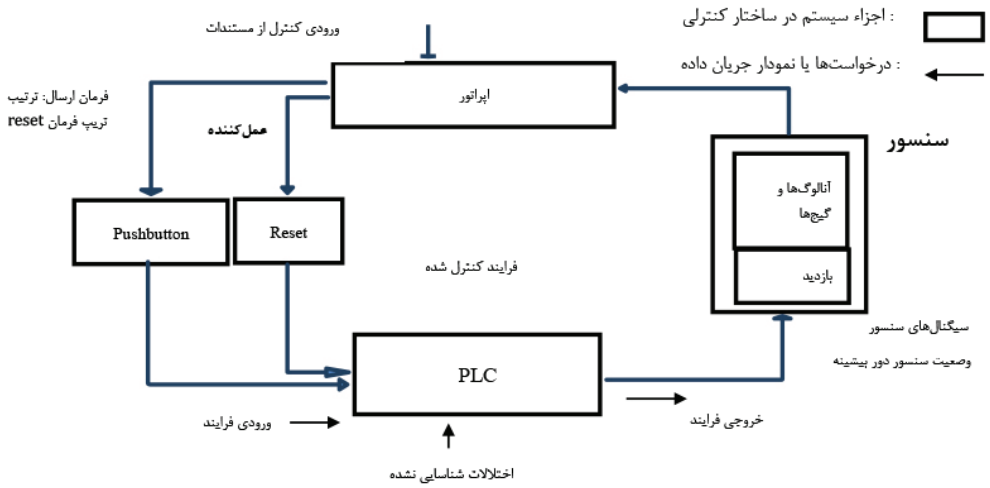
شکل ۳ ساختار کنترلی ایمنی تریپ توربین توسط کنترل کننده PLC با ایجاد کانال تریپ و ارسال سیگنال به Solenoid Valve به عنوان عمل کننده را نشان می دهد. شکل ۴ نیز ساختار کنترلی ایمنی تریپ PLC توسط اپراتور با ایجاد کانال تریپ توسط کلید PUSHBUTTON را نشان می دهد.

۳- *شناسایی اقدام های کنترلی ناکافی*

در سیستم های خاموش کننده نیروگاه، به طور کلی چندین پارامتر تریپ مستقل (به عنوان نمونه: افزایش دور توربین از محدوده set point) شناسایی شد که هر کدام از این پارامترها را می توان به عنوان یک عملکرد از سیستم مشاهده کرد. در سیستم خاموش کننده، فرمان تریپی که می‌توان از کنترل کننده به فرایند کنترل شده



شکل ۳. ساختار کنترلی ایمنی کلی مربوط تریپ توربین



شکل ۳. ساختار کنترلی ایمنی کلی مربوط تریپ توربین

فرستاد، فرمان نوع کانال تریپ است که فرمان تریپ می‌تواند از طریق PLC یا اپراتور فرستاده شود. از آن جا که PLC ها به عنوان کنترل کننده برای توقف اضطراری بخش اصلی و برای جلوگیری از آسیب به قسمت های دیگر نیاز به خاموش کردن اجزای دیگر نیز دارند، بنابراین در این تحقیق تمرکز بر روی رله های اصلی و دکمه توقف اضطراری معطوف گردید. بخشی از اقدامات کنترلی مرتبط با خاموش کننده توربین در دور بالا در جدول ۱ ارایه شده است.

جدول ۲ نیز اقدام های احتمالی کنترل ناکافی بر روی تریپ دور بیش از نقطه تنظیم

جدول۱. اقدام کنترلی برای تریپ دور بیشینه

اقدام کنترلی	از	به	توضیحات
تریپ PLC روی دور بیشینه	PLC	Solenoid valve	خاموشی توربین (بسته شدن بخار ورودی توربین) با تریپ PLC در شرایط دور بیشینه
تریپ گاورنر اضطراری روی دور بیشینه	گاورنر	Cies valve	خاموشی توربین(بسته شدن بخار ورودی) توسط Cies valve (یک نوع ولو خاص)

جدول ۲. شناسایی اقدام کنترلی ناکافی برای افزایش دور توربین

اقدام کنترلی	۱-اقدام کنترلی مورد نیاز برای ایجاد ایمنی فراهم نشده ،یا به‌دنبال نداشته است.	۲- اقدام کنترلی ناامن فراهم شده که منجربه حالت خطرناک برای سیستم شده است.	۳- اقدام کنترلی ایمن خیلی زود ، یا خیلی دیر شده است.	۴-اقدام کنترلی ایمن خیلی زود متوقف شده است.
تریپ PLC روی دور بالاتر از حد مجاز	PLC فرمان تریپ را در دور توربین بالاتر از حد نقطه تنظیم، ارسال نکند. (A1)	اگر تریپ گاورنر روی دور بیشینه انجام شود خطری اتفاق نخواهد افتاد.	PLC پارامتر تریپ را در حالی که دور توربین برابر یا کمتر از حد set point است ارسال کند.(A2)	تریپ PLC خیلی زود متوقف می‌شود قبل از اینکه ولوهای مسیر بخار بسته شوند.(A1)
تریپ توربین با گاورنر روی دور بیشینه	وقتی که PLC در زمان مورد نیاز نتواند فرمان تریپ ارسال کند و گاورنر نیز نتواند سیستم را تریپ دهد. (B1)	اگر تریپ PLC روی دور بیشینه به‌جای تریپ گاورنر انجام شود، خطری سیستم را تهدید نمی‌کند.	گاورنر فرمان تریپ را در حالی که دور توربین برابر یا کمتر از حد set point است ارسال کند.(B2)	تریپ گاورنر خیلی زود متوقف شود قبل از این که نیروی گریز از مرکز به نیروی فنر غلبه پیدا کند.(B1)
تریپ بویلر روی تریپ ATC دور بیشینه	وقتی که ATC نتواند فرمان تریپ را به بویلر ارسال کند.	اگر اپراتور فرمان تریپ را ارسال کند اتفاقی رخ نخواهد داد.	ATC فرمان تریپ را زمانی که توربین تریپ نشده فرمان تریپ را با بویلر ارسال کند.	فرمان تریپATC خیلی زود متوقف شود قبل از اینکه بویلر متوقف شود.
تریپ رله 86B روی تریپ ATC دور بیشینه	وقتی که ATC نتواند فرمان تریپ را به ژنراتور ارسال کند.	اگر اپراتور فرمان تریپ را ارسال کند اتفاقی رخ نخواهد داد	ATC فرمان تریپ را زمانی که توربین تریپ نشده فرمان تریپ را با ژنراتور ارسال کند.	فرمان تریپATC خیلی زود متوقف شود قبل از اینکه رله 86B در حالت ON قرار گیرد

توربین را در ۴ دسته کلی نشان می دهد. هر سلول در این جدول نشان می دهد که چه نوع اقدام کنترلی ناکافی می تواند رخ دهد. هر اقدام کنترل ناکافی در واقع یک خطر محسوب می شود. در حال حاضر ۴ خطر اصلی در سطح سیستم برای عملکرد تریپ توربین روی دور بیشینه با علامت A و B و C و D شناسایی شده است.

- تعیین احتمال وقوع اقدامات کنترلی ناکافی

با تجزیه و تحلیل خطرات برای توربین، بیش از ۵۴ عامل سببی با جزییات مربوطه شناسایی گردید که به دلیل حجم زیاد نمودارها و جداول، نوع خطر 1A برای تجزیه تحلیل عوامل سببی انتخاب شده که عوامل سببی منجر به خطر 1A در جدول ۳ ارایه شده‌اند.

بحث و نتیجه گیری

همان‌طور که در تجزیه و تحلیل خطرات در سیستم خاموش کننده واحد بخار دیده شد، بروز خطرات توربین (دور توربین بیش از حد Set Point) می‌تواند کل سیستم را به شدت تحت تاثیر قرار دهد. با توجه به شکل ۳ ملاحظه می شود که چندین حلقه کنترلی در ساختار کنترلی ایمنی کلی تریپ توربین در تعامل با هم و مرتبط با یکدیگر هستند. مثلاً در ساختار تریپ PLC، ساختار کنترلی دیگری نیز وجود دارد که در آن اپراتور به عنوان کنترل کننده حلقه فرآیندی ایفای نقش می‌نماید. در سیستم های پیچیده، هر یک از اجزاء ساختار کنترلی، دارای منطق خاص خود می باشند و یا مدلی از الگوریتم و یا حتی در ساختار کنترل دیگری نقش ایفاء می کنند. برای

جدول ۳. عوامل سببی منجر به خطر 1A

بخشی از حلقه کنترلی	عوامل سببی خطر A۱		
کنترل کننده (تریپ PLC)	ورودی کنترل (اپراتور) اشتباه یا فراموش شده	نیاز به بسط و توسعه بیشتر (نیاز به ایجاد حلقه کنترلی)	
		نیاز به بسط و توسعه بیشتر	
	الگوریتم کنترل ناکافی	میزان کالیبراسیون خیلی کم سیگنال دور بیشینه (عملکرد غلط)	خطای نرم‌افزاری مدل الگوریتم
		محاسبه نقطه set point خیلی بالا (بیش از دور بیشینه)	خطای نرم‌افزاری مدل الگوریتم
	مدل منطق غلط	خطای مقایسه بین سیگنال دور بیشینه با set point	خطا در مدل منطق پارامتر تریپ
	نقص اجزاء سخت افزاری	خطا در باز کردن کانال تریپ PLC (دیجیتال خروجی)	خطای سخت افزاری تریپ (نقص کارت دیجیتال خروجی ، نقص در IO BUS)
		خطا در تعیین صحت سیگنال AI/DI به CPU (Validity)	نقص سخت افزاری تریپ PLC (خطای کارت AI/DI نقص در IO BUS)
انتقال بین تریپ PLC و سنسور(سنسور ها و آمپلی فایرها و انتقال دهنده ها)	فیدبک ناکافی	سیگنال آنالوگ (AI)، سنسور خیلی کم در طول انتقال وارد می‌شود	خطا در کانال انتقال
	فیدبک گم شده	سیگنال (AI)، سنسور در طول انتقال گم می شود	
	فیدبک با تاخیر	سیگنال (AI)، سنسور در طول انتقال خیلی با تأخیر وارد می‌شود	
انتقال بین تریپ PLC و عمل کننده (سلنوئید ولو)	گم شدن یا فقدان کانال تریپ	سیگنال کانال تریپ از بین رفته	خطا در کانال انتقال
سنسور (سنسورها و آمپلی فایرها)	عملیات ناکافی	عملکرد ناکافی سنسور و آمپلی فایر باعث به وجود آمدن سیگنال ضعیف می‌شود.	نقص در اجزاء سنسور و آمپلی فایر
		عملکرد ناکافی انتقال دهنده‌ها باعث گم شدن سیگنالAI می‌شود.	خطای اجزاء انتقال دهنده‌ها
عمل کننده (سلنوئید ولو)	عملکرد ناکافی	عملکرد ناکافی دمپرهای بسته کننده دریچه‌ها باعث از دست رفتن کانال تریپ می‌شود	خطای سخت‌افزاری عمل‌کننده‌ها
هدف کنترل شده (توربین)	نقص در اجزاء	نقص در ولوها	خطای سخت افزاری
	تغییرات اضافه بار	نیاز به جزییات و اطلاعات بیشتر	نیاز به جزییات و اطلاعات بیشتر
	اختلالات شناسایی نشده	نیاز به جزییات و اطلاعات بیشتر	نیاز به جزییات و اطلاعات بیشتر
	ورودی فرآیند اشتباه یا فراموش شده	نیاز به جزییات و اطلاعات بیشتر	نیاز به جزییات و اطلاعات بیشتر
انتقال بین توربین و عمل کننده	تأخیرات عملیاتی	تأخیر در ارسال سیگنال کانال تریپ	خطا در کانال انتقال
انتقال بین توربین و سنسور	عدم دقت و صحت در اندازه گیری	خطا در کالیبراسیون	خطا در کانال انتقال

مثال در شکل۴، اپراتور به عنوان کنترل کننده است و PLC هدف کنترل شده می‌باشد. اپراتور ی‌ی تواند درخواست خود را از طریق Pushbut-ton برای تریپ توربین اعمال نماید، بنابراین این فرایند یک مسیر مستقیم می باشد. بازدید و اطلاعات دریافتی از دیگر اپراتورها و روش های مشاهده‌ای به عنوان یک سنسور برای اپراتور عمل می کند و اگر اپراتور تشخیص دهد، می تواند دستور تریپ سیستم را صادر نماید. Pushbutton به اپراتور اجازه می دهد که نظارت کامل بر سیستم داشته و در مواقع اضطراری به صورت استراتژیک عمل کرده و سیستم را خاموش کند.

یکی دیگر از موارد حساس و ویژه، زمانی است که کنترل‌کننده یک کنترل کننده انسانی است، که آنالیز آن بسیار پیچیده خواهد بود. بنابراین، وقتی مدل اپراتورها از جمله مدل الگوریتم و مدل منطق اپراتور آنالیز می شود، باید دستورالعمل های عملیاتی، آموزش و تجربه های عملیاتی را در نظر بگیریم، زیرا این عوامل بین مدل طراح و مدل اپراتور نقش به سزایی را ایفا می کند.

عوامل سببی شناسایی شده مربوط به خطر 1A نظیر کنترل ورودی (از اپراتور) اشتباه یا فراموش شده که تحت عنوان "نیاز به توصیف و بسط بیشتر" مشخص شده است. بدین معنا که در ساختار کنترلی سیستم، PLC نقش کنترل کننده را بازی می کنند. در حالی که در سطح پایین تر ساختار کنترلی، PLC نقش هدف کنترل شده را دارد و اپراتور دو اقدام کنترلی (فرمان تریپ و فرمان reset) را به ترتیب ارسال می‌کند. بنابراین با توجه به اهمیت اقدام، "کنترل ورودی (از اپراتور) اشتباه یا فراموش شده" درآینده برای

ساختار کنترلی سطوح پایین تر باید بسط و آنالیز بیشتری یابد.

برخی از گزینه های مشخص شده تحت عنوان "نیاز به اطلاعات بیشتر می‌باشد"بدان معنی است که اطلاعات و جزییات بیشتری مورد نیاز است. در این تحقیق، تنها از مستندات و مدارکی که در دفترچه راهنمای توسعه نیروگاه ارایه شده بود استفاده گردید. بنابراین، عوامل سببی قسمت های دیگر در حلقه کنترلی با "نیاز به اطلاعات بیشتر" مشخص شده است.

نتایج مطالعه حاضر با شناسایی حالت های نقص و علل احتمالی قسمت های نرم افزاری اجزای PLC مانند الگوریتم کنترل، بر وجود نقاط ضعف متعدد در سایر روش‌های سنتی تجزیه و تحلیل خطر در سیستم مورد مطالعه تاکید می‌کند. در این روش به دلیل وجود یک ساختار کنترلی مناسب که دید تحلیل گر را به سمت تمام حلقه کنترلی سیستم هدایت می‌کند، تمام قسمت‌های سیستم خاموش کننده را تحت پوشش دارد. به طوری که هیچ یک از مطالعات قبلی کاربردی شناسایی خطرات با استفاده از روش FMEA و غیره در نیروگاه نتوانسته این قسمت های خاص از سیستم را شناسایی و کشف کند. در این خصوص، مطالعه‌ای که توسط یائو سانگ یاو (Yao Sung) در سال ۲۰۱۲ با عنوان کاربرد مدل تئوریک حادثه (STAMP) در تجزیه و تحلیل خطرات سیستم های خاموش کننده نیروگاه اتمی تولید برق آنتاریو بر روی راکتورها انجام شد، بیان می‌کند که در صورت وجود یک روش با ایجاد یک ساختار کنترلی مناسب و راهنمایی واضح با روش STPA، می‌توان نقاط ضعف FMEA را پوشش داد که قسمت های مدل نرم افزاری توسط کامپیوتر برای هدایت راکتورها با مطالعه حاضر همخوانی دارد.

نتایج مطالعه‌ای که سان های لی (SunHwiLee) و همکارانش در سال ۲۰۱۲ با کاربرد نرم افزاری STPA جهت تجزیه و تحلیل خطر انجام دادند، نشان داد که این روش به کارشناس ایمنی در شناسایی عمیق خطرات و با در نظر گرفتن همه جوانب کمک خواهد کرد و در تجزیه و تحلیل خطر سیستم های حساس (خاموش کننده ها) و برای همه فازهای سیستم مناسب است. (Lee *et al.,* 2012). در این راستا و در مطالعه ای که توسط آقای فردریک آسپلوند (Fredrik Asplund) و همکاران در سال ۲۰۱۲ با عنوان "طراحی راهنمای ایمنی از طریق آنالیز سیستم تئوریک"، انجام گرفت، ایشان شناسایی خطرات را با رویکرد سیستماتیک و یکپارچه سازی اصول مهندسی و ایمنی در قالب طراحی مجدد سیستم پیشنهاد نمودند (Fredrik *et al.,* 2012).

نتایج نشان می دهد که روش STPA در سیستم هایی که دارای حساسیت و پیچیدگی می باشند به خوبی قابلیت اجرا دارد و می تواند به عنوان یک راهنما تحلیل گر را به سمت شناسایی و تجزیه و تحلیل بهتر خطر سوق دهد. با توجه به نتایج مطالعه حاضر روش STPA با توجه به ساختار مدون و سیستماتیک خود می‌تواند در شناسایی کامل تر خطرات و عوامل سببی ایجاد کننده ی خطرات در سیستم‌های خاموش کننده اضطراری مؤثر باشد. بنابراین توسعه چنین ابزارهایی برای افراد درگیر با سیستم های حساس از نظر ایمنی مفید خواهد بود

تشکر و قدردانی

این مقاله بخشی از پایان نامه کارشناسی ارشد اسماعیل کرمی به شماره‌ی U-92039 می‌باشد که با حمایت مالی دانشگاه علوم پزشکی جندی شاپور اهواز انجام شده است که بدینوسیله از دانشگاه مذکور تقدیر و تشکر می شود.

منابع

Asplund Fredrik, El-khoury Jad, Royal KTH, Törngren M. Safety-Guided Design through System-Theoretic Process Analysis, Benefits and Difficulties. 2012. Ebookbrows. Available at:http://ebookbrowse.com/safety-guided-design-through-system-theoretic-process analysis-benefits-and-issues-pdf-d391575967

Haapanen Pentti, Helminen Atte. Failure mode and effects analysis of software -based automation systems. STUK-YTO-TR 190 (VTT Industrial Systems) 2002; 35.

Hollnagel, E. Barriers and Accident Prevention. England Ashgate Publishing Company Suite 420 101 Cherry Street Burlington. Ashgate.2004.

Ishimatsu et al. Modeling and Hazard Analysis Using STPA, Proceedings of the 4th IAASS Conference, Making Safety Matter SP-680. (2010).

Konstantinos Kazaras, Konstantinos Kirytopoulos, Athanasios Rentizelas. Introducing the STAMP method in road tunnel safety assessment. Safety Science 2012; 50:1806–1817

Leveson, N. G. A New Accident Model for Engineering Safer Systems. Safety Science. 2004;42: 237-270.

Leveson, N. G. Engineering a Safer World. Engineering Systems. The MIT Press. 2011.

Leveson, N. G. Safety as a System Property. Communications of the ACM 1995; 38:1-11.

Misra, K. B. Handbook of Performability Engineering.Springer.2008;38(1)

Parnas, D. L., van Schouwen, A. J., and Kwan, S. P. Evaluation of Safety-Critical Software. Communications of the ACM 1990; 33: 1-6

Shirali, Gh. A. (In translation) Resilience engineering: Concepts and precepts. Hollnagel, E. Tehran: yazda.2011.

Song, Yao .Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis. Open Access Dissertationsand Theses.2012. http://digitalcommons.mcmaster.ca/opendissertations/6801.

Sun Hwi Lee, sanghyun Yoon, Junbeom Yoo. SW_ STEPA :A software Hazard Analysis Technique based on STEPA. Korea-Japan Workshop on ICT.2012;03:20-22

Weber, W., Tondok, H., and Bachmayer, M. Enhancing Software Safety by Fault Trees: Experiences from an Application to Flight Critical SW. In Knowledge Based Intelligent Information and Engineering Systems, 2003; 289-302.

Analyzing Hazards using System Theoretic process analysis (STPA) Methodology: A Case Study In The emergency extinguishing systems of Thermal power plant

E. Karami[1]; Z. Goodarzi[2]; T. Hosseinzadeh[2]; G. A. Shirali[3*]

[1]M.sc., Department of Occupational Health Engineering, School of Public Health, University of Medical Sciences, Semnan, Iran.
[2]M.sc., School of Public Health, Jundishapur University of Medical Sciences, Ahvaz, Iran.
[3]Assistant Professor, Department of Occupational Health Engineering, School of Public Health, Jundishapur University of Medical Sciences, Ahvaz, Iran.

Abstract

Introduction: The weaknesses of traditional hazard analysis methods lead to their inefficiency to utilization for modern socio-technical systems. System Theoretic Process Analysis (STPA), which is in the category of systematic analysis methods, has a powerful logic to identify hazards in such systems,as a suitable alternative method. This study aimed to analyze hazards associated with extinguishing systems of steam unit of a power plant, using STPA method.

Material and Method: The present research is a qualitative case study. The related hazards were defined using STPA method.Following, the safety control structure diagrams in different parts were plotted and inadequate control measures and its causal factors were identified.

Result: For steam unit of power plant, the most tragic incidents wererelated to hazards and risks of turbine device (switch the turbine cycle). Then, according to the plotted diagram for structure of safety control extinguishing systems associated with switching the turbine cycle, PLC system was determined as the most important part of the control system and operator was identified as the strategic and effective part of a control system. Following, more than 54 causal factors were identified, considering the relevant details about the risks analysis of the turbine.

Conclusion: Due to its systematic structure,STPA method can be effective for a more complete identification of risks and causal factors which causing hazards in the emergency extinguishing systems. Therefore, development of such tools for those operators involved in safety-critical systems will be useful in terms of safety.

Key words: *Hazard analysis, Thermal power plant, emergency extinguishing systems, STPA*

* Corresponding Author Email: *shirali@ajums.ac.ir*