



مدل‌سازی چرخه عملیاتی سامانه اسکادا با استفاده از شبکه پتری

پیام محمودی نصر

دانشگاه مازندران، دانشکده فنی و مهندسی، گروه مهندسی کامپیوتر، مازندران، بابلسر، ایران

چکیده

سامانه‌های اسکادا وظیفه کنترل زیرساخت‌های حیاتی را به عهده داشته و مطالعه بر روی آن‌ها از اهمیت فراوانی برخوردار است. در سامانه اسکادا وضعیت سلامت تمامی فرآیندهای صنعتی و تجهیزات میدانی در پست‌های راه دور به وسیله رویدادها و هشدارهای دریافتی در مرکز کنترل مورد پایش لحظه‌ای قرار می‌گیرند. اپراتورها با مشاهده رویدادها و هشدارها، دستورهای لازم را به منظور مدیریت و حفظ پایداری شبکه صادر می‌کنند. هرگونه تصمیم اشتباه اپراتور برای برطرف شدن هشدار می‌تواند موجب ایجاد هشدارهای جدید در شبکه شود. از آنجاکه هشدارها نقش کلیدی در سامانه اسکادا دارند، مدل‌سازی چرخه عملیاتی سامانه اسکادا برای مدیریت هشدارها تأثیر فراوانی در تحلیل عملکرد اپراتور و بررسی ناهنجاری در شبکه می‌تواند داشته باشد. در این مقاله یک مدل جدید از چرخه عملیاتی سامانه اسکادا از مرحله ایجاد هشدار تا برطرف شدن آن توسط اپراتور با استفاده از شبکه‌های پتری رنگی ارائه شده است. به منظور ارزیابی مدل پیشنهادی، چند سناریو در چند مورد کاوی مختلف بررسی شده، و نتایج به دست آمده نشان می‌دهد که مدل ارائه شده از کارایی لازم در شبیه‌سازی رفتارهای پست، شبکه و اپراتور برخوردار است.

واژگان کلیدی: چرخه عملیاتی، هشدار، مدل‌سازی، اسکادا، شبکه‌های پتری.

A Petri-net Model for Operational Cycle in SCADA Systems

Payam Mahmoudi Nasr

Department of Computer Engineering and Information Technology, University of Mazandaran, Mazandaran, Iran

Abstract

Supervisory control and data acquisition (SCADA) system monitors and controls industrial processes in critical infrastructures (CIs) and plays the vital role in maintaining the reliability of CIs such as power, oil, and gas system. In fact, SCADA system refers to the set of control process, which measures and monitors sensors in remote substations from a control center. These sensors usually have a type of automated response capability when a certain criteria is met. When an abnormal system status occurs, an alarm signal is raised in control center and as a result the operator will be notified. In this way, all normal and abnormal system statuses are monitored in control center. In CI's application, since several substation resources and their related sensors are too high (because the CI's grid is often large, complex and wide), the number of alarms is very high. It gets worse when the operator mistakes and as a result, cascading alarms are flooded. In this condition, the rate of raising alarms may be more than clearing them.

In SCADA system, alarm clearing is one of the main duties of operators. When an alarm is raised in control center, the operator should clear it as soon as possible. However, the recent reports confirm the poor alarm clearing causes accidents in the SCADA system. As any operator mistake can increase the number of

* Corresponding author

*نویسنده عهده‌دار مکاتبات

alarms and jeopardize the system reliability, alarms processing and decision-making for clearing them are a stressful and time-consuming for the SCADA operators. In a large and complex CI such as power system, when operators are overwhelmed by the system alarms, they may take wrong decisions and even ignore alarms. Alarm flooding, lots of operator's workload and his/her fatigue as a result, are the main causes of operator's mistake.

If generating of an alarm in a remote substation is denoted as an *operational cycle* in an SCADA system until clearing it by the operator in control center, the aim of this paper is modeling the operational cycle by using colored petri nets. The proposed model is based on a general approach which alarm messages are integrated with the operator's commands. Of course, the model focuses on generating of alarms by substation resources. To verify the proposed model, a real data set of power system of Iran is used and to demonstrate the potential of the proposed model some scenarios about operator's workload and alarm flooding are simulated.

Keywords: Alarm, Modeling, Operational cycle, Petri nets, SCADA.

امروزه با وجود آن که سامانه‌های اتوماسیون در کاربردهای مختلفی استفاده می‌شوند، اما همچنان اپراتورها در سامانه‌های اسکادا نقش اساسی ایفا می‌کنند. هرگونه تأخیر و اشتباه (عمدی یا غیرعمدی) آن‌ها می‌تواند خسارت‌های جبران‌ناپذیری به همراه داشته و پایداری شبکه را با مشکل روبه‌رو کند [4, 5]؛ به همین دلیل پژوهش‌های فراوانی تاکنون در مورد سامانه هشدار اسکادا با هدف کمک به اپراتور انجام گرفته است. پژوهشی در مورد اثر فراوانی هشدارها و نحوه نمایش آن‌ها بر کارایی اپراتور در [6] انجام شده است. روشی برای استخراج انواع الگوی خطا با توجه به هشدارهای ثبت‌شده و وزندهی هشدارها با هدف کمک به اپراتور در تشخیص خطا در [7] ارائه شده است. منبع [8] روشی برای یافتن الگوی تکرار ترافیک هشدارها در شبکه‌های صنعتی ارائه کرده است. منبع [9] با استفاده از شبکه‌های پتری یک سامانه هشدار مبتنی بر فازی ارائه کرده است. در منبع [10] یک سامانه استنتاج مبتنی بر فازی و ریسک با هدف کمک به اپراتور برای تشخیص خرابی در شبکه برق ارائه شده است. یک مدل پتری از سامانه‌های حفاظتی به منظور پیدا کردن محل خرابی در شبکه الکتریکی هوشمند در [11] ارائه شده است. در مرجع [12] با استفاده از شبکه‌های پتری مبتنی بر فازی یک سامانه هشدار با توجه به جنبه‌های اقتصادی در بازار برق ارائه شده است.

از آنجایی که در میان حجم زیاد ترافیک داده‌های ورودی اسکادا، توجه به هشدارها برای حفظ پایداری شبکه از اهمیت بالایی برخوردار است، این مقاله مدلی مبتنی بر شبکه‌های پتری رنگی برای چرخه هشدار سامانه اسکادا (از پست تا مرکز کنترل و برعکس) در شبکه الکتریکی ارائه کرده است. در این مدل (۱) ترافیک هشدارهای سامانه اسکادا و (۲) رفتار اپراتور در مرکز کنترل با استفاده از قابلیت‌های موجود در شبکه‌های پتری رنگی مدل‌سازی شده

۱- مقدمه

سامانه‌های اسکادا^۱ در زیرساخت‌های حیاتی^۲ متفاوتی مانند شبکه‌های توزیع برق، آب، نفت و گاز استفاده می‌شوند و نقش به‌سزایی در حفظ پایداری شبکه، امنیت ملی و فعالیت‌های اقتصادی در هر کشور دارند. یکی از بخش‌های مهم اسکادا، سامانه هشدار آن است. هنگامی که خطا یا خرابی در یکی از تجهیزات شبکه به وجود می‌آید، سامانه‌های حفاظتی در پست، هشدار(های) مربوطه را برای سامانه هشدار اسکادا ارسال کرده تا توسط اپراتور اقدام مقتضی به منظور برطرف شدن آن(ها) انجام گیرد.

در شبکه‌های گسترده و پیچیده‌ای مانند شبکه انتقال و توزیع برق، یک اختلال اساسی ممکن است گاهی صدها هشدار و رویداد تکراری/غیرتکراری تولید کند که البته همگی آن‌ها معتبر نیستند. بررسی این حجم زیاد هشدار و رویداد خارج از توان اپراتور اسکادا بوده و مانع از بررسی دقیق و تصمیم‌گیری صحیح در مورد نحوه برطرف کردن آن‌ها خواهد شد. این موضوع موجب می‌شود تا اپراتور با استرس کاری فراوانی مواجه شده و گاه برحسب عادت، هشدارها را به‌طور گروهي تصدیق^۳ و یا نادیده^۴ فرض کند [1]. با توجه به مطالعات انجام‌شده، چنین وضعیتی هنگامی به وجود می‌آید که هشدارها دارای اولویت نبوده و تعداد آن‌ها بیش از ده عدد در هر ده دقیقه باشد [2]. پژوهشی از ۸۷ شرکت توزیع برق نشان می‌دهد که تعداد زیاد هشدارهای تکراری و عدم اولویت‌بندی آنها از جمله بزرگ‌ترین مشکلات اپراتورهای اسکادا بوده و بیش از یک دهه است که اپراتورها با چنین مشکلی مواجه هستند [3]. هدف این مقاله ارائه مدلی برای درک بهتر سامانه هشدار اسکادا و نحوه عملکرد آن است.

¹ Supervisory Control And Data Acquisition (SCADA)

² Critical Infrastructure

³ Acknowledge

⁴ Ignore

آینده، کاربرد فراوان دارد. شکل (۱) ساختار کلی سامانه اسکادا را نشان می‌دهد.



(شکل-۱): ساختار کلی سامانه اسکادا
(Figure-1): SCADA system architecture

(جدول-۱): تعدادی از هشدارهای اصلی و فرعی

در اسکادای برق [12]

(Table-1): Sample Major/Minor alarms of Power system SCADA [12]

توضیحات	نوع
-CB failure, e.g. air or gas low pressure -AC/DC supply failure, e.g. DC indication supply failure -Sensitive over current alarm -Transformer mechanical alarm e.g. cooling system fail -Line distance faulty, e.g. distance power swing blocking	هشدارهای اصلی
-Bus bar high/low voltage alarm -Line distance protection operated -Feeder protection trip, e.g. over current protection operated -Trans. main protection trip e.g. differential relay operated -CB blocking and auto tripping	هشدارهای فرعی

۲-۲- داده‌های اسکادا

ترافیک داده‌های اسکادا شامل مجموعه رویدادها و هشدارها است که به صورت زیر گروه‌بندی می‌شوند [14]: (۱) داده‌های اندازه‌گیری شده برای مقادیر آنالوگ، مانند مقادیر ولتاژ، جریان، توان اکتیو و راکتیو. (۲) داده‌های وضعیتی برای مقادیر دیجیتال، مانند وضعیت باز یا بسته بودن کلیدهای قدرت. (۳) هشدارها برای نشان دادن هر تغییر غیرعادی، خرابی و خطا در عملکرد تجهیزات، مانند هشدار پایین بودن سطح روغن، هشدار خرابی سامانه خنک‌کننده. (۴) دستورهای کنترلی دیسپاچر، مانند دستور باز یا بسته شدن کلید قدرت.

به منظور داشتن تصویری پویا و زنده از شرایط شبکه، داده‌های سامانه اسکادا به طور معمول در هر دو تا پنج ثانیه جمع‌آوری می‌شوند. در این میان هشدارها که نیازمند توجه بیشتر اپراتور هستند سهم کوچکی را به خود اختصاص

است. به عبارتی این مقاله یک توصیف شیء‌گرا از جریان هشدارها و فعالیت‌های اپراتور با استفاده از قابلیت‌های خصیصه (رنگ و نوع) و تابع در شبکه‌های پتری رنگی ارائه کرده است. به منظور راستی‌آزمایی مدل پیشنهادی از داده‌های واقعی یکی از مراکز دیسپاچینگ در شبکه برق ایران استفاده شده است. همچنین برای نشان دادن طریقه استفاده از مدل پیشنهادی، چندین مورد کلیدی^۱ به همراه سناریوهای مختلف برای اندازه‌گیری حجم کاری اپراتور و بررسی نرخ ایجاد هشدارهای آشناری^۲ در سامانه اسکادای شبیه‌سازی شده ارائه شده است.

در ادامه در بخش دوم، مبانی سامانه‌های اسکادا و شبکه‌های پتری به اختصار مرور و مدل پیشنهادی برای سامانه هشدار اسکادا در بخش سوم ارائه می‌شود. بخش چهارم نحوه ارزیابی مدل و نتایج شبیه‌سازی را نشان می‌دهد. در بخش پنجم نتایج حاصل از این مقاله آورده شده است.

۲- پیش‌زمینه

۲-۱- سامانه اسکادا

سامانه‌های اسکادا وظیفه پایش^۳ و کنترل عملیات شبکه‌های صنعتی را به عهده دارند. در این سامانه‌ها داده‌های اندازه‌گیری شده در پست‌ها به وسیله پایانه‌های راه دور^۴ جمع‌آوری و از طریق یک شبکه مخابراتی خصوصی و یا عمومی برای مرکز کنترل ارسال و در صفحه‌نمایش کاربر نشان داده می‌شوند. سامانه هشدار اسکادا در سرویس‌دهنده HMI^۵ داده‌های دریافتی در مرکز کنترل را به اپراتور نمایش داده و برعکس فرمان‌های کنترلی اپراتور را برای تجهیزات داخل پست‌ها ارسال می‌کند [13]. هرگونه تغییر در شرایط سامانه که نیازمند توجه اپراتور باشد در قالب یک هشدار اعلام خواهد شد. اپراتور با بررسی رویدادها و هشدارهای دریافتی، ابتدا آن‌ها را تصدیق کرده و سپس دستورهای کنترلی لازم را به منظور برطرف کردن هشدارها ارسال می‌کند. تمامی داده‌ها و فرمان‌ها در سرویس‌دهنده بایگانی^۶ ذخیره می‌شوند. این داده‌ها در ارزیابی نحوه عملکرد تجهیزات، بررسی مهارت اپراتور و در تصمیم‌گیری‌های

¹ Case study

² Cascade alarms

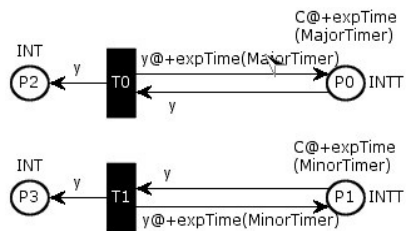
³ Monitoring

⁴ Remote Terminal Unit (RTU)

⁵ Human Machine Interface (HMI)

⁶ Historian Server

در هر زمان با نشانه‌های موجود در مکان‌ها نشان داده می‌شود. رنگ‌های تعریف شده برای مکان‌ها مانع ورود هر نوع نشانه در آن‌ها می‌شود. به عبارت دیگر رنگ نشانه‌های موجود در هر مکان با رنگ مکان یکسان است. انتقال‌ها به‌عنوان توابع عملیاتی سامانه در مدل هستند. توابع وابسته به انتقال‌ها و بردارها اجرای مدل را کنترل می‌کنند. یک انتقال به شرطی عمل می‌کند که (۱) مکان‌های ورودی آن شامل نشانه باشند، (۲) مقدار بازگشتی تابع گارد آن (در صورت وجود) درست باشد، (۳) توابع بردارهای ورودی آن اجرا شوند. در شبکه‌های پتری رنگی برای هر یک از مکان‌ها، انتقال‌ها، و نشانه‌ها می‌توان زمان تعریف کرد. زمان هر نشانه معین می‌کند که در چه زمانی آن نشانه می‌تواند از مکان خود خارج شود. نشانه‌های زمان‌دار در مکان‌های زمان‌دار قرار می‌گیرند. زمان هر انتقال مقدار تأخیر ایجاد شده توسط آن انتقال هنگام اجرای مدل را نشان می‌دهد. برای انتقال‌های زمان‌دار از مستطیل سفید و برای انتقال‌های بدون زمان از مستطیل سیاه استفاده می‌شود [15, 16].



(شکل-۲): مدل پتری رنگی ایجاد هشدارهای اصلی و فرعی در

یک منبع تولید هشدار

(Figure-2): A color Petri net model for Major/Minor alarms

۳-۲-۳ مدل پیشنهادی سامانه هشدار اسکادا

در سامانه هشدار اسکادا، هشدارها و اپراتورها نقش اساسی دارند. در مدل‌سازی سامانه هشدار اسکادا با استفاده از شبکه‌های پتری رنگی می‌توان از نشانه‌ها به‌عنوان هشدارها و از رنگ نشانه‌ها برای تعیین نوع هشدار استفاده و همچنین با استفاده از ویژگی زمان برای هر نشانه می‌توان زمان ایجاد هشدار و برطرف شدن آن را شبیه‌سازی و برای شبیه‌سازی رفتار اپراتور در هر مرحله از پردازش می‌توان از انتقال‌ها و توابع آنها استفاده و همچنین از انتقال‌های زمان‌دار برای شبیه‌سازی تأخیر اپراتور در پردازش هشدارها می‌توان استفاده کرد.

می‌دهند. رویدادها در مقایسه با هشدارها، ارزش چندانی ندارند و تنها برای آگاهی اپراتور از وضعیت جاری سامانه استفاده می‌شوند. هشدارها از نظر ماندگاری به دو گروه گذرا و پایدار تقسیم می‌شوند. هشدارهای گذرا هشدارهایی هستند که با ارسال دستور اپراتور از راه دور به‌راحتی برطرف می‌شوند؛ درحالی‌که هشدارهای پایدار نیازمند عملیات تعمیر و نگهداری برای برطرف شدن هستند و به همین دلیل برای مدت بیشتری (گاهی تا چند روز) بر روی صفحه‌نمایش اپراتور باقی می‌مانند. هشدارها به‌لحاظ درجه اهمیت نیز به دو گروه اصلی^۱ و فرعی^۲ تقسیم می‌شوند [14]:

(۱) هشدارهای اصلی: این گروه از هشدارها که ممکن است گذرا و یا پایدار باشند، به این دلیل اصلی نامیده می‌شوند که اپراتور برای برطرف کردن آن‌ها بایستی هرچه سریع‌تر اقدام کند تا از بروز هشدارهای جدی‌تر جلوگیری به عمل آید. عواملی مانند الگوی مصرف صحیح، دمای مناسب محیط، بازدیدهای دوره‌ای و تعویض تجهیزات قدیمی تأثیر فراوانی در کاهش تعداد هشدارهای اصلی دارند.

(۲) هشدارهای فرعی: این گروه از هشدارها خرابی‌های جدی و گاهی خاموشی‌های گسترده‌تری را در پی دارند؛ اما به این دلیل فرعی نامیده می‌شوند که تعداد آن‌ها در شبکه بسیار کم است. درواقع اپراتور با برطرف کردن به‌موقع هشدارهای اصلی مانع به‌وجود آمدن هشدارهای فرعی، خواهد شد. عدم بازدیدهای دوره‌ای، برطرف نشدن به‌موقع هشدارهای اصلی و بلایای طبیعی تأثیر فراوانی در افزایش تعداد هشدارهای فرعی دارد. جدول (۱) تعدادی از هشدارهای اصلی و فرعی برای سامانه اسکادا در شبکه الکتریکی را نشان می‌دهد.

۳-۲-۳ شبکه‌های پتری رنگی

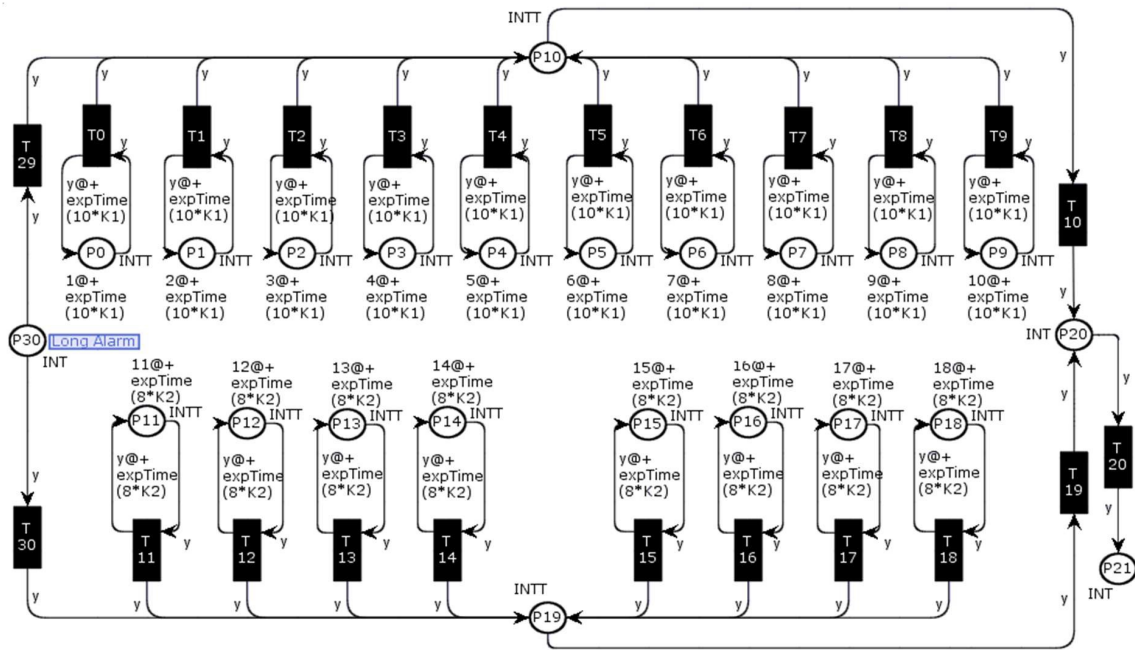
شبکه‌های پتری ابزاری ساده و گرافیکی برای مدل‌سازی رفتار سامانه‌های با رویدادهای غیرهم‌زمان، پردازش هم‌زمان و مدیریت منابع است. شبکه‌های پتری ابزاری مناسب برای تحلیل رفتار سامانه‌های صنعتی مانند تأسیسات تولیدی و شبکه‌های توزیع برق، آب، گاز و نفت است [15].

در شبکه پتری رنگی مکان‌ها برای نمایش منابع و وضعیت‌های سامانه استفاده می‌شوند. هر مکان می‌تواند حاوی تعدادی نشانه^۳ باشد. هر نشانه حاوی اطلاعاتی است که تحت عنوان رنگ نشانه شناخته می‌شود. وضعیت سامانه

¹ Major alarms

² Minor alarms

³ Token



(شکل-۳): مدل پتری رنگی ایجاد ترافیک هشدارها در پست
 (Figure-3): A Colored petri net model for alarm generation in substation

۱-۳- مدل ایجاد ترافیک هشدارها در پست

برای هر یک از منابع تولید هشدار در پست با توجه به آن که هشدار اصلی/فرعی و یا هر دو را ایجاد می‌کند می‌توان یک یا دو مکان به ترتیب برای هشدارهای اصلی و فرعی در نظر گرفت. در شکل (۲) مدل پتری رنگی برای ایجاد هشدارهای اصلی و فرعی در یک منبع هشدار نشان داده شده است. مکان‌های زمان دار P_0 و P_1 به ترتیب برای ایجاد هشدارهای اصلی و فرعی در نظر گرفته شده‌اند. از انتقال‌های T_0 و T_1 برای انتقال هشدارهای ایجاد شده به مکان‌های دیگر (مانند P_2 و P_3) و همچنین ایجاد نشانه در مکان‌های P_0 و P_1 برای به منظور ایجاد هشدارهای جدید استفاده شده است. برای نزدیکی بیشتر به دنیای واقعی از توزیع پواسون به منظور مدل‌سازی تعداد هشدارهای ایجاد شده در یک منبع (مکان‌های P_0 و P_1) استفاده شده است. لازم به توضیح است که همواره در سامانه‌های کاربردی از توزیع پواسون برای مدل‌سازی توزیع آماری تعداد انواع رویدادهای ایجاد شده استفاده می‌شود (مانند تعداد قطعات معیوب در یک خط تولیدی، تعداد خطاهای ایجاد شده در یک پردازش، تعداد پیام‌های دریافتی در واحد زمان، تعداد عبور ماشین از یک خیابان و غیره) [17]. لازمه این استفاده آن است که منابع بالقوه برای ایجاد رویدادها بی‌نهایت زیاد و احتمال مشاهده رویداد در هر یک از منابع ثابت و کم باشد. در سامانه اسکادا

از آنجایی که احتمال وقوع هشدار در هر یک از منابع کم بوده و تعداد منابع بالقوه تولید هشدار به دلیل بزرگی و گستردگی شبکه انتقال و توزیع به اندازه کافی زیاد است، از توزیع پواسون برای مدل‌سازی ترافیک هشدارهای ایجاد شده در آن می‌توان استفاده کرد [18, 19]. چنانچه تعداد رویدادها از توزیع پواسون با پارامتر $1/K$ پیروی کند، زمان وقوع بین رویدادها از توزیع نمایی با پارامتر K پیروی خواهد کرد $(exp(k))$ [17]. به همین دلیل در مکان‌های P_0 و P_1 از توزیع نمایی با پارامترهای MajorTimer و MinorTimer برای هر یک از هشدارهای اصلی و فرعی استفاده شده است. به منظور ایجاد تمایز بین هشدارها در منابع مختلف می‌توان از مقادیر متفاوتی برای متغیر C (در مکان‌های P_0 و P_1) به ازای هر منبع تولید هشدار استفاده کرد.

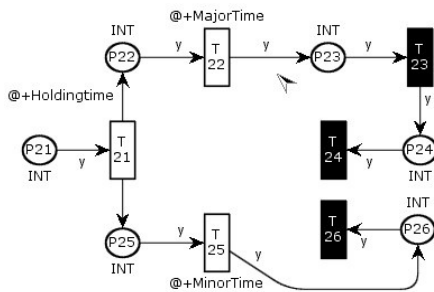
شکل (۳) مدل ایجاد هشدارهای اصلی و فرعی در یک پست را با توجه به منابع مختلف تولید هشدار نشان می‌دهد. از آنجایی که منابع تولید هشدار در پست‌های انتقال و فوق توزیع به طور معمول به نه بخش شامل خطوط انتقال، فیدرهای خروجی، باسبار، ترانس‌های قدرت، خازن‌ها، راکتورها، تجهیزات عمومی پست، مقادیر اندازه‌گیری و تغییر وضعیت‌ها تقسیم می‌شوند [14]، در شکل (۳) نیز منابع تولید هشدار به نه بخش تقسیم شده‌اند. جداول (۲) و (۳) به ترتیب مکان‌ها و انتقال‌ها استفاده شده در مدل پیشنهادی

را نمایش می‌دهد. مکان‌های زمان‌دار P_0 تا P_8 منابع تولید هشدارهای اصلی، و مکان‌های زمان‌دار P_{11} تا P_{17} منابع تولید هشدارهای فرعی را نشان می‌دهند. به دلیل آن که هشدارهای مربوط به مقادیر اندازه‌گیری و تغییر وضعیت‌ها تنها به‌عنوان هشدارهای اصلی در سامانه اسکادا بررسی می‌شوند [14] لذا از تعداد مکان کمتری برای هشدارهای فرعی استفاده شده است. نشانه‌های موجود در مکان‌های نام‌برده شده زمان‌دار بوده و هر یک از آن‌ها نماینده یک خرابی یا خطا در منبع مربوطه هستند. مکان‌های زمان‌دار P_9 و P_{18} به‌ترتیب برای ایجاد هشدارهای کاذب و تکراری (اصلی و فرعی) در نظر گرفته شده‌اند. به‌منظور ایجاد تمایز بین هشدارهای منابع مختلف، از مقادیر یک تا ده به‌عنوان رنگ نشانه‌های هشدارهای اصلی، و یازده تا هجده به‌عنوان رنگ نشانه‌های هشدارهای فرعی استفاده شده است. به این ترتیب مکان‌های P_{10} ، P_{19} به‌ترتیب مجموع هشدارهای اصلی و فرعی ایجاد شده در پست را نشان می‌دهند. این هشدارها به‌وسیله انتقال‌های T_{10} ، T_{19} به RTU (مکان P_{20}) و توسط انتقال T_{20} به مرکز کنترل (مکان P_{21}) منتقل می‌شوند. مکان P_{21} حاوی تمامی هشدارهای اصلی و فرعی دریافتی در مرکز کنترل است. به‌منظور آن که از توزیع پواسون با پارامترهای $1/K_1$ ، $1/K_2$ به‌ترتیب برای تعداد هشدارهای اصلی و فرعی استفاده شود و از آنجا که تعداد منابع تولید هشدارهای اصلی و فرعی (با در نظر گرفتن هشدارهای کاذب) در مدل ارائه شده به‌ترتیب ده و هشت در نظر گرفته شده است، از مقادیر $\exp(10 \cdot k_1)$ ، $\exp(8 \cdot k_2)$ به‌عنوان مقدار اولیه در مکان‌های هشدارهای اصلی و فرعی در مکان‌های P_{10} ، P_{19} دارای توزیع نمایی با مقادیر $\exp(k_1)$ ، $\exp(k_2)$ در نظر گرفته شوند.

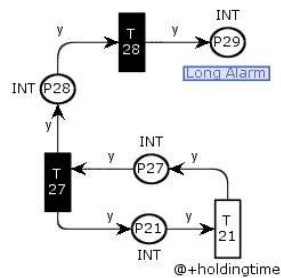
عامل دیگری که در یک پست ممکن است موجب ایجاد هشدارهای جدید شود، هشدارهای برطرف‌نشده طولانی است. هشدار که برای مدت طولانی برطرف نشده باشد برحسب تأثیری که در پست دارد، می‌تواند به‌صورت آشناری عامل ایجاد هشدارهای جدید گردد [20]. برای این منظور از مکان P_{30} برای نمایش هشدارهای برطرف نشده طولانی استفاده شده است. نشانه‌های موجود در مکان P_{30} توسط انتقال T_{29} یا T_{30} یک هشدار جدید اصلی یا فرعی را ایجاد می‌کنند.

۳-۲- مدل پردازش هشدار توسط اپراتور

شکل (۴) مدل پردازش هشدار توسط اپراتور هنگام برطرف کردن هشدارها را نشان می‌دهد. تصمیم‌گیری برای انتخاب فرمان صحیح به‌منظور برطرف کردن هر یک از هشدارها نیاز به زمان دارد؛ لذا انتقال‌های T_{21} ، T_{22} ، T_{25} از نوع انتقال‌های زمان‌دار در نظر گرفته شده‌اند. هر یک از هشدارها ابتدا در انتقال T_{21} تصدیق شده (تأیید دریافت و مشاهده توسط اپراتور) و سپس فرمان لازم برای برطرف شدن آن‌ها در انتقال‌های T_{22} (برای هشدارهای اصلی) یا T_{25} (برای هشدارهای فرعی) صادر می‌شود. از آنجایی که تأخیر پاسخ‌گویی و نحوه برطرف کردن هشدارهای اصلی و فرعی می‌تواند متفاوت باشد، از انتقال‌های جداگانه‌ای برای برطرف شدن آن‌ها استفاده شده است. به‌منظور نزدیک شدن به شرایط واقعی از متغیرهای $HoldingTime$ ، $MajorTime$ ، $MinorTime$ به‌ترتیب برای شبیه‌سازی تأخیر اپراتور هنگام تصدیق و پاسخ‌گویی به هر یک از هشدارهای اصلی و فرعی در انتقال‌های T_{21} ، T_{22} ، T_{25} استفاده شده است.



(شکل-۴): مدل پتری رنگی پردازش هشدار توسط اپراتور
(Figure-4): A Colored petri net model for alarm processing



(شکل-۵): مدل پتری رنگی برای هشدارهای آشناری
(Figure-5): A Colored petri net model for cascading alarms

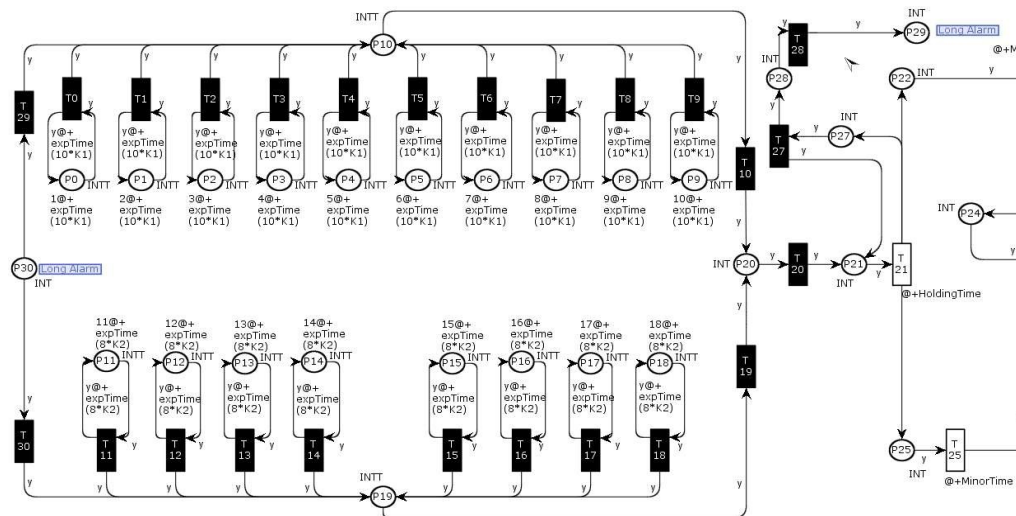
۳-۳- مدل ایجاد هشدارهای آشناری

همان‌طور که اشاره شد، چنانچه هشدار به‌موقع برطرف نشود، ممکن است عامل ایجاد هشدارهای آشناری جدید در همان پست و یا دیگر پست‌ها شود. ایجاد هشدارهای آشناری

متغیر m به عنوان درصد صدور فرمان اشتباه در تابع وابسته به انتقال T_{21} استفاده کرد. بدین ترتیب در انتقال T_{21} به احتمال $d\%$ پس از گذشت زمان $HoldingTime$ هم چنان هشدار با عدم تصدیق و بی توجهی در پاسخ گویی همراه است، و یا پس از گذشت زمان $HoldingTime$ به احتمال $m*(100-d)\%$ می شود. مکان P_{27} شامل هشدارهایی است که دچار تأخیر زیاد و یا فرمان اشتباه اپراتور شده اند. بدین ترتیب احتمال تصدیق به موقع هشدار و قرار گرفتن در چرخه صدور فرمان صحیح برای برطرف شدن در انتقال های T_{22} , T_{25} برابر با $(100 - d - m*(100-d))$ خواهد بود. انتقال T_{27} هشدارهای موجود در P_{27} را علاوه بر آن که دوباره در مکان P_{21} برای بررسی مجدد اپراتور قرار می دهد، آنها را در مکان P_{28} برای ایجاد هشدارهای آبخاری قرار می دهد. انتقال T_{28} با احتمال $CP\%$ از نشانه های موجود در مکان P_{28} برای ایجاد هشدارهای آبخاری و ایجاد نشانه در مکان P_{29} استفاده می کند.

به عوامل مختلفی بستگی دارد که می توان آنها را به دو دسته کلی (الف) میزان مهارت اپراتور در برطرف کردن هشدارها و (ب) رفتار شبکه در لحظه (مانند شرایط پایداری شبکه، میزان بار شبکه، قدیمی بودن تجهیزات، نوع هشدار و غیره) تقسیم کرد. در این مقاله به منظور ساده سازی هرچه بیشتر (به دلیل آنکه نحوه ایجاد هشدارهای آبخاری خارج از موضوع این مقاله است)، از متغیرهای ساده عددی m , d , CP به ترتیب برای شبیه سازی میزان مهارت اپراتور و رفتار شبکه در لحظه استفاده شده است.

شکل (۵) مدل بسیار ساده ای را برای ایجاد هشدارهای آبخاری نشان می دهد. چنانچه اپراتور از مهارت کافی در برطرف کردن هشدارها برخوردار نباشد، ممکن است هر یک از رفتارهای زیر را هنگام پردازش هشدار از خود نشان دهد: (الف) تأخیر، به صورت عدم تصدیق و بی توجهی به هشدار و یا تأخیر در پاسخ گویی به هشدار پس از تصدیق هشدار (ب) صدور فرمان اشتباه. به منظور شبیه سازی رفتار اپراتور می توان از متغیر d به عنوان درصد تأخیر اپراتور و از



(شکل-۶): مدل پتری رنگی سیستم هشدار اسکادا برای یک پست و یک مرکز کنترل
(Figure-6): A colored Petri net model for SCADA alarm system by single substation and control center

اپراتور در مرکز کنترل به صورت مشترک برای همه پست ها استفاده خواهند شد. مکان P_{21} هشدارهای دریافت شده از تمامی پست ها را در مرکز کنترل نشان می دهد. مکان P_{29} با نام مستعار جدید در هر پست و با استفاده از ابزار پیوند به صورت مشترک بین تمامی پست ها استفاده می شود. بدین ترتیب هر هشدار که برای مدت طولانی برطرف نشده باشد، می تواند عامل ایجاد خطایی جدید در همان پست و یا دیگر پست ها شود.

۴-۳- مدل نهایی سامانه

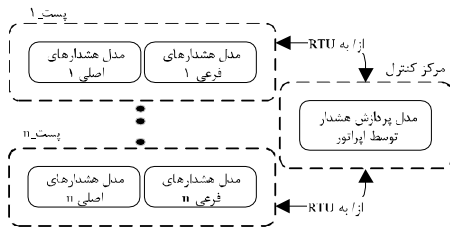
شکل (۶) مدل نهایی سامانه و جداول (۲) و (۳) به ترتیب انتقال ها و مکان های استفاده شده را برای یک مرکز کنترل و یک پست نشان می دهند. شکل (۷) نحوه افزایش تعداد پست ها را به صورت نمودار قطعی نمایش می دهد. برای هر پست جدید مدل هشدارهای اصلی و فرعی (با شماره های جدید برای مکان ها و انتقال ها) دوباره ترسیم خواهند شد. مدل های ایجاد هشدارهای آبخاری، و پردازش هشدار توسط

¹ Fusion

(جدول-۲): انتقال‌های مربوط به مدل پتری رنگی پیشنهادی

(Table-2): Transitions of the proposed model

انتقال	توضیح
T0 to T9	ایجاد هشدار اصلی
T10, T19	ارسال هشدار به RTU
T11 to T18	ایجاد هشدار فرعی
T20	ارسال هشدار از RTU به مرکز کنترل
T21	تصدیق و پردازش هشدار در مرکز کنترل
T22	ایجاد پاسخ صحیح برای برطرف شدن هشدار اصلی
T23	ارسال پاسخ صحیح به RTU
T24	برطرف شدن هشدار اصلی
T25	تصمیم‌گیری برای برطرف شدن هشدار فرعی و انجام تعمیرات
T26	برطرف شدن هشدار فرعی
T27	برطرف نشدن هشدار، ارسال پاسخ اشتباه به RTU
T28	ایجاد خطای جدید برای هشدارهای آشناری
T29	ایجاد هشدار آشناری جدید از نوع اصلی
T30	ایجاد هشدار آشناری جدید از نوع فرعی



(شکل-۷): نمودار قطعه‌ای مدل پیشنهادی برای سامانه اسکادا با چند پست

چند پست

(Figure-7): Block diagram of the proposed model by multi substations.

۴- راستی‌آزمایی و شبیه‌سازی

به‌منظور تنظیم اولیه پارامترهای کنترلی مدل پیشنهادی از داده‌های واقعی یکی از مراکز دیسپاچینگ در شبکه برق ایران که ۳۱ پست انتقال و فوق توزیع را پایش و کنترل می‌کند، استفاده شده است. جدول (۴) نتایج تحلیل داده‌های واقعی جمع‌آوری شده از ده پست انتقال و فوق توزیع به‌مدت سه ماه به‌منظور تخمین بهترین تابع توزیع برای میزان تأخیر اپراتور هنگام پردازش هشدارها را نمایش می‌دهد. همان‌طور که مشاهده می‌شود با توجه به مقادیر $P_Values > 0.05$ می‌توان از تابع توزیع $lognormal()$ به‌منظور شبیه‌سازی میزان تأخیر اپراتور هنگام تصدیق (HoldingTime) و پاسخ‌گویی به هشدارهای اصلی (MajorTime) و فرعی (MinorTime) استفاده کرد. با این فرض که هیچ‌گونه تهدیدی برای برطرف‌شدن هشدارها از طرف اپراتور وجود ندارد. همچنین با استفاده از تحلیل تعداد هشدارهای ایجادشده در داده‌های واقعی مقدار پارامتر تابع توزیع نمایی برای هشدارهای اصلی و فرعی به‌ترتیب برابر $K_1 = 100$ to $150h$ و $K_2 = 4000$ to $8760h$ (میانگین بین چهار تا هفت هشدار اصلی در ماه و بین یک تا دو هشدار فرعی در سال) و مقدار $m=d=0$ در نظر گرفته شده‌اند.

(جدول-۴): تابع توزیع تأخیر اپراتور هنگام پردازش هشدار

(Table-4): Distribution timing of timed transitions

انتقال	نوع هشدار	میزان تأخیر (دقیقه)	تابع توزیع	P-value
T ₂₁	اصلی/فرعی	[2,34]	lognormal(2.08,0.83)	0.073
T ₂₂	اصلی	[7,6100]	lognormal(4.63,1.69)	0.084
T ₂₅	فرعی	[18,28100]	lognormal(5.15,1.95)	0.099

به‌منظور راستی‌آزمایی و تحلیل مدل پیشنهادی شاخص‌های میانگین تأخیر برطرف‌شدن هشدارهای اصلی (ADJ) و فرعی (ADI) با در نظر گرفتن تعداد پست‌های

(جدول-۳): مکان‌های مربوط به مدل پتری رنگی پیشنهادی

(Table-3): Places of the proposed model

انتقال	توضیح	مقدار اولیه
P0	خطای اصلی در خطوط	$1@exp(10*K_1)$
P1	خطای اصلی در فیدرهای خروجی	$2@exp(10*K_1)$
P2	خطای اصلی در باس بار	$3@exp(10*K_1)$
P3	خطای اصلی در ترانس قدرت	$4@exp(10*K_1)$
P4	خطای اصلی در خازن‌ها	$5@exp(10*K_1)$
P5	خطای اصلی در راکتورها	$6@exp(10*K_1)$
P6	خطای اصلی در مقادیر اندازه‌گیری	$7@exp(10*K_1)$
P7	خطای اصلی در مقادیر دیجیتال	$8@exp(10*K_1)$
P8	خطای اصلی در تجهیزات عمومی	$9@exp(10*K_1)$
P9	خطای اصلی کاذب یا تکراری	$10@exp(10*K_1)$
P10	هشدار اصلی در پست	---
P11	خطای فرعی در خطوط	$11@exp(8*K_2)$
P12	خطای فرعی در فیدرهای خروجی	$12@exp(8*K_2)$
P13	خطای فرعی در باس بار	$13@exp(8*K_2)$
P14	خطای فرعی در ترانس قدرت	$14@exp(8*K_2)$
P15	خطای فرعی در خازن‌ها	$15@exp(8*K_2)$
P16	خطای فرعی در راکتورها	$16@exp(8*K_2)$
P17	خطای فرعی در تجهیزات عمومی	$17@exp(8*K_2)$
P18	خطای فرعی کاذب یا تکراری	$18@exp(8*K_2)$
P19	هشدار فرعی در پست	---
P20	درگاه خروجی RTU	---
P21	هشدار در مرکز کنترل (HMI Screen)	---
P22	هشدار اصلی تصدیق شده	---
P23	دستور یا پاسخ صحیح اپراتور	---
P24	درگاه ورودی RTU	---
P25	هشدار فرعی تصدیق شده	---
P26	تجهیزات تعمیر شده در پست	---
P27	هشدارهایی که دچار پاسخ اشتباه یا تأخیر اپراتور شده‌اند.	---
P28	هشدار برطرف نشده با مدت‌زمان طولانی	---
P29, P30	خطای آشناری جدید	---
P31, P32	ناهنجاری در شبکه و پست	---

$$K_2 = 4000 \text{ to } 8760h$$

(میانگین بین یک تا دو هشدار فرعی در سال)

$$d = m = 2\%$$

در سناریوی دوم (اپراتور ضعیف) رفتار شبکه همچنان متناظر با داده‌های واقعی فرض شده، اما اپراتور (عمدی یا غیرعمدی) در برطرف کردن هشدارها بسیار ضعیف عمل خواهد کرد:

$$d = m = 50\%$$

در سناریوی سوم (شبکه ضعیف) نرخ ایجاد هشدار در پست‌ها بیشتر از شرایط طبیعی فرض شده و رفتار اپراتور نیز از مهارت کافی برخوردار نیست:

$$K_1 = 24h \text{ (میانگین یک هشدار اصلی در روز)}$$

$$K_2 = 720h \text{ (میانگین یک هشدار فرعی در ماه)}$$

$$d = m = 10\%$$

مقدار $CP = 10\%$ در همه سناریوها به صورت مشترک در نظر گرفته شده است. در تمامی سناریوها از ابزارهای شبیه‌سازی، فضای حالت^۱ و پایش در محیط CPNTools استفاده شده است. برای شمارش تعداد نشانه‌ها در مکان‌های مورد نظر از ابزار پایش فایل^۲ بهره گرفته شده است.

(جدول-۷): مقدار پارامترهای کنترلی برای سناریوها

(Table-7): parameter values for simulation scenarios

پست‌ها					پارامترها	
E	D	C	B	A		
۱۵۰	۱۰۰	۱۲۰	۱۰۰	۱۲۰	K_1	سناریوی ۱ کنترل شبکه
۸۷۶۰	۷۰۰۰	۶۰۰۰	۵۰۰۰	۴۰۰۰	K_2	
۲	۲	۲	۲	۲	d	
۲	۲	۲	۲	۲	m	سناریوی ۲ اپراتور ضعیف
۱۵۰	۱۰۰	۱۲۰	۱۰۰	۱۲۰	K_1	
۸۷۶۰	۷۰۰۰	۶۰۰۰	۵۰۰۰	۴۰۰۰	K_2	
۵۰	۵۰	۵۰	۵۰	۵۰	d	سناریوی ۳ شبکه ضعیف
۵۰	۵۰	۵۰	۵۰	۵۰	m	
۲۴	۲۴	۲۴	۲۴	۲۴	K_1	
۷۲۰	۷۲۰	۷۲۰	۷۲۰	۷۲۰	K_2	
۱۰	۱۰	۱۰	۱۰	۱۰	d	
۱۰	۱۰	۱۰	۱۰	۱۰	m	

۱-۴- حجم کاری اپراتور

شکل (۸) حجم کاری اپراتور در هفته را برای هر سه سناریو در مدت شش ماه نشان می‌دهد. از تعداد هشدارهای دریافتی در مرکز کنترل به عنوان معیاری برای اندازه‌گیری حجم کاری اپراتور استفاده شده است. مشاهده می‌شود که اگرچه تأخیر و اشتباه اپراتور در سناریوی اپراتور ضعیف تأثیر فراوانی در افزایش تعداد هشدارهای شبکه و افزایش حجم کاری وی داشته، اما حجم کاری اپراتور در سناریوی شبکه

¹ State space

² Write in file monitoring

متفاوت (۸، ۹ و ۱۰ پست) اندازه‌گیری شده و با استفاده از آزمون میانگین تک‌نمونه‌ای با مقادیر متناظر از داده‌های واقعی مورد مقایسه و ارزیابی قرار گرفته‌اند. جداول (۵) و (۶) نتایج آزمون میانگین تک‌نمونه‌ای را برای مدت سه ماه نشان می‌دهد. نتایج به دست آمده نشان می‌دهند که اختلاف معناداری بین مقادیر اندازه‌گیری شده از داده‌های واقعی و شبیه‌سازی شده وجود ندارد. لازم به توضیح است که مقادیر شاخص‌های اندازه‌گیری شده در مدل شبیه‌سازی شده در محیط [21] CPNTools و پس از ۱۲۹۶۰۰ مرحله (معادل سه ماه) و در هر مرحله پس از هزار بار تکرار مستقل و با فاصله اطمینان ۹۵٪ اندازه‌گیری شده‌اند.

(جدول-۵): نتایج آزمون تک‌نمونه‌ای برای شاخص ADJ

به مدت سه ماه

(Table-5): Single mean test results for ADJ at 3 months

تعداد پست	t	Sig.	میانگین اختلاف	میانگین خطای استاندارد	میانگین واقعی	میانگین شبیه‌سازی شده
8	0.47	0.82	18.74	49.54	246.26	228.63
9	0.82	0.58	35.74	49.62	261.63	226.91
10	0.49	0.81	20.13	50.71	248.56	229.54

(جدول-۶): نتایج آزمون تک‌نمونه‌ای برای شاخص ADI

به مدت سه ماه

(Table-6): Single mean test results for ADI at 3 months

تعداد پست	t	Sig.	میانگین اختلاف	میانگین خطای استاندارد	میانگین واقعی	میانگین شبیه‌سازی شده
8	0.9	0.5	2658.1	2927.2	3104.8	566.9
9	-0.6	0.7	-82.3	293.2	463.1	566.3
10	-0.6	0.8	-74.6	293.2	463.2	548.6

در ادامه به منظور نمایش کاربرد مدل پیشنهادی دو موردکاوی مورد مطالعه قرار گرفته است. در هر یک از موردکاوی‌ها با تغییر در مقادیر پارامترهای کنترلی چندین سناریو با هدف تغییر در رفتار اپراتور و پست قابل مطالعه و مقایسه هستند. مدل اسکادای شبیه‌سازی شده در موردکاوی‌ها شامل پنج پست و یک مرکز کنترل است. جدول (۷) مقادیر پارامترهای کنترلی را در سه سناریوی مختلف برای هر یک از موردکاوی‌ها نشان می‌دهد. در سناریوی نخست (کنترل شبکه) با توجه به داده‌های واقعی، پارامترها به نحوی تنظیم شده‌اند که نرخ ایجاد هشدار در پست‌ها متناظر با داده‌های واقعی بوده و اپراتور نیز به نسبت از مهارت کافی برای برطرف کردن هشدارها برخوردار است:

$$K_1 = 100 \text{ to } 150h \text{ (میانگین بین چهار تا هفت هشدار اصلی در ماه)}$$

اصلی در ماه)

۵- نتیجه گیری

در این مقاله یک مدل جدید برای سامانه هشدار اسکادا با استفاده از شبکه‌های پتری رنگی ارائه شده است. این مقاله با توجه به نوع هشدارها توانست مدلی جدید برای ایجاد هشدارها در پست و پردازش آن‌ها در مرکز کنترل ارائه دهد. با برقراری ارتباط بین هشدارهای سامانه اسکادا و مکان‌های شبکه پتری رنگی، نشان داده شد که می‌توان وضعیت شبکه را در هر لحظه مورد ارزیابی قرار داد و ناهنجاری‌های احتمالی را در پست و شبکه شناسایی کرد.

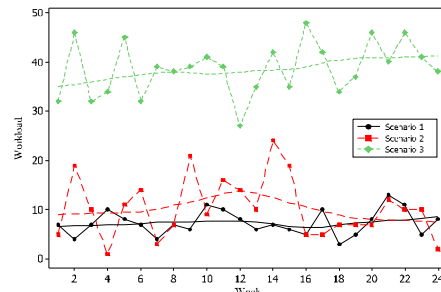
با استفاده از پارامترهای کنترلی و تغییر در آن‌ها، تأثیر بالا رفتن عوامل ایجاد هشدار در پست، عدم پردازش هشدار، تأخیر در پاسخ و پاسخ اشتباه به هشدارها در افزایش حجم کاری اپراتور، ایجاد ناهنجاری در شبکه و تعداد هشدارهای آبخاری بررسی شد. این مقاله نشان داد که شبکه‌های پتری ابزار مناسبی برای مدل‌سازی رفتار پست هنگام ایجاد هشدار و رفتار اپراتور هنگام پردازش هشدارها است.

6- References

۶- مراجع

- [1] J. Wang, F. Yang, T. Chen, and S. L. Shah, "An overview of industrial alarm systems: main causes for alarm overloading, research status, and open problems," *IEEE Transactions on Automation Science and Engineering*, vol. 13, pp. 1045-1061, 2016.
- [2] D. Li, J. Hu, H. Wang, and W. Huang, "A distributed parallel alarm management strategy for alarm reduction in chemical plants," *Journal of Process Control*, vol. 34, pp. 117-125, 2015.
- [3] Y. Wu, M. Kezunovic, and T. Kostic, "An advanced alarm processor using two-level processing structure," in *Power Tech, 2007 IEEE Lausanne, 2007*, pp. 125-130.
- [4] محمودی نصر، پیام، یزدیان ورجانی، علی، "یک سامانه مدیریت دسترسی برای کاهش تهدیدهای عملیاتی در سامانه اسکادا"، پردازش علائم و داده‌ها، دوره ۱۴، شماره ۴ - (۱۲-۱۳۹۶).
- [4] P. Mahmoudi-Nasr and A. Yazdian-Varjani, "An Access Management System to Mitigate Operational Threats in SCADA System", *JSDP*, vol. 14 (4), pp. 3-18, 2018.
- [5] P. Mahmoudi-Nasr and A. Yazdian-Varjani, "Toward Operator Access Management in SCADA System: Deontological Threat

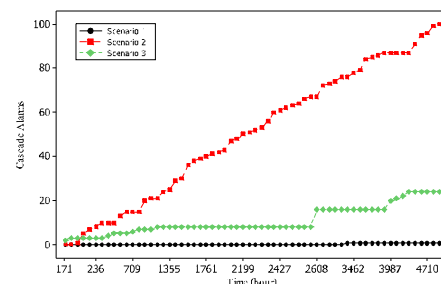
ضعیف همواره بیشترین مقدار را داشته است. این نمودار نشان می‌دهد که عواملی غیر از اپراتور که باعث افزایش تعداد هشدار در شبکه می‌شوند (مانند عدم سرویس‌های تعمیر و نگهداری به موقع و عملکرد نامناسب تجهیزات) تأثیر بیشتری در افزایش حجم کاری نسبت به تأخیر و اشتباه اپراتور دارند.



(شکل-۸): حجم کاری اپراتور برای هر سه سناریو در مدت ۶ ماه
(Figure-8): Operator workload in 6 months.

۲-۴ هشدارهای آبخاری

در این مورد کای تعداد هشدارهای آبخاری در هر سه سناریو اندازه‌گیری شده و مقایسه آن‌ها با یکدیگر در شکل (۹) نشان داده شده است. مشاهده می‌شود که اگرچه احتمال به وجود آمدن هشدارهای آبخاری به طور ثابت در هر سه سناریو برابر با ۱۰٪ در نظر گرفته شده، اما تعداد آن‌ها در سناریوی اپراتور ضعیف به دلیل خطای بیشتر اپراتور افزایش چشم‌گیری داشته است. در سناریوی شبکه ضعیف برخلاف نرخ بالای ایجاد هشدار در پست‌ها، تعداد هشدارهای آبخاری رشد کمتری داشته و در سناریوی کنترل شبکه که شبکه در شرایط پایدار است، تعداد هشدارهای آبخاری بسیار کم و در بیشتر موارد صفر است؛ لذا می‌توان نتیجه گرفت که میزان تأخیر و اشتباه اپراتور تأثیر مستقیم در نرخ ایجاد هشدارهای آبخاری دارد.



(شکل-۹): مقایسه تعداد هشدارهای آبخاری در سناریوهای مختلف
(Figure-9): Cascade alarms

Transport Solutions from Research to Deployment, 2014.

- [17] D. C. Montgomery, *Introduction to statistical quality control*: John Wiley & Sons (New York), 2009.
- [18] X. Dong, K. Hopkinson, X. Tong, X. Wang, and J. Thorp, "IP-based communication systems for wide-area frequency stability predictive control," in *Critical Infrastructure (CRIS), 2010 5th International Conference on*, 2010, pp. 1-7.
- [19] J. Zhao, Y. Xu, F. Luo, Z. Dong, and Y. Peng, "Power system fault diagnosis based on history driven differential evolution and stochastic time domain simulation," *Information Sciences*, vol. 275, pp. 13-29, 2014.
- [20] V. Rodrigo, M. Chioua, T. Hagglund, and M. Hollender, "Causal analysis for alarm flood reduction," *IFAC-PapersOnLine*, vol. 49, pp. 723-728, 2016.
- [21] (2017). <http://CPNTools.org>



پیام محمودی نصر تحصیلات خود را

در مقاطع کارشناسی و کارشناسی ارشد

مهندسی کامپیوتر به ترتیب در سال‌های

۱۳۷۳ و ۱۳۷۵ از دانشگاه صنعتی

امیرکبیر و در مقطع دکترا مهندسی

قدرت در سال ۱۳۹۵ از دانشگاه تربیت مدرس به پایان

رسانده و هم‌اکنون استادیار دانشکده فنی و مهندسی

دانشگاه مازندران است. زمینه‌های پژوهشی مورد علاقه

ایشان عبارتند از: امنیت شبکه‌های صنعتی و رایانه‌ای، امنیت

داده‌ها و شبکه‌های رایانه‌ای.

نشانی رایانامه ایشان عبارت است از:

P.mahmoudi@umz.ac.ir

Mitigation," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 3314-3324, 2018.

- [6] P. T. Bullemer, M. Tolsma, D. Reising, and J. Laberge, "Towards improving operator alarm flood responses: alternative alarm presentation techniques," *Abnormal Situation Management Consortium*, 2011.
- [7] S. Charbonnier, N. Bouchair, and P. Gayct, "Fault template extraction to assist operators during industrial alarm floods," *Engineering Applications of Artificial Intelligence*, vol. 50, pp. 32-44, 2016.
- [8] R. R. R. Barbosa, R. Sadre, and A. Pras, "Exploiting traffic periodicity in industrial control networks," *International journal of critical infrastructure protection*, vol. 13, pp. 52-62, 2016.
- [9] M. Kczunovic and Y. Guan, "Intelligent alarm processing: From data intensive to information rich," in *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, 2009, pp. 1-8.
- [10] S. Khanmohammadi, K. Rezaie, J. Jassbi, and S. Tadayon, "A model of the failure detection based on fuzzy inference system for the control center of a power system," *Appl. Math. Sci.*, vol. 6, pp. 1747-1758, 2012.
- [11] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano, "Failure identification in smart grids based on petri net modeling," *IEEE Transactions on Industrial Electronics*, vol. 58, pp. 4613-4623, 2011.
- [12] Y. Guan and M. Kezunovic, "Contingency-based nodal market operation using intelligent economic alarm processor," *IEEE Transactions on Smart Grid*, vol. 4, pp. 540-548, 2013.
- [13] D. Hadžiosmanović, D. Bolzoni, and P. H. Hartel, "A log mining approach for process monitoring in SCADA," *International Journal of Information Security*, pp. 1-21, 2012.
- [۱۴] پژوهشگاه نیرو، "استاندارد سیستم های اتوماسیون پست‌های انتقال و فوق توزیع"، شرکت توانیر، ۱۳۸۶.
- [14] Niroo Research Instituc, "Substation automation systems standard (transmission and subtransmission substations), *Ministry of Energy of Iran*, 2008.
- [15] T. M. Chen, J. C. Sanchez-Aarmoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, pp. 741-749, 2011.
- [16] C. Fecarotti, J. Andrews, and R. Remenyte-Prescott, "Analysis of the Design, Operation and Maintenance Options to Provide a Fault Tolerant Railway System," in *Transport Research Arena (TRA) 5th Conference*:

