دانشکده مهندسی

پایان‌نامه کارشناسی ارشد

گروه مهندسی کامپیوتر

ارائه سیستم تشخیص نفوذ هوشمند برای سیستم‌های اسکادا

نگارنده:

رامین ربانی

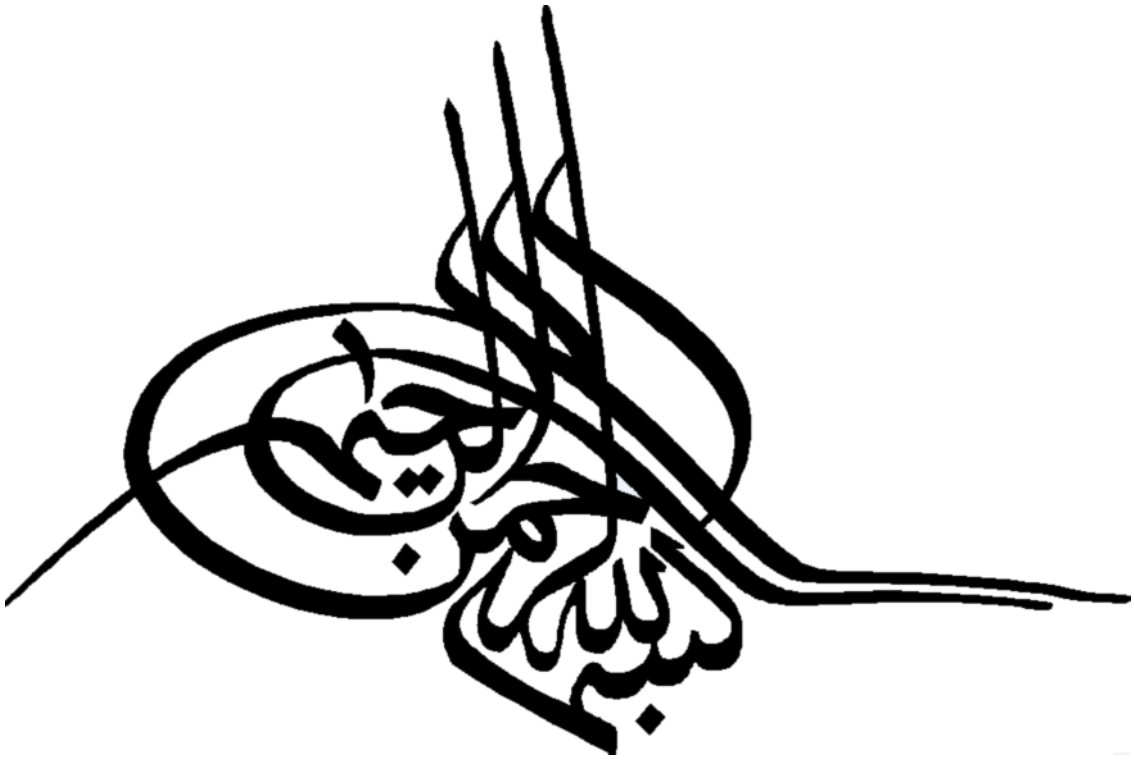
استاد راهنما:

دکتر محمد حسین یغمایی مقدم

استاد مشاور:

دکتر جواد حدادنیا

تابستان 92


بسم الله الرحمن الرحيم

اظهارنامه

اینجانب رامین ربانی دانشجوی دوره کارشناسی ارشد رشته مهندسی کامپیوتر دانشکده مهندسی دانشگاه فردوسی مشهد نویسنده پایان‌نامه ارائه سیستم تشخیص نفوذ هوشمند برای سیستم‌های اسکادا تحت راهنمایی دکتر محمد حسین یغمایی مقدم متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط این‌جانب انجام شده و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان‌نامه تاکنون توسط خود و یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است.
- کلیه حقوق معنوی این اثر متعلق به دانشگاه فردوسی مشهد می باشد و مقالات مستخرج با نام "دانشگاه فردوسی مشهد" و یا "Ferdowsi University of Mashhad" به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند در مقالات مستخرج از رساله رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است، اصل رازداری، ضوابط و اصول اخلاق انسانی رعایت شده است.

تاریخ

امضای دانشجو

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه فردوسی مشهد می‌باشد. این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد.

تقدیر و تشکر

سپاس گزار معلمی، هستم که اندیشیدن را به من آموخت، نه اندیشه ها را...

از جناب آقای دکتر محمد حسین یغمایی مقدم که در طی انجام این اثر، صبورانه کمال همکاری را با اینجانب داشتند و راهنمایی ها و حمایت هایشان همواره کارگشای اینجانب بوده، کمال سپاس گذاری و تشکر را دارم.

زحمات، راهنمایی ها و دلسوزی های استاد ارجمند و گرانقدر جناب آقای دکتر حداد نیارا که راهگشای کاربنده در بسیاری از مراحل بود، ارج می نهم.

همچنین از شرکت برق منطقه‌ای خراسان و به خصوص مدیر محترم امور دیسپاچینگ جناب آقای مهندس ذاکر عنبرانی جهت حمایت هایشان سپاس گذارم.

چکیده

امروزه سیستم‌های اسکادا از نقش حساسی در کنترل و پردازش سیستم‌های اطلاعاتی و صنعتی مدرن برخوردارند و نقشی حیاتی در زیرساخت‌های حساس کشورها پیدا کرده‌اند. نیروگاه‌های تولید برق، نیروگاه‌های هسته‌ای و سیستم‌های کنترلی عبور و مرور مترو در شهرهای بزرگ از نمونه‌های بارز استفاده از این سیستم‌ها می‌باشد. به دلیل نقش مهم این سیستم‌ها، امنیت داده‌ها و کنترل دسترسی‌های مختلف به این سیستم‌ها از مهمترین چالش‌های هر دولتی برای بخش‌های حساس کنترلی خود می‌باشد. از ابتدای پیدایش سیستم‌های اسکادا تا کنون کارهای زیادی در زمینه‌های مختلف بر روی امنیت آن‌ها صورت گرفته است که هرکدام به بخشی از موارد امنیتی سیستم پرداخته‌اند. اما امروزه با گسترش شبکه‌های کامپیوتری، محیط کاری این سیستم‌ها از یک محیط ایزوله، به شبکه‌های بزرگ‌تری از جمله اینترنت ارتقا یافته است. به این دلیل مباحث جدیدی در زمینه امنیت این سیستم‌ها مطرح شده است. یکی از برجسته ترین راهکارهای امنیتی در این زمینه، استفاده از سیستم‌های تشخیص نفوذ است. سیستم‌های تشخیص نفوذ فعلی برای سیستم‌های اسکادا، اکثراً با پروتکل‌های اسکادا آشنا نبوده و از هوشمندی و پویایی لازم برخوردار نیستند؛ به این دلیل کارایی لازم برای جلوگیری از نفوذ به این سیستم‌ها را ندارند.

در این پایان‌نامه سعی شده است تا سیستم تشخیص نفوذ هوشمند پویایی ارائه شود که بر مبنای روش فیلترینگ بر اساس حالات بحرانی به همراه دسته‌بندی حالات برای کاهش تأخیر سیستم و دخیل کردن نظر کاربر برای دقت بیشتر، عمل نماید. در نهایت پس از تست سیستم پیشنهادی با روش‌های قبلی، بهبود متوسط 80 درصدی در تأخیر وارد شده به سیستم مشاهده می‌گردد که با توجه به بلادرنگ بودن سیستم‌های اسکادا این میزان کاهش تأخیر موفقیت بزرگی محسوب می‌شود.

کلمات کلیدی: سیستم اسکادا، امنیت سیستم‌های اسکادا، اتوماسیون صنعتی، سیستم‌های تشخیص نفوذ، تحلیل حالت بحرانی، پروتکل‌های اسکادا، الگوریتم *SOM* .

فهرست مطالب

فهرست شکل‌ها

فهرست جداول

فصل اول:

مقدمه

1 – مقدمه

1 – 1– انگیزه

سیستم‌های اسکادا امروزه در مهمترین بخش‌های زیرساختی کشورها نفوذ کرده‌اند. کنترل بخش‌های حساسی چون نیروگاه‌های برق، نیروگاه‌های هسته‌ای، توزیع برق و ... امروزه توسط این سیستم‌ها صورت می‌گیرد. به همین دلیل فعالیت عاری از عیب این سیستم‌ها همواره یکی از بزرگترین دغدغه‌های هر کشوری می‌باشد. در زمینه امنیت سیستم‌های اسکادا از ابتدای پیدایش آن‌ها تا کنون کارهای زیادی انجام شده و در نتیجه به میزان امنیت مناسبی برای فعالیت در رده کاری خود رسیده بودند.[1] در گذشته شبکه‌های این سیستم‌ها شبکه‌هایی کوچک و مجزا از سایر شبکه‌ها بودند. اما در سال‌های اخیر با گسترش شبکه‌های کامپیوتری و نیز نفوذ اینترنت در زمینه‌های مختلف، نیاز به ارائه این سیستم‌ها بر روی شبکه‌های گسترده‌تر احساس می‌شد. به این ترتیب بحث‌های جدیدی در زمینه امنیت این سیستم‌ها مطرح شده و تا برطرف نشدن این نیازهای امنیتی، امکان ارائه چنین سیستمی وجود نداشت. از آن زمان تاکنون تلاش‌های زیادی در زمینه امنیت این سیستم‌های جدید صورت گرفته و کارهای خوبی در زمینه سیستم‌های تشخیص نفوذ و دیواره‌های آتش صورت پذیرفته است.[2, 3] لازم به ذکر است سیستم‌های اسکادا یک سری محدودیت‌هایی دارند، از جمله به دلیل برخط[1] بودن این سیستم‌ها باید به صورت بلادرنگ فعالیت کنند، همچنین تجهیزاتی در این شبکه‌ها دارای توان محدود پردازشی می‌باشند. به دلیل این قبیل محدودیت‌ها، یک سری از روش‌های برقراری امنیت در سیستم‌های IT بر روی این سیستم‌ها قابل استفاده نخواهد بود.[4] کارهای جدید صورت گرفته بر روی سیستم‌های اسکادا نیز به نوبه خود موارد امنیتی زیادی را در نظر گرفته و نقص‌های امنیتی زیادی را پوشش داده‌اند. اما یکی از بحث‌هایی که در سیستم‌های اسکادا مطرح است و اخیرا توجه بیشتری به آن شده است، بحث فرامینی است که به صورت تکی بدون هیچگونه مشکلی برای سیستم بوده و قالب آن‌ها نیز کاملاً منطبق بر

[1] Online

پروتکل اسکادا می‌باشد اما در صورتی که در کنار هم به سیستم وارد شوند می‌توانند مشکلات جدی‌ای بر سیستم تحمیل کنند. دیواره‌های آتش و سیستم‌های تشخیص نفوذ فعلی سیستم‌های اسکادا اکثراً به صورت مبتنی بر امضا عمل نموده و در نتیجه توانایی تشخیص چنین حملاتی را به سیستم ندارند. یکی از کارهایی که روشی را برای پوشش این مشکل ارائه کرده است در [5] معرفی شده است. این روش با تعریف حالات بحرانی و چک کردن وضعیت بعدی سیستم قبل از اینکه فرمان را اجرا کند، متوجه می‌شود که آیا سیستم با آن فرمان به حالت بحرانی وارد می‌شود یا خیر. به این ترتیب می‌تواند تصمیم بگیرد که آیا یک فرمان اجازه اعمال شدن به سیستم را دارا می‌باشد یا باید از اعمال آن جلوگیری شود. این قبیل الگوریتم‌ها ایده‌ای نو را در کنترل دستورات وارد شده به سیستم ارائه کرده اند. اما با توجه به بلادرنگ بودن یک سیستم اسکادا پس از بررسی این الگوریتم‌ها به این نتیجه می‌رسیم که استفاده از آن‌ها برای سیستم‌های اسکادای بزرگ با تعداد نقاط بالا عملی نمی‌باشد. به این ترتیب با توجه به نقاط ضعف آن در این پایان‌نامه روشی ارائه خواهد شد که مشکلات موجود را پوشش داده و قابلیت استفاده از آن را برای سیستم‌های حقیقی با حجم بالای اطلاعات فراهم سازد. روش ارائه شده با استفاده از روش‌های هوش مصنوعی به کاهش فضای مسئله پرداخته و با انعطافی که در تعریف حالات جدید به سیستم در حال کار وارد می‌کند، قابلیت استفاده از این روش‌ها را در سیستم فراهم می‌سازد. برای مشاهده نتایج کار خود خوشبختانه طبق رایزنی‌هایی که با شرکت برق منطقه‌ای خراسان صورت گرفت، مقرر شد این سیستم بر روی سیستم اسکادای نصب شده در این شرکت قرار داده شده و نتایج عملیاتی آن به صورت عملی مشاهده و ثبت گردد. بدین ترتیب امکان عملی شدن سیستم پیشنهادی در یک سیستم اسکادای واقعی با تعداد نقاط بالا بررسی خواهد شد. در نهایت با این سیستم مقایسه نتایج مشاهده شده در روش ارائه شده با روش پایه صورت خواهد پذیرفت.

1 – 2– طرح پیشنهادی

در روش‌های برآورد حالت بحرانی با هر تغییری که در سیستم اعمال می‌شود بخش "تحلیلگر قواعد" با استفاده از خروجی که از بخش "کنترل کننده حالت" دریافت می‌کند بررسی می‌نماید که آیا سیستم به یکی از حالات بحرانی وارد شده است یا خیر. طبق تستی که در [6] انجام شده است در سیستمی که آن‌ها برای تست در نظر گرفته اند در بدترین حالت 2 میلی ثانیه به مدت زمان اجرای دستورات اضافه گشته بود. این میزان افزایش با افزایش تعداد نقاط متصل به سیستم و نیز اضافه شدن حالات بحرانی سیستم می‌تواند مقدار بیشتری به خود بگیرد. به این خاطر و با توجه به اهمیت بحث بلادرنگ بودن سیستم‌های اسکادا باید به دنبال راهکاری جهت کمتر کردن این میزان پردازش اطلاعات باشیم. در این روش‌ها حالت جدید سیستم با تک تک حالت‌های بحرانی تعریف شده در سیستم مقایسه شده و با رسیدن به انتهای لیست و پیدا نشدن تشابه بین دو طرف، نتیجه گرفته می‌شود که فرمان ارسالی امن می‌باشد. به این ترتیب هر فرمان امن - که روزانه تعداد آن‌ها کم نمی‌باشد- قبل از اجرا باید منتظر سپری شدن این مدت زمان برای بررسی باشد. مقایسه کردن حالت جدید سیستم با تمامی حالت‌های بحرانی در اکثر مواقع امری غیر منطقی است. با بررسی بردارهای معرف حالات بحرانی می‌توان ابعاد آن‌ها را به طرق مختلفی کاهش داد. به این ترتیب با هر فرمان جدید در سیستم دیگر نیاز نیست که حالت بعدی سیستم با حجم بالایی از حالات بحرانی مقایسه شود بلکه تنها مقایسه با کاهش یافته حالات بحرانی کفایت خواهد کرد. در روش پیشنهادی ما کار کاهش ابعاد ماتریس حالت بحرانی توسط الگوریتم SOM صورت می‌گیرد و پس از آن ماتریس کاهش یافته جایگزین ماتریس حالات بحرانی خواهد گشت. همچنین در روش قبلی تعریف حالت بحرانی در سیستم تنها در فاز اولیه راه‌اندازی سیستم مقدور بوده و پس از آن حالت جدید در سیستم تعریف نمی‌شود در صورتی که با توجه به یادگیری برخط در الگوریتم SOM، در سیستم پیشنهادی خود قادر به اضافه نمودن حالات بحرانی جدید نیز خواهیم بود. بدین ترتیب طرح پیشنهادی خود را پیاده‌سازی کرده و به تست نتایج جهت بررسی عملی بودن پیاده سازی این الگوریتم خواهیم پرداخت.

1 – 3– ساختار پایان‌نامه

این نوشتار شامل پنج فصل دیگر به شرح ذیل خواهد بود:

فصل دوم(معرفی سیستم‌های اسکادا): با توجه به اهمیت سیستم‌های اسکادا و ویژگی‌های خاصی که این سیستم‌ها دارند فصل دوم به معرفی کلی این سیستم‌ها و عملکرد آن‌ها اختصاص داده شده است. در این فصل با بخش‌های مختلف سخت‌افزاری و نرم‌افزاری این سیستم‌ها آشنا شده و مختصری در مورد پروتکل‌های ارتباطی مطرح‌تر این سیستم‌ها بحث خواهد شد.

فصل سوم (سیستم‌های تشخیص نفوذ): همانطور که ذکر شد، با توجه به اهمیت سیستم‌های اسکادا، کارهای مختلفی در زمینه امنیت آن‌ها صورت پذیرفته است. با توجه به کار خود در زمینه سیستم‌های تشخیص نفوذ، در این فصل در ابتدا به معرفی کلی سیستم‌های تشخیص نفوذ و کارکرد آن‌ها پرداخته و سپس به مرور بخشی از کارهای صورت گرفته در این زمینه پرداخته خواهد شد و ایده‌های مختلف در این زمینه بررسی می‌گردد.

فصل چهارم (روش پیشنهادی): در این فصل روش پیشنهادی خود برای بهبود عملکرد سیستم تشخیص نفوذ برای سیستم اسکادا معرفی خواهد شد. همچنین با نحوه پیاده سازی آن در سیستم اسکادای شرکت برق منطقه‌ای خراسان آشنا شده و عملکرد آن مشاهده خواهد شد.

فصل پنجم (ارزیابی روش پیشنهادی): در این فصل سیستم پیشنهادی را با سیستم‌های قبلی که پیاده‌سازی شده است مقایسه کرده تا معایب و مزایای تغییرات اعمال شده ملاحظه شود. در این فصل به بررسی میزان تغییرات سرعت و دقت در الگوریتم جدید نسبت به روش قبلی پرداخته شده، تا میزان کارایی روش پیشنهادی برای استفاده در سیستم اسکادای واقعی برآورد شود.

فصل ششم (جمع بندی و نتیجه‌گیری): در این فصل با توجه به ارزیابی‌های صورت گرفته در فصل پنجم، به جمع‌بندی کار ارائه شده پرداخته و همچنین کارهایی که در این زمینه در آینده قابل اعمال هستند ذکرشده‌اند

فصل دوم:

معرفی سیستم های اسکادا

2– آشنایی با سیستم های اسکادا

در این فصل ابتدا مفهوم سیستم اسکادا شرح داده شده و سپس در مورد ساختار این نوع سیستم‌ها بصورت کلی مطالبی ارائه می‌شود.

2 – 1– مفهوم اسکادا

اسکادا در زبان انگلیسی، مخفف Supervisory Control And Data Acquisition به معنای سامانه‌های کنترل مدیریتی و گرد آوری اطلاعات است و به سیستم های کنترل و اندازه گیری در مقیاس بزرگ و صنعتی ، اطلاق می شود.[7]

سیستم‌های SCADA برای نظارت یا کنترل فرآیندهای شیمیایی، حمل و نقل، سیستم‌های آبرسانی شهری، کنترل تولید و توزیع انرژی الکتریکی و در خطوط نفت و گاز و سایر فرآیندهای گسترده (توزیع یافته) استفاده می‌شود[7]. نیازهای مختلف بخش‌های صنعتی روز به روز در حال افزایش است به همین خاطر این سیستم‌ها از نظر سایز و پیچیدگی و غیر قابل پیش بینی شدن روز به روز گسترش پیدا می کنند.[8]

اسکادا برای انجام یکسری از کارهای تکراری با کمترین مداخله انسان در یک سیستم ایجاد می‌شود. هر سیستم اسکادا بدون درنظر گرفتن نوع سیستمی که بایستی روی آن پیاده شود و یا اینکه چرا و چگونه پیاده‌سازی انجام گیرد معمولاً دارای اجزاء زیر می‌باشد:

- تجهیزات متغیر
- کنترل تجهیزات متغیر
- نمایش تجهیزات متغیر
- کنترل هماهنگ تجهیزات فوق
- ارتباط مخابراتی با تجهیزات

- شبیه‌سازی پاسخ سیستم

2 – 1 – 1– تجهیزات متغیر

اگر در یک سیستم عملکرد، وضعیت و یا خروجی تجهیزات آن قابل تغییر نباشد آن سیستم ایستا می‌باشد و بنابراین قابل خودکار نمودن نیست. اگرچه می‌توان در این سیستم وضعیت تجهیزات را مشاهده نمود که خود یک قابلیت مهم است ولی برای بهره‌برداری مناسب از سیستم بایستی تجهیزات مهم و استراتژیک آن را کنترل نمود.

برای مثال اگر هدف بهبود پروفیل ولتاژ در یک شبکه توزیع باشد، بایستی نقاط مناسب شبکه به خازن‌های متغیر، رگولاتور ولتاژها و تپ چنجر (LTC) تجهیز گردند.

2 – 1 – 2– کنترل تجهیزات متغیر

با توجه به توضیحات بند قبل، بایستی کلیه تجهیزات مهم و استراتژیک کنترل گردند. بعبارتی یک سیستم اسکادا فرامین کنترلی لازم را به آن‌ها اعمال نماید. بعنوان مثال یک سیستم اسکادای برق بایستی بتواند یک کلید را از راه دور باز کرده و یا آنرا ببندد و یا اینکه یک خازن را به مدار آورده و یا از مدار خارج سازد.

2 – 1 – 3– نظارت بر وضعیت سیستم

اگر یک سیستم اسکادا بخواهد به اهداف خود برسد بایستی بتواند وضعیت کل سیستم را جمع‌آوری کرده و نمایش دهد. بعنوان مثال برای بهبود پروفیل ولتاژ بایستی مقادیر ولتاژ از نقاط مختلف و حساس یک شبکه توزیع در مرکز جمع‌آوری گردد.

2 – 1 – 4– نظارت بر تجهیزات متغیر

در یک سیستم اسکادا علاوه بر وضعیت نقاط مختلف بایستی وضعیت تجهیزاتی که کنترل می‌شود را جمع‌آوری نمود. چرا که برای اعمال فرمان نیاز به این است که وضعیت آنها مشخص باشد.

مثلاً برای قطع و وصل یک بانک خازنی بایستی وضعیت قطع و یا وصل بودن آن مشخص باشد و نیز برای اعمال فرمان افزایش و یا کاهش به تپ ترانس، موقعیت آن بایستی در مرکز مشخص باشد.

2 – 1 – 5 – کنترل هماهنگ تجهیزات متغیر

یک سیستم اسکادا بایستی هماهنگی‌های لازم را برای کنترل تجهیزات مختلف فراهم آورد به‌طوریکه کنترل یک تجهیز حداقل ناهماهنگ با کنترل تجهیز دیگر نباشد.

بعنوان نمونه در یک سیستم اسکادا برق بایستی تغییر تپ رگولاتور ولتاژها بطور هماهنگ با کلیدزنی خازنها طوری انجام شود که پروفیل ولتاژ در محدوده مجاز تعیین شده با حداقل تلفات قرار گیرد.

2 – 1 – 6 – ارتباط مخابراتی با تجهیزات

برای بهره‌برداری بهینه از یک سیستم، ایجاد اسکادا مرکزی ضروری می‌باشد و لازمه آن این است که مخابرات بین تجهیزات و مرکز برقرار باشد.

2 – 1 – 7 – شبیه‌سازی پاسخ سیستم

یکی از مسائل حساس و مهم در یک سیستم مشخص نمودن نوع نقاط کنترلی و نحوه اعمال فرمان به آن‌ها می‌باشد. اصولاً لازم است در یک مرکز مشخص شود که کنترل یک تجهیز چه عکس‌العملی در کل سیستم ایجاد خواهد نمود. به عبارتی رفتار سیستم دراین مورد چه خواهد بود. بنابراین عموماً در مراکز از شبیه‌ساز پاسخ سیستم استفاده می‌شود. این نوع شبیه‌سازها از نوع زمان حقیقی و بلادرنگ می‌باشند. این سیستم بطور کلی امکانات زیر را خواهد داشت:

- در اختیار داشتن کل اطلاعات جمع‌آوری شده