دانشگاه تبریز

دانشکده مهندسی برق و کامپیوتر

گروه مهندسی کامپیوتر

**پایان‌نامه**

برای دریافت درجه‌ی کارشناسی ارشد در رشته‌ی مهندسی کامپیوتر، گرایش هوش مصنوعی

# عنوان

ارائه یک الگوریتم جدید تشخیص نفوذ مبتنی بر ناهنجاری در شبکه‌های صنعتی

**استادان راهنما**

دکتر سید ناصر رضوی

دکتر علی فانیان (دانشگاه صنعتی اصفهان)

**پژوهشگر**

مستعان فریدونی

**شهریور ماه ۱۳۹۳**

# تشکر و قدردانی

حمد و سپاس خداوند را که به نام او کار را آغاز کردیم و به یاری حضرتش به پایان رساندیم.

بر خود لازم می دانم مراتب سپاس و قدردانی خود را نسبت به همه عزیزان و بزرگوارانی که در تکمیل این پایان نامه مرا یاری داده اند ابراز نمایم. بدین وسیله از اساتید راهنمای گرامی جناب آقای دکتر علی فانیان و جناب آقای دکتر سید ناصر رضوی که در تمام مراحل پژوهش، یاری گر و پشتیبان بنده بوده اند، کمال تشکر و قدردانی را دارم. از آنجایی که از ابتدا تا انتها، تمامی مراحل این پروژه به صورت کامل در دانشگاه صنعتی اصفهان انجام گرفته است بر خود لازم می دانم تا مراتب قدردانی خود را از مسئولین محترم این دانشگاه، که در طول این مدت کمال همکاری را بابنده داشته اند اعلام نمایم.

از آقایان مهندس مختاری و مهندس بزرگی در سازمان انرژی اتمی به خاطر کمک های بی دریغشان تشکر و قدردانی می کنم.

از دوست عزیزم آقای مهندس امیر حسین پورشمس در مرکز تخصصی آپای دانشگاه صنعتی اصفهان که مراد انجام این پژوهش یاری نمود، صمیمانه سپاسگزارم.

از خانم دکتر لیلی محمد خانلی به خاطر قبول زحمت داوری، مطالعه پایان نامه و ارائه پیشنهادات ارزنده شان بسیار سپاسگزارم.

در پایان از حمایت های بی دریغ همسر فداکار و خانواده عزیزم که همواره در این مدت از هیچ کوششی جهت انجام هرچه بهتر این اثر فروگذار ننمودند سپاسگزاری می نمایم و از خدای متعال برای همه عزیزان سعادت و بهروزی طلب می نمایم.

# اگر شایسته باشد.....

تقدیم به شهید اصغر قصاب عبداللهی فرمانده ی گردان امام حسین از لشکر ۳۱ عاشورا. عاشق و دلیر بی نام و نشانی که به تاریخ ۶۳/۱۲/۲۵ در عملیات بدر، بر روی اتوبان بصره- العماره بال در بال ملائک گشود و آسمانی شد. او که در باغ ملکوت شهره و در عالم خاک غریب است.

**نام خانوادگی دانشجو:** فریدونی **نام:** مستعان

**عنوان پایان‌نامه:** ارائه الگوریتم جدید تشخیص نفوذ مبتنی بر ناهنجاری در شبکه‌های صنعتی

**استادان راهنما:** دکتر سید ناصر رضوی، دکتر علی فانیان (دانشگاه صنعتی اصفهان)

**مقطع تحصیلی:** کارشناسی ارشد **رشته:** مهندسی کامپیوتر **گرایش:** هوش مصنوعی

**دانشگاه:**تبریز

**دانشکده:** برق و کامپیوتر **تاریخ فارغ التحصیلی:** ۱۳۹۳/۶/۱۹ **تعداد صفحه:** ۸۰

**کلید واژه‌ها:** سیستم‌های کنترل صنعتی، شبکه‌های صنعتی، سیستم‌های تشخیص نفوذ

**چکیده:** امروزه امنیت در شبکه‌های کامپیوتری دارای اهمیت فراوانی است. اما از آنجایی که شبکه‌های صنعتی در مقایسه با شبکه‌های معمولی دارای تفاوت‌ها و ضروریات خاص خود هستند، همین تفاوت‌ها سبب تفاوت در اولویت‌بندی و روش‌های امن‌سازی در شبکه‌های صنعتی نسبت به شبکه‌های عادی می‌شود. از طرفی به دلیل اینکه کاربرد شبکه‌های صنعتی در کنترل فرآیندهای صنعتی است و این فرآیندها در صنایع حساس و زیرساختی کشورها همانند پالایشگاه‌ها، تاسیسات تولید و انتقال برق، سدهای ذخیره و نگهداری آب و نیروگاه-های هسته‌ای بکار می‌روند، طبیعی است که وجود ناامنی و امکان نفوذ در این شبکه‌ها سبب بروز خطرات و آسیب‌های جبران ناپذیری برای کشورها خواهد داشت، در نتیجه حفظ امنیت و امکان تشخیص نفوذ در شبکه-های صنعتی دارای اهمیت به سزایی است. با در نظر گرفتن مطالب بیان شده، در این پروژه با بررسی کارهای اندک صورت گرفته در این حوزه، هدف ما ارائه الگوریتم جدید تشخیص نفوذی است که در آن به ویژگی‌های شبکه‌های صنعتی توجه گردد و علاوه بر این از روش‌های یادگیری و هوش مصنوعی نیز الهام گرفته شود. در الگوریتم ارائه شده در این پایان‌نامه علاوه بر مطالب بیان شده از دانش فرد خبره به عنوان کسی که اطلاعات و آگاهی لازم در خصوص شبکه‌ی صنعتی را دارد نیز بهره گرفته می‌شود که بکارگیری نقش فرد خبره در طراحی الگوریتم پیشنهادی برای نخستین بار در این حوزه صورت می‌گیرد. سیستم تشخیص نفوذ پیشنهادی برای تشخیص ناهنجاری‌های موجود در شبکه اقدام به ساخت گراف ارتباطی شبکه با توجه به ویژگی‌های پروتکل مدباس و دستگاه‌های بکار رفته در شبکه می‌نماید که این روش، در تعیین ترافیک نرمال شبکه برای اولین بار در سیستم‌های تشخیص نفوذ ارائه شده در شبکه‌های صنعتی، بکار رفته است. در این سیستم یک پایگاه داده حملات رایج در شبکه‌های مدباس نیز قرار داده شده است تا در صورت امکان، سیستم اقدام به تشخیص حمله‌ی ناشی از ناهنجاری تشخیص داده شده نماید. برای ارزیابی سیستم پیشنهادی در این پایان‌نامه با توجه به عدم وجود مجموعه داده در حوزه شبکه‌های صنعتی و لزوم ارائه ارزیابی عملکرد سیستم در گزارش پایانی، خود اقدام به تولید مجموعه داده و شبیه‌سازی محیط شبکه‌های صنعتی کردیم. سپس این مجموعه داده برای آزمایش روش پیشنهادی مورد استفاده قرار گرفت که نتایج آن نتایجی قابل قبول بوده و نتایج مربوطه در فصل نتیجه-گیری قرار داده شده است. در مجموع در سیستم پیشنهادی در این پایان‌نامه از گراف ارتباطی برای مدل کردن ترافیک عادی شبکه و از نقش فرد خبره در فرآیند یادگیری سیستم بهره برده خواهد شد که هریک از آن‌ها

برای اولین بار در سیستم تشخیص نفوذ شبکه‌های صنعتی بکار رفته است.

فهرست مطالب

# فصل اول - مقدمه

## ۱-۱ بیان مسئله

امروزه امنیت در شبکه‌های کامپیوتری دارای سه مشخصه اصلی و عمده است. این مشخصات عبارتند از در دسترس بودن یک جز توسط سایر اجزای شبکه[۱]، توانایی امن نگاه داشتن و دقت در همه ابزارها[۲]، تضمین در دسترس نبودن اطلاعات برای افراد نامعتبر[۳]. اما امنیت در شبکه‌ها و سیستم‌های کنترل صنعتی دارای تفاوت‌ها و ضروریات خاص خود است که همین تفاوت‌ها سبب تفاوت در اولویت‌بندی این فاکتورها در شبکه‌های تجاری شخصی با شبکه‌های صنعتی می‌شود. برای مثال در شبکه‌های صنعتی به دلیل نوع کاربرد آنها که معمولا در زیرساخت‌های حیاتی مانند شبکه‌های آب و برق مورد استفاده قرار می‌گیرند، در دسترس بودن دارای اولویت نخست است، در حالی که در شبکه‌های تجاری تضمین در دسترس نبودن اطلاعات برای افراد نامعتبر، اولویت نخست را دارد. بنابراین نصب کردن[۴] که یک امر متداول و معمول برای افزایش امنیت در شبکه‌های متعارف است، به دلیل نیاز به قطع سرویس در هنگام نصب، فاکتور در دسترس بودن در سیستم‌های صنعتی را تحت تاثیر قرار می‌دهد، که این امر می‌تواند بحران آفرین باشد[۱]. امروزه تلاش زیادی برای حفظ امنیت شبکه‌های تجاری صورت گرفته است اما تحقیقات و تلاش‌های کمی در راستای حفاظت از زیرساخت‌های حیاتی انجام شده است، زیرا سیستم‌های کنترلی، مبتنی بر پروتکل‌های خاص بوده و نیز از شبکه‌های عمومی مجزا می‌باشند. اما امروزه به دلیل افزایش درخواست برای اتصالات داخلی و همگرا شدن به سوی استاندارد کردن پروتکل‌های ارتباطی به پروتکل‌های خاصی همانند TCP/IP، خطر حملات جدید در این گونه سیستم‌ها افزایش یافته است[۲].

سیستم‌های صنعتی متشکل از چندین نوع از سیستم‌های کنترلی هستند، که این سیستم‌ها شامل سیستم کنترل و بدست آوردن اطلاعات به صورت نظارت شده[۵] ( اسکادا ) ، سیستم‌های کنترلی توزیع شده[۶] و سیستم‌های کنترل منطقی قابل برنامه‌نویسی[۷] هستند[۳].

سیستم‌های اسکادا سیستم‌هایی با توزیع شدگی بالا هستند که برای کنترل دستگاه‌های دارای پراکندگی جغرافیایی بکار می‌روند که در این دستگاه‌ها کنترل و بدست آوردن داده به صورت مرکزی امری حیاتی است. سیستم کنترل مرکزی اسکادا، ارتباطات شبکه‌ای با مسافت‌های طولانی را کنترل و رصد می‌کند. این کنترل شامل رصد کردن هشدارها و پردازش داده‌های وضعیت می‌باشد. عملکرد اسکادا

[1] Availability
[2] Integrity
[3] Confidentiality
[4] Patching
[5] SCADA
[6] Distributed control system (DCS)
[7] Programmable logic controller (PLC)

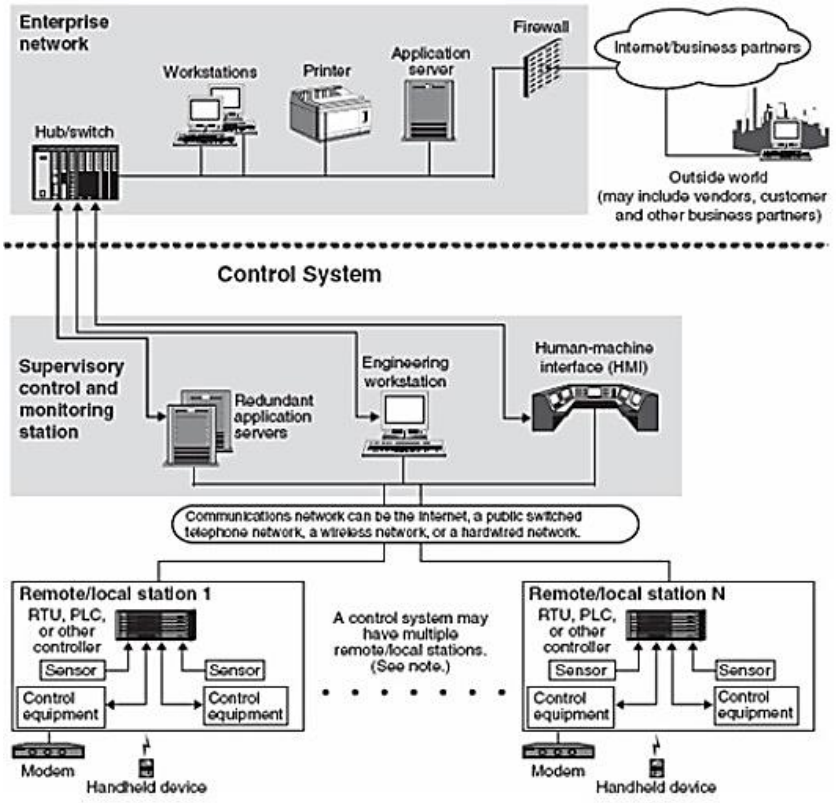
بر اساس اطلاعات دریافت شده از پایگاه‌های راه دور است. دستورات خودکار یا صادر شده از جانب ناظر می‌تواند به دستگاه‌های کنترلی موجود در پایگاه‌های راه دور که به آن‌ها دستگاه‌های سطح[1] می‌گویند ارسال شود. دستگاه‌های فیلد برای کنترل عملیات‌های محلی مانند باز و بسته کردن دریچه‌ها و موج‌شکن‌ها، جمع‌آوری داده از حسگرهای سیستم‌ها و رصد کردن شرایط هشدار در محیط محلی بکار می‌روند[۴].

DCS دارای سطح کنترلی نظارت شده برای زیر سیستم‌هایی است که مسئول کنترل فرآیندهای محلی هستند. معمولا کنترل محصولات و فرآیندها با چرخه‌های بازخورد رو به عقب[2] و بازخورد رو به جلو[3] حاصل می‌شود و شرایط حساس محصول و یا فرآیند در اطراف نقطه مورد نظر حفظ می‌شود. بدین منظور و برای نگه‌داشتن دامنه تغییرات محصول و یا فرآیند، حول نقطه مطلوب PLCهای خاصی استفاده می‌شوند[۵].

PLCها ابزاری برای کنترل تجهیزات و فرآیندهای صنعتی هستند و جزئی از سیستم‌های کنترلی‌ای می‌باشند که توسط اسکادا و DCS بکار برده می‌شوند. PLCها ابتدایی ترین تجهیزات برای کنترل کردن فرآیندهایی همانند خطوط خودکار سرهم کردن ماشین هستند و تقریبا به صورت گسترده‌ای در همه فرآیندهای صنعتی استفاده می‌شوند[۲].

اما همان‌طور که به صورت جزئی بیان شد سیستم‌های صنعتی در مقایسه با شبکه‌های IT دارای تفاوت‌هایی هستند بنابر این طبیعی است که نیازمندی‌های امنیتی در این سیستم‌ها با شبکه‌های عادی دارای تفاوت‌هایی باشد. معمولا سیستم‌های کنترل صنعتی در مکان‌های حساس و حیاتی همانند زیرساخت‌های صنعت برق، سازمان انرژی اتمی، صنایع نفتی و پتروشیمی و .... کاربرد دارند. به دلیل حساسیت و نوع خسارات ناشی از حمله به این صنایع حیاتی که در مواردی با جان انسان‌ها در ارتباط است، لازم است تا ابزارها و تجهیزات امنیتی مناسبی که متناسب با ویژگی‌های موجود در این سیستم-هاست طراحی شود. یکی از این ابزارها که برای جلوگیری از نفوذ و خرابکاری کاربرد بسیاری دارد سیستم تشخیص نفوذ است[4].

[1] Field device
[2] Feed back
[3] feed forward
[4] Intrusion detection system




**شکل ۱-۱** نمایی از یک شبکه‌ی صنعتی[۶]

سیستم‌های تشخیص نفوذ دارای دو نوع کلی می‌باشند: سیستم‌های مبتنی بر امضاء[1] و سیستم‌های مبتنی بر ناهنجاری[2]. در روش مبتنی بر امضاء، الگوی حمله از طریق یک قانون در اختیار سیستم تشخیص نفوذ قرار می‌گیرد. بنابراین در صورتی که در ترافیک مورد مبادله این الگو یافت شود، آن ترافیک، حمله تشخیص داده شده و بر اساس سیاست تعیین شده، وضعیت آن مشخص می‌شود. در این روش به دلیل نبود الگوی حملات جدید[3]، امکان شناسایی آنها وجود ندارد اما روش ساده و بادقتی است.

در روش مبتنی بر ناهنجاری، از یک مدل آماری که نشان دهنده ترافیک عادی شبکه است، استفاده می‌شود. در این روش هر رفتار غیرعادی در شبکه به عنوان ناهنجاری در نظر گرفته می‌شود و بر خلاف روش مبتنی بر امضاء، امکان شناسایی حملات جدید وجود دارد اما معمولا خطای آن نسبتا بالا است.

معماری سیستم‌های تشخیص نفوذ بر پایه چهار واحد اصلی زیر تعریف می‌شوند[۷]:

[1] signature-based(SB)
[2] Anomaly-based(AB)
[3] Zero-day

واحد رخداد[1]: ترکیبی از سنسورهایی است که سیستم هدف را مانیتور می‌کنند و اطلاعات بدست آمده توسط آن به وسیله‌ی واحدهای دیگر آنالیز می‌شود.

واحد پایگاه داده[2]: اطلاعات بدست آمده از واحد رخداد برای پردازش در واحدهای دیگر، در این واحد ذخیره می‌شود.

واحد آنالیز[3]: آنالیزکننده اتفاقات و تشخیص‌دهنده رفتارهای تجاوزکارانه‌ی احتمالی است که منجر به تولید هشدار می‌گردد.

واحد پاسخ[4]: مهمترین عملکرد این واحد، پاسخ مناسب به تجاوز اتفاق افتاده است.

## ۱-۲ اهداف پایان‌نامه

با توجه به اهمیت استفاده از سیستم‌های تشخیص نفوذ در شبکه‌های متعارف، و با توجه به لزوم امن-سازی فرآیندها و تجهیزات موجود در شبکه‌های صنعتی، بکارگیری این سیستم‌ها برای شناسایی تهدیدات و حملات احتمالی در این نوع از شبکه‌ها ضروری است. از این رو باید سیستم‌های تشخیص نفوذ جدیدی با توجه به ویژگی‌های این شبکه‌ها ارائه شوند که قادر به شناسایی تهدیدات مرتبط هستند. عموم پژوهش‌های صورت گرفته در حیطه تشخیص نفوذ، سعی بر این داشته‌اند که روشی جامع برای حل این مسئله ارائه دهند، مسئله‌ی تشخیص نفوذ ذاتا مسئله‌ای پیچیده و دارای جنبه‌ها و ظرایف گوناگون است، به همین دلیل ارائه یک مدل جامع باید متناسب با موارد کاربرد و اهداف مورد نظر، انتخاب شود.

بر اساس مطالب بیان شده در این تحقیق تلاش می‌شود تا الگوریتمی مناسب برای سیستم تشخیص نفوذ در شبکه‌های صنعتی ارائه گردد. با توجه به مکان‌های استفاده سیستم‌های صنعتی که در زیرساخت-های حیاتی کشور است طبیعی است حملاتی که بر علیه این زیرساخت‌ها انجام می‌گردد حملاتی جدید باشد. به همین دلیل الگوریتم پیشنهادی با هدف کاربرد در سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری ارائه می‌گردد. از آنجایی که پروتکل‌های مورد استفاده در این شبکه‌ها دارای انواع متفاوتی هستند در تحقیق حاضر پروتکل پرکاربرد مدباس در نظر گرفته خواهد شد. از این رو در این پژوهش سعی بر آن است تا تنها یک الگوریتم جدید تشخیص نفوذ مبتنی بر ناهنجاری در شبکه‌های صنعتی ارائه شود که در آن به ویژگی‌ها و خصوصیات شبکه‌ی هدف توجه می‌گردد.

[1] Event module
[2] Database module
[3] Analyze module
[4] Response module

## ۱-۳ ساختار پایان‌نامه

در فصل بعد ابتدا برخی جنبه‌های سیستم‌های صنعتی و شبکه‌های تجاری را مورد مقایسه قرار خواهند گرفت و سپس به بررسی اجمالی سیستم‌های صنعتی و پروتکل مدباس می‌پردازیم و پس از آن به مرور پژوهش‌های صورت گرفته در این حوزه خواهیم پرداخت. در فصل سوم مدل پیشنهادی ارائه می‌شود. در فصل چهارم به نتایج آزمایشات صورت گرفته اشاره خواهد شد و در نهایت در فصل آخر به نتیجه‌گیری و ارائه پیشنهادات برای کارهای آینده می‌پردازیم.

# فصل دوم - مرور مطالب

## ۲-۱ مقدمه

در این فصل، در ابتدا به مقایسه سیستم‌های کنترل صنعتی[1] و شبکه‌های تجاری خواهیم پرداخت و نحوه عملکرد این سیستم‌ها را به صورت اجمالی بررسی می‌کنیم و پس از آن به معرفی پروتکل مدباس می‌پردازیم و سپس برخی پژوهش‌های انجام شده در این زمینه که مرتبط با موضوع این تحقیق هستند بررسی می‌شوند.

## ۲-۲ مقایسه سیستم‌های کنترل صنعتی و شبکه‌های تجاری

همان‌گونه که در مقدمه بیان شد سیستم‌های کنترل صنعتی شباهت کمی با سیستم‌های IT دارند. از طرفی به علت افزایش ارتباط و قابلیت دسترسی از راه دور، سیستم‌های کنترل صنعتی در حال انطباق با روش‌های IT هستند، اما از طرف دیگر در طراحی و پیاده‌سازی، از کامپیوترها و سیستم عامل‌ها و پروتکل‌های استانداری که مختص شبکه‌های صنعتی است استفاده می‌گردد. این مسائل موجب شده است تا شباهت این سیستم‌ها با سیستم‌های IT افزایش بیابد. اما این مسئله سبب شده که ویژگی ایزوله بودن در سیستم‌های کنترل صنعتی نسبت به سیستم‌های مشابه پیشین کاهش یابد و نیاز بیشتری به امنیت این سیستم‌ها به وجود بیاید، اما هنگامی که راه حل‌های IT را برای بکارگیری در این محیط‌ها انتخاب می‌کنیم نیازمند مراقبت‌های خاصی هستیم[۸]. سیستم‌های کنترل صنعتی دارای خصوصیت‌های زیادی هستند که آنها را از سیستم‌های IT متمایز می‌کند، از جمله تفاوت در خطرها و اولویت‌های امنیتی. در ادامه با توجه به [۲] تعدادی از مراقبت‌های خاص که باید در امنیت سیستم‌های صنعتی در نظر گرفته شوند اشاره خواهد شد.

**نیاز عملکردی**[2]: به صورت کلی در ICSها زمان یکی از فاکتورهای حیاتی محسوب می‌گردد و در هنگام نصب باید سطح قابل قبولی از میزان تاخیر زمانی مشخص گردد. بعضی از سیستم‌های صنعتی نیازمند پاسخ قطعی هستند، به همین دلیل میزان تاخیر زمانی در این سیستم‌ها باید به حداقل ممکن کاهش بیابد. بر خلاف سیستم‌های IT که نیازمند بازده حداکثری هستند و می‌توانند نسبت به میزان تاخیر مقاوم باشند بازده حداکثری برای سیستم‌های کنترل صنعتی امری ضروری نیست.

**نیاز به در دسترس بودن**[3]: به دلیل اینکه بسیاری از فرآیندهای ICS در طبیعت به صورت پیوسته عمل می‌کنند، قطع شدن ناگهانی سیستم‌های کنترل کننده در فرآیندهای صنعتی قابل قبول نمی‌باشد و

[1] Industrial control system (ICS)
[2] Performance requirements
[3] Availability Requirements

در این سیستم‌ها باید اغلب قطعی‌ها، از روی برنامه‌ریزی باشند. بدین منظور ضروری است که پیش از انجام تغییر در این سیستم‌ها، آزمایش‌های جامعی صورت بگیرد تا این اطمینان حاصل شود که پس از ایجاد تغییرات همچنان سیستم کنترل صنعتی، در دسترس خواهد بود. بسیاری از سیستم‌ها نمی‌توانند بدون تاثیرگذاری بر روی تولید، متوقف و راه‌اندازی شوند. در بعضی از موارد محصولات و تجهیزات مورد استفاده از اطلاعات مهم‌تر هستند، بنابراین استفاده از رویکردهای معمولی IT همانند راه‌اندازی مجدد یک قطعه، به دلیل تاثیر منفی‌ای که بر روی نیازهایی همانند در دسترس بودن و قابلیت اطمینان و نگهداری در سیستم‌های کنترل صنعتی دارند، قابل قبول نمی‌باشند. برخی از سیستم‌های کنترل صنعتی دارای تجهیزات اضافی‌ای هستند که به صورت موازی اجرا می‌شوند تا در هنگامی که تجهیزات اولیه از دسترس خارج می‌شوند، پیوستگی فرآیند حفظ گردد.

**نیاز مدیریت خطر**[1]: در سیستم‌های IT، اطمینان و تمامیت داده‌ها مهمترین جنبه می‌باشند، اما در سیستم‌های کنترل صنعتی پرهیز از، از دست دادن جان انسان‌ها و سلامت عمومی و... مهمترین جنبه را تشکیل می‌دهند. به همین دلیل افراد مسئول در اجرا و امنیت و نگهداری سیستم‌های کنترل صنعتی باید رابطه مهم بین امنیت و ایمنی را بدانند.

**معماری امنیتی:** در سیستم‌های IT مهمترین بخش در بحث امنیت، امن نگهداشتن عملیات دستگاه‌ها است اما در سیستم‌های کنترل صنعتی کاربرهای حاشیه[2] همانند PLC، ایستگاه عملیات و یا کنترل کننده DCS، به دلیل اینکه فرآیند انتهایی را کنترل می‌کنند باید به دقت محافظت شوند. بعلاوه نگهداری سرور مرکزی، به دلیل اینکه این سرور می‌تواند تاثیر مخربی بر روی دستگاه‌های حاشیه داشته باشد بسیار مهم است.

**فعل و انفعال فیزیکی**[3]: در یک سیستم IT، هیچ فعل و انفعال فیزیکی با محیط وجود ندارد در حالی که سیستم‌های کنترل صنعتی می‌توانند فعل و انفعالات پیچیده‌ای را با محیط و فرآیندهای فیزیکی داشته باشند. همه‌ی فعالیت‌های امنیتی مرتبط با سیستم‌های کنترل صنعتی باید در حالت Off-line تست شوند تا اثبات شود که فعالیت عادی سیستم کنترل صنعتی را تحت تاثیر قرار نمی‌دهند.

**پاسخ‌های حساس به زمان**[4]: در سیستم‌های کنترل صنعتی زمان خودکار پاسخ یا پاسخ سیستم به فعل و انفعال با انسان بسیار مهم است، برای مثال نیاز به تایید شدن کلمه عبور و احراز هویت در واسط

[1] Risk Management
[2] Edge Client
[3] Physical Interaction
[4] Time-Critical Response

کاربری انسان نباید مانع فعالیت‌های ضروری سیستم کنترل صنعتی شود و جریان اطلاعات مختل گردد و یا در معرض خطا قرار بگیرد.

**محدودیت منابع[1]:** سیستم‌های کنترل صنعتی و سیستم عامل‌های real-time آنها اغلب سیستم‌هایی دارای محدودیت منابع هستند. از طرفی ممکن است محاسبه منابع موجود در این سیستم‌ها امکان‌پذیر نباشد تا بتوان آنها را بهبود بخشید.

**ارتباط[2]:** وسایل و پروتکل‌های ارتباطی مورد استفاده در محیط سیستم‌های کنترل صنعتی برای دستگاه‌های کنترلی و ارتباطات داخلی، معمولا با نوع مورد استفاده در محیط IT متفاوت هستند و باید متناسب با این محیط باشند.

**مدیریت تغییرات[3]:** از آنجایی که نرم‌افزارهای وصله نشده[4] یکی از بزرگترین آسیب‌پذیری‌های موجود در سیستم هستند بروز رسانی این نرم‌افزارها، بر اساس سیاست‌ها و روندهای پذیرفته شده در بازه‌های زمانی مختلف انجام می‌گیرد اما بروزرسانی در سیستم کنترل صنعتی نمی تواند همیشه بر اساس زمان انجام بپذیرد زیرا ابتدا باید این بروزرسانی‌ها به صورت کامل پیش از پیاده‌سازی آزمایش شود زیرا قطع سرویس در سیستم‌های صنعتی باید بر اساس برنامه و زمانبندی روزانه و هفتگی باشد.

**طول عمر اجزا[5]:** طول عمر اجزای IT به سبب پیشرفت سریع تکنولوژی در حدود ۳-۵ سال است اما در سیستم‌های کنترل صنعتی در جاهایی که تکنولوژی در موارد خاصی برای استفاده و پیاده‌سازی توسعه یافته است، عمر تکنولوژی‌های گسترش یافته در حدود ۱۵-۲۰ سال می‌باشد.

**دسترسی به اجزا[6]:** اجزای سیستم‌های IT معمولا محلی هستند و به راحتی قابل دسترسی می‌باشند، در حالی که سیستم‌های کنترل صنعتی دارای اجزا ایزوله و راه دور هستند و دستیابی به آنها نیازمند تلاش وسیعی است.

**جدول ۲-۱** مقایسه‌ی سیستم‌های صنعتی و شبکه‌های تجاری [۲]

| دسته‌بندی | سیستم‌های IT | ICS |
|---|---|---|
| نیازهای عملکردی | Real-time نمی‌باشند. | Real-time |

[1] Resource Constraint
[2] Communication
[3] Change Management
[4] Unpatched
[5] Component Lifetime
[6] Access to Components

| | | |
|---|---|---|
| | پاسخ‌ها باید پایدار باشند.<br>بازده حداکثری نیاز است.<br>تاخیر زیاد ممکن است مورد قبول باشد. | پاسخ‌ها به زمان حساس هستند.<br>بازده معمولی قابل قبول است.<br>تاخیر بیش از حد قابل قبول نیست. |
| نیازهای در دسترس بودن | کارهایی مانند ریست کردن قابل قبول است.<br>بر اساس عملیات سیستم، کمبودهای در دسترس بودن قابل تحمل است. | به دلیل نیاز به در دسترس بودن اعمالی مانند ریست کردن قابل قبول نمی‌باشد.<br>نیاز به در دسترس بودن سیستم‌های جایگزین را ضروری می‌کند.<br>قطعی‌ها باید بر اساس برنامه‌ریزی باشند.<br>اهمیت در دسترس بودن نیاز به آزمایش پیش از توسعه را ایجاد می‌کند. |
| نیازهای مدیریت خطر | قابلیت اطمینان و بی‌عیبی داده‌ها مهمتر است.<br>تحمل خطا چندان مهم نیست، از کار افتادگی زودگذر مشکل عمده‌ای نمی‌باشد.<br>تاثیر خطر عمده در عملیات تجاری است. | ایمنی بشر فاکتور مهمتری می‌باشد که با حفاظت از فرآیندها به وجود می‌آید.<br>تحمل خطا ضروری است، حتی ازکار افتادگی زودگذر نیز قابل قبول نمی‌باشد.<br>تاثیر خطای عمده، معمولا غیرقابل قبول است و شامل تاثیرات محیطی و از دست دادن جان و تجهیزات و محصولات می‌باشد. |
| تمرکز معماری امنیتی | مهمترین تمرکز، نگهداری وسایل IT و اطلاعات ذخیره شده و تبادل شده در میان این تجهیزات است.<br>سرور مرکزی ممکن است نیازمند حفاظت بیشتری باشد. | هدف اصلی حفاظت از کاربران در حاشیه است، شامل: دستگاه‌های سطح فیلد همانند کنترل‌کننده‌های فرآیند همچنین نگهداری از سرور مرکزی |
| نتایج تصادفی | راه‌حل‌های امنیتی معمول پیرامون سیستم‌های IT طراحی شده است. | ابزارهای امنیتی باید در حالت Off-line آزمایش شوند تا مطمئن شویم که بر روی عملکرد عادی سیستم‌های کنترل صنعتی تاثیر نمی‌گذارند. |

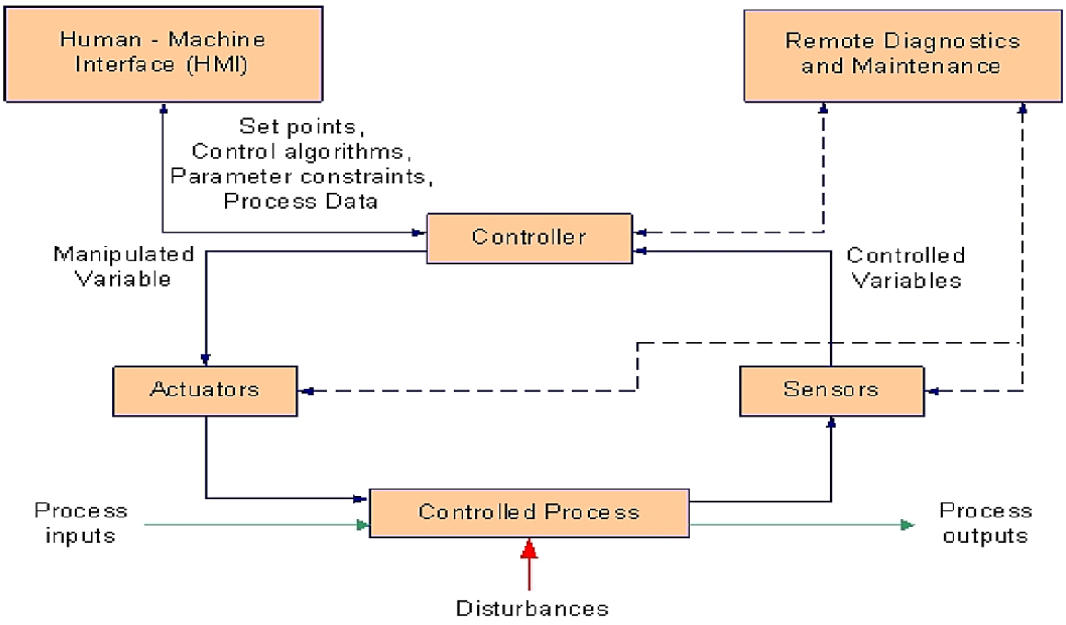
| | | |
|---|---|---|
| فعل‌وانفعال‌های حساس به زمان | دارای فعل و انفعال‌های کمتری است که حساسیت به زمان داشته باشند<br>کنترل دسترسی شدید می‌تواند برای درجات ضروری امنیت اجرا شود | پاسخ به فعل و انفعال‌های ضروری و انسان حیاتی است.<br>دسترسی به سیستم‌های کنترل صنعتی باید محدود و کنترل شده باشد، اما نباید مانع تعامل به واسط کاربر گردد. |
| سیستم‌عامل | سیستم‌ها برای کار با سیستم‌عامل‌های خاصی طراحی شده‌اند.<br>ترفیع با توجه به در دسترس بودن ابزارها کار درستی است. | سیستم‌عامل‌های مختلف و مناسبی که اغلب دارای امکانات امنیتی توکار نمی‌باشند.<br>تغییر در نرم‌افزارها باید با دقت و معمولا توسط شرکت‌ها انجام گیرد زیرا دارای الگوریتم‌های کنترلی و نرم‌افزارها و سخت‌افزارهای اصلاح شده هستند. |
| محدودیت منابع | سیستم‌ها مشخص شده دارای منابع کافی هستند تا بتوانند برنامه‌های کاربری اضافی همانند راه‌کارهای امنیتی را پشتیبانی کنند. | سیستم‌ها برای پشتیبانی از فرآیندهای صنعتی طراحی شده‌اند و ممکن است منابع و حافظه کافی برای پشتیبانی از امکانات امنیتی اضافی را نداشته باشند. |
| ارتباطات | پروتکل‌های ارتباطی استانداردی استفاده می‌کنند. | تعداد زیادی پروتکل‌های ارتباطی و استاندارد و<br>انواع مختلفی از وسایل ارتباطی شامل سیمی و بیسیم استفاده می‌شوند.<br>شبکه‌های پیچیده‌ای هستند و گاهی اوقات نیازمند مهندسان خبره برای کنترل می‌باشند. |
| مدیریت تغییرات | اگر سیاست‌ها و روندهای امنیتی مناسبی وجود داشته باشد تغییرات در نرم‌افزارها به صورت دوره‌های زمانی انجام می‌گردد و این فرآیندها معمولا به صورت خودکار انجام می‌شود. | تغییرات در نرم‌افزارها باید به صورت کامل آزمایش شود تا اطمینان داشته باشیم که تمامیت سیستم کنترلی حفظ می‌گردد. قطع سیستم‌های کنترل صنعتی باید به صورت برنامه‌ریزی شده در ماه/ هفته صورت بگیرد. سیستم‌های کنترل صنعتی |

| | | |
|---|---|---|
| | | ممکن است از سیستم عامل‌هایی استفاده کنند که مدت زمان زیادی است پشتیبانی نشده است. |
| عمر قطعات | معمولا بین ۳-۵ سال است. | معمولا بین ۱۵-۲۰ سال می‌باشد. |
| دسترسی به قطعات | قطعات معمولا محلی و در دسترس هستند. | قطعات می‌توانند ایزوله و قابل دسترسی از راه دور باشند. |

به دلیل اینکه ارائه یک سیستم مناسب نیازمند شناخت کافی سیستم‌های صنعتی است، در اینجا لازم است تا با اجزای مختلف تشکیل دهنده‌ی یک سیستم صنعتی آشنا شویم.

## ۲-۳ عملکرد سیستم‌های کنترل صنعتی

همان‌طور که در شکل ۲-۱ نشان داده شده است عملکرد سیستم‌های کنترلی، شامل چرخه‌ی کنترل و برخی اجزای مختلف است. در ادامه به بررسی آن‌ها خواهیم پرداخت.




**شکل ۲-۱** نحوه عملکرد سیستم‌های کنترل صنعتی [۲]