به نام خدا

گزارش هدف امنیتی سامانه پایا اسکادا

شرکت موج نیرو

تیر ۱۴۰۰

نسخه ۱,۰

شرکت موج نیرو

۱ معرفی

پایا-اسکادا یک نرم‌افزار اسکادا و اتوماتیک برای کنترل شبکه برق، آب و فاضلاب، گاز و سیستم نقل و انتقال است. این نرم افزار محدوده وسیعی از ویژگی‌ها و قابلیت‌ها را برای مدیریت سیستم‌های پیچیده بزرگ فراهم می‌کند. نرم‌افزار پایا-اسکادا شامل برنامه‌های SERVER (پردازشگر)، HMI (واسط کاربر)، System Engineering (مهندسی سیستم)، HIS (اطلاعات تاریخی) و DAC (جمع‌آوری داده) است.

نرم‌افزار پایا-اسکادا شامل برنامه‌های SERVER (پردازشگر)، HMI (واسط کاربر)، System Engineering (مهندسی سیستم)، HIS (اطلاعات تاریخی) و DAC (جمع‌آوری داده) است. در ادامه به توضیح هر برنامه می‌پردازیم.

SERVER

این واحد پرداز شگر و ه سته ا صلی سی ستم ا ست و وظیفه ارتباط با بخش‌های مختلف سی ستم و جمع‌آوری داده‌های آن‌ها بر ا ساس پروتکل‌های ا ستاندارد را بر عهده دارد. تبدیل‌های پروتکلی جهت ارتباط با سایر اجزای سیستم نیز بر عهده SERVER است. این استانداردها شامل WebSocket و IEC 60870-104 که فریم‌های آن تماماً توسط الگوریتم رمزنگاری AES128 رمز می‌شود.

HMI

واسط کاربر و ماشین در نرم افزار اسکادا است. در این برنامه نمایش اطلاعات شبکه بصورت نقشه‌های تک خطی با رنگ‌های استاندارد و دینامیک صورت گرفته و علاوه بر آن کلیه هشدارها و رویدادهای سیستم در لیست‌های جداگانه‌ای قابل دسترسی و مدیریت هستند.

همچنین اپراتور به کمک این برنامه علاوه بر دریافت کلیه اطلاعات نقاط مختلف پست و شبکه در صورت مطابقت با اینترلاک[1] قابلیت ارسال فرامین کنترلی را نیز خواهد داشت.

ارتباط بین HMI و سرور اسکادا شامل دو قسمت Restful API و WebSocket است.

System Engineering

ایجاد و اعمال تغییر در اطلاعات نقاط مختلف سیستم در مهندسی سیستم انجام می‌شود. مهندس سیستم با سطح دسترسی تعریف شده خود اقداماتی همچون تعریف نقاط، پارامترهای سیستم، محدودیت‌ها و هشدارها، مقیاس‌بندی، آدرس‌دهی، تنظیمات سیستم اسکادا، تعریف نواحی رویداد و هشدار، اینترلاک و بسیاری از موارد مهندسی دیگر را انجام می‌دهد.

[1] interlock

شرکت موج نیرو

HIS

سیستم اطلاعات تاریخی که به اختصار HIS نامیده می‌شود، اطلاعات دینامیکی پروسه تحت کنترل را در فواصل زمانی مشخص دریافت و آن‌ها را به صورت داده سری زمانی در یک پایگاه داده ذخیره و بایگانی می‌نماید. این سیستم همچنین این امکان را فراهم می‌آورد که از این اطلاعات ذخیره شده، گزارش‌های جدولی و منحنی تهیه و جهت تحلیل رفتار سیستم و برنامه‌ریزی‌های آینده مورد استفاده قرار گیرد. این اطلاعات می توانند به فرمت‌های مختلفی چون Excel ،pdf و html ارائه گردند.

DAC

واحد DAC به عنوان درگاه اتصال سیستم اسکادا به RTU های نصب شده در ایستگاه‌ها محسوب می‌گردد و نقش مفسر پروتکل ارتباطی را دارد. DAC در سیستم پایا اسکادا وظایف زیر را نیز برعهده دارد:

- جمع آوری داده: دریافت داده از RTU ها به صورت پریودیک، طی زمان‌های از پیش تعیین شده و یا برحسب درخواست سرور اسکادا شامل اطلاعات دیجیتال یک بیتی و دو بیتی و اطلاعات آنالوگ.
- پوشش پروتکلی: واحد DAC با استفاده از پروتکل‌های استانداردی چون IEC 60870-5- 101 , 104 ، DNP 3.0، Modbus، IEC 61850 و سایر پروتکل‌های رایج با RTU ها و IED ها ارتباط برقرار می‌نماید.
- ارسال فرامین: ارسال فرامین کنترلی دریافتی از سرور به RTU ها جهت کنترل شبکه‌های الکتریکی و پست‌ها و تجهیزات شبکه قدرت توسط این واحد انجام می‌شود.
- گزارش‌گیری: گزارش‌گیری از متغیرهای مختلف یا وضعیت و کیفیت RTU ها و خطوط مخابراتی به صورت پریودیک یا بنا به درخواست دیسپاچر بر عهده واحد DAC است.

۲ موارد امنیتی رعایت شده در پایا- اسکادا

۲ـ۱ کنترل احراز هویت و شناسایی

در این بخش به شناسایی و احراز هویت تمامی کاربران (افراد، فرآیندهای نرم‌افزاری و تجهیزات) قبل از اجازه به آن‌ها برای دسترسی به سیستم پایا-اسکادا پرداخته شده‌است. الزامات سیستمی برای این الزام اساسی به طور مختصر در جدول زیر آمده است و در ادامه به شرح هر مورد و سطح امنیتی آن پرداخته شده است.

۲ـ۱ـ۱ شناسایی و احراز هویت کاربران انسانی

در سیستم پایا-اسکادا تمام کاربران انسانی برای هر نوع دسترسی به سیستم شناسایی و احراز هویت می‌شوند. احراز هویت در این سیستم از طریق کلمات عبور انجام می‌شود. پایا-اسکادا در گام اول هویت تمام کاربران انسانی را تأیید می‌کند سپس در گام دوم مجوزهای اختصاص داده شده به کاربران انسانی شناسایی شده اعمال می‌گردد. در سیستم مهندسی نرم‌افزار پایا-اسکادا از لیست درختی و در قسمت user امکان تغییر و اعمال سیاست‌های امنیتی بر روی ورود و سطح دسترسی کاربران وجود دارد.

۲ـ۱ـ۲ شناسایی و احراز هویت فرآیندهای نرم‌افزاری و تجهیزات

در سیستم پایا-اسکادا تمام ماژول‌ها برای اجرا شدن نیاز به لایسنس دارند که مطابق با mac سیستم‌ها است. همچنین HMI و HIS_UI برای متصل شدن به Server و HIS_Server باید mac آدرس آن‌ها در مهندسی سیستم تعریف شده باشد.

۲ـ۱ـ۳ مدیریت حساب کاربری

مدیریت حساب کاربری در سیستم پایا-اسکادا به صورت گروه‌بندی حساب‌های کاربری شامل مبتنی بر نقش، مبتنی بر دستگاه و ایجاد شرایط برای عضویت در گروه و اختصاص مجوزهای مرتبط است. در سیستم مهندسی نرم افزار از لیست درختی و در قسمت user امکان تغییر و اعمال سیاست‌های امنیتی بر روی ورود و سطح دسترسی کاربران وجود دارد.

۲ـ۱ـ۴ مدیریت شناسه کاربری

در سیستم پایا-اسکادا قابلیت مدیریت شناسه‌های کاربری به واسطه نقش و گروه را دارد. این اقدام در سامانه SysEng در بخش user انجام می‌شود.

۲ـ۱ـ۵ مدیریت شناسه‌ی احراز هویت

در سیستم پایا-اسکادا علاوه بر شناسه کاربری یک شناسه احراز هویت یعنی کلمه عبور برای کاربران درنظر گرفته شده‌است. اپراتور برای ورود به HMI، SysEng و HIS_UI علاوه بر شناسه کاربری کلمه عبور درست را نیز باید وارد نماید.

۲ـ۱ـ۶ قدرت احراز هویت مبتنی بر کلمات عبور

در سیستم پایا-اسکادا از احراز هویت بر اساس نام کاربری و کلمه عبور اختصاصی است در این سیستم حداقل طول و تنوع کاراکترهای مورد استفاده برای کلمه عبور در نظر گرفته شده تا فرصت‌های نفوذ مهاجم را کاهش دهد. در صورت تغییر پسورد توسط کاربر پیغامی در صورت موفقیت آمیز بودن تغییر پسورد به کاربر نشان داده شده و در بخش Event ذخیره می‌شود.

۲ـ۱ـ۷ گواهینامه‌های زیر ساخت کلید عمومی (PKI)

در سیستم پایا-اسکادا از زیرساخت کلید عمومی و ارتباط TLSv1.2 جهت ارتباط HMI با سرور اسکادا استفاده می شود. این ارتباط با پروتکل https پیاده شده و تمامی عملیات و درخواست های کاربر با توکن اختصاص داده شده به آن کاربر کنترل می شود.

۲ـ۱ـ۸ قدرت احراز هویت کلید عمومی

در سیستم پایا-اسکادا کلید عمومی جهت احراز هویت certificate دریافت شده از سمت سرور به صورت پیش فرض بوده و غیر قابل دسترس کاربر است.

۲ـ۱ـ۹ بازخورد شناسه احراز هویت

سیستم پایا-اسکادا با مبهم‌سازی بازخورد، اطلاعات را در برابر افشای احتمالی آن‌ها توسط افراد غیرمجاز محافظت می‌کند. در نرم‌افزارهای HMI، SysEng و HIS UI که کاربر باید نام کاربری و کلمه عبور وارد کند کلمه عبور به صورت کاراکتر * نمایش داده می‌شود. همچنین علت عدم موفقیت در احراز هویت نمایش داده نمی‌شود و پیام نام کاربری یا کلمه عبور اشتباه است نمایش داده می‌شود.

۲ـ۱ـ۱۰ تلاش‌های ورود ناموفق به سیستم

به دلیل احتمال وجود حمله‌ی DOS بر روی سیستم، تعداد تلاش‌های ناموفق دسترسی به سیستم به طور متوالی به سه بار محدود شده‌است. در نرم‌افزارهای HMI، SysEng و HIS_UI اگر کاربر به طور متوالی سه بار کلمه عبور را اشتباه وارد کند کاربر غیر فعال می‌شود و تنها با فعال‌سازی کاربر توسط مدیر سامانه در سیستم مهندسی، کاربر موفق به احراز هویت می‌گردد.

۲ـ۱ـ۱۱ اعلان استفاده از سیستم

در سیستم پایا-اسکادا اعلان استفاده از سیستم در هنگام دسترسی به یک سیستم کنترلی خاص و تغییرات در سیستم به صورت نام کاربری ثبت می‌شود. در نرم افزار HMI که کاربر اجازه تغییرات در سیستم کنترلی را داراست در بخش Event تمام فعالیت‌های کاربر با نام کاربری وی ثبت می‌گردد. بخش Event دارای دیتابیس جدا است.

فعالیت‌های کاربر در نرم‌افزارهای HMI و SysEng و HIS_UI در log مربوط به هر کدام ذخیره می‌گردد. تمام logها براساس زمان ایجاد در پوشه log که در پوشه اصلی نرم‌افزار پایا-اسکادا قرار دارد ذخیره می‌شوند. پس از احراز هویت کاربر در سامانه پایا-اسکادا، در صفحه اصلی اعلام می‌شود که چه کاربری در حال استفاده از سامانه است. همچنین تمامی لاگ‌های مرتبط با احراز هویت کاربران در سیستم ثبت می‌شود.

۲ـ۲ کنترل استفاده (UC)

هدف از این بخش اعمال امتیازات اختصاص داده شده به یک کاربر احراز هویت شده به منظور انجام فعالیت مورد درخواست بر روی سیستم کنترل صنعتی و نظارت بر چگونگی استفاده از این امتیازات است. الزامات سیستمی برای این الزام اساسی به طور مختصر در جدول زیر آمده است و در ادامه به شرح هر الزام و سطح امنیتی آن پرداخته شده‌است.

۲ـ۲ـ۱ اعمال مجوز

در سیستم پایا-اسکادا در نرم افزار SysEng مهندس سیستم می‌تواند دسترسی کاربران به نرم‌افزار را مبتنی بر نقش مدیریت نماید. این قابلیت در لیست درختی و در قسمت user وجود دارد.

۲ـ۲ـ۲ قفل نشست

در سیستم پایا-اسکادا در نرم افزار سیستم مهندسی دسترسی کاربران تنظیم می‌شود. مهندس سیستم زمان قفل نشست را تنظیم می‌کند به این صورت که اگر کاربر برای مدت معینی (قابل تنظیم در سامانه مهندسی) در نرم افزار HMI فعالیت نداشته باشد HMI قفل شده و کاربر برای فعالیت باید مجدد login کند. همچنین مهندس سیستم می‌تواند برای کاربرانی قفل نشست را غیرفعال نماید. این قابلیت در لیست درختی و در قسمت user وجود دارد.

۲ـ۲ـ۳ خاتمه‌ی نشست راه دور

گاهی workstation در فاصله زیادی قرار دارد به همین علت در سیستم پایا-اسکادا امکان نشست از راه دور در نظر گرفته شده‌است. امنیت نشست از راه دور از طریق روتر، IP و firewall ایجاد می‌شود. در نرم‌افزار مهندسی سیستم با ایجاد کاربر جدید و یا مشاهد کاربران تعریف شده می‌توان مدت زمان نشست کاربر را تنظیم کرده، که بعد از این مدت کاربر نیاز به login مجدد دارد. این قابلیت در لیست درختی و در قسمت user وجود دارد.

۲ـ۲ـ۴ کنترل نشست‌های همزمان

در سیستم پایا-اسکادا برای کنترل نشست همزمان هر نام کاربری فقط در یک سیستم اجازه login شدن دارد و هر workstation فقط یک کاربر دارد که مهندسی سیستم آن را تنظیم می‌نماید. در نرم‌افزار مهندسی سیستم در قسمت مدیریت کابران تعریف شده می‌توان برای تعداد نشست‌های همزمان کاربران محدودیت تعریف کرد، که در اینصورت بعد از رسیدن به این تعداد سرور اجازه اتصال کاربر جدید را نمی‌دهد.

۲ـ۲ـ۵ رخدادهای قابل ممیزی

در سیستم پایا-اسکادا تمام رخدادهای مهمی که به ممیزی نیاز دارند در سیستم ذخیره می‌شود. رخدادها و log شامل اطلاعات برچسب زمانی، منبع، دسته بندی، نوع، شماره شناسایی رخداد و نتیجه رخداد است. رخدادها دارای دیتابیس جداگانه و logها در پوشه log در مسیر فایل اصلی پایا-اسکادا وجود دارد.

۲ـ۲ـ۶ ظرفیت حافظه ذخیره‌سازی ممیزی

در سیستم پایا-اسکادا فایل‌هایی مانند فایل‌های ممیزی، فایل تنظیمات و فایل‌های خروجی گزارش‌گیری در مسیر فایل‌های اجرایی ذخیره نمی‌شود. پوشه log در پوشه اصلی نرم‌افزار قرار دارد. رخدادها که مهمترین ممیزی

سیستم پایا-اسکادا است در دیتابیس جداگانه ذخیره شده و می‌توان تنظیم کرد که در مدت زمان‌های معین پشتیبان‌گیری شود. همچنین در سیستم مهندسی برای حافظه درایو ذخیره‌سازی لاگ یک محدودیت در نظر گرفته می‌شود و در صورت رسیدن حافظه ذخیره سازی به آن مقدار در HMI پیام "فضای حافظه رو به اتمام است" به صورت Alarm نمایش داده می‌شود تا کاربر بتواند از حافظه پشتیبان بگیرد.

۲ـ۲ـ۷ واکنش به خطاهای پردازشی ممیزی

در سیستم پایا-اسکادا با بوجود آمدن خطای پردازشی ممیزی تغییری در نحوه ذخیره‌سازی ممیزی بوجود نمی‌آید. تمامی رخدادها در سامانه ذخیره می‌شود و هنگام به وجود آمدن خطاهای سخت‌افزاری و نرم‌افزاری برای جلوگیری از دست دادن سرویس‌ها به کارکنان هشداد داده می‌شود. به عنوان مثال زمان رسیدن آستانه ظرفیت ذخیره‌سازی هشدار داده می‌شود.

۲ـ۲ـ۸ برچسب‌های زمانی

در سیستم پایا-اسکادا ممیزی‌ها شامل زمان و تاریخ طبق ساعت سیستم بر اساس تاریخ (سال/ روز/ ساعت/دقیقه/ثانیه) هستند. Log نرم‌افزارها در پوشه Log ذخیره می‌شوند که در پوشه اصلی نرم‌افزار قرار دارد. رخدادها که مهم‌ترین ممیزی سیستم پایا-اسکادا است در دیتابیس جداگانه ذخیره می‌شوند. رخدادها در بخش Event در سامانه HMI قابل مشاهده توسط کاربران است.

۲ـ۲ـ۹ عدم انکار

در سیستم پایا-اسکادا فعالیت‌های انجام شده توسط کاربران از جمله انجام فعالیت‌های اپراتوری، تغییر پیکره‌بندی سیستم کنترلی، ایجاد و تولید اطلاعات، ارسال پیام، تأیید اطلاعات و دریافت پیام به طور کامل ذخیره می‌گردد. بخشی از این فعالیت‌ها در Event و بخشی در Log ذخیره می‌گردد. کاربران امکان ایجاد تغییرات بر روی مقادیر ثبت شده را ندارد.

۲ـ۳ یکپارچگی سیستم (SI)

در این بخش به ویژگی تضمین یکپارچگی و صحت سیستم پایا-اسکادا به منظور حفاظت از هر گونه دستکاری غیرمجاز می‌پردازیم. الزامات سیستمی برای این الزام اساسی به طور مختصر در جدول زیر آمده است و در ادامه به شرح هر مورد و سطح امنیتی آن پرداخته شده‌است.

۲ـ۳ـ۱ یکپارچگی ارتباطات

در سیستم پایا-اسکادا ارتباطات از طریق پروتکل های امن پیاده سازی شده که محتوای پیام‌ها رمز نگاری شده است همچنین داده های مبادله شده بین سیستم ها رمز نگاری شده است. به عنوان مثال منابع خاصی که سیستم

شرکت موج نیرو

پایا اسکادا از آن‌ها جهت کار خود استفاده می‌کند مانند اطلاعات اتصال به پایانه‌ها که در فایل ini ذخیره می‌شود به صورت رمزشده است و در برابر هر گونه تغییر غیر مجاز محافظت شده است.

۲ـ۳ـ۲ حفاظت از کدهای مخرب

بر روی سیستم‌های استفاده کننده از نرم‌افزار پایا-اسکادا، firewall ویندوز و آنتی ویروس پادویش فعال شده که از سیستم در برابر کدهای مخرب جلوگیری می‌کند.

۲ـ۳ـ۳ تأیید عملکرد امنیتی

سیستم پایا-اسکادا یک سند مرتبط با انجام تست‌های FAT و SAT (چک لیست) در اختیار مراکز قرار می‌دهد. این سند علاوه بر دستورالعمل‌هایی برای تست نرم‌افزارهای پایا-اسکادا، دستور العمل‌هایی برای تست‌های امنیتی فراهم می‌آورد. نمونه تست‌ها به صورت زیر است:

۱- تأییدیه اعتبار آنتی ویروس‌ها
۲- تأیید اعتبار شناسایی و احراز هویت (سطوح دسترسی و اقدامات مجاز کاربران)
۳- تعریف Operation یا هر عملیات مجاز کاربران
۴- تعریف Security Levelها و داده‌های حساس
۵- تعریف نظارت بر روی Back up
۶- تأییدیه نظارت بر روی firewall

۲ـ۳ـ۴ یکپارچگی اطلاعات و نرم‌افزار

در سیستم پایا-اسکادا آشکارسازی و ثبت و ضبط و گزارش‌دهی و حفاظت در برابر هر گونه تغییر غیر مجاز بر روی نرم‌افزارها و سخت افزارها اعمال می‌گردد. به عنوان مثال فایل‌های ذخیره شده در سیستم پایا-اسکادا با استفاده از رمزنگاری در برابر تغییرات غیر مجاز محافظت می‌شود. همچنین اطلاعات و داده‌های پردازشی به صورت رمزشده ذخیره می‌شوند تا در برابر هرگونه تغییر غیر مجاز محافظت شوند. ایجاد محدودیت‌های کاربری و محدودیت‌های دسترسی کاربران و سخت افزارها (کاربران با تعریف نقش‌ها و سخت‌افزارها با تعریف mac address که در سیستم مهندسی اعمال می‌گردد) قابلیتی برای حفاظت از تغییر غیر مجاز در سیستم پایا-اسکادا است.

۲ـ۳ـ۵ مدیریت خطا

در سیستم پایا-اسکادا مدیریت خطاها به گونه‌ای است که خروجی هر خطا شامل اطلاعات اضافی نبوده تا از افشای اطلاعات مخافظت شود. به عنوان مثال اگر کاربر نام کاربری و رمز عبور را اشتباه وارد کند؛ مشخص نمی‌شود که کدام مورد اشتباه بوده است. همچنین در کنترل MacAddress پیام "شما اجازه دسترسی از این دستگاه را ندارید" نمایش داده می‌شود.

۲ـ۳ـ۶ یکپارچگی نشست

در سیستم پایا-اسکادا نشست میان مؤلفه‌های HMI، HIS و Server به صورت یکپارچه برقرار می‌شود. برقراری این نشست به این صورت است که در هر یک از نرم‌افزارهای HMI، SysEng و HIS_UI بعد از وارد کردن username و password درخواستی به سرور مرکزی ارسال و نشست برقرار می‌شود. در صورتی که هر کاربر Log Out کند و یا نرم‌افزار بسته و یا ارتباط بین سرور و آن نرم‌افزار قطع شود این نشست خاتمه می‌یابد. همچنین زمان خاتمه این نشست در مهندسی سیستم قابل تنظیم است و در زمان فرارسیدن خاتمه (کاربر چه در حال استفاده از سیستم باشد یا خیر) نشست پایان می‌یابد.

۲ـ۴ محرمانگی داده‌ها (DC)

تضمین محرمانگی اطلاعات بر روی کانال های ارتباطی و مخابراتی و در مخازن داده‌ها برای جلوگیری از افشای غیرمجاز آن‌ها در سیستم پایا-اسکادا در این الزام بیان می‌شود. در ادامه به شرح هر مورد و سطح امنیتی آن پرداخته شده‌است.

۲ـ۴ـ۱ محرمانگی اطلاعات

در توسعه سیستم پایا-اسکادا برای تضمین محرمانگی اطلاعات از رمزنگاری اطلاعات استفاده شده‌است. در این سیستم برای رمزنگاری از تولید بیت تصادفی قطعی ارائه شده توسط پلتفرم سیستم عامل ویندوز بهره‌گرفته شده‌است. عملیات رمزنگاری در کل برنامه با کمک کتابخانه CRYPTOPP پیاده سازی شده و تولید بیت تصادفی با روش HMAC-DRGB انجام شده‌است. همچنین این پیاده‌سازی مبتنی بر استاندارد NIST SP 800-57 بوده است. همچنین سیستم پایا اسکادا در هنگام نصب، سطوح دسترسی و حفاظتی مناسب را بر روی فایل‌های مهم و حساس خود ایجاد می‌نماید تا از دسترسی سایر برنامه‌ها و افراد بدون سطح دسترسی مناسب جلوگیری کند. در پیکربندی سیستم پایا-اسکادا از ظرفیت‌های سیستم عامل ویندوز استفاده می‌شود. محدودسازی کاربر جهت دسترسی به منابع غیر مجاز مانند پورت‌های USB و فایل‌های سیستمی با توجه به قابلیت‌های پلتفرم مورد استفاده یعنی ویندوز سرور ۲۰۱۲ و آنتی ویروس پادویش اعمال می‌گردد.

۲ـ۴ـ۲ استفاده از رمزنگاری

سیستم پایا-اسکادا از روش رمزگذاری متقارن AES256 استفاده می‌کند .در نرم‌افزار پایا-اسکادا پیاده‌سازی کارکرد برای استقرار رمزنگاری مطابق با طرح‌های استقرار کلید مبتنی بر RSA بر اساس استاندارد NIST SP 800-56B و طرح برقرارای کلید مبتنی بر منحنی بیضوی که برآروده کننده استاندارد NIST SP 800-56A است انجام گرفته است. سیستم پایا-اسکادا رمزنگاری/رمزگشایی را مطابق با الگوریتم AES-CBC mode و AES-GSM و اندازه کلید رمزنگاری ۲۵۶ بیت انجام می‌دهد. سیستم پایا اسکادا خدمات درهم‌سازی را مطابق با الگوریتم MD5 و اندازه چکیده پیام ۲۵۶ بیت انجام می‌دهد که استاندارد FIPS Pub 180-4 را برآورده می‌نماید همچنین کد اصالت سنجی را بر پایه درهم سازی HMAC مطابق الگوریتم MD5 با اندازه کلید ۲۵۶ و اندازه خلاصه پیام ۲۵۶ بیت انجام می‌دهد. در توسعه سیستم پایا اسکادا جهت رمزنگاری از تولید بیت تصادفی قطعی ارائه شده توسط پلتفرم سیستم عامل ویندوز بهره گرفته شده‌است. عمیات رمزنگاری در کل برنامه با کمک کتابخانه CRYPTOPP پیاده‌سازی شده و تولید بیت تصادفی با روش HMAC-DRGB انجام شده‌است. همچنین این پیاده‌سازی مبتنی بر استاندارد NIST SP 800-57 بوده است. در نرم افزار پایا اسکادا اطلاعات کاربری مانند رمز عبور به صورت HASH شده در داخل پایگاه داده‌ای که در حافظه غیر فرار قرار دارد ذخیره می‌شود. دسترسی به پایگاه داده نیازمند کلید اتصال بوده که این کلید در داخل یک توکن سخت‌افزاری قرار گرفته است و تنها توسط برنامه پایا اسکادا قابل استفاده است. رمز دسترسی به توکن تنها در اختیار نرم‌افزار پایا بوده و تنها نرم‌افزار با استفاده از آن می‌تواند محتویات توکن که کلید رمزگذاری در سیستم است را قرائت کند.