باسمه تعالی

عنوان مستند

امنیت محیط توسعه CODESYS

برای برنامه نویسی برنامه های کنترلرها

فهرست مطالب

۱ امنیت در برنامه های کنترل صنعتی

۱-۱ مقدمه

با وجود اینکه امنیت IT کامپیوترهای بازرگانی یک امر متداول است، در گذشته حفاظت از برنامه های کنترل صنعتی در مقابل دسترسی غیرمجاز یا حتی حملات شدید مورد توجه نبوده است. ولی از زمان حمله معروف Stuxnet، این وضعیت تغییر کرده است. مؤسسات دولتی مانند ICS-CERT یا دفتر فدرال آلمان برای امنیت اطلاعات (BSI، مخفف نام آلمانی آن) افزایش چشمگیری در حوادث امنیتی را در کارخانه ها، نیروگاه ها و دیگر برنامه های اتوماسیون صنعتی گزارش کردند.

ضمناً، آسیب پذیری ها توسط مشاوران امنیتی به طور سیستمی جستجو و شناسایی شده اند. امروزه، حفاظت در مقابل انواع حوادث برای تجهیزات اتوماسیون ماشین های صنعتی، کارخانه ها و نیروگاه ها به منظور حفاظت از موارد زیر اجتناب ناپذیر است:

- دسترس پذیری عملکرد کنترلر
- عملکرد برنامه
- محرمانگی برنامه و کد منبع برنامه
- یکپارچگی عملکرد برنامه، عملکرد سیستم توسعه و اجزای بکار گرفته شده
- کنترل کل عملکرد
- صحت کنترلرها و اطلاعات آنها

به علاوه بهبود عملکرد، بهبود امنیت باید به طور دائمی رو به افزایش باشد. اما دستیابی به امنیت ۱۰۰ درصدی امکان پذیر نیست. حتی زمانی که سیستمی با جدیدترین عناصر امنیتی طراحی شده باشد، ممکن است از طریق اتصالات به شبکه های تأمین کنندگان، پیمانکاران و شرکا آسیب پذیر باشد.

۱-۲ نحوه بکارگیری و هدف این گزارش

این گزارش سازندگان دستگاه های اتوماسیون هوشمند، «یکپارچه سازان سیستمی[1]» و اپراتورهای برنامه های کنترل صنعتی را قادر خواهد ساخت تا با استفاده از معیارهای یکپارچه امنیتی در CODESYS (نرم افزار اتوماسیون سازگار با استاندارد IEC ۶۱۱۳۱-۳) از تأسیسات خود محافظت کنند. این گزارش مقدمه ای درباره موضوعات امنیتی در اتوماسیون و سیستم های کنترل صنعتی ارائه کرده، مسئولیت نهادهای مشارکت کننده را مشخص کرده و نشان می دهد کدام معیارهای کنونی و آتی CODESYS در ایجاد سطح مطلوب امنیت کمک رسانی خواهند کرد. به علاوه، نحوه مدیریت آسیب پذیری های شناسایی شده CODESYS را نیز نشان می دهد.

۱-۳ پیامدها

صرف نظر از تهدیدات حاصل از سوءاستفاده سهوی یا حملات عمدی با سطح شدت گوناگون، امنیت سامانه اتوماسیون وظیفه ای است که تمام بخش های برنامه کنترل صنعتی را دربرمی گیرد (برای مثال، در ماشین ها یا نیروگاه ها و بخش هایی که از طریق یک معیار امنیتی قابل تضمین نیستند). به علاوه، امنیت به تلاش های خاصی نیاز دارد:

- کنترل دسترسی فیزیکی به تأسیسات حیاتی امنیتی
- قدرت پردازش بیشتر روی دستگاه ها
- تلاش پیکربندی برای برنامه نویس و اپراتور برنامه
- از بین رفتن راحتی در عملیات و پشتیبانی
- آموزش امنیتی برای یکپارچه سازان و اپراتورهای سیستمی

هر شرکت عملیاتی باید میزان امنیت مورد نیاز و میزان آمادگی برای هزینه در آن هدف را برای خود ارزیابی کنند. بدین ترتیب، سازندگان محصولات اتوماسیون باید ابزارهای مناسب حفاظت از بخش های حیاتی سامانه اتوماسیون خود را برای یکپارچه ساز و اپراتور سیستمی چنین برنامه های صنعتی فراهم کنند.

پلتفرم نرم افزار اتوماسیون CODESYS با استاندارد IEC ۶۱۱۳۱-۳ چندین معیار ارائه می کند. این معیارها جایگزین مسئولیت یکپارچه ساز یا اپراتور سیستمی برنامه کنترل صنعتی، فعالیت های امنیتی مانند نشانه های تهدیدات و تعریف اقدامات ضروری به منظور دستیابی به سطح مطلوب امنیتی، نیستند ولی به دستیابی به آنها کمک می کنند.

[1] افرادی که سیستمی را یکپارچه می کنند (سر هم می کنند).

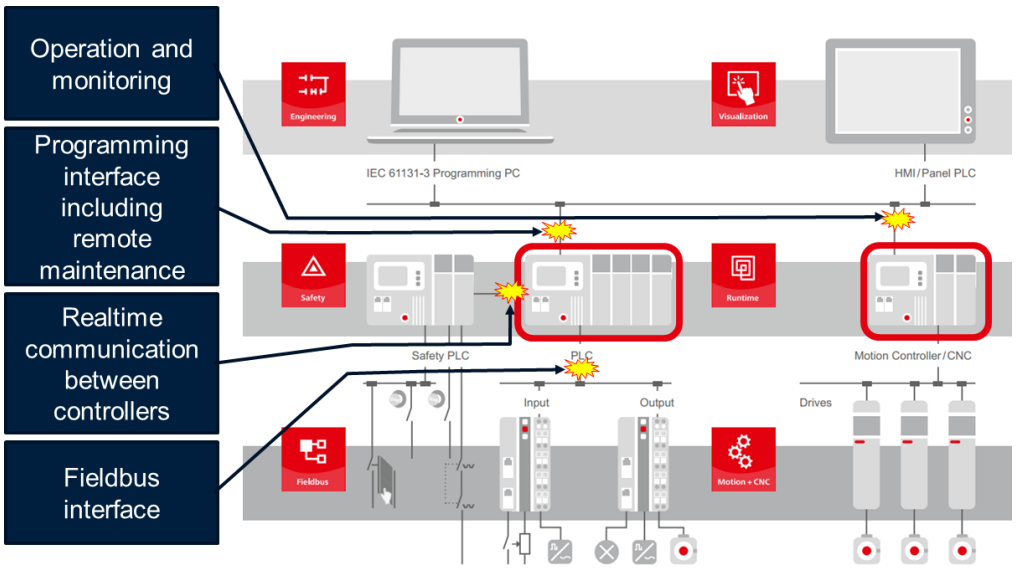
۲ شرایط و تعاریف

۲-۱ تجهیزات

هدف محیط های اتوماسیون صنعتی، برای مثال تولید اجناس یا حفظ فعالیت های دستگاه یا جریان های فرآیند است. بخش های مختلف محیط های صنعتی توسط خطرات امنیتی تهدید شده اند که می توانند به این هدف آسیب وارد کرده یا از آن جلوگیری کنند. با توجه به شکل ۱، تجهیزات محیط اتوماسیون صنعتی کنترلر شامل برنامه اجرا شده روی کنترلر، سیستم توسعه استفاده شده برای ساخت برنامه و مدیریت کل سیستم می شود.

۲-۲ آسیب پذیری

محیط های اتوماسیون رایج ممکن است در مکان های مختلف آسیب پذیر باشند:



شکل ۱- آسیب پذیری های احتمالی در محیط اتوماسیون رایج

۲-۳ سطوح امنیتی

استاندارد بین المللی IEC ۶۲۴۴۳ سطوح امنیتی گوناگونی را تعریف می کند:

- **سطح ۱: تهدیدات کمیاب و تصادفی**

مثال: خرابی هارد دیسک، خطای عملیاتی

- **سطح ۲: تهدیدات عمدی از طریق ساده ترین ابزار**

مثال: حدس صحیح رمز عبور

- **سطح ۳: تهدیدات عمدی از طریق ابزارهای بسیار پیشرفته**

مثال: ابزارهای هکرها

- **سطح ۴: تهدیدات عمدی از طریق ابزارهای بسیار پیشرفته و منابع توسعه یافته**

مثال: توسعه برنامه خاص، آگاهی از برنامه یا فساد عوامل داخلی

ترتیب سطح به احتمالی اینکه تهدیدات ذکر شده واقعاً رخ خواهند داد بستگی دارد.

۲-۴ کنترلر

کامپیوتر صنعتی که یک تأسیسات صنعتی را کنترل می کند می تواند «PLC»[۲]، «PAC»[۳]، کنترلر حرکتی، «ECU»[۴]، «DCS»[۵]، «PCS»[۶] یا دیگر عبارات فنی نام بگیرد. در هر صورت این کامپیوتر، فعالیت خودکار را انجام می دهد. بدین ترتیب این دستگاه هوشمند قابل برنامه ریزی، هدف اصلی حملات امنیتی است. به علاوه، این کنترلرها باید برای کاربری معین شده خود، برنامه ریزی شوند. بدین معنی که همگی حاوی یک رابط برنامه نویسی هستند که به سادگی قابل بهره برداری است. به دلیل این کاربری معین شده، جلوگیری قطعی از دسترسی به برنامه نویسی یا برنامه نویسی مجدد برنامه هایی که روی کنترلر اجرا شده اند غیرممکن است. بنابراین، محافظت از این کنترلرها و رابط های ارتباطی آنها برای یکپارچه سازان و اپراتورهای سیستمی چنین دستگاه هایی از اولویت بالایی برخوردار است.

۲-۵ برنامه

قابلیت عملیاتی که روی کنترلر اجرا شده، تعریف عملیاتی هدف محیط های اتوماسیون صنعتی در نرم افزار را نشان می دهد. این قابلیت از طریق رابط برنامه نویسی در کنترلر بارگذاری شده است.

---

[۲] Programmable Logic Controller
[۳] Programmable Automation Controller
[۴] Electronic Control Unit
[۵] Distributed Control System
[۶] Process Control System

۲-۶ تهدیدات

قابلیت عملیاتی یک سامانه اتوماسیون صنعتی می تواند به شکل های گوناگونی آسیب دیده یا با اختلال مواجه شود. غالباً تهدیدات عمدی مانند خرابکاری یا جاسوسی به عنوان تمرکز اصلی معیارهای امنیتی در نظر گرفته شده اند. با اینحال، اشکالات عملکردی غیرعمدی که به سبب سخت افزار یا نرم افزار معیوب، عملکرد معیوب حین اجرا یا در سرویس ها رخ می دهند، غالباً به تجهیزات آسیب می رسانند.

۲-۷ محیط محافظت شده

سامانه های اتوماسیون صنعتی باید در محیط هایی اجرا شوند که از عملیات معیوب عمدی یا غیرعمدی و خطر آسیب پذیری تجهیزات جلوگیری کنند. با اینحال، هر سامانه به دسترسی حین نصب، راه اندازی، عملیات یا نگهداری نیاز دارند. بدین ترتیب، جداسازی زیرسیستم های کل سامانه به منظور فعال سازی دسترسی کنترل شده به هر زیرسیستم فقط برای پرسنل مجاز ضروری است. برای اطلاعات بیشتر بخش ۳.۱ مشاهده شود.

۳ ابزارهای عمومی برای حفاظت از برنامه های کنترل صنعتی

در مرحله اول، تمام معیارهای امنیتی عموماً شناخته شده برای PCهای استاندارد باید در شبکه های تجهیزات اتوماسیون صنعتی اعمال شوند، مانند:

- حفاظت با آنتی ویروس
- رمزهای عبور قدرتمند و به طور منظم تغییر یافته

- حفاظت با دیوار آتش
- استفاده از VPN برای اتصالات بین شبکه ای
- برخورد محتاطانه با حافظه های جداشدنی اطلاعاتی مانند کارت های حافظه USB

به علاوه، مدیریت به خوبی تعریف شده کاربر و مجوز برای دسترسی به کنترلرها و شبکه های بهم پیوسته آنها اجباری است. به علاوه، چندین معیار عمومی و اضافی برای هر دستگاه یا سازنده نیروگاه الزامی است.

۳-۱ استفاده در محیط حفاظت شده

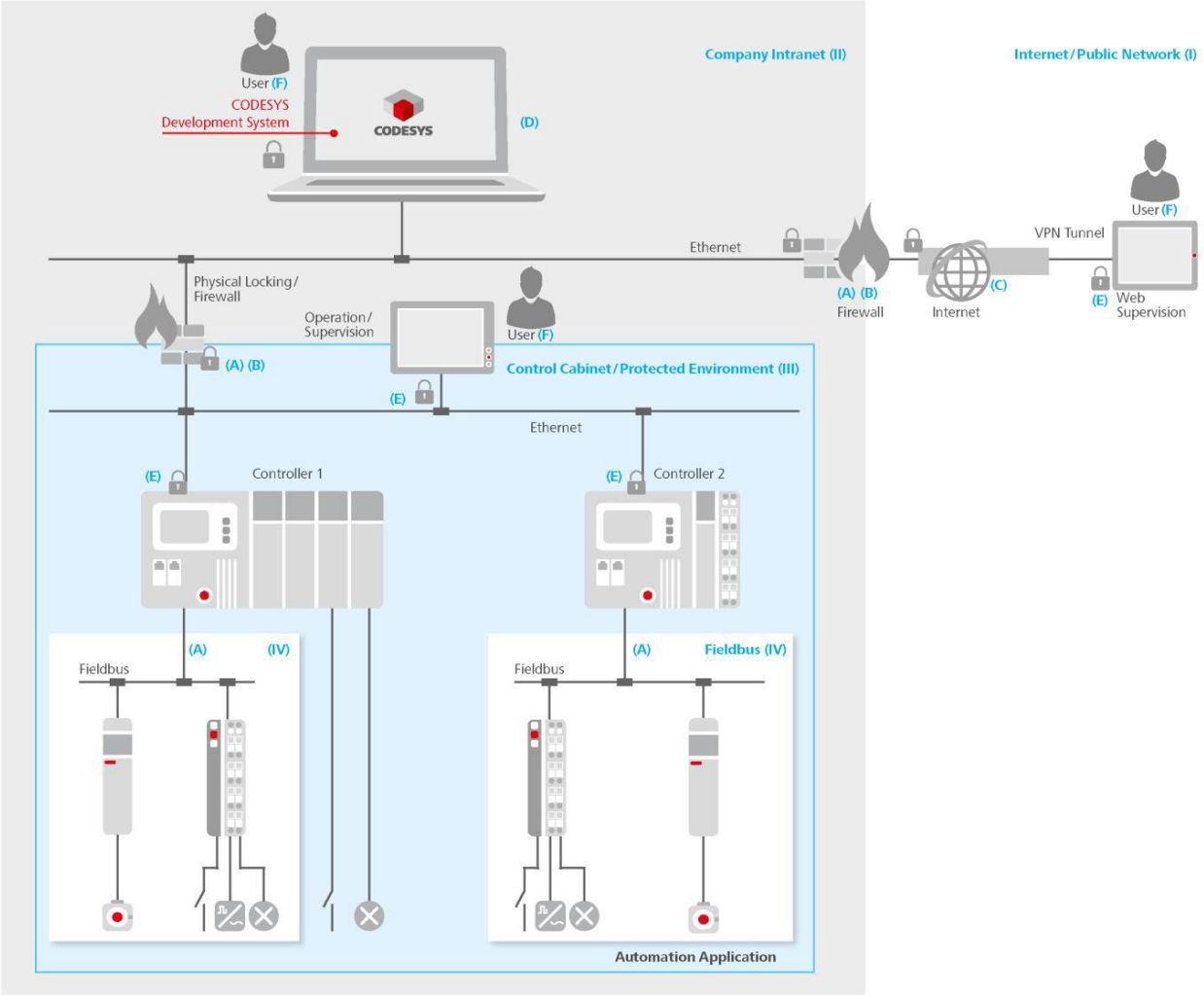
مکان یابی کنترلر در محیط حفاظت شده، به منظور اجتناب از دسترسی تصادفی یا عمدی به کنترلر یا برنامه آن (که برای عملیات دستگاه یا نیروگاه اجرا شده) کاملاً ضروری است. برای مثال چنین محیط حفاظت شده ای می‌تواند در:

- محفظه های قفل شده و الکتریکی و فاقد دسترسی ارتباطی از بیرون باشد.
- یک شبکه اینترانت با حقوق کاربری به خوبی تعریف شده و فاقد دسترسی از بیرون باشد.
- یک شبکه با دسترسی اینترنتی فقط از طریق یک دیوار آتش به خوبی حفظ شده و از طریق تونل VPN باشد.

واضح است که میزان حفاظت در این لیست کاهش می یابد. برای ایجاد چنین محیط محافظت شده ای، بایستی از چندین قانون پیروی شود:

- شبکه مطمئن تا حد امکان کوچک و مستقل از دیگر شبکه ها نگهداری شود.
- از ارتباط متقابل کنترلرها و ارتباط بین کنترلرها و دستگاه های میدانی از طریق پروتکل های استاندارد ارتباطی (سیستم های Fieldbus[۷]) و به وسیله معیارهای مناسب حفاظت شود.
- چنین شبکه هایی قفل شده و حتماً مجزا شوند.
- از سیستم Fieldbus فقط در محیط های حفاظت شده استفاده شود. این سیستم ها با معیارهای اضافی مانند رمزگذاری حفاظت نشده اند. یک دسترسی فیزیکی یا اطلاعاتی به سیستم های Fieldbus و تجهیزات آنها یک خطر امنیتی جدی است.

[۷] Fieldbus نام خانواده ای از پروتکل های شبکه کامپیوتری صنعتی است که برای کنترل بلادرنگ و توزیع شده استفاده می شود.



شکل ۲- محیط رایج در برنامه های اتوماسیون با نواحی امنیتی متفاوت

توضیحات شکل ۲:

شبکه های مجزا (کاملاً مجزا یا پیوسته از طریق دیوار آتش ایمن):

۱. شبکه خارجی مانند اینترنت، اتصال Dial-Up
۲. شبکه سازمانی
۳. دستگاه / شبکه سایت تولیدی
۴. Fieldbus

حفاظت از زیرساخت:

۱. حفاظت از دسترسی مکانیکی (مانند محفظه های کنترلی قفل شده)
۲. دیوار آتش

۳. شبکه خصوصی مجازی (VPN)
۴. حفاظت با آنتی ویروس، مدیریت کاربر شبکه / ویندوز
۵. مدیریت کاربر با روش احراز هویت مناسب (برای مثال، دانگل[۸]، رمز عبور)
۶. آموزش کارمندان در زمینه معیارهای امنیتی

۳-۲ کاربران آگاه از امنیت

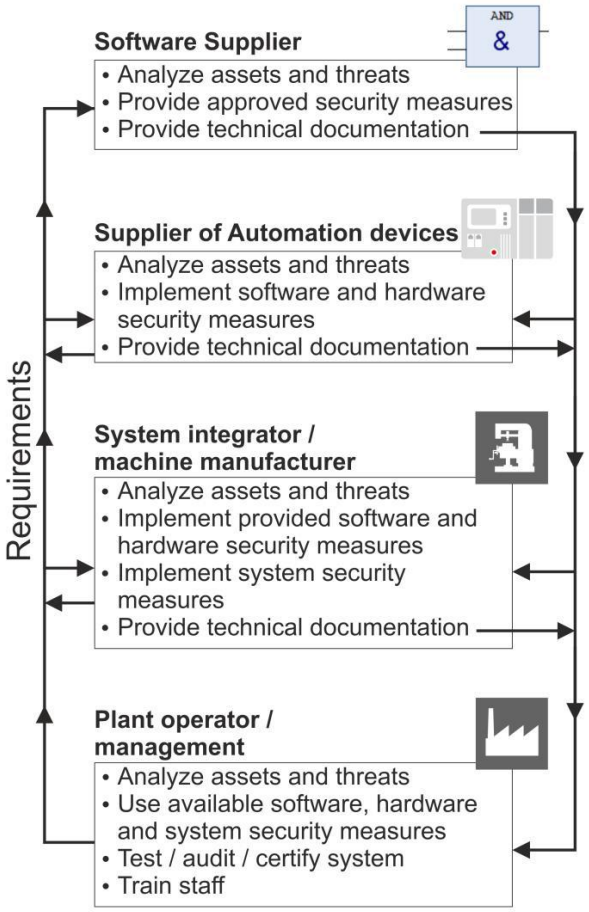
از آنجایی که اکثر حوادث امنیتی گزارش شده به دلیل خطاهای مدیریتی یا دستگاه سهواً رخ داده اند، کاربر کنترلرهای صنعتی نقش حیاتی در زمینه حفاظت امنیتی دارد. بدین ترتیب، دانستن تهدیدات احتمالی و معیارهای زیرساختی که برای اجتناب از این تهدیدات ضروری هستند، برای سازندگان تجهیزات/دستگاه ها و اپراتورها الزامی است.

کاربران CODESYS Development System و کنترلرهای قابل برنامه ریزی باید درباره خصوصیات امنیتی موجود و مورد نیاز حین برنامه نویسی برنامه کنترل، اطلاعات بیشتری داشته باشند. به منظور دستیابی به این هدف، توصیه می شود کاربران به آموزش مخصوص از طرف متخصصان امنیتی در شرکت یا خارج از آن بپیوندند.

۴ مسئولیت های امنیتی در برنامه های کنترل صنعتی

در راه اندازی برنامه های کنترل صنعتی، چندین نهاد و تأمین کننده فعال حضور دارند: تأمین کننده مؤلفه های نرم افزاری و سخت افزاری، یکپارچه ساز سیستمی یا سازنده برنامه های کنترل صنعتی و اپراتور. از آنجایی که امنیت IT عملیات جامعی است، تمام نهادهای ذکر شده باید در حفاظت از برنامه در مقابل حملات تلاش های خاصی انجام دهند.

[۸] دستگاه کوچکی که توانایی اتصال و استفاده با کامپیوتر را دارد، مخصوصاً برای صدور مجوز دسترسی به شبکه بی سیم.



شکل ۳- ارتباط بین نهادهای گوناگون در برنامه های کنترل صنعتی در زمینه امنیت

اطلاعات بیشتر درباره مسئولیت ها و وظایف گوناگون در نهاد در استاندارد «VDI/VDE ۲۱۸۲[۹]» توضیح داده شده است.

[۹] این استاندارد، بکارگیری مدل عمومی برای امنیت IT را نشان می دهد.

۵ معیارهای امنیتی موجود و قابل دسترسی در CODESYS

هدف شرکت 3S-Smart Software Solutions (سازنده نرم افزار اتوماسیون CODESYS با استاندارد IEC ۶۱۱۳۱-۳) ارائه معیارهایی است که به کاربر در انجام وظیفه حفاظت از برنامه در زمینه دسترس پذیری، یکپارچگی و محرمانگی کمک کند. این معیارها حفاظت در مقابل تهدیدات سطح ۱ و ۲ را دربرمی گیرند (بخش ۲.۳ مشاهده شود). در طولانی مدت، تهدیدات سطح ۳ نیز پوشش داده خواهند شد.

معماری CODESYS حاوی دو بخش است: محیط توسعه یکپارچه (CODESYS Development System ـ IDE[۱۰]) که به عنوان رابط کاربری در کامپیوتر پایانه اجرا می شود و سیستم Runtime (CODESYS Control) روی دستگاه قابل برنامه ریزی که کد برنامه را اجرا می کند. در زمان برنامه نویسی یک برنامه اتوماسیون صنعتی، هر دو بخش با یکدیگر به طور یکپارچه کار می کنند. بنابراین معیارهای امنیتی بر این بخش های اصلی نیز تأثیر می گذارد. به علاوه، CODESYS معیارهایی ارائه می کند که توسط کاربر از کد برنامه نویسی شده قابل فعال سازی هستند. از آنجایی که CODESYS Development System چندین قابلیت تصویرگرایی را ادغام می کند که باعث دسترسی حیاتی امنیتی به برنامه و دستگاه/نیروگاه می شود، معیارهای امنیتی برای این حوزه نیز توسط سیستم ارائه می شود.

بخش های بعد، معیارها و خصوصیاتی را توصیف می کنند که در آخرین نسخه CODESYS (نسخه ۳) قابل دسترسی هستند یا خواهند بود. به منظور حفاظت از برنامه و کنترلر، استفاده از CODESYS Development System ضروری است. آخرین نسخه به صورت رایگان در سایت www.codesys.com قابل دانلود است. به علاوه، استفاده از سیستم Runtime مناسب روی کنترلر نیز ضروری است. همانطور که در بخش ۷ تشریح شده، آسیب پذیری های شناسایی شده در نسخه های Patch برطرف خواهند شد. بدین ترتیب، توصیه می شود از آخرین نسخه های نرم افزاری به همراه این وصله ها استفاده شود.

جداول زیر چکیده ای از معیارها، مکان های آنها در CODESYS و کاربری آنها ارائه می کنند. هر معیار توضیح داده شده است. برای اطلاعات فنی درباره مفهوم هر معیار توضیح داده شده، توصیه می شود به CODESYS Online Help که به همراه CODESYS Development System نصب شده مراجعه شود.

[۱۰] Integrated Development Environment

جدول ۱- CODESYS Development System

معیار	ارائه شده در بخش	ارتباط معیار با ...			
		تأمین کنندگان تجهیزات اتوماسیون	یکپارچه سازان سیستمی / سازندگان دستگاه	اپراتور	معیار مناسب علیه ...
رمزگذاری کد منبع برنامه	۵.۱.۱		✓		تهدیدات و حملات دوره ای/غیرعمدی
مدیریت کاربر در سطح پروژه	۵.۱.۲		✓		تهدیدات و حملات دوره ای/غیرعمدی
امضا و رمزگذاری فایل های مربوط به CODESYS	۵.۱.۳	✓	✓	✓	حملات

جدول ۲- CODESYS Runtime System

معیار	ارائه شده در بخش	ارتباط معیار با ...			
		تأمین کنندگان تجهیزات اتوماسیون	یکپارچه سازان سیستمی / سازندگان دستگاه	اپراتور	معیار مناسب علیه ...
دسترسی به سیستم Runtime با مدیریت احراز هویت/مجوز	۵.۲.۱	✓	✓	✓	تهدیدات و حملات دوره ای / غیرعمدی
رمزگذاری و امضای کد برنامه اجرایی	۵.۲.۲	✓	✓		حملات
حالت فعالیت کنترلر	۵.۲.۳		✓		تهدیدات و حملات دوره ای / غیرعمدی
Login واکنش گرا	۵.۲.۴	✓	✓		تهدیدات دوره ای / غیرعمدی
بازیابی از فاجعه	۵.۲.۵	✓	✓	✓	تهدیدات دوره ای / غیرعمدی
رمزگذاری ارتباط بین IDE و کنترلر	۵.۲.۶	✓	✓	✓	حملات

جدول ۳- کد برنامه با استاندارد IEC ۶۱۱۳۱-۳

معیار	ارائه شده در بخش	ارتباط معیار با ... تأمین کنندگان تجهیزات اتوماسیون	یکپارچه سازان سیستمی / سازندگان دستگاه	اپراتور	معیار مناسب علیه ...
محدودیت های دسترسی خارج از برنامه / کتابخانه	۵.۳.۱	✓	✓		تهدیدات و حملات دوره ای / غیرعمدی
باز کردن قابلیت های اضافی	۵.۳.۲	✓	✓		تهدیدات و حملات دوره ای / غیرعمدی

جدول ۴- CODESYS Visualization

معیار	ارائه شده در بخش	ارتباط معیار با ... تأمین کنندگان تجهیزات اتوماسیون	یکپارچه سازان سیستمی / سازندگان دستگاه	اپراتور	معیار مناسب علیه ...
مدیریت کاربر تصویرگرایی	۵.۴.۱		✓	✓	تهدیدات و حملات دوره ای/غیرعمدی
رمزگذاری ارتباط برای CODESYS WebVisu	۵.۴.۲	✓	✓	✓	حملات

۵-۱ معیارهای امنیتی قابل دسترسی و موجود CODESYS Development System

۵-۱-۱ رمزگذاری کد منبع برنامه

معیاری برای یکپارچه سازان سیستمی

کد منبع برنامه حاوی اطلاعات مفصلی درباره عملکرد دستگاه/نیروگاه و «دارایی لمس ناپذیر»[۱۱] سازنده خود است. بنابراین، حفاظت از کد منبع برنامه در هر زمانی که حاوی اطلاعات محرمانه است، از اهمیت بالایی برخوردار است.

در CODESYS Development System، کل پروژه از طریق رمز عبور یا به طور اختیاری با دانگل USB سخت افزار پایانه (کلید امنیتی CODESYS) قابل رمزگذاری است. راهکار رمز عبور از الگوریتم AES[۱۲] استفاده می کند، دانگل سخت افزاری مبتنی بر یک راهکار اختصاصی از شرکت WIBU Systems است. بدون رمز عبور یا کلید(های) امنیتی محدود، باز کردن یا ویرایش فایل منبع پروژه امکان پذیر نیست.

مزیت حفاظت با رمز عبور، عدم نیاز به سخت افزار اضافی است، در حالی که حفاظت با کلید سخت افزاری، سطح حفاظت بسیار بیشتری دارد، به دلیل اینکه رمز عبور قابل هک شدن یا انتشار است. پروژه می تواند به طور همزمان به چندین کلید این چنینی محدود شود. بدین ترتیب، دسترسی به کد منبع می تواند به چندین کلید امنیتی محدود شده و سپس به طور همزمان به چندین کاربر منتقل شود. به علاوه، خطر از دست دادن دسترسی به کد منبع به دلیل کلید تخریب شده یا از بین رفته، از طریق اتصال به حداقل یک کلید دیگر قابل کاهش است.

در CODESYS V۳.۵ SP۱۰، کد منبع را می توان با استفاده از مجوزهای X.۵۰۹[۱۳] نیز محافظت کرد. در این سناریو، کد منبع به طور متقارن رمزگذاری خواهد شد (الگوریتم AES). کلید متقارن نیز با استفاده از کلید عمومی هر کاربری که کد منبع را به اشتراک می گذارد، به طور نامتقارن رمزگذاری خواهد شد (الگوریتم RSA[۱۴]). به طور اختیاری، کد منبع با استفاده از کلید خصوصی مربوط به مجوز X.۵۰۹ کاربر کنونی به طور دیجیتالی قابل امضا است. این امضا در کنار کد منبع در یک فایل با پسوند «p۷s.» و با قالب «PKCS□۷» برای امضاهای دیجیتالی ذخیره خواهد شد. این معیار از محرمانگی دارایی لمس ناپذیر محافظت می کند.

---

[۱۱] Intellectual Property: دارایی لمس ناپذیری که نتیجه خلاقیت مانند حق ثبت، امتیاز کپی و غیره است.

[۱۲] Advanced Encryption Standtard

[۱۳] استانداردی که قالب مجوزهای کلید عمومی را تعریف می کند.

[۱۴] Rivest-Shamir-Adleman (RSA) یکی از اولین سیستم های رمزگذاری کلید عمومی است.

۵-۱-۲ مدیریت کاربر در سطح پروژه

معیاری برای یکپارچه سازان سیستمی

به علاوه حفاظت از کل کد منبع برنامه، CODESYS قابلیت حفاظت از خواندن/نوشتن اشیای منحصر به فرد در پروژه با مدیریت کاربر را فراهم می کند. چنین قابلیتی برای دستورات منو و انواع اشیای خاص (برای مثال ایجاد وظایف، POUها[۱۵]، روش ها، GVLها[۱۶] و غیره) یا اشیای کنونی در پروژه (مانند تنظیمات پروژه یا POUها یا وظایف اختصاصی) قابل تعریف است.

با استفاده از این مدیریت کاربری، محدودسازی بازه فعالیت به صورت پیچیده محتمل تر خواهد بود. بنابراین امتیازات دسترسی برای الزامات امنیتی خاص قابل تطبیق هستند (برای مثال، فعالیت های حیاتی امنیتی مانند استفاده از گزینه های اسکریپت نویسی، می توانند فقط به کاربران دارای مجوزهای آشکار محدود شوند). این معیار از محرمانگی دارایی لمس ناپذیر و یکپارچگی کد منبع محافظت می کند.

۵-۱-۳ امضا و رمزگذاری فایل های مربوط به CODESYS

معیاری برای تجهیزات اتوماسیون، یکپارچه سازان سیستمی و اپراتورها

هرگونه دسترسی فایل از طرف CODESYS Development System قابل احراز است. بنابراین یک امضای X.۵۰۹ در زمان خواندن هر فایل بررسی می شود و امضای X.۵۰۹ در زمان نوشتن یک فایل ایجاد می شود. زمانی که امضا نامعتبر یا وجود نداشته باشد، یک پیام خطای معنی دار از طرف PlugIn که سعی در دسترسی به فایل داشته گزارش می شود. فایل های مربوط به CODESYS عبارتند از:

- کتابخانه ها/پروژه ها
- توضیحات دستگاه ها
- تمام فایل های DLL و EXE از برنامه استاندارد CODESYS

[۱۵] شئ POU (Program Organization Unit) در CODESYS یک واحد سازمان دهی برنامه است.
[۱۶] Global Variable List (GVL): لیست متغیر عمومی

۵-۲ معیارهای امنیتی موجود و قابل دسترسی CODESYS Runtime System

۵-۲-۱ دسترسی به سیستم Runtime با مدیریت احراز هویت / مجوز

معیاری برای تأمین کنندگان تجهیزات اتوماسیون، یکپارچه سازان سیستمی و اپراتورها

فازهای گوناگونی از برنامه صنعتی وجود دارد: از شروع توسعه کد منبع کنترل تا راه اندازی محصول با دستگاه یا نیروگاه و پشتیبانی آن. عموماً این فازها توسط متخصصین مختلف و با صلاحیت انجام می شوند. با در نظر گرفتن این صلاحیت ها و تهدیدات مربوط به استفاده احتمالی فراتر از وظیفه یا رقابت، محدودسازی استفاده برای گروه های کاربری خاص منطقی به نظر می رسد.

CODESYS از چنین مدیریت احراز هویت و مجوز با مدیریت کاربر و گروه کاربری پشتیبانی می کند. به طور پیش فرض، تمام افراد، عضوی از گروه مدیر هستند و دارای امتیازات نامحدودی به کنترلر هستند. با دستورات آسان در CODESYS Development System، مدیر کنونی کنترلر می تواند به سادگی کاربران آنلاین را اضافه یا حذف کند. به علاوه، مدیر می تواند کاربران را به منظور محدودسازی مجوزها در یک گروه کاربری ادغام کند. یک سیستم مجوزدهی از پیش تعریف شده قابل دسترسی بوده و برای درخواست ها به سادگی قابل تطبیق است. به محض اینکه یک کاربر جدید اضافه شود، تمام کاربران باید با نام های کاربری و رمزهای عبور برای هر اتصال آنلاین به کنترلر احراز هویت شوند.

مطابق با سطح ۱ و ۲ امنیتی، این معیار تهدیدات دسترسی تصادفی یا عمدی به کنترلر اجراشونده کاهش می دهد که با دسترس پذیری و یکپارچگی برنامه کامپایل شده که روی کنترلر اجرا شده ارتباط دارند.

۵-۲-۲ رمزگذاری و امضای کد برنامه اجرایی

معیاری برای تأمین کنندگان تجهیزات اتوماسیون و یکپارچه سازان سیستمی

توسعه برنامه به محض اینکه کد برنامه اجرایی روی کنترلر اجرا شد و عملکرد برنامه صنعتی منتشر شد، به جز در مواقع پشتیبانی خاتمه می یابد. حتی اگر کد برنامه در یک باینری کامپایل شده، غیر قابل خواندن و قابل ویرایش موجود باشد، یک تهدید امنیتی جدی برای سازنده برنامه وجود دارد. کل سیستم کنترل از جمله کد برنامه اجرایی بدون مجوز قابل تولید مجدد و استفاده است.

۵-۲-۲-۱ رمزگذاری با CodeMeter

به منظور اجتناب از این تهدیدات، کد برنامه اجرایی از طریق دانگل سخت افزاری دارای فناوری CodeMeter که متعلق به شرکت WIBU Systems بوده، قابل رمزگذاری است. این دانگل سخت افزاری می تواند یک کلید USB (CODESYS Runtime Key) مانند سیستم های مبتنی بر ویندوز یا لینوکس یا یک فلش کارت

از پیش برنامه ریزی شده و خاص که توسط WIBU Systems ارائه شده، باشد. هر کدام از این کلیدها یک شماره سریال منحصر به فرد دارند. حین رمزگذاری کد برنامه اجرایی، کد باینری به طور انحصاری به کلید متصل می شود.

به عبارت دیگر کد باینری رمزگذاری شده قابل مهندسی معکوس نیست. در نتیجه اتصال کد باینری، برنامه نمی تواند روی این کنترلر یا هر کنترلر دیگری بدون کلید اتصال اجرا شود. بدین ترتیب، از تهدید استفاده مجدد و غیرمجاز از برنامه های سرقت شده اجتناب شده و محرمانگی برنامه محافظت شده است.

۵-۲-۲-۲ رمزگذاری و امضا با مجوزهای X.۵۰۹

از زمان انتشار CODESYS V۳.۵ SP۱۰، استفاده از مجوزهای X.۵۰۹ برای رمزگذاری کد برنامه اجرایی بجای استفاده از فناوری CodeMeter امکان پذیر است. بنابراین کد فقط روی سیستم Runtime اجرا می شود که دارای کلید خصوصی یک مجوز است؛ مجوزی که برنامه به آن پیوست شده است. اتصال برنامه به مجوزهای متفاوت کنترلر نیز امکان پذیر است. در این مورد، کد روی هر کنترلری اجرا می شود که دارای کلید خصوصی از حداقل یکی از آن مجوزها است.

به علاوه رمزگذاری، برنامه با یک مجوز X.۵۰۹ قابل امضا است. در نتیجه برنامه فقط اجرا می شود، در صورتی که مجوز خاص سازنده در Runtime معتبر باشد. این معیار از کنترلر در مقابل اجرای کد از طرف سازندگان غیرمجاز یا نامطمئن جلوگیری می کند.

۵-۲-۳ حالت عملیات کنترلر

معیاری برای یکپارچه سازان سیستمی

یک کنترلر تفاوت بین عملیات، راه اندازی و توسعه کارآمد را تشخیص نمی دهد. همین مسئله باعث بروز خطر امنیتی می شود که با معرفی یک حالت عملیاتی قابل پیشگیری است.

CODESYS قابلیت اختصاص سه حالت عملیاتی متفاوت برای کنترلر ارائه می کند. حالت عملیاتی «Debug» پیش فرض است و اجازه تمام دستورات آنلاین از جمله حذف، دستکاری و بروزرسانی برنامه را می دهد. حالت «Locked» از توسعه دهنده در مقابل دسترسی ناخواسته به کنترلر محافظت می کند (برای مثال، در زمان برنامه نویسی همزمان چندین کنترلر). به محض اینکه راه اندازی برنامه خاتمه یافت، کنترلر می تواند به حالت «Operational» تغییر وضعیت دهد که از تمام دسترسی های ناخواسته به برنامه اجراشونده جلوگیری می کند. بدین ترتیب، این حالت تضمین می کند که کنترلر پس از راه اندازی مجدد برنامه مناسبی بارگذاری کرده و هیچگونه معیارهای عیب‌یابی فعال نشده باشد.

در ترکیب با مدیریت کاربر روی کنترلر (بخش ۵.۲.۱ مشاهده شود)، تغییر وضعیت حالت عملیات می تواند به کاربران خاصی محدود شود. با حالت عملیات کنترلر، از یکپارچگی و دسترس پذیری دستگاه در مقابل دسترسی ناخواسته به اطلاعات خارجی محافظت می شود.

۵-۲-۴ ورود واکنش گرا

معیاری برای تأمین کنندگان تجهیزات اتوماسیون و یکپارچه سازان سیستمی

دسترسی ناخواسته به کنترلر اشتباهی در یک شبکه دارای چندین دستگاه می تواند به ماشین یا فرآیند تولید آسیب وارد کند. CODESYS از ورود واکنش گرا به منظور اجتناب از این مسئله پشتیبانی می کند. ورود از طریق فشردن کلیدی روی کنترلر، از طریق وارد کردن شماره سریال کنترلر اختصاصی یا از طریق چشمک زدن کنترلر قابل تأیید است. این سطح ۱ امنیتی از قبل در CODESYS Development System پیاده سازی شده است. از آنجایی که این معیار به عملکرد سخت افزاری کنترلر وابسته است، پیاده سازی واکنش مناسب در این دستگاه وظیفه سازنده خواهد بود. ورود واکنش گرا از یکپارچگی و قابلیت اطمینان برنامه دانلود شده و کنترلر محافظت می‌کند.

۵-۲-۵ بازیابی از حادثه (پشتیبان گیری / بازگردانی)

معیاری برای تأمین کنندگان تجهیزات اتوماسیون، یکپارچه سازان سیستمی و اپراتورها

حتی اگر از قبل معیارهایی برای حفاظت از کد برنامه اجرا شده روی کنترلر در مقابل دسترسی مضر و ناخواسته وجود داشته باشد، با این وجود چنین دسترسی مضری مخصوصاً به دلیل خرابی خود کنترلر می تواند رخ دهد. به منظور کاهش پیامدهای این تهدید، قابلیت پشتیبان گیری جامع و بازیابی از حادثه وجود دارد. در صورت بروز آسیب غیرمنتظره، بازگردانی نسخه پشتیبان کامل برنامه کنترلر با رویه های ساده امکان پذیر خواهد بود.

۵-۲-۶ رمزگذاری ارتباطی بین IDE و کنترلر

معیاری برای تأمین کنندگان تجهیزات اتوماسیون، یکپارچه سازان سیستمی و اپراتورها

حتی اگر احراز هویتی برای دسترسی به کنترلر وجود داشته باشد، ارتباط بین CODESYS Development System و CODESYS Control Runtime System قابل هک شدن است و می تواند به برنامه آسیب وارد کند. رمزگذاری TLS ۲.۱ ارتباط بین CODESYS IDE و کنترلر قابل دسترسی بوده و در CODESYS IDE قابل فعالسازی است. این کار از یکپارچگی و محرمانگی ارتباط کاملاً آنلاین بین CODESYS IDE و کنترلر محافظت می‌کند که حاوی کد برنامه و تمام اطلاعات تبادل شده است (برای مثال، مقادیر نظارت شده).

۵-۲-۷ OPC UA Server[۱۷]: پشتیبانی از ارتباط مبتنی بر X.۵۰۹

معیاری برای تأمین کنندگان تجهیزات اتوماسیون، یکپارچه سازان سیستمی و اپراتورها

OPC UA یک پروتکل ارتباط صنعتی برای تعامل متقابل بوده که توسط OPC Foundation توسعه داده شده است. CODESYS Runtime System به طور اختیاری با قابلیت OPC UA Server قابل تجهیز است تا بتواند دسترسی به کنترلر و برنامه موجود در کنترلر را فراهم کند. یک خصوصیت OPC UA Server، فعالیت با ارتباط رمزگذاری شده مبتنی بر مجوزهای X.۵۰۹ است. پروفایل های امنیتی گوناگون توسط OPC Foundation تعریف شده اند.

با توجه به پروفایل انتخابی، OPC UA Server از یکپارچگی (برای پروفایل هایی فقط امضا شده اند) یا یکپارچگی و محرمانگی اطلاعاتی محافظت می کند (برای پروفایل های امضا شده و رمزگذاری شده) که با

[۱۷] Open Platform Communications Unified Architecture (OPC UA): معماری یکپارچه ارتباطات باز پلتفرم

سرویس گیرندگان متصل شده تبادل شده اند. این معیار از نسخه CODESYS OPC UA V۳.۵.۱۱.۰ Server قابل دسترسی است.

۵-۳ معیارهای امنیتی که خارج از کد برنامه CODESYS قابل فعالسازی هستند

۵-۳-۱ محدودیت های دسترسی خارج از برنامه / کتابخانه

معیاری برای تأمین کنندگان تجهیزات اتوماسیون و یکپارچه سازان سیستمی

برنامه نویس CODESYS می تواند دسترسی به کنترلر و برنامه را از طریق کد برنامه محدود کند. یک کتابخانه مخصوص، دستوراتی ارائه می کند که می توانند دسترسی حیاتی به کنترلر مانند تغییرات آنلاین برنامه، نقاط اختلال، انتقال فایل یا دسترسی به متغیرها را غیرفعال کنند. معمولاً این معیار برای جلوگیری از تغییرات کد یا تنظیمات حین اجرای کد برنامه حیاتی استفاده می شود. این معیار از یکپارچگی کد برنامه محافظت می کند.

۵-۳-۲ فعال کردن قابلیت های اضافی

معیاری برای تأمین کنندگان تجهیزات اتوماسیون و یکپارچه سازان سیستمی

در صورتی که کد برنامه حاوی قابلیت های اضافی باشد (مثلاً برای وظایف خدمات رسانی یا پشتیبانی)، ممکن است این قابلیت ها برای عملیات استاندارد غیرفعال باشند. با استفاده از دانگل سخت افزاری (برای مثال، کلید امنیتی CODESYS، کلید CODESYS Runtime)، چنین قابلیت هایی برای کارکنان مجاز قابل فعالسازی هستند. ممکن است قابلیت غیرفعال کردن در کد منبع برنامه ریزی شده باشد و از برنامه در مقابل تهدیدات سطح ۱ و ۲ محافظت می کند.

۵-۴ معیارهای امنیتی با CODESYS Visualization

۵-۴-۱ مدیریت کاربر تصویرگرایی[۱۸]

معیاری برای یکپارچه سازان و اپراتورهای سیستمی

تصویرگرایی موجود در CODESYS باعث فعالیت مستقیم برنامه کنترلر و کل دستگاه ها یا نیروگاه می شود. جداسازی عملیات به بخش ها یا صفحات مختلف براساس سطح تأثیر عملکردی یا امنیتی آنها به شدت پیشنهاد می‌شود. CODESYS قابلیت حفاظت از معیارهای منحصر به فرد تصویرگرایی و تمام صفحات تصویرگرایی پروژه را با استفاده از مدیریت کاربر تصویرگرایی ارائه می کند. مدیریت کاربر می تواند بازه عملکرد را برای اپراتورهای خاص محدود کند. حالت های عملیاتی حیاتی امنیتی مانند استخراج اطلاعات تولیدی، فرآیند شروع/توقف دستگاه یا نیروگاه و دسترسی به قابلیت های اختصاصی خدمات، می توانند به اپراتورهای دارای مجوزهای کاملاً اختصاصی محدود شوند. این معیار از محرمانگی دارایی لمس ناپذیر و دسترس پذیری و قابلیت اطمینان فرآیند دستگاه یا نیروگاه محافظت می کند.

۵-۴-۲ رمزگذاری ارتباط برای CODESYS WebVisu

معیاری برای تأمین کنندگان تجهیزات اتوماسیون، یکپارچه سازان سیستمی و اپراتورها

به منظور جلوگیری از هک شدن بین کنترلر سازگار CODESYS که از CODESYS WebVisu پشتیبانی می کند و مرورگر اینترنت روی PC یا دستگاه موبایل، یک اتصال HTTPS دارای رمزگذاری قابل دسترسی است. این معیار از یکپارچگی اطلاعات نمایش داده شده محافظت می کند.

[۱۸] Visualization User Management

۶ معیارهای امنیتی داخلی، آتی و اضافی CODESYS

به علاوه معیارهای امنیتی کنونی، چندین معیار وجود دارد که شاید در CODESYS پیاده سازی شوند یا حتماً پیاده سازی خواهند شد. مشابه معیارهای موجود کنونی، این معیارها در جدول زیر لیست و توضیح داده شده اند.

جدول ۴- معیارهای امنیتی، آتی و اضافی در CODESYS

معیار	ارائه شده در بخش	ارتباط معیار با ...			معیار مناسب علیه ...
		تأمین کنندگان تجهیزات اتوماسیون	یکپارچه سازان سیستمی / سازندگان دستگاه	اپراتور	
احراز هویت آسانتر	۶.۱.۱		✓	✓	تهدیدات دوره ای / غیرعمدی
پیکربندی رابط های برنامه نویسی و عملیاتی	۶.۱.۲		✓		تهدیدات و حملات دوره ای / غیرعمدی
پشتیبانی از تنظیمات خصوصیات امنیتی	۶.۱.۳	✓	✓	✓	تهدیدات و حملات دوره ای / غیرعمدی
حالت فقط خواندنی	۶.۱.۵		✓		تهدیدات و حملات دوره ای / غیرعمدی

۶–۱ معیارهای امنیتی داخلی، آتی و اضافی CODESYS

به علاوه معیارهای امنیتی کنونی، معیارهای بیشتری در نظر گرفته شده اند:

۶–۱–۱ احراز هویت آسانتر

معیاری برای یکپارچه سازان سیستمی و اپراتورها

همان طور که قبلاً اشاره شد، افزایش امنیت با استفاده از معیارهای امنیتی (برای مثال، از طریق وارد کردن کد دسترسی) فقط با از دست رفتن راحتی به دست می آید. بدین ترتیب، احتمال دارد که از این معیارها اجتناب شود. با نگاشت اختیاری احراز هویت روی دانگل سخت افزاری یا روی LDAP[۱۹] (مدیریت کاربر سیستم IT) از دست رفتن راحتی قابل جبران است. بدین ترتیب چنین نگاشتی می تواند تأثیر مثبت روی استفاده از معیارهای امنیتی و روی حفاظت از برنامه داشته باشد. این تأثیر از طریق احراز هویت آسانتر در سطح پایانه[۲۰] و سطح کنترلر قابل دستیابی است.

مثال:

- دانگل پایانه (کلید امنیتی CODESYS) حاوی اطلاعات کاربری برای دسترسی به کنترلر است.
- دانگل Runtime (کلید CODESYS Runtime) که به کنترلر متصل شده حالت عملیاتی «Debug» را فعال می کند.

۶–۱–۲ پیکربندی رابط های برنامه نویسی و عملیاتی

معیاری برای یکپارچه سازان سیستمی

تا بدینجا هیچگونه محدودیتی در خصوص رابط های برنامه نویسی و عملیاتی کنترلر وجود ندارد. به عبارت دیگر CODESYS آدرس IP کاربری که به کنترلر دسترسی دارد را بررسی نمی کند. پروفایل های خاص می توانند دسترسی به کنترلر را محدود کنند (برای مثال، برای عیب یابی برنامه نویسی، عملیاتی یا فقط خواندنی). این پروفایل ها مجموعه ای از آدرس های IP مجاز (لیست سفید سازی از IPها) را برای وظایف ذکر شده تعریف خواهند کرد. به علاوه چنین پروفایلی می تواند گزینه مسیریابی را غیرفعال کند. این معیار از دسترسی ناخواسته به کنترلرها در شبکه باز جلوگیری خواهد کرد.

---

[۱۹] Lightweigh Directory Access Protocol (LDAP): پروتکل کاربردی استاندارد صنعتی و باز برای دسترسی و نگهداری از سرویس های اطلاعاتی توزیع یافته از طریق شبکه پروتکل اینترنت (IP) است.

[۲۰] Workstation

۶-۱-۳ پشتیبانی از تنظیمات خصوصیات امنیتی

معیاری برای تأمین کنندگان تجهیزات اتوماسیون، یکپارچه سازان سیستمی و اپراتورها

تمام خصوصیات امنیتی تشریح شده، پیکربندی و چگونگی انجام صحیح آن را درخواست می کنند. به منظور پشتیبانی از این درخواست ها، گزینه های گوناگون در نظر گرفته شده اند:

- نصب معیارهای امنیتی برای نصب تمامی خصوصیت ها.
- مستندات خصوصیات امنیتی بیشتر از جمله راهنما و چک لیست های کاربری در CODESYS Online Help وجود دارد.
- ماژول آموزشی پوشش دهنده موضوع «امنیت» به مبحث آموزش پایه اضافه خواهد شد. بخشی از آموزش، نمایش آسیب پذیری های عمومی و اتصال کنترلر به اینترنت خواهد بود (مثلاً، پیکربندی دیوار آتش و VPN و قطع اتصال از شبکه های باز).
- آموزش و مجوز برای آگاهی امنیتی پایه در سیستم های اتوماسیون.

۶-۱-۴ حالت فقط خواندنی

معیاری برای یکپارچه سازان سیستمی

در زمان باز کردن یک پروژه، کاربر می تواند گزینه ای را تنظیم کند که پروژه و برنامه روی کنترلر قابل تغییر نباشند. این پروژه از کد منبع برنامه و کنترلر در مقابل تغییرات ناخواسته محافظت می کند.

۷ درگاه های شبکه های استفاده شده توسط CODESYS

همانطور که توضیح داده شد، کنترلرها برای برنامه ریزی تعیین شده اند. بدین ترتیب، کنترلرهای سازگار CODESYS به درگاه های خاص شبکه برای کاربری تعیین شده نیاز دارند. درگاه های پیش فرض ارتباطی در زیر لیست شده اند.

درگاه ها	هدف ارتباط	پیکربندی مجدد امکان پذیر است؟
۱۷۴۰-۱۷۴۳	ارتباط UDP Runtime	امکان پذیر نیست
۱۱۷۴۰	ارتباط TCP Runtime	امکان پذیر است
۱۲۱۷	ارتباط درگاه TCP	امکان پذیر است
۸۰۸۰	CODESYS WebServer	امکان پذیر است
۴۴۳	CODESYS WebServer (SSL)	امکان پذیر است
۴۸۴۰	CODESYS OPC UA Server	امکان پذیر است (از نسخه CODESYS V۳.۵ SP۷)

به علاوه این درگاه ها، یکپارچه سازان سیستمی یا اپراتورها می توانند درگاه های ارتباطی را برای دیگر اهداف باز کنند (برای مثال، سرور FTP، چارچوب های پشتیبانی یا عیب یابی، برنامه های پایانه و غیره). یکپارچه سازان سیستمی و اپراتورها کاملاً مسئول حفاظت از این درگاه ها در مقابل دسترسی غیرمجاز هستند.

۸ مدیریت آسیب پذیری های امنیتی در CODESYS

CODESYS با در نظر گرفتن جنبه های امنیتی توسعه داده شده است. امنیت محصول، اهمیت ویژه ای برای ۳S-Smart Software Solutions دارد. با این وجود آسیب پذیری هایی شناسایی شده اند. آسیب پذیری ها براساس سیاست افشای هماهنگ شده ۳S-Smart Software Solutions مدیریت شده اند. این سیاست، فرآیند کامل اطلاعات دریافتی، مدیریت داخلی و افشای آسیب پذیری ها در محصولات CODESYS را توضیح می دهد.

تمام مسائل امنیتی گزارش شده به ۳S-Smart Software Solutions به طور کامل تحقیق، ارزیابی و اولویت بندی شده اند. هدف اصلی شناسایی تمام محصولات تحت تأثیر احتمالی، تعیین دلیل اصلی آسیب پذیری و توسعه یک راهکار است. ۳S-Smart Software Solutions آسیب پذیری های امنیتی را در کنار مشکل گزارش شده و در محصولات و پروتکل های CODESYS نیز جستجو می کند.

در کل وصله های امنیتی برای آخرین نسخه محصولات تحت تأثیر CODESYS منتشر شده اند. زمانی که یک راهکار (معمولاً بروزرسانی نرم افزار) یا پیشگیری وجود داشته باشد، ۳S-Smart Software Solutions یک اطلاعیه امنیتی منتشر خواهد کرد.

۹ نتیجه گیری

امنیت سیستم های کنترل در برنامه های اتوماسیون صنعتی بسیار حیاتی شده، از آنجایی که شبکه های گوناگون بهم پیوسته بوده و سیستم ها یکپارچه هستند. بنابراین، یکپارچه سازان سیستمی و کاربران برنامه های اتوماسیون صنعتی باید به این مسائل توجه بیشتری کنند. امنیت باید اقدامی ادامه دار در کنار ارزیابی اصولی خطر و مشابه پیشرفت های عملکردی و ایمنی باشد. حتی اگر امنیت نتواند ۱۰۰٪ مؤثر باشد، پیاده سازی معیارهای امنیتی موجود و برنامه ریزی دقیق می توانند امنیت را به سطحی برسانند که برای هر برنامه یا تأسیسات خاص کافی باشد.