به نام خدا

سند هدف امنیتی

iSCADA – Ver 4.5

شرکت صبا انرژی

۱۴۰۰/۰۵/۱۶

نسخه ۳,۲

فهرست

اصطلاحات

اصطلاح	توضیح
مستند	به هر سندی که حاوی اطلاعات برای اجرا و پشتیبانی عملیات و فعالیتهای سازمانی مورد استفاده قرار می‌گیرند، مستند گفته می‌شود.
رکورد	مستندی که اطلاعات فعالیتها، رویدادها و نتایج حاصله را نگهداری میکند؛ به عبارت دیگر یک رکورد مستندی است که مدرک انجام یک فعالیتی مشخص است. یک رکورد می تواند شامل دو یا چند مستند باشد.
رکورد ممیزی	رکوردی که حاوی اطلاعات رویدادهایی است که برای ممیزی برنامه کاربردی تحت شبکه مورد نیاز است و در محل ذخیره‌سازی ممیزی، ذخیره می‌شود.
داده‌های کاربری ذخیره شده	فایل‌های داده و اطلاعاتی هستند که توسط کاربر ایجاد و ذخیره می‌شوند. این داده‌ها می‌تواند شامل مستندات تولید شده با استفاده از برنامه کاربردی Microsoft Office ، نامه‌های ارجاع کار و پاسخ الکترونیکی و اسکن تصاویر باشد.
موجودیت فعال	موجودیتی در محصول که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون مدیر، کاربر نهایی و غیره.
موجودیت غیرفعال	موجودیتی در محصول، که حاوی اطلاعات است و یا اطلاعات را دریافت می‌کند و توسط موجودیت‌های فعال، عملیاتی بر روی آن انجام می‌گیرد. همانند لیست کردن رکوردها توسط مدیر سیستم، حذف فایلها توسط مهاجم. (رکوردها و فایلها موجودیتهای غیرفعال هستند.)
مشخصه‌های موجودیت فعال	مشخصه‌های هر موجودیت فعال می‌تواند از قبیل نام کاربری، کلمه عبور، آدرس IP کاربر باشد.
مشخصه‌های موجودیت غیرفعال	مشخصه‌های هر موجودیت غیرفعال می‌تواند از قبیل نوع، نام و اندازه مستند باشد.
اسکادا SCADA	Supervisory Control And Data Acquisition سیستم کنترل سطح بالا و جمع‌آوری داده‌ها
پلنت	مرکز صنعتی که فعالیت تجهیزات و تأسیسات آن باید توسط اسکادا کنترل و مانیتور شود.
پایانه راه دور (RTU)	دستگاهی که در پلنت نصب می‌شود و اطلاعات را توسط پروتکل‌های مشخص از جمله IEC 60870-5-101/104 یا DNP3.0 به اسکادا ارسال می‌کند.
پروژه‌ی اسکادا	هر پروژه که در نرم‌افزار اسکادا برای کنترل و جمع‌آوری داده‌های یک پلنت ایجاد و پیکربندی می‌شود.
مهندس سیستم	نقشی که می‌تواند پیکربندی پروژه‌ی اسکادا را انجام دهد.
اپراتور	نقشی که می‌تواند اطلاعات زمان اجرا را ببیند و روی پلنت کنترل داشته باشد.

فرمان (Command)	فرمان در سیستم اسکادا به معنی درخواست تغییر مقدار توسط کاربر به سیستم است. این فرمان می‌تواند منجر به باز و بسته کردن یک کلید، یک شیر، یا تغییر وضعیت یک تجهیز صنعتی در فیلد شود.

۱- چکیده

مستند پیش‌رو تحت عنوان سند هدف امنیتی سامانه‌های اسکادا (SCADA) مبتنی بر استاندارد بین‌المللی IEC-62443-3-3 تهیه شده است. این استاندارد، بخشی از مجموعه استانداردهایی است که به موضوع امنیت اتوماسیون صنعتی و سیستم های کنترل (IACS) می‌پردازد و امروزه به عنوان یک استاندارد مبنا در سطح جهانی شناخته می‌شود. این سند، الزامات امنیتی را برای سیستم‌های کنترلِ مربوط به هفت مورد اساسیِ تعریف شده در IEC-62443-1-1 تجویز می‌کند و سطوح امنیتی سیستم (SL) را به سیستم مورد بررسی (SuC) اختصاص می دهد. هدف اصلی سری IEC 62443، ارائه چارچوبی انعطاف‌پذیر است که رسیدگی به آسیب‌پذیری‌های فعلی و آینده IACS و استفاده از تخفیف‌های لازم به روشی سیستماتیک و قابل دفاع را تسهیل می کند. درک این نکته مهم است که هدف سری IEC 62443 ایجاد برنامه های الحاقی برای امنیت شرکت است که الزامات سیستم‌های فناوری اطلاعات تجاری را تطبیق داده و آن‌ها را با نیازهای منحصر به فرد برای دسترسی قوی مورد نیاز IACS ترکیب کند.

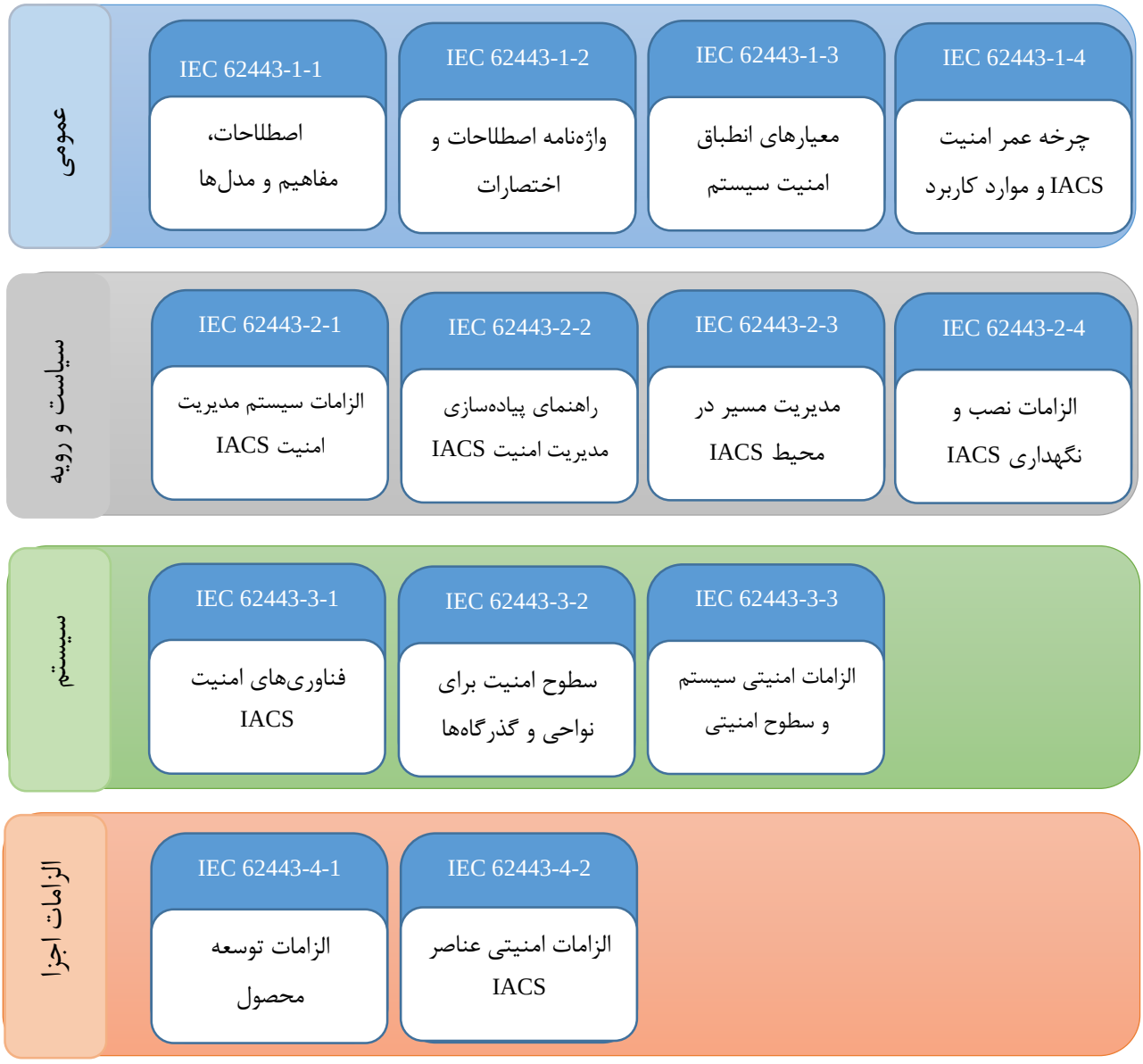
۲- مقدمه

مجموعه استانداردهای IEC 62443-3-3، الزامات سیستم کنترل فنی دقیق (SRs) مرتبط با هفت نیاز بنیادیِ (FRs) شرح داده شده در IEC 62443-1-1، شامل تعریف الزامات برای کنترل سطوح امنیتی سیستم، SL-C، فراهم می‌کند. این الزامات باید توسط اعضای مختلف جامعه اتوماسیون صنعتی و سیستم کنترل (IACS) همراه با مناطق و مجراهای تعریف شده برای سیستم مورد بررسی، (SuC)، در حالی که سیستم کنترل مناسب SL، SL-T (سیستم کنترل) را ایجاد می کند، مورد استفاده قرار گیرد. شکل ۱ تصویری گرافیکی از سری IEC 62443 را نشان می دهد. عناصر استاندارد ۶۲۴۴۳ در چهار گروه قرار می گیرند که مربوط به تمرکز اصلی و مخاطبان مورد نظر می باشد. پاراگراف های زیر هر عنصر و وضعیت فعلی آن را توصیف می کند.

- عمومی: این گروه شامل عناصری است که موضوعاتی را که برای کل مجموعه‌ها رایج است را در بر می‌گیرد.
- استاندارد IEC62443-1-1، مفاهیم و مدل های مورد استفاده در سرتاسر سری را معرفی می‌کند. مخاطب مورد نظر شامل افرادی است که مایل به آشنایی با مفاهیم اساسی هستند که پایه ای برای این سری هستند. اولین نسخه این استاندارد در سال ۲۰۰۷ منتشر شد.
- گزارش فنی IEC62443-1-2، شامل یک واژه نامه اصلی از اصطلاحات و اختصارات استفاده شده در سرتاسر سری است.
- استاندارد IEC62443-1-3، مجموعه ای از معیارهای کمی را که مشتق از الزامات بنیادی، الزامات سیستم و مرتبط با آن است، شرح می‌دهد.

- گزارش فنی IEC62443-1-4، شرح مفصلی از چرخه زندگی پایه‌ای برای امنیت IACS را فراهم می کند، همچنین موارد متعددی از موارد کاربردی که کاربردهای مختلف را نشان می‌دهد.
- سیاست ها و رویه ها: عناصر در این گروه بر سیاست‌ها و رویه‌های مرتبط با امنیت IACS تمرکز دارند.
- استاندارد IEC62443-2-1، توصیف آنچه لازم است برای تعریف و پیاده سازی یک سیستم مدیریت ایمن سایبری IACS موثر است. مخاطبان مورد نظر شامل کاربران نهایی و صاحبان دارایی‌هایی هستند که مسئولیت طراحی و اجرای چنین برنامه‌هایی را دارند. اولین نسخه از این استاندارد در سال ۲۰۰۹ منتشر شد.
- استاندارد IEC62443-2-2، راهنمایی‌های خاصی در مورد آنچه لازم است برای مدیریت یک سیستم مدیریت ایمن سایبری IACS موثر است. مخاطبان مورد نظر شامل کاربران نهایی و صاحبان دارایی‌هایی هستند که مسئولیت اجرای چنین برنامه‌ای را دارند.
- گزارش فنی IEC62443-2-3، شامل راهنمایی در مورد موضوع خاص مدیریت پچ برای IACS است. مخاطب مورد نظر شامل هر کسی است که مسئول طراحی و اجرای نظم مدیریت پچ است. این گزارش توسط هر دو ISA و IEC در سال ۲۰۱۵ تأیید و منتشر شد.
- استاندارد IEC62443-2-4، الزامات مورد نیاز برای تامین کنندگان IACS را مشخص می کند. مخاطبان اصلی شامل تامین کنندگان راه حل های سیستم های کنترل است. این استاندارد توسط IEC TC65 WG10 توسعه یافته است و به طور رسمی توسط ISA به عنوان بخشی از سری ISA-62443 تصویب شد.
- سیستم مورد نیاز: عناصر در گروه سوم نیازهای آدرس در سطح سیستم.
- گزارش فنی IEC62443-3-1، کاربرد فن آوری‌های مختلف امنیتی را به محیط IACS توصیف می‌کند. مخاطب مورد نظر شامل هر کسی است که مایل است اطلاعات بیشتری در مورد کاربرد فناوری های خاص در یک محیط کنترل سیستم کسب کند. نسخه دوم در سال ۲۰۰۷ منتشر شد.
- استاندارد IEC62443-3-2، در مورد ارزیابی ریسک امنیت و طراحی سیستم برای IACS است. این استاندارد در درجه اول به صاحبان دارایی یا کاربران نهایی هدایت می‌شود.
- استاندارد IEC62443-3-3، نیازهای امنیتی سیستم پایه و سطح اطمینان امنیتی را توصیف می‌کند. این استاندارد توسط هر دو ISA و IEC در سال ۲۰۱۳ منتشر شد.
- الزامات اجزاء: گروه چهارم و نهایی شامل عناصری است که اطلاعات مربوط به نیازهای خاص و دقیق مرتبط با توسعه محصولات IACS را ارائه می‌دهد.

- استاندارد IEC62443-4-1، الزامات مشتق شده را که برای توسعه محصولات قابل استفاده است توصیف می کند. مخاطبان اصلی شامل تامین‌کنندگان راه حل های سیستم های کنترل است.
- استاندارد IEC62443-4-2، شامل مجموعه ای از الزامات مشتق شده است که نقشه دقیق مورد نیاز سیستم را برای زیر سیستم ها و اجزای سیستم مورد نظر فراهم می کند. مخاطبان اصلی شامل تامین کنندگان راه حل های سیستم های کنترل است.



شکل ۱. ساختار سری IEC 62443

در این سند حفاظتی، فرض بر آن است که پیش از این یک برنامه‌ی مدیریت امنیت سایبری برروی سیستم کنترل صنعتی (CSMS)[۱] مطابق با استاندارد IEC62443-2-1 ایجاد و عملیاتی شده است. علاوه براین، در استاندارد IEC62443-2-1 به توصیف چگونگی تعریف سطوح امنیتی (SL)[۲] مبتنی بر ارزیابی مخاطرات در یک سیستم کنترل صنعتی پرداخته می‌شود که با استفاده از آن می‌توان محصولات مناسب با قابلیت‌های امنیتی فنی مطلوب ارائه شده در این سند حفاظتی را انتخاب کرد. مطابق با استاندارد IEC62443-3-2، سیستم کنترل صنعتی براساس میزان اهمیت و مخاطرات سایبری باید به نواحی سایبری (Zones) تقسیم‌بندی شود. به عبارت دیگر، یک ناحیه گروهی از تجهیزات فیزیکی و منطقی می‌باشد که دارای الزامات امنیتی یکسانی است. گذرگاه‌ها (Conduits)، به مجموعه‌ی منطقی از کانال‌های ارتباطی اطلاق می‌شود که دو یا چند ناحیه را به یکدیگر متصل می‌کند و این کانال‌ها دارای الزامات امنیتی یکسانی می‌باشند.

۲-۱- مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی iSCADA – Ver 4.0
نسخه	۱,۰
تاریخ	۱۴۰۰/۰۴/۲۰
نویسندگان	شرکت صبا انرژی

نام تولید کننده (شرکت)	صبا انرژی
نام محصول	iSCADA
نوع محصول	نرم‌افزار اتوماسیون صنعتی
نسخه	4.5

[۱] Cyber Security Management System
[۲] Security Level