INSO-ISO-IEC-TR

27019

1st. Edition

2014
Identical with
ISO/IEC TR
27019:2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ایران-ایزو-آی ای سی – تی آر

۲۷۰۱۹

چاپ اول

۱۳۹۳

فناوری اطلاعات – فنون امنیتی – راهنماهای مدیریت امنیت اطلاعات برای سامانه‌های کنترل فرآیند خاص صنایع انرژی همگانی مبتنی بر استاندارد ISO/IEC 27002

Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization

2 - International Electrotechnical Commission

3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات – فنون امنیتی –راهنماهای مدیریت امنیت اطلاعات برای سامانه‌های کنترل فرآیند خاص صنایع انرژی همگانی مبتنی بر استاندارد ISO/IEC 27002 »

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء : (اسامی به ترتیب حروف الفبا)	
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس شرکت مخابرات ایران
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
ناظمی، اسلام (دکترای کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
یوسف زاده، سمیرا (فوق‌لیسانس مهندسی کامپیوتر-نرم افزار)	پژوهشگر دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات – فنون امنیتی –راهنماهای مدیریت امنیت اطلاعات برای سامانه‌های کنترل فرآیند خاص صنایع انرژی همگانی مبتنی بر استاندارد ISO/IEC 27002 » که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و چهل و چهارمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۳/۰۳/۰۳ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC TR 27019:2013, Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

فناوری اطلاعات – فنون امنیتی – راهنماهای مدیریت امنیت اطلاعات برای سامانه‌های کنترل فرآیند خاص صنایع انرژی همگانی[1] مبتنی بر استاندارد ISO/IEC 27002[2]

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنما با پوشش سامانه‌های کنترل فرآیند مورد استفاده صنایع انرژی همگانی برای کنترل و پایش بر تولید، انتقال، ذخیره‌سازی و توزیع برق، گاز و حرارت در ترکیب با کنترل فرایندهای حمایتی می‌باشد. این امر شامل سامانه‌ها، کاربردها و مولفه‌های زیر است:

- کنترل فرآیند مرکزی و توزیع‌شده با حمایت همه‌جانبه‌ی فناوری اطلاعات(IT)[3]، فناوری پایش و خودکارسازی مانند سامانه‌های IT به‌کار برده شده در عملیات خود، مانند افزاره‌های برنامه‌نویسی و پارامترسازی[4]؛

- کنترل‌کننده‌های رقمی و مولفه‌های خودکارسازی مانند افزاره‌های کنترل و میدان یا کنترل‌کننده‌های منطقی قابل برنامه‌ریزی(PLCs)[5] شامل حسگرهای رقمی و عناصر محرک؛

- کلیه سامانه‌های حمایتی فناوری اطلاعات به‌کار برده شده در دامنه‌های کنترل فرایند، برای مثال، برای اطلاعات تکمیلی کارهای دیداری‌سازی و اهداف کنترل، پایش، بایگانی داده‌ها و مستندسازی؛

- فناوری ارتباطات فراگیر به‌کار گرفته شده در دامنه‌های کنترل فرایند، برای مثال، شبکه‌ها، برنامه‌های کاربردی از راه دور و فناوری کنترل از راه دور؛

- اندازه‌گیری رقمی و دستگاه‌های اندازه‌گیری، به‌عنوان مثال برای اندازه‌گیری مصرف، تولید و یا انتشار انرژی؛

- حفاظت رقمی و سامانه‌های ایمنی، برای مثال رله‌های حفاظتی یا PLC های ایمنی؛

- مولفه‌های توزیع‌شده محیط‌های شبکه‌های هوشمند آینده؛

- کلیه نرم‌افزارها، ثابت‌افزار[6] و برنامه‌های کاربردی نصب شده در سامانه های ذکر شده در بالا؛

تجهیزات کنترل معمولی یا کلاسیک که غیر رقمی، یعنی فقط سامانه‌های الکترومکانیک یا پایش الکترونیکی

---

1 - energy utility industry

۲ - استاندارد بین‌المللی ISO/IEC 27002:2005 در سال ۱۳۸۷ با شماره ملی ۲۷۰۰۲ منتشر شده است.

3 - Information Technology

4 - Parameterization

5 - Programmable Logic Controller

6 - Firmware

و کنترل فرآیند می‌باشند، در خارج از دامنه این راهنما هستند. علاوه بر این سامانه‌های کنترل فرآیند انرژی در فضاهای خصوصی و دیگر تاسیسات ساختمان‌های مسکونی مشابه، در خارج از دامنه کاربرد این راهنما هستند.

سامانه‌های مخابراتی و مولفه‌های مورد استفاده در محیط کنترل فرآیند به طور مستقیم در دامنه کاربرد این راهنما نمی‌باشند. این سامانه‌ها توسط «*استاندارد ملی ایران شماره ۲۷۰۱۱: سال ۱۳۸۹، فناوری اطلاعات – فنون امنیتی – راهنماهای مدیریت امنیت اطلاعات برای سازمان‌های ارتباط از راه دور بر پایه استاندارد ISO/IEC 27002*» تحت پوشش می‌باشند. توصیه می‌شود که کاربران این راهنما اقدامات تعریف شده در این استاندارد را جهت سامانه‌ها و مولفه‌های مخابراتی به‌کار گرفته شده در محیط‌های کنترل فرایند، پیاده‌سازی نمایند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات – الزامات

۲-۲ استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات

۳ اصطلاحات وتعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ و استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

خاموشی[1]

قطعی گسترده برق است.

1- Blackout

۲ـ۳

گروه واکنش اضطراری رایانه

(CERT) [1]

گروهی از کارشناسان امنیتی جهت پشتیبانی از ساماندهی مدیریت حوادث امنیت اطلاعات است.

۳ـ۳

زیرساخت‌های حیاتی [2]

سازمان‌ها و تسهیلاتی که جهت کارکرد کلی جامعه و اقتصاد ضروری می‌باشند.

یادآوری- خرابی چنین سازمان‌ها و تسهیلاتی در کمبود عرضه پایدار بارزتر بوده و تاثیر قابل توجهی بر امنیت عمومی و تاثیراتی وسیع دیگر خواهد داشت.

٤ـ۳

اِشکال زدایی [3]

تحلیل سوء عمل در سامانه‌های رایانه‌ای است.

٥ـ۳

توزیع [4]

انتقال انرژی برق ولتاژ بالا، متوسط و پایین از طریق یک شبکه و انتقال گاز یا حرارت از طریق شبکه‌های توزیع محلی یا منطقه‌ای است.

٦ـ۳

نصب تجهیزات انرژی [5]

تجهیزات و یا وسایل جهت تولید، تبدیل، ذخیره‌سازی، انتقال یا تامین انرژی است.

۷ـ۳

تامین انرژی

فرآیند ایجاد، تولید یا ذخیره‌سازی انرژی جهت تحویل به مشتریان و بهره‌برداری از شبکه تامین انرژی است.

۸ـ۳

صنایع انرژی همگانی

شخص حقوقی یا حقیقی که انرژی را در اشکال برق، گاز یا حرارت جهت توزیع در شبکه یا ذخیره‌سازی انرژی تامین می‌کند.

---

1 - Computer Emergency Response Team
2 - Critical infrastructure
3 - Debugging
4 - Distribution
5 - Energy equipment installation

۹-۳

واسط انسان-ماشین

(HMI) [1]

واسط کاربر جهت به‌کارگیری و کنترل سامانه‌های کنترل فرآیند و یا تجهیزات است.

۱۰-۳

نگهداری [2]

کلیه اقدامات مورد استفاده در زمینه عرضه انرژی که به‌طور معمول با بازرسی، نگهداری و رفع اشکال [3] و بهبود در ارتباط هستند.

۱۱-۳

PLC [4]

کنترل‌کننده منطقی قابل برنامه‌ریزی است.

۱۲-۳

سامانه کنترل فرآیند

سامانه‌ای که در کنترل و پایش تولید، انتقال، ذخیره‌سازی و توزیع برق، گاز و حرارت در رابطه با کنترل فرایندهای پشتیبانی، به‌کار می‌آیند.

۱۳-۳

ایمنی

ایمنی کارکردی است.

۱۴-۳

سامانه‌های ایمنی [5]

سامانه‌ها و مولفه‌های مورد نیاز برای اطمینان از ایمنی کارکردی است.

۱۵-۳

شبکه هوشمند [6]

سامانه شبکه‌ای الکتریکی است که مشخصه آن استفاده از شبکه‌های ارتباطی و کنترل مولفه‌ها و بارهای شبکه است.

---

1 - Human-machine interface
2 - Maintenance
3 - Fault clearance
4 - Programmable logic controller
5 - Safety systems
6 - Smart grid

۱۶-۳

بیانیه کاربست‌پذیری[1]

SOA

بیانیه‌ی مستند است که کنترل اهداف و کنترل‌های مرتبط و کاربردپذیر برای سامانه مدیریت امنیت اطلاعات (ISMS)[2] سازمان را توصیف می‌کند.

۱۷-۳

سامانه انتقال[3]

شبکه‌ی انتقال جهت انتقال انرژی با استفاده از شبکه ولتاژ بالا و یا ولتاژ بسیار بالا یا شبکه انتقال گاز طبیعی با استفاده از شبکه خط لوله فشار قوی است.

٤ مرور کلی

٤-١ ساختار این راهنما

این راهنما در قالبی سازگار با استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ساختار یافته است. به گونه‌ای که هیچ نیازی به اطلاعات اضافی نیست. ارجاع مستقیم به مشخصه‌های کاربردپذیر در اهداف و اقدامات مندرج در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ در این جا صورت گرفته است. در مواردی که اقدامات مندرج در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ نیاز به روش پیاده‌سازی دارد که خاص بخش تامین انرژی یا برخی موارد پیاده‌سازی توسعه یافته بوده می‌باشد، این راهنما در قالب راهنماهای پیاده‌سازی برای بخش تامین انرژی یا به‌عنوان اطلاعات بیشتر فراهم شده است. یک فهرست از اهداف کنترل‌های جدید و/یا اقدامات جهت بخش تامین انرژی در پیوست الف درج شده است. نظرات تکمیلی و یادداشت‌ها در پیوست ب درج شده است.

توصیه‌های بیشتر در مورد پیاده‌سازی و اطلاعات خاص درباره صنایع انرژی در بندهای زیر ذکر شده است:

- سازمان امنیت اطلاعات(طبق بند ۶)؛
- مدیریت دارایی (طبق بند ۷)؛
- امنیت منابع انسانی (طبق بند ۸)؛
- امنیت فیزیکی و محیطی (طبق بند ۹)؛
- مدیریت ارتباطات و عملیات (طبق بند ۱۰)؛
- کنترل دسترسی (طبق بند ۱۱)؛

1 - Statement of applicability
2 - Information Security Management System
3 - Transmission system

- اکتساب، بهبود و نگهداری سامانه‌های اطلاعاتی (طبق بند ۱۲)؛

- مدیریت استمرار کسب‌وکار(طبق بند ۱۴)؛

- انطباق[1](طبق بند ۱۵).

۴-۲ سامانه‌های مدیریت امنیت اطلاعات برای صنایع تامین انرژی

۴-۲-۱ اهداف

از منظر طراحی و عملکرد، سامانه‌های کنترل فرآیند به‌کار برده شده توسط بخش صنایع انرژی همگانی در واقع سامانه‌های پردازش اطلاعات هستند. این سامانه‌ها با استفاده از حسگرها داده‌های فرآیند را جمع کرده و وضعیت فرآیند فیزیکی را پایش می‌کنند. این سامانه‌ها، بعد از پردازش داده‌ها، خروجی‌های کنترل را تولید می‌کنند که اقدامات ناشی از محرک‌ها را تنظیم می‌نمایند. کنترل و تنظیم به طور خودکار انجام می‌شود، اما اقدامات دستی کارکنان بهره‌برداری کننده نیز ممکن می‌باشد. سامانه‌های پردازش اطلاعات، بخش اساسی از فرایندهای عملیاتی در صنایع انرژی هستند. به این معنا که توصیه می‌شود اقدامات حفاظتی مناسب به همان شیوه که برای سایر بخش‌های سازمان وجود دارد، به‌کارگرفته شوند.

مولفه‌های نرم‌افزار و سخت‌افزار مبتنی بر فناوری اطلاعات (IT) استاندارد به طور فزاینده‌ای در محیط‌های کنترل فرآیند مورد استفاده قرار می‌گیرند.

امروزه، اطلاعات و سامانه‌های پردازش اطلاعات در محیط‌های کنترل فرآیند به طور فزاینده‌ای در معرض تهدیدها و آسیب‌ها هستند. بنابراین ضروری به نظر می‌رسد که، در دامنه کنترل فرآیند صنایع انرژی همگانی، امنیت اطلاعات از طریق پیاده‌سازی و بهبود مستمر سامانه مدیریت امنیت اطلاعات (ISMS) مطابق با ISO/IEC 27001[2] به‌دست می‌آید.

امنیت اطلاعات موثر در دامنه فرآیند کنترل بخش صنایع انرژی همگانی از طریق ایجاد، اجرا، کنترل و بازنگری و در صورت لزوم بهبود اقدامات قابل اجرای مندرج در این راهنما به‌منظور دستیابی به امنیت خاص و اهداف کسب‌وکار سازمانی به دست می‌آید. در اینجا توصیه می‌شود توجهی خاص نسبت به نقش ویژه صنایع انرژی در جامعه و ضرورت اقتصادی منبع امن و قابل اعتماد انرژی داده شود.

۴-۲-۲ ملاحظات امنیتی برای سامانه‌های کنترل فرآیند به‌کار رفته توسط صنایع انرژی

الزامات و موارد مورد نیاز جهت یک چارچوب کلی امنیت اطلاعات برای دامنه کنترل فرآیند صنایع انرژی همگانی بر چندین الزامات اساسی استوار است:

الف- مشتریان انتظار یک منبع امن و قابل اعتماد انرژی را دارند؛

1- Compliance

۲ - استاندارد بین‌المللی ISO/IEC 27001:2005 در سال ۱۳۸۷ با شماره ملی ۲۷۰۰۱ منتشر شده است.

ب- الزامات قانونی و مقرراتی خواستار عملکرد ایمن و اطمینان‌پذیر سامانه‌های تامین انرژی هستند؛ و

پ- تامین‌کنندگان انرژی خود نیاز به امنیت اطلاعات به‌منظور حفاظت از منافع کسب‌وکار و تحقق نیازهای مشتریان مطابق با مقررات قانونی دارند.

٤-٢-٣ دارایی‌های اطلاعاتی که باید محافظت شوند

به منظور ایجاد یک سامانه مدیریت امنیت اطلاعات، شناسایی کلیه دارایی‌های سازمانی توسط سازمان ضروری است. شناسایی دارایی‌های سازمانی و روشن شدن اهمیت آن‌ها امکان به‌کارگیری کنترل‌های مناسب را به وجود می‌آورد.

توضیح بیشتر در مورد نوع دارایی‌های سازمانی که توصیه می‌شود توسط سازمان تامین انرژی مورد محافظت قرار گیرد، در زیربند ۷-۱-۱، موجودی دارایی‌ها درج شده است.

٤-٢-٤ تعیین مدیریت امنیت اطلاعات

٤-٢-٤-١ چگونگی تعیین الزامات امنیتی

ضروری است که سازمان‌های صنایع انرژی همگانی، الزامات امنیتی خود را شناسایی کنند. سه منبع اصلی از الزامات امنیتی وجود دارد:

الف- نتایج حاصل از ارزیابی مخاطره یک سازمان، که راهبردهای کسب‌وکار و اهداف سازمان در نظر گرفته شده است. از طریق ارزیابی مخاطره، تهدیدات وارده به دارایی‌های سازمان مورد شناسایی قرار می‌گیرند، آسیب‌پذیری آن مشخص شده و تاثیرات بالقوه آن تخمین زده خواهد شد.

ب- الزاماتی که از قوانین وآیین‌نامه ها ، مقررات و قراردادها که باید توسط سازمان و الزامات اجتماعی فرهنگی برآورده شوند، ناشی می‌شوند. نمونه‌های خاص شامل حفاظت از تامین انرژی اطمینان‌پذیر، موثر و امن، مانند تحقق اطمینان‌پذیر الزامات در بازار آشفته‌ی انرژی است، که به صورت خاص، انتقال اطمینان‌پذیر و امن داده‌ها توسط اشخاص سوم است.

پ- اصول، اهداف و الزامات کسب وکار قرار گرفته بر پردازش اطلاعات که توسط سازمان برای حمایت از عملیات کسب‌وکار خود توسعه داده است.

٤-٢-٤-٢ ارزیابی مخاطرات امنیتی

کنترل‌ها و اقدامات امنیتی لازم با استفاده از روش‌های ارزیابی مخاطرات امنیتی تعیین شده‌اند. باید بین هزینه‌ی کنترل‌ها و زیان‌های اقتصادی که ممکن است به دلیل مسائل امنیتی وارد شده باشند تعادل ایجاد شود. نتایج حاصل از ارزیابی مخاطره، تعریف اقدامات مدیریتی مناسب و اولویت‌بندی برای مدیریت مخاطرات امنیتی اطلاعات و همین طور پیاده‌سازی کنترل‌های انتخاب شده جهت محافظت در برابر این مخاطرات را تسهیل می‌کند. توصیه می‌شود ارزیابی مخاطره به‌صورت دوره‌ای به‌منظور اعمال تغییرات در حساب‌ها، تکرار

گردد، که این امر در نتایج ارزیابی نیز موثر خواهد بود.

٤-٢-٤-٣ انتخاب کنترل‌ها

هنگامی که الزامات امنیتی و مخاطرات شناخته شدند و تصمیم‌گیری‌ها در مورد چگونگی مقابله با آن‌ها گرفته شد، توصیه می‌شود برای اطمینان از این‌که مخاطرات به سطح قابل قبول‌تری کاهش یافته‌اند، کنترل‌های مناسب انتخاب و پیاده‌سازی شوند.

علاوه بر کنترل‌های ارائه شده توسط سامانه جامع مدیریت اطلاعات، این راهنما کمک‌های اضافی و اقدامات بخش خاص برای سامانه‌های کنترل فرآیند که توسط بخش همگانی انرژی به‌کار برده شده را با در نظر گرفتن الزامات ویژه ارائه می‌دهد. بنابراین توصیه می‌شود که بخش صنایع انرژی طبق معیارهای مندرج در این راهنما پیاده‌سازی شوند. در صورت نیاز، اقدامات اضافی در برای تکمیل الزامات خاص می‌تواند توسعه داده شود. انتخاب اقدامات امنیتی بستگی به تصمیمات اتخاذ شده توسط سازمان مبتنی بر معیارهای پذیرش مخاطره، گزینه‌های مربوط به مخاطره و روش مدیریت آن دارد. توصیه می‌شود انتخاب اقدامات با ملاحظه‌ی قانون ملی و بین‌المللی مرتبط، احکام حقوقی و مقررات صورت گیرد.

٤-٢-٥ عوامل حیاتی موفقیت[1]

مضامین طبق استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ بند ۰-۷ اعمال می‌شود.

٥ خط‌مشی امنیتی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

٦ سازمان امنیت اطلاعات

٦-١ سازمان داخلی

٦-١-١ تعهد مدیریت به امنیت اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

٦-١-٢ هماهنگی امنیت اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

٦-١-٣ تخصیص مسوولیت‌های امنیت اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

٦-١-٤ فرآیند مجوزدهی برای امکانات پردازش اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

1- Critical success factors

۶-۱-۵ توافق‌نامه‌های محرمانگی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۶-۱-۶ برقراری ارتباط با مراجع دارای اختیار

کنترل زیربند ۶-۱-۶ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

کاربردها و زیرساخت‌های سامانه‌های کنترل فرآیند صنایع انرژی همگانی ممکن است به‌عنوان بخشی از زیرساخت‌های حیاتی و ممکن است برای عملکرد جامعه و اقتصاد به‌عنوان یک کل در نظر گرفته شود. بنابراین توصیه می‌شود بهره‌برداری کنندگان چنین سامانه‌هایی، ارتباط با همه مراجع دارای اختیار را حفظ نمایند. علاوه بر این بخش عمومی مرتبط با این موضوع شامل موارد زیر است:

- بنگاه‌های ملی و بین‌المللی و همکاری‌های پیش‌قدم برای حفاظت از زیرساخت‌های حیاتی؛
- سازمان‌های CERT ملی و بین المللی؛ و
- سازمان‌های حفاظت شهری و تیم‌های امدادرسانی؛

برای بهره‌برداری کنندگان از زیرساخت‌های حیاتی ممکن است قوانین ومقررات محلی اعمال شود که باید به نسبت سازگار باشند.

سایر اطلاعات برای دامنه صنایع انرژی همگانی

در طول دوره بهره‌برداری سامانه، برنامه‌ریزی عملیاتی و در طول کارهای مقدماتی جهت شرایط آب و هوایی استثنایی، اطلاعات آب و هوا، پیش بینی و مشاوره‌های آب وهوایی ممکن است مورد نیاز باشد. توصیه می‌شود ارتباط مستقیم با توجه به خدمات هواشناسی محلی، منطقه‌ای و ملی و خدمات اطلاع رسانی برقرار شود (مانند اخطار رعدوبرق، تشخیص آذرخش).

۶-۱-۷ برقراری ارتباط با گروه‌های با منافع خاص

کنترل زیربند ۶-۱-۷ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

به منظور تبادل اطلاعات در مسائل امنیتی خاص کنترل فرآیند و تسهیل همکاری بین سازمانی، توصیه می‌شود ارتباط با فروشنده ملی و بین‌المللی و انجمن‌های عملیاتی و گروه‌های کاری متناظر با آن‌ها که با مسائل امنیتی سروکار دارند، حفظ شود.

۶-۱-۸ بازنگری مستقل امنیت اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۶-۲ اشخاص بیرونی

۶-۲-۱ شناسایی مخاطرات مرتبط با اشخاص بیرونی

کنترل زیربند ۶-۲-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

سامانه‌های کنترل فرآیند ممکن است شامل سامانه‌های پیچیده و جدا از هم باشد. فروشندگان سامانه، ائتلاف‌ها و دیگر اشخاص بیرونی اغلب درگیر فرایندهای حفظ و نگهداری و عملیاتی این سامانه‌ها در سطوح بالاتر هستند. به منظور حفظ و نگهداری و فرایندهای اصلاح خطا و اشتباه ممکن است نیاز به استفاده از ارتباطات از راه دور باشد که اجازه می‌دهد نگهداری از مکان‌های دور صورت گیرد. کارمندان طرف‌های بیرونی برای انجام نگهداری در محل ممکن است نیاز به دسترسی به مناطق تحت کنترل امنیتی داشته باشند.

همکاری نزدیک بین متصدیان سامانه‌های مختلف در مورد سطوح تولید، انتقال و توزیع ممکن است نیاز به ارتباطات نزدیک سامانه‌های کنترل و شبکه‌های ارتباطی سازمان‌های مختلف داشته باشد. علاوه بر این، بخش‌های خارجی مانند فروشندگان، فروشندگان سامانه و شرکای تجاری ممکن است نیاز به دسترسی به اطلاعات حساس و مهم داشته باشند.

توصیه می‌شود مخاطرات ناشی از چنین دسترسی طرف سوم به سامانه‌های حساس، شبکه‌ها و اطلاعات مورد ارزیابی قرار گیرد و ملاحظه شود، به‌خصوص در شرایطی که در معرض مخاطره‌ی فرآیند فیزیکی است که باید کنترل و پایش شوند.

۶-۲-۲ نشانی‌دهی امنیت هنگام سرو کار داشتن با مشتریان

کنترل زیربند ۶-۲-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

روابط پیچیده و متنوع بین صاحبان دارایی، بهره‌برداری کنندگان سامانه، ارائه دهندگان خدمت و مشتریان داخلی و خارجی در بخش صنایع انرژی همگانی ممکن است به مسوولیت‌های مشخص در رابطه با نگهداری، بهره‌برداری و مالکیت دارایی‌ها شود.

نمونه‌هایی از این دست شامل موارد زیر هستند:

- ارائه دهنده خدمات داخلی که مسؤول بهره‌برداری و نگهداری زیرساخت‌ها یا شبکه توزیع که به یک واحد

سازمانی جداگانه داخلی اختصاص یافته است؛

- ارائه دهنده خدمات مسؤول بهره‌برداری و نگهداری تجهیزات برقی یا مولدهای توزیع‌شده می‌باشد؛ و

- ارائه دهنده خدمات داخلی و خارجی که مسؤول بهره‌برداری از زیرساخت‌های کنترل فرآیند می‌باشد.

توصیه می‌شود چنین روابط متنوع و پیچیده کسب‌وکار زمان شناسایی و توجه به الزامات امنیتی برای دسترسی مشتریان به اطلاعات حساس در نظر گرفته شود. هنگامی که سامانه‌های کنترل فرآیند به هم پیوسته هستند، توصیه می‌شود اقدامات شرح داده شده در زیربند ۱۱-۴-۸ ارتباط منطقی سامانه‌های کنترل فرآیند در نظر گرفته شوند.

۶-۲-۳ نشانی‌دهی امنیت در توافق‌نامه‌های طرف سوم

کنترل زیربند ۶-۲-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

توصیه می‌شود تحت شرایط توافق‌نامه‌های قراردادی[1] اطمینان حاصل شود که به الزامات حمایتی در مورد اطلاعات حساس توجه کافی می‌شود.

توصیه می‌شود صاحبان دارایی تمامی قراردادهایی که شامل دسترسی شخص سوم به سامانه‌های کنترل فرآیند می‌شوند را مورد مطالعه قرار دهند. همچنین توصیه می‌شود صاحبان دارایی‌ها نیاز به دسترسی شخص سوم به سامانه‌های کنترل فرآیند را مورد بازنگری قرار دهند.

جایی که خدمات مخابراتی برای سامانه‌های کنترل فرآیند به‌کار رفته در صنایع انرژی توسط شخص سوم فراهم می‌گردند، توصیه می‌شود الزامات خاص مرتبط با بحران و ارتباطات اضطراری، به ویژه در مورد خاموشی‌های بزرگ، بلایای طبیعی، حوادث یا سایر مواقع اضطراری، تعریف شده و به صورت قراردادی مشخص و پایش شوند. این امر به ویژه در مورد هر اقدام پیشگیرانه که ممکن است برای اجتناب از بار اضافی خدمت و جهت حصول اطمینان از درجه قابل قبول بودن استقلال خدمات مخابراتی از تامین انرژی خارجی، اعمال می‌شود (مقاومت در برابر خاموشی).

۷ مدیریت دارایی

۷-۱ مسوولیت دارایی‌ها

۷-۱-۱ فهرست موجودی دارایی‌ها

کنترل زیربند ۷-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

1- Contractual agreements

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

در زمان تهیه و تعیین فهرست موجودی دارایی‌های مهم سازمان، توصیه می‌شود مسوولیت‌های متمایز به وضوح مشخص و مستند شوند.

توصیه می‌شود فهرست موجودی دارایی‌ها ، همه‌ی سامانه‌های کنترل فرآیند مرتبط را که شامل دارایی‌های اطلاعاتی و برنامه‌های کاربردی است، تحت پوشش قرار دهند.

اطلاعات بیشتر برای صنایع انرژی

اضافه بر طبقه‌بندی بالا، دارایی‌ها در دامنه تامین انرژی شامل طیف گسترده‌ای از سایر طبقه‌های دارایی بخش خاص است، هم‌چون:

الف- **اطلاعات**: طرح‌های شبکه‌ای[1]، زمان‌بندی و توزیع داده‌ها، اطلاعات جغرافیایی و مراجع جغرافیا، طرح‌های بحران و اضطرار، طرح‌های بازیابی فاجعه شبکه[2]، داده‌های عملیات سودهی[3]، مقادیر سنجش شده و داده‌های سنجش، داده‌های اندازه‌گیری[4] و اندازه‌گیری شده[5]، سوابق عملیاتی، داده‌های پارامترسازی، بایگانی-های اندازه‌گیری و پیام و غیره؛

ب- **نرم‌افزار**: نرم‌افزار کنترل فرایند، سامانه‌های دیداری‌سازی[6]، نرم‌افزار مدیریت و بهینه سازی انرژی و، نرم‌افزار شبیه‌سازی، نرم‌افزار پارامترسازی، سامانه‌های مدیریت و پایش، سامانه‌های برنامه‌ریزی منابع عملیاتی، محیط‌های برنامه نویسی، ثابت‌افزار، نرم‌افزار بایگانی و غیره؛

پ- **دارایی‌های فیزیکی**: مولفه‌های کنترل خودکارسازی، مولفه‌های مسافت‌سنج و کنترل از راه دور، مولفه‌های سامانه انتقال داده، مولفه‌های حفاظت و ایمنی رقمی، دستگاه‌های اندازه‌گیری و سنجش رقمی، اندازه‌گیرهای هوشمند، حس‌گر رقمی و عناصر محرک، افزاره‌های پارامترسازی و برنامه‌نویسی، مولفه‌های دیداری‌سازی و عملیاتی، سامانه‌های پایش و ضبط رقمی و غیره؛

ت- **خدمات**: خدمات مخابراتی، خدمات ارتباطاتی اضطراری، خدمات اطلاع رسانی، خدمات هواشناسی و غیره.

۷-۱-۲ مالکیت دارایی‌ها

کنترل زیربند ۷-۱-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

---

1 - Grid and network plans
2 - Grid disaster recovery plans
3 - Switching
4 - Meter
5 - Metered
6 - Visualization

اطلاعات بیشتر برای صنایع انرژی

ساختار پیچیده بالقوه برای سازمان‌هایی که سامانه‌های کنترل فرآیند را به‌کار می‌گیرند ممکن است به این منظور باشد که وجود مسوولیت‌های متنوع با توجه به مالکیت تجاری و عملیاتی است. در نتیجه توصیه می‌شود، مالکان و مسؤولان مرتبط با دارایی‌ها و نقش صاحبان دارایی و متصدی دارایی در رابطه با امنیت اطلاعات بادقت تعریف و مستند شود.

۷-۱-۳ استفاده قابل قبول از دارایی‌ها

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۷-۲ طبقه‌بندی اطلاعات

۷-۲-۱ رهنمودهای طبقه‌بندی

کنترل زیربند ۷-۲-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

معیارهای طبقه‌بندی خاص صنایع انرژی همگانی برای شامل نمودن نقاط زیر می‌تواند توسعه یابد:

- دارایی‌ها، سامانه‌ها و اطلاعات از عملکرد زیرساخت‌های حیاتی و سامانه‌های حساس حمایت می‌کنند؛
- دارایی‌ها،سامانه‌ها و اطلاعات مورد نیاز برای بازسازی سامانه تامین انرژی به دنبال وقوع یک اختلال عمده در تامین ، برای مثال، سامانه‌ها و مولفه‌های با قابلیت «blackstart» (فرآیند بازیابی ایستگاه قدرت برای ادامه عملیات، بدون اتکا به شبکه انتقال برق خارجی)؛
- دارایی‌ها، سامانه‌ها و اطلاعات لازم برای اطمینان از ایمنی کاربردی/ وسایل و تجهیزات امنیتی؛ و
- دارایی‌ها، سامانه‌ها و اطلاعات لازم جهت اجرای الزامات مقرراتی هم‌چون تشریح[1] الزامات، یا آن‌چه که به منظور تکمیل پیاده‌سازی دیگر الزامات خاص مورد نیاز است.

۷-۲-۲ برچسب‌گذاری و اداره‌کردن اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

1- Unbundling

۸ امنیت منابع انسانی

۸-۱ پیش از اشتغال[1]

۸-۱-۱ نقش‌ها و مسولیت‌ها

کنترل زیربند ۸-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

توصیه می‌شود کارکنان شاغل در بخش صنایع انرژی همگانی که مسؤول فناوری سامانه‌های کنترل فرآیند می‌باشند دانش و مهارت مناسب برای مدیریت و پایش بر نصب تاسیسات، نگهداری و بهره‌برداری از سامانه‌های کنترل فرآیند را داشته باشند. توصیه می‌شود این موضوع شامل تخصص کافی در حوزه فناوری مدرن سامانه‌های اطلاعاتی و امنیت آن‌ها باشد.

توصیه می‌شود مهندسان مرتبط سامانه کنترل و سایر کارکنان از نقش‌ها و مسوولیت‌های مختص خود به ویژه جنبه‌های امنیتی اطلاعات این سامانه‌ها اطلاع داشته باشند.

۸-۱-۲ گزینش[2]

کنترل زیربند ۸-۱-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

توصیه می‌شود فرآیند گزینش سخت‌گیرانه برای کارکنان کلیدی که به دارایی‌های اطلاعاتی حساس دسترسی داشته و یا مسؤول عملیات یا فرایندهای نگهداری سامانه‌های حساس می‌باشند، به دقت لحاظ شود. این امر به ویژه در صورتی است که دارایی‌های اطلاعاتی یا سامانه‌ها بخشی از زیرساخت‌های حیاتی بوده و یا این دارایی‌ها نیاز به بهره‌برداری از این زیرساخت‌ها داشته باشند.

ممکن است نیاز باشد قبل از این که افراد محتمل اجازه کار بر روی مولفه‌هایی که بخشی از زیرساخت‌های حیاتی هستند داده شود، متناسب با قوانین (محلی)، مجوز امنیتی خاص توسط سازمان‌های دولتی فراهم گردد.

۸-۱-۳ ضوابط و شرایط استخدام

کنترل زیربند ۸-۱-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

2 - Prior to employment
1 - Screening

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

توصیه می‌شود محدودیت در حقوق کارمندان هم‌چون حق اعتصاب، یا صدور مجوز به حداکثر زمان کاری در شرایط اضطراری، برای کارمندان کلیدی که مسؤول عملیات زیرساختی حیاتی و سامانه‌های حساس هستند، با در نظر گرفتن الزامات قانونی قابل اجرا، مد نظر گرفته شود.

توافق در مورد پایش و ثبت اقدامات خاص مانند عملیات سودهی نیز توصیه می‌شود موقع تدوین قرارداد استخدام در نظر گرفته شود.

۸-۲ حین خدمت

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۸-۳ خاتمه استخدام یا تغییر در شغل

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹ امنیت فیزیکی و محیطی

۹-۱ نواحی امن[1]

۹-۱-۱ حصار امنیت فیزیکی[2]

کنترل زیربند ۹-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

به ویژه در انتقال انرژی و سامانه‌های توزیع و در نواحی مولدهای پراکنده، مولفه‌ها در سراسر بخش‌های متمرکز توزیع یافته‌اند. تجهیزات در اتاق‌های فنی و کنترل ساختمان سازمان‌ها و محل‌های جانبی مستقر شده‌اند. گاهی اوقات تجهیزات در مکان‌های طرف سوم و یا در محیط‌های عمومی واقع شده‌اند. دستیابی به سطح جامع از حفاظت فیزیکی برای محل‌های جانبی در حالت عادی امکان پذیر نمی‌باشد، بنابراین توصیه می‌شود مخاطرات باقیمانده مورد ارزیابی قرار گرفته و در صورت لزوم با استفاده از اقدامات تکمیلی و کنترل‌ها کاهش یابند.

۹-۱-۲ کنترل‌های مدخل فیزیکی

کنترل زیربند ۹-۱-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

توصیه می‌شود استفاده از سامانه‌های کنترل دسترسی فیزیکی برای محل‌های جانبی که دارای تجهیزات

1 - Secure areas
2 - Physical security perimeter

کنترل فرآیند می‌باشند در نظر گرفته شوند. به زیربند ۹-۱-۹، امن‌سازی محل‌های جانبی مراجعه شود.

۹-۱-۳ امن‌سازی دفاتر، اتاق‌ها و امکانات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹-۱-٤ حفاظت در برابر تهدیدهای بیرونی و محیطی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹-۱-٥ کار در نواحی امن

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹-۱-٦ نواحی دسترسی عمومی، نواحی تحویل و بارگیری

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹-۱-۷ امن‌سازی مراکز کنترل

یک کنترل اضافه بر زیربند ۹-۱، مناطق امن از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر است:

کنترل

اقدامات لازم به منظور حصول اطمینان از امنیت فیزیکی مراکز کنترل، که در آن سامانه‌های کنترل مرکزی هم‌چون سرورهای کنترل، HMI و سامانه‌های حمایتی کار گذاشته شده‌اند، توصیه می‌شود طراحی شده، توسعه یافته و به‌کار گرفته شوند.

راهنمای پیاده‌سازی

به منظور محافظت از تاسیسات سامانه کنترل مرکزی هم‌چون مراکز کنترل شبکه یا اتاق‌های کنترل متمرکز یا توزیع شده برای تجهیزات نیرو یا واحدهای تولید (از این پس به‌عنوان مراکز کنترل نامیده می‌شوند)، توصیه می‌شود موارد زیر در نظر گرفته شوند:

الف- توصیه می‌شود برای ساخت مرکز کنترل، محلی واقع در زمین سفت و محکم انتخاب شود. هنگامی که چنین زمینی موجود نمی‌باشد، توصیه می‌شود اقدامات لازم جهت اطمینان از ظرفیت تحمل بار خاک پایه به عمل آید.

ب- توصیه می‌شود محلی برای مراکز کنترل مورد انتخاب قرار گیرد که در آن آسیب‌های زیست محیطی از نظر آب و باد و غیره در کمینه باشند. اگر محل انتخاب شده در معرض تهدید چنین آسیب‌هایی باشد توصیه می‌شود اقدامات لازم به منظور جلوگیری از این آسیب‌ها اعمال گردد.

پ- توصیه می‌شود محلی برای مراکز کنترل مورد انتخاب قرار گیرد که در آن آسیب‌های بالقوه ناشی از میدان‌های الکترومغناطیسی ناچیز باشند. اگر محل انتخاب شده در معرض میدان‌های الکترومغناطیسی قوی باشد توصیه می‌شود اقدامات لازم با استفاده از حفاظ الکترومغناطیسی برای محافظت از اتاق‌های تجهیزات سامانه کنترل انجام شود.

ت- توصیه نمی‌شود مراکز کنترل در مجاورت مستقیم امکانات ذخیره‌سازی مواد خطرناک که مخاطره انفجار یا احتراق دارند واقع شوند.

ث- اگر مرکز کنترل در منطقه زلزله خیز واقع شود، توصیه می‌شود ساختمان‌های مرکز کنترل با ساختار مقاوم در برابر زلزله باشند.

ج- توصیه می‌شود ساختمان‌های مرکز کنترل ضد آتش و مقاوم در برابر آتش باشند.

چ- توصیه می‌شود ساختمان مرکز کنترل با ثبات ساختاری مناسب با کلیه شرایط لازم جهت طبقات اضافه طراحی گردد.

ح- توصیه می‌شود سامانه‌های اعلام حریق خودکار در مراکز کنترل نصب گردند.

اطلاعات بیشتر برای صنایع انرژی

دارایی‌های سامانه کنترل فرآیند گاهی اوقات در یک مرکز داده‌ها که به صورت خارجی بهره‌برداری می‌شود، همراه با سایر دارایی‌های اطلاعاتی و مخابراتی(ICT) قرار دارند. تفکیک فیزیکی بین سامانه‌های کنترل و دیگر سامانه‌های فناوری ارتباطات و اطلاعات و «تفکیک وظایف[1]» به هنگام کار متصدی‌ها با سامانه کنترل دارای اهمیت زیادی می‌باشد، در بسیاری از موارد این کار در تاسیسات دور از مرکز داده‌ها و تحت کنترل صنایع انرژی همگانی می‌باشد.

۹-۱-۸ امن‌سازی اتاق‌های تجهیزات

استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، شامل این کنترل نیست.

کنترل

توصیه می‌شود اقدامات لازم به منظور حصول اطمینان از امنیت فیزیکی اتاق تجهیزات که در آن امکانات سامانه کنترل به‌کار رفته در صنایع انرژی واقع شده است، طراحی و توسعه و پیاده‌سازی گردد.

1-Segregation of duties

راهنمای پیاده‌سازی

توصیه می‌شود به منظور محافظت از اتاقی که در آن امکانات سامانه کنترل به‌کار رفته در صنایع انرژی قراردارد(از این پس به‌عنوان اتاق‌های تجهیزات سامانه کنترل نامیده می‌شود) کنترل‌های زیر در نظر گرفته شوند:

الف- توصیه می‌شود اتاق‌های تجهیزات سامانه کنترل در محلی واقع شود که در آن کمینه مخاطرات خارجی از قبیل شرایط محیطی شدید یا بلایای طبیعی باشد.

ب- توصیه می‌شود اتاق تجهیزات سامانه کنترل در محلی واقع شود که دسترسی افراد غیر مجاز به آن محدود باشد و توصیه می‌شود اقدامات کافی برای جلوگیری و کشف امکان نفوذ غیرمجاز به‌کار گرفته شود.

پ- در صورت امکان، توصیه می‌شود اتاق تجهیزات سامانه کنترل پوشیده باشد. توصیه می‌شود کمینه نشانه‌ی استفاده‌ی این اتاق به‌عنوان اتاق تجهیزات سامانه کنترل برای سامانه‌های کنترل فرآیند وجود داشته باشد.

ت- توصیه می‌شود اتاق تجهیزات سامانه کنترل در محلی باشد که کم‌ترین امکان وجود سیل یا آب گرفتگی را داشته باشد. اگر این شرط رعایت نشود، توصیه می‌شود اقدامات لازم برای جلوگیری از این مورد اعمال شود، هم‌چون بالا بردن سطح کف، طراحی ضد آب، نصب امکانات فاضلاب و غیره.

ث- توصیه می‌شود اتاق تجهیزات سامانه کنترل در مکانی باشد که به بهترین نحو از میدان‌های الکترومغناطیسی قوی محافظت شود. اگر این شرط رعایت نشود، توصیه می‌شود توسط محافظ الکترومغناطیسی و سایر اقدامات مناسب محافظت شود. این امر به ویژه در مورد مجاورت با تجهیزات ولتاژ بالا و یا مبدل‌ها[1] صادق است.

ج- توصیه می‌شود مولفه‌های مهم در یک اتاق تجهیزات سامانه کنترل اختصاصی با حفاظ فیزیکی مناسب قرار داده شوند.

چ- توصیه می‌شود در مناطق با مخاطره زلزله بالا، اقدامات لازم برای جلوگیری از فرو ریختن اقلام و مواد به کاررفته در کف، دیوارها، سقف در نظر گرفته شود.

ح- مواد مورد استفاده در کف، دیوار، سقف و غیره توصیه می‌شود غیر قابل اشتعال و مقاوم در برابر آتش باشند.

خ- اقدامات لازم جهت خرابی ناشی از الکتریسیته ساکن در نظر گرفته شود.

1-Transformers

د- داکت‌های اتصال اتاق تجهیزات سامانه کنترل توصیه می‌شود مناسب با کم کردن سرعت آتش یا جلوگیری از گسترش آن طراحی شود.

ذ- در صورت لزوم، اقداماتی برای محافظت اتاق تجهیزات سامانه کنترل از تداخل الکترومغناطیسی آن‌ها در صورتیکه به‌عنوان اتاق ذخیره‌سازی و بایگانی اطلاعات استفاده شده باشد، به‌کار گرفته شود.

ر- اقدامات ضد آتش برای اتاق ذخیره‌سازی اطلاعات به‌کار گرفته شود.

ز- هشدارهای خودکار اعلام حریق در اتاق تجهیزات سامانه کنترل و اتاق تجهیزات تهویه مطبوع کار گذاشته شود.

ژ- سامانه آتش نشانی در اتاق تجهیزات سامانه کنترل و اتاق تجهیزات تهویه مطبوع کار گذاشته شود.

س- اتاق تجهیزات سامانه کنترل توصیه می‌شود دارای سامانه تهویه مطبوع باشد.

ش- تهویه مطبوع اتاق تجهیزات سامانه کنترل و سایر اتاق‌ها توصیه می‌شود توسط یک سامانه مجزا که مختص ادارات و سایر ساختمان‌ها است، تامین گردد.

۹-۱-۹ امن‌سازی محل‌های جانبی

استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، شامل این کنترل نیست.

کنترل

برای محل‌های جانبی که در آن اتاق تجهیزات سامانه کنترل به‌کار رفته در صنایع انرژی وجود دارد، توصیه می‌شود کنترل‌های امنیت فیزیکی طراحی، توسعه و پیاده‌سازی گردد.

جایی که محافظت فیزیکی مناسب و کافی قابل دست‌یابی نباشد، توصیه می‌شود مخاطره موجود و احتمالی مورد توجه قرار گرفته و اقدامات متقابل در جهت کاهش آن‌ها صورت گیرد. توصیه می‌شود هنگام انتخاب چنین اقدامات متقابلی، اولین ملاحظات به حساسیت سامانه‌های کنترل فرآیند بهره برداری شده در محل-های جانبی و همین‌طور مفاهیم افزونگی و ذخیره[1] پیاده‌سازی شده برای عملکرد متناسب سامانه، درنظر گرفته شود.

راهنمای پیاده‌سازی

به خصوص در انتقال انرژی و شبکه‌های توزیع و سامانه‌های تولید توزیع شده، مولفه‌های زیرساخت سامانه کنترل ممکن است در سراسر محل‌های جانبی پراکنده باشند. به منظور حفاظت از چنین محل‌های غیر

1- Fallback

متمرکز که تجهیزات کنترل سامانه در آن جای دارند (از این پس به‌عنوان محل‌های جانبی نامیده می‌شود)، توصیه می‌شود کنترل‌های زیر در نظر گرفته شوند:
الف- اگر محل جانبی در منطقه زلزله خیز قرار دارد، توصیه می‌شود با توجه به استانداردهای ملی و منطقه‌ای به صورت ضد زلزله ساخته شود.

ب- در صورت نیاز و بنا به حساسیت سامانه‌های کنترل فرآیند اجرا شده در محل‌های جانبی، تجهیزات خودکار کنترل آتش توصیه می‌شود نصب گردند.

پ- محل‌های جانبی توصیه می‌شود به منظور عیب یابی مولفه، قطعی برق مورد کنترل قرار گیرند. در صورت نیاز میزان رطوبت هوا و درجه دما نیز کنترل شوند.

ت- توصیه می‌شود حصار امنیت فیزیکی مناسب نصب شود، برای مثال با استفاده از حصارکشی و سامانه هشدار خودکار به وجود آید که از یک مقر مرکزی مورد پایش باشد.

۹-۲ امنیت تجهیزات

۹-۲-۱ استقرار و حفاظت تجهیزات[1]

کنترل زیربند ۹-۲-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

تحت شرایط معین، مولفه‌های سامانه کنترل فرآیند و حفاظت زیرساخت‌ها ممکن است در مناطقی که در معرض گرد و غبار، گرما، سرما، تابش الکترومغناطیسی، رطوبت و غیره هستند نصب شود. توصیه می‌شود تجهیزات به طور مناسب جهت کار در چنین شرایط محیطی طراحی و ساخته شود، در غیر این صورت اقدامات افزونه متقابل محافظتی هم‌چون پیاده‌سازی قفسه‌های خارجی مناسب برای اطمینان از عملکرد مطمئن آن‌ها به اجرا در آید.

۹-۲-۲ امکانات پشتیبانی[2]

کنترل ۹-۲-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی صنایع انرژی همگانی

برای جلوگیری از وابستگی‌های حلقوی[3]، کلیه سامانه‌های بحرانی، خدمات ارتباطی و سایر تجهیزات مورد نیاز برای بازسازی سامانه برق بعد از قطعی برق توصیه می‌شود به گونه‌ای طراحی و اجرا شود که مستقل از خدمات خارجی و برای یک دوره مناسب زمانی باشد. این امر به ویژه در مورد فراورده‌های خارجی انرژی

1 - Equipment siting and protection
2 - Supporting utilities
3 - Cyclic dependencies

به‌کار برده می‌شود.

اطلاعات بیشتر در مورد صنایع انرژی همگانی

توصیه می‌شود بسته به طرح‌های بازسازی سامانه، مولفه های حیاتی و ضروری برای بازسازی سامانه بتوانند مستقل از منبع برق خارجی به مدت ۸ الی ۱۲ ساعت کار کنند. در مناطق دور افتاده ممکن است تامین یک منبع تغذیه مستقل برای چند روز کار ضروری باشد. این کار، به‌عنوان مثال، شامل یک مولد برق اضطراری خودکار و نیز ذخایر مربوط به سوخت می‌باشد.

۹-۲-۳ امنیت کابل‌کشی[1]

کنترل ۹-۲-۳ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی صنایع انرژی همگانی

به خصوص در حوزه انتقال انرژی و شبکه‌های توزیع، شبکه‌های ارتباطی در مناطق وسیعی نصب شده‌اند که اجازه ارتباط با محل‌های جانبی را می‌دهد. امکان ارائه سطح یکسانی از کابل کشی محل همانند کابل‌کشی منزل مسکونی وجود ندارد. مخاطرات مرتبط نیز توصیه می‌شود به همان صورت ارزیابی شده و اقدامات لازم مکمل جهت ارزیابی به عمل آید. با توجه به حساسیت انتقال داده‌ها، توصیه می‌شود اقداماتی هم‌چون حفاظت از رمز نگاری نیز صورت گیرد.

۹-۲-٤ نگهداری تجهیزات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹-۲-٥ امنیت تجهیزات خارج از ابنیه اماکن سازمان[2]

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹-۲-٦ امحا[3] یا استفاده مجدد از تجهیزات به صورت امن

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۹-۲-۷ خروج اموال[4]

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

---

4 - Cabling
1 - Off-premises
2 - Disposal
3 - Removal of property

۹-۳ امنیت در محل طرف‌های سوم

یک هدف کنترلی اضافه بر از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، بند ۹، امنیت فیزیکی و محیطی به شرح زیر است:

هدف: محافظت از تجهیزات واقع در خارج از سازمان صنایع انرژی همگانی در مقابل تهدیدات فیزیکی و زیست محیطی.

۹-۳-۱ تجهیزات مستقر در محل دیگر سازمان‌های صنایع انرژی همگانی

کنترل

زمانی‌که سازمان‌های صنایع انرژی همگانی تجهیزات را خارج از محل خود و حوزه‌ی صنایع دیگر نصب می‌نمایند، برای مثال ایستگاه‌های اتصال متقابل، در این صورت توصیه می‌شود تجهیزات در یک منطقه حفاظت شده قرار گیرند طوری که مخاطرات و تهدیدات زیست محیطی و امکان دسترسی‌های غیر مجاز کاهش یابد.

راهنمای پیاده‌سازی

به منظور محافظت از سازمان صنایع انرژی همگانی که در محل سازمان‌های صنایع انرژی همگانی دیگر مستقر شده است، توصیه می‌شود کنترل‌های زیر در نظر گرفته شود:

الف- توصیه می‌شود محدوده‌ی مسوولیت‌ها و واسطها با سایر سازمان‌های صنایع انرژی همگانی مشخص شود و توصیه می‌شود امکان جداسازی تجهیزات از سازمان‌های دیگر در صورت لزوم وجود داشته باشد. (به زیربند ۹-۳-۳، سامانه‌های کنترل و ارتباطی با اتصال متقابل، مراجعه شود).

ب- توصیه می‌شود موافقت نامه‌ها با دیگر سازمان صنایع انرژی همگانی به منظور تامین خدمات زیرساختی حمایتی هم‌چون تامین انرژی، سرمایش، گرمایش و غیره به صورت قراردادی به نتیجه برسد.

پ- توصیه می‌شود اطیمنان حاصل شود که نیازهای امنیتی محل عملیاتی که در آن قرار است تجهیزات نصب شود، رعایت شده باشد.

اطلاعات اضافی

به منظور اطمینان از سازگاری سطح امنیت اصول دیگر سازمان با اصول خود سازمان صنایع انرژی همگانی، توصیه می‌شود اصطلاحات و شرایط مربوطه به صورت پیشرفته مورد مذاکره قرار گیرد.

۹-۳-۲ تجهیزات مستقر در محل مشتری

کنترل

زمانی که سازمان‌های صنایع انرژی همگانی تجهیزات خود را در محل مشتری نصب می‌نمایند، برای مثال، به منظور کنترل و اندازه‌گیری تامین انرژی و/یا تحویل خدمات اضافی، توصیه می‌شود تجهیزات سازمان از هر گونه مخاطرات ناشی از تهدیدات زیست محیطی محافظت شده و امکان دسترسی‌های غیر مجاز به آن کاهش یابد.

راهنمای پیاده‌سازی

به منظور محافظت از تجهیزات واقع در محل مشتری، توصیه می‌شود کنترل‌های زیر مورد نظر قرار گرفته شوند:
الف- توصیه می‌شود قفسه‌های تجهیزات نصب‌شده در محل مشتری محکم باشند و توصیه نمی‌شود که کاربران غیر مجاز بتوانند به آسانی آن‌ها را باز کنند. توصیه می‌شود هر گونه دستکاری به آسانی قابل کشف باشد.

ب- توصیه می‌شود محدوده‌ی مسوولیت‌ها و واسط‌ها با مشتری مشخص شود و توصیه می‌شود امکان جداسازی تجهیزات از مشتری در صورت لزوم وجود داشته باشد.

پ- توصیه می‌شود امکان پایش بر وضعیت تجهیزات یا اجرای از راه دور تجهیزات وجود داشته باشد.

۹-۳-۳ سامانه‌های کنترل و ارتباطی با اتصال متقابل

کنترل

هنگامی که سامانه‌های کنترل و خطوط ارتباطی با طرف سوم خارجی متقابلا متصل هستند، توصیه می‌شود محدوده‌ی مسوولیت و واسط‌ها با مشتری به روشنی تعریف شود طوری که امکان قطع ارتباط و جداسازی هر سازمان از سایرین در مدت زمان مناسب به منظور جلوگیری از مخاطرات شناخته‌شده وجود داشته باشد.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان‌های صنایع انرژی همگانی وضعیت اتصالات متقابل خود را پایش کنند.

به منظور تشخیص نواحی مشکل و انجام اقدامات اصلاحی، توصیه می‌شود سازمان‌ها وسیله‌ی جداسازی اتصالات بین خود و اشخاص ثالث خارجی و اتصال دوباره‌ی اتصالات جداشده را داشته باشند.
توصیه می‌شود سازمان‌های صنایع انرژی همگانی در قراردادها و موافقت نامه‌های خود مشخص نمایند در مواردی که دخالت جدی در خدمات خود سازمان حادث می‌شود، اتصالات متقابل سامانه ممکن است به

حالت تعلیق درآیند.
توصیه می‌شود معیار و شرایط لازم برای تعلیق اتصالات متقابل سامانه به روشنی تعریف شود. علاوه بر این، توصیه می‌شود اثرات محتمل تعلیق اتصالات متقابل سامانه ارزیابی شده و در صورت لزوم توصیه می‌شود اقدامات مجدد در جایی که لازم است تعریف و فراهم گردد.

۱۰ مدیریت ارتباطات و عملیات

۱۰-۱ روش‌های اجرایی عملیاتی و مسوولیت‌ها

۱۰-۱-۱ روش‌های اجرایی عملیاتی مستند شده

کنترل زیربند ۱۰-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

در مستندسازی فرایندهای بهره‌برداری توصیه می‌شود به طور دقیق مشخص شود که تحت چه شرایط حادثه، روش‌های اجرایی ساماندهی بحرانی یا اضطراری باید فراخوانی شوند. (به بند ۱۳-۲، مدیریت حوادث و بهبودهای امنیت اطلاعات مراجعه شود).

۱۰-۱-۲ مدیریت تغییر

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۱-۳ تفکیک وظایف

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۱-٤ جداسازی امکانات توسعه، آزمون و عملیاتی

کنترل بند ۱۰-۱-۴ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

در دامنه فرآیند کنترل صنایع انرژی، جداسازی سامانه‌های عملیاتی، آزمون و توسعه در سطح وسیعی امکان پذیر نمی‌باشد. این امر به ویژه هنگام پردازش داده‌ها در زمان واقعی به منظور توسعه، آزمون و عیب یابی اشکال زدایی اهداف مورد نیاز است. در موارد خاصی هم‌چون، که در آن ارتباطات بین سامانه‌های توسعه، آزمون و عملیاتی مورد نیاز است و یا آزمون و اشکال زدایی در سطح سامانه عملیاتی ضروری است، این هم‌پوشانی‌ها توصیه می‌شود به کمینه کاهش یابند. مخاطرات حاصله توصیه می‌شود شناخته شده و امکان جایگزینی داشته باشند، هم‌چون روند شبیه سازی داده‌ها و یا اشکال زدایی از راه دور (اشکال زدایی از سامانه عملیاتی با استفاده از واسطهای سامانه‌های ارتباطی امن) توصیه می‌شود در نظر گرفته شود.

اگر جداسازی توسعه، آزمون و سامانه‌های عملیاتی قابل پیاده‌سازی نباشد، توصیه می‌شود مدیریت تغییر و

روش‌های اجرایی ساماندهی رخداد، اضطرار و بحران به صورت بومی تعیین شود تا اجازه دهد واکنش سریع و مناسب نسبت به شکست‌ها و مشکلات در سامانه عملیاتی، سازگار با حساسیت سامانه مورد بحث باشد صورت گیرد.

توصیه می‌شود اطمینان حاصل شود که سامانه‌های توسعه و آزمون با استفاده از آخرین فناوری امن‌سازی شود. توجه به حساسیت آن‌ها توصیه می‌شود اطمینان حاصل کرد که سامانه‌های آزمون و توسعه به طور مناسب از سایر سامانه‌ها و شبکه‌ها جداسازی شده‌اند.

۱۰-۲ مدیریت تحویل خدمت شخص سوم

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۳ طرح‌ریزی و پذیرش سامانه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-٤ حفاظت در برابر کدهای مخرب و سیار[1]

۱۰-٤-۱ کنترل‌هایی در برابر کدهای مخرب

کنترل بند ۱۰-۴-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

اگر به دلایل فنی امکان ایجاد نرم‌افزاری که حفاظت در برابر کدهای مخرب را به عهده دارد وجود ندارد ، (به طور مثال در نتیجه‌ی عدم حمایت فروشنده یا تایید فروشنده و یاعدم امکان نصب به موقع به روز رسانی‌ها) توصیه می‌شود مخاطرات حاصل شناسایی شود و توصیه می‌شود انواع دیگری از اقدامات متقابل پیاده‌سازی شود که میزان مناسبی از حفاظت را تامین نماید.

کنترل‌های تکمیلی در برابر کدهای مخرب در میان سایر عوامل شامل موارد زیر می‌باشند:

- امن‌سازی کلیه واسطهای فیزیکی و منطقی داده‌ها؛
- جداسازی شبکه و اجرای امنیت شبکه تقسیم مناطقی که محدود به تحت تاثیر قرار گرفتن یک تروجان باشند؛
- اقدامات جامع برای سخت‌سازی[2] سامانه از جهت کمینه کردن مخاطرات کدهای مخرب ؛

1 - Malicious and mobile code
1 - Hardening

- پیاده‌سازی راه‌حل‌های فهرست سفید[1] که اجرای نرم‌افزارها و کدهای تایید نشده را محدود می‌نماید.

به طور خاص توصیه می‌شود اثرات احتمالی رخدادهای کدهای مخرب بر تجهیزات به‌کار برده جهت کنترل فرآیند بلادرنگ[2] و ارتباطات مرتبط در نظر گرفته شده و با پیاده‌سازی کنترل‌های مناسب کاهش یابند.

۱۰-٤-۲ کنترل‌هایی در برابر کدهای سیار

کنترل زیربند ۱۰-۴-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

فناوری شبکه‌های هوشمند ممکن است مبتنی بر شبکه‌های ارتباطی و نصب و راه‌اندازی سامانه‌های کنترل مستقر در محل مشتری باشند. برای این منظور، عوامل نرم‌افزارهای سیار ممکن است به‌کار برده شود که قادر به تامین و نصب توسط مشتری یا سایر طرف‌های سوم باشد. توصیه می‌شود مخاطرات ناشی از به‌کارگیری کد سیار در نظر گرفته شده و به طور مناسب با آن‌ها رفتار شود.

۱۰-۵ نسخه‌های پشتیبان

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-٦ مدیریت امنیت شبکه

۱۰-٦-۱ کنترل‌های شبکه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-٦-۲ امنیت خدمات شبکه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-٦-۳ امن‌سازی ارتباطات داده‌های کنترل فرآیند

یک هدف کنترلی اضافه بر استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، زیربند ۱۰-۶، مدیریت امنیت شبکه به شرح زیر است:

کنترل

توصیه می‌شود اقدامات لازم جهت حصول اطمینان از محرمانه بودن، یکپارچگی و در دسترس بودن کنترل فرایندهای داخلی و خارجی ارتباطات داده‌ها طبق سطح حساسیت انتقال داده‌ها طراحی و توسعه و اجرا شوند.

---

2 - Whitelisting Solutions
3 - Real-time

راهنمای پیاده‌سازی

در زمینه کنترل فرآیند ارتباطات داده‌ها چندین نوع بخش و استانداردهای فنی و عمومی وجود دارند. هم‌چون:

- IEC 60870-5
- IEC 60870-6 (TASE.2)
- DNP3
- IEC 61850
- IEC 61400-25
- MODBUS

پروتکل‌های ارتباطی استاندارد معمولا شامل سازوکارهای امنیتی اختصاص یافته نمی‌شوند.

توصیه می‌شود مخاطرات ناشی از این موارد با اجرای اقدامات متقابل اصلاح‌شده در نظر گرفته شوند. اقدامات متقابل ممکن است شامل فعال سازی ویژگی‌های امنیتی که معمولا به صورت محافظت شده (برای مثال با توجه به IEC 62351) و یا محافظت از رمزنگاری اضافی باشند.

۱۰-۷ ساماندهی محیط‌های ذخیره‌سازی[1]

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۸ تبادل اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۹ خدمات تجارت الکترونیک

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۱۰ پایش

۱۰-۱۰-۱ رویدادنگاری ممیزی[2]

کنترل زیربند ۱۰-۱۰-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

در بخش صنایع انرژی همگانی، رویدادنگاری‌های ممیزی مربوط ممکن است شامل برخی اعمال معین انجام شده توسط کارکنان عملیاتی هم‌چون عملیات‌های راه‌گزینی باشد. رویداد نگاشت‌های ممیزی و تعهدات

1- Media handling
1- Audit logging

حفظ این سوابق ممکن است در قوانین خاص صنعت و توسط نهادهای تنظیم مقررات[1] برای طیف گسترده‌ای از اسناد الکترونیکی تصریح شده باشد.

توصیه می‌شود اکتساب، پردازش و مدیریت پروتکل‌ها و داده‌های ممیزی مطابق با کلیه الزامات کاربردپذیر تجاری و قانونی، مقرراتی و داخلی پیاده‌سازی شوند.

۱۰-۱۰-۲ پایش کاربرد سامانه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۱۰-۳ حفاظت از اطلاعات ثبت شده‌ی وقایع

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۱۰-٤ اطلاعات ثبت شده‌ی وقایع مربوط به راهبر و متصدی سامانه[2]

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۱۰-۵ رویدادنگاری خرابی[3]

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۰-۱۰-٦ همزمان‌سازی ساعت[4]

کنترل زیربند ۱۰-۱۰-۶ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

برای کلیه سامانه‌هایی که به طور مستقیم یا غیر مستقیم مرتبط با شرکای خارجی هستند توصیه می‌شود یک زمان استاندارد مورد توافق و مشترک هم‌چون زمان اروپایی مرکزی (CET)[5] و یا زمان جهانی هماهنگ شده (UTC)[6] مورد استفاده قرار گیرد.

اطلاعات بیشتر در مورد صنایع انرژی همگانی

بسته به حساسیت سامانه کنترل فرآیند مورد نظر، به‌کارگیری پیام‌های زمان کارسازان[7] NPT اختصاص یافته و غیراینترنتی و یا NTPهای به صورت رقمی امضا شده توصیه می‌شود به منظور جلوگیری از

2- Regulatory
3- Administrator
4- Fault
5- Clock synchronization
1- Central European Time
2- Coordinated Universal Time
3- Servers

دست‌کاری سیگنال‌ها مد نظر گرفته شوند.

۱۰-۱۱ سامانه‌های قدیمی[1]

یک هدف کنترلی اضافه بر از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، بند ۱۰، مدیریت ارتباطات و عملیات‌ها به شرح زیر است:

هدف: محافظت در برابر مخاطرات ناشی از استفاده از سامانه‌های قدیمی، در جایی که اقدامات امنیتی لازم نمی‌توانند پیاده‌سازی شوند.

۱۰-۱۱-۱ طرز عمل[2] با سامانه‌های قدیمی

کنترل

توصیه می‌شود کلیه فناوری‌های سامانه کنترل فرآیند قدیمی، سامانه‌ها و مولفه‌ها (از این پس به‌عنوان سامانه‌های قدیمی نامیده می‌شوند) به همراه آسیب پذیری‌های اطلاعات امنیتی شناخته شوند.

توصیه می‌شود کنترل های مناسب به منظور کاهش کلیه مخاطرات شناخته شده در ارتباط با چنین سامانه‌هایی اجرا گردند.

راهنمای پیاده‌سازی

تعداد زیادی از سامانه‌های کنترل فرآیند مورد استفاده در صنعت صنایع انرژی همگانی مبتنی بر فناوری‌های قدیمی که فاقد ویژگی‌های امنیتی هستند می‌باشند. توصیه می‌شود برای ارائه سطح مناسبی از امنیت، مخاطرات ناشی از ادامه استفاده از سامانه‌های قدیمی و فناوری‌ها شناخته شوند. توصیه می‌شود در شرایطی که کنترل‌های استاندارد قابل اجرا نمی‌باشند سایر انواع کنترل‌ها به‌کار گرفته شوند، برای مثال:
الف- اجرای دقیق و مناسب تفکیک شبکه

ب- توصیه می‌شود از دسترسی از راه دور برای اهداف پیکربندی و نگهداری اجتناب شود. اگر دسترسی از راه دور کاملا ضروری است، توصیه می‌شود از ایزوله کردن مناسب شبکه، برای مثال با استفاده از خدمات پروکسی امن اطمینان حاصل شود. توصیه می‌شود دسترسی برای اهداف نگهداری از طریق نقاط اتصال متقابل تعریف شده که به طور امن در حال پایش و بهره‌برداری می‌باشند فراهم گردد.

پ- توصیه می‌شود قوانین کنترل دسترسی اکید در سطوح شبکه، سامانه و برنامه‌کاربردی اجرا شود.

توصیه می‌شود اطمینان حاصل شود که فقط تجهیزات و مولفه‌های دارای بالاترین سطح فناوری برای اهداف پیکربندی و نگهداری به‌کار گرفته می‌شود.

4- Legacy systems
5- Treatment

۱۰-۱۲ کارکردهای ایمنی[1]

یک هدف کنترلی اضافه بر از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، بند ۱۰، مدیریت ارتباطات و عملیات‌ها به شرح زیر است:

هدف: اطمینان از یکپارچگی و دسترس‌پذیری کارکردهای ایمنی

۱۰-۱۲-۱ یکپارچگی و دسترس‌پذیری کارکردهای ایمنی

کنترل

توصیه می‌شود یکپارچگی و دسترس‌پذیری دارایی‌های اطلاعاتی، سامانه‌ها و مولفه‌ها و کارکردهایی که جهت حصول اطمینان از کارکردهای ایمنی مورد نیاز هستند، مطابق با استانداردهای خاص بخش و الزامات قانونی محافظت شوند.

راهنمای پیاده‌سازی

به منظور اطمینان از بهره‌برداری کارکردهای ایمنی توصیه می‌شود اقدامات زیر در نظر گرفته شود:
الف- به‌کارگیری سامانه‌های اختصاصی و ارتباطی به منظور انتقال داده‌های ارتباطی مربوط به ایمنی.

ب- حصول اطمینان از این‌که کارکردهای ایمنی مستقل از کنترل فرآیند و سامانه‌های خودکارسازی هستند.

پ- اجتناب از تغییرات در سامانه‌های ایمنی حساس و داده‌های پیکر بندی مربوط به ایمنی با استفاده از تجهیزات کنترل از راه دور.

ت- رویدادنگاری تغییرات پیکربندی سامانه‌های ایمنی

۱۱ کنترل دسترسی

۱-۱۱ الزامات کسب‌وکار برای کنترل دسترسی

۱-۱-۱۱ خط‌مشی کنترل دسترسی

کنترل زیربند ۱-۱-۱۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

به علاوه، توصیه می‌شود خط‌مشی موارد زیر را نیز مورد توجه قرار گیرد:
الف- کاربرد شرایط و مقررات مربوط به استفاده از حساب‌های گروهی، زمانی که استفاده از حساب‌های شخصی امکان پذیر نمی‌باشد. به منظور حصول اطمینان از سطح مناسب امنیت دسترسی و قابلیت ردیابی، توصیه می‌شود قوانین دقیقی به همراه اقدامات مکمل تعریف شوند.

1- Safety functions

ب- شرایط و مقرراتی که در سامانه‌هایی کاربردپذیر هستند که دارای خط‌مشی اسم‌رمزی قوی نبوده و یا چنین خط‌مشی اسم‌رمزی به دلیل عملیاتی ممکن نیست. به منظور حصول اطمینان از سطح مناسب امنیت دسترسی، توصیه می‌شود اقدامات مکمل تعریف شوند.

۱۱-۲ مدیریت دسترسی کاربر

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-۳ مسوولیت‌های کاربر

۱۱-۳-۱ استفاده از اسم‌رمز[1]

کنترل زیربند ۱۱-۳-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

در دامنه کنترل فرایند، اطمینان از استفاده‌ی رمز عبور امن، همیشه امکان پذیر نیست.

- سامانه‌های قدیمی اغلب قابلیت داشتن اسم‌رمزهای فردی و/یا اسم‌رمزهای قوی را نمی‌دهند.

- اغلب اتصال به سامانه‌های عملکردی در تجیهزات غیر متمرکز غیر ممکن است؛ هم‌چون واحدهای تولیدی غیر متمرکز، خدمات فهرست راهنمای[2] مرکزی، که به این معنی است که اسم‌رمز و حساب‌های محلی مورد استفاده قرار می‌گیرد. و این باعث می‌شود که امکان تغییر اسم‌رمز وجود نداشته باشد.

بنابراین توصیه می‌شود به وضوح برای کاربر مشخص شود که چه زمانی خط‌مشی اسم‌رمز عمومی به‌کار برده شده و کجا اسم‌رمزهای متفاوت به‌کار برده شده و یا کجا به‌کار بردن هر اسم‌رمز یی غیر ممکن است (در سامانه‌های قدیمی).

به صورت خاص، در شرایطی که تنها یک اسم‌رمز منحصر به فرد برای دسترسی عمومی سامانه استفاده می‌شود، توصیه می‌شود یک اسم‌رمزی که تا حد امکان امن است، انتخاب شود. به طور ویژه توصیه می‌شود کلمه‌های عبور استاندارد به‌کار رفته توسط فروشندگان سامانه ناامن تلقی شود. کلمه‌های عبور توصیه می‌شود توسط افرادی که در به‌کارگیری سامانه درگیر هستند قابل دسترس باشد.

۱۱-۳-۲ تجهیزات بدون مراقبت کاربر

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-۳-۳ خط‌مشی میز پاک و صفحه پاک

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

1- Password
2- Directory

۱۱-٤ کنترل دسترسی به شبکه

۱۱-٤-۱ خط‌مشی استفاده از خدمات شبکه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-٤-۲ احراز اصالت کاربر برای اتصالات بیرونی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-٤-۳ شناسایی تجهیزات در شبکه‌ها

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-٤-٤ حفاظت از درگاه عیب‌یابی و پیکربندی راه دور

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-٤-٥ تفکیک در شبکه‌ها

کنترل زیربند ۱۱-۳-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

توصیه می‌شود زیرساخت‌های شبکه‌ی سامانه‌های کنترل فرآیند زمانی که کاربردپذیر و از لحاظ فنی امکان-پذیر باشد، به چند حوزه مختلف با عملکردها و الزامات حفاظتی مختلف تقسیم گردند. به طور خاص، توصیه می‌شود دامنه‌های فنی و عملکردی از یکدیگر جدا گردند.

زمانی که از نظر فنی میسر باشد، حوزه‌های شبکه توسط دیوارهای آتش، مسیریاب‌ها یا دروازه‌های پالایش جداسازی شوند. اتصالات شبکه به شبکه‌های خارجی، هم‌چون شبکه دفتر شرکت، شرکای خارجی یا اتصالات نگهداری از راه دور، توصیه می‌شود به صورت انحصاری از طریق پراکسی‌های کاربردی که به صورت ویژه مستحکم شده، مسیریابی شوند، که در یک حوزه شبکه جداگانه مستقر شده (برای مثال، حوزه غیرنظامی) و برای این منظور طراحی شده است.

توصیه می‌شود شبکه و سامانه‌های پراکنده زمانی که از لحاظ فنی و کابردی میسر باشد، به دو بخش مستقل افقی تقسیم گردند. توصیه می‌شود این بخش توسط دیوارهای آتش، مسیریاب‌ها یا دروازه‌های پالایش جداسازی شوند.

۱۱-٤-٦ کنترل اتصال به شبکه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد

۱۱-٤-۷ کنترل مسیریابی در شبکه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد

۱۱-٤-۸ اتصال منطقی سامانه‌های کنترل فرآیند بیرونی

یک کنترل اضافه بر استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، بند ۱۱-۴، کنترل دسترسی شبکه به شرح زیر است:

کنترل

قبل از سامانه‌های کنترل فرایند، ارتباطات مرتبط با اشخاص بیرونی توصیه می‌شود به وجود آیند، سازمان صنایع انرژی همگانی توصیه می‌شود اطمینان حاصل کند که تنها ارتباطات مجاز و جریان اطلاعات، شامل دستورات سامانه کنترل و پیغام‌ها بر روی یک پیوند می‌توانند تغییر یابند. توصیه می‌شود مخاطرات ناشی از چنین اتصال سامانه‌ای ارزیابی گردند.

راهنمای پیاده‌سازی

توصیه می‌شود سامانه‌های کنترل فرایند، تنها در صورت لزوم و به دلایل عملیاتی با طرف‌های سوم خارجی اتصال داشته باشند. توصیه می‌شود این اتصال در نقاط معین شده برای اتصال که از نظر عملیاتی و پایشی امن هستند، انجام گردد.

نوع و میزان ارتباطات مجاز، از جمله تبادل اطلاعات لازم و دستورات کنترل توصیه می‌شود مورد تایید باشند. به‌کارگیری افزاره‌های پالایش (هم‌چون پروکسی‌ها و نرم‌افزارهای دیوار آتش) اجازه می‌دهد تا تنها اطلاعات و ارتباطات مجاز جریان در نظر گرفته شوند.

۱۱-۵ کنترل دسترسی به سامانه عامل

۱۱-۵-۱ روال‌های اجرایی برقراری ارتباط امن

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-۵-۲ شناسایی و احراز اصالت کاربر

کنترل زیربند ۱۱-۵-۲ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

استفاده از شناسه‌های کاربر منحصر به فرد در سامانه‌های کنترل فرآیند انرژی ممکن است میسر و ممکن نباشد، برای مثال، برای دسترسی به سامانه اجرایی یا سامانه عامل هم‌چون کنترل‌کننده‌ها/PLCها یا به منظور فرایندهای نگهداری در سامانه‌های پراکنده. مخاطرات ناشی از این موضوع توصیه می‌شود در نظر

گرفته شده و اقدامات متقابل کاهش مخاطرات توصیه می‌شود صورت گیرد.

به‌کار کیری حساب کاربری فردی یا گروهی توصیه می‌شود مطابق با الزامات حسابرسی کاربردپذیر باشد.

۱۱-۵-۳ سامانه مدیریت اسم‌رمز

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-۵-٤ استفاده از برنامه‌های کمکی سامانه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد

۱۱-۵-۵ خروج زمانی از لایه ارتباطی

کنترل زیربند ۱۱-۵-۵ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

فعال‌سازی زمان‌های دوره و محافظ صفحه نمایش‌ها در برخی از برنامه‌های کاربری کنترل فرآیند مناسب نیست، به عنوان مثال، در HMIها و برنامه‌های تجسمی کاربردی استفاده‌شده برای روند پایش مستمر توسط پرسنل اجرایی، که برای مثال می‌تواند برای مراکز کنترل باشد. توصیه می‌شود برای چنین برنامه‌های کاربردی مخاطرات ناشی از نشست‌های بدون‌حضور در نظر گرفته شده و اقدامات متقابل مکمل اجرا گردد.

۱۱-۵-٦ محدودسازی زمان اتصال

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-٦ کنترل دسترسی برنامه‌های کاربردی و اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۱-۷ محاسبه سیار و دورکاری[1]

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۲ اکتساب، بهبود و نگهداری سامانه‌های اطلاعاتی

۱۲-۱ الزامات امنیتی سامانه‌های اطلاعاتی

۱۲-۱-۱ مشخصات و تحلیل الزامات امنیتی

کنترل زیربند ۱۲-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

1- Teleworking

اطلاعات بیشتر در مورد صنایع انرژی همگانی

جهت پشتیبانی از اکتساب سامانه‌های کنترل فرایند، مقاله BEDEW «الزامات برای سامانه‌های کنترل و مخابراتی امن» [۱] اقدامات امنیتی خاص سامانه کنترل اساسی را با مثال بیان می‌کند، که می‌تواند در آماده سازی سامانه مفید باشد. نگاشتی از کنترل‌های این مستند و الزامات BEDEW در پیوست ب موجود می‌باشد.

۱۲-۲ پردازش صحیح در برنامه‌های کاربردی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۲-۳ کنترل‌های رمزنگاری

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۲-٤ امنیت پرونده‌های سامانه[1]

۱۲-٤-۱ کنترل نرم‌افزار عملیاتی

کنترل زیربند ۱۲-۴-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

سازمان‌های صنایع انرژی همگانی توصیه می‌شود مخاطرات فساد سامانه‌های عملیاتی را با رعایت راهنماهای زیر کمینه نمایند (مدیریت تغییر):

الف- اگر تغییرات در برنامه‌های کاربردی و سامانه‌های مرکزی و هسته‌ای (برای مثال نرم افزارهای سامانه عملیاتی و سامانه عامل) سامانه‌های حساس اجرا شود، توصیه می‌شود آزمایش و آزمون‌های جامع و کامل در یک محیط خاص صورت گیرد که شبیه سامانه محیط عملیاتی و قابل تعامل با فرایندهای فیزیکی باشد. (طبق زیربند ۱۰-۱-۴، جداسازی توسعه، آزمون و امکانات عملیاتی).

ب- در مورد برنامه‌های کاربردی سامانه‌های کنترل فرآیند حساس، توصیه می‌شود کمینه سه نسل از نرم‌افزارها، مجموعه پارامترها و داده‌های پیکربندی مورد محافظت قرار گیرند.

۱۲-٤-۲ حفاظت از داده‌های آزمون سامانه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۲-٤-۳ کنترل دسترسی به کد منبع برنامه

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

1- System files

۱۲-۵ امنیت در فرایندهای بهبود و پشتیبانی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۲-۶ مدیریت آسیب‌پذیری فنی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۳ مدیریت رخدادهای امنیت اطلاعات

۱۳-۱ گزارش‌دهی وقایع و ضعف‌های امنیت اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۳-۲ مدیریت رخدادها و بهبودهای امنیت اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۴ مدیریت استمرار کسب وکار

۱۴-۱ جنبه‌های امنیت اطلاعات مدیریت استمرار کسب وکار

۱۴-۱-۱ لحاظ کردن امنیت اطلاعات در فرآیند مدیریت استمرار کسب وکار

کنترل زیربند ۱۴-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

توصیه می‌شود سازمان‌های صنایع انرژی همگانی استمرار تامین انرژی را به‌عنوان یکی از عناصر کلیدی مدیریت استمرار کسب‌وکار در نظر بگیرند. به همین دلیل، جنبه‌ها و روش‌های بازیابی برای مواقع اضطراری و بحران مربوطه موثر در سامانه کنترل فرایند، برای مثال توصیه می‌شود انکسارها، خرابی‌ها و نقص‌ها در نظر گرفته شوند.

۱۴-۱-۲ استمرار کسب وکار و ارزیابی ریسک

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۴-۱-۳ ایجاد و پیاده‌سازی طرح‌های استمرار در بر گیرنده امنیت اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۴-۱-۴ چارچوب طرح‌ریزی استمرار کسب وکار

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۴-۱-۵ حفظ و نگهداری آزمون و ارزیابی مجدد طرح‌های استمرار کسب وکار

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۴-۲ خدمات اضطراری اساسی[1]

یک هدف کنترلی اضافه بر از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، بند ۱۰، مدیریت استمرار کسب وکار به شرح زیر است:

هدف: جهت حصول اطمینان از در دسترس بودن خدمات اضطراری اساسی در مورد اختلالات عمده، بلایای طبیعی، حوادث یا سایر مواقع اضطراری گسترده.

۱۴-۲-۱ ارتباط اضطراری[2]

کنترل

توصیه می‌شود در صورت مشکلات عمده، بلایای طبیعی، حوادث یا هر گونه شرایط اضطراری و یا بروز حوادث، سازمان‌های صنایع انرژی اطمینان حاصل کنند که پیوندهای ارتباطی اساسی با کارکنان اضطراری خود و/یا باکارکنان اضطراری دیگر صنایع، با سامانه‌های کنترل اساسی و یا با سازمان‌های اضطراریِ خارجی برای حفاظت و رسیدگی یا بازیابی از چنین رخدادهایی، نگهداری می‌شود.

راهنمای پیاده‌سازی

پیوندهای ارتباطی اساسی ممکن است شامل انتقال صدا و داده‌ها و برای مثال همراه با موارد زیر باشد:

- کارکنان اجرایی در مناطق مرکزی و محیطی
- مدیریت بحران داخلی و خارجی
- ایستگاه‌های قدرت
- روش‌های اجرایی توزیع انرژی
- متصدی‌های سامانه‌های انتقال و توزیع
- سازمان‌های هواشناسی
- سازمان‌های پیشگیری از سیل
- سازمان‌های خدمات آتش نشانی
- سازمان‌های امداد رسانی

1- Essential emergency services
1- Emergency communication

- مقامات امنیتی
- ارائه دهندگان خدمات مخابراتی
- موسسات پزشکی
- سازمان‌های ملی یا محلی مسؤول رسیدگی خدمات عمومی

علاوه بر این، ممکن است ارتباطات اضطراری شامل پیوندهای داده‌ای زیر باشند:
- سامانه‌های کنترل اضطراری و مولفه‌های مرتبط
- هشدار اضطراری و سامانه‌های پایش و زیرمولفه‌های مرتبط

به‌خصوص در زمینه تامین انرژی، توصیه می‌شود تشخیص داده شود که پیوندهای ارتباطی که ممکن است برای بازسازی سامانه مورد نیاز باشد می‌تواند متکی به تامین قدرت برق باشد.

۱۵ انطباق

۱-۱۵ انطباق با الزامات قانونی

۱-۱-۱۵ شناسایی قوانین قابل اجرا

کنترل زیربند ۱-۱-۱۴ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، به شرح زیر تکمیل شده است:

راهنمای پیاده‌سازی خاص صنایع انرژی همگانی

الزامات خاص مربوط به بخش صنایع انرژی همگانی ممکن است شامل موارد زیر باشد:
- الزامات مربوط به عملیاتِ امن، ایمن و قابل اعتماد مولفه ها، سامانه‌ها و شبکه‌های تسهیلات انرژی
- الزامات مربوط به عدم تبعیض و تمرکز در بازارهای انرژی
- الزامات مربوط به حفاظت از زیرساخت‌های حیاتی
- قوانین ملی و بین‌المللی حافظت از داده‌ها
- سایر الزامات قانونی

در دوره سامانه‌های برنامه‌ریزی که دارای عمر خدمت طولانی باشند، توصیه می‌شود تغییرات قابل پیش بینی در الزامات تا حد ممکن در نظر گرفته شود، به طوری که این موارد را می‌توان با تلاش‌های اصلاحی قابل مدیریت پیاده‌سازی کرد.

۱۵-۱-۲ حقوق مالکیت فکری (IPR)[1]

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۵-۱-۳ حفاظت از سوابق سازمانی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۵-۱-٤ حفاظت داده‌ها و حریم خصوصی اطلاعات شخصی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۵-۱-۵ پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۵-۱-٦ مقررات کنترل‌های رمزنگاری

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی و انطباق فنی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

۱۵-۳ ملاحظات ممیزی سامانه‌های اطلاعاتی

اطلاعات اضافی خاص دامنه صنایع انرژی همگانی وجود ندارد.

1- Intellectual property rights

پیوست الف

(اطلاعاتی)

مجموعه کنترلی توسعه یافته صنایع انرژی همگانی

رده‌های امنیتی بخش خاص، اهداف کنترل و کنترل‌ها برای سامانه‌های کنترل فرآیند به‌کار گرفته در صنعت صنایع انرژی همگانی که در بندهای ۵ تا ۱۵ مندرج شده و آن‌هایی که در استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، شامل نشده اند در قالب مرور کلی فهرست شده است.

جدول الف- ۱- مرور کلی تکمیلی بر رده‌های امنیت و اهداف کنترل

زیربند	عنوان	اهداف کنترل	صفحه
۳-۹	امنیت در محل طرف‌های سوم	محافظت از تجهیزات واقع در خارج از سازمان صنایع انرژی همگانی در مقابل تهدیدات فیزیکی و زیست محیطی	۱۹
۱۱-۱۰	سامانه‌های قدیمی	محافظت در برابر مخاطرات ناشی از استفاده از سامانه‌های قدیمی، در جایی که اقدامات امنیتی لازم نمی‌توانند پیاده‌سازی شوند	۲۵
۱۲-۱۰	کارکردهای ایمنی	اطمینان از یکپارچگی و دسترس‌پذیری کارکردهای ایمنی	۲۶
۲-۱۴	خدمات اضطراری اساسی	جهت حصول اطمینان از در دسترس بودن خدمات اضطراری اساسی در مورد اختلالات عمده، بلایای طبیعی، حوادث یا سایر مواقع اضطراری گسترده	۳۲

جدول الف - ۲- مرور کلی کنترل‌های تکمیلی

زیربند	عنوان	اهداف کنترل	صفحه
۷-۱-۹	امن‌سازی مراکز کنترل	اقدامات لازم به منظور حصول اطمینان از امنیت فیزیکی مراکز کنترل، که در آن سامانه‌های کنترل مرکزی هم‌چون کارسازهای کنترل، HMI و سامانه‌های حمایتی کار گذاشته شده اند، توصیه می‌شود که طراحی شده، توسعه یافته و به‌کار گرفته شوند.	۱۴
۸-۱-۹	امن‌سازی اتاق‌های تجهیزات	توصیه می‌شود اقدامات لازم به منظور حصول اطمینان از امنیت فیزیکی اتاق تجهیزات که در آن امکانات سامانه کنترل به‌کار رفته در صنایع انرژی همگانی واقع شده است، طراحی و توسعه و پیاده‌سازی گردد.	۱۵
۹-۱-۹	امن‌سازی محل‌های جانبی	برای محل‌های جانبی که در آن اتاق تجهیزات سامانه کنترل به‌کار رفته در صنایع انرژی همگانی وجود دارد، توصیه می‌شود کنترل‌های امنیت فیزیکی طراحی، توسعه و پیاده‌سازی گردد.	۱۷
۱-۳-۹	تجهیزات مستقر در محل دیگر سازمان‌های	در جایی که سازمان‌های صنایع انرژی همگانی تجهیزات را خارج از محل خود نصب می‌نمایند که در منطقه‌ای با مسوولیت دیگر تسهیلات است، هم‌چون ایستگاه‌های اتصال متقابل برای نمونه، در این صورت توصیه می‌شود تجهیزات در یک منطقه حفاظت شده قرار گیرند طوری که هرگونه مخاطرات منتج از تهدیدات و خطرهای	۱۹

زیربند	عنوان	اهداف کنترل	صفحه
	صنایع انرژی همگانی	زیست محیطی کاهش یافته و امکان دسترسی‌های غیر مجاز به کمینه برسد.	
۹-۳-۲	تجهیزات مستقر در محل مشتری	زمانی که سازمان‌های صنایع انرژی همگانی تجهیزات خود را در محل مشتری نصب می‌نمایند، برای مثال، به منظور کنترل و اندازه‌گیری تامین انرژی و/یا تحویل خدمات اضافی، توصیه می‌شود تجهیزات سازمان از هر گونه مخاطرات ناشی از تهدیدات زیست محیطی محافظت شده و امکان دسترسی‌های غیر مجاز به آن کاهش یابد.	۲۰
۹-۳-۳	سامانه‌های کنترل و ارتباطی با اتصال متقابل	هنگامی که سامانه‌های کنترل و خطوط ارتباطی با طرف سوم خارجی متقابلا متصل هستند، توصیه می‌شود محدوده‌ی مسوولیت و واسطها با مشتری به روشنی تعریف شود، طوری که امکان قطع ارتباط و جداسازی هر سازمان از سایرین در مدت زمان مناسب به منظور جلوگیری از مخاطرات شناخته شده وجود داشته باشد.	۲۰
۱۰-۶-۳	امن‌سازی ارتباطات داده‌های کنترل فرایند	توصیه می‌شود اقدامات لازم جهت حصول اطمینان از محرمانه بودن، یکپارچگی و در دسترس‌پذیری ارتباطات داده‌های کنترل فرایندهای داخلی و خارجی مطابق با سطح حساسیت انتقال دادها طراحی و توسعه و پیاده‌سازی شوند.	۲۳
۱۰-۱۱-۱	طرزعمل سامانه‌های قدیمی	توصیه می‌شود کلیه فناوری‌های سامانه کنترل فرآیند قدیمی، سامانه‌ها و مولفه‌ها (از این پس به‌عنوان سامانه‌های قدیمی نامیده می‌شوند) به همراه آسیب پذیری‌های اطلاعات امنیتی شناخته شوند. توصیه می‌شود کنترل‌های مناسب به منظور کاهش کلیه مخاطرات شناخته شده در ارتباط با چنین سامانه‌هایی اجرا گردند.	۲۵
۱۰-۱۲-۱	یکپارچگی و دسترس‌پذیری کارکردهای ایمنی	توصیه می‌شود یکپارچگی و دسترس‌پذیری دارایی‌های اطلاعاتی، سامانه‌ها و مولفه‌ها و کارکردهایی که جهت حصول اطمینان از کارکردهای ایمنی مورد نیاز هستند، مطابق با استانداردهای خاص بخش و الزامات قانونی محافظت شوند.	۲۶
۱۱-۴-۸	اتصال منطقی سامانه‌های کنترل فرآیند بیرونی	قبل از سامانه‌های کنترل فرایند، توصیه می‌شود ارتباطات مرتبط با اشخاص بیرونی به وجود آیند، سازمان صنایع انرژی همگانی توصیه می‌شود اطمینان حاصل کند که تنها ارتباطات مجاز و جریان اطلاعات، شامل دستورات سامانه کنترل و پیغام‌ها بر روی یک پیوند می‌توانند تغییر یابند. توصیه می‌شود مخاطرات ناشی از چنین سامانه ارزیابی گردند.	۲۸
۱۴-۲-۱	ارتباط اضطراری	مشکلات عمده، بلایای طبیعی، حوادث یا هر گونه شرایط اضطراری و یا در صورت بروز حوادث، سازمان‌های تهسیلات انرژی توصیه می‌شود اطمینان حاصل کنند که پیوندهای ارتباطی ضروری با کارکنان اضطراری خود حفظ شده باشد، که با سامانه‌های کنترل ضروری و یا با سازمان‌های خارجی برای حفاظت یا بازیابی می‌تواند باشد.	۳۲

پیوست ب
(اطلاعاتی)
کمینه الزامات مستندسازی برای انتقال شواهد

انجمن آلمانی BEDEW[1] (انجمن آلمانی صنایع آب و انرژی) مقاله‌ی «الزامات برای سامانه‌های کنترل و مخابراتی امن» (مقاله BEDEW [۱]) توسعه داده که اقدامات امنیتی ضروری برای سامانه‌های مخابراتی و کنترلی برای دامنه کنترل فرآیند در صنعت صنایع انرژی همگانی را با نمونه نشان می‌دهد.

در جدول ب-۱ زیر نگاشتی از کنترل‌های بندهای ۵ تا ۱۵ از این مستند و الزامات مقاله BEDEW فهرست شده است.

لطفا توجه نمایید که مقاله BEDEW اساسا الزامات امنیتی برای سامانه‌ها و مولفه‌ها و فرایندهای توسعه و نگهداری متناظر را تعریف می‌کند. روش‌های اجرایی عملیاتی در دامنه صنایع انرژی همگانی مانند الزامات سازمانی یک سامانه مدیریت امنیت اطلاعات، در دامنه این مقاله نیست. علاوه بر این، رویکرد مقاله BEDEW با استانداردهای مجموعه خانواده ۲۷۰۰۰ تفاوت دارد. بنابراین، مقالهBEDEW که مورد ارجاع قرار گرفته است، ممکن است تنها قسمتی از جنبه‌های کنترل مربوطه از این مستند را پوشش دهد.

جدول ب-۱- نگاشت کنترل‌های استاندارد ملی و الزامات مقاله BEDEW

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
۵-۱-۱	مستند خط‌مشی امنیت اطلاعات		
۵-۱-۲	بازنگری خط‌مشی امنیت اطلاعات		
۶-۱-۱	تعهد مدیریتی به امنیت اطلاعات		
۶-۱-۲	هماهنگی امنیت اطلاعات		
۶-۱-۳	تخصیص مسوولیت‌های امنیت اطلاعات		
۶-۱-۴	فرآیند مجوزدهی برای امکانات پردازش اطلاعات		
۶-۱-۵	توافق‌نامه‌های محرمانگی	۲-۵-۲	انتقال و ذخیره امن داده‌ها
۶-۱-۶	برقراری ارتباط با مراجع دارای اختیار		
۶-۱-۷	برقراری ارتباط با گروه‌های با منافع خاص		
۶-۱-۸	بازنگری مستقل امنیت اطلاعات		
۶-۲-۱	شناسایی مخاطرات مرتبط با اشخاص بیرونی		
۶-۲-۲	نشانی‌دهی امنیت هنگام سرو کار داشتن با مشتریان		

1- Bundesverband der Energie- und Wasserwirtschaft

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
۶-۲-۳	نشانی‌دهی امنیت در توافق‌نامه‌های شخص سوم		
۷-۱-۱	لیست موجودی اموال	۲-۳-۱-۳	مستندسازی طراحی و پیکربندی شبکه
		۲-۶-۱	پشتیبان‌گیری: مفهوم، روش، مستندسازی، آزمون
۷-۱-۲	مالکیت دارایی‌ها		
۷-۱-۳	استفاده قابل قبول از دارایی‌ها		
۷-۲-۱	رهنمودهای طبقه‌بندی		
۷-۲-۲	برچسب‌گذاری و اداره‌کردن اطلاعات		
۸-۱-۱	نقش‌ها و مسولیت‌ها		
۸-۱-۲	گزینش		
۸-۱-۳	ضوابط و شرایط استخدام		
۸-۲-۱	مسوولیت‌های مدیریتی	۲-۲-۱-۲	مستندسازی متولی و کاربر
۸-۲-۲	هوشیاری، تحصیل و آموزش امنیت اطلاعات	۲-۲-۱-۲	مستندسازی متولی و کاربر
۸-۲-۳	فرآیند انضباطی		
۸-۳-۱	مسوولیت‌های پایان دهی[1]		
۸-۳-۲	بازگشت دارایی‌ها		
۸-۳-۳	حذف حقوق دسترسی	۲-۴-۱-۱	مدل دسترسی مبتنی بر نقش[2]
۹-۱-۱	حصار امنیت فیزیکی		
۹-۱-۲	کنترل‌های مدخل فیزیکی		
۹-۱-۳	امن‌سازی دفاتر، اتاق‌ها و امکانات		
۹-۱-۴	حفاظت در برابر تهدیدهای بیرونی و محیطی		
۹-۱-۵	کار در نواحی امن		
۹-۱-۶	نواحی دسترسی عمومی، نواحی تحویل و بارگیری		
۹-۱-۷	ایمن‌سازی مراکز کنترل		
۹-۱-۸	ایمن‌سازی اتاق‌های تجهیزات		
۹-۱-۹	ایمن‌سازی محل‌های جانبی		
۹-۲-۱	استقرار و حفاظت تجهیزات		
۹-۲-۲	امکانات پشتیبانی		
۹-۲-۳	امنیت کابل‌کشی		
۹-۲-۴	نگهداری تجهیزات		

1- Termination
2- Role-Based Access Model

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
۹-۲-۵	امنیت تجهیزات خارج از ابنیه اماکن سازمان		
۹-۲-۶	امحا یا استفاده مجدد از تجهیزات به صورت ایمن		
۹-۲-۷	خروج اموال		
۱۰-۱-۱	روش‌های اجرایی عملیاتی مستند شده	۲-۱-۲-۱	مستندسازی طراحی، مشخصات مولفه‌های مرتبط با امنیت و مشخصه‌های پیاده‌سازی
		۲-۲-۱-۲	مستندسازی متولی و کاربر
		۲-۲-۱-۳	مستندسازی پارامترهای امنیت و رویدادها یا هشدارهای رویداد نگاشت امنیت
		۲-۲-۱-۴	مستندسازی الزامات و فرضیات مورد نیاز برای عملیات سامانه ایمن
		۲-۶-۱	پشتیبان‌گیری: مفهوم، روش، مستندسازی، آزمون
۱۰-۱-۲	مدیریت تغییر	۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار[1]
		۲-۵-۵	پیکربندی و مدیریت تغییر، عقب گرد[2]
۱۰-۱-۳	تفکیک وظایف	۲-۴-۱-۱	مدل دسترسی مبتنی بر نقش
۱۰-۱-۴	تفکیک امکانات توسعه، آزمون و عملیاتی	۲-۵-۳	توسعه، آزمون و سامانه‌های مرحله‌ای[3]، وارسی‌های یکپارچگی ایمن
۱۰-۲-۱	تحویل خدمت		
۱۰-۲-۲	پایش و بازنگری خدمات طرف سوم	۲-۱-۱-۸	آزمون‌های داخلی و خارجی نرم‌افزار و امنیت و مستندسازی مرتبط
۱۰-۲-۳	مدیریت تغییرات در خدمات طرف سوم		
۱۰-۳-۱	مدیریت ظرفیت		
۱۰-۳-۲	پذیرش سامانه	۲-۱-۱-۸	آزمون‌های داخلی و خارجی نرم‌افزار و امنیت و مستندسازی مرتبط
		۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار
		۲-۵-۴	فرایندهای به روزرسانی و نگهداری ایمن
		۲-۵-۵	پیکربندی و مدیریت تغییر، عقب گرد
۱۰-۴-۱	کنترل‌هایی در برابر کدهای مخرب	۲-۲-۲	نرم‌افزار ضد ویروس

1- Release Processes

2- Rollback

3- Staging Systems

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
۱۰-۴-۲	کنترل‌هایی در برابر کدهای سیار	۲-۲-۲	نرم‌افزار ضد ویروس
۱۰-۵-۱	پشتیبان‌گیری اطلاعات	۲-۶-۱	پشتیبان‌گیری: مفهوم، روش، مستندسازی، آزمون
۱۰-۶-۱	کنترل‌های شبکه	۲-۳-۱-۱	فناوری‌های ارتباطی مستقرشده و پروتکل‌های شبکه
		۲-۳-۳	فناوری‌های بی‌سیم: الزامات امنیت و ارزیابی
۱۰-۶-۲	امنیت خدمات شبکه	۲-۳-۱-۲	طراحی شبکه ایمن
		۲-۳-۳	فناوری‌های بی‌سیم: الزامات امنیت و ارزیابی
		۲-۴-۳	پروتکل‌های برنامه‌های کاربردی
۱۰-۶-۳	ایمن‌سازی ارتباطات داده‌های کنترل فرایند	۲-۱-۱-۷	استانداردهای رمزنگاری
		۲-۳-۱-۱	فناوری‌های ارتباطی مستقرشده و پروتکل‌های شبکه
		۲-۳-۱-۲	طراحی شبکه ایمن
		۲-۴-۳	پروتکل‌های برنامه‌های کاربردی
۱۰-۷-۱	مدیریت رسانه برداشته شدنی		
۱۰-۷-۲	دفع رسانه		
۱۰-۷-۳	روش‌های اجرایی ساماندهی اطلاعات		
۱۰-۷-۴	امنیت مستندسازی سامانه		
۱۰-۸-۱	خط‌مشی‌ها و روش‌های اجرایی تبادل اطلاعات		
۱۰-۸-۲	موافقت نامه‌های تبادل	۲-۵-۲	انتقال و ذخیره ایمن داده‌ها
۱۰-۸-۳	رسانه فیزیکی در گذر	۲-۵-۲	انتقال و ذخیره ایمن داده‌ها
۱۰-۸-۴	پیام رسانی الکترونیکی	۲-۵-۲	انتقال و ذخیره ایمن داده‌ها
۱۰-۸-۵	سامانه‌های اطلاعاتی کسب وکار		
۱۰-۹-۱	تجارت الکترونیک		
۱۰-۹-۲	تراکنش‌های برخط	۲-۴-۲	اعتبارسنجی فعالیت‌ها در سطح کاربر و سامانه
۱۰-۹-۳	اطلاعات با دسترسی عمومی		
۱۰-۱۰-۱	رویدادنگاری ممیزی	۲-۴-۶	رویدادنگاری، دنباله‌های حسابرسی، مهرهای زمانی
۱۰-۱۰-۲	پایش کاربرد سامانه	۲-۴-۶	رویدادنگاری، دنباله‌های حسابرسی، مهرهای زمانی
۱۰-۱۰-۳	حفاظت از اطلاعات ثبت شده‌ی وقایع	۲-۱-۱-۶	رمزگذاری داده‌های حساس حین ذخیره‌سازی و انتقال
		۲-۴-۶	رویدادنگاری، دنباله‌های حسابرسی، مهرهای زمانی

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
۱۰-۱۰-۴	اطلاعات ثبت شده‌ی وقایع مربوط به راهبر و متصدی سامانه	۲-۴-۶	رویدادنگاری، دنباله‌های حسابرسی، مهرهای زمانی
۱۰-۱۰-۵	رویدادنگاری خرابی	۲-۴-۶	رویدادنگاری، دنباله‌های حسابرسی، مهرهای زمانی
۱۰-۱۰-۶	همزمان‌سازی ساعت‌ها	۲-۴-۶	رویدادنگاری، دنباله‌های حسابرسی، مهرهای زمانی
۱۰-۱۱-۱	طرز عمل با سامانه‌های قدیمی		
۱۰-۱۲-۱	یکپارچگی و دسترس‌پذیری کارکردهای ایمنی	۲-۳-۱-۱	فناوری‌های ارتباطی مستقرشده و پروتکل‌های شبکه
		۲-۳-۱-۲	طراحی شبکه ایمن
		۲-۵-۵	پیکربندی و مدیریت تغییر، عقب گرد
۱۱-۱-۱	خط‌مشی کنترل دسترسی		
۱۱-۲-۱	ثبت کاربر		
۱۱-۲-۲	مدیریت امتیاز		
۱۱-۲-۳	مدیریت رمز عبور کاربر		
۱۱-۲-۴	بازنگری حقوق دسترسی کاربر		
۱۱-۳-۱	استفاده از اسم‌رمز	۲-۴-۱-۲	احراز هویت کاربر و فرآیند ثبت ورود
۱۱-۳-۲	تجهیزات بدون مراقبت کاربر		
۱۱-۳-۳	خط‌مشی میز پاک و صفحه پاک		
۱۱-۴-۱	خط‌مشی استفاده از خدمات شبکه	۲-۳-۲-۱	دسترسی از راه دور ایمن
		۲-۳-۲-۲	فرایندهای نگهداری
۱۱-۴-۲	احراز اصالت کاربر برای اتصالات بیرونی	۲-۳-۲-۱	دسترسی از راه دور ایمن
		۲-۳-۲-۲	فرایندهای نگهداری
۱۱-۴-۳	شناسایی تجهیزات در شبکه‌ها		
۱۱-۴-۴	حفاظت از درگاه عیب‌یابی و پیکربندی راه دور	۲-۱-۱-۹	پیکربندی استاندارد ایمن، نصب و راه اندازی
		۲-۲-۱	سخت سازی سامانه
		۲-۳-۲-۱	دسترسی از راه دور ایمن
		۲-۳-۲-۲	فرایندهای نگهداری
۱۱-۴-۵	تفکیک در شبکه‌ها	۲-۳-۱-۱	فناوری‌های ارتباطی مستقرشده و پروتکل‌های شبکه
		۲-۳-۱-۲	طراحی شبکه ایمن
۱۱-۴-۶	کنترل اتصال به شبکه	۲-۳-۲-۱	دسترسی از راه دور ایمن
		۲-۳-۲-۲	فرایندهای نگهداری

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
۱۱-۴-۷	کنترل مسیریابی در شبکه	۲-۳-۱-۲	طراحی شبکه ایمن
		۲-۳-۲-۱	دسترسی از راه دور ایمن
۱۱-۴-۸	اتصال منطقی سامانه‌های کنترل فرآیند بیرونی	۲-۳-۱-۲	طراحی شبکه ایمن
		۲-۴-۳	پروتکل‌های برنامه‌های کاربردی
۱۱-۵-۱	روال‌های اجرایی برقراری ارتباط امن	۲-۲-۳	احراز هویت کاربر خودکار
		۲-۳-۲-۱	دسترسی از راه دور ایمن
		۲-۴-۱-۲	احراز هویت کاربر و فرآیند ثبت ورود
۱۱-۵-۲	شناسایی و احراز اصالت کاربر	۲-۲-۳	احراز هویت کاربر خودکار
		۲-۳-۲-۲	فرایندهای نگهداری
		۲-۴-۱-۲	احراز هویت کاربر و فرآیند ثبت ورود
۱۱-۵-۳	سامانه مدیریت اسم‌رمز	۲-۳-۱-۱	فناوری‌های ارتباطی مستقرشده و پروتکل‌های شبکه
		۲-۴-۱-۲	احراز هویت کاربر و فرآیند ثبت ورود
۱۱-۵-۴	استفاده از برنامه‌های کمکی سامانه	۲-۱-۱-۹	پیکربندی استاندارد ایمن، نصب و راه اندازی
		۲-۲-۱	سخت سازی سامانه
۱۱-۵-۵	خروج زمانی از لایه ارتباطی		
۱۱-۵-۶	محدودسازی زمان اتصال		
۱۱-۶-۱	محدودیت دسترسی اطلاعات	۲-۱-۱-۱	معماری سامانه ایمن
		۲-۴-۲	اعتبارسنجی فعالیت‌ها در سطح کاربر و سامانه
		۲-۴-۱-۱	مدل دسترسی مبتنی بر نقش
۱۱-۶-۲	جداسازی سامانه حساس	۲-۱-۱-۱	معماری سامانه ایمن
		۲-۳-۱-۱	فناوری‌های ارتباطی مستقرشده و پروتکل‌های شبکه
		۲-۳-۱-۲	طراحی شبکه ایمن
		۲-۳-۲-۱	دسترسی از راه دور ایمن
		۲-۳-۲-۱	دسترسی از راه دور ایمن
۱۱-۷-۱	ارتباطات و رایانش سیار	۲-۵-۲	انتقال و ذخیره ایمن داده‌ها
۱۱-۷-۲	دورکاری		
۱۲-۱-۱	مشخصات و تحلیل الزامات امنیتی	۲-۳-۳	فناوری‌های بی‌سیم: الزامات امنیت و ارزیابی
۱۲-۲-۱	اعتبارسنجی داده ورودی	۲-۴-۴	برنامه‌های کاربردی وب
		۲-۴-۵	وارسی یکپارچگی داده‌های مرتبط
۱۲-۲-۲	کنترل پردازش داخلی	۲-۴-۴	برنامه‌های کاربردی وب
		۲-۴-۷	خود-آزمون و رفتار سامانه
۱۲-۲-۳	یکپارچگی پیام	۲-۴-۳	پروتکل‌های برنامه‌های کاربردی

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
		۲-۴-۴	برنامه‌های کاربردی وب
		۲-۴-۵	وارسی یکپارچگی داده‌های مرتبط
۱۲-۲-۴	اعتبارسنجی داده خروجی	۲-۴-۴	برنامه‌های کاربردی وب
		۲-۴-۵	وارسی یکپارچگی داده‌های مرتبط
۱۲-۳-۱	خط‌مشی در استفاده‌ی کنترل‌های رمزنگاری	۲-۱-۱-۷	استانداردهای رمزنگاری
		۲-۳-۱-۱	فناوری‌های ارتباطی مستقرشده و پروتکل‌های شبکه
		۲-۳-۳	فناوری‌های بی‌سیم: الزامات امنیت و ارزیابی
		۲-۴-۳	پروتکل‌های برنامه‌های کاربردی
		۲-۵-۲	انتقال و ذخیره ایمن داده‌ها
۱۲-۳-۲	مدیریت کلیدی	۲-۱-۱-۷	استانداردهای رمزنگاری
۱۲-۴-۱	کنترل نرم‌افزار عملیاتی	۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار
		۲-۵-۲	انتقال و ذخیره ایمن داده‌ها
		۲-۵-۴	فرایندهای به روزرسانی و نگهداری ایمن
		۲-۵-۵	پیکربندی و مدیریت تغییر، عقب گرد
۱۲-۴-۲	حفاظت از داده‌های آزمون سامانه	۲-۱-۱-۹	پیکربندی استاندارد ایمن، نصب و راه اندازی
		۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار
۱۲-۴-۲		۲-۵-۳	توسعه، آزمون و سامانه‌های مرحله‌ای وارسی‌های یکپارچگی ایمن
۱۲-۴-۳	کنترل دسترسی به کد منبع برنامه	۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار
		۲-۵-۳	توسعه، آزمون و سامانه‌های مرحله‌ای وارسی‌های یکپارچگی ایمن
۱۲-۵-۱	روش‌های کنترل تغییر	۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار
		۲-۵-۴	فرایندهای به روزرسانی و نگهداری ایمن
		۲-۵-۵	پیکربندی و مدیریت تغییر، عقب گرد
۱۲-۵-۲	بازنگری فنی برنامه‌های کاربردی پس از تغییرات سامانه عملیاتی	۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار
		۲-۵-۴	فرایندهای به روزرسانی و نگهداری ایمن
۱۲-۵-۳	محدودیتها بر تغییرات در بسته‌های نرم‌افزاری	۲-۲-۱	سخت سازی سامانه
		۲-۵-۱	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
			و فرایندهای انتشار
۴-۵-۱۲	نشت اطلاعات		
۵-۵-۱۲	توسعه نرم‌افزار برون سپاری شده	۱-۱-۱-۲	معماری سامانه ایمن
		۵-۱-۱-۲	حمایت طرف سوم
		۸-۱-۱-۲	آزمونهای داخلی و خارجی نرم‌افزار و امنیت و مستندسازی مرتبط
		۱-۲-۱-۲	مستندسازی طراحی، مشخصات مولفه‌های مرتبط با امنیت و مشخصه‌های پیاده‌سازی
		۴-۴-۲	برنامه‌های کاربردی وب
		۱-۵-۲	استانداردهای توسعه‌ی ایمن، مدیریت کیفیت و فرایندهای انتشار
		۳-۵-۲	توسعه، آزمون و سامانه‌های مرحله‌ای وارسی‌های یکپارچگی ایمن
		۴-۵-۲	فرایندهای به روزرسانی و نگهداری ایمن
		۷-۵-۲	موافقت کد منبع
۱-۶-۱۲	کنترل آسیب پذیری‌های فنی	۲-۱-۱-۲	تماس با شخص
		۳-۱-۱-۲	سر هم بندی و مدیریت تکه
		۴-۱-۱-۲	تامین تکه‌های امنیتی برای کلیه مولفه‌های سامانه
		۵-۱-۱-۲	حمایت طرف سوم
		۶-۵-۲	درست کردن آسیب پذیری‌های امنیتی
۱-۱-۱۳	گزارش رویدادهای امنیت اطلاعات	۶-۵-۲	درست کردن آسیب پذیری‌های امنیتی
۲-۱-۱۳	گزارش ضعف امنیتی	۶-۵-۲	درست کردن آسیب پذیری‌های امنیتی
۱-۲-۱۳	مسوولیت‌ها و روش‌های اجرایی		
۲-۲-۱۳	یادگیری از رخدادهای امنیت اطلاعات		
۳-۲-۱۳	مجموعه شواهد		
۱-۱-۱۴	لحاظ کردن امنیت اطلاعات در فرآیند مدیریت استمرار کسب وکار		
۲-۱-۱۴	استمرار کسب وکار و ارزیابی ریسک		
۳-۱-۱۴	ایجاد و پیاده‌سازی طرح‌های استمرار در بر گیرنده امنیت اطلاعات	۱-۶-۲	پشتیبان‌گیری: مفهوم، روش، مستندسازی، آزمون
		۲-۶-۲	بازیابی فاجعه

کنترل استاندارد ملی		الزامات مقاله BEDEW [۱]	
شماره	عنوان	شماره	عنوان
۴-۱-۱۴	چارچوب طرح‌ریزی استمرار کسب وکار	۲-۶-۲	بازیابی فاجعه
۵-۱-۱۴	حفظ و نگهداری آزمون و ارزیابی مجدد طرح‌های استمرار کسب وکار	۲-۶-۲	بازیابی فاجعه
۱-۲-۱۴	ارتباط اضطراری		
۱-۱-۱۵	شناسایی قوانین قابل اجرا		
۲-۱-۱۵	حقوق مالکیت فکری (IPR)		
۳-۱-۱۵	حفاظت از سوابق سازمانی	۶-۱-۱-۲	رمزگذاری داده‌های حساس در حین ذخیره‌سازی و انتقال
		۶-۴-۲	رویدادنگاری، دنباله‌های حسابرسی، مهرهای زمانی
۴-۱-۱۵	حفاظت از داده‌ها و حریم خصوصی اطلاعات شخصی	۶-۱-۱-۲	رمزگذاری داده‌های حساس در حین ذخیره‌سازی و انتقال
۵-۱-۱۵	پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات		
۶-۱-۱۵	مقررات کنترل‌های رمزنگاری	۷-۱-۱-۲	استانداردهای رمزنگاری
۱-۲-۱۵	انطباق با خط‌مشی‌های امنیتی و استانداردها		
۲-۲-۱۵	وارسی انطباق فنی		
۱-۳-۱۵	کنترل‌های حسابرسی سامانه‌های اطلاعاتی		
۲-۳-۱۵	حفاظت از ابزارهای حسابرسی سامانه‌های اطلاعاتی		

کتاب‌نامه

[1] IEC/TS 62443-1-1 Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models

[2] BDEW Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW German ssociation of Energy and Water Industries): Whitepaper “Requirements for Secure Control and Telecommunication Systems” http://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/2008-06-10_Whitepaper_Sichere%20Steuerungs-_Telekommunikationssysteme.pdf

[3] US Department of Homeland Security: Cyber Security Procurement Language for Control Systems

[4] NIST: SP 800-82 Guide to Industrial Control Systems (ICS) Security

[5] DIN SPEC 27009:2012-04 Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002