



تعیین جایگاه الزامات استانداردهای سیستمی مطرح مؤلفه‌های مدیریت نگهداری و تعمیرات

محمدحسین کریمی گوارشکی^۱، استادیار و عضو هیئت علمی، جعفر قیدر خلجانی^۲، استادیار و عضو هیئت علمی، حسین بیگیان^۳،

دانشجوی دکتری مهندسی صنایع

۱- مجتمع مدیریت و فناوری‌های نرم- دانشگاه صنعتی مالک اشتر- تهران- ایران

mh_karimi@aut.ac.ir

۲- مجتمع مدیریت و فناوری‌های نرم- دانشگاه صنعتی مالک اشتر- تهران- ایران

kheljani@aut.ac.ir

۳- مجتمع مدیریت و فناوری‌های نرم- دانشگاه صنعتی مالک اشتر- تهران- ایران

prqinfo@yahoo.com

کیفیت ISO9001:2008 (بند ۶.۳) و مدیریت امنیت اطلاعات ISO 27001:2005 (ISMS) به بررسی نقش استانداردهای مدیریتی در حوزه مدیریت نگهداری و تعمیرات بپردازد. شناخت صحیح استانداردهای سیستمی به همراه درک صحیح این ارتباطات می‌تواند به مدیران حوزه نت در به‌کارگیری هر یک از الزامات استانداردهای سیستمی به‌منظور افزایش اثربخشی و کارایی حوزه مدیریتی خود کمک شایان توجهی نماید. نگارندگان بر آنند تا در پژوهش‌های آتی مدل کاربردی مدیریت نگهداری و تعمیرات را مبتنی بر این استانداردها در سازمان‌های فن‌آور ارائه نمایند.

چکیده: در دنیای امروز استاندارد و توجه به آن امری ضروری به نظر می‌رسد. مدیریت نگهداری و تعمیرات نیز از این قاعده مستثنا نیست. استانداردهای مرتبط با حوزه نگهداری و تعمیرات به دلیل نقش بارزی که در فعالیت‌های مرتبط با این حوزه دارند، یکی از بارزترین عناصر مفهومی سازمان به شمار می‌روند. در این راستا با توجه به شرایط خاص سازمان هدف، در یک مطالعه توصیفی، بخشی از استانداردهای مرتبط با حوزه مدیریت نگهداری و تعمیرات ملی- بین‌المللی جمع‌آوری و مورد بررسی قرار گرفتند. مقاله حاضر بر آن است با معرفی چهار استاندارد سیستم مدیریت دارایی ISO 55000:2014، مدیریت قابلیت اعتماد بر مبنای سری استاندارد IEC 60300:2003، مدیریت



۱. مقدمه

امروزه مباحث نگهداری و تعمیرات یکی از مباحث مهم در صنایع می‌باشد و با توجه به محدودیت منابع اعم از انرژی، نیروی انسانی و سرمایه، با برنامه‌ریزی صحیح و اجرای اصولی آن‌ها می‌توان موجبات افزایش بهره‌وری و کار آیی تجهیزات را محقق نمود [05,06]. نقش استانداردهای ملی و بین‌المللی در حوزه‌های نگهداری و تعمیرات همواره نقشی اساسی بوده است. شناخت صحیح این نقش از اهداف این مقاله می‌باشد. این بخش حاوی خلاصه مدونی از مقاله‌ها، فصلنامه‌ها، کتاب‌ها و دیگر مستندات است که وضعیت گذشته و حال اطلاعات موضوع پژوهش را توصیف می‌کند.

۱- مروری بر استانداردهای سیستمی در حوزه نگهداری و تعمیرات

۱-۱ استاندارد سیستم مدیریت دارایی ISO 55000:2014
۲-۱ سیستم مدیریت قابلیت اعتماد بر مبنای سری استاندارد IEC 60300:2003

۳-۱ سیستم مدیریت کیفیت ISO9001:2008 (بند ۶.۳)
سیستم مدیریت امنیت اطلاعات (INFORMATION SECURITY MANAGEMENT SYSTEM – ISMS) ISO 27001:2005

هر یک از استانداردهای معرفی شده در بالا به صورت مختصر توضیح داده می‌شود:

۱-۱ استاندارد سیستم مدیریت دارایی ISO 55000:2014

ISO 55000:2014 جدیدترین استاندارد سازمان جهانی، یک مرور کلی از مدیریت دارایی‌ها، اصول و اصطلاحات و منافع مورد انتظار از اتخاذ مدیریت دارایی را فراهم می‌کند و می‌تواند برای تمام انواع دارایی‌ها و با هر نوع و اندازه از سازمان استفاده شود. این استاندارد توسط کمیته فنی ISO/PC 251 تهیه و ارائه شده است. همخوانی این استاندارد با بند ۶ استاندارد ISO 9001:2008 باعث استقبال زیاد افراد از این استاندارد شده است. این همخوانی می‌تواند مدیریت یکپارچه‌ای با تلفیق استاندارد ISO 9001 و ISO 55000 به وجود آورد [01].

این استاندارد تحت عنوان سیستم مدیریت دارایی و در سه نسخه به شرح زیر منتشر شده است:

• ISO 55000 اصول و واژگان سیستم مدیریت دارایی

• ISO 55001 الزامات سیستم مدیریت دارایی

• ISO 55002 راهنمای پیاده‌سازی سیستم مدیریت دارایی

ایزو ۵۵۰۰۱، ایزو ۵۵۰۰۲ و استاندارد بین‌المللی حاضر را می‌توان همراه با سایر راهنماهای فنی و استانداردهای مدیریت دارایی‌های مرتبط با انواع دارایی‌ها یا بخش‌های مختلف صنعت استفاده کرد. ایزو ۵۵۰۰۱ الزامات سیستم مدیریت دارایی‌ها را مشخص می‌کند، درحالی‌که سایر استانداردها جزئیات الزامات فنی فعالیت‌های مختلف، صنایع مختلف یا دارایی‌های مختلف را مطرح می‌کنند یا رهنمودهایی درباره‌ی نحوه‌ی تفسیر و اجرای ایزو ۵۵۰۰۱ در یک صنعت خاص یا برای یک نوع خاص از دارایی‌ها ارائه می‌کنند.

دامنه کاربرد مدیریت دارایی:

ایزو ۵۵۰۰۱، ایزو ۵۵۰۰۲ و استاندارد بین‌المللی حاضر را می‌توان همراه با سایر راهنماهای فنی و استانداردهای مدیریت دارایی‌های مرتبط با انواع دارایی‌ها یا بخش‌های مختلف صنعت استفاده کرد. ایزو ۵۵۰۰۱ الزامات سیستم مدیریت دارایی‌ها را مشخص می‌کند، درحالی‌که سایر استانداردها جزئیات الزامات فنی فعالیت‌های مختلف، صنایع مختلف یا دارایی‌های مختلف را مطرح می‌کنند یا رهنمودهایی درباره‌ی نحوه‌ی تفسیر و اجرای ایزو ۵۵۰۰۱ در یک صنعت خاص یا برای یک نوع خاص از دارایی‌ها ارائه می‌کنند.

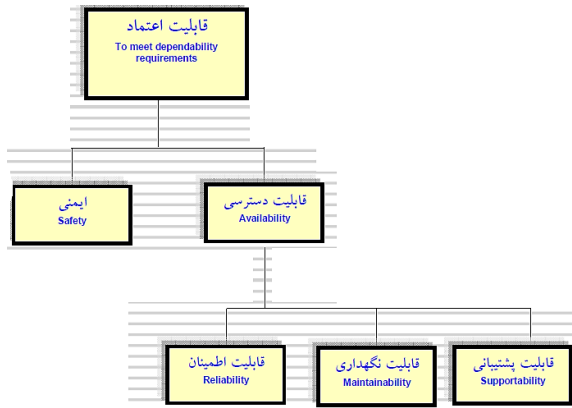
عناوین هفت‌گانه الزام سیستم مدیریت دارایی در ISO55000 عبارتند از: زمینه کاری سازمان، رهبری، برنامه‌ریزی، پشتیبانی، عملیات، ارزیابی عملکرد و بهبود.

مزایای استاندارد ISO55000:2014

بهره‌گیری از ایزو ۵۵۰۰۲، به سازمان امکان می‌دهد تا از طریق مدیریت مؤثر و کارآمد دارایی‌هایش، به اهداف عینی خود دست یابد. استفاده از سیستم مدیریت دارایی‌ها تضمین می‌کند که این اهداف عینی به صورت پایدار و سازگار در طی زمان قابل تحقق هستند. وزارت نفت در سال ۱۳۹۳ نظامنامه راهبردی مدیریت دارایی‌های فیزیکی صنعت نفت PHYSICAL ASSET MANAGEMENT خود را بر اساس این استاندارد طراحی و به موردا اجرا گذاشته است [10].

محدودیت‌های کلی آن نیز به شرح زیر می‌باشد:

▪ همانند (PAS 55) وارد جزئیات و نحوه اجرا نشده و کاربردی نیست.



شکل (۱): سیستم مدیریت قابلیت اعتماد

در صورتی یک سیستم دارای شرایط زیر باشد می‌توان گفت که سیستم قابلیت اطمینان دارد:

• قابلیت دسترسی: احتمال اینکه بتواند کار مشخص شده را در شرایط و زمان تعیین شده انجام دهد.

• قابلیت نگهداری و تعمیر پذیری: احتمال اینکه یک عمل یا اعمال مشخص تعمیرات برای یک موجود تحت شرایط معین در مدت‌زمان معین انجام شود، به شرط اینکه در زمان صفر خراب نباشد. مقصود از موجود یعنی هر چیزی که به صورت مجرد و فردی در واقعیت وجود داشته باشد و یا اینکه بتوان در ذهن تصور کرد که وجود دارد.

• قابلیت اعتماد Reliability

• قابلیت دوام و استفاده

• قابلیت ایمنی Safety

این قابلیت‌ها تحت اصطلاح RAMS در سطح بین‌المللی شناخته می‌شوند. سیستم مدیریت قابلیت اطمینان به عنوان یک رویکرد مدیریتی - سیستمی توسط موسسه بین‌المللی IEC به شکل سری استانداردهای IEC 60300-2003 معرفی و ارتقاء رضایت مشتری، کارایی و بهبود عملکرد مستمر سازمان را با تمرکز بر چهار مشخصه RMAًS دنبال می‌کند.

۱-۳ سیستم مدیریت کیفیت ISO9001:2008 [03]

استانداردهای سری ۹۰۰۰ استانداردهای مدیریتی هستند که مبانی یک سامانه مدیریت کیفیت را بیان می‌کنند (شکل (۲)). به عبارت دیگر استانداردهای سری ایزو ۹۰۰۰ استاندارد محصول نیستند ولی راهکارهای اجرایی برای رسیدن به کیفیت مناسب محصولات و رضایت مصرف‌کننده ارائه می‌کند.

استانداردهای سری ISO9000 کاملاً عمومی بوده و در تمام بخش‌های صنعت و خدمات قابل پیاده‌سازی است. از بین

▪ مشخص نشده است که ارزیابی انطباق چگونه باید انجام گیرد.

▪ بیشتر به استانداردهای دیگر ارجاع شده است مانند استاندارد ریسک ISO 31000 و خود استاندارد جامع و فراگیر نمی‌باشد.

۱-۲ سیستم مدیریت قابلیت اعتماد بر مبنای سری استاندارد IEC 60300:2003 [02]

قابلیت اعتماد مطابق با استاندارد ISO 9000:2005 واژه کلی برای توصیف عملکرد مربوط به قابلیت دسترسی* و عوامل تأثیرگذار بر آن در یک سیستم یعنی قابلیت اطمینان[†] و قابلیت نگهداری و تعمیرات[‡] است. مدیریت قابلیت اعتماد به عنوان یک رویکرد دستگاهی، بخشی از فعالیت‌های مدیریتی است که عملکرد سازمان را در مباحث قابلیت اطمینان، دسترس‌پذیری، قابلیت نگهداری و تعمیرات، ایمنی (RAMS) به منظور حصول اطمینان از کارایی و توانمندی فرآیندهای عملیاتی و تجهیزات و محصولات مورد توجه قرار می‌دهد و بهبود مستمر آن را میسر می‌سازد [08].

این استاندارد مبانی سیستم‌های مدیریت قابلیت اعتماد را تشریح می‌کند و اصول کلی را فراهم می‌آورد برای سازمان‌هایی که قصد دارند:

الف- یک سیستم مدیریت قابلیت اعتماد برای دستیابی به اهداف قابلیت اعتماد محصول ایجاد نمایند.

ب- نیازها و انتظارات قابلیت اعتماد مشتری و چگونگی برآورده شدن آن‌ها را تعیین نمایند.

ج- در توسعه طرح‌های قابلیت اعتماد کمک بگیرند.

د- اثربخشی سیستم مدیریت قابلیت اعتماد را اندازه‌گیری نمایند و بهبود دهند.

ه- ارتباطات فعالیت‌های قابلیت اعتماد را تسهیل نمایند.

قابلیت اطمینان معمولاً برای بیان درجه‌ی اطمینان از کارکرد صحیح یک قطعه یا به‌طور کلی مجموعه‌ای از عوامل در طی مدت‌زمان و دوره‌ی زمانی مشخص به کار می‌رود [07]؛ اما توجه به این نکته ضروری است که اگر قطعه‌ای خراب شود، بدین معنا نیست که لزوماً غیرقابل اعتماد است. تمامی روابط قابلیت اطمینان، بر پایه‌ی احتمالات بنا شده و برای شرایط عدم قطعیت محاسبه شده است؛ که در شکل (۱) نمایش داده شده است.

* Availability

† Reliability

‡ Maintainability

۴-۱ سیستم مدیریت امنیت اطلاعات (INFORMATION SECURITY MANAGEMENT SYSTEM – ISMS)
[04] ISO 27001:2005

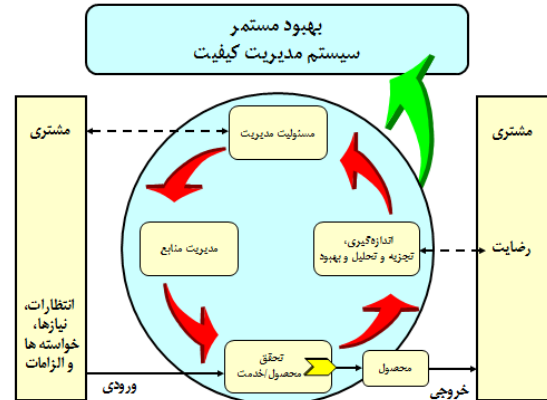
توجه روز افزون به مباحث مدیریت امنیت اطلاعات از طریق برقراری قوانین و ضوابط ملی / منطقه ای / بین‌المللی و همچنین توجه به راهبرد های جدید به منظور پاسخگویی به انتظارات و الزامات طرف های ذینفع نسبت به اطمینان از امنیت و ایمنی شبکه ها و سیستم های اطلاعاتی، باعث پدید آمدن استاندارد هایی برای استقرار سیستم های مدیریت امنیت اطلاعات شده است.

بدیهی است که استاندارد سازی در سطح بین‌المللی، برای مدیریت امنیت اطلاعات و پدیدآوری رویکردی مشابه و حتی الامکان یکسان، به منظور جلوگیری از نقص امنیت اطلاعات و اتلاف مالی و پیشگیری از تنش های منتج از این موضوع در درون سازمان ها و یا در درون زنجیره های تامین می باشد. اطلاعات کلید رشد و موفقیت یک سازمان است. سیستم مدیریت امنیت اطلاعات ثبت شده، به سازمان اطمینان خواهد داد که اطلاعات سازمان – چه در ثبت الکترونیک و چه بر روی کاغذ و یا در اذهان کارکنان- به نحو مناسب حفاظت شده است.

سیستم مدیریت امنیت اطلاعات سازمان را در شناسایی و کاهش ریسک های بحرانی امنیتی، از طریق تمرکز بر تلاشهایی جهت امنیت اطلاعات و حفاظت از آنها، یاری می نماید. کشف نقاط قوت، نقاط ضعف و فرصتهای بهبود در مدیریت ریسک های امنیتی امری حیاتی است. با رویکرد Risk Based، ممیزان قادر به ارزیابی میزان پشتیبانی سیستم مدیریت امنیت اطلاعات سازمان در زمینه هایی که دارای اهمیت بیشتر برای سازمان هستند خواهند بود و بدین وسیله میزان تطابق این سیستم را با استاندارد انتخاب شده تعیین خواهند نمود.

امنیت اطلاعات چیزی بیش از تکنولوژی اطلاعات است. با استفاده از سیستم مدیریت امنیت اطلاعات می توان، از کار صحیح بر اطلاعات سازمان با وجود جلوگیری از نشر اطلاعات اطمینان یابد.

استانداردهای خانواده ۹۰۰۰ تنها استاندارد ISO 9001 دارای گواهینامه می‌باشد و سایر استانداردها نقش راهنما را دارد.



شکل (۲): یک سامانه مدیریت کیفیت

استاندارد ISO 9001:2008 تفاوت ساختاری زیادی با ویرایش ۲۰۰۰ آن نداشت و بیشتر به شفاف‌سازی الزامات ۹۰۰۱ پرداخته است.

اما یکسری الزامات مانند لزوم کالیبراسیون نرم‌افزارهای پایش و اندازه‌گیری، تغییرات در پایش فرآیندها، تغییر در هرم مستندات، اضافه کردن ارزیابی اثربخشی سیستم کیفیت در اقدامات اصلاحی و پیشگیرانه و ... به آن اضافه‌شده بود. این استاندارد در حال حاضر به‌طور گسترده‌ای در جهان مورداستفاده قرار می‌گیرد بر اساس بعضی آمارها بین ۹۵۰۰۰۰ تا یک‌میلیون گواهینامه تا سال ۲۰۱۰ در جهان صادرشده است.

برخی از مزایای مهم استاندارد ایزو ۹۰۰۱ عبارتند از:

- ایجاد اطمینان در مشتریان
- بهبود ارتباطات درون سازمانی
- بهبود عملکرد و افزایش بهره‌وری
- عملکرد سیستماتیک و قابل پیش‌بینی
- ایجاد کنترل بیشتر بر فرآیندهای سازمان
- کاهش میزان شکایات مشتریان و محصول
- گسترش فرهنگ سازی و تفکر سیستماتیک
- کاهش ضایعات و دوباره کاری‌ها در خط تولید
- اصلاح خطاها و پیشگیری از وقوع مجدد آن‌ها



▪ طبقه بندی انواع تهدیدهای امنیتی

تهدیداتی که ممکن است در مورد امنیت اطلاعات رخ دهد از نظر منبع وقوع در دو گروه تقسیم بندی می‌شوند که در جدول (۱) قابل مشاهده است و کلیه تصمیم‌گیری‌ها در خصوص الزامات امنیتی در سازمان باید با در نظر گرفتن تمامی این تهدیدات و تمامی جنبه‌های مربوط به آن‌ها شناسایی و کلیه حفاظ‌هایی که در سازمان پیاده‌سازی می‌شود باید مطابق با این الزامات انتخاب گردد:

جدول (۱): طبقه‌بندی انواع تهدیدهای امنیتی

تهدیدات با ریشه محیطی	تهدیدات با ریشه انسانی	
	خرابکاری	تصادفی
زلزله	دزدی	خطاها و اشتباهات فردی
رعد و برق	استراق سمع	پاک شدن فایل‌ها
سیل	دستکاری اطلاعات	مسیریابی اشتباه (در شبکه)
آتش سوزی	هک کردن سیستم	حوادث فیزیکی
	کدهای مخرب (ویروس‌ها و ...)	

با توجه به موارد فوق و طیف گسترده تهدیداتی که سازمان در معرض آن‌ها قرار دارد، وجود یک سیستم امنیت اطلاعات مدرن، به روز، پویا و رو به بهبود برای کمک به نیل به اهداف متعالی سازمان، بسیار لازم و ضروری است.

هدف سیستم ISMS فراهم آوردن مدلی برای ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری و بهبود یک سیستم مدیریت امنیت اطلاعات است. پذیرش این سیستم برای سازمان یک تصمیم استراتژیک است.

با به‌کارگیری یک سیستم مدیریت شما می‌توانید امنیت اطلاعات خود را پایه‌گذاری، استقرار، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود دهید. شما ابزاری برای شناسایی دارایی‌های بحرانی و حفاظت آن‌ها خواهید داشت. هم‌زمان با ایجاد اطمینان در مدیران، کارکنان و درنهایت جامعه، موجب تقویت سازمان خود در دستیابی به اهداف استراتژیک خواهید داشت.

حال با توجه به موارد امنیتی و همچنین چالش موجود در مدیریت دانش در حوزه نت در محیط سازمان هدف، آیا محدودیت‌های امنیتی و چالش‌های مرتبط با عدم رسوب دانش کارکنان حوزه نت در فرآیند رهاسازی آن‌ها از سازمان (مانند

موج بازنشستگی‌های زودتر از موعد) در حوزه دارایی‌های فیزیکی را به کمک این استاندارد می‌توان مدیریت نمود و از این استاندارد به‌طور مؤثر در مدل مدیریت نگهداری و تعمیرات موضوع این پژوهش استفاده کرد. در طول پژوهش سعی بر دست یافتن به پاسخ این دغدغه برای سازمان هدف است. این موضوع با توجه به رویکرد شبکه بزرگ تأمین‌کنندگان حوزه نت می‌تواند از اهمیت خاصی برخوردار گردد.

۲- نتیجه‌گیری

شناخت صحیح مدیران از استانداردهای حوزه مدیریت نگهداری و تعمیرات موجبات ارتقاء سیستم نگهداری و تعمیرات را به دنبال داشته و به تحقق مأموریت مدیران حوزه نت مبنی بر بهینه‌کردن توانایی‌های ماشین‌آلات کمک شایانی می‌نماید. به‌منظور رسیدن به حداکثر تولید و کاهش فرسایش و خرابی آن‌ها برای داشتن حداکثر راندمان تجهیزات و دستیابی به بیشترین سود با کمترین هزینه فراهم می‌کند. با توجه به بهبودهای حاصل از به‌کارگیری استانداردهای مطرح در این مقاله شامل: استاندارد سیستم مدیریت دارایی ISO 55000:2014، سیستم مدیریت قابلیت اعتماد بر مبنای سری استاندارد IEC 60300:2003، سیستم مدیریت کیفیت ISO 9001:2008 (بند ۶.۳) و سیستم مدیریت امنیت اطلاعات ISO 27001:2005، پیش‌بینی می‌شود که هزینه‌های موردنیاز جهت طراحی و پیاده‌سازی این استانداردها در سازمان‌های مورد مطالعه، بسیار کمتر از خسارات ناشی از عدم رعایت الزامات این استانداردها باشد. در نتیجه سرمایه‌گذاری در این زمینه توجیه اقتصادی قابل قبولی خواهد داشت.

در خاتمه جدول (۲) ارتباط بین استانداردهای سیستمی با ابعاد، مؤلفه‌ها و زیر مؤلفه‌های یک مدل مدیریت نگهداری و تعمیرات [09] را نشان می‌دهد. شناخت صحیح از استانداردهای سیستمی و درک صحیح این ارتباطات می‌تواند به مدیران حوزه نت در به‌کارگیری هریک از الزامات استانداردهای سیستمی به‌منظور افزایش اثربخشی و کارایی حوزه مدیریت خود کمک شایان توجهی نماید. نگارنده بر آن است تا در پژوهش‌های آتی مدل کاربردی مدیریت نگهداری و تعمیرات مبتنی بر این استانداردها در سازمان‌های فن‌آور ارائه نماید.



۳- مراجع

جدول (۲): ارتباط بین استانداردها و ابعاد یک مدل نت

- [01] ISO 55000, 55001, 55002
 [02] RCM II & IEC 60300
 [03] ISO 9001:2008
 [04] ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements
 [05] EN 13306:2010, Maintenance Terminology. European Standard. CEN (European Committee for Standardization), Brussels
 [06] Maintenance management: literature review and directions Amik Garg and S.G. Deshmukh Mechanical Engineering Department, Indian Institute of Technology Delhi, New Delhi, India- Journal of Quality in Maintenance Engineering Vol. 12 No. 3, 2006 pp. 205-238
 [07] Moubray, J. “Reliability Centered Maintenance”, Butterworth-Heinemann, 1997.
 [08] - T.Wireman, preventive maintenance. : industrial press, 2008.
 [09] مطالعه تطبیقی مدل‌های مدیریت نگهداری و تعمیرات دکتر محمد گوارشکی) - دکتر حسین کریمی (استادیار دانشگاه صنعتی مالک اشتر خلیجانی (استادیار دانشگاه صنعتی مالک اشتر) - حسین بیگیان (۱۳۹۵) دانش آموخته دکتری مهندسی صنایع دانشگاه صنعتی مالک اشتر)
 [10] نظامنامه راهبردی مدیریت دارایی‌های فیزیکی صنعت نفت
 سند: MOP-DSM-002 سال ۱۳۹۳ تهیه‌کننده مدیر کل راهبری نگهداری و تعمیرات صنعت نفت

ردیف	ابعاد	مولفه‌ها	زیر مولفه‌ها	استانداردهای مدیریتی (مدل نت)
۱	زیمنه	استراتژی	چشم انداز	ISO 27001
۲			خط مشی	ISO 9001
۳			اهداف	IEC 60300
۴			تعهد مدیریت	ISO 55000
۵			منابع انسانی	مدیریت دانش
۶		مراقبت‌های پایه	سیستم‌های انگیزشی	ISO 9001
۷			صلاحیت، آموزش و آگاهی	IEC 60300
۸			ساختار سازمانی	ISO 55000
۹			چند مهارتی کردن کارکنان	ISO 27001
۱۰			نگهداری پیشگیرانه	ISO 9001
۱۱			کالیبراسیون	IEC 60300
۱۲		طرح ریزی تحقق فرآیند نت	اقدام فوری برای رفع مشکلات تجهیزات (RCA)	ISO 55000
۱۳			طرح ریزی تحقق فرآیند نت	ISO 9001
۱۴		تأسیک‌ها	ایجاد نظام دستورکار و گزارش‌گیری	IEC 60300
۱۵			مدیریت تغییر	ISO 27001
۱۶			نت پیشگویانه	ISO 9001
۱۷		تأمین	نت پیش اقدام	ISO 27001
۱۸	ت براساس وضعیت CBM		IEC 60300	
۱۹	نگهداری کیفی		ISO 55000	
۲۰	پیشگیری از نگهداری MP		ISO 27001	
۲۱	استانداردهای مدیریتی	مدیریت موجودی (نگهداری، جابجایی، انبارش) / مدیریت زنجیره تأمین / مدیریت تجهیزات و فرآیندهای ویژه پروتسپاری شده	ISO 14224	ISO 27001
۲۲			AS 9100	ISO 9001
۲۳			ISO 14000	IEC 60300
۲۴			OHSAS 18000	ISO 55000
۲۵			ISO 55000	ISO 27001
۲۶	یادافند غیرعامل	کاهش آسیب پذیری ها، افزایش بایاداری ملی / تداوم فعالیت تجهیزات / تسهیل مدیریت بحران در مقابل تهدیدات	IEC 60300-3-11	ISO 27001
۲۷			خط مشی امنیتی	ISO 9001
۲۸			امنیت فیزیکی و محیطی	IEC 60300
۲۹	مدیریت داده‌ها	مدیریت ارتباطات و عملیات / مدیریت حوادث امنیتی اطلاعات / امنیت منابع انسانی و تأمین کنندگان اطلاعاتی	مدیریت ارتباطات و عملیات	ISO 27001
۳۰			مدیریت حوادث امنیتی اطلاعات	ISO 9001
۳۱			امنیت منابع انسانی و تأمین کنندگان اطلاعاتی	IEC 60300
۳۲			امنیت داده‌ها	ISO 55000
۳۳	مدیریت اندازه‌ها	تدوین شاخص‌های کلیدی KPI / مدیریت ارزیابی و نظارت بر تأمین کنندگان / بکارگیری کارت امتیازی متوازن BSC / جلسات بازنگری مدیریت / اندازه‌گیری شاخص‌ها / تحلیل داده‌ها	CMMS	ISO 27001
۳۴			شناسایی و کدننگ	ISO 9001
۳۵			ولایت بندی دارایی‌ها براساس مأموریت	IEC 60300
۳۶			استقرار ERP	ISO 55000
۳۷			تدوین شاخص‌های کلیدی KPI	ISO 27001
۳۸			مدیریت ارزیابی و نظارت بر تأمین کنندگان	ISO 9001
۳۹	TPM	بکارگیری کارت امتیازی متوازن BSC / جلسات بازنگری مدیریت / اندازه‌گیری شاخص‌ها / تحلیل داده‌ها	بکارگیری کارت امتیازی متوازن BSC	IEC 60300
۴۰			جلسات بازنگری مدیریت	ISO 55000
۴۱			اندازه‌گیری شاخص‌ها	ISO 27001
۴۲	RCM	نت خود گردان / شش سیگما 6σ / Fault Tree / RBI / SFMEA	نت خود گردان	ISO 9001
۴۳			شش سیگما 6σ	IEC 60300
۴۴			Fault Tree	ISO 55000
۴۵			RBI	ISO 27001
۴۶	بهبود سازی	پروژه‌های بهبود جهشی / بازمهندسی فرآیندها	SFMEA	ISO 9001
۴۷			پروژه‌های بهبود جهشی	ISO 55000
۴۸			بازمهندسی فرآیندها	ISO 27001