استاندارد ایران- آی ای سی

۶۰۳۰۰-۳-۱۵

چاپ اول

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد و تحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

ISIRI- IEC
60300-3-15
1st. Edition

مدیریت قابلیت اعتماد-
قسمت ۳-۱۵: راهنمای کاربرد- مهندسی قابلیت اعتماد سیستم

Dependability management – Part 3-15: Application guide – Engineering of system dependability

ICS:03.120.01

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی 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.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی 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، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی 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 می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند 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. مؤسسه می‌تواند 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 سیستم‌های مدیریت کیفیت و مدیریت زیست-محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، مؤسسهٔ استاندارد این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تصدیق صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تصدیق صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. 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 مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1- International organization for Standardization
2 - International Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«مدیریت قابلیت اعتماد-

قسمت ۳-۱۵: راهنمای کاربرد- مهندسی قابلیت اعتماد سیستم»

رئیس:	**سمت و/ یا نمایندگی**
ذره، مهدی (کارشناسی ارشد مهندسی برق)	کارشناس استاندارد
دبیر:	
راعی، جلال (کارشناسی ارشد مدیریت)	عضو هیات علمی دانشکده برق دانشگاه هوایی شهید ستاری و کارشناس استاندارد
اعضاء: (اسامی به ترتیب حروف الفبا)	
اسمی خان، علی (کارشناس مهندسی مکانیک)	کارشناس
افراز، شهاب (کارشناسی مهندسی رایانه)	مدیر تدوین شرکت مهندسی سیستم‌های مدیریت قابلیت اعتماد توازن
بستان دوست راد، احسان (کارشناسی مهندسی صنایع)	رئیس هیات مدیره شرکت مهندسی سیستم‌های مدیریت قابلیت اعتماد توازن
حسن آبادی، سیاوش (کارشناسی ارشد زبان انگلیسی)	عضو هیات علمی دانشگاه هوایی و کارشناس استاندارد
حکیمی زاده، صدف (کارشناسی ارشد مترجمی زبان)	کارشناس شرکت مهندسی سیستم‌های مدیریت قابلیت اعتماد توازن
سیدی نیاکی، کیوان (کارشناسی ارشد مهندسی مکانیک)	عضو هیات علمی سازمان پژوهش های علمی و صنعتی ایران

شهابی، حامد (کارشناسی برق الکترونیک)	کارشناس شرکت خدمات فنی و مهندسی نهال
صفی صمغ آبادی، محمد (کارشناس مهندسی برق)	کارشناس
فرج زاده، عبد الحد (کارشناسی ارشد مدیریت)	کارشناس استاندارد
قربان اشرفی، افشین (کارشناسی مهندسی برق- الکترونیک)	مدیر عامل شرکت خدمات فنی و مهندسی نهال

فهرست مندرجات

عنوان	صفحه
آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران	ب
کمیسیون فنی تدوین استاندارد	ج
پیش گفتار	ز
مقدمه	ح
۱ هدف و دامنه کاربرد	۱
۲ مراجع الزامی	۱
۳ اصطلاحات و تعاریف	۲
۴ مهندسی قابلیت اعتماد سیستم و کاربردها	۳
۴-۱ مرور کلی مهندسی قابلیت اعتماد سیستم	۳
۴-۲ صفات قابلیت اعتماد سیستم و ویژگی‌های عملکردی	۴
۵ مدیریت قابلیت اعتماد سیستم	۵
۵-۱ مدیریت قابلیت اعتماد	۵
۵-۲ پروژه‌های قابلیت اعتماد سیستم	۶
۵-۳ سازگارسازی برای برآورده کردن نیازهای پروژه	۶
۵-۴ تضمین قابلیت اعتماد	۷
۶ تحقق قابلیت اعتماد سیستم	۷
۶-۱ فرآیندی برای قابلیت اعتماد مهندسی در سیستم‌ها	۷
۶-۱-۱ مقصود فرآیند قابلیت اعتماد	۷
۶-۱-۲ چرخه‌ی عمر سیستم و فرآیندها	۸
۶-۱-۳ کاربردهای فرآیند در طول چرخه‌ی عمر سیستم	۹
۶-۲ دستیابی به قابلیت اعتماد سیستم	۱۱
۶-۲-۱ هدف از دستیابی‌های قابلیت اعتماد سیستم	۱۱
۶-۲-۲ معیارهایی برای دستیابی‌ها به قابلیت اعتماد سیستم	۱۱
۶-۲-۳ روش‌شناسی برای دستیابی‌های قابلیت اعتماد سیستم	۱۳
۶-۲-۴ تحقق وظایف سیستمی	۱۴
۶-۲-۵ رویکردهایی برای تعیین دستیابی به قابلیت اعتماد سیستم	۱۶
۶-۲-۶ شواهد عینی دستیابی‌ها	۱۶
۶-۳ ارزیابی قابلیت اعتماد سیستم	۱۷
۶-۳-۱ مقصود ارزیابی‌های قابلیت اعتماد سیستم	۱۷
۶-۳-۲ انواع ارزیابی	۱۷

فهرست مندرجات - ادامه

عنوان	صفحه
۶-۳-۳ روش‌شناسی برای ارزیابی‌های قابلیت اعتماد سیستم	۲۰
۶-۳-۴ مفاهیم و مقدار ارزیابی	۲۱
۶-۴ اندازه‌گیری قابلیت اعتماد سیستم	۲۲
۶-۴-۱ مقصود از اندازه‌گیری‌های قابلیت اعتماد سیستم	۲۲
۶-۴-۲ طبقه‌بندی اندازه‌گیری‌های قابلیت اعتماد سیستم	۲۲
۶-۴-۳ منابع اندازه‌گیری	۲۳
۶-۴-۴ سیستم‌های توانا ساز اندازه‌گیری‌های قابلیت اعتماد	۲۴
۶-۴-۵ تفسیر اندازه‌گیری‌های قابلیت اعتماد	۲۵
پیوست الف (اطلاعاتی) فرآیندها و کاربردهای چرخه‌ی عمر سیستم	۲۷
پیوست ب (اطلاعاتی) روش‌ها و ابزارهایی برای تکوین و تضمین قابلیت اعتماد سیستم	۴۰
پیوست پ (اطلاعاتی) راهنمایی درباره محیط کاربردی سیستم	۴۹
پیوست ت (اطلاعاتی) فهرست‌های وارسی مهندسی قابلیت اعتماد سیستم	۵۵
کتابنامه	۶۴

پیش گفتار

استاندارد " مدیریت قابلیت اعتماد- قسمت ۳-۱۵: راهنمای کاربرد- مهندسی قابلیت اعتماد سیستم" که پیش نویس آن در کمیسیون‌های مربوط توسط شرکت مهندسی سیستم‌های قابلیت اعتماد توازن تهیه و تدوین شده و در یکصد و هفتمین اجلاس کمیتهٔ ملی استاندارد مدیریت کیفیت مورخ ۱۳۸۹/۱۰/۱۹ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ 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 تجدیدنظر استانداردهای ملی استفاده کرد.

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

IEC 60300-3-15:2009, Dependability management – Part 3-15: Application guide – Engineering of system dependability

مقدمه

در محیط‌های کاربردی امروزی، پیچیدگی سیستم‌ها رو به رشد است. قابلیت اعتماد سیستم به یک صفت عملکردی مهم تبدیل شده است که بر راهبردهای کسب و کار در تحصیل سیستم و صرفه اقتصادی در مالکیت و بهره‌برداری سیستم، تأثیر می‌گذارد. قابلیت اعتماد کلی یک سیستم نتیجه‌ای ترکیب شده از تعامل‌های پیچیده عناصر سیستم، محیط‌های کاربردی واسط‌های انسان-ماشین ، نوع به کارگیری خدمات پشتیبانی و دیگر عوامل تأثیرگذار می‌باشد.

این استاندارد در مورد مهندسی کل سیستم برای دستیابی به اهداف قابلیت اعتماد آن، راهنمایی ارائه می‌کند. رویکرد مهندسی در این استاندارد کاربرد دانش علمی مناسب و رشته‌های فنی مرتبط را برای تحقق قابلیت اعتماد الزام شده برای سیستم مورد نظر، ارائه می‌دهد.

در این استاندارد به چهار جنبه مهم برای مهندسی قابلیت اعتمادِ سیستم‌های مورد نظر، مطابق ذیل، پرداخته شده است:

- فرآیند؛
- دستیابی؛
- ارزیابی؛
- اندازه‌گیری.

رشته‌های مهندسی شامل فرآیندهای فنی می‌شود که برای مراحل مختلف چرخه‌ی عمر سیستم کاربرد دارند. فرآیندهای فنی خاص توصیف شده در این استاندارد با ترتیبی از فعالیت‌های فرآیند مرتبط برای دستیابی به اهداف هر مرحله از چرخه‌ی عمر سیستم، پشتیبانی می‌شوند.

این استاندارد برای سیستم‌های عام با وظایف سیستمی تعاملی شامل سخت‌افزار، نرم‌افزار و عناصر انسانی برای دستیابی به اهداف عملکرد سیستم قابل کاربرد است. در بسیاری از موارد یک وظیفه می‌تواند توسط محصولات بازاری تحقق یابد. یک سیستم می‌تواند برای تشکیل شبکه با دیگر سیستم‌ها پیوند داشته باشد. مرزهای جدا کننده محصول از سیستم و سیستم از شبکه، می‌تواند با تعریف کاربرد موجودیت تشخیص داده شود. به طور مثال، زمان‌سنج دیجیتالی به عنوان محصول می‌تواند برای همزمان کردن بهره‌برداری یک رایانه استفاده شود؛ رایانه به عنوان سیستم می‌تواند در یک اداره کسب و کار برای ارتباطات به صورت یک شبکه‌ی ناحیه‌ای محلی با دیگر رایانه‌ها پیوند داشته باشد. محیط کاربرد برای تمام انواع سیستم‌ها قابل کاربرد است. مثال‌هایی از سیستم‌های قابل کاربرد شامل سیستم‌های کنترل برای تولید برق، سیستم‌های محاسبه مقاومت در برابر خرابی و سیستم‌هایی برای تدارک خدمات پشتیبانی نگهداری می‌باشند.

راهنمایی برای مهندسی قابلیت اعتماد، برای سیستم‌های عام ارائه می‌شود. این راهنما سیستم‌ها را برای کاربردهای خاص طبقه‌بندی نمی‌کند. به طور کلی، اغلب سیستم‌های مورد استفاده بنا به دلایل اقتصادی و کاربردهای عملی، طی بهره‌برداری چرخه‌ی عمر خود، قابل تعمیر هستند. سیستم‌های غیرقابل تعمیر از قبیل ماهواره‌های ارتباطی، تجهیزات پایش/حسگری از راه دور و وسایل یکبار مصرف به عنوان سیستم‌های با کاربرد خاص در نظر گرفته می‌شوند. آن‌ها برای دستیابی به اهداف ماموریت خود به شناسایی بیشتر محیط

کاربرد خاص، شرایط بهره‌برداری و اطلاعات تکمیلی درباره ویژگی‌های عملکردی منفرد نیاز دارند. زیر سیستم‌ها و اجزاء غیرقابل تعمیر به عنوان اقلام دور انداختنی در نظر گرفته می‌شوند. انتخاب فرآیندهای قابل کاربرد در مهندسی قابلیت اعتماد برای یک سیستم خاص از طریق سازگارسازی پروژه و فرآیند مدیریت قابلیت اعتماد، انجام می‌شود.

این استاندارد قسمتی از استانداردهای چارچوب درباره‌ی جنبه‌های سیستمی قابلیت اعتماد را برای پشتیبانی استانداردهای ایران-آی ای سی ۱-۶۰۳۰۰ و ۲-۶۰۳۰۰ درباره‌ی مدیریت قابلیت اعتماد، تشکیل می‌دهد. مراجعی قابل کاربرد برای سیستم‌ها به منظور فعالیت‌های مدیریت پروژه ایجاد می‌شوند. این مراجع شناسایی عناصر و تکالیف قابلیت اعتماد مرتبط با سیستم و راهنماهایی برای بازنگری مدیریت قابلیت اعتماد و سازگارسازی پروژه‌های قابلیت اعتماد را شامل می‌شوند.

مدیریت قابلیت اعتماد-

قسمت۳-۱۵: راهنمای کاربرد- مهندسی قابلیت اعتماد سیستم

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد فراهم کردن راهنمایی برای مهندسی قابلیت اعتماد سیستم و توصیف فرآیندی برای تحقق قابلیت اعتماد سیستم طی چرخه‌ی عمر آن می‌باشد.

این استاندارد برای تکوین سیستمی جدید و برای ارتقای سیستم‌های موجود شامل تعاملات داخلی وظایف سیستم متشکل از سخت‌افزار، نرم‌افزار و عناصر انسانی، قابل کاربرد است.

این استاندارد همچنین برای فراهم‌کنندگان زیرسیستم‌ها و تأمین‌کنندگان محصولاتی که اطلاعات سیستم و معیارهایی برای یکپارچگی سیستم را جستجو می‌کنند، به کار برده می‌شود. روش‌ها و ابزاری برای ارزیابی قابلیت اعتماد سیستم و تصدیق نتایج دستیابی به اهداف قابلیت اعتماد، فراهم شده‌اند

۲ مراجع الزامی[1]

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

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 ایران-آی ای سی ۱-۶۰۳۰۰: مدیریت قابلیت اعتماد-قسمت اول -سیستم های مدیریت قابلیت اعتماد؛

۲-۲ ایران-آی ای سی ۲-۶۰۳۰۰: مدیریت قابلیت اعتماد-قسمت دوم -راهنمایی هایی برای مدیریت قابلیت اعتماد.

1- Normative references

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می رود:

۱-۳

سیستم **system**

مجموعه‌ای از اقلام وابسته به یکدیگر که برای مقصودی تعریف شده، مجزا از اقلام دیگر به عنوان یک کل در نظر گرفته می‌شوند.

یادآوری۱- به طور کلی یک سیستم از منظر اجرایی یک وظیفه‌ی معین، تعریف می‌شود.

یادآوری۲- فرض بر آن است که سیستم با یک سطح مجازی مرز بندی می‌شود که این سطح پیوندهای بین سیستم و محیط و دیگر سیستم‌های خارجی را قطع می‌کند.

یادآوری۳- برای بهره‌برداری سیستم ممکن است به منابع خارجی (یعنی خارج از مرز سیستم) نیاز باشد.

یادآوری۴- ساختار سیستم می‌تواند سلسله مراتبی باشد، به طور مثال، سیستم، زیر سیستم، جزء، غیره.

۲-۳

زیر سیستم **subsystem**

سیستمی که قسمتی از یک سیستم پیچیده‌تر است.

۳-۳

پروفایل بهره‌برداری **operating profile**

مجموعه‌ای کامل از تکالیف برای دستیابی به هدف خاص سیستم

یادآوری۱- سناریوهای پیکره‌بندی و بهره‌برداری قسمتی از مُد بهره‌برداری سیستم را تشکیل می‌دهند.

یادآوری۲- پروفایل بهره‌برداری ترتیبی از تکالیف مورد نیاز است که توسط سیستم انجام می‌شود تا هدف بهره‌برداری آن به دست آید. پروفایل بهره‌برداری یک سناریوی بهره‌برداری خاص را برای سیستم مورد بهره‌برداری نشان می‌دهد.

۴-۳

وظیفه **function**

عملیات ابتدایی انجام شده توسط سیستم که در ترکیب با دیگر بهره‌برداری ابتدایی (وظایف سیستم) سیستم را قادر به انجام تکلیف می‌سازد.

[IEC 61069-1[1]:1991, 2.2.5] [1][2]

---

۱ -استاندارد ملی ایران با استفاده از این منبع در دست تدوین می‌باشد.

۲ -ارقام داخل کروشه به کتابنامه ارجاع می‌دهند.

۵-۳

عنصر **element**

ترکیبی از اجزائی که بلوک ساخت پایه را برای انجام یک وظیفه‌ای معین تشکیل می‌دهند

یادآوری۱- یک عنصر می‌تواند حاوی سخت‌افزار، نرم‌افزار، اطلاعات و/ یا اجزای انسانی باشد.

یادآوری۲- برای برخی از سیستم‌ها، اطلاعات و داده‌ها قسمت مهمی از بهره‌برداری‌های سیستم است.

۶-۳

انسجام **integrity**

قابلیت یک سیستم برای حفظ شکل، پایداری و استحکام آن و حفظ سازگاری حین عملکرد و استفاده

۴ مهندسی قابلیت اعتماد سیستم و کاربردها

۴-۱ مرور کلی مهندسی قابلیت اعتماد سیستم

قابلیت اعتماد، قابلیت یک سیستم در هنگام الزام برای برآورده ساختن اهداف خاص تحت شرایط معین استفاده می‌باشد. ویژگی‌های قابلیت اعتماد شامل آمادگی و عوامل تاثیرگذار خارجی و ذاتی آن، از قبیل: قابلیت اطمینان، مقاومت در برابر خرابی، قابلیت بازیابی، انسجام، امنیت، قابلیت نگهداری، قابلیت دوام و پشتیبانی نگهداری می‌شود. قابلیت اعتماد یک سیستم اشاره به این دارد که سیستم مطمئن و توانمند برای انجام خدمات مطلوب طبق تقاضا برای برآورده کردن نیازهای کاربر است. هدف سیستم، ساختار، مشخصات و شرایط تاثیرگذار بر روی عملکرد قابلیت اعتماد سیستم در IEC 62347[2] توصیف شده‌اند که راهنمایی را برای تعیین وظایف سیستم مرتبط برای تعیین قابلیت اعتماد سیستم فراهم می‌کنند.

چهار جنبه عمده برای قابلیت اعتماد مهندسی در سیستم وجود دارد:

الف) فرآیند قابلیت اعتماد – فرآیندهایی فنی برای قابلیت اعتماد مهندسی در سیستم‌ها ایجاد می‌کند. فرآیند شامل ترتیبی از فعالیت‌های اجرا شده در هر مرحله از چرخه‌ی عمر مربوط به دستیابی به اهداف خاص قابلیت اعتماد در عملکرد سیستم می‌شود. فرآیند قابلیت اعتماد برای فرآیندهای طراحی و مدیریت باید کاملاً منسجم باشد.

ب) دستیابی به قابلیت اعتماد – پیاده‌سازی تلاش اثربخش مهندسی و تجربه دانش به کار برده شده در مراحل چرخه‌ی عمر مقتضی سیستم. هدف پیشرفت تدریجی اهداف قابلیت اعتماد وظایف سیستم تشکیل‌دهنده است که برای تحقق زیر سیستم و یکپارچگی سیستم (رشد قابلیت اطمینان) مناسب است؛

پ) ارزیابی قابلیت اعتماد – صفات قابلیت اعتماد را می‌سنجد و اثربخشی آن‌ها را هنگامی که برای یک سیستم پیاده‌سازی می‌شوند تعیین می‌کند. این فرآیند، صفات قابلیت اعتماد خاص را برای برآورده ساختن نیازهای پروژه شناسایی می‌کند و روش‌شناسی و دلیل اینکه چطور این صفات می‌توانند تعیین شوند را فراهم می‌کند؛

ت) اندازه‌گیری قابلیت اعتماد – صفات قابلیت اعتماد را برای اهداف قرارداد، مشخصات و ارزیابی تعیین می‌کند. فرآیند، انتساب[1] یک یا چند مقدار کمی برای طراحی یک موجودیت هدف است که نشاندهنده یک ویژگی قابلیت اعتماد خاص می‌باشد.

هدف، اظهار بیانیه‌ای از قصد با اصطلاحات قابل سنجش برای تسهیل درک متقابل موضوع مورد نظر و برای استفاده به عنوان پایه‌ای برای مذاکرات در رسیدن به توافقات است.

۴-۲ صفات قابلیت اعتماد سیستم و ویژگی‌های عملکردی

صفات قابلیت اعتماد سیستم، قابلیت اعتماد خاص مربوط به خصایص و ویژگی‌های عملکردی وابسته به زمان ذاتی در سیستم توسط طراحی و ساخت است. برخی از خصایص، از قبیل ویژگی‌های عملکردی سیستم می‌توانند تعیین و اندازه‌گیری شوند. دیگر خصایص قابلیت اعتماد که قابل کمی سازی نیستند ممکن است مقدار معین یا اطلاعات مفیدی را وابسته به آن صفات نشان دهند. این خصایص غیرقابل کمی سازی می‌توانند در اصطلاحات کیفی برای ایجاد مقدار آن برای ارزیابی قابلیت اعتماد فردی توصیف شوند. خصایص غیرقابل کمی سازی و قابل کمی سازی برای توصیف صفات قابلیت اعتماد سیستم مهم هستند. مثال‌هایی از خصایص غیرقابل کمی سازی شامل ارزش علامت تجاری محصول، بهره‌برداری مساعد کاربر و دستورالعمل‌های اطلاعاتی می‌شود. مثال‌هایی از ویژگی‌های عملکردی قابل تعیین شامل مدت زمان آماد، فراوانی زمان ناآماد، زمان میانگین بین وقوع خرابی‌ها و زمان برای توان‌یابی از حالت تنزل یافته به عملکرد عادی سیستم می‌شود.

صفات عمده قابلیت اعتماد سیستم عبارتند از:

الف) آمادگی: قابلیت سیستم برای بودن در یک حالت برای انجام یک وظیفه مورد نیاز هنگامی که یک درخواست بر روی سیستم واقع می‌شود. عملکرد آمادگی بر حسب مقیاس‌هایی از قبیل درصد زمان آماد از مدت بهره‌برداری عملکرد سیستم طبق تقاضا؛ فراوانی خروج و مدت زمان ناآماد مشخص می‌شود؛

ب) قابلیت اطمینان: قابلیت سیستم برای انجام یک وظیفه مورد نیاز طی یک دوره زمانی معین تحت شرایط معین استفاده. عملکرد قابلیت اطمینان بر حسب اندازه‌گیری‌هایی از قبیل زمان میانگین بین وقوع خرابی‌ها و مدت زمان عاری از وقوع خرابی مشخص می‌شود؛

پ) قابلیت نگهداری: قابلیت سیستمی که در پی وقوع خرابی بازیابی به یک حالت شود که در آن حالت می‌تواند تحت شرایط معین استفاده و نگهداری یک وظیفه مورد نیاز را فراهم کند، یا در یک حالت آماد نگهداشته شود. عملکرد قابلیت نگهداری بر حسب اندازه‌گیری‌هایی از قبیل زمان میانگین تا توان‌یابی و زمان بازیابی مشخص می‌شود.

ت) پشتیبانی نگهداری: قابلیت یک سازمان که در صورت نیاز، منابع مورد نیاز برای نگهداری از یک سیستم را، تحت شرایط معین فراهم کند. عملکرد پشتیبانی نگهداری بر حسب مقیاس‌هایی از قبیل استفاده عملی از منابع نگهداری، نیازهای آموزش، توانا ساختن ابزار و تسهیلات، زمان تأخیر لجستیک و زمان بازگشت برای تأمین ذخیره اضافی مشخص می‌شود.

---

1 - Assignment

صفات دیگری مرتبط با قابلیت اعتماد برای کاربردهای خاص سیستم وجود دارند. این صفات شامل موارد زیر شده ولی محدود به آن‌ها نمی‌شوند:

ج) قابلیت بازیابی: قابلیت سیستمی که در پی وقوع خرابی یک حالت بازیابی می‌شود که در آن حالت می‌تواند یک وظیفه مورد نیاز را بدون تعمیر سخت‌افزار یا نرم‌افزار انجام دهد. این مورد بر حسب اندازه‌گیری‌هایی از قبیل زمان میانگین تا بازیابی مشخص می‌شود؛

چ) قابلیت آزمون‌دهی: قابلیت سیستمی که قرار است در سطوح نگهداری طراحی شده تحت آزمون برای اقدام تعمیر/ جایگزین کردن قرار گیرد تا شمول خرابی را تعیین کند. این مورد بر حسب اندازه‌گیری‌هایی از قبیل درصد شمول آزمون مشخص می‌شود.

ح) قابلیت دسترسی خدمات: قابلیت یک خدمت که درون رواداری‌های خاص و دیگر شرایط معین هنگامی که بوسیله کاربر درخواست می‌شود، بتواند به دست آید. این مورد برحسب اندازه‌گیری‌هایی از قبیل احتمال دستیابی به یک خدمت مشخص می‌شود؛

خ) قابلیت حفظ خدمات: قابلیت یک خدمت، که هنگامی به دست آمد بتواند ادامه یابد تا تحت شرایطی معین برای مدت درخواست فراهم شود. این مورد برحسب اندازه‌گیری‌هایی از قبیل احتمال حفاظت در یک مدت زمان مشخص می‌شود.

عملکرد قابل بازیابی وابسته به طراحی معماری سیستم، خصایص رواداری- خرابی و خود- درمانی تلفیق شده در یک سیستم است. عملکرد خدمات وابسته به ویژگی‌های تسهیلات سیستم، ترکیب و زیرساخت به کارگیری منابع است. صفات عملکرد سیستم در حالت کلی در طراحی سیستم ذاتی می‌باشند. صفات عملکردی از توانمندی سیستم و خصیصه قابلیت اعتماد سیستم نتیجه می‌شوند.

ویژگی‌های عملکردی سیستم از اندازه‌گیری‌های زمان و نقص نتیجه می‌شوند. یک نقص رخدادی غیر منتظره یا نامطلوب است که طی آزمون‌های سیستم یا بهره‌برداری حین خدمت حاکی از یک وقوع خرابی که ممکن است رخ داده باشد مشاهده شده است. همه نواقص بایستی ثبت و تحقیق و بررسی شوند. این کار برای تعیین اینست که چه نقصی توسط وقوع خرابی واقعی سبب می‌شود یا به علت خطای انسانی یا مشاهده نادرست است. یک وقوع خرابی انحراف از وظایف عملکردی مورد نیاز سیستم است. به هر حال، در زمان مشاهده، یک وقوع خرابی ممکن است سبب قطع کامل وظایف سیستم نشود ولی ممکن است عملکرد سیستم را وخیم کند. گستره وخامت قبل از طبقه‌بندی به عنوان وقوع خرابی بایستی تعریف و برای اندازه‌گیری‌ها ایجاد شود.

۵ مدیریت قابلیت اعتماد سیستم

۵-۱ مدیریت قابلیت اعتماد

قابلیت اعتماد یک نظام فنی است و توسط اصول و طرز کارهای مهندسی مدیریت می‌شود. ایران-آی ای سی ۶۰۳۰۰-۱ و ایران-آی ای سی ۶۰۳۰۰-۲ در این استاندارد برای فرمول بندی راهبردهای مدیریت قابلیت اعتماد و کاربرد کلی رویکردهای فنی برای پیاده‌سازی عناصر و تکالیف استفاده می‌شوند. فرآیندهای مدیریت تکمیلی برای نشان دادن موضوعات مدیریت خاص سیستم عرضه می‌شوند. مدیریت قابلیت اعتماد با طرح

پروژه، تخصیص منبع، انتصابات تکلیف قابلیت اعتماد، پایش و تضمین، اندازه‌گیری نتایج، تحلیل داده‌ها و بهبود مداوم سروکار دارد. فعالیت‌های قابلیت اعتماد بایستی در ارتباط با دیگر نظام‌های فنی هدایت شود تا آثار مربوط به کار مورد نیاز به دست آید و ارزش‌هایی را به خروجی پروژه بیافزاید. سازگارسازی پروژه برای مدیریت صرفه اقتصادی پروژه‌های سیستم تأکید می‌شود. تحلیل هزینه چرخه‌ی عمر، جایی که قابل کاربرد است، بایستی برای تخصیص و بهینه‌سازی منبع برای سنجش هزینه‌های مالکیت و اکتساب استفاده شود.

۵-۲ پروژه‌های قابلیت اعتماد سیستم

قابلیت اعتماد یک عامل تصمیم کلیدی در مدیریت پروژه است. قابلیت اعتماد روی هزینه پیاده‌سازی پروژه تأثیر می‌گذارد. قابلیت اعتماد روی موضوعات کاربردی قابلیت اعتماد خاص در تکالیف پروژه که نیاز به تفکیک‌پذیری اثربخش دارد تمرکز می‌کند. قابلیت اعتماد تأثیر وسیعی روی نتایج تحویل‌های پروژه برای برآورده کردن انتظارات مشتری دارد. از منظر مهندسی یک سیستم، تحقق قابلیت اعتماد در سیستم‌ها یک موضوع تصمیم کسب و کار مهم است که نیاز به یکپارچگی کامل مهندسی و طراحی با فرآیند تصمیم مدیریت دارد. مدیریت کهنگی، ارزیابی ریسک پروژه، سبک سنگین کردن طرح فنی، هزینه‌یابی چرخه‌ی عمر، برون سپاری و هماهنگی زنجیره تأمین برخی از مثال‌های فعالیت‌های قابلیت اعتماد در فعالیت‌های مهندسی سیستم‌ها می‌باشند.

تمام پروژه‌ها با تکوین سیستم جدید کامل درگیر نیستند. اغلب سیستم‌ها توسط یکپارچگی زیرسیستم‌ها و کاربرد محصولات تجاری با مواد در دسترس برای تحقق وظایف سیستم ساخته می‌شوند. در تکوین سیستم اصلی یا برای پروژه‌های ارتقاء سیستم، ممکن است چندین توسعه‌دهنده زیر سیستم و پیمانکار جزء روی تأمینات و خدمات برای دستیابی به تحویل به موقع پروژه سیستم درگیر شوند. در این مورد، مدیریت پروژه برای هماهنگی تلاش‌های مختلف برای پروژه ضروری است. پروژه‌های قابلیت اعتماد سیستم ممکن است با فعالیت‌های قابلیت اعتماد خاص از قبیل موارد زیر ارتباط داشته باشند:

الف) پذیرش فناوری جدید؛

ب) تکوین مشخصات قابلیت اعتماد برای سیستم و زیر سیستم‌ها؛

پ) سنجش قابلیت اعتماد محصولات تجاری برای استفاده در وظایف سیستم؛

ت) ارزیابی توانمندی تأمین‌کننده در ایفای الزامات قابلیت اعتماد پروژه؛

ث) تضمین قابلیت اعتماد برای قبولی سیستم.

فعالیت‌های قابلیت اعتماد سیستم ممکن است در هر مرحله از چرخه‌ی عمر سیستم رخ دهند. برخی از انتصابات تکلیف قابلیت اعتماد ممکن است مهارت‌های ویژه و آموزش در نظام‌های فنی خاص از قبیل مهندسی نرم‌افزار، پشتیبانی لجستیک و قابلیت اطمینان انسان را نیاز داشته باشد.

۵-۳ سازگارسازی برای برآورده کردن نیازهای پروژه

یک پروژه قابلیت اعتماد سیستم برای حل موضوعات قابلیت اعتماد خاص مربوط به سیستم بنیاد نهاده می‌شود. هدف سازگارسازی مدیریت تخصیص منابع در دسترس پروژه و انتخاب روش‌های مقتضی برای

تفکیک‌پذیری اثربخش مسئله می‌باشد. مثال‌هایی از فعالیت‌های پروژه قابلیت اعتماد سیستم که برای سازگارسازی مناسب است شامل موارد زیر می‌شوند:

الف) طرح بودجه برای تخصیص منابع قابلیت اعتماد برای برآورده ساختن اهداف تحویل پروژه؛

ب) سنجش فناوری‌های مختلف برای کسب محصول با قابلیت اطمینان بالا؛

پ) منبع‌یابی از خارج در تکوین زیر سیستم برای برآورده ساختن معیارهای دقیق در الزامات مدل تکامل توانمندی نرم‌افزار که در آن پایش فرآیندی تعیین‌کننده است؛

ت) زمان آموزش مورد نیاز برای به دست آوردن تجربه کافی در استفاده از یک وسیله تحلیل قابلیت اطمینان جدید؛

ث) انتخاب پیمانکاران جزء برای تدارک نگهداری در محل سیستم‌های بحرانی برای انتظارات عملکرد آمادگی بالا بدون هیچ زمان ناآماد برنامه‌ریزی شده مجاز.

رهنمودهایی برای فرآیند سازگارسازی در ایران-آی ای سی ۲-۶۰۳۰۰ توصیف می‌شوند.

۵-۴ تضمین قابلیت اعتماد

فعالیت‌های تضمین قابلیت اعتماد بایستی قسمتی از فرآیند تضمین کیفیت را برای پروژه‌های قابلیت اعتماد سیستم تشکیل دهد. این کار برای حصول اطمینان از تمام فعالیت‌های سیستماتیک و طرح‌ریزی شده پیاده‌سازی شده درون سیستم کیفیت است و در صورت نیاز اجرا می‌شود تا اطمینان کافی از اینکه الزامات کیفیت محصول و سیستم انجام می‌شود را فراهم می‌کند. فعالیت‌های کلیدی با طرح پروژه، واگذاری مسؤولیت مدیریتی و فنی، تصدیق نتایج ارزیابی قابلیت اعتماد، صحه‌گذاری داده‌های عملکرد قابلیت اعتماد برای پذیرش سیستم، پایش اثربخشی فرآیند قابلیت اعتماد، گزارش‌دهی وقوع خرابی و تحلیل داده‌ها برای اقدامات پیشگیرانه و اصلاحی فوری، مستندسازی اطلاعات قابلیت اعتماد مرتبط و نگهداری سوابق آزمون برای پشتیبانی از شواهد عینی و بازنگری مدیریت برای بنیاد نهادن بهبودهای فرآیند ارتباط سروکار دارد. ایران-آی ای سی ۲-۶۰۳۰۰ اطلاعات تکمیلی درباره انتخاب عناصر و تکالیف برنامه قابلیت اعتماد برای سازگارسازی پروژه‌های قابلیت اعتماد سیستم را ارائه می‌کند.

۶ تحقق قابلیت اعتماد سیستم

۶-۱ فرآیندی برای قابلیت اعتماد مهندسی در سیستم‌ها

۶-۱-۱ مقصود فرآیند قابلیت اعتماد

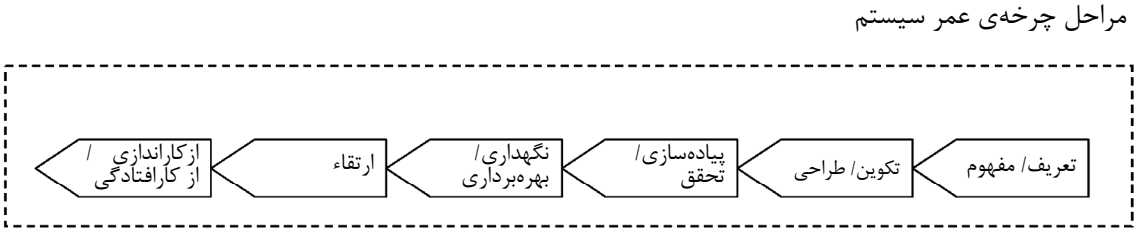
ایجاد یک فرآیند برای مدیریت موفق تکالیف پروژه و هماهنگی فعالیت‌ها ضروری است. فرآیند قابلیت اعتماد بایستی برای فرآیندهای فنی یکپارچه باشد تا قابلیت اعتماد مهندسی را در سیستم تسهیل کند. فرآیند قابلیت اعتماد ورودی‌های خاصی را در نقاط اصلی تصمیم پروژه برای چرخه‌ی عمر سیستم فراهم می‌کند تا پیاده‌سازی پروژه تسهیل کند. این نقاط اصلی تصمیم در تکمیل فازهای مدیریت بحرانی پروژه برای شناسایی بازار، تکوین سیستم، تحقق محصول، پذیرش سیستم، بهره‌برداری در حال خدمت، ارتقاء و از

کارافتادگی رخ می‌دهد. اطلاعات قابلیت اعتماد در این نقاط اصلی تصمیم برای توجیه سرمایه‌گذاری‌های کسب و کار مهم است.

۶-۱-۲ چرخه‌ی عمر سیستم و فرآیندها

نقطه شروع قابلیت اعتماد مهندسی در یک سیستم بایستی در زودترین مرحله چرخه‌ی عمر باشد. کاربر بایستی یک فرآیند مهندسی اثربخش را در این مرحله چرخه‌ی عمر به کار ببرد.

توصیف مراحل چرخه‌ی عمر سیستم می‌تواند از منظر مهندسی سیستم‌های عام دیده شود. توصیفات چرخه‌ی عمر سیستم دیگری وجود دارند. ایران-آی ای سی ۲-۶۰۳۰۰ فازهای چرخه‌ی عمر محصول را از منظر مدیریت پروژه توصیف می‌کند. ISO/IEC 15288 [3] توصیفی را برای چرخه‌ی عمر سیستم مشابه از منظر یک فناوری اطلاعات و مهندسی نرم‌افزار فراهم می‌کند. راهنمای فراهم شده توسط این استاندارد بر پایه مفهوم مراحل چرخه‌ی عمر سیستم است، همانگونه که در شکل ۱ توصیف شده است. مراحل سیستم نقاط گذر فنی دقیقی هستند، در حالیکه فازهای پروژه ممکن است توسط توصیف‌کننده‌های مدیریت برای دستیابی به تصمیمات کسب و کار اصلی همپوشانی داشته باشند. مدیریت ریسک پروژه که در ایران-آی ای سی ۲-۶۰۳۰۰ ارجاع شده تماماً در فرآیندهای چرخه‌ی عمر به کار می‌رود.



شکل ۱ – مروری کلی از چرخه‌ی عمر سیستم

فرآیندهای فنی برای مهندسی شامل ترتیبی از فعالیت‌های فرآیند پیاده‌سازی شده در هر مرحله از چرخه‌ی عمر سیستم مربوط برای دستیابی به عملکرد سیستم مورد نظر و اهداف قابلیت اعتماد می‌شود. قابلیت اعتماد مهندسی در یک سیستم به صورت جدا انجام نمی‌شود. این کار در ارتباط با نظام‌های فنی دیگر (به طور مثال طراحی ساختاری) و فعالیت‌های پشتیبانی (تضمین کیفیت) برای تحقق وظایف سیستم برای کاربردهای مورد نظرشان انجام می‌شود. پیوست الف ترتیبی نوعی از فرآیندهای چرخه‌ی عمر سیستم را توصیف می‌کند.

فعالیت‌های فرآیند کلیدی در چرخه‌ی عمر سیستم به صورت زیر می‌باشد:

الف) تعریف الزامات، نیازهای کاربران و قیود کاربردهای سیستم را شناسایی می‌کند؛

ب) تحلیل الزامات دید کاربر را روی سیستم به یک دید فنی برای مهندسی سیستم تبدیل می‌کند و شامل تکوین یک مأموریت مرجع طراحی/ خط زمان/ پروفایل استفاده مربوط به بهره‌برداری خواهد بود.

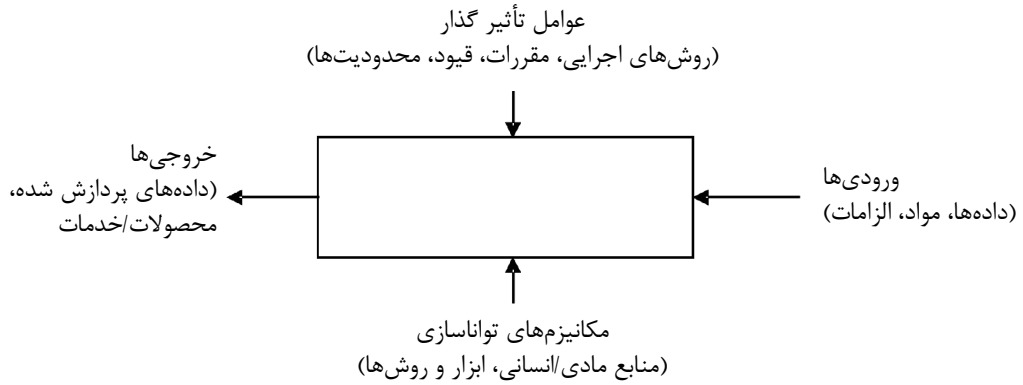
پ) طراحی معماری روشی را ترکیب می‌کند که الزامات سیستم را برای سناریوی بهره‌برداری با تخصیص وظایف مورد نیاز سیستم برای سخت‌افزار، نرم‌افزار و عناصر انسانی برآورده می‌کند؛

ت) طراحی و سنجش بهره‌برداری وسایل سودمندی را برای تحقق وظایف به منظور تسهیل در سبک سنگین کردن طراحی و بهینه‌سازی تعیین می‌کند؛
ث) مستندات طراحی سیستم اطلاعات سیستم، شامل داده‌های قابلیت اعتماد مناسب برای طراحی سیستم را در بر می‌گیرد؛
ج) طراحی سیستم و تکوین زیر سیستم وظایف سیستم و زیر سیستم خاص را ایجاد می‌کند؛
چ) تحقق، عناصر سیستم و زیر سیستم را در اشکال نرم‌افزاری و سخت‌افزاری عرضه می‌کند؛
ح) یکپارچگی، سیستم و زیرسیستم‌ها را سازگار با طراحی معماری مونتاژ می‌کند؛
خ) تصدیق، ثابت می‌کند که الزامات طراحی خاص توسط سیستم تکمیل می‌شوند؛
د) گذر/ نصب، توانمندی سیستم را ایجاد می‌کند تا خدمت عملکرد مورد نیاز را در یک محیط مربوط به بهره‌برداری خاص فراهم کند؛
ذ) راه‌اندازی/ صحه‌گذاری، شواهد عینی را که سیستم الزامات انجام وظیفه را تکمیل می‌کند فراهم می‌کند؛
ر) بهره‌برداری، سیستم را به تحویل خدمت مربوط به بهره‌برداری آن هدایت می‌کند؛
ز) پشتیبانی نگهداری، توانمندی سیستم را برای خدمت مربوط به بهره‌برداری پایدار حفظ می‌کند؛
ژ) ارتقاء، عملکرد سیستم را با خصایص افزوده شده بهبود می‌بخشد؛
س) از کار انداختن/ از کارافتادگی وجود موجودیت سیستم را پایان می‌بخشد.

۶-۱-۳ کاربردهای فرآیند در طول چرخه‌ی عمر سیستم

یک فرآیند مجموعه‌ای جامع از فعالیت‌های متقابل یا وابسته به هم است که ورودی‌ها را به خروجی‌ها تبدیل می‌کند. فرآیندها به عنوان مدل‌های مرجع برای سازمان وظیفه‌ای (به طور مثال سیستم‌های مدیریت کیفیت (QMS[1])، مدیریت پروژه)، تراکنش کسب و کار (به طور مثال اکتساب، توافق زنجیره تأمین) و پیاده‌سازی و طرح فنی (به طور مثال تکوین محصول، ارزیابی‌های سیستم) استفاده می‌شوند. این استاندارد روی فرآیندهای فنی برای قابلیت اعتماد مهندسی در سیستم تمرکز می‌کند.
شکل۲ مثالی از مدل فرآیند را نشان می‌دهد. در زمینه مهندسی ورودی‌های اولیه معمولاً شامل داده‌های فراهم‌کننده مجموعه‌ای از الزامات، یا نیازهای بیان شده توسط مشتری می‌باشند. خروجی‌ها ممکن است شامل داده‌های پردازش شده‌ای باشند که توصیف‌کننده یک راه حل مطلوب از قبیل یک مشخصه، ساخت یک محصول یا تحویل یک خدمت باشند. ورودی‌های دیگری وابسته به فرآیند برای اهداف کنترل و توانا سازی وجود دارند. فعالیت‌های فرآیند ورودی‌های اولیه را به خروجی‌های مطلوب تبدیل می‌کنند یا تغییر می‌دهند. این تبدیل مربوط به مجموعه شرایط توسط مکانیزم‌های توانا سازی و عوامل تاثیرگذار مرتبط است. برخی از عوامل تاثیرگذار از قبیل روش‌های اجرایی بهره‌برداری برای فعال سازی فرآیند، قابل کنترل هستند؛ دیگر عوامل مانند شرایط آب و هوایی یا تغییر ناگهانی اقلیم ممکن است غیرقابل کنترل باشند. مکانیزم‌های توانا سازی از قبیل روش‌ها و ابزار برای تأثیر گذاری در تبدیل ضروری هستند. این مدل فرآیند برای پیاده‌سازی فرآیندهای فنی توصیف شده در این استاندارد استفاده می‌شود.

1 -Quality management system



شکل ۲ – مثالی از یک مدل فرآیند

فرآیندهای فنی دو هدف را به کار می‌گیرند:

الف) انجام تکالیف مهندسی و هدایت فعالیت‌های مهندسی مجدد طی مفهوم و تکوین سیستم؛

ب) انجام فعالیت‌های بهره‌برداری، نگهداری و وارهایی با توجه به سیستم.

کاربردهای فرآیندهای فنی، تکرار شونده و بازگشتی می‌باشد تا راه حل مطلوب را کامل کنند. این کار برای تمام مراحل چرخه‌ی عمر سیستم به کار می‌رود. روابط فرآیندهای فنی مستقل از ساختار و اندازه سیستم می‌باشد. فعالیت‌های فرآیند از قبیل تعریف الزامات، تحلیل الزامات و طراحی معماری "بالا به پایین" رویکردهای فنی برای مهندسی راه‌حل مطلوب می‌باشند (یعنی تجزیه سیستم به عناصر اجزای آن)؛ در حالیکه یکپارچگی و تصدیق رویکردهای پایین به بالا برای تحقق پیکره‌بندی سیستم و اعتبار بخشیدن به عملکرد آن می‌باشند (یعنی ساخت عناصر تا حدود ساخت سیستم). گذر از رویکردهای بالا به پایین به رویکردهای پایین به بالا طی مرحله پیاده‌سازی در تکمیل نصب سیستم رخ می‌دهد که در آن راه‌اندازی آغاز می‌شود. این مورد همانگونه که در [3] ISO/IEC 15288 توصیف شده به عنوان مدل "V" در اقدامات مهندسی شناخته می‌شود.

یادآوری– برای اطلاعات بیشتر در مورد مدل "V" به [4] ISO/IEC/TR 15271 مراجعه کنید.

[5] ISO/IEC 12207 چارچوبی را برای فرآیندهای چرخه‌ی عمر نرم‌افزار ایجاد می‌کند. این چارچوب شامل فرآیندها، فعالیت‌ها و تکالیفی می‌شود که طی اکتساب یک خدمت یا محصول نرم‌افزاری و طی تأمین، تکوین، بهره‌برداری، نگهداری و وارهایی محصولات نرم‌افزاری می‌توانند به کار برده شوند. ISO/IEC 12207 [5] به تنهایی یا در ارتباط با [3] ISO/IEC 15288 می‌تواند استفاده شود.

مثال‌هایی نوعی از کاربردهای فرآیند در هر مرحله چرخه‌ی عمر سیستم می‌تواند در پیوست الف یافت شود. آگاهی از نوع سیستم و محیط کاربردی برای سازگارسازی کاربرد فرآیند در مراحل چرخه‌ی عمر سیستم مقتضی به منظور برآورده سازی نیازهای خاص پروژه ضروری است.

۶-۲ دستیابی به قابلیت اعتماد سیستم

۶-۲-۱ هدف از دستیابی‌های قابلیت اعتماد سیستم

دستیابی اقدامی برای انجام یک هدف است. دستیابی نتایج آورده شده توسط تفکیک مسئله موفق را منعکس می‌کند. اقدامات مورد نیاز برای دستیابی به قابلیت اعتماد سیستم می‌تواند بوسیله تلاش مهندسی اثربخش و تجربه آگاهی کاربردی در مراحل چرخه‌ی عمر سیستم مقتضی انجام شود. هدف انجام پیش رونده اهداف قابلیت اعتماد وظایف سیستم سازنده است که منجر به یکپارچگی سیستم می‌شود. دستیابی به قابلیت اعتماد سیستم هدفی مهم در پروژه است که نیاز است برای پذیرش سیستم هماهنگ شود و عملاً اثبات شود. پذیرش سیستم معمولاً یک توافق قراردادی برای برآورده سازی الزامات مشتری است. هدف نهایی برآورده شدن انتظارات عملکرد سیستم از طرف کاربر می‌باشد.

۶-۲-۲ معیارهایی برای دستیابی‌ها به قابلیت اعتماد سیستم

قابلیت اعتماد سیستم با مشارکت موفق صفات قابلیت اعتماد مناسب و خصایص عملکردی مرتبط در سیستم به دست می‌آید. معیارهایی برای دستیابی‌ها به قابلیت اعتماد سیستم بایستی منعکس شوند:

الف) تحقق درست از اهداف عملکردی سیستم؛

ب) تحقق درست از شرایط بهره‌برداری؛

پ) پیاده‌سازی اثربخش اصول قابلیت اعتماد در زیرساخت‌های بهره‌برداری؛

ت) شرایط استفاده؛

ث) کاربرد فرآیندهای مقتضی برای تحقق سیستم؛

ج) استفاده عملی از آگاهی و تجربه برای عرضه صرفه اقتصادی خدمات سیستم.

این معیارها با تمرکز بر روی عواملی کلیدی اثربخش بر موضوعات قابلیت اعتماد مرتبط با سیستم می‌توانند انجام شوند. معیارهای مهمی شناسایی می‌شوند که از کاربردهای فرآیند و تحقق اهداف سیستم پشتیبانی می‌کنند. دلایلی برای واضح ساختن مفهوم پیاده‌سازی قابلیت اعتماد فراهم می‌شوند. این معیارها بایستی در طرح و پیاده‌سازی پروژه در نظر گرفته شوند. کاربر برای برآورده ساختن نیازهای خاص پروژه بایستی فعالیت‌های قابلیت اعتماد مقتضی را از منظر چرخه‌ی عمر سیستم تنظیم کند.

۱) خط مشی مدیریت قابلیت اعتماد – این معیار بر روی زیرساخت بهره‌برداری، تخصیص منابع مقتضی، انتصاب مسئولیت برای پاسخگویی مدیریت و رهبری قابلیت اعتماد پروژه تأثیر می‌گذارد. مفهوم خط مشی قابلیت اعتماد تمرکز مشتری را روی راهبرد و التزامات مدیریت قابلیت اعتماد، تلاش همکاری و رویکرد فرآیند سیستماتیک به سمت کاربرد اثربخش اصول مدیریت قابلیت اعتماد همانگونه که در ایران-آی ای سی ۱-۶۰۳۰۰ توصیف شده منعکس می‌کند. خط مشی مدیریت قابلیت اعتماد که در ایران-آی ای سی ۱-۶۰۳۰۰ توصیف شده فرآیندهای مهندسی توصیف شده در این استاندارد را به کار می‌برد؛

۲) پایگاه دانش از قابلیت اعتماد – این معیار روی درستی تفسیر نیازهای بازار، کفایت اطلاعات مرتبط مورد نیاز برای شروع پروژه، کاربردهایی از استاندار ها و مشخصات در دسترس، قدرت نفوذ رقابتی در مذاکره

قرارداد و تحقق قابلیت اعتماد برای هدف عینی تأثیر می‌گذارد. مفهوم پایگاه دانش از قابلیت اعتماد در مزیت رقابتی بازار و رهبری فناوری هنگام برخورد با چالش‌های جدید در موضوعات قابلیت اعتماد سیستم واقع می‌شود؛

۳) معماری طراحی – این معیار روی استفاده از فناوری‌ها برای کاربردهای سیستم، انتخاب سخت‌افزار، نرم‌افزار و عناصر انسانی برای تحقق وظایف سیستم، یکپارچگی سیستم و بهره‌برداری حین خدمت از سیستم و تسهیل ارتقا و پیشرفت سیستم تأثیر می‌گذارد. معماری طراحی یک چارچوب سازنده و به هم پیوسته برای انسجام و تحقق سیستم ایجاد می‌کند. این مورد همچنین ارتقای توانمندی، توسعه توانمندی، بهره‌برداری با صرفه اقتصادی و تدارک کیفیت خدمت را آسان می‌کند. استفاده عملی از فناوری مقتضی با مشارکت خصایص پیشرفته و وسعت بخشیدن حدود فنی برای کاربردها، سبک سنگین کردن طراحی را مجاز می‌سازد؛

۴) همکاری زنجیره تأمین – این معیار روی تصمیمات ساخت- خرید، نقشه‌های قرارداد فرعی و برون سپاری، روش‌های اجرایی و مستندات صحه‌گذاری و تصدیق و فرآیندهای پایش و تضمین تأثیر می‌گذارد. مفهوم مدیریت زنجیره تأمین بر پایه همکاری تأمین‌کننده- خریدار و اشتراک اطلاعات مرتبط در فرآیند اکتساب و تهیه و تدارک است. زنجیره تأمین ارتباط لازم را برای ردگیری اطلاعات مهم فراهم می‌کند. پیامد آن روی کسب و کار اقتضاء در فرآیند اجرایی، کاهش هزینه‌های تدارک و انگیزه‌هایی برای تحویل محصولات و خدمات کیفی می‌باشد.

۵) سیستم‌های تواناساز- این معیار روی استفاده از روش‌ها و ابزار، اقتضاء ظرفیت‌های کاری طراحی، نیازهای آموزش مهارت‌ها، تولید محصولات جدید و به کارگیری سیستم، راهبردهای پشتیبانی لجستیک و نگهداری تأثیر می‌گذارد. مفهوم سیستم‌های توانا ساز در بهبود فرآیند تحویل و طراحی و استفاده عملی اثربخش از روش‌ها و ابزار برای تسریع در تفکیک مسئله دیده می‌شود. سیستم‌های توانا ساز همیشه از لحاظ فنی پیچیده نیستند که نیاز به مهارت‌های ویژه برای استفاده و ادراک آن داشته باشد. برخی از روش‌شناسی‌ها، دستورالعمل‌ها و فهرست‌های وارسی ساده‌ای هستند که تصمیمات در محل برای انجام اقدامات شایسته را برای اپراتورها و متخصص نگهداری‌ها آسان می‌کنند. اطلاعات بیشتر در مورد سیستم‌های توانا ساز در استاندارد ISO/IEC 15288 [3] داده شده است؛

۶) بازخورد مشتری و مدیریت اطلاعات – این معیار روی روابط مشتری بر حسب رضایت‌مندی و صداقت، تدارک خدمات توجه اثربخش مشتری، درستی در گزارش رخداد، ضبط داده‌های خدمت برای تحلیل، پیاده‌سازی اثربخش اقدامات پیشگیرانه و اصلاحی، ایجاد روندهای عملکرد سیستم و سوابق تاریخچه‌ای عملکرد قابلیت اعتماد تأثیر می‌گذارد. مفهوم اطلاعات بازخورد مرتبط قابلیت ایجاد روندهای عملکردی، شناسایی نواحی بحرانی نیازمند توجه و فراهم نمودن شواهد عینی برای صحه‌گذاری و تصدیق است.

۶-۲-۳ روش‌شناسی برای دستیابی‌های قابلیت اعتماد سیستم

انتخاب روش‌های قابل کاربرد می‌تواند با آگاهی از معیارها و تحقق مفهوم آن‌ها برای دستیابی‌های قابلیت اعتماد سیستم همراه شود. هدف، استفاده از این روش‌ها برای ساختن قابلیت اعتماد در سیستم است. کاربرد در مشارکت صفات قابلیت اعتماد مرتبط در وظایف سیستم هدف‌گذاری می‌شود.

روش‌شناسی برای پیاده‌سازی قابلیت اعتماد در وظایف سیستم می‌تواند از دو منظر دیده شود:

الف) رویکرد بالا به پایین برای ترکیب قابلیت اعتماد سیستم بر پایه الزامات خاص سیستم و اطلاعات بازار برای تکوین معماری سیستم؛

ب) رویکرد پایین به بالا برای ساختن قابلیت اعتماد در وظایف سیستم بر پایه قواعد طراحی قابلیت اعتماد برای ساده‌سازی، رواداری وقوع خرابی، تقلیل و کاهش ریسک.

هر دو رویکرد با شناسایی صفات قابلیت اعتماد و تعیین مقادیر آن‌ها ارتباط دارند. صفات قابلیت اعتماد مقیاس‌های اساسی برای ارزیابی و دستیابی به قابلیت اعتماد سیستم می‌باشند.

صفات قابلیت اعتماد که مرتبط با ویژگی‌های عملکردی سیستم هستند وابسته به زمان می‌باشند. آن‌ها می‌توانند از اندازه‌گیری‌های رخداد و زمان نتیجه‌گیری و مشخص شوند. مثال‌ها شامل درصد زمان آماد برای عملکرد آمادگی سیستم، احتمال موفقیت یک وظیفه بهره‌برداری سیستم با مدت زمان عاری از وقوع خرابی برای اثبات عملی قابلیت اعتماد و تکمیل توان‌یابی سیستم درون زمان ناآماد برنامه ریزی شده برای نشان دادن اقتضاء در اقدامات پشتیبانی نگهداری می‌شوند.

به هر حال، تمام صفات قابلیت اعتماد به علت قیود زمانی و هزینه، محدودیت‌های فنی، یا به خاطر دلایل دیگر مرتبط با پروژه نمی‌توانند به آسانی تعیین شوند. مثال‌ها شامل سیستم‌های پیچیده با قابلیت اطمینان بالا، سیستم‌های جدید با تجربه به کار گیری میدان محدود، سیستم‌های نرم‌افزاری عام برای استفاده در محیط کاربردی جدید و برخی محصولات تجاری بدون تاریخچه قابلیت اطمینان عملکرد می‌شوند. دیگر روش‌ها برای فراهم کردن اعتماد برای تضمین قابلیت اعتماد و استفاده نیاز می‌شوند. بایستی توجه شود که صفات قابلیت اعتماد سیستم به طور ذاتی احتمالی یا اتفاقی می‌باشند. آن‌ها غیر از ویژگی‌های عملکردی مربوط که می‌توانند از اندازه‌گیری‌های مستقیم نتیجه شوند ممکن است به طور غیر مستقیم خصایص قابل ارزیابی را احاطه کنند. روش‌های نوعی قابل کاربرد شامل مطالعات موردی R&M، موارد آزمون شبیه‌سازی شده، مدل‌های تکامل توانمندی و برنامه‌های رشد قابلیت اطمینان می‌شوند.

تعداد و مقادیر قابل سنجش اغلب نیاز به تفسیر دارند. یک اندازه‌گیری نرخ وقوع خرابی بدون مرجع مناسب برای زمینه یا تفسیر موضوعات مرتبط احاطه‌کننده آن ممکن است بدون معنی باشد. درحالی که تعداد نرخ وقوع خرابی ممکن است به عنوان نمایش‌دهنده‌ای برای مقایسه گزینه‌های طراحی مختلف استفاده شود، که مفروضات تضمین‌کننده برای پشتیبانی منطق و توجیه حیاتی هستند. این کار کاربرد ابزار آماری را برای تعیین مرزهای استنتاجی و حدود اعتماد مواجهه با ریسک بالقوه میسر می‌سازد. در یک مثال کسب و کار، زمان میانگین بین وقوع خرابی‌ها برای یک دستگاه کپی ممکن است برای مالک کسب و کار معنای زیادی

نداشته باشد ولی تعداد کپی‌های خالی ظاهر شده بر هر ماه استفاده از دستگاه هزینه تلف شده را نشان خواهد داد.

پیوست ب مثال‌هایی از روش‌ها و ابزار قابل کاربرد برای تسهیل در دستیابی‌های قابلیت اعتماد سیستم را ارائه می‌کند. آگاهی از وظایف بهره‌برداری سیستم و محیط کاربردی آن که در پیوست پ توصیف شده است برای انتخاب روش‌ها و ابزار مرتبط ضروری است. کاربردهای اثربخش بایستی روی موضوعات حیاتی در حل مسائل فنی تمرکز داشته باشند. محدودیت‌های این روش‌ها و ابزار برای کاربردهای خاص آن‌ها بایستی برای اجازه تفسیر مناسب نتایج یادآوری شود.

۶-۲-۴ تحقق وظایف سیستمی

وظایف سیستم با استفاده از سخت‌افزار، نرم‌افزار، یا عناصر انسانی، یا هر ترکیبی از آن‌ها برای دستیابی به اهداف عملکردی خاص سیستم می‌تواند تحقق یابد. موارد ذیل موضوعات کلی مرتبط با انتخاب و کاربرد این عناصر را برای دستیابی‌های موفقیت‌آمیز به قابلیت اعتماد سیستم نشان می‌دهد.

الف) عنصر سخت‌افزاری - سخت‌افزار معمولاً در ساخت سیستم استفاده می‌شود. سخت‌افزار می‌تواند شامل اجزای مکانیکی، الکتریکی، الکترونیکی، نوری و فیزیکی باشد. آن‌ها در پیکره‌بندی‌های مختلف برای تحقق وظایف سخت‌افزار استفاده می‌شوند. امروزه اغلب محصولات الکترونیکی ساخته شده با عناصر سخت‌افزاری در کاربردهای فناوری نسبتاً دارای بلوغ کامل می‌باشند. قواعد طراحی به خوبی ایجاد می‌شوند. محصولات الکترونیکی در تولید تحت محیط فرآیند ساخت کنترل شده از خود سازگاری نشان می‌دهند. کیفیت محصول و قابلیت اعتماد آن می‌تواند توسط برنامه‌های تضمین مقتضی معین شود. همچنین پایگاه‌های داده "تجربه" وسیعی برای پشتیبانی عملکرد قابلیت اطمینان این محصولات الکترونیکی برپایه سخت‌افزار وجود دارد. به هر حال، برخی از محصولات با اجزای الکترونیکی فعال به تغییر محیط‌های کاربردی حساس هستند. در فیزیک وقوع خرابی‌های این اجزا وقوع خرابی‌های سخت‌افزاری و پدیده مرگ و میر کودکی غالب است. طراحی قابلیت اطمینان مناسب، غربالگری و بسته‌بندی می‌تواند در کاهش چشمگیر وقوع خرابی‌های سریع کمک نماید. برخی از عناصر سخت‌افزاری ممکن است به علت بهره‌برداری یا استفاده گسترده فرسوده شوند در حالی که دیگر عناصر ممکن است دارای خواب محدود باشند. این مشکلات قابلیت اطمینان ذاتی می‌توانند با پیاده‌سازی تلاش‌های نگهداری برنامه‌ریزی شده یا پیشگیرانه حل شوند. ساختار سیستم سخت‌افزاری سلسله مراتبی است. راهبرد پشتیبانی نگهداری می‌تواند توسط طراحی وظیفه‌ای مناسب و راهبرد بسته‌بندی پایین‌ترین مونتاژ قابل تعویض یا واحد به کار گرفته شود. این کار طراحی قابلیت نگهداری و فعالیت‌های پشتیبانی لجستیک را برای بهبود عملکرد آمادگی سیستم آسان می‌کند.

ب) عنصر نرم‌افزاری- نرم‌افزار می‌تواند شامل دستورالعمل‌های کد شده، برنامه‌های رایانه‌ای، قواعد ایجاد شده و روش‌های اجرایی برای بهره‌برداری از سیستم باشد. دستورات کد شده برای دستور دادن به یک برنامه رایانه‌ای برای اجرای وظیفه سیستم برای کاربرد استفاده می‌شود. آزمون کدهای نرم‌افزاری برای خطاهای کد گذاری مشکل است مگر اینکه در بهره‌برداری رایانه واقعی اجرا شود. یک خطای برنامه نرم‌افزاری که در یک وقوع خرابی سیستم نتیجه شده است به علت فعال سازی یک وقوع خرابی پنهان یا "اشکال" درون برنامه

نرم‌افزاری می‌باشد. نظام‌های طراحی نرم‌افزاری برای کمینه کردن تولید بالقوه خطاهای نامطلوب در طراحی ضروری می‌باشند. رویکردهای استفاده شده شامل اجتناب از خرابی، حذف خرابی و مقاومت در برابر خرابی می‌شوند. آن‌ها روش‌هایی رسمی در نظام‌های طراحی نرم‌افزاری می‌باشند. اگرچه نرم‌افزار فرسوده نمی‌شود وظایف آن می‌تواند به عنوان نتیجه منطقی تغییرات وخیم تر شود. به علت اینکه نرم‌افزار توسط منبع انسانی در یک شکل یا اشکال دیگر خلق می‌شود، نظام‌های کنترل طراحی روی محیط طراحی نرم‌افزار متمرکز می‌شوند. قبول یک زیرساخت با استفاده از روش‌شناسی از قبیل مدل‌های تکامل توانمندی به عنوان یک چارچوب برای تکوین نرم‌افزاری می‌تواند دستیابی به قابلیت اعتماد را در وظایف نرم‌افزاری آسان نماید. موضوعات و نسخه‌های نرم‌افزاری برای ارتقاء بایستی توسط یک فرآیند مدیریت پیکره‌بندی سیستم کنترل شوند تا قابلیت همکاری وظایف و ارتقاء قابلیت اعتماد را با یکدیگر در عملکرد تقویت کنند؛

پ) عنصر انسانی – ارتباط متقابل انسان با بهره‌برداری از سیستم می‌تواند به عنوان قسمتی از وظایف سیستم یا به عنوان کاربر نهایی سیستم دیده شود. نقش انسان در عملکرد سیستم می‌تواند با توجه به قابلیت انسان برای تخفیف یا کنترل موقعیت‌های مداوم سودمند باشد. به هر حال، بیشتر رخدادهای صنعتی گزارش شده و حوادث اصلی مطالعه شده می‌توانند به خطاهای انسانی به عنوان دلیل اولیه عیب فنی یا قطع خدمت عملکرد ردیابی شوند. سیستم‌های طراحی شده برای بهره‌برداری یا استفاده انسان بایستی عواملی انسانی را با طراحی سیستم ترکیب نمایند تا ریسک وقوع خرابی‌های حیاتی سیستم، افت ویژگی‌ها، نواقص امنیتی یا تهدیدات ایمنی را کمینه نمایند. قابلیت اعتماد می‌تواند توسط کاربرد عواملی انسانی در قواعد طراحی و ساده‌سازی تکالیف برای بهره‌برداری انسانی به دست آیند. مطالعه عواملی انسانی با تلاشی چند-رشته‌ای در جمع‌آوری اطلاعات درباره توانمندی‌های انسانی و محدودیت‌ها برای کاربردهای اثربخش بر عملکرد سیستم- انسان ارتباط دارد. جنبه‌های مهندسی شامل کاربرد اطلاعات عواملی انسانی برای طراحی ابزار، دستگاه‌ها، سیستم‌ها، تکالیف، کارها و محیطی برای استفاده انسانی ایمن، راحت و اثربخش می‌شود. تعلیم و آموزش، پیش‌نیازهایی مهم برای هر بهره‌برداری از سیستم که نیاز به ارتباط متقابل انسانی دارد می‌باشند. استانداردسازی عواملی انسانی یکپارچگی سیستم را تسهیل می‌کند، قابلیت همکاری متقابل عناصر سیستم را ارتقاء می‌بخشد و قابلیت خدمات‌دهی و عملکرد قابلیت اعتماد کلی را بهبود می‌بخشد.

بیشتر وظایف سیستم در محصولات الکترونیکی امروز از عناصر سخت‌افزاری و نرم‌افزاری ترکیبی در طراحی-های سیستم استفاده می‌کنند. آن‌ها گستره وسیعی از خصایص طراحی را برای کاربردهای گوناگون عرضه می‌کنند. قابلیت اعتماد وظایف سیستم توسط مشارکت قواعد طراحی و فرآیندهای ایجاد شده برای کاربردها به دست می‌آید. سبک سنگین کردن طراحی می‌تواند توسط ترکیبی شایسته از فناوری‌های مناسب برای برآورده کردن نیازهای کاربردی خاص به دست آید. مقادیر اقتصادی می‌تواند از طریق بسته‌بندی و استانداردسازی ماژولار برای تولید در مقیاس انبوه به دست آیند. وظایف سیستم می‌تواند به منظور بهبود تأثیر عملکرد بوسیله آزمون توکار یا دیگر نقشه‌های پایش برای خود وارسی خودکار شوند. نفوذ انسان در وظایف سیستم فقط توسط مقررات امنیتی و ایمنی ضرورت می‌یابد، یا توسط دلایل اقتصادی یا اجتماعی

دیکته می‌شود. پیوست ت فهرست‌های وارسی را برای سخت‌افزار، نرم‌افزار و کاربردهای طراحی عامل انسانی فراهم می‌کند.

۶-۲-۵ رویکردهایی برای تعیین دستیابی به قابلیت اعتماد سیستم

سه رویکرد عام وجود دارد که تعیین می‌کند قابلیت اعتماد سیستم به دست آمده است. این سه رویکرد اهداف متفاوتی را با تغییر درجه دقت مهندسی به کار می‌گیرند. در عمل، احتمالاً ترکیبی از این سه رویکرد استفاده می‌شود:

الف) اثبات عملی- این مورد بوسیله بهره‌برداری واقعی از سیستم در یک محیط کاربردی طی یک دوره زمانی برنامه‌ریزی شده به دست می‌آید تا عملکرد قابلیت اعتماد را به طور عملی اثبات کند. مثال‌های نوعی شامل موارد زیر می‌شوند:

تاریخچه عملکرد قابلیت اعتماد سیستم‌های تحت بهره‌برداری میدانی؛

اثبات عملی قابلیت اطمینان رسمی؛

عملکرد آمادگی طی دوره وارانتی.

ب) استنتاج- این مورد بوسیله روش‌های آماری با استفاده از داده‌های مشاهده شده وظایف سیستم تشکیل‌دهنده بر پایه معیارها و مفروضات ایجاد شده به دست می‌آید تا به یک مقدار عددی نشان دهنده صفات قابلیت اعتماد سیستم برسد (ویژگی‌ها/ عملکرد). مثال‌های نوعی شامل موارد زیر می‌شوند:

- پیش‌بینی سیستمی با پیکره‌بندی معین؛
- شبیه‌سازی سیستم؛
- مدل‌های تکامل توانمندی؛
- تصدیق موردی آزمون عملکرد سیستم.

پ) شواهد پیش رونده- این مورد توسط اجرای پیش رونده سنگ نشانه‌های پروژه با آرگومان‌های قابل ممیزی برای پشتیبانی از شواهد هدف به دست می‌آید. مثال‌های نوعی شامل موارد زیر می‌شوند:

- مورد R&M؛
- برنامه رشد قابلیت اطمینان.

۶-۲-۶ شواهد عینی دستیابی‌ها

موارد ذیل بیانیه‌هایی کلیدی در مورد ویژگی‌های قابلیت اعتماد سیستم برای استفاده به عنوان شواهد عینی می‌باشند که از پذیرش سیستم و محصولات در مراحل چرخه‌ی عمر سیستم قابل کاربرد پشتیبانی می‌کنند. شواهد عینی برای اهداف ممیزی و قراردادی نیاز به مستندسازی و احراز اصالت دارند.

الف) بیانیه‌ای درباره صفات قابلیت اعتماد سیستم و محیط بهره‌برداری برای انعکاس انتظارات کاربر در مشخصات تجاری یا طرح پیشنهادی بر پایه اطلاعات تحقیق بازار. این مورد اطلاعاتی را برای شروع طرح و تکوین مشخصات قابلیت اعتماد سیستم فراهم می‌کند؛

ب) بیانیه‌ای درباره ویژگی‌های عملکردی سیستم در مشخصات قابلیت اعتماد سیستم. این مورد اطلاعاتی را برای ایجاد اهداف طراحی قابلیت اعتماد و معماری سیستم فراهم می‌کند؛

پ) بیانیه‌ای درباره ویژگی‌های عملکردی قابلیت نگهداری و قابلیت اطمینان برای هر وظیفه سیستم در مشخصات طراحی وظیفه‌ای. این مورد اطلاعاتی را برای انتخاب فناوری، تصمیمات ساخت- خرید و ایجاد الزامات تهیه و تدارک فراهم می‌کند؛

ت) بیانیه‌ای درباره ویژگی‌های قابلیت اطمینان و قابلیت نگهداری برای نگهداری و بهره‌برداری حین خدمت از سیستم. این مورد اطلاعاتی را برای طرح پشتیبانی لجستیک، نگهداری قرارداد و نیازهای آموزشی ویژه فراهم می‌کند؛

ث) بیانیه‌ای درباره ویژگی‌های قابلیت اعتماد مرتبط برای پذیرش محصول، انطباق تصدیق و صحه‌گذاری روی نتایج عملکرد سیستم. این مورد پایه اجرای موافقت‌های قراردادی برای اقلام قابل تحویل قرارداد را تشکیل می‌دهد؛

ج) تمام گزارشات پروژه قابلیت اعتماد شامل داده‌های تحلیل قابلیت اعتماد وضعیت آزمون و نتایج اثبات عملی. این مورد اطلاعاتی را در مورد بازنگری پروژه، تغییرات طراحی، به روز رسانی‌های روش اجرایی، اقدامات پیشگیرانه و اصلاحی برای بهبود پیش رونده فراهم می‌کند.

۶-۳ ارزیابی قابلیت اعتماد سیستم

۶-۳-۱ مقصود ارزیابی‌های قابلیت اعتماد سیستم

ارزیابی یک سنجش از وضعیت یا نتیجه یک فعالیت یا موضوع قابلیت اعتماد خاص است. مقصود ارزیابی تعیین اینست که چطور یک مسئله می‌تواند حل شود. یافته‌ها برای پشتیبانی از اقدامات پیشنهاد شده با توجیه و منطق استفاده می‌شوند. فرآیند ارزیابی، شناسایی گزینه‌ها یا جایگزین‌های ممکن را برای تفکیک مسئله تسهیل می‌نماید. این کار سبک سنگین کردن‌های طراحی و انتخاب محصول ارجح را مجاز می‌سازد. تلاش ارزیابی در قابلیت اعتماد سیستم بایستی برای برآورده سازی نیازهای پروژه و برای ارتقای فرآیند تنظیم شود.

۶-۳-۲ انواع ارزیابی

ارزیابی می‌تواند عینی یا ذهنی باشد. ارزیابی عینی توسط اندازه‌گیری مستقیم یک موجودیت برای به دست آوردن نتایج است. ارزیابی ذهنی برای انتساب یک مقدار به یک ماهیت، کاراکتر، یا کیفیت یافته‌های آن است. به طور مثال، برای ارزیابی کیفیت یک وظیفه نرم‌افزاری در کاربرد سیستم، ممکن است بینش‌هایی در مورد اینکه چطور نرم‌افزار تکوین‌یافته می‌شود به دست آوریم. بازنگری فرآیند طراحی آن برای تشکیل عقیده ذهنی برای سنجش می‌تواند این کار را انجام دهد. هدف حصول اطمینان کاربر از اعتماد به کفایت نرم‌افزار برای کاربرد است. تا زمانی که نرم‌افزار را در سیستم رایانه‌ای برای اثبات خصایص کیفیت آن در عملکرد واقعی اجرا نکنیم نمی‌توانیم مطمئن باشیم. این کار اثبات عملی قاطعی را برای شواهد عینی فراهم می‌کند. در اقدامات مهندسی، ارزیابی‌های عینی و ذهنی استفاده می‌شوند که یکدیگر را در فرآیند سنجش کامل کنند.

موارد ذیل اهداف اصلی مرتبط پروژه را با ارزیابی قابلیت اعتماد سیستم در نقاط تصمیم اصلی روی چرخه‌ی عمر سیستم فراهم می‌کنند:

الف) شناسایی بازار – هدف شناسایی نیازهای بازار برای توجیه سرمایه‌گذاری‌ها برای تکوین سیستمی جدید یا ارتقای یک سیستم موجود برای رقابت است. تحلیل بازار برای توجیه سرمایه‌گذاری‌های اصلی مرتبط با تعهدات منبع ضروری است. فعالیت‌های مهندسی سیستم‌ها با توانمندی و شناسایی منبع، سنجش فناوری جدید برای کاربرد ممکن، تحلیل رقابتی و انتظار عملکرد سیستم از طرف کاربر وسعت پشتیبانی نگهداری لازم برای تقویت یا بهره‌برداری خدمت ارتقاء یافته یا جدید، قیود هزینه و زمان برای ورودی بازار و پیامد محیطی و تنظیمی روی عرضه سیستم ارتباط دارد. ساختار و پیکره‌بندی سیستم اولیه بایستی برای برآورده کردن سناریوهای بهره‌برداری قابل کاربرد سیستم در نظر گرفته شود. هزینه‌های چرخه‌ی عمر سیستم بایستی بر یک مبنای بازگشت به سرمایه آزمایش شود. ارزیابی قابلیت اعتماد کلیدی برای پشتیبانی شناسایی بازار شامل موارد زیر می‌شود:

- پیش‌بینی قابلیت اعتماد سیستم برای برآورده کردن نیازهای پیش‌بینی شده بازار؛
- سنجش تکامل فناوری جدید مناسب برای کاربردهای سیستمی اثربخش برای عملکرد قابلیت اعتماد؛
- شناسایی موضوعات قابلیت اعتماد حیاتی مرتبط با پیامد قابلیت خدمات‌دهی و تأثیر قابلیت بهره‌برداری؛
- سنجش توانمندی قابلیت اعتماد بالقوه تأمین‌کنندگان و پیمانکاران جزء؛
- تضمین استمرار خدمت نگهداری، آمادگی و ایمنی تا زمانی که سیستم کاملاً از کار می‌افتد.

ب) طراحی و تکوین سیستم – هدف توجیه عقلانی رویکرد طراحی سیستم و سنجش گزینه‌ها و جایگزین‌های طراحی است. طراحی منتخب بوسیله تکوین سیستم دنبال می‌شود. این کار یک تعهد اصلی برای سرمایه‌گذاری‌های منبع و ثابت است. فعالیت‌های مهندسی سیستم با تحلیل الزامات، پیکره‌بندی طراحی معماری، طراحی وظیفه‌ای و سنجش فناوری، منبع‌یابی از خارج برای کار قرارداد فرعی و انتخاب تأمین‌کنندگان، یکپارچگی و تحقق سیستم، آزمون احراز شرایط و تصدیق، نصب سیستم و گذر برای خدمات بهره‌برداری مورد نیاز ارتباط دارد. ارزیابی قابلیت اعتماد کلیدی برای پشتیبانی طراحی و تصمیم تکوین شامل موارد زیر می‌شود:

- سنجش وظایف اثربخش سیستم بر روی عملکرد قابلیت اعتماد؛
- سنجش ساختار سیستم برای بهینه‌سازی قابلیت اطمینان پیکره‌بندی سیستم؛
- سنجش دسترسی به نگهداری؛
- شبیه‌سازی عملکرد آمادگی سیستم و سنجش عملکرد برای تعیین عیب فنی حیاتی سیستم، کاهش وقوع خرابی و نیازهای پشتیبانی خدمات؛
- تصدیق قابلیت اطمینان و تحلیل مشکل برای اقدامات اصلاحی؛
- سنجش برنامه‌های قابلیت اعتماد تأمین‌کنندگان و پیمانکاران جزء؛
- ارزیابی قابلیت ساخت برای زمینه تولید اثربخش بر رشد قابلیت اطمینان؛
- سنجش محرک‌های وارانتی قابلیت اطمینان و الزامات پشتیبانی لجستیک.

پ) تحقق و پیاده‌سازی سیستم – هدف اجرای تصمیمات ساخت- خرید برای اکتساب و به کارگیری عناصر زیر سیستم و پیاده‌سازی تعهدات منبع برای ساخت و یکپارچگی سیستم است. ارزیابی قابلیت اعتماد کلیدی برای پشتیبانی تحقق و پیاده‌سازی سیستم شامل موارد زیر می‌شود:

- ارزیابی عناصر سیستم و تطابق محصولات بازاری (COTS[1]) با الزامات قابلیت اعتماد برای یکپارچگی زیر سیستم؛
- ارزیابی تابعیت زیر سیستم از الزامات قابلیت اعتماد؛
- ارزیابی فرآیند تضمین از کیفیت؛
- سنجش نتایج عملکرد آزمون زیر سیستم برای یکپارچگی سیستم؛
- سنجش نتایج عملکرد آزمون سیستم برای تدارک پذیرش سیستم.

ت) پذیرش سیستم برای بهره‌برداری حین خدمت- هدف حصول اطمینان مشتری از اعتماد به پذیرش سیستم است. این مورد با انتقال مسؤولیت برای مشتری در بهره‌برداری حین خدمت ارتباط دارد. این مورد با دوره وارانتی آغاز می‌شود تا اطمینان حاصل شود که عملکرد سیستم انتظارات کاربر نهایی را برآورده می‌سازد. ارزیابی قابلیت اعتماد کلیدی برای حصول اطمینان از پذیرش سیستم شامل موارد زیر می‌شود:

- سنجش عملکرد سیستم توسط معرفی ردگیری میدانی و نقشه‌های گزارش رخداد؛
- ارزیابی نیازهای آموزش و شایستگی اپراتورها و متخصص نگهداری‌های مشتری؛
- ایجاد یک نقطه مرکزی برای جمع‌آوری داده‌ها و تحلیل گزارش رخداد برای تعیین روندهای عملکرد قابلیت اعتماد و بحرانیت عیب فنی سیستم نیازمند اقدامات اصلاحی فوری؛
- سنجش خدمت نگهداری سیستم و تأثیر پشتیبانی لجستیک؛
- روش‌های اجرایی برای مجوز دادن به تغییر طراحی و مدیریت پیکره‌بندی.

ث) ارتقای سیستم– هدف توجیه سرمایه‌گذاری برای ارتقاء، یا پیشرفت سیستم موجود می‌باشد. این مورد با فعالیت‌های مشابه برای تکوین و طراحی سیستم جدید برای قسمت ارتقای سیستم ارتباط دارد. برای حصول اطمینان از عملکرد داخلی و بهبود توانمندی خدمت باید به موضوعات موروثی از سیستم‌های موجود پرداخته شود. ارزیابی قابلیت اعتماد کلیدی برای پشتیبانی تصمیم ارتقای سیستم شامل موارد زیر می‌شود:

- تحلیل منفعت‌های هزینه برای مشارکت در تغییر؛
- سنجش پیامد عملکرد قابلیت اعتماد به علت تغییرات با خصایص اضافه شده جدید؛
- واکنش مشتری به تغییرات پیشنهاد شده؛
- ارزیابی‌های مقدار و ریسک.

ج) کنار گذاری سیستم– هدف کنار گذاری سیستم از خدمت است. ارزیابی قابلیت اعتماد کلیدی برای پشتیبانی تصمیم به کنار گذاری شامل موارد زیر می‌شود:

- سنجش پیامد هزینه برای پایان خدمت سیستم؛
- سنجش پیامد محیطی و تنظیمی برای پایان خدمت سیستم.

---

1 - Commercial Off-The-Shelf

۶-۳-۳ روش‌شناسی برای ارزیابی‌های قابلیت اعتماد سیستم

روش‌شناسی ارزیابی به موضوعات پیاده‌سازی مرتبط با فرآیندها، رویکردها و راهبردها را می‌پردازد.

روش‌شناسی ارزیابی دو فرآیند مهم را به همراه دارد:

الف) تصدیق- فرآیند تصدیق یک روش برای تطابق نتایج ارزیابی است. این مورد بایستی برای پشتیبانی نقاط تصمیم اصلی در هر مرحله چرخه‌ی عمر سیستم هدایت شود؛

ب) صحه‌گذاری- فرآیند صحه‌گذاری شواهد عینی را فراهم می‌کند که سیستم الزامات واقعی را برآورده می‌سازد و انتظارات کاربر را برآورده می‌کند.

رویکردهای ارزیابی اغلب برای تطبیق موقعیت‌های پیاده‌سازی مختلف پروژه منحصر به فرد می‌باشند. آن‌ها شامل ترکیبی از رویکردهای ذیل می‌شوند:

۱. **رویکرد تحلیلی**- این رویکرد با فعالیت‌هایی از قبیل تحلیل طراحی، شبیه‌سازی عملکرد سیستم، انطباق استانداردسازی و سنجش مشخصات انطباق ارتباط دارد.
۲. **رویکرد آزمایشگاهی**- این رویکرد با فعالیت‌هایی از قبیل آزمون عملکرد و سنجش فنی وظایف سیستم، مونتاژهای فیزیکی، محصولات تأمین‌کننده، یکپارچگی زیرسیستم‌ها و پذیرش واقعی سیستم ارتباط دارد.
۳. **رویکرد مشاوره‌ای**- این رویکرد با فعالیت‌هایی از قبیل بازنگری‌های متخصص، استفاده از بهترین تمارین صنعتی، مشاوره تأمین‌کنندگان درباره اطلاعات محصول، نظرسنجی مشتری و بازخورد کاربر، اشتراک زنجیره تأمین، تکوین و ارتقای زیرساخت‌ها ارتباط دارد.
۴. **رویکرد مذاکره**- این رویکرد با فعالیت‌هایی از قبیل ایجاد حدود ریسک قابل پذیرش برای قرار گرفتن سیستم مورد بهره‌برداری در معرض محیط، شرایطی برای به کارگیری محصول در نواحی خاص، بازیافت محصول جانبی و ضایعات وارهایی شده، انگیزه‌های اقتصادی و منافع اجتماعی در موافقت‌های قرارداد و انطباق با تغییر مقررات ارتباط دارد.

راهبردهای ارزیابی بایستی روی دو جنبه عمده در مهندسی قابلیت اعتماد درون سیستم تمرکز کنند:

I) **تمرکز بر کاربرد**- این مورد با برآورده‌سازی کاربردهای خاص پروژه برای انطباق با الزامات قراردادی ارتباط دارد. فعالیت‌های ارزیابی ضروری روی سنجش و تحلیل قابلیت اعتماد سیستم در نقاط تصمیم اصلی چرخه‌ی عمر قابل کاربرد سیستم تمرکز دارند. این روش‌ها و ابزار قرار گرفته برای ارزیابی به طور مشترک برای تصدیق محصول و صحه‌گذاری سیستم یا زیر سیستم استفاده می‌شوند.

II) **تمرکز بر فناوری**- این مورد با سنجش فناوری راهبرد طراحی و نقشه‌های پشتیبانی سیستم برای تسهیل دستیابی‌های عملکرد قابلیت اعتماد ارتباط دارد. فعالیت‌های ارزیابی ضروری روی سنجش شیوه به کار بردن فناوری تمرکز دارند که می‌تواند برای طراحی سیستم و تعیین دوام سیستم‌های توانا ساز برای پشتیبانی از استمرار بهره‌برداری حین خدمت از سیستم بهره‌برداری شود. موضوعات مرتبط با سیر تکامل فناوری و از کارافتادگی بایستی قسمتی از راهبردهای ارزیابی را تشکیل دهند.

۶-۳-۴ مفاهیم و مقدار ارزیابی

ارزیابی یک پیش‌نیاز و ورودی تعیین‌کننده برای تصمیم‌گیری در پروژه‌ها می‌باشد. تلاش ارزیابی بایستی برای کاربرد اقداماتی به طور عقلانی توجیه شود. تفکیک موضوعات مرتبط بایستی درون حدود زمانی منطقی برای تحقق مقدار مورد انتظار یا منافع پروژه کامل شود. این کار اطمینان مورد نیاز را برای پشتیبانی از تصمیمات پروژه ایجاد می‌کند. موضوعات کلیدی ذیل که با مثال مقدار ارزیابی را نشان می‌دهند برای تفسیر یادآوری می‌شوند. مثال‌های نوعی برای بیشتر مشخص کردن معانی اصلی برای نتایج پروژه نشان داده می‌شوند.

الف) زمان‌بندی ارزیابی برای فراهم نمودن نتایج معنادار تعیین‌کننده است. مقدار ارزیابی هنگامی که نتایج ارزیابی در زمان مورد نیاز برای پشتیبانی تصمیمات اصلی در دسترس نیستند به طور عمده تقلیل می‌یابد. به طور مثال، یک پیش‌بینی قابلیت اطمینان هدایت شده طی طراحی سیستم ممکن است بینش‌های با ارزشی را برای انتخاب فناوری مناسب، ساختار طراحی معماری، پیکره‌بندی اجزاء و انتخاب عناصر و اجزای سیستم برای تحقق وظایف سیستم فراهم کند. یک پیش‌بینی انجام شده بعد از تکمیل طراحی مقداری محدود دارد هنگامی که سیستم پیکره‌بندی و برای تولید آماده می‌شود.

ب) توجیه منافع هزینه ارزیابی مقدم بر شروع آن برای احتیاط در مورد طرح پروژه و مدیریت اثربخش آن است. به طور مثال، فرآیند طرح-اجرا-بررسی-عمل در سیستم‌های مدیریت کیفیت (QMS) به طور مشترک به عنوان پایه‌ای برای فعالیت‌های ارزیابی طرح استفاده می‌شود. تحلیل سرمایه‌گذاری مرتبط با ارزیابی برای توجیه مخارج و اکتسابات عمده اصلی حیاتی است.

پ) حصول اطمینان از پشتیبانی زیرساخت‌ها برای پیاده‌سازی ابزار ارزیابی کافی است. این کار ممکن است با تغییرات روش‌های اجرایی فنی و هنجارهای فرهنگی ارتباط داشته باشد که زمان و تلاش را به کار می‌برند. به طور مثال، جابجایی از فرآیند مدل تکامل توانمندی نرم‌افزار به فرآیند یکپارچگی تکامل توانمندی نرم‌افزار یک تلاش برای هر شرکت سهامی است. منابع فنی و فرهنگ مدیریت نیاز به تنظیماتی برای دستیابی به گواهی و وضعیت به رسمیت شناخته شده صنعتی خواهد داشت.

ت) طرح بهره‌برداری احتمالی برای اجتناب از پیامدهای ناخواسته پروژه یا تأخیرهای برنامه‌ریزی نشده ضروری است. این کار ممکن است پیامد تخصیص منبع و دوباره به کارگیری کار، توزیع زنجیره تأمین و تحویل محصولات تأمین‌کننده باشد و روی تعهدات برنامه‌ریزی شده برای راه‌اندازی سیستم و پذیرش مشتری تأثیر بگذارد. به طور مثال، در نقاط اصلی تصمیم، طرح‌های وقایع بایستی قسمتی از فرآیند ارزیابی را شامل شود، از قبیل شناسایی تأمین‌کنندگان جایگزین در مورد قطع تأمین‌کننده، به کارگیری تجربه فنی برای کار روی طراحی‌های حیاتی برای برآورده سازی اهداف دقیق تحویل و کاوش در مورد وسایل قابل دوام مالی برای سرمایه‌گذاری‌های ثابت.

۶-۴ اندازه‌گیری قابلیت اعتماد سیستم

۶-۴-۱ مقصود از اندازه‌گیری‌های قابلیت اعتماد سیستم

از منظر مهندسی، اندازه‌گیری‌های قابلیت اعتماد سیستم فرآیند انتساب مقدار کمی را برای مشخص کردن صفت قابلیت اعتماد نشان می‌دهد. مقدار کمی از داده‌های تخمین زده شده یا مشاهده شده در طی زمان و تعداد وقوع رخدادها نتیجه می‌شود تا ویژگی‌های عملکرد قابلیت اعتماد را منعکس کند. فرآیند اندازه‌گیری شامل موارد زیر می‌شود:

الف) شناسایی نوع و هدف اندازه‌گیری تحت قرارداد، بهره‌برداری یا برای شرایط خاص از قبیل سنجش محصول نیازمند کمی‌سازی صفات قابلیت اعتماد؛

ب) تعیین داده‌های مرتبط و ماهیت منابع داده‌ها برای اندازه‌گیری؛

پ) استفاده عملی از سیستم‌های توانا ساز اثربخش برای تسهیل فرآیند اندازه‌گیری از قبیل به کار گیری سیستم‌های جمع‌آوری داده‌ها، گزارش وقوع خرابی، سیستم‌های تحلیل و اقدام اصلاحی، پرسشنامه‌های نظرسنجی، یا نقشه‌های پشتیبانی دیگر؛

ت) تفسیر نتایج اندازه‌گیری برای ایجاد روندهای عملکرد، شناسایی موضوعات حیاتی و پیشنهاد اقدامات مدیریت با استدلالات و توجیه‌ها؛

ث) مستندسازی یافته‌های اندازه‌گیری برای حفظ سابقه، ممیزی‌های کیفیت و شواهد عینی.

ج) [6] ISO/IEC 15939 یک فرآیند اندازه‌گیری قابل کاربرد را برای مهندسی نرم‌افزار و سیستم تعریف می‌کند.

۶-۴-۲ طبقه‌بندی اندازه‌گیری‌های قابلیت اعتماد سیستم

چهار طبقه کلی برای اندازه‌گیری‌های قابلیت اعتماد برای برآورده ساختن نیازهای خاص پروژه وجود دارد.

الف) اندازه‌گیری صفات ذاتی قابلیت اعتماد سیستم- هدف انتساب یک مقدار کیفیِ عددی برای نمایش صفات ذاتی قابلیت اعتماد سیستم است. این طبقه از اندازه‌گیری برای مقایسه صفات قابلیت اعتماد معماری‌های طراحی مختلف و پیکره‌بندی‌های سیستم مفید می‌باشد. فرآیند اندازه‌گیری طی مرحله تعریف/ مفهوم برای تعیین توانمندی گزینه‌های جایگزین عملکرد ذاتی قابلیت اعتماد هدایت می‌شود. مقصود در فراهم نمودن شواهد توانمندی سیستم در برآورده‌سازی اهداف قابلیت اعتماد برای درخواست‌های قرارداد یا طرح پیشنهادی هدف‌گذاری می‌شود. مقادیر عددی می‌توانند بر حسب احتمال موفقیت، زمان بهره‌برداری میانگین بین وقوع خرابی‌ها، طول عمرها یا نرخ‌های وقوع خرابی که آمادگی سیستم یا ویژگی‌های عملکرد قابلیت اطمینان را تعیین می‌کنند، بیان شوند. اندازه‌گیری‌ها همانگونه که در استاندارد ایران آی ای سی ۱-۳-۶۰۳۰۰ [7] توصیف شده به طور مشترک توسط روش‌های پیش‌بینی انجام می‌شوند.

ب) اندازه‌گیری قابلیت اعتماد سیستم برای سنجش عملکرد و بهره‌برداری حین خدمت – هدف انتساب یک عدد برای معین کردن عملکرد قابلیت اعتماد سیستم در بهره‌برداری واقعی است. این طبقه از اندازه‌گیری برای ارزیابی صفات قابلیت اعتماد طی مرحله تکوین/ طراحی مفید است که در آن محصولات و زیرسیستم‌ها برای تصدیق کفایت عملکرد تحت آزمون قرار می‌گیرند. این طبقه همچنین طی مرحله

نگهداری/ بهره‌برداری برای تعیین انطباق با اهداف مربوط به بهره‌برداری ایجاد شده برای دستیابی‌ها به قابلیت اعتماد استفاده می‌شود. فرآیند اندازه‌گیری توسط آزمون تدریجی محصولات، زیرسیستم‌ها و سیستم جامع برای تصدیق و صحه‌گذاری عملکرد و توسط ردیابی وضعیت بهره‌برداری حین- خدمت از سیستم هدایت می‌شود. داده‌های اندازه‌گیری از آزمون‌های احراز شرایط محصول، نتایج آزمون تأمین‌کنندگان در مورد زیر سیستم‌ها، آزمون پذیرش و سوابق عملکرد میدانی و گزارش‌های نقص گرفته می‌شوند. مقادیر عددی می‌توانند به عنوان قابلیت اطمینان، احتمال وقوع خرابی، زمان عاری از وقوع خرابی (زمان تا اولین وقوع خرابی)، طول عمر، درصد زمان آماد (آمادگی)، فراوانی و مدت زمان خروج بیان شوند.

پ) اندازه‌گیری قابلیت اعتماد سیستم برای بهبودهای عملکرد- هدف انتساب مقداری برای تعیین کمی و کیفی درجه رضایت مشتری، یا تعیین گستره مقدار مشتری برای بهبودهای عملکرد می‌باشد. این کار یک اندازه‌گیری غیرمستقیم است که به شناسایی پیامد صفات قابلیت اعتماد معنادار در عملکرد سیستم کمک می‌کند. این طبقه از اندازه‌گیری در جستجوی بازخورد مستقیم کاربر در مورد عملکرد سیستم، یا تعیین مقدار تدارک خدمت طی مرحله نگهداری/ بهره‌برداری سیستم هدف‌گذاری می‌شود. فرآیند اندازه‌گیری توسط نظرسنجی‌های مشتری، ممیزی‌های عملکرد، ارزیابی‌های مقدار و تماس‌ها و مکالمه‌های مستقیم مشتری‌ها و تأمین‌کنندگان هدایت می‌شود. نظرسنجی‌های رضایت مشتری روی شناسایی موضوعات جاری در مورد ارتباطات مشتری متمرکز می‌شود. به کارگیری وظیفه کیفیت به طور مشترک برای ارزیابی مقدار عملکرد برای تعریف نیازهای مشتری و تفسیر آن‌ها به الزامات فنی مقتضی برای اقدامات در برآورده کردن آن نیازها استفاده می‌شود. انتساب مقدار می‌تواند در یک مقیاس ۱ تا ۵ شامل نمایش نرخ‌هایی از قبیل ضعیف به عالی بیان شود.

ت) اندازه‌گیری قابلیت اعتماد سیستم برای مواجهه با ریسک - هدف انتساب مقادیر عددی برای نمایش گستره مواجهه با ریسک است هنگامی که سیستم برای کاربردهای ایمنی و امنیتی استفاده می‌شود. این مورد یک اندازه‌گیری غیرمستقیم برای شناسایی وضع بحرانی صفات قابلیت اعتماد اثربخش بر وظایف عملکرد سیستم است. این طبقه از اندازه‌گیری طی مرحله تعریف/ مفهوم برای شناسایی وظایف حیاتی سیستم و عناصر بهره‌برداری یا مأموریت خاص سیستم هدایت می‌شود. فرآیند ارزیابی شامل تعیین تهدید یا زیان توسط شناسایی شدت و فراوانی رخداد می‌شود. طبقه‌بندی ریسک‌ها می‌تواند به طور کیفی توسط گستره‌ای از حوادث فاجعه‌بار، بحرانی، عمده، جزئی یا قابل چشمپوشی ایجاد شود. مقادیر احتمالی می‌توانند برای نمایش شدت وضعیت توسط بیانیه‌ای از قبیل یک رخداد وقوع خرابی حیاتی در هر ۱۰ سال انتساب شوند. استاندارد ملی ایران آی ای سی ۹-۳-۶۰۳۰۰ روش‌های ارزیابی ریسک فناورانه اثربخش بر صفات عملکرد سیستم را توصیف می‌کند. یک روش مشابه در IEC 61508 series [9] درباره سطوح انسجام-ایمنی برای رتبه‌بندی وظایف ایمنی استفاده می‌شود (برای جزئیات بیشتر به IEC 61508-1 [10] مراجعه کنید).

۶-۴-۳ منابع اندازه‌گیری

اندازه‌گیری‌های صفات قابلیت اعتماد سیستم می‌تواند توسط آزمون عملکرد مستقیم تحت شرایط شبیه‌سازی شده یا در محیط بهره‌برداری واقعی تعیین شود که در آن داده‌های مرتبط می‌توانند جمع شوند.

صفات قابلیت اعتماد سیستم می‌تواند بوسیله پیش‌بینی‌هایی بر پایه تاریخچه عملکرد میدان برای سیستم-های مشابه ارزیابی شود، یا می‌تواند از پایگاه داده قابلیت اطمینان ایجاد شده با آگاهی از پیکره‌بندی سیستم و وظایف بهره‌برداری عناصر سیستم تشکیل‌دهنده آن نتیجه شود.
داده‌های اندازه‌گیری مربوط به صفات قابلیت اعتماد می‌توانند از منابع دیگر از قبیل برنامه‌های آزمون تأمین‌کنندگان، داده‌های پشتیبانی نگهداری، اطلاعات وارانتی و نظرسنجی‌های مشتری گرفته شوند. مهم است که انسجام داده‌های استفاده شده در ارزیابی قابلیت اعتماد برای اهداف تضمین صحه‌گذاری شود.

۶-۴-۴ سیستم‌های توانا ساز اندازه‌گیری‌های قابلیت اعتماد

انسجام داده‌ها در اندازه‌گیری‌های قابلیت اعتماد برای حصول اطمینان از درستی، اعتبار و سازگاری فرآیند اکتساب و جمع‌آوری داده‌ها مهم است. این کار اطمینان می‌دهد که داده‌های مرتبط به طور صحیح در تحلیل داده‌ها استفاده می‌شوند و تفسیر مناسبی از نتایج تحلیل‌ها را مجاز می‌سازد. طراحی و قالب‌بندی سیستم بایستی ساده و برای ضبط اطلاعات مورد نیاز مرتبط صریح باشد. ورودی‌های داده‌های خودکار و دسترسی به اطلاعات بر پایه وب سرعت پیاده‌سازی سیستم را ارتقاء می‌بخشد. چندین سیستم پشتیبانی‌کننده مختلف وجود دارند که در اقدامات مهندسی برای توانا سازی جمع‌آوری داده‌های صرفه اقتصادی و تسهیل در اندازه‌گیری‌های قابلیت اعتماد استفاده می‌شوند. این سیستم‌ها قسمت‌های ضروری زیرساخت سیستم مدیریت قابلیت اعتماد می‌باشند. برای نقش‌های پشتیبانی‌کننده خاص آن‌ها، این سیستم-ها می‌توانند به عنوان سیستم‌های توانا ساز قابلیت اعتماد مهندسی در سیستم مورد نظر طبقه‌بندی شوند. سیستم‌های توانا ساز نوعی به طور مشترک استفاده شده برای جمع‌آوری داده‌ها، گزارش نواقص، تحلیل مشکل و اقدام اصلاحی شامل موارد زیر می‌شوند:
الف) سیستم گزارش وقوع خرابی، تحلیل و اقدام اصلاحی برای ضبط اطلاعات عدم تطابق و داده‌های وقوع خرابی آزمون طی تکوین، یکپارچگی و آزمون سیستم؛
ب) آزمون سیستم اکتساب داده‌ها را به ضبط موارد غیرعادی ساخت برای ردیابی نرخ‌های بازده محصول وادار می‌سازد تا تولید را برای نرخ‌های شناسایی مشکل و تحلیل علت-ریشه‌ای طی مونتاژ محصول؛
پ) گزارش رخدادها طی بهره‌برداری حین خدمت از سیستم برای ضبط نواقص اثربخش بر استمرار خدمت عملکرد سیستم، گزارش اقدامات نگهداری در محل، انتصاب وضع بحرانی نقص و ثبت درخواست‌های پشتیبانی پیگیرانه و زمان مورد نیاز برای تفکیک؛
ت) سیستم تدارک یدکی‌ها برای ثبت داده‌های مصرف یدکی‌ها و زمان بازگشت برای تجدید تدارکات یدکی-ها، توزیع یدکی‌ها و ثبت موجودی؛
ج) سیستم بازخورد اطلاعات برای ثبت شکایات مشتری، نگرانی‌های تأمین‌کنندگان و پیشنهادات کارمند برای بهبود زیرساخت، طرح راهبردی و تفکیک مشکلی که ارزشی را به پروژه‌ها و مدیریت سازمانی اضافه نماید.

۶-۴-۵ تفسیر اندازه‌گیری‌های قابلیت اعتماد

تفسیر مناسب نتایج اندازه‌گیری‌ها برای اقدامات پیشگیرانه و اصلاحی بی درنگ به منظور پشتیبانی از بهره‌برداری با صرفه اقتصادی ضروری است. مثال‌های ذیل اهمیت داده‌های تحلیل شده یا اندازه‌گیری شده را نشان می‌دهند هنگامیکه برای اقدامات پیگیرانه تفسیر داده می‌شوند و نقل می‌شوند.

الف) اکتساب و جمع‌آوری داده‌های مرتبط بایستی مقداری را برای برآورده ساختن نیازهای پروژه جاری فراهم کند. این کار اشاره به طرح و طراحی مناسب آزمایشات دارد. این کار نیاز به زمان و تلاش برای اکتساب داده‌ها دارد. اگر این داده‌ها نتوانند به حل مسائل جاری کمک کنند، آنگاه نبایستی جمع‌آوری شوند. هدف فرآیند اندازه‌گیری بایستی به طور واضح تعریف شود. به طور مثال، جمع‌آوری داده‌های عملکرد میدان برای سیستم‌های قدیمی به کار گرفته شده که مدت زیادی در تولید نبوده و پشتیبانی نشده‌اند برای طراحی سیستمی جدید با استفاده از فناوری متفاوت زیاد مفید نخواهد بود.

ب) اندازه‌گیری‌های نقل شده و نتایج تفسیر داده شده بایستی فرجامی منطقی برای اقدامات پیشنهاد شده نشان دهند. داده‌های اندازه‌گیری شده و اطلاعات ضبط شده بایستی تحلیل بیشتر را مجاز سازند اگر نیاز به پشتیبانی از دلایل زیربنایی یا آرگومان‌ها در رسیدن به یک تصمیم منطقی برای توجیه اقدامات پیشنهاد شده باشد. بایستی یادآوری شود که تفسیر متفاوت از اندازه‌گیری‌های قابلیت اعتماد ممکن است منجر به تحقق متفاوت توسط دریافت‌کننده شود، کسی که معمولاً نیاز به اطلاعاتی برای گرفتن تصمیمات دارد. به طور مثال، یک عدد عملکرد آمادگی٪ ۰٫۰۹۹۹۹۹۷ که به یک سیستم کلید زنی منتسب شده ممکن است عددی کافی برای استفاده در محاسبه احتمال وظایف سیستم باشد ولی درست کردن یک نقشه برای اثبات عملی آمادگی سیستم مشکل خواهد بود.

پ) مسائل قابلیت اعتماد شناسایی شده بایستی به بحرانیت موضوعات در دست را بپردازند تا اقدامات مدیریتی را هشدار دهند. مشکلات شناسایی شده در یک فرآیند نیازمند توجه به قابلیت اعتماد تحت موقعیت‌هایی رخ می‌دهد که ممکن است باعث پیامد ایمنی یا امنیتی قابل توجه شوند اگر سریع مورد توجه قرار نگیرند. این موضوعات قابلیت اعتماد ممکن است دارای موضوعات مسئولیتی بالقوه و مواجهه با ریسک باشند اگر در زمانی که اتفاق می‌افتند به طور مناسب ارزیابی نشوند. بهره‌برداری حین خدمت از سیستم روش‌های اجرایی بهره‌برداری ایجاد شده را به دنبال دارد. رخدادهای خروجی سیستم مطابق با ارزیابی وضع بحرانی آن‌ها گزارش می‌شوند. برخی از موضوعات حیاتی بایستی فوراً یا درون یک دوره زمانی محدود حل شوند. دیگر موارد غیر حیاتی ممکن است به یک به روز سازی سیستم یا ارتقای نگهداری بعدی معوق شوند. به طور مثال، یک تعدیل میدانی در طراحی یک سیستم برای تعمیر یک مشکل موقتی بدون مجوز تغییر مناسب در طراحی ممکن است مخاطره‌های ایمنی ناشناخته با زمان طولانی بیافریند. تعمیرات نرم‌افزاری موقتی برای تعمیر یک مسئله موضعی بدون بررسی کامل ممکن است منجر به نقص امنیتی یا خرابی بهره‌برداری سیستم داخلی شود. طراحی قابلیت اعتماد ممکن است خصایص حفاظت مقاومت در برابر خرابی را ترکیب کند. خصایص حفاظتی اگر خنثی شوند یا به علت کنار گذر شدن دسترسی به تعمیرات موقتی بدون مجوز مناسب قطع ارتباط پیدا کنند برای مدت طولانی اثربخش نیستند. فرآیند تفسیر بایستی

شناسایی شود و برای موضوعات مشکل بالقوه را هشدار دهد تا از وقوع دوباره نواقص اجتناب کند. علائم و برچسب‌های هشداردهنده قرار داده شده در موقعیت‌های مناسب می‌توانند جلب توجه کنند.

پیوست الف

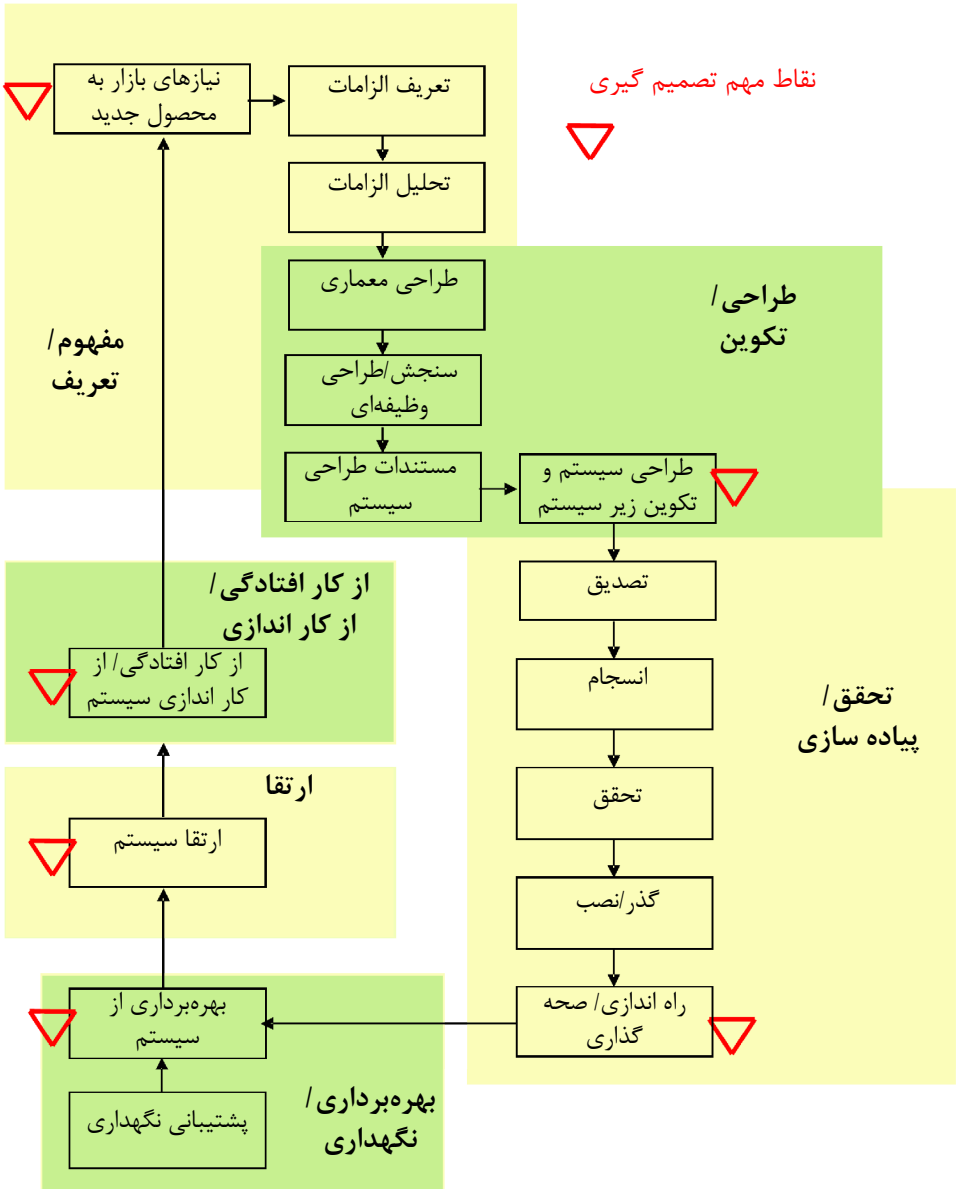
(اطلاعاتی)

فرآیندها و کاربردهای چرخه‌ی عمر سیستم

الف-۱ فرآیندهای چرخه‌ی عمر سیستم

الف-۱-۱ توصیف فرآیندهای چرخه‌ی عمر سیستم

شکل الف-۱ ترتیبی منطقی را از فعالیت‌های قابل کاربرد فرآیند برای هر مرحله از چرخه‌ی عمر برای مهندسی قابلیت اعتماد در سیستم فراهم می‌کند.



شکل الف-۱ مرور کلی فرآیندهای چرخه‌ی عمر سیستم

سه مرحله اول چرخه سیستم، یعنی تعریف/ مفهوم، تکوین/ طراحی و پیاده‌سازی/ تحقق، قبل از گذر به مرحله نگهداری/ بهره‌برداری، به علت تکرار فرآیندها با یکدیگر همپوشانی پیدا می‌کنند. این مورد نشان می‌دهد که نیاز به فراهم نمودن استمرار گردش کار وابسته به نیازهای پروژه وجود دارد. گستره تلاش مهندسی عبوری از مرزهای تعریف شده دلخواه مراحل نزدیک وابسته به خط زمان پروژه و فعالیت‌های هماهنگی است. این مورد برای اکتساب اطلاعات کافی برای پشتیبانی فرآیند تصمیم گیری کسب و کار و فنی نیز استفاده می‌شود. موارد ذیل خلاصه‌ای از توصیف هر مرحله از چرخه‌ی عمر سیستم را فراهم می‌کنند:

الف) مرحله تعریف/ مفهوم برای شناسایی نیازهای بازار، شناسایی/ تعریف استفاده مربوط به بهره‌برداری خط زمان/ محیط، تعریف الزامات ابتدائی سیستم و تصدیق راه‌حل‌های طراحی ممکن توسط عرضه مشخصات فنی برای طراحی سیستم است. انتخاب گزینه‌های طراحی بر پایه تحلیل ریسک، سنجش پیامد و رویکردهای مهندسی عملی است. فعالیت‌های فرآیند با تعریف الزامات، تحلیل الزامات، طراحی معماری و سنجش/ طراحی وظیفه‌ای برای فراهم کردن مشخصات سطح بالای سیستم ارتباط دارد.

ب) مرحله تکوین/ طراحی برای طرح و اجرای روش‌های حل انتخاب شده طراحی مهندسی برای تحقق وظایف سیستم است. این مورد در تلاش تکوین سیستم مقتضی شامل مدلسازی مهندسی، تفسیر نمونه اولیه، ارزیابی ریسک و شناسایی واسط عناصر سیستم و زیر سیستم نقل می‌شود. سنجش سیستماتیک وظایف جامع سیستم هدایت می‌شود تا عملکرد داخلی سیستم و تقابل‌ها با محیط‌های خارجی برای صحه‌گذاری پیاده‌سازی نهایی سیستم تصدیق شود. طرح پشتیبانی نگهداری، دسترسی نگهداری، روش‌های اجرایی بهره‌برداری و تضمین به همراه فرآیندهای پشتیبانی بایستی مقدم بر تحقق سیستم به خوبی ایجاد شود.

پ) مرحله پیاده‌سازی/ تحقق برای اجرای تصمیماتی برای اکتساب و به کارگیری عناصر زیر سیستم می‌باشد. تلاش‌های تحقق با فعالیت‌هایی از قبیل کاربردهای فناوری، ساخت، بسته‌بندی و تأمین منبع‌یابی برای حصول اطمینان از تبدیلی کامل از طراحی سیستم به محصول خاص یا عناصر زیر سیستم ارتباط دارد. محصولات یا عناصر تحقق یافته ممکن است ترکیبی از وظایف سخت‌افزار و نرم‌افزار را دربر داشته باشند. پیاده‌سازی شامل فعالیت‌هایی از قبیل یکپارچگی وظایف سیستم، تصدیق زیرسیستم‌ها و نصب سیستم می‌شود. روش‌های اجرایی پذیرش سیستم بایستی با مشتری برای امتحانات سیستم در محیط بهره‌برداری واقعی مقدم بر راه‌اندازی ایجاد شود. صحه‌گذاری بایستی قسمتی از امتحان فراهم نمودن شواهد عینی برای مطابقت با مشخصات سیستم باشد. بایستی یادآوری شود که تصدیق و صحه‌گذاری فعالیت‌هایی هستند که در هر مرحله از چرخه‌ی عمر سیستم اتفاق می‌افتند و فقط در یکپارچگی سیستم همانگونه که در شکل ۲ نشان داده شده اتفاق نمی‌افتند.

ت) مرحله نگهداری/ بهره‌برداری برای به کارگیری سیستم برای تحویل خدمات و پشتیبانی از توانمندی بهره‌برداری سیستم توسط نگهداری استفاده می‌شود. فعالیت‌های فرآیند شامل بهره‌برداری و نگهداری سیستم برای خدمات بر طبق الزامات عملکردی سیستم، اپراتورها و متخصص نگهداری‌های آموزش دیده

برای شایستگی مهارت‌ها واسط مشتری برای ایجاد رابطه خدمات و نگهداری سوابق وضعیت عملکردی سیستم و گزارش رخدادهای وقوع خرابی برای آغاز اقدامات پیشگیرانه و اصلاحی بهنگام می‌شود. عملکرد سیستم بایستی پایش شود و روی اصلی منظم وارسی شود تا اطمینان حاصل شود که قابلیت اطمینان و کیفیت اهداف خدمت برآورده می‌شوند.

ث) مرحله ارتقاء برای بهبود عملکرد سیستم با خصایص اضافه برای برآورده‌سازی رشد تقاضای کاربر در مورد سیستم است. فعالیت‌های فرآیند شامل ارتقاء نرم‌افزاری، افزایش‌های سخت‌افزاری، آموزش مهارت‌های ساده‌سازی روش‌های اجرایی برای بهبود کارایی مربوط به بهره‌برداری، مدیریت کهنگی، بازسازی سازمانی برای افزایش مقدار مشتری و مصلحت می‌شود.

ج) مرحله از کار اندازی/ از کار افتادگی برای پایان دادن موجودیت سیستم است. به همراه پایان خدمات سیستم برای مشتری، سیستم ممکن است دمونتاژ شود، برای استفاده‌ای دیگر دوباره به کار گرفته شود، یا از امکان تأثیر محیط وارهایی شود. برای سیستم‌های پیچیده، راهبردی برای از کار اندازی بایستی برای رسمی کردن طرح و پیاده‌سازی فرآیند از کار اندازی برای برآورده‌سازی الزامات تنظیمی ایجاد شود. قواعد تنظیمی برای محصولات مصرفی در نظر می‌گیرد که بازگشت و استفاده مجدد یا وارهایی ممکن است وجود داشته باشد.

الف-۱-۲ فعالیت‌های فرآیند برای مراحل چرخه‌ی عمر سیستم

شکل الف-۱ اتصال فعالیت‌های فرآیند مرحله به مرحله در سیستم را در یک چرخه‌ی عمر سیستم نشان می‌دهد. نقاط تصمیم‌گیری اصلی برای نمایش شروع و پایان فعالیت‌های فرآیند در هر مرحله را که در آن تعهدات منبع برای ترقی فرآیندهای فنی ایجاد می‌شوند، نشان داده شده‌اند. داده‌های مرتبط طی فعالیت‌های فرآیند ضبط می‌شوند. آن‌ها اطلاعات ضروری را برای تحلیل هزینه چرخه‌ی عمر و سنجش ریسک برای پشتیبانی تفکیک‌ها و تصمیمات کسب و کار فراهم می‌کنند.

داده‌های مرتبط گرفته شده شامل ورودی‌های کلیدی لازم برای شروع فعالیت‌های فرآیند در هر مرحله، فعالیت‌های قابلیت اعتماد اصلی که انجام می‌شوند، عوامل تاثیرگذار مرتبط برای ملاحظه و خروجی‌های نتیجه شده از تلاش‌های ایجاد شده توسط فرآیند می‌شوند. هنگامی که ممکن است، تقدم و پیامد مربوط به فعالیت‌های فرآیند بایستی نشان داده شوند. این کار اطلاعات مفیدی را برای ارزیابی ریسک و هزینه چرخه-ی عمر فراهم می‌کند. جایی که مقتضی باشد، رویکردهای فنی و روش‌های مهندسی برای فعالیت‌های فرآیند بایستی شناسایی شوند.

الف-۲ مثال‌هایی از کاربردهای فرآیند مهندسی

الف-۲-۱ فرآیندی برای مرحله تعریف/ مفهوم سیستم

ورودی‌ها:

- الزامات مشتری، نیازها و خواسته‌ها؛
- الزامات قراردادی مرتبط با سلامتی، ایمنی، امنیت و نگرانی‌های محیطی؛
- خط مشی شرکت در مورد تصمیمات پیشنهادی؛

- آگاهی از بازار و رقابت‌ها.

فعالیت‌های کلیدی فرآیند	فعالیت‌های مرتبط با قابلیت اعتماد
تعریف الزامات	
• شناسایی مشتری سیستم، چطور سیستم استفاده می‌شود و برای چه مدت؛ • شناسایی محیط‌های کاربردی سیستم؛ • شناسایی قیود مرتبط با روش‌های حل بالقوه سیستم؛ • شناسایی موضوعات مرتبط با عملکرد متقابل سیستم‌های موجود؛ • ایجاد پروفایل بهره‌برداری سیستم؛ • مستندسازی مشخصات سیستم؛ • شناسایی برنامه‌های زمان‌بندی و اهداف قابل تحویل سیستم؛ • پاسخ به RFP[1] مشتری (درخواست برای پیشنهاد) اگر قابل کاربرد باشد.	• شناسایی نیازهای قابلیت اعتماد مرتبط با کاربردهای سیستم؛ • شناسایی آمادگی سیستم و زمانهای ناآماد خروج مجاز قابل قبول توسط مشتری؛ • شناسایی قیود فناوری مرتبط با دامنه کاربرد و گستره دستیابی به اهداف قابلیت اعتماد؛ • آگاهی از بهره تاریخچه عملکرد میدانی موجود یا سیستم‌های مشابه اگر در دسترس باشند.

1 - Reguest for proposal

تحلیل الزامات	
• تعیین مرزهای سیستم وظایف بهره‌برداری و ویژگی های عملکردی از مجموعه الزامات تعریف شده سیستم؛ • سنجش قیود شناسایی شده اثربخش بر طراحی معماری؛ • تعیین امکان پذیری و رویکردهای فنی برای تحقق سیستم؛ • تعیین مقیاس‌های کیفیت و فنی که ارزیابی‌های سیستم را ممکن می‌سازد؛ • شناسایی توانمندی برای تعهد کار سیستم؛	• تعیین سناریوی بهره‌برداری برای ارزیابی‌های قابلیت اعتماد؛ • تعریف وقوع خرابی‌های سیستم و حدود تنزل عملکرد؛ • شناسایی مواجهات با ریسک و بحرانیت وقوع خرابی‌های سیستم؛ • تعیین تعداد متخصص نگهداری‌ها و سطح مهارت مرتبط مورد نیاز آن‌ها؛ • تحلیل ساختار سیستم و تجزیه وظایف سیستم؛ • تحلیل آمادگی سیستم با کمک پیکره‌بندی وظیفه‌ای طراحی سیستم؛ • اجرای تحلیل درخت وقوع خرابی برای تعیین نواحی بحرانی نیازمند توجه به طراحی؛ • هدایت مُدها و آثار وقوع خرابی سطح سیستم و تحلیل بحرانیت برای پشتیبانی از توجیهات و جایگزین‌های طراحی؛ • سنجش آمادگی سیستم و سبک سنگین کردن هزینه اثربخش بر گزینه‌های طراحی؛ • تعیین وسایلی برای ارزیابی‌های قابلیت اعتماد. • شناسایی شراکت بالقوه و الزامات تأمین‌کنندگان.
طراحی معماری	
• تعیین گزینه‌های طراحی معماری منطقی کافی؛ • ایجاد پیکره‌بندی سیستم؛ • قسمت‌بندی وظایف سیستم؛ • ایجاد معیارها و واسط‌های طراحی؛ • فرمول بندی تصمیمات وظایف سیستم؛ • انتخاب فناوری‌هایی برای طراحی و انتخاب نرم‌افزار/ سخت‌افزار برای تحقق وظایف؛ • فرمول بندی راه‌حلی برای برآورده‌سازی الزامات سیستم؛ • ایجاد وسایلی برای تصدیق و یکپارچگی وظایف سیستم.	• ایجاد طرح برای سنجش قابلیت اعتماد؛ • تخصیص آمادگی برای وظایف سیستم؛ • تعیین معیارهای وقوع خرابی برای وظایف سیستم؛ • سنجش قابلیت اطمینان هر وظیفه جزءبندی شده پیشنهاد تعویض گزینه‌های طراحی در صورت نیاز؛ • شناسایی وظایف بحرانی نیازمند توجه؛ • ایجاد معیارهای قابلیت نگهداری برای طراحی؛ • ایجاد قابلیت آزمون در وظایف سیستم برای تشخیص عیب و پیشنهاد به اقدامات نگهداری.

سنجش/ طراحی وظیفه‌ای	
• فرمول بندی فرآیند طراحی وظیفه‌ای؛ • شناسایی ترکیب طراحی عناصر نرم‌افزار/ سخت‌افزار برای هر وظیفه؛ • ترکیب وظایف آزمون برای تصدیق عملکرد؛ • ایجاد معیارهای طراحی عواملی انسانی؛ • ایجاد معیارهای طراحی محیطی؛ • ایجاد معیارهای طراحی آرگونومیک؛ • ایجاد معیارهای طراحی EMC؛ • ایجاد معیارهای طراحی ایمنی، امنیت و قابلیت اطمینان؛ • ایجاد قواعد طراحی سخت‌افزاری؛ • ایجاد نقشه‌های طراحی تکامل نرم‌افزاری؛ • شبیه‌سازی عملکرد سیستم در سطح وظیفه‌ای برای تعیین پوشش خرابی و راهبرد بازیابی سیستم؛ • تصدیق حدود عملکرد و ارتباط متقابل طراحی وظیفه‌ای برای برآورده‌سازی الزامات طراحی معماری.	• هدایت ارزیابی قابلیت اعتماد؛ • هدایت سنجش قابلیت نگهداری؛ • هدایت مُدها و آثار وقوع خرابی سطح وظیفه‌ای و تحلیل وضع بحرانی؛ • هدایت سبک سنگین کردن طراحی سطح وظیفه‌ای، مقاومت در برابر خرابی و سنجش ریسک؛ • ایجاد طرح نگهداری و پشتیبانی لجستیک؛ • ایجاد فرآیندی برای سنجش پشتیبانی‌کننده برای تضمین کیفیت و مطابقت از قابلیت اطمینان؛ • ایجاد فرآیندی برای پذیرش و سنجش محصول تجاری.
مستندات طراحی سیستم	
• مستندسازی مشخصات سیستم.	• ترکیب الزامات قابلیت اعتماد در مشخصات سیستم.

عوامل تاثیرگذار برای ملاحظه:

- رقابت‌ها؛
- موضوعات اقتصادی؛
- موضوعات فناوری؛
- موضوعات توانمندی؛
- موضوعات محیطی؛
- موضوعات قانونی؛
- زمانبندی برای موضوعات سرمایه‌گذاری‌ها.

مکانیزم‌های توانا ساز برای کاربردهای فرآیند:

- منابع انسانی؛
- منابع مالی؛
- تسهیلات؛
- فرآیندهای پیاده‌سازی و طراحی جامع؛

- فرآیند تضمین.

خروجی‌ها:

- مشخصات سیستم؛
- آگاهی از طراحی سیستم.

الف-۲-۲ فرآیندی برای مرحله تکوین/ طراحی سیستم

ورودی‌ها:

- مشخصات سیستم؛
- الزامات طراحی معماری؛
- طرح قابلیت اعتماد.

فعالیت‌های کلیدی فرآیند	فعالیت‌های مرتبط با قابلیت اعتماد
طراحی سیستم	
• ایجاد طرح تکوین/ طراحی سیستم؛ • مشخص کردن الزامات واسط سیستم/ زیر سیستم؛ • ایجاد ارتباط با سیستم‌های متقابل؛ • ایجاد الزامات واسط انسانی؛ • ایجاد طرح مدیریت پیکره‌بندی و روش‌های اجرایی تغییر طراحی؛ • ایجاد ابعاد فیزیکی و استاندارد کردن رد پاهای مونتاژ؛ • ایجاد قواعد آمادگی و انتشار برای ساخت تسهیلات، سیم‌کشی و سیم‌بندی درون و خارج ساختمان‌ها و ساختارهای تجهیزاتی خانه‌سازی؛ • رسیدن به توافقاتی با تأمین‌کنندگان برای تکوین و اکتساب عناصر نرم‌افزاری/ سخت‌افزاری؛ • آغاز ساخت نمونه اولیه برای زیر سیستم‌ها؛ • ایجاد روش‌های اجرایی یکپارچگی سیستم؛ • ایجاد طرح آزمون و معیارهای پذیرش سیستم؛ • ایجاد پایش، نقشه‌های عیب‌یابی، گزارش رخدادها و سیستم مدیریت داده‌ها برای سیستم؛ • ایجاد برنامه‌های آموزش.	• ایجاد برنامه قابلیت اعتماد سیستم؛ • ایجاد برنامه تضمین کیفیت برای سیستم؛ • فرمول بندی الزامات قابلیت اعتماد برای سیستم، زیر سیستم و وظایف؛ • ایجاد برنامه‌های قابلیت اعتماد تأمین‌کنندگان؛ • ایجاد معیارهای پذیرش قابلیت اعتماد و برنامه‌های رشد قابلیت اطمینان؛ • ایجاد برنامه پشتیبانی لجستیک و نگهداری برای سیستم؛ • ایجاد گزارش وقوع خرابی، تحلیل، سیستم جمع‌آوری داده و بازخورد؛ • تعریف معیارهای قابلیت اطمینان انسانی؛ • تعریف شرایط وارانتی.
تکوین زیر سیستم	
• آغاز تکوین داخلی برای زیر سیستم‌ها؛ • آغاز تکوین واسط برای عملکرد متقابل با قسمت-های دیگر؛ • پایش و همکاری با برون سپاری و تلاش‌های تکوین خارجی متعهد؛ • آماده‌سازی طرح تولید؛ • آماده‌سازی طرح بهره‌برداری؛ • آماده‌سازی طرح پشتیبانی لجستیک و نگهداری؛ • آماده‌سازی طرح بسته‌بندی، جابجایی، انبارش و حمل و نقل؛ • آماده‌سازی طرح نصب؛ • آماده‌سازی طرح یکپارچگی. **یادآوری**- طرح‌های فهرست شده ممکن است به عنوان فعالیت-هایی در طرح پروژه اصلی برای راحتی به روز سازی و هماهنگی فعالیت‌های پروژه جمع شوند.	• پیاده‌سازی برنامه قابلیت اعتماد زیر سیستم؛ • پیاده‌سازی برنامه قابلیت اعتماد تأمین‌کنندگان؛ • تکوین برنامه تدارک یدکی؛ • تکوین برنامه عیب‌یابی و آزمون نرم‌افزاری.

عوامل تاثیرگذار برای ملاحظه:

- آمادگی و دسترسی به منابع مهارت‌های مرتبط؛
- اهداف تعهد برای برنامه‌های زمانبندی تکوین؛
- ریسک‌های پروژه.

مکانیزم‌های توانا ساز برای کاربردهای فرآیند:

- آمادگی ابزار خاص مورد نیاز برای تکوین؛
- نیازهای آموزش.

خروجی‌ها:

- نمونه اولیه سیستم؛
- الزامات پشتیبانی سیستم و زیر سیستم.

الف-۲-۳ فرآیندی برای مرحله پیاده‌سازی/ تحقق سیستم

ورودی‌ها:

- نمونه اولیه سیستم؛

فعالیت‌های کلیدی فرآیند	فعالیت‌های مرتبط با قابلیت اعتماد
تحقق	
• اجرای تولید فیزیکی زیر سیستم‌ها؛ • تحقق ساخت عناصر نرم‌افزاری/ سخت‌افزاری؛ • اجرای سنجش آزمون برای وظایف؛ • انجام آموزش اپراتورها و متخصص نگهداری‌ها؛ • حصول اطمینان از اینکه تجهیزات آزمون و تسهیلات آزمون آماده می‌باشند؛ • حصول اطمینان از اینکه بسته‌بندی، هدایت، انبار کردن و دستورالعمل‌های حمل و نقل آماده باشند.	• پیاده‌سازی برنامه قابلیت اعتماد سیستم؛ • پیاده‌سازی برنامه تضمین کیفیت؛ • پیاده‌سازی برنامه‌های قابلیت اعتماد تأمین‌کنندگان؛ • پیاده‌سازی برنامه پشتیبانی لجستیک و نگهداری سیستم؛ • پیاده‌سازی گزارش وقوع خرابی، تحلیل، جمع‌آوری داده‌ها و سیستم بازخورد.
یکپارچگی	
• اجرای طرح یکپارچگی؛ • مونتاژ و یکپارچه کردن موجودیت سیستم؛ • آماده‌سازی طرح‌ها و روش‌های اجرایی تصدیق و صحه‌گذاری؛ • آماده سازی طرح پذیرش سیستم.	• پیاده‌سازی یکپارچگی مرتبط با برنامه قابلیت اعتماد سیستم؛ • پیاده‌سازی یکپارچگی مرتبط با برنامه تضمین کیفیت.
تصدیق	
• پیاده‌سازی طرح تصدیق؛ • مستندسازی نتایج آزمون تصدیق؛ • آماده‌سازی طرح پذیرش سیستم؛ • وارسی نتایج تصدیق در مقابل طرح پذیرش سیستم.	• هدایت ارزیابی‌های قابلیت اعتماد زیر سیستم؛ • مستندسازی گزارش‌های وقوع خرابی از آزمون‌های تصدیق؛ • ساختن گزارش‌های رخداد برای اقدامات پیشگیرانه/ اصلاحی پیشنهاد شده؛ • حل موارد غیرعادی یافت شده طی تصدیق.
گذار/ نصب	
• اجرای طرح نصب؛ • مستندسازی سوابق و روش‌های اجرایی نصب؛ • سنجش راهبرد گذر برای بهبود.	• ایجاد پشتیبانی نگهداری و نقشه‌های گزارش به اشتراک گذاشته شده شده با متخصص نگهداری‌های مشتری در سیستم نصب شده بر مبنای فرضیات مشتری؛ • پایش زمان بازگشت برای توان‌یابی سیستم و تجدید تدارکات یدکی؛ • نگهداری فهرست موجودی یدکی مناسب درباره قسمت مشتری/ متخصص نگهداری
صحه‌گذاری/ راه‌اندازی	
• پیاده‌سازی طرح صحه‌گذاری؛ • مستندسازی نتایج آزمون صحه‌گذاری؛ • اجرای طرح پذیرش سیستم؛	• صحه‌گذاری بر اینکه عملکرد سیستم الزامات قابلیت اعتماد را برآورده می‌سازد؛ • مستندسازی گزارش‌های وقوع خرابی از آزمون‌های

• پیاده‌سازی نقشه‌های وارانتی اگر قابل کاربرد باشند؛ • اعلام خاتمه در پذیرش سیستم برای شروع بهره‌برداری از سیستم.	صحه‌گذاری؛ • تولید گزارش‌های نا مطابق برای اقدامات پیشگیرانه/ اصلاحی پیشنهاد شده؛ • رفع موارد غیرعادی یافت شده طی صحه‌گذاری؛ • رفع موضوعات وارانتی با مشتریان.

عوامل تاثیرگذار برای ملاحظه:

- مدیریت گذار؛
- اهداف تعهد برای برنامه زمانبندی تحویل محصول؛
- الزامات و انگیزه‌های وارانتی.

مکانیزم‌های توانا ساز برای کاربردهای فرآیند:

- مدیریت پروژه؛
- آموزش مشتری.

خروجی‌ها:

- بهره‌برداری سیستم برای خدمت؛
- پشتیبانی از مشتری.

الف-۲-۴ فرآیندی برای مرحله نگهداری/ بهره‌برداری از سیستم

ورودی‌ها:

- سیستم در بهره‌برداری خدمت کامل.

فعالیت‌های کلیدی فرآیند	فعالیت‌های مرتبط با قابلیت اعتماد
بهره‌برداری	
• پیاده‌سازی راهبرد بهره‌برداری؛ • پایش عملکرد سیستم؛ • فراهم نمودن مقدار مشتری.	• پیاده‌سازی برنامه رشد قابلیت اطمینان؛ • پیاده‌سازی سیستم جمع‌آوری داده‌های میدانی؛ • هدایت نظرسنجی رضایت مشتری.
نگهداری	
• پیاده‌سازی راهبرد پشتیبانی نگهداری؛ • پایش تلاش‌های نگهداری سیستم؛ • فراهم نمودن خدمت توجه مشتری؛ • پیاده‌سازی فعالیت‌های نگهداری برای اصلاحات تطبیقی.	• تحلیل روندهای وقوع خرابی؛ • هدایت تحلیل علت- ریشه‌ای نواحی مسئله؛ • پیشنهاد تغییرات طراحی یا رویه‌ای برای بهبود مداوم؛ • تعیین کیفیت خدمت.

عوامل تاثیرگذار برای ملاحظه:

- ظرفیت خدمت سیستم؛
- زنجیره تأمین برای تدارک یدکی؛
- اقدامات نگهداری پاسخگو.

مکانیزم‌های توانا ساز برای کاربردهای فرآیند:

- مدیریت پروژه؛
- آموزش متخصص نگهداری‌ها و اپراتورها.

خروجی‌ها:

- عملکرد سیستم قابل اعتماد؛
- نتایج رضایت مشتری.

الف-۲-۵ فرآیندی برای مرحله ارتقای سیستم

ورودی‌ها:

- الزامات مشتری جدید؛
- خصایص ارتقا یافته.

فعالیت‌های کلیدی فرآیند	فعالیت‌های مرتبط با قابلیت اعتماد
ارتقاء	
• شناسایی الزامات جدید؛ • ایجاد راهبرد و طرح ارتقاء؛ • سنجش نیاز برای منافع تغییر و نتیجه‌گیری؛ • پیاده‌سازی تلاش‌های ارتقاء؛ • پیاده‌سازی فعالیت‌هایی برای اصلاحات تکمیلی.	• سنجش پیامد عملکرد قابلیت اعتماد به علت تغییرات با خصایص جدید افزوده؛ • هدایت مطالعه پیامد هزینه چرخه‌ی عمر برای مشارکت در تغییر؛ • هدایت ارزیابی‌های مقدار و ریسک؛ • هدایت نظرسنجی رضایت مشتری نتیجه شده از واکنش‌های تغییر.

عواملی اثربخش برای ملاحظه:

- زمانبندی برای تغییر؛
- بازده سرمایه.

مکانیزم‌های توانا ساز برای کاربردهای فرآیند:

- مدیریت تغییر؛
- مدیریت کهنگی؛

- خرید مشتریان یا واکنش به مشارکت در خصایص جدید.

خروجی‌ها:

- عملکرد سیستم ارتقاء یافته؛
- مقایسه نتایج رضایت مشتری قبل و بعد از تلاش‌های ارتقاء.

الف-۲-۶ فرآیندی برای مرحله از کار اندازی/ کنار گذاری سیستم

ورودی‌ها:

- وضعیت توانمندی عملکرد پیری سیستم؛
- قابلیت عرضه در بازار و رقابت برای خدمت بهره‌برداری موجود؛
- هزینه‌های پشتیبانی و نگهداری افزایش یافته.

فعالیت‌های کلیدی فرآیند	فعالیت‌های مرتبط با قابلیت اعتماد
ازکاراندازی/ کنار گذاری	
• اجرای طرح ازکاراندازی/ کنار گذاری سیستم؛ • پیاده‌سازی راهبرد استفاده به کارگیری دوباره و استفاده دوباره؛ • پیاده‌سازی تدبیر در مورد تضییع اقلام وارهایی؛ • اطلاع دادن به مشتریان در مورد پایان خدمت؛ • فراهم نمودن اطلاعات در مورد تدارک خدمت جایگزین یا جدید.	• سنجش قیود غیر فعال سازی سیستم و پیامد حذف سیستم از بهره‌برداری؛ • سنجش پیامد روی محیط‌های اقلام وارهایی؛ • هدایت نظرسنجی رضایت مشتری به علت پایان خدمت.

عوامل تاثیرگذار برای ملاحظه:

- زمان بندی برای کنار گذاری؛
- فرسودگی فناوری؛
- قیود قراردادی؛
- پیامد اجتماعی به علت پایان خدمت.

مکانیزم‌های توانا ساز برای کاربردهای فرآیند:

- مدیریت پروژه.

خروجی‌ها:

- پایان خدمت.

پیوست ب

(اطلاعاتی)

روش‌ها و ابزارهایی برای تکوین و تضمین قابلیت اعتماد سیستم

ب-۱ کلیات

روش‌ها و ابزارها کمک‌هایی مفید برای حل مسائل فنی عام شامل مهندسی قابلیت اعتماد برای سیستم در مراحل مختلف چرخه‌ی عمر می‌باشند. ابزارهای بیشمار و تعداد زیادی از فروشندگان ابزار در بازار وجود دارند. برخی از این ابزارها اشکال و فهرست‌های وارسی ساده استاندارد هستند. دیگر ابزارها سیستم‌های تعاملی پیچیده هستند که اغلب نیازمند توافقات پروانه‌دار برای دسترسی به پایگاه داده و پشتیبانی فنی می‌باشند. روش‌ها و ابزارها به طور عادی تکوین یافته درون- سازمانی بر پایه تجربه گذشته مهندسی هستند، یا می‌توانند از فروشندگان ابزار برای تسهیل در آموزش کارکنان و چند کاربرد پروژه خریداری شوند. انتخاب روش‌های مقتضی برای راه حل فنی بایستی در صلاحدید مهندسان یا نمایندگان اجرا کننده تکلیف قابلیت اعتماد باشد. به علت اینکه سرمایه‌گذاری‌ها به انتخاب ابزارها، مرتبط می‌شود، مهندسی یا نمایندگی بایستی رابطه طبقه مشکلات مهندسی قابلیت اعتمادی را که نیاز است حل شود، فراوانی استفاده از ابزار، تلاش آموزش مورد نیاز برای استفاده اثربخش از ابزار برای دستیابی به نتایج و آمادگی روش‌های جایگزین برای حل مسائل یکسان با یک مجموعه ابزار ساده تکوین یافته درون- سازمانی را ملاحظه نماید. موارد ذیل مثال-های نوعی از کاربردهای کلی، کاربردهای خاص سخت‌افزاری و کاربردهای خاص نرم‌افزاری روش‌ها و ابزار برای مهندسی قابلیت اعتماد در سیستم را فراهم می‌کنند.

ب-۲ کاربردهای کلی روش‌ها و ابزارها برای مهندسی قابلیت اعتماد در سیستم

ب-۲-۱ مورد قابلیت اطمینان و قابلیت نگهداری

مورد قابلیت اطمینان و قابلیت نگهداری (R&M) توسط یک فراگیرنده سیستم استفاده می‌شود تا اطمینان حاصل کند که الزامات R&M خریدار تعیین می‌شوند و توسط تأمین‌کننده و خریدار یک سیستم تحقق می‌شوند. ابزار وسایلی را برای دستیابی به تضمین پیش رونده از این که الزامات R&M وجود دارند یا درون عمر سیستم ارضا خواهند شد فراهم می‌کنند.

ابزار یک چارچوب را فراهم می‌کند برای:

الف) مورد R&M – یک آرگومان قابل ممیزی مستدل برای پشتیبانی از مباحثه که یک سیستم تعریف شده الزامات R&M را ارضا می‌کند؛

ب) گزارش موردی R&M – خلاصه یا چکیده‌ای از آرگومان‌ها و شواهد R&M از مورد R&M برای پشتیبانی از سنگ‌نشانه‌های برنامه؛ و

پ) تضمین پیش رونده R&M از طریق سنگ‌نشانه‌های پروژه؛

سند مرجع: [11] DEF STAN 00-42.

ب-۲-۲ برنامه‌های رشد قابلیت اطمینان

برنامه‌های رشد قابلیت اطمینان برای بهبود قابلیت اطمینان سیستم طی مرحله تکوین/ طراحی سیستم استفاده می‌شود. هدف رشد قابلیت اطمینان تحقق اهداف قابلیت اطمینان بالقوه سیستم توسط بهبودهای قدم به قدم با استفاده از فنی در تحلیل طراحی و آزمون قابلیت اطمینان ماژول‌ها یا وظایف سیستم می‌باشد. فعالیت قابلیت اعتماد حیاتی برای شناسایی و حذف ضعف‌های طراحی در سیستم برای ارتقای پیش رونده قابلیت اطمینان می‌باشد. سیستم‌های نوعی که از کاربرد برنامه‌های رشد قابلیت اطمینان سود می‌برند سیستم‌های استفاده کننده از فن طراحی معماری جدید، اجزای جدید و غیرثابت سیستم و محتوای متمرکز نرم‌افزاری برای ترکیب در بهره‌برداری سیستم می‌باشند. مفهوم رشد قابلیت اطمینان کاهش رویداد وقوع خرابی به علت ضعف طراحی از طریق بهبودهای پیش رونده طراحی در سیستم و وظایف تشکیل‌دهنده آن از طریق فرآیند تکوین و طراحی است. برنامه‌های رشد قابلیت اطمینان برای دستیابی به راه‌حل‌های با صرفه اقتصادی بایستی در فرآیند سنجش و طراحی سیستم گنجانده شده باشند. برنامه رشد قابلیت اطمینان در IEC 61014 [12] توصیف شده است. مدل‌های رشد قابلیت اطمینان و روش‌های تخمین برای ارزیابی‌های رشد قابلیت اطمینان بر پایه داده‌های وقوع خرابی ضبط شده در برنامه رشد قابلیت اطمینان در IEC 61164 [13] توصیف شده‌اند.

ب-۲-۳ مدیریت پیکره‌بندی

مدیریت پیکره‌بندی‌های مختلف و متوالی در سیستم یک نگرانی عمده برای قابلیت اعتماد است (یعنی پشتیبانی نگهداری). این مورد به علت تنوع واسطهای ایجاد شده از طریق پیکره‌بندی‌های مختلف است. تقاضای افزاینده برای قابلیت تغییر داخلی اجزاء (سخت‌افزاری و نرم‌افزاری) و قابلیت بهره‌برداری داخلی در سیستم‌ها رابطه تجاری مستقیم دارند و اشاره به ملاحظه خاص به مدیریت پیکره‌بندی سیستم دارند. این مورد خصوصاً برای سیستم‌های با عمر طولانی و با اجزایی با عمر کوتاهتر صحیح است، که ممکن است بارها در فناوری عمر سیستم تغییر کند. طی تکوین سیستم، یک سیستم مدیریت پیکره‌بندی خوب به طور چشمگیری در دستیابی به قابلیت اعتماد اثربخش کمک می‌کند. مدیریت پیکره‌بندی برای کنترل‌های تغییر سیستم و ارزیابی‌های قابلیت اعتماد معنادار ضروری است. راهنمایی برای مدیریت پیکره‌بندی کلی در ISO 10007 [14] توصیف شده است.

ب-۲-۴

شبکه‌های باور بیزی (BBN[1]) یک اعتقاد گرافیکی قدرتمند برای پشتیبانی مستدل از حوادث نا معین با استفاده از اشکال گوناگون شواهد است. آن‌ها مدل‌سازی عدم قطعیت و ترکیب انواع مختلف شواهد، شامل اطلاعات ذهنی بر پایه قضاوت خبره و شواهد "سخت" از اندازه‌گیری را مقدور می‌سازند. یک BBN شواهدی را که کاربر در دسترس دارد یا می‌خواهد وارد نماید بقدری کم خواهد پذیرفت، بنابراین می‌تواند یک

1 - Bayesian Belief Network

پیش‌بینی با داده‌های از دست رفته یا نا کامل صورت دهد. این فناوری یک رویکرد مفید برای پیش‌بینی قابلیت اعتماد یک سیستم در تمام مراحل چرخه‌ی عمر سیستم پیشنهاد می‌دهد هنگامی که ترکیبی از اندازه‌گیری‌های مستقیم و غیرمستقیم قابلیت اعتماد آماده می‌باشند.
محصولات شبکه بیزی تجاری زیادی وجود دارند که ورود داده‌ها و تنظیم BBNها را تسهیل می‌نمایند.

ب-۳ کاربردهای خاص سخت‌افزاری روش‌ها و ابزارها برای مهندسی قابلیت اعتماد درون سیستم

ب-۳-۱ ارتقای قابلیت اطمینان

ارتقای قابلیت اطمینان سیستم برای عناصر سخت‌افزاری روی ویژگیهای ذاتی وظایف سیستم و تأثیر عواملی اثربخش برای عملکرد قابلیت اطمینان تمرکز می‌نماید. تمرکز اولیه روی فناوری استفاده شده در ساخت سیستم، محیط بهره‌برداری سیستم و کاربرد وظایف سیستم برای دستیابی به اهداف عملکرد سیستم است. چندین روش قابلیت اطمینان کلاسیک و فن قابل کاربرد برای ارزیابی‌های قابلیت اطمینان همانگونه که در IEC 60300-3-1 توصیف شده وجود دارد. بهبود قابلیت اطمینان می‌تواند بوسیله مشارکت مناسب نتایج پیشنهاد شده با راه‌حل‌های عملی بر پایه ورودی‌های ارزیابی قابلیت اطمینان مرتبط به دست آید. در بیشتر موارد، سبک سنگین کردن طراحی برای تعیین بهترین راه حل ضروری است. برخی از این روش‌ها می‌تواند برای وارسی‌ها و توازن در تصدیق نتایج تحلیل ارزیابی‌های انجام شده در همان عنصر سخت‌افزاری استفاده شود.
مثال‌های نوعی در استفاده از روش‌ها و ابزار قابلیت اطمینان شامل موارد زیر می‌شوند:

- استفاده از دیاگرام بلوکی قابلیت اطمینان (RBD) برای تعیین نیازهای فراوانی در ازای استفاده از یک عنصر سخت‌افزاری قابلیت اطمینان بالاتر مربوط به فناوری جدید با یک هزینه اضافه؛
- استفاده از تحلیل مارکوف برای سنجش ساختارهای سیستمی پیچیده و راهبردهای نگهداری پیچیده؛
- استفاده از تحلیل درخت خرابی (FTA) برای شناسایی وقوع خرابی‌های بحرانی در سیستم؛
- استفاده از تحلیل آثار و مُدهای وقوع خرابی (FMEA) برای تعیین مُدهای وقوع خرابی بالقوه، علل و آثار، بحرانیت مرتبط با مواجهه با ریسک؛
- استفاده از پیش‌بینی نرخ وقوع خرابی برای تخمین قابلیت اطمینان ذاتی عناصر سخت‌افزاری.

بایستی یادآوری شود که محدودیت‌هایی در استفاده از روش‌ها و ابزار قابلیت اطمینان وجود دارند. مفروضات ساخته شده در فرمول بندی مشکل برای توجیه و استدلال عقلانی رویکرد فنی به کار برده شده ضروری می‌باشند. قضاوت مهندسی مبتنی بر تجربه عملی برای تفسیر نتایج ارزیابی قابلیت اطمینان برای پیشنهادات نیاز می‌شود.
به علت اینکه اثر گرمایی و تداخل الکترومغناطیسی روی عملکرد اجزای الکترونیکی در وظایف سیستم اثر می‌گذارد، برای تحلیل سیستم، تکوین وسایلی برای بودجه‌بندی گرمایی و بودجه‌بندی قابلیت سازگاری الکترومغناطیسی برای محدود کردن مواجهه با ریسک فاجعه‌آمیز در سیستم امری محتاطانه است. این رویکرد یک روش تحلیل مهندسی قابل دوام را برای دستیابی به عملکرد قابلیت اطمینان سیستم ارائه

می‌دهد. اجتناب از خرابی و طراحی‌های مقاومت در برابر خرابی برای طراحی مشارکت شده در کاربردهای حیاتی بسیار تعیین‌کننده می‌باشند.

ب-۳-۲ ارتقای قابلیت نگهداری

برای ارتقای قابلیت نگهداری توجه به تسهیل نگهداری یک قلم سخت‌افزاری قابل تعمیر در شکل یک واحد مونتاژ مهم است. این مورد دلالت بر این دارد که هنگام عملکرد اشتباه یا فرسودگی می‌تواند شناسایی شود، مجزا شود، حذف شود یا با قلم جدید جایگزین شود. معیارهای ایجادکننده قابلیت نگهداری در طراحی سیستم با جزءبندی مونتاژ سیستم برای دسترسی آسان، ساخت پایین‌ترین واحد قابل جایگزینی برای جایگزین کردن، قابلیت آزمون‌دهی پایین‌ترین واحد قابل جایگزینی برای آشکارسازی خرابی و هزینه و قابلیت اطمینان پایین‌ترین واحد قابل جایگزینی برای تدارک یدکی ارتباط دارد. این مورد همچنین جنبه‌های اقتصادی یک قلم دورانداختنی یا پایین‌ترین واحد قابل جایگزینی قابل تعمیر را تعیین می‌کند.

قابلیت نگهداری سیستم به طور کلی با سه سطح تعمیرات ارتباط دارد:

الف) سطح سازمانی- توان‌یابی سیستم در موقعیت سیستم که معمولاً با جایگزینی پایین‌ترین واحد قابل جایگزینی به عنوان یک ماژول وصل شدنی با زمان‌های جداسازی و جایگزینی نسبتاً کوتاه ارتباط دارد؛

ب) سطح واسطه- توان‌یابی پایین‌ترین واحد قابل جایگزینی در یک کارگاه واسطه آزمون اضافی، عیب‌یابی، کارکرد دوباره/ تعمیر و توان‌یابی واحد را به حالت مربوط به بهره‌برداری آن برای بازیافت تسهیل می‌کند. این مورد نیازمند مدت زمان طولانی‌تر است.

پ) سطح انبار- تعمیر گسترده‌تر و کارکرد دوباره می‌تواند برای توان‌یابی قلم به حالت بهره‌برداری آن برای بازیافت انجام شود. این مورد زمان طولانی‌تری را نیاز دارد.

اگر پایین‌ترین واحد قابل جایگزینی یک قلم دور انداختنی باشد آنگاه قابلیت نگهداری سیستم فقط با دو سطح نگهداری بسیار ساده‌تر است. جایگزینی واحد خراب فقط در سطح سازمانی رخ می‌دهد و واحد یدکی از انبار می‌آید، که می‌تواند کارخانه یا سازنده تجهیزات اصلی باشد. هیچ کارگاه تعمیراتی نیاز نمی‌شود. چالش و انگیزه اینجا طراحی یک قلم دور انداختنی با صرفه اقتصادی است که از لحاظ محیطی مساعد برای وارهایی است.

قابلیت آزمون‌دهی یک پارامتر اهمیت برای ارتقای قابلیت نگهداری سخت‌افزاری است. گستره عیب‌یابی‌ها و پوشش خطای واحد خراب شده اغلب زمان و تلاش گذرانده در تعیین قلم بدون وقوع خرابی را دیکته می‌کند، که منابع نگهداری را به جریان می‌اندازد. خط مشی تعمیر بایستی به طور واضح این اقلام بدون وقوع خرابی را ردیابی کند و شناسایی کند که چند بار یک قلم خراب شده از خط کارکرد دوباره/ تعمیر عبور کرده است قبل از اینکه به عنوان یک قلم دور انداختنی دور انداخته شود. خط مشی تعمیر همچنین بایستی بازنگری شود و از درستی و اثربخشی تجهیزات آزمون اطمینان حاصل شود تا به طور واضح قلم خراب را شناسایی و تعیین کند.

طراحی قابلیت نگهداری بایستی به جنبه‌های عواملی انسانی برای تسهیل تقابلات برای توان‌یابی و بهره‌برداری خدمت نگهداری توجه نماید. موضوعات ایمنی و امنیتی بایستی طی کار نگهداری اصلاحی و

پیشگیرانه در نظر گرفته شود. راهنمایی برای طراحی و کاربردهای قابلیت نگهداری در IEC 60300-3-10 [15] توصیف شده است.

ب-۳-۳ ارتقای پشتیبانی لجستیک و نگهداری

پشتیبانی لجستیک و نگهداری سیستم روی حفظ عملکرد سیستم در برآورده‌سازی اهداف بهره‌برداری آن تمرکز می‌کند. عمدتاً فعالیت‌ها طی مرحله نگهداری/ بهره‌برداری سیستم هدایت می‌شوند. ارتقاء برای پشتیبانی لجستیک و نگهداری می‌تواند با بهبود در قابلیت پشتیبانی سیستم درون محدودیت‌های ایجاد شده پیکره‌بندی سیستم و سناریوی بهره‌برداری به دست آید. مقادیری وجود دارند که با بهبود در خدمت 'توجه[1]' مشتری و ساده‌سازی روش‌های اجرایی خدمت به دست می‌آیند. بهبود می‌تواند همچنین با اتوماسیون اثربخش در گزارش فعالیت نگهداری و به کارگیری سیستم تحلیل پشتیبانی لجستیک ایجاد شود. موضوعات پشتیبانی لجستیک مرتبط با سیستم انبار پشتیبانی متمرکز یا غیر متمرکز، و طرح‌ریزی و برنامه زمانبندی راهبردی تکالیف پشتیبانی نگهداری می‌تواند کاهش زمان و تلاش نگهداری را نتیجه دهد. در محیط رقابتی بازار امروز که در آن سیستم‌ها بر فرضیات مشتری مستقر می‌باشند و به طور گسترده بر مبنایی جهانی توزیع شده‌اند، توجه به کار نگهداری ضروری انجام شده توسط نگهداری قرارداد شخص سوم امری احتیاط‌آمیز است. برون سپاری کار پشتیبانی نگهداری نیازمند آموزش اضافی کارکنان نگهداری قراردادی با مهارت‌های مناسب و شایستگی برای انجام خدمت لازم برای مشتریان می‌باشد. آن‌ها اولین خط کارکنان نگهداری برای ارتباط با شکایت‌های مشتریان هستند. اطلاعات جمع‌آوری شده از نگرانی‌های مشتری روی کار خدمت انجام شده و اطمینان مشتری در سیستم، چالش اصلی برای هماهنگی فرآیند پشتیبانی نگهداری سیستم است. روش‌های مختلف برای فن ارتقاء شامل نگهداری مرکزی قابلیت اطمینان (RCM) همانگونه که در [16] IEC 60300-3-11 توصیف شده و فرآیند پشتیبانی لجستیکی یکپارچه (ILS) همانگونه که در [17] IEC 60300-3-11 توصیف شده به کار گرفته شده است.

ب-۴ کاربردهای خاص نرم‌افزاری روش‌ها و ابزارها برای مهندسی قابلیت اعتماد در سیستم

ب-۴-۱ روش‌شناسی شی‌گرا

روش‌شناسی شی‌گرا رویکردی برای مدل‌سازی سیستم به عنوان مجموعه‌ای از اشیاء متعامل با رفتار و داده مشترک می‌باشد. این رویکرد بر پایه تجزیه الزامات یا طراحی سیستم در یک مجموعه سلسله مراتبی از اشیاء و طبقات می‌باشد.

ب-۴-۲روش‌شناسی ساختاری

روش‌شناسی ساختاری، فنی بر پایه تجزیه الزامات و طراحی سیستم در مجموعه‌ای از فرآیندهای الگوریتمیک[2] متعامل توسط جریان داده‌های تعریف شده، می‌باشد. فرآیندها تبدیلی را روی داده‌های ورودی برای تولید داده‌های خروجی انجام می‌دهند. تجزیه می‌تواند روش اجرایی گرا، داده گرا، یا اطلاعات گرا باشد.

1- Care
2- Algorithmic

روش‌شناسی‌های ساختاری می‌توانند همچنین می‌تواند مشخص شوند که آیا هدف روش‌شناسی سیستم زمان- واقعی است یا خیر.

الف) روش "روش اجرایی محور"- رویکردی که فرآیندهای الگوریتمیک را در مدل‌سازی سیستم به عنوان تعیین مشخصات بنیادی در نظر می‌گیرد. تعریف داده‌ها از فرآیندهای تعریف شده می‌آید.

ب) روش "داده محور" – رویکردی که قسمت‌های ورودی و خروجی مدل سیستم را به عنوان تعیین مشخصات بنیادی در نظر می‌گیرد. فرآیندهای الگوریتمیک از ساختارهای داده‌ها نتیجه می‌شوند.

پ) روش "اطلاعات محور" - رویکردی که از مدل داده منطقی برای جمع‌آوری اجزای اطلاعات سیستم استفاده می‌کند. این رویکرد الزامات راهبردی را برای داده در یک سیستم سطح بنگاه تجاری تأکید می‌کند. اجزای اطلاعات سیستم سپس بر پایه الزامات مدل داده‌های منطقی ساخته می‌شوند.

ب-۴-۳ طراحی تجزیه وظیفه‌ای

طراحی تجزیه وظیفه‌ای رویکردی است که روی تعریف ماژول‌ها و واسط‌ها با قسمت‌بندی وظایف خاص سیستم نرم‌افزاری تمرکز می‌کند. فرآیند طراحی معمولاً تعهد می‌شود بعد از آن الزامات سیستم تکوین می‌یابد و یک مفهوم برای ساختار سیستم انتخاب می‌شود. فرآیند تکراری طراحی به صورت تکمیلی بالا به پایین و پایین به بالای تصحیح می‌شود. این کار با تجزیه سیستم به وظایف متقابل یا انجام وظیفه عناصر سیستم به دست می‌آید. سلسله مراتب طراحی سیستم به طور کلی شامل سه سطح می‌شود: طراحی سطح-بالا، طراحی سطح متوسط و پایین‌ترین سطح طراحی تفصیلی. رفتار هر سطح سلسله مراتب سیستم می‌تواند با دیاگرام توصیف شود که نشاندهنده ورودی‌ها و خروجی‌ها و فرآیند تبدیل وظایف مرتبط است. در هر سطح با استفاده از اطلاعات به دست آمده از فرآیند تجزیه وظیفه‌ای یک دیاگرام بلوکی می‌تواند رسم شود. این دیاگرام‌ها نشان می‌دهند که چطور عناصر سیستم در معماری سیستم می‌توانند با یکدیگر کار کنند و توصیف وظیفه‌ای هر بلوک می‌تواند به بهره‌برداری از آن مرتبط شود. رویکرد بسیار شبیه به روش دیاگرام بلوکی قابلیت اطمینان (RBD) با شناسایی متفاوت وظایف بلوک است. روش تجزیه وظیفه‌ای ابزاری قدرتمند برای سیستم‌های طراحی است که رویکردی سیستماتیک برای ضبط توصیف سلسله مراتب سیستم و وظایف تشکیل‌دهنده آن فراهم می‌کند. کاربرد رسمی فنون طراحی وظیفه‌ای، کیفیت طراحی‌ها را بهبود می‌بخشد و قابلیت اعتماد در قابلیت بهره‌برداری عملکرد را ارتقاء می‌دهد. مثال‌هایی از روش‌های طراحی تجزیه وظیفه‌ای تصحیح گام به گام، طراحی ساختار یافته و طراحی زمان واقعی می‌باشد.

ب-۴-۴ تحلیل خطا

تحلیل خطا شامل موارد زیر می‌شود:

- فرآیند بررسی یک خرابی نرم‌افزاری مشاهده شده به منظور ردیابی خرابی تا منبع آن؛
- فرآیند بررسی یک خرابی نرم‌افزاری مشاهده شده برای شناسایی اطلاعاتی از قبیل دلیل خرابی، فاز فرآیند تکوین که طی آن خرابی ایجاد شده، روش‌شناسی که توسط آن خرابی می‌تواند زودتر آشکار شود یا از آن جلوگیری شود و روشی که توسط آن خرابی آشکار می‌شود؛
- فرآیند بررسی خطاها، وقوع خرابی‌ها و خرابی‌های نرم‌افزاری برای تعیین نرخ‌ها و روندهای کمی؛

تحلیل خطا با تعیین اینکه آیا مشکل در سخت‌افزار یا نرم‌افزار است سرو کار دارد.

ب-۴-۵ تکنیک دلفی[1]

این تکنیک یک تکنیک پیش‌بینی گروهی است، که معمولاً برای رخدادهای آینده از قبیل تکوین‌های فناورانه استفاده می‌شود، که تخمین‌هایی از افراد خبره و خلاصه‌های بازخورد از این تخمین‌ها را برای تخمین‌های تکمیلی توسط این افراد خبره استفاده می‌کند تا اتفاق آرای منطقی رخ دهد. این تکنیک در فعالیت‌های تخمین-نرم‌افزاری مختلف، شامل تخمین عواملی اثربخش بر هزینه‌های نرم‌افزاری استفاده می‌شود. برای درک تفصیلی تکنیک دلفی مرجع بایستی به یک مدرک دیکته شده به تکنیک دلفی از قبیل روش دلفی مراجعه شود: "Techniques and applications, edited by H. A. Linstone and M. Turoff".

ب-۴-۶ ابزارهای مهندسی نرم‌افزار با کمک رایانه (CASE)

ابزارهای CASE[2] ابزارهای مهندسی نرم‌افزار با کمک رایانه هستند که به اتوماتیک کردن یک یا جنبه‌های بیشتری از فرآیند مهندسی نرم‌افزار کمک می‌کنند. ابزارهای CASE به طور عادی در کار نگهداری و تکوین مهندسی نرم‌افزار استفاده می‌شوند. ابزارهای CASE زیادی توسط تأمین‌کنندگان نرم‌افزار خلق شده و برای کاربردهای سازمان‌های مختلف استفاده می‌شوند. ابزارهای CASE به طور تجاری برای تسهیل کاربردهای نرم‌افزاری از قبیل تحلیل ساختار سیستم، مدیریت الزامات، مدل‌سازی و شبیه‌سازی، طراحی گرافیکی نرم‌افزاری، تولید کد، مهندسی دوباره، ردیابی "اشکال"، تولید گزارش و کمک به مسؤولیت در دسترس می‌باشند. ابزارهای CASE محصولات نرم‌افزاری COTS هستند. انتخاب و کاربرد ابزارهای CASE بایستی فرآیند سنجش استانداردی را برای اهداف تضمین دنبال نماید. راهنمایی درباره طبقه‌بندی ابزارهای CASE در [18] IEEE Std 1175.1 توصیف شده است. رهنمود سنجش و انتخاب ابزارهای CASE در ISO/IEC 14102 [19] توصیف شده است.

ب-۴-۷ خدمات محیط‌های مهندسی نرم‌افزار (SEE[3])

SEE مجموعه‌ای از خدمات نرم‌افزاری، تا حدی یا کاملاً خودکار با ابزار نرم‌افزاری است که برای پشتیبانی از اجرای فعالیت‌های انسانی در مهندسی نرم‌افزار استفاده می‌شود. فعالیتهای SEE معمولاً درون یک محیط پروژه نگهداری و تکوین نرم‌افزاری انجام می‌شود. آن‌ها نواحی از قبیل مشخصات، مهندسی دوباره یا نگهداری سیستم‌های بر پایه نرم‌افزار را پوشش می‌دهند. کاربردهای SEE ممکن است چندین موقعیت را پوشش دهد؛ از اجرای تعداد کمی از ابزارها روی همان سیستم بهره‌برداری، برای محیط کاملاً جامع، توانایی برای هدایت، پایش و کنترل تمام داده‌ها، فرآیندها و فعالیت‌ها در چرخه‌ی عمر نرم‌افزار. یک SEE پشتیبانی از فعالیت‌های انسان را از طریق یک سری از خدماتی که توانمندی‌های محیط را توصیف می‌کنند، فراهم می‌کند. فرآیند نرم‌افزاری پشتیبانی شده توسط SEE یک فرآیند نرم‌افزاری خودکار یا کمکی می‌شود. SEE

1 -Delphi

2 -Computer-aided software engineering

3 -Software engineering environments

می‌تواند به عنوان یک سیستم توانا ساز ملاحظه شود. اطلاعات بیشتر راجع به SEE می‌تواند در ISO/IEC 15940 [20] یافت شود.

ب-۴-۸ مدل‌های تکامل توانمندی

مدل تکامل توانمندی (CMM[1]) توسط سازمان‌ها برای توصیف تکامل فرآیند نرم‌افزاری آن‌ها استفاده می‌شود. CMM یک سازمان را در سطوح ۱ تا ۵ رتبه‌بندی می‌کند.

- سطح ۱: کاربرد موردی یا بی‌نظمی ملاحظه شده؛
- سطح ۲: فرآیندهای قابل تکرار؛
- سطح ۳: فرآیندهای تعریف شده (استاندارد مینیمال صنعتی روی فرآیندهای فنی)؛
- سطح ۴: فرآیندهای اندازه‌گیری شده؛
- سطح ۵: فرآیندهای بهینه‌شده.

مدل CMM در روشی سیستماتیک بر پایه مجموعه‌ای از اصول برای استنتاج یک پرسشنامه تکامل استفاده می‌شود. یک مدل می‌تواند توسط جزئیات دقیق و کامل چارچوب تکامل پدیدار شود. این مورد استفاده از مدل با راهنمایی اثربخش برای فرآیند ایجاد برنامه‌های بهبود فرآیند را فراهم می‌کند.

CMM برای نرم‌افزار (SW-CMM) به سازمان در افزایش تکامل فرآیندهای نرم‌افزاری با استفاده از آگاهی مورد نیاز از ارزیابی‌های فرآیند نرم‌افزار و بازخورد گسترده از بهترین اقدامات صنعتی کمک می‌کند.

CMM روی فرآیند تکوین تمرکز می‌کند. نواحی فرآیند بلوک‌های ساختاری یا نهادهای آگاهی بر پایه اقدامات صنعتی را تعریف می‌کند. سطوح تکامل وابستگی‌ها و تقدمات برای بهبود را تعریف می‌کند.

سطح ۱ برای راهنمایی سازمان‌ها به تمرکز روی منابع بهبود فرآیند محدود شده در مهمترین تغییرات می‌باشد. اولویت‌دهی مهم است زیرا سازمان‌های تکاملی کوچکتر داده‌های تاریخچه‌ای ضروری برای تعیین اینکه یک تغییر واقعاً یک بهبود باشد را ندارند. به این صورت، تغییر یک بهبود قابل توجه آماری را درون برخی از دوره‌های زمانی پیش‌بینی شده، شامل تمام هزینه‌های مرتبط با ایجاد تغییر، مقایسه شده با حالت بدون تغییر تولید خواهد کرد.

سطح ۲ عمدتاً فرآیندهای مدیریتی را برای طرح‌ریزی بهتر برنامه زمانبندی، زمان و منابع، ردیابی و کنترل پروژه ارائه می‌کند.

سطح ۳ یک فرآیند تکوین قابل تکرار تعریف شده به طور سازمانی را ایجاد می‌کند که خط اصلی‌ای برای اقدامات آتی می‌شود. همچنین مکانیزم‌هایی برای جمع‌آوری داده‌های تولید/ فرآیند و روش‌هایی برای تعیین اینکه چطور عملکرد و کیفیت فرآیند در مقابل اهداف کسب و کار را ایجاد می‌کند.

سطح ۴ به تغییراتی که قسمتی از سیستم علل مشترک نیستند می‌پردازد. این مورد به رسمیت می‌شناسد که فرآیند تکوین، یک سیستم است و فنون آماری می‌توانند به کار برده شوند. این مورد برای پیش‌بینی عملکرد و کیفیت بر پایه تجربه و داده‌ها استفاده می‌شود.

---

1 -Capability Maturity Model

سطح ۵ علل مشترک واریانس، برای تحلیل علت عیب‌ها، تغییرات بالقوه اندازه‌گیری برای کاهش یا جلوگیری از این عیب‌ها و تعیین اینکه آیا تغییرات واقعاً بهبودها هستند می‌پردازد. این فرآیند بهینه‌سازی یا بهبود مداوم است.

CMM یک محک[1] برای مقایسه توانمندی فرآیند تکوین سازمانی و استفاده از آن مقیاس به عنوان یک پیش‌بینی‌کننده کیفیت محصول را فراهم می‌کند.

هنگامی که استفاده و تجربه با SW-CMM افزایش می‌یابد، مدل‌ها برای رشته‌های مختلف و کاربردهای فنی تکوین می‌یابند. یک چنین مدلی، مدل تکامل توانمندی مهندسی سیستم (SE-CMM) است. توانمندی مهندسی نرم‌افزار توانایی یک سازمان نرم‌افزاری برای عملکرد موفقیت‌آمیز بر حسب هزینه، برنامه، انجام وظیفه محصول و کیفیت می‌باشد. توانمندی چندین بعد دارد که شامل موارد زیر می‌شود

۱. مهارت، تجربه ، آموزش و انگیزه به افرادی که کار را انجام و مدیریت می‌کنند؛
۲. توانمندی فرآیند و
۳. فناوری که در دسترس است و به کار برده می‌شود.

مدل‌های مجزا برای مهندسی نرم‌افزار (SW-CMM) و مهندسی سیستم‌ها (SE-CMM) که توسط سازمان-ها استفاده شده در صنعت نرم‌افزار سردرگمی به وجود آورده است. این مدل‌ها ردوندانت شده‌اند و در عمل اغلب ضد- تولید[2] می‌باشند. تفاوت‌ها بین مدل‌های SW و SE استفاده همزمان از هر دو مدل را برای یک سازمان مشکل کرده است.

راه‌حل این سردرگمی اقدام برای این ناهماهنگی با ایجاد یکپارچگی مدل تکامل توانمندی (CMMi) است. CMMi برای تطبیق تناقضات در معماری، رویکرد، اصطلاح‌شناسی و دیگر موضوعات توانمندی بین SW-CMM و SE-CMM و مدل‌های مرتبط است. حاصل این ایجاد، مجموعه‌ای از مدل‌ها و زیرساخت پشتیبانی، جمع‌آوری نام گذاری شده به عنوان CMMi می‌باشد.

CMM توسط مؤسسه مهندسی نرم‌افزاری (SEI) تکوین یافت که به نام دانشگاه کارنیگ ملون[3] ثبت شده است. مرجع CMM می‌تواند در www.sei.cmu.edu [21] یافت شود.

1- Benchmark

2- Counter - productive

3 - Carnegie Mellon

پیوست پ

(اطلاعاتی)

راهنمایی درباره محیط کاربردی سیستم

پ-۱ درک محیط کاربردی سیستم

راهنمایی درباره محیط کاربردی سیستم، دیدگاه سیستمی برای محیط محصول نهایی را ارائه می‌دهد هنگامی که در بهره‌برداری سیستم جمع می‌شوند. این کار برای فراهم نمودن اطلاعات مربوط به محیط بهره‌برداری سیستم برای طراحی‌های محصول قابل اعتماد و محکم و انتخاب مواد مناسب برای کاربرد سیستم است. معیاری مرتبط برای تکوین یا انتخاب محصولات سخت‌افزاری برای ملاحظات وظیفه‌ای طراحی فراهم می‌شوند. مثال‌های نشان داده شده در محیط کاربردی برای سیستم‌های زمینی عام می‌باشند.

مقدار نشان‌دهنده[1] یک مجموعه فراگیر از معیار طراحی مرتبط، توسط عوامل ذیل برانگیخته می‌شود:

الف) تجربه نشان داده است که طراحی‌های محصول خاص یا اکتسابات اغلب از ارتباطات واسطه‌های انسانی، الکترومغناطیسی، اقلیمی[2] و شرایط مکانیکی و سایر عوامل عملکردی همانگونه که از منظر سیستم برای کاربردهای محصول نهایی دیده می‌شود، چشم‌پوشی می‌کنند. رویکرد ارائه شده در اینجا طراحی معماری سیستم و یکپارچگی برای تطبیق با الزامات بازار جهانی را تسهیل می‌کند؛

ب) جمع‌آوری داده‌ها و مراجعه متقابل به استانداردها در مقابل الزامات مشتری می‌تواند تلاشی گسترده را به کار گیرد. این راهنمایی یک مرجع آماده و ورودی‌هایی برای مشخصات طراحی فراهم می‌کند؛

پ) روند تکوین محصول جاری به علت محدودیت‌های زمان ارائه به برای- بازار از طراحی به برآورده‌سازی یک الزام خاص مشتری حرکت می‌کند. این راهنما گستره‌ای وسیع از بخش‌های کاربرد را ارائه می‌دهد که در آن محیط استفاده و نیازهای محصول می‌توانند برای تکوین محصول با صرفه اقتصادی و اکتساب برای تسهیل یکپارچگی سیستم استدلال شوند؛

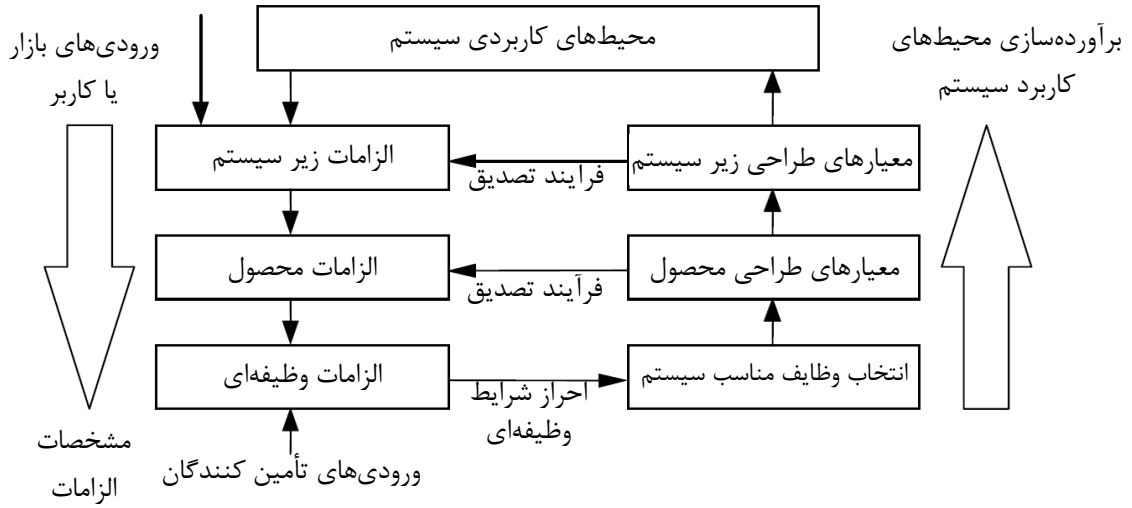
ت) کنترل‌های محیط و ویژگی‌های عملکرد محصول به طور پیش رونده در سیستم، زیر سیستم و سطوح محصول به عنوان مقیاس‌هایی برای دستیابی به راه‌حل‌های طراحی بهینه برای برآورده‌سازی تغییر تقاضاهای بازار جهانی به کار برده می‌شوند. این مورد روند را به سمت همکاری بین‌المللی و هماهنگ‌سازی استانداردها برای تسهیل تکوین محصول منعکس می‌کند.

1-Presenting

2-Climatic

پ-۲ فرآیند تعریف الزامات محیطی

شکل پ-۱ یک دید کلی از فرآیند تعریف الزامات ارائه می‌دهد.



شکل پ-۱ فرآیند تعریف الزامات محیطی

تعریف الزامات فرآیندی بالا به پایین است که بوسیله محیط سیستم برای یکپارچگی مورد نظر زیر سیستم، محصولات و کاربردهای وظیفه‌ای تعریف می‌شود. این شرایط محیطی سیستم به الزاماتی برای محصولات و وظایف متشکله معنا می‌شوند. نیازهای کاربر و ورودی‌های بازار به طور کلی برای راهنمایی تکوین مشخصات الزامات استفاده می‌شوند.

یک فرآیند تصدیق طراحی موازی برای تکمیل فرآیند تعریف الزامات به کار گرفته می‌شود. این یک فرآیند پایین به بالا برای حصول اطمینان از اجرای الزامات در هر مرحله از طراحی مورد نظر، از انتخاب کاربردهای وظیفه‌ای، از طریق تکوین محصول تا یکپارچگی سیستم می‌باشد. هدف برآورده‌سازی یا فراتر رفتن از الزامات عملکرد کاربرد سیستم استفاده نهایی است.

شرایط محیطی سیستم استفاده نهایی در بند پ-۳ ارائه می‌شوند. الزامات وابسته به محیط استفاده قابل کاربرد برای محصولات جامع در سیستم بر حسب ویژگی‌های عملکردی خاص شناسایی می‌شوند. آن‌ها طبقه‌بندی‌های محیط محصول و شناسایی معرض‌های محیطی قابل کاربرد را مجاز می‌سازند.

پ-۳ شرایط محیطی سیستم

پ-۳-۱ طبقه‌بندی شرایط محیط سیستم

شکل پ-۲ نگاشت در معرض قرارگرفتن محیط‌های کاربرد سیستم را نشان می‌دهد. شرایط الکترومغناطیسی، آب و هوایی و مکانیکی نشان داده شده، همان گونه که در معرض یک کاربرد شناسایی شده سیستم قرار گیرد، نامه طراحی برای طبقه‌بندی محیط خاص محصول را فراهم می‌کند.

ارتباط بین در معرض قرار گرفتن و ویژگی‌های عملکردی مرتبط با صفات طراحی محصول بایستی یادآوری شود (به سری استانداردهای IEC 60721 مراجعه کنید) [22].

محیط‌های کاربردی سیستم

در معرض	مفروضات کنترل شده محیطی	مفروضات مشتری صنعتی	کسب و کار	مسکونی	بیرونی	متحرک	حمل و نقل	انبارش
الکترومغناطیسی	E1	E3	E3	E3	E2	E4		
آب و هوایی	C1	C3	C2	C2	C4 C5	C4		C6
مکانیکی	M1 M2 M5	M1	M1 M2	M1 M2	M1	M3	M4	

شکل پ-۲ نگاشت در معرض قرار گرفتن محیط‌های کاربرد سیستم

پ-۳-۲ شرایط الکترومغناطیسی

شرایط الکترومغناطیسی شامل در معرض قرار گرفتن محیطی ذیل می‌شود:

E1 مفروضات کنترل شده محیطی (به طور مثال آزمایشگاه‌ها، اتاق‌های تمیز)

E2 موقعیت‌های بیرونی

E3 مفروضات مشتری

E4 کاربردهای متحرک و قابل حمل

پ-۳-۳ شرایط آب و هوایی

شرایط آب و هوایی شامل در معرض گذاری محیطی ذیل می‌شود:

C1 آب و هوای کنترل شده (به طور مثال آزمایشگاه‌ها، اتاق‌های تمیز)

C2 دمای کنترل شده درونی

C3 دمای درونی کنترل نشده (به طور مثال گاراژ بدون گرمایش)

C4 فضای بیرونی محافظت شده (به طور مثال دارای حفاظ)

C5 فضای بیرونی محافظت نشده (به طور مثال فضای باز)

C6 انبارش

پ-۳-۴ شرایط مکانیکی

شرایط مکانیکی شامل در معرض گذاری محیطی ذیل می‌شود:

M1 سکون

M2 قابل حمل

M3 متحرک

M4 حمل و نقل

M5 زلزله

پ-۴ ویژگی‌های طراحی تأثیرپذیر از محیط کاربرد سیستم

ویژگی‌های طراحی توسط محیط کاربردی سیستم تأثیر می‌پذیرند. این ویژگی‌ها در صفات عملکرد سیستم ذاتی هستند. ویژگی‌ها روی معماری طراحی سیستم، فناوری‌های استفاده شده در وظایف سیستم و راهبرد بسته‌بندی برای دستیابی به بهره‌برداری عملکرد بهینه تأثیر می‌گذارند. همبستگی و نگاشت ویژگی‌های طراحی برای محیط کاربر-نهایی، برای تکوین محیط کاربرد سیستم ضروری می‌باشند. فرآیند نگاشت برای شناسایی ویژگی‌های مشترک و قیود بدترین مورد برای طراحی محصول مناسب برای کاربرد سیستم می‌باشد. هدف حصول اطمینان از انسجام و استحکام محصول است هنگامی که در سیستم برای استفاده در شرایط مختلف محیطی مجتمع می‌شود. تمرین نگاشت یک رویکرد فنی برای ملاحظه گزینه‌های طراحی محصول و انتخاب فناوری‌های جایگزین فراهم می‌کند.

صفات عملکردی سیستم	ویژگی‌های طراحی تأثیرپذیر از محیط کاربرد سیستم
• قابلیت سازگاری الکترومغناطیسی	• معماری طراحی سیستم • حدود انتشار و بودجه EMC • نرخ‌های ساعت • الزامات فیلترینگ و حفاظت
• دمایی	• مصرف و توزیع توان • بودجه دمایی و محدودهای دما • روش‌های خنک کردن • مکانیزم‌های انتقال گرما
• کیفیت	• فرآیند کیفیت • معیار پذیرش • پایش و حذف غیر تطابقی • احراز شرایط تأمین‌کننده
• قابلیت اعتماد	• عملکرد آمادگی و تکرار/ زمان ناآماد قابل فرض • زمان میانگین بین وقوع خرابی‌ها • زمان میانگین تا توان‌یابی • پشتیبانی نگهداری و راهبرد تدارک یدکی‌ها • طول عمرها و بازه‌های عاری از وقوع خرابی
• قابلیت سازگاری محیطی	• فرآیند چرخه‌ی عمر محیطی • طراحی برای کاهش، استفاده مجدد و بازیافت • پیامد محیطی • در معرض ریسک قرار گرفتن

پ-۵ صفات عملکرد سیستم برای ملاحظات طراحی

پ-۵-۱ کلیات

اطلاعات شامل شده در همبستگی و نگاشت شکل پ-۲ و شکل پ-۳ می‌تواند طراحی وظیفه یا محصول خاص سیستم را برای استفاده در محیط کاربرد سیستم شناسایی شده تسهیل نماید. توصیفات ذیل برای صفات عملکردی خاص سیستم، اطلاعات پس‌زمینه‌ای ضروری برای ملاحظات طراحی را فراهم می‌کنند.

پ-۵-۲ ملاحظات طراحی EMC

قابلیت سازگاری الکترومغناطیسی (EMC)، توانمندی محصول برای وظیفه بدون انتشار یا تحت تأثیر قرار گرفتن توسط نویز الکترومغناطیسی می‌باشد. انتشار، انرژی الکترومغناطیسی یا نویز ناخواسته بر آمده از یک منبع است. این انتشار می‌تواند از منابعی از قبیل ساعت با فرکانس بالا تعبیه شده در یک مدار الکترونیکی یا ماژول یک محصول بیاید. مصونیت، قابلیت یک محصول برای مقاومت در مقابل نویز الکترومغناطیسی می‌باشد. این مورد می‌تواند در بهره‌برداری نزدیک از فرستنده‌های تلویزیون یا رادیویی، یا از تخلیه بار الکترواستاتیکی بیاید. سطوح انتشار در بسیاری از کشورها برای پیشگیری از تداخل تنظیم می‌شوند. طراحی‌های محصول الکترونیکی بایستی محدودیت‌های انتشار مربوط به آن‌ها را برای مقصود تجاری و کاربرد محصول برآورده سازد. جزءبندی، فن استفاده برای طراحی یک محصول برای برآورده سازی الزامات EMC است. ترجمان الزامات EMC از سطح سیستم به سطح محصول و به سطح ماژول نیاز به فرآیند بودجه‌بندی EMC دارد. این کار با تحلیل تشریحی وسایل استفاده شده در ماژول، راهبرد شیلدینگ و قرار دادن اجزاء، مسیر یابی کابل‌ها و سیم‌بندی چاپی ارتباط دارد. سهم تمام منابع انتشار در دسترس درون ماژول برای تعیین سطح حاشیه‌های طراحی استفاده می‌شوند. این حاشیه رواداری طراحی ماژول است که ممکن است پیامد عملکرد ماژول درون یک محصول باشد هنگامی که درون یک سیستم برای قرار گرفتن در معرض محیط الکترومغناطیسی جمع می‌شوند.

پ-۵-۳ ملاحظات طراحی حرارتی

الزامات گرمایی از وظیفه کاربردی سیستم و در معرض قرار گرفتن‌های محیطی مربوط به محصول یا ماژول-های در حال بهره‌برداری درون سیستم بسیار تأثیر می‌پذیرند. موضوع گرمای بنیادی، نگرانی در مورد تولید گرما و حذف گرما برای اجازه انسجام عملکرد قابل تحمل می‌باشد. تولید از وظیفه مورد نیاز وسیله برای کاربرد، مصرف و تلفات توان تمام اجزاء درون حدود طراحی فیزیکی ماژول تأثیر می‌پذیرد. راهبرد حذف گرما می‌تواند هدایتی، ارتباطی و با تابش باشد. نوعاً وضعیت‌های خنک‌سازی هوای فشرده یا تبادل دمایی طبیعی می‌باشد. عملکرد یک ماژول بسته‌بندی چگالی بالا حساس به منابع گرمایی تولید شده داخلی درون ماژول توزیع شده توسط وسایل استفاده شده در طراحی ماژول است. دمای گرداگرد محیط یا مجاور بهره‌برداری ماژول روی عملکرد ماژول تأثیر می‌گذارد. بالارفتن غیرعادی دما به علت منابع گرمایی نامطلوب داخلی یا انتقال گرمای خارجی روی عملکرد قابلیت اطمینان ماژول تأثیر می‌گذارد. بودجه‌بندی حرارتی تلفات توان منابع بالقوه تولیدکننده گرما، پله‌ای برای شناسایی، کاهش و حذف گرمای ناخواسته تولید شده درون ماژول

را فراهم می‌کند. طراحی حرارتی بایستی در ملاحظات تلفات توان، بالارفتن دما، نرخ خنک‌سازی و حدود بهره‌برداری حرارتی وسایل در نظر گرفته شود. بودجه‌بندی حرارتی بایستی در تمام سطوح سلسله مراتب سیستم از منظر سیستم مدیریت اداره شود.

پ-۵-۴ ملاحظات طراحی کیفیت

کیفیت تمام ویژگی‌های ذاتی یک موجودیت (سیستم، محصول، ماژول، یا جزء) را می‌پذیرد که مربوط به قابلیت آن برای ارضای نیازهای ضمنی و بیان شده می‌شود. کیفیت، دلالت بر انطباق با الزامات دارد؛ از این رو معیارهای پذیرش و روش‌های اجرایی کنترل برای انطباق با پذیرش ایجاد می‌شوند. این کار برای حصول اطمینان از انطباق مداوم با استانداردهای ایجاد شده با مکانیزم‌های مقتضی ساخته شده داخل سیستم یا فرآیند برای تسهیل بهبود مداوم می‌باشد. فرآیندهای تضمین کیفیت و کنترل کیفیت در صنایع به خوبی ایجاد می‌شوند. روش‌های طراحی کیفیت در نوشته‌ها و ملاحظات طراحی کیفیت در اینجا به دقت شرح داده نخواهند شد.

پ-۵-۵ ملاحظات طراحی قابلیت اعتماد

قابلیت اعتماد توانمندی ذاتی یک سیستم برای فراهم نمودن عملکرد آمادگی در فراهم نمودن سطحی از خدمت رضایت بخش بر حسب تقاضا می‌باشد. آمادگی، یک ویژگی عملکردی وابسته به عواملی اثربخش بر آن شامل وظایف عملکرد قابلیت اطمینان، قابلیت نگهداری و پشتیبانی نگهداری است. ملاحظات طراحی قابلیت اعتماد در بخش‌های دیگر این استاندارد نشان داده شده و در اینجا با دقت شرح داده نخواهند شد.

پ-۵-۶ ملاحظات طراحی قابلیت سازگاری محیطی

قابلیت سازگاری محیطی در بازار امروز ضروری است. پیامد محیطی محصول و ماژول در زمان جایگزینی یا وارهایی یک موقعیت چالش‌انگیز برای توسعه‌دهندگان و سازندگان محصولات را نشان می‌دهد. نوعاً تقاضاهای مشتری و کاربر در شکل قرارداد قابل پس دادن هستند که در آن فراهم‌کننده یا تأمین‌کننده محصول مسئول پس گرفتن جایگزینی محصول پیش از نصب یک محصول جدید برای خدمت می‌باشد. قراردادهای باز خرید همچنین در کسب و کار امروز معمول هستند که در آن نیاز است فراهم‌کننده یا تأمین‌کننده یدکی‌ها، مقدار تأمین شده یدکی‌های نگه داشته شده یا خریده شده توسط کاربر یا مشتری که در پایان یک دوره زمانی توافق شده استفاده نشده‌اند را باز خرید کند. در طراحی و ساخت محصولات و ماژول‌ها، ملاحظات بایستی برای استفاده دوباره از قسمت‌های وارهایی معین باشد. بازیافت محصول- فرعی در فرآیند تولید برای کمینه کردن وارهایی هدر رفته، عاملی دیگر است که در مطالعات پیامد محیطی مورد ملاحظه قرار می‌گیرد. کاهش نشر و هدر رفتن از فرآیند چرخه‌ی عمر محیطی محصول بایستی تحت ملاحظه قرار گیرد.

پیوست ت

(اطلاعاتی)

فهرست‌های وارسی[1] مهندسی قابلیت اعتماد سیستم

ت-۱ فهرست‌های وارسی برای مدیریت پروژه قابلیت اعتماد سیستم

ت-۱-۱ کلیات

فهرست‌های وارسی قابلیت اعتماد سیستم برای چرخه‌ی عمر سیستم در نقاط تصمیم اصلی برای تسهیل بازنگری‌های مدیریت پروژه قابل کاربرد می‌باشند. این فهرست‌های وارسی موضوعات حیاتی را که نیاز است برای صحه‌گذاری انجام فعالیت‌های قابلیت اعتماد کلیدی سیستم در هر فاز پروژه نشان داده شوند را شناسایی می‌کند. بازنگری‌های منظم پروژه بین نقاط تصمیم اصلی برای پیاده‌سازی پیش رونده تکالیف برای دستیابی‌های قابلیت اعتماد پیشنهاد می‌شوند. این کار برای حصول اطمینان از اینست که تمام موضوعات حیاتی ارزیابی و حل شوند. سوابق بازنگری می‌توانند به عنوان شواهد عینی برای پشتیبانی از فرآیند تضمین قابلیت اعتماد پروژه استفاده شوند. فهرست‌های وارسی فرآیندهایی برای انتقال قابلیت پاسخگویی پروژه و گذار مالکیت سیستم طی کل چرخه‌ی عمر سیستم را منعکس می‌کنند. این فهرست‌های وارسی می‌توانند توسط تأمین‌کننده و مشتری برای سازگارسازی نیازهای کاربردی خاص آن‌ها استفاده شوند.

ت-۱-۲ فهرست وارسی شناسایی بازار

الف) ماهیت و کاربردهای عملکرد قابلیت اعتماد سیستم تعریف شده و قصد جایگزینی یک سیستم موجود را دارند یا اینکه ارتقای آن شناخته شده‌اند؛

ب) زمان‌بندی برای عرضه سیستم جدید با خصایص قابلیت اعتماد خاص ایجاد شده‌اند؛

پ) محیط‌های بهره‌برداری سیستم، عوامل تاثیرگذار خاص قابلیت اعتماد و موضوعات تنظیمی مرتبط شناسایی شده‌اند؛

ت) توانمندی‌های فنی برای مهندسی قابلیت اعتماد تکوین سیستم شناسایی شده‌اند؛

ث) منابع مورد نیاز برای پشتیبانی از پروژه قابلیت اعتماد شناسایی و تخمین زده شده‌اند؛

ج) سرمایه‌گذاری‌های بزرگ و اکتساب ابزارهای خاص قابلیت اعتماد و مکانیزم‌های توانا ساز برای تکوین سیستم شناسایی شده‌اند؛

چ) مشتریان بالقوه و رقیبان احتمالی علاقه‌مند به تکوین سیستم با تمرکز بر عملکرد قابلیت اعتماد شناسایی شده‌اند؛

1 - Checklist

خ) الزامات عملکردی مورد انتظار سیستم و خصایص ویژه سیستم شامل شناسایی موضوعات قابلیت اعتماد منحصر به فرد و انتظارات مشتری به طور مثال استحکام نرم‌افزار تعریف شده‌اند؛
د) سناریوهای بهره‌برداری قابلیت اعتماد سیستم، قابلیت بهره‌برداری متقابل با سیستم‌های دیگر، تقدم طراحی فناورانه و موضوعات موروثی مرتبط شناسایی شده‌اند؛
ذ) الزامات پشتیبانی لجستیک و نگهداری سیستم برای بهره‌برداری قابل اعتماد شناسایی شده‌اند؛
ر) راهبرد بازاریابی و طرح برای شیوه به کار بردن قابلیت اعتماد در عملکرد سیستم ایجاد شده‌اند؛
ز) یک گروه پروژه برای کار فنی و پیشنهادی با پشتیبانی تجربه قابلیت اعتماد ایجاد شده‌اند؛
ژ) تصمیم برو/ نرو برای تکوین سیستم می‌تواند با یک تمرکز روی عملکرد قابلیت اعتماد راهبردی توجیه شود.

ت-۱-۳ فهرست وارسی تکوین سیستم

الف) یک طرح تکوین پروژه برای پیاده‌سازی تکالیف قابلیت اعتماد ایجاد شده‌اند؛
ب) الزامات سیستم تحلیل شده‌اند و ویژگی‌های قابلیت اعتماد ارزیابی شده‌اند؛
پ) راهبرد طراحی، انتخاب فناوری و فعالیت‌های قابلیت اعتماد برای تکوین سیستم تعیین شده‌اند؛
ت) طرح کیفیت و فرآیند تضمین قابلیت اعتماد ایجاد و پیاده‌سازی شده‌اند؛
ث) فرآیند استانداردسازی و قواعد طراحی قابلیت اعتماد پیاده‌سازی ایجاد شده‌اند؛
ج) معماری سیستم و پیکره‌بندی فیزیکی در برآوردسازی الزامات عملکرد سیستم تعیین شده‌اند؛
چ) طرح یکپارچگی سیستم و زیر سیستم ایجاد شده‌اند؛
ح) جزءبندی سخت‌افزار، واسط‌های نرم‌افزار و طراحی‌های عواملی انسانی برای برآورده‌سازی الزامات عملکرد سیستم تعیین شده‌اند؛
خ) الزامات عملکرد قابلیت اعتماد سیستم و شرایط بهره‌برداری مشخص شده‌اند؛
د) راهبرد آزمون سیستم، پوشش آزمون و سنجش وظیفه‌ای انجام شده‌اند؛
ذ) وظایف سیستم برای برآورده‌سازی نیازهای عملکرد قابلیت اعتماد سنجیده شده‌اند؛
ر) طراحی‌های سیستم و قابلیت اعتماد وظایف سیستم صحه‌گذاری شده‌اند؛
ز) کار پروژه برون‌سپاری، شرکای تکوین و تأمین‌کنندگان مقدم هماهنگ و کامل شده‌اند؛
ژ) منابع ثانویه شناسایی می‌شوند و برای پشتیبانی از جایگزین کردن نیازهای پروژه هماهنگ شده‌اند؛
س) سیستم‌های توانا ساز قابل کاربرد و راهبرد پشتیبانی برای دستیابی‌های قابلیت اعتماد سیستم به کار گرفته شده‌اند؛
ش) قابلیت ساخت برای تحقق محصول و موضوعات قابلیت اعتماد مرتبط تعیین شده‌اند؛
ص) مستندات طراحی، دستورالعمل‌های آموزشی و روش‌های اجرایی آزمون انجام شده‌اند؛
ض) بهره‌برداری از سیستم و طرح پشتیبانی ایجاد شده‌اند؛
ط) طرح پشتیبانی لجستیک ایجاد شده‌اند؛
ظ) خط مشی نگهداری و سطوح تعمیر مونتاژ کمترین سطح ایجاد شده‌اند؛

ع) تصمیم برو/ نرو برای تحقق محصول می‌تواند توجیه شود.

ت-۱-۴ فهرست وارسی تحقق محصول

الف) طرح پیاده‌سازی محصول ایجاد شده‌اند؛

ب) کیفیت محصول و تکالیف تضمین قابلیت اعتماد پیاده‌سازی شده‌اند؛

پ) هماهنگی تأمین‌کننده محصول و کنترل ارزیابی قابلیت اعتماد انجام شده‌اند؛

ت) محصولات بازاری مورد نیاز برای مشارکت در وظایف سیستم سنجیده شده‌اند؛

ث) سنجش زیر سیستم و محصول برای تصدیق قابلیت اعتماد انجام شده‌اند؛

ج) سنجش عملکرد و آزمون سیستم و زیر سیستم انجام شده‌اند؛

چ) یکپارچگی سیستم و مشارکت زیر سیستم به دست آمده است؛

ح) مسدود کردن طراحی و طرح کنترل پیکره‌بندی ایجاد شده‌اند؛

خ) الزامات عملکرد سیستم صحه‌گذاری شده‌اند؛

د) راهبرد پذیرش سیستم ایجاد شده‌اند؛

ذ) تحلیل گزارش وقوع خرابی و سیستم اقدام اصلاحی ایجاد و پیاده‌سازی شده‌اند؛

ر) تصمیم برو/ نرو برای انتقال سیستم و پذیرش مشتری می‌تواند توجیه شود.

ت-۱-۵ فهرست وارسی پذیرش سیستم

الف) طرح پذیرش سیستم با مشورت مشتری ایجاد شده‌اند؛

ب) طرح اثبات عملی عملکرد قابلیت اعتماد سیستم و دوره وارانتی قابل کاربرد ایجاد می‌شود و توسط مشتری پذیرفته شده‌اند؛

پ) سیستم گزارش رخداد پیاده‌سازی می‌شود و معیارهایی برای گزارش ایجاد شده‌اند؛

ت) طرح پشتیبانی و بهره‌برداری سیستم برای دستیابی به عملکرد قابلیت اعتماد پیاده‌سازی شده‌اند؛

ث) آموزش برای اپراتورها و متخصص نگهداری‌های سیستم هدایت شده و برای کارآموزان جایی که قابل کاربرد باشند، صدور گواهی صورت گرفته است؛

ج) پشتیبانی سیستم برای شرکت شخص ثالث از قبیل خدمات کالیبراسیون، شناسایی، هماهنگ و تصدیق شده‌اند؛

چ) روش‌های اجرایی تنفیذ سیستم برای انتقال به بهره‌برداری مشتری ایجاد شده‌اند؛

ح) انتقال قانونی مالکیت سیستم به مشتری تحت قرارداد کامل شده‌اند؛

خ) تصمیم برو/ نرو برای بهره‌برداری حین خدمت می‌تواند توجیه شود.

ت-۱-۶ فهرست‌های بهره‌برداری حین خدمت

الف) طرح پشتیبانی و بهره‌برداری سیستم پیاده‌سازی شده‌اند؛

ب) پایش عملکرد سیستم و روش‌های اجرایی کنترل پیاده‌سازی شده‌اند؛

پ) سیستم گزارش رخداد برای ردیابی عملکرد قابلیت اعتماد، بهره‌برداری تداوم خدمت، فعالیت‌های پشتیبانی نگهداری و اقدامات اصلاحی و پیشگیرانه پیاده‌سازی شده‌اند؛

ت) اقدامات نگهداری ردیابی شده‌اند؛
ث) روش‌های اجرایی تغییر طراحی و کنترل پیکره‌بندی فعال شده‌اند؛
ج) طرح پشتیبانی لجستیک پیاده‌سازی شده‌اند؛
چ) تحلیل مربوط به بهره‌برداری سیستم پیاده‌سازی شده‌اند؛
ح) موارد غیرعادی و نواحی مربوط به بهره‌برداری برای بهبود شناسایی شده‌اند؛
خ) روند عملکرد قابلیت اعتماد سیستم ایجاد شده‌اند؛
د) نظرسنجی‌های رضایت کاربر نهایی هدایت شده‌اند؛
ذ) تصمیم برو/ نرو برای حفاظت از بهره‌برداری حین خدمت سیستم موجود می‌تواند توجیه شود.

ت-۱-۷ فهرست وارسی ارتقاء

الف) نیازهای بازار برای ارتقای سیستم ایجاد شده‌اند؛
ب) ارزیابی‌های مقدار و ریسک برای توجیه تلاش ارتقاء ارزیابی شده‌اند؛
پ) پیامد عملکرد قابلیت اعتماد به علت تغییرات ارتقاء تصدیق شده‌اند؛
ت) پیامد محیط و دیگر عواملی اثربخش شامل مقررات، ایمنی و موضوعات امنیتی مرتبط با تغییرات ارتقاء بررسی و صحه‌گذاری شده‌اند؛
ث) برنامه زمان‌بندی زمان و هزینه برای کار ارتقاء تخمین زده شده‌اند؛
ج) منابع مورد نیاز برای کار ارتقاء تعیین شده‌اند؛
چ) تصمیم برو/نرو برای ارتقای سیستم می‌تواند توجیه شود.

ت-۱-۸ فهرست وارسی کنار گذاری

الف) نیاز و زمان‌بندی برای کنار گذاری سیستم ایجاد شده‌اند؛
ب) علل کنار گذاری از قبیل کهنگی، محدودیت‌های اقتصادی و مقرراتی تعیین شده‌اند؛
پ) جایگزینی سیستم برای فراهم نمودن خدمت مداوم سیستم تعیین شده‌اند؛
ت) مفاهیم اجتماعی به علت پایان خدمت ارزیابی شده‌اند؛
ث) تصمیم برو/نرو برای کنارگذاری سیستم می‌تواند توجیه شود؛
ج) طرح برای گذار یکپارچه از سیستم قدیمی به جدید ایجاد و تضمین شده‌اند؛

ت-۲ فهرست‌های وارسی برای کاربردهای طراحی عوامل سخت‌افزاری، نرم‌افزاری و انسانی

ت-۲-۱ کلیات

فهرست‌های وارسی برای کاربردهای طراحی عواملی سخت‌افزاری، نرم‌افزاری و انسانی می‌تواند برای مهندسی قابلیت اعتماد در سیستم استفاده شود. این موارد فرآیند طراحی محصول و تکوین سیستم را تسهیل می‌کنند. انتخاب عناصر سخت‌افزاری و نرم‌افزاری ترکیب شده برای طراحی وظایف سیستم اغلب فرصتی برای سبک سنگین کردن‌ها را برای تسهیل تقابل‌های انسانی نشان می‌دهد. عواملی انسانی نقش مهمی را در

بیشینه کردن عملکرد قابلیت اعتماد سیستم بازی می‌کنند. طراحی‌های سیستم بایستی فهرست‌های وارسی مکمل برای کاربردهای طراحی بهینه را مورد توجه قرار دهد.

ت-۲-۲ فهرست‌های وارسی طراحی سخت‌افزار سیستم

الف) الزامات سخت‌افزاری سیستم ایجاد شده است؛

ب) عناصر سخت‌افزاری انتخاب شده برای طراحی وظایف سیستم شناسایی شده است؛

پ) فناوری سخت‌افزاری و تاریخچه قابلیت اطمینان شناخته می‌شود و ارزیابی شده است؛

ت) پیکره‌بندی سخت‌افزاری سیستم تعیین شده است؛

ث) مشخصات طراحی سخت‌افزاری ایجاد شده است؛

ج) مفهوم بسته‌بندی سخت‌افزاری و نقشه ماژول‌بندی تعیین شده است؛

چ) بودجه حرارتی در یک پروفایل بهره‌برداری برای تعیین نقاط گرم و نقشه‌های خنک‌سازی با توجه به شرایط محیط ماژول و محیط بهره‌برداری سیستم تحلیل شده است؛

ح) بودجه قابلیت سازگاری الکترومغناطیسی در یک پروفایل بهره‌برداری برای شناسایی الزامات گستره حفاظت، فیلترینگ، جزءبندی و قرارگیری ایجاد شده است؛

خ) اتصال و واسط ماژول وظیفه‌ای ایجاد شده است؛

د) طرح تأمین و تغذیه توان و استانداردسازی ولتاژ برای سیستم تعیین شده است؛

ذ) مدلسازی عملکرد قابلیت اطمینان سیستم برای گزینه‌های ردوندانسی و طراحی سنجیده شده است؛

ر) تحلیل وظیفه‌ای و تخصیص قابلیت اطمینان برای هر وظیفه سیستم تعیین شده است؛

ز) طرح یکپارچگی سیستم و زیر سیستم تکوین یافته است؛

ژ) قابلیت آزمون‌دهی و نگهداری سیستم تحلیل می‌شود و پوشش آزمون تعیین شده است؛

س) خصایص خود-وارسی و توانمندی آزمون توکار جایی که قابل کاربرد باشند در طراحی ماژول برای تسهیل شناسایی خرابی و تجزیه خرابی به کار گرفته شده است..؛

ش) طراحی‌های مقاومت در برابر خرابی و اجتناب از خرابی در وظایف سیستم به کار گرفته شده است؛

ص) مفهوم نگهداری سیستم و سطوح نگهداری ایجاد شده است؛

ض) تدارک یدکی کمترین سطح مونتاژها تعیین شده است؛

ط) زمان بازگشت برای تجدید یدکی‌ها تعیین شده است؛

ظ) شبیه‌سازی سیستم که در آن نیاز به اثبات عملی عملکرد آمادگی هدایت شده است؛

ع) موارد آزمون سیستم برای آشکارسازی خرابی، تعمیر و جداسازی و زمان توان‌یابی تصدیق شده است؛

غ) محصولات سخت‌افزاری تجاری با مواد در دسترس برای مشارکت در وظایف سیستم سنجیده شده اند؛

ف) روش‌های اجرایی و طرح‌های آزمون ماژول سیستم، زیر سیستم و وظیفه‌ای تکوین یافته است؛

ق) مستندات طرح برای محصول سخت‌افزاری و تولید مونتاژ کامل است.

ت-۲-۳ فهرست‌های وارسی طراحی نرم‌افزاری سیستم

الف) الزامات نرم‌افزاری سیستم ایجاد شده است؛

ب) معماری سیستم تعیین شده است؛
پ) استانداردهای نرم‌افزار برای طراحی و تکوین نرم‌افزار پیاده‌سازی شده است؛
ت) ابزار و خدمات نرم‌افزار برای پشتیبانی از تکوین نرم‌افزاری حاصل شده است؛
ث) جزءبندی نرم‌افزار و تخصیص وظایف ایجاد شده است؛
ج) واسط و پروتکل وظایف نرم‌افزاری ایجاد شده است؛
چ) مشخصات طراحی نرم‌افزار ایجاد شده است؛
ح) برنامه‌های زمانبندی تحویل و طرح‌ها برای طراحی مقدماتی و طراحی با جزئیات ایجاد شده است؛
خ) وظایف ماژول نرم‌افزاری تحت آزمون قرار می‌گیرد و برای برآورده‌سازی مشخصات طراحی تصدیق شده است؛
د) محصولات نرم‌افزاری بازاری برای مشارکت در وظایف سیستم سنجش شده است؛
ذ) معیارهای پذیرش محصول و زیر سیستم نرم‌افزاری ایجاد شده است؛
ر) آزمون پذیرش برای تعیین محصول و زیر سیستم نرم‌افزاری برای برآورده‌سازی معیارهای پذیرش هدایت شده است؛
ز) سنجش و آزمون سیستم نرم‌افزاری برای برآورده‌سازی مشخصات عملکرد صحه‌گذاری شده است؛
ژ) ابزارهای نرم‌افزاری بهره‌برداری و پشتیبانی نگهداری سیستم شناسایی شده است؛
س) مستندات طراحی برای پاسخگویی‌های محصول نرم‌افزاری انجام است.

ت-۲-۴ فهرست‌های وارسی طراحی عواملی انسانی

الف) هدف طراحی عواملی انسانی تعریف شده است؛
ب) طرح عواملی انسانی برای کاربردهای طراحی ایجاد شده است؛
پ) مفاهیم طراحی عواملی انسانی برای قابلیت استفاده، قابلیت مربوط به بهره‌برداری، تخصیص وظیفه و سطح اتوماسیون، تصدیق توانمندی‌های انسانی و محدودیت‌ها در بهره‌برداری و نگهداری سیستم ایجاد شده است؛
ت) واسط‌های سیستم انسانی بر حسب سادگی طراحی وظایف یکسان برای پایداری در بهره‌برداری، قابلیت سازگاری با دیگر سیستم‌های موجود از آن نوع و نمایش‌ها و ارتباطات آگاهی اطلاعاتی کاربر سنجش شده است؛
ث) واسط‌های انسان به رایانه بر حسب طراحی صفحه نمایش برای تسهیل تقابل مناسب کاربر، کنترل‌های ورودی و مکانیزم‌های کنترل، آسانی وارد کردن و ویرایش داده‌ها، نمایش و اطلاعات گرافیکی، خصایص قطع و به روز سازی وظایف مدیریت فایل، پنجره‌های پیغام و خدمات کمکی سنجیده می‌شوند. مهم است که پیغام‌های سیستم صحیح، کامل باشند و برای تحقق آسان گمراه‌کننده نباشند؛
ج) طراحی‌های سیستم خصایص خرابی- ایمن، مقاومت و رواداری خطا، آسانی هدایت موقعیت‌های بحرانی و اضطراری، آسانی توانا سازی و ناتوان کردن وظایف اتوماتیک شده، روال‌های عیب‌یابی ساده برای مدیریت خرابی و آسانی هدایت از طریق مُد تنزل یافته بهره‌برداری سیستم برای اقدام اصلاحی به کار می‌گیرند؛

چ) طراحی‌های سیستم آسانی دسترسی به جایگزین کردن واحدهای قابل حذف و کمترین سطح مونتاژها، برچسب‌گذاری مناسب برای هشدار و بهره‌برداری ایمنی، دسترسی به نظام نامه‌های فنی و مدارک پشتیبانی برای نگهداری، نصب و دستورالعمل‌های تعمیر را به کار می‌گیرند؛
ح) طراحی‌های سیستم برای بهره‌برداری، سطح اتوماسیون و نیازهای آموزش و مهارت را برای اپراتورها و متخصص نگهداری‌ها تعیین می‌کنند؛
خ) مستندات طراحی برای تکوین نظام نامه‌های بهره‌برداری و نگهداری سیستم کامل است.

ت-۲-۵ فهرست‌های وارسی قابلیت سازگاری محیطی

الف) هدف طراحی برای محیط تعریف شده است؛
ب) الزامات طراحی محیطی برای کاربردهای طراحی ایجاد شده است؛
پ) استانداردها و مقررات محیطی بازنگری می‌شوند و در مفاهیم طراحی محیطی و طرح پیاده‌سازی متمرکز روی کاهش تعداد مونتاژهای سخت‌افزار و قسمت‌ها و هدف‌گذاری در استفاده دوباره یا بازیافت ترکیب شده است؛
ت) تعداد قسمت‌های استفاده شده در یک مونتاژ برای کاهش زمان مونتاژ و دمونتاژ برای بهبود کارایی فرآیند بازیافت کمینه شده است؛
ث) طراحی ماژولی برای کمترین سطح واحد قابل جایگزینی با یک وظیفه تک برای مجاز ساختن گزینه‌های خدمت، ارتقای وظیفه‌ای و بازیافت قسمت‌ها ملاحظه شده است؛
ج) دسته‌بندی قسمت‌های غیر بازیافتی در یک موقعیت برای تسهیل دمونتاژ و حذف سریع وارهایی ملاحظه شده است؛
چ) برای زبری و پایداری در ارتقای دمونتاژ دستی ملاحظه شده است؛
خ) اجتناب از جا دادن فلز ذوب شده و تقویت در قسمت‌های پلاستیکی در مونتاژ برای ارتقای جداسازی و بازیافت قسمت‌های پلاستیکی ملاحظه شده است؛
د) ایجاد نقاط شکست و دسترسی مشخص در ترتیب منطقی برای ارتقای آموزش خدمت نگهداری و دمونتاژ ملاحظه شده است؛
ذ) شرایط خاموش کردن یا حالت انتظار هنگامی که برای ذخیره انرژی و کاهش آلودگی ممکن است؛
ر) تعداد چفت و بست‌ها برای کاهش زمان مونتاژ و دمونتاژ کمینه شده است؛
ز) استانداردسازی استفاده از ابزار برای مونتاژ و دمونتاژ برای ذخیره زمان و هزینه تجهیز کردن ملاحظه شده است؛
ژ) دسترسی آسان به نقاط چفت و بست برای ارتقای قابلیت نگهداری و خدمات‌دهی ملاحظه شده است؛
س) استفاده از اتصال چفت دار[1] جایی که قابل کاربرد و سودمند باشد برای ارتقای دمونتاژ و آسانی حذف قسمت‌ها ملاحظه شده است؛

1 - Snap-fit

ش) استفاده از مواد چفت و بست سازگار با ارتباط قسمت‌ها برای ارتقای قسمت‌های بازیافت ملاحظه شده است؛
ص) ساختن قسمت‌های سازگار به آسانی قابل جدا شدن هنگام وصل به هم برای ارتقای جداسازی قسمت‌ها برای بازیافت ملاحظه شده است؛
ض) استفاده از مواد چسبناک به طور کلی به علت سختی دمونتاژ قسمت‌ها توصیه نمی‌شوند، به ویژه هنگامی که دو ماده به هم وصل شده در بازیافت ناسازگار هستند. حتی برای مواد سازگار مواد چسبناک می‌تواند باعث آلودگی مواد و بازیافت سخت آن‌ها شود؛
ط) تعداد و طول سیم‌های و کابل‌های مرتبط بایستی برای کاهش زمان مونتاژ و دمونتاژ و اجتناب از تداخل-های الکترومغناطیسی بالقوه کمینه شود؛
ظ) طراحی ارتباطات قابل جدایی برای قسمت‌های دور انداختنی بایستی برای ارتقای دمونتاژ ملاحظه شود.

ت-۳ فهرست‌های وارسی برای استفاده محصولات بازاری در سیستم‌ها

ت-۳-۱ کلیات

محصولات بازاری (COTS) به طور گسترده در کاربردهای سیستم به علت جنبه‌های اقتصادی مهندسی و موقعیت‌های زمان ارائه به بازار در تکوین سیستم استفاده می‌شوند. محصولات COTS به طور کلی هدایت شده توسط بازار هستند و تناسب آن‌ها برای استفاده توسط طیف وسیعی از کاربردهای تجاری به طور عملی اثبات می‌شود. یک محصول COTS، در شکل سخت‌افزار یا نرم‌افزار، یا در ترکیبات مختلف آن‌ها، یک بسته آماده برای خرید تجاری را فراهم می‌کند. مثال‌های نوعی از محصولات COTS شامل تأمینات توان، نرم‌افزار کاربردهای کسب و کار و تجهیزات کنترل الکترونیکی قابل برنامه‌ریزی می‌شوند ولی محدود به آن‌ها نمی‌شوند. خریدار یک محصول COTS هیچ تأثیری روی خصایص محصول و مشخصات مربوط به بهره‌برداری آن ندارد. انتخاب محصولات COTS درست برای مشارکت در سیستم اهمیت ابتدائی برای قابلیت اعتماد مهندسی در سیستم مورد نظر می‌باشد. ریسک‌های معینی مرتبط با انتخاب یک محصول COTS و صحه‌گذاری تناسب آن برای کاربرد خاص سیستم، صرف نظر از خواسته‌های محصول COTS و تطابق اثبات شده آن وجود دارد. این مورد به علت حضور نداشتن تأثیر خریدار روی خصایص محصول و ویژگی‌های عملکرد می‌باشد. استفاده از یک محصول COTS برای کاربرد حیاتی سیستم نیاز به تلاش سنجش اضافی برای تضمین خواهد داشت. فهرست‌های وارسی برای تسهیل شناسایی الزامات، سنجش عملکرد و تضمین محصول COTS برای مشارکت مناسب در کاربرد سیستم فراهم می‌شوند.

ت-۳-۲ فهرست‌های وارسی برای شناسایی الزامات

الف) محصول COTS به طور تجاری با یک شناسایی منحصر به فرد برای خرید در دسترس است و اطلاعات کافی محصول و توصیف وظیفه‌ای برای سنجش تناسب آن برای استفاده در کاربرد مورد نظر را دارد.
ب) چندین تأمین‌کننده محصولات مشابه در بازار تجاری برای انتخاب وجود دارند؛
پ) شناسایی محصول توسط نام، مدل یا نوع، شماره سریال یا تاریخ برچسب سازنده محصول شناسایی شده است؛

ت) توصیف محصول مشخصات محصول، دستورالعمل‌هایی برای نصب و بهره‌برداری محصول، روش‌های اجرایی ارتباطات محصول و الزامات واسط برای کاربرد و نیاز و گستره برای نگهداری و خدمات پشتیبانی محصول را در بر دارد.

ث) برچسب‌های هشداردهنده و روش‌های اجرایی برای بهره‌برداری‌های مرتبط با ایمنی جایی که قابل کاربرد باشند فراهم شده است؛

ج) اطلاعات وارانتی محصول فراهم شده است؛

چ) اطلاعات قابلیت نگهداری و قابلیت اطمینان محصول، تاریخچه عملکرد و پشتیبانی داده‌های آزمون برای تصدیق در دسترس می‌باشند؛

ح) یک بیانیه برای تصدیق کیفیت محصول فراهم شده است؛

ت-۳-۳ فهرست‌های وارسی برای سنجش سوابق عملکرد مستند شده

الف) سوابق عملکرد محصول حاوی مستندات مرتبط با اثبات تطابق با مشخصات محصول برای تصدیق در دسترس می‌باشند؛

ب) مستندات مرتبط شامل طرح آزمون، روش‌های اجرایی آزمون، شرایط و محیط آزمون و سوابق آزمون برای اثبات عملی تطابق محصول با مشخصات استفاده شده است؛

پ) موارد آزمونی طراحی شده برای سنجش شرایط مقاومت در برابر خرابی جایی که قابل کاربرد باشند برای خواسته‌های محصول در تصدیق در دسترس می‌باشند؛

ت-۳-۴ فهرست‌های وارسی برای تضمین محصول

الف) اطلاعات کیفیت محصول و سوابق کیفیت برای تصدیق در دسترس هستند؛

ب) داده‌های ارزیابی تطابق محصول برای تصدیق در دسترس هستند؛

پ) داده‌های میدانی محصول برای پشتیبانی از خواسته‌های عملکرد قابلیت اطمینان در دسترس می‌باشد؛

ت) نرخ‌های بازگشت محصول و روندهای وقوع خرابی برای تصدیق در دسترس هستند؛

ث) سوابق نگهداری محصول برای تصدیق در دسترس هستند.

ج) ارزیابی ریسک محصول و سنجش خصایص محصول و صفات مرتبط فرآیند برای کاربرد حیاتی سیستم انجام می‌شوند. سنجش خاص شامل آشکارسازی خرابی، نیازهای ردوندانسی و ایجاد سطح انسجام محصول COTS مقتضی برای بهره‌برداری سیستم حیاتی می‌شود ولی محدود به آن‌ها نمی‌شود. سطح انسجام تشخیص گستره مقادیر ضروری ویژگی محصول برای نگهداری ریسک‌های سیستم درون حدود قابل رواداری می‌باشد. روش‌شناسی برای تعیین سطوح انسجام در استاندارد ISO/IEC 15026[23] توصیف شده است.

کتابنامه

[1] IEC 61069-1:1991, Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1 General considerations and methodology
[2] IEC 62347, Guidance on system dependability specifications
[3] ISO/IEC 15288, Systems and software engineering – System life cycle processes
[4] ISO/IEC TR15271, Information technology – Guide for ISO/IEC 12207 (Software Life Cycle Processes)
[5] ISO/IEC 12207, Systems and software engineering – Software life cycle processes
[6] ISO/IEC 15939, Systems and software engineering – Measurement process
[7] IEC 60300-3-1, Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology
[8] IEC 60300-3-9, Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems
[9] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems
[10] IEC 61508-1, Functional safety of electrical/electronic/ programmable electronic safetyrelated systems – Part 1 General requirements
[11] DEF STAN 00-42, Part 3. Reliability and Maintainability Assurance Guide – Reliability and Maintainability Case
[12] IEC 61014, Programmes for reliability growth
[13] IEC 61164, Reliability growth – Statistical test and estimation methods
[14] ISO 10007, Quality management systems – Guidelines for configuration management
[15] IEC 60300-3-10, Dependability management – Part 3-10: Application guide – Maintainability
[16] IEC 60300-3-11, Dependability management – Part 3-11: Application guide – Reliability centred maintenance
[17] IEC 60300-3-12, Dependability management – Part 3-12: Application guide – Integrated logistic support
[18] IEEE Std 1175.1, IEEE guide for CASE tool interconnections – Classification and description
[19] ISO/IEC 14102, Information technology – Guideline for the evaluation and selection of CASE tools
[20] ISO/IEC 15940, Information Technology – Software Engineering Environment Services
[21] www.sei.cmu.edu.
[22] IEC 60721(all parts), Classification of environmental conditions
[23] ISO/IEC 15026, Information technology – System and software integrity levels
IEC 60300-3-4, Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements
IEC 60812, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)
IEC 61025, Fault tree analysis (FTA)
IEC 61078, Analysis techniques for dependability – Reliability block diagram and Boolean methods
IEC 61508-7, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures
IEC 61709, Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion

IEC 61713, Software dependability through the software life-cycle processes – Application guide
IEC 61882, Hazard and operability studies (HAZOP studies) – Application guide
IEC 62198, Project risk management – Application guidelines
IEC 62308, Equipment reliability – Reliability assessment methods
IEC PAS 62508, Guidance on human factors engineering for system dependability life cycle applications
ISO 13407, Human-centred design processes for interactive systems
ISO/TR 18529, Ergonomics – Ergonomics of human-system interaction – Human-centred lifecycle process descriptions
ITU-T Recommendation E.800, Terms and definitions related to the quality of service and network performance including dependability
QFD Institute, The official source for Quality Function Deployment, http://www.qfdi.org
References for functional analysis and modelling
EN 1325-1, Value management, value analysis, functional analysis vocabulary – Part 1: Value analysis and functional analysis
EN 12973, Value management
EN 14514, Space engineering standards – Functional analysis
NF X 50-153, Value Analysis – Recommendation for the implementation
IEC/TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment
Federal Information Processing Standards (FIPS) Publication 183: Integration definition for function modeling (IDEF0) US National Institute of Standards and Technology
The Delphi method: Techniques and applications, edited by H. A. Linstone and M. Turoff