INSO
20473
1st. Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ملی ایران
۲۰۴۷۳

چاپ اول

۱۳۹۴

تضمین محصول فضایی - قابلیت اتـــکا

Space product assurance - Dependability

ICS: 03.100.50

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

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

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، 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، سازمان های دولتی و غیر دولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

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

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

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه-بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات آن‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید 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 سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
«تضمین محصول فضایی- قابلیت اتــکا»

رئیس:	**سمت و/ یا نمایندگی**
مظاهری، کریم (دکترای مهندسی هوافضا، آیرودینامیک)	هیأت علمی دانشکده هوافضای دانشگاه صنعتی شریف
دبیر:	
اعوانی، شهریار (کارشناسی‌ارشد مهندسی مکانیک و هوافضا)	مدیر مهندسی تضمین کیفیت پژوهشگاه فضایی ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابراهیمی کچویی، مسعود (دکترای مهندسی هوافضا، مکانیک پرواز و کنترل)	عضو هیئت علمی گروه هوافضا دانشکده فنی و مهندسی دانشگاه تربیت مدرس
اصلانی‌منش، محمد (دکترای مهندسی مکانیک، طراحی کاربردی)	کارشناس مستقل و مشاور مهندسی قابلیت اطمینان
امیری مطلق، جواد (کارشناس ارشد مهندسی هوافضا، جلوبرندگی)	کارشناس پژوهشی پژوهشکده حمل و نقل فضایی- پژوهشگاه فضایی ایران
پاکمنش، محمدرضا (کارشناس ارشد مهندسی مواد- شناسایی، انتخاب و مواد مهندسی)	مدیر فنی آزمایشگاه‌ها پژوهشکده مواد و انرژی- پژوهشگاه فضایی ایران
پورعلی، زهرا (کارشناسی‌ارشد مهندسی صنایع، صنایع)	کارشناس مدیریت تضمین محصول پژوهشکده سامانه‌های ماهواره پژوهشگاه فضایی ایران
تاریخی، پرویز (دکترای فیزیک، اتمی)	کارشناس آزمایشگاه سنجش از دور سازمان فضایی ایران
تیمناک، فرزاد (کارشناسی‌ارشد مهندسی مواد- شناسایی، انتخاب و روش ساخت مواد فلزی)	مدیر تضمین کیفیت پژوهشکده مکانیک پژوهشگاه فضایی ایران

اعضاء: (اسامی به ترتیب حروف الفبا)	**سمت و/ یا نمایندگی**
حبیب‌زاده حقیقی دشتکی، عبدالحسین (کارشناسی مهندسی مکانیک)	کارشناس پژوهشی پژوهشکده مکانیک شیراز پژوهشگاه فضایی ایران
خیری، محمد (کارشناسی‌ارشد مهندسی برق، الکترونیک دیجیتال)	کارشناس پژوهشی مرکز تحقیقات فضایی دانشگاه علم و صنعت
شهپری، سیده زهرا (کارشناسی‌ارشد مهندسی مکانیک، طراحی کاربردی)	کارشناس مدیریت مهندسی تضمین کیفیت پژوهشگاه فضایی ایران
صفایی اردستانی، محمدرضا (کارشناس مهندسی برق، الکترونیک)	کارشناس پژوهشی مرکز تحقیقات فضایی دانشگاه علم و صنعت
عسگری، محمد مهدی (کارشناس ارشد مهندسی صنایع، سیستم‌های اقتصادی اجتماعی)	کارشناس تضمین محصول مرکز تحقیقات فضایی دانشگاه علم و صنعت
عیدی، اعظم (کارشناسی‌ارشد مهندسی کامپیوتر، نرم افزار)	کارشناس پژوهشی پژوهشگاه ارتباطات و فناوری اطلاعات
مخیر، مریم (کارشناسی‌ارشد مهندسی برق، مخابرات)	کارشناس اداره ارتباطات ماهواره‌ای سازمان صدا و سیما جمهوری اسلامی ایران
یادگاری، علیرضا (کارشناسی‌ارشد مهندسی برق، مخابرات)	کارشناس اداره ارتباطات ماهواره‌ای سازمان صدا و سیما جمهوری اسلامی ایران

فهرست مندرجات

پیش‌گفتار

استاندارد «تضمین محصول فضایی- قابلیت اتکا» که پیش‌نویس آن در کمیسیون‌های مربوط توسط پژوهشگاه فضایی ایران تهیه و تدوین شده است و در یکصد و هفتاد و ششمین اجلاس کمیته ملی استاندارد مدیریت کیفیت مورخ ۱۳۹۴/۱۲/۰۲ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

منبع و مأخذی که برای تدوین این استاندارد ملی، مورد استفاده قرار گرفته است به شرح زیر است:

ECSS-Q-ST-30C: 2009,(third issue): Space product assurance- Dependability

مقدمه

استانداردهای ملی فضایی ایران منعکس‌کننده دیدگاه‌های صنعت فضایی ایران است و برای استفاده در پروژه‌های فضایی و به منظور تولید محصولات فضایی و بهره‌برداری از خدمات آنها تهیه شده است. استانداردهای ملی فضایی ایران، بر اساس استانداردهای فضایی اروپا که توسط اتحادیه استانداردسازی فضایی اروپا (ECSS)[1] منتشر می‌شود، تهیه شده است. همچنین در این استاندارد ملی فضایی بر اساس تجربیات صنعت فضایی کشور الزاماتی به طور تکمیلی یا اصلاحی لحاظ شده است و شامل مباحث محتوایی هم چون برنامه قابلیت اتـکا، مهندسی قابلیت اتـکا، تحلیل‌های قابلیت اتـکا و آزمون قابلیت اتـکا می‌باشد که در بخش‌های ۴ تا ۷ این استاندارد تشریح شده است. لازم به توضیح است حوزه قابلیت اتـکا خود مشتمل بر سه موضوع قابلیت اطمینان، قابلیت دسترسی و قابلیت نگهداری است. این استاندارد به روشی انعطاف‌پذیر تدوین شده است تا کاربران بتوانند بر اساس نیازهای خود آنها را متناسب‌سازی نمایند.

در این استاندارد به‌منظور بیان الزامات و تأکید بر موارد از عبارت «لازم است» استفاده می‌کند. از این روی الزامات این استاندارد، تنها بر مبنای اینکه لازم است چه چیزی انجام گیرد تعریف شده و در خصوص چگونگی سازماندهی و نحوه انجام فعالیت‌ها بحثی نمی‌کند. این کار اجازه می‌دهد روش‌ها و ساختارهای سازمانی موجود که کارایی دارند به کار گرفته شوند و برای ابداع روش‌ها و ساختارهای لازم احتیاج به بازنویسی استانداردها نباشد. با این حال ممکن است این استاندارد تمام الزامات و نیازمندی‌های پروژه را پوشش ندهد. در این‌گونه موارد باید الحاقیه‌ای که نیازهای خاص پروژه را تأمین می‌نماید تهیه و پیوست شود. این الحاقیه به همراه استاندارد مربوط، مشخصات فنی آن پروژه یا کار خاص را تشکیل خواهند داد.

استاندارد حاضر در برگیرنده اصول، مقررات و الزامات مربوط به قابلیت اتکا است که برای حوزه‌های مدیریت، مهندسی و تضمین محصول در پروژه‌ها فضایی و کاربردهای آن‌ها قابل استفاده است. لازم به ذکر است که مجموعه استانداردهای ملّی فضایی مطابق استانداردهای فضایی اروپا شامل سه سطح است:

سطح-۱ : خط مشی و اهداف

سطح-۲ : چه‌چیزی انجام گیرد و نتیجه مورد انتظار چیست

سطح-۳ : چطور انجام شود (استانداردهای راهنما)

به هر حال، این استاندارد به‌عنوان معیار و ابزار اجرایی برای کاربران است تا از این طریق بتوانند به ایجاد یک هماهنگی جامع میان گرایش‌های تضمین محصول، مهندسی سیستم و مدیریت پروژه‌های فضایی دست یابند.

1- European Cooperation for Space Standardization (ECSS)

تضمین محصول فضایی –

قابلیت اتــکا

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین برنامهٔ تضمین قابلیت اتـکا و الزامات قابلیت اتـکا[۱] برای سیستم‌های فضایی است. تضمین قابلیت اتـکا یک فرآیند پیوسته و تکرار شونده در تمام چرخه عمر پروژه است. خط‌مشی قابلیت اتـکا محصولات فضایی با اجرای برنامهٔ تضمین قابلیت اتـکا اعمال می‌شود. این برنامه شامل موارد زیر است:

- شناسایی همهٔ ریسک‌های فنی با در نظر گرفتن نیازهای کارکردی[۲] که می‌تواند منجر به عدم انطباق[۳] با الزامات قابلیت اتـکا شود؛
- استفاده از روش‌های طراحی و تحلیل برای حصول اطمینان از برآورده شدن[۴] اهداف[۵] قابلیت اتـکا؛
- بهینه‌سازی هزینهٔ کلی و زمانبندی برای حصول اطمینان[۶] از اینکه:
  - قوانین طراحی، تحلیل‌های قابلیت اتـکا و اقداماتی[۷] برای کاهش ریسک با توجه به طبقه‌بندی شدت مقتضی، متناسب‌سازی شده باشد.
  - اقدامات کاهش ریسک به صورت پیوسته از مرحله اولیهٔ یک پروژه، خصوصاً در طول مرحله طراحی، پیاده‌سازی و اجرا می‌شود.
- درون دادهای[۸] فعالیت‌های تولید متوالی[۹].

الزامات قابلیت اتـکا برای وظایف اجرا شده[۱۰] در نرم‌افزار و برهم‌کنش بین سخت‌افزار و نرم‌افزار در این استاندارد مشخص می‌گردد.

یادآوری ۱– الزامات برای تضمین محصول نرم افزار در استاندارد ECSS-Q-ST-80 تعریف می‌گردد.

۱- واژه انگلیسی «Dependability» بنا به نوع کاربرد دارای معانی مختلفی است، زمانی که این واژه برای سیستمی ذی‌شعور و صاحب اختیار به‌کار می‌رود، معنی فارسی معادل با آن «قابلیت اعتماد» می‌باشد. همانند «Human Dependability» که به معنای «قابلیت اعتماد انسانی» است. زمانی که واژه انگلیسی «Dependability» برای سیستم یا محصول فاقد درک و شعور تصمیم‌گیری به‌کار می‌رود، حتی برای محصولات فضایی که دارای پیچیدگی‌های زیادی هستند به آن«قابلیت اتــکا» یا «اتکاپذیری» اطلاق می‌شود.

2- Functional needs
3- Non-compliance
4- Meet
5- Targets
6- Ensure
7- Actions
8- Inputs
9- Serial production activities
10- Implemented

یادآوری ۲- برنامهٔ تضمین قابلیت اتـکا، فرآیند مدیریت ریسک پروژه را همان‌طورکه در استاندارد ECSS-M-ST-80 شرح داده شده است، پشتیبانی می‌کند.

این استاندارد برای تمام پروژه‌های فضایی قابل استفاده است. قوانین این استاندارد برای همهٔ مراحل پروژه به‌کار می‌رود. این استاندارد را می‌توان برای مشخصات ویژه و قیود[1] پروژه‌های فضایی در انطباق با استاندارد ECSS-S-ST-00 متناسب‌سازی کرد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که درمتن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد 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 تجدیدنظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ECSS-S-ST-00-01, ECSS system - Glossary of terms

2-2 ECSS-Q-ST-10, Space product assurance - Product assurance management

2-3 ECSS-Q-ST-10-04, Space product assurance - Critical- item control

2-4 ECSS-Q-ST-30-02, Space product assurance - Failure modes, effects (and criticality) analysis (FMEA/ FMECA)

2-5 ECSS-Q-ST-30-11, Space product assurance - Derating- EEE components

۳ اصطلاحات، تعاریف و اختصارات

۳-۱ اصطلاحات و تعاریف برگرفته از دیگر استانداردها

در این استاندارد، علاوه بر اصطلاحات و تعاریف اشاره شده در استاندارد ECSS-ST-00-01، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

- سیستم فضایی
- سیستم‌های زمینی

۳-۲ اصطلاحات و تعاریف خاص این استاندارد

۳-۲-۱

سناریوی خرابی

شرایط و توالی رخدادهایی[2] که از علت ریشه‌ای اولیه، منجر به خرابی[3] نهایی می‌گردد.

1- Constraints
2- Events
3– Failure

۲-۲-۳

المان[1] فضایی

محصولاتی که قرار است در فضا کار کنند.

۳-۲-۳

بخش[2] فضایی

یک یا چند المان فضایی

۴-۲-۳

اقلام با عمر محدود

اقلامی که در طی عمر مفید یا در محدوده چرخه‌های عملیاتی خود مستعد فرسودگی، تنزل عملکرد یا کاهش کیفیت به سطحی کمتر از حداقل کارایی لازم برسند که زمان آن در زمانی کمتر از زمان انبارش یا مأموریت است.

۳-۳ اختصارات

در این استاندارد، از اختصارات ارائه شده در استاندارد ECSS-S-ST-00-01 و نیز اختصارات زیر استفاده می‌شود:

فارسی	عبارت انگلیسی	اختصارات
هیئت کنترل پیکربندی	Configuration Control Board	CCB
الکتریکی، الکترونیکی و الکترومکانیکی	Electrical, Electronic and Electromechanical	EEE
آشکارسازی، جداسازی و بازیابی خرابی	Failure Detection, Isolation and Recovery	FDIR
تحلیل حالات خرابی و اثرات آن‌ها	Failure Modes and Effects Analysis	FMEA
تحلیل حالات خرابی، اثرات و شدت بحرانی بودن آن‌ها	Failure Modes, Effects and Criticality Analysis	FMECA
تحلیل درخت عیب	Fault Tree Analysis	FTA
تحلیل برهم‌کنش سخت‌افزار- نرم‌افزار	Hardware-Software Interaction Analysis	HSIA
واسط انسان و ماشین	Man-Machine Interface	MMI
هیئت بازنگری مواد	Material Review Board	MRB
زمان میانگین بین دو خرابی متوالی	Mean Time Between Failure	MTBF
میانگین زمان تعمیر	Mean Time To Repair	MTTR
هیئت بازنگری عدم انطباق	Nonconformance Review Board	NRB
تضمین محصول	Product Assurance	PA
هیئت بازنگری آزمون	Test Review Board	TRB
تحلیل بدترین حالت	Worst Case Analysis	WCA

1- Element
2- Segment

۴ برنامه قابلیت اتــکا

۴-۱ اصول کلی

الف- تضمین قابلیت اتـکا باید از طریق یک فرآیند نظام‌مند برای تعیین الزامات قابلیت اتـکا و اثبات[۱] دست‌یافتنی بودن این الزامات، پیاده سازی و اجرا شود.

ب- لازم است فرآیند تضمین قابلیت اتـکا با طرح برنامهٔ تضمین قابلیت اتـکا برای پروژه تطابق داشته باشد.

۴-۲ سازمان[۲]

الف- لازم است تأمین‌کننده مدیریت برنامهٔ قابلیت اتـکا را با مدیریت برنامهٔ تضمین محصول (PA)[۳] هماهنگ، پیاده‌سازی و یکپارچه[۴] نماید.

۴-۳ طرح برنامه[۵] قابلیت اتــکا

الف- لازم است تأمین‌کننده طرح قابلیت اتـکا را برای تمامی مراحل پروژه، مطابق با تعریف الزامات سند (DRD)[۶] در پیوست پ توسعه، برقرار و اجرا نماید.

ب- لازم است طرح، الزامات کاربردی این مدرک را نشان دهد.

یادآوری- این طرح می‌تواند در طرح برنامه تضمین محصول گنجانده شود.

پ- به میزان و سطحی که تضمین قابلیت اتـکا به‌کار می‌رود، لازم است تا میزان شدت پیامدهای خرابی‌ها مطابق جدول ۱ تعریف شود.

ت- لازم است، برقراری، پیاده‌سازی و اجرای طرح برنامه قابلیت اتـکا با توجه به جنبه‌های ایمنی این برنامه در نظر گرفته شود.

ث- لازم است تأمین‌کننده اطمینان حاصل کند که هرگونه تضاد بالقوه بین الزامات قابلیت اتـکا و الزامات ایمنی مدیریت می‌شود.

ج- لازم است مسئولیت تمام وظایف قابلیت اتـکا در هر مرحله از چرخه عمر تعریف شود.

۴-۴ ارزیابی[۷] و کنترل ریسک قابلیت اتــکا

الف- به عنوان بخشی از فرآیند مدیریت ریسک پیاده‌سازی شده در پروژه، لازم است مهندس قابلیت اتـکا مسئول شناسایی و گزارش‌دهی ریسک‌های مرتبط با قابلیت اتـکا باشد.

یادآوری- استاندارد مدیریت پروژه فضایی - مدیریت ریسک، فرآیند مدیریت ریسک را توضیح می‌دهد.

ب- لازم است تحلیل، کاهش و کنترل ریسک قابلیت اتـکا شامل مراحل زیر باشد:

1- Demonstring
2- Organization
3- Product Assurance
4- Integrate
5- Programme plan
6- Document Requirements Definition
7- Assessment

۱- شناسایی و طبقه‌بندی رخدادهای نامطلوب مطابق با شدت پیامدهای آن‌ها؛
۲- تحلیل سناریوهای خرابی، تعیین حالات خرابی مرتبط، علل یا منشاء خرابی؛
۳- طبقه‌بندی بحرانی بودن[1] وظایف و محصولات مرتبط بر طبق شدت پیامدهای خرابی مرتبط؛
۴- تعریف اقدامات و توصیه‌هایی برای ارزیابی دقیق ریسک، برای رفع یا کنترل و کاهش ریسک به یک سطح قابل قبول؛
۵- وضعیت کاهش و پذیرش ریسک؛
۶- پیاده‌سازی کاهش ریسک؛
۷- تصدیق کاهش ریسک و ارزیابی ریسک‌های باقیمانده.

یادآوری- فرآیند شناسایی و ارزیابی ریسک هم به صورت رویکرد کیفی و هم رویکرد کمی انجام می گیرد.

پ- لازم است اقدامات[2] کاهش ریسک که برای قابلیت اتـکا پیشنهاد می‌شود در سطح سیستم ارزیابی شوند، تا اینکه با استفاده از نتایج آن بتوان راه حلی بهینه برای کاهش ریسک سطح سیستم انتخاب کرد.

۴-۵ اقلام بحرانی قابلیت اتـکا

الف- لازم است اقلام بحرانی قابلیت اتـکا با استفاده از تحلیل قابلیت اتـکا شناسایی شوند تا بتوان با کمک آن از فرآیندهای کنترل و کاهش ریسک، پشتیبانی به عمل آورد.

یادآوری- معیارهای شناسایی اقلام بحرانی قابلیت اتـکا در زیربند ۶-۵ ارائه شده است.

ب- لازم است اقلام بحرانی قابلیت اتـکا، بـه‌عنـوان بخشـی از لیسـت اقـلام بحرانـی مطـابق بـا اسـتاندارد ECSS-Q-ST-10-04 مورد ارزیابی ریسک و کنترل اقلام بحرانی قرار گیرد.

پ- لازم است اقدامات کنترلی شامل موارد زیر باشد:

۱- بازنگری تمامی مستندات و مدارک طراحی، ساخت و آزمون مرتبط با کارکردهای بحرانی، اقلام و روش‌های اجرایی[3] بحرانی،
۲- ارائه قابلیت اتـکا در هیأت بازنگری مربوطه برای اطمینان از اینکه در بیان وضع موجود، سطح بحرانی بودن آن‌ها در نظر گرفته می‌شود.

ت- لازم است جنبه‌های قابلیت اتـکا در تمامی مراحل فرآیند تصدیق اقلام بحرانی قابلیت اتـکا تا انتها در نظر گرفته شود.

۴-۶ بازنگری‌های طراحی

الف- لازم است تأمین‌کننده اطمینان دهد که تمام داده‌های قابلیت اتـکا برای بازنگری طراحی را مطابق با برنامهٔ زمانبندی بازنگری پروژه به کارفرما[4] ارائه شده است.

1- Criticality
2- Measures
3- Procedures
4- Customer

ب- لازم است تمام داده‌های قابلیت اتـکا ارائه شده بر مبنای طراحی دلالت نمایند و لازم است با تمام مدارک فنی پشتیبانی‌کننده دارای ارتباط منطقی[1] باشند.

پ- لازم است تمام تغییرات طراحی به واسطهٔ اثراتشان بر قابلیت اتـکا ارزیابی شده و ارزیابی مجددی بر قابلیت اتـکا انجام شود.

۴-۷ درس آموخته‌های قابلیت اتــکا

الف- لازم است درس آموخته‌های قابلیت اتـکا، در حین چرخه عمر پروژه شامل مراحل بهره‌برداری و وارهایی[2] جمع‌آوری شود.

یادآوری- درس آموخته‌های قابلیت اتـکا، موارد زیر را در نظر می‌گیرد:

- اثر الزامات تحمیلی جدید؛
- ارزیابی تمام کارکردهای نامطلوب[3]، نابهنجاری‌ها، انحراف‌ها و چشم‌پوشی‌ها؛
- اثربخشی راهبردهای پروژه؛
- روش‌ها و ابزارهای جدید قابلیت اتـکا که توسعه یا اثبات[4] شده است؛
- تصدیق‌های مؤثر در مقابل تصدیق‌های غیرمؤثری که انجام شده است.

۴-۸ گزارش پیشرفت

الف- لازم است تأمین‌کننده پیشرفت قابلیت اتـکا را به‌عنوان قسمتی از فعالیت‌های تضمین محصول که با استاندارد ECSS-Q-ST-10 همخوانی دارد، به کارفرما گزارش دهد.

۴-۹ مستندات

الف- لازم است تأمین‌کننده تمام داده‌های مورد استفاده برای برنامهٔ قابلیت اتـکا را نگه‌داری نماید.

۵ مهندسی قابلیت اتــکا

۵-۱ یکپارچگی قابلیت اتــکا در پروژه

الف- لازم است قابلیت اتـکا در فرآیند طراحی یکپارچه شود.

ب- لازم است در تمام مرحله‌های پروژه، میان خصوصیات[5] قابلیت اتـکا با بقیهٔ ویژگی‌های[6] سیستم از قبیل جرم، ابعاد، هزینه و عملکرد سیستم طی بهینه‌سازی طراحی، فرایند موازنه مهندسی[7] انجام شود.

یادآوری- قابلیت اتـکا از مشخصات ذاتی سیستم یا محصول است.

پ- لازم است فرایندهای ساخت، مونتاژ، یکپارچه‌سازی، آزمون و بهره‌برداری به‌گونه‌ای باشد که موجب تنزل ویژگی‌های قابلیت اتـکای معرفی شده در طراحی نشود.

1- Coherent
2- Disposal
3- Malfunction
4- Demonstrate
5- Characteristics
6- Attributes
7- Trade Off

۵-۲ الزامات قابلیت اتــکا در مشخصات فنی

الف- لازم است مشخصات الزامات قابلیت اتـکا قسمتی از الزامات کل پروژه باشد.

ب- به‌منظور برقراری و ایجاد الزامات قابلیت اتـکا برای اجرای سطوح پایین‌تر، لازم است الزامات قابلیت اتـکا در یک فرایند بالا به پایین تسهیم[1] شود.

پ- لازم است الزامات قابلیت اتـکا در حین آماده‌سازی و بازنگری مشخصات طراحی و آزمون به‌کار رود.

ت- لازم است الزامات قابلیت اتـکا در مشخصات فنی گنجانده شود.

یادآوری- مشخصات فنی معمولاً شامل موارد زیر است:

- الزامات کارکردی، عملیاتی و محیطی،
- الزامات آزمون شامل سطوح تنش، پارامترهای آزمون و معیارهای رد یا پذیرش،
- حاشیه‌های عملکرد طراحی، عوامل کاهش توان کارکردی (بکارگیری قطعات در کمتر از بار اسمی)[2]، الزامات کمّی قابلیت اتـکا و الزامات کیفی قابلیت اتـکا (شناسایی و طبقه‌بندی رخدادهای نامطلوب) تحت شرایط محیطی مشخص،
- شناسایی عوامل انسانی و چگونگی تأثیر آن‌ها بر قابلیت اتـکا در طول مدت چرخه عمر پروژه،
- شناسایی عوامل داخلی، خارجی و شرایط نصب[3] که می‌تواند بر روی قابلیت اتـکا در مدت چرخه عمر پروژه تأثیر می‌گذارد،
- میزان تحمل خرابی‌ها[4] برای سخت‌افزار و یا کارکرد نامطلوب برای نرم‌افزار،
- آشکارسازی، جداسازی، تشخیص عیب و بازیابی سیستم از خرابی و بازگرداندن آن به یک وضعیت قابل قبول،
- الزامات جلوگیری از خرابی‌هایی که منجر به پیامدهای غیرقابل قبول در فصل مشترک می‌شوند،
- تعریف مفاهیم نگهداری[5]،
- وظایف و الزامات نگه‌داری برای مهارت‌های خاص،
- الزامات برای نگه‌داری پیشگیرانه، ابزارهای خاص و تجهیزات آزمون خاص،
- الزامات مربوط به اثبات[6] و صلاحیت سنجی برای فرآیند و حاشیه فناوری[7]،
- الزامات برای راهبرد نمونه‌برداری از تولیدات متوالی[8] و برای اثبات دوره‌ای حفظ شرایط احراز[9]

۵-۳ معیارهای طراحی قابلیت اتــکا

۵-۳-۱ اصول کلی

الف- لازم است شناسایی نواحی بحرانی طراحی و ارزیابی شدت پیامدهای خرابی، با توجه به سطحی که تحلیل در آن انجام می‌گیرد، تفسیر شود.

1- Apportioned
2- Derating factors
3- Installation
4- Degree of tolerance
5- Maintenance
6- Demonstration
7- Technology margin
8- Serial production
9- Periodical demonstration of qualification preservation

یادآوری- می‌توان سطح سیستم فضایی را به دو بخش فضایی و زمینی تقسیم نمود که برای هر کدام از آن‌ها می‌توان الزامات جداگانه‌ای مهیا کرد. بخش‌های فضایی و زمینی می‌تواند بسته به الزامات قراردادی خاص به دیگر اجزای سطوح پایین‌تر (مانند زیرسیستم، تجهیزات و غیره) تقسیم گردد.

ب- لازم است معیارهای موفقیت (گاهی اوقات به آن معیارهای موفقیت مأموریت می‌گویند) برای هر سطحی که باید تحلیل شود[1]، تعریف گردد.

۵-۳-۲ پیامدها

الف- لازم است طبقه‌بندی شدت[2] (بر حسب نام یا درجه شدت) مطابق با جدول ۱ برای هر یک از حالات خرابی شناسایی شده که مطابق با اثرات (پیامدهای) خرابی تحلیل شده است، اختصاص داده شود[3].

ب- لازم است رده‌های شدت بدون در نظر گرفتن تمهیدات[4] جبرانی موجود، جهت فراهم کردن یک مقیاس مقیاس کیفی[5] از بدترین پیامدهای بالقوهٔ حاصلِ هریک از اقلام خرابی[6] تعیین شوند.

پ- برای تحلیل‌های پایین‌تر از سطح سیستم، شدتی که به علت انتشار خرابی احتمالی است، لازم است مانند شدت سطح ۱ شناخته شود، به عبارتی دیگر برای تحلیل قابلیت اتکا در سطوح پایین‌تر از سطح سیستم، شدتی که منجر به انتشار احتمالی خرابی شود، باید در سطح ۱ دسته‌بندی شود.

یادآوری- همانند تحلیل برای سطوح زیرسیستمو تجهیز.

ت- بعد از عددی که رده شدت را مشخص می‌کند، لازم است پسوندی برای نشان دادن افزونگی (R)[7]، خرابی‌های تک نقطه‌ای (SP)[8]، یا مخاطرات ایمنی (SH)[9] قرار داده شود.

ث- لازم است درک معیارهای مشخص شده در جدول ۱، مورد توافق کارفرما و تأمین‌کننده قرار گیرد.

1- To be analyzed
2- Severity classification
3- Assigned
4- Provision
5- Qualitative measure
6- Item failure
7- Redundancy
8- Single Point failure
9- Safety Hazard

جدول ۱- شدت پیامدها

شدت	سطح	قابلیت اتــکا	ایمنی بدست آمده از استاندارد ECSS-Q-ST-40C
فاجعه آفرین	۱	انتشار خرابی (به زیربند ۵-۳-۲-ج مراجعه شود.)	تلفات جانی، تهدیدات جانی یا آسیب‌های ناتوان کنندهٔ دائمی یا بیماری شغلی
			از دست دادن سیستم واسط پرواز سرنشین دار[1]
			اثرات زیست محیطی زیان‌بار شدید
			از دست دادن امکانات پایگاه پرتاب
			از دست دادن سیستم
بحرانی	۲	از دست دادن مأموریت	ناتوانی موقتی امّا به نحوی که آسیب تهدید جانی نداشته باشد یا موجب بیماری موقتی شغلی نشود
			اثرات عمده زیست محیطی زیان‌بار
			خسارات بزرگ و عمده به اموال عمومی یا خصوصی
			خسارات بزرگ و عمده به سیستم‌های واسط پرواز
			خسارات بزرگ و عمده به تأسیسات زمینی
عمده	۳	تنزل عمده مأموریت	
جزیی یا قابل چشم‌پوشی	۴	تنزل جزیی مأموریت یا هر اثر دیگر	

۵-۳-۳ تحمل خرابی[2]

الف- لازم است الزامات تحمل خرابی در مشخصات عملکرد تعریف گردد.

ب- لازم است در تصدیق، تحمل خرابی تمام حالات خرابی[3] که شدت پیامدهای آن‌ها به‌عنوان فاجعه‌آفرین، بحرانی و عمده طبقه‌بندی می‌شود، نشان داده شود.

۵-۳-۴ رویکرد طراحی

الف- لازم است تأمین‌کننده تأیید کند که قابلیت اطمینان در طراحی بر اساس تحمل عیب و حاشیه‌های طراحی در نظر گرفته شده است.

ب- لازم است تأمین‌کننده به‌منظور شناسایی نواحی مورد ضعف طراحی، خصوصیات خرابی سیستم را تحلیل نماید و راه حل‌های اصلاحی را پیشنهاد دهد.

پ- لازم است به‌منظور پیاده سازی و اجرای جنبه‌های قابلیت اتـکا در طراحی، رویکردهای زیر به‌کار رود:

۱- طراحی کارکردی:

1- Interfacing manned flight system
2- Failure tolerance
3- Failure modes

۱-۱- استفادهٔ ترجیحی از روش‌ها یا طراحی‌های نرم‌افزاری که در کاربردهای مشابه با موفقیت عمل نموده است؛

۱-۲- پیاده‌سازی و اجرای تحمل خرابی؛

۱-۳- پیاده‌سازی و اجرای آشکار سازی عیب[1]، جداسازی و بازیابی با استفاده از اقدامات زمینی و پروازی اختصاصی، اجازه می‌دهد پردازش خرابی به صورت مناسبی انجام شده و زمان‌های عیب‌یابی یا پیکربندی مجدد در ارتباط با زمان‌های انتشار رخدادها، تحت بدترین شرایط در نظر گرفته شود؛

۱-۴- انجام پایش پارامترهایی که برای انجام مأموریت ضروری می‌باشند با در نظر گرفتن حالات خرابی سیستم نسبت به توانایی واقعی وسایل عیب‌یابی و همچنین در نظر گرفتن شرایط محیطی قابل قبول که برای محصول باید حفظ شود[2].

۲- طراحی فیزیکی:

۲-۱- به‌کارگیری قوانین طراحی تأیید شده؛

۲-۲- استفادهٔ گزینشی از طرح‌هایی که در محیط مأموریتی مشابه با موفقیت عمل کرده‌اند؛

۲-۳- انتخاب قطعاتی که سطح کیفیت آن‌ها مطابق با مشخصات پروژه باشد؛

۲-۴- در نظر گرفتن کاهش توان کاری قطعات و اجزای الکتریکی، الکترونیکی و الکترومکانیکی (EEE)[3] و حاشیه‌های تنش برای قطعات مکانیکی؛

۲-۵- استفاده از شیوه‌های طراحی به‌منظور بهینه ساختن افزونگی (مادامی که پیچیدگی طراحی سیستم تا حد ممکن، پایین نگه داشته شود)؛

۲-۶- اطمینان از اینکه تجهیزات توکار[4] قابلیت آزمون و بازرسی داشته باشند؛

۲-۷- تأمین امکان دسترسی به تجهیزات.

یادآوری- طراحی کارکردی برای دلالت بر به‌کارگیری طراحی غیر فیزیکی در نظر گرفته شده است. به‌عنوان مثال، طراحی نرم‌افزار از این نوع است.

۴-۵ طبقه‌بندی محصولات و کارکردهای بحرانی

الف- لازم است پیمان‌کار در طی مرحله طراحی اولیه، کارکردها، عملکردها و محصولات را مطابق با سطح بحرانی بودن[5] آن‌ها طبقه‌بندی کند.

ب- لازم است طبقه‌بندی توسط کارفرما تأیید شود.

پ- لازم است بحرانی بودن کارکردها (سخت‌افزار و/یا نرم‌افزار) و بهره‌برداری‌ها[6] به طور مستقیم به شدت پیامدهای نتیجه شده از خرابی کارکرد همان‌طور که در جدول ۱ تعریف شده است، ارتباط داده شود.

1- Fault detection
2- To be maintained
3- Electrical, Electronic and Electromechanical
4- Built-in equipment
5- Criticality
6- Operations

یادآوری- برای مثال یک کارکرد که خرابی آن پیامد فاجعه آفرین دارد، لازم است در بالاترین سطح شدت بحرانی بودن طبقه‌بندی گردد.

ت- لازم است شدت بحرانی بودن یک محصول (سخت‌افزار و نرم‌افزار) بر اساس بالاترین شدت بحرانی بودن کارکردهای آن محصول تعیین گردد.

ث- لازم است از این طبقه‌بندی برای تلاش‌های متمرکز بر بحرانی‌ترین نواحی در طی مراحل پروژه استفاده شود.

۵-۵ مشارکت[1] در فرایند آزمون

الف- لازم است تأمین‌کننده اطمینان حاصل کند که جنبه‌های قابلیت اتـکا در تمام مراحل توسعه، صلاحیت‌سنجی، طرح‌ریزی آزمون پذیرش و بازنگری‌ها، شامل آماده‌سازی[2] آزمون، روش‌های اجرایی و ارزشیابی[3] نتایج آزمون، پوشش داده شده است.

ب- لازم است گرایش (حوزه)[4] قابلیت اتـکا مراحل زیر را پشتیبانی کند:

۱- تعریف مشخصات آزمون و اهداف آزمون،

۲- انتخاب پارامترهای اندازه‌گیری، و

۳- ارزشیابی آماری نتایج آزمون.

۵-۶ مشارکت در جنبه‌های بهره‌برداری

الف- لازم است تأمین‌کننده اطمینان دهد که کارکنان آگاه[5] قابلیت اتـکا:

۱- در تعریف نظام‌نامه[6] و روش‌های اجرایی بهره‌برداری همکاری می‌نمایند، و

۲- نظام‌نامه و روش‌های اجرایی بهره‌برداری را به‌منظور تصدیق میزان سازگاری[7] با تحلیل‌های قابلیت اتـکا اتـکا بازنگری می‌کنند.

ب- لازم است روش‌های اجرایی بهره‌برداری به‌منظور شناسایی و ارزیابی ریسک‌های مربوط به بهره‌برداری، مراحل کاری و موقعیت‌هایی که می‌تواند عملکرد قابلیت اتـکا را تحت تأثیر قرار دهد، تحلیل گردد.

پ- لازم است تحلیل‌های مذکور در زیربند ۵-۶-ب، محیط انسانی و فنی را در نظر بگیرد و تصدیق کند که دستورالعمل‌ها:

۱- شامل وضعیت‌هایی[8] برای مواجه شدن با شرایط غیر عادی است و اقدامات لازم برای حفاظت ایمنی را فراهم می‌کند؛

1- Involvement
2- Preparation
3- Evaluation
4- Discipline
5- Cognizant
6- Manual
7- Consistency
8- Dispositions

۲- قابلیت اطمینان تجهیزات را با شرایطی پایین‌تر از حد استاندارد مصالحه نکند[1]؛
۳- مطابق با اقدامات نگهداری باشد؛
۴- شامل مواضعی برای حداقل‌سازی خرابی‌های ناشی از خطای انسانی[2] باشد.

۵-۷ توصیه‌های قابلیت اتــکا

الف- لازم است تأمین‌کننده سیستمی برای پیگیری[3] نمودن توصیه‌های قابلیت اتـکا را به‌منظور کمک به فرایند کاهش ریسک، برقرار و نگه‌داری کند.

یادآوری- این توصیه‌ها از تحلیل‌های قابلیت اتـکا و مطالعات موازنه‌ایی (معمولاً در طی مرحله A و B)[4] منتج می‌شود. توصیه‌های قابلیت اتـکا می‌تواند در ترکیب با توصیه‌های ایمنی پیگیری گردد.

ب- لازم است تمام توصیه‌های زیربند ۵-۷ الف توجیه شوند و پس از مستندسازی پیگیری گردند.
پ- لازم است مدیریت تأمین‌کننده سند رسمی از پذیرش یا عدم پذیرش توصیه فراهم کند.
ت- لازم است توصیه‌های قابلیت اتـکا پذیرفته شده در اسناد متناظر مربوطه اعمال شوند.

یادآوری- به‌عنوان یک مثال از مستندسازی متناظر[5] می‌توان به اسناد طراحی و نظام‌نامه‌های بهره‌برداری اشاره کرد.

۶ تحلیل‌های قابلیت اتــکا

۶-۱ شناسایی و طبقه‌بندی رخدادهای نامطلوب

الف- لازم است تأمین‌کننده رخدادهای نامطلوب که منجر به تنزل یا از بین رفتن عملکردهای محصول می‌شود را همراه با طبقه‌بندی رده‌های[6] مرتبط با شدت، پیامدهای خرابی آن‌ها را شناسایی کند. (جدول ۵-۵-۱ را ببینید.)
ب- لازم است شناسایی و طبقه‌بندی اولیه رخدادهای نامطلوب از تحلیل معیارهای موفقیت مأموریت، در طی مرحله‌های طراحی مفهومی و طراحی اولیه تعیین گردد.
پ- تمام رخدادهای نامطلوب که وقوع آن‌ها می‌تواند موفقیت مأموریت را به خطر بیندازد[7]، یا آن را با شرایطی پایین‌تر از حد استاندارد مصالحه کند[8] یا اینکه آن را تنزل دهد، لازم است در بالاترین سطح محصول (سیستم کلی شامل بخش‌های زمینی و فضایی) ارزیابی گردد.
ت- رخدادهای نامطلوب در سطوح پایین‌تر درختِ محصول، که اثرات خرابی آن‌ها می‌تواند رخدادهای نامطلوب را برای بالاترین سطح محصول ایجاد کند، لازم است شناسایی گردند.

1- Do not compromise
2- Human errors
3- Tracking
۴- به استاندارد ملی «مدیریت پروژه فضایی- طرح ریزی و پیاده سازی پروژه» مراجعه شود.
5- Corresponding documentation
6- Categories
7- Jeopardize
8- Compromise

یادآوری- برای مثال مراجعه شود به بخش فضایی، بخش زمینی، زیرسیستم، و سطح تجهیزات.

ث- لازم است شناسایی و طبقه‌بندی رخدادهای نامطلوب بعد از ارزیابی سناریوهای خرابی نهایی گردند (به زیربند ۶-۲ مراجعه شود).

۶-۲ ارزیابی سناریوهای خرابی

الف- لازم است تأمین‌کننده سناریوهای ممکنی که منجر به وقوع رخدادهای نامطلوب می‌شود را تحلیل کند،

ب- لازم است تأمین‌کننده حالات خرابی، منشأ و علل خرابی، جزئیات آثار خرابی که منجر به رخدادهای نامطلوب می‌گردد را شناسایی کند.

۶-۳ تحلیل‌های قابلیت اتـکا و چرخه عمر پروژه

الف- لازم است تحلیل‌های قابلیت اتـکا در سراسر چرخه عمر تمام پروژه‌های فضایی به‌منظور پشتیبانی از فعالیت‌ها و الزامات تعیین شده در بند ۵ انجام شود.

ب- لازم است تحلیل‌های قابلیت اتـکا در ابتدا برای مشارکت در تعریف طراحی مفهومی و الزامات سیستم انجام شود.

پ- لازم است تحلیل‌ها به‌منظور پشتیبانی از توسعه و بهینه‌سازی طراحی‌های مفهومی، اولیه و دقیق، به انضمام مرحله آزمون که منجر به صلاحیت‌سنجی طراحی می‌شود، انجام شود.

پ- لازم است تحلیل‌های قابلیت اتـکا برای موارد زیر انجام شود:

۱- حصول اطمینان از تطابق الزامات قابلیت اطمینان، قابلیت دسترس‌پذیری و قابلیت نگهداری،

۲- شناسایی تمام حالات خرابی بالقوه و ریسک‌های فنی در ارتباط با الزامات کارکردی که می‌تواند منجر به عدم انطباق[1] از الزامات قابلیت اتـکا شود،

۳- تأمین درون دادها برای ارزیابی ریسک و کاهش ریسک و اقدامات کنترلی آن‌ها که با فرآیند مدیریت ریسک به‌کار رفته در پروژه مطابقت دارد،

ت- لازم است نتایج تحلیل‌های قابلیت اتـکا در پرونده توجیه طراحی[2] به‌منظور پشتیانی از پیشرفت طراحی طراحی افزوده[3] شود.

۶-۴ تحلیل‌های قابلیت اتـکا - روش‌ها

۶-۴-۱ اصول کلی

الف- لازم است تحلیل‌های قابلیت اتـکا در تمام سطوح سیستم فضایی به نسبتِ سطحی که در حال ارزیابی است یعنی سیستم، زیرسیستم و سطوح تجهیزات، هدایت و اجرا گردد.

1- Non-compliance
2- Design justification file
3- Incorporate

یادآوری- هدف اصلی از تمام تحلیل‌های قابلیت اتـکا، بهبود دادن طراحی از طریق بازخورد به موقع به طراح است، تا در فرآیندهایی که منجر به تحقق[1] محصولات می‌شوند و همچنین به‌منظور تأیید تطابق با الزامات قابلیت اتـکا تعیین شده، ریسک‌ها کاهش یابد.

ب- لازم است تحلیل‌های تعیین‌شده در زیربندهای ۶-۴-۲ تا ۶-۴-۴ در قالب موارد زیر باشند:

۱- در صورت لزوم طی قراردادی بین تأمین‌کننده و کارفرما اجرا شوند،

۲- به‌منظور تطبیق الزامات کلی در هر پروژه، متناسب‌سازی شوند،

۳- سخت‌افزار، نرم‌افزار و وظایف انسانی موجود در سیستم را در نظر بگیرند.

یادآوری- از آنجا که امکان ارزیابی کارکردهای نرم‌افزار به صورت کمی امکان‌پذیر نیست، فقط ارزیابی کیفی می‌تواند به‌عنوان قابلیت اتـکا نرم‌افزار طی فرآیند توسعه نرم‌افزار انجام پذیرد.

پ- لازم است مجموعهٔ تحلیل‌های برگزیده از زیربندهای ۶-۴-۲ تا ۶-۴-۴ به‌عنوان بخشی از الزامات قرارداد تعریف شوند.

۶-۴-۲ تحلیل‌های قابلیت اطمینان

۶-۴-۲-۱ پیش‌بینی قابلیت اطمینان

الف- لازم است شیوه‌های پیش‌بینی قابلیت اطمینان با اهداف زیر انجام گیرد:

۱- بهینه کردن قابلیت اطمینان طراحی با توجه به قیود رقابتی همچون هزینه و جرم،

۲- پیش‌بینی قابلیت اطمینان محصول در هنگام بهره‌برداری،

۳- فراهم کردن داده‌های احتمال خرابی در اهدافی مانند ارزیابی ریسک.

ب- لازم است منابع و روش‌های داده‌های قابلیت اطمینان مورد استفاده در پیش‌بینی‌های قابلیت اطمینان، مطابق با خواسته‌های کارفرما مشخص شوند[2].

پ- اگر منابع و روش‌های داده‌های قابلیت اطمینان توسط کارفرما مشخص نگردد، لازم است تأمین‌کننده از منابع داده‌های منتخب و روش‌های مورد استفاده به‌منظور تأیید و تصویب، کارفرما را توجیه کند.

یادآوری- استاندارد ECSS-Q-HB-30-08 یک راهنما برای انتخاب منابع داده‌های قابلیت اطمینان و استفادهٔ آن‌ها است.

ت- لازم است مدل‌های قابلیت اطمینان برای پشتیبانی از پیش‌بینی‌ها و حالات خرابی و اثرات آن‌ها/ تحلیل حالات خرابی، اثرات و شدت بحرانی بودن آن‌ها (FMEA/FMECA)[3] تهیه گردند.

1- Realization
2- Specified
3- Failure Modes, Effects Analysis/Failure Modes, Effects and Criticality analysis

۶-۴-۲-۲ تحلیل حالات خرابی و اثرات آن/ تحلیل حالات خرابی، اثرات و شدت بحرانی بودن آن‌ها (FMEA/FMECA)

الف- لازم است تحلیل FMEA/ FMECA برای طراحی کارکردی و فیزیکی محصول انجام شود، (به ترتیب آن‌ها را FMECA کارکردی و FMECA محصولی گویند) و چنانچه در قرارداد الزام شده باشد، در فرایندهایی که برای تحقق محصول نهایی به‌کار می‌روند، باید FMECA فرایندی انجام گیرد.

ب- لازم است تمام حالات خرابی بالقوه مطابق با شدت پیامد (FMEA) یا میزان بحرانی بودن پیامد آن‌ها (FMECA) شناسایی و طبقه‌بندی شوند.

پ- لازم است اقداماتی طی تحلیل پیشنهاد شوند و در طراحی محصول و کنترل فرایندها برای اولین بار به‌کار گرفته شوند تا تمام پیامدها در پروژه قابل قبول واقع شوند.

ت- زمانی که هرگونه تغییراتی در فرایند یا طراحی انجام می‌گیرد، لازم است FMEA/FMECA به‌روزرسانی شده و اثرات حالات خرابی جدید مطرح شده به‌وسیلهٔ تغییرات، ارزیابی شوند.

ث- لازم است تمهیداتی برای آشکارسازی خرابی و اقدامات بازیابی به‌عنوان بخشی از FMEA/FMECA شناسایی شوند.

ج- لازم است فرایندهای FMEA/FMECA برای پشتیبانی از تصدیق مدل‌سازی قابلیت اطمینان، تحلیل‌های ایمنی و قابلیت اطمینان، تحلیل قابلیت نگهداری، فعالیت پشتیبانی لجستیک[1]، برنامه‌ریزی نگه‌داری و آزمون، و خط مشی آشکارسازی، جداسازی و بازیابی خرابی FDIR[2] به‌کار رود.

چ- لازم است انتشار بالقوهٔ خرابی به‌عنوان بخشی از FMEA/FMECA، ارزیابی گردد.

یادآوری- برای FMEA/FMECA به استاندارد ECSS-Q-ST-30-02 مراجعه کنید.

۶-۴-۲-۳ تحلیل برهم کنش سخت افزار- نرم افزار (HSIA)[3]

الف- لازم است تحلیل (HSIA) برای اطمینان از اینکه نرم‌افزار به خرابی ناشی از سخت‌افزار به طرز قابل قبولی پاسخ می‌دهد، انجام شود.

ب- لازم است تحلیل (HSIA) در سطح مشخصات فنی نرم‌افزار انجام شود.

یادآوری- HSIA می‌تواند بخشی از FMEA/FMECA باشد. به استاندارد ECSS-Q-ST-30-02 مراجعه کنید.

۶-۴-۲-۴ تحلیل احتمال وقوع[4]

الف- لازم است تحلیل پیشامدهای احتمالی مطابق با پیوست ت به‌منظور موارد زیر انجام گیرد:

۱- شناسایی خرابی، شناسایی علت، کنترل اثرات و نشان دادن اینکه چگونه به بازیابی یکپارچگی مأموریت[5] می‌توان دست یافت.

1- Logistic support

2- Failure Detection, Isolation and Recovery

3- Hardware- Software Interaction Analysis

4- Contingency analysis

5- Mission Integrity

۲- شناسایی روش‌های بازیابی کارکردهای اسمی[1] یا تنزل یافته با توجه به خط مشی قابلیت اتـکا پروژه.

یادآوری ۱- اهداف قابلیت دسترسی.

یادآوری ۲- معمولاً تحلیل پیشامدهای احتمالی یک وظیفه در سطح سیستم است.

یادآوری ۳- FMEA/FMECA به‌عنوان درون داد تحلیل پیشامدهای احتمالی است.

۶-۴-۲-۵ تحلیل درخت عیب (FTA)[2]

الف- لازم است تحلیل FTA برای حصول اطمینان از اینکه طراحی با الزامات تحمل خرابی برای ترکیبی از خرابی‌ها تطابق دارد، انجام شود.

یادآوری ۱- استاندارد ECSS-Q-ST-40-12 راهنمایی برای FTA است.

یادآوری ۲- تأمین کنندهٔ سیستم، FTA را به‌منظور مشخص کردن ترکیبی از رخدادهای ممکن که منجر به رخدادهای نهایی نامطلوب (برای مثال «از دست دادن مأموریت») می‌شود، انجام می‌دهد. تأمین کنندهٔ زیر سیستم، درون داد را برای این فعالیت با انجام FTA در سطح زیر سیستم با توجه به رخدادهای بالادستی زیر فراهم می‌کند:

- افت کارکرد[3] زیر سیستم، و
- فعال شدن غیرعمدی کارکرد زیر سیستم.

۶-۴-۲-۶ تحلیل علت مشترک[4]

الف- لازم است تحلیل علت مشترک بر روی قابلیت اطمینان و ایمنی اقلام بحرانی مطابق با پیوست خ، برای مشخص کردن علت ریشه‌ای خرابی‌ها که به طور بالقوه می‌توانند از سطح تحمل خرابی عدول کنند، انجام شود (به زیربند ۵-۳-۳ مراجعه کنید).

یادآوری ۱- تحلیل‌ها می‌تواند به‌عنوان بخشی از FMEA/FMECA یا FTA انجام گیرد.

یادآوری ۲- یک مثال از چک لیست (فهرستی از) پارامترهای علت مشترک عمومی در پیوست ر قرار داده شده است.

۶-۴-۲-۷ تحلیل بدترین حالت (WCA)[5]

الف- لازم است تحلیل WCA برای تجهیزات الکتریکی مطابق با پیوست د انجام شود، این تحلیل نشان می‌دهد که تجهیزات الکتریکی علی‌رغم تغییرات پارامترهای اجزای تشکیل دهنده و شرایط تحمیلی محیطی در محدودهٔ کاری خود عمل می‌کنند.

1- Nominal
2- Fault tree analysis
3- Loss of function
4- Common-cause
5- Worst Case Analysis

ب- لازم است گزارش WCA شامل همهٔ اطلاعات مبنا اعم از (فرضیات، روش‌ها و فنون) که برای تحلیل[1]، اخذ نتایج و مقایسهٔ پارامترهای تعیین شده که از مشخصات تجهیزات یا ماژول استخراج می‌شود، تهیه گردد.

پ- چنانچه الزامات پروژه معین نشده باشد، لازم است تأمین‌کننده میزان انحراف پارامترهای[2] عملکردی و کارکردی تجهیزات الکتریکی ساخته شده در شرایط طراحی که ناشی از پیری یا کهنگی جزء[3] سازنده است را برای تأیید کارفرما پیشنهاد دهد.

یادآوری ۱- استاندارد ECSS-Q-TM-30-12 منبعی برای انحراف پارامترهای ناشی از گذر عمر جزء سازنده است، اما لازم است با دیگر درون دادهایی که به طور کامل در اجزای EEE پوشش داده نشده است، تکمیل گردد.

یادآوری ۲- استاندارد ECSS-Q-HB-30-01 روش WCA را تشریح می‌کند.

۶-۴-۲-۸ تحلیل تنش قطعه

الف- لازم است کاهش توان کاری قطعه مطابق با استاندارد ECSS-Q-ST-30-11 برای حصول اطمینان از اینکه سطح تنش‌های اعمالی برای تمام اجزای الکتریکی، الکترونیکی و الکترومکانیکی EEE در محدوده تعریف شده هستند، انجام شود.

ب- لازم است تحلیل‌های تنش قطعه در سطح قطعه به‌منظور تصدیق اینکه قواعد کاهش توان کاری به‌کار برده شده است، انجام شود.

۶-۴-۲-۹ تحلیل ناحیه‌ای[4]

الف- لازم است تحلیل ناحیه‌ای مطابق با پیوست چ، به‌منظور ارزشیابی[5] پیامدها به علت برهم‌کنش ذاتی زیرسیستم با زیرسیستم در نصب سیستم، انجام شود.

۶-۴-۲-۱۰ تحلیل آشکارسازی جداسازی و بازیابی خرابی (FDIR)

الف- لازم است تحلیل FDIR در سطح سیستم مطابق با پیوست ج، برای حصول اطمینان از اینکه الزامات تحمل خرابی و خودگردانی سیستم تأمین می‌شود، انجام گیرد.

یادآوری- فرآیند FDIR در استاندارد ECSS-E-ST-70-11 تشریح می‌گردد.

۶-۴-۳ تحلیل‌های قابلیت نگهداری[6]

الف- لازم است الزامات قابلیت نگه‌داری باید متناسب با الزامات قابلیت نگه‌داری محصولات سطح پایین بخش‌بندی[7] شود تا با مفهوم نگه‌داری و الزامات قابلیت نگه‌داری مطابقت داشته باشد.

1- Preparation of the analysis

2- Parameter drift

3 -Component aging

4- Zonal

5 -Evaluate

6- Maintainability

7- Apportioned

ب- لازم است پیش‌بینی قابلیت نگه‌داری در سطح سیستم مطابق با پیوست ح انجام گیرد و به‌عنوان ابزار طراحی برای ارزیابی و مقایسه کردن جایگزین‌های طراحی با توجه به الزامات کمی قابلیت نگه‌داری تعیین شده زیر استفاده شود:

۱- زمان لازم برای تشخیص دادن (یعنی آشکارسازی و جداسازی) علل خرابی اقلام،

۲- زمان لازم برای بیرون آوردن و جایگزین کردن هریک از اقلام معیوب[1]،

۳- زمان لازم برای برگرداندن سیستم یا زیرسیستم به پیکربندی نامی خودش و انجام دادن بررسی‌های[2] لازم، و

۴- نرخ خرابی اقلام[3].

پ- لازم است تحلیل نگه‌داری پیشگیرانه برای تعیین طرح نگهداری[4] در سطح سیستم انجام گیرد.

یادآوری- هر اقدام نگه‌داری پیشگیرانه[5] بر مبنای نتایج به‌کارگیری از منطق تصمیم‌گیری سیستمی که مورد تأیید کارفرما است، خواهد بود.

ت- لازم است تحلیل قابلیت نگه‌داری اقلام بحرانی قابلیت نگه‌داری را مشخص کند.

یادآوری- اقلام بحرانی از نظر قابلیت نگه‌داری شامل موارد زیر است:

- محصولاتی که پس از یکپارچه سازی[6] نمی‌توانند بررسی و آزمایش شوند،
- محصولات با عمر محدود،
- محصولاتی که نمی‌توانند مطابقت الزامات قابلیت نگه‌داری را صحه‌گذاری‌کنند یا نمی‌توانند آن الزامات را برآورده نمایند.

۶-۴-۴ تحلیل قابلیت دسترسی[7]

الف- لازم است تأمین‌کننده تحلیل قابلیت دسترسی یا شبیه‌سازی را به‌منظور ارزیابی دسترس‌پذیر بودن سیستم انجام دهد.

یادآوری- نتایج برای موارد زیر به‌کار می‌رود:

- بهینه ساختن مفهوم سیستم با توجه به طراحی، بهره‌برداری و نگهداری،
- تصدیق سیستم در جهت مطابقت با الزامات قابلیت دسترسی،
- فراهم کردن درون دادها برای تخمین هزینهٔ کل بهره‌برداری از سیستم.

ب- لازم است تأمین‌کننده تحلیل از کار افتادگی‌ها[8] را به‌منظور فراهم کردن داده‌های درون داد برای تحلیل تحلیل قابلیت دسترسی انجام دهد.

1- Defective item
2- Checks
3- Failure rate
4- Maintenance plan
5- Preventive maintenance action
6- Integration
7- Availability
8– Outage

پ- لازم است برون داد[1] تحلیل قابلیت دسترسی شامل فهرستی از تمام از کارافتادگی‌های بالقوهٔ شناسایی شده (همان‌طور که در پروژه تعریف شده است)، علل آن‌ها، احتمال وقوع آن‌ها و مدت زمان وقوع آن‌ها باشد.

یادآوری- به جای احتمال از کار افتادگی‌ها، نرخ‌های خرابی وابسته به از کارافتادگی‌ها را می‌توان تهیه کرد.

ت- لازم است ابزار شناسایی از کار افتادگی و روش‌های بازیابی در تحلیل تعیین گردد.

ث- لازم است تحلیل قابلیت دسترسی در سطح سیستم با استفاده از مدل‌های قابلیت اطمینان سیستم و قابلیت دسترسی و نیز داده‌های از کارافتادگی‌ها انجام شود.

یادآوری- برای تحلیل قابلیت دسترسی به استاندارد ECSS-Q-ST-30-09 مراجعه کنید.

۶-۵ فهرست اقلام بحرانی قابلیت اتـکا

الف- لازم است اقلام بحرانی قابلیت اتـکا شناسایی شده به‌وسیلهٔ تحلیل‌های قابلیت اتـکا مطابق با استاندارد ECSS-Q-ST-10-04 نگاشته شود.

ب- اقلامی که به‌عنوان خرابی تک نقطه[2] با حداقل یکی از موارد شدت پیامد خرابی طبقه‌بندی شده تحت عناوین فاجعه‌آمیز، بحرانی یا عمده باشد، لازم است در فهرست اقلام بحرانی قابلیت اتـکا گنجانده شود.

پ- لازم است اقلامی که دارای عدد بحرانی بودن[3] بزرگتر یا مساوی شش هستند، در فهرست اقلام بحرانی قابلیت اتـکا مطابق با استاندارد ECSS-Q-ST-30-02 گنجانده شوند.

ت- لازم است تمام اقلامی که پیامد خرابی آن‌ها به‌عنوان فاجعه‌آمیز طبقه‌بندی شده است در فهرست اقلام بحرانی قابلیت اتـکا گنجانده شوند.

ث- محصولاتی که پس از مونتاژ امکان آزمودن و بررسی آن‌ها وجود ندارد، محصولات با عمر محدود، محصولاتی محصولاتی که الزامات قابلیت نگه‌داری اجرایی را نمی‌تواند برآورده نمایند یا نمی‌توانند آن‌ها را تصدیق کنند، لازم است در فهرست اقلام بحرانی قابلیت اتـکا گنجانده شوند.

ج- لازم است مستندسازی برای هر مورد بحرانی قابلیت اتـکا شامل توجیهی برای نگه‌داری آن مورد به همراه تأیید کارفرما باشد.

یادآوری- معیارهای بیشتر برای طبقه‌بندی اقلام بحرانی قابلیت اتـکا می‌تواند توسط کارفرما هم راستا با خط مشی مدیریت ریسک تعریف شده در پروژه تعیین گردد.

1- Out puts

2- Single-Point Failure

3- Criticality Number

۷ آزمون، اثبات[1] و جمع‌آوری داده‌های قابلیت اتــکا

۷-۱ آزمون و اثبات قابلیت اطمینان

الف- لازم است آزمون و اثبات قابلیت اطمینان مطابق با الزامات پروژه به‌منظور اهداف زیر انجام گیرد:

۱- صحه‌گذاری بر حالات خرابی و اثرات آن‌ها،

۲- بررسی تحمل خرابی، شناسایی و بازیابی خرابی،

۳- به‌دست آوردن داده‌های آماری از خرابی برای پشتیبانی از پیش‌بینی‌ها و ارزیابی ریسک،

۴- تثبیت ارزیابی‌های قابلیت اطمینان،

۵- صحه‌گذاری بر قابلیت سخت‌افزار در کار با نرم‌افزار یا به‌کارگیری سخت‌افزار توسط انسان مطابق با مشخصات،

۶- اثبات قابلیت اطمینان اقلام بحرانی، و

۷- صحه‌گذاری نمودن یا توجیه پایگاه‌های داده‌های مورد استفاده برای اثبات نظری[2].

۷-۲ آزمون و اثبات قابلیت دسترسی

الف- لازم است آزمون و اثبات قابلیت دسترسی مطابق با الزامات پروژه به‌منظور صحه‌گذاری یا توجیه پایگاه‌های داده‌ای که برای اثبات نظری به‌کار می‌رود (مدت زمان از کارافتادگی و احتمال وقوع) انجام شود.

۷-۳ اثبات قابلیت نگهداری

الف- لازم است اثبات قابلیت نگه‌داری با تصدیق الزامات قابلیت نگه‌داری کاربردی انجام شود، همچنین لازم است اثبات قابلیت نگه‌داری را با تضمین اینکه فعالیت‌های نگه‌داری پیشگیرانه[3] و اصلاحی[4] به طور موفق در دامنه کاربرد مفهوم نگه‌داری انجام می‌شوند، تکمیل نمود.

ب- «اثبات قابلیت نگهداری» توانایی موارد زیر را تصدیق خواهد کرد:

۱- آشکارسازی، تشخیص دادن[5] علت خرابی و جداسازی هر واحدِ قابل تعویض خطِ معیوب یا واحد تعویض‌پذیر درمدار؛

۲- بیرون‌آوردن و جایگزین کردن هر واحد قابل تعویض خط[6] یا واحد تعویض‌پذیر مدار؛

۳- انجام تعمیرات ضروری برای انجام مأموریت در واحدهایی که قرار نیست تعویض گردند؛

۴- بررسی اینکه محصول پس از اتمام اقدامات نگهداری، تمامی کارکردهای خود را انجام می‌دهد؛

۵- اثبات اینکه هیچ‌گونه مخاطرهٔ ایمنی در نتیجهٔ انجام اقدامات نگه‌داری ایجاد نشده است؛

۶- اثبات اینکه عملیات نگه‌داری می‌تواند مطابق با قیود اجرایی، شامل عملیات لازم برای آماده‌سازی سیستم در حین پرتاب، انجام شود.

1- Demonstration
2- Theoretical demonstration
3- Preventive
4- Corrective
5- Detect
6- Line

یادآوری ۱- مثالی از این قیود اجرایی می‌تواند زمان، حجم یا قابلیت دسترسی باشد.

یادآوری ۲- مثالی از این عملیات‌ها می‌تواند موارد «بیرون آوردن برخی اقلام قبل از پرواز[1]» یا تعویض باتری‌ها باشد.

۷-۴ جمع‌آوری داده‌های قابلیت اتـکا و پایش عملکرد قابلیت اتـکا

الف- داده‌های قابلیت اتـکا که در قرارداد مشخص شده‌اند، باید در بازه‌های زمانی که به توافق کارفرما رسیده است، از منابعی از قبیل گزارش‌های عدم انطباق، مشکل یا خرابی، و گزارش‌های نگه‌داری جمع‌آوری شوند.

یادآوری- داده‌های قابلیت اتـکا می‌تواند برای پایش عملکردهای قابلیت اتـکا از طریق مدل‌های مشخص شده یا مدل‌های مورد توافق استفاده شود.

1- Remove before flight item

پیوست الف

(اطلاعاتی)

ارتباط بین فعالیت‌های قابلیت اتــکا و مراحل پروژه

الف-۱ تحلیل مأموریت/ مرحله شناسایی نیازها (مرحله صفر)

در این مرحله معمولاً هیچ فعالیت تضمین قابلیت اتـکای مشخصی انجام نمی‌گیرد.

الف-۲ مرحله امکان‌سنجی (مرحله A)

در این مرحله وظایف تضمین قابلیت اتـکا معمولاً شامل موارد زیر می‌باشد:

الف- تدوین و برقراری خط مشی قابلیت اتـکای پروژه برای برآوردن الزامات قابلیت اتـکا؛

ب- پشتیبانی از موازنه طراحی و انجام تحلیل‌های اولیهٔ قابلیت اتـکا برای شناسایی و مقایسهٔ جنبه‌های بحرانی قابلیت اتـکا برای هر گزینهٔ طراحی؛ انجام ارزیابی اولیه قابلیت دسترسی در صورت لزوم؛

پ- انجام شناسایی و طبقه‌بندی اولیهٔ ریسک؛

ت- طرح‌ریزی فعالیت‌های تضمین قابلیت اتـکا در مرحله تعریف پروژه.

الف-۳ مرحله تعریف اولیه (مرحله B)

در این مرحله فعالیت‌های تضمین قابلیت اتـکا معمولاً موارد زیر می‌باشد:

الف- برای تأیید مطالعات موازنه‌ای به‌منظور انتخاب طراحی اولیه؛

ب- ایجاد رده‌های شدتِ اثرات خرابی پروژه و تخصیص دادن الزامات قابلیت اتـکا کمی به تمام سطوح سیستم؛

پ- انجام ارزیابی اولیهٔ سناریوهای ریسک؛

ت- ایجاد الزامات تحمل خرابی قابل اجرا؛

ث- انجام تحلیل‌های اولیهٔ قابلیت اتـکا؛

ج- تعریف اقدامات و توصیه‌ها برای کاهش ریسک، فراهم کردن فهرست اولیهٔ اقلام بحرانی قابلیت اتـکا؛

چ- تهیه کردن طبقه‌بندی شدت بحرانی بودن کارکردها و محصولات؛

ح- پشتیبانی از تعریف مفهوم نگه‌داری و طرح نگهداری؛

خ- طرح‌ریزی وظایف تضمین قابلیت اتـکا برای طراحی تفصیلی (دقیق) و مرحله توسعه‌ای پروژه و تهیه نمودن طرح قابلیت اتـکا به‌عنوان بخشی از طرح تضمین محصول پروژه.

الف-۴ مراحل تعریف تفصیلی و تولید/ آزمون صلاحیت‌سنجی زمینی[1] (مرحله C/D)

در این مرحله وظایف تضمین قابلیت اتـکا معمولاً دربرگیرندهٔ موارد زیر می‌باشد:

الف- انجام ارزیابی دقیق ریسک و تحلیل‌های دقیق قابلیت اتـکا؛

1 -Detailed definition and production/ground qualification testing phases

ب- پایش و بازنگری رده‌بندی‌های شدت بحرانی بودن کارکردها و محصولات؛
پ- تعریف اقدامات و توصیه‌هایی برای کاهش ریسک، انجام تصدیق کاهش ریسک؛
ت- به‌روزرسانی و تصحیح فهرست اقلام بحرانی قابلیت اتـکا و منطق استفاده شده (برای حفظ و نگهداری)؛
ث- تعریف معیارهای طراحی قابلیت نگه‌داری و قابلیت اطمینان؛
ج- پشتیبانی از شناسایی نقاط بازرسی کلیدی و اجباری، شناسایی پارامترهای بحرانیِ اقلام بحرانی قابلیت اتـکا و شروع و پایش برنامهٔ کنترل موارد بحرانی قابلیت اتـکا؛
چ- انجام تحلیل‌های احتمال وقوع در ارتباط با طراحی و مهندسی بهره‌برداری؛
ح- پشتیبانی از بازنگری‌های طراحی و پایش تغییرات به‌منظور بررسی تأثیر آن‌ها بر قابلیت اتـکا؛
خ- تعریف ابزار مورد نیاز و انجام آموزش قابلیت نگه‌داری و اثبات تجربی قابلیت نگهداری؛
د- پشتیبانی از تضمین کیفیت در طی ساخت، یکپارچه‌سازی و آزمون؛
ذ- پشتیبانی از هیأت بازنگری عدم انطباق‌ها (NRB)[1] و هیأت بازنگری خرابی؛
ر- بازنگری طراحی و مشخصات و دستورالعمل‌های آزمون؛
ز- بازنگری دستورالعمل‌های بهره‌برداری برای ارزیابی مسائل قابلیت اطمینانِ انسانی وابسته به واسط انسان و ماشین (MMI)[2]، بررسی سازگاری با مفروضات در نظر گرفته شده در انجام تجزیه و تحلیل قابلیت اتـکا یا تعیین اثرات ناسازگاری‌ها؛
ژ- جمع‌آوری داده‌های قابلیت اتـکا.

الف-۵ مرحله بهره‌برداری (مرحله E)

در این مرحله وظایف تضمین قابلیت اتـکا معمولاً دربرگیرندهٔ موارد زیر می‌باشد:
الف- حمایت از بازنگری‌های آمادگی پرواز؛
ب- حمایت از عملیات پروازی و زمینی؛
پ- ارزیابی اثرات قابلیت اتـکا که از سیر تکاملی طراحی نتیجه شده‌اند؛
ت- بررسی قابلیت اتـکا وابسته به ناهنجاری‌های پروازی؛
ث- جمع‌آوری داده‌های قابلیت اتـکا حین عملیات.

الف-۶ مرحله وارهایی (مرحله F)

در این مرحله وظایف تضمین قابلیت اتـکا معمولاً دربرگیرندهٔ موارد زیر می‌باشد:
الف- بازنگری بهره‌برداری برای توقف[3] کلی یا جزیی به‌منظور استفاده از سیستم و محصولات تشکیل دهندهٔ سیستم و کنارگذاری نهایی آن‌ها؛
ب- تهیهٔ طبقه‌بندی شدت بحرانی بودن کارکردها و محصولات؛
پ- تعریف اقدامات و توصیه‌ها برای کاهش ریسک.

1- Nonconformance Review Board
2- Man-Machine Interface
3- Cessation

پیوست ب

(اطلاعاتی)

فهرست الزامات سند (DRL)[1]

فهرست الزامات سند به‌عنوان برنامهٔ قابلیت اتـکا برای فهرست الزامات سند کلی پروژه به‌کار می‌رود. یک روش توصیه‌شده، بررسی عدم وجود مستندات تکراری تولید شده توسط تأمین‌کننده در برنامه‌های ایمنی و قابلیت اتـکا است.

مشتری(کارفرما) می‌تواند تعیین یا توافق کند که دو یا تعدادی از اسناد در یک گزارش واحد آورده شود.

فهرست زیر اسناد مستندات تعیین شده در این استاندارد را پوشش می‌دهد:

- طرح قابلیت اتـکا؛
- تحلیل حالات خرابی و اثرات (و شدت بحرانی بودن) آن‌ها-FMEA/FMECA؛
- پیش‌بینی قابلیت اطمینان[2]؛
- تحلیل برهم‌کنش سخت‌افزار- نرم‌افزار؛
- تحلیل علت مشترک؛
- تحلیل درخت عیب؛
- تحلیل پیشامدهای احتمالی؛
- تحلیل قابلیت نگهداری؛
- تحلیل قابلیت دسترسی؛
- تحلیل ناحیه‌ای؛
- تحلیل بدترین حالت؛
- تحلیل تنش قطعه؛
- آشکارسازی، شناسایی و بازیابی خرابی؛
- فهرست اقلام بحرانی از لحاظ قابلیت اتـکا؛
- گزارش شناسایی ریسک، ارزیابی، کاهش و کنترل آن.

متناسب‌سازی DRL وابسته به زیربندهای قراردادی پروژه است.

تعریف الزامات سند، به‌منظور نشان دادن تحلیل‌هایی که در سطح-۳ استاندارد ECSS پوشش داده نشده‌اند، می‌باشد.

برای ارجاع به سطح-۳ استاندارد ECSS یا DRDها به پیوست ذ مراجعه شود.

1- Document Requirements List

2- Reliability

پیوست پ

(الزامی)

طرح قابلیت اتــکا- DRD

پ-۱ مقدمه

طرح قابلیت اتـکا پاسخی را برای الزامات قابلیت اتـکای کارفرما فراهم می‌کند.

پ-۲ دامنه کاربرد و قابلیت اجرا

هدف طرح قابلیت اتـکا فراهم کردن اطلاعات در مورد جنبه‌های سازمانی و رویکرد فنی برای اجرای برنامهٔ قابلیت اتـکا است.

پ-۳ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا؛

استاندارد ECSS-Q-ST-10: تضمین محصول فضایی- مدیریت تضمین محصول.

پ-۴ اصطلاحات،تعاریف و اختصارات

اصطلاحات و تعاریف باید مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ از استاندارد ECSS-Q-ST-30 باشد.

پ-۵ شرح و هدف

هدف طرح قابلیت اتـکا، توصیف چگونگی برقراری ارتباط میان گرایش‌های فنی و علمی و فعالیت‌های مربوطه به‌منظور برآورده نمودنِ هماهنگ و یکپارچه الزامات می‌باشد.

همچنین رویکردِ این طرح باید با مدیریت فرایندهای قابلیت اتـکا و همچنین با زمانبندی مناسب و مقرون به‌صرفه پروژه به طور اطمینان‌بخشی سازگار باشد.

این طرح تمام فعالیت‌ها شامل برنامه‌ریزی‌ها، پیش‌بینی‌ها، تحلیل‌ها و اثبات تجربی توانایی کارها را مشخص نموده و به یکدیگر ارتباط داده و همچنین روش‌ها و شیوه‌هایی را برای انجام دادن الزامات قابلیت اتـکا تعریف خواهد کرد.

پ-۶ کاربرد و روابط متقابل

این بند، مسئولیت اصلی برنامهٔ قابلیت اتـکا را تعیین خواهد کرد، همچنین این برنامه شامل جزئیات مرحله‌های اجرایی، محصولات و سخت‌افزار یا نرم‌افزارهای مرتبط با برنامه خواهد بود.

همچنین این بند چگونگی مدیریت نمودن قابلیت اتـکا طی مراحل اجرای پروژه را توصیف می‌کند.

یادآوری- برنامهٔ قابلیت اتـکا می‌تواند بخشی از طرح تضمین محصول باشد.

پ-۷ محتوای مطالب

الف- لازم است طرح قابلیت اتـکا حداقل شامل موارد زیر باشد:

- فهرست اسناد مرجع و اجرایی؛
- الزامات قابلیت اتـکای اجرایی؛
- شرح مدیریت و سازماندهی قابلیت اتـکا؛
- مدیریت تأمین کننده[1]/پیمانکار[2]؛
- شرح جزئیات وظایف قابلیت اتـکا برای هر مرحله؛
- گزارش وضعیت فعالیت‌های قابلیت اتـکا.

1- Supplier
2- Contractor

پیوست ت

(الزامی)

تحلیل احتمال وقوع- DRD

ت-۱ مقدمه

هدف از تحلیل احتمال وقوع، تعیین کردن تمام وقایع احتمالی است که از خرابی سیستم ناشی می‌گردد.

ت-۲ دامنه کاربرد و قابلیت اجرا

این DRD، الزامات محتوی داده‌ها را برای تحلیل حوادث احتمالی ایجاد می‌کند.

ت-۳ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا.

ت-۴ اصطلاحات،تعاریف و اختصارات

اصطلاحات و تعاریف باید مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ استاندارد ECSS-Q-ST-30 باشد.

ت-۵ شرح و هدف

اهداف تحلیل احتمال وقوع عبارتند از:

- شناسایی خرابی، شناسایی علت، کنترل اثر و نشان دادن اینکه چگونه می‌توان به بازیـابی مأموریـتِ بی‌نقص دست یافت.
- شناسایی روش‌های بازیابیِ کارکردهای اسمی یا تنزل یافته با توجه به خـط مشـی قابلیـت اتــکای پروژه (به عنوان مثال اهداف قابلیت دسترسی).

تحلیل احتمال وقوع معمولاً فعالیتی در سطح سیستم است.

ت-۶ کاربرد و روابط متقابل

تحلیل احتمال وقوع با دیگر تحلیل‌های قابلیت اتـکا مانند موارد زیر در ارتباط است:

- پیش‌بینی قابلیت اطمینان؛
- تحلیل درخت عیب؛
- FDIR؛
- تحلیل قابلیت نگهداری؛
- FMEA/FMECA.

ت-۷ محتوا

الف- لازم است سند تحلیل احتمال وقوع شامل موارد زیر باشد:

- توصیف سیستم؛
- تشریح روش اجرایی به‌منظور تحلیل احتمال وقوع؛
- جزئیات روش خرابی؛
- جزئیات تشخیص علت آشکارسازی خرابی؛
- جزئیات اقدامات یا روش‌های اجرایی بازیابی؛
- اقدامات و توصیه‌ها برای تیم پروژه.

پیوست ث

(الزامی)

تخمین قابلیت اطمینان[1] – DRD

ث-۱ مقدمه

اهداف پیش بینی قابلیت اطمینان عبارتند از:

- مقایسهٔ راه حل‌های معماری ممکن راجع به معیار قابلیت اطمینان در طی فرایند موازنه(مصالحه) کردن،
- فراهم کردن داده‌های احتمال خرابی به‌منظور مقایسه با اهداف قابلیت اطمینان و فراهم کردن درون دادها برای ارزیابی ریسک.

تخمین قابلیت اطمینان اولیه نشانه‌ای برای نتیجهٔ سهم قابلیت اطمینان به‌کار رفته در پیش‌بینی را فراهم می‌کند.

ث-۲ دامنه کاربرد و قابلیت اجرا

این DRD الزامات محتوی داده‌ها را برای تخمین قابلیت اطمینان به وجود می‌آورد.

ث-۳ مراجع

ث-۳-۱ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا.

ث-۳-۲ دست‌نامه‌های[2] مرجع

دست‌نامه ECSS-Q-HB-30-08: تضمین محصول فضایی- منابع داده‌های قابلیت اطمینان اجزا و استفادهٔ آن‌ها.

ث-۴ اصطلاحات،تعاریف و اصطلاحات اختصاری

لازم است اصطلاحات و تعاریف مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ استاندارد ECSS-Q-ST-30 باشد.

ث-۵ شرح و هدف

تخمین قابلیت اطمینان بر اساس دو بخش می‌باشد:

- مدل قابلیت اطمینان: با در نظر گرفتن انواع افزونگی‌های ممکن،
- تعیین نرخ خرابی یا معادل هر بخش تحت تحلیل.

راه‌های زیادی برای محاسبهٔ نرخ خرابی پیش‌بینانه از جمله موارد زیر وجود دارد:

1- Reliability prediction

2– Handbooks

- تجربیات حین خدمت محصول بر اساس آزمون‌های شتاب داده شده[1] یا براساس جمع‌آوری داده‌های حین خدمت. در این مورد، هماهنگی جمع‌آوری داده‌ها باید توجیه شود،
- قضاوت مهندسی،
- پایگاه داده‌های قابلیت اطمینان: به‌منظور محاسبهٔ نرخ خرابی مطابق با پارامترهایی همچون بهره‌برداری (یعنی سیکل کاری)، مشخصات فیزیکی (تعداد درون دادهای مدار مجتمع)، محیط (برای مثال دما) و سطوح کیفیت (یعنی غربال‌گری)،
- داده‌های سازنده.

ث-۶ کاربرد و روابط متقابل

تخمین قابلیت اطمینان می‌تواند به‌عنوان درون داد یا برون داد با دیگر تحلیل‌های قابلیت اتـکا مانند موارد زیر ارتباط داشته باشد:

- FMEA، FMECA و تحلیل درخت عیب: تخمین قابلیت اطمینان یک درون داد است (فراهم کردن نرخ‌های خرابی برای موارد اختصاصی) در حالی‌که FMEA، FMECA و تحلیل درخت عیب درون دادهایی را برای تخمین قابلیت اطمینان نیز فراهم می‌کنند،
- تحلیل تنش قطعه درون دادهایی را برای محاسبهٔ نرخ خرابی فراهم می‌کند،
- درون دادهایی برای تحلیل قابلیت دسترسی،
- فهرست اقلام بحرانی قابلیت اطمینان بر اساس برون دادهای تخمین قابلیت اطمینان است.

ث-۷ محتوا

الف- لازم است سند تخمین قابلیت اطمینان شامل موارد زیر باشد:

- شناسایی واضح از طراحی‌هایی که تحلیل می‌شوند،
- نمودار بلوکی قابلیت اطمینان،
- روش مورد استفاده به همراه «منطق و توضیح اصول[2]» آن،
- تحلیل نتایج،
- توصیه‌هایی برای تصمیم‌گیری پروژه.

1- Accelerated tests

2- Rationales

پیوست ج

(الزامی)

شناسایی، آشکارسازی و بازیابی خرابی FDIR- DRD

ج-۱ مقدمه

هدف اصلی از FDIR، حفاظت از یکپارچگی مأموریت می‌باشد. یعنی برای جلوگیری از، از دست دادن کل یا جزئی از مأموریت در جایی که استمرار مأموریت بتواند توسط اقدامات پیشگیری مناسب محافظت شود.

-۲ دامنه کاربرد و قابلیت اجرا

این تعریف الزامات سند (DRD) الزامات محتوی داده‌ها را برای FDIR به وجود می‌آورد.

ج-۳ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا.

ج-۴ اصطلاحات،تعاریف و اختصارات

لازم است اصطلاحات و تعاریف مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ استاندارد ECSS-Q-ST-30 باشد.

ج-۵ شرح و هدف

اهداف تحلیل FDIR عبارتند از:

- نشان دادن تطابق با الزامات تحمل خرابی پروژه؛
- فراهم کردن فهرست اقدامات و توصیه‌ها برای تصمیم‌گیری پروژه.

ج-۶ کاربرد و روابط متقابل

FDIR با دیگر تحلیل‌های قابلیت اتـکا از قبیل موارد زیر ارتباط دارد:

- FMEA/FMECA؛
- تحلیل برهم‌کنش سخت‌افزار و نرم‌افزار؛
- تحلیل قابلیت دسترسی.

ج-۷ محتوا

الف. سند تحلیل FDIR باید شامل موارد زیر باشد:

- توصیف سیستم؛
- توصیف روشی برای اجرای FDIR (برای مثال نتیجه‌گیری از FMEA/FMECA، بازنگری FDIR)؛
- جزئیات خرابی مورد نظر؛
- نشانه‌های خرابی (برای مثال دورسنجی (TM)[1]، قابل مشاهده بودن از راه دور)؛

1- Telemetry

- جزئیات اثر خرابی بر سیستم؛
- اقدامات بازیابی (برای مثال فرمان از راه دور (TC)[1]، مکانیزم‌های روی برد خودکار[2])؛
- اقدامات و توصیه‌ها برای تیم پروژه.

1- Telecommand

2- Automatic on board mechanism

پیوست چ

(الزامی)

تحلیل ناحیه‌ای – DRD

چ-۱ مقدمه

هدف تحلیل ناحیه‌ای، ارزشیابی پیامدهای ناشی از برهم‌کنش ذاتی بالقوهٔ یک زیرسیستم با زیرسیستم دیگری است که در یک سیستم نصب می شود.

چ-۲ دامنه کاربرد و قابلیت اجرا

این DRD الزامات محتوی داده‌ها را برای تحلیل ناحیه‌ای به وجود می‌آورد.

چ-۳ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا.

چ-۴ اصطلاحات،تعاریف و اختصارات

لازم است اصطلاحات و تعاریف مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ استاندارد ECSS-Q-ST-30 باشد.

چ-۵ شرح و هدف

اهداف تحلیل ناحیه‌ای عبارتند از:

- شناسایی بر هم‌کنش‌های ممکن بین زیرسیستم‌ها؛
- فراهم نمودن ارزیابی از این بر هم‌کنش‌های بالقوه؛
- ارائهٔ توصیه‌ها برای کاهش دادن برهم کنش‌ها.

چ-۶ کاربرد و روابط متقابل

تجزیه و تحلیل ناحیه‌ای با دیگر تحلیل‌های قابلیت اتـکا از قبیل موارد زیر ارتباط دارد:

- FMEA/FMECA؛
- علت مشترک.

چ-۷ محتوا

الف- لازم است سند تحلیل ناحیه‌ای شامل موارد زیر باشد:

- شناسایی محیط (محدوده) پیرامون[1] تحت رسیدگی[2]؛
- تعریف تفصیلی (دقیق) فصل مشترک‌ها؛
- توصیف برهم‌کنش‌های بالقوه؛
- فهرست اقدامات و توصیه‌ها برای تصمیم‌گیری پروژه.

1- Perimeter
2- Investigation

پیوست ح

(الزامی)

تحلیل قابلیت نگهداری – DRD

ح-۱ مقدمه

هدف از تحلیل قابلیت نگهداری، نشان دادن تطابق یا شناسایی عدم تطابق با الزامات قابلیت نگه‌داری است. تحلیل قابلیت نگه‌داری مقدماتی، اشاره بر نتایج سهم قابلیت نگه‌داری به‌کار رفته در تحلیل دارد.

ح-۲ دامنه کاربرد و قابلیت اجرا

این DRD الزامات محتوی داده‌ها را برای تحلیل قابلیت نگه‌داری به وجود می‌آورد.

ح-۳ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا.

ح-۴ اصطلاحات،تعاریف و اختصارات

لازم است اصطلاحات و تعاریف مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ استاندارد ECSS-Q-ST-30 باشد.

ح-۵ شرح و هدف

اهداف تحلیل قابلیت نگه‌داری عبارتند از:

- تعیین امکان‌پذیری وظایف اصلاحی و پیشگیرانهٔ قابلیت نگهداری؛
- فراهم آوردن زمان متوسط بین دو خرابی متوالی (MTBF) و زمان متوسط تعمیر (MTTR) برای تحلیل دسترس‌پذیری؛
- ارائهٔ توصیه‌ها به‌منظور بهسازی.

ح-۶ کاربرد و روابط متقابل

تحلیل قابلیت نگه‌داری با دیگر تحلیل‌های قابلیت اتـکا از قبیل موارد زیر ارتباط دارد:

- تحلیل قابلیت اطمینان؛
- تحلیل قابلیت دسترسی؛
- درخت عیب؛
- FDIR؛
- FMEA/FMECA.

ح-۷ محتوا

الف. لازم است سند تحلیل قابلیت نگه‌داری حداقل شامل موارد زیر باشد:

- سطوح نگهداری: برای اقدامات پیشگیرانه و اصلاحی؛
- شناسایی خط مشی FDIR؛

- توصیف مدل ریاضی؛
- شاخص‌های نگه‌داری (یعنی MTTR، زمان تعمیر و نگه‌داری در سال، تکرار نگهداری)؛
- توصیه‌های برای قطعات یدکی (برای مثال تعداد قطعات یدکی، وزن و ظرفیت انتقال قطعات یدکی)؛
- شناسایی اقلام بحرانی قابلیت نگهداری.

پیوست خ

(الزامی)

تحلیل علت مشترک – DRD

خ-۱ مقدمه

هدف از تحلیل علت مشترک مشخص کردن علت ریشه‌ای خرابی‌هایی است که به طور بالقوه می‌توانند سطوح تحمل خرابی را بی‌اثر کنند.

خ-۲ دامنه کاربرد و قابلیت اجرا

این DRD، الزامات محتوی داده‌ها را برای تحلیل علت مشترک تعیین می کند.

خ-۳ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا.

خ-۴ اصطلاحات،تعاریف و اختصارات

لازم است اصطلاحات و تعاریف مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ استاندارد ECSS-Q-ST-30 باشد.

خ-۵ شرح و هدف

هدف از تحلیل علت مشترک، شناسایی و تحلیل اثرات پارامترهای مشترک مانند (تابش[1]، درجه حرارت، موقعیت فیزیکی، ارتعاشات) بر روی طراحی خاص تحت رسیدگی است.

خ-۶ کاربرد و روابط متقابل

تحلیل علت مشترک با دیگر تحلیل‌های قابلیت اتـکا از قبیل موارد زیر ارتباط دارد:

- تحلیل درخت عیب؛
- تحلیل قابلیت دسترسی؛
- تحلیل ایمنی؛
- FMEA/FMECA.

خ-۷ محتوا

الف- لازم است سند تحلیل علت مشترک شامل موارد زیر باشد:

- توصیف محیط (محدوده) پیرامونِ طراحی که تحلیل شده است؛
- فهرست پارامترهای علت مشترک و اثرات آن‌ها؛
- اقدامات و توصیه‌ها برای تیم پروژه،

یادآوری- به نمونه پارامترهای چک لیست در پیوست ر مراجعه کنید.

1- Radiation

پیوست د

(الزامی)

تحلیل بدترین حالت WCA- DRD

د-۱ مقدمه

هدف از تحلیل بدترین حالت، نشان دادن این است که مواردی که تحلیل می‌شوند علی‌رغم تغییرات پارامترهای اجزای تشکیل دهندهٔ آن‌ها و شرایط تحمیلی محیطی، در محدودهٔ کاری خود عمل می‌کنند.

د-۲ دامنه کاربرد و قابلیت اجرا

این DRD الزامات محتوی داده‌ها را برای تحلیل بدترین حالت ایجاد می‌کند.

د-۳ مراجع

د-۳-۱ مراجع الزامی

استاندارد ECSS-Q-ST-30: تضمین محصول فضایی- قابلیت اتـکا.

د-۳-۲ دست‌نامه‌های مرجع

دست‌نامه ECSS-Q-HB-30-01: تحلیل بدترین حالت.

د-۴ اصطلاحات،تعاریف و اختصارات

لازم است اصطلاحات و تعاریف مطابق با استاندارد ECSS-S-ST-00-01 و بند ۳ استاندارد ECSS-Q-ST-30 باشد.

د-۵ شرح و هدف

گزارش WCA، اجرای آزمون و نتایج تحلیل را توصیف می‌کند.

تحلیل بدترین حالت شامل روش‌های تحلیل و مفروضات مورد استفاده است و همچنین مدل را توصیف می‌کند و نتایج تحلیل را نیز ارائه می‌دهد.

کاربرد اصلی آن، اثبات این است که که تجهیزات قادر به برآورده نمودن الزامات عملکردی خاص تحت بدترین شرایطِ بهره برداری است و اثبات می‌کند[1] که حاشیه‌های بهره برداری برای تمام شرایط بهره‌برداری کفایت می‌کند.

د-۶ کاربرد و روابط متقابل

تحلیل بدترین حالت با دیگر تحلیل‌ها از قبیل موارد زیر ارتباط دارد:

- تحلیل تابش؛
- تحلیل حرارتی.

1- Demonstration

د-۷ محتوا

الف- لازم است سند تحلیل بدترین حالت شامل موارد زیر باشد:

- مفروضات قابل اجرا برای شرایط محیطی؛
- فهرست پایگاه داده‌ای اجزای انتخاب شده با پارامترهای بدترین حالت؛
- توصیف روش کلی؛
- تشریح روش فنی تحلیل عددی؛
- دستاوردها و نتیجه‌گیری از تحلیل بدترین حالت.

پیوست ذ

(اطلاعاتی)

ماتریس تحلیل‌های اجرایی

دامنهٔ کاربرد جدول ذ-۱، نشان دادن ارتباط اسناد مرتبط با فعالیت‌های قابلیت اتـکا برای پشتیبانی از اهداف بازنگری پروژه همان‌طور که در استاندارد ECSS-M-ST-10 تعیین شده است، می‌باشد.

یادآوری- این جدول شامل اولین نشانه محتوای بستهٔ داده‌ها[1] در بازنگری‌های مختلف است. محتوای کامل بستهٔ داده‌ها به‌عنوان قسمتی از پیمان تجاری می‌باشد که در آن تحویل اسناد بین بازنگری‌ها را تعریف می‌کند.

این جدول، اسنادی که برای بازنگری پروژه لازم است را فهرست کرده است (با "X" مشخص شده است). علامت‌های ضربدر مختلف در ردیف‌ها نشان دهندهٔ سطح افزایشی بلوغ مورد انتظار به طور پیش‌رونده در طی بازنگری است. آخرین علامت در ردیف دلالت بر این دارد که در آن بازبینی انتظار می‌رود که سند کامل و نهایی شده باشد.

یادآوری- تمام اسناد، حتی هنگامی که در جدول ذ-۱ به‌عنوان مورد قابل تحویل نشانه گذاری نشده‌اند، باید تحت مدیریت پیکربندی همچنان که در استاندارد ECSS-M-ST-40 است، در دسترس و برقرار باشند (برای مثال در موارد تغییرات برای رهگیری از انتها به ابتدا).

اسنادی که در جدول ذ-۱ می‌باشند از DRDهای همین استاندارد می‌باشند یا از بقیهٔ استانداردهای ECSS-Q-ST-XX، یا در مراجع DRDها تعریف می‌شوند.

1- Data package

جدول ذ-۱ - ماتریس تحلیل‌های اجرایی- DRD

عنوان DRD یا سند	مرحله												سطح قابل اجرا	توجه
	A	B		C	D		E					F		
	PRR	SRR	PDR	CDR	QR	AR	ORR	FRR	LRR	CRR	ELR	MCR		
تحلیل حالات خرابی و اثرات آن / تحلیل حالات خرابی، اثرات و شدت بحرانی بودن آن‌ها FMEA/FMECA	×	×	×	×	×	×							SS, SE, LL	استاندارد ECSS-Q-ST-30-02 معمولاً FMEA برای تمام پروژه‌ها درخواست می‌شود. معمولاً FMECA برای ارتباطات از راه دور، مشاهدات زمینی و فضاپیماهای علمی و بخش‌های زمینی انجام نمی‌شود. فرایند FMECA معمولاً لازم نمی‌شود.
تحلیل برهم‌کنش سخت‌افزار- نرم‌افزار (HSIA)				×	×	×							SS, SE	استاندارد ECSS-Q-ST-30-02 می‌تواند در FMECA گنجانده شود. بر روی درخواست پروژهٔ خاص انجام می‌شود.
تحلیل پیشامدهای احتمالی				×	×	×							SS, GS, SE	پیوست ت می‌تواند به‌عنوان قسمتی از نظام‌نامه عملیات با استفاده از درون دادها از FMECA و FDIR گنجانده شود.
تحلیل درخت عیب	×	×	×	×	×	×							کلیهٔ سطوح	استاندارد ECSS-Q-ST-40-12 بر روی درخواست پروژهٔ خاص انجام می‌شود.
تحلیل علت مشترک				×	×	×							SS, SE	پیوست خ می‌تواند به‌عنوان قسمتی از FMECA/FTA انجام شود.
پیش‌بینی قابلیت اطمینان	×	×	×	×	×	×							کلیهٔ سطوح	پیوست ث همچنین استاندارد ECSS-Q-HB-30-08 را مشاهده نمایید.

جدول ذ-۱ - ادامه

عنوان DRD یا سند	مرحله												سطح قابل اجرا	توجه
	A	B		C	D		E					F		
	PRR	SRR	PDR	CDR	QR	AR	ORR	FRR	LRR	CRR	ELR	MCR		
تحلیل بدترین حالت (WCA)				×	×	×							LL تجهیزات الکتریکی	پیوست د همچنین استاندارد ECSS-Q-HB-30-01 را مشاهده نمایید.
تحلیل تنش قطعه				×	×	×							LL تجهیزات الکتریکی	ECSS-Q-ST-30-11
تحلیل ناحیه‌ای		×	×	×	×	×							SS, GS	پیوست چ بر روی درخواست پروژهٔ خاص انجام می‌شود (معمولاً بر روی پرتابگرها لازم است).
تحلیل آشکارسازی، جداسازی و بازیابی خرابی (FDIR)		×	×	×	×	×							SS, GS	پیوست ج
تحلیل‌های قابلیت نگهداری		×	×	×	×	×							GS	پیوست ح فقط در حین فعالیت‌های نگه‌داری لازم می‌شود.
تحلیل قابلیت دسترسی		×	×	×	×	×							کلیهٔ سطوح (درون دادهای از کارافتادگی‌ها، فقط از LL)	استاندارد ECSS-Q-ST-30-09

پیوست ر

(اطلاعاتی)

چک لیست‌های علت مشترک

جدول ر-۱ - چک لیست‌های علت مشترک

اقلام	چک لیست طراحی علت مشترک
۱	اقلام اصلی و افزونه[1]، منابع توان مستقل دارند.
۲	عایق حرارتی بین منابع توان بیشینه است.
۳	گذرگاه‌های داده‌های مستقل.
۴	مدارهای گذرگاه مسیر واسط (I/F)[2] طراحی شده برای اطمینان از اینکه عیوب مانع گذرگاه نشوند.
۵	اتصال دهنده‌های مجزا به طور ایده‌آل کارکردهای اصلی و مازاد را ارائه می‌دهند (یعنی توان، داده‌ها و غیره).
۵-۱	اگر بعضی اوقات بخش ۵ امکان‌پذیر نباشد، دستیابی به ملاحظات فضایی می‌تواند دشوار شود، سیم‌های مربوط به کارکردهای اصلی و افزونه درون اتصال دهنده‌ها (توصیه می‌شود) به‌وسیلهٔ گیره‌های استفاده نشده جدا شوند.
۶	در صورت امکان کارکردهای اصلی و افزونه در جعبه‌ها و جایگاه‌های مجزا قرار دارند.
۶-۱	هنگامی که بند شش امکان نداشته باشد، آیا عایق بین نواحی/اجزای اصلی و افزونه به‌کار رفته برای کاهش احتمال انتشار خرابی مثل اثرات حرارتی، اثرات ظرفیتی و غیره بر روی هر دو کارکردهای اصلی و افزونه اثر می‌گذارد.
۷	در تجهیزات با افزونگی داخلی، مدارهای اصلی و افزونگی[3]، از مدارهای مجتمع (IC)[4] جداگانه استفاده می‌کنند و استفادهٔ حداقل از مدارهای چاپی مشترک/سهم‌بندی شده وجود دارد.
	در جایی که بند ۷ امکان‌پذیر نباشد، بنابراین:
۷-۱	آیا عایقی که بین نواحی/اجزای اصلی و افزونه گذاشته شده برای کاهش احتمال انتشار خرابی مثل اثرات حرارتی، انتشار اثرات سرگردان ظرفیتی، بر روی هر دو کارکردهای اصلی و افزونه اثر می‌گذارد.
۷-۲	آیا جداسازی بین المان‌ها با اتلاف بالا و المان‌های حساس به گرما در نظر گرفته شده است؟
۷-۳	آیا جایگزینی میان‌راه[5] از طریق صفحه‌های مدار اسمی و افزونه در برد مدار چند لایه‌ای برای حذف اثرات علت مشترک در نظر گرفته شده است؟
۷-۴	اقلام ۵ یا ۵-۱ برآورده می‌شود.
۷-۵	آیا طراحی چیدمان سیم‌کشی برای مفصل‌های لحیم شده و مسیر هدایت PCB برای حذف اثرات علت مشترک در نظر گرفته شده است (تفکیک کافی مفصل‌های لحیم شده، سیم‌ها و مسیرها).
۷-۶	آیا اجزای اختصاصی با چند کاربرد، تنها با یک مسیر اسمی یا افزونگی[6] استفاده شده است؟

[1] Redundant
[2] Interface
[3] Redundancy
[4] Integrated Circuit
[5] Vias
[6] Redundant path

جدول ر-۱ - ادامه

۸	کارکردهای کنترلی و نظارتی، از مدارهای مجتمع مجزا (به عنوان مثال، مدارهای مجتمع (IC)هایی که ویژگی کارکردهای چهارگانه[1] دارند)، استفاده می‌کنند. (یک حالت خرابی با مود مشترک بالقوه).
۹	کارکردهای محافظتی و حفاظت شده، از مدارهای مجتمع مجزا (به عنوان مثال، مدارهای مجتمع (IC)هایی که ویژگی کارکردهای چهارگانه دارند)، استفاده می‌کنند. (یک حالت خرابی با مود مشترک بالقوه).
۱۰	پین‌ها/ اتصالات با سیم‌های مشترک/ چندگانه، سبب اثرات علت مشترک نمی‌گردند.
۱۱	ابعاد تمام منافذ هوا مناسب است.
۱۲	هیچ اتصالی بین فلزات با پتانسیل الکتروشیمیایی کمتر از ۰/۵ v(ولت) وجود ندارد (ناخالصی فلزی باعث خرابی‌های اتصال کوتاه/اتصال باز نیست).
۱۳	خطاهای نرم‌افزاری[2] باعث اثرات علت مشترک نمی‌گردد.
۱۴	تدارک قطعات EEE (کیفیت قطعات، هشدارهای خرابی، اجزای مشترک با نقص شناخته شده و غیره) لحاظ شده است.
۱۵	تمام پایه‌ها و حفاظ بین مسیرهای اصلی و مازاد مناسب است. تمام زمین کردن[3] و حفاظ گذاری[4] بین مسیرهای اصلی و مازاد مناسب است.
۱۶	پین، ابعاد سیم و مسیرهای برد مدار چاپی (PCB)[5] با حفاظت‌های جریان بیش از اندازه سازگار است.
۱۷	الزامات سطح تجهیزات، نادرست[6]، متناقض[7] یا مغایر[8] نیست.
۱۸	انتخاب مواد اثرات علت مشترک را مطرح نمی‌کند (تنزل سطح، سست شدن، شکست و ...)

[1] Quadruple functionality
[2] Software errors
[3] Grounding
[4] Shielding
[5] Printed Circuit Board
[6] Erroneous
[7] Inconsistent
[8] Contradictory

جدول ر-۲ - چک لیست محیطی علت مشترک

اقلام	چک لیست محیطی علت مشترک
۱	کل میزان تابش خورشید (ذرات پروتون، آلفا و بتا، EM) به سر حد تحمل اجزای سازنده نمی‌رسد.
۲	تابش یون‌های سنگین باعث رخداد معکوس شدن وضعیت بیت (Bit-flip) در سیگنال‌های دیجیتالی نمی‌شوند. پوشش کافی فراهم شده است.
۳	تشعشع یون‌های سنگین باعث رخدادهای تکی سوختن (SEB)[1] از اتصالات MOSFET توان نمی‌شوند. پوشش کافی فراهم شده است.
۴	رله‌ها[2] (یا دیگر اجزای حساس) به خاطر ارتعاش تغییر وضعیت نمی‌دهند (مخصوصاً حین پرتاب، که شدیدترین مورد عملیات است) مکان اجزا به‌گونه‌ای در نظر گرفته شده است که این اثر را کمینه کرده است.
۵	برهم‌کنش میدان مغناطیسی، برای مثال از مبدل‌های توان یا موتورها، باعث اثرات علت مشترک نمی‌شوند.
۶	برخورد و نفوذ ریز شهاب‌سنگ‌ها باعث خسارت نمی‌گردد.
۷	آلودگی ناشی از اجسام خارجی/پسماندها
۸	خرابی کنترل حرارتی بر تجهیزات اصلی و مازاد تأثیر نمی‌گذارد.

[1] Single Event Burn-out
[2] Relays

جدول ر-۳ - چک لیست عملیات غیرمنتظره علت مشترک

اقلام	چک لیست عملیات غیر منتظره علت مشترک
۱	هیچ فرمان نادرست از بخش کنترل زمینی (GSC)[1] به محموله فرستاده نمی‌شود.
۲	فرمان از راه دور (TC)[2] نادرستی همراه محموله فرستاده شود.
۳	تابش یون‌های سنگین باعث سوختن (SEB) اتصالات MOSFET توان نمی‌شوند.
۴	رله‌ها (یا دیگر اجزاء حساس) به خاطر ارتعاش تغییر وضعیت نمی‌دهند (مخصوصاً حین پرتاب، که شدیدترین مورد عملیات است) مکان اجزاء به‌گونه‌ای در نظر گرفته شده است که این اثر را کمینه کرده است.
۵	بر هم کنش میدان مغناطیسی، برای مثال از مبدل‌های توان یا موتورها، باعث اثرات علت مشترک نمی‌شوند.
۶	برخورد و نفوذ پسماندهای فضایی یا ریز شهاب‌سنگ‌ها باعث خسارت نمی‌گردد.

[1] Ground segment control
[2] Tele-Command

کتاب‌نامه

[1] ECSS-S-ST-00, ECSS system – Description, implementation and general requirements

[2] ECSS-Q-ST-30-09, Space product assurance — Availability analysis

[3] ECSS-Q-ST-40, Space product assurance – Safety

[4] ECSS-Q-ST-40-12, Space product assurance — Fault tree analysis - Adoption notice ECSS/IEC 61025

[5] ECSS-Q-ST-80, Space product assurance — Software product assurance

[6] ECSS-Q-HB-30-01, Space product assurance — Worst case analysis

[7] ECSS-Q-HB-30-08, Space product assurance — Component reliability data sources and their use

[8] ECSS-Q-HB-80-03, Space product assurance - Software dependability and safety methods and techniques

[9] ECSS-Q-TM-30-12, Space product assurance — End of life parameter drifts

[10] ECSS-E-ST-70-11, Space engineering — Space segment operability

[11] ECSS-M-ST-10, Space project management – Project planning and implementation

[12] ECSS-M-ST-40, Space project management – Configuration and information management

[13] ECSS-M-ST-80, Space project management – Risk management