مهندسی نرم افزار ۱

فصل های ۹ و ۱۰

تمام فصل ها : ۱۴

تهیّه و تنظیم :

WWW.SabzElco.IR

مطالب این مجموعه براساس مطالبی از آقای پورامینی (مولف : سامرویل) نوشته شده است.

فصل ۹

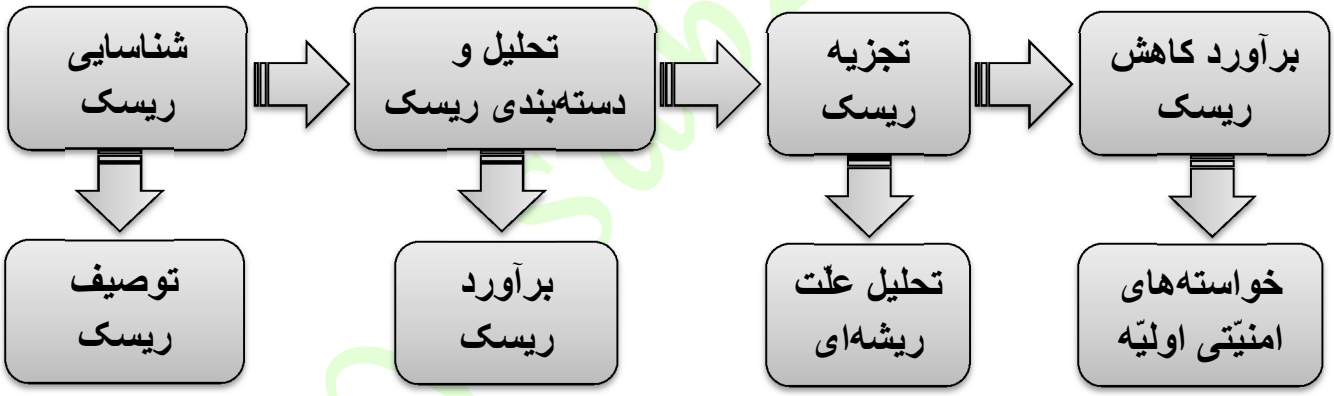
مشخّصات سیستم های حیاتی

تعیین مشخّصات مبتنی بر ریسک :

هدف تعیین مشخّصات سیستم‌های حیاتی ،درک ریسک‌هایی است که سیستم با آن‌ها روبه‌رو است و تولید خواسته‌های قابلیّت اتکا برای مقابله با آن ریسک‌ها است و شامل مراحل زیر است :

۱- شناسایی ریسک
۲- تحلیل و دسته بندی ریسک
۳- تجزیه ریسک
۴- برآورد کاهش ریسک

تعیین مشخّصات مبتنی بر ریسک



برای سیستم‌های بزرگ ،تحلیل ریسک در چند مرحله انجام می‌شود :

۱- تحلیل اولیّه ریسک ،که در آن ریسک‌های مهم ،شناسایی می‌شوند.
۲- تحلیل مشروح‌تری از ریسک سیستم و زیر سیستم.
۳- تحلیل ریسک نرم افزار ،که در آن ریسک‌های خطر نرم افزار ،در نظر گرفته می‌شوند.
۴- تحلیل ریسک عملیاتی ،که به واسط کاربر مربوط می‌شود و ریسک‌هایی که از خطاهای اپراتور ناشی می‌شوند.

شناسایی ریسک :

شناسایی ریسک‌هایی است که سیستم حیاتی باید با آنها مقابله کند.

در سیستم‌های امنیّتی - حیاتی ،ریسک‌های اصلی ،خطراتی هستند که منجر به حادثه می‌شوند.

تحلیل و دسته بندی ریسک‌ها :

با درک احتمال وقوع ریسک و اثرات بالقوّه آن ،در اثر سوانح حاصل از آن ،سر و کار دارد.

ریسک‌ها می توانند به سه طریق دسته بندی شوند :

۱- غیر قابل تحمّل
۲- حداقل بودن اثر ریسک
۳- قابل قبول

تجزیه ریسک :

فرایند کشف علل ریشه‌ای ریسک‌ها ،در یک سیستم خاص است.

درخت عیب :

تحلیل درخت عیب ،شامل شناسایی رویداد نامطلوب و کارکردن عقبگرد از آن رویداد برای یافتن آسان می‌باشد.

برآورد کاهش ریسک :

وقتی ریسک‌های بالقوّه وعلل ریشه‌ای آن‌ها شناسایی شدند ،باید خواسته‌های قابلیّت اعتماد سیستم را بیابید که ریسک‌ها را مدیریت کند وتضمین نماید که سانحه رخ نمی‌دهد.

سه راهبرد برای این کار وجود دارد :

۱- اجتناب از ریسک
۲- تشخیص و حذف ریسک
۳- محدود سازی خسارات

مشخّصات امنیّتی :

در این مدل ،سیستم کنترلی ،تجهیزاتی را کنترل می‌کند که خواسته‌های امنیّتی سطح بالایی دارند. این خواسته‌های سطح بالا ،دو نوع خواسته‌های امنیّتی مشروح‌تر را تولید می‌کند که برای سیستم حفاظت تجهیزات اعمال می‌شود :

۱- خواسته‌های امنیّتی عملکردی
۲- خواسته‌های جامعیّت امنیّتی

مشخّصات حفاظتی :

مشخّصات خواسته‌های حفاظتی برای سیستم‌ها تا حدودی شبیه خواسته‌های امنیّتی است. آن‌ها مشخّصاتی هستند که نمی‌توان به‌صورت کمی بیان کرد.

خواسته‌های حفاظتی معمولاً خواسته‌های "نبایدها" هستند که رفتارهای غیر قابل قبول سیستم را مشخّص می‌کنند.

مراحل این فرایند عبارت‌اند از :

۱- شناسایی و ارزیابی دارایی
۲- تحلیل تهدید و برآورد ریسک
۳- انتساب تهدید
۴- تحلیل فن‌آوری
۵- تعیین مشخّصات حفاظت

خواسته‌های حفاظتی که "فایر اسمیت" شناسایی کرد :

۱- خواسته‌های شناسایی
۲- خواسته‌های تأیید
۳- خواسته‌های اعطای مجوز
۴- خواسته‌های مصونیت
۵- خواسته‌های جامعیّت
۶- خواسته‌های تشخیص تجاوز
۷- خواسته‌های عدم تکذیب
۸- خواسته‌های محرمانگی
۹- خواسته‌های حسابداری حفاظتی
۱۰- خواسته‌های حفاظتی نگهداری سیستم

مشخّصات قابلیّت اعتماد نرم افزار :

هنگام تعیین قابلیّت اعتماد سیستم ،باید سه بعد را در نظر گرفت :

۱- قابلیّت اعتماد سخت افزار
۲- قابلیّت اعتماد نرم افزار
۳- قابلیّت اعتماد اپراتور

معیارهای قابلیّت اعتماد :

انتخاب معیار به نوع سیستم و خواسته‌های دامنه کاربرد بستگی دارد.

نمونه‌هایی از انواع سیستم‌هایی که این معیارها می توانند در آنها به‌کار روند عبارت‌اند از :

۱- احتمال خرابی در تقاضا
۲- نرخ وقوع خرابی
۳- میانگین زمان شکست
۴- قابلیّت دسترسی

در برآورد قابلیّت اعتماد سیستم ،از سه نوع اندازه گیری می‌توان استفاده کرد :

۱- تعداد خرابی‌های سیستم با توجه به تعداد درخواست‌های سرویس از سیستم
۲- زمان (یا تعداد تراکنش‌های) بین خرابی‌های سیستم
۳- زمان مصرفی برای ترمیم یا راه اندازی مجدد سیستم

خواسته‌های قابلیّت اعتماد غیر عملکردی :

مراحل تعیین مشخّصات قابلیّت اعتماد :

۱- برای هر زیر سیستم ،انواع خرابی‌های سیستم را شناسایی کنید و نتایج این خرابی‌ها را تحلیل نمایید.
۲- از تحلیل خرابی سیستم ،خرابی‌ها به دسته‌های مناسبی افراز کنید.
۳- برای هر دسته از خرابی ،با استفاده از معیار قابلیّت اعتماد مناسب ،خواسته قابلیّت اعتماد را تعریف کنید.
۴- در صورت لزوم ،خواسته‌های قابلیّت اعتماد عملکردی را شناسایی کنید.

دسته بندی خرابی‌ها :

۱- موقّت
۲- دائمی
۳- قابل ترمیم
۴- غیر قابل ترمیم
۵- بدون تخریب
۶- مخرّب

دو نوع خرابی را می‌توان شناسایی کرد :

۱- **خرابی‌های موقتی :** خرابی‌هایی هستند که کاربر می‌تواند آن‌ها را ترمیم کند.
۲- **خرابی‌های دائمی :** خرابی‌هایی هستند که توسط کارخانه سازنده ترمیم می‌شوند.

فصل ۱۰

مشخّصات رسمی

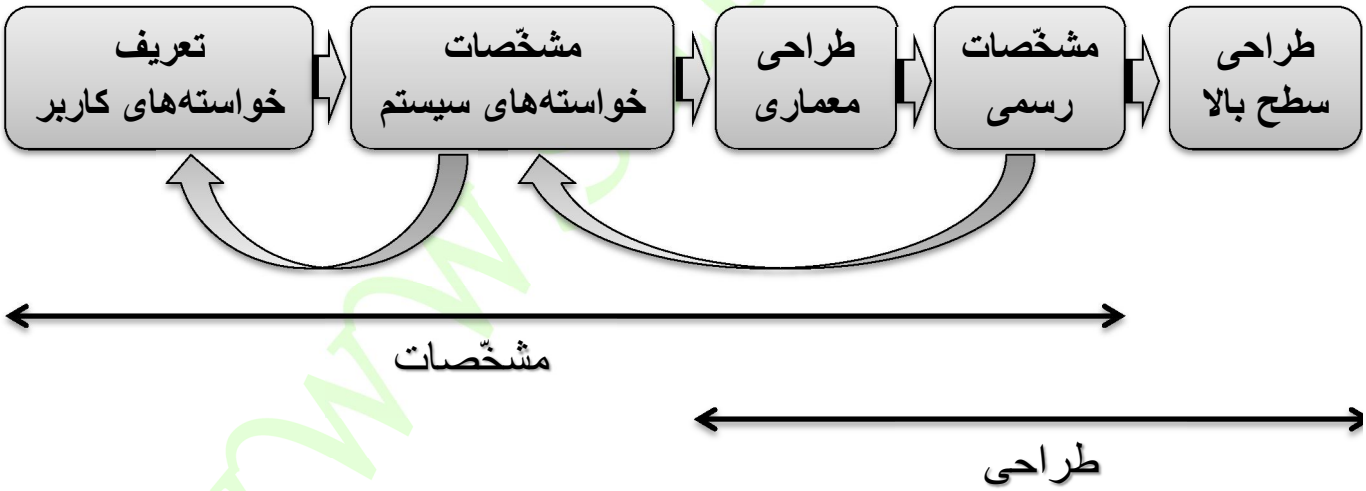
مشخّصات رسمی در فرایند نرم افزار :

ایجاد مشخّصات رسمی منجر به تحلیل‌های مشروحی از سیستم‌ها می‌شود که خطا ها و ناسازگاری‌های موجود در مشخّصات خواسته‌ها را آشکار می‌کند.

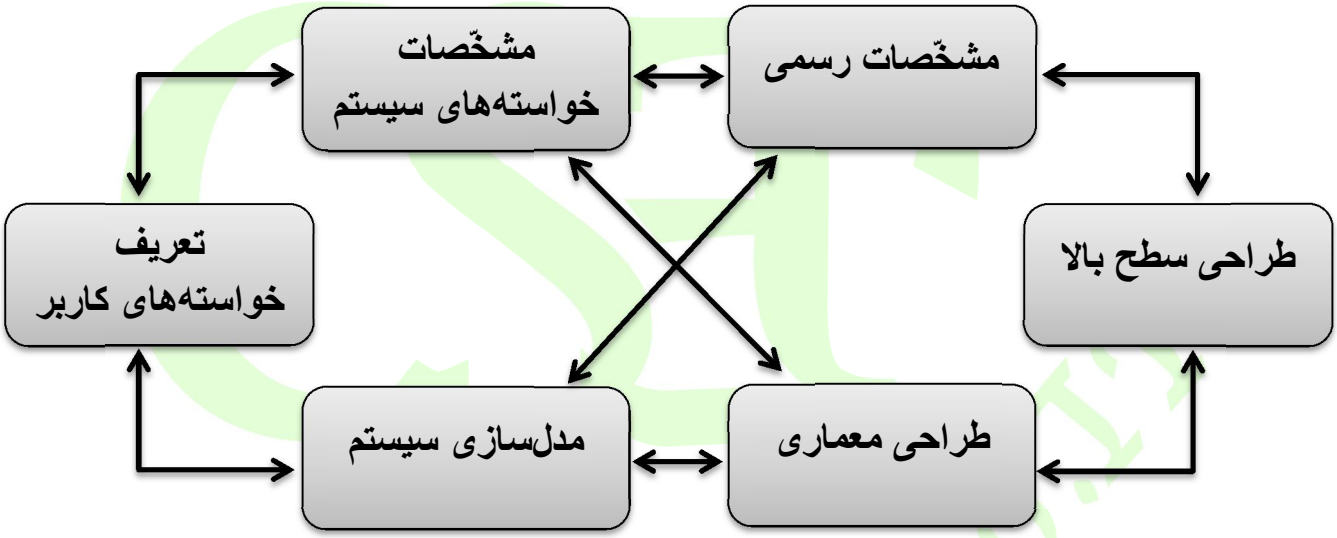
دو روش برای تعیین مشخّصات رسمی وجود دارد :

۱- روش جبری
۲- روش مبتنی بر مدل

مشخّصات و طراحی



مشخّصات رسمی در فرایند نرم افزار



تعیین مشخّصات واسط زیر سیستم :

واسطهای زیر سیستم‌ها معمولاً به صورت مجموعه‌ای از انواع داده انتزاعی یا اشیا تعریف می‌شوند. این‌ها ،داده‌ها و عملیاتی را توصیف می‌کنند که از طریق واسط زیر سیستم قابل دستیابی است.

فرایند توسعه مشخّصات رسمی واسط زیر سیستم ،باید شامل فعّالیت‌های زیر باشد :

۱- سازماندهی مشخّصات
۲- نامگذاری مشخّصات
۳- انتخاب عملیات
۴- مشخّصات عملیات غیر رسمی
۵- تعریف نحو
۶- تعریف اصل موضوع

عملیات‌های روی نوع داده انتزاعی دو دسته‌اند :

۱- **عملیات سازنده :** نهادهایی از گونه تعریف شده ،مشخّصات را ایجاد و اصلاح می‌کنند.
۲- **عملیات بررسی :** صفات گونه تعریف شده ،مشخّصات را بازیابی می‌کنند.

مشخّصات رفتاری :

تکنیک‌های مبتنی بر مدل ،سیستم را با استفاده از ساختارهای ریاضی مثل مجموعه‌ها و توابع ، مدل‌سازی می‌کنند. این تکنیک‌ها حالت سیستم را نشان می‌دهند و در نتیجه ،تعیین مشخّصات رفتاری آسان‌تر می‌گردد.

عملیات موجود در مشخّصات مبتنی بر مدل ،با تعریف پیش شرطها و پس شرطها روی حالت سیستم مشخص می‌شوند.

اسامی تعریف شده در این طرح :

۱- ورودی‌های سیستم
۲- خروجی‌های سیستم
۳- متغیرهای حالت برای انجام محاسبات