انواع نيازمندي هاي نرم افزار را نام ببريد ؟

1-نیاز مندی های وظیفه مندی )Requirements Functional) :وظايفي كه سيستم بايد انجام بدهد را توصيف مينمايد .

2-نیاز مندی های غیروظیفه مندی: (Requirements Functional-Non ) خصوصیات کیفی نرم افزار که نحوه انجام وظایف سیستم را توصیف می‌نماید .

چه وقت نیاز های غیروظیفه مندی به نرم افزار افزوده می شوند؟

یک روش قدیمی

ابتدا نرم افزاری می سازیم که نیازهای وظیفه مندی را برآورده سازد و سپس خصوصیات غیر وظیفه مندی را به آن اضافه یا کم می کنیم. θ از دست دادن منابع و زمان θ کیفیت پائین نرم افزار بخاطر عدم تاثیر این دو نیازمندی بریکدیگر

روش جدید

در توسعه سیستم های نرم افزاری این دو را همزمان باید پیش برد.

نسبت وظیفه مندی و خصوصیات کیفی چگونه است ؟

وظیفه مندی و خصوصیات کیفی متعامدند، یعنی در رابطه تنگاتنگ با یکدیگر هستند .

**آیا هر سطح از وظیفه مندی قابل دستیابی با هر سطح از خصوصیات کیفی است ؟**

اما هر سطح از وظیفه مندی )عملکرد( قابل دستیابی با هر سطح از خصوصیات کیفی نیست

مثالً، مرتب کردن )sort )بانک های اطالعاتی حجیم ممکن است با کارآیی باال انجام نشود )از این رو: معمار، یک سطح مناسبی از کیفیت را برای هر خصوصیت بر می گزیند(

**دلایل طراحی مجدد سیستم ها چیست؟**

طراحی مجدد سیستم ها همیشه به دلیل پوشش نیازهای وظیفه مندی نیست،بلکه بیشتر به دلیل مشکالتی در زمینه نگهداشت پذیری، مقیاس پذیری، سرعت پاسخ گویی و امنیت آن ها است.

**معماری چگونه ابزار است ؟**

معماری ابزاری است برای دستیابی به خصوصیات کیفی )این کار با ساختاردهی به وظیفه مندی در قالب مولفه ها/ماژول ها انجام می شود(.

**دستیابی به خصوصیات کیفی مرتبط با معماری مربوط به چه مراحلی است ؟**

دستیابی به خصوصیات کیفی مرتبط با معماری )نیازهای غیروظیفه مندی( مربوط به کلیه مراحل طراحی، پیاده سازی و استقرار سیستم است. یعنی: این نوع خصوصیات کیفی، مربوط به تنها یک مرحله از تولید نرم افزار مثالً طراحی یا پیاده سازی نیست. در واقع، خصوصیات کیفی هم دارای جنبه های معمارانه و هم غیرمعمارانه هستند.

**آیا خصوصیات کیفی مستقل هستند ؟**

خصوصیات کیفی مستقل نیستند و نمی توانند به تنهایی انجام شوند )لزوم ایجاد توازن بین آن ها(

همبستگی مثبت: قابلیت اصلاح در مقابل قابلیت ساخت )در بیشتر موارد(. ν

همبستگی منفی: قابلیت اطمینان در مقابل امنیت ،کارایی در مقابل بقیه خصوصیات کیفی

**انواع خصوصیات کیفی را نام ببرید؟**

1-خصوصیات کیفی سیستمی شامل:

الف) قابلیت دسترسی ب) کارایی ث) امنیت پ)قابلیت جابجایی ج)قابلیت استفاده چ)قابلیت تغییر ح)عملکرد خ)قابلیت استفاده مجدد ر)قابلیت تجمیع پدیری ز) قابلیت آزمون

2-خصوصیات کیفی حرفه(معماری بر آنها تاثیر می‌گذارد) شامل :

الف) زمان ارائه به بازار ب)سود و هزینه ت) طول عمر پیش بینی شده . ع) زمان بندی راه اندازی ف) تجمیع با سیستم های موروثی غ) بازار هدف

3-خصوصیات کیفی معماری (معماری را تحت تاثیر قرار میدهند.شامل:

یکپارچگی مفهومی ، قابلیت ساخت ، صحت و تکامل

**طبقه بندی خصوصیات کیفی برحسب اجرا چیست ؟**

1. قابل مشاهده از طریق اجرا )نرم افزار باید اجرا شود تا مشخص شود چنین خصوصیاتی فراهم شده است یاخیر؟( مانند کارایی و امنیت
2. غیر قابل مشاهده از طریق اجرا )این خصوصیات در زمان اجرا قابل رویت و ارزیابی نیستند(. مانند قابلیت اصالح، قابلیت آزمون و قابلیت استفاده مجدد θ خصوصیات غیر قابلمشاهده برخی اوقات بسیار مهم می شوند. )این خصوصیات نشان می دهد که تحلیل، طراحی و آزمایش سیستم با چه میزان سهولت و راحتی انجام می گیرد (

**مشکلات گدشته خصوصیات کیفی چیست ؟**

1)‌ تعاریف ارائه شده برای یک خصوصیت کیفی، عملیاتی نیست. مثال: امنیت با توجه به کدام جنبه سیستم؟ در مورد خطای سیستم یا نفوذ پذیری سیستم

2) یک جنبه خاص به کدام خصوصیت کیفی تعلق دارد. ν آیا خطای سیستم یکی از جنبه های کارایی، امنیت یا قابلیت استفاده است؟

3) هر خصوصیت کیفی فرهنگ اصطالحات خاص خود را دارد . خصوصیت کارایی شامل مفهوم »رویداد« است که در سیستم رخ می دهد، ν خصوصیت امنیت دربردارنده مفهوم »حمله« است، ν خصوصیت قابلیت دسترسی شامل مفهوم »خرابی« است.

**آیا راه حلی برای مشکلات بالا وجود دارد ؟**

برای مشکالت اول و دوم می توان: ♣ از سناریوهای خصوصیات کیفی استفاده نمود )به عنوان ابزاری برای مشخص کردن خصوصیات کیفی(. θ برای مشکل سوم می توان: ♣ توصیف کوتاهی برای مفهوم هر خصوصیت کیفی ارائه نمود. θ سناریوها می توانند عمومی یا منحصربفرد )برای سیستم خاص( باشند.

سناریوی خصوصیات کیفی چیست و شامل چه مواردی است ؟

هر سناریوی خصوصیات کیفی، یک نیازمندی مرتبط با خصوصیات کیفی است که شامل شش قسمت است:

1. منبع تحریک (stimulus of Source ): موجودیتی که تحریک را ایجاد می کند )مانند: انسان، سیستم کامپیوتری یا هر محرک دیگری که مولد یک تحریک است(.
2. محرک (Stimulus ) : شرط یا شرایطی است که وقتی وارد یک سیستم می شود باید مورد توجه قرار گیرد. )مانند: خطا، یا پاسخ یک مولفه با یک مقدار نادرست(. θ
3. محیط )Environment :)تحریک در وضعیت ها و شرایط خاص و معینی روی می دهد. )مثالً وقتی یک تحریک رخ می دهد، سیستم ممکن است در حال اجرا با شرایط اضافه بار )overload )باشد(. θ
4. فرآورده )Artifact :)قسمت هایی از سیستم که نیاز است در دسترس باشند، به عبارت دیگر فرآورده موجودیتی است که هدف تحریک است- فرآورده ممکن است کل سیستم یا بخشی از آن باشد )مانند پردازنده، کانال های ارتباطی، فرایند، ذخیره سازی و ...( θ
5. پاسخ )Response:)واکنش مورد نظر سیستم به یک محرک )ثبت خرابی، اطالع رسانی به اپراتور سیستم و غیره( θ
6. اندازه گیری پاسخ )measure Response :)پاسخ باید با استفاده از روش هایی قابل اندازه گیری باشد تا نیازمندی بتواند آزمایش شود

**بخش های اصلی سنارویها خصوصیت کیفی؟**

سناریوهای عمومی )مستقل از سیستم بوده و می توانند در ارتباط با هر نوع سیستمی باشند(

. ♣ سناریوهای عینی )برای سیستم های خاص استفاده می شوند(

**سناریوهای عمومی چه چیزی را فراهم می کنند؟**

سناریوهای عمومی چارچوبی را فراهم می کنند برای تولید تعدادی از سناریوهای مستقل از سیستم.

**برای اینکه سناریوی عمومی برای یک سیستم خاص مفید باشد باید چه کار کرد ؟**

برای اینکه سناریوی عمومی برای یک سیستم خاص مفید باشد، ♦ باید آنها را خاص سیستم موردنظر ) specific-system (تعریف نمود.

**specific-system نمودن یک سناریوی عمومی، یعنی چه؟**

Specific-system نمودن یک سناریوی عمومی، یعنی ترجمه آن به عبارات و اصطالحات کامالً مرتبط با یک سیستم خاص.

**هر سناریوی عمومی می تواند چه تعداد نسخه سناریوی specific-system داشته باشد؟**

هر سناریوی عمومی می تواند چندین نسخه سناریوی specific-system داشته باشد.

مثال )سناریوی عمومی(: درخواستی برای ایجاد یک تغییر در یک وظیفه مندی دریافت می شود و تغییر باید در یک بازه زمانی مشخص در داخل فرایند اِعمال گردد.

مثال1( یک نسخه خاص سیستم(: درخواستی برای اضافه کردن یک Browser جدید به سیستم مبتنی بر وب دریافت می شود وآن تغییر باید در بازه زمانی دو هفته انجام شود.

مثال2( یک نسخه خاص سیستم(: سیستمی که از مرورگر جدید حمایت می کند، باید از یک رسانه جدید نیز حمایت نماید.

**قابلیت دسترسی با چه چیزی مرتبط است و چه زمانی اتفاق میافتد و مهمترین مسئله در زمان این رخداد چیست؟**

قابلیت دسترسی با شکست سیستم )failure system )و پیامدهای آن مرتبط است.

شکست سیستم وقتی اتفاق می افتد که سیستم قادر به ارائه سرویس های پیش فرض خود نیست.

در زمان شکست سیستم، مهمترین مسئله مدت زمان الزم برای تعمیر آن است.

**استراتژی تعمیر اتومات سیستم چیست ؟**

:اگر در زمان اجرای سیستم نقصی روی دهد، سیستم بدون اینکه دچار شکست شود، نقص را اصالح کند )با این راهبرد، شکست در سیستم وجود نخواهد داشت(.

**تفاوت شکست و نقص را توضیح دهید ؟**

نقص می تواند به شکست تبدیل شود اگر اصالح یا پوشش داده نشود. θ

شکست توسط کاربران قابل مشاهده است ولی نقص قابل مشاهده نیست.

θ نقص وقتی قابل مشاهده می گردد که به شکست تبدیل می شود.

**قابلیت دسترسی چیست؟**

احتمال اینکه وقتی به سیستم نیاز داریم، سیستم در حالت عملیاتی باشد.

**قابلیت اصالح دربارة چیست؟.**

قابلیت اصالح دربارة هزینة تغییرات است.

**قابلیت اصلاح چه نگرانی های را به وجود میآورد ؟**

1 -چه چیزی می تواند تغییر کند ؟

تغییر می تواند در هر یک از جنبه های سیستم باشد مانند: ν

1. وظایفی که سیستم انجام می دهد )متداول ترین تغییرات(.
2. سکویی که سیستم روی آن قرار دارد )سخت افزار، سیستم عامل و ...(. ν
3. محیطی که سیستم در آن اجرا می شود )سیستمی که سیستم موردنظر باید با آن ارتباط داشته باشد(. ν
4. خصوصیات کیفی که سیستم ارائه می دهد )کارآیی، قابلیت اطمینان(. ν
5. ظرفیت سیستم )تعداد کاربران پشتیبانی شده، تعداد عملیات همزمان(.

2 -چه زمانی و چه کسی تغییر را انجام می دهد ؟

یک تغییر ممکن است توسط: کاربر، توسعه دهنده یا مدیر سیستم انجام گیرد

تغییرات می تواند در کد برنامه در مواقع زیر اعمال گردد:

1. در زمان کامپایل،
2. در زمان ساخت،
3. در زمان استقرار،
4. در زمان پیکره بندی نصب،
5. یا در طول اجرای سیستم

**کارایی با چه موضوعی در ارتباط است ؟**

کارایی با زمان در ارتباط است.

رویدادهایی (وقفه ها، پیام ها، درخواست های کاربران) در سیستم رخ می دهند و سیستم باید به آنها پاسخ دهد.

وقتی رویدادی اتفاق می افتد چه مدت طول می کشد تا سیستم پاسخ دهد.

**چه چیزی باعث پیچیدگی کارایی میشود ؟**

تعداد منابع رویداد، ترتیب وقوع آنها و الگوهای ورودی (دوره ای مثالً هر 10 میلی ثانیه یا آماری با توجه به یک تابع توزیع احتمال(.

**رویداد ها از چه چیزهایی ممکن است صادر شوند؟**

رویدادها ممکن است از درخواست های کاربران، از سیستم های دیگر یا از داخل سیستم صادر شوند**.**

**ویژگی های اغلب سناریوهای کاربری را توضیح دهید ؟**

1. با درخواست برای یک سرویس در سیستم شروع می شوند.
2. برآورده نمودن درخواست با مصرف منابع همراه است
3. معموالً رویدادها به صورت موازی به کار می روند (همزمان وارد سیستم می شوند(

**انواع الگوهای رسیدن رویداد ها را نام ببرید؟**

دوره ای: اغلب در سیستم های بالدرنگ دیده می شوند.

احتمالی )آماری(: رویدادها بر طبق تابع توزیع احتمالی خاص دریافت می شوند.

منفرد )پراکنده(: الگویی که نمی تواند با دیگر الگوها نمایش داده شود.

**امنیت چه معیاری است ؟**

امنیت معیاری برای توانایی سیستم به منظور:

مقاومت در مقابل استفاده غیرمجاز است در حالیکه سیستم خدمات خود را برای کاربران مجاز ارائه می دهد.

**حمله چیست ؟**

هر تالشی برای شکستن امنیت، حمله نامیده می شود. حمله می تواند برای اهداف زیر باشد:

1. دستیابی غیرمجاز به داده ها یا خدمات،
2. تغییر آنها،
3. از کار انداختن سرویس دهنده برای کاربران مجاز.

**امنیت بیان گر چه صفتی است ؟**

امنیت می تواند به عنوان صفت برای سیستمی بیان شود که فراهم کنندة محرمانگی، تمامیت، عدم انکار، قابلیت دسترسی و ثبت وقایع است

**قابلیت آزمون چیست ؟**

به میزان راحتی آزمون نرم افزار برای نمایش خطاهای آن، اطالق می شود

**قابلیت آزمون چه چیزی را بیان می دارد ؟**

در عمل، قابلیت آزمون، به احتمال اینکه نرم افزار حداقل دارای یک خطا باشد، اشاره دارد که در اجرای بعدی بروز خواهد نمود. البته، محاسبه این احتمال آسان نیست ونیازمند به کارگیری الگوریتم های پیچیده ای است

.

**چگونه یک سیستم باید قابلیت درست آزمون کردن را داشته باشد ؟**

باید بتوان حالت داخلی و ورودی های هر مولفه را کنترل نموده و سپس خروجی را مشاهده کرد**.**

**چه چیزهای در آزمون مورد ارزیابی قرار می گیرد؟**

ممکن است بخش های از کد، طراحی یا کل سیستم مورد آزمون قرار گیرد

**اندازه گیری پاسخ برای قابلیت آزمون با چه مواردی سر و کار دارد؟**

اندازه گیری پاسخ برای قابلیت آزمون با موارد زیر سروکار دارد:

چگونگی اثربخشی آزمون ها در کشف خطاها،

ν مدت زمان آزمون ها برای سطح مناسبی از پوشش

**خصوصیت کیفی قابلیت استفاده چه چیزی را بیان میدارد؟**

چقدر برای یک کاربر آسان است که کار (وظیفه ) دلخواه خود را انجام دهد.

**سیستم برای انجام کارها، از کاربران چه حمایت هایی می نماید؟**

یادگیری ویژگی های سیستم )features system Learning)

**چه نکاتی در مورد سناریوهای عمومی وجود دارد ؟**

نقش سناریوهای عینی ( Concrete )برای نیازمندی های خصوصیات کیفی همانند: نقش موارد کاربری (Cases Use )برای نیازمندی های وظیفه مندی است. ν

مجموعه ای از سناریوهای عینی می توانند: برای نمایش نیازمندی های خصوصیات کیفی یک سیستم استفاده شوند.

ν یکی از کاربردهای سناریوهای عمومی: برقراری ارتباط بین ذینفعان است.

**مراحل اجرای خصوصیات کیفی را نام ببرید؟**

1. نیازمندی های حرفه
2. خصوصیات کیفی
3. انتخاب تاکتیک
4. پیاده سازی تاکتیک: الگوهای طراحی و الگوهای معماری

**تاکتیک چیست ؟**

تاکتیک یک تصمیم طراحی است که کنترل پاسخ خصوصیت کیفی را تحت تاثیر قرار می دهد.

هر تاکتیک یک گزینه طراحی برای معمار است (مثال: تاکتیک افزونگی یکی از گزینه های طراحی معمار برای افزایش »قابلیت دسترسی« است(.

**راهبرد معماری چیست ؟**

مجموعه ای از تاکتیک ها، یک راهبرد معماری ( strategies Architectural )را تعریف می کنند.

**الگو چیست ؟**

الگوها، تاکتیک ها را بسته بندی می کنند ( مجموعه ای از تاکتیک ها هستند(. الگویی که از »قابلیت دسترسی« حمایت می کند، مطمئناً دربرگیرنده هر دو نوع »تاکتیک افزونگی« و »تاکتیک همگام سازی« است.

**تاکتیک های معماری از چه طریقی فراهم می شوند ؟**

تاکتیک هایی که معمار برای طراحی یک سیستم استفاده می کند، از طریق : الگوهای طراحی، الگوهای معماری یا راهبردهای معماری فراهم می شوند.

**معمار پس از انتخاب خصوصیات کیفی، برای اجرای آنها چه کاری می کند؟**

معمار پس از انتخاب خصوصیات کیفی، برای اجرای آنهااز الگوها یا سبک های معماری استفاده می نماید. هر الگو یا سبک، مجموعه ای از تاکتیک ها است.

**هدف از تاکتیک های قابلیت دسترسی چیست ؟**

1. عدم تبدیل نقص به شکست : شکست سببِ عدم توانایی سیستم در ارائه خدمات می شود.
2. کاهش اثرات نقص : نقص کمترین اثر را بر عملکرد کاربران داشته باشد.
3. اصالح نقص : وضعیت سیستم به حالت قبل از نقص برگردد.

**تاکتیک های قابلیت دسترسی دارای چه ویژگی هایی است ؟**

همه تاکتیک های »قابلیت دسترسی« دارای روش هایی از نوع زیر هستند:

1. افزونگی،
2. کنترل صحت سیستم برای شناسایی نقص )سیستم کنترل و آزمون شود تا تقسیم بر صفر اتفاق نیفتد(،
3. بازیافت )ترمیم( سیستم وقتی شکست اتفاق می افتد.

**تاکتیک های دسته بندی را نام ببرید؟**

1. تشخیص نقص )Fault Detection(
2. بازیافت (ترمیم )نقص )Recovery Fault )
3. جلوگیری از نقص )Prevention Fault )

**تاکتیک های تشخیص نقص را نام ببرید؟**

1. انعکاس/صدا Ping/echo )): یک مولفه، پیامی را ارسال میکند و انتظار دارد تا در بازه زمانی مشخصی پاسخ را دریافت نماید. عدم دریافت پاسخ به معنای خطا تلقی می شود )رابطه بین سرویس گیرنده ها و سرویس دهنده ها(
2. ضربان قلب ( Heartbeat ) : یک مولفه، به صورت دوره ای یک پیام )ضربان قلب( را در بازه زمانی مشخصی منتشر می کند و مولفه دیگر آنها را دریافت می کند. اگر مولفه دریافت کننده پیام، قطع شدن پیام را متوجه شود به معنای وجود خطا است )در اینصورت مولفه اصالح نقص را فراخوانی می کند(.
3. Exceptions (استثنائات ) : وقتی خطایی رخ می دهد یک استثناء اتفاق می افتد و مدیر استثنائات آن را تشخیص و رسیدگی به آن را آغاز می نماید )در نهایت حالت خود را به حالت قبل از وقوع خطا برمی گرداند(

**تاکتیک های بازیافت نقص (ترمیم ) را نام ببرید ؟**

1. رای گیری (voting ) : فرآیندهایی که بصورت افزونه روی پردازنده های مجزا اجرا می شوند، ورودی یکسان دریافت می کنند و خروجی خود را به یک رای دهنده )Voter )ارسال می کنند. رای دهنده اگر انحرافی یا اشتباهی در رفتار هر پردازنده دریافت کند آن را به عنوان یک نقص در نظر می گیرد. کاربرد: در سیستم های کنترلی- برای اصالح نقص یک الگوریتم یا خطای یک پردازنده. Voter از الگوریتم »قانون اکثریت« یا »مولفه های برتر« استفاده می کند و پاسخ درست را انتخاب می کند.
2. :)افزونگی فعال )Active Redundancy : همه مولفه های افزونه، به صورت موازی به رویدادها پاسخ می گویند )وضعیت مولفه ها مشابه یعنی همه به روز هستند(. ν در این تاکتیک، تنها اولین پاسخ مورد استفاده قرار می گیرد و مابقی نادیده گرفته می شوند. در صورت بروز نقص، زمان دردسترس نبودن سیستم بسیار کوتاه )چند میلی ثانیه( است، زیرا مولفه پشتیبان فعال شده و سرویس های مربوطه را پاسخ می دهد )مولفه پشتیبان در آن لحظه فعال است( . این تاکتیک اغلب در سیستم های سرویس گیرنده/سرویس دهنده به کار گرفته می شود )مانند سیستم های مدیریت پایگاه داده(
3. افزونگی غیر فعال (passive redundancy ) :

یک مولفه )به عنوان نسخه اصلی( به رویدادها پاسخ می دهد و دیگر مولفه ها را مطلع می سازد تا حالت خود را به روزرسانی کنند )تغییرات را در خود اعمال نمایند(

وقتی نقص اتفاق می افتد، ابتدا سیستم مطمئن می شود که نسخه های پشتیبان به روز هستند و سپس آنها را استفاده می کند )انتقال از مولفه اصلی به مولفه پشتیبان(

همگام سازی بین مولفه های پشتیبان وظیفه مولفه اصلی است.

این تاکتیک در سیستم های کنترلی استفاده می شود )به ویژه حالتی که ورودی از طریق کانال های ارتباطی یا سنسورها است و ضرورت ایجاب می کند در صورت بروز نقص، انتقال از مولفه اصلی به مولفه پشتیبان صورت گیرد(

1. Spare(یدک) :

در این تاکتیک، یک سکوی محاسباتی یدکی جانشین، جایگزین مولفه های دارای خطا می شود .

حالت های متفاوتی از سیستم )یک نقطه وارسی از وضعیت سیستم( به صورت دوره ای در یک رسانه ماندگار ثبت می شود )تمامی تغییرات در وضعیت سیستم در آن رسانه ثبت می شود(

هنگام وقوع خطا، حالت مناسب تشخیص داده شده و یدک جایگزین آن می شود )این عمل چند دقیقه طول می کشد(

1. عملیات در سایه ( Shadow Operation ):

مولفه ای که قبالً خطا داده است، برای مدت کوتاهی در حالت سایه کار می کند تا مطمئن شود همان رفتاری را دارد که که قبل از حالت ترمیم داشت )برگشت مولفه به سیستم پس از اصالح(. یعنی مولفه خطادار از حالت اجرا خارج می شود و بازیافت روی آن اعمال می گردد و پس از مدت کوتاه در صورت اصالح رفتار، مجددا به سیستم بر می گردد.

1. همگام سازی مجدد حالت ) resynchronization State ) :

تاکتیک های افزونگی فعال و غیرفعال نیاز به روشی دارند که مولفه جایگزین قبل از شروع سرویس خود، به روز باشد، لذا همزمانی ضرورت دارد )همزمانی اِعمال تغییرات در مولفه های پشتیبان(

1. نقطه وارسی / عقبگرد ( checkpoint /rollback )

نقطه وارسی یک ذخیره سازی از وضعیت سازگار سیستم در رسانه ماندگار است.

ثبت حالت سازگار، به صورت دوره ای یا موقع پاسخ به یک رویداد خاص انجام می شود.

هنگام وقوع خطا، سیستم به آخرین حالت پایدار با توجه به آخرین نقطه وارسی برگردانده می شود.

**تاکتیک های جلوگیری از نقص را نام ببرید؟**

1. خارج کردن از سرویس (removal from service ):

مولفه ای که دارای مشکل است از عملیات خارج می شود تا سبب خطا نشود.

اینکار می تواند دستی یا خودکار انجام شود )خودکار: نیاز به یک راهبرد معماری دارد(.

1. تراکنش ها ( transactions ) :

تراکنش مجموعه ای از دستورات هستند که یا همه باهم اجرا می شوند و یا هیچیک اجرا نمی شوند

اگر خطایی در یک دستور درون تراکنش اتفاق افتد، کلیه دستورات دیگر اعم از اجراشده یا نشده، نادیده گرفته می شوند

1. نظارت بر فرایند (process monitor ) :

کنترل کننده فرآیندها با مشاهده نقص، می تواند فرآیند را حذف نماید و یا یک نمونه جدید از آن ایجاد کرده و آن را شروع مجدد نماید.

**هدف از تاکتیک قابلیت اصلاح چیست ؟**

کنترل زمان و هزینه پیاده سازی، آزمایش و استقرار تغییرات است .

**دسته بندی تاکتیک های قابلیت اصلاح را نام ببرید ؟**

1. محلی سازی تغییرات )modifications Localize:

هدف، کاهش تعداد ماژول هایی است که در اثر یک تغییر تحت تاثیر قرار می گیرند( یعنی مسئولیت آن ها به طور مستقیم تغییر می کند). این عمل باعث کاهش هزینه تغییرات می شود.

1. جلوگیری از تاثیرات موجی )Effects Ripple Prevent:

هدف، ایجاد تغییر در ماژولی است که به طور مستقیم تحت تاثیر آن تغییر نیست.

یعنی مسئولیت ماژول تغییر نمی کند ولی برای دیده شدن اثر تغییر در یک ماژول، پیاده سازی آن باید تغییر کند.

1. به تاخیر انداختن زمان انقیاد )Time Binding Defer:

هدف، کنترل زمان و هزینه استقرار است

به کاربر یا مدیر سیستم اجازه می دهد تغییراتی را ایجاد کنند و یا ورودی را فراهم کنند تا رفتار سیستم را تحت تاثیر قرار دهد.

**تاکتیک های محلی سازی استقرار را نام ببرید ؟**

1. حفظ انسجام معنایی :

پیوستگی معنایی به ارتباط بین مسئولیت ها در یک ماژول اشاره دارد.

هدف از این تاکتیک، نگه داشتن تمام وظایف مرتبط در یک ماژول بدون استفاده از ماژول دیگر است. )معیارهای اندازه گیری انسجام معنایی عبارت است از: Coupling و Cohesion.)

1. پیش بینی تغییرات مورد انتظار:

در این تاکتیک، تغییرات پیش بینی شده در تقسیم بندی ماژول ها موثر است. ν

این تاکتیک با حداقل کردن اثرات تغییرات در ماژول ها مرتبط است.

1. عمومی سازی ماژول ها

عمومی تر نمودن ماژول سبب می شود که توابع بیشتری از آن استفاده نمایند**.**

1. محدود کردن گزینه ها ی ممکن

محدود کردن گزینه ها سبب کاهش تغییرات و اصلاحات خواهد شد. ν مثال: در یک خط تولید اگر اجازه تغییر پردازنده داده شود، محدود کردن استفاده از پردازنده های هم خانواده، گزینه های ممکن برای تغییرات و لذا اثرات ناشی از آن تغییرات را محدود می کند.

**انواع تاکتیک های جلوگیری از تاثیرات موجی را نام ببرید .**

1-‌ پنهان سازی اطلاعات (hide information ):

تجزیه وظایف یک ماژول به قسمت های کوچکتر و انتخاب اینکه کدام یک از این قسمت ها عمومی و کدام خصوصی باشند

هدف: تغییرات در داخل یک ماژول ایزوله شود و از انتشار به سایر ماژول ها جلوگیری گردد.

2- نگه داری رابط های موجود (maintain exiting interfaces )

اگر ماژول B وابسته به نام و امضای یکی از رابط های ماژول A باشد، ثابت نگه داشتن این رابط اجازه می دهد که B نیز بدون تغییر باقی بماند )از طریق جدا کردن واسط از پیاده سازی(.

3-‌ محدود کردن مسیرهای ارتباطی (restrict communication paths )

کاهش تعداد ماژول هایی که داده ی تولید شده یک ماژول را مصرف می کنند و نیز کاهش تعداد ماژول هایی که داده تولید می کنند )کاهش تعداد ماژول های تولید کننده و مصرف کننده داده)

این عمل تاثیر موجی را کاهش می دهد، زیرا تولید و مصرف داده، وابستگی تعریف می کند و باعث انتشار موجی می شود.

4-‌ استفاده از یک میانجی/واسطه (use an intermediary )

در صورتی که دو ماژول به یکدیگر وابسته باشند، استفاده از یک میانجی کمک می کند تا فعالیت های بین ماژول ها را مدیریت نمود

. ν انواع مختلفی از میانجی ها وجود دارند که از آن جمله می توان به میانجی های زیر اشاره کرد: θ

داده یا مخزن )سبک blackboard و passive – )رابط بین مصرف کننده و تولید کننده داده θ

مخزن ها، می توانند گرامر تولید شده بوسیله A را به فرضیات B تبدیل کنند

. θ سرویس )الگوهای facade( نمای خارجی(، bridge ،mediator ،strategy )و ... رابطی فراهم می کنند که گرامر یک سرویس را به دیگری تبدیل می کنند

**تاکتیک های به تاخیر انداختن زمان انقیاد را نام ببرید ؟**

1-‌ ثبت نام زمان اجرا (runtime registration ):

ماژول ها در زمان اجرا و به صورت play and plug ثبت و مورداستفاده قرار می گیرند )الگوی Subscribe/Publish هم در زمان اجرا قابل پیاده سازی است(

2- فایل های پیکربندی (configuration files )

فایل های پیکره بندی تمایل دارند که در زمان شروع، پارامترها را مقداردهی کنند.

3- ‌چند ریختی (polymorphism )

اجازه انقیاد دیر هنگام فراخوانی متدها را می دهد .

4-‌ جایگزینی مولفه ها (component replacement )

اجازه بارگذاری مولفه ها در زمان اجرا را می دهد.

1. پایبندی به پروتوکول های تعریف شده :

اجازه انقیاد فرآیندهای مستقل در زمان اجرا را می دهد.

**هدف تاکتیک های کارایی چیست ؟**

هدف تاکتیک های کارایی ارائه پاسخ به یک رویداد ورودی در زمان تعیین شده است .

**رویداد ها چگونه میتوانند باشند و نمونه ای از رویداد ها را نام ببرید ؟**

رویدادها می توانند به صورت جریانی از رویدادها یا منفرد باشند (شروع کننده یک درخواست( و مونه ای از رویدادها: رسیدن یک پیام، انقضای بازه زمانی، تشخیص یک تغییر وضعیت. با وقوع یک رویداد، سیستم رویداد مربوطه را پردازش کرده و پاسخ مناسب را تولید می کند.

**تاکتیک های کارایی چه چیز را کنترل می کنند ؟**

مدت زمان تولید پاسخ برای یک رویداد را کنترل می کنند.

**زمان تاخیر چیست ؟**

زمان بین رسیدن یک رویداد تا تولید یک پاسخ است.

**دو مفهوم مهم که بر زمان پاسخ تاثیر دارند را نام ببرید ؟**

1. )Resource consumption( مصرف منابع

پردازنده، رسانه های ذخیره سازی داده، پهنای باند شبکه ارتباطی، حافظه و

2- زمان مسدود شدن (blocked time )

زمانی که یک فرآیند بنا به دالیل ذیل مسدود می شود و باعث تاخیر در زمان پاسخ می شود:

o رقابت بین منابع )رقابت فرایندها برای دسترسی به یک منبع(. O

قابل دسترس نبودن منابع )به دلیل برون خط )offline )بودن منبع، خطا در مولفه های آن و ...(. o

وابستگی یک محاسبه به نتایج دیگر محاسبات )که هنوز تولید نشده اند

**دسته بندی های مختلف تاکتیک های خصوصیت کیفی (کارایی ) را نام ببرید ؟**

1. تقاضای منابع (resource demand )
2. مدیریت منابع (resource management )
3. داوری منابع (resource arbitration )

**سرچشمه تقاضای منابع چیست ؟**

جریان رویدادها سرچشمه و منشاء تقاضای منابع هستند.

**دو خصوصیت (ویژگی ) تقاضای منابع به شرح زیر است :**

1. زمان بین رویداد ها در یک جریان چقدر است .
2. چقدر منبع برای هر درخواست مصرف میشود .

**تاکتیک های خصوصیت کیفی (امنیت )**

تاکتیک های امنیت به سه گروه زیر تقسیم می شوند :

1. مقاومت در برابر حملات (resisting attacks )
2. تشخیص حملات (detecting attacks )
3. بازیابی از حملات ( recovering from attacks )
4. مثل: قراردادن قفل بر روی درب خانه، تاکتیک مقاومت در برابر حمله است. قراردادن یک سنسور حرکتی در داخل خانه، تاکتیک شناسایی حمله است و داشتن بیمه نامه خانه، تاکتیک بازیابی از حمله است

**مجموعه تاکتیک های مقاومت resisting attacks) ): در برابر حملات را نام ببرید ؟**

1. احراز هویت کاربران(authenticate users) :

:احراز هویت کاربران با استفاده از کلمات عبور، کلمات عبور دو مرحله ای، گواهینامه های دیجیتال، شناسه های بایومتریک و غیره

2-‌ انتساب حق دسترسی به کاربان (authorize users ):

انتساب حق دسترسی به داده ها و سرویس های مختلف پس از تصدیق کاربران

3- ‌حفظ محرمانگی داده ها (maintain data confidentiality )

:استفاده از الگوریتم های رمزگذاری روی داده ها و پیوندهای ارتباطی )VPN یا SSL )برای حفظ محرمانگی و دسترسی های نامعتبر

4- حفظ یک پارچگی (maintain integrity )

تحویل داده ها به همان شکلی که از ابتدا مدنظر بوده با استفاده از کدگذاری آن ها

داده می تواند اطالعات اضافی رمزگذاری شده در درون خود داشته باشد )مانند checksums یا نتایج hash( )checksums به منزله اثر انگشت فایل شما است(

5- نمایش محدود (limit exposure )

سرویس هایی که مورد نیاز کاربران نیستند، نباید توسط کاربران دیده شوند. ν

معمار می تواند با محدود نمودن سرویس های قابل رویت توسط کاربران، امکان حمله به آنها را کاهش دهد.

6-دسترسی محدود (limit access )

استفاده از دیواره آتش )Firewall )می تواند دستیابی کاربران غیرمجاز به سرویس ها و داده ها را کاهش دهد

**تاکتیک های تشخیص حملات را نام ببرید ؟**

1-‌ تشخیص نفوذ (intrusion detection ):

سیستم های تشخیص نفوذ می توانند برای شناسایی حمالت با استفاده از روش هایی نظیر الگوبرداری از ترافیک شبکه و ... مورد استفاده قرار گیرند )مثالً اگر دسترسی یک فرد به شبکه در خارج از ساعت اداری باشد، می تواند یک نفوذ تلقی شود(.

**تاکتیک های بازیابی پس از حمله را نام ببرید ؟**

1. رد ممیزی (audit trial )

تاکتیک موردنیاز برای شناسایی حمله کننده، نگهداری یک رد ممیزی است. ν

رد ممیزی، ثبت تمام تراکنش های انجام شده بر روی داده ها به همراه اطالعات تشخیص هویت است. ν

ردگیری فعالیت های حمله کننده و جلوگیری از عدم انکار وی و پشتیبانی از بازیابی سیستم است. )بازگرداندن سیستم به وضعیت قبل از حمله(