



**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**

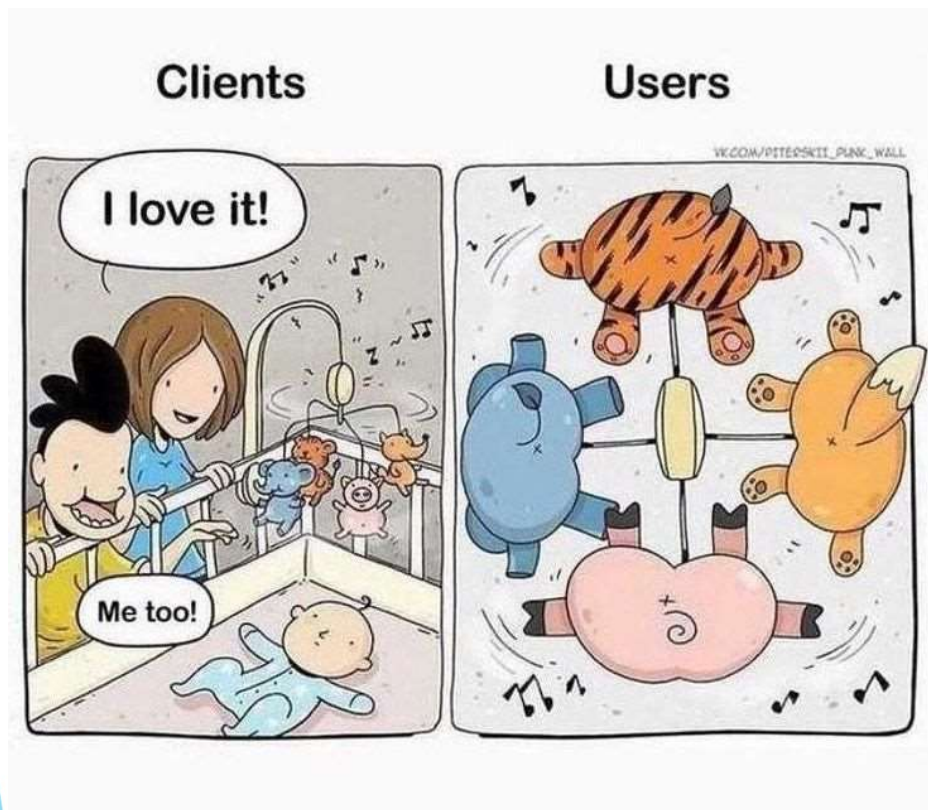
Інформаційні системи

Викладач: к.т.н., доц. Саяпіна Інна Олександрівна

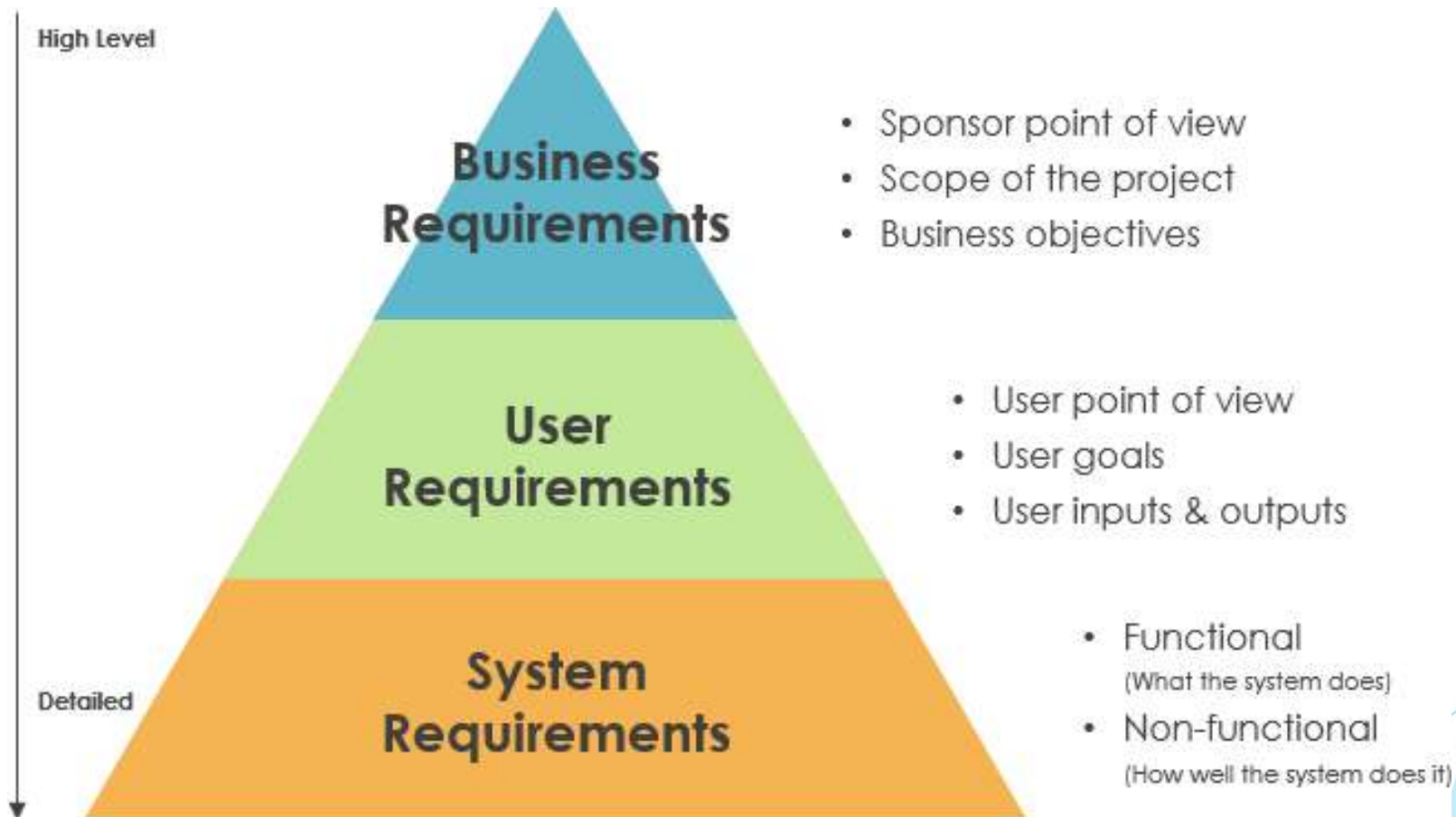
План заняття

- ▶ 1. Атрибути якості (quality attributes QA)
- ▶ 2. Сценарії атрибутів якості.
- ▶ 3. Функціональність та архітектура
- ▶ 4. Готовність (availability)
- ▶ 5. Здатність до модифікації (modifiability)
- ▶ 6. Продуктивність (performance)
- ▶ 7. Безпека (security)
- ▶ 8. Контролепридатність (testability)
- ▶ 9. Зручність використання (usability)
- ▶ 10. Deployability (можливість розгортання)
- ▶ 11. Integrability (здатність до інтеграції)

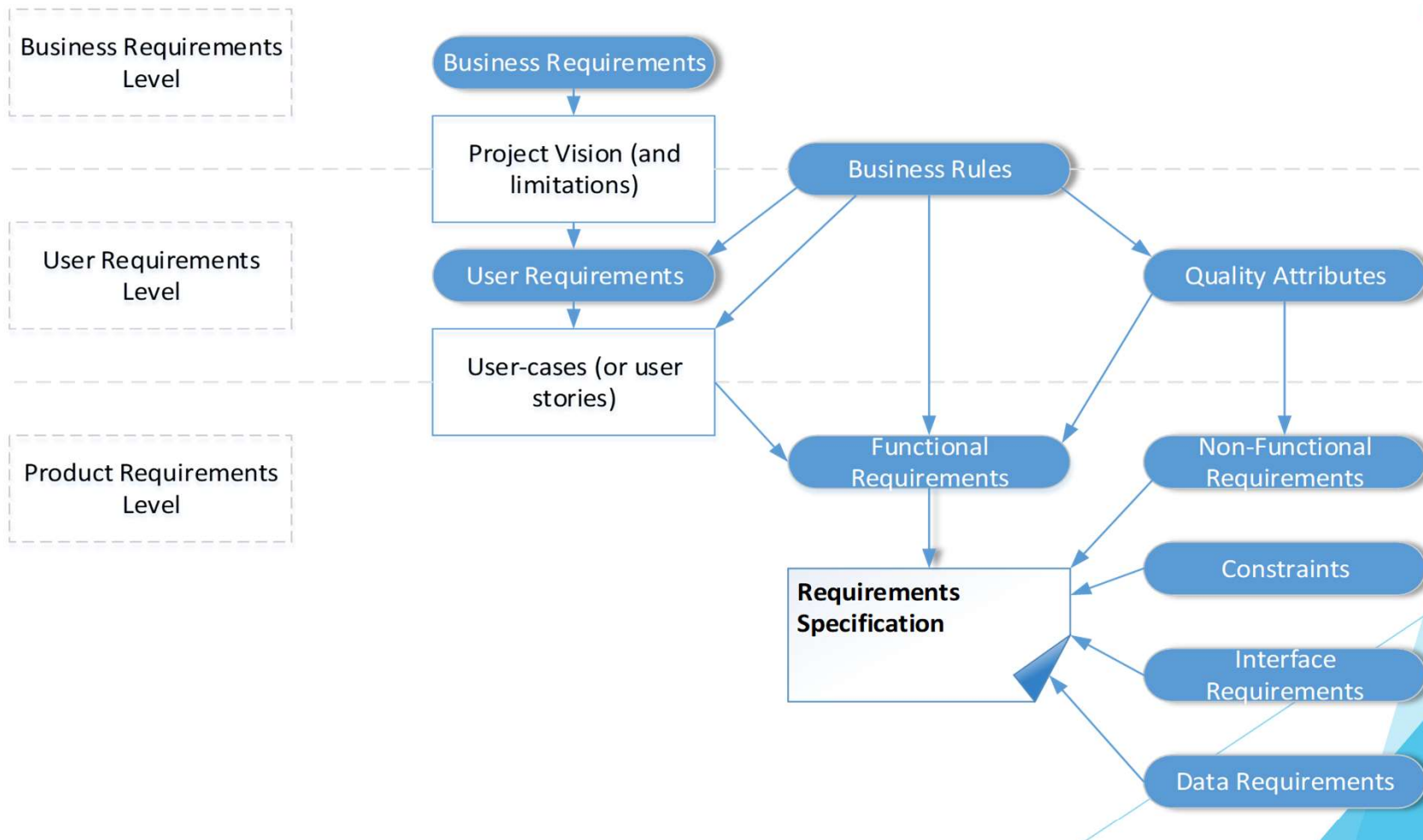
Формування вимог. Що може піти не так?



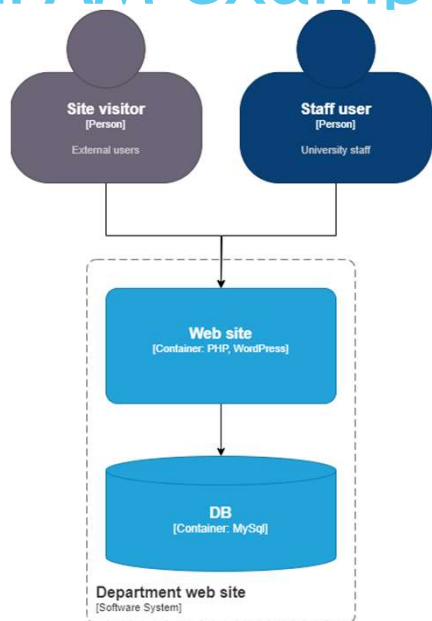
Типи вимог



Типи вимог (en)

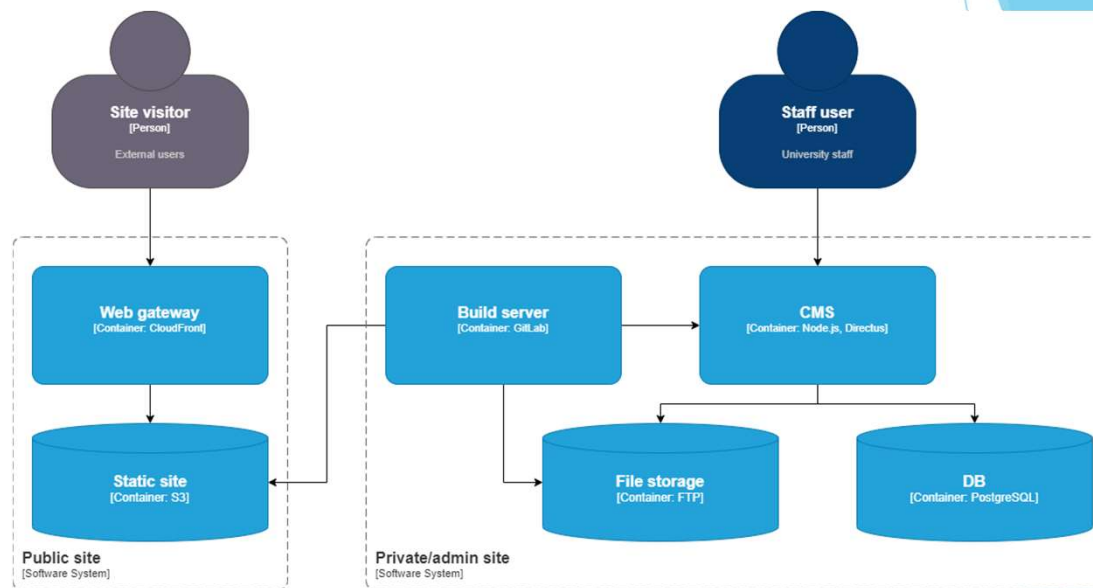


На що впливає визначення вимог? (EPAM example)



Option #1

- Simple deployment
- Use LAMP stack
- Time to market
- Easy content editing



Option #2

- Rendering performance on different devices
- Modern design
- Cost of infrastructure

Функціональність

- ▶ **Функціональність** - це здатність системи виконувати роботу, для якої вона була призначена.
- ▶ *Чи функціональність визначає архітектуру?*
- ▶ Для забезпечення потрібного набору необхідних функціональних можливостей є безліч архітектур, за допомогою яких їх можна реалізувати. Принаймні, функціональність можна розподілити різними способами та призначити виконання тих чи інших функцій різним архітектурним елементам.

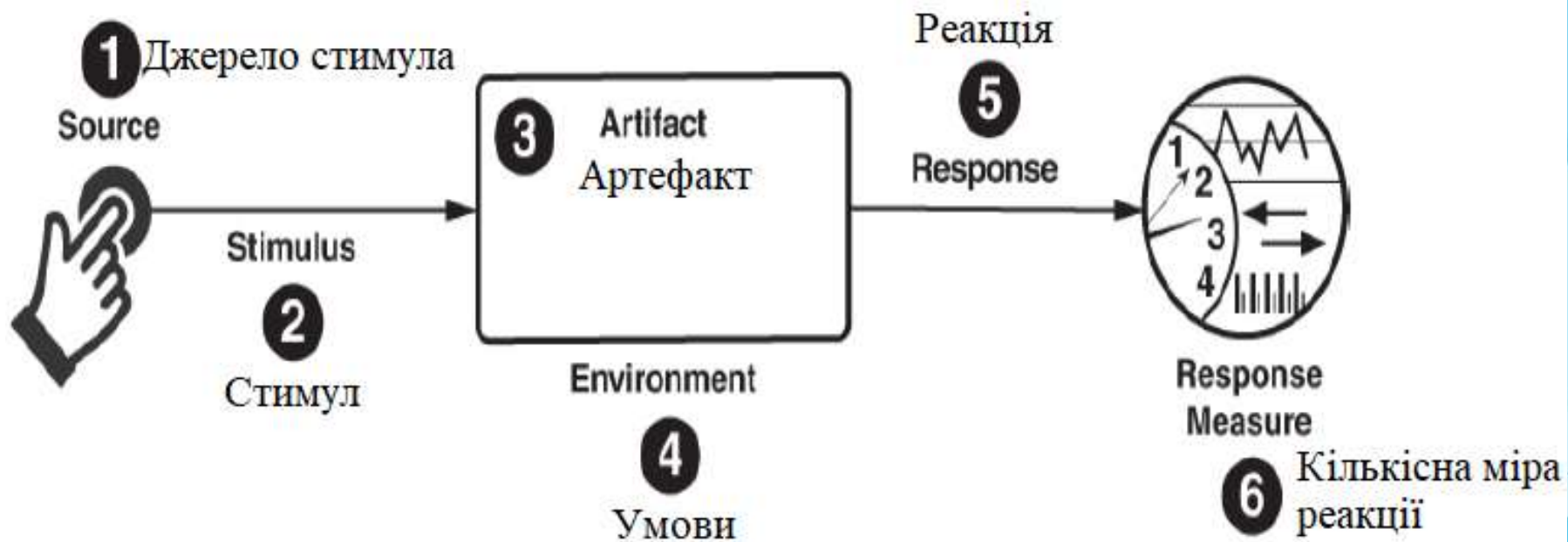
Проблеми оцінки якісних характеристик:

- ▶ Визначення, надані для атрибута, не можливо перевірити.
Наприклад, система може бути здатною до модифікації щодо одного набору змін і не здатна щодо іншого. Система може бути надійною щодо одних недоліків і ненадійною щодо інших.
- ▶ Рішенням проблеми є використання сценаріїв атрибутів якості
- ▶ Досягнення одних якісних атрибутів завжди впливає на покращення чи погіршення інших.
Наприклад, покращення майже усіх атрибутів якості негативно впливає на продуктивність.

Сценарії атрибутів якості

- ▶ **Сценарій атрибуту якості** - вимога, шляхом виконання якої цей атрибут реалізується. Сценарій складається з 6 елементів:
- ▶ **Джерело стимулу (*Stimulus source*)** - деякий суб'єкт (людина, обчислювальна система чи інший), який породжує стимул.
- ▶ **Стимул (*Stimulus*)** - явище, що спостерігається у системі, та вимагає до себе уваги.
- ▶ **Артефакт.** Об'єктом дії стимулу є деякий артефакт. У якості нього може виступати як система в цілому, так і її окремі елементи.
- ▶ **Умови.** Стимул виникає у певних умовах. Наприклад, система може знаходитись у стані перевантаження чи у звичайному режимі.
- ▶ **Реакція (*Response*)** - це дія, здійснена у відповідь на появу стимула.
- ▶ **Кількісна міра реакції (*Response measure*)**. Здійснені у відповідь на стимул дії повинні бути можливими для вимірювання. Лише так відповідність можна перевірити.

Сценарії атрибутів якості

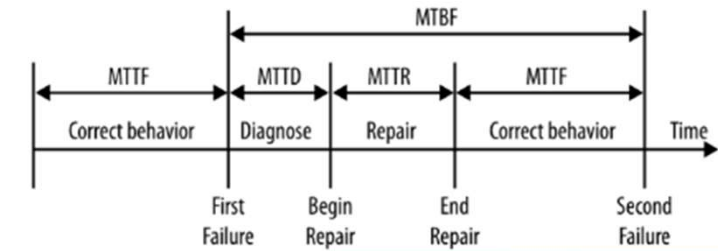


Availability (Готовність)

- ▶ **Готовність** відноситься до властивості програмного забезпечення, що воно готове виконувати своє завдання у час, коли це потрібно.
- ▶ Розраховується як

$$\alpha = \frac{\text{середній_час_між_відмовами}(MTBF)}{\text{середній_час_між_відмовами}(MTBF) + \text{середній_час_відновлення}(MTTR)}$$

- ▶ Планове простоювання системи не враховують - вважається, що в ці моменти вона не потрібна.
- ▶ Відмова (failure) - це стан, у якому система втрачає здатність надання послуг, заявлених у специфікації.
- ▶ **Чи є різниця між несправністю (Fault) та відмовою (Failure)?**
- ▶ Користувач системи може спостерігати відмову, але про несправність він не має уявлення. Коли несправність стає видимою для користувача, вона стає відмовою.
- ▶ Якщо код, де спостерігається несправність, виконується, а потім система усуває наслідки цієї несправності, не виводячи її на зовнішній рівень, відмови не відбувається.



Post-factum (easy)

Uptime / (Uptime + Downtime)

N nines

99.9% -- 8.77 hour/year

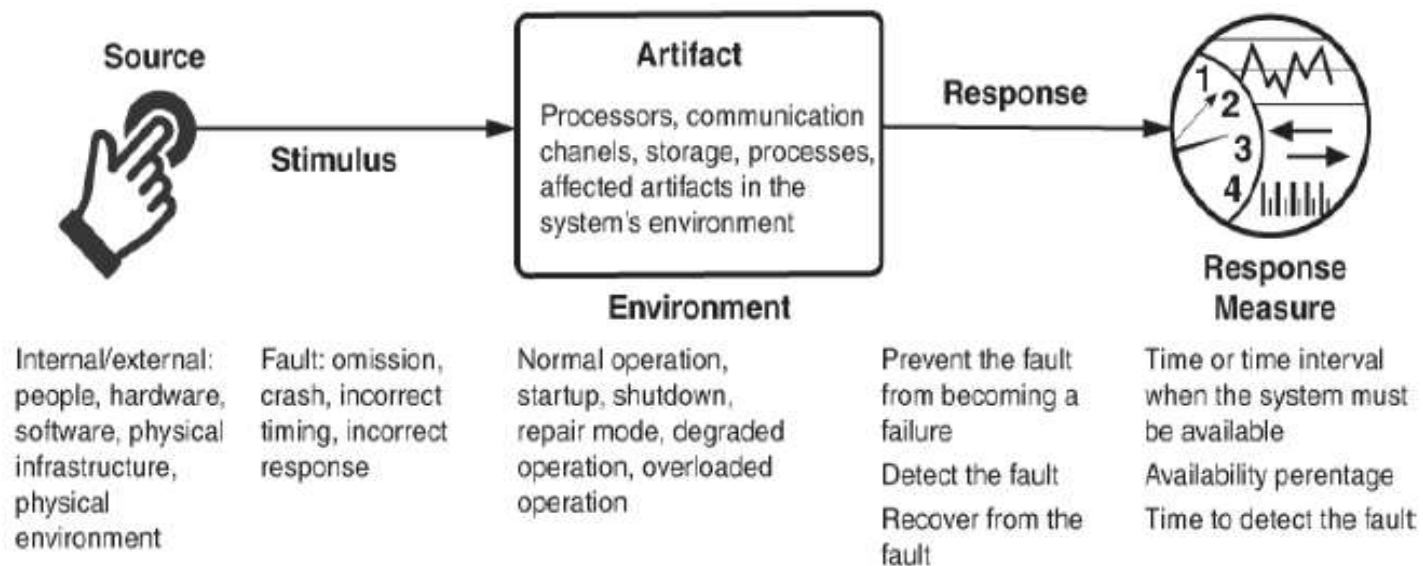
99.99% -- 52.6 min/year

99.999% -- 5.26 min/year

In advance (difficult):

MTBF / (MTBF + MTTR)

Приклад сценарію Availability

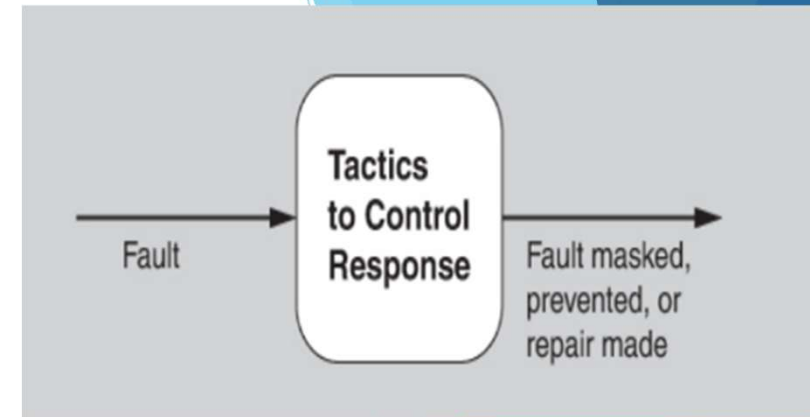
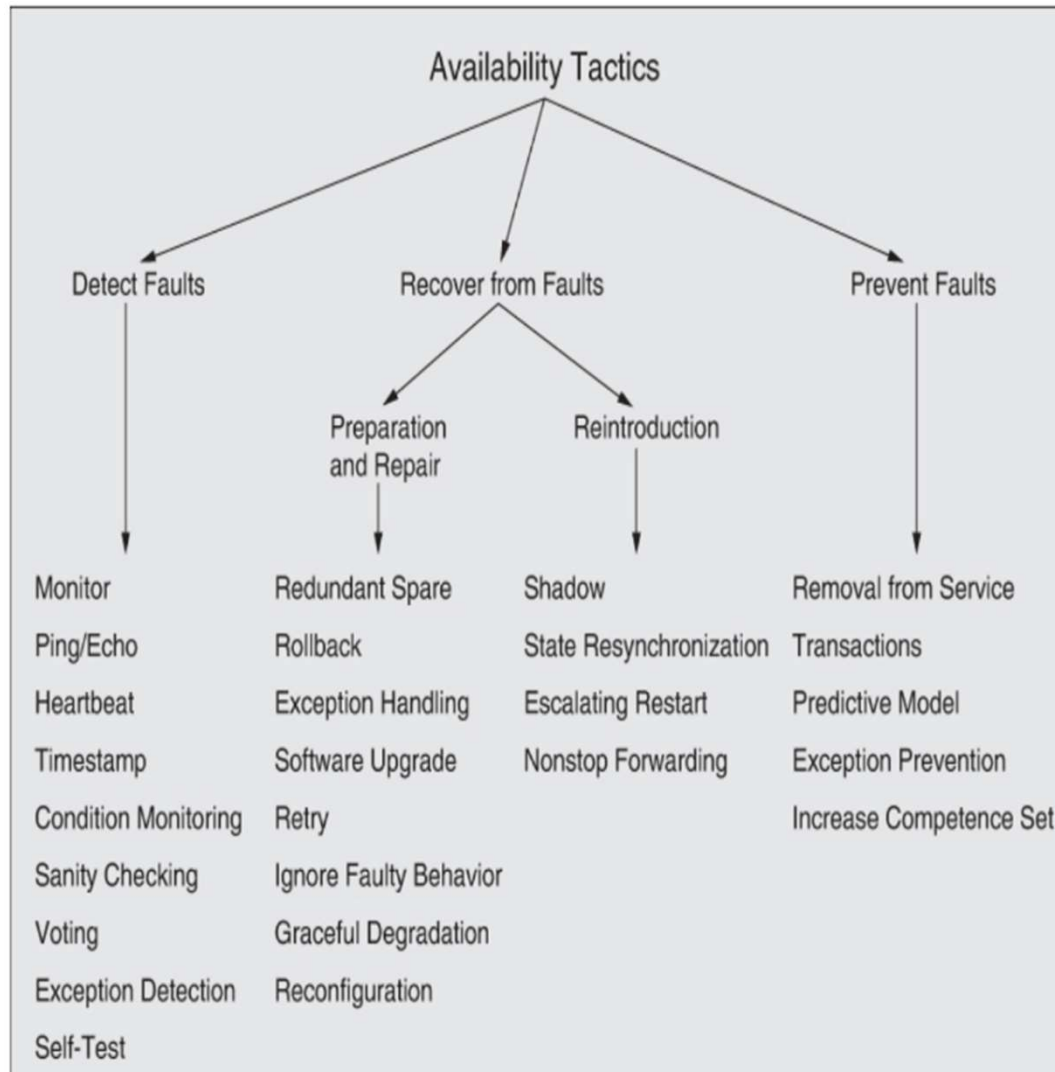


Загальний сценарій Availability

Portion of Scenario	Description	Possible Values
Source	This specifies where the fault comes from.	Internal/external: people, hardware, software, physical infrastructure, physical environment
Stimulus	The stimulus to an availability scenario is a fault.	Fault: omission, crash, incorrect timing, incorrect response
Artifact	This specifies which portions of the system are responsible for and affected by the fault.	Processors, communication channels, storage, processes, affected artifacts in the system's environment
Environment	We may be interested in not only how a system behaves in its "normal" environment, but also how it behaves in situations such as when it is already recovering from a fault.	Normal operation, startup, shutdown, repair mode, degraded operation, overloaded operation
Response	The most commonly desired response is to prevent the fault from becoming a failure, but other responses may also be important, such as notifying people or logging the fault for later analysis. This section specifies the desired system response.	Prevent the fault from becoming a failure Detect the fault: <ul style="list-style-type: none"> Log the fault Notify the appropriate entities (people or systems) Recover from the fault Disable the source of events causing the fault Be temporarily unavailable while a repair is being effected Fix or mask the fault/failure or contain the damage it causes Operate in a degraded mode while a repair is being effected

Portion of Scenario	Description	Possible Values
Response measure	We may focus on a number of measures of availability, depending on the criticality of the service being provided.	<ul style="list-style-type: none"> Time or time interval when the system must be available Availability percentage (e.g., 99.999 per cent) Time to detect the fault Time to repair the fault Time or time interval in which system can be in degraded mode Proportion (e.g., 99 percent) or rate (e.g., up to 100 per second) of a certain class of faults that the system prevents, or handles without failing

Тактики Availability



Modifiability (здатність до модифікації)

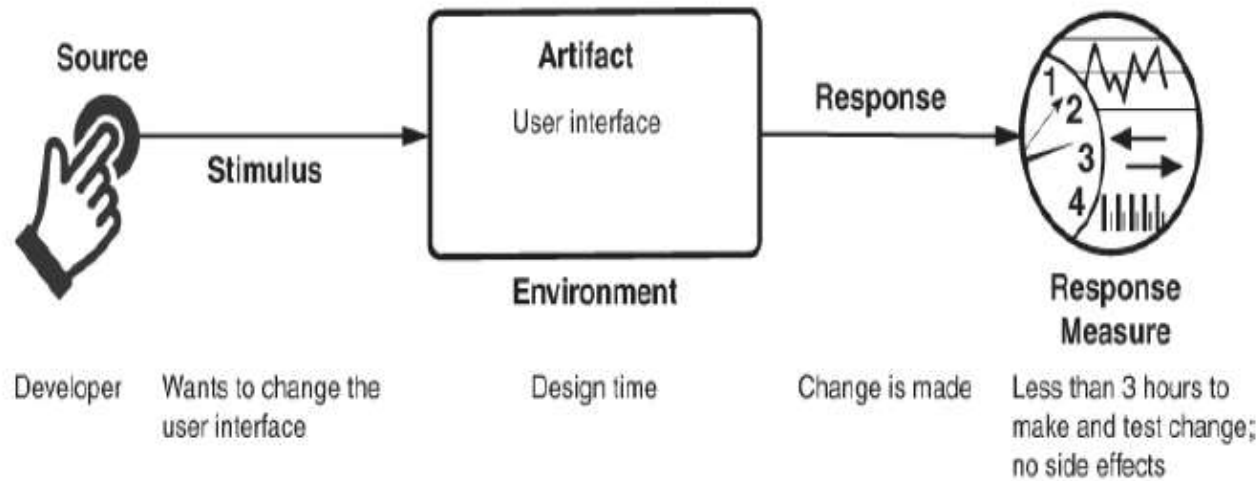
- ▶ Суть **modifiability** - зменшення коштів та ризиків при впровадженні змін.
- ▶ *Що може змінюватись?*
- ▶ Функції системи, платформа (апаратна частина, операційна система), системи, з якими взаємодіє система, протоколи, за допомогою яких обмінюється інформацією, атрибути якості, можливості (кількість користувачів, одночасних операцій) і.т.д.
- ▶ *Хто виконує модифікацію?*
- ▶ Розробники, кінцеві користувачі та адміни. Раніше розробник вносив інформацію у код, виконував модифікацію, яка тестувалася та впроваджувалась у новій версії.
Зараз модифікованість все більше покладається на кінцевого користувача: зміна заставки, вибір тих чи інших бібліотек, налаштування конфігурації.

Modifiability

- ▶ Забезпечення модифікованості системи складається з двох значень:
 - Вартість запровадження механізму(ів), щоб зробити систему більш здатною до модифікації
 - Вартість здійснення модифікації за допомогою механізму(ів)
- ▶ Поширені терміни, що відносяться до модифікованості:
- ▶ Масштабованість (scalability) полягає в розміщенні більшої кількості елементів.
- ▶ Варіативність означає здатність системи та її допоміжних артефактів (код, вимоги, плани тестування та документація) підтримувати створення набору варіантів, які відрізняються один від одного визначеним способом
- ▶ Портативність означає легкість, з якою програмне забезпечення, створене для роботи на одній платформі, можна змінити для роботи на іншій платформі.
- ▶ Проектування системи незалежної від розташування (Location independence) означає, що розташування буде легко змінювати з мінімальним впливом на решту системи.

Modifiability. Приклад сценарію.

► Приклад сценарію модифікованості

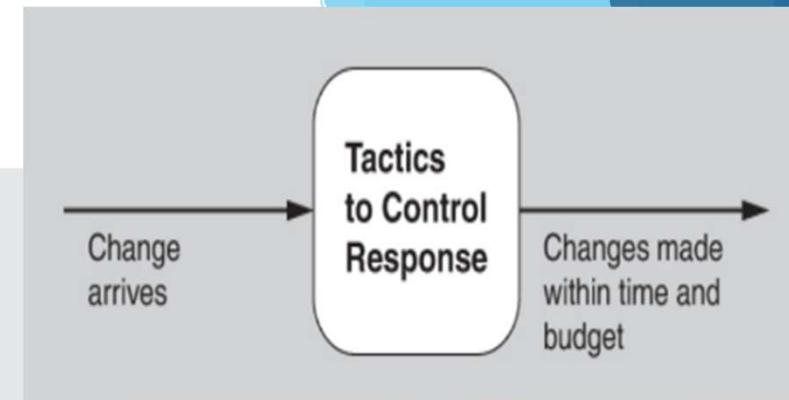
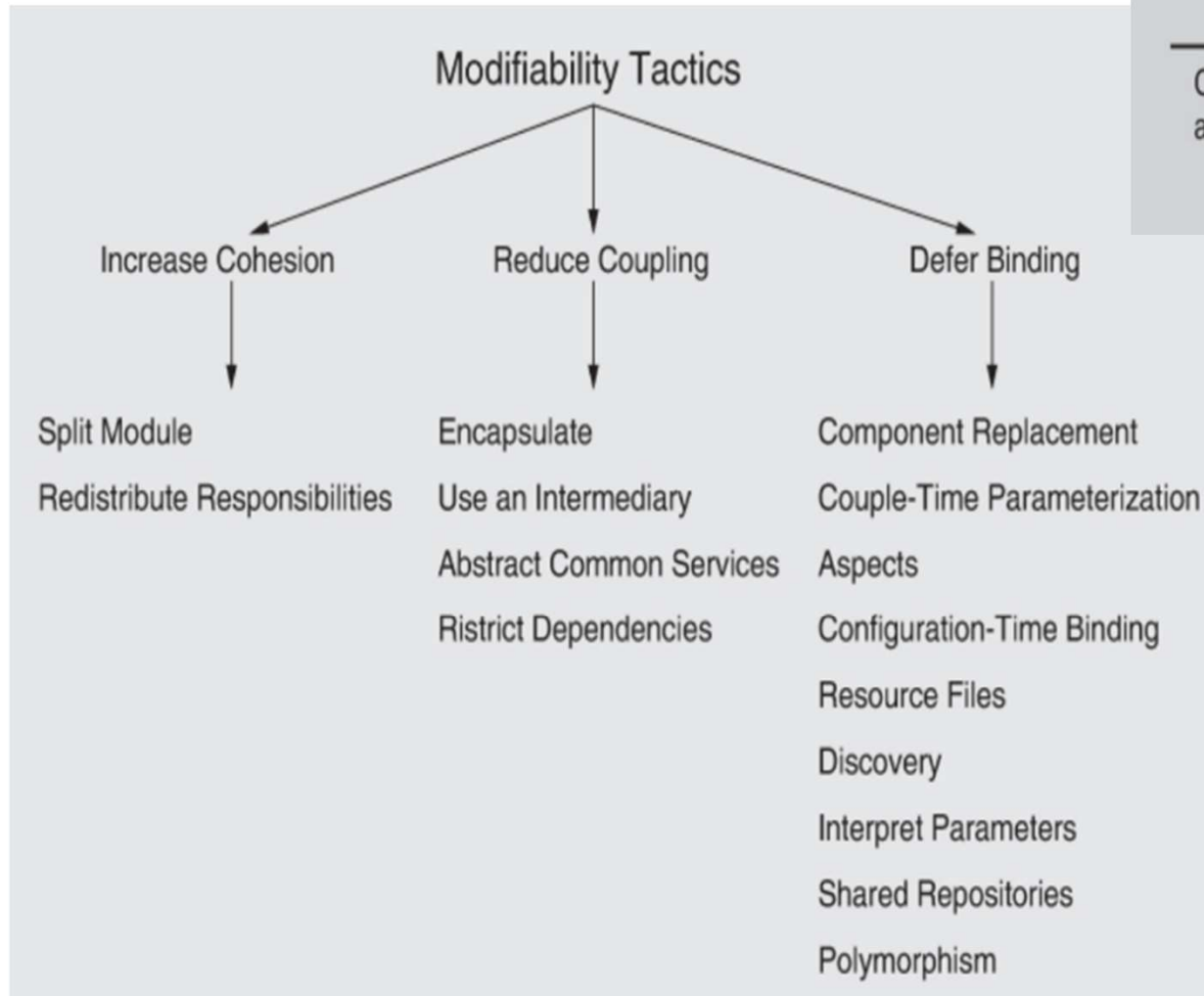


Загальний сценарій Modifiability

Portion of Scenario	Description	Possible Values
Source	The agent that causes a change to be made. Most are human actors, but the system might be one that learns or self-modifies, in which case the source is the system itself.	End user, developer, system administrator, product line owner, the system itself
Stimulus	The change that the system needs to accommodate. (For this categorization, we regard fixing a defect as a change, to something that presumably wasn't working correctly.)	A directive to add/delete/modify functionality, or change a quality attribute, capacity, platform, or technology; a directive to add a new product to a product line; a directive to change the location of a service to another location
Artifacts	The artifacts that are modified. Specific components or modules, the system's platform, its user interface, its environment, or another system with which it interoperates.	Code, data, interfaces, components, resources, test cases, configurations, documentation

Portion of Scenario	Description	Possible Values
Response	Make the change and incorporate it into the system.	One or more of the following: <ul style="list-style-type: none"> • Make modification • Test modification • Deploy modification • Self-modify
Response measure	The resources that were expended to make the change.	Cost in terms of: <ul style="list-style-type: none"> • Number, size, complexity of affected artifacts • Effort • Elapsed time • Money (direct outlay or opportunity cost) • Extent to which this modification affects other functions or quality attributes • New defects introduced • How long it took the system to adapt

Тактики Modifiability

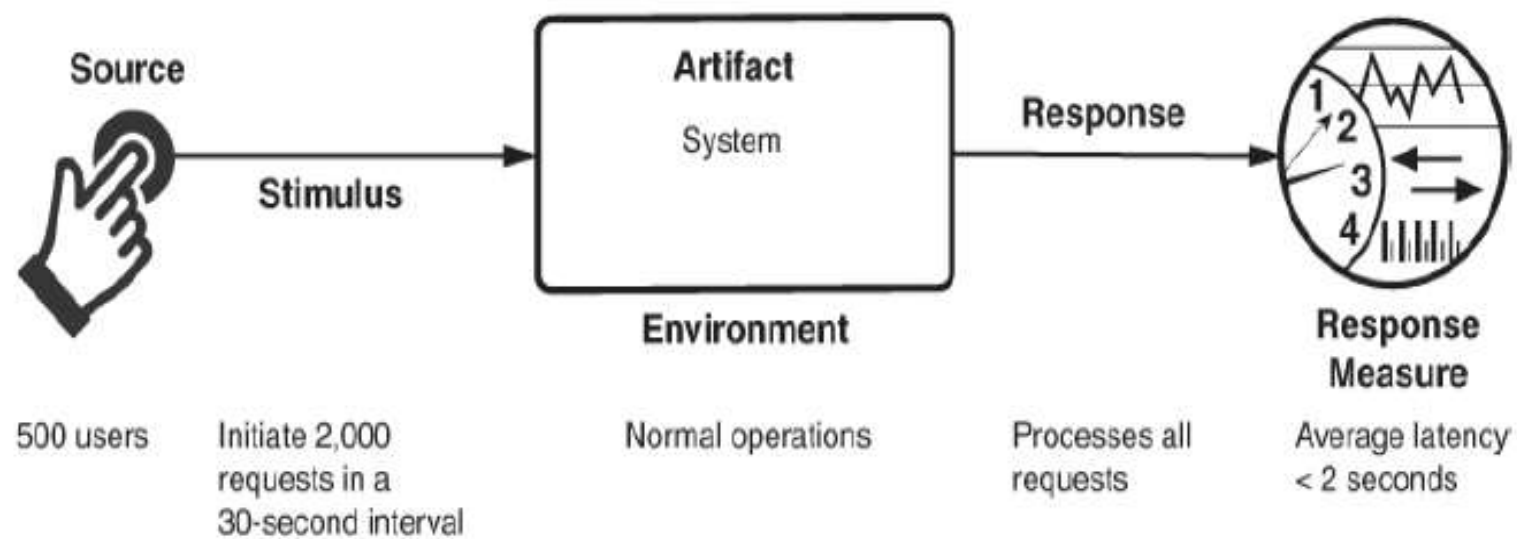


Performance (Продуктивність)

- ▶ **Продуктивність** - характеристика здатності програмної системи відповідати вимогам часу.
- ▶ Час, що витрачається:
 - Обчислення у системі - тисячі наносекунд,
 - доступ до диска (твердотільного чи обертового) - десятки мілісекунд
 - доступ до мережі: у цьому ж центрі обробки даних - від сотень мікросекунд, при міжконтинентальному сполученні - до 100 мілісекунд.
- ▶ Коли відбуваються події (переривання, повідомлення, запити від користувачів чи інших систем або сповіщення годинника, що відзначає плин часу), — система або відповідний її елемент має вчасно на них відповісти.
- ▶ Для веб-систем події надходять у формі запитів від користувачів через їхні клієнти, наприклад веб-браузери.
- ▶ Продуктивність завжди пов'язана з масштабованістю.
- ▶ Паралельність процесів є однією з найважливіших концепцій, яку повинен розуміти архітектор.

Performance

► Приклад сценарію продуктивності

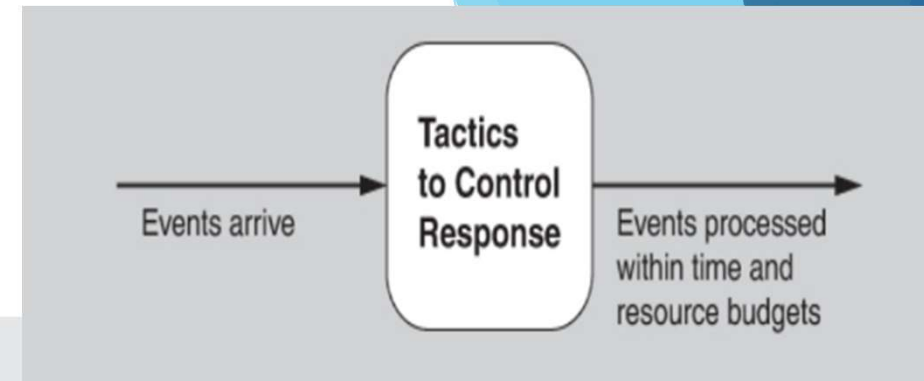
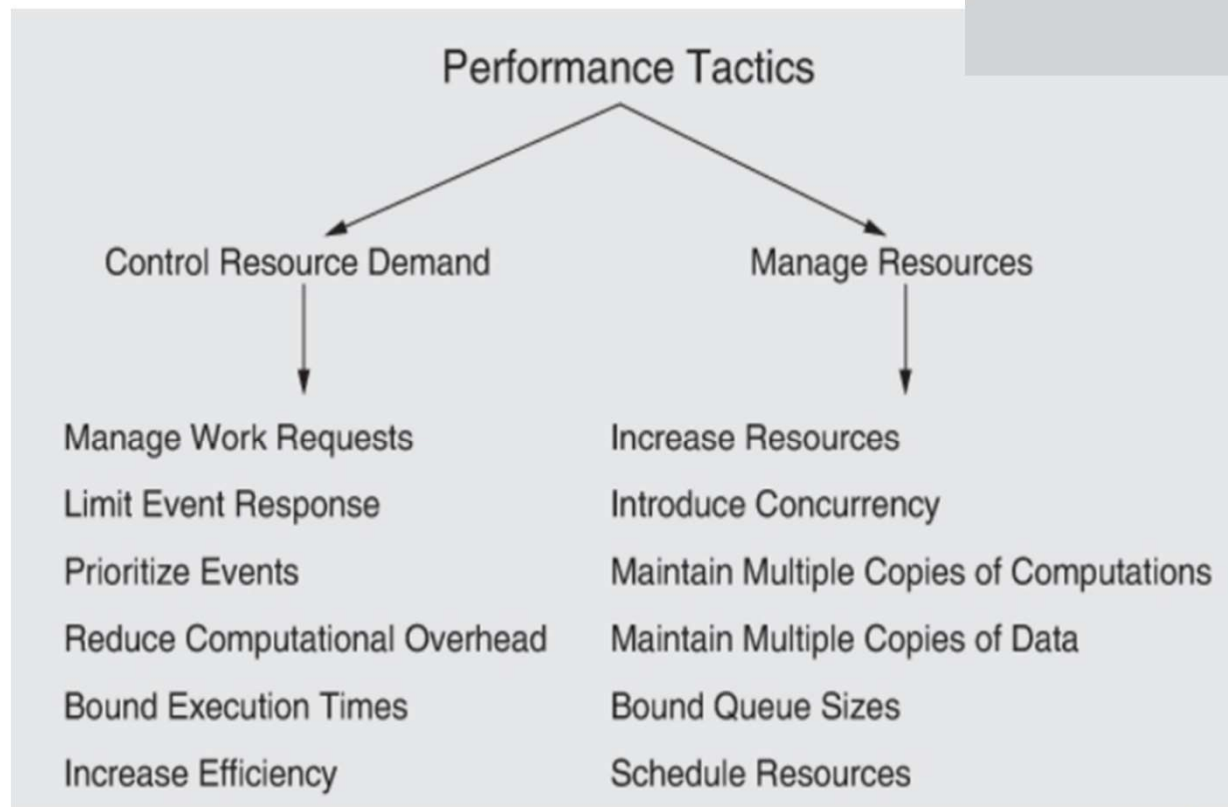


Загальний сценарій Performance

Portion of Scenario	Description	Possible Values
Source	The stimulus can come from a user (or multiple users), from an external system, or from some portion of the system under consideration.	<p>External:</p> <ul style="list-style-type: none"> • User request • Request from external system • Data arriving from a sensor or other system <p>Internal:</p> <ul style="list-style-type: none"> • One component may make a request of another component. • A timer may generate a notification.
Stimulus	The stimulus is the arrival of an event. The event can be a request for service or a notification of some state of either the system under consideration or an external system.	<p>Arrival of a periodic, sporadic, or stochastic event:</p> <ul style="list-style-type: none"> • A periodic event arrives at a predictable interval. • A stochastic event arrives according to some probability distribution. • A sporadic event arrives according to a pattern that is neither periodic nor stochastic.
Artifact	The artifact stimulated may be the whole system or just a portion of the system. For example, a power-on event may stimulate the whole system. A user request may arrive at (stimulate) the user interface.	<ul style="list-style-type: none"> • Whole system • Component within the system

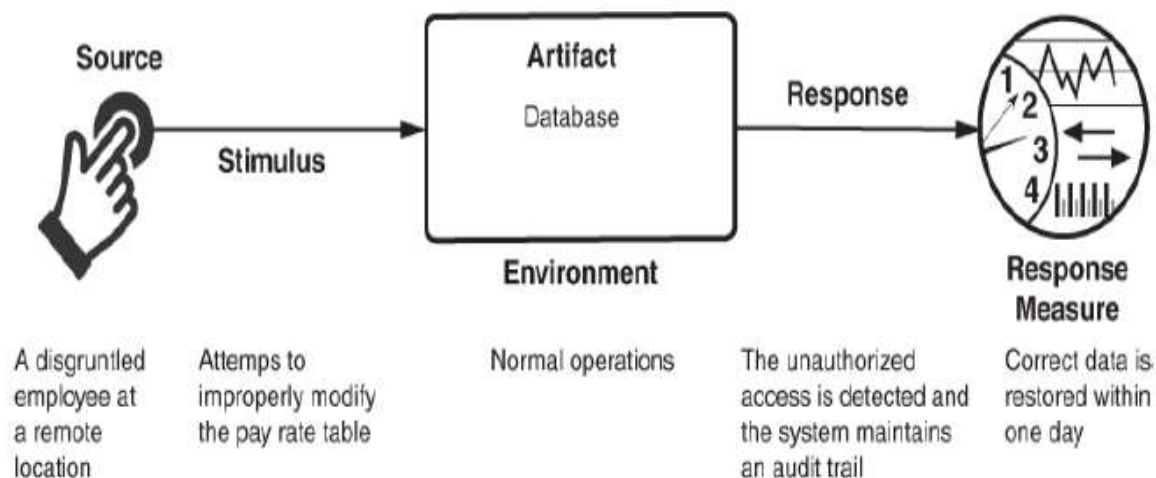
Portion of Scenario	Description	Possible Values
Environment	The state of the system or component when the stimulus arrives. Unusual modes—error mode, overloaded mode—will affect the response. For example, three unsuccessful login attempts are allowed before a device is locked out.	<p>Runtime. The system or component can be operating in:</p> <ul style="list-style-type: none"> • Normal mode • Emergency mode • Error correction mode • Peak load • Overload mode • Degraded operation mode • Some other defined mode of the system
Response	The system will process the stimulus. Processing the stimulus will take time. This time may be required for computation or it may be required because processing is blocked by contention for shared resources. Requests can fail to be satisfied because the system is overloaded or because of a failure somewhere in the processing chain.	<ul style="list-style-type: none"> • System returns a response • System returns an error • System generates no response • System ignores the request if overloaded • System changes the mode or level of service • System services a higher-priority event • System consumes resources
Response measure	Timing measures can include latency or throughput. Systems with timing deadlines can also measure jitter of response and ability to meet the deadlines. Measuring how many of the requests go unsatisfied is also a type of measure, as is how much of a computing resource (e.g., a CPU, memory, thread pool, buffer) is utilized.	<ul style="list-style-type: none"> • The (maximum, minimum, mean, median) time the response takes (latency) • The number or percentage of satisfied requests over some time interval (throughput) or set of events received • The number or percentage of requests that go unsatisfied • The variation in response time (jitter) • Usage level of a computing resource

Тактики Performance



Security (Безпека)

- ▶ **Безпека** - відображає здатність системи протистояти намаганням несанкціонованого доступу при одночасному обслуговування легальних користувачів.
- ▶ **Атака** - намагання порушити систему захисту. Вони можуть бути спрямовані на отримання доступу до даних, послуг чи зміні даних або - на перешкоджання обслуговування легальних користувачів.
- ▶ Безпеку можна виділити як атрибут якості системи, що передбачає суворе виконання обов'язків, конфіденційність, цілісність, гарантування, готовність та аудит.

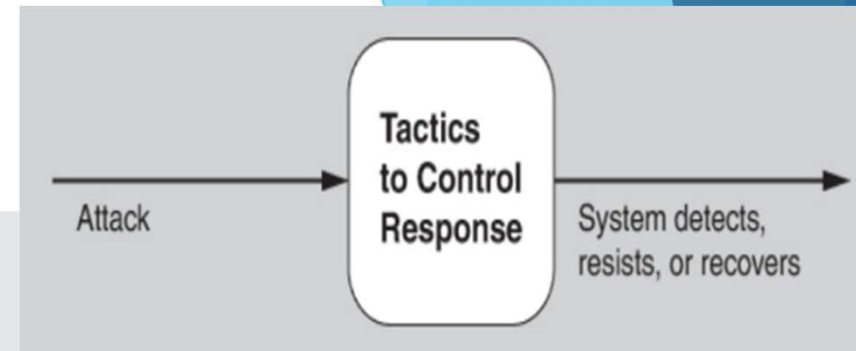
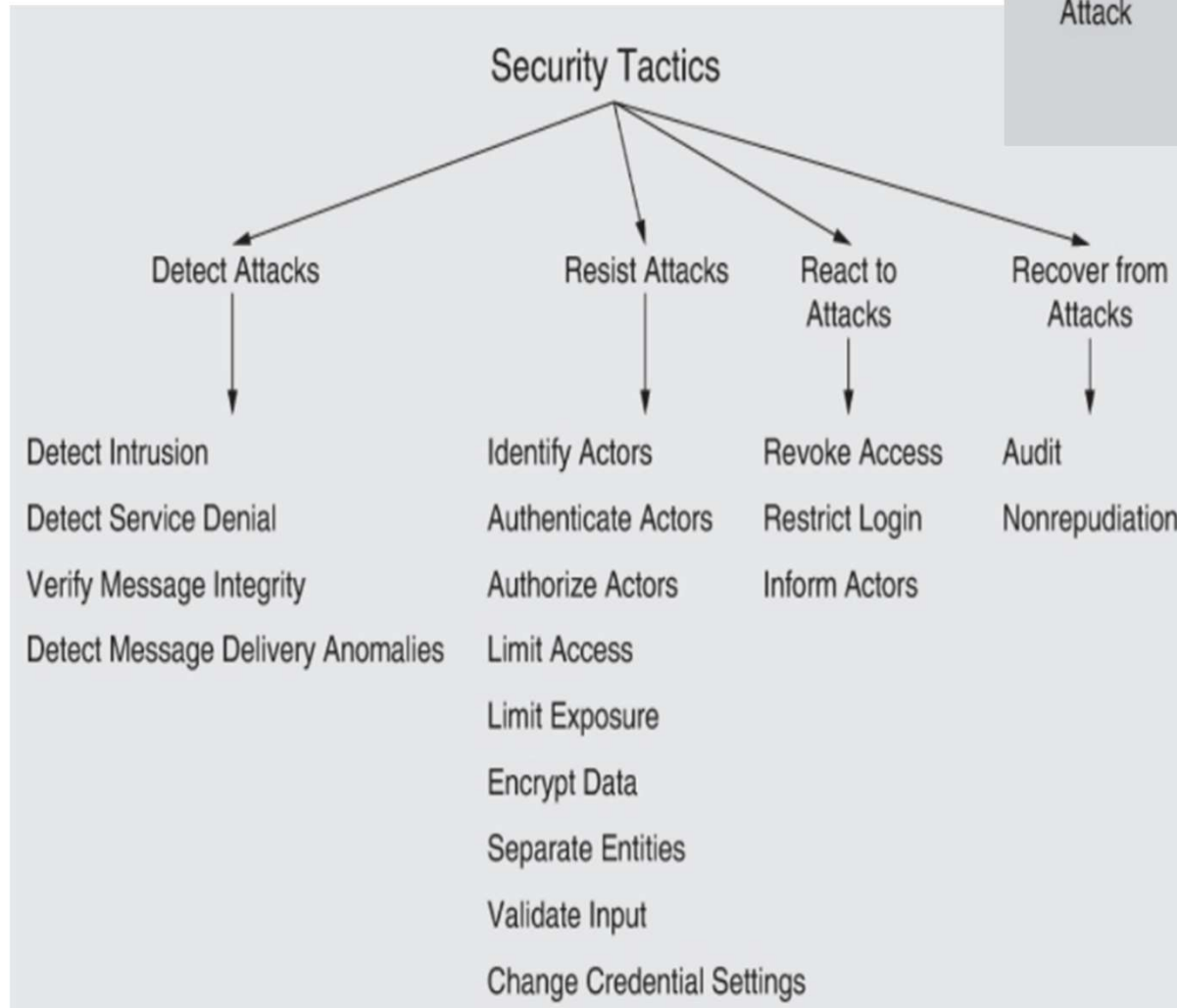


Загальний сценарій безпеки

Portion of Scenario	Description	Possible Values
Source	The attack may be from outside the organization or from inside the organization. The source of the attack may be either a human or another system. It may have been previously identified (either correctly or incorrectly) or may be currently unknown.	<ul style="list-style-type: none"> • Human • Another system which is: <ul style="list-style-type: none"> • Inside the organization • Outside the organization • Previously identified • Unknown
Stimulus	The stimulus is an attack.	An unauthorized attempt to: <ul style="list-style-type: none"> • Display data • Capture data • Change or delete data • Access system services • Change the system's behavior • Reduce availability
Artifact	What is the target of the attack?	<ul style="list-style-type: none"> • System services • Data within the system • A component or resources of the system • Data produced or consumed by the system
Environment	What is the state of the system when the attack occurs?	The system is: <ul style="list-style-type: none"> • Online or offline • Connected to or disconnected from a network • Behind a firewall or open to a network • Fully operational • Partially operational • Not operational

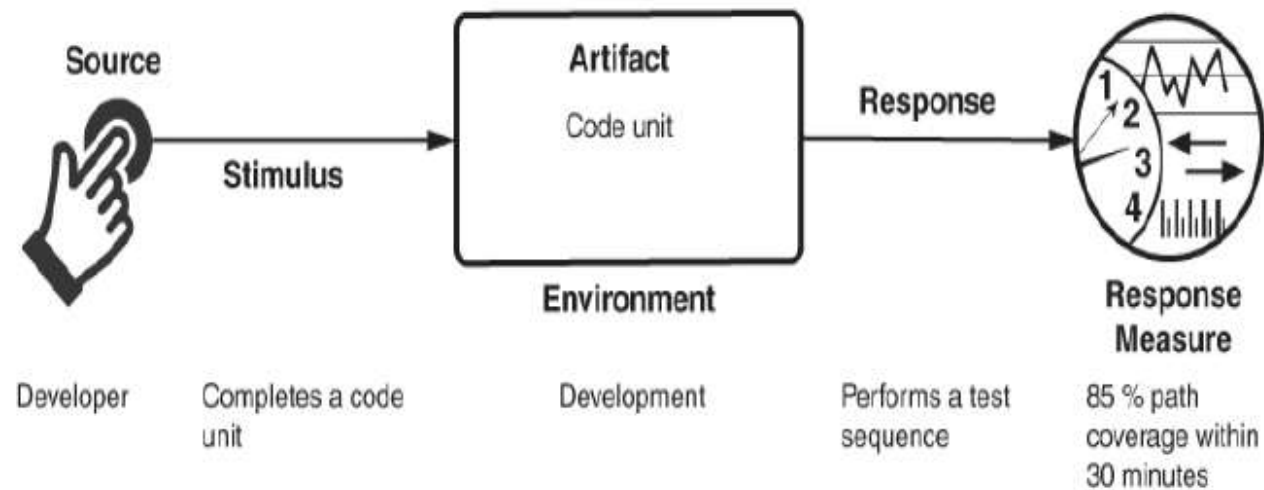
Portion of Scenario	Description	Possible Values
Response	The system ensures that confidentiality, integrity, and availability are maintained.	Transactions are carried out in a fashion such that <ul style="list-style-type: none"> • Data or services are protected from unauthorized access • Data or services are not being manipulated without authorization • Parties to a transaction are identified with assurance • The parties to the transaction cannot repudiate their involvements • The data, resources, and system services will be available for legitimate use The system tracks activities within it by <ul style="list-style-type: none"> • Recording access or modification • Recording attempts to access data, resources, or services • Notifying appropriate entities (people or systems) when an apparent attack is occurring
Response measure	Measures of a system's response are related to the frequency of successful attacks, the time and cost to resist and repair attacks, and the consequential damage of those attacks.	One or more of the following: <ul style="list-style-type: none"> • How much of a resource is compromised or ensured • Accuracy of attack detection • How much time passed before an attack was detected • How many attacks were resisted • How long it takes to recover from a successful attack • How much data is vulnerable to a particular attack

Тактики Security



Контролепридатність (testability)

- ▶ Контролепридатність - здатність до демонстрування несправностей шляхом тестування.

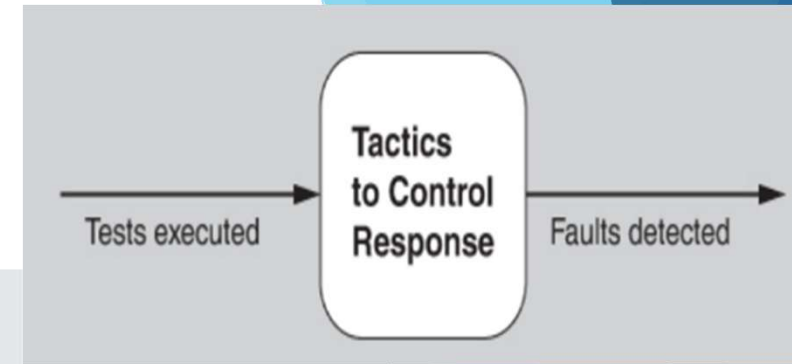
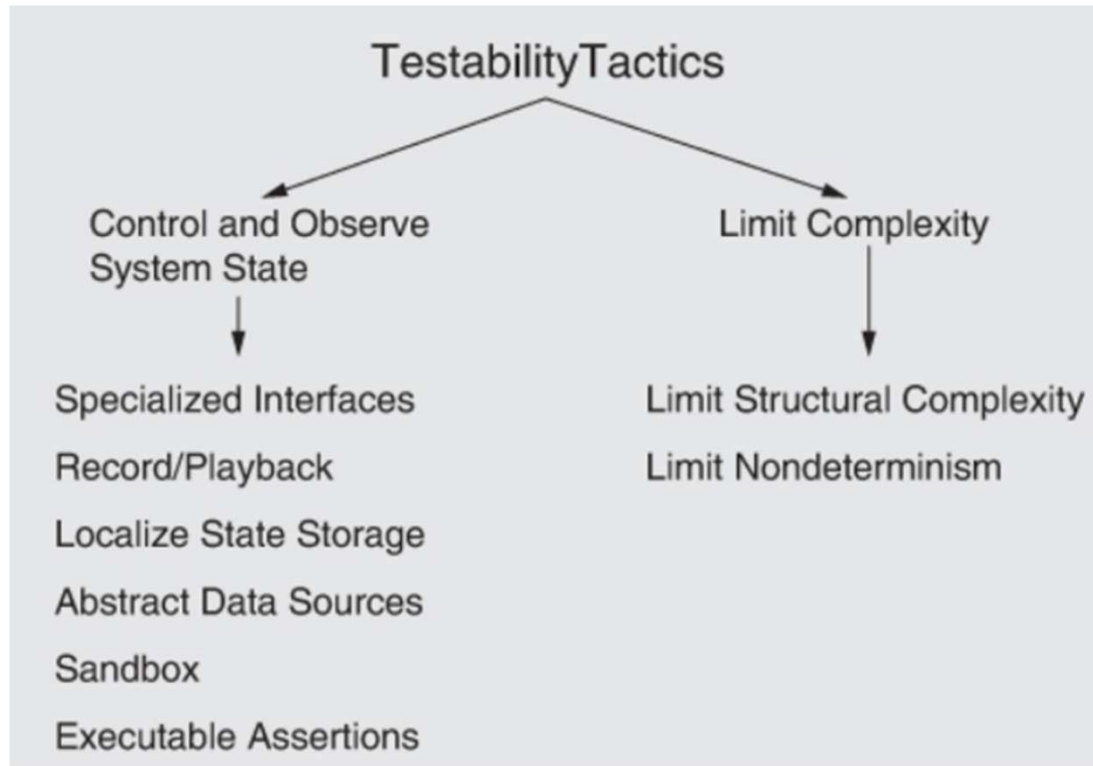


Загальний сценарій контролепридатності

Portion of Scenario	Description	Possible Values
Source	The test cases can be executed by a human or an automated test tool.	<ul style="list-style-type: none"> • Unit testers • Integration testers • System testers • Acceptance testers • End users <p>Either run tests manually or use automated testing tools</p>
Stimulus	A test or set of tests is initiated.	<p>These tests serve to:</p> <ul style="list-style-type: none"> • Validate system functions • Validate qualities • Discover emerging threats to quality
Environment	Testing occurs at various events or life-cycle milestones.	<p>The set of tests is executed due to:</p> <ul style="list-style-type: none"> • The completion of a coding increment such as a class, layer, or service • The completed integration of a subsystem • The complete implementation of the whole system • The deployment of the system into a production environment • The delivery of the system to a customer • A testing schedule
Artifacts	The artifact is the portion of the system being tested and any required test infrastructure.	<p>The portion being tested:</p> <ul style="list-style-type: none"> • A unit of code (corresponding to a module in the architecture) • Components • Services • Subsystems • The entire system <p>The test infrastructure</p>

Portion of Scenario	Description	Possible Values
Response	The system and its test infrastructure can be controlled to perform the desired tests and the results from the test can be observed.	<p>One or more of the following:</p> <ul style="list-style-type: none"> • Execute test suite and capture results • Capture activity that resulted in the fault • Control and monitor the state of the system
Response measure	Response measures are aimed at representing how easily a system under test “gives up” its faults or defects.	<p>One or more of the following:</p> <ul style="list-style-type: none"> • Effort to find an faults or class of faults • Effort to achieve a given percentage of state space coverage • Probability of a fault being revealed by the next test • Time to perform tests • Effort to detect faults • Length of time to prepare test infrastructure • Effort required to bring the system into a specific state • Reduction in risk exposure: $\text{size}(\text{loss}) \times \text{prob}(\text{loss})$

Тактики Testability



Зручність використання (usability)

- ▶ Практичність виражає ступінь складності виконання користувачем задачі, зо перед ним стоїть, та тип реалізованого у системі механізму допомоги користувачу. Сторони, що включає цей атрибут:
- ▶ Вивчення можливостей системи. Яким вином можна полегшити задачу користувача, пов'язану з вивченням незнайомої системи чи одного з її аспектів.
 1. *Ефективне використання системи.* Яким чином система сприяє підвищенню ефективності роботи з нею?
 2. *Мінімізація наслідків помилок.* Що система може зробити, щоб помилка, допущена користувачем, не призвела до серйозних наслідків?
 3. *Адаптація системи до потреб користувача.* Що може зробити користувач, щоб виконати його задачу стало простіше?
 4. *Впевненість та задоволення користувача.* Як система може впевнити користувача, що він виконав вірну дію?

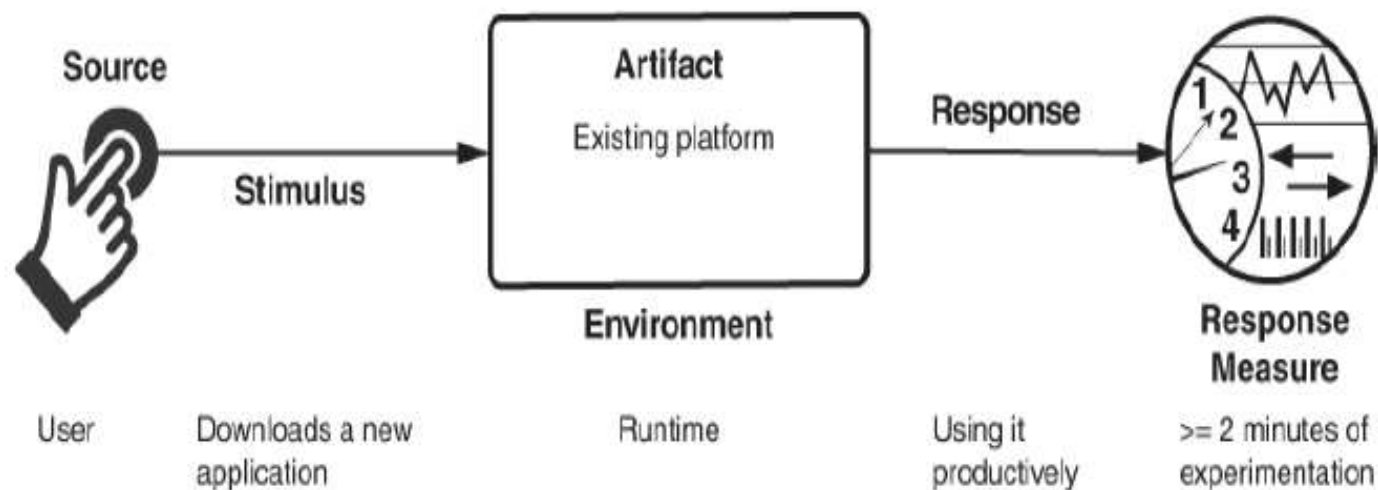
Загальний сценарій Usability

Portion of Scenario	Description	Possible Values
Source	Where does the stimulus come from?	The end user (who may be in a specialized role, such as a system or network administrator) is the primary source of the stimulus for usability. An external event arriving at a system (to which the user may react) may also be a stimulus source.
Stimulus	What does the end user want?	End user wants to: <ul style="list-style-type: none"> ▪ Use a system efficiently ▪ Learn to use the system ▪ Minimize the impact of errors ▪ Adapt the system ▪ Configure the system
Environment	When does the stimulus reach the system?	The user actions with which usability is concerned always occur at runtime or at system configuration time.
Artifacts	What portion of the system is being stimulated?	Common examples include: <ul style="list-style-type: none"> ▪ A GUI ▪ A command-line interface ▪ A voice interface ▪ A touch screen

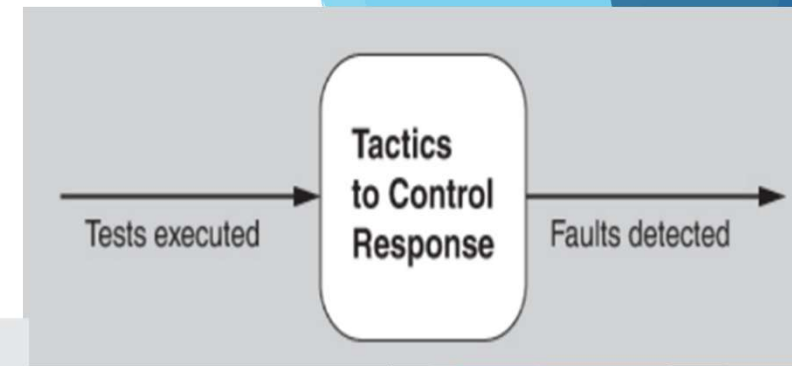
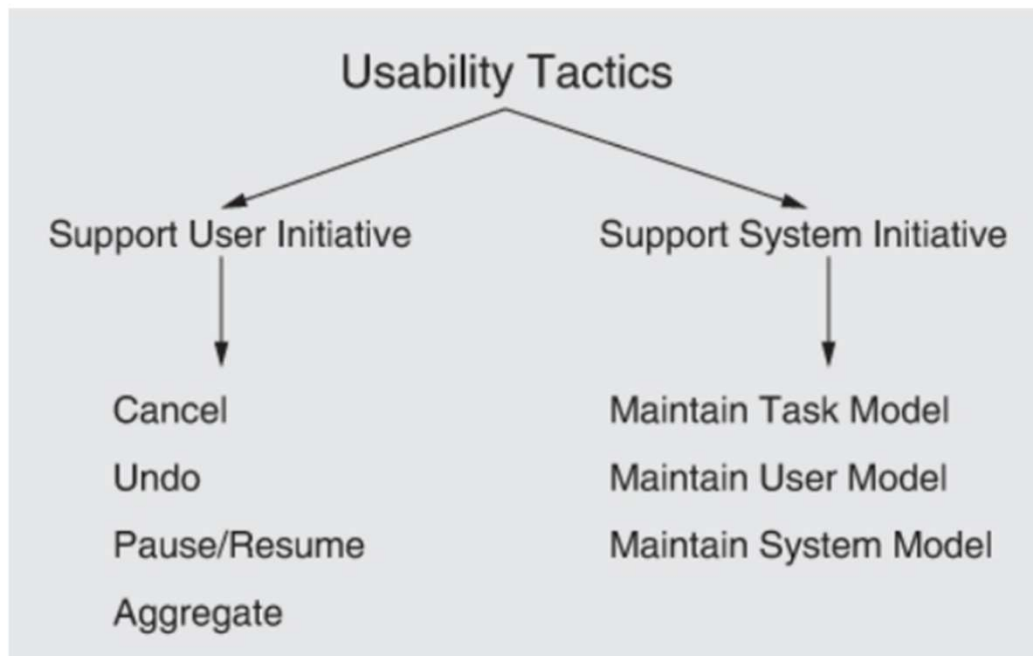
Portion of Scenario	Description	Possible Values
Response	How should the system respond?	The system should: <ul style="list-style-type: none"> ▪ Provide the user with the features needed ▪ Anticipate the user's needs ▪ Provide appropriate feedback to the user
Response measure	How is the response measured?	One or more of the following: <ul style="list-style-type: none"> ▪ Task time ▪ Number of errors ▪ Learning time ▪ Ratio of learning time to task time ▪ Number of tasks accomplished ▪ User satisfaction ▪ Gain of user knowledge ▪ Ratio of successful operations to total operations ▪ Amount of time or data lost when an error occurs

Приклад сценарію Usability

- ▶ Користувач завантажує новий додаток і використовує його продуктивно після 2 хвилин експерименту.



Тактики Usability

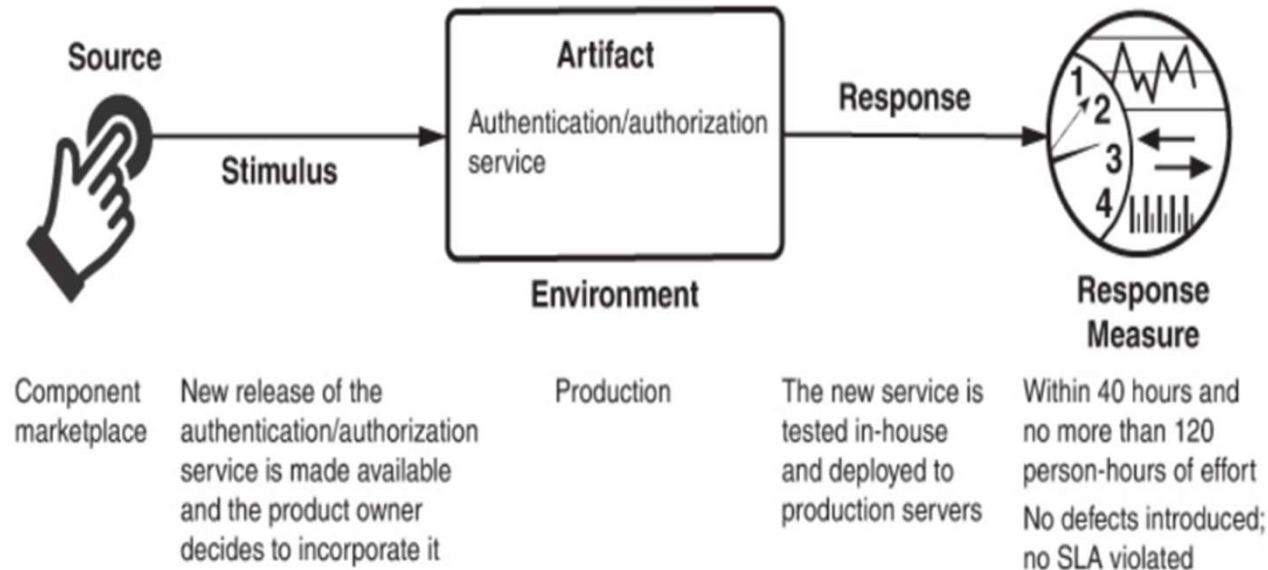


Стимули атрибутів якості

Атрибут якості	Стимул
Готовність	Непередбачена подія, ненадходження очікуваної події
Модифікованість	Вимога по додаванню/видаленню/зміні/видозміні функціональності, платформи, атрибуту якості, потужності
Продуктивність	Періодичний, неперіодичний, випадковий
Безпека	Намагання продивитись, відкоригувати, змінити/видалити інформацію, отримати доступ до системних служб чи понизити рівень їх готовності
Контролепридатність	Завершення етапа розробки системи
Практичність	Намір вивчити можливості систем, добитись ефективного використання системи, мінімізувати наслідки допущених помилок, підлаштувати систему під свої потреби, забезпечити зручність користування системою.

Deployability (можливість розгортання)

- ▶ **Розгортання** — це процес, який починається з кодування та закінчується взаємодією реальних користувачів із системою у робочому середовищі.
- ▶ Якщо цей процес повністю автоматизований, тобто без втручання людини, він називається **continuous deployment** (безперервним розгортанням). Якщо процес автоматизовано до моменту розміщення (частини) системи у виробництві та для цього останнього етапу потрібне втручання людини, процес називається **continuous deliverv** (безперервною поставкою).

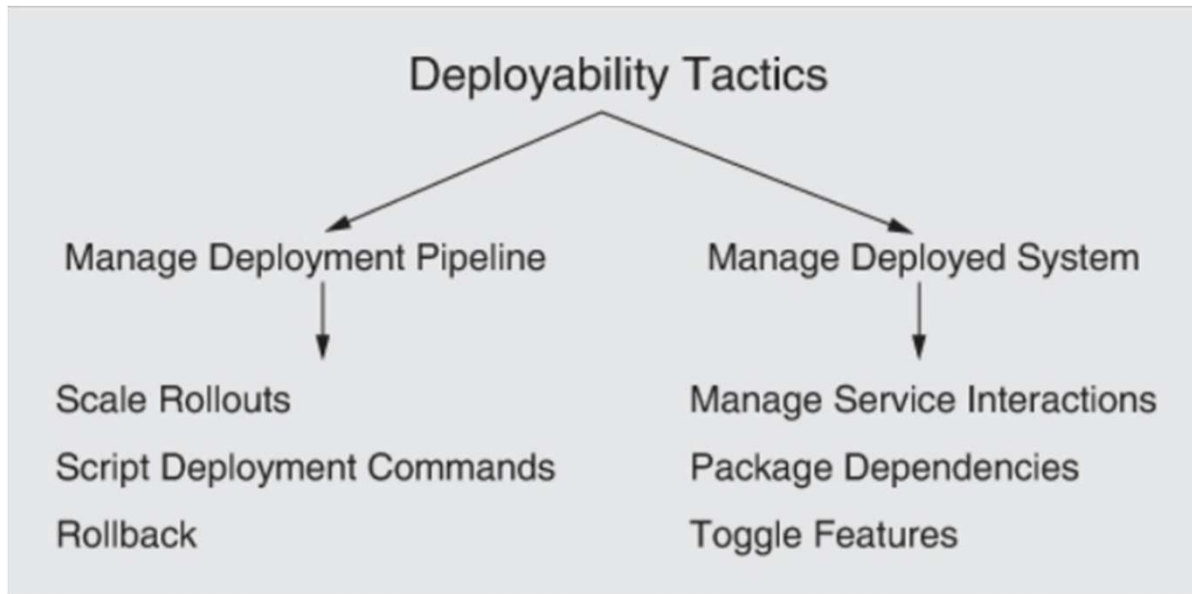


Загальний сценарій можливості розгортання

Portion of Scenario	Description	Possible Values
Source	The trigger for the deployment	End user, developer, system administrator, operations personnel, component marketplace, product owner.
Stimulus	What causes the trigger.	<p>A new element is available to be deployed. This is typically a request to replace a software element with a new version (e.g., fix a defect, apply a security patch, upgrade to the latest release of a component or framework, upgrade to the latest version of an internally produced element).</p> <p>New element is approved for incorporation.</p> <p>An existing element/set of elements needs to be rolled back.</p>
Artifacts	What is to be changed	Specific components or modules, the system's platform, its user interface, its environment, or another system with which it interoperates. Thus the artifact might be a single software element, multiple software elements, or the entire system.
Environment	Staging, production (or a specific subset of either)	<p>Full deployment.</p> <p>Subset deployment to a specified portion of: users, VMs, containers, servers, platforms.</p>

Portion of Scenario	Description	Possible Values
Response	What should happen	<p>Incorporate the new components.</p> <p>Deploy the new components.</p> <p>Monitor the new components.</p> <p>Roll back a previous deployment.</p>
Response measure	A measure of cost, time, or process effectiveness for a deployment, or for a series of deployments over time	<p>Cost in terms of:</p> <ul style="list-style-type: none"> • Number, size, and complexity of affected artifacts • Average/worst-case effort • Elapsed clock or calendar time • Money (direct outlay or opportunity cost) • New defects introduced <p>Extent to which this deployment/rollback affects other functions or quality attributes.</p> <p>Number of failed deployments.</p> <p>Repeatability of the process.</p> <p>Traceability of the process.</p> <p>Cycle time of the process.</p>

Тактики можливості розгортання



Загальний сценарій Integrability

Portion of Scenario	Description	Possible Values
Source	Where does the stimulus come from?	One or more of the following: <ul style="list-style-type: none"> ▪ Mission/system stakeholder ▪ Component marketplace ▪ Component vendor
Stimulus	What is the stimulus? That is, what kind of integration is being described?	One of the following: <ul style="list-style-type: none"> ▪ Add new component ▪ Integrate new version of existing component ▪ Integrate existing components together in a new way
Artifact	What parts of the system are involved in the integration?	One of the following: <ul style="list-style-type: none"> ▪ Entire system ▪ Specific set of components ▪ Component metadata ▪ Component configuration

Portion of Scenario	Description	Possible Values
Environment	What state is the system in when the stimulus occurs?	One of the following: <ul style="list-style-type: none"> ▪ Development ▪ Integration ▪ Deployment ▪ Runtime
Response	How will an “integrable” system respond to the stimulus?	One or more of the following: <p>Changes are {completed, integrated, tested, deployed}</p> <p>Components in the new configuration are successfully collaborating</p> <p>Components in the new configuration do not violate any resource limits</p>
Response measure	How is the response measured?	One or more of the following: <p>Cost, in terms of one or more of:</p> <ul style="list-style-type: none"> ▪ Number of components changed ▪ Percentage of code changed ▪ Lines of code changed ▪ Effort ▪ Money ▪ Calendar time <p>Effects on other quality attribute response measures (to capture allowable tradeoffs)</p>

Тактики Integrability

