Zusammenfassung

**Lernziele**Verteilte Software-Systeme (VSS) sind allgegenwärtig in beruflichem und privatem Alltag; sie führen Konzepte und Technologien aus unterschiedlichen Bereichen der Informatik zusammen. Nach dem Besuch dieses Moduls sind Sie in der Lage, VSS zu analysieren, zu entwerfen und mit Hilfe von Middleware und Frameworks zu realisieren:

* Sie können die charakteristischen Eigenschaften von VSS und die grundlegenden Fragestellungen beim Entwurf von VSS nennen.
* Sie können synchrone Remote Procedure Calls (RPC) und asynchrone Messaging-Kommunikationskanäle konzipieren und implementieren.
* Sie können die Konzepte und Funktionsweisen der wichtigsten Middleware-Dienste zum Bau von VSS erklären und beispielhafte Middleware-Implementierungen vergleichen und bewerten.
* Sie können operationale Infrastrukturen für verteilte Systeme unter Verwendung von Deployment Patterns entwerfen.

**Unterlagen / Bücher (nicht Pflicht)**

* Tanenbaum, M. van Steen, Distributed Systems, 2nd Edition, Pearson Education, 2007 (zweite Hälfte der Vorlesung; auch auf Deutsch verfügbar)
* J. Dunkel, A. Eberhart, S. Fischer, C. Kleiner, A. Koschel, Systemarchitekturen für verteilte Anwendungen, Hanser, 2008 (als E-Book in der Bibloithek vorhanden)
* P. Brown, Implementing SOA – Total Architecture in Practice, Addison Wesley 2008 (ausgewählte Kapitel, im letzten Teil der Vorlesung)
* M. Nygard, Release It!, http://www.infoq.com/articles/nygard-release-it
* MSDN Deployment Patterns, Operational (Topology) Modeling White Paper von IBM und weitere Assets zum Operational Modelling (z.B. IBM Hardware Sizing Tool, Palladio Developer Wiki)
* INCOSE Systems Engineering for Large Infrastructure Projects
* Online Resourcen wie highscalability.com und Udacity Web Application Design Lecture (mit Reddit-Architekturevolution)

**Lerninhalte***Charakteristische Eigenschaften verteilter Software-Systeme:*

* Vom Programm zum System: Verteilungsdimensionen, Kopplungsarten, Designherausforderungen
* VSS-Anwendungsgebiete in der Praxis, z.B. Unternehmensanwendungen, Distributed Control Systems, World-Wide Web (WWW)
* Wichtige Architekturstile und Anwendungstopologien: Client-Server, Hub-and-Spoke, Peer-to-Peer

*Remoting (Netzwerkprogrammierung):*

* Synchrone Kommunikation: TCP/IP Sockets, Remote Procedure Calls, HTTP Web Services
* Asynchrone Kommunikation mit Message-Oriented Middleware (MOM), Enterprise Integration Patterns
* weitere Message Exchange Patterns und Kommunikationsprotokolle im Überblick

*Zentrale Konzepte für den Entwurf verteilter Systeme:*

* Naming
* Synchronization

*Verteilte Algorithmen und Datenstrukturen:*

* Namensauflösung
* Verteilte Hash-Tabellen
* Lamport-Uhr
* Vektor-Uhr

*Anwendung verteilter Systeme. Zum Beispiel:*

* BitTorrent
* Bitcoin
* Distributed batch processing

*Operationale Modelle und Deployment Patterns für das qualitätsgetriebene Infrastrukturdesign:*

* Performance und Skalierbarkeit
* Robustheit und Verfügbarkeit
* Systemmanagement und Auditierbarkeit
* Middleware-Produkte und Frameworks zum Bau von VSS
* Plattform-Auswahlkriterien und Designentscheidungen im VSS-Entwurf

*Ausblick auf spezielle VSS – Event-Driven Architectures, Cloud Computing, Service-Oriented Architectures*

*Fallstudien aus der Industriepraxis*

***Einen Teil des Moduls wird in Englisch gehalten.***

Übersicht des Modules

[Einführung 5](#_Toc476555973)

[Motivation 5](#_Toc476555974)

[Software Programm und Software System 5](#_Toc476555975)

[Definition Distributed System (zu Deutsch: Verteiltes System) 5](#_Toc476555976)

[Centralization and Transparency Types (ISO) 6](#_Toc476555977)

[Design-Herausforderungen und Lösungsansätze 6](#_Toc476555978)

[Vorteile verteilter Software-Systeme (VSS) 6](#_Toc476555979)

[Herausforderungen bei der Entwicklung verteilter Anwendungen 6](#_Toc476555980)

[Middleware als VSS Enabler 7](#_Toc476555981)

[ACID 7](#_Toc476555982)

[Problemstellungen und Lösungsstrategien 7](#_Toc476555983)

[Architekturstile zum Bau von VSS 8](#_Toc476555984)

[Verschiedene Stile 8](#_Toc476555985)

[Client-Server 8](#_Toc476555986)

[Peer-to-Peer VSS Architecture Style 10](#_Toc476555987)

[WWW und Netzwerkprogrammierung in Java (erste Schritte) 10](#_Toc476555988)

[WWW ist meistens eine REST-basierte Architektur 10](#_Toc476555989)

[REST Beispiel 10](#_Toc476555990)

[Media Typen (MIME Types) 11](#_Toc476555991)

[Architektonische und Designtechnische Aspekte für verteilte Software 11](#_Toc476555992)

[Idempotent 11](#_Toc476555993)

[Beispiel zur Wichtig von Time-Outs und Error Handling 12](#_Toc476555994)

[Netzwerkprogrammierung 12](#_Toc476555995)

[Architekturstile im Vergleich 12](#_Toc476555996)

[Inter-Process Kommunikation Varianten 12](#_Toc476555997)

[TCP/IP Sockets 13](#_Toc476555998)

[Sockets im Überblick 13](#_Toc476555999)

[Generic TCP Application 13](#_Toc476556000)

[Socket-Programmierung: Grundkonzepte 13](#_Toc476556001)

[Java Socket API 14](#_Toc476556002)

[Beispiel 14](#_Toc476556003)

[Berkeley Sockets und das Message Passing Interface (MPI) 14](#_Toc476556004)

[IPv4 vs. IPv6 14](#_Toc476556005)

[Vorteile und Nachteile von Java Sockets 14](#_Toc476556006)

[WebSockets 15](#_Toc476556007)

[Das Protokoll 15](#_Toc476556008)

[Client API und Support 15](#_Toc476556009)

[Server Support 15](#_Toc476556010)

[UDP (User Datagram Protocol) 🡺 Vergleich mit TCP 15](#_Toc476556011)

[Struktur eines UDP Programms 16](#_Toc476556012)

[Beispiel - Sender und Empfänger 16](#_Toc476556013)

[UDP vs. TCP 16](#_Toc476556014)

[TCP/IP vs. UDP/IP 17](#_Toc476556015)

[Message Exchange Patterns 17](#_Toc476556016)

[Asynchronous Messaging 18](#_Toc476556017)

[Einführung in Messaging 18](#_Toc476556018)

[Nachrichtenkonzept und die Komponenten 18](#_Toc476556019)

[Message-Queuing Model und RPC’s 18](#_Toc476556020)

[Nachrichten nutzen um Applikationen zu verbinden und Daten zu verteilen 18](#_Toc476556021)

[Message-Oriented-Middleware (MOM) 19](#_Toc476556022)

[Hub-and-Spoke Architecture with CMB 19](#_Toc476556023)

[Java Message Service (JMS) API 19](#_Toc476556024)

[Reliability levels 19](#_Toc476556025)

[JMS Message-Struktur 19](#_Toc476556026)

[Beispiel für einen JMS Message Provider 20](#_Toc476556027)

[Andere APIs oder Provider 20](#_Toc476556028)

[Messaging Middleware Provider 20](#_Toc476556029)

[IBM MQ 20](#_Toc476556030)

[MS MQ 22](#_Toc476556031)

[Active MQ 22](#_Toc476556032)

[MOM API Primitives (Platform-Independet Level) 22](#_Toc476556033)

[Enterprise Integration Patterns 22](#_Toc476556034)

[RabbitMQ (based on AMQP) 22](#_Toc476556035)

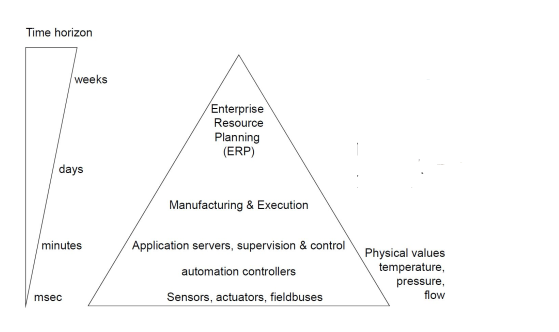
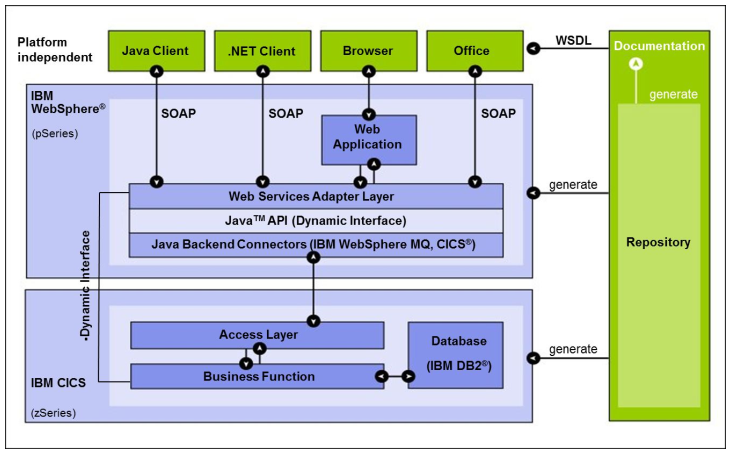
[Patterns 22](#_Toc476556036)

[Vorlesung Woche 4 24](#_Toc476556037)

# Einführung

## Motivation

Verteilte Software-Systeme (VSS) sind allgegenwärtig in beruflichen und privaten Alltag. Sie führen Konzepte und Technologien aus unterschiedlichen Bereichen der Information zusammen. Dazu zählen die Netzwerkprogrammierung (Remoteing), Betriebssysteme und Middleware, User Interfaces, Datenbanken und Algorithmen.

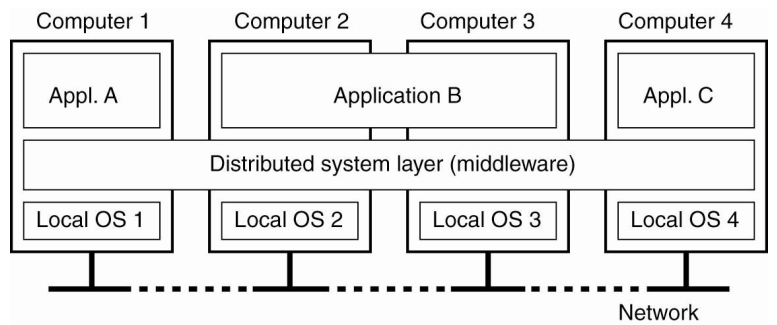
Beispiele dafür sind Unternehmenanwendungen im Core Banking oder auch Prozessautomation und-überwachung aus der Industrie.  


### Software Programm und Software System

|  |  |
| --- | --- |
| **Programm**   * Hat ein Anfang und ein Ende * Wird meist anhand von Parametern ausgeführt. * Kann offline geupdatet werden (Stop, Neustart) * Ist Zeitlich gesteuert, hat einen Callstack | **System (von Programmen/Systemen)**   * Hört vielleicht gar nie auf. * Akzeptiert den Input zu jeder Zeit (Asynchron über externe Schnittstellen) * Meistens wird es dynamisch während der Laufzeit rekonfiguriert. * Ist Event-gesteuert. |

### Definition Distributed System (zu Deutsch: Verteiltes System)

Ein verteiltes System ist eine Sammlung von unabhängigen Computer die gegenüber dem Benutzer als ein ganzes System auftreten.



### Centralization and Transparency Types (ISO)

|  |  |
| --- | --- |
| **Konzept** | **Beispiel** |
| Centralized services | A single server for all users |
| Centralized data | A single on-line telephone book |
| Centralized algorithms | Doing routing based on complete information |

|  |  |
| --- | --- |
| **Transparency** | **Beschreibung** |
| *Access* | Hide differences in data represendation and how a resource is accessed. |
| *Location* | Hide where a resource is located |
| *Migration* | Hide that a resource may move to another location |
| *Relocation* | Hide that a resource may be moved to another location while in use |
| *Replication* | Hide that a resource is replicated |
| *Concurrency* | Hide that a resource may be shared by several competivitve users |
| *Failure* | Hide the failure and recovery of a resource. |

## Design-Herausforderungen und Lösungsansätze

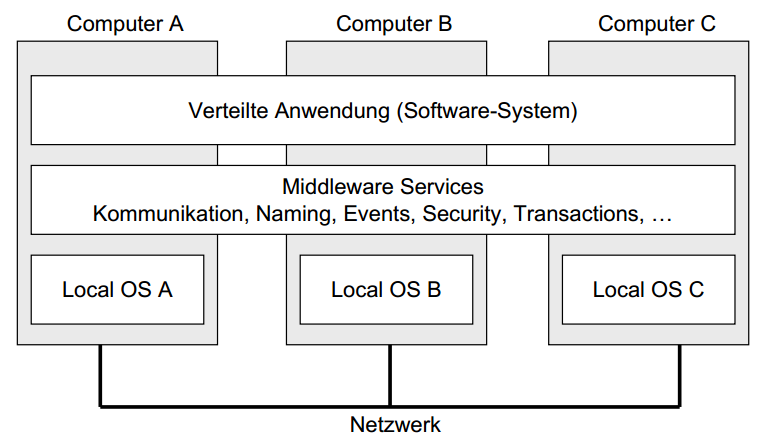
### Vorteile verteilter Software-Systeme (VSS)

VSS bilden die verteilte Realität ab. Die Benutzer arbeiten an verschiedenen Arbeitsplätzen. Die Unternehmensstandorte und Abteilungen sind in der Regel verteilt. VSS führen zu einer Performance Steigerung, wenn mehrere Rechner an einer Aufgabe parallel arbeiten können. Eine Skalierbarkeit ist dadurch gegeben, dass Leistungsengpässe durch zusätzliche Hardware kompensiert werden können. Zudem ist ein System so Fehlertoleranter, da Software auf mehreren Rechnern repliziert werden.

### Herausforderungen bei der Entwicklung verteilter Anwendungen

* Komplexe Kommunikation / Systeme
  + Interprozess-Kommunikation statt lokaler Methodenaufrufe
  + Heterogene Systeme (Rechner, Betriebssysteme, Hardware, Sprachen)
* Performanz Problem
  + Kommunikation über langsame Netzwerke (Latenz, Durchsatz)
* Zuverlässigkeit 🡺 CFIA – Component Failure Impact Analysis
  + Alle Netzzugriffe sind potentiell unsicher
  + Maschinenausfälle
* Transaktionssicherheit
  + Mehrere Benutzer greifen gleichzeitig auf Daten zu (zur Sicherstellung der Konsistenz ist Isolation von Transaktionen erforderlich).

### Middleware als VSS Enabler

Eine Middleware ist eine infrastrukturelle Software zur Kommunikation zwischen Software-Komponenten und Anwendungen auf verschiedenen Computern.

* Verteilungsplattform mit entsprechenden Protokollen
* Höheres Abstraktionsniveau als einfacher Datenaustausch
* Verbirgt Komplexität der zugrundeliegenden Applikation/Infrastruktur.

Gründe für die Einführung einer Middleware sind die Überwindung von der Heterogenität oder die Vereinfachung der Erstellung verteilter Anwendungen.

**Kommunikationsorientierte Middleware**  
Der Schwerpunkt liegt in der Abstraktion (Vereinfachung) von der Netzwerkprogrammierung (TCP/IP, Socket APIs). Beispiele sind Java Remote Method Invocation (RMI) oder Webservices wie SOAP.

**Anwendungsorientierte Middleware**  
Der Schwerpunkt liegt in der weiterreichenden Unterstützung verteilter Anwendungen. Ein komplexer Aufbau führt zu zahlreichen Zusatzdiensten wie Discovery, Sicherheit, Zuverlässigkeit, verteile Transaktionen und Session. Beispiele dafür sind CORBA, J2EE oder verteilte Betriebssysteme.

### ACID

**Atomicity**  
Von einer atomaren Operation spricht man, wenn eine Sequenz von Daten-Operationen entweder ganz oder gar nicht ausgeführt wird (Alles-oder-nichts-Eigenschaft)

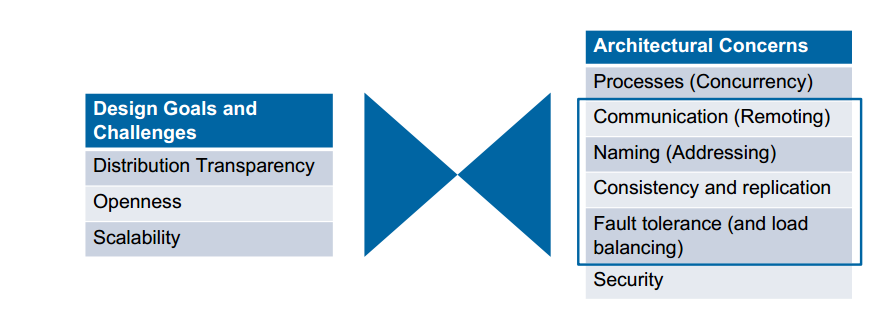
**Consistency**  
Konsistenz heißt, dass eine Sequenz von Daten-Operationen nach Beendigung einen konsistenten Datenzustand hinterlässt, falls die Datenbank davor auch konsistent war.

**Isolation (Abgrenzung)**Durch das Prinzip der Isolation wird verhindert/eingeschränkt, dass sich gleichzeitig in Ausführung befindliche Daten-Operationen gegenseitig beeinflussen.

**Durability**  
Der Begriff Dauerhaftigkeit sagt aus, dass Daten nach dem erfolgreichen Abschluss einer Transaktion garantiert dauerhaft in der Datenbank gespeichert sind. Die dauerhafte Speicherung der Daten muss auch nach einem Systemfehler (Software-Fehler oder Hardware-Ausfall) garantiert sein. Insbesondere darf es nach einem Ausfall des Hauptspeichers nicht zu Datenverlusten kommen. Dauerhaftigkeit kann durch das Schreiben eines Transaktionslogs sichergestellt werden. Ein Transaktionslog erlaubt es, nach einem Systemausfall alle in der Datenbank fehlenden Schreib-Operationen zu reproduzieren

### Problemstellungen und Lösungsstrategien

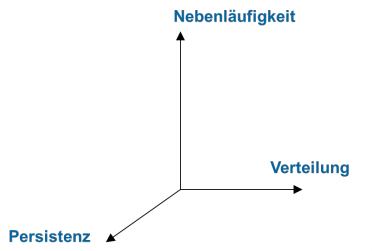
Die VSS-Vorlesung soll eine Mischung aus Wissen und Können vermitteln bezüglicher dieser Problemstellungen und Lösungsstrategien.



## Architekturstile zum Bau von VSS

### Verschiedene Stile

* Client-Server
* Distirbuted objects
* Hub-and-spoke
* Event-Driven Architecture
* Peer-to-Peer (P2P)

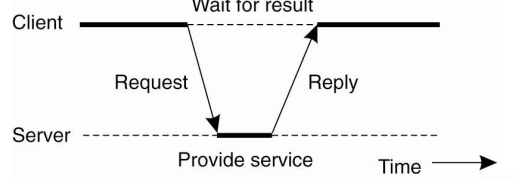
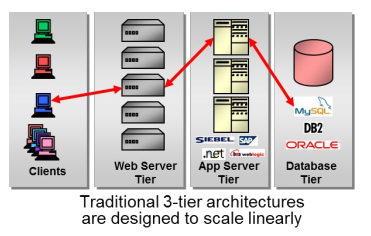
Die unterschiedlichen Architektur-Stile werden durch Integrations-Optionen beeinflusst.

**Transparenz betreffend Nebenläufigkeit**  
Daten oder andere Ressourcen möglicherweise gleichzeitig von konkurrierenden Benutzern bzw. Applikationen verwendet werden.

**Transparenz betreffend Persistenz**  
verbirgt, ob Ressource im lokalen Speicher (Memory) oder auf einer Festplatte ist.

**Transparenz betreffend Verteilung**  
verbirgt, ob die aufgerufene Komponente lokal oder entfernt ist.

### Client-Server

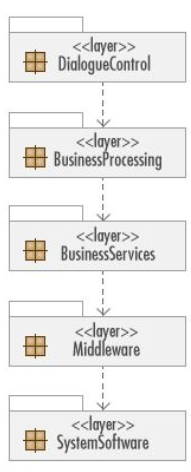
**Tier 1** User PC running browsers (front-end)

**Tier 2** Web server and presentation logic, Application server und business logic, integration

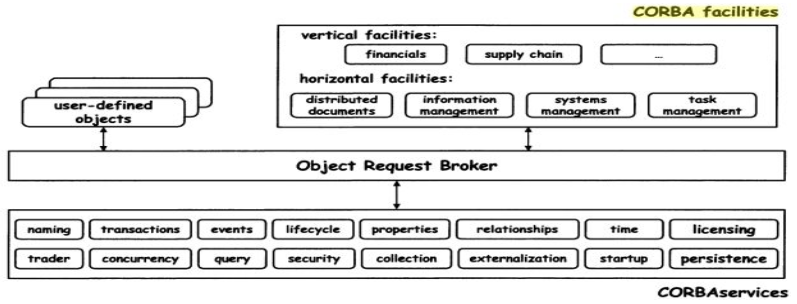
**Tier 3** Database and other backend systems

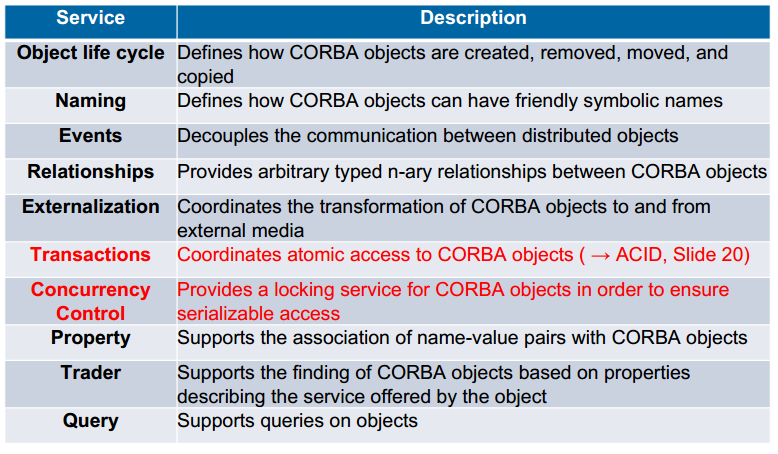
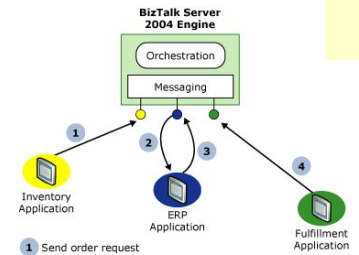
Jedes Tier hat seine eigenen Layer Architektur. Es kann gleiche Teile geben, muss es aber nicht.

**Beispiel einer geschichteten Architektur**



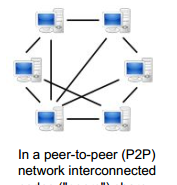
|  |  |
| --- | --- |
| **DialogueControl** | The dialogue control layer handles user-system interactions and use case logic. |
| **BusinessProcessing** | The business processing layer contains application-specific services that handle use case step logic and choreography |
| **BusinessServices** | The business services layer contains more general business components that may be used in several applications. |
| **Middleware** | The middleware layer contains components such as interfaces to databases and platform-independent operating system services. |
| **SystemSoftware** | The system software layer contains components such as operating systems and databases. |

**CORBA (Common Object Request Broker Architecture)**  


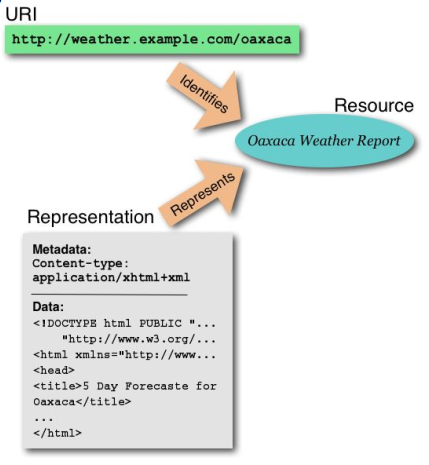
 

### Peer-to-Peer VSS Architecture Style

P2P Systeme implementieren eine verteile Applikationsarchitektur, welche den Workload in Partitionen zwischen den Peers aufteilt. Die Peers sind alle gleichberechtigt. Ein P2P System verbindet dynamisch alle Nodes um Traffic zu routen und somit Tasks auszulagern. Es bietet den Vorteil, dass man skalieren kann ohne die zentralen Ressourcen auszubauen. Es werden die Prozessor- und Netzwerkpower der Client genutzt. Meist sind dort mehr als genug Leistung vorhanden. Dabei gibt es keinen Single Point of Failure. Beispiele sind Skype oder BitTorrent.

## WWW und Netzwerkprogrammierung in Java (erste Schritte)

Das weltweit grösste verteilte Software Systeme, ist das WWW. Es entspricht in etwa dem Client-server architectural style. Ein Naming findet mit Uniform Resource Identifiers (URIs) statt. Die Kommunikation geschieht mit http über TCP/IP. Im Internet gibt es eigentlich keinen Point of Failure, da unglaublich viel Redundanz vorhanden ist.

### WWW ist meistens eine REST-basierte Architektur

REST (Represential State Transfer = Architekturstyle für verteilte Applikationen. REST unterstützt alle vier CRUD Operationen. Es basiert auf einem «stateless» Client-Server Kommunikationsprotokoll. Logisch gesehen ist http simple und einfach dazu da, Aufrufe zwischen zwei Maschinen auszutauschen. Es ist weniger kompliziert als CORBA, RPC oder SOAP.

### REST Beispiel

#### Abfrage in einer Telefonbuchapplikation für Details zu einem Benutzer

**Nutzung von Web Services und SOAP**

Das Resultat könne eine XML-Datei sein, welche als Payload in der SOAP-Antwort eingebettet ist.

**Nutzung von Rest**

Der URL wird mit einem GET Request zum Server gesendet. Als Antwort werden die reinen Daten zurückgeben ohne jeglichen Müll rund herum.

### Media Typen (MIME Types)

Es gibt bereits hunderte von definierten Media Typen. Beispiele sind text/plain oder image/png. Einen bestehenden Typen zu wählen oder einen neuen Typen zu entwerfen ist eine wichtige Designentscheidung bei der Erstellung von http API’s. (Client und Server müssen es verstehen).

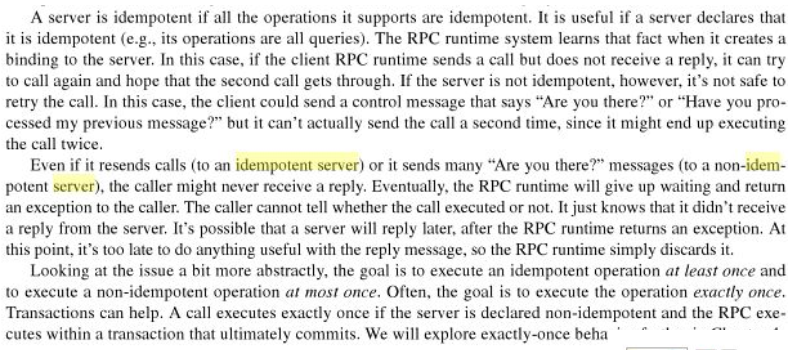
Netzwerkklassen im JDK  


## Architektonische und Designtechnische Aspekte für verteilte Software

* **Kommunikations Topologie**
  + Ein Client, ein Server? Mehrere Clients für einen Server? Dynamisches Setup?
* **Location Autonomy (Transparenz)**
  + Wirkliche Adressen vs. Virtuelle Adressen (Was wenn ein Server verschoben wird?)
* **Invocation and Message Semantics**
  + Bytestream vs. Document vs. Procedure vs. Remote Object
* **Timeout Management**
  + 1ms? 30 Sekunden? Unendlich?
* **Error Handling**
  + Erneute Requests
  + Server idempotent machen?

## Idempotent

Definition gemäss Internet: “*Idempotence is a funky word that often hooks people. Idempotence is sometimes a confusing concept, at least from the academic definition. From a RESTful service standpoint, for an operation (or service call) to be idempotent, clients can make that same call repeatedly while producing the same result. In other words, making multiple identical requests has the same effect as making a single request. Note that while idempotent operations produce the same result on the server (no side effects), the response itself may not be the same (e.g. a resource's state may change between requests). The PUT and DELETE methods are defined to be idempotent. However, there is a caveat on DELETE. The problem with DELETE, which if successful would normally return a 200 (OK) or 204 (No Content), will often return a 404 (Not Found) on subsequent calls, unless the service is configured to "mark" resources for deletion without actually deleting them. However, when the service actually deletes the resource, the next call will not find the resource to delete it and return a 404. However, the state on the server is the same after each DELETE call, but the response is different. GET, HEAD, OPTIONS and TRACE methods are defined as safe, meaning they are only intended for retrieving data. This makes them idempotent as well since multiple, identical requests will behave the same*.”



## Beispiel zur Wichtig von Time-Outs und Error Handling

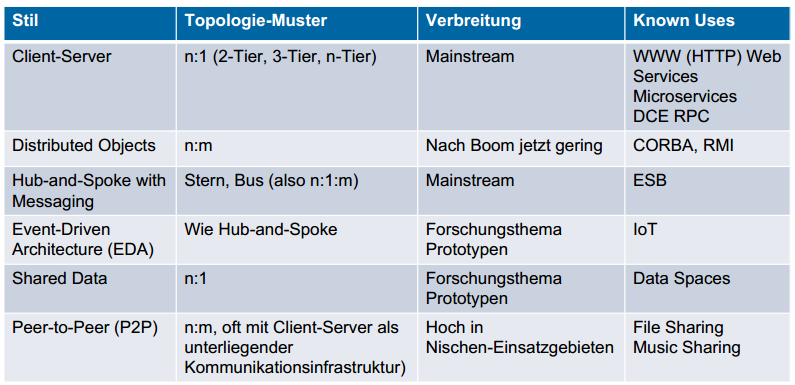
**Eine Exception, welche eine Airline gegrounded hat.**  
Eine JDBC Exception wurde auf einem Applikationsserver nicht gefangen (not caught). Dies führte dazu, dass alle Self Check-In Kioske der Airline offline gingen. Die Kioske waren dann offline für mehrere Stunden. Zur Normalität kam es erst als alle Applikations- und Datenbankserver neugestartet wurden.

**Hauptgründe, wieso es dazu kam**

* Unangemessenes Wiederholungs-/Failover-Management auf den Applikationsservern
* Kein Timeout Management auf den Applikationsservern
* Unvollständiges Monitoring der Applikationsserver (Sie wurden immer noch als Grün angezeigt, obwohl Sie geblockt waren).

# Netzwerkprogrammierung

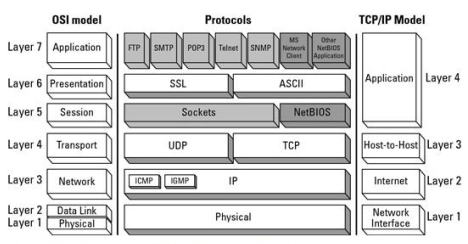
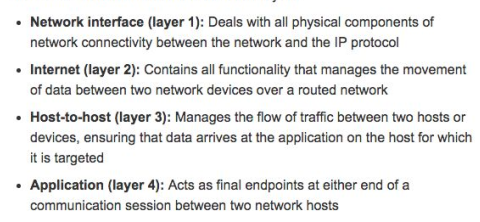
## Architekturstile im Vergleich



## Inter-Process Kommunikation Varianten

|  |  |  |
| --- | --- | --- |
| **Datenaustauch** Sockets (UDP oder TCP über IP), File Transfer, Shared Database | **Nachrichtenaustausch** Message-Oriented Middleware, http GET, POST | **Remote Procedure Call** DCE RPC, Java RMI, CORBA, Web Services, RESTFul HTTP |

## TCP/IP Sockets

Verbindung zwischen dem OSI und dem TCP/IP Model  
 

### Sockets im Überblick

Sockets sind ein Basis-Mechanismus für alle komplexeren Verfahren wie http oder RMI. Es dient zum Austausch von Bytestörmen auf der Programmierebene. Das Sockets ist eine Verbindung zwischen zwei Kommunikations-Endpunkten (IP + Port). Beim Konzept gibt es die zwei Rollen: Client und Server.

**Nachteile von Sockets**  
Es wird ein Konstruieren und Parsen der Byteströme erforderlich (keine Objekte und daher auch keine Typsicherheit). Zudem muss das Message Exchange Pattern (MEP) selbst spezifiziert, implementiert und überprüft werden. Das MEP definiert die Reihenfolge der send/receive Calls durch Client und Server.

### Generic TCP Application

**Server Sockets** Warten auf Request, welche für das Netzwerk kommen

**Client Sockets** Sendet und bekommt Daten, Implementiert mit der java.net.Socket-Klasse.

**Algorithmus für den TCP Client**Finden der IP und der Portnummer des Servers, Erstellen eines TCP Sockets, Verbinden des Sockets mit dem Server (Server muss laufen und auf Request hören), Senden/Empfangen von Daten durch das Socket, Verbindung schliessen.

Algorithmus für den TCP Server  
Ein TCP Server Socket erstellen, Binden des Server Sockets auf die Server IP und Port, Akzeptieren von neuen Verbindungen von den Clients, Senden / Empfangen von Daten über das Server Socket, Schliessen der Verbindung mit dem Client.

### Socket-Programmierung: Grundkonzepte

|  |  |
| --- | --- |
|  |  |

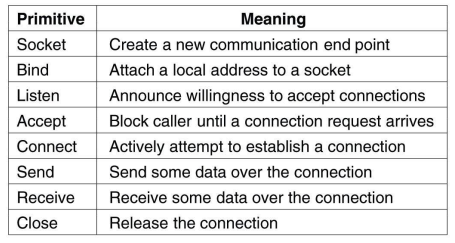
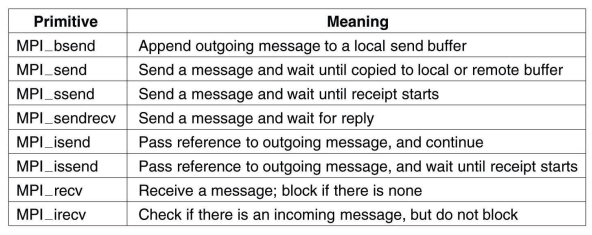
## Java Socket API

### Beispiel

|  |  |
| --- | --- |
| **Socket Server** Ein Socket (engl. Steckdose) ist ein Verbindungsendpunkt, der vom Programm wie eine gewöhnliche Datei beschrieben und gelesen werden kann. Der Serverprozess muss von außen eindeutig angesprochen werden können. Dazu bindet er sich an einen festen Port, den sogenannten “well known port”, über den er erreichbar ist | **Socket Client**  Der Client braucht keinen festen  Port. Er holt sich einen normalen Socket, dem vom System eine freie Nummer zugeteilt wird.  Der Server erfährt die Nummer des Clients aus der Anfrage und kann ihm unter diesem Port  Antworten. Im nächsten Schritt ruft der Client connect() auf, um eine Verbindung mit dem Server aufzunehmen, der in den Parametern beschrieben wird. Sobald die Verbindung da ist,  sendet der Client seine Anfrage per write() oder alternativ send() und wartet per read() oder recv() auf die Antwort des Servers. |

### Berkeley Sockets und das Message Passing Interface (MPI)

Gleiches Protokoll auf allen Platformen und in allen Sprachen. Der API Komfort ist je nach Sprache und Bibliothek unterschiedlich. Dabei müssen die System Resourcen gemanaged werden.

### IPv4 vs. IPv6

Es gibt einige Änderungen für die Socket-Programme (auch Java). Das Socket API und das primitive Interface bleiben das Gleiche. Die Adressierung hat geändert und daher auch die Formate der Antworten. Zudem unterscheidet sich das Quality-of-Service (Performance, Timeout Management).

### Vorteile und Nachteile von Java Sockets

**Vorteile**  
Flexibel, Mächtig, Generiert nur wenig Netzwerk Traffic (wenn es effizient genutzt wird).

**Nachteile**  
Können nur Raw Daten senden, Client und Server müssen einen Mechanismus haben um die Daten zu interpretieren, Zudem müssen beide die State Informationen halten.

## WebSockets

### Das Protokoll

Eine auf TCP basierendes Netzwerkprotokoll, das entworfen wurde, um eine bidirektionale Verbindung zwischen einer Webanwendung und einem WebSocket-Server bzw. einem Webserver herzustellen. Während bei einer reinen HTTP-Verbindung jede Aktion des Servers eine vorhergehende Anfrage des Clients erfordert, reicht es beim WebSocket-Protokoll, wenn der Client die Verbindung öffnet. Der Server kann dann diese offene Verbindung aktiv verwenden und kann neue Informationen an den Client ausliefern, ohne auf eine neue Verbindung des Clients zu warten. Bei WebSockets entfallen die durch den HTTP-Header verursachten zusätzlichen Daten, die bei jeder Anfrage einige Hundert Bytes umfassen können

### Client API und Support

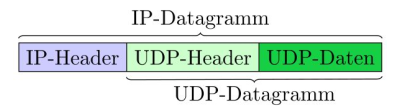
Web Sockets ist eine state-of-the-art Kommunikationtechnologie für Webapplikationen. Es arbeitet über Sockets. Ist sichtbar für ein JavaScript Interface oder kompatible HTML5 Browser. Sobald man eine WebSocket Verbindung hat, ist es möglich Daten mit send() an den Server zu senden.

### Server Support

* C++: libwebsockets
* Erlang: Shirasu.ws
* Java: Jetty (and others)
* Node.JS: ws
* Ruby: em-websocket
* Python: Tornado, pywebsocket
* PHP: Ratchet, phpws

Eine Demo zu Websockets gibt es unter <http://www.websocket.org/echo.html>

## UDP (User Datagram Protocol) 🡺 Vergleich mit TCP

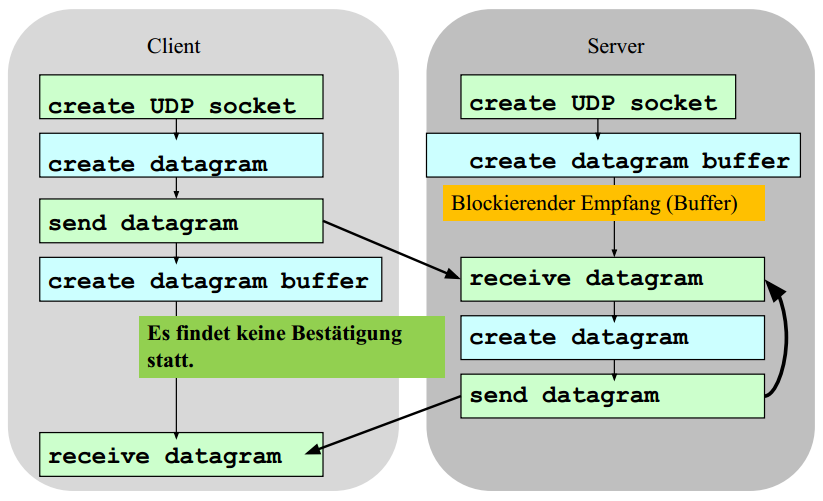


Verbindungsloses Netzwerkprotokoll für den Versand von Datagrammen in IP-basierten Netzen Die Entwicklung von UDP begann 1977, als man für die Übertragung von Sprache ein einfacheres Protokoll benötigte als das bisherige verbindungsorientierte TCP.

* Keine Verzögerungen bei der Sprachübertragung
* Dafür keine Garantie, dass ein Datagram ankommt
* Keine Garantie, dass Datagramme in der gleichen Reihenfolge ankommen, in der sie gesendet wurden
* Keine Garantie, dass ein Datagram nur einmal beim Empfänger eintrifft.

Eine Anwendung, die UDP nutzt, muss daher gegenüber verlorengegangenen und unsortierten Paketen unempfindlich sein oder selbst entsprechende Korrekturmaßnahmen und je nachdem auch Sicherungsmaßnahmen vorsehen.

### Struktur eines UDP Programms



### Beispiel - Sender und Empfänger

|  |  |
| --- | --- |
| **Sender** | **Empfänger** |

### UDP vs. TCP

Da mit UDP vor Übertragungsbeginn nicht erst eine Verbindung aufgebaut werden muss, kann der Datenaustausch schneller beginnen. *Das fällt vor allem bei Anwendungen ins Gewicht, bei denen nur kleine Datenmengen ausgetauscht werden müssen.*

Einfache Frage-Antwort-Protokolle wie DNS (Domain Name System) verwenden UDP, um die Netzwerkbelastung gering zu halten und damit den Datendurchsatz zu erhöhen. *Ein Drei-Wege-Handschlag wie bei TCP (dem Transmission Control Protocol) für den Aufbau der Verbindung würde unnötigen Overhead erzeugen.*

Daneben bietet die ungesicherte Übertragung auch den Vorteil von geringen Übertragungsverzögerungsschwankungen: Geht bei einer TCP-Verbindung ein Paket verloren, wird es automatisch neu angefordert. Das braucht Zeit, die Übertragungsdauer kann daher schwanken, was für Multimediaanwendungen schlecht ist. Bei VoIP z. B. käme es zu plötzlichen Aussetzern, bzw. die Wiedergabepuffer müssten größer angelegt werden. *Bei UDP bringen verlorengegangene Pakete nicht die gesamte Übertragung ins Stocken, sondern vermindern lediglich die Qualität.*

Bei Übertragungsfehlern oder bei Überlast löscht IP Pakete. *Datagramme können daher fehlen. UDP bietet hierfür keine Erkennungs- oder Korrekturmechanismen, wie etwa TCP.*

Im Falle von mehreren möglichen Routen zum Ziel kann IP bei Bedarf neue Wege wählen. Dadurch ist es in seltenen Fällen möglich, dass später gesendete Daten früher gesendete überholen. Außerdem kann ein einmal abgesendetes Datenpaket mehrmals beim Empfänger eintreffen.

### TCP/IP vs. UDP/IP

* Verbindungsorientiert vs. Nicht-verbindungsorientiert
* IP-Level Addressing und Routing via DNS, ARP, etc.
* Unterschiede in den Quality of Server (QoS)
  + Sequencing
  + How to deal with packet loss?
* Broadcast und Multicast möglich

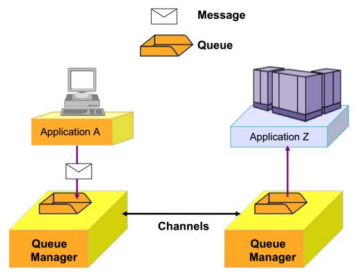
## Message Exchange Patterns

|  |  |
| --- | --- |
| **Basic Messaging Pattern** Applikationen kommunizieren indem sie Nachrichten senden über Message Channels. Die Applikation weiss über das Message Format, Channels, oder andere Details zur Verbindung. | **Blocking Receiver Message Pattern** Synchrone Nachrichtenendpunkte, welche solange blockieren bis eine Nachricht empfangen wird. |
| **Polling (Non-Blocking) Receiver Message Pattern** Polling Consumer, einer der explizit einen Aufruf macht, wenn er eine Nachricht empfangen möchte. | **Service Activator Message Pattern** Design und Implementation eines Service Activator, welcher die Nachrichten zu den Channels verbinden (die durch die Services genutzt warden). Dieser kann one-way oder Two-Way sein. |

# Asynchronous Messaging

## Einführung in Messaging

### Nachrichtenkonzept und die Komponenten

**Message Descriptor**  
Identifiziert die Nachricht und enthält Steuerinformationen (z. B. Nachrichtentyp und Priorität), die der Nachricht durch die sendende Anwendung zugewiesen wurde.

**Message data**  
Enthält die Anwendungsdaten. Die Struktur der Daten wird durch die Anwendungsprogramme definiert, die sie verwenden, und der Warteschlangenmanager ist weitgehend unbekümmert mit seinem Format oder Inhalt.

**Queue Manage**r  
Ist verantwortlich für das Akzeptieren und Zustellen der Nachrichten. Er verwaltet die Queues aller Nachrichten, welche warten. Warteschlangenmanager sind über ein Kommunikationsnetzwerk über logische Kanäle verbunden. Nachrichten fliessen automatisch über diese Kanäle vom Produzenten einer Nachricht an den Verbraucher dieser Nachricht, basierend auf der Konfiguration der Warteschlangenmanager in der Infrastruktur.

### Message-Queuing Model und RPC’s

|  |  |  |
| --- | --- | --- |
| **Loose Coupling / Asynchronous Processing** | **Synchronous RPC** | **Asynchronous RPC** |

### Nachrichten nutzen um Applikationen zu verbinden und Daten zu verteilen

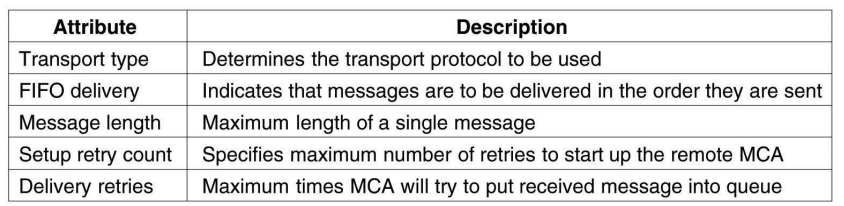
|  |  |
| --- | --- |
|  |  |

Asynchrone Verarbeitung kann über verschiedene Wege genutzt werden. Warteschlange große Mengen an Arbeit, die dann einmal pro Tag durch einen Batch-Prozess eingereicht wird. Die Arbeit kann auch sofort eingereicht und dann verarbeitet werden, wenn die empfangende Bewerbung den Umgang mit einer vorherigen Anfrage beendet hat. Asynchrone Verarbeitung impliziert nicht unbedingt alle Antwortzeiten.

|  |  |
| --- | --- |
| Message-Oriented-Middleware (MOM) | Hub-and-Spoke Architecture with CMB |

## Java Message Service (JMS) API

Point-to-Point Channel über die Queue API, Publish-Subscribe Channel über die Topic API.



### Reliability levels

**Best effort nonpersistent**  
Nachrichten werden verworfen, wenn eine Messaging-Engine stoppt oder fehlschlägt. Nachrichten können auch verworfen werden, wenn eine Verbindung, die verwendet wird, um sie zu senden, nicht verfügbar ist oder als Ergebnis von eingeschränkten Systemressourcen.

**Express nonpersistent**Nachrichten werden verworfen, wenn eine Messaging-Engine stoppt oder fehlschlägt. Nachrichten können auch verworfen werden, wenn eine Verbindung, die verwendet wird, um sie zu senden, nicht verfügbar ist.

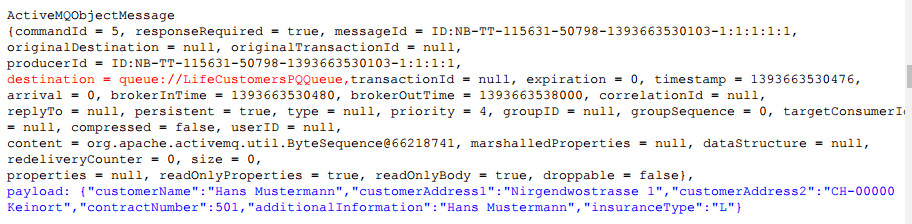
**Reliable nonpersistent**  
Nachrichten werden verworfen, wenn eine Messaging-Engine stoppt oder fehlschlägt.

**Reliable persistent**  
Nachrichten können verworfen werden, wenn eine Messaging-Engine ausfällt.

**Assured persistent**  
Nachrichten werden nicht verworfen.

### JMS Message-Struktur

Eine JMS-Message besteht aus a) Header, b) Properties und c) Body. Ein Header wird immer gesendet. Er enthält Informationen für das Routing und die Identifikation. Ein MOM-Provider normiert seine Messsage Header. Properties sind optional – sie enthalten zum Beispiel Informationen, mit deren Hilfe ein Coustomer Nachrichten filtern oder weiterrouten kann (Erweiterung des Standard-Headers). Der Body ist auch zwingend erforderlich – er enthält die auszutauschenden Nutzdaten (Text, Objekte, Binärdaten).



### Beispiel für einen JMS Message Provider

|  |  |
| --- | --- |
| **Queue Sender** | **Queue Receiver** |

### Andere APIs oder Provider

* Provider, welche die Java Messaging Service (JMS) Spezifikation beinhalten
  + Apache ActiveMQ
  + Any Java Enterprise Edition (JEE) Application Server: IBM, JBoss, Oracle
* RabbitMQ (eigene API, nicht kompatibel zu JMS)
  + Open Source, Implementiert das AMQP Protokoll.
* Cloud Provider z.B. Amazon Simple Queueing Server (SQS)
* Apache Camel oder Sprint Integration
* ZeroMQ
  + Alternativer Weg zum Queue basierten Nachrichten.

## Messaging Middleware Provider

### IBM MQ

Ermöglicht es, Anwendungen asynchron zu kommunizieren, d.h. Nachrichten können zu unterschiedlichen Zeiten gesendet, empfangen und verarbeitet werden. Kann jede Art von Daten als Nachrichten transportieren. Arbeitet mit einer breiten Palette von Computing-Plattformen, Anwendungen, Web-Services und Kommunikationsprotokolle.

#### Two-Phase Commit (2PC)

**Erste Phase**  
Der Koordinator sendet ein prepare an alle Teilnehmer. Die Teilnehmer verarbeiten die Transaktion bis zu dem Punkt, wo die Transaktion entweder mit commit oder rollback abgeschlossen wird. Dabei schreiben sie Einträge in ihr undo log und in ihr redo log. Die Teilnehmer antworten mit ready, wenn die Transaktion erfolgreich war - oder sie antworten mit failed, wenn die Transaktion fehlgeschlagen ist.

**Zweite Phase**  
Wenn der Koordinator von allen Teilnehmern eine ready Meldung bekommen hat: Der Koordinator sendet commit an alle Teilnehmer. Die Teilnehmer schließen die Transaktion mit commit ab und geben alle Locks und Ressourcen frei. Die Teilnehmer senden ein acknowledgment zurück. Der Koordinator beendet die Transaktion, wenn er von allen Teilnehmern die Bestätigung erhalten hat.

Wenn zumindest einer der Teilnehmer ein failed schickt: Der Koordinator sendet abort an alle Teilnehmer. Die Teilnehmer schließen die Transaktion mit rollback ab (mittels des undo logs) und geben alle Locks und Ressourcen frei. Die Teilnehmer senden ein acknowledgment zurück. Der Koordinator beendet die Transaktion ebenso mit rollback, wenn er von allen Teilnehmern die Bestätigung erhalten hat.

#### Persistente und nicht persistente Nachrichten

Meldungen, die kritische Geschäftsdaten enthalten, wie z. B. Zahlungseingang für eine Bestellung, sollten zuverlässig aufrechterhalten werden und dürfen im Falle eines Fehlers nicht verloren gehen. Einige Nachrichten können nur Abfragedaten enthalten, wobei der Verlust der Daten nicht entscheidend ist, da die Abfrage wiederholt werden kann. In diesem Fall gilt die Leistung als wichtiger als die Datenintegrität.

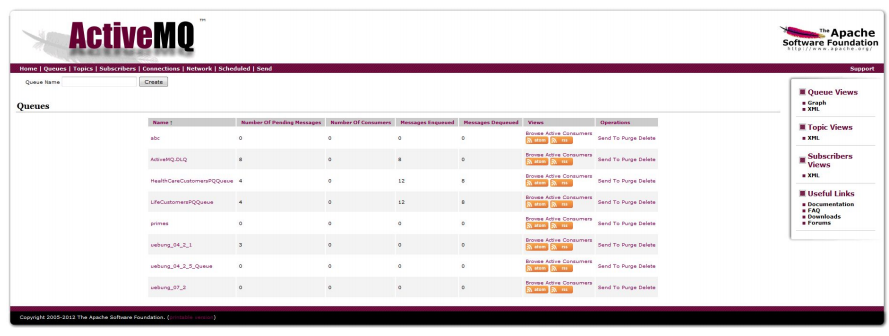
**Persistente Nachrichten**  
IBM MQ verliert keine anhaltende Nachricht durch Netzwerkfehler, Lieferfehler oder Neustart des Warteschlangenmanagers. Jeder Warteschlangenmanager hält ein fehlertolerantes Wiederherstellungsprotokoll aller Aktionen, die bei persistenten Nachrichten ausgeführt werden. Dieses Protokoll wird manchmal als Zeitschrift bezeichnet

**Nicht-persistierende Nachrichten**  
IBM MQ optimiert die Aktionen, die auf nicht persistenten Nachrichten für die Leistung durchgeführt werden. Die nicht-persistente Nachrichtenspeicherung basiert im Systemspeicher, so dass es möglich ist, dass sie in Situationen wie Netzwerkfehlern, Betriebssystemfehlern, Hardwarefehlern, Warteschlangenmanager-Neustart und internem Softwarefehler verloren gehen können.

### MS MQ

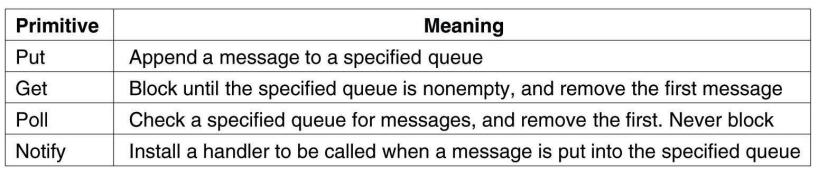
Message Queuing (MSMQ) -Technologie ermöglicht es Anwendungen, die zu unterschiedlichen Zeiten laufen, um über heterogene Netzwerke und Systeme zu kommunizieren, die vorübergehend offline sein können. Anwendungen senden Nachrichten an Warteschlangen und lesen Nachrichten aus Warteschlangen. Die folgende Abbildung zeigt, wie eine Warteschlange Meldungen enthalten kann, die von mehreren Sendeanwendungen erzeugt und von mehreren empfangenden Anwendungen gelesen werden. Es ist Bestandteil von Windows aber nicht installiert/aktiviert im Default Setup.

### Active MQ



### MOM API Primitives (Platform-Independet Level)

Write (Put), Consuming Read/Receive (Get) – Synch and asynchronous (event-or callback-based), Non-Consuming Read/Receive (Browse) – Like top() in stack.



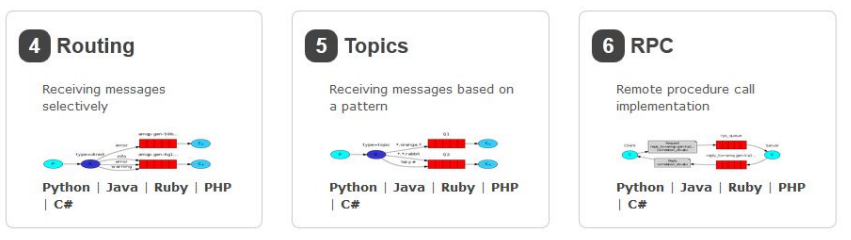
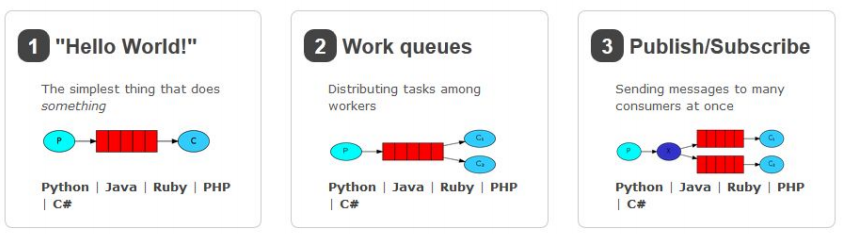
## Enterprise Integration Patterns

Siehe Vorlesungfolien.

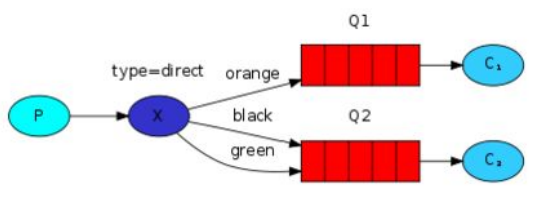
## RabbitMQ (based on AMQP)

### Patterns

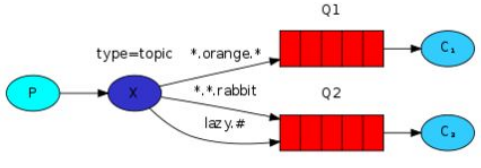
Basierend auf dem AMQP (Advanced Message Queueuing Protocol)



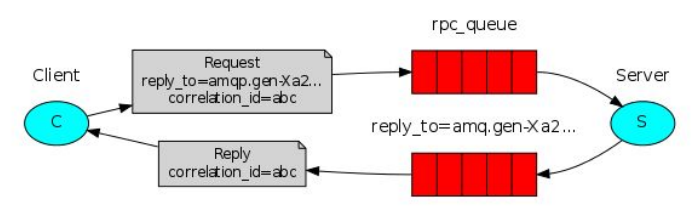
#### Routing

Beispiel von einem direkten Austausch mit zwei gebundenen Warteschlangen. Die erste Warteschlange ist mit dem Key «Orange» gebunden, die zweite Warteschlange hat zwei Bindings von schwarz und green. Die Zustellung erfolgt entsprechend den Bindings. Alle anderen Nachrichten werden verworfen.

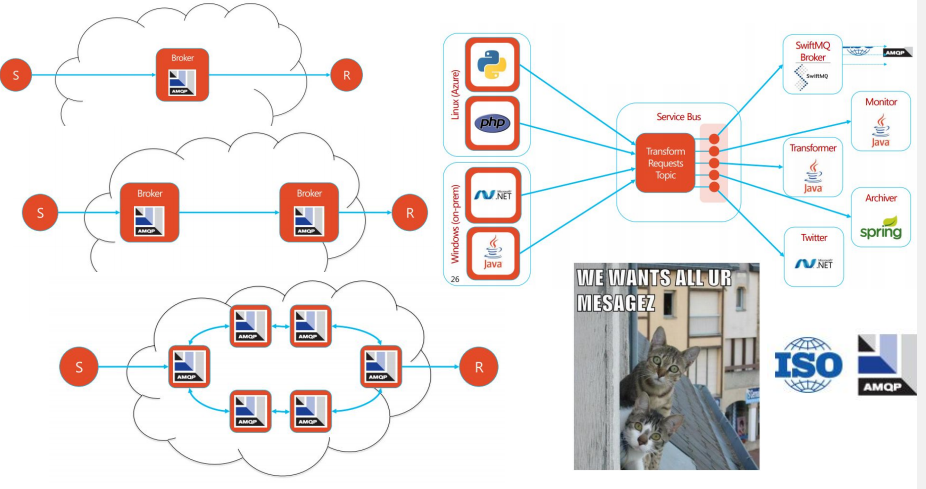
#### Topics

In this example, messages describe animals. Messages have a routing key that consists of three words .. Q1 is bound "\*.orange.\*" and Q2 with "\*.\*.rabbit" and "lazy.#". Q1 is interested in all the orange animals. Q2 wants to hear everything about rabbits, and everything about lazy animals. Messages with "quick.orange.rabbit" will be delivered to both queues. Messages "lazy.orange.elephant" also will go to both of them. "quick.orange.fox" will only go to the first queue, and "lazy.brown.fox" only to the second. "lazy.pink.rabbit" will be delivered to the second queue only once, even though it matches two bindings. "quick.brown.fox" doesn't match any binding so it will be discarded. 

#### RPC

Wenn der Client startet, erstellt er eine anonyme, exklusive Callback-Warteschlange. Für eine RPC-Anforderung sendet der Client eine Nachricht mit zwei Eigenschaften: reply\_to, die auf die Callback-Warteschlange und correlation\_id gesetzt ist, die für jede Anfrage auf einen eindeutigen Wert gesetzt wird. Die Anforderung wird an eine rpc\_queue-Warteschlange gesendet. Der RPC-Arbeiter (aka: server) wartet auf Anfragen auf diese Warteschlange. Wenn eine Anforderung erscheint, führt sie den Job aus und sendet eine Nachricht mit dem Ergebnis an den Client zurück, wobei die Warteschlange aus dem Feld reply\_to verwendet wird. Der Client wartet auf Daten in der Rückrufwarteschlange. Wenn eine Meldung erscheint, prüft sie die Eigenschaft cororrect\_id. Wenn es dem Wert aus der Anfrage entspricht, gibt er die Antwort an die Anwendung zurück.

#### AMQP Adanved Message Queueing Protocol



# RMI und Web Services

## Remote Procedure Calls (RPC)

Da spricht man von einer Technik zum Aufbau von verteilten Client-Server Applikationen. Es erweitert die Notation der lokalen Aufrufe um die Remote Procedure Aufrufe (Calls) und macht damit das Client-Server Model einfacher zu programmieren.

Es verdeckt somit die Details des Netzwerks und isoliert die Applikation von den physischen und logischen Elementen der Datenkommunikation. Ein RPC ist wie ein Funktionsaufruf, welcher man mit Parametern aufrufen kann.

### Events während einem RPC

1. Der Client ruft den client stub auf. Dieser Aufruf ist ein lokaler Call, welcher die Parameter auf den Stack legt.
2. Der Client stub packt die Parameter in eine Nachricht und macht einen Systemaufruf um die Nachricht zu versenden. Die Packetierung heisst «Marshalling».
3. Das lokale OS sendet die Nachricht von der Client Maschine zur Server Maschine.
4. Das lokale Server OS gibt die Packete an den Sever Stub weiter.
5. Der Server Stub entpackt die Parameter aus der Nachricht.
6. Der Server Stub ruft abschliessend die Server Prozedur auf. Die Antwort macht den gleichen Weg, einfach umgekehrt.

### Potentielle Fehler

Der Client sendet eine Request-Nachricht zu einem entfernten Server um eine bestimmte Prozedur mit den angegeben Parametern auszuführen. Der Remote Server sendet eine Antwort an den Client, welcher dann sein Programm weiterfährt. Während der Server den Aufruf verarbeitet ist der Client typischerweise geblockt und wartet auf die Antwort. RPC können aufgrund von Netzwerkproblemen fehlschlagen. Der Aufrufer muss also mit sollen Problemen umgehen können ohne zu wissen, dass der RPC nicht angekommen ist..

## RMI (Java Remote Method Invocation)

RMI ist ein Teil des OO-Ansatzes von Java. Er kann komplette Objekte als Argumente und Return-Werte mitgeben und nicht nur vordefinierte Datentypen. So können Sie auch ganze Hash-Tables übermitteln.

Somit ist es mögliche die volle Power der OO-Technologie auf in verteilten Systemen zu verwenden. Denn RMI macht es einfach Java Servers und Java Client zu schreiben, welche auf die Server zugreifen. Das Remote Interface ist ein Java Interface. Der Server hat nur ein paar Zeilen Code um den Server zu beschreiben, alles andere wie Java-Objekte.

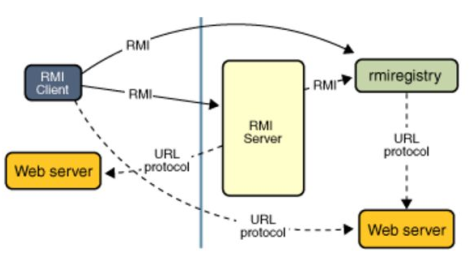
### Zwei Programme – Client und Server

Ein typisches Server-Programm erstellt einige entfernte Objekte, macht Verweise auf diese Objekte zugänglich und wartet darauf, dass Clients Methoden auf diesen Objekten aufrufen. Ein typisches Client-Programm erhält eine Remote-Referenz auf ein oder mehrere entfernte Objekte auf einem Server und ruft dann Methoden auf sie auf. RMI stellt den Mechanismus zur Verfügung, mit dem der Server und der Client kommunizieren und Informationen hin und her versenden.

Eine verteilte Objekt-Applikation braucht folgendes:

* Lokalisieren von Remote Objekten
* Kommunikation mit Remote Objekten
* Laden der Klassendefinitionen, von den Objekten welche mitgegeben werden

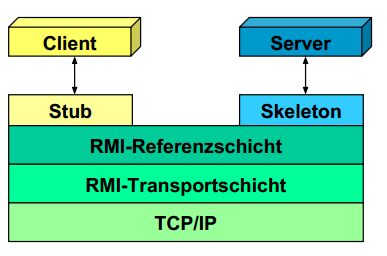
### RMI Registry benutzen um eine Referenz eines Java-Objekts zu erhalten

Der Server ruft die Registriy auf um den Namen mit einem Remote-Objekt zu binden. Der Client schaut dann nach dem Remote Objekt mit dem Namen in der Server Registry und ruft eine Methode darauf auf. Das RMI System nutzt Webserver um die Klassendefinitonen zu laden (Client-Server und Server-Client).

### Businesslogik nur auf dem Server

RMI kann die Klassenimplementationen vom Client auf den Server verschieben und umgekehrt. Beispielsweise können Sie eine Schnittstelle für die Prüfung von Mitarbeiter-Expense-Reports definieren, um zu sehen, ob sie mit der aktuellen Firmenpolitik übereinstimmen. Wenn ein Expense Report erstellt wird, kann ein Objekt, das diese Schnittstelle implementiert, durch den Client der Server abgerufen werden. Wenn die Richtlinien geändert werden, beginnt der Server, eine andere Implementierung dieser Schnittstelle zurückzugeben, die die neuen Richtlinien verwendet. Die Einschränkungen werden daher auf der Client-Seite überprüft und sorgen für eine schnellere Rückmeldung an den Benutzer und weniger Belastung des Servers - ohne eine neue Software auf dem System des Benutzers zu installieren. Dies gibt Ihnen maximale Flexibilität, da die Änderung von Richtlinien erfordert, dass Sie nur eine neue Java-Klasse schreiben und sie einmal auf dem Server-Host installieren.

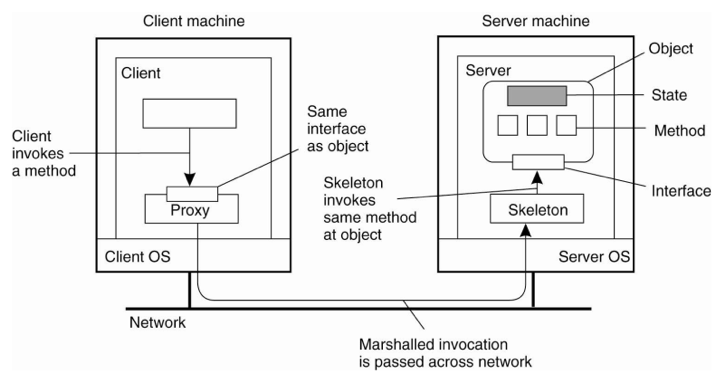
### Architektur

Ein Stub ist ein Stellvertreterobjekt (Remote Proxy), das die Clientaufrufe an den Server weiterreicht.

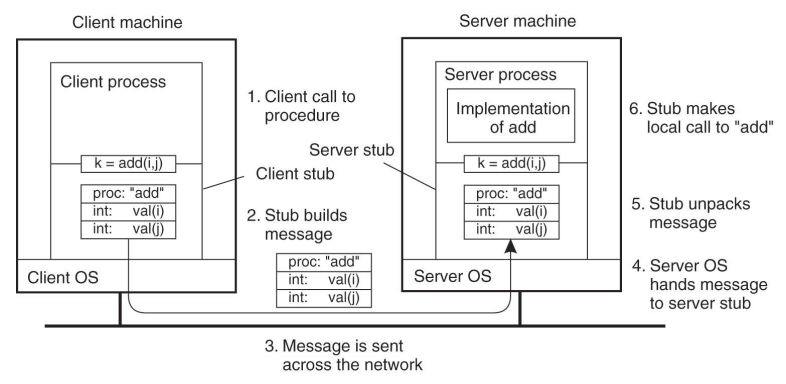
Ein Skeleton nimmt Aufrufe des Stubs entgegen und leitet sie an ein Serverobjekt weiter.

Die RMI-Referenzschicht stellt den Namensdienst (=Registry) zur Verfügung. Die RMI-Transportschicht verwaltet Verbindungen und wickelt die Kommunikation ab.

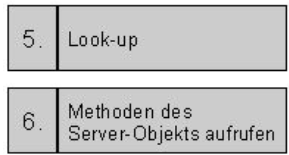
### Klassen und Interfaces

Die Interfaces definieren die Methoden. Die Klassen implementieren die Methode der Interfaces. Ein Objekt wird zu einem Remote-Objekt wenn es das Remote Interface implementiert (java.rmi.Remote).

### Innvolvierte Schritte



### Schritte vor einem RMI Aufruf



|  |  |
| --- | --- |
| Stub-Klasse in RMI (Remote Proxy) Die Stub-Klasse baut eine Socket-Verbindung zum Server auf (Connect-Call). Sie schickt Namen der Methode und Parameter und holt das Ergebnis ab. | Skeleton-Klasse in RMI Erzeugt das Server-Socket, der den Port aus dem Stub bindet (bind/listen/accept). Wartet dann auf den Methodenaufruf vom Client und delegiert diesen an ein Objekt. Zu letzt liefert es einen Rückgabewert über die Socketverbindung an den Client zurück. |

### RMI-Programmierung auf der Serverseite

|  |  |
| --- | --- |
| **Interface für Remote-Methoden**  Wird von den beiden Rollen (Client und Server) benötigt. Es muss von Remote aus dem java.rmi Package abgeleitet sein. Alle Methoden müssen eine RemoteException werden. Die Remote-Interfaces haben fachliche Namen ohne Suffix. | **Klasse zur Implementierung des Remote-Interfaces**  Es implementiert das Interface (in diesem Fall «Hello». Jedes entfernte Objekt ist eine Unterklasse von UnicastRemoteObject. Es wird ein Konstruktor benötigt, welcher die RemoteException wirft. |
| **Remote-Objekte erzeugen und in RMI-Registry anmelden**  Auf dem Server-Rechner wird ein Objekt der Implementierungsklasse erzeugt. Es wird unter dem Namen remoteHello beim Rechner registriert. Standard-Port-Nummer für den rmiRegistry-Prozess auf dem Server ist 1099. | RMI-Programmierung auf dem Client |

### Schwächen von RMI

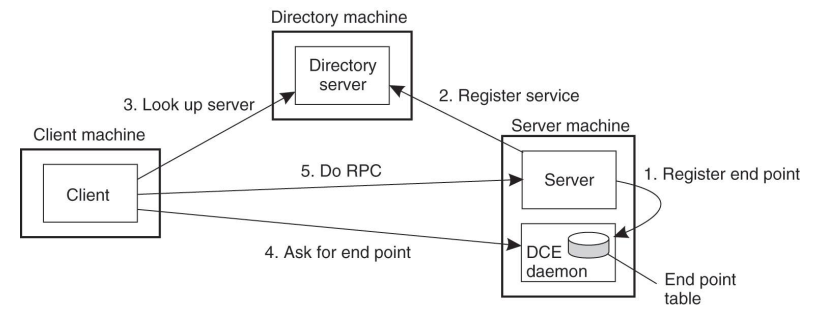
* «The exception that grounded an airline» (Kein Timeout Management.)
* Java versions differ in the way they implement RMI
* All CORBA problems when RMI is used with Java Enterprise Edition
* Practical project experience 🡺 nur wenige nutzten es in purer Form
  + MOM oder http werden heute bevorzugt.

## Interface Description Languages (IDLs)

### Einführung

Ein IDL ist eine Spezifikationssprache, mit der Programmierschnittstellen sprachunabhängig beschrieben werden können. IDLs werden verwendet, um die Kommunikation zwischen Clients und Servern in Remote Procedure Calls (RPC) aufzubauen.

### DCE (Distributed Computing Environment) from the 1990s



#### IDP Processing Steps

#### IDL Verwendung

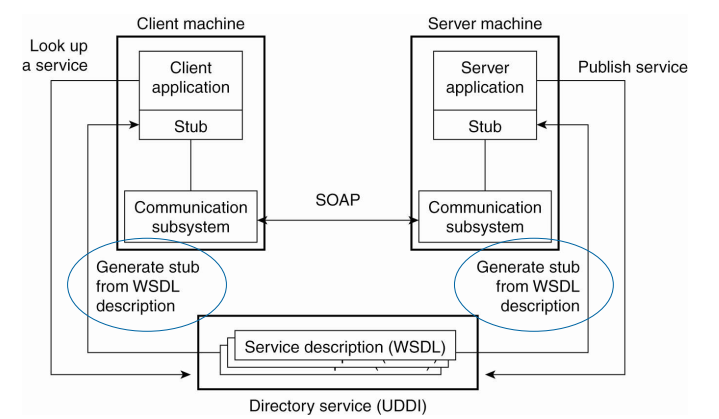
OMG IDL basiert auf DCE IDL von den 1990s. Es benutzt CORBA und unterstützt den RMI Compiler und die .NET Tools. Es hat ein eigenes Typensystem welches die Programmierspezifikationen abstrahiert.

## Web Services

### Einführung

WSDL ist eine XML-basierte Schnittstellendefinitionssprache, die verwendet wird, um die Funktionalität eines Webdienstes zu beschreiben. Maschinell lesbare Beschreibung, wie der Service aufgerufen werden kann, welche Parameter es erwartet und welche Datenstrukturen es zurückgibt. Standard, maschinenlesbares Format, aus dem Clients und Skelett eines Service automatisch erstellt werden können. Entwicklet wurde es von IBM, Mircosoft und Ariba.

### Architektur



### RPC vs. Document

|  |  |
| --- | --- |
| **RPC Style SOAP Nachrichten**  Es ist um die Annahme gebaut, dass du den Web-Service anrufen möchtest, genau wie du eine normale Funktion oder Methode nehmen würdest, die Teil deines Anwendungscodes ist. Der Nachrichtentext enthält für jeden "Parameter" der Methode ein XML-Element. Diese Parameter-Elemente werden in ein XML-Element eingehüllt, das den Namen der aufgerufenen Methode enthält. |  |
| **Document Style Web Service** Es erlaubt Ihnen, alle Daten, die Sie wollen, in XML einzuschließen und auch ein Schema für dieses XML zu enthalten. Dies bedeutet, dass der Client- und Server-Anwendungscode die Marshalling- und Unmarshalling-Arbeit durchführen müssen. Dies steht im Gegensatz zu RPC, in dem der Marshalling / Unmarshalling-Prozess von der SOAP-Bibliothek abgewickelt wird. |

### Vor-und Nachteile von RPC und Document WSDL Styles

**RPC WSDL-Stil** schafft eine enge Kopplung zwischen Dienstanbieter und Client. Das Ändern der Reihenfolge der Parameter oder der Typen der Parameter ändert die Definition des Web Service selbst (so wie es die Definition einer normalen Funktion oder Methode beeinflusst).

**Dokument WSDL-Stil-Services** implementieren eine lose gekoppelte Art der Interaktion zwischen Dienstanbieter und Client. Der Hauptunterschied des Dokumentenstils auf den RPC-Stil besteht darin, dass der Client die Serviceparameter in einem normalen XML-Dokument an den Server sendet, anstatt einen diskreten Satz von Parameterwerten von Methoden. Es gibt keine direkte Zuordnung zwischen den Serverobjekten (Parameter, Methodenaufrufe usw.) und den Werten in XML-Dokumenten. Der Hauptnachteil des Dokumentenstils besteht darin, dass es keine Standardmethode gibt, welche Methode des Webdienstes die Anfrage beantragt.

### Schwächen von Web Services

* Ausführlichkeit von XML
  + SOAP envelope size (normalerweise 4-20 mal grösser als der Payload)
* WSDL Sprache Design
  + Es gibt zu viele redundante Elemente in WSDL 1.1
  + Von WSDL 2.0 gibt es nur wenige Implementationen
* Notwendigkeit von Spezifikationen und Generatoren
  + Die REST Community sagt das es die formalen Service Contracts und die Code Generation nicht braucht.

# Operationale Modelle, Design for Performance

## Non-Functional Requirements (NFRs)

Nicht-funktionale Anforderungen (oder NFRs) definieren die wünschenswerten Qualitäten eines Systems und die Einschränkungen, innerhalb derer das System aufgebaut werden muss

**Qualitäten** definieren die Eigenschaften und Merkmale, die das gelieferte System nachweisen sollte. **Einschränkungen** sind die Einschränkungen, Standards und Umweltfaktoren, die in der Lösung berücksichtigt werden müssen.

### Constraints

Die Geschäftsaspekte des Projekts, die Geschäftsumgebung des Kunden oder die IT-Organisation, die die Architektur beeinflussen. Das technische Umfeld und die vorherrschenden Standards, die das System und das Projekt in Betrieb nehmen müssen.

### Qualities

Runtime-Qualitäten sind "messbare" Eigenschaften, die oft als "Service Level Requirements" ausgedrückt werden.

Qualitäten könnten auch mit den Entwicklungs-, Wartungs- oder Betriebsanliegen zusammenhängen, die zur Laufzeit nicht ausgedrückt werden.



### SEI Software Engineering Institute

#### Quality Attributes des Technical Reports

Der Report stammt zwar aus dem Jahre 1995, es ist aber zu grossen Teilen heute immer noch aktuell. Zu den Attributen zählen folgende Begriffe: Availability, Compliance, Maintainability, Performance, Privary, Recovery, Resilience, Scalability und Usability.

### Relevante Standards

* NFR nach ISO 9126
* ISO 25010 (Mehrheitlich eine Aktualisierung des ISO 9126)

### QoS Summary

Trotz fortgesetzter technologischer Fortschritte verbringen IT-Architekten erheblichen Zeitaufwand um den Anforderungen an Servicequalität gerecht zu werden. Die aufgrund der signifikanten Einschränkungen. Software sowie Infrastruktur Design soll iterativ geplant werden um dieses Ziel zu erreichen.

Nicht-funktionale Anforderungen und Service-Levels können vertraglich bindend sein. Eine Nicht-Einhaltung kann in der IT einen Penalty bedeuten und resultiert dann in einer Strafzahlung.

Modellierungstheorie, Techniken und Werkzeuge stehen zur Verfügung, um bei der Bewertung von Designalternativen zu helfen. Unabhängig von der Qualität des Designs muss die Qualität der Umsetzung durch Testing überprüft werden.

Der Aufwand sollte immer proportional zum Risiko sein.

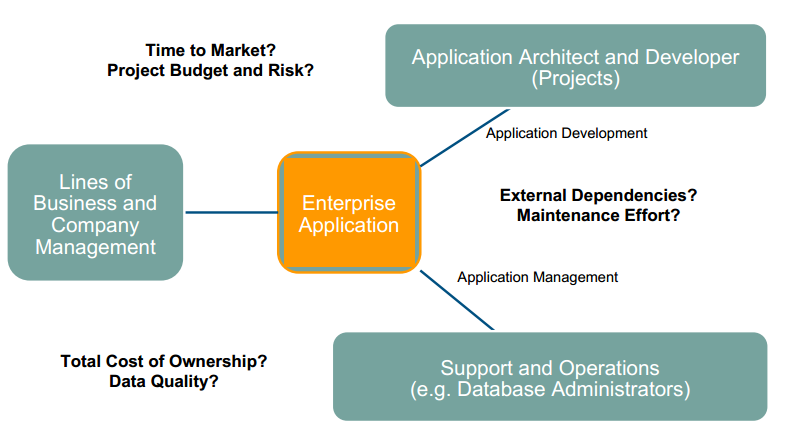
### Beispiel für Design Tradeoff – Security vs. Performance

Ein Kompromiss ist eine Situation, bei der es darum geht, eine Qualität oder einen Aspekt von etwas im Gegenzug zu verlieren, um eine andere Qualität oder einen Aspekt zu gewinnen.

**Herausforderungen für Architekten und Designer**

* Verschiedene NFRs können miteinander in Konflikt stehen
* Verschiedene Stakeholder können unterschiedliche Prioritäten haben
* Unzureichende Informationen stehen zur Verfügung
* Informationen können sich änder

#### Stakeholders und ihre Bedenken



Die beste Technik zur Verringerung des Risikos einer schlechten Dienstqualität ist es, die Qualitäten von Anfang an zu betrachten. Fixen Sie es früh und sparen sich damit Geld und Probleme, welche später auftauchen.

## Performance NFR

### Was ist Performance

**Definition**  
"Performance. Der Grad, zu dem ein System oder eine Komponente seine beabsichtigten Funktionen innerhalb vorgegebener Einschränkungen, wie Geschwindigkeit, Genauigkeit oder Speicherverbrauch, erfüllt. "

**Im Allgemeinen**  
Rechtzeitigkeit der Reaktion und Vorhersagbarkeit sind die beiden Hauptziele. "Schneller" ist nicht immer genug, wie zum Beispiel ein Echtzeit-System eine äußerst gleichbleibende Leistung erfordert.

### Performance Mythen

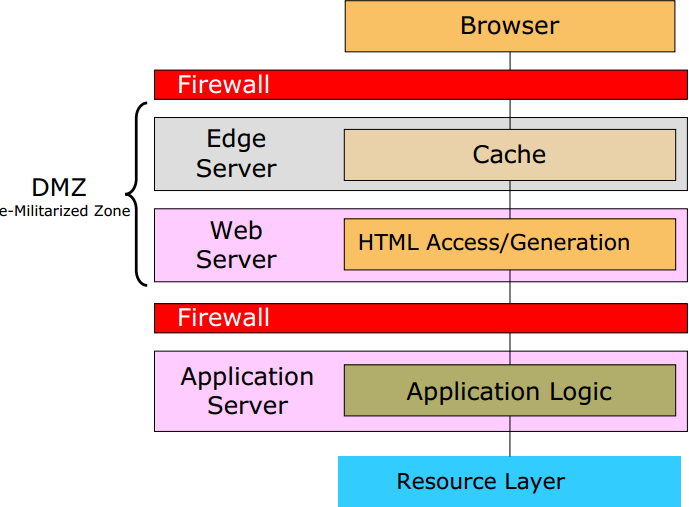
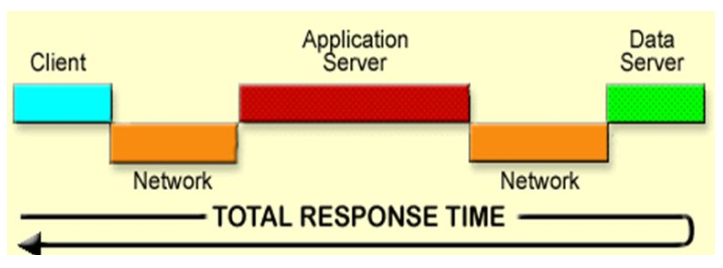
* CPU ist billig
  + Aufsummierung der Ineffizienz (auf der Serverseite)
* Concurrency verbessert immer die Performance
  + Ist nicht so. Kommunikation und Synchronisation haben auch Kosten
* Caching verbessert die Performance
  + «In memory caching speeds up applications until it slows them down.»

### Die drei Hauptaspekte der Performance

|  |  |
| --- | --- |
| **Antwortzeiten**  On-Line Antwortzeiten, Batch Durchlaufzeiten |  |
| **Durchsatz**  Transaktionen pro Sekunde, Records verarbeitet pro Stunde |
| **Kapazität**  Komponenten Sizing um den Load bewältigen zu können |

### End-zu-End Antwort Zeit

Ist die Summe der Antwortzeit aller Komponenten.



**Die Ansprechzeiten verschlechtern bei hoher Auslastung.**

## Component and Operational Modeling

### Functional Model (Components) / Operational Model (Nodes)

Deployment Units = Eine Kollection von Komponenten, welche auf Nodes plaziert sind.

### UML Komponenten Modelle

|  |  |
| --- | --- |
| **Componenten Relationships** Server provided, Services requried (Dependencies) | **Hierarchies** “contains” – Relationship between components |
| **Schließen der Lücke zwischen den Anforderungen (das "Was") und der Lösung (das "Wie")**  Leitfaden und stellen Sie den Kontext für das Design ein, damit er die funktionalen und nicht funktionalen Anforderungen erfüllt (z. B. Erweiterbarkeit oder Wartbarkeit, etc.). Es visualisiert das System und hilft es zu begreifen. | |

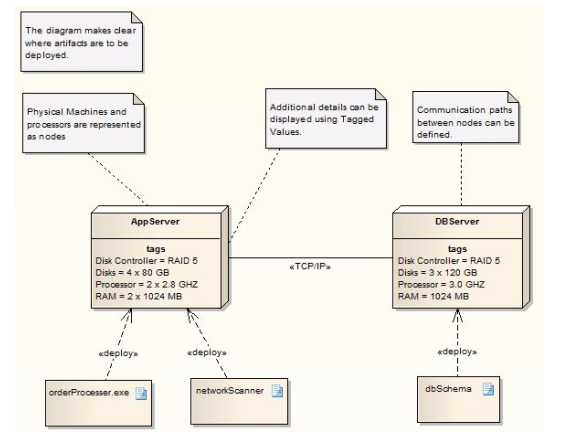
### Operational Model

Es repräsentiert die System Infrastruktur Architektur. Die geografische Struktur der Standorte und deren Grenzen, über die das IT-System eingesetzt und betrieben wird. Die Platzierung der Knoten des Systems in diese Orte. Die Verbindungen zwischen den Knoten. Die Organisation der Systemelemente in Zonen. Sowie Sizing und andere Hardware-Spezifikationen für alle Computer, Speichergeräte und Netzwerk-Technologien.

|  |  |
| --- | --- |
| **Locations** | **Logical Operational Model** |

***Deployment Units*** = Klebstoff zwischen logischer Sicht (Komponentenmodell) und Infrastruktursicht (Einsatz / Betriebsmodell). Denn das Component Modeling und das Operational Modelling beeinflussen sich gegenseitig.

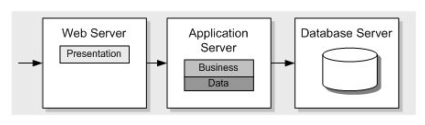
#### UML Deployment Diagramm



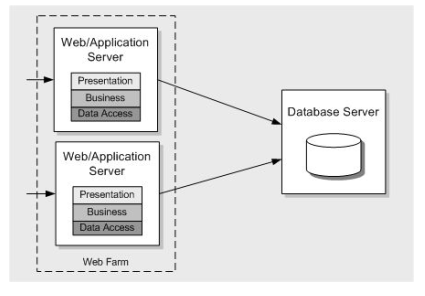
## MSDN Deployment patterns

### Nicht-verteiltes Deployment

### Verteiltes Deployment

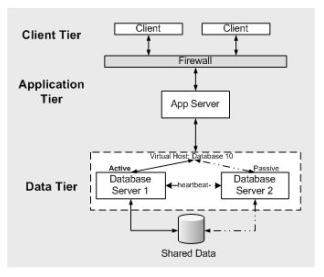


### Webfarm



### Load-balancing cluster

### Failover Cluster



# Design for Scalability and Availability

## Scalability NFR

### Scalability

Die Skalierbarkeit ist die Fähigkeit des Aushaltens von sich erhöhenden Workloads, ohne die SLA zu brechen. Natürlich unter der Voraussetzung, dass die Ressourcen auch erhöht werden.

**Linear scalability**  
Dies ist der meiste Fall. Der Mögliche Workload ist abhängig von den zur Verfügung stehenden Ressourcen.

Dafür gibt es drei verschiedene Wege. Entweder arbeitet man härter / schnell (durch Erhöhung des Speeds), man arbeitet smarter (Besser Algorithmen) oder man holt sich «Hilfe» indem man Parallelität einführt.

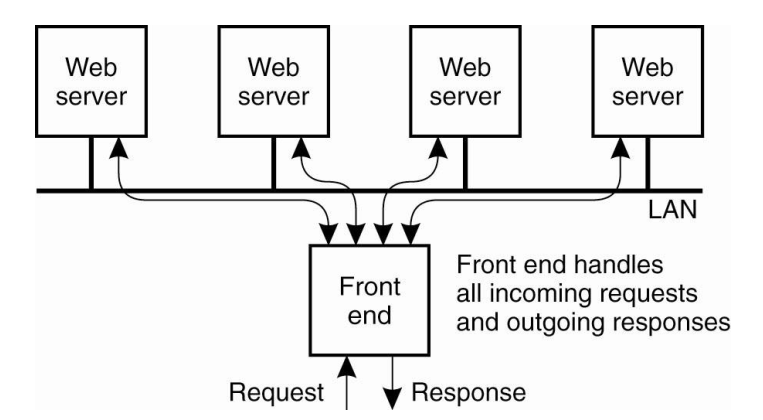
### Scalability Types

**Generation Scalability (Technology Evolution)**  
Bessere, schnellere, grossere Komponenten, welche durch neue Technologien ermöglicht warden.

**Vertical Scalability (Scale Up)**Das Erhöhen der Performance der individuellen Servers (CPU, Storage, bandwidth).

**Horizontal Scalability (Scale Out)**  
Das Erhöhen der Server bzw. Links.

### Horizontal Scaling (Scale Out)



### Load Balancer

Ein Load Balancer wird zwischen dem Internet und dem Unternehmens Backend-Server installiert.

Er fungiert als der einzige Point-of-Presence-Knoten des Unternehmens im Internet, auch wenn das Unternehmen mehrere Back-End-Server aufgrund der hohen Nachfrage oder einer großen Menge an Inhalt verwendet. Zudem fängt Datenanforderungen von Clients ab und leitet jede Anfrage an den Server weiter, der derzeit die Anfrage füllen kann.

**HA (High availability)**  
Kann durch die Installation eines Backups Load Balancer erreicht werden, um zu übernehmen, wenn die primäre vorübergehend ausfällt. Die Verfügbarkeit erfolgt durch Parallelität, Lastverteilung und Failover-Unterstützung.

Load Balancer verbessert die Verfügbarkeit und Skalierbarkeit einer Website durch transparente Clustering von Content-Servern. Wenn ein Server ausfällt, wird dieser nicht belastet.

### Edge Servers – IP Spraying

Ein Edge Server (Load Balancer) hat eine eigene virtuelle IP Adresse. Die Applikationsserver haben alle ihre eigenen physikalischen IP Adressen.

**IP Spraying**  
Verteilt die Last auf Server in einem Cluster (Satz von Servern, die dieselbe Anwendung ausführen, und können den Clients denselben Inhalt zur Verfügung stellen).

Load Balancer sendet Anfragen für virtuelle IP-Adressen an eine oder mehrere oder die physikalischen IP-Adressen. (Nach Round Robin, Least-Recently-Used, Workload-Based).

**Beispiele**

* HAProxy
* Nginx
* WebSphere Application Server Edge Componentes

### Session Affinity / Sticky Sessions

Session Affinität überschreibt den Load-Balancing-Algorithmus, indem er alle Anfragen in einer Session an einen bestimmten Applikationsserver weiterleitet. Session Affinität verwendet Cookies, um Sitzungsinformationen zu verfolgen und potenziell Anmeldeinformationen zu pflegen. Session-Affinität füllt diese Cookies mit einer Session-ID, die die folgenden Informationen enthält:

* Ein **Bezeichner** für die Wiederherstellung von Sitzungsdaten
* **Routing-Informationen**, um sicherzustellen, dass alle Anfragen in dieser Sitzung immer auf denselben Anwendungsserver weitergeleitet werden

## Availability NFR

Ein System gilt als «available», wenn es läuft und richtige Ergebnisse liefert und ndere NFRS zu treffen, zum Beispiel Reaktionszeit. Die Verfügbarkeit eines Systems ist der Bruchteil der Zeit, die es Verfügbar ist. Je mehr Fehler das ein System hat, desto weniger ist es verfügbar. Gleichst gilt, je länger es dauert ein System zu reparieren nach einem Fehler, je weniger verfügbar ist es.

### Availability – Gründe für Fehler

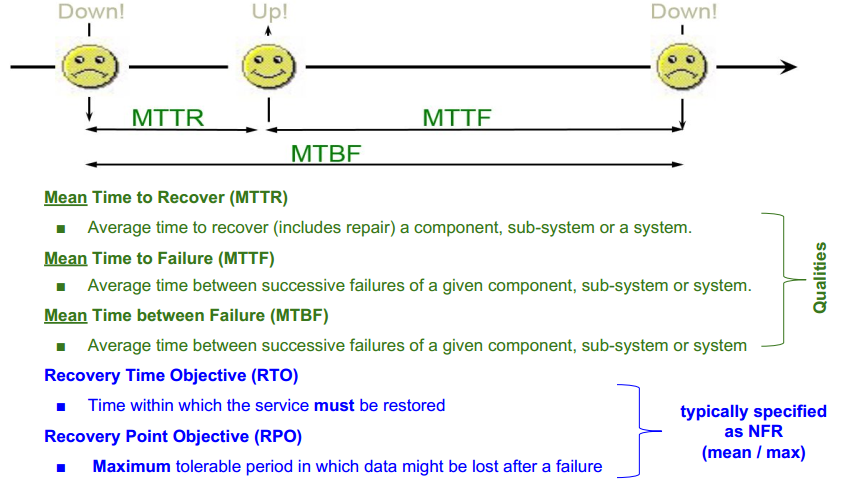
**Aspekt 1 – Architektur und Umwelt**

* Kommunikationssysteme
  + Mehr Zahlen für unterbruchsfreiere Leitungen
  + Mehr als eine Leitung im Einsatz haben (am besten von verschiedenen Anbietern)
* Power
  + Battery Backup, damit der Main Memory noch erhalten bleibt
  + UPS
* Air Conditioning
* Höhere Gewalt
  + Bunker, Backup in einer anderen Region

**Aspekt 2 – System Management**  
Auch der beste Operator wird das System irgendwann zum Fallen bringen. Daher lassen sich dort Vorkehrung treffen. Zum einen die Automatisierung, redundante Maintenance Procedures, sodass der Operator mindestens zwei Sachen falsch machen muss, weiteres Training und nicht zuletzt Konfigurationstools, welche das Ausmass einer Änderung aufzeigen. Bei Software Installation sind dies Prozeduren, welche keinen Neustart benötigen.

**Aspekt 3 - Transiente Softwarefehler**

### Key Availability Terms



### Was heist 99.99x Availabilty?

24x7 Verfügbarkeit ist nahe zu unmöglich. Dies geht sehr in die Kosten.



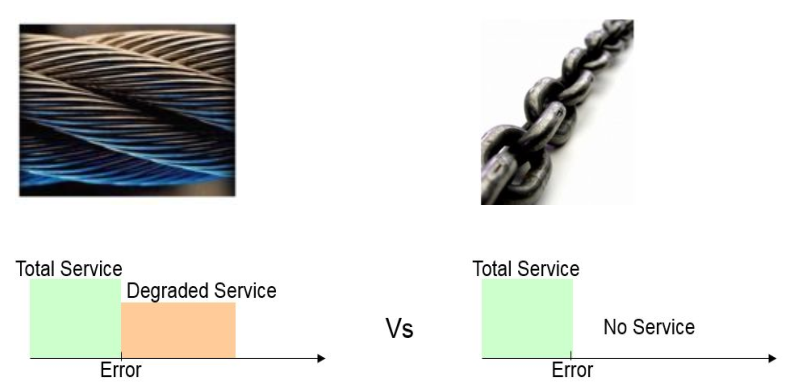
### Cost

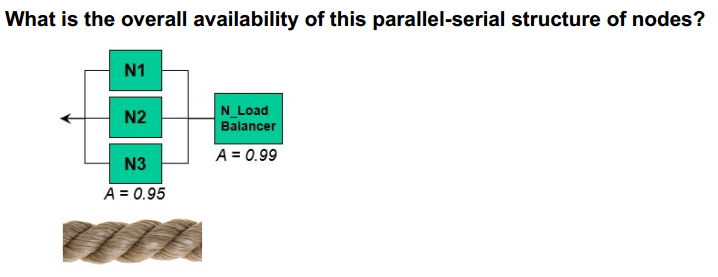
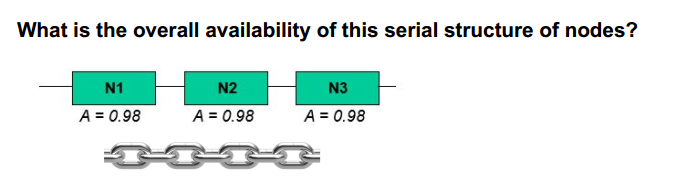
|  |  |
| --- | --- |
| **Cost of Availability** | **Cost of downtime vs. cost of availability optimization** |
| **Cost of Downtime in Several Domains** | |

### Using components

|  |  |
| --- | --- |
| **In Series** | **In Parallel** |

### Serial vs. Parallel Availabilty

**Analogie**  




## Techniques to improve the availability of a (distributed) system

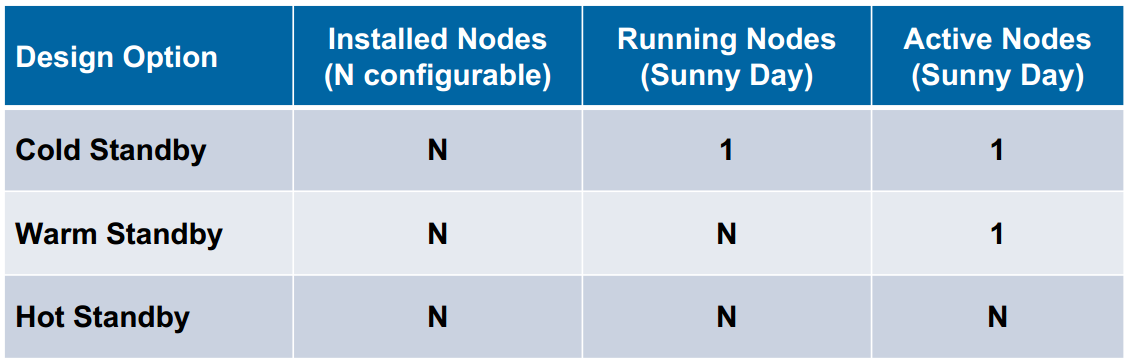
### Avoid Single Points of Failure

### Redundancy

Schlagwörter hier sind Clusters, Warm Backups und Hot Backups.

**Warm Backup**  
Wenn der Fehler erkannt wird, wird der Backup-Server sofort zum primären Server und erholt sich nach dem letzten nicht wiederherstellbaren Betrieb des ehemaligen Primärs in den Zustand. MTTR wird reduziert, da die Zeit für die Erstellung des Prozesses für den Backup-Server nicht benötigt wird.

**Hot Backup**  
Die Kopplung zwischen Primär- und Backup ist sehr dicht. Die beiden Server laufen immer synchron, sodass der Backup sofort übernehmen kann. Diese Lösung ist sehr kostenintensiv, da eigentlich jede Komponente doppelt ausgelegt werden muss.



### Detect failures as fast as possible

Die Zeit vom Versagen, den Fehler zu detektieren, trägt zu MTTR bei, d.h. verringert die Verfügbarkeit! Das Prinzip Fail Fast kann hier eingesetzt werden.

# VSS-Management

## Wieso und Was?

|  |  |
| --- | --- |
| System Management | Configuration Management |

### IT Infrastructure Library (ITIL) 🡺 Service Management Framework

|  |  |
| --- | --- |
|  |  |

## System Management Patterns

Systems Management Patterns zur Überwachung und Steuerung von Message- / Queuing-basierten verteilten Softwaresystemen.

|  |  |
| --- | --- |
| **Wire Tap**  Überprüfen Sie Nachrichten, die auf einem Punkt-zu-Punkt-Kanal fahren. Verbrauchen Sie Nachrichten aus dem Eingangskanal und veröffentlichen die Nachrichten, die nicht am Zielkanal modifiziert sind auf einem separaten Prüfkanal. Da die Inspektionslogik in einer zweiten Komponente ist, ist der Wire Tap generisch und wiederverwendbar |  |

|  |  |
| --- | --- |
| **Detour** Vermitteln Sie eine Nachricht durch Zwischenschritte, um Validierung, Test oder Debugging durchzuführen. Kontextbasierter Router: In einem Zustand leitet der Router eingehende Nachrichten durch zusätzliche Schritte, während er im anderen die Nachrichten direkt an den Zielkanal leitet. Komponenten im Umweg können die Nachricht überprüfen und / oder ändern. Letztendlich führen diese Komponenten die Nachricht an das ursprüngliche Ziel. |  |

|  |  |
| --- | --- |
| **Test Message** Sicherstellung der Gesundheit einer Nachrichtenverarbeitungskomponenten. Identifizieren von Nachrichtenverarbeitungskomponenten, die aktiv Nachrichten verarbeiten, aber ausgehende Nachrichten aufgrund eines internen Fehlers verwerfen. |  |

|  |  |
| --- | --- |
| **Smart Proxy** Verfolgen / Überprüfen von Nachrichten an / von einem Dienst, der Antwortnachrichten an die vom Anforderer angegebene Rücksendeadresse sendet (d.h. die Rücksendeadresse ist in der Anforderungsnachricht enthalten, das einfache Wire-Tap-Muster funktioniert nicht). Smart Proxy fängt Nachrichten ab, die an den Service gesendet werden. Smart Proxy speichert die vom ursprünglichen Absender angegebene Rücksendeadresse. SmartProxy ersetzt die Rücksendeadresse in der Nachricht mit eigener Adresse. Wenn eine Antwortnachricht eingeht, ruft der Smart Proxy die gespeicherte Rücksendeadresse ab und leitet die unveränderte Antwortadresse an den ursprünglichen Anforderer weiter. |  |

|  |  |
| --- | --- |
| **Message Store** Erfassen Sie Informationen über jede Nachricht an zentraler Stelle. Jede Komponente sendet Duplikate an den zentralen Message Store. Um die resultierende Netzwerkverkehrszunahme zu minimieren, können Sie nur Schlüsselfelder duplizieren, die für Systemverwaltungs- und Protokollierungszwecke erforderlich sind, z. B. Nachrichten-ID, Zeitstempel usw. |  |

|  |  |
| --- | --- |
| **Message History** Erstellen Sie eine Liste aller Anwendungen, die die Nachricht seit ihrer Entstehung durchlaufen hat, um bei der Analyse und dem Debugging des Nachrichtenflusses zu helfen. Jede Komponente, die die Nachricht verarbeitet (einschließlich des Originators), fügt einen Eintrag zur Liste hinzu. Die Nachrichtenhistorie wird normalerweise im Nachrichtenkopf gespeichert, so dass sie von dem Nachrichtentext getrennt ist, der anwendungsspezifische Daten enthält. |  |

|  |  |
| --- | --- |
| **Channel Purger** Eliminieren Sie 'left-over' Nachrichten (von vorherigen, möglicherweise fehlgeschlagenen Tests), so dass sie nicht neue Tests oder das laufende System stören. Entfernen einer einzelnen Nachricht oder eines Satzes von Nachrichten, die auf bestimmten Kriterien basieren, z. B. Nachrichten-ID oder die Werte bestimmter Nachrichtenfelder (insbesondere erforderlich, um Probleme bei der Ausführung von Produktionssystemen zu beheben) |  |

## Java Management Extensions (JMX)

Verwalten und Überwachen von Anwendungen, Systemobjekten und Geräten (z. B. Druckern).

**Drei Level Architektur**

* **Probe Level** (Instrumentierungsebene): enthält die Sonden (MBeans), die die Ressourcen stützen
* **Agent-Level** (MBeanServer): als Vermittler zwischen den MBeans und den Anwendungen
* **Remote Management Level**: ermöglicht es Anwendungen, über Connectors und Adapter auf den MBeanServer zuzugreifen.

### Managed Beans (MBeans)

Implementiert eine Business-Schnittstelle mit Setter und Getter für die Attribute und die Operationen (d.h. Methoden). Stellt eine Ressource dar, die in der virtuellen Java-Maschine ausgeführt wird und über JMX verwaltet und überwacht werden kann. Kann zum Sammeln von Statistiken über Leistung, Ressourcenverbrauch oder Probleme (Pull) verwendet werden. Kann zudem zum Erhalten und Setzen von Anwendungskonfigurationen oder Eigenschaften verwendet werden (Push / Pull). Des weiteren kann es auch für die Benachrichtigung von Ereignissen wie Fehlern oder Zustandsänderungen (Push) verwendet werden.

### JConsole – JMX Client

|  |  |
| --- | --- |
|  |  |

## Logging

### Die Herausforderungen beim verteilten Logging

Das Logging in einer verteilten Umgebung stellt viele weitere Probleme dar:

* Die Logging-Lösung sollte für einen Entwickler einfach zu bedienen, über verschiedene Anwendungen wiederverwendbar und erweiterbar auf neue Bedürfnisse zugeschnitten sein.
* Die Protokollierung sollte zu einem einzigen Punkt zentralisiert werden, damit ein Administrator von einem Ort aus darauf zugreifen kann.
* Die Protokollierung sollte wenig Einfluss auf die Anwendungsleistung haben.
* Die Logging-Lösung sollte die Meldungen über die Konfiguration nach Art filtern, um bestimmte Ereignisse auszulösen. Dazu gehören Dinge wie die Aufrechterhaltung der Nachricht und die Durchführung von Alarm Benachrichtigung, wie Paging an einen Administrator.
* Die Protokollierungsumgebung sollte eine zentrale und lokale Protokollierung ermöglichen, indem sie verschiedene Typen identifiziert.

### Logging Szenarios und Log Formate

Log-Inhalt sollte Entwickler und Betreiber während der Unterstützung unterstützen bei…

* **Ereignis-Korrelation** über verteilte Knoten
* **Ursachenanalysen** (auf dem Weg von Symptomen zu Korrekturmaßnahmen)
* **Event-Stürmen** (hohe Anzahl von Ereignissen, z. B. während der Peak-Workload oder wenn ein Denial-of-Service-Angriff durchgeführt wird)

### Splunk

|  |  |
| --- | --- |
| Log-Konsolidierung mit spezialisierten operativen Intelligenz-Tools am Beispiel von Splunk (<https://www.splunk.com/de_de> ). | **Data Sources** |
| **Architecture** | **Hierarchical Processing** |

### Tips und Tricks

* Nutzen Sie populäre Logging Frameworks und bauen Sie keine Eigenen (Log4j, Logback)
* Definieren und Verwenden Sie Protokollebenen und die anderen Tags
* Verwenden Sie die Analogie / Metapher eines Notrufs bei der Gestaltung von Log-Formaten

# Component Failure Impact Analysis (CFIA)

**Das Problem**  
Ein einziger Komponentenfehler hat dazu geführt, dass das ganze System abgestürzt ist. Zum Reparieren einer einzigen Komponente muss dann das ganze System heruntergefahren werden. Weitere Probleme können bei der System und Netzwerkdokumentation vorhanden sein, weil sie nicht mehr up-to-date oder dafür gar kein Manual vorhanden ist. Dies führt dazu, dass nur eine spezifische Person das ganze System wiederherstellen kann.

**Component Failure Impact Analysis (CFIA)** ist eine proaktive Verfügbarkeits Management Methode. Sie dient zur Bereitstellung von IT mit der Geschäfts- und Anwenderperspektive und gibt Auskunft darüber, wie sich Defizite in der Infrastruktur und dem Underpinning-Prozess, Verfahren und Service Delivery Fähigkeiten auf den Geschäftsbetrieb auswirken. Anders gesagt eine Methode zur Optimierung der Leistungsfähigkeit der IT-Infrastruktur, der Services und der unterstützenden Organisation, um eine kostengünstige und nachhaltige Verfügbarkeit zu ermöglichen, die es dem Unternehmen ermöglicht, ihre Ziele zu erreichen.

## Der Zweck von CFIA und wie die Resultate genutzt werden können

Der Zweck eines CFIA ist es, Informationen zur Verfügung zu stellen, um sicherzustellen, dass die Kriterien für die Verfügbarkeit und die Wiederherstellung von neuen oder bestehenden IT-Services beeinflusst werden, um die Auswirkungen des Ausfalls des Geschäftsbetriebes und der Nutzer zu verhindern oder zu minimieren.

CFIA kann verwendet werden, um die Auswirkungen auf den IT-Service, die sich aus Komponentenfehlern innerhalb der Technologie ergeben, vorherzusagen und zu bewerten. Die Resultate von einem CFIA kann verwendet werden, um zu ermitteln, wo zusätzliche Resilienz betrachtet werden sollte, um die Auswirkung des Komponentenversagens auf den Geschäftsbetrieb und die Benutzer zu verhindern oder zu minimieren, und wo Verbesserungen an Prozeduren oder Prozessen und Fähigkeiten vorgenommen werden sollten. Dies ist besonders wichtig während der Entwurfsphase, wo es notwendig ist, die Auswirkungen auf die IT-Service-Verfügbarkeit, die sich aus Komponentenfehlern im Rahmen des vorgeschlagenen IT Service Design ergeben, vorherzusagen und zu bewerten.

## Hauptziele

* Identifizieren Sie kritische Verfügbarkeiten und Leistungsrisiken für einige oder alle geschäftskritischen Anwendungen.
* Identifizieren Sie Maßnahmen, die getroffen werden können, um die Wahrscheinlichkeit von Ausfällen zu reduzieren.
* Identifizieren Sie Maßnahmen, die getroffen werden können, um die Zeit zu reduzieren, die es braucht, um diesen Fehler zu erkennen und zu reparieren.

## Typisches Resultat

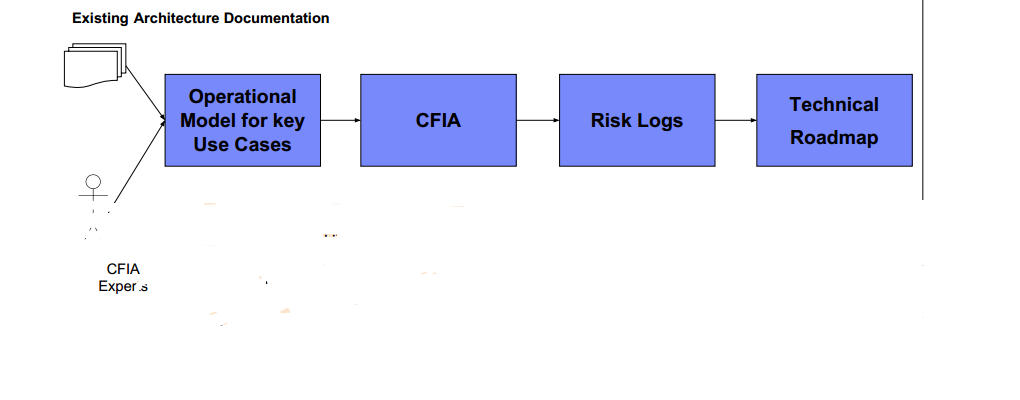
Eine auf Phasen aufgeteilte Lösungsroadmap, welche die technischen, die organisatorischen und die prozessnahen Aspekte behandelt.

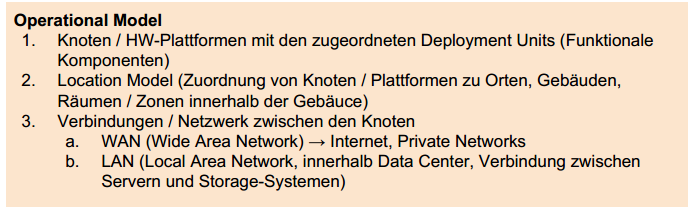
**Phase 1**  
Verbesserungen, die sofort bzw. innerhalb von wenigen Wochen erreicht werden können und müssen.

**Phase 2**  
Hochprioritäre Verbesserungen, die mittelfristig, z. B. innerhalb weniger Monate, erreicht werden müssen und können.

**Phase 3**  
Tiefprioritäre Verbesserungen und Verbesserung, welche eine grundlegend architektonische Veränderung erfordern.

## High-Level Steps





## Beispiel

|  |  |
| --- | --- |
| Gestartet wird mit einem statischen Anblick des logischen Operational Modell. | Gehen dann alle «Architecturall Significant» Use Cases durch und identifiziere alle Verbindungen, Nodes und Komponenten welche involviert sind. |

|  |  |
| --- | --- |
| Die Ausarbeitung auf die physikalische Ebene identifiziert alle Komponenten (Software sowie Hardware) und deren Ausfallmodi für die CFIA. | Beispiele für Symbole, die in einem physikalischen Operationsmodell verwendet werden. |

## Basics CFIA Matrix

Erstellen Sie ein Raster mit Konfigurationselementen (CIs, die Bestandteile, Knoten, Links etc. sein können, je nach den Umständen) auf einer Achse und die IT-Services, die eine Abhängigkeit vom CI haben auf der anderen Achse.

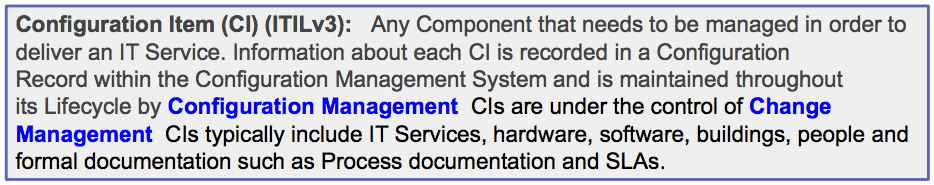
**Die Tabelle sollte wie folgt ausgefühlt werden.**

* Leer lassen, wenn ein Ausfall des CI den Dienst in keiner Weise beeinträchtigt
* Schreiben Sie ein 'X', wenn der Ausfall des CI den IT-Dienst inaktiv macht
* Setzen Sie ein 'A' ein, wenn es einen alternativen CI gibt, um den Service bereitzustellen
* Setzen Sie ein 'M' ein, wenn es einen alternativen CI gibt, aber der Service erfordert manuelle Eingriffe, die wiederhergestellt werden sollen.

### Example of Configurations Items (CIs)

Ein CFIA kann in verschiedenen Graden der Granularität durchgeführt warden.

* Hardwarekomponenten wie Server, Netzwerkkarten, SAN Switches, Netzwerk Switches oder Routers
* Betriebssystemkomponenten wie das OS selber, oder wichtige Services wie TCP/IP
* Middleware Software Komponenten wie Datenbanken, Application Servers, Message Queues oder Workflow Managers.
* Applikationssoftware wie SAP....

**Gemäss ITIL  
**

### How to read the CFIA matrix

CIs, die eine große Anzahl von Xs haben, sind für viele Dienste kritisch und können zu einer hohen Auswirkung führen, falls die Komponente ausfällt.

IT-Dienste mit hohen Zählungen von Xs sind komplex und sind anfällig für Misserfolge.

**Erweitern** Sie dann die CFIA Matrix mit Failure Modes, Failure Effects und Recovery Prozeduren

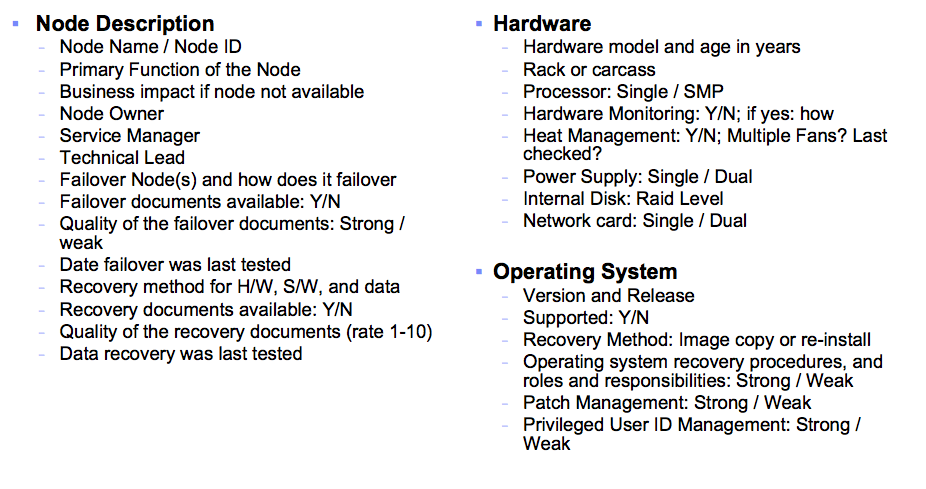
Für jede Komponente beschreiben Sie:

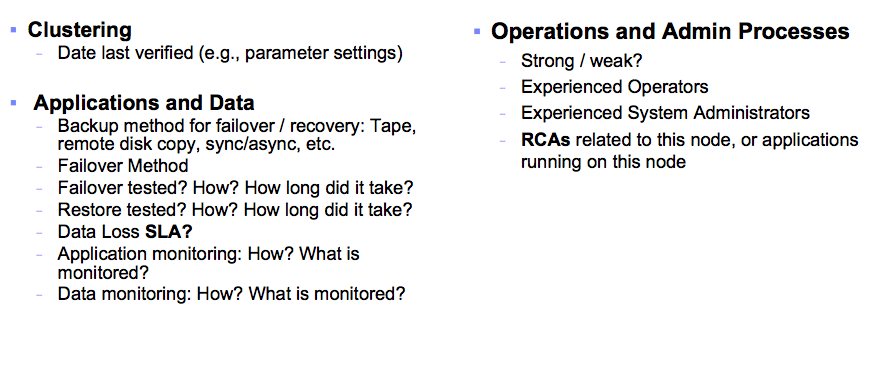
* Was ist es?
* Wie kann es scheitern?
* Wie kann ein Komponentenfehler detektiert werden (Wie schnell?...)
* Was sind die Effekte wenn diese Komponente ausfällt?
* Was sind die Wiederherstellungs oder Failoverprozeduren?



## Node Analysis

Je nach den Umständen und dem Umfang der CFIA untersuchen und dokumentieren sie folgendes:





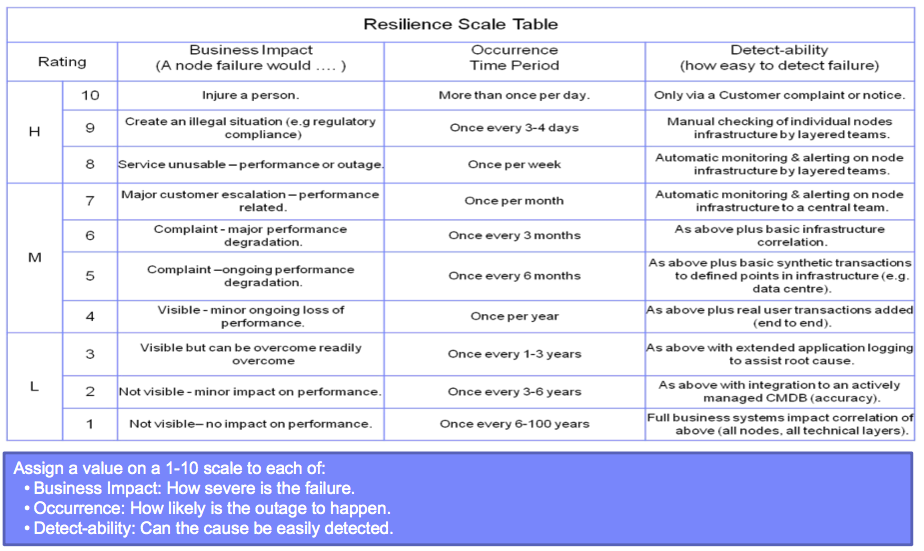
## Risk Log

Dokumentschlüsselbefunde für jeden CI (Knoten, Komponente, Link etc.) zur Unterstützung der Priorisierung von Risiken und Auswahl der Risiken, für die eine Lösung vorgeschlagen wird.

Risiken, die aus der Systemarchitektur vor einer formalen Komplettlösung offensichtlich sind. Risiken, die sich aus der CFIA-Tabelle auf Systemebene ergeben. Risiken, die sich aus der detaillierten "Knoten" -Analyse ergeben. Risiken, die aus früheren Problemsätzen und RCAs entstehen.

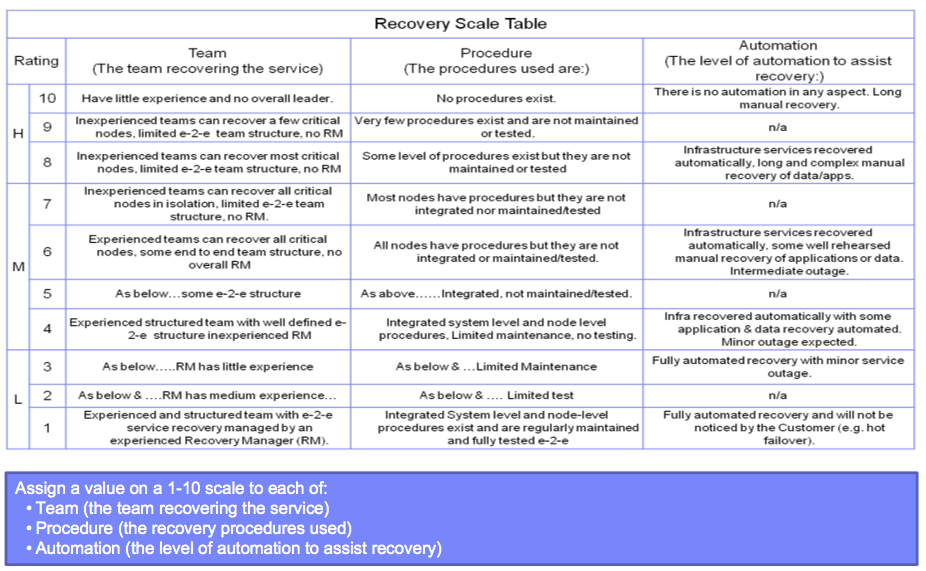
## Resilience Scale Table

Für Resilience Risks, geben Sie ein Risiko-Rating für Auswirkungen, Auftreten und Erkennbarkeit, mit der Rating-Skala in der Resilience Scale Tabelle an.

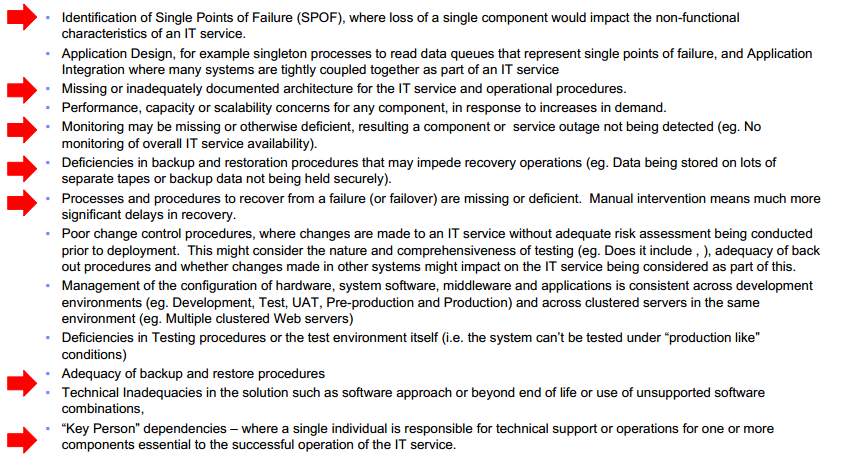


## Recovery Scale Table

Für jedes CI (Knoten, Component, Link, etc.), geben Sie eine Risikobewertung für Teaming, Prozedur und Automation mit der Recovery Scale Tabelle an.



## Cheat Sheet – «Most Popular» Problems



# Vorlesung Woche 10