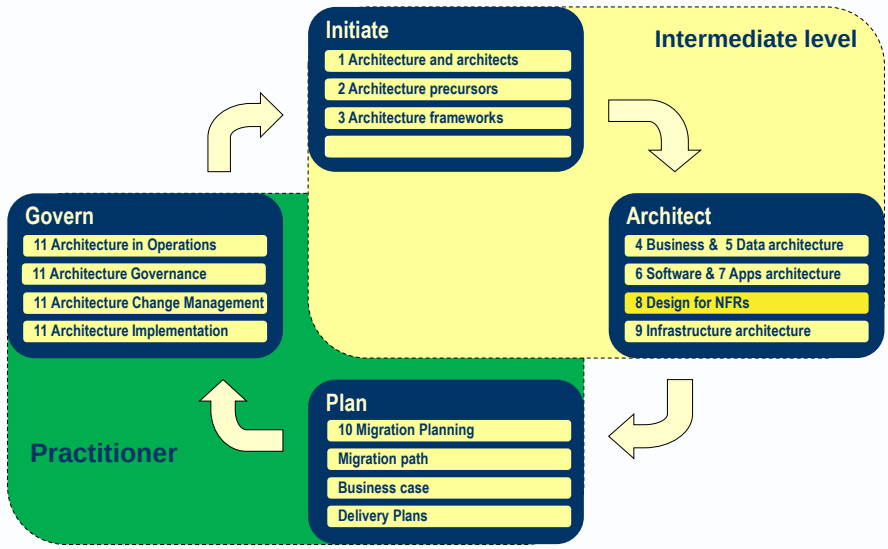
Avancier

Avancier Reference Model

Design for NFRs (ESA 8)

Avancier

8. Design for NFRs



8. Design for NFRs

8. Design for NFRs
NFRs
Design for NFRs bar security
Design for security

Requirements: PARRISSS

Non-functional requirement	A requirement about the ability of a system to perform its functions (whatever they are) effectively and efficiently. Usually quantitatively measurable.
Performance	Subdivides into two measures, often in opposition: •Throughput: number of services executed in a time period. •Response or cycle time (aka latency): time taken from request to response.
Availability	The amount or percentage of time that the services of a system are ready for use, excluding planned down time.
Recoverability	The ability of a system to be restored to live operations after a failure.
Reliability	The mean time between failures. Usually applied to the technologies in the Infrastructure, ignoring the more likely risk of application failure.
Integrity	See Data integrity and Data flow integrity.
Scalability	The ability of a system to grow to accommodate increased work loads.
Security	The ability of a system to prevent unauthorized access to its contents.
Serviceability	The ability of operations team to monitor and manage a system in operation.

Requirements: UMPIIE

Avancier

Usability	The ability of actors to use a system.
Maintainability	The ability of maintenance teams to revise or enhance a system.
Portability	The ability to move a component from one platform to another, or convert it to run on another platform. In practice, it can be difficult to set or estimate this quality metric realistically.
Interoperability	The ability for subsystems to exchange data at the technical level using shared protocols and networks.
Integratability	The ability of interoperable subsystems to understand each other, which requires either common data types or brokers to translate between data types.
Extensibility	A synonym of maintainability

8. Design for NFRs – end of pass 1

Avancier

8. Design for NFRs

8. Design for NFRs
NFRs
Design for NFRs bar security
Design for security

Design for NFRs

Design for performance (response time and throughput)	The general advice is to look for bottlenecks and tackle them one by one. Poor performance is very often the result of poor design, such as •needless distribution of processes, •wasteful use of a network or accesses to a database, •delays and failures caused by message queues filling up. Given a reasonable design, further optimization often involves running processes in parallel.

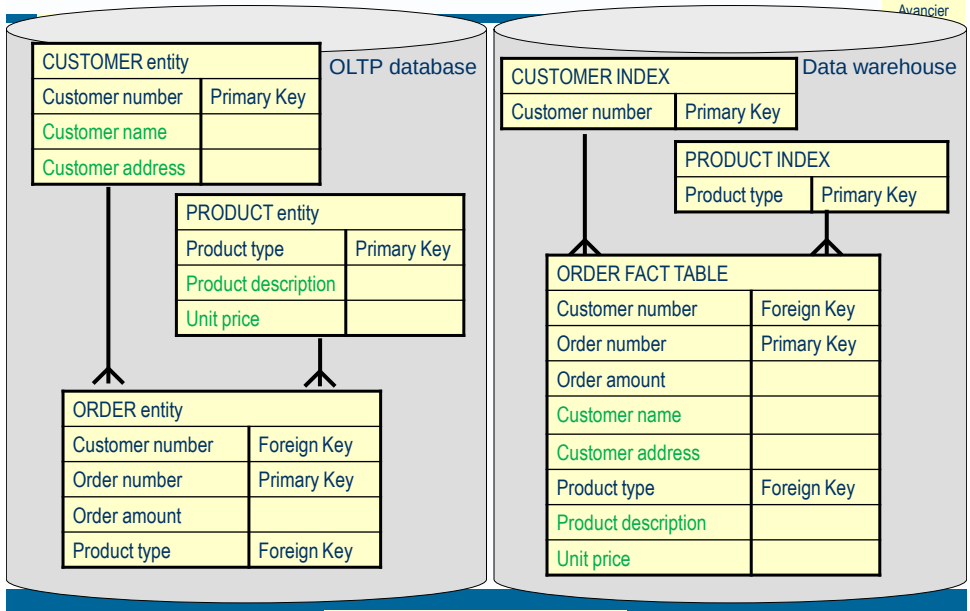
Design for NFRs - Other

Caching	Holding data in a temporary storage area - usually frequently-accessed data. Placing copies of persistent data in a location nearer to the user than the original data source. Generally good for response or cycle time. Can raise concerns about data integrity and security.
Scale up	Increase the power of one processing node. Usually means add resources (processors or memory) to a node on a computer network. Generally good for response time and throughput.
Scale out (aka clustering)	Increase the number of parallel processing nodes. Usually means add more nodes to a cluster. Usually requires some kind of load balancer to sit in front of the cluster and distribute service requests between them. Generally good for throughput. Not necessarily good for response time.

Design for NFRs - Database

Database optimization	Techniques usually involve optimizing processes by devices that eliminate needless database access. Three of many techniques are included in this reference model.
Normalisation	Relational data analysis. A technique for defining a data store structure that assists data integrity by storing each fact once. It also optimizes update processes by minimising redundant data storage.
Denormalisation	A design technique that optimizes input and/or output processes by structuring a data store structure to reflect the most important input or output data flow structures, at the expense of duplicating some stored data.
Index	A list of pointers to elements of stored data. Usually used to optimize output processes. May be temporarily disabled to optimize on-line update processes (and updated later off-line).

Separation of update and reporting databases



Design for NFRs - Database

Access path analysis	Study of the route a process takes through a data store structure. A very common source of performance problems is that an SQL programmer does not know the access path their procedure takes through a database. So it is advisable to use access path analysis and/or employ highly skilled SQL resources for critical database access programs.

Design for AVAILABILITY

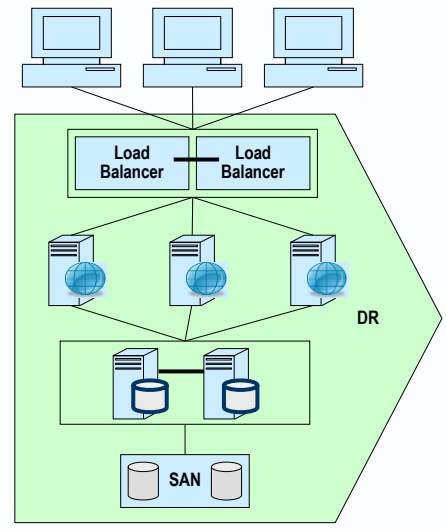
Avancier

Design for resilience (availability and reliability)	The primary technique is to build redundancy into the system. E.g. to scale out, or add one to the number of servers in cluster that calculation or prototyping suggests is needed. Designers can also provide failover capability and/or defensive design and programming techniques.
Fail over	Automatic switch over to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active server, system, or network. Failover happens suddenly and generally without warning.
Defensive design	Designing a client component so that it does not fall over if a server component does not work properly (which implies asynchronous invocation), and designing a server component so that it does not depend on its input data being valid (which implies testing all data types and business rules before processing).The opposite of “design by contract”.

Design for RECOVERABILITY

Avancier

- **Synchronous replication**
  - replicates data storage in real time
    - needs high bandwidth and low latency
    - limited by distance 150K?.
- **Asynchronous replication**
  - replicates data storage off-line
    - makes and keeps copies of data at a remote site
    - operations can be resumed at the remote location using a remote copy.
    - not subject to distance limits.



Design for RECOVERABILITY

Design for recoverability	The principal technique is to back up and provide some kind of switch-over or fail-over procedure. Procedures must address also “fail back”, to return operations from a disaster recovery site to the normal production site.
Back up	A copy of data that may be used to restore the original after data loss. Used in disaster recovery. Also used to restore individual files that have been deleted or corrupted. Backups are typically the last line of defense, coarse-grained and can be inconvenient to use.
Backup site	A location where systems are or can be duplicated. A cold site has no equipment. A warm site has infrastructure but no up-to-date data or software. A hot site has up-to-date software and more or less up to date copies of data.

Design for INTEGRITY

Design for integrity	The two general techniques are to •reduce data replication and •ensure updates are made via ACID transactions. More specific techniques are: •normalize stored data, •switch on automated referential integrity checks, •apply transaction management to update processes, •remove caches, and •consolidate distributed databases.

Design for SERVICEABILITY

Avancier

- This RM entry refers to serviceability of business applications rather than server and network devices

Design for serviceability	The principal technique is to instrument applications so that they report on what they are doing, and how well they are doing it.

8. Design for NFRs

Avancier

8. Design for NFRs
NFRs
Design for NFRs bar security
Design for security

Design for NFRs - Security

Design for security	Design for security is addressed elsewhere in this reference model under the headings of business, data, applications and infrastructure architecture..
ISO/IEC 17799	Information technology: Code of practice for information security management.
ISO/IEC 24762:2008	Information technology — Security techniques — Guidelines for information.
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements.

Design for human and organisation security

Design for human and organisational security	Definition of all the things that can be done outside of software systems to secure business information, such as: • security guards, • locks, • definition and roll out of policies and procedures.

Design for data security

Avancier

Data security	1: Confidentiality alone. 2: A combination of Confidentiality, Integrity and Availability.
Security protection	Prevention of access to data designed to maintain the required data qualities of confidentiality, availability, and integrity.
Security feature	A feature of a system that enables its data and processes to be protected, such as: Encryption, Checksum, HTTPs.
Security policy	A policy that defines which actors have (or do not have) Access rights to objects in a given domain - along with any other protections.
Information domain	A uniquely identified set of objects with a common security policy. Access to any data within the domain limited and constrained by the same rules.
Identity	One or more data items (or attributes) that uniquely label an entity or actor instance. E.g. passport number or user name.

Design for data security

Avancier

Encryption	A process to encode data items (in a data store or data flow) so that they are meaningless to any actor who cannot decode them.
Checksum	A redundant data item added to a message, the result of adding up the bits or bytes in the message and applying a formula. This enables the receiver to detect if the message has been changed. It protects against accidental data corruption, but does not guarantee data flow integrity, since it relies on the formula being known only to sender and receiver.
Digital signature	A cryptographic scheme that simulates the security properties of a handwritten signature. More secure than a check sum, it is said to guarantee the data flow integrity of a message, since the signature is corrupted if the message content is changed.

Application security processes

Avancier

Identification	A process via which an entity or actor reveals their Identity. Usually followed by authentication.
Authentication	A process to confirm or deny that an actor is trusted - is the entity to whom an Identity was given. E.g. A password check. Usually followed by authorisation. Authentication of an actor produces one of four results: true positive, true negative, false negative (which leads to wrongly-denied access) or false positive (which leads to unauthorised access).
Authorisation	A process giving Access to a trusted actor, based on that actor's known Access rights. Usually followed by Access.
Access	A process to look inside a system to find data (or processes) of interest. Data can include files containing executable processes.

Authentication

Avancier

Three-factor authentication	Authentication that involves checking three facts about an identified actor. Factors can include something they •remember (e.g. password, mother's name), •carry (e.g. credit card or key) •are (e.g. biometric data.).

► 3 factor NOT = identity + password + key

Security: Design for infrastructure security

Avancier

Design for infrastructure security	Techniques for protecting client and server computers from malicious access.
Client security	Features that protect client-end computers from malicious access.
Server security	Features that protecting server computers and databases from malicious clients.

Firewalls

Avancier

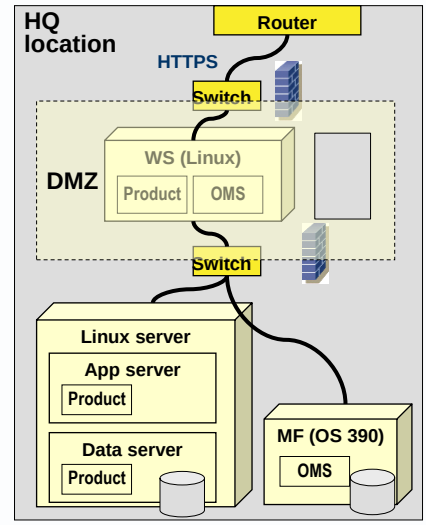
- Firewalls monitor and control access to a particular network
- If properly configured, provide a means of limiting system availability to authorized personnel or devices.
- So use firewalls to keep people out or restrict access to internal security domains.
- But firewalls form only a part of an overall security solution.

Firewall 	Software at the boundary of a network that is used to detect, filter out and report messages that are unauthorised and/or not from a trusted source.

Security: De-Militarised Zone (DMZ)

Avancier

De-Militarised Zone (DMZ)	An area of a network, usually between the public internet and the enterprise network. It uses firewalls to filters out messages that fail security checks. It also contains web servers.



Security: Web security protocols

Avancier

HTTPS	The combination of a normal HTTP interaction over • an encrypted Secure Sockets Layer (SSL) , or • Transport Layer Security (TLS) connection. This ensures reasonable protection of data content from those who intercept the data flow in transit. An HTTPS URL may specify a TCP port. If it does not, the connection uses port 443 (whereas unsecured HTTP typically uses port 80).

Security: web sites

Avancier

Web site security	Usually, a process whereby a web browser checks the public key certificate of a web server at the other end of an **HTTPS** connection. The aims are to check the web server is authentic (who it claims to be) and that messages to/from with the web server cannot be read by eavesdroppers.

Security: Public key certificate

Avancier

Public key certificate	An electronic document that enables a web server to accept https connections, or [a client?] to verify that a public key belongs to an individual. It incorporates a digital signature to bind together **a public key** with **an identity** (the name of a person or an organization, their address, and so forth).

Encrypting File System	Encrypting and decrypting documents.
File recovery	Recovering encrypted files if the EFS certificate is accidentally deleted or damaged.
Server authentication	Verifying the identity of a server to computers that are connecting to it.
Client authentication	Verifying the identity of a computer to a server it is connecting to.
Secure e-mail	Encrypting and digitally signing e-mail.
Code signing	Verifying the publisher of a program. For example, if you download an ActiveX program, its digital signature verifies that it is published by the organization that is listed as the publisher.

Security: Certificate authority

Avancier

Certificate authority	The web site administrator must get a public key certificate signed by a certificate authority. This signature certifies (authenticates) that the certificate holder is the entity it claims to be. Web browsers are generally distributed with the signing certificates of major certificate authorities, so that they can verify web-server certificates.