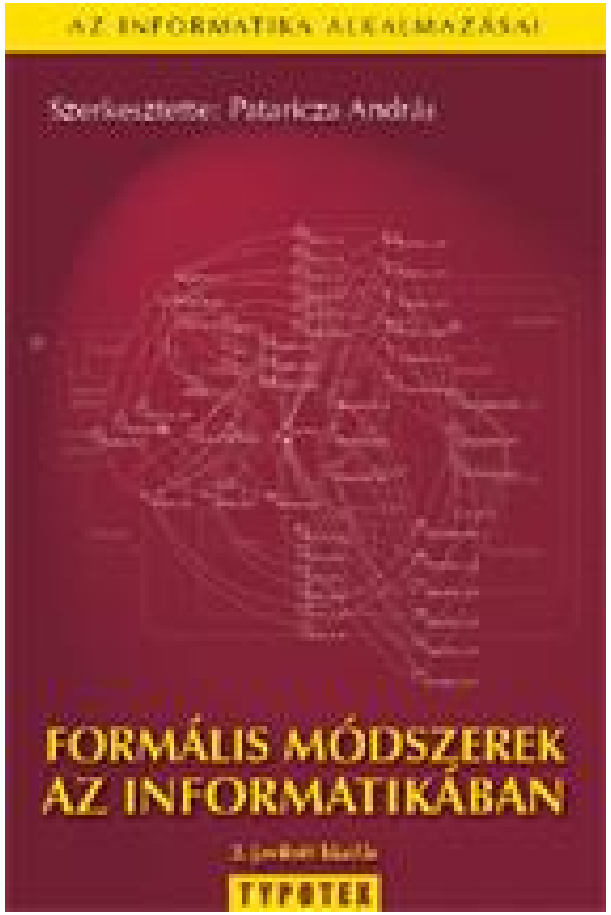
Formális módszerek az informatikában

dr. Pataricza András
és dr. Bartha Tamás előadása alapján
BME Méréstechnika és Információs Rendszerek Tanszék

Időrend



- Február
  - 11
  - 25
- Március
  - 12
  - 26
- Április
  - 2 (Zh)
  - 9
  - 23
- Május
  - 5

Komplex IT alkalmazás

- Tervezés (specifikáció):
  - **együttműködés « interdiszciplinaritás**
    - egyértelműség
    - érthetőség
    - teljesség, ellentmondás-mentesség
  - **szolgáltatásbiztonság**
- Fejlesztés (implementáció):
  - bizonyítottan helyes rendszer:
    - verifikáció
    - validáció
  - **minőség « költség « idő**
  - automatizálás/komponens integráció

iteratív folyamat (életciklus)

fokozatos finomítással (refinement)

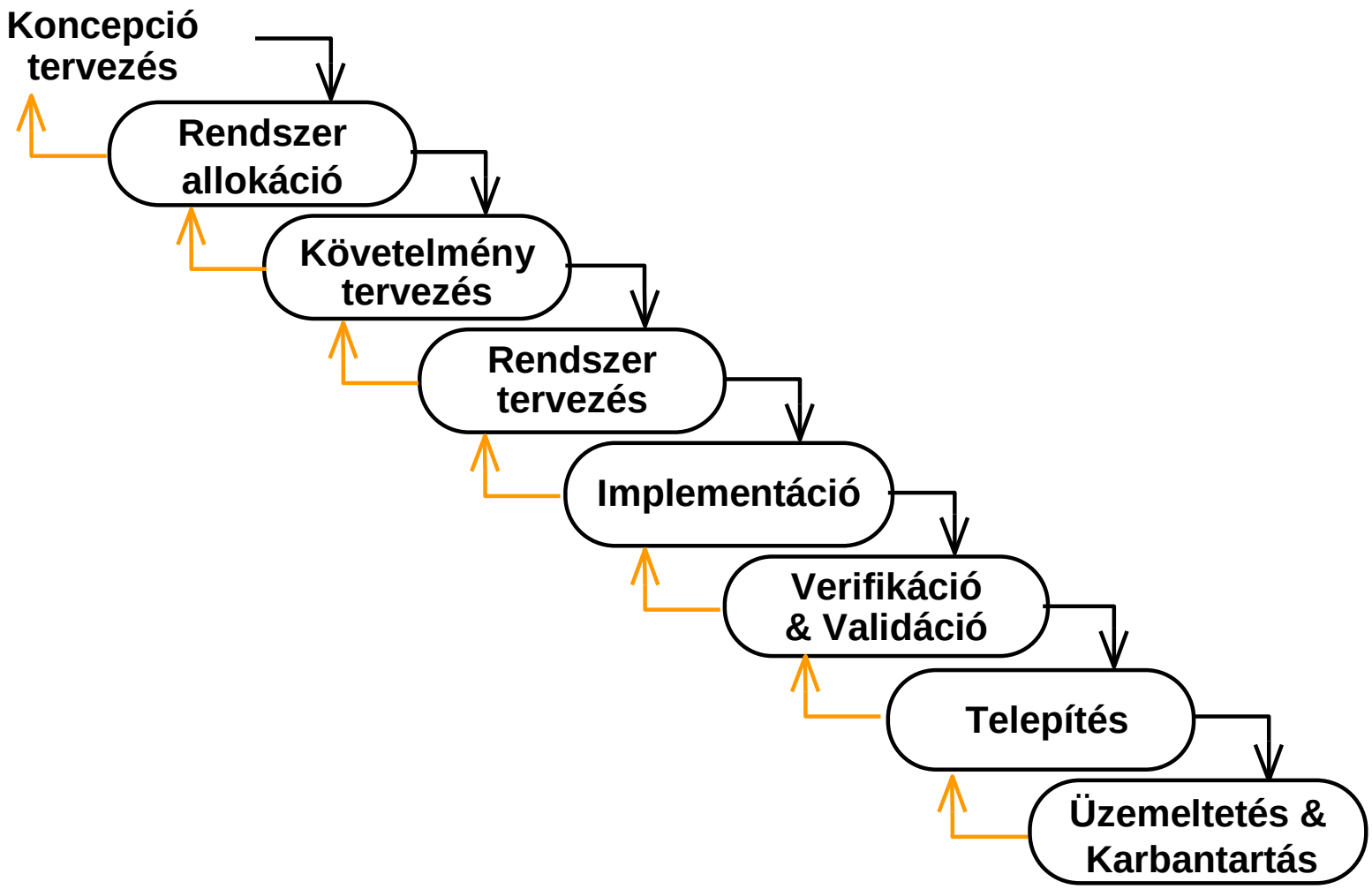
A fejlesztés életciklus modelljei

- Miért van szükség életciklus modellre?
  - Komplexitás kezelése
  - Változások kezelése
    - követelmények, új megoldások
  - Jól definiált fejlesztési fázisok
    - Mérföldkövek
      - ellenőrizhetőség, számonkérhetőség
      - tervezhetőség (pénz, idő)
    - Visszalépés lehetősége
    - Elosztott fejlesztés, integráció

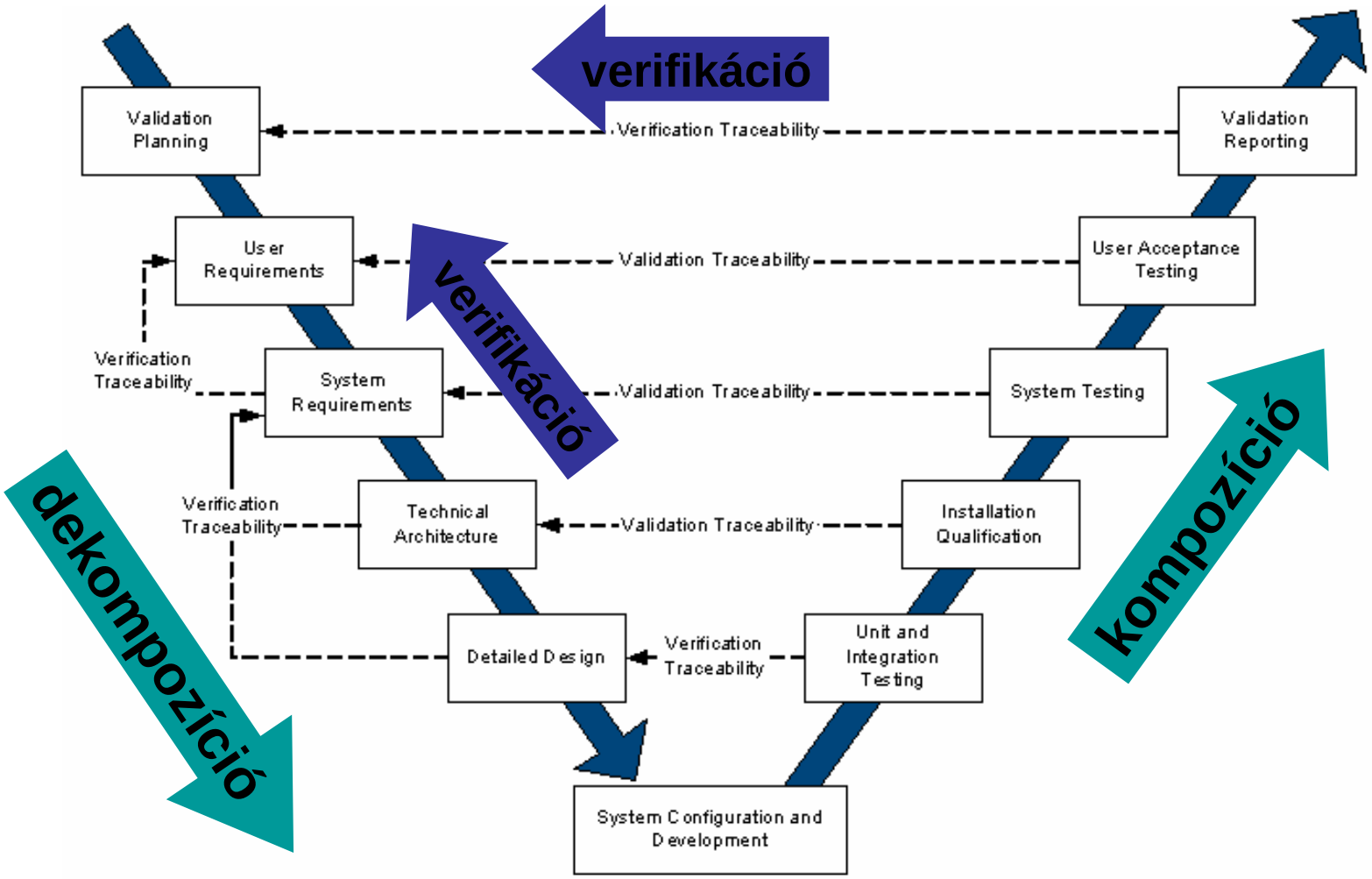
Fejlesztési tevékenységek

Követelményanalízis	Mi a megoldandó probléma?	**Probléma**
Koncepciótervezés	Milyen megoldási módszerek/ eszközök léteznek?	
Rendszertervezés	Hogyan oldható meg a feladat?	Implementáció
Implementáció	Hogyan valósítható meg a feladat megoldása?	
Tesztelés	Megoldottuk a problémát?	
Üzembehelyezés	A megrendelő megfelelőnek tartja a kész rendszert?	
Üzemeltetés, karbantartás	Továbbfejlesztés szükséges?	

Vízesés modell

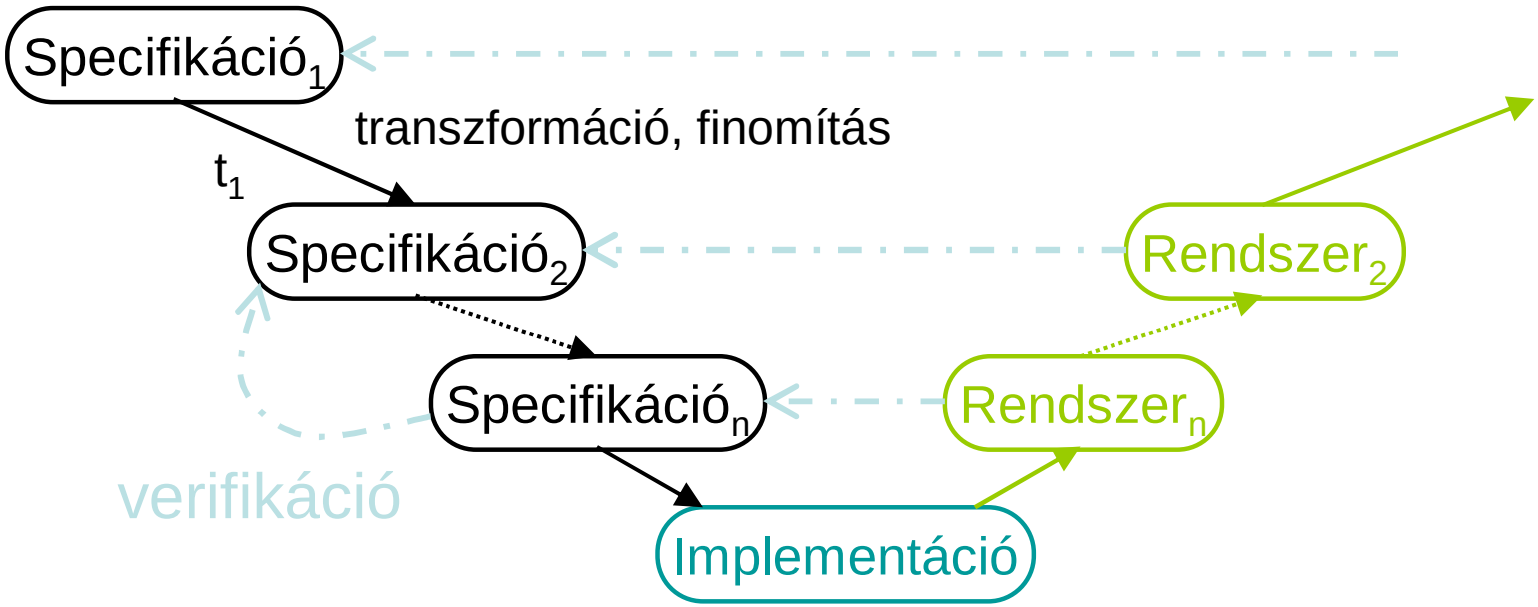


V modell


verifikáció
Validation Planning
Verification Traceability
Validation Reporting
User Requirements
Validation Traceability
User Acceptance Testing
verifikáció
Verification Traceability
System Requirements
Validation Traceability
System Testing
dekompozíció
Verification Traceability
Technical Architecture
Validation Traceability
Installation Qualification
kompozíció
Detailed Design
Verification Traceability
Unit and Integration Testing
System Configuration and Development

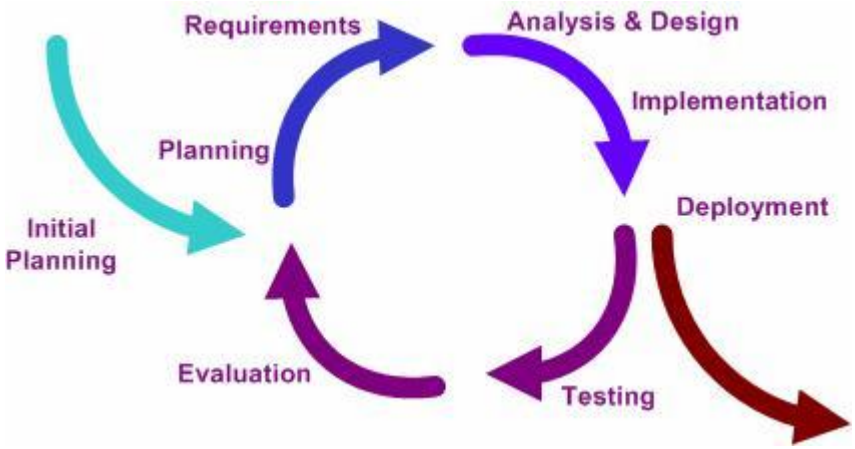
Verifikáció és validáció szerepe

- **Verifikáció**:
  - jól építjük-e a rendszert?
- **Validáció**:
  - jó rendszert építünk-e?

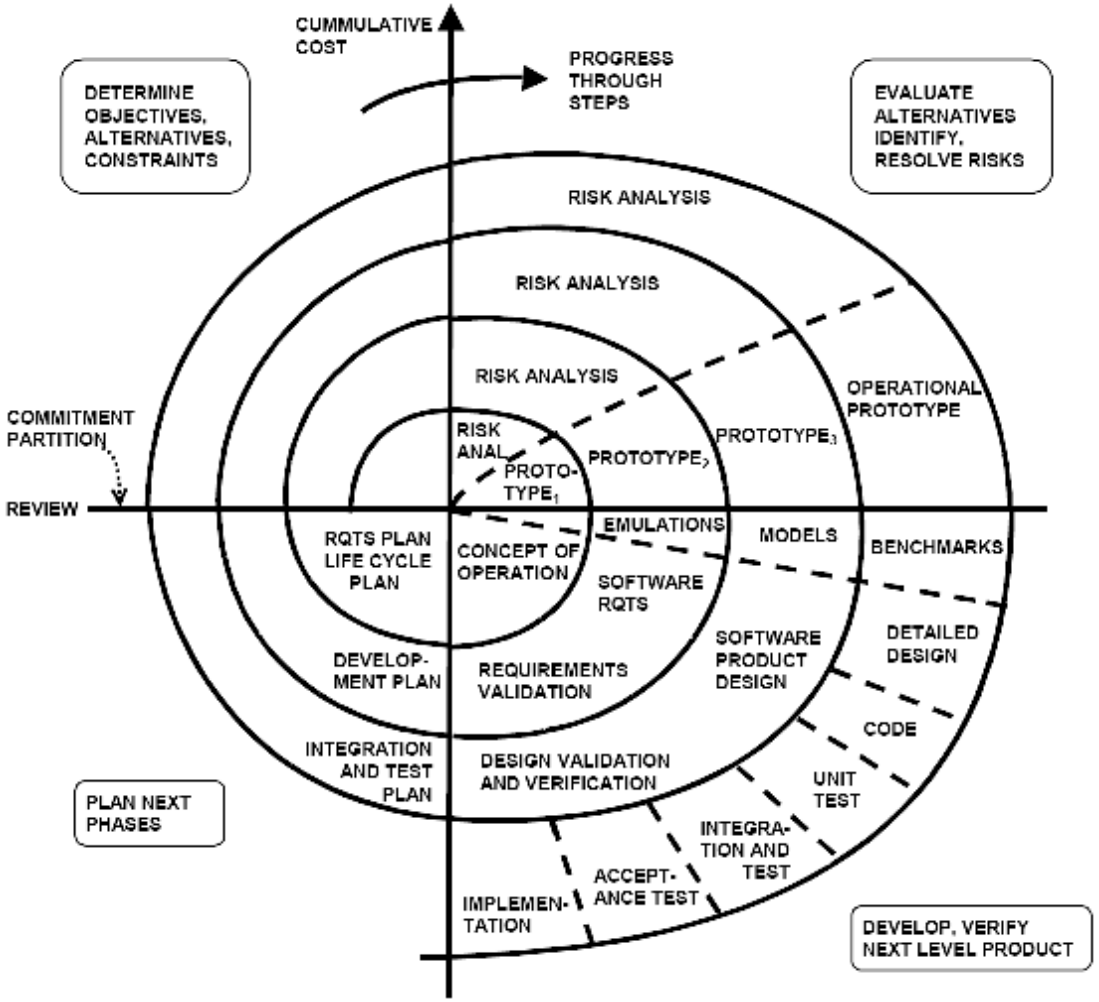


Verifikáció és validáció, prototípusok, tesztelés

- eddigi modellek „egy-verziós” életciklust írnak le
- rendszerfejlesztés iteratív:
  - prototípus → felfedett hibák → továbbfejlesztés → új prototípus
- spirál modell

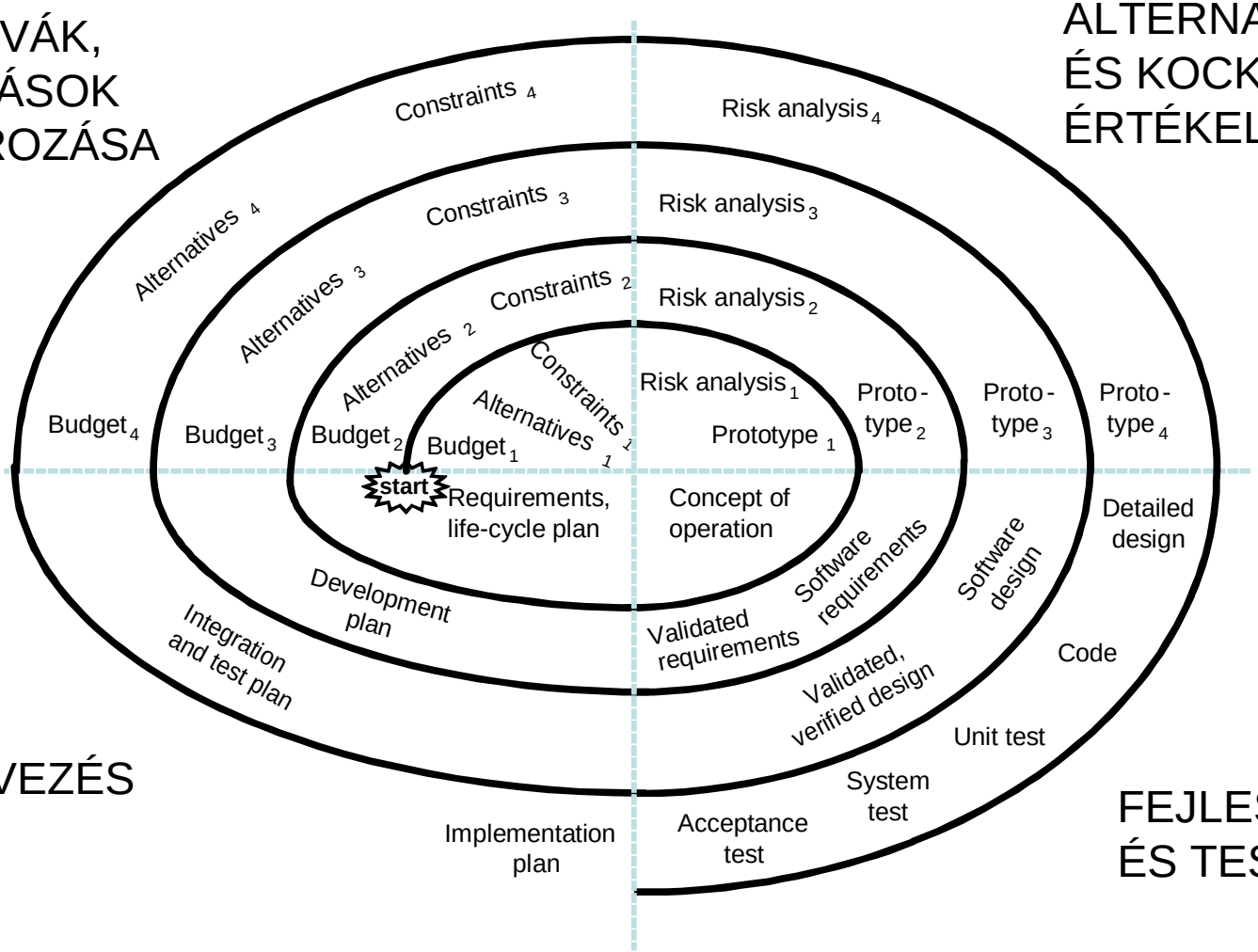


Spirál modell (lásd: Boehm)



CÉLOK,
ALTERNATÍVÁK,
KORLÁTOZÁSOK
MEGHATÁROZÁSA

ALTERNATÍVÁK
ÉS KOCKÁZATOK
ÉRTÉKELÉSE



TERVEZÉS

FEJLESZTÉS
ÉS TESZTELÉS

Elvárások

- IT rendszerek szolgáltatásminősége
- ISO 9000 nem elég
  - csak termékminőség
  - reprodukálás konstrukció helyett
- Hibátlan specifikáció kell
  - zártság
  - ellentmondás-mentesség
  - megfelelés
- Hibátlan implementáció is kell
  - minősített (és lehetőleg automatizált) fejlesztés
  - ellenőrizhető (validáció, automatikus tesztgenerálás)

Elvárások

- Formális szintaktika + szemantika
  - formális specifikációs nyelv
    - matematikai eszközrendszer, matematikai precizitás
    - formális szintakszis: strukturális tulajdonságok
    - formális szemantika: jelölésmód interpretációja
  - leíróeszköz
- Módszer
  - a formális modellről ismeretet adó matematikai eljárás
- Támogatóeszköz
  - a leíróeszközt értelmező, a módszert megvalósító sw.

- Feladatok:
  - hibátlan feladat-/rendszerspecifikáció
    - specifikációhoz szükséges eszközök (részben, félformális)
  - komponensek együttműködése, időzítések
    - statikus (strukturális) / dinamikus modellek
    - elosztott rendszerek: szinkronizáció, átlapolás, hazárdok felfedése
- Problémák:
  - valósághű modellezés (modellméret, állapottér méret)
  - időkezelés (IT: hibrid, idővariáns, nemlineáris)
  - környezetmodellezés (modellbázisú / nem modell bázisú)
  - sokféle matematika kell hozzá

- Matematikai leírás
  - funkcionális (célrendszer funkciói)
  - strukturális (belső struktúra) célszerűen grafikus formában
  - időzítés, teljesítmény, megbízhatóság
  - környezet
- Végrehajthatóság
- Ellenőrizhetőség (Validáció Verifikáció)
  - konzisztencia, ellentmondás-mentesség
  - teljesség, zártság
  - megfelelés
    - verifikáció: modellek között
    - validáció: a modellek és a rendszer között

- Megkötések
  - diszkrét állapotú
  - diszkrét idejű
  - diszkrét eseményterű rendszerek modellezése
- Problémák
  - nehéz matematikai jelölésrendszer
  - csak „kisméretű” problémákra átlátható
  - speciális ismeretekre van szükség a felhasználótól a véletlenszerű folytathatóság esetében

- matematika, algoritmus hatékonyság
- időzítési osztályok szűkek
- modellkészítés
- nyelvek kifejezésgazdagsága (VHDL)
- nyelvek nem pontos definíciója (UML)

Példa a rendszertípuspkra

- Z, VDM: sorrendi hálózatok tervezése
  - halmazok
  - relációk
  - függvények
- CSP, állapottérkép: konkurens rendszerek
  - sorozatok, fák
  - eseménysorok

Működő rendszerek

- Példák
  - CICS az IBM felhasználói rendszere (Z)
  - London légiforgalom irányítás (VDM)
  - USA légi összeütközés elkerülés (állapottérkép)
  - További területek
    - adatbázisok
    - hardver tervezés, mikro-elektronika
    - orvosi műszerek
    - nukleáris technika, biztonságkritikus rendszerek
    - távközlés, közlekedés

További lehetőségek

- Modellellenőrzés (véges modell)
  - temporális logika
  - automaták
- példák:
  - IEEE Futurebus
  - AT&T ISDN/ISUP
  - Fujitsu HDCL vezérlő
  - földrengés kompenzálás

További lehetőségek

- Tételbizonyítás (végtelen állapottér)
  - matematikai logika
  - axiómák, következtetések
  - levezetések (kézi segítség)
- példák
  - IBM PowerPC, S390
  - Motorola 68020, Intel Pentium

További lehetőségek

A színezett Petri hálók:

1. grafikus reprezentációval rendelkeznek
   - áttekinthető és érthető, követi a feladatstruktúrát
2. kevés, egyszerű működésű építőelemből állnak
3. jól definiált szemantikával rendelkeznek
4. leíróereje nagy
   - bizonyítottan Turing-ekvivalens algoritmikus rendszert adnak
5. explicit kifejezik az állapotot és az eseményeket
6. a modellstruktúra együtt van jelen a vezérlési és szinkronizációs feltételekkel