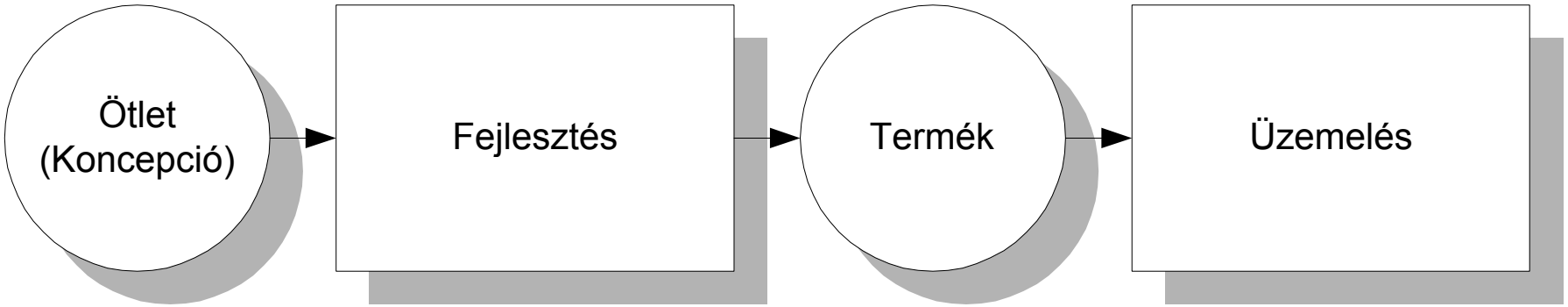
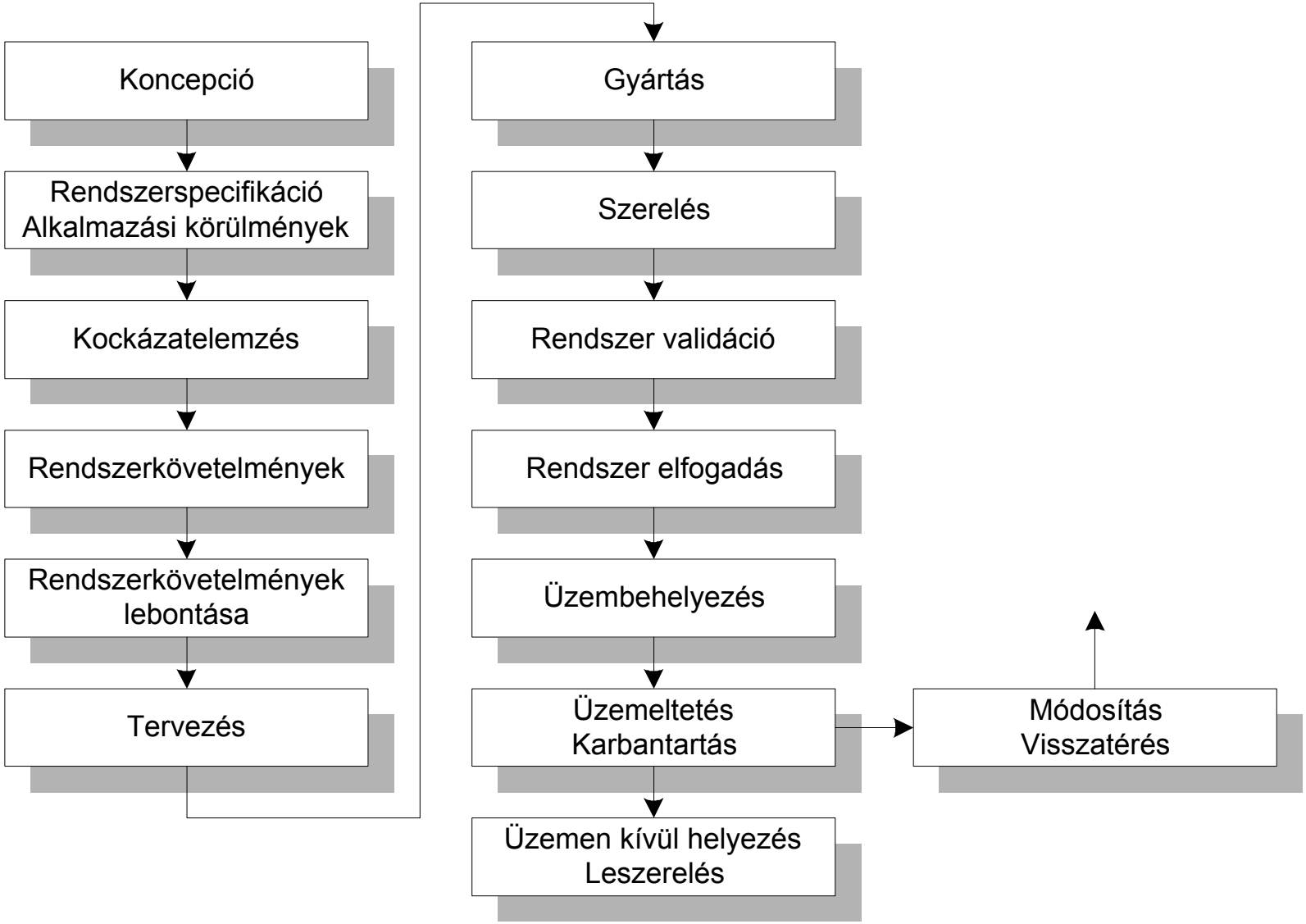
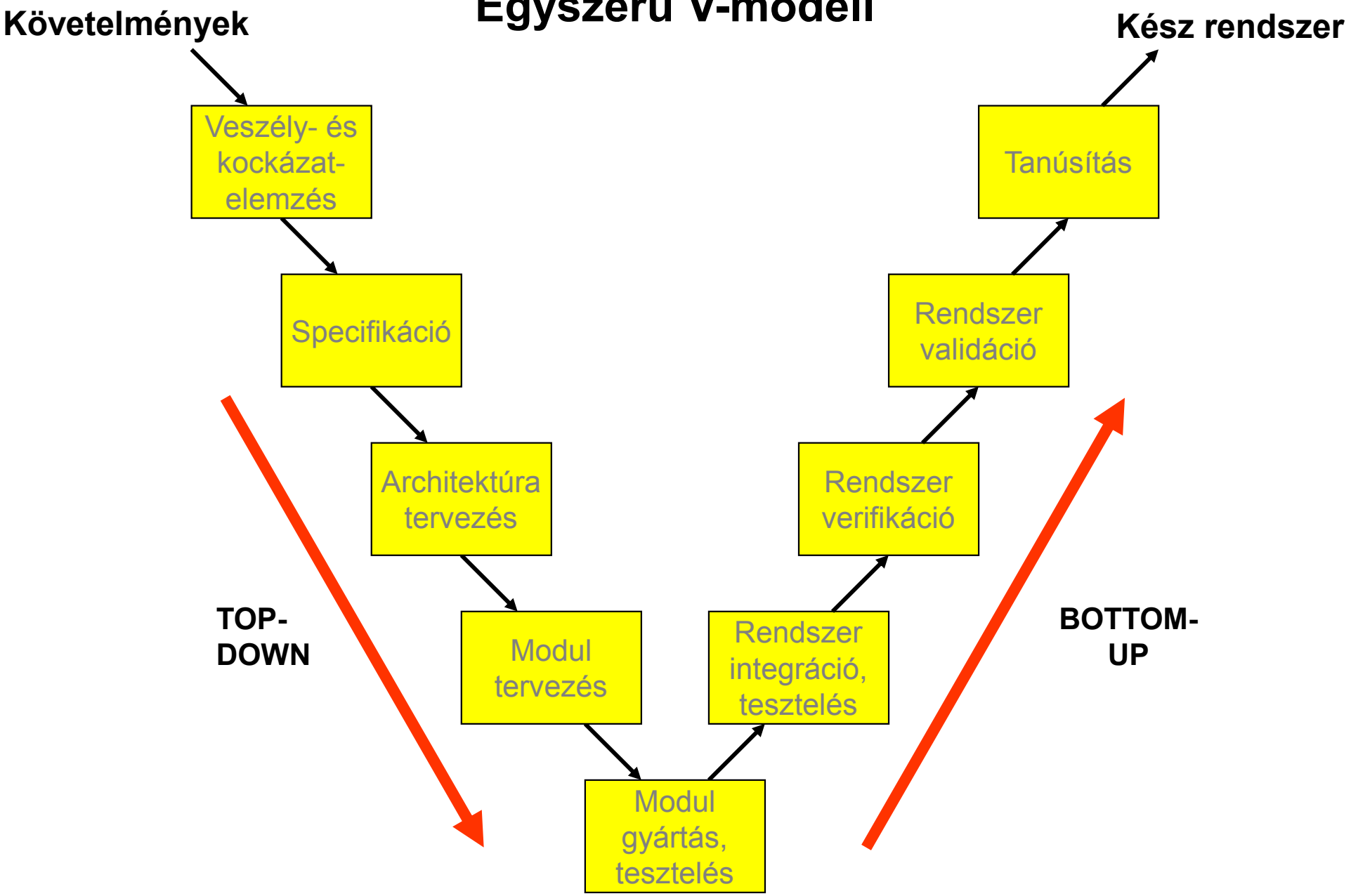
Egyszerű fejlesztési modell



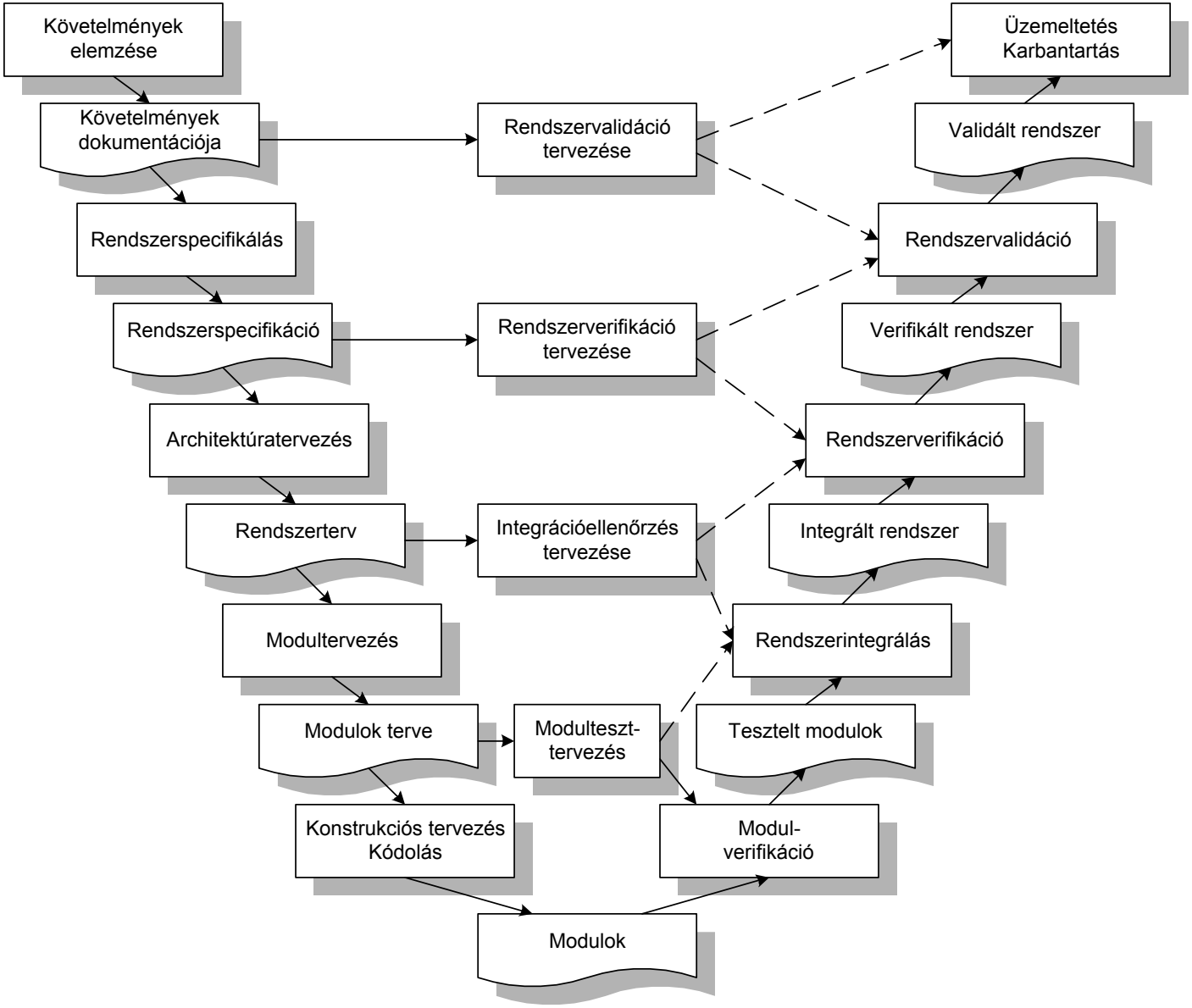
Fázismodell



Egyszerű V-modell



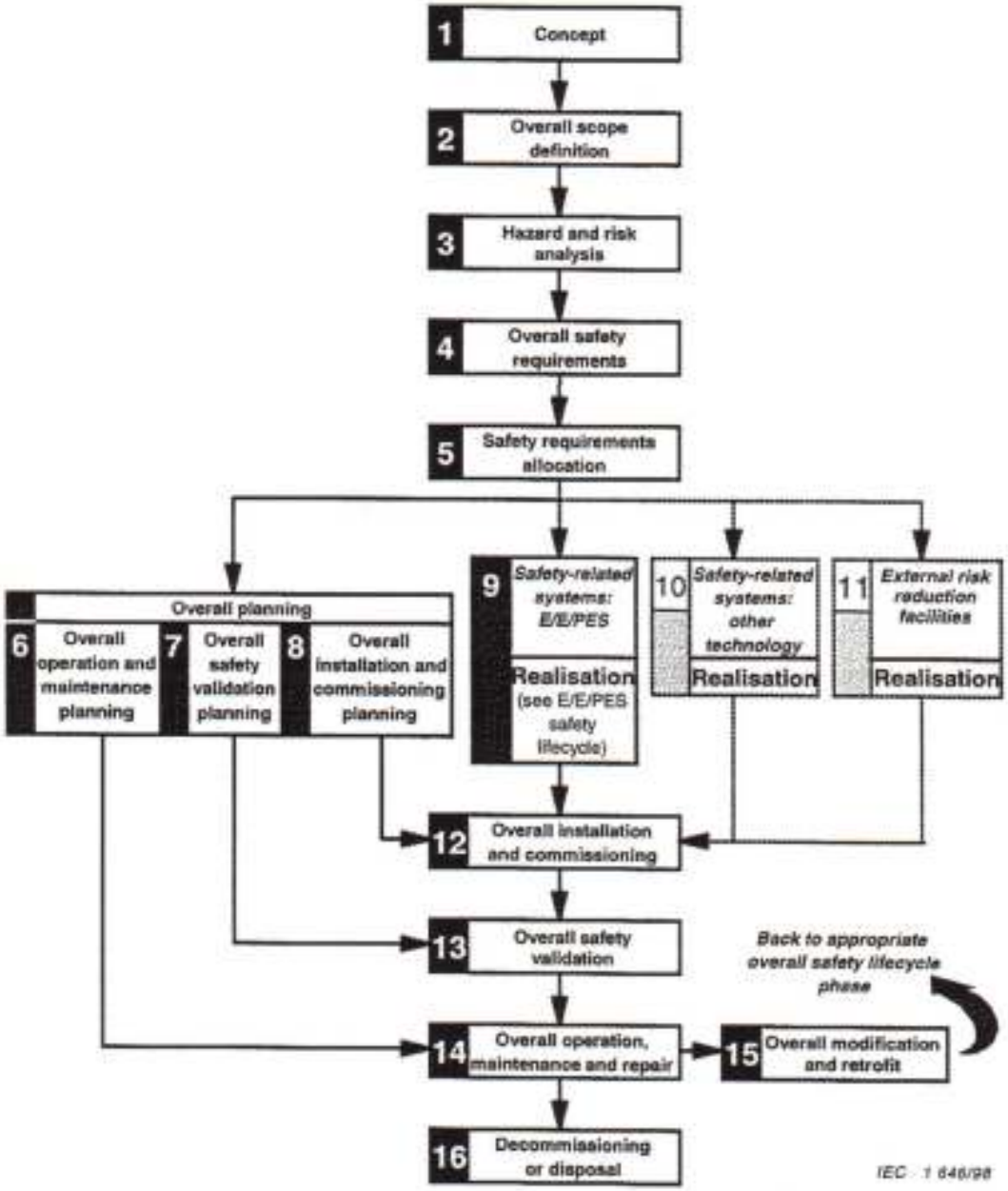
Bővített V-modell



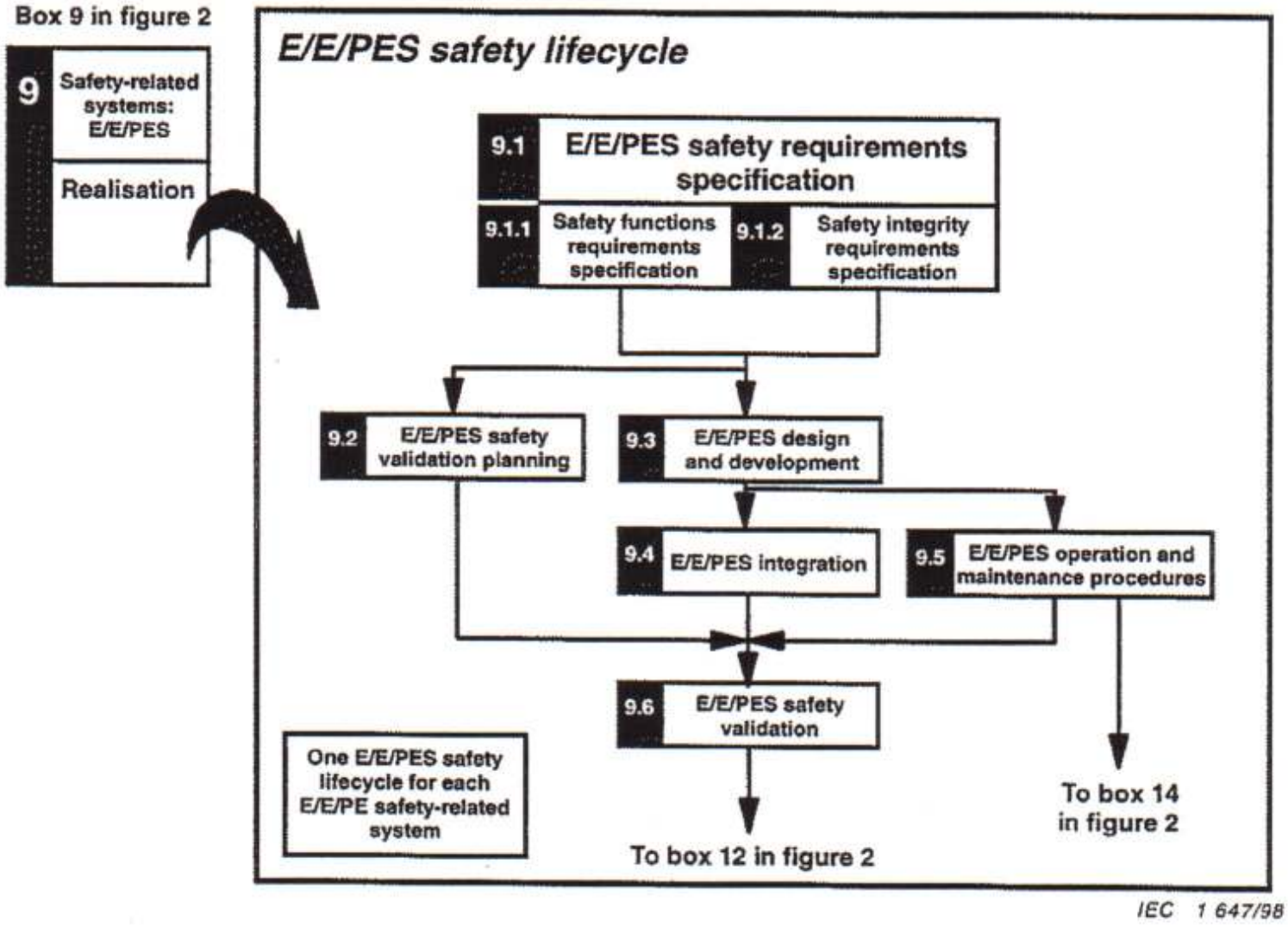
Bővített V-modell

- Többlet-információ
  - Az egyes fázisok „terméke” (dokumentáció stb.)
  - A fázisok közötti információáramlás
- Még ez is erősen egyszerűsített
  - Nem mutatja az iterációkat (bonyolult lenne)
    - Fázisokon belül
    - Fázisok között
  - Nem mutatja
    - Az egyes fázisokban párhuzamosan (pl. HW+SW) és
    - a több fázison keresztül folytatandó tevékenységeket

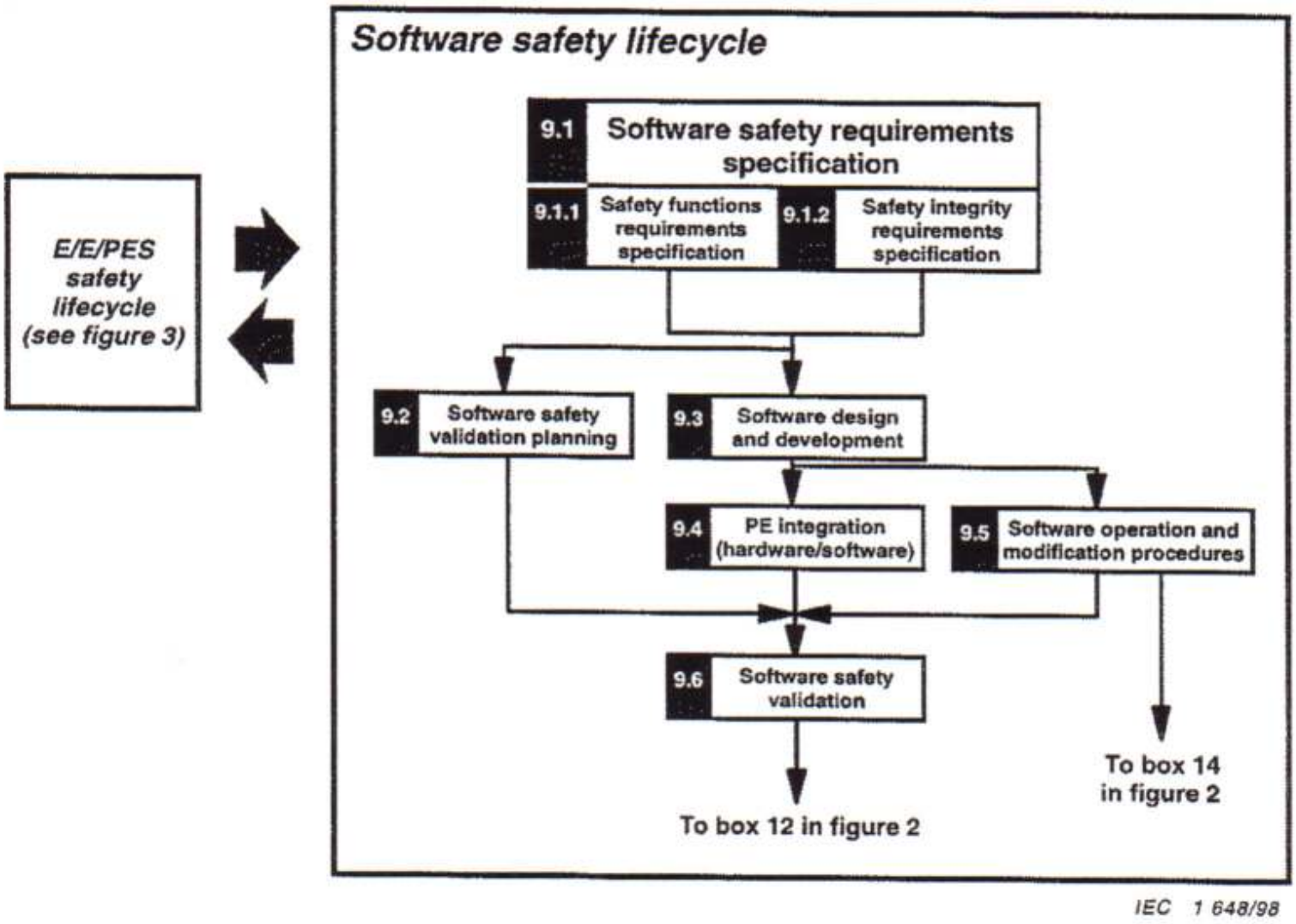
IEC 61508 biztonsági életciklus m.



IEC 61508 - megvalósítás



IEC61508 - szoftver



61508 életciklus modell

- A teljes (nemcsak a fejlesztési) életciklus valamennyi tevékenysége
  - kezdve a koncepciós fázistól
  - mindaddig, amíg a rendszer használatra alkalmatlanná nem válik
- Minden fázishoz tartozik biztonsági célú tevékenység, pl.
  - Veszély- és kockázatelemzés
- A fejlesztést követő fázisok is befolyásolják a biztonságot
- Megvalósítási módok
  - Villamos/elektronikus/programozható technológiák
  - Egyéb (mechanikai, hidraulikai stb.) technológiák
  - Külső (rendszeren kívüli) kockázatcsökkentési lehetőségek
  - A biztonság érdekében mindig a legegyszerűbbet kell választani!

61508 életciklus modell

- Párhuzamos tervezési tevékenységek a későbbi fázisok számára
- Ez a modell is egyszerűsített, pl.
  - Nem mutatja az értékelési és verifikációs tevékenységeket - ezek minden fázisnál szükségesek a továbblépés előtt
- A modell bármely integritási szint esetén használható
  - Az egyes fázisokban szükséges tevékenységek azonban a SIL-től függően erősen eltérhetnek

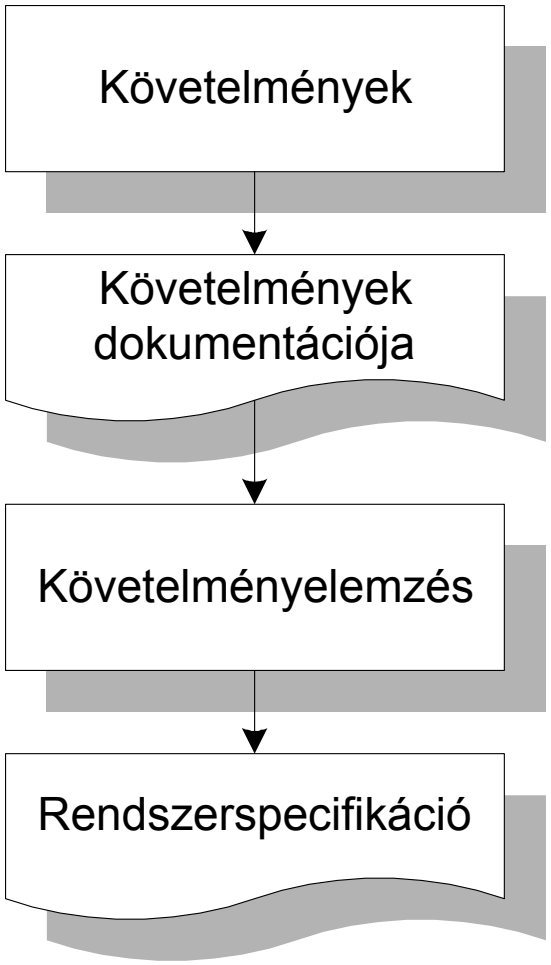
Fejlesztési módszerek, lépések

- Felhasználói követelmények
  - Funkcionális
  - Biztonsági
- Előzetes veszélyelemzés
- Specifikáció - a specifikáció animációja
- Top-level design
- Részletes tervezés
- A modulok megvalósítása és tesztelése
- Rendszer-integráció és rendszerteszt
- Engedélyezés

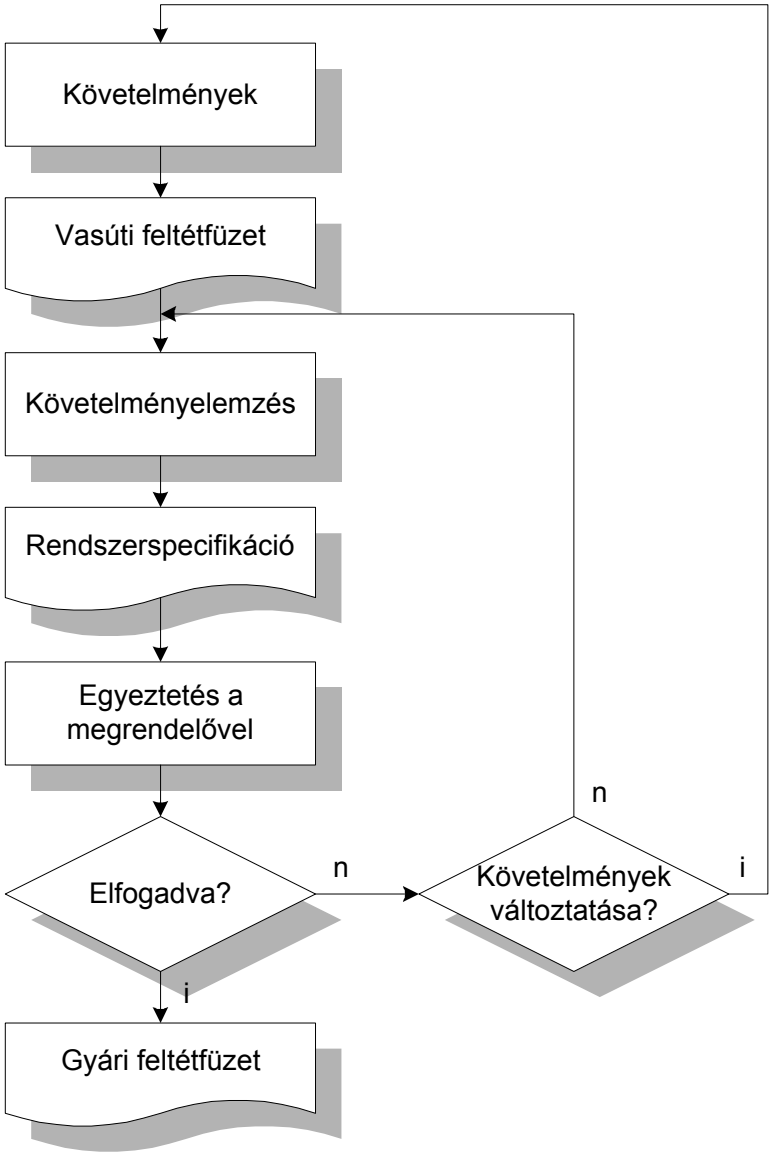
Specifikáció

- A rendszer működésének leírása
  - Funkciók
  - Együttműködés más rendszerekkel
  - Operátori kapcsolatok
  - Biztonsági jellemzők
    - Tervezési „kényszerek”
- Konzultációk a megbízó és a szállító között
- A szerződéses kapcsolat alapja
- A fejlesztési folyamat végén bizonyítani kell, hogy az eredmény minden tekintetben megfelel a specifikációnak (és remélhetőleg a megbízói követelményeknek)

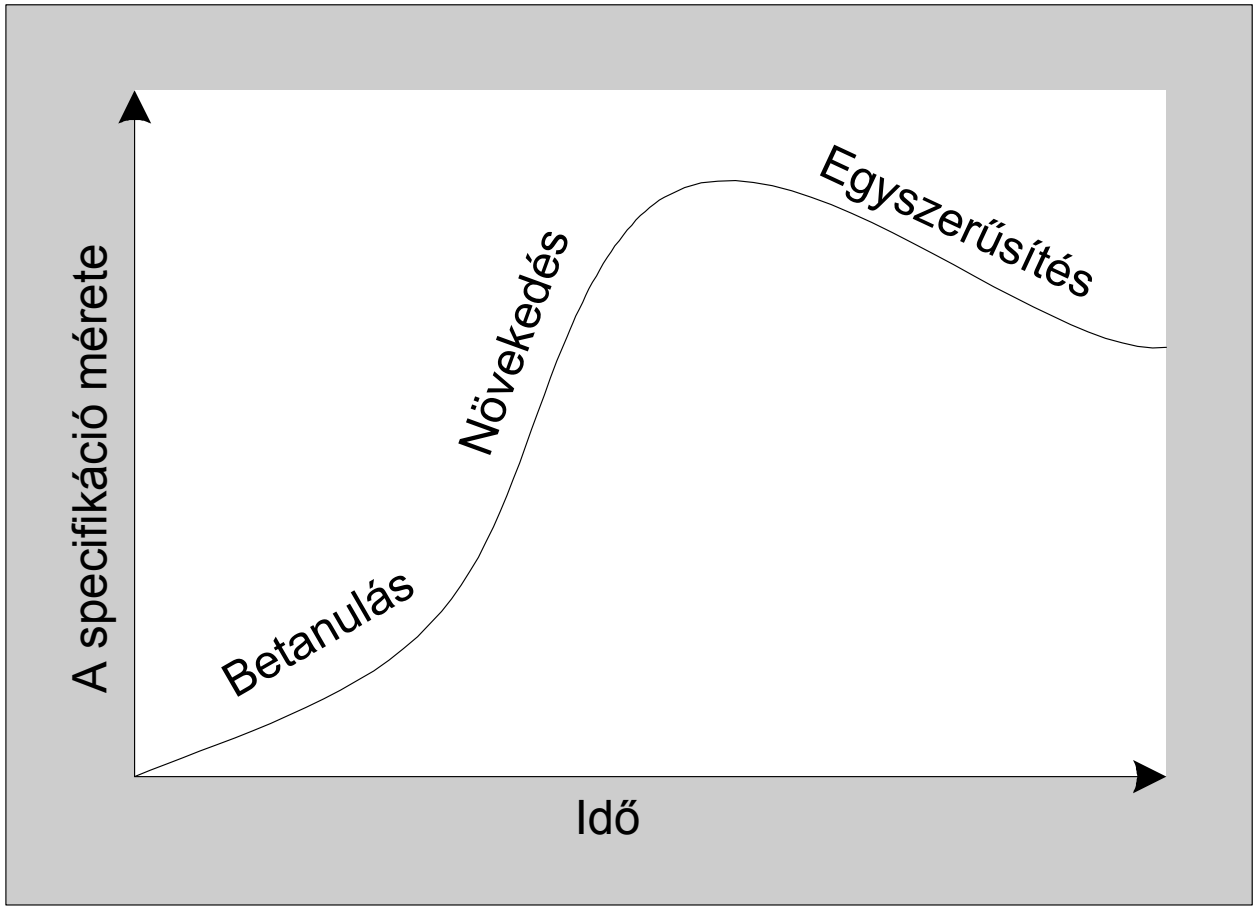
Specifikáció



Iteratív specifikációs modell



A specifikáció kialakulása



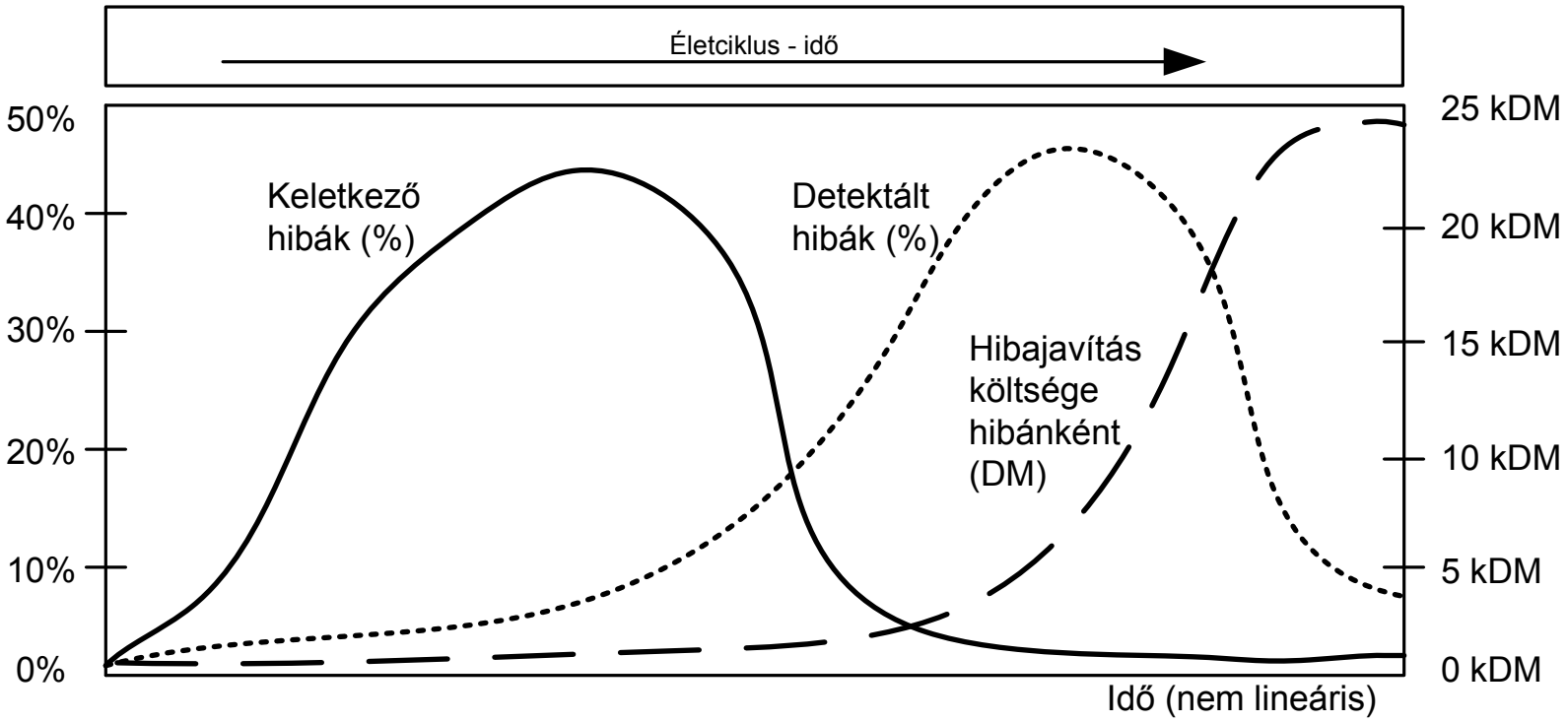
Az ideális specifikáció tulajdonságai

- Korrekt
- Teljes (nemcsak normál körülményekre)
- Konzisztens (ellentmondásmentes)
- Féreérthetetlen (természetes nyelvek!)
  - A természetes nyelven írt specifikációk helyességének ellenőrzése nehéz
- Lehetőségek
  - Strukturált szerkezet (félformális)
  - Formális matematikai módszerek

A specifikáció hibái

- A biztonságkritikus rendszerek egyik legnagyobb problémája a hibás specifikáció
  - A felhasználói követelmények meg nem felelősége
  - A specifikáció nem felel meg a felhasználói követelményeknek
- A specifikációs hibák gyakran csak a kész rendszer vizsgálatakor derülnek ki, amikor a hibajavítás már igen költséges

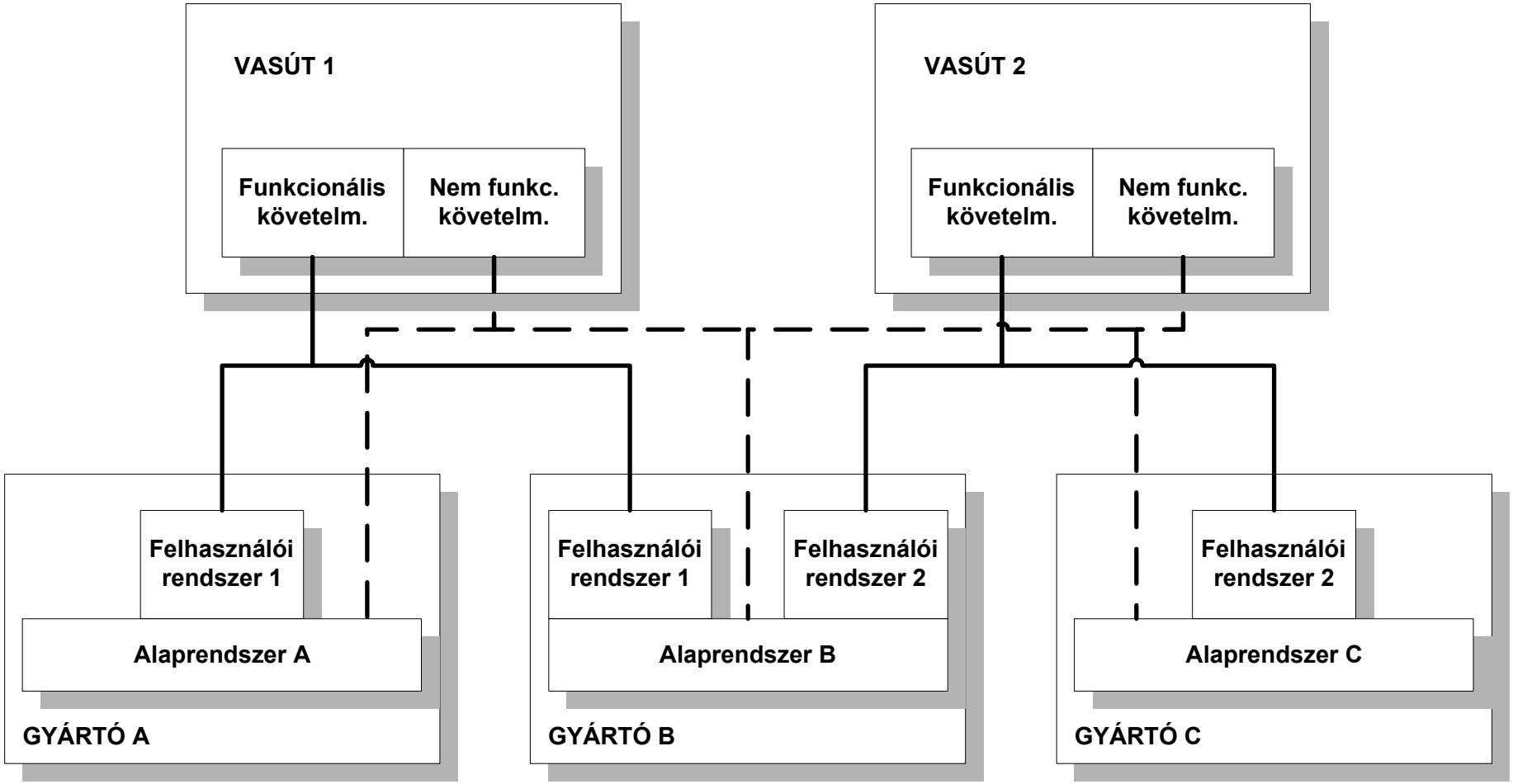
Hibák keletkezése és detektálása

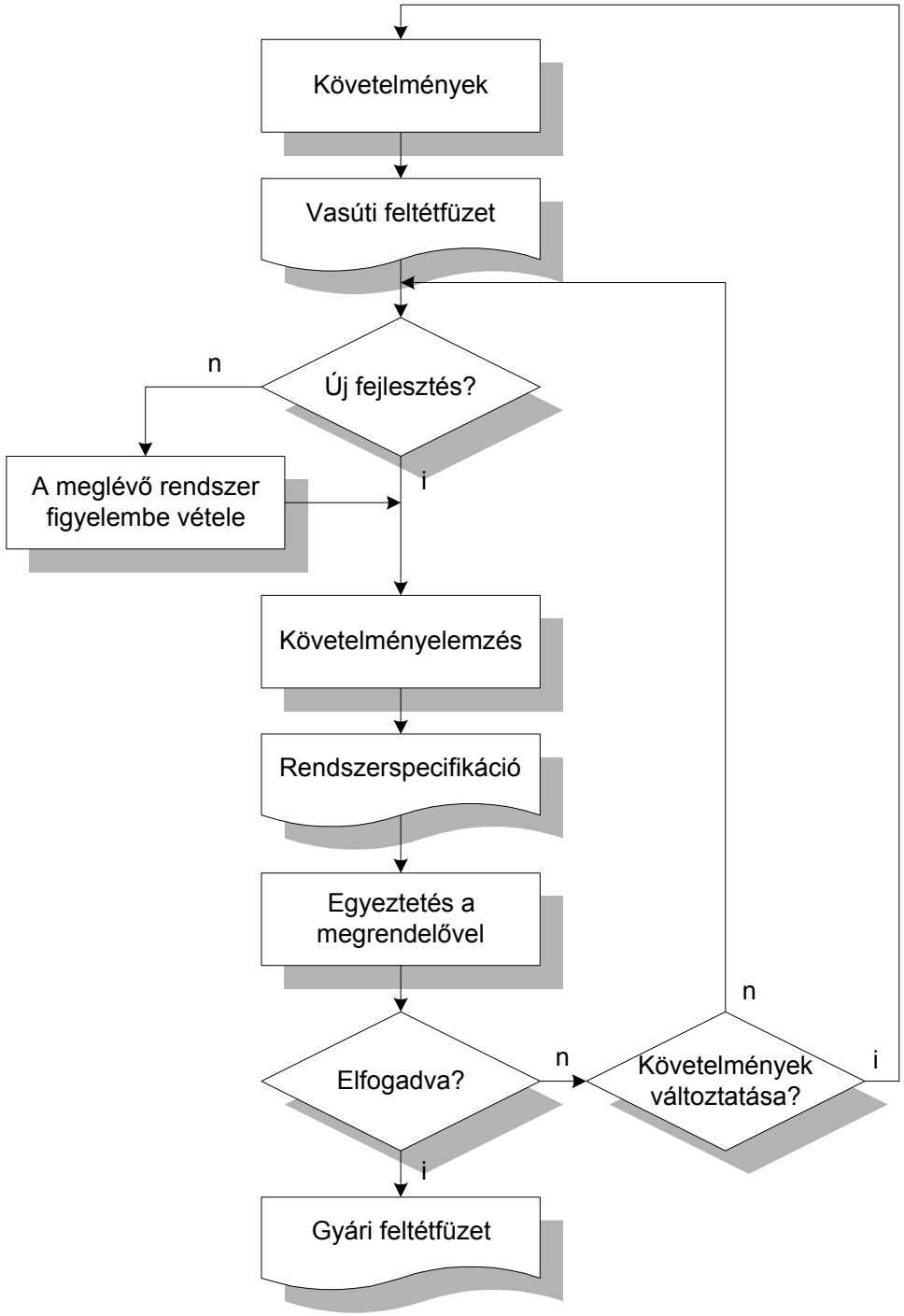


A specifikáció animálása

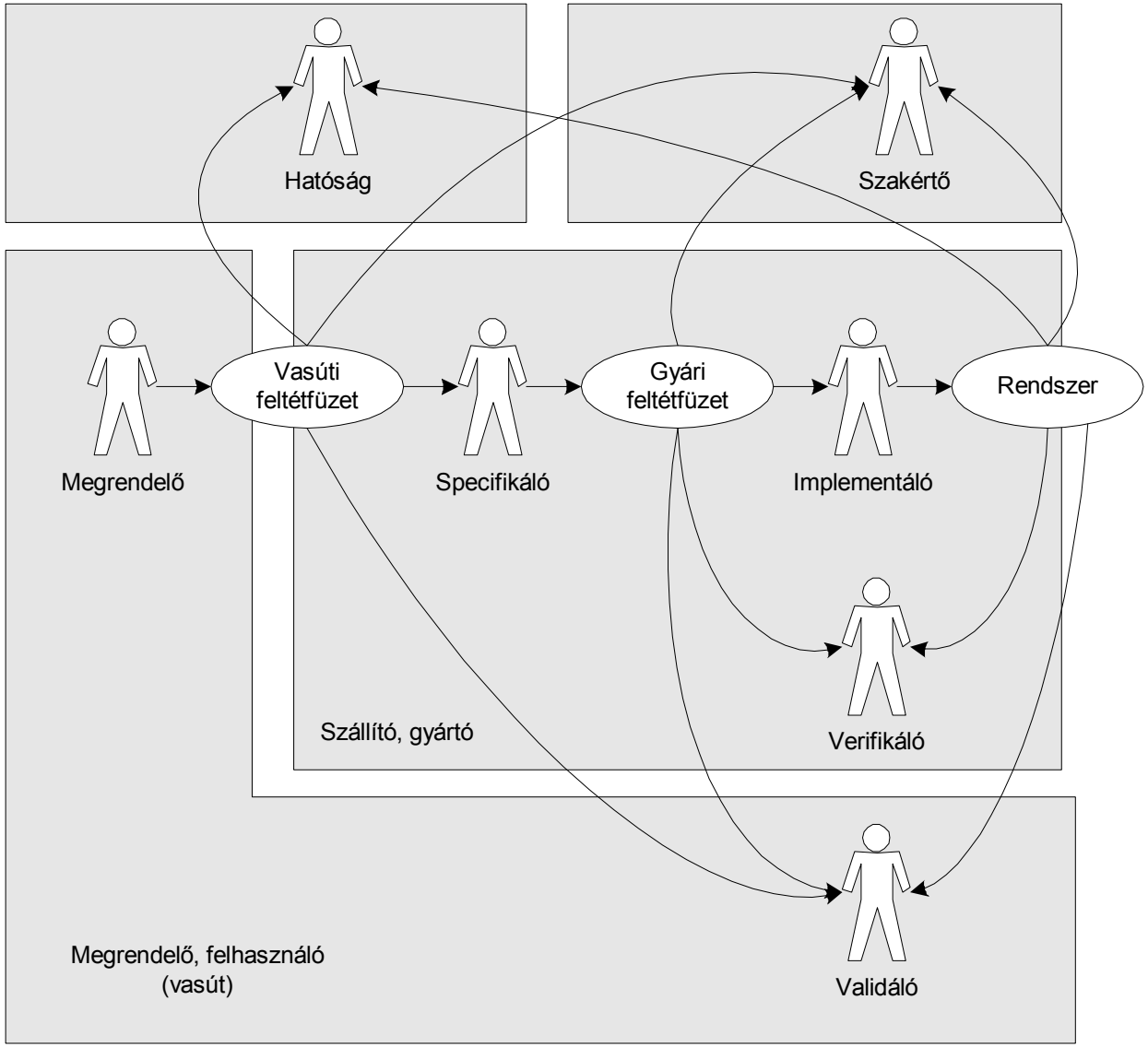
- **Egy lehetőség az animáció** (SW prototipus)
  - Nem feltétlenül a teljes specifikációra terjed ki
  - Speciális szempontokra irányulhat, pl
    - Belső logikai funkciók
    - MMI
- **Általában nem veszi figyelembe**
  - Az időzítési követelményeket
  - A hibatűrést
  - A beépített teszteket
- A prototípust a végső termékben nem használjuk, így fejlesztése sokkal **kevésbé szigorú**, illetve ráfordítás-igényes
- Az **animáció** a specifikáció szimulációja a specifikáció validálására
- Az általános értelemben vett **szimuláció** a kifejlesztett rendszer szimulációja a fejlesztés helyességének vizsgálatára
  - Olcsóbb, mint a fizikai prototípus vizsgálata

Több gyártó/több megrendelő

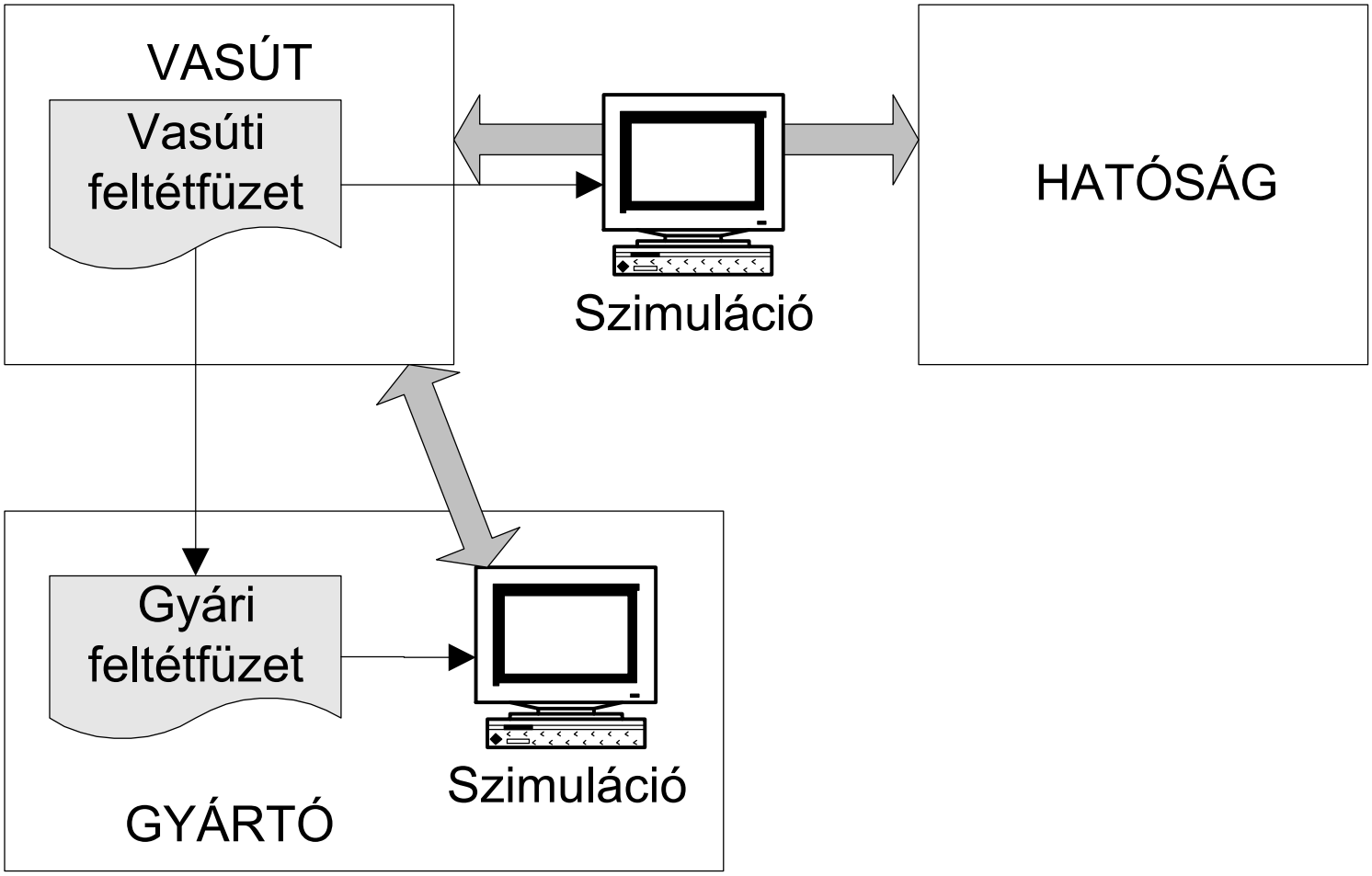



Követelmények
Vasúti feltétfüzet
Új fejlesztés?
n
i
A meglévő rendszer figyelembe vétele
Követelményelemzés
Rendszerspecifikáció
Egyeztetés a megrendelővel
Elfogadva?
n
i
Követelmények változtatása?
n
i
Gyári feltétfüzet

Vasúti spec. használói



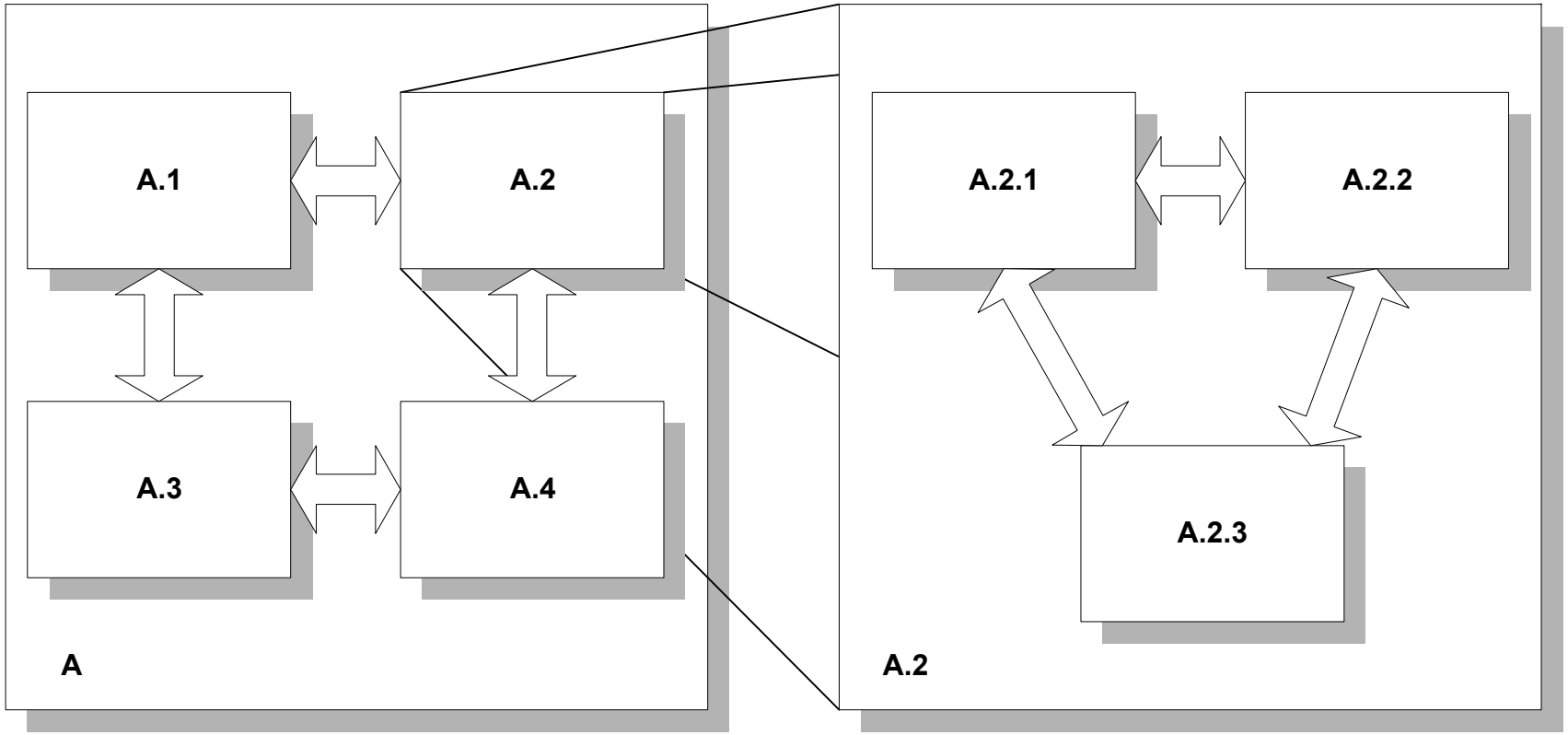
Szimuláció alkalmazása



Top-level design - Detailed design
Magasszintű tervezés – Részl. terv.

- Rendszerfunkciók szétbontása
  - Hardver
  - Szoftver
- Architektúrák kidolgozása (HW és SW)
  - Modulokra bontás (hierarchikus struktúra)
  - Modulkapcsolatok meghatározása (interfész)
  - Meghatározni a modulok
    - Funkcióit
    - Biztonsági jellemzőit
  - Lényeges SW adatsruktúrák meghatározása
- Modulok részletes tervezése
  - A dekompozíció gyakran iteratív (szubmodulok)

Dekompozíció



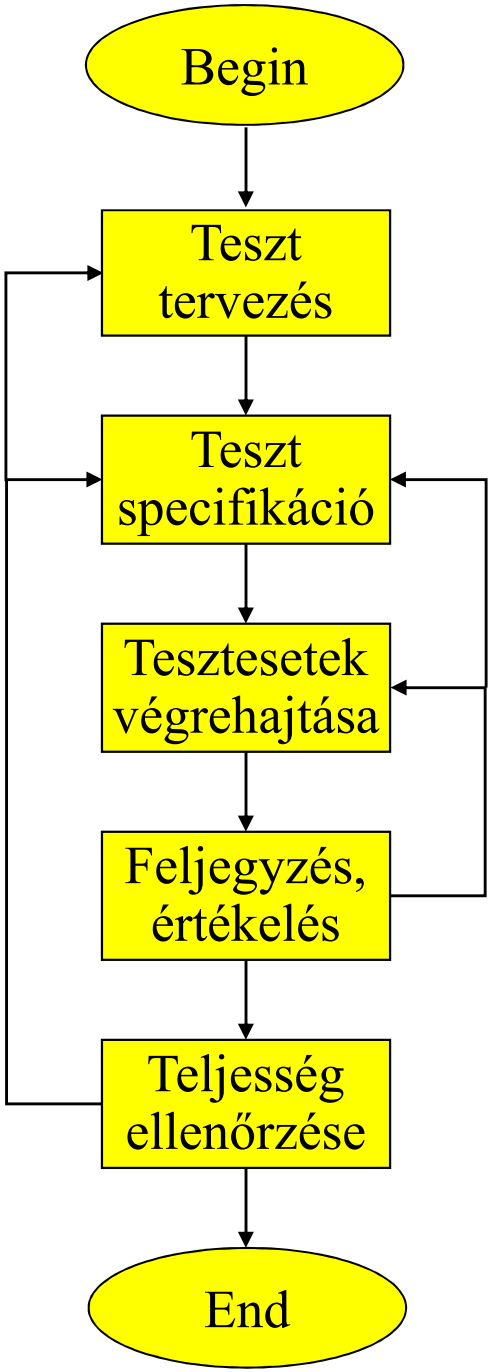
A modulok megvalósítása

- HW és SW modul implementáció
- Programnyelv választása
  - A programnyelv tulajdonságai
  - Fejlesztő eszközök elérhetősége
  - A fejlesztő csapat gyakorlottsága, tapasztalatai

A modulok tesztelése

- Annak igazolása, hogy a modul megfelel specifikációjának
  - **Dinamikus**
    - A HW/SW modul működtetésével
    - Tesztkörnyezet
      - Adja a bemenő jeleket
      - Fogadja és értékeli a kimenő jeleket
    - Számos jellemző, így pl. a válaszidő is vizsgálható
  - **Statikus (analízis)**
    - A modul működtetése nélkül
    - A tervezés felülvizsgálata
    - Statikus kódelemzés
    - Vizsgálhatók olyan jellemzők, amelyek dinamikussal, pl. a tesztek nagy száma vagy más ok miatt, nem vizsgálhatók
    - Nem vizsgálható minden jellemző, pl. az időzítések

A TESZTELÉS FOLYAMATA



Tesztelési terv, teszt-esetek

- Tesztelési terv
  - A teszt-eseteket meghatározó technika megadása
  - A tesztelési eljárás megfelelőségét értékelő módszerek
  - A tesztelendő rendszer fejlesztését és teszt-tervezését végzők függetlensége
  - A teszt-környezet
  - A tesztelés teljességének kritériumai
- Teszt-esetek meghatározása
  - A tesztelendő rendszer kezdeti állapota
  - A bemenetek
  - A várt válaszok

Rendszer integráció

- Progresszív integráció - hagyományos
  - A modulok kis csoportját (minimális rendszer) tesztelik, a hibákat javítják
  - Fokozatosan újabb modulokkal bővítenek, tesztelnek, javítanak
  - Az egyszerű kezdés és a kis lépésekben való bővítés miatt egyszerű a hibadetektálás és a diagnózis
  - Hátrány: A teljes rendszer jellemzői csak az integráció befejeztével vizsgálhatók - az ilyen funkciókkal kapcsolatos hibák késői, drága feltárása, javítása
- „Big bang” módszer
  - Tesztelés csak az integráció befejeztét követően
  - Feltételezés: a modulok kialakítása és tesztelése megfelelő volt
  - Előny: a durva követelmény- vagy specifikációs hibák viszonylag korán kiderülnek, javításuk kevésbé költséges
  - Hátrány: a tesztelendő rendszer bonyolultsága miatt a tesztelés feladata jóval nehezebb

Rendszerteszt, engedélyezés

- A rendszer integrációt követően
  - A teljes rendszer megfelel a specifikációnak
  - Dinamikus és statikus módszerek kombinációja
  - Szimulált vagy valós környezetben

- Független tanúsító (az engedélyezéshez)
  - A fejlesztés valamennyi fázisát megfelelő gondossággal és kompetenciával hajtották végre
  - Dokumentálni kell
    - Valamennyi munkafázist
    - A tesztelés részleteit és eredményeit
  - A tanúsítás folyamatát már a projekt elején tervezni kell
  - A szabványok, irányelvek megadják az egyes fejlesztési fázisokban szükséges dokumentációk listáját