Mintapélda:
Rendszertesztelés a SAFEDMI projektben

Majzik István
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék
http://www.inf.mit.bme.hu/

Tartalomjegyzék

A SAFEDMI konzorcium

Partners:

Project Co-ordinator

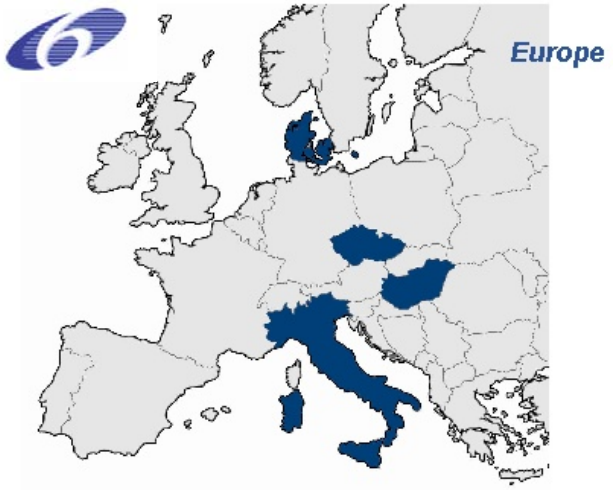
AnsaldoSTS
A Finmeccanica Company

AALBORG UNIVERSITET

PRAHA

ISTITUTO DI SCIENZA E TECNOLOGIE DELL'INFORMAZIONE "A. FAEDO"

MŰEGYETEM 1782



Safe Driver Machine Interface for ERTMS Automatic Train Control
(SAFEDMI, EC FP6 Transport 031413, 2006-2008, www.safedmi.org)

A mozdonyvezetői kezelőfelület

A rendszer áttekintése

Train driver

DMI

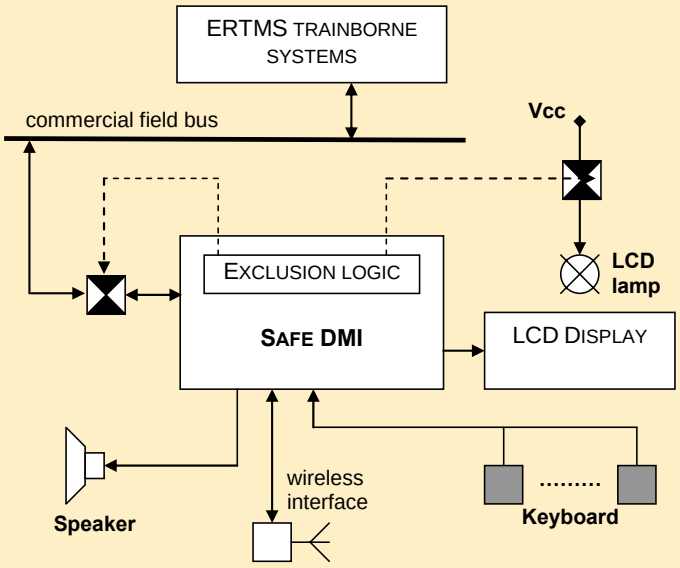
EVC
European
Vital
Computer
on board

Maintenance Centre

- Safety Integrity Level 2
  - Információ megjelenítés
  - Parancs feldolgozás
  - EVC kommunikáció
- Biztonságos vezeték nélküli kommunikáció
  - Konfiguráció
  - Diagnosztika
  - Szoftver frissítés

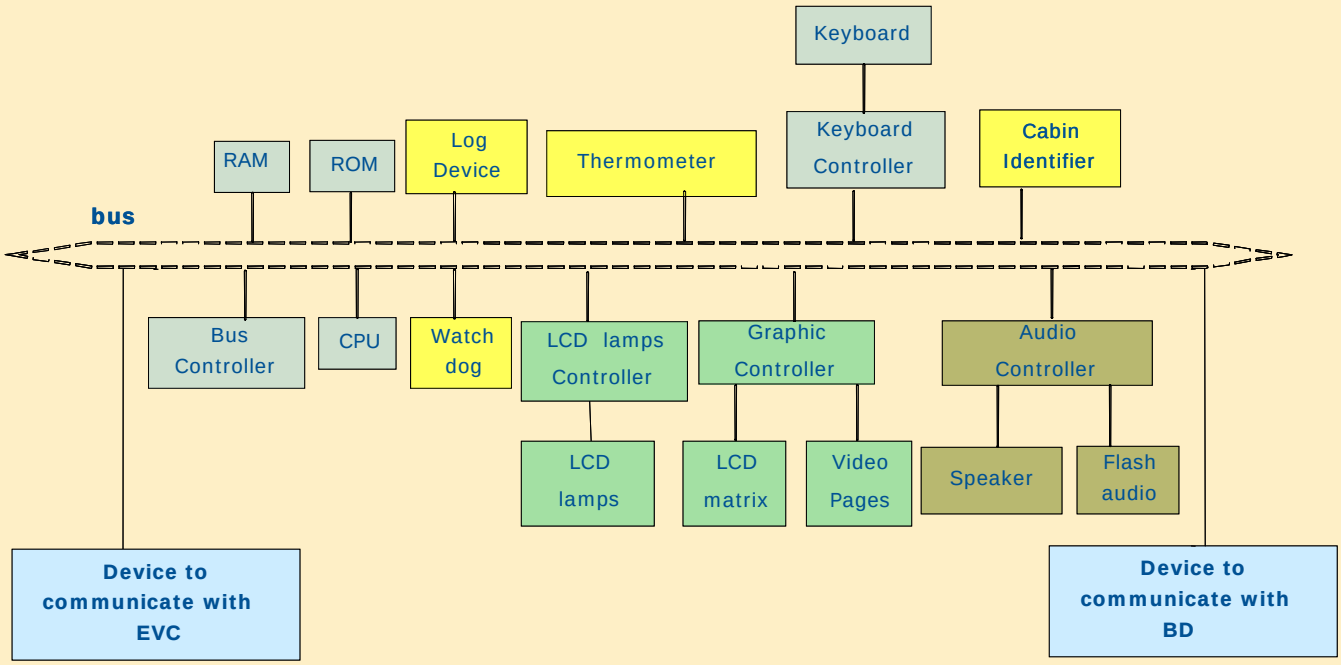
A hardver architektúra

- Reaktív fail-safety (hibadetektálás és hibakezelés)
- Generikus hardver komponensek
- A hibadetektálás és hibakezelés megvalósítása szoftver alapú megoldásokkal



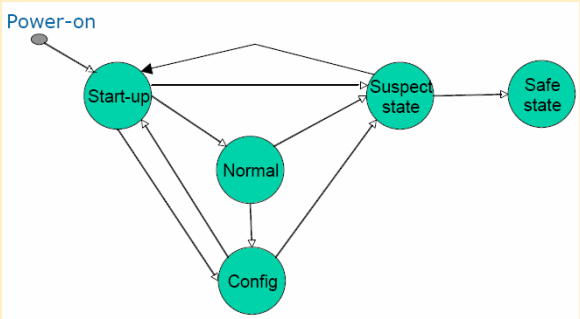
A hardver architektúra

Komponensek:



A szofver architektúra

- Üzemmódok:
  - Startup, Normal, Configuration, Safe módok
  - Suspect state valósítja meg a hiba utáni műveleteket



- Hibadetektálási technikák:
  - Startup: Öntesztelés az állandósult hibák detektálására
  - Normal/Configuration: Periodikus önteszt és on-line ellenőrzés
    - Adat elfogadhatósági / hihetőségi vizsgálatok: Kommunikáció, konfiguráció esetén
    - Vezérlési folyam monitorozása: Vezérlés-orientált funkciókra
    - Duplikált számítás és összehasonlítás: Adat-orientált funkciókra
- Biztonságos protokollrétegek a vezeték nélküli kommunikációhoz:
  - Low safety layer: Védett kapcsolat a hálózathoz
  - High safety layer: Végpontok közötti biztonságos kommunikáció

Tartalomjegyzék

- A SAFEDMI rendszer
  - Célkitűzések
  - Hardver architektúra
  - Szoftver architektúra
- Rendszertesztelés
  - ERTMS funkciók
    - Robusztusság tesztelés
  - Belső biztonsági mechanizmusok
    - Célzott hibainjektálás
  - Vezeték nélküli kommunikáció
    - Scenario alapú tesztelés

Teszt specifikáció

Train driver

DMI

EVC
European
Vital
Computer
on board

Maintenance Centre

Fő teszt csoportok:

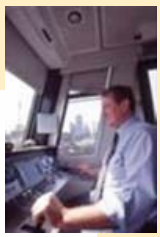
- ERTMS funkciók
  - Interakció a vezetővel
  - Interakció a fedélzeti számítógéppel
- Belső biztonsági mechanizmusok
- Vezeték nélküli kommunikáció

1. Teszt specifikáció az ERTMS funkciókhoz

- Teszt bemenetek (teszt sorozat):
  - A DMI kezelése (nyomógombok): Teszt mérnök (nem automatizált tesztelés)
  - Külső terhelés: Az ETC működtetése pályaszimulátorral
- Teszt kimenet:
  - DMI kimenetek: Képernyő, hangjelzés
  - Diagnosztikai eszköz: Hozzáférés a belső állapothoz
- Teszt értékelés:
  - Teszt mérnök (kézi)

Step	Action	Expected Event
1.	**Driver:** give traction to the train	**SAFEDMI:** the current train speed increases.
2.	None	**SAFEDMI:** • The text message "Entry in Full Supervision Mode" is shown and a sound is produced. • the FS mode icon  is shown in area B7; • in area A2 the distance to target is shown;
3.	**Driver:** give traction to the train until the current train speed overcomes the permitted speed.	**SAFEDMI:** - In area A1 the warning to avoid brake intervention is displayed and sound is produced; - In area E1 the icon  (Brake applied) is shown; • In area C9 the icon  (Service brake intervention or emergency brake intervention) is shown.

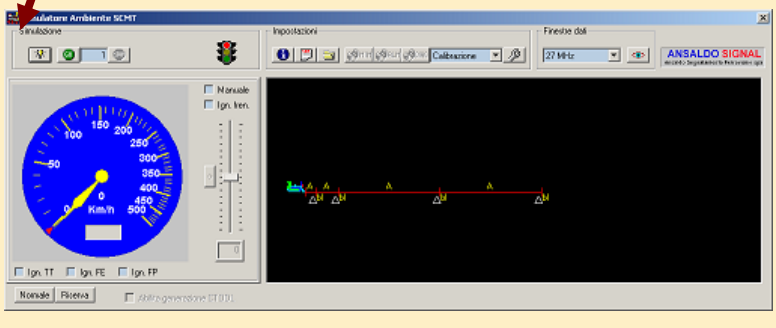
A teszt környezet



Track simulator

ERTMS OnBoard equipment

SAFEDMI



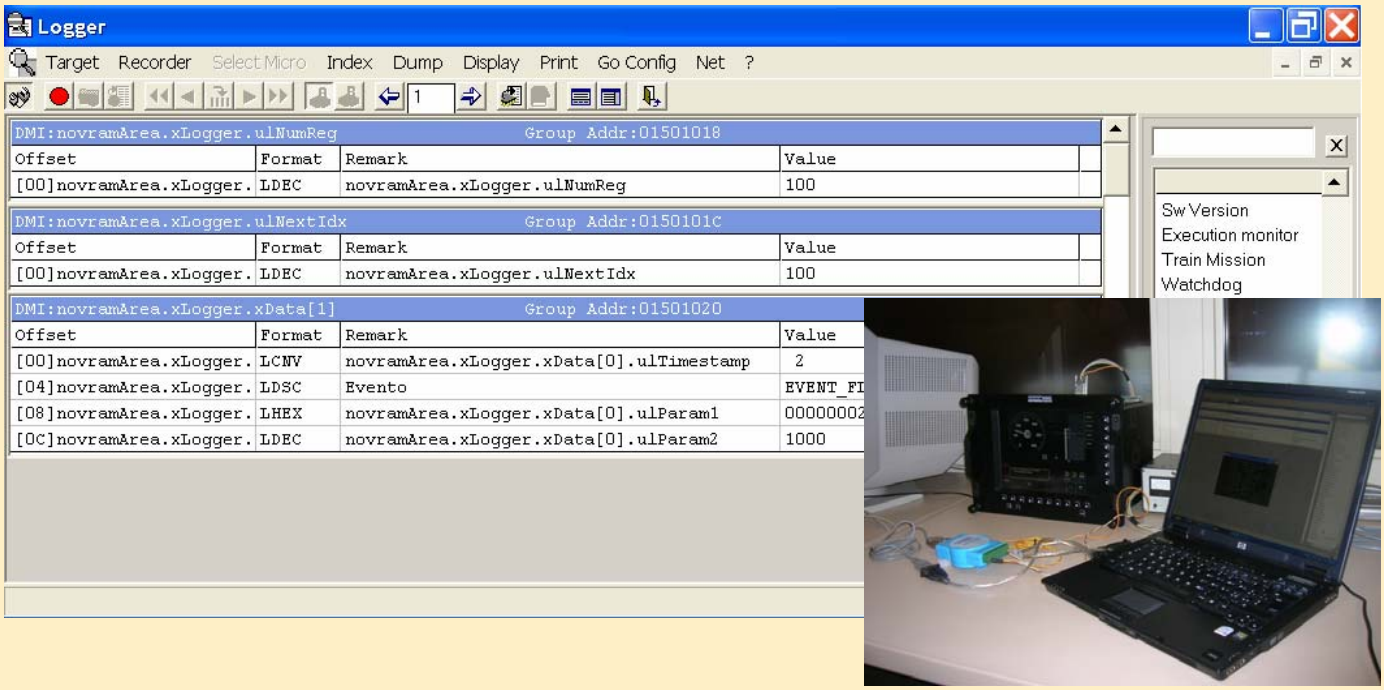
Teszt workload:

- A mozdony haladása: Az ETC környezetének szimulációja
- Alternatívák: HIL, SIL, MIL tesztelés

A diagnosztikai eszköz

Hibrid monitorozás:

- Felműszerezett szoftver: Állapot hozzáférés, esemény triggerelés
- Külső naplózás: Soros kommunikáció külső PC felé



Robusztusság tesztelés

Train driver

DMI

EVC

- Robusztus viselkedés a vezetői kezelőfelületen:
  - Nyomógombok kezelése: Nagy gyakoriság, egyszerre több, …
  - Beviteli mezők: Üres, teli, érvénytelen karakterek, …
- Robusztus viselkedés az EVC interfész felől (protokoll):
  - Érvénytelen üzenetek: Érvénytelen struktúra, érvénytelen mezők (üres, maximálisan kitöltött, szemét, …)
  - Extrém időzítés: Túl lassú, túl gyors, túl gyakori (elárasztás), …

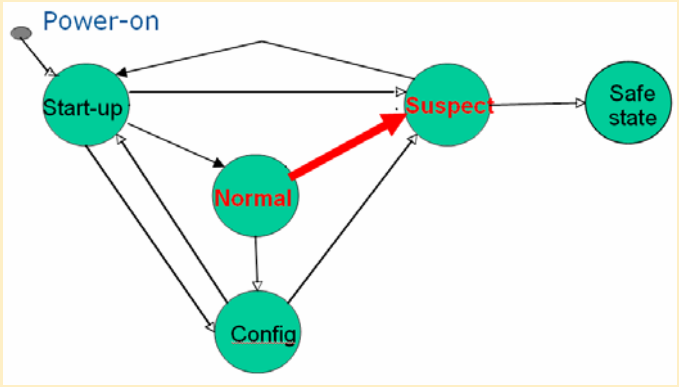
2. A belső biztonsági mechanizmusok tesztje

- Üzemmódok és a kapcsolódó funkciók tesztelése:
  Az üzemmódok állapotgépének teljes fedése (útvonalak)
  - Üzemmódok aktiválása, üzemmód váltások végigjárása
  - Safe állapot: Lekapcsolás a külvilágról
  - Suspect állapot: A hibaszámlálás (belső állapotgép) fedése
  - Normal állapot: Biztonsági jóváhagyás kritikus funkciókra
- Kritikus időzítések tesztelése:
  - Az EVC interfész specifikáció szerinti határidők tesztelése
  - Időzítések betartása maximális terhelés esetén
- Hőmérsékletfigyelés tesztje:
  - Indítási és üzemi hőmérséklet korlátok figyelembe vétele (ASF klímaterem)

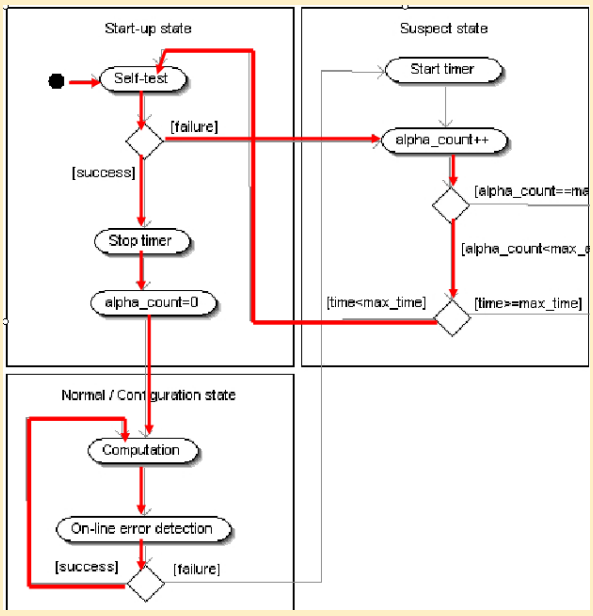
Szisztematikus teszt tervezés

Üzemmódok tesztje (biztonságos állapotba jutás):

- Minden állapot és állapotátmenet lefedése



Üzemmód állapotgép



Hibaszámlálás FSM

A belső biztonsági funkciók tesztje

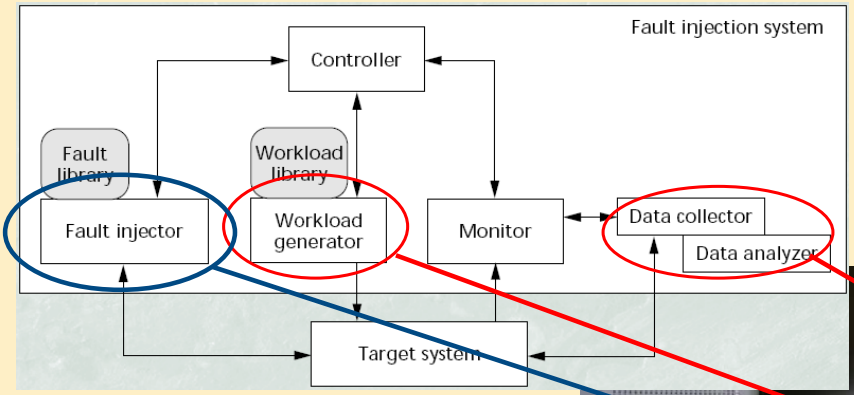
1. Determinisztikus hibainjektálás: Hibadetektálás és hibakezelés implementációjának tesztelése

- Tesztelési cél:
  - Az injektált hibákat detektálják a beépített hibadetektáló eljárások
  - Megfelelő hibakezelés indul
- On-line mechanizmusok tesztelése:
  - Vezérlési folyamat ellenőrzése (függvények és utasítások szintje)
  - Adat elfogadhatósági ellenőrzés
  - Duplikált végrehajtás és komparálás
  - Time-out ellenőrzés
- Indítási és periodikus öntesztek tesztelése:
  - Beavatkozás: CPU, RAM, ROM, video page hibák teszt közben
  - Specifikus konfiguráció: I/O eszközök (kabin, LCD lámpa)

2. Véletlen hibainjektálás:

- Hibafedés vizsgálata (statisztika felvétele)

Szoftver alapú determinisztikus hibainjektálás

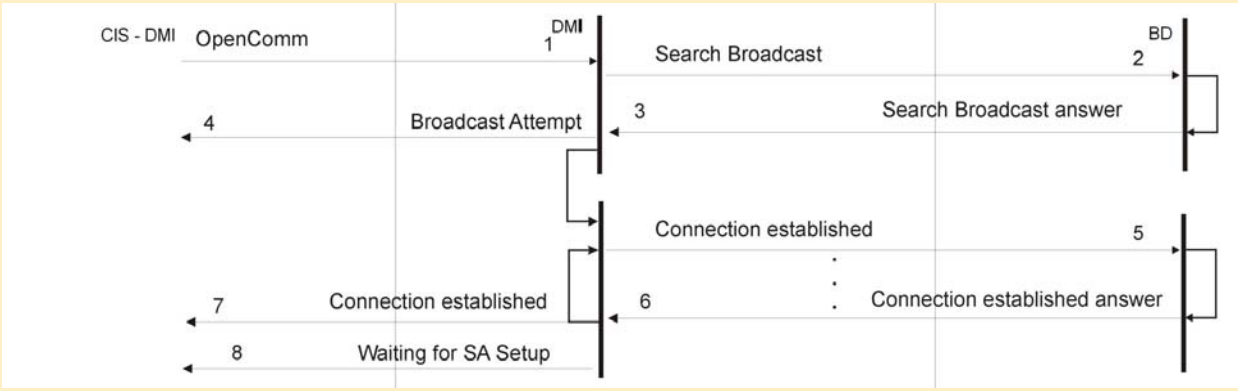


- Szoftver felműszerezése (feltételes hiba)
- Hiba aktiválás külső eszközzel
- Hibrid monitorozás

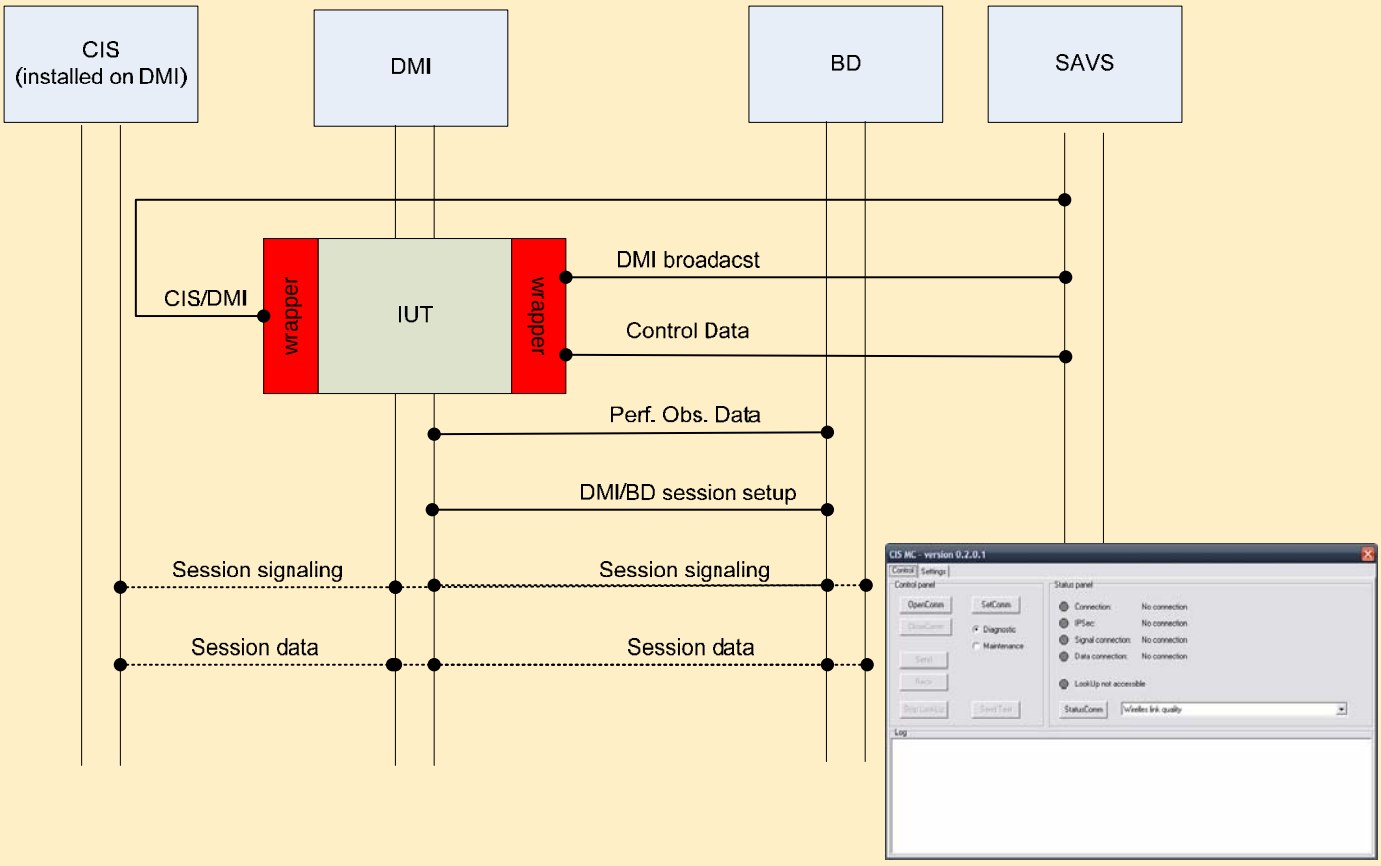
3. A vezeték nélküli kommunikáció tesztje

Scenario alapú tesztelés a protokoll funkciókra

- Normál működés:
  - Kapcsolatfelvétel, üzenet feldolgozás, kapcsolat bontás
- Működés átviteli hibák esetén:
  - Hibadetektáló mechanizmusok (EDC, ECC)
  - Kapcsolatbontás nagy hibagyakoriság esetén



Wrapper konfiguráció (hibainjektálás)



A verifikációs tevékenységek összefoglalása

ERTMS és konfigurációs funkciók ellenőrzése teszteléssel

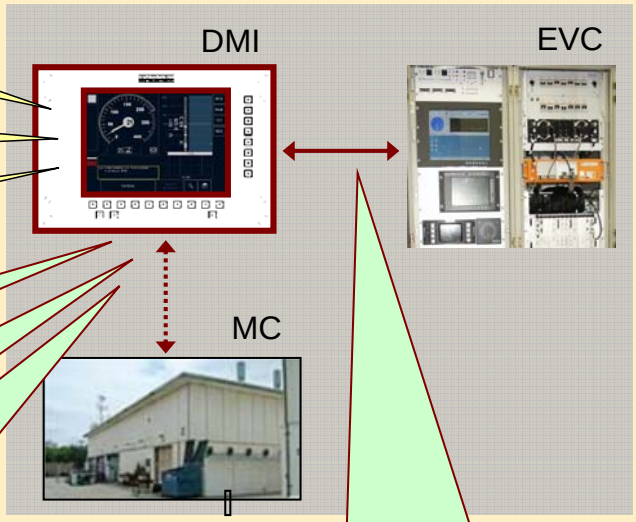
Hibadetektálás és **hibakezelés** vizsgálata hibainjektálással

Ütemezhetőség és **valósidejű követelmények** vizsgálata méréssel

Megbízhatóság és **biztonság** elemzése modell alapú analízissel

Hibadetektáló kódok jellemzőinek (hibaszökés) analitikus vizsgálata

A vezeték nélküli kommunikáció **teljesítményének** és **biztonságának** modell alapú vizsgálata



A DMI hibák **rendszerszintű hatásának** modellezése