Szabó Géza
egyetemi adjunktus
BME Közlekedésautomatikai Tanszék

Energiaellátás biztonságkritikus rendszerekben:

Megbízhatósági követelmények meghatározása és teljesülésük igazolása

Tartalom:

- Bevezetés, motiváció
- Biztonságkritikus és nagy biztonságú rendszerek
- Követelmények az áramellátással szemben
- Vasúti biztosítóberendezések áramellátása
- Hibafa-analízis és megbízhatósági becslés
- PQ áramellátó rendszerek hibafa-analízise
- Összefoglalás

Bevezetés, motiváció

Biztonságkritikus rendszerek esetén hatósági jóváhagyás szükséges az üzemeltetéshez, a jóváhagyás alapja a gyártó által készített biztonságigazolás.

Motiváció:

A Magyar Államvasutak Rt. megbízása a BME Közlekedésautomatikai Tanszék részére a vasúti áramellátó rendszerek megbízhatóságának vizsgálatára

Biztonságkritikus és nagy biztonságú rendszerek

Definíciók

Biztonságkritikus rendszer (safety critical system):

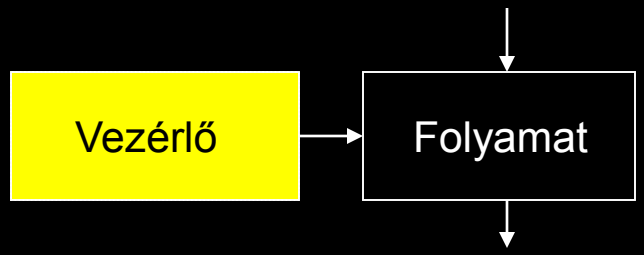
Olyan rendszer, amely működése során az emberi életre vagy anyagi javakra veszélyes helyzet alakulhat ki.

(Mire használom…?)

Nagy biztonságú rendszer (high dependable system):

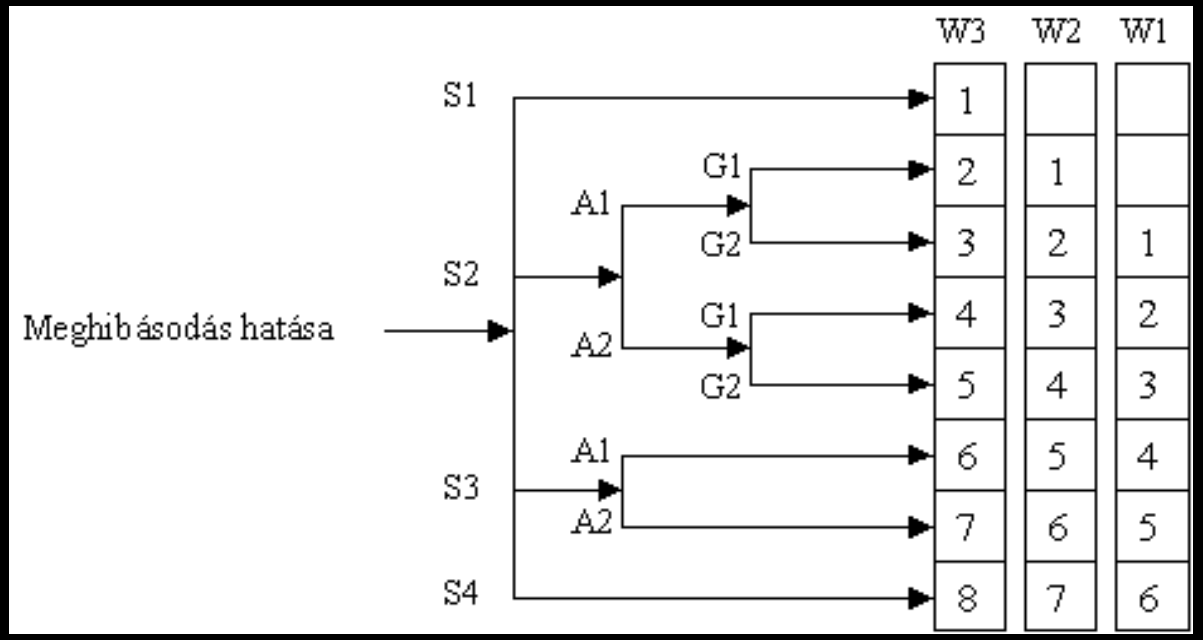
Olyan rendszer, amely működése során mind a **véletlen meghibásodások**, mind **a szisztematikus hibák** hatásai ellen bizonyos fokú védettséget biztosít.

(Mit használok…?)



A veszélyes helyzetek (a kockázat) értékelése

DIN 19250



Értékelési szempontok:

1. A veszély következményeként keletkező kár mértéke: S1-S4
2. A veszélyes zónában való tartózkodás: A1-A2
3. A veszély elhárításának lehetősége: G1-G2
4. A veszély gyakorisága: W1-W3

A veszélyes helyzetek (a kockázat) értékelése

MSZ-EN 50126

	Kár kihatási kategória			
Valószínűségi szint	Jelentéktelen	Csekély	Kritikus	Katasztrofális
Gyakori	*nem kívánatos*	*nem tűrhető*	*nem tűrhető*	*nem tűrhető*
Valószínű	*tűrhető*	*nem kívánatos*	*nem tűrhető*	*nem tűrhető*
Esetleges	*tűrhető*	*nem kívánatos*	*nem kívánatos*	*nem tűrhető*
Csekély	*elhanyagolható*	*tűrhető*	*nem kívánatos*	*nem kívánatos*
Valószínűtlen	*elhanyagolható*	*elhanyagolható*	*tűrhető*	*tűrhető*
Nem hihető	*elhanyagolható*	*elhanyagolható*	*elhanyagolható*	*elhanyagolható*

Értékelési szempontok:

1. A veszély következményeként keletkező kár mértéke: 1-4
2. A veszélyes zónában való tartózkodás: A1-A2
3. A veszély elhárításának lehetősége: G1-G2
4. A veszély gyakorisága: 1-6

Nagy biztonságú rendszerek

Nagy élettartamú rendszer (safe life)

Nagy megbízhatóságú alkatrészekből felépített rendszer - nem számolunk az alkatrész meghibásodásával az élettartamon belül.

Hibabiztos rendszer (fail safe)

A rendszer meghibásodás esetén **biztonsági állapotot** vesz fel.

Példák: Vasúti biztosítóberendezés vagy nukleáris erőmű.

Hibatűrő rendszer (fault tolerant)

A rendszernek nincsen biztonsági állapota, meghibásodás esetén funkcióvesztés nélkül működik tovább.

Példa: Repülőgép fedélzeti rendszerek.

Megbízhatósági követelmények az áramellátással szemben

Az áramellátás nem megfelelő voltából adódó veszteség:

Gazdasági kritérium - A folyamat megakadásából származó veszteség (bevételkiesés). Az áramellátás **rendelkezésre állását** szabja meg.

Az áramellátás javítási igényéből adódó veszteség:

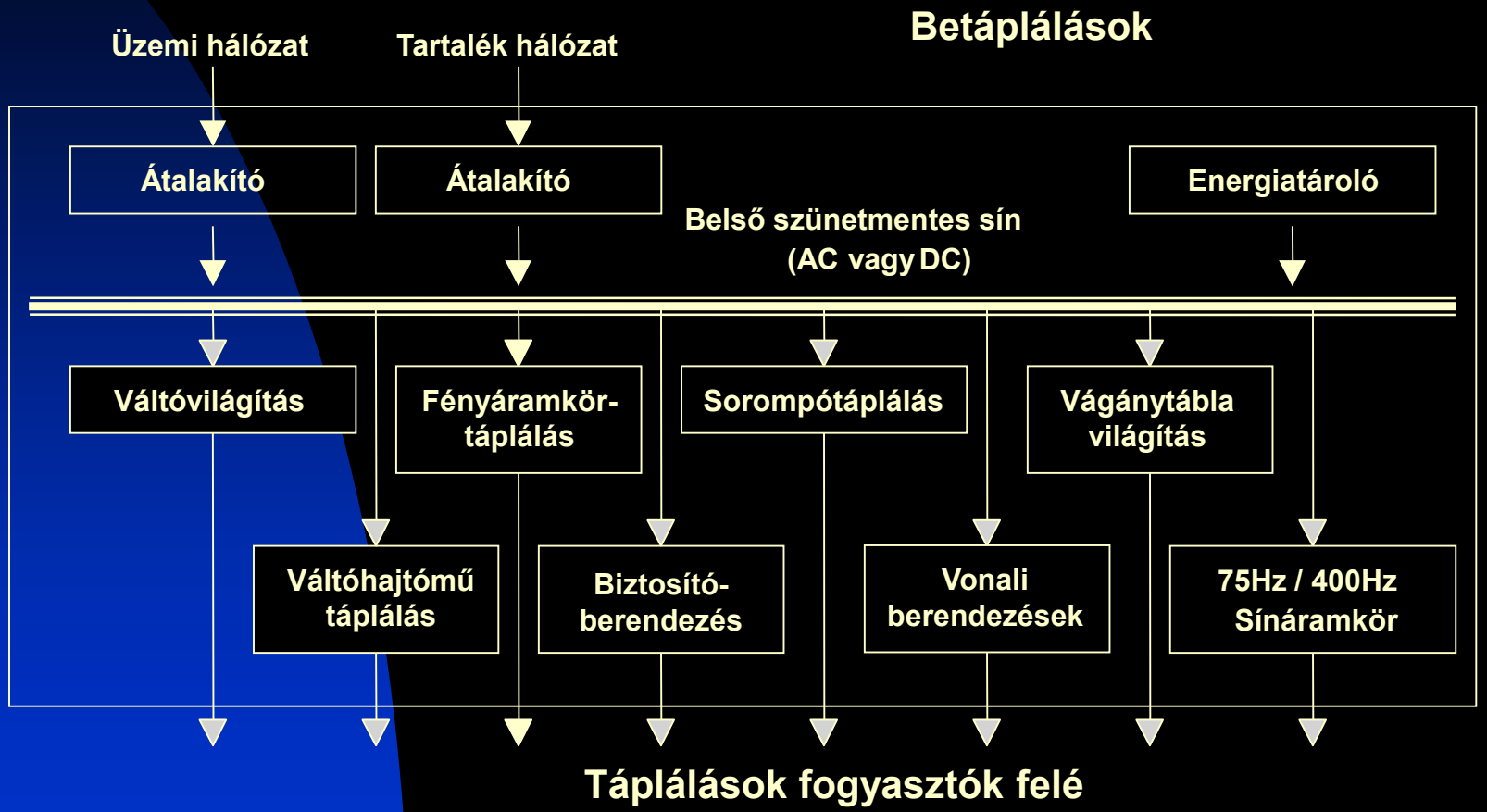
Gazdasági kritérium - A javítás humán és anyagköltsége. Az áramellátás **hibafellépési rátáját** és **javíthatóságát (karbantarthatóságát)** szabja meg.

Az áramellátás nem megfelelő voltából adódó kockázati kár

Kockázati kritérium - Biztonságkritikus rendszerek esetén az energia kimaradásából származó kár (sokszor nem forintosítható).

Az áramellátás rendelkezésre állását (illetve **eltűrhető kockázati rátáját**) szabja meg

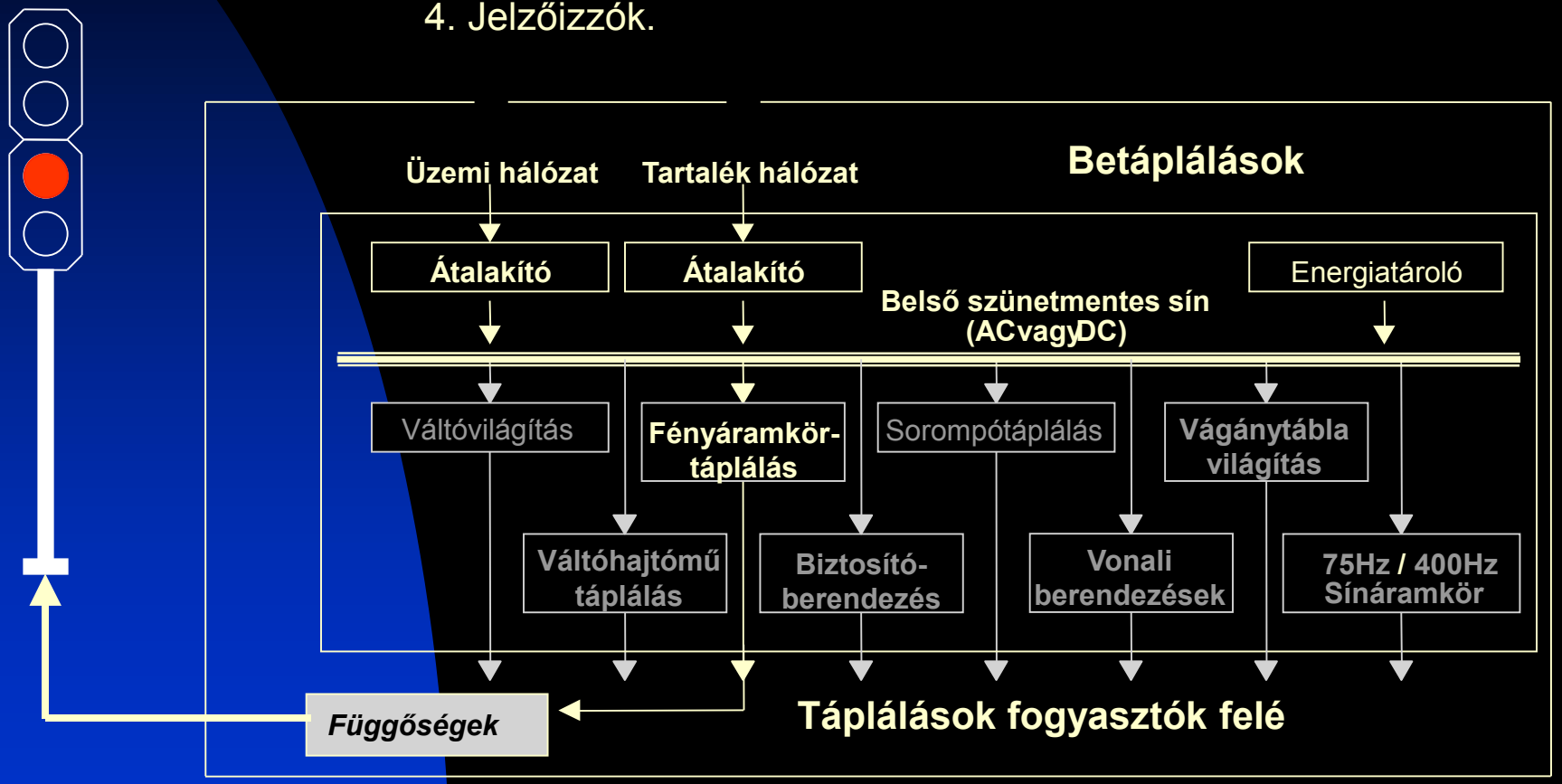
Vasúti biztosítóberendezések áramellátása



Vasúti biztosítóberendezések áramellátása - Jelzőtáplálás

Jelzőtáplálás:

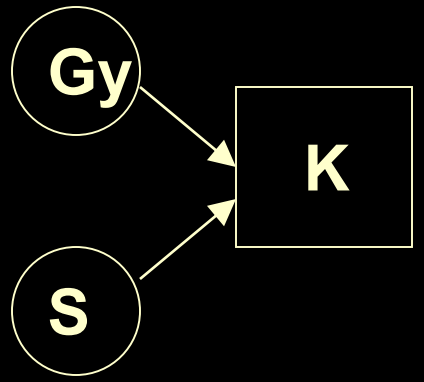
1. Áramellátás,
2. Biztosítóberendezési függőségek,
3. Tápkábelek,
4. Jelzőizzók.



Vasúti biztosítóberendezések áramellátása - Jelzőtáplálás, kockázati kritérium

Kategóriák:

K I: Nem elfogadható
K II: Elfogadható, ha nem csökkenthető
K III: Elfogadható, ha gazdaságosan nem csökkenthető
K IV: Elfogadható



Valószínűségi (gyakoriási) szint		Kár kihatási kategória			
		Katasztófális	Kritikus	Csekély	Jelentéktelen
		4	3	2	1
Gyakori	A	I	I	I	II
Valószínű	B	I	I	II	III
Esetleges	C	I	II	II	III
Csekély	D	II	II	III	IV
Valószinütlen	E	III	III	IV	IV
Nem hihető	F	IV	IV	IV	IV

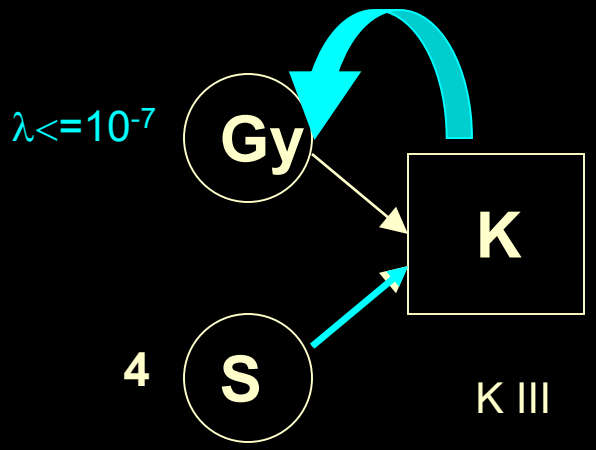
Vasúti biztosítóberendezések áramellátása - Jelzőtáplálás, kockázati kritérium

Áramellátásból származó kockázat:
Sötét jelző veszélyes meghaladása

Súlyosság: 4

Elfogadható kockázati szint: KIII vagy K IV

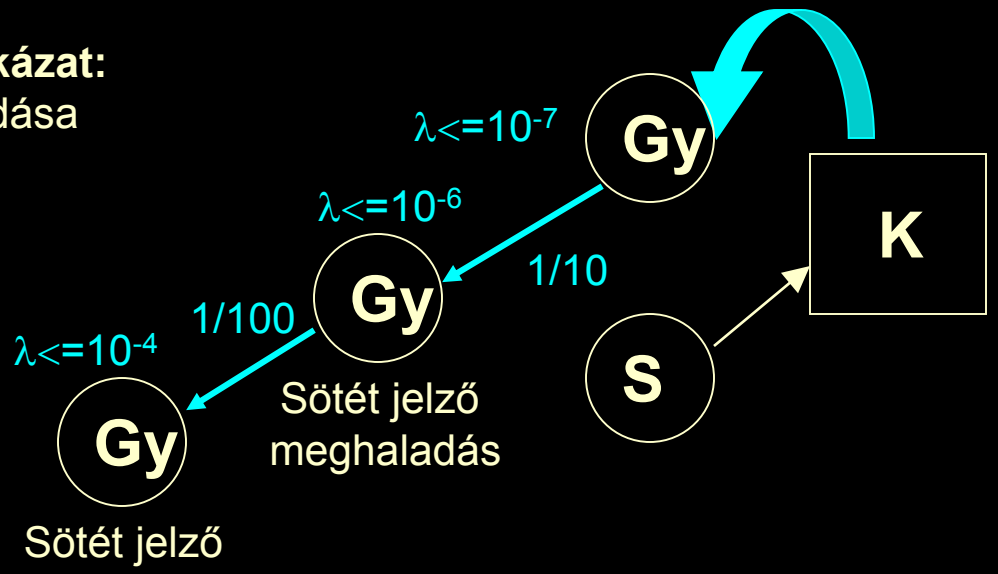
Kiadódó megengedett gyakoriság: $\lambda <= 10^{-7}$



Valószínűségi (gyakorisági) szint		Kár kihatási kategória: Katasztófális 4	Kritikus 3	Csekély 2	Jelentéktelen 1
Gyakori Valószínű	A	I	I	I	II
	B	I	I	II	III
Esetleges	C	I	II	II	III
Csekély	D	II	II	III	IV
Valószinütlen	E	III	III	IV	IV
Nem hihető	F	IV	IV	IV	IV

Vasúti biztosítóberendezések áramellátása - Jelzőtáplálás, kockázati kritérium

Áramellátásból származó kockázat:
Sötét jelző veszélyes meghaladása



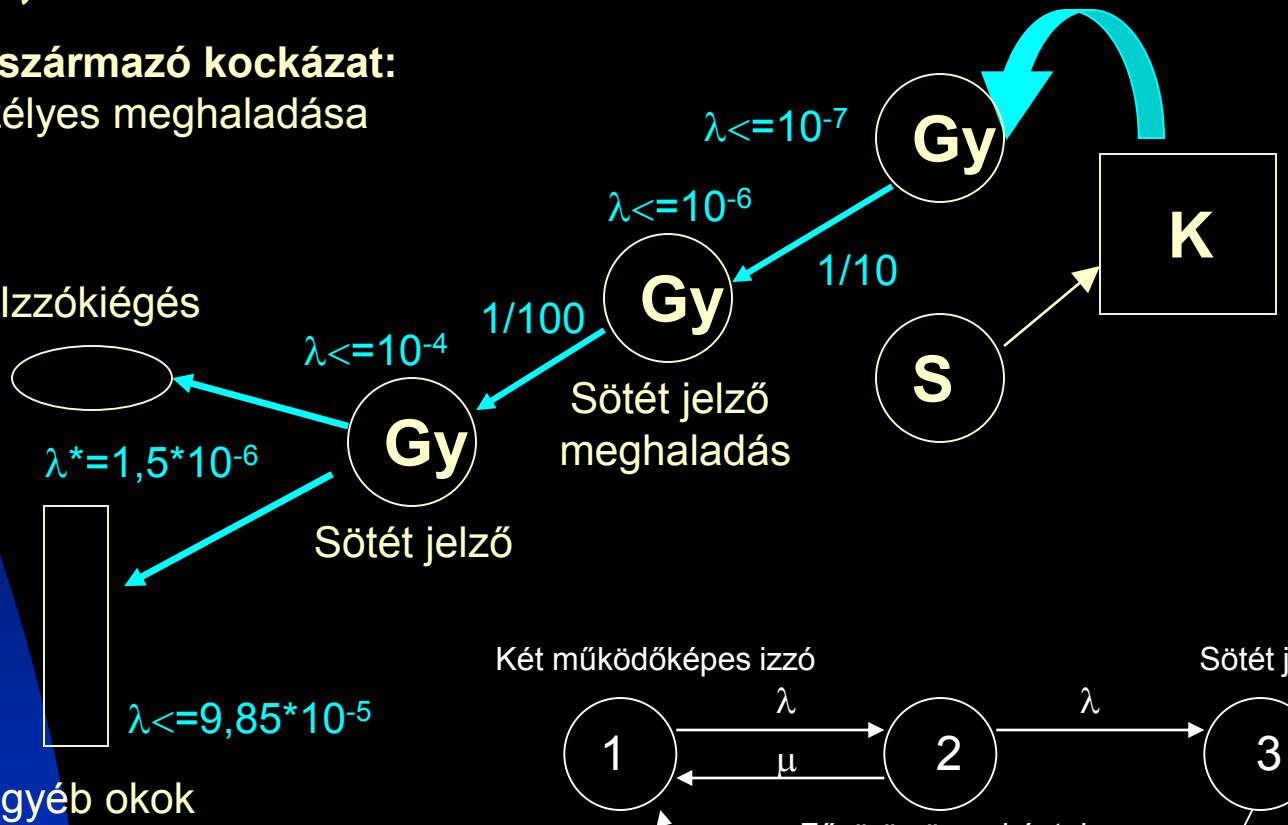
1. Sötét jelző meghaladása nem mindig balesetveszélyes

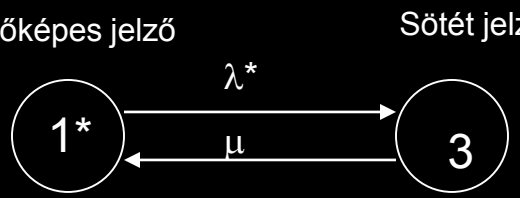
2. a. Sötét jelző esetén a sötét jelző meghaladását elősegítő tényezők

2. b. Sötét jelző esetén a sötét jelző meghaladását gátoló tényezők

Vasúti biztosítóberendezések áramellátása - Jelzőtáplálás, kockázati kritérium

Áramellátásból származó kockázat:
Sötét jelző veszélyes meghaladása



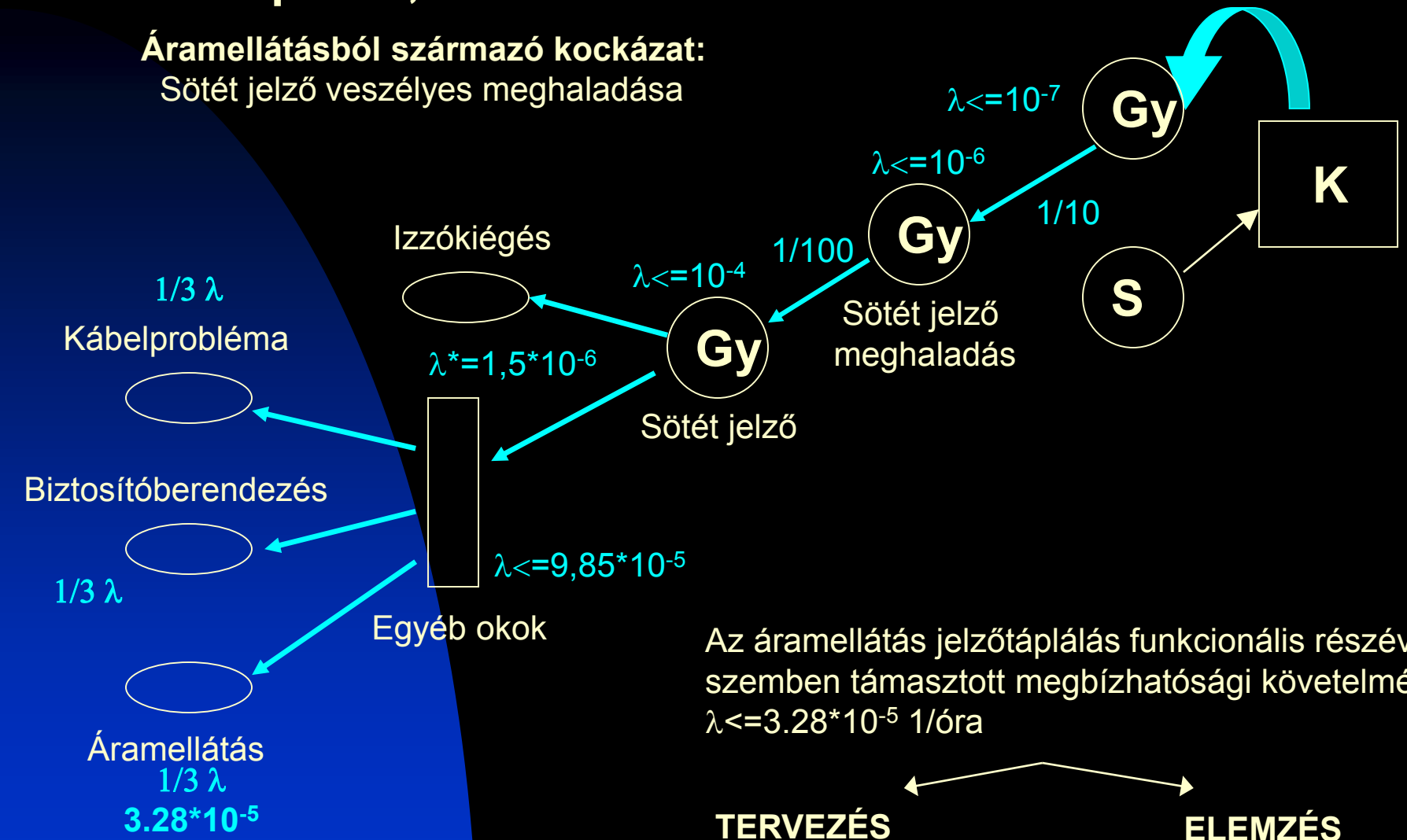


Izzókiégés gyakorisága:
- Vörös és pótvörös izzók
- Élettartam (MTTF) > 4000 óra
- Javítási idő (MTTR) < 24 óra

$\lambda^* = 1{,}5 \cdot 10^{-6}$

Vasúti biztosítóberendezések áramellátása - Jelzőtáplálás, kockázati kritérium

Áramellátásból származó kockázat:
Sötét jelző veszélyes meghaladása



Az áramellátás jelzőtáplálás funkcionális részével szemben támasztott megbízhatósági követelmény:
$\lambda <= 3.28*10^{-5}$ 1/óra

TERVEZÉS ⟷ **ELEMZÉS**

Megbízhatósági technikák

Egység, alegység szinten alkalmazható: ***FTA - Hibafa analízis*** (top-down)

Alkatrész és egység szinten alkalmazható: ***FMEA - Meghibásodási módok és hatások analízise*** (bottom-up)

Alkatrész szinten alkalmazható: ***Megbízhatósági becslés***

Megbízhatósági technikák

Megbízhatósági becslés

MIL-HDBK-217F (Notice 2)

Közös jellemzők:

- Nem kezel redundanciákat
- Igénybevételi csoportokat használ
- Meghibásodási rátát határoz meg
- Módszerek
- Alkatrész igénybevétel módszere
- Alkatrész számbavétel módszere

Megbízhatósági technikák

FMEA

Klasszikus “Mi történik, ha...” típusú kérdésekre adott válaszok

Módszertana:

- A rendszer strukturálása,
- Lehetséges meghibásodások feltárása (hibakatalógus),
- Az egyes meghibásodások hatásának elemzése (detektáltság is).

Hátrány: egy időben csak egy meghibásodással számol (egy hiba elv).

Megbízhatósági technikák

FTA

Fa szerű hibamodell felépítése

A fa elemei:

- Csúcsesemény (a vizsgált esemény),
- Közbenső események,
- Alapesemények (valószínűségi/gyakorisági információval).

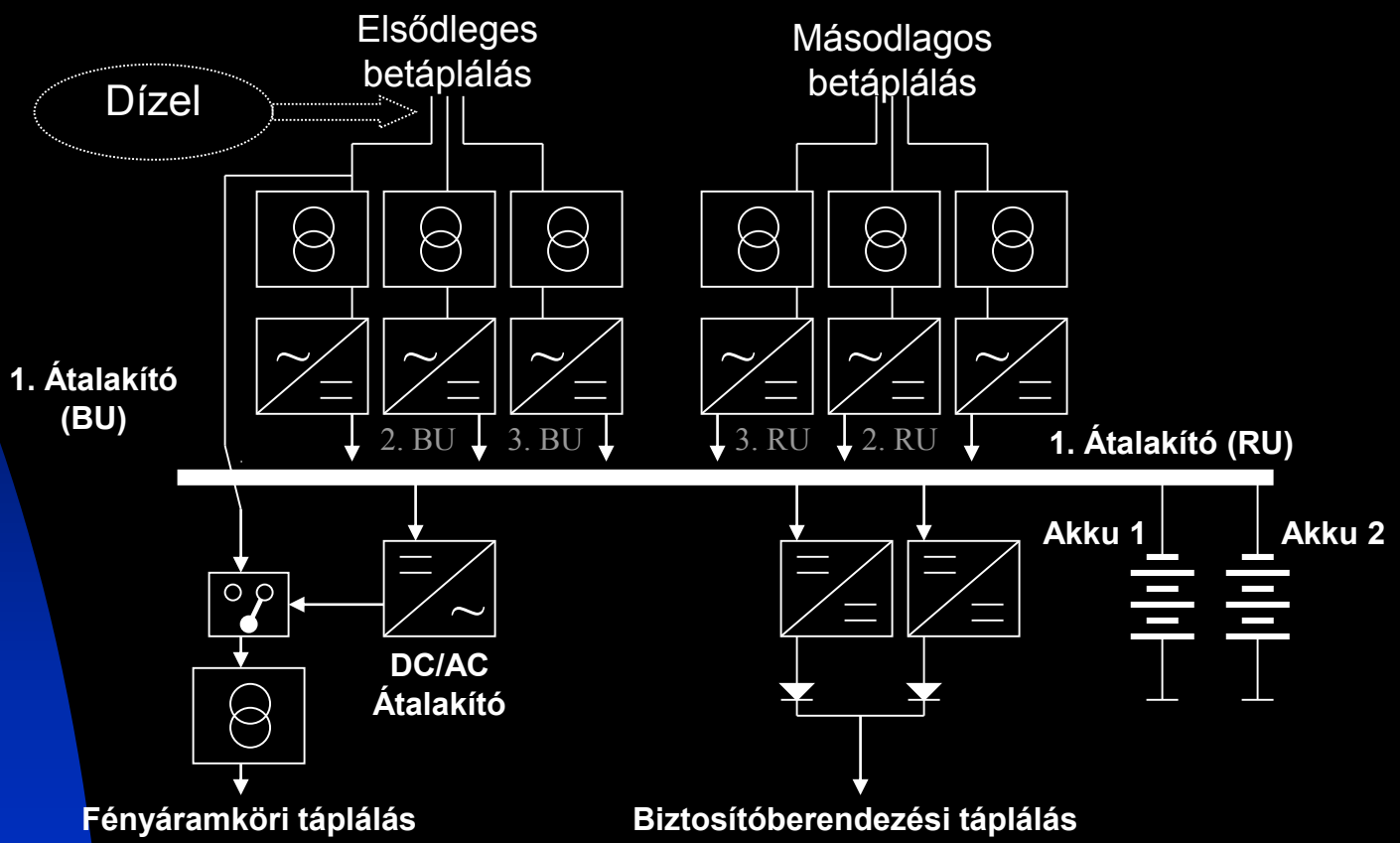
Kapcsolatok a fa elemei között:
ÉS, VAGY, (NOT), (KvN)

Eredmények:

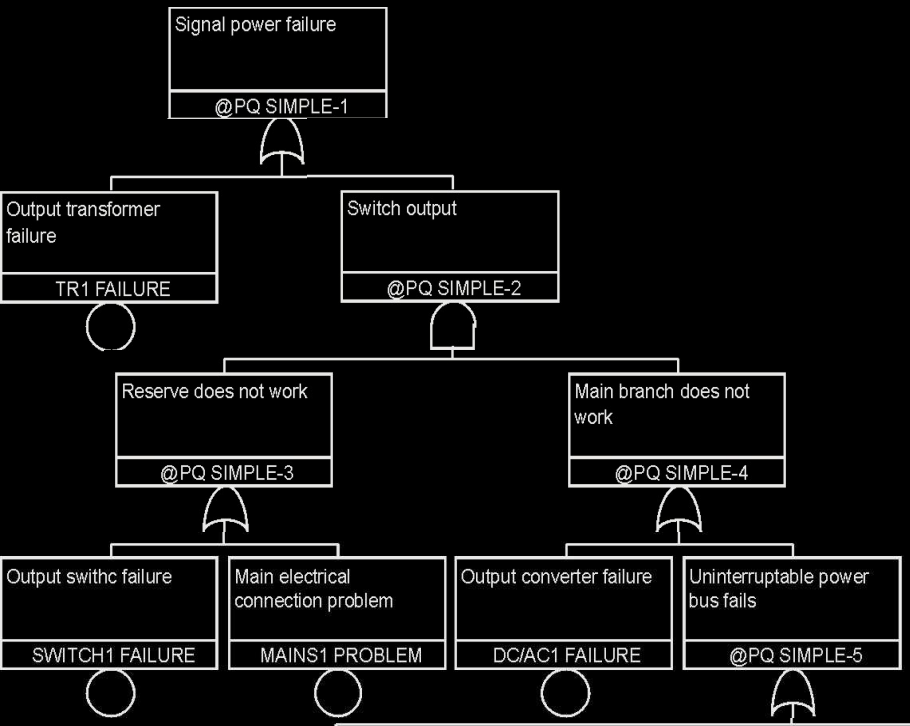
- Minimális vágatok (MCS),
- Csúcsesemény valószínűség/gyakoriság,
- Érzékenységi adatok,
- Időfüggő eredmények.

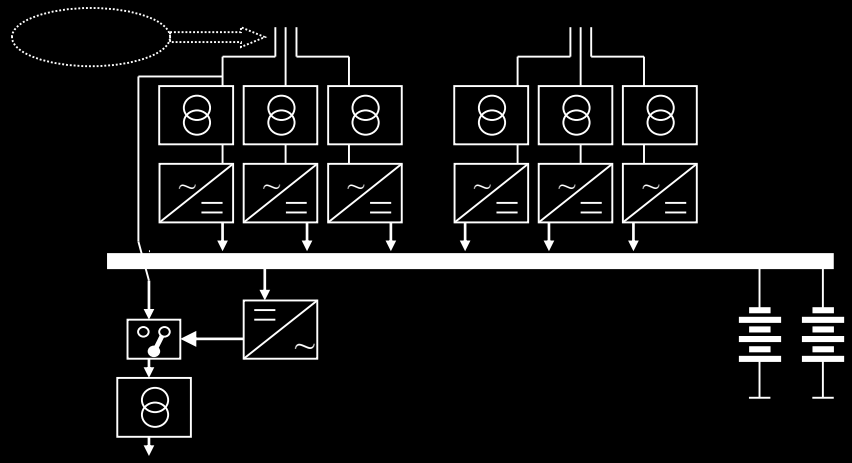
PQ áramellátás elemzése

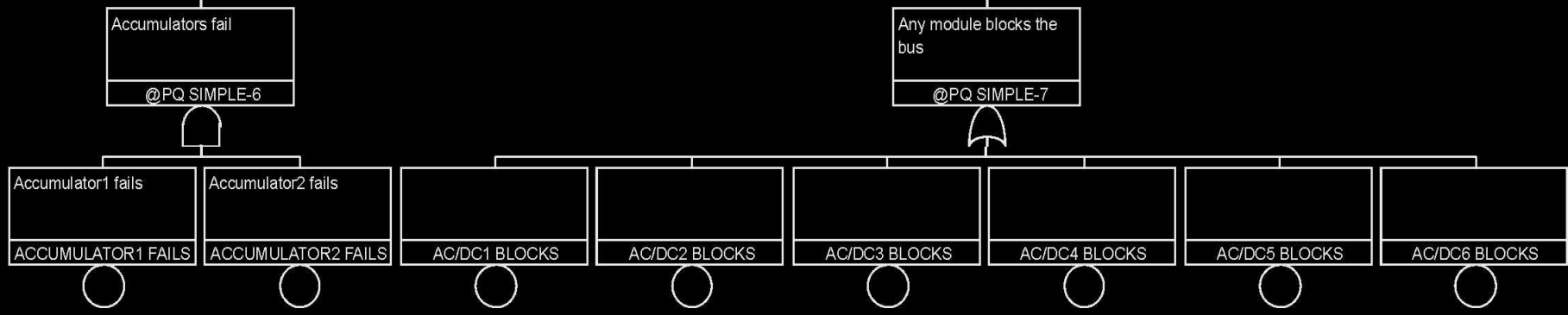
Meghibásodások:
1. BU, RU hiba,
2. Akku hiba,
3. Belső sin blokkolás,
4. Átkapcsoló hiba
 (periodikusan tesztelt!)
5. Kimeneti DC/AC hiba,
6. Kimeneti trafó hiba,
7. Hálózatkimaradás.



PQ áramellátás elemzése



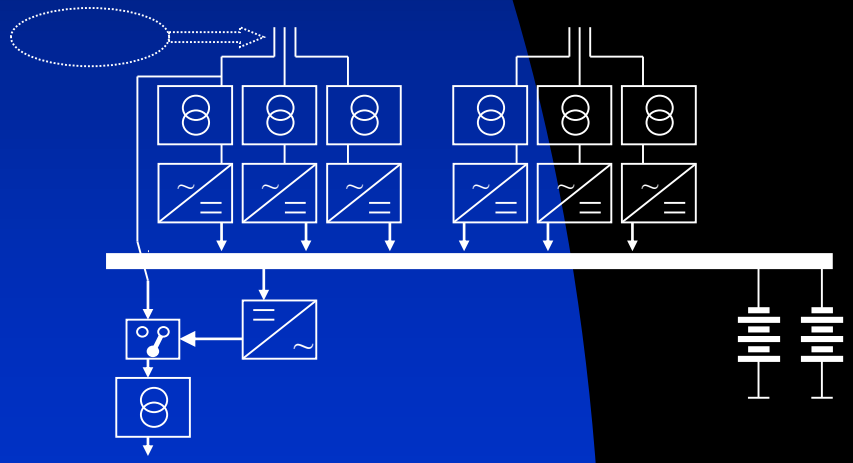


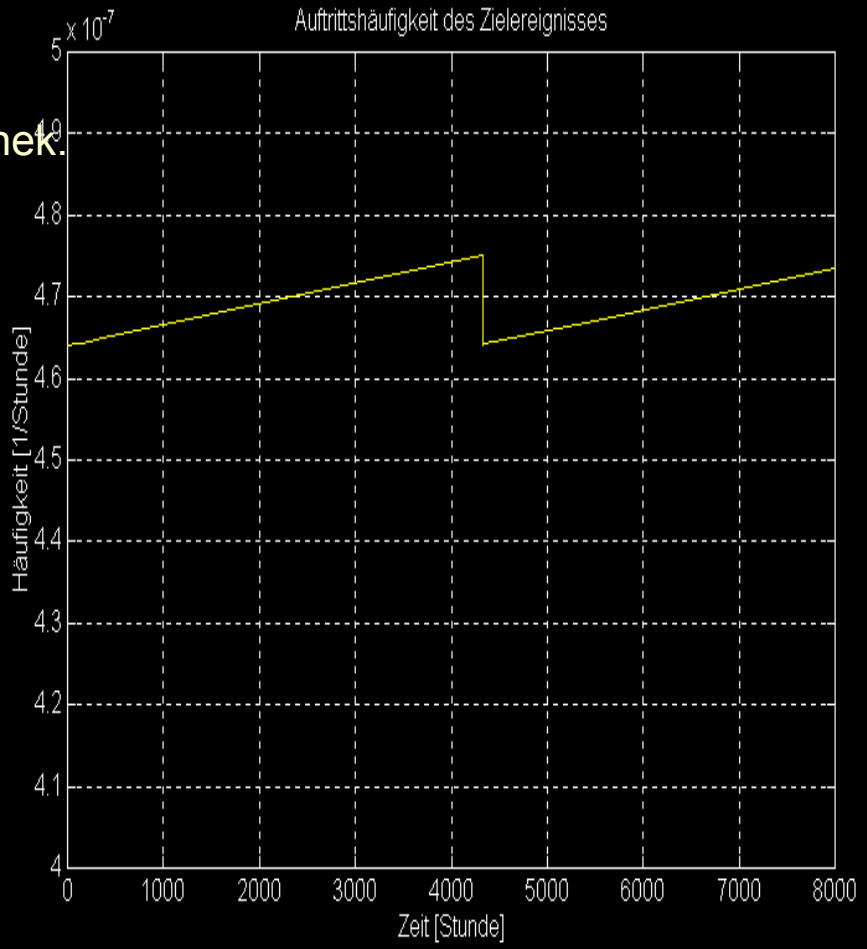


PQ áramellátás elemzése

EREDMÉNYEK

1. Numerikus analízis: A követelmények teljesülnek.
2. Érzékenységvizsgálat:
   - 2 a.: A legkritikusabb elem a kimeneti trafó,
   - 2 b.: A hálózatkiesés értéke nem kritikus.





Szabó Géza
egyetemi adjunktus
BME Közlekedésautomatikai Tanszék

Energiaellátás biztonságkritikus rendszerekben:

Megbízhatósági követelmények meghatározása és teljesülésük igazolása

Összefoglalás