Elemzési módszerek

Egyes módszerek ágazat-specifikusak, mások teljesen általánosan használatosak. A **leggyakoribb** veszélyelemző módszerek:

- Hibamód és -hatás elemzés - failure modes and effects analysis (FMEA)
- Hibamód, -hatás és kritikusság elemzés - failure modes, effects and criticality analysis (FMECA)
- Veszély- és működőképesség elemzés - Hazard and operability studies (HAZOP)
- Eseményfa elemzés - event tree analysis (ETA)
- Hibafa elemzés - fault tree analysis (FTA)

Hibamód és -hatás elemzés (FMEA)

- Az elemzés végrehajtható
  - Hardver elemekre vagy
  - Funkciókra vonatkoztatva
- Feltevésekkel él az elemek/funkciók lehetséges hibamódjairól, majd meghatározza ezek hatását
  - az adott egységre és
  - a teljes rendszerre
- Ennek során figyelembe veszi a rendszer valamennyi elemének/funkciójának valamennyi lehetséges hibamódját
- Esetenként javaslatot tesz a talált problémák orvoslására.

Hibamód és -hatás elemzés (FMEA)

Potential
Failure Mode and Effects Analysis
(Design FMEA)

___System
___Subsystem
_X_Component: Connector System

Design Responsibility: Workgroup

Model Year/Vehicle(s): / 42 VOLT SYS

Key Date: October 2000

Core Team: Refer to workgroup list

Item / Function	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s)/ Mechanism(s) Failure	Occur	Current Design Controls	Detec	R.P.N.
- handles rated electrical current with maximum voltage drop of (50mV), for up to xxx sec. over and ambient temperature range of -40C to 80C. Voltage drop spec. referenced to end-of-conditioning status, including Meet stds.for underhood environment (corrosion resistance) Must withstand SAEJ537 spec.for vibration Must satisfy thermal cycling spec.	Excessive voltage drop	Overheating Reduced voltage to loads	8		decreased normal force		end-of-line check test		
					partially backed-out connector				
					partially backed-out terminal				
					loss of asparities(terminal interface)				
					Environmental conditions				
					material properties				
	system not electrically connected	open circuit	7		excessive mating force				
					broken connector latch				
					inadequate connector latch				
	terminal not connected	open circuit	7		terminal partially seated				
					damaged terminal				
					improper terminal orientation				
					excessive mating force				
maintains mechanical integrity	doesn't support cable load	open, short, or intermittent circuit, or overheating			inadequate material selection(housing or terminal)				
					inadequate strain relief				
	unmated connectors	Open circuit overheating Reduced voltage to loads			partially backed-out connector				
					partially backed-out terminal				

Printed on: 2000 03 01 12:47:35

Design FMEA

Revision 6.0 2/11/98

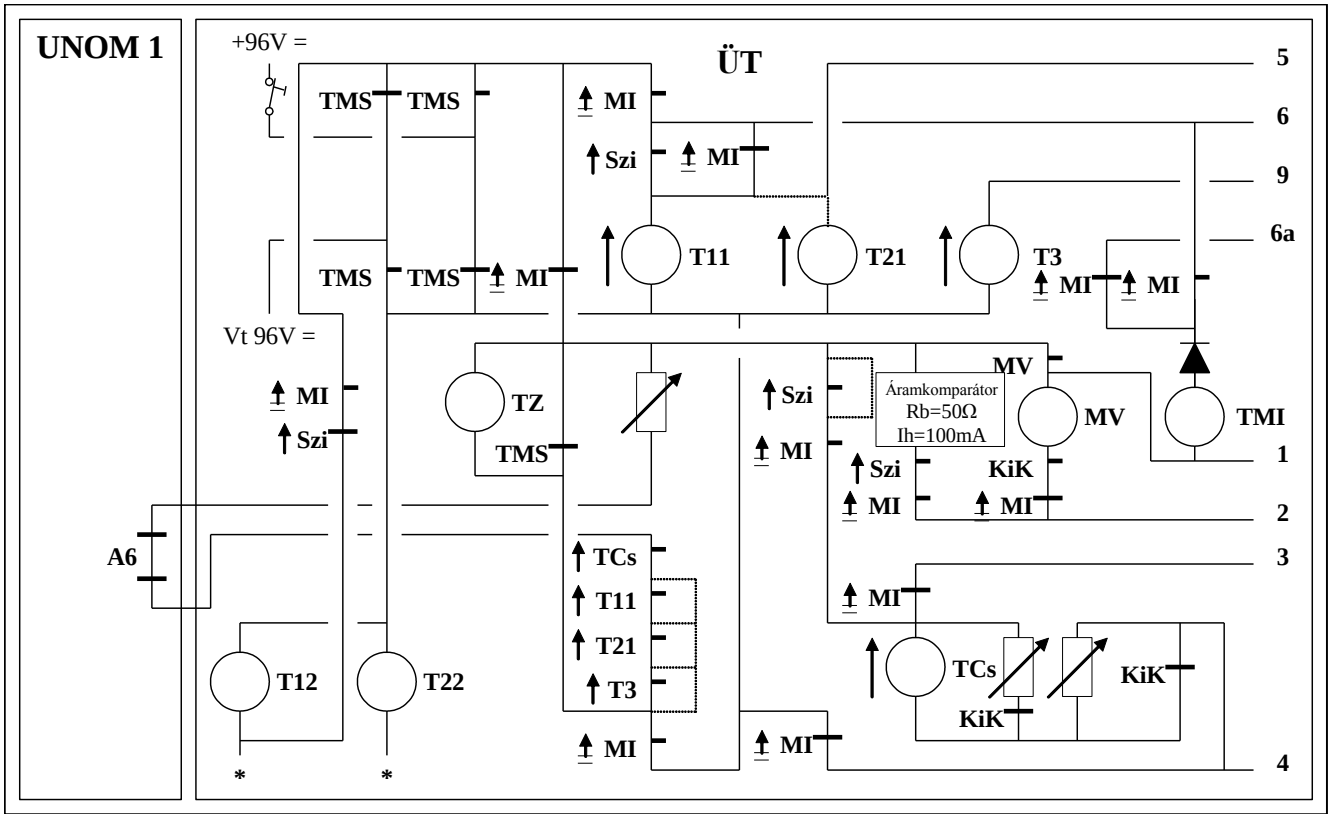
☐ System ☐ Subsystem ☑ Component	**Customer** Chrysler Motors Corporation		**Customer Part No.** DC-77323-XYZ	**Org. Date** 2/11/98	**Page** 1 of 2
	Supplier Any Company, Inc.	**Code** ACI-001	**Supplier Part No.** A-9514	**Dwg. Rev.** 8	**Key Date** 2/11/98	**FMEA No.** DFMEA-001
Part Name Filter			**Design Responsibility** Brad Anderson	**Application/Model Year** Sedan / 1998		
Core Team Brad Anderson,Jerry Benware,Lisa Brown,Ken Caracci,Bill Cox,Fred Jordan,Ken Kratz			**Prepared By** Brad A. Anderson		**Date** 2/11/98	

Item / Function	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s) / Mechanisms of Failure	Occur	Current Design Controls	Detec	R.P.N.	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	Sev	Occ	Det	R.P.N.
Filter for assembly with B44 to firewall	Insufficient wax coverage over specified surface	Deteriorated life of door leading to: Unsatisfactory appearance due to rust through paint over time, Impaired function of interior door hardware	4	◇	Insufficient wax thickness specified	4	Supplier certification	1	16	None	N/A 2/11/98					
					Inappropriate wax specified	5	set up set up	4	80							
							Five piece setup, in-process, end of run study	2	40	None	N/A 2/11/98					
	Corroded interior lower door panels	Improper oxide coating	6	🛡	Entrapped air prevents wax from entering corner/edge access	6	Test spray pattern at startup and after idle periods, and ...	5	180	Add team evaluation using production spray equipment and specified wax	Engineering and Assembly Operations 2/18/98	Based on test reults (Test #9989) spray head modified to ...	6	2	5	60
				🛡	Spray heads clogged: Viscosity too high, Temperature too low, Pressure too low	4	Incomming audit per 200-16 certification, SPC Lot/Qtr	2	48							
							Laboratory test using "worst case" wax and application hole size	3	72	Add laboratory accelerated corrosion testing	ABC Labs 2/27/98	Test results show specified ...	6	3	3	54
										Conduct DOE on wax thickness	Engineering Associates 2/18/98	DOE shows 25% variation in specified thickness is acceptable	6	2	2	24
					Feeder not properly or	3										

	Approved By Brad A. Anderson	**Date** 2/11/98

FMEA - biztonságigazoláshoz

- jelfogók:
  - érintkező nemzárása,
  - jelfogó el nem ejtése,
  - jelfogó meg nem húzása,
- diódák:
  - rövidzár,
  - szakadás,
- ellenállások, potenciométerek:
  - szakadás,
  - ellenállásnövekedés,
  - rövidzár (csak fémrétegnél),
- kondenzátorok:
  - rövidzár,
  - szakadás,
  - kapacitáscsökkenés,
- kismegszakítók:
  - szakadás,
- belsőtéri rendszerkábelek:
  - érszakadás,
- szekrény belső huzalozás:
  - szakadás,
- vezetőpálya a NYÁK-lapon (kártya vagy backpanel):
  - szakadás.



FMEA bizt. ig.

Jelfogó neve	**Kártya**
Térközjelzők Megállj! segédjelfogó (TMS)	ÜT1-S

Érintkező	**Nemzárás következménye**
II.5/6	a térközjelzők Megállj!-ra kapcsolt állapotában antivalenciahiba a SIMIS-IS bemenetén, zavarjelzés a kezelőfelületen
I.5/6	a Térközjelzők Megállj! kezelés hatástalan
II.3/4	a vonali hurok áramkör nem épül fel, a Térközjelzők Megállj! kezelés hatástalan
I.3/4	a vonali hurok áramkör nem épül fel, a Térközjelzők Megállj! kezelés hatástalan
II.1/2	a vonali hurok áramkör nem épül fel, hamisfoglaltság-visszajelentések a térközből, vonat nem indítható, menetirány nem fordítható
I.1/2	a vonali hurok áramkör nem épül fel, hamisfoglaltság-visszajelentések a térközből, vonat nem indítható, menetirány nem fordítható

El nem ejtés következménye	kijárat esetén a térközjelzők szándékolatlanul Megállj! állásban maradnak
Meg nem húzás következménye	a Térközjelzők Megállj! kezelés hatástalan

Az FMEA alkalmazása

- A fejlesztési folyamat legkülönbözőbb fázisaiban alkalmazható
- Az életciklus korai fázisában, funkciókra alkalmazva, a SIL meghatározásában játszhat szerepet
- A rendszer kialakításának jóval későbbi fázisaiban már hardver elemekre is alkalmazható → biztonságigazolás
- Kiválóan alkalmas az egyes szinteken az elemzés finomítására
  - Motorhiba hatása a repülőgépre
  - Üzemanyag-szivattyú hibájának hatása a motorra
  - szelephiba hatása az üzemanyag-szivattyúra
- Az analízis kiegészíthető valószínűségi információval is
- Gyakran „szállít” bemenő adatokat az FTA számára

Az FMEA értékelése

- Mivel a módszer minden lehetséges hibát figyelembe vesz, különösen alkalmas az **egyszeres hibák detektálási feltételeinek** meghatározására
- Ugyanakkor **nem** veszi figyelembe a többszörös hibákat
- Mivel minden hibát figyelembe vesz, igen sok ráfordítást igényelnek azok a hibák, amelyek nem okoznak veszélyeztetést
- Nagy, komplex rendszerek esetén rendkívül ráfordítás-igényes
- Ezért sok esetben csak a fejlesztési folyamat végső fázisaiban, és csak a kritikus területek vizsgálatára alkalmazzák

Hibamód, -hatás és kritikusság elemzés (FMECA)

- A FMEA kiterjesztése
- Figyelembe veszi az elemek meghibásodásainak fontosságát is:
  - az egyes hibák következményeit és
  - fellépésének gyakoriságát vagy valószínűségét
- Ezzel meghatározza a rendszer azon részeit, amelyekben a hibák a leginkább kritikusak
- Ezáltal lehetővé teszi, hogy az erőfeszítéseket arra a területre irányítsák, ahol azokra a legnagyobb szükség van

Veszély- és működőképesség elemzés (HAZOP)

- Eredetileg vegyipari, ma már széleskörű alkalmazás
- „Guide words” - „Mi történik, ha …” típusú kérdésekre adott válaszokkal igyekszik meghatározni a normál működési feltételektől való eltérések hatásait, pl.:
  - Mi történik, ha megnő a hőmérséklet?
  - Mi történik, ha csökken a nyomás?
- Különösen alkalmas a paraméterváltozások és az előírt tartományokból való kilépések (out-of-range) biztonságra gyakorolt hatásának vizsgálatára
- Elemző team - jártasság
  - A fejlesztési módszerekben
  - Az adott alkalmazási területen
  - A HAZOP és más veszélyelemzési technikák területén
- Rendkívül munka- és időigényes

Vezérszavak (guide words)

Vezérszó (guide word)		JELENTÉS
ANGOL	**MAGYAR**	
NO	Nincs	Tervezési célok teljes elmaradása
LESS	Kevesebb, kisebb	Mennyiségi csökkenés
MORE	Több, nagyobb	Mennyiségi növekedés
PART OF	Részben	Minőségi csökkenés
AS WELL AS	Még	Minőségi növekedés
REVERSE	Fordított	Tervezési célok fordítottja
OTHER THAN	Más mint	Teljes helyettesítés
LATER THAN	Később	Szakaszos folyamatban később
SOONER THAN	Előbb	… előbb
TOO QUICKLY	Túl gyorsan	…előírtnál gyorsabban
TOO SLOWLY	Túl lassan	… előírtnál lasabban

HAZOP példa

Process Unit: DAP Production

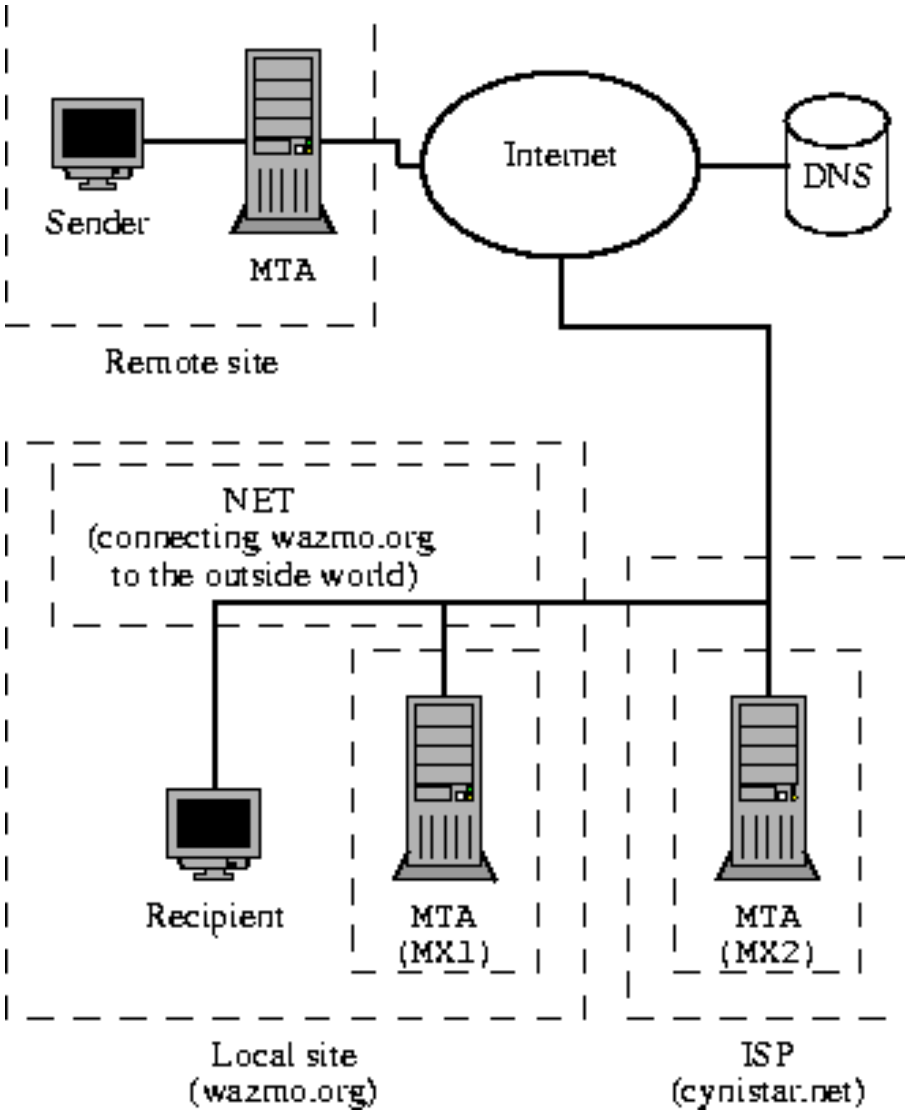
Node: 1 Process Parameter: Flow

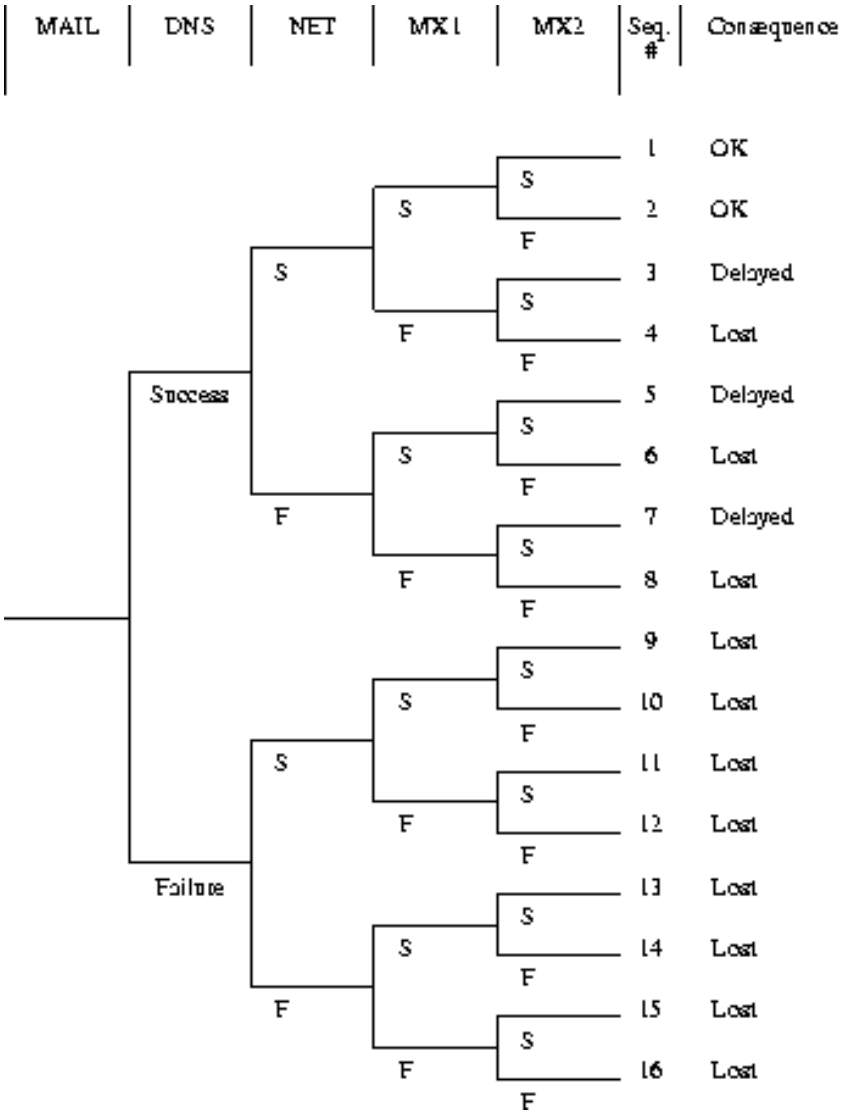
GUIDE WORD	DEVIATION	CONSEQUENCES	CAUSES	SUGGESTED ACTION
No	No Flow	Excess ammonia in reactor. Release to work area.	(1) Valve A fails closed	Automatic closure of valve B on loss of flow from phosphoric acid supply
			(2) Phosphoric acid supply exhausted	
			(3) Plug in pipe; pipe ruptures	
Less	Less Flow	Excess ammonia in reactor. Release to work area, with amount released related to quantitative reduction in supply. Team member to calculate toxicity vs. flow reduction.	(1) Valve A partially closed	Automatic closure of valve B on reduced flow from phosphoric acid supply. Set point determined by toxicity vs. flow calculation
			(2) Partial plug or leak in pipe	
More	More Flow	Excess phosphoric acid degrades product. No hazard to work area.	--	--
Part of	Normal flow of decreased concentration of phosphoric acid	Excess ammonia in reactor. Release to work area, with amount released related to quantitative reduction in supply.	(1) Vendor delivers wrong material or concentration	Check phosphoric acid supply tank concentration after charging
			(2) Error in charging phosphoric acid supply tank	

Eseményfa elemzés (ETA)

- A kiindulópont egy olyan esemény, amely hatással lehet a rendszerre (de önmagában nem feltétlenül veszélyeztető)
- A kiinduló esemény hatását rendre kombináljuk minden további, számbajövő esemény hatásával
- A hatást
  - mind normál,
  - mind hibás működésre vizsgálják
- Fa-struktúra szerű szétágazás - „n” esemény: 2^n ág
- Igazi haszna komplexebb esetekben van, amikor az eredmény nem annyira nyilvánvaló

ETA példa


Sender
MTA
Internet
DNS
Remote site
NET
(connecting wazmo.org
to the outside world)
Recipient
MTA
(MX1)
MTA
(MX2)
Local site
(wazmo.org)
ISP
(cynistar.net)


MAIL
DNS
NET
MX1
MX2
Seq. #
Consequence
Success
Failure
S
F
1 OK
2 OK
3 Delayed
4 Lost
5 Delayed
6 Lost
7 Delayed
8 Lost
9 Lost
10 Lost
11 Lost
12 Lost
13 Lost
14 Lost
15 Lost
16 Lost

Hibafa elemzés (FTA)

- Az elemzés fordított irányban halad, mint az ETA-nál:
  - Egy már - esetleg FMEA vagy HAZOP révén - azonosított, veszélyeztető hatású, ún. **csúcseseményből** kiindulva
  - visszafelé haladva határozzuk meg a csúcseseményt kiváltó ún. **elemi eseményeket**

- A hatások kombinálásánál logikai (Boole) operátorokat használunk

- A hibafában csak azok az események szerepelnek, amelyek veszélyeztető hatásúak, így az FTA-struktúra jóval egyszerűbb lehet, mint az ETA-struktúra

Hibafa analízis
Fault Tree Analysis

Elsősorban biztonsági felelősségű rendszerek megbízhatósági elemzésére szolgáló módszer.

Alkalmazásával meghatározható a vizsgált rendszer

- kiválasztott, ún. **csúcseseményének** és az ún. **elemi eseményeknek** a logikai kapcsolata,
- csúcseseményének bekövetkezési valószínűsége,
- ún. minimális vágatainak halmaza,
- hibatűrő képessége.

A módszer alkalmas a tervezett rendszer

- megbízhatósági jellemzőinek az elvárásokkal való összevetésére,
- gyenge pontjainak kimutatására,
- megbízhatósági szempontból alul- és túlméretezésének elkerülésére.

Hibafa szerkesztése

1. lépés

Definiáljuk azt az eseményt, az ún. **csúcseseményt**, amelynek szempontjából számoljuk a megbízhatósági jellemzőket. Ez az esemény valamilyen hibás működés, illetve a működés elmaradása.

2. lépés

Keressük azokat az ún. **elemi eseményeket**, amelyeknek fellépésekor, esetleg más elemi események fellépésétől is függően, a csúcsesemény bekövetkezik.

3. lépés

Meghatározzuk az elemi események és a csúcsesemény **logikai kapcsolatát**.

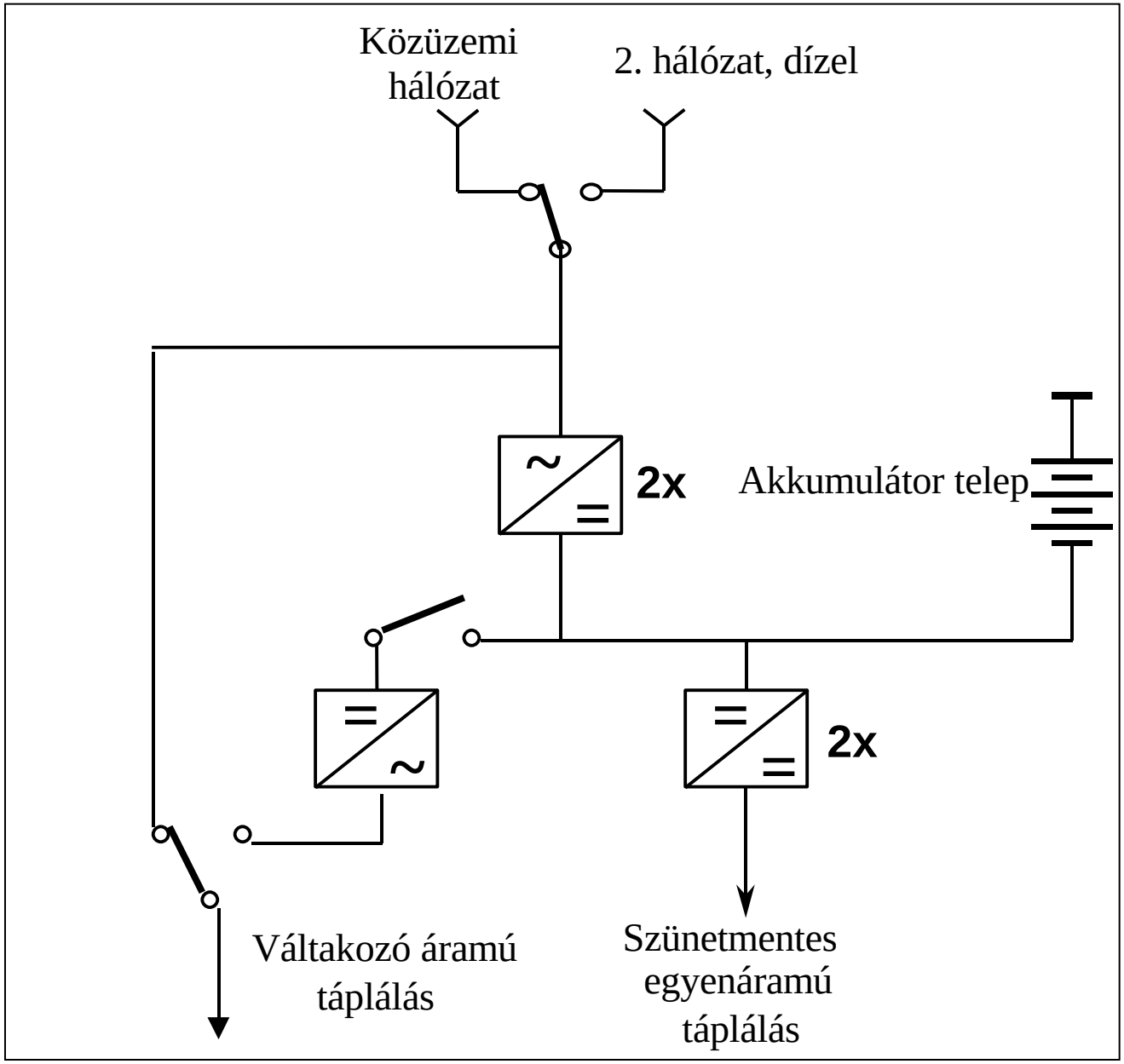
4. lépés

Az elemi események fellépésének valószínűsége alapján meghatározzuk a csúcsesemény **bekövetkezésének valószínűségét**.

5. lépés

Szükség esetén **további elemzéseket** hajtunk végre.

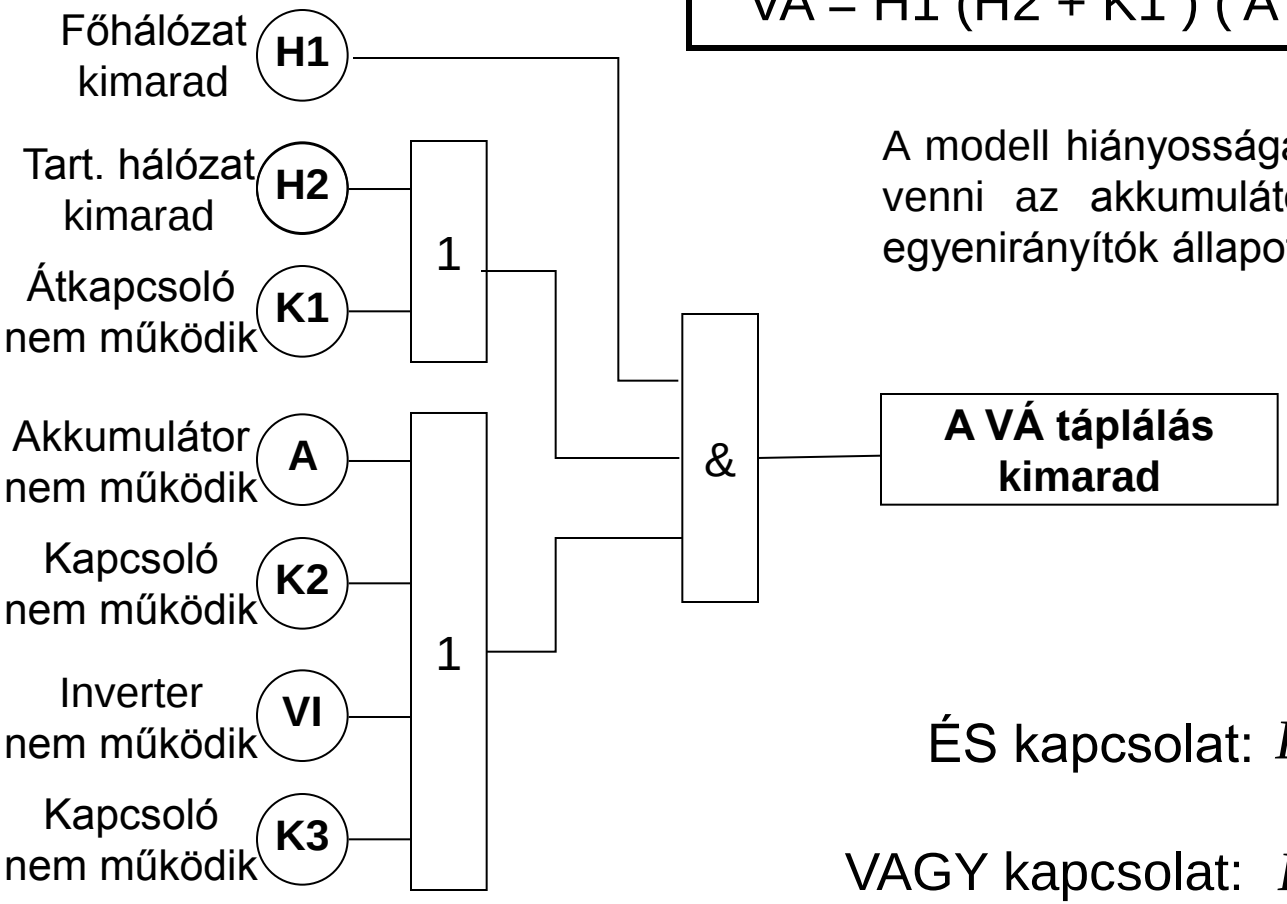
ÁRAMELLÁTÁSI RENDSZER PRIMER ÉS SZEKUNDER OLDALI TARTALÉKOLÁSSAL



ÁRAMELLÁTÓ BERENDEZÉS HIBAFÁJA

Csúcsesemény: a váltakozó áramú táplálás kimarad

VA = H1 (H2 + K1) (A + K2 + VI + K3)



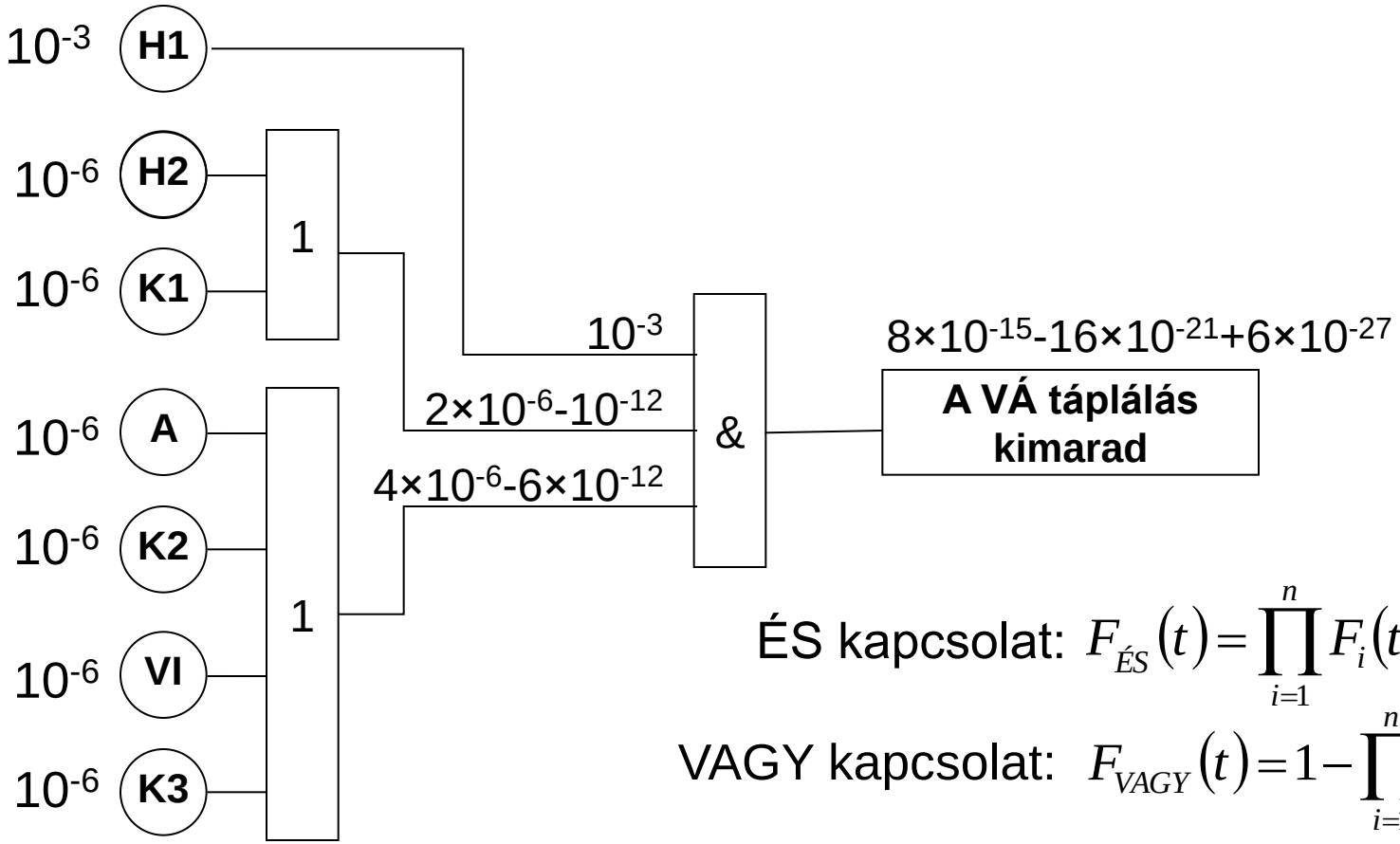
A modell hiányossága, hogy nem tudja figyelembe venni az akkumulátor működőképességének az egyenirányítók állapotától való függését.

ÉS kapcsolat: $F_{ÉS}(t) = \prod_{i=1}^{n} F_i(t)$

VAGY kapcsolat: $F_{VAGY}(t) = 1 - \prod_{i=1}^{n} (1 - F_i(t))$

A csúcsesemény bekövetkezési valószínűsége

Csúcsesemény: a váltakozó áramú táplálás kimarad



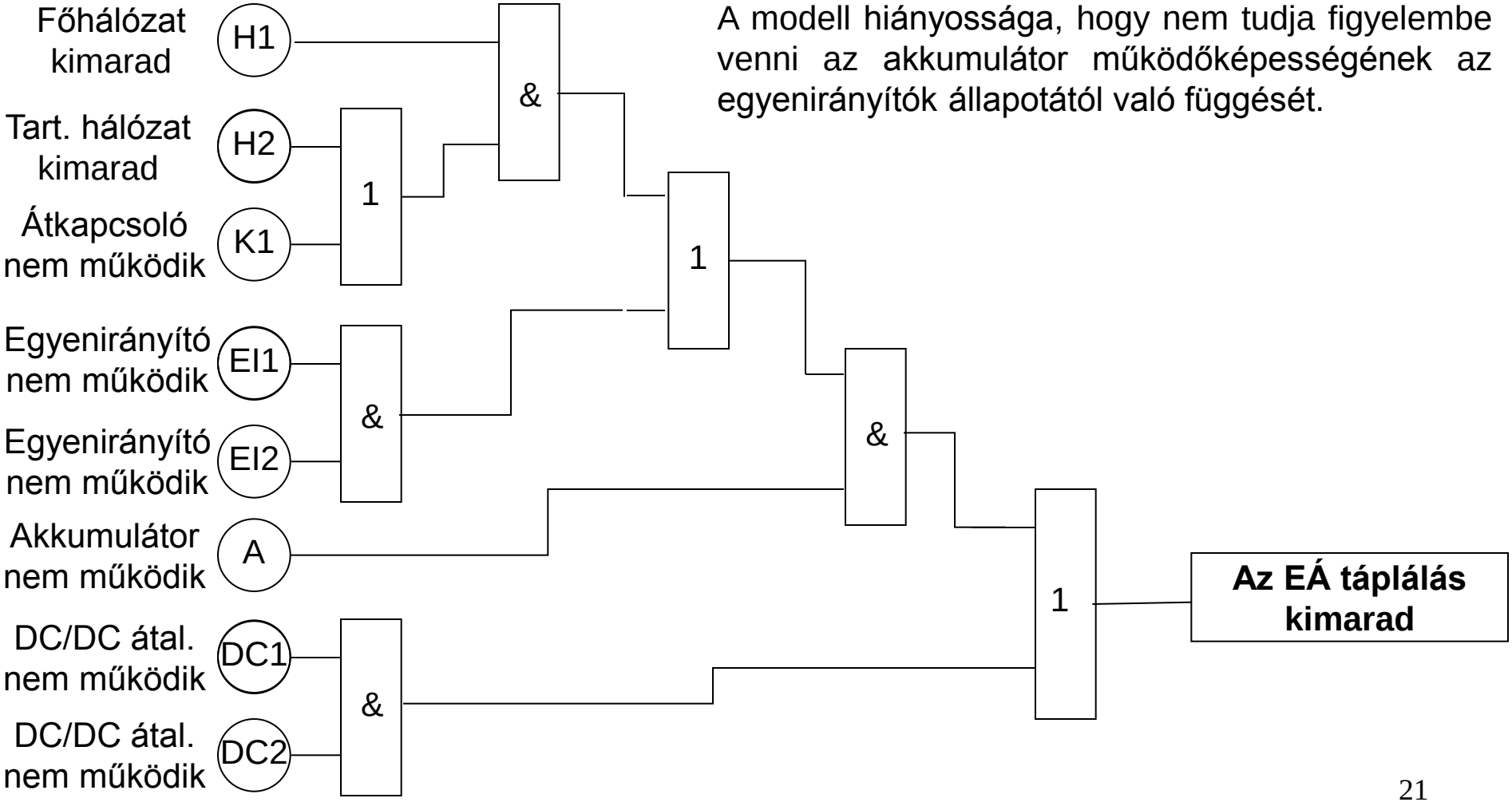
ÉS kapcsolat: $F_{ÉS}(t) = \prod_{i=1}^{n} F_i(t)$

VAGY kapcsolat: $F_{VAGY}(t) = 1 - \prod_{i=1}^{n} (1 - F_i(t))$

ÁRAMELLÁTÓ BERENDEZÉS HIBAFÁJA

Csúcsesemény: az egyenáramú táplálás kimarad

$$EA = [\, H1\,(\, H2 + K1\,) + (\, E1\, E2)\,]\, A + (\, DC1\, DC2\,)$$



A modell hiányossága, hogy nem tudja figyelembe venni az akkumulátor működőképességének az egyenirányítók állapotától való függését.

Minimális vágatok

Vágat
Azoknak az elemi eseményeknek a halmaza, amelyek együttes fellépésekor a csúcsesemény bekövetkezik.

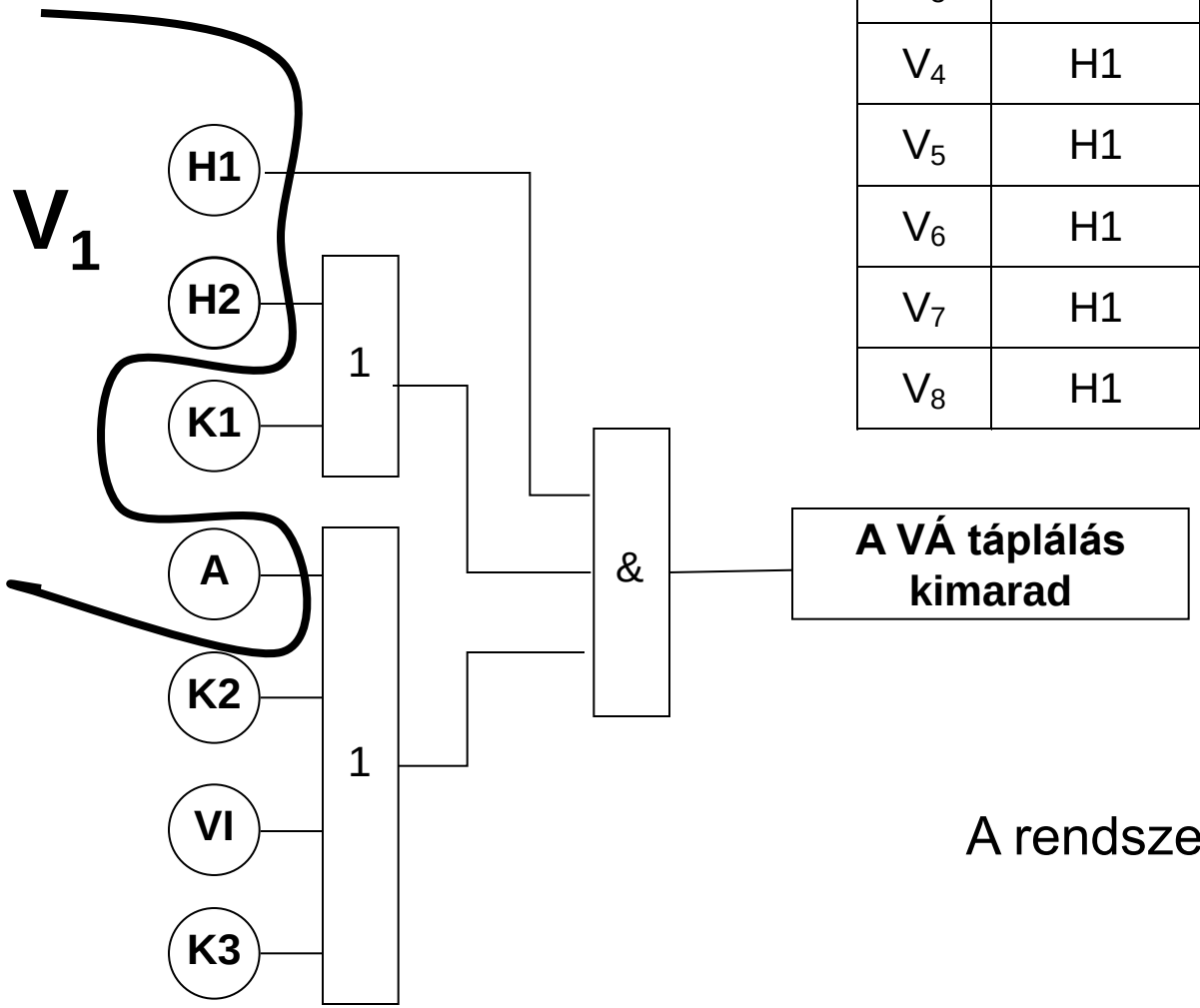
Minimális vágat
Azoknak az elemi eseményeknek a halmaza, amelyek együttes fellépésekor a csúcsesemény bekövetkezik, azonban ezek közül bármelyik esemény elmaradásakor a csúcsesemény sem következik be.

Gyenge pontok meghatározása
A minimális vágatokhoz hozzárendeljük a bennük szereplő események fellépési valószínűségének szorzatát. Az így kapott értékek alapján a vágatokat sorba rendezve látható, hogy elsősorban mely elemi események felelősek a csúcsesemény bekövetkezéséért.

Hibatűrő képesség
A rendszer hibatűrő képessége eggyel kisebb, mint a legkevesebb elemi eseményt tartalmazó minimális vágat elemszáma.

Minimális vágatok

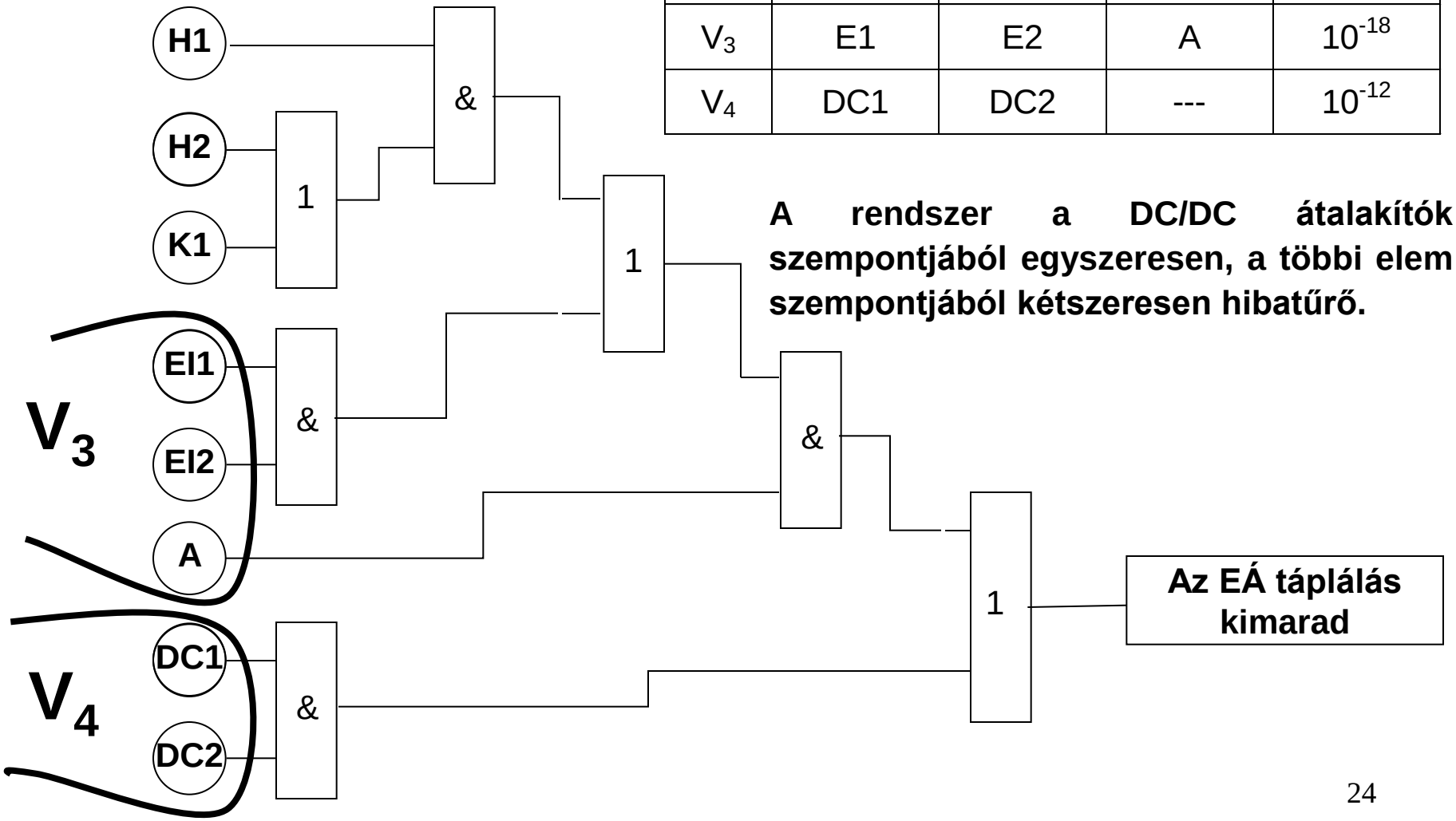
Vágat jele	1. elemi esemény	2. elemi esemény	3. elemi esemény	Valószí-nűség
V_1	H1	H2	A	10^{-15}
V_2	H1	H2	K2	10^{-15}
V_3	H1	H2	VI	10^{-15}
V_4	H1	H2	K3	10^{-15}
V_5	H1	K1	A	10^{-15}
V_6	H1	K1	K2	10^{-15}
V_7	H1	K1	VI	10^{-15}
V_8	H1	K1	K3	10^{-15}



A rendszer kétszeresen hibatűrő

Minimális vágatok

Vágat jele	1. elemi esemény	2. elemi esemény	3. elemi esemény	Valószí-nűség
V_1	H1	H2	A	10^{-15}
V_2	H1	K1	A	10^{-15}
V_3	E1	E2	A	10^{-18}
V_4	DC1	DC2	---	10^{-12}



A rendszer a DC/DC átalakítók szempontjából egyszeresen, a többi elem szempontjából kétszeresen hibatűrő.