MODELING AND ANALYSIS OF FAILURES IN COMPUTER NETWORKS USING CAUSE-AND-CONSEQUENCE METHODS*

NELI A. ARABADZHIEVA-KALCHEVA, TSVETOSLAV S. TSANKOV

ABSTRACT: *The paper presents an integrated fault tree and event tree model for network service unavailability. A redundant-link network with a common-cause failure and an imperfect automatic failover mechanism is investigated. Five hypothetical infrastructure scenarios are evaluated using exact Boolean probability expressions and Monte Carlo simulation with three million trials per scenario. The effect of redundancy, failover reliability and shared infrastructure faults on service availability is quantified. The results demonstrate the value of combining causal modeling and probabilistic verification for selecting reliability improvements. All input probabilities are illustrative rather than field measurements.*

KEYWORDS: *computer networks, fault tree analysis, event tree analysis, network reliability, redundancy, Monte Carlo simulation*

DOI: https://doi.org/10.46687/MT26NAT

МОДЕЛИРАНЕ И АНАЛИЗ НА ОТКАЗИ В КОМПЮТЪРНИ МРЕЖИ ЧРЕЗ ПРИЧИННО-СЛЕДСТВЕНИ МЕТОДИ

НЕЛИ А. АРАБАДЖИЕВА-КАЛЧЕВА, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Предложен е модел за изследване на недостъпността на мрежова услуга, който съчетава дърво на отказите и дърво на събитията. Разгледана е мрежа с две комуникационни линии, общи точки на отказ и автоматично превключване към резервната линия. За пет моделни конфигурации са изчислени аналитични вероятности и са проведени по три милиона Монте Карло изпитвания. Анализирано е влиянието на резервирането, надеждността на превключването и общите причини за отказ. Резултатите илюстрират приложимостта на комбинираното моделиране при избор на мерки за повишаване на надеждността; използваните вероятности са хипотетични.*

1 Въведение

Надеждността на компютърните мрежи зависи не само от характеристиките на отделните устройства, но и от структурата на зависимостите между тях. Отказ на един елемент може да остане незабелязан при наличие на резервен път, докато обща причина, засягаща няколко елемента, може да обезсмисли резервирането. За обосновано планиране на защитни и възстановителни мерки са необходими модели, които разграничават причините за прекъсване от развитието на инцидента и последствията.

Анализът чрез дърво на отказите (Fault Tree Analysis, FTA) изследва логическите комбинации от базови събития, които предизвикват предварително зададено нежелано събитие [3]. Анализът чрез дърво на събитията (Event Tree Analysis, ETA) проследява възможните изходи след начално събитие и действието на възстановителните механизми [4]. Съвместното им приложение е регламентирано като възможен подход в методическите документи за надеждност [4, 5].

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

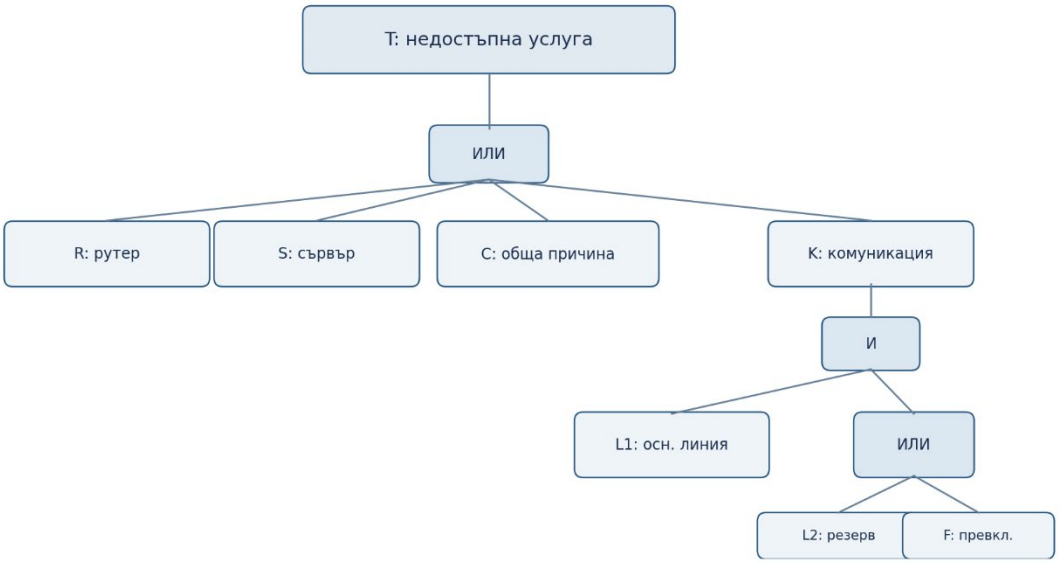
В предходни публикации авторите разглеждат оценяване на мрежови откази чрез FMEA [1] и причинно-следствен анализ на конкретен сценарий [2]. Настоящото изследване надгражда тези постановки, като въвежда изричен вероятностен модел на резервирана мрежа, изчислява вероятността за недостъпност при пет конфигурации и проверява резултатите чрез симулация. Целта е да се оцени как автоматичното превключване и общите точки на отказ влияят върху ползата от резервната комуникационна линия.

2 Модел и методи

Разглежда се условна корпоративна информационна услуга, достъпна през основна комуникационна линия L1 и резервна линия L2. За функционирането ѝ са необходими маршрутизатор R, приложен сървър S и обща инфраструктура C (например общо електрозахранване). При отказ на L1 системата използва L2, ако тя е налична и автоматичното превключване е успешно. F обозначава неуспешно превключване. Анализът се отнася за един предварително фиксиран наблюдателен интервал; събитията са двоични, а вероятностите им не представляват измерени стойности от действаща система.

Върховото събитие T е недостъпност на услугата. Логическата му структура е представена с булевия израз и с дървото на отказите на фиг. 1. Минималните сечения са {R}, {S}, {C}, {L1, L2} и {L1, F}. В модела общата причина C се отчита изрично и не се отъждествява с независимите откази на двете линии.

$$T = R \vee S \vee C \vee [L_1 \wedge (L_2 \vee F)] \tag{1}$$

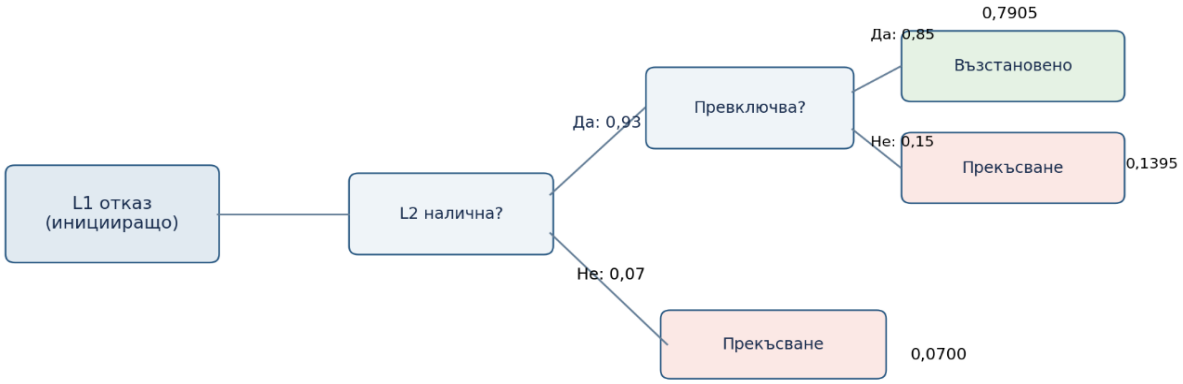


Фиг. 1. Логическа структура на дървото на отказите

При допускане за независимост на базовите събития вероятността за върховото събитие се определя чрез формула (2), където pX е вероятността за събитие X, а pF е условната вероятност за неуспешно превключване, когато то се изисква. Независимостта е моделиращо допускане; при реално приложение то трябва да бъде проверено.

$$p_T = 1 - (1 - p_R)(1 - p_S)(1 - p_C)\{1 - p_{L1}[p_{L2} + (1 - p_{L2})p_F]\} \tag{2}$$

За ЕТА се приема, че началното събитие е отказ на основната линия. Първо се проверява наличността на резервната линия, а след това — успехът на превключването. При pL2 = 0,07 и pF = 0,15 условната вероятност за възстановяване е (1−0,07)(1−0,15) = 0,7905; останалите два изхода са отказ на превключването при налична резерва (0,1395) и недостъпна резерва (0,0700). Трите изхода са взаимно изключващи се и сумата им е единица. Последователността на разклоненията и вероятностите за трите възможни изхода са представени на фиг. 2.



Фиг. 2. Дърво на събитията след отказ на основната линия

3 Постановка на изчислителния експеримент

Използвани са шест параметъра, избрани единствено за демонстриране на метода. Всички вероятности се отнасят до едно и също наблюдателно време; не са извеждани от реални журнали за инциденти или експлоатационна статистика. Стойностите са: pR = 0,020; pS = 0,015; pC = 0,010; pL1 = 0,060; pL2 = 0,070; pF = 0,150. Изследвани са пет сценария: (А) само основна линия; (Б) резервна линия със 85% успешно превключване; (В) подобрено превключване с 97% успех; (Г) сценарий В с по-надеждни R, S и C; (Д) сценарий Б с увеличена вероятност за общ отказ до pC = 0,040.

За сценарий Г се задават pR = 0,010, pS = 0,010 и pC = 0,005. Аналитичните вероятности се изчисляват по формула (2); за сценарий А отпада резервният път и L1 става единствено комуникационно условие. След това всеки сценарий се симулира чрез 3 000 000 независими Бернулиеви опита с фиксиран генератор NumPy (seed 20261031). В отделен опит се генерира състоянието на всеки базов елемент и се изчислява булевото T. Монте Карло оценката е отношението на броя откази към общия брой опити.

$$\hat{p}_T = \frac{1}{N}\sum_{i=1}^{N} 1(T_i), SE \approx \sqrt{\frac{\hat{p}_T(1-\hat{p}_T)}{N}} \quad (3)$$

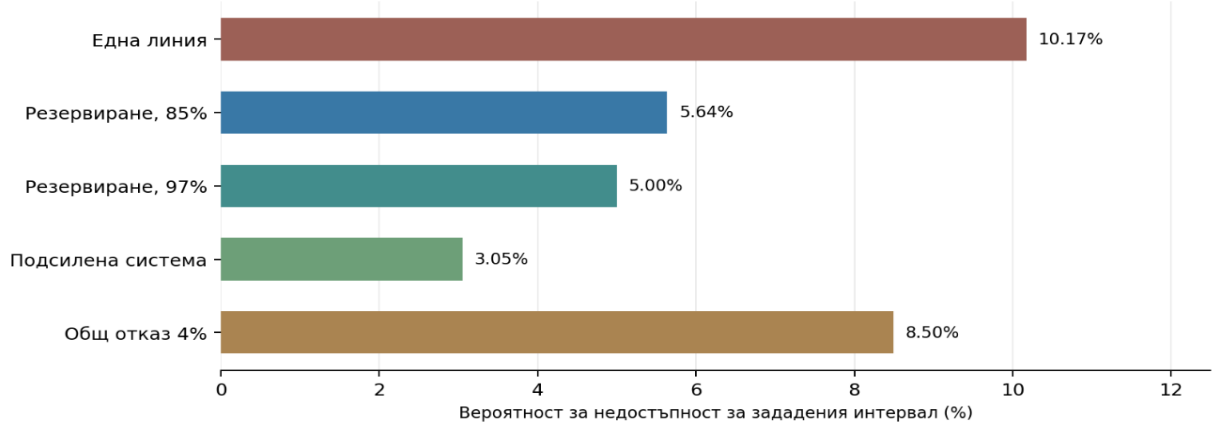
При представените N стойности приблизителният 95-процентен интервал е p̂T ± 1,96·SE. Това е интервал за случайното отклонение на симулацията при фиксирани входни параметри, а не интервал на доверие за действителната надеждност на реална мрежа. Изследванията върху Монте Карло оценяване на мрежова надеждност обосновават използването на симулационна проверка наред с аналитичните модели [6].

4 Резултати и анализ

Таблица 1. Сравнение на изчислените вероятности за недостъпност

Сценарий	Аналитично pT	Монте Карло p̂T	95% полуширина
А. Една линия	0,101692	0,101723	0,000342
Б. Резерва; 85% превключване	0,056365	0,056426	0,000261
В. Резерва; 97% превключване	0,049966	0,050036	0,000247
Г. Подсилена инфраструктура	0,030529	0,030611	0,000195
Д. Общ отказ pC = 0,04	0,084960	0,085013	0,000316

Резултатите в табл. 1 показват съвпадение на симулационните оценки с аналитичните вероятности в рамките на изчислените интервали. При добавяне на резервна линия (Б спрямо А) моделната вероятност за недостъпност намалява от 10,17% на 5,64%, т.е. приблизително с 44,6%. Увеличаването на надеждността на превключването от 85% на 97% (В спрямо Б) води до допълнително относително намаление с 11,4%. Резултатите за петте конфигурации са показани на фиг. 3.



Фиг. 3. Аналитична вероятност за недостъпност при пет конфигурации

Усилването на общите компоненти в сценарий Г намалява вероятността до 3,05%. Обратно, увеличаването на вероятността за общ отказ от 1% на 4% при непроменени комуникационни линии повишава pT от 5,64% до 8,50% (Д спрямо Б). Това показва, че само резервирането на линковете не е достатъчно, когато услугата зависи от едно захранване, маршрутизатор или сървър.

Логическата структура има и практическо значение: минималните сечения с един елемент {R}, {S}, {C} представляват единични точки на отказ. Сеченията {L1,L2} и {L1,F} показват кои комбинации остават критични дори при налична резервна линия. Следователно мерките могат да бъдат насочени към независими източници на захранване, резервирани маршрутизатори, отказоустойчиви сървъри и регулярно изпитване на превключването.

5 Дискусия и ограничения

FTA и ETA дават различни, но съгласувани гледни точки: FTA установява достатъчните комбинации от причини за недостъпност, а ETA описва разклоненията след конкретно начално събитие. Чрез свързването им може да се премине от качествено описание към проверими числови изводи. В подобни модели формалната проверка на вероятностните изрази и симулационното сравнение са утвърдени изследователски направления [7].

Резултатите имат ясно определени граници на приложимост: вероятностите са зададени условно; не се моделират продължителност на престоя, ремонти, времеви зависимости, претоварване и частична деградация. Общият отказ C е опростено представяне на зависимите причини; в реални мрежи може да има и корелации между линковете, поведенчески и конфигурационни грешки. Затова числата не трябва да се използват за прогнозиране на реална фирмена инфраструктура без калибриране с данни и допълнителна валидация.

При бъдещо развитие е целесъобразно да се използват измерени времена между откази и възстановяване, да се изследват зависимости в съвместно трасе и да се сравни моделът с изпитвания в мрежова виртуализация. Възможно е също допълване със състояния на деградация и времеви метрики за достъпност.

6 Заключение

Предложен е възпроизводим изчислителен подход за анализ на надеждността на мрежова услуга, който комбинира дърво на отказите, дърво на събитията, аналитично изчисляване на вероятности и Монте Карло симулация. При разгледаните хипотетични параметри резервната линия води до намаляване на вероятността за недостъпност, но ефектът ѝ е ограничен от надеждността на превключването и общите точки на отказ. Петте сценария позволяват да се различат ползата от резервиране и необходимостта от защита на общите компоненти. Моделът представлява основа за последваща оценка с действителни експлоатационни данни.

ЛИТЕРАТУРА:

[1] Arabadzhieva-Kalcheva, N., Tsankov, Ts. Failure Modes and Effects Analysis – FMEA. MATTEH 2022, Conference Proceedings, vol. 2 (2022), 58–62.

[2] Arabadzhieva-Kalcheva, N., Tsankov, Ts., Todorova, M. Cause-Consequence Analysis as a Risk Management Method. Annual of Konstantin Preslavsky University of Shumen, XIV E (2024), 184–188. DOI: 10.46687/YT24NEL.

[3] IEC 61025:2006. Fault Tree Analysis (FTA). International Electrotechnical Commission, Geneva (2006).

[4] IEC 62502:2010. Analysis Techniques for Dependability – Event Tree Analysis (ETA). International Electrotechnical Commission, Geneva (2010).

[5] IEC 31010:2019. Risk Management – Risk Assessment Techniques. International Electrotechnical Commission, Geneva (2019).

[6] Hui, K.-P., Bean, N., Kraetzl, M., Kroese, D. The Tree Cut and Merge Algorithm for Estimation of Network Reliability. Probability in the Engineering and Informational Sciences, 17(1) (2003), 23–45. DOI: 10.1017/S0269964803171021.

[7] Abdelghany, M., Ahmad, W., Tahar, S. Event Tree Reliability Analysis of Safety-Critical Systems Using Theorem Proving. IEEE Systems Journal, 16(2) (2022), 2899–2910. DOI: 10.1109/JSYST.2021.3077558.