**ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**
**Факултет Компютърни системи и технологии**
**Катедра „Информационни технологии в индустрията“**

**Маг. инж. Камелия Стоянова Райнова**

# ИЗСЛЕДВАНЕ НА МЕТОДИ И СРЕДСТВА ЗА ПОВИШАВАНЕ НА ОТКАЗОУСТОЙЧИВОСТТА НА КОМПЮТЪРНИ СИСТЕМИ

## А В Т О Р Е Ф Е Р А Т

на дисертация за придобиване на образователна и научна степен
**"ДОКТОР"**

Област: 5. Технически науки

Професионално направление: 5.3 Комуникационна и компютърна техника
Научна специалност: „Компютърни системи, комплекси и мрежи”

**Научен ръководител: доц. д-р Георги Попов**

СОФИЯ, 2018 г.

Дисертационният труд е обсъден и насочен за защита от Катедрения съвет на катедра „Информационни технологии в индустрията“ към Факултет Компютърни системи и технологии на ТУ-София на редовно заседание, проведено на 08.10.2018 г.

Публичната защита на дисертационния труд ще се състои на 05.02.2019 г. от 15.00 часа в Конферентната зала на БИЦ на Технически университет – София на открито заседание на научното жури, определено със заповед № ОЖ-5.3-04/18.10.2018 г. на Ректора на ТУ-София в състав:

1. Проф. д-р Милена Лазарова – председател
2. Доц. д-р Георги Попов – научен секретар
3. Проф. д.т.н. Павел Мартинов
4. Проф. д-р Стойчо Стойчев
5. Проф. д-р Веселин Павлов

Рецензенти:

1. Проф. д-р Милена Лазарова
2. Проф. д.т.н. Павел Мартинов

Материалите по защитата са на разположение на интересуващите се в канцеларията на Факултет Компютърни системи и технологии на ТУ-София, блок №1, кабинет № 1441.

Дисертантът е задочен докторант към катедра „Информационни технологии в индустрията“ на факултет Факултет Компютърни системи и технологии. Изследванията по дисертационната разработка са направени от автора.

Автор: маг. инж. Камелия Райнова
Заглавие: Изследване на методи и средства за повишаване ан отказоустойчивостта на компютърни системи
Тираж: 30 броя
Отпечатано в ИПК на Технически университет – София

# I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

## Актуалност на проблема

В съвременния компютърно зависим свят надеждността и достъпността се налагат като фактори от ключово значение. Основно изискване към системите е те да бъдат критични по безопасност (safety critical systems), което означава, че правилното функциониране на тези системи ще гарантира безопасността на човека. В днешно време ролята на компютрите и машините нараства все повече и обществото става все по-зависимо от техниката. Грешките и неизправната работа на редица компютърни приложения могат да доведат както до скъпи, така и понякога, до катастрофални последици. От по-простите примери, като например режещи инструменти до по-сложни проекти, като проектиране на мостове, асансьори и атомни централи, надеждността винаги е била фактор от изключително значение.

Съвременните компютърни системи стават все по-сложни, изградени от множество компоненти, което води до многократно повишаване на възможността за отказ. С течение на времето методите за предотвратяване на отказите и повишаване на надеждността на системите се развиха значително. В дисертацията са предложени нови методи, които допълват, а не заместват, съществуващите по-стари методи в анализа на надеждността.

Решаваните в дисертацията задачи са предмет на силен изследователски интерес с оглед необходимостта от осигуряване на много висока надеждност в съвременните компютърни системи. Усилията да се постигнат целевите изисквания за отказоустойчивост и да се осигури безпроблемна и непрекъсната работа на системите налага необходимостта от подходящи аналитични средства за определяне и оценяване на надеждност и факторите, които влияят върху показателите за надеждността, както и съответни подходи за идентификация на повреди и грешки.

За да се подобри отказоустойчивостта на системите в настоящата дисертация са разгледани средства като диверситета, като начин за идентификация на повреди и грешки. Изведени са математически зависимости за определяне на  количествена оценка на факторите, които влияят върху показателите за надеждността. Предложен е аналитичен подход за изследване на диверситетни системи на базата на метода stress-strength, при който се разглеждат обекти с недефинирани надеждностни параметри. Направени са симулационни изследвания, чрез които да се верифицират изведените формули.

## Цел на дисертационния труд, основни задачи и методи за изследване

Целта на дисертационната работа е да се усъвършенстват и детайлизират методите и средствата за постигане на отказоустойчивост на системите и да се намерят модели за количествена оценка на влияещите фактори върху

показателите за надеждност, която да се верифицира чрез симулационни средства.

За постигането на тази цел ще бъдат извършени следните задачи:

- Ще се изследва диверситетът като средство за индентификация на откази като ключов фактор за постигане на висока надеждност;
- Ще се направи модел на диверситетна система и на негова база да се изведат нови аналитични зависимисти за отказите, възникващи по обща причина. Получените формули да бъдат доказани чрез симулация;
- Ще се свърже класическата надеждност със подхода сила-здравина. Ще се изведат нови формули, които да бъдадт доказани чрез симулация;
- Ще се изведат и верифицират нови формули, даващи възможност за компаративен анализ между глобалното и парциално резервиране в редундантните системи.

**Научна новост**

В дисертацията се разглежда диверситетът като средство за откриване на откази и начин за повишаване на отказоустойчивостта на компютърни системи. Изведени са математически зависимости за определяне на количествена оценка на факторите, които влияят върху показателите за надеждността. Също така е предложен аналитичен подход за изследване на диверситетни системи на базата на метода stress-strength, при който се разглеждат обекти с недефинирани надеждностни параметри.

**Практическа приложимост**

В днешно време компютърната техника се развива главоломно и това налага високи изисквания за надеждност и отказоустойчивост на системите. Получените аналитични формули в дисертационния труд въвеждат нови надеждностни показатели, които могат да се използват като допълнение за определяне на параметрите на компютърните системи, с цел повишаване на отказоустойчовостта им.

**Апробация**

Резултатите от дисертационното изследване са базирани на изведени аналитични зависимости за надеждностните показатели на компютърни системи. Същите зависимости са изследвани с програми за симулация и анализ на надеждностни показатели – симулационна среда BlockSim на ReliaSoft и програма за симулации Relex на Windchill Quality Solutions.

**Публикации**

Основни постижения и резултати от дисертационния труд са публикувани в 4 научни статии, от които 2 са публикувани в научни списания, едното международно, а другите 2 статии са докладвани на международни научни конференции у нас и са публикувани в съответните сборници с трудове. Една от статиите е самостоятелна, а останалите в съавторство с научния ръководител.

**Структура и обем на дисертационния труд**

Дисертационният труд е в обем от **150** страници, като включва увод, **4** глави за решаване на формулираните основни задачи, списък на основните приноси, списък на публикациите по дисертацията и използвана литература. Цитирани са общо **108** литературни източници, като **99** са на латиница и **5** на кирилица, а останалите **4** са интернет адреси. Работата включва общо **68** фигури, **5** таблици и **90** формули. Номерата на фигурите и таблиците в автореферата съответстват на тези в дисертационния труд.

## II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

## ГЛАВА 1. ОБЗОР ПО ПРОБЛЕМА

В глава 1 на дисертационния труд е направен литературен обзор на проблема на надеждността. Разгледани са основните понятия, свързани с надеждността на системите от самото начало на възникване на класическата надеждност до наши дни. Описани са свойствата и показателите на системите, като са разгледани поотделно параметрите за възстановими и невъзстановими компютърни системи. Описани са методите за предотвратяване на грешки, за отстраняване на повреди, както и за прогнозиране за появата на възможни неизправности в системите. Специално внимание е отделено на съществуващите методи за повишаване на отказоустойчовостта на системите, както програмна, така и апаратна. Разгледани са съществуващите класификации на заплахите в компютърните системи и е предложен нов поглед върху системите, от гледна точна на диверситета.

На базата на направения обзор на съществуващата специализирана литература могат да бъдат направени следните изводи:

- Не е изследван достатъчно задълбочено системния диверситет като фактор за откриване/детекция на откази, както и за повишаване на отказоустойчивостта и сигурността на системите. В множество от разгледаните в обзора трудове са дадени математически зависимости, но не са изведени аналитични формули, които да показват количествено-качествена взаимовръзка между отделните надеждностни параметри на системите.

- В специализираната литература не са разгледани подробно системите с излишък, т.нар. редундантни системи и не е направен анализ на начините за резервиране при тях.

- Не е изследван познатият метод „сила-якост“ (stress-strength) от гледна точна на безопасност и надеждност на системите и не са изведени надеждностни зависимости на базата на този метод, както и не е разгледана тяхната евентуална връзка с класическата надеждност.

## ГЛАВА 2. Диверситет, излишък и отказоустойчивост

В глава 2 от дисертационния труд се разглежда диверситетът. Добавянето на излишък, както и използването на диверситет (разнообразие) намират широко приложение при защита от грешки и откази в компютърните системи. Ако се разгледа простият случай на паралелна система с излишък, терминът "излишък" обикновено означава копиране на един компонент в идентични копия, като предпазване от "произволни" хардуерни повреди. За първи път терминът "диверситет" се използва специално за "софтуер с множествена версия" [16] [32], в който са добавени N версии на софтуера, с цел да е отказоустойчив. Диверситетът е метод за решаване на определена задача (математическа, логическа, техническа или др.) по два различни начина, при еднакви входни данни. Смята се, че съществуват минимум две различни решения, но с един и същи верен резултат, който може да се получи при отсъствие на грешки в решенията. Критерий за вярност на резултата е идентичността на получените данни при двете решения. Необходимостта от различие на двете решения произтича от разбирането, че когато информацията се обработва по различен начин, е вероятно по другия начин да няма грешки или ако има, те да не са същите и така да се стигне до различен резултат.

Диверситетът в програмното осигуряване най-често се постига чрез различие и независимост на програмните екипи, които решават различни версии на една и съща задача. Различието се проявява в представянето на данните, в кода на програмата, в алгоритмите, в документацията и тн. Диверситетът в апаратните средства се постига като за двете решения на една и съща задача се използват различни хардуерни компоненти. Това могат да бъдат устройства с еднакво предназначение от различни производители или модули, които работят на различен принцип.

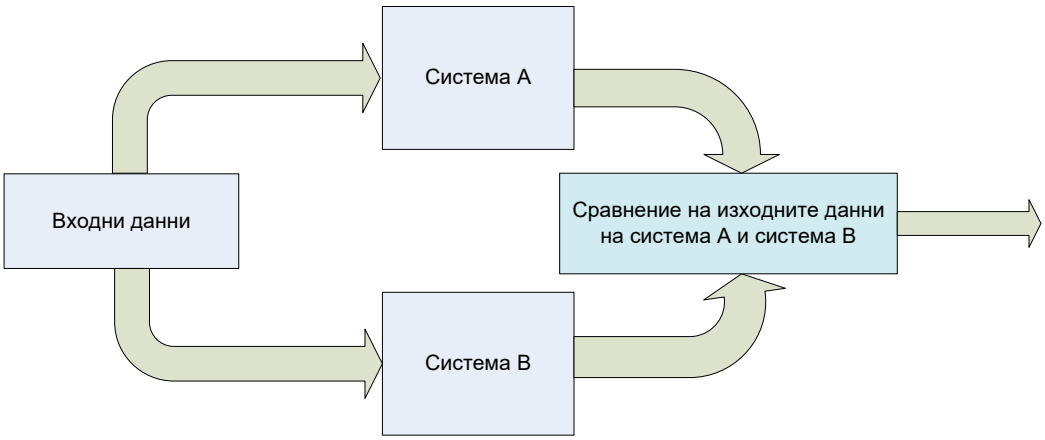
Диверситетът е ефективно средство за откриване на грешки, защото чрез него грешките се поставят в положението на независимост, в което са неизправностите. Ако две събития А и Б са независими, то условната вероятност за всяко от тях при условие, че е настъпило другото, е равна на безусловната му вероятност – вероятността да настъпи събитие А не зависи от това, дали е настъпило или не събитието Б, т.е получава се следното равенство Р(АБ)=Р(А).Р(Б)

Диверситетът може да се разглежда и като средство за постигане на независимост – например колкото повече са независими програмистите на двете версии, толкова по-вероятно е да не допуснат неоткриваеми грешки. Чрез диверситета могат да се постигнат две основни цели:

- Да се откриват грешки и неизправности. Освен това при откриването на проблем може да се предизвика преход в неработещо състояние до отстраняването на грешката,т.е диверситетът може да се разглежда като fail-safe средство.

- Да се маскират грешки и неизправности, като едната програма или устройство резервира другата, като по този начин не се прекъсва работата на цялата система. Едната от версиите може да се натъкне на грешка, а другата при същите входни данни да работи и чрез диверситета да се повиши надеждността на системата, т.е диверситетът може да бъде fault-tolerance средство. [105]

В техниката, диверситетът (фиг.1.) е метод за решаване на поставена задача по два или повече различни начина при еднакви входни данни, съгласно, които критерий за перфектност на решението е съответствието на получените изходни резултати [46] [47] [48]. Презумпцията е, че съществуват поне два възможни начина на решение.




Фиг. 1 - Структура на двуканална диверситетна система

Различието в сравняваните изходни резултати е признак за грешка или отказ. В [48] са дадени изчисления, които показват, че вероятността за отказ поради грешка може да бъде редуцирана десетки милиони пъти.

Техниката на прилагане на диверситетния излишък е същата като при хомогенните системи. В зависимост от нивото на резервиране (глобално, парциално или поелементно резервиране) системата се декомпозира на независими по отношение на възникване на отказите паралелно работещи канали (модули, системи и т.н). Показаната фиг.1. е свързана с идентификация на отказа. Системната надеждност може да се определи по формулата:

$$P_{sys}(t)=P_A(t)+Q_A(t)P_B(t) \qquad (1)$$

където $P_{SYS}$, $P_A$, $P_B$ е надеждността на системата и отделните канали, респ $Q_A$ – вероятността за отказ на канал А.

Неизправността е състояние, при което не се изпълняват някои (макар и едно) от изискванията на нормативно-техническата документация

(включително спецификацията) на изделието (продукта). Спецификацията се приема за вярна. След тестване, преди пускане на изделието в експлоатация се счита, че са отстранени всички неизправности и в момент t=0 се пуска за работа напълно изправна система. По време на експлоатацията настъпва събитието повреда, която привежда обекта в състояние на неизправност и тя може да остане скрита, докато се създадат условията за изявата й като функционален отказ. Отказът води до отклонение от зададения алгоритъм на функциониране или неправилен (нефункционален) изходен сигнал. Отказите се появяват с интензивност $\lambda_{fr} = \lambda_f + \lambda_e$, където $\lambda_f$ е интензивност на отказите, породени от повреди, а $\lambda_e$ - от грешки.

Повредите са независими, макар и в еднакви, хомогенни единици. Пространството на независимостта, в което е валидна формула (1), е различно. При хомогенните единици пространството на независимостта генерира откази с интензивност $\lambda_f$. Ако двете единици са еднакви, те имат само общи (еднакви) откази (common case), произтичащи от еднаквите грешки. Отказът в първата единица А ще предизвика превключване към втората В, в която същата грешка ще доведе незабавно до провал на системата.

При диверситетните системи пространството на независимостта е по-голямо. В него се включват и отказите, дължащи се на грешки, защото грешките при диверситета са независими така, както повредите в хомогенните единици. В случай, че отказите настъпват поради смущаващи фактори (S), които влияят по различен начин на двата канала, формула (1) придобива вида (2), като вероятностите се заменят с условни.

$$P = P(A|S) + P(B|S)Q(A|S) \qquad (2)$$

Диверситетът е мощно средство за увеличаване на сигурността на системите [53]. Например ако за надеждно съхранение на важна информация се използват N сървъра. Когато сървърите са идентични, те представляват лесна за хакерите цел, тъй като е достатъчно да бъде преодоляна защитата на един от тях. От друга страна, защитите на сървърите се изграждат на няколко нива и ако при защитата на N-те сървъра има пълен диверситет, т.е всички нива са различни и са M на брой, надеждността се увеличава значително. Пример за това как разходите за получаване на диверситетна информационна защита нарастват линейно, а усилията за предоляването им – квадратично е даден в [49]. Там е представена аналитичната зависимост между дълбочината на диверситета и нейния ефект върху сигурността на системата:

$$\text{P(A\_and\_B\_both\_fail\_to Detect\_X)} = \sum_{x\in D} P(x)\theta_A(x), \theta_B(x) = Q_A Q_B + cov\, x(\theta_A(x), \theta_{\boldsymbol{B}}(x)), \qquad (3),$$

където D е множеството на възможните атаки x, а cov x дава ковариацията на двете функции .

Нека са дадени две независими диверситетни системи (A и B), работещи за идентификация на дадено събитие, както на фиг.1. Ако може да се определи изходната функция, която да дава изходен резултат на базата на данните постъпващи от двата канала, то диверситетът от сферата на надеждността би могъл да се прехвърли към идентификацията, напр. на образи. За реализация на тази функция би могло да бъдат използвани невронни мрежи, размита логика или други методи.

Използване на резервиране за подобряване на надеждността на системата се основава на предположението, че ако една версия на дадено приложение е неуспешна, то останалите версии вероятно ще работят правилно, правейки системата устойчива на повреди. За да бъде ефективно, добавянето на излишък изисква различните версии да се провалят независимо (т.е., да няма припокриващи се модели на отказ) [35]. Идеята е, че различните версии се разработват от различни екипи, независимо една от друга, като се използват различни подходи.

Когато се прилагат само за процесите на разработка на софтуер, подходите, основани на разнообразието, са до голяма степен ограничени до влиянието върху разнообразието на приложеното приложение, въпреки че разнообразието на дизайна може да предизвика различен вид данни в заобикалящите недисперсни подсистеми, ниско ниво на взаимодействие с тези подсистеми. Ако обаче поддържащите елементи на дадена система, като например хардуер, операционни системи и многослойни подсистеми, съдържат грешки или неизправности, надеждността на системата може да бъде понижена, без значение колко надежден е самият софтуер на приложението.

Концептуално погледнато най-простата техника за откриване на грешки и постигане на отказоустойчивост е дублирането, когато се използват две идентични копия. При възникване на повреда, двете копия вече не са идентични и лесното сравнение води до установяване на грешката. В този подход опростеността, ниската цена и ниския фактор на производителност на сравняващата логика са от голямо предимство. Дублирането е приложимо за всички области и нива на компютърния дизайн и затова се използва широко. Добавянето на излишък успешно открива всички единични неизправности, с изключение на отказ в сравняващата логика.

В научната литература има сведения и резултати от изследвания на влиянието на диверситета върху идентификацията на отказите в отказоустойчивите компютърни системи [1], както и количествени оценки за зависимостта между показателите за надеждност и степента на независимост на диверситета $\Omega$ (0 – 1) между диверситетните структурни единици, от

които са изградени. Установено е, например, че вероятността за безотказна работа P(t) (респ. готовността на системата A(t)) на такива системи, не е линейна функция от Ω, а е особено чувствителна в края на интервала, т.е. при високите стойности на независимостта. Това означава, че решаващо значение за идентификацията на отказите и отказоустойчивостта имат общите за структурата откази (CCF – common case failures)[93].

В повечето случаи на изследване на този проблем се предполага, че са известни първичните данни за надеждността на структурните единици – интензивностите на отказите λ и възстановяванията μ. Това се отнася както за общите части на системата (входно-изходна организация, компаратори, захранващи устройства и др., т.е. CCF), така и в независимите функционално паралелни диверситетни единици.

Направени са изследвания, които доказват, че stress-strength моделът може да се използва като начин за изчисляване на надеждността[108]. Този модел е подходящ в ситуации, където надеждността на компонент или система се дефинира от вероятността случайна променлива X (представляваща якост) да е по-голяма от друга случайна променлива У (представляваща стрес). По презумция даден компонент ще откаже ако неговата якост е по-малка от приложения върху него стрес. Този модел може да се приложи в различни ситуации, където случайната променлива X представлява характеристика, свързана с изпълнението на въпросната система, а Y служи като критерий, който определя нейния провал. Всеки компонент или състояние, за които X има стойност по-малка от стойността на Y, се отнася за ситуация, при която има отказ. След като се определят разпределенията и параметрите на X и Y, надеждността може да бъде получена чрез оценка на вероятността X>Y, която се изчислява, както е показано на формулата:

$$R = \int_{-\infty}^{\infty} \int_{Y}^{\infty} f(y) f(x) dx dy \qquad (4)$$

където f(y) е плътността на разпределение на стреса, а f(x) е плътност на разпределение на якостта.

По-често се предполага че метода stress-strength се отнася за статичен надеждностен модел. При него стресът и якостта са представени от произволни променливи, описващи състоянието на компонента в един единствен момент във времето. От уравнението (4) става ясно, че в изчисляването на тази форма на надеждност не съществува компонента "време" и следователно този модел се използва само при условия, при които функцията за разпределение на вероятностите на стреса и якостта не се променя по отношение на времето. Този модел е полезен също, ако се изчислява функцията за вероятностна плътност за единичен момент във времето (чрез тестване или аналитични данни) и надеждността на компонента трябва да бъде изчислена в същия този момент. Начинът, по който вероятността за разпределение (променливите f (Y) и f (X)) се променя

по отношение на времето, може да се използва, за да се разработи динамичен модел за оценяване на надеждността чрез stress-strength.

Но какво трябва да се направи, когато първичните данни за надеждността не са известни, напр. ако се изследват нови системи, за които все още няма получена стандартна статистика за стойностите на показателите λ и μ [71]. Единият от вариантите в случая е да се съчетае stress-strength метода (SSM) с класическата надеждност. По този начин могат да бъдат установени липсващите първични параметри на надеждността, като се допусне, че са известни основните надеждностни стойности за вероятност на отказите, вероятност за безопасна работа и интензитет на отказите.

Един основен недостатък на stress-strength анализа, е че той е разработен като математически апарат за влиянието на един стрес върху даден елемент или система, имащи типично приложение в съпромата (респ. механиката). На практика системите представляват сложни комплекси и на тях въздействат различни стресове. Би могло да се изследват уязвимостите на системите и тяхната сила (здравина, якост) спрямо различните стресове. За целта трябва да се извърши многомерен stress-strength анализ, като по този начин могат да бъдат определени слаби страни на системите. Подобно изследване би могло да бъде извършено на два етапа:

- изследване на единичното влияние на всеки един от възможните стресове за дадена система, т.е. като се приема, че върху системата въздейства само един стрес в даден момент;
- изследване при наслагването на няколко независими стреса (суперпозиция) върху системата, където фунциите за Stress и Strength са n мерни вектори.

Допуска се, че за дадена система S, съществуват n на брой линейно независими по своя характер стресове Z:

$$\{Z = \{(z_1, z_2, \dots z_n) | z_i \ni R\} \quad (5)$$

На всеки стрес от (2.18) се съпоставя неговата функция на разпределение:

$$\{S\,(Z) = (s(z_1), s(z_2) \dots\dots s(z_n)\} \quad (6)$$

Аналогично, системата S има здравина R, специфицирана в пространството на X:

$$\{R = \{(r_1, r_2, \dots r_n) | n_i \ni R\} \quad (7)$$

Отразявайки влиянието на отделните стресове Z и здравината на изследваната системата R, може да се запише:

$$\{R\,(Z) = (r(z_1), r(z_2) \dots\dots r(z_n)) \quad (8)$$

Вероятността за отказ на i-тия компонент се описва в интегрален вид и ако се отчетат всички стресове и здравини за цялата система се получава:

$$Q = \sum_{i=1}^{n} Q_i = \sum_{i=1}^{n} \int_0^{\infty} s_i(x) r_i(x) dx \qquad (9)$$

Дадена е система $S_\Sigma$, която е съставена от два независими диверситетни канала A и B и съответните стресове за тях $S_{\Sigma A}$ и $S_{\Sigma B}$, имащи съответно димeнсиите $n_a$ и $n_B$ (фиг.1.).

Стресовете, на които е подложена диверситетната система $S_{\Sigma AB}$ се представят в линейното независимо пространство с димeнсия $n = n_A \cup n_B$, което представлява обединението на линейните пространства на стресовете на двата канала A и B.

Липсващите линейни независими координати се запълват със стойности 0 или 1, както следва:

- за стреса, ако за даден линеен независим признак i на даден канал не съществува $x_i$, то $x_i$ =0, т.е. въвежда се стрес с интензивност 0;
- за системата (респ. каналите) – ако за дадено линейно независимо измерение на стреса $x_i$ няма устойчивост $r_i$, то $r_i$=1, т.е. системата е напълно уязвима по този признак.

Нека всички стресове на диверситетната система се представят чрез формула (8), а силата на каналите A и B се описва с вектора от функции:

$$\{R_A(Z) = r_A(z_1), r_A(z_2) \dots r_A(z_n)\} \qquad (10)$$

$$\{R_B(Z) = r_B(z_1), r_B(z_2) \dots r_B(z_n)\} \qquad (11)$$

Надеждностните показатели на диверситетна система са изследвани в [77].

За двуканална система $S_{\Sigma AB}$ с два независими канала A и B, вероятността за безотказна работа има следната логическа функция на работоспособността:

$$z_{div} = z_a^0 z_b^0 + z_a^0 z_b^1 + z_a^1 z_b^0 = z_a^0 (z_b^0 + z_b^1) + z_a^1 z_b^0 \qquad (12)$$

$$z_{div} = z_a^0 + z_a^1 z_b^0 \qquad (13)$$

След логико-вероятностен преход [99] за вероятността за безотказна работа се получава:

$$p_{div} = p_a + (1 - p_a) p_b \qquad (14)$$

$$p_{div} = p_a + p_b - p_a p_b \tag{15}$$

След преобразуване за вероятността за отказ $q_{div}$ се получава следния израз:

$$q_{div} = 1 - p_{div} = 1 - (p_a + p_b - p_a p_b) = q_a q_b \tag{16}$$

Вероятността за отказ на канал А е:

$$Q_a = \int_0^\infty s(x) r_a(x) dx \tag{17}$$

Респективно за вероятността за отказ на канал В се получава:

$$Q_b = \int_0^\infty s(x) r_b(x) dx \tag{18}$$

За вероятността за отказ на диверситетната система се получава израза:

$$Q_{div} = Q_a Q_b = \int_0^\infty s(x) r_a(x) dx . \int_0^\infty s(x) r_b(x) dx \tag{19}$$

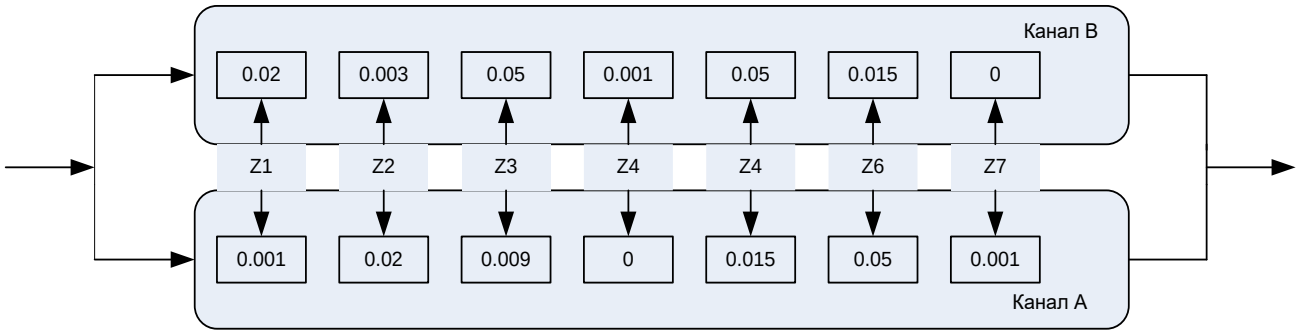
Функциите $Q_a$ и $Q_b$ показват вероятността за отказ на отделните канали А и В. Функцията $Q_{div}$ дава вероятността за отказ на двуканалната система, състояща се от два различни канала А и В. Функциите $Q_{AA}$ и $Q_{BB}$ показват вероятността за отказ на двуканална система с два еднакви канала А и В.

Ако (19) се замести в израз (9) се получава зависимост за вероятността за отказ на диверситетна система срещу n- мерен стрес:

$$Q_{div} = \sum_{i=1}^{n} Q_{div_i} = \sum_{i=1}^{n} \int_0^\infty s(x) r_a(x) dx . \int_0^\infty s(x) r_b(x) dx \tag{20}$$

От гледна точка на SSM една система може да се представя с последователна схема на надеждността, т.е. всеки един от стресовете може да доведе системата до отказ с определена вероятност [105].

Нека разгледаме модел на двуканална диверситетна система, която е подложена на седем стреса, (Z1÷Z7), като вероятността всеки от стресовете да се прояви за време t=10 000 часа, за всеки от двата канала А и В, са дадени на фиг. 2 и Таблица 1.




Фиг. 2 - Надеждностна схема на двуканална диверситетна система

| Канал / Стрес | Канал A | Канал B | Диверситетна система Канал A & Канал B |
|---|---|---|---|
| **Z1** | 0.02 | 0.001 | 0.00002 |
| **Z2** | 0.003 | 0.02 | 0.00006 |
| **Z3** | 0.05 | 0.009 | 0.00045 |
| **Z4** | 0.001 | 0 | 0 |
| **Z5** | 0.05 | 0.015 | 0.00075 |
| **Z6** | 0.015 | 0.05 | 0.00075 |
| **Z7** | 0 | 0.001 | 0 |

Табл. 1 Аналитични данни за двуканалната диверситетна система

Приема се, че плътността на разпределение на отказите (pdf) има експоненциално разпределение, характерно за техниката и електрониката.

$$f(t) = \lambda . e^{-\lambda t} \tag{21}$$

Тогава:

$$q = \int_0^t f(t)dt = \int_0^t \lambda . e^{-\lambda t} dt \tag{22}$$

При стойност за интензивността на отказите λ=const:

$$q = 1 - e^{-\lambda t} \approx 1 - (1 - \lambda t) \approx \lambda t \tag{23}$$

Вероятността за отказ на двуканалната диверситетна система, показана на фиг.2. е:

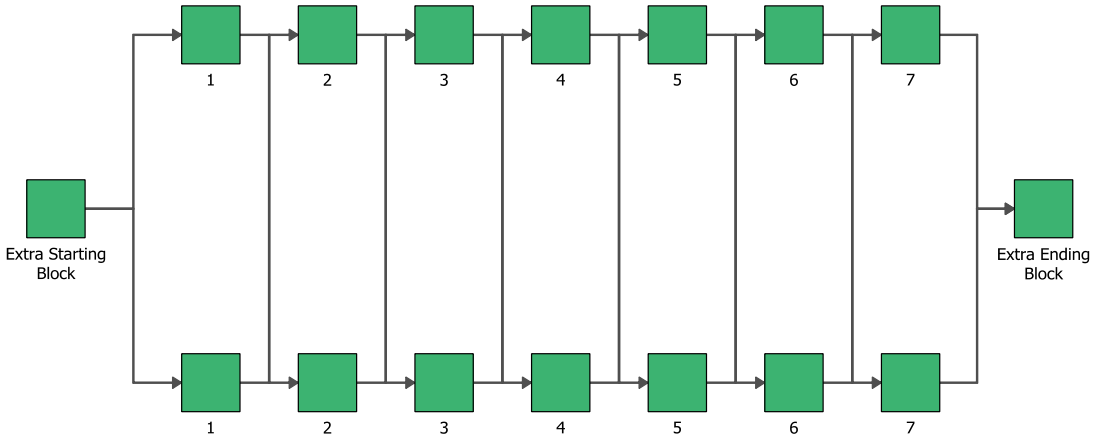
$$Q_{div} = Q_A Q_B \tag{24}$$

След заместване за диверситетната система се получава:

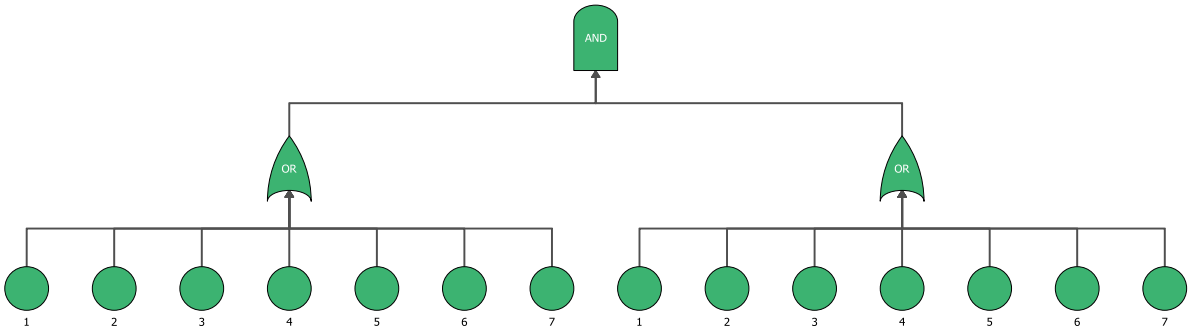
$$Q_{div} = (1 - \prod_{i=1}^{7}(1 - q_{i_A})).(1 - \prod_{i=1}^{7}(1 - q_{i_B})) \tag{25}$$

Направени са изследванията на диверситетната система от фиг.2., чрез симулационната програма BlockSim на ReliaSoft. Зададени са стойности на всеки от стресовете, съответно за двата канала A и B, за вероятността за отказ на всеки канал, по въздействието на съответния стрес $Z_i$. Проведено е изследване за време 10 000ч., като отказите в двата канала са възникващи по обща причина и системите са невъзстановими.

Следващите фигури илюстрират съответните на системата блокова схема на надеждността (фиг.3) и аналитично дърво на отказите (фиг.4).




Фиг.3- Блокова схема на надеждността на двуканална диверситетна система, изложена на 7 стреса




Фиг. 4 - Аналитично дърво на отказите на двуканална диверситетна система, изложена на 7 стреса

С програмата BlockSim са изследвани седемте стреса и тяхното влияние върху диверситетната система. В таблица 2 са дадени резултатите от симулацията.

| Канал / Стрес | Канал А | Канал В | Диверситетна система Канал А & Канал В |
|---|---|---|---|
| **Z1** | 0.02 | 0.001 | 0.00002 |
| **Z2** | 0.003 | 0.02 | 0.00006 |
| **Z3** | 0.05 | 0.009 | 0.00045 |
| **Z4** | 0.001 | 0 | 0 |
| **Z5** | 0.05 | 0.015 | 0.00075 |
| **Z6** | 0.015 | 0.05 | 0.00075 |
| **Z7** | 0 | 0.001 | 0 |

Табл. 2. Симулационни данни, получени при изследването на влиянието на седемте стреса върху двуканалната система

От сравнението на данните от двете таблици е видно, че данните – аналитични и симулационни – съвпадат напълно! Като извод от направените изследвания и симулации може да се отбележи, че е разгледан диверситетът като средство за индентификация на откази. Реализиран бе модел на двуканална диверситетна система и на негова база се получиха нови аналитични зависимисти за отказите, възникващи по обща причина. Получените формули се потвърдиха от направените симулации чрез програма BlockSim на надеждностния пакет ReliaSoft, който е водещ софтуерен продукт за изследване и надеждностна диагностика на системи. Беше доказано, че диверситетът може да се прилага като фактор за постигане на по-високи стойности на надеждността на системите.

## ГЛАВА 3. Изследване на хомогенни структури

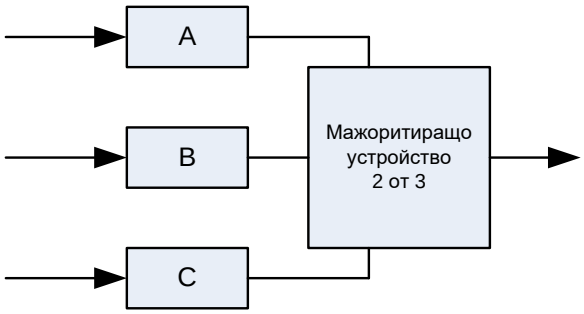
Определението за хомогенна или хетерогенна система до голяма степен зависи от мястото на приложение на системата. За хомогенни се считат системите, които имат еднаква вътрешна структура и работят по един и същи начин, под въздействието на еднакви външни фактори [106]. Когато

системите са изградени от еднакви модули с излишък е възможно постигането на по-висока надеждност.

Един от възможните методи за повишаване на надеждността на системите е прогнозирането на грешките (fault forecasting) [33], т.е предвиждането на отказите в системите и възможните последици от тях.

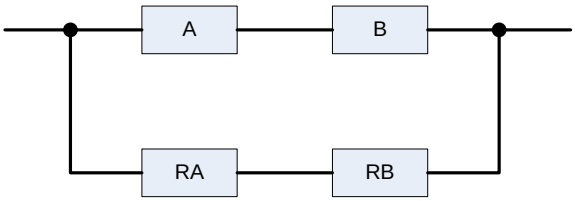
Използват се отказоустойчиви системи с различни форми на добавяне на излишък. В контекста на тази задача е важно да се установи как зависи надеждността от формата на излишък. Интересно е да се предвиди доколко той е ефективен, т.е дали действително ще доведе до повишаване на надеждността. В тази глава на дисертацията се разглежда надеждностния анализ и съпоставката на три от най-често срещаните отказоустойчиви системи. Тези системни структури са:

- **Мажоритарната структура „2 от 3” (фиг.5);**



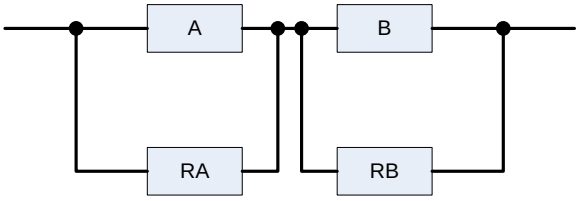

Фиг. 5 - Стандартна блокова схема на TMR структура

- **Система „2 от 2” с глобално резервиране чрез заместване (фиг.6)**




Фиг. 6 - Блокова схема на структура "2от2" с глобално резервиране

- **Система „2 от 2” с парциално резервиране чрез заместване (фиг.7)**




Фиг. 7 - Блокова схема на структура "2от2" с парциално резервиране

Разглеждат се възстановими компютърни системи, като показателите, по които се извършват наблюдение за надеждността са коефициент на готовност A(t) и средно време между отказите MTBF.

Изследването е проведено с предположението, че потокът от откази и възстановявания е пуасоновски, което предполага, че интензивностите на отказите $\boldsymbol{\lambda}$ и на възстановяванията $\boldsymbol{\mu}$ са постоянни величини. Такъв е преобладаващия случай в електрониката, компютърната, комуникационната и осигурителната техника.

Показателите на TMR структурата са изследвани в [66]. Получени са формули за коефициента на готовността и средното време между отказите.

Готовността $K_{г(2v3)}$ на TMR структурата се определя по формулата:

$$К_{г(2v3)} = К_г^3 + 3К_г^2(1 - К_г) = К_г^2(3 - 2К_г) \qquad (26),$$

където готовността $K_г$ на отделната структурна единица, участваща в 2 от 3 структурата е:

$$К_г = \frac{\mu}{\mu + \lambda} \qquad (27)$$

Средното време между отказите $MTBF_{2v3}$ е намерено като:

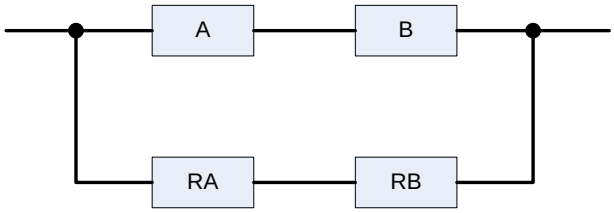
$$MTBF_{2v3} = \frac{1}{6К_г^2(1 - К_г)\lambda} = \frac{MTBF}{6К_г(1 - К_г)} \qquad (28),$$

където $MTBF$ е средното време между отказите на отделната структурна единица:

$$MTBF = \frac{1}{Н} = \frac{1}{К_г\lambda} \qquad (29)$$

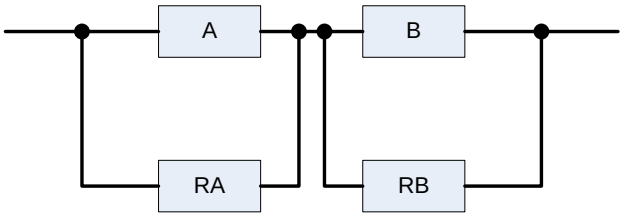
## ГЛАВА 4. Симулационно изследване на хомогенни и диверситетни системи

Разгледани са системи от тип „2 от 2” с глобално резервиране и „2 от 2” с парциално резервиране. Блоковите им схеми са показани на фиг.6. и фиг.7.




Фиг. 6 - Блокова схема на структура "2от2" с глобално резервиране

При системата „2 от 2” с глобално резервиране (фиг.6.) се състои от основен модул, състоящ се от блокове A и B и резервен модул, съответно изграден от модули RA и RB. При отказ на блок от основния модул, се извършва подмяна със съответната резервирана структура.




Фиг. 7 - Блокова схема на структура "2от2" с парциално резервиране

Системата „2 от 2” с парциално резервиране (фиг.7.) е случай, когато вместо целия модул, в който е открит отказ, се подменя само отказалия блок. Това предполага, че диагностиката обхваща контрола на всички компоненти и позволява всеки от тях да бъде заместен с горещ резерв на конкретния отказал елемент. И тук е разгледана двуелементна структура. В тези схемни структури не се разглежда проблема с диагностиката и средствата за откриване на отказа, който е самостоятелен проблем. Приема се, че заместването става автоматично във времето на допустимата за случая информационна неопределеност, без да се прекъсва работата. Също така не се разглежда надеждността на превключващото устройство.

За изследването на двете резервирани системи са използвани програми за симулация и анализ на надеждностни показатели за системите – симулационна среда BlockSim на ReliaSoft и програма за симулации Relex на Windchill Quality Solutions.

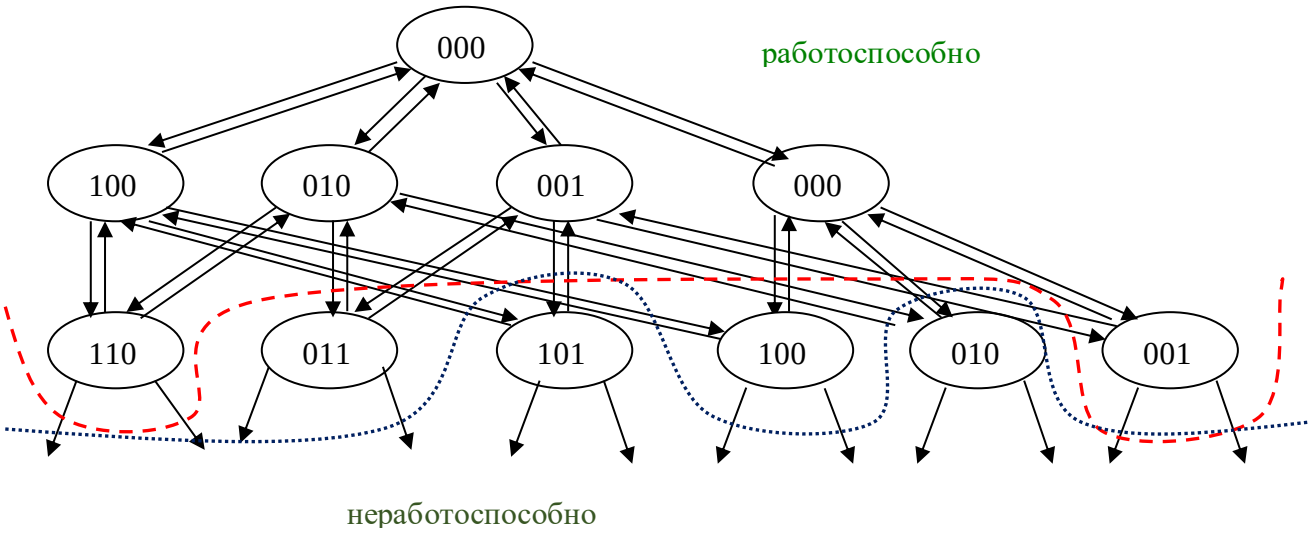
## 4.1. Изследване на система „2 от 2” с глобално резервиране чрез заместване

### 4.1.1. Граф на състоянията

Системната структура на фиг.6. има граф на състоянията, показан на фиг.8. Графът има върхове, които са парциални надеждностни състояния на системата, формирани от двоични вектори с толкова разряда, колкото са елементите в структурата (в случая 4). Състояние „0” е изправно, а „1” – неработоспособно. Върхът 0000 означава, че в това състояние всички елементи (1, 2, 3 и 4) са работоспособни. На следващия ред в графа са състоянията, в които има по един отказал елемент – първият, вторият, третият и четвъртият. Дъгите на графа, свързващи неговите върхове (състоянията), са интензивностите на съответния преход. За да не се претоварва чертежа, те не са означени на фигурата, но следва да се разбират като интензивност на отказ на съответния елемент $\boldsymbol{\lambda}$ (стрелки надолу) и интензивност на възстановяването му (стрелки нагоре) $\boldsymbol{\mu}$.

Очевидно е, че единичният отказ се толерира от работещата система, поради което всички парциални състояния 1000, 0100, 0010 и 0001 са работоспособни. Но освен тях, работоспособни са и две парциални състояния с по два отказа: 1100 и 0011. В тези случаи отказалата система се заменя с резервната, и обратно.

На фиг.8. границата между работоспособност и неработоспособност на система „2 от 2” с глобално резервиране е прокарана с пунктирана червена линия, която добавя тези две състояния към работоспособните. Останалите 4 парциални състояния не са резервирани и остават под чертата. Така, граничните състояния, от които се прави преход към неработоспособност, стават 6.




Фиг. 8 - Граф на състоянията

### 4.1.2. Готовност на система „2 от 2” с глобално резервиране

Парциалните състояния са несъвместими, което значи, че не могат да съществуват едновременно. Следователно в Булев контекст те са ортогонални и тогава вероятността за работоспособно състояние на системата е проста сума от вероятностите за всяко от състоянията. Логическите нули в парциалния вектор означават вероятност за работа (коефициент на готовност $K_г$), а логическата единица „1” – вероятност да не работи (коефициент на неготовност $K_n = 1 - K_г$). Следователно, за готовността $К_{г(2v2)gr}$ на цялата система с глобално резервиране (global reservation) може да се напише:

$$К_{г(2v2)gr} = К_{г_1г_2г_3г_4} + К_{n_1г_2г_3г_4} + К_{г_1n_2г_3г_4} + К_{г_1г_2n_3г_4} + \\ + К_{г_1г_2г_3n_4} + К_{n_1n_2г_3г_4} + К_{г_1г_2n_3n_4} \tag{30}$$

Ако всички елементи имат еднаква готовност:

$$К_{г(2v2)gr} = К_г^4 + 4К_г^3(1 - К_г) + 2К_г^2(1 - К_г)^2 = \\ = К_г^2[К_г^2 + 4К_г(1 - К_г) + 2К_г^2(1 - К_г)^2] = К_г^2[К_г^2 + 2(1 - К_г^2)] \tag{31}$$

### 4.1.3. Средно време до отказ на система „2 от 2” с общо резервиране

Търсеното средно време $MTBF_{(2v2)gr}$ е реципрочно на честотата $Н_{(2v2)gr,}$ с която системата отказва:

$$MTBF_{(2v2)gr} = \frac{1}{H_{(2v2)gr}} \tag{32}$$

От своя страна общата честота $Н_{(2v2)gr}$ на нейните откази е сумата от парциалните честоти $H_i$ на прехода ѝ в неработоспособност поради отказ на елемент от граничните върхове на графа:

$$H_{(2v2)gr} = \sum H_i \tag{33}$$

По общовалидно правило честотата е произведение от вероятността за състоянието (при единичен елемент - неговата готовност $K_г$), от което излиза за да направи преход с интензивност $\lambda$ към неработоспособно състояние:

$$H_i = К_г\lambda \tag{34}$$

От графа на фиг.8. се вижда, че шестте гранични парциални състояния, от които се прави преход към неработоспособност, попадат в две групи:

- 4 върха с по един отказал елемент, като от всеки връх излизат две дъги за преход към неработоспособност, всяка с интензивност $\lambda$.
- 2-та върха с по два отказали елемента, като от всеки връх излизат две дъги за преход към неработоспособност, всяка с интензивност $\lambda$.

При различни по надеждност елементи на изследваната система за общата честота $H_{(2v2)gr}$ може да се напише:

$$H_{(2v2)gr} = К_{n_1г_2г_3г_4}(\lambda_3+\lambda_4) + К_{г_1n_2г_3г_4}(\lambda_3+\lambda_4) + К_{г_1г_2n_3г_4}(\lambda_1+\lambda_2) + К_{г_1г_2г_3n_4}(\lambda_1+\lambda_2) + К_{n_1n_2г_3г_4}(\lambda_3+\lambda_4) + К_{г_1г_2n_3n_4}(\lambda_1+\lambda_2) \quad (35)$$

Ако елементите имат еднаква надеждност:

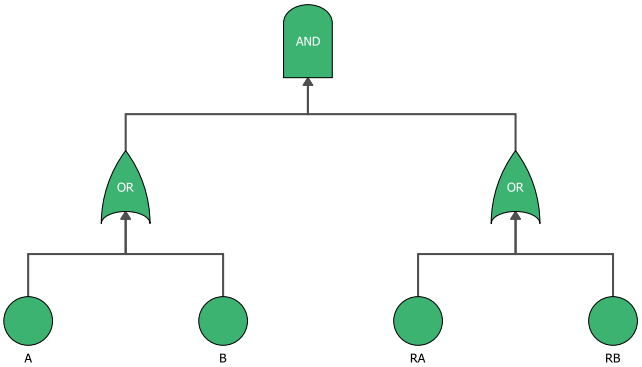
$$H_{(2v2)gr} = 4К_г^3(1-К_г)2\lambda + 2К_г^2(1-К_г)^2 2\lambda = 4К_г^2(1-К_г^2)\lambda \quad (36)$$

Следователно, средното време до отказ на система „2 от 2” с глобално резервиране ще бъде:

$$MTBF_{(2v2)gr} = \frac{1}{4К_г^2(1-К_г^2)\lambda} = \frac{MTBF}{4К_г(1-К_г^2)} \quad (371)$$

Реализирана е блокова диаграма на надеждността на системата „2 от 2” с глобално резервиране в симулационна среда BlockSim. Задават се еднакви надеждностни параметри на основните и на резервните блокове. Системата е възстановима. Всеки един от блоковете има средно време до отказ MTBF=100ч и средно време за възстановяване след отказ MTTR=4ч, като възстановяването започва веднага след откриване на отказ.

За системата „2 от 2” с глобално резервиране, блоковата схема, на която е показана на фиг.6. в симулационна среда BlockSim се реализира аналитично дърво на отказите /фиг.10./




Фиг. 10 - Аналитично дърво на отказите на структура "2от2" с глобално резервиране

Моделът на задаване на разпределението на отказите на компонентите е експоненциален. Експоненциалното разпространение е често използвано

разпределение в надеждността на инженерството. Математически това е доста просто разпространение, което многократно води до неговото използване при неопределими ситуации. Всъщност това е специален случай на разпределението на Weibull, където β=1. Експоненциалното разпределение се използва за моделиране на поведението на компоненти, които имат постоянен процент на неуспех или с времето се износват [67]. Според [68] причината, поради която се използва експоненциалното разпределение е, че моделът с постоянна честота на отказите се използва за сложни системи. Експоненциалната честота на отказите отразява случайните откази, които се появяват в комплексните системи.

## 4.2. Изследване на система „2 от 2" с парциално резервиране чрез заместване

### 4.2.1. Подход за изследване

Системата с парциално резервиране (parting reservation) има същият граф (фиг.8.), както вече разгледаната система с глобално резервиране. Разликата между тях се състои само в разделителните линии между работоспособно и неработоспособно състояния. Като се отчете обстоятелството, че неработоспособни са само състоянията, в които и основният елемент, и неговия резерв са едновременно отказали (1010 и 0101), се получава друга картина на работоспособността, очертана със синя пунктирана разграничителната линия. Освен парциалните състояния без отказ и с един отказ, работоспособни са и четири парциални състояния с по два отказа. Те са: 1100, 0110, 1001 и 0011. Като се направят същите разсъждения и се приложи същия подход и ред, както в предходната система, могат да се установят модели за търсените показатели.

### 4.2.2. Готовност на система „2 от 2" с парциално резервиране

Сумирайки вероятността за всички работещи парциални състояния за готовността $K_{г(2v2)pb}$ на системата с парциално резервиране намираме:

$$\begin{aligned} К_{г(2v2)pr} &= К_{г_1г_2г_3г_4} + К_{n_1г_2г_3г_4} + К_{г_1n_2г_3г_4} + К_{г_1г_2n_3г_4} + \\ &+ К_{г_1г_2г_3n_4} + К_{n_1n_2г_3г_4} + К_{г_1г_2n_3n_4} + К_{n_1n_2n_3г_4} + К_{n_1г_2г_3n_4} \end{aligned} \quad (38)$$

Ако всички елементи имат еднаква готовност:

$$К_{г(2v2)pr} = К_г^4 + 4К_г^3(1 - К_г) + 4К_г^2(1 - К_г)^2 = К_г^2(2 - К_г)^2 \quad (39)$$

### 4.2.3. Средно време до отказ на система „2 от 2" с парциално резервиране

При новата разграничителна линия всеки от 4-те върха с по един отказал елемент има само един преход към неработоспособност. Затова 4-те върха с по два отказали елемента имат по два прехода.

При различни по надеждност елементи на изследваната система за общата честота $H_{(2v2)pr}$ може да се напише:

$$H_{(2v2)pr} = К_{n_1г_2г_3г_4}\lambda_3 + К_{г_1n_2г_3г_4}\lambda_4 + К_{г_1г_2n_3г_4}\lambda_1 + К_{г_1г_2г_3n_4}\lambda_2 + К_{n_1n_2г_3г_4}(\lambda_1 + \lambda_4) + К_{г_1n_2n_3г_4}(\lambda_2 + \lambda_3) + К_{г_1г_2n_3n_4}(\lambda_1 + \lambda_2) \quad (40)$$

Ако елементите имат еднаква надеждност:

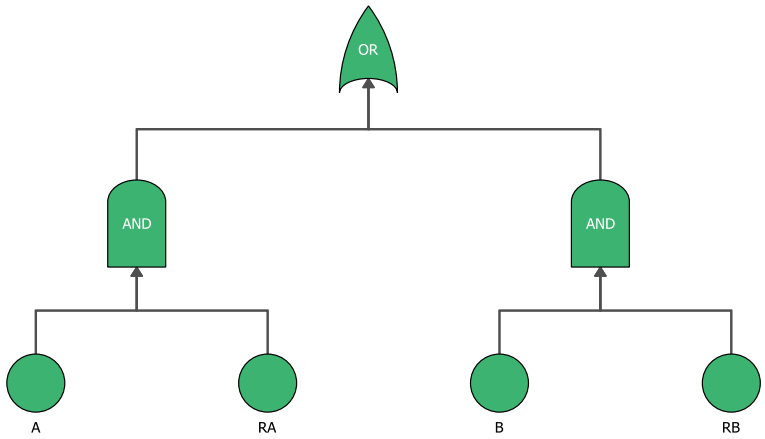
$$H_{(2v2)pr} = 4К_г^3(1 - К_г)\lambda + 4К_г^2(1 - К_г)^2 2\lambda = 4К_г^2(1 - К_г)\lambda(2 - К_г) \quad (41)$$

Следователно, средното време до отказ на система „2 от 2” с глобално резервиране ще бъде:

$$MTBF_{(2v2)pr} = \frac{1}{4К_г^2(1 - К_г)\lambda(2 - К_г)} \quad (42)$$

Реализирана е блокова диаграма на надеждността на система „2 от 2” с парциално резервиране в симулационната среда BlockSim. Блоковете в системата имат следните параметри: средно време до отказ MTBF=100ч и средно време за възстановяване след отказ MTTR=4ч, като възстановяването започва веднага след откриване на отказ. Съответно могат да се изчисляват и надеждностните параметри на системата λ и μ: съответно λ=0,01 и μ=0,25.

За системата „2 от 2” с парциално резервиране, която е илюстрирана на блоковата схема от фиг.7. в симулационната среда BlockSim се реализира аналитично дърво на отказите /фиг.11./




Фиг. 11 - Аналитично дърво на отказите на система „2 от 2” с парциално резервиране

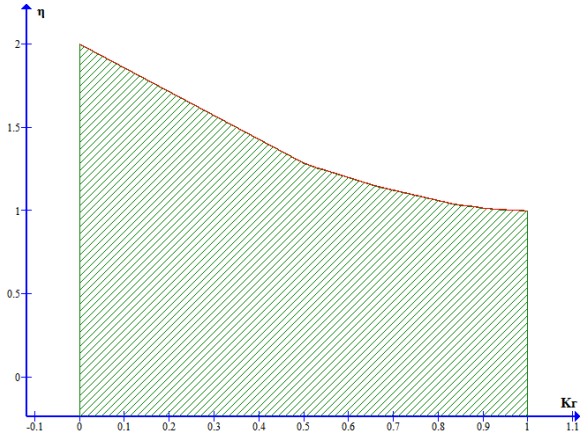
## 4.3. Съпоставка на резервираните системи „2 от 2” по надеждностни показатели

Нека отношението на системи с парциално към глобално резервиране да означим с $\eta$ - по готовност, и с $\varsigma$ - по средни времена между отказите им.

За $\eta_{2v2}$ се получава:

$$\eta_{2v2} = \frac{К_{г(2v2)pr}}{К_{г(2v2)gr}} = \frac{К_г^2(2-К_г)^2}{К_г^2[К_г^2+2(1-К_г^2)]} = \frac{(2-К_г)^2}{К_г^2+2(1-К_г^2)} \qquad (43)$$

Графичната интерпретация на тази зависимост е показана на фиг.12. Вижда се, че с намаляване на готовността на отделната градивна компонента ефектът на подобрение на готовността на системата с парциално резервиране нараства спрямо тази на глобално резервиране. Максимумът на ефекта от двукратно подобрение се получава при най-ниска готовност.



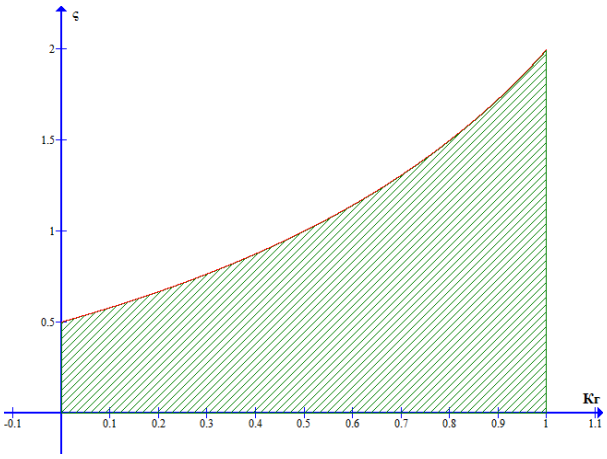

Фиг. 12 – Графична интерпретация на зависимостта (43)

Когато се заместят изведените изрази за средното време между отказите на двете системи за $\varsigma_{2v2}$ се получава зависимостта:

$$\varsigma_{2v2} = \frac{4К_г^2(1-К_г^2)\lambda}{4К_г^2(1-К_г)\lambda(2-К_г)} = \frac{1+К_г}{2-К_г} \qquad (44)$$

Когато стойността на коефициента на готовност се изменя $/K_г = 0 \div 1/$ сравнителният анализ показва дробно-линейната зависимост илюстрирана на фиг.13. Интерес представляват стойностите на коефициента на готовността $K_г$, които са близки до единица. Вижда се, че средното време между отказите на системата с парциално резервиране е толкова по-голямо, колкото е по-

висока надеждността на отделните компоненти $K_г$, които участват в състава на структурата.




Фиг. 13 - Графична интерпретация на зависимостта (44)

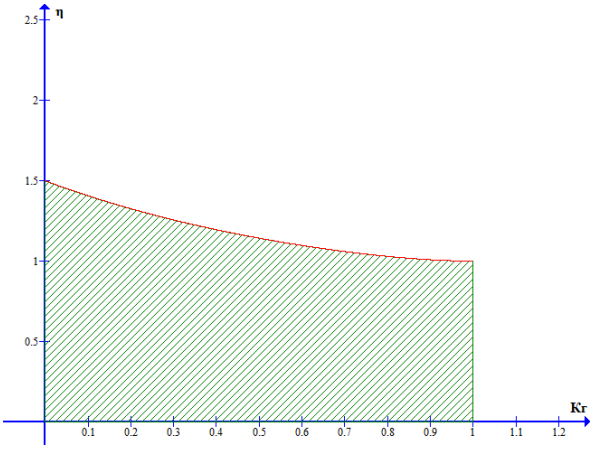
## 4.4. Сравнителен анализ на система TMR със системи „2 от 2”

За да се направи сравнителен анализ между мажоритарната система TMR и двете системи от тип DMR, се дефинират сравнителни величини, аналогични на въведените по-горе – коефициент на готовност и средно време до отказ. Получават се следните зависимости:

- Отношение между коефициентите на готовност на мажоритарната система и на системата с глобално резервиране:

$$\eta_{TMR/2v2gr} = \frac{К_г^2(3 - 2К_г)}{К_г^2[К_г^2 + 2(1 - К_г^2)]} = \frac{(3 - 2К_г)}{К_г^2 + 2(1 - К_г^2)} \qquad (45)$$

Графичната интерпретация на отношението получената зависимост е показана на фиг.14.




Фиг. 14 - Графична интерпретация на зависимостта (45)

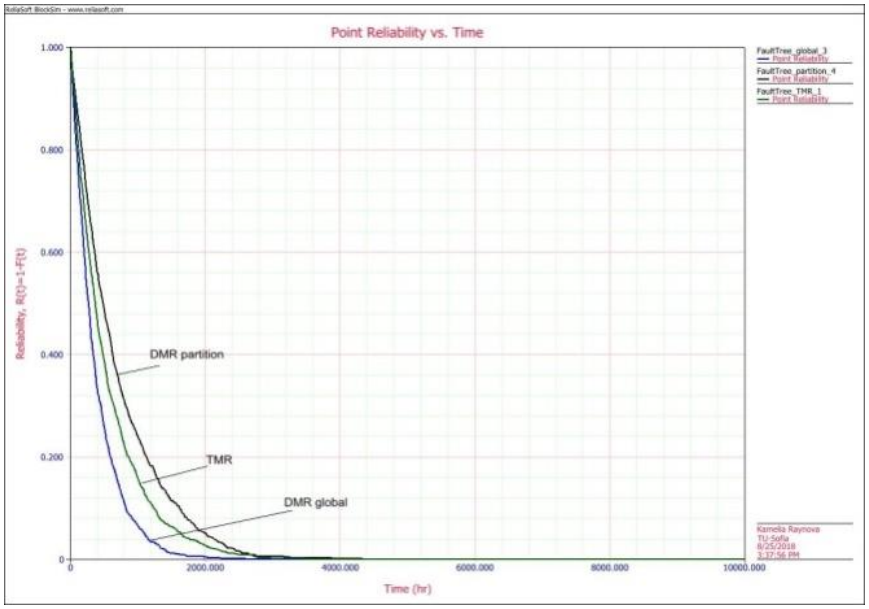
Когато се съпостави тази графика с графиката на фиг.12, за този параметър се вижда, че структурата от тип TMR е по-надеждна по отношение

на параметъра готовност от системата “2 от 2” с глобално резервиране, но има по-ниски стойности за коефициента на готовност спрямо система “2 от 2” с парциално резервиране.

Като се заместят в така дефинираната дроб изразите за средното време между отказите $MTBF_{tmr}$ и за $MTBF_{(2v2)gr}$ се получава следната зависимост:

$$\varsigma_{TMR/2v2gr} = \frac{\frac{MTBF}{6К_г(1-К_г)}}{\frac{MTBF}{4К_г(1-К_г^2)}} = \frac{2}{3}(1+К_г) \qquad (46)$$

Тя показва, че при висока готовност мажоритартната система може да се получи до 25% по-голямо време между отказите от готовността на системата с глобално резервиране.




Фиг. 15. Сравнителна зависимост между вероятността за надеждна работа и времето t при трите системи

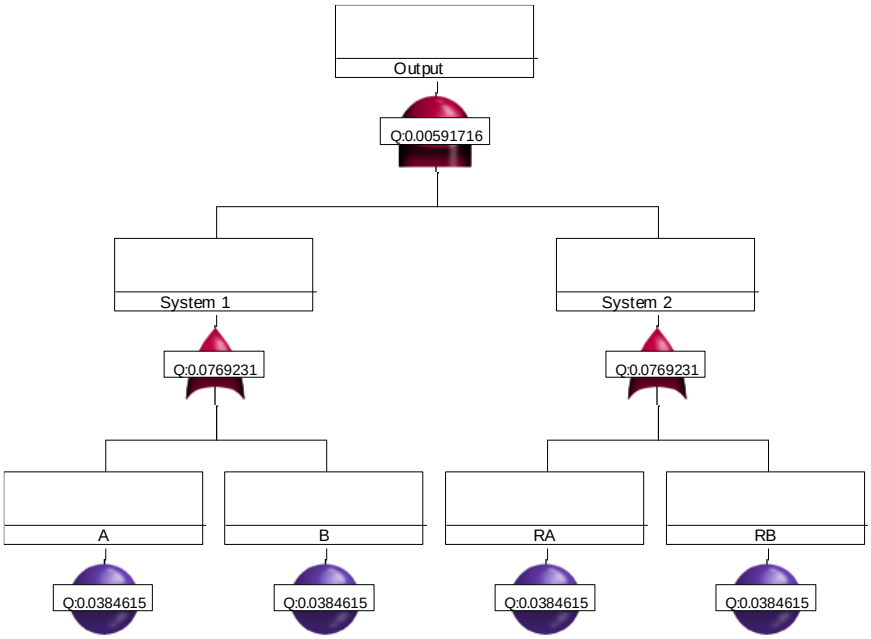
На фиг.15 е показано сравнението на трите хомогенни системи. При ниски стойности на готовност глобалната система е по-надеждна по този показател. При $K_г = 0{,}5$ системите имат еднакви времена между отказите. Може да се използва отново симулационната среда BlockSim, за да бъдат изследвани същите стойности за трите архитектури.

## 4.5. Изследване на надеждностни показатели със симулационна среда Relex

### 4.5.1. Изследване на система „2 от 2” с глобално резервиране

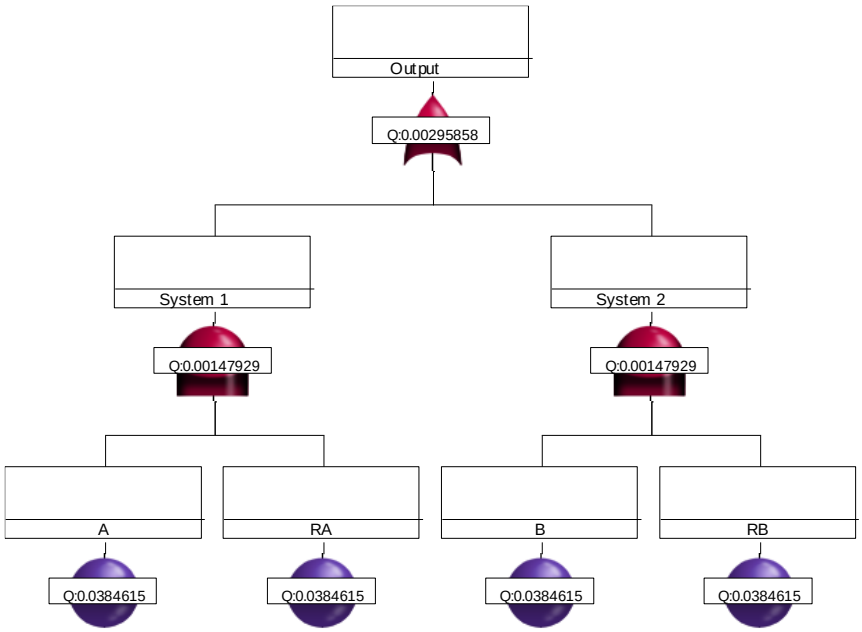
Направени са изследвания на системата от тип „2 от 2” с глобално резервиране със симулационната среда Relex. Отново се задават параметрите на основните блокове и на тяхните резервни копия. В програмата се

дефинира стойност за MTBF=100ч. и за времето за възстановяване от 4ч при поява на отказ. Фиг.16. показва начина на дефиниране на параметрите на блоковете в системата като възстановими и се задават стойности на средното време до отказ и времето за възстановяване.




Фиг.16 - Аналитично дърво на отказите на глобална система „2 от 2”

За парциалната система от тип „2 от 2” също е реализирано аналитично дърво на отказите в симулационната среда Relex /фиг.17./. Задават се параметрите на основните блокове и на тяхните резерви. В програмата отново се дефинира стойност за средното време за отказ MTBF=100ч. и за времето за възстановяване от 4ч при поява на отказ.




Фиг. 17- Аналитично дърво на отказите на парциална система „2 от 2”

Табл.3. показва стойностите, които се получават за коефициента на готовност на двете изследвани системи, получени с направените симулации на програмата Relex, при зададени стойности на отделен елемент в системите.

| $К_г$ на отделен елемент | $К_г$ на глобалната система | $К_г$ на парциалната система |
|---|---|---|
| 0,6 | 0,36 | 0,68153 |
| 0,7 | 0,6401 | 0,8201 |
| 0,8 | 0,84 | 0,92 |
| 0,9 | 0,96 | 0,98 |

Табл.3. Резултати от направените симулации на двете системи със симулационна среда Relex

Получените резултати със симулационна програма Relex, показани в табл.3. дават сходни стойности с вече направените аналогични изследвания за системите със симулационната среда BlockSim. От направения сравнителен анализ отново може да се направи извода, че като по-надеждна се явява системата от тип “2 от 2” с парциално резервиране. И двете системи се възстановяват успешно при така зададените параметри.

## НАУЧНО-ПРИЛОЖНИ И ПРИЛОЖНИ ПРИНОСИ

- **Научни приноси:**

• Предложен е подход за оценяване на надеждност на компютърни системи с използване на диверситет като средство за идентификация на откази;
• Предложен е метод за оценяване на надеждността на компютърни системи на базата на аналитични зависимости за диверситета;

- **Научно-приложни приноси:**

• Предложен е модел на диверситетна система, на базата на който чрез аналитични зависимости се описва поведението на диверситетна и хомогенна системи;
• Предложена е методика за количествено определяне на отказите по обща причина с използване на модел на диверситетна система;
• Предложен е аналитичен подход на базата на метода stress-strength за изследване на обекти с неизвестни надеждностни показатели;
• Предложен е аналитичен подход за избор на глобално или парциално резервиране в системи с излишък чрез аналитичен компаративен анализ;

- **Приложни приноси:**

• Изследван е и е верифициран симулационно предложеният модел на диверситетна система за описание на поведението на диверситетни и хомогенни системи;
• Изследван е и е верифициран симулационно предложеният аналитичен подход на базата на метода stress-strength за изследване на диверситетни системи с неизвестни надеждностни показатели;
• Изследван е и е верифициран симулационно предложеният аналитичен подход за избор на глобално или парциално резервиране в системи с излишък;

## СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

**Публикации в международни списания:**

1. G. Popov, K. Raynova, Comparative dependability analysis of tmr and dmr systems with general and separate reservation, In proceeding of: IX međunaroni naučno-stručni skup - Informacione Tehnologije za e-Obrazovanje - ITeO, Sept. 2018, Banja Luka

**Публикации в списания:**

1. G. Popov, K. Raynova, A. Balevsky, Measuring of identificaton in diversity recogniton systems, academic journal "Mechanics Transport Communications", volume 16, issue 1, 2018, article № 1551

**Публикации в международни конференции:**

1. К. Райнова, Методи за повишаване на надеждността в компютърните системи чрез използване на редундантна архитектура, Sixth International Scientific Conference "Education, Science, Innovations", ESI-2016, Pernik
2. G. Popov, K. Raynova, Diversity in nature and technology — Tool for increase the reliability of systems, 15th International Conference on Electrical Machines, Drives and Power Systems (ELMA), IEEE, Sofia, June 2017

# STUDY OF METHODS AND TOOLS FOR INCREASING THE FAULT TOLERANCE OF COMPUTER SYSTEMS

**Msc. eng. Kamelia Raynova**

Modern computer systems are becoming increasingly sophisticated, built from multiple components, resulting in repeatedly increasing the possibility of fault. Over time, the methods of preventing failures and increasing the reliability of systems have evolved considerably. New methods are proposed, which complement rather than replace existing older methods in the reliability analysis.

To improve the fault tolerance of the systems in the present dissertation are considered means such as diversity, as a way to identify failures and errors. Mathematical dependencies have been derived to determine the quantification of the factors influencing the reliability parameters. An analytical approach is proposed for the study of diversity systems based on the stress-strength method, which discusses objects with undefined reliability parameters. Simulation studies have been performed to verify the derived mathematic formulas.