БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Едита Ананиева Джамбазова

Изследване на надеждностните характеристики на отказоустойчива разпределена система за работа в реално време с настройваема надеждност

АВТОРЕФЕРАТ

на дисертация
за придобиване на образователната и научна степен „доктор“

по докторска програма „Компютърни системи, комплекси и мрежи“

професионално направление 5.3 Комуникационна и компютърна техника

Консултант:
доц. д-р Румен Андреев

София, 2023 г.

Увод

Актуалност на темата

Системите за работа в реално време се прилагат за управление на различни процеси (като индустриални производства, автомобили, авиационни системи и др.), където понятието за време е вградено в цялостния процес на производство. Те са разпределени компютърни системи с всички характеристики, които им позволяват да обработват данни и да обменят информация с външния за тях свят. Те „общуват“ с околната среда посредством сензори и активатори, което им дава възможност да управляват реални процеси. Това определя основната им характеристика – работа при времеви ограничения, наложени от средата. Поради функционирането си между управляван процес в реална физическа среда и компютърната си същност те са определяни като кибер-физични системи. Системите за работа в реално време обикновено са разпределени, което означава, че са съставени от самостоятелни компоненти, които комуникират помежду си през комуникационен канал. Те често са свързани с критични за безопасността приложения и към тях се поставят високи изисквания за гарантоспособност, които се вземат предвид още на етапа на тяхното проектиране. Гарантоспособността е интегрално понятие, което определя доверието в способността на една система да доставя коректна услуга. Всички тези аспекти на реалновременните системи – кибер-физични, разпределени, работещи с ограничения по време, отказоустойчиви – прави проектирането им сложно и многообхватно. Това поражда редица изследователски проблеми, които през годините и с развитието на технологиите са намирали различни решения. Изискването за отказоустойчивост е част от процеса на проектиране. Реалновременната функция определя гарантоспособните разпределени системи да работят с глобална времева база, според която да синхронизират всички операции, като предоставят коректна услуга както в областта на стойностите, така и в областта на времето. Кибер-физичната им природа изисква да съчетават разнообразни изисквания. Често изискванията за отказоустойчивост и работа в реално време са трудно съвместими и се налага търсенето на приемлив компромис между тях.

Отказоустойчивостта е неотменимо свойство на тези системи. Тя се постига чрез прилагането на различни подходи и техники за откриване на грешки и възстановяване от тях. В голяма степен те се основават на понятието за излишък. Излишъкът е елемент от структурата на дадена система, без който тя може да изпълнява основните си функции и който подпомага функционирането ѝ в случай на промяна в работната ѝ среда, породена от настъпването на неизправности. Управлението на излишъка е важно за отказоустойчивите системи, защото той води до повишаване на техните надеждностни характеристики, но в същото време внася

допълнителни елементи, които имат своята цена от гледна точка на производителността и разходите за системата. Въвеждането на структурен излишък с цел повишаване на гарантоспособността води до допълнителни закъснения за синхронизация, възстановяване след отказ, включване и изключване на нови компоненти и т.н., което усложнява постигането на изискванията за работа в реално време. Намирането на компромис е сложна задача и е предмет на сериозни изследователски усилия. Търсенето на нов подход за управление на излишъка в гарантоспособни разпределени системи мотивира това дисертационно изследване.

Мотивация

Изискванията за гарантоспособност на реалновременните системи при критични приложения и повишаването на разходите на системата с цел управление на излишъка мотивира идейния замисъл на дисертацията да се създаде архитектура на отказоустойчива разпределена система за работа в реално време, която да позволява разпределение на структурния излишък според изискванията на приложението – наречена от автора *система с настройваема надеждност*. Основният изследователски въпрос е дали могат отказоустойчивите разпределени компютърни системи за работа в реално време да постигнат гъвкавост по отношение на изискванията за надеждност на приложението чрез предложения в дисертацията подход на настройваема надеждност.

Предложената в дисертационния труд архитектура на отказоустойчива разпределена система за работа в реално време с настройваема надеждност е изградена от самостоятелни отказоустойчиви компоненти с различна модулност, съобразена с тяхната критичност. Критичността на компонентите се определя от тежестта на последствията от техен отказ за управляваната система. Системата е моделирана посредством разработена за целта симулационна програма и са изследвани надеждностните ѝ характеристики при различни параметри. Предложеният в дисертацията научно-приложен подход, наречен подход на настройваема надеждност, определя разпределение на хардуерния структурен излишък, съобразено с изискванията на приложението за обща системна надеждност. Системата и подходът на настройваема надеждност предлагат постигане на висока надеждност посредством разпределение на системните хардуерни ресурси по начин, който е съобразен с нуждите на приложението. Това прави отказоустойчивата разпределена система с настройваема надеждност удобна за внедряване в области с разнообразни изисквания за надеждност и смесена критичност на компонентите, във вградени системи, при по-малко отговорни приложения и пр.

Подходът на настройваема надеждност има предимства пред други широко известни разработки при: постигане на по-висока надеждност със същите ресурси, постигане на висока

готовност, гъвкавост при разпределението на системните ресурси на етапа на проектиране, приложимост в компактни системи. Моделирането на предлаганата разпределена система с настройваема надеждност и сравнението ѝ с моделите на подобни системи показва, че има възможност по-добре да се разпределят ресурсите на системата при запазване на добри нива на нейните надеждностни характеристики.

Научна постановка на изследването

Обект на изследването са отказоустойчиви разпределени системи за работа в реално време.

Предмет на дисертацията е настройваема надеждност в отказоустойчиви разпределени системи за работа в реално време.

Целта на дисертационния труд е да се изследват надеждностните характеристики на предложената от автора отказоустойчива разпределена система за работа в реално време с настройваема надеждност, като те се съпоставят с познатите подобни системи, и на тяхна основа да се разработи подход (на настройваема надеждност) за използване в отказоустойчиви системи за работа в реално време.

Хипотеза

Гарантоспособните разпределени системи постигат отказоустойчивост по много различни начини и на различни нива от своята архитектура. Водещ метод за изграждането им е въвеждането на структурен излишък. Съществуват два основни подхода за прилагане на структурен излишък – посредством специализирани хардуерни и софтуерни компоненти и посредством използване на готови софтуерни и хардуерни компоненти. И при двата подхода отказоустойчивостта срещу физически неизправности се постига чрез репликиране на хардуерните компоненти и се търси гъвкавост при репликирането на софтуерните компоненти. Хипотезата, която се поставя в настоящата дисертация, е, че може да се постигне висока надеждност и гъвкавост на разпределението на системните ресурси посредством настройваема надеждност, реализирана с разпределение на хардуерния структурен излишък.

Доказателствата на хипотезата се измерват чрез верифициране на следните твърдения:

1. Отказоустойчивата система с настройваема надеждност постига висока обща надеждност, съпоставима с надеждността на системи без разпределение на структурния излишък.
2. Съществуват конфигурации на системата с настройваема надеждност, при които се постигат по-добри надеждностни характеристики от тези на системи без разпределение на структурния излишък.

3. Може да се идентифицират условията, при които отказоустойчивата система с настройваема надеждност има по-добри надеждностни характеристики от сравняваните системи.

Методология на изследването

В дисертацията са застъпени основните прийоми на научното познание - анализ, синтез, сравнение и обобщение. Направен е обзор на гарантоспособните разпределени системи от гледна точка на разпределението на структурния излишък, като са откроени техните предимства и недостатъци. На базата на този критичен анализ е поставена целта на настоящото изследване и е формулирана основната хипотеза. Предложен е концептуален модел за вземане на решения при вграждане на гарантоспособност в системи. Въз основа на класификацията на гарантоспособни разпределени системи е направена връзка между жизнения цикъл на разработване на системи и проектирането на системи за критични приложения.

След проучването на съществуващите гарантоспособни системи е предложена архитектура на отказоустойчива система с настройваема надеждност. Направен е преглед на методите за моделиране на гарантоспособни системи и е избран и обоснован изследователски подход – симулационно моделиране. За неговата реализация е създаден програмен продукт, с който са проведени множество експерименти. Получените резултати са систематизирани и анализирани и с тяхна помощ е разработен подход на настройваема надеждност, чрез който да се определят системните конфигурации с обща надеждност според изискванията на приложението.

Основни задачи на изследването:

1. Да се направят проучване, обзор и критичен анализ на гарантоспособни разпределени системи. Да се синтезира класификация на съществуващите гарантоспособни разпределени системи. Да се очертаят изследователски възможности при разпределение на структурния излишък.
2. Да се предложат модел и архитектура на отказоустойчива разпределена система с настройваема надеждност, които дават решение на изискванията за висока надеждност според нуждите на приложението.
3. Да се дефинира метод за изследване на предложения модел. Да се разработи инструмент, реализиращ този метод. Да се състави изследователски протокол.
4. Да се проектират и проведат експериментални изследвания за тестване и анализ на надеждностните характеристики на предложената отказоустойчива система с настройваема надеждност посредством избрания изследователски подход и

реализирания програмен продукт. Да се разработи и приложи подход на настройваема надеждност.

Структура на съдържанието

Дисертационният труд е организиран в увод, четири глави, заключение, библиографска справка и две приложения.

В *Увода* са посочени темата, обектът и предметът на дисертационния труд. Описана е накратко актуалността на темата и мотивацията за извършване на дисертационното изследване. Поставена е целта на изследователската работа и задачите, чрез които тя да бъде постигната, водещата хипотеза и приложената при проведените изследвания методология.

В *Глава 1* са представени основополагащите понятия, свързани с гарантоспособните разпределени системи за работа в реално време. Описани са основните методи и техники за постигане на отказоустойчивост. Разгледани са начините за въвеждане на излишък и неговото управление. Представен е обзор и критичен анализ на познатите гарантоспособни разпределени системи. Изведен е концептуален модел на подход за вземане на решение при осигуряване на гарантоспособност и е синтезирана класификация на гарантоспособни разпределени системи. Очертани са възможностите за нови изследвания.

В *Глава 2* е представена архитектурата на предложената от автора отказоустойчива разпределена система с настройваема надеждност. Представени са методите за моделиране на гарантоспособни разпределени системи, както и модела и допусканията на отказоустойчивата система с настройваема надеждност. Там са описани изследваните надеждностни характеристики, въз основа на които системата може да бъде оценявана и сравнявана с други подобни системи. Обоснован е изборът на изследователски подход – симулационно моделиране.

В *Глава 3* са описани изследователските задачи и са представени резултатите от симулационно изследване на отказоустойчивата разпределена система с настройваема надеждност. Представен е програмният продукт за симулационно моделиране на системата с настройваема надеждност. Изследвани са надеждностните характеристики на компонент на системата и на цялата система: надеждност, готовност, средно време до отказ, средно време за ремонт и т.н. Представен е разработеният в дисертацията подход на настройваема надеждност, който позволява избиране на подходяща конфигурация на структурния излишък в зависимост от изискванията за обща системна надеждност на приложението.

Глава 4 представлява анализ и обсъждане на резултатите. Посочени са предимствата и възможните приложения на предложената отказоустойчива система с настройваема надеждност. Изведени са основните научни и научно-приложни резултати на дисертацията.

Очертани са възможностите за по-нататъшни изследвания и приложение на отказоустойчивата разпределена система с настройваема надеждност.

Дисертационният труд завършва със *Заключение*, в което се обобщават получените резултати. В края е посочена *Библиография*, съдържаща 102 източника. В *Приложение А* са изведени математическите представяния на надеждностните характеристики, с които борави изследването. В *Приложение В* е представен кодът на програмата за симулационно моделиране NMRSIM.

Глава 1. Гарантоспособни разпределени системи за работа в реално време

1.1 Гарантоспособност – основни понятия

Понятието гарантоспособност[1] (на англ. dependability) е въведено от Жан-Клод Лапри през 80-те години на 20. в. [1], [2], за да се обхванат различните аспекти на отказоустойчивите системи и да се въведе системност в използването на понятията, свързани със защитата от откази на високонадеждните системи. Основната дефиниция за *гарантоспособност* [2], [3], [4] гласи, че „Гарантоспособност е способността на една компютърна система да доставя услуга, на която може обосновано да се разчита“. Тази дефиниция поставя ударението върху обоснованото доверие в услугата, предоставяна от системата. В [3] е добавена и втора дефиниция на гарантоспособност, която подчертава значението на предотвратяването на откази: „Гарантоспособност на дадена система е способността ѝ да предотвратява откази в услугата, които са по-чести и по-тежки от допустимото“.

Специфичната терминологична основа, използвана в дисертацията, са утвърдените и широко прилагани в областта на гарантоспособните системи понятия и определения [3], [4], [5] и техните български еквиваленти [6].

Услуга е системното поведение от гледна точка на потребителя на системата. *Коректна услуга* се предоставя, когато услугата прилага системната функция.

1.1.1 Заплахи за гарантоспособността: откази, грешки, неизправности

Заплахите за компютърните системи са причините, които водят до отклонение от коректното им функциониране. Проявата на това отклонение на системно ниво се нарича отказ

[1] Преводът на основните термини, свързани с понятието гарантоспособност, е направен от колектива на секция „Отказоустойчиви компютърни системи“ на Института по компютърни системи (ИКС – БАН) [6]. По-съвременната им интерпретация и превод са на автора.

на услугата [3]. *Отказ* е събитие, което настъпва, когато предоставяната услуга се отклонява от коректната. Отклонението от коректната услуга може да приеме различни форми, наречени режими на отказ и са подредени според *сериозността на отказа* - степента на последствията на отказа за системната среда.

Отказ в услугата означава, че поне едно (или повече) външни състояния на системата се отклонява от състоянието на коректна услуга. Това отклонение се нарича грешка. Доказаната или хипотетичната причина за грешка се нарича *неизправност*. Определението за *грешка* е частта от общото състояние на системата, която е възможно да доведе до отказ.

1.1.2 Атрибути и средства на гарантоспособността

В основополагащата статия [3] са представени основните понятия и дефиниции, свързани с гарантоспособността. Те се използват и в настоящата работа, като тук са цитирани само дефинициите, които имат отношение към темата на дисертацията. Според наложилата се през последните тридесет години терминология гарантоспособността е интегрално понятие, което се характеризира със следните атрибути:

- *Готовност*: наличност на системата за предоставяне на коректна услуга;
- *Надеждност*: непрекъснатост на коректната услуга;
- *Безопасност*: отсъствие на катастрофални последствия за потребителя и средата;
- *Цялостност*: отсъствие на неправилни изменения на системата;
- *Ремонтопригодност*: способност да се предприемат модификации и ремонти.

Средствата за постигане на гарантоспособност на компютърните системи [2], [3] са *предпазване от неизправност*, *отказоустойчивост*, *отстраняване на неизправност* и *прогнозиране на неизправност*. Отказоустойчивостта обединява методи и средства, имащи за цел предотвратяването на откази в присъствието на неизправности.

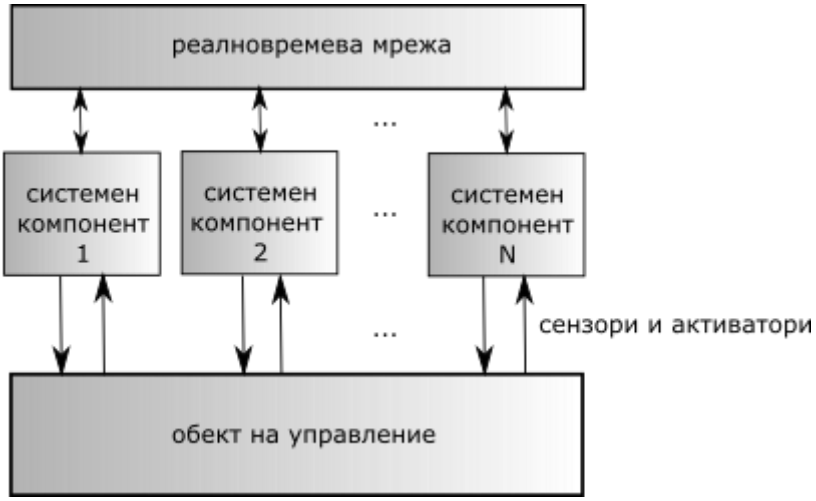
Фокусът на дисертационния труд е върху постигането на отказоустойчивост на разпределени компютърни системи за работа в реално време.

1.2 Разпределени системи за работа в реално време

Разпределените системи са изградени от компоненти, които обменят съобщения през комуникационна магистрала (реалновременна мрежа) и изпълняват общ алгоритъм за управление (*Фигура 1-2*). От гледна точка на отказоустойчивостта компонентите на системата трябва да осигуряват неразпространение на неизправностите към други компоненти. Компонентът на системата е *блок на ограничаване на неизправност* [17], [19], ако прекият ефект от единична неизправност влияе само върху функционирането на един-единствен компонент [17]. Допуска се, че блоковете на ограничаване на неизправност отказват

независимо един от друг. Това допускане е приложимо за хардуерни неизправности, които са обект на настоящото изследване.

Системата управлява индустриален процес, наречен обект на управление. Компонентите получават входни данни от сензорите на обекта на управление, изпълняват управляваща програма, която изчислява резултати, и извеждат тези резултати към активаторите на обекта на управление (*Фигура 1-2*). За да изпълняват задачите си, те трябва да комуникират с останалите компоненти чрез обмен на данни. Системните компоненти са проектирани да имат безопасно поведение, т.е. нито една неизправност не трябва да достига до изходите на компонента, както и да се разпространява към други части на системата.



Фигура 1-2. Разпределена система за работа в реално време

Разпределените системи за работа в реално време работят с крайни времеви интервали, налагани от средата и обекта на управление. При тях коректната услуга трябва да бъде коректна в областта на стойностите и в областта на времето [17]. Това означава системата да предоставя коректен резултат на обекта на управление и да го извежда в рамките на специфицирания времеви интервал. Когато времевите интервали в системата за реално време изискват стриктно спазване, за да бъде доставена коректна услуга, системата за реално време е с *твърди времеви ограничения* [17]. В противен случай тя е система за реално време с *меки времеви ограничения* [17]. Често системите работят и при двата вида ограничения едновременно, но наличието на поне една функция с твърди ограничения по време прави системата система с твърди времеви ограничения. Друго съществено разграничение на системите за реално време е в зависимост от задействащия фактор, който определя взаимодействията между системните компоненти: *събитийни разпределени системи* (задействани според момента на настъпване на съществено събитие в системата) и *периодични разпределени системи* (задействани според определен момент от течението на физическото/реалното време) [17]. Гарантоспособните разпределени системи често

изпълняват функции с твърди времеви ограничения и са периодични. Това дава възможност тяхното поведение да бъде предсказуемо и позволява да се използват по-икономично ресурсите им. Този вид системи са обект на настоящото изследване.

За постигането на отказоустойчиво поведение на компонентите в гарантоспособните разпределени системи те се конструират с репликирани модули [17], [21], [22], [23], [24]. *Модул* е най-малката заменима единица на системата. Това понятие има отношение към техниките за репликиране и метода на въвеждане на излишък в системата. Репликирането на ниво компонент може да бъде хардуерно или софтуерно реализирано. Добавят се и допълнителни средства за откриване на грешки към всеки модул [25], [26], [27], [28] – блокове за самопроверка. Самата комуникационна магистрала също може да бъде репликирана [25], [29], [30], [31]. Разнообразието от техники за репликиране дава възможност за избор на най-подходящите решения за конкретно приложение.

1.3 Управление на излишъка в отказоустойчиви разпределени системи за работа в реално време

Гарантоспособните разпределени системи за работа в реално време обикновено са предназначени за критични по отношение на безопасността приложения. Едно от основните изисквания за тяхната работа е да бъдат отказоустойчиви. Отказоустойчивостта се постига чрез използване на разнообразни техники, повечето от които се основават на някаква форма на излишък. Съществуват различни видове излишък и техники за прилагането му.

Въвеждането на излишък в компютърните системи, като метод за постигане на отказоустойчивост, и репликирането, като техническа реализация на излишъка, са добре познати и проучени [23], [24], [33], [34], [35], [36], [37], [38]. Въпреки че управлението на излишъка е разработено и приложено в различни отказоустойчиви системи отдавна, проектирането на нови гарантоспособни разпределени системи, разработването на системи от системи и кибер-физични системи [40], [41] налагат нов поглед и търсене на нови подходи за реализиране на излишъка. В критичните инфраструктури (енергийна система, водоснабдителна система, електрическа система и др.), например, критичните елементи на системата, като системата за надзорно управление и събиране на данни (Supervisory Control and Data Acquisition - SCADA), се реализират чрез използване на структурен излишък [39].

1.3.1 Проектиране на системата

Цикълът на разработване, наречен още развой, на разпределената система може да бъде представен като итеративен процес [44], който разглежда системата от две гледни точки: практическа и абстрактна. Практическата гледна точка към системата е нейното внедряване, а

абстрактният поглед върху системата е нейният модел. Тези гледни точки трябва да обменят информация помежду си, за да постигнат цялостен системен модел, който може да бъде валидиран и верифициран.

На *Фигура 1-3* е представена концепцията за осъществяване на подход за вземане на решение по отношение на осигуряване на гарантоспособността на една система чрез използване на излишък. Дадена разпределена система управлява промишлен процес, т.е. разпределена компютърна среда. Системата е подложена на неизправности, които нарушават нейната работа и застрашават управлявания процес. Проблемът с гарантоспособността на системата става въпрос на проектирането: как да бъде направена системата отказоустойчива. Неизправностите са неизбежни и непредсказуеми. Затова системата трябва да има ресурси, с които да доставя услугата, за която е предназначена, дори в присъствието на неизправности. Въвеждането на излишък е една от стратегиите за решаване на проблема с необходимата отказоустойчивост. Инженерните въпроси с прилагането на излишъка трябва да бъдат съчетани с изследователски решения. На *Фигура 1-3* те са обединени под общото наименование оценка на гарантоспособността. Моделите и техните параметри зависят от приложението (например кибер-физични системи, критични за безопасността системи, автомобили и др.) и от работната среда, т.е. разпределената компютърна среда. Атрибутите на гарантоспособността се определят въз основа на конкретното приложение. Резултатите, получени от изследването на моделите, се използват при проектирането на системата. Определя се подходящата техника на репликиране.

Фигура 1-3. Концептуален модел на подход за вземане на решение при осигуряване на гарантоспособност

Описаният процес на определяне на техниката за репликиране (*Фигура 1-3*) може да бъде използван като входни данни на схемата на жизнения цикъл на разработване на системи

или да бъде вграден в него, като по този начин специфицира изискванията за гарантоспособност.

1.4 Излишък при гарантоспособните разпределени системи за работа в реално време

Дефиницията на понятието „излишък“, която ще използваме, е следната:

Излишъкът е функционалност или компонент на една компютърна система, който добавя ресурси за изпълнение на коректната ѝ услуга.

Това е метод за внедряване на отказоустойчивост при гарантоспособни компютърни системи и на свой ред се реализира чрез техники за репликиране. Излишъкът може да бъде структурен, времеви или функционален [23], [33], [34], [37], [38].

1.4.1 Стил на репликиране при структурен излишък

Стилът на репликиране определя начина, по който репликираните компоненти изпълняват своята работа. Отказоустойчивите компоненти имат репликирани модули и само един от тях, първичният, извежда изходния резултат. Останалите реплики са вторични. В зависимост от стила на репликиране излишъкът може да бъде пасивен или активен. Резервирането е пасивна форма на излишък [23], [33], [35]. Репликирането представлява едновременна работа на идентични модули, които изпълняват едни и същи функции върху едни и същи входни данни и сравняват резултатите си [23], [33], [35], [37], [38].

1.4.2 Степен на репликиране при структурен излишък

Степента на репликиране определя броя на модулите в даден компонент. В зависимост от важността на компонента за системната работа той може да има един или повече репликирани модули или въобще да няма излишък. Степента на репликиране зависи и от изискванията за отказоустойчивост на компонентите.

При хардуерните реализации репликирането приема формата на *N-модулен излишък* [23], [34], [35], [37], [38]. Той най-често се прилага във вид на двоен и троен модулен излишък. При *двоен модулен излишък* (ДМИ) двете реплики сравняват своите резултати и, в случай на разминаване, компонентът не извежда резултат, като остава мълчалив при отказ. Обикновено модулите имат допълнителни механизми за отказоустойчивост, наречени *блокове за самопроверка*, за да решат кой модул е отказал. При *троен модулен излишък* (ТМИ) има три активни модула и гласуващ блок. Активните модули работят едновременно, а гласуващият блок определя мажоритарния резултат, който бива изведен към обекта на управление.

Репликирането на софтуера се реализира като блокове за възстановяване и N-версионно програмиране. При подхода с *блокове за възстановяване* [49], [50] се правят две алтернативни

програми (наречени алтернативи) от обща спецификация на услугата и се въвежда приемащ тест, който решава дали резултатът е правилен. Приемащият тест се прилага последователно върху резултатите на двете алтернативи. Ако резултатите на първичната алтернатива не преминат приемащия тест, се изпълнява втората алтернатива. Подходът с блокове за възстановяване съответства на резервирането в готовност при хардуера.

При *N-версионното програмиране* [49], [51], [52] съществуват N ($N \geq 2$) варианта на софтуера, които се изпълняват едновременно и резултатите им се сравняват. Вариантите са софтуерни програми, които са написани от различни екипи от програмисти и по възможност използват различни алгоритми. Предполага се, че това спомага да бъдат избегнати общите грешки, които програмистите са склонни да правят. Резултатите на софтуерните версии се гласуват и се извежда мажоритарният резултат. Хардуерният еквивалент на N-версионното програмиране е N-модулният излишък.

При *N-самопроверяващото програмиране* [49] се изпълняват N самопроверяващи се софтуерни компонента, като един от тях се смята за действащ, а останалите самопроверяващи се компоненти са негови „горещи“ резерви. При отказ на действащия компонент действието се превключва към някой от резервните самопроверяващи се компоненти.

1.4.3 Времеви излишък

Времевият излишък изисква да бъде заделено допълнително време за изпълнението на задачи [23], [37], [53], [54]. Той създава по-малък разход в сравнение със структурния излишък, но може да повлияе на производителността на системата и затова трябва да бъде подчинен на ограниченията за реално време.

1.4.4 Функционален излишък

Функционалният излишък се внедрява в софтуера. В [33] той се дефинира като квалифициране на поведението на системата по отношение на нейните входни/изходни взаимоотношения. Функционалният излишък е полезен при откриването на грешки.

1.5 Въвеждане на излишък

Гарантоспособността в разпределените системи за реално време, които работят в критични за безопасността приложения, е станала част от тяхното проектиране. Всички параметри и системни компоненти, които са важни за отказоустойчивото функциониране на системата, се включват в жизнения цикъл на разработване на системата. Описателен многослоен модел на проектиране на разпределени системи със структурен излишък е илюстриран на *Фигура 1-4*.

Въвеждането на структурен излишък включва определянето на критичните елементи, на важните системни параметри и на нивата на критичност. Компонентите на разпределената система управляват различни параметри на обекта на управление с различна значимост за отказоустойчивото функциониране на системата. На етапа на определяне на изискванията в жизнения цикъл на разработване на системата трябва да бъдат определени контролираните параметри и да бъдат откроени нивата на критичност. Компонентите, които управляват важните параметри, получават високо ниво на критичност и трябва да бъдат отказоустойчиви.

Фигура 1-4. Синтез на подход на гарантоспособни разпределени системи със структурен излишък

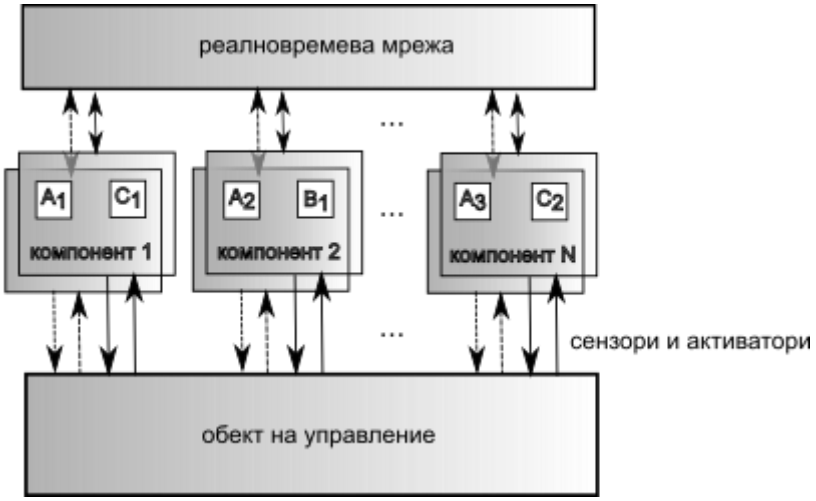
На етапа на проектиране на системата се определят степента и стила на репликиране. Степента на репликиране определя дали ще бъдат приложени компоненти с единичен (ЕМИ), двоен (ДМИ) или троен модулен излишък (ТМИ). Избраният стил на репликиране определя дали ще бъде използвано активно или пасивно репликиране. Модулите в системните компоненти могат да бъдат равномерно разпределени, т.е. всички компоненти могат да имат еднакъв брой модули, или могат да използват смесен излишък. На етапа на действителното изграждане в жизнения цикъл на разработване на системата се внедрява определената системна архитектура, например GUARDS [56], [57], многостранна гарантоспособност [47], [48] или DECOS [58], [59], както е показано на *Фигура 1-4*.

1.6 Внедряване на различни степени на репликиране

1.6.1 Еднакъв излишък за всички компоненти

Най-прекият начин да се приложи излишък е да бъдат репликирани активните компоненти и да бъдат сравнявани техните резултати. При разпределените системи компонентите могат да бъдат изградени от два или три идентични модула, които да изпълняват една и съща задача (*Фигура 1-5*). Резултатите на репликираните модули се сравняват (както е

в [25], [28], [49], [58]) или се гласуват в случай на използване на ТМИ (както е в [17], [62]). Ако няма разминаване, предполагаемо верният резултат се извежда към обекта на управление. При разлика не се извежда резултат, а компонентът се поставя в безопасно състояние според конвенциите на системата.



Фигура 1-5. Гарантоспособна разпределена система за работа в реално време

Хардуерните компоненти на системата имат еднаква степен на репликиране, но софтуерните компоненти, изпълняваните задачи, могат да имат различен излишък. Например, на *Фигура 1-5* са изобразени три задачи – A, B и C; задача A има три копия, задача B има едно, а задача C има две. Копията могат да бъдат разположени в различни системни компоненти, като по този начин се постига изолиране на грешките.

1.6.2 Различен излишък за компонентите

Има системи, които използват различна степен на репликиране за своите компоненти. В GUARDS [57] съществуват нива на доверие и нива на критичност. Нивата на доверие се дефинират според степента, до която може да се има доверие на даден системен компонент – колкото по-доверен е компонентът, толкова по-високо ниво на доверие има [56]. Степента на доверие, възложена на компонента, зависи от неговата критичност. За критични компоненти се смятат тези, чийто отказ води до тежки последствия. Такива компоненти имат по-висока степен на доверие.

Моделът на репликиране в DEAR-COTS [28], [66] използва активен излишък на софтуерните компоненти и позволява определянето на степента на репликиране на специфични части от приложението за реално време в съответствие с надеждността на компонентите и желаното ниво на надеждност за приложението. Архитектурата DEAR-COTS е насочена към разпределени компютърно управляеми системи, които работят в реално време и може да използва както равномерно, така и смесено разпределение на излишъка.

Проектът DECOS [58], [59] предлага интегрирана разпределена архитектура, която да поддържа системи със смесена критичност. Системите със смесена критичност се състоят от разпределени части на приложението с различни нива на критичност, изпълняващи се върху един и същ физически хардуер.

Системата MEAD [48] предлага съчетаване на противоречивите изисквания за отказоустойчивост и реално време при прилагане на гарантоспособност на ниво мидълуер. MEAD е инфраструктура, която предлага прозрачна и регулируема отказоустойчивост в реално време, проактивна гарантоспособност, системно адаптиране към пълен отказ, неизправности в комуникацията и във времето с отчитане на наличните ресурси и скалируемо и бързо откриване на неизправности и възстановяване от тях. Регулируемата отказоустойчивост се постига чрез т.нар. подход на многостранната гарантоспособност (versatile dependability) [47], [48]. Този подход дава възможност за изграждане на гарантоспособни софтуерни архитектури, като се отчитат три важни аспекта – отказоустойчивост, производителност и ресурси. Той предоставя набор от инструменти, наречени „копчета“, за настройване на баланса между тези аспекти.

Повечето гарантоспособни разпределени системи за реално време следват архитектурния стил, изобразен на *Фигура 1-5*. Те използват еднакво репликирани физически компоненти и смесен излишък на софтуерните компоненти. Съществуват възможности за разработване на системи, които се адаптират към конкретни приложения чрез разпределение на хардуерния структурен излишък.

1.7 Изводи и резултати

В *Глава 1* са представени основните понятия от предметната област на дисертацията – гарантоспособни разпределени системи за работа в реално време. Откроена е тяхната структура по отношение на гарантоспособността и реалното време. Управлението на структурния излишък е разгледано през призмата на системното проектиране. Създаден е концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност. Този модел се вписва в жизнения цикъл на проектиране на системи и отговаря на изискването гарантоспособността да бъде заложена в системните спецификации.

Направен е обзор на методите и техниките за въвеждане на излишък в отказоустойчиви системи и е синтезирана класификация на гарантоспособни разпределени системи със структурен излишък, която показва вграждането на изискванията за гарантоспособност в етапите на проектиране на системата.

Представен е кратък обзор на известните гарантоспособни разпределени системи от гледна точка на управлението на структурния излишък. Двете тенденции са да се използва

еднакъв излишък за всички системни компоненти или компонентите да имат различен излишък.

Изложението в *Глава 1* отговаря на изпълнението на задача 1 на дисертацията.

Постигнатите научни и научно-приложни резултати са:

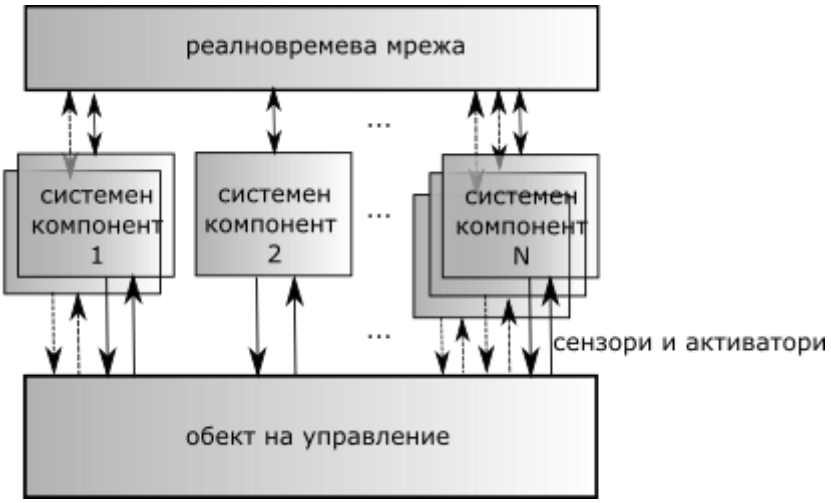
1. Създаден е концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност;
2. Предложен е синтез на класификация на гарантоспособни разпределени системи със структурен излишък.

Глава 2. Моделиране на отказоустойчивата разпределена система с настройваема надеждност

Предложената в дисертацията архитектура на отказоустойчива разпределена система (ОРС) с настройваема надеждност е основана върху понятието за настройваемост.

Настройваемост е свойството на гарантоспособната разпределена система за реално време да разпределя структурния излишък според изискванията за надеждност на приложението.

Отказоустойчивата разпределена система с настройваема надеждност [73], [74], [75], [76] прилага различни степени на репликиране на хардуерните компоненти (*Фигура 2-1*).



Фигура 2-1. Гарантоспособна разпределена система за реално време с настройваема надеждност

Необходимостта системата да има компоненти с различна степен на репликиране е свързана с тяхната критичност. За разлика от подходите, прилагащи смесена критичност на частите на приложния софтуер, които се изпълняват на еднакво/равномерно репликиран

хардуер, подходът с настройваема надеждност предлага степента на репликиране на хардуерните компоненти да се определя според тяхната критичност на етапа на проектиране и те да работят със смесен излишък. В дисертацията е направена количествена оценка на възможностите за реализиране на гарантоспособни разпределени системи с предложения подход и те са сравнени със системи без разпределение на структурния излишък. Сравнението е направено с помощта на модели, решени посредством симулационно моделиране, и резултатите (представени в *Глава 3* и [76]) показват, че съществуват разпределения на излишъка, които постигат общата системна надеждност, изисквана от приложението.

Отказоустойчивата разпределена система с настройваема надеждност (*Фигура 2-1*) е изградена от компоненти, ограничаващи неизправностите. Компонентите могат да имат различна степен на репликиране в зависимост от критичността си. Всеки модул има блок за самопроверка, чрез който се откриват грешки и се осигурява спиране/мълчание при отказ. Системата работи при твърди времеви ограничения. Този подход позволява предвидимост на поведението на системата, като времената за изпълнение на системните задачи са гарантирани. Чрез промяна на структурния излишък на компонентите в етапа на проектиране се цели промяна на надеждността на системата според изискванията на приложението. Моделират се хардуерни неизправности и се цели постигане на хардуерна надеждност.

2.1 Анализ на начините за моделиране на гарантоспособни системи

Моделирането е често използван похват за изследване на системи, преди те да бъдат реално проектирани и внедрени. Това дава възможност да се проверят различни хипотези и да се намери подходящият модел, въз основа на който да се търсят конкретни инженерни решения. Моделирането позволява сравнение между различни варианти за изграждане на системата или на части от нея по ефективен начин по отношение на цената, тъй като възможните инженерни реализации не винаги могат да се оценят количествено при сложни системи.

Поради стохастичната природа на неизправностите показателите, с които се оценява тяхното въздействие върху функционирането на гарантоспособните системи, имат вероятностен характер. Затова за описанието им се използват понятия от областта на теорията на вероятностите и математическата статистика.

2.1.1 Методи за моделиране на гарантоспособни системи

Моделите на системата могат да бъдат анализирани или математически оценявани посредством три различни подхода [77]: симулационен, аналитичен и хибриден (комбинация от симулационни и аналитични методи). Моделират се само основните характеристики на

системата. При *симулирането* тя се описва в компютърна програма, която имитира нейната динамика. При аналитичните методи се съставят и решават системи от математически уравнения, които определят системната динамика [77], [78], [79], [80]. Предимството на симулирането е, че могат да се представят подробно характеристиките на изследваната система, без да се налагат много ограничения върху модела. При аналитичните модели допусканията често се опростяват, за да могат да се решат системите от уравнения. Точността при симулирането се ограничава единствено от времето, необходимо за получаване на краен резултат. Възможно е и комбинираното прилагане на двата подхода, което все още не е честа практика [77].

При друга класификация [81] моделите се разглеждат като комбинаторни и модели, основани на пространство на състоянията. *Комбинаторните модели* включват диаграми с блокове на надеждност [77], [82], [83], [84], дървета на събитията [81] и дървета на неизправностите [77], [85], [86]. Те са сравнително лесни за проектиране и обработване и могат да се анализират с комбинаторни методи. Техен недостатък е ограничената им моделираща способност, дължаща се на допускането за статистическа независимост на събитията.

Моделите с пространство на състоянията включват Марковски вериги и мрежи на Петри [84], [87]. Те представят поведението на системата посредством достижими състояния и възможни преходи между тях. Те имат по-голяма моделираща мощност от комбинаторните модели, които не могат да обхванат характеристиките на моделираната система.

Проблемът при методите с пространство на състоянията е т.нар. ефект на „експлозия“ на пространството на състоянията – експоненциално нарастване на пространството на състоянията при нарастване на броя на компонентите. Това води до повишаване на цената на изчисленията. В такъв случай мрежите на Петри и Марковските вериги могат да бъдат симулирани [81].

2.1.2 Надеждностни характеристики на отказоустойчивата система с настройваема надеждност

Като част от изискванията към симулационната програма за моделиране на отказоустойчивата система с настройваема надеждност се изчисляват следните характеристики на системата: надеждност *R*, средно време до отказ *MTTF*, средно време до спиране *MTTS*, общо време на престой, средно време между отказите *MTBF*, средно време между спиранията *MTBS*, средно време за ремонт след отказ *MTTR*, готовност *A*.

Най-често използваната функция на разпределение при моделиране на отказоустойчиви системи е експоненциалното разпределение. То е подходящо заради свойството си да не съдържа памет за състоянието на системата. Експоненциалното

разпределение в достатъчна степен отразява динамиката на гарантоспособните системи и предлага удобно математическо представяне. При моделирането се допуска също, че интензивността на неизправностите е постоянна [84].

Надеждността е вероятността системата да бъде в работно състояние в даден момент *t*. При допускането за експоненциално разпределение на събитията в системата функцията на разпределение става [37], [84]

$$F(t) = 1 - e^{-\lambda t}. \quad (1)$$

Плътността на разпределение е [37], [84]

$$f(t) = \lambda e^{-\lambda t}. \quad (2)$$

Надеждността на системата се изразява като експоненциална функция [37], [84]

$$R(t) = e^{-\lambda t} = 1 - F(t). \quad (3)$$

Средното време до отказ MTTF се изчислява като средна стойност на времето до отказ на компонент за определен период на работа. То е математическото очакване на времето до (първи) отказ. При постоянна интензивност на неизправностите *MTTF* е [37], [84]

$$MTTF = \frac{1}{\lambda}. \quad (4)$$

Средното време между отказите MTBF може да се изчисли като средно аритметичното време между отказите на системата. *MTBF* се измерва за ремонтируеми системи. При експоненциално разпределение и постоянна интензивност на неизправностите $MTBF = 1/\lambda$.

Средното време за ремонт MTTR представлява средното време, което се изисква за ремонт на отказали елементи на системата. При експоненциално разпределение с постоянна интензивност на неизправностите

$$MTTR = 1/\mu. \quad (5)$$

Готовността A се измерва с вероятността системата да е работоспособна в момент *t*, независимо от това колко пъти е била неработоспособна в интервала (0,*t*). За постоянни интензивности на неизправностите и ремонтите готовността може да бъде изразена чрез следната формула [37], [84]

$$A = \frac{\mu}{\lambda+\mu} = \frac{MTBF}{MTBF+MTTR}. \quad (6)$$

Общото време на *престой* е сумата от всички периоди, през които системата е била неработеща. Средното време за престой се изразява с (П12) (*Приложение А*).

Системата работи при следните определения за отказ и стоп. *Отказ* на системата настъпва, когато повече от половината компоненти откажат с неоткрит отказ или при повече от половината отказали компоненти броят на тези с неоткрит отказ е по-голям от броя на компонентите с открит отказ.

$$N_u > \frac{N}{2} \text{ или } N_u + N_d > \frac{N}{2} \text{ и } N_u \geq N_d, \quad (7)$$

където N_u е броят на компонентите с неоткрит отказ, а N_d – броят на компонентите с открит отказ. Системата *спира*, когато повече от половината компоненти откажат с открит отказ или при повече от половината отказали компоненти броят на тези с открит отказ е по-голям от броя на компонентите с неоткрит отказ.

$$N_d > \frac{N}{2} \text{ или } N_u + N_d > \frac{N}{2} \text{ и } N_d > N_u. \quad (8)$$

2.2 Допускания при моделирането на системата

Моделът на отказоустойчивата система с настройваема надеждност е изграден въз основа на допускания, отразяващи нейното поведение и възприетите за изследването режими на неизправност, отказ и ремонт.

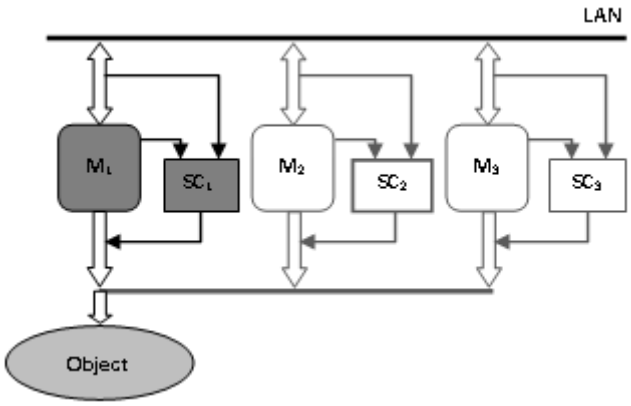
Разпределената система с настройваема надеждност [73], [74], [75], [76] е изградена от компоненти с активен излишък. Компонентите имат еднотипни модули, всеки от които притежава средства за самопроверка с покритие C. Степента на репликиране на компонентите се определя в зависимост от тяхната критичност – колкото по-важен за приложението е даден компонент, толкова по-критичен е той и е по-висока степента му на репликиране. Разглеждат се три степени на критичност/репликиране. Компонентите, чийто отказ не застрашава нормалното функциониране на системата и не води до катастрофални последствия, могат да разчитат само на средствата си за самопроверка и да не бъдат репликирани. Техният коефициент на покритие е C_1. Компонентите с по-голяма критичност за приложението, които обаче е достатъчно просто да спрат да извеждат управляващо въздействие в случай на отказ, са компоненти с ДМИ. При тях е възможно отказалият модул да бъде ремонтиран, стига неизправността му да е открита от блока за самопроверка. Компонентите с ДМИ имат коефициент на покритие $C_2 > C_1$. Най-критичните компоненти за системата, чийто отказ би имал катастрофални последствия за приложението, се изграждат с ТМИ и имат коефициент на покритие $C_3 > C_2 > C_1$.

Отказоустойчивата система с настройваема надеждност толерира постоянни хардуерни неизправности с интензивност λ_p. При компоненти с двоен и троен модулен излишък е

възможно възстановяване (локален ремонт) след неизправност на модул с интензивност на възстановяване μ_p. Системата може да работи без или с ремонт, като при ремонтируема система интензивността на ремонтите е μ_{sys}.

2.3 Модел на компонент на системата

Компонентът на разпределената система с настройваема надеждност е изграден от еднотипни модули M_i (i=1, 2, 3), всеки от които има собствен блок за самопроверка SC_i (*Фигура 2-2*) [94]. В зависимост от критичността им модулите могат да се дублират или триплират, за да се постигне по-висока надеждност в точката от управляващия контур, където е разположен компонентът.



Фигура 2-2. Компонент на разпределената система с настройваема надеждност

Един от модулите е основен и той единствен извежда управляващо въздействие към обекта на управление. Всички модули изпълняват едновременно управляващата програма и изчисляват управляващото въздействие (активен излишък). Модулите, които не извеждат резултат към обекта на управление, извършват контрол на основния модул и участват при сравнението на резултатите. Те могат да поемат управлението при отказ на основния модул.

При единичен модул само средствата за самопроверка могат да открият отказ при изпълнението на управляващата програма и да забранят извеждането на управляващо въздействие. Ако приложението налага по-силна защита на изходите и по-високо покритие на неизправностите, към единичния модул се добавят допълнителни един или два модула със собствени средства за самопроверка, като по този начин може да се отговори на различни нива на критичност, диктувани от приложението на ОРС с настройваема надеждност.

2.3.1 Функции на системен компонент

Характерно за предложения подход е вграждането на локален блок за самопроверка във всеки модул, реализация на протокол за разпределено гласуване и следене на състоянието.

Блокът за самопроверка [73] е вграден като допълнителен блок към конфигурацията на модула и има проверяващи и управляващи функции.

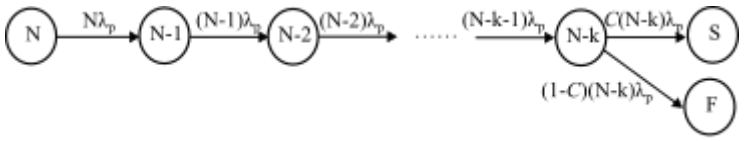
2.3.2 Режим на отказ

Компонентът отказва, когато откажат всички негови модули. Благодарение на въвеждането на средства за самопроверка и излишък не всеки неоткрит отказ в отделен модул води до отказ на целия компонент. Възможни са две състояния при отказ на модул – стоп и отказ.

2.4 Модел на системата

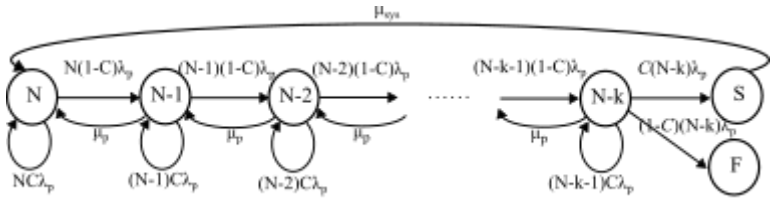
Работата на системата е представена с Марковски процес, където всяко от състоянията в Марковската верига изобразява състоянието на системата след настъпила неизправност според броя на работещите компоненти *N*, а дъгите са преходите между отделните състояния при възникване на постоянна неизправност с интензивност на потока на неизправностите λ_p. Покритието на механизмите за самопроверка е *C*. Разгледани са различни възможности за работата на системата: с и без възстановяване след постоянна неизправност и с и без системен ремонт.

Когато системата е без ремонт, тя работи до изчерпване на ресурсите си и влиянието на коефициента на покритие *C* върху надеждността е незабележимо (*Фигура 2-3*).



Фигура 2-3. Марковски модел на система без възстановяване след постоянна неизправност и без ремонт

Ако системата има възможност за локален ремонт, *C* спомага за удължаване на живота на компонента, това влияе и върху надеждността на системата. Влиянието на *C* расте, защото само при детектиран отказ на компонент той може да бъде ремонтиран преди да настъпи системен отказ. Системен ремонт се извършва след попадане на системата в стопово състояние. Изправните компоненти продължават работа след ремонта със същите начални характеристики. Отказоустойчивата разпределена система с настройваема надеждност може да работи и със системен ремонт и възстановяване на компонент от постоянна неизправност (*Фигура 2-6*). Това предполага постигане на по-добри надеждностни характеристики.



Фигура 2-6. Марковски модел на система с ремонт и възстановяване от постоянна неизправност

Всички описани възможности в Марковските модели (*Фигура 2-3* - *Фигура 2-6*) са изследвани чрез симулационното моделиране на системата.

2.5 Изводи и резултати

В *Глава 2* е представена разработената от автора отказоустойчива разпределена система с настройваема надеждност. Тя предлага различни степени на репликиране на хардуерните компоненти. Необходимостта системата да има компоненти с различна степен на репликиране е свързана с тяхната критичност, която се определя от изискванията на приложението. Отказоустойчивата система с настройваема надеждност е моделирана при определени допускания за нейната работа с цел да се провери тази хипотеза.

Предложената от автора отказоустойчива разпределена система с настройваема надеждност е моделирана въз основа на използване на Марковски вериги и валидирана чрез симулация. Методът на симулационното моделиране е избран, защото симулацията дава възможност да се моделират системи с множество компоненти и голяма степен на детайлизация. Представени са моделите на компонент на системата и на цялата система. Предвидени са възможности за моделиране на системата с настройваема надеждност с и без възстановяване от постоянна неизправност, както и с и без системен ремонт.

Представените в *Глава 2* резултати изпълняват задачи 2 и 3 на дисертацията. Постигнатите научни резултати са създаването на модел на предложената отказоустойчива разпределена система с настройваема надеждност и представянето на авторски архитектурен модел на отказоустойчива разпределена система с настройваема надеждност, като са дефинирани изискванията към нейните компоненти и системата като цяло.

Глава 3. Изследване на отказоустойчивата система с настройваема надеждност

Отказоустойчивата система с настройваема надеждност управлява обект, като получава входни данни от неговите сензори, изпълнява управляващ алгоритъм и изчислява изходни резултати, които извежда към активаторите на обекта. Параметрите на обекта на управление могат да имат различна важност за коректната системна работа. Затова компонентите на

системата са репликирани според своето ниво на критичност. Настройването на системната надеждност посредством разпределяне на степента на репликиране на компонентите според нуждите на управлявания обект може да използва ресурсите на системата по-ефикасно и би могло да подобри нейната надеждност.

Симулационното моделиране на системата с настройваема надеждност изследва как промяната на структурния излишък влияе върху общата системна надеждност. Компонентите с различна степен на репликиране имат различно ниво на критичност за системата. Това определя и коефициента на покритие на техните средства за самопроверка: C_1 за единичните компоненти, $C_2 > C_1$ за компонентите с двоен модулен излишък и $C_3 > C_2 > C_1$ за триплираните компоненти. Коефициентите на покритие могат да се изменят в зависимост от условията на средата или от условията на функциониране в рамките на някакви граници. Тези коефициенти заедно с интензивността на неизправностите λ_p определят поведението на компонентите в симулационния модел на отказоустойчивата система с настройваема надеждност. Събитията в системата са свързани с промяната на нейното състояние. Това са случайни събития, характеризиращи се със съответната интензивност на възникване: λ_p, μ_p и μ_{sys}. Допуска се, че отказал компонент може винаги да бъде възстановен след постоянна неизправност (локален ремонт), а времената до отказ са нормално разпределени.

Разработен е следният *изследователски протокол*:

1. Изследване на компонент
2. Изследване на системата
   - Входни данни: брой компоненти в системата N, брой модули в системата M, λ_p, μ_p, μ_{sys}, граници на коефициентите на покритие C_1, C_2 и C_3.
   - Изходни резултати: $R(t)$, *A, MTTF, MTTR, MTTS, MTBF, MTBS, downtime*
   - Определяне на възможните разпределения на структурния излишък при зададените N и M.
3. Определяне на времената до отказ при дадените входни параметри за всички разпределения на модулния излишък на системи с и без настройване на структурния излишък.
4. Изследване на влиянието на различни параметри върху надеждностните характеристики на отказоустойчивата система с настройваема надеждност и на системи без разпределение на структурния излишък.
5. В зависимост от резултатите определяне на конфигурациите с най-висока системна надеждност.

3.1 Симулационно моделиране на отказоустойчива система с настройваема надеждност

Избраният в *Глава 2* изследователски метод на симулационно моделиране е приложен чрез разработване на симулационна програма. Тя е проектирана според описания изследователски протокол и определя надеждностните характеристики на изследваната система, формулирани в т. 2.1.2. Програмата симулира отказоустойчиви системи с различно разпределение на структурния излишък и системи без разпределение на структурния излишък, което дава възможност за тяхното сравнение и анализиране.

3.1.1 Симулационна програма

Разработеният програмен продукт NMRSIM за симулиране на поведението на отказоустойчиви разпределени системи (представен по-пълно в *Приложение В*) определя показателите на системите от интерес за изследването и дава възможност за сравнение на предложената система със системи без настройване на надеждността. Програмата е написана на език за програмиране C++ и разработването ѝ изпълнява следните изисквания:

1. Да симулира поведението на системата във времето, като отразява зададените дефиниции за стоп и отказ;
2. Да представя настъпването на постоянна неизправност като стохастичен процес с експоненциално разпределение и интензивност на неизправностите λ_p;
3. Да има възможност да моделира система с ремонт и без ремонт;
4. Да представя моментите на извършване на ремонтите като стохастичен процес с експоненциално разпределение и интензивност на ремонтите μ_p (за локален ремонт) и μ_{sys} (за системен ремонт);
5. Да моделира система с произволен брой модули и компоненти;
6. Да изчислява надеждностните характеристики, посочени в *Глава 2*, т. 2.1.2;
7. Да моделира поведението при неизправност на компонент и цялата система;
8. Да разпределя структурния излишък при зададен общ брой компоненти и общ брой модули;
9. Да моделира коефициента на покритие на средствата за самопроверка;
10. Да изчислява надеждността като функция на времето;
11. Да изчислява статистическите показатели на получените резултати;
12. Да съхранява получените резултати.

Програмният продукт за симулационно моделиране на предложената отказоустойчива разпределена система с настройваема надеждност е основан на моделиране на

функционирането на системата във времето и моментите на настъпване на неизправност. Блоковата структура на симулационната програма е изобразена на *Фигура 3-2*.

Фигура 3-2. Структура на симулационна програма NMRSIM

В блока на входни данни се задават N, M, λ_p, μ_p, μ_{sys}, C_1, C_2, C_3 и R_{total}. Програмата използва генератор на псевдослучайни числа, работещ според алгоритъма, представен в [98]. Той се използва при определяне на момента на настъпване на неизправност и за генериране на случайни стойности на коефициентите на покритие. При дадени N и M в блока за определяне на конфигурациите на структурния излишък се определят всички възможни разпределения на структурния излишък. Блокът за определяне на неизправност в компонент определя моментите на неизправност за съответния компонент. Текущата неизправност се определя в съответния блок след сравнение на моментите на неизправност във всички компоненти.

В зависимост от степента на репликиране в блока за определяне на коефициентите на покритие се задават коефициентите C_1, C_2 и C_3 на отделните компоненти. В блока за определяне на състоянието на компонент се определя дали компонентът е отказал, дали отказът му е открит и дали е в ремонт. В блока за определяне на системното състояние се определя дали системата е в стопово или отказово състояние. При наличие на системен отказ се записват всички натрупани времена до отказ и се преминава към определяне на надеждностните характеристики. Ако системата е в стопово състояние цикълът продължава, а моментът на спиране се записва.

В блока за изчисляване на надеждностните характеристики се определят *R*, *MTTF*, *MTTR*, *MTBF*, *MTBR*, *MTTS*, *MTBS*, *A* и *downtime*. За реализиране на подхода на настройваема надеждност се използва блока за определяне на конфигурациите, които постигат зададената системна надеждност R_{total}. Всички получени данни се обработват статистически в блока за определяне на статистически параметри. Получените резултати за надеждностните характеристики на всички конфигурации на структурния излишък се записват във файлове. Това се прави в блока на изходните резултати. Взаимодействието между отделните блокове на симулационната програма е изобразено схематично на *Фигура 3-2*.

Блоковата структура на програмата дава възможност тя да бъде разширявана и надграждана, за да могат да се моделират и други гарантоспособни разпределени системи.

3.2 Резултати от симулационно моделиране на системата

Отказоустойчивата система с настройваема надеждност е симулирана при следните параметри: брой компоненти N=10 и N=20, брой модули съответно M=20 и M=40, интензивност на постоянните неизправности $\lambda_p=10^{-3}$ 1/h и $\lambda_p=10^{-4}$ 1/h, интензивност на възстановяване след постоянна неизправност μ_p=0.1 1/h, интензивност на ремонтите μ_{sys}=0.1 1/h, граници на коефициентите на покритие $C_1 \in [0.8, 0.9)$, $C_2 \in [0.9, 0.95)$ и $C_3 \in [0.95,\ 1.0)$.

При изследването на различните разпределения на структурния излишък в компонентите е използвана следната нотация:

система (i, j, k),

където i – брой на единичните компоненти, j – брой на компонентите с двоен модулен излишък, k – брой на компонентите с троен модулен излишък. Например, система (3,4,3) при N=10 и M=20 означава система с 3 единични, 4 дублирани и 3 триплирани компонента.

Изследвани са разпределения на структурния излишък, които запазват общия брой на модулите в системата. Хипотезата на настоящото изследване предполага проучване на възможностите за разпределение на хардуерните ресурси на системата според тяхната критичност при определени изисквания за надеждност, съобразени с приложението. Като

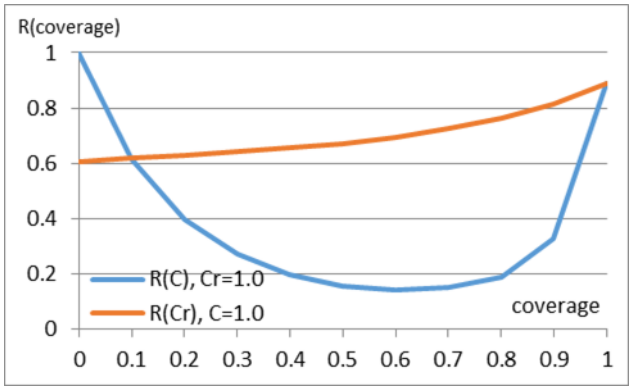
еталонна система за сравнение е избрана система, изградена само от дублирани компоненти, която не разпределя структурния излишък. При това положение броят на модулите в системата е $M=2N$. Интерес представляват само конфигурациите, които удовлетворяват това ограничение.

3.2.1 Изследване на компонент

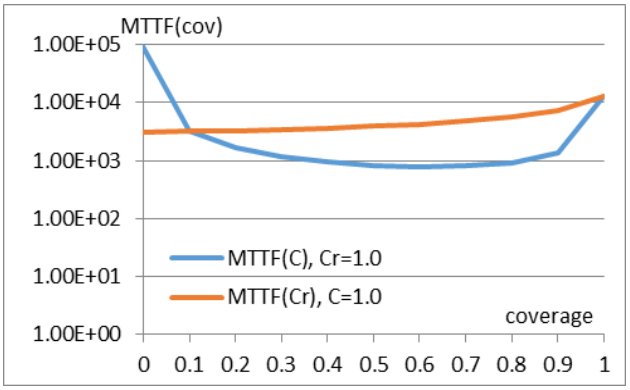
Резултатите от симулационното моделиране са представени за компонент, изграден от два и от три модула. Показателите на надеждността са отчетени за случаите на компонент с локален ремонт и без локален ремонт. Изследвано е влиянието на постоянни и случайни неизправности. Данните са за следните интензивности на неизправностите и ремонтите: постоянни неизправности на процесор $\lambda_p=10^{-2}$ 1/h, случайни неизправности на процесор $\lambda_t=0.1$ 1/h, възстановяване на процесор след постоянна неизправност $\mu_p=0.1$ 1/h, ремонт на компонент $\mu_c=0.1$ 1/h.

При компонент с двоен модулен излишък отказоустойчивостта се постига чрез блоковете за самопроверка на двата модула (с коефициент на покритие C) и чрез сравнение на резултатите на модулите. Компонентът *отказва*, когато едновременно откажат и двата процесора на модулите **и** средствата за самопроверка не са открили отказа. Компонентът попада в *стопово състояние*, когато сравнението показва разлика, но средствата за самопроверка **не са** открили отказа.

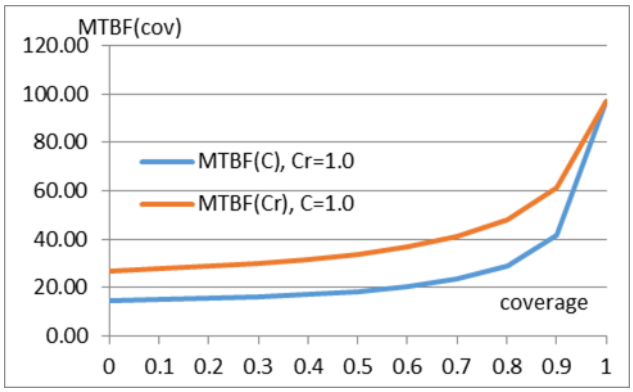
На *Фигура 3-3 – Фигура 3-10* са показани надеждностните характеристики на дублиран компонент във функция от коефициентите C и C_r за система с локален ремонт. За ниски и високи стойности на коефициента на покритие дублираният компонент има по-висока надеждност и *MTTF* (*Фигура 3-3* и *Фигура 3-4*), отколкото за средни стойности на този коефициент. Това се дължи на влиянието на сравнението, което при ниски стойности на C на практика го неутрализира, защото при сравнение неизправностите в компонента се откриват с вероятност 1. При високи стойности на C покритието на неизправностите има силно значение за по-добрите надеждностни показатели на компонента. Коефициентът на покритие на средствата за самопроверка подобрява готовността на компонента (*Фигура 3-9*).



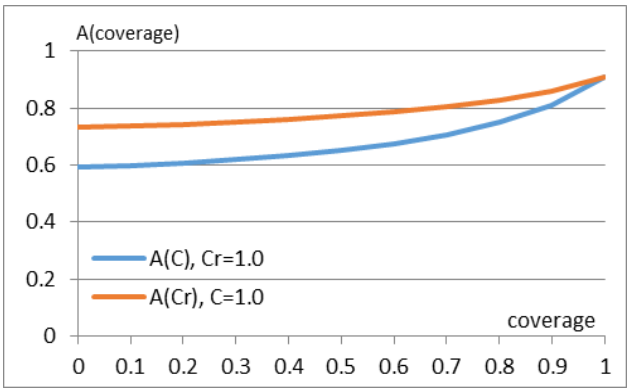
Фигура 3-3. Надеждност на дублиран компонент на система с локален ремонт



Фигура 3-4. MTTF на дублиран компонент на система с локален ремонт

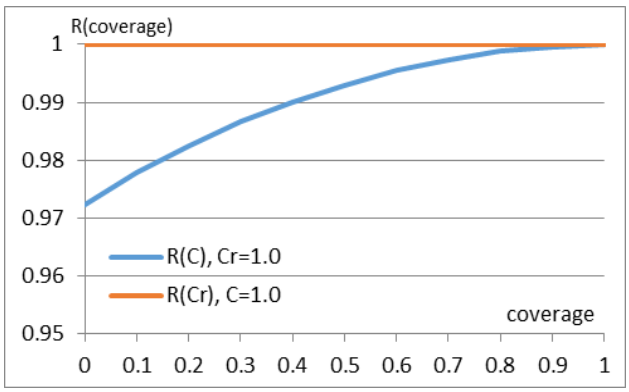


Фигура 3-8. MTBF на дублиран компонент на система с локален ремонт

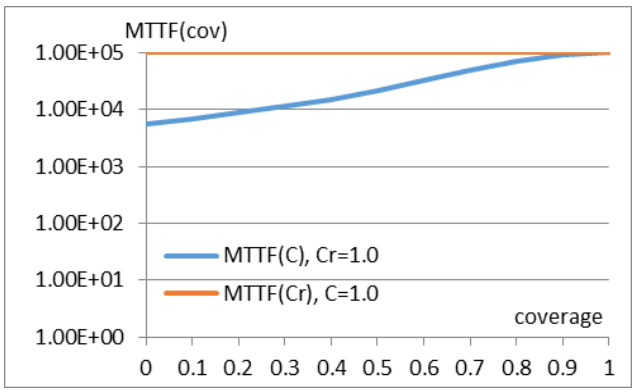


Фигура 3-9. Готовност на дублиран компонент на система с локален ремонт

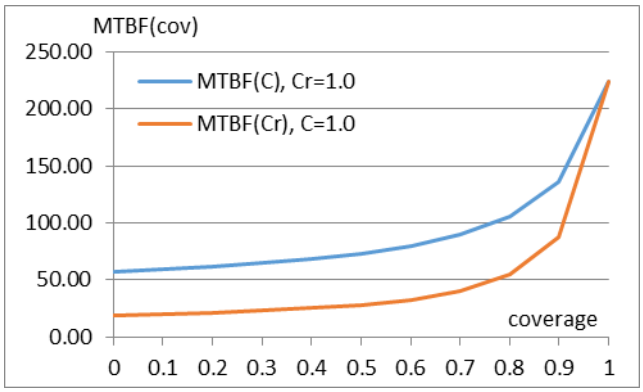
При компонент с троен модулен излишък отказоустойчивостта се постига отново чрез блоковете за самопроверка, а сравнението е всъщност мажоритарно гласуване. *Отказ* настъпва, когато повече от половината модули са с неоткрита неизправност. Компонентът попада в *стопово състояние*, когато повече от половината модули са с открита неизправност. На *Фигура 3-13 – Фигура 3-20* са представени надеждностните характеристики на компонента за система с локален ремонт. Коефициентът C_r влияе слабо върху повечето надеждностни показатели на триплирания компонент (*Фигура 3-13 - Фигура 3-16*). Той обаче води до намаляване на времената между отказите и на готовността на компонента (*Фигура 3-17 - Фигура 3-20*).



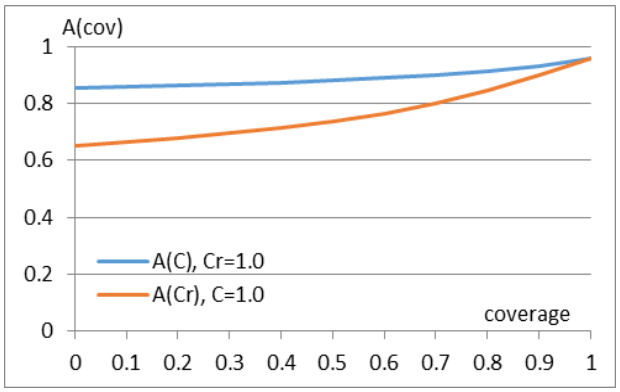
Фигура 3-13. Надеждност на триплиран компонент на система с локален ремонт



Фигура 3-14. MTTF на триплиран компонент на система с локален ремонт



Фигура 3-19. MTBF на триплиран компонент на система с локален ремонт



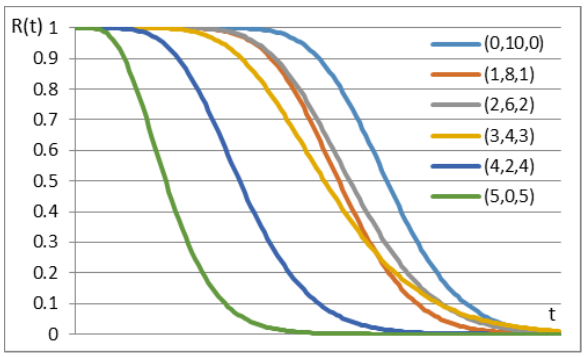
Фигура 3-20. Готовност на триплиран компонент на система с локален ремонт

Коефициентът на покритие на блока за самопроверка очаквано подобрява надеждността и времето до отказ (*Фигура 3-13* и *Фигура 3-14*), както и показателите, свързани с работоспособността на компонента (*Фигура 3-19* и *Фигура 3-20*).

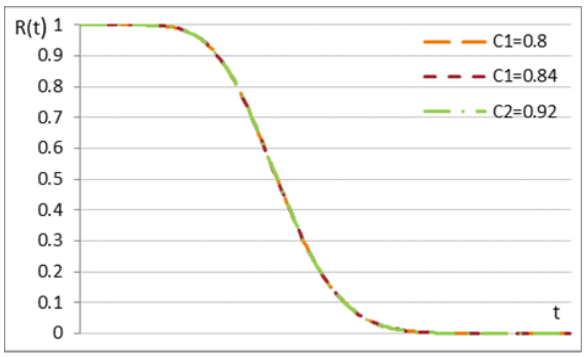
От направените изследвания на дублиран и триплиран компонент на отказоустойчива разпределена система може да се направи извод, че добавянето на блокове за самопроверка към всеки модул от компонента подобрява значително надеждностните характеристики на системата.

3.2.2 Система с 10 компонента

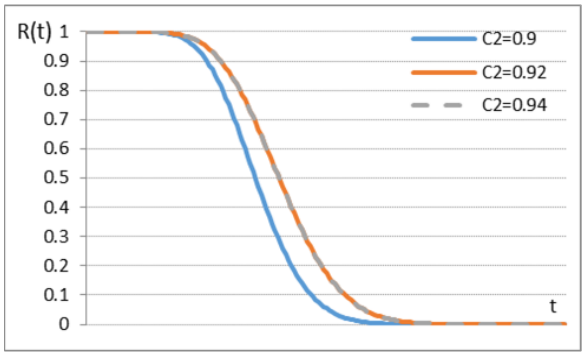
Системата има възможност за възстановяване от постоянна неизправност на компонент и за ремонт след системен отказ. Изследвани са 6 конфигурации на структурния излишък. Тяхната надеждност при C_1=0.88, C_2=0.94 и C_3=0.99 е показана на *Фигура 3-23*. Стойностите на коефициентите на покритие на компонентите с различна степен на репликиране, C_1, C_2 и C_3, са максимални за изследването.



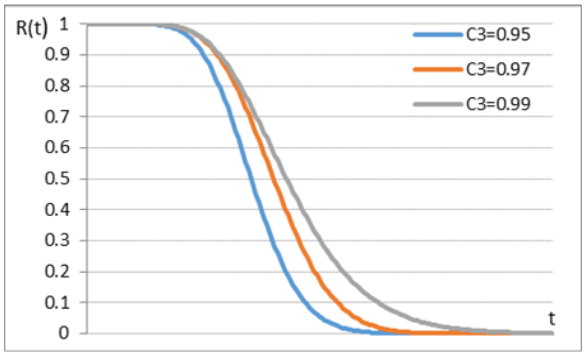
Фигура 3-23. Надеждност на система с 10 компонента за C_1=0.88, C_2=0.94 и C_3=0.99



Фигура 3-24. Надеждност на система (3,4,3) за различни стойности на C_1, при C_2=0.94 и C_3=0.97



Фигура 3-25. Надеждност на система (3,4,3) за различни стойности на C_2, при C_1=0.88 и C_3=0.97



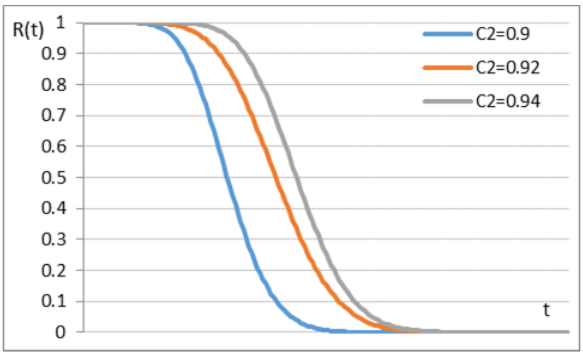
Фигура 3-26. Надеждност на система (3,4,3) за различни стойности на C_3, при C_1=0.88 и C_2=0.94

При тези условия най-висока надеждност има системата (0,10,0) (светло синята графика на *Фигура 3-23*). Тази система представлява известните системи, които работят само с дублирани компоненти, т.е. без разпределение на структурния излишък. Най-ниска надеждност има система (5,0,5) (зелената графика на *Фигура 3-23*), която е изградена само от единични и триплирани компоненти. Системи (1,8,1) (оранжевата графика на *Фигура 3-23*) и (2,6,2) (сивата графика на *Фигура 3-23*) имат близки стойности на надеждността. Система (3,4,3) (жълтата графика на *Фигура 3-23*) се доближава по надеждност до системи (1,8,1) и (2,6,2). Интерес представляват системите (3,4,3), (2,6,2) и (0,10,0) поради сравнително по-високата си надеждност.

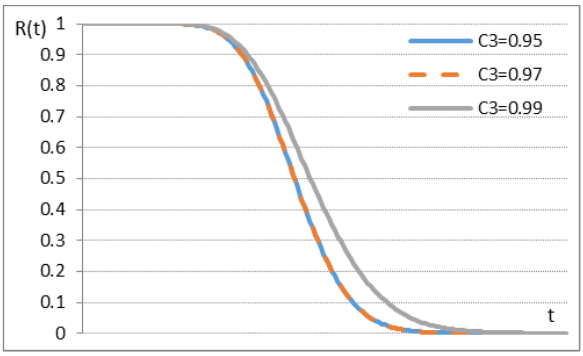
Надеждността на системата (3,4,3) е изследвана, за да се проследи влиянието на коефициентите на покритие на компонентите (*Фигура 3-24* - *Фигура 3-26*). Коефициентът на покритие на единичните компоненти C_1 не влияе въобще върху надеждността на системата (3,4,3) – графиките на надеждността за трите стойности на C_1 съвпадат (*Фигура 3-24*).

Система (2,6,2) е по-силно повлияна от увеличаването на коефициента на покритие C_2 (*Фигура 3-28*), отколкото от увеличението на C_3 (*Фигура 3-27*). Това се обяснява с по-големия брой дублирани компоненти в сравнение с броя на триплираните компоненти. Резултатите за C_3=0.95 (синята графика на *Фигура 3-28*) и C_3=0.97 (оранжевата графика на *Фигура 3-28*) са почти еднакви. Само най-голямата стойност на C_3=0.99 води до подобряване на системната

надеждност (сивата графика на *Фигура 3-28*). От друга страна, увеличаването на коефициента на покритие C_2 води до значително подобряване на надеждността (*Фигура 3-27*).

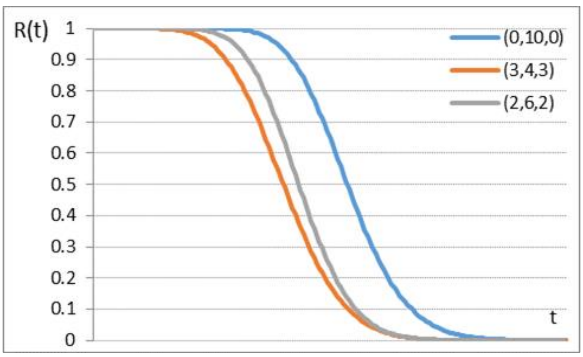


Фигура 3-27. Надеждност на система (2,6,2) за различни стойности на C_2, при C_1=0.88 и C_3=0.97

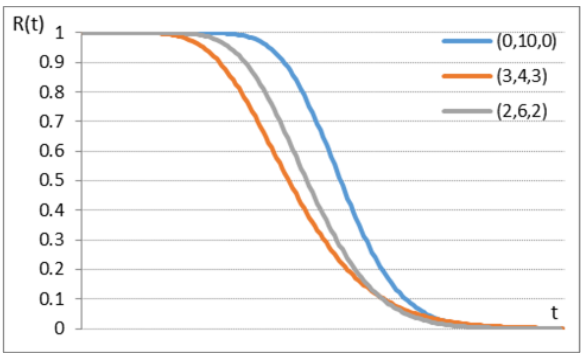


Фигура 3-28. Надеждност на система (2,6,2) за различни стойности на C_3, при C_1=0.88 и C_2=0.94

На *Фигура 3-29* и *Фигура 3-30* е направено сравнение на надеждността на системите (3,4,3), (2,6,2) и (0,10,0) при C_1=0.88 и C_2=0.94, а коефициентът C_3 е различен (C_3=0.97 на *Фигура 3-29* и C_3=0.99 на *Фигура 3-30*). Най-висока надеждност има системата, изградена изцяло от дублирани компоненти (0,10,0). Системата (3,4,3) е с най-ниска надеждност, която се подобрява при увеличение на C_3 (*Фигура 3-30, C_3*=0.99). Системата (2,6,2) показва средна стойност на надеждността. Може да се направи изводът, че системите с преобладаващ брой дублирани компоненти, (2,6,2) и (0,10,0), постигат по-висока системна надеждност.



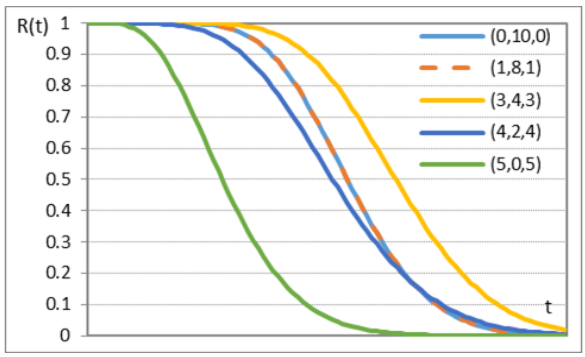
Фигура 3-29. Надеждност на системите (3,4,3), (2,6,2) и (0,10,0) при C_1=0.88, C_2=0.94 и C_3=0.97



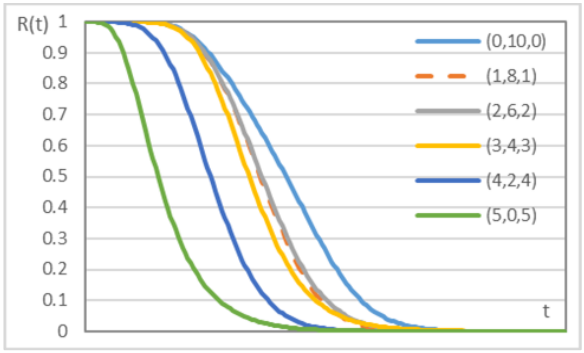
Фигура 3-30. Надеждност на системите (3,4,3), (2,6,2) и (0,10,0) при C_1=0.88, C_2=0.94 и C_3=0.99

При сравнение на системи с различно разпределение на структурния излишък за по-малък коефициент на покритие C_2=0.9 (C_1=0.88 и C_3=0.97) (*Фигура 3-31*) подреждането на системите по надеждност се променя. Най-висока надеждност има системата (3,4,3) (жълтата крива на *Фигура 3-31*), следвана от системите (1,8,1) (оранжевата крива на *Фигура 3-31*) и (0,10,0) (светло синята крива на *Фигура 3-31*), които имат еднаква надеждност, и системите (4,2,4) (тъмно синята крива на *Фигура 3-31*) и (5,0,5), която има най-ниска надеждност (зелената крива на *Фигура 3-31*).

На *Фигура 3-32* е изобразена надеждността на всички конфигурации на системата с 10 компонента, когато коефициентите на покритие на компонентите се менят в зададените в т. 3.2 интервали. Тези резултати са разгледани по-подробно в т. 3.3.



Фигура 3-31. Сравнение на надеждността на системи с различен структурен излишък при C_1=0.88, C_2=0.9 и C_3=0.97



Фигура 3-32. Сравнение на надеждността на системи с различен структурен излишък при $C_1 \in [0.8, 0.9)$, $C_2 \in [0.9, 0.95)$ и $C_3 \in [0.95,\ 1.0)$

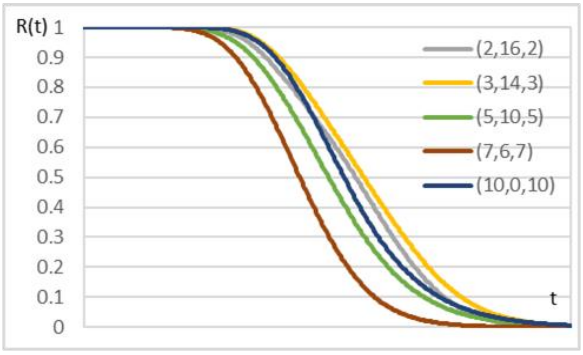
На *Фигура 3-32* се вижда, че най-висока надеждност има системата без настройване на надеждността, (0,10,0) (светло синята крива), следвана от системите (1,8,1) (оранжевата крива) и (2,6,2) (сивата крива). Близка, но по-ниска, надеждност има системата (3,4,3) (жълтата крива). Тези резултати са сходни с надеждността на системите от *Фигура 3-23*, но се различават от резултатите на *Фигура 3-31*.

Симулационното моделиране на отказоустойчивата система с настройваема надеждност с 10 компонента показва, че системата има добри надеждностни характеристики. От резултатите се вижда, че има разпределения на структурния излишък, които подобряват системната надеждност при определени условия.

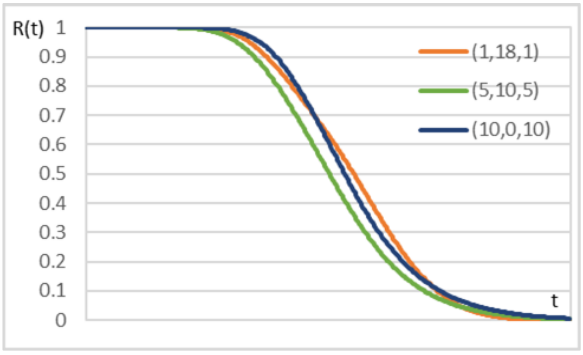
3.2.3 Система с 20 компонента

Отказоустойчивата система с настройваема надеждност с 20 компонента и 40 модула е симулирана при същите параметри като системата с 10 компонента (т. 3.2.2). Изследвани са 11 разпределения на модулния излишък в компонентите. Влиянието на постоянните неизправности е разгледано при две различни интензивности на неизправностите, за да се изследват различни условия на работната среда на системата. Допускането е, че системите, които функционират при по-неблагоприятни условия, търпят повече неизправности, което в модела се изразява с по-голяма интензивност на постоянните неизправности $\lambda_p=10^{-3}$ 1/h. По-малката интензивност на неизправностите $\lambda_p=10^{-4}$ 1/h моделира среди, където неизправностите настъпват по-рядко, но системата трябва да е в състояние да ги толерира.

Системата с настройваема надеждност има различни разпределения на излишъка в компонентите. Тяхната надеждност, R_d, във функция от времето е показана на *Фигура 3-33*, където интензивността на постоянните неизправности е $\lambda_p=10^{-4}$ 1/h.



Фигура 3-33. Надеждност на системи с различни разпределения на структурния излишък, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h



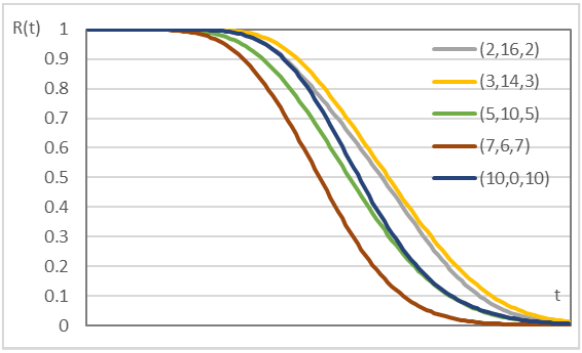
Фигура 3-34. Надеждност на системи с различен брой триплирани компоненти, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

Системите със сравнително малък брой единични и триплирани компоненти демонстрират висока надеждност (системи (3,14,3) в жълто и (2,16,2) в сиво на *Фигура 3-33*). Не може да се твърди обаче, че това е тенденция. Системата, състояща се само от единични и триплирани компоненти (система (10,0,10) в тъмно синьо на *Фигура 3-33*) има близка надеждност.

За да се покаже влиянието на триплираните компоненти, на *Фигура 3-34* е изобразена надеждността на системи (1,18,1), (5,10,5) и (10,0,10). Въвеждането на повече единични и триплирани компоненти в системата (система (10,0,10) в тъмно синьо на *Фигура 3-34*) подобрява надеждността и удължава периода, през който системата поддържа висока надеждност. Функционирането с по-малко единични и ТМИ компоненти (система (1,18,1) в оранжево на *Фигура 3-34*) обаче не влошава значително системната надеждност. Система (5,10,5), която има най-ниската надеждност от трите системи на *Фигура 3-34*, все пак има добра надеждност в сравнение с останалите системи, както се вижда от *Фигура 3-33*.

Не може да се изведе ясна зависимост между разпределението на структурния излишък и надеждността (*Фигура 3-33* и *Фигура 3-34*). Разпределението на излишъка влияе върху системната надеждност и някои разпределения са по-благоприятни за системата от други. Изборът на системна конфигурация в зависимост от изискванията на приложението може да доведе до подобряване на надеждността и готовността на системата.

ОРС с настройваема надеждност е симулирана за по-голяма интензивност на постоянните неизправности, за да се провери дали разпределението на излишъка влияе по различен начин върху нейната надеждност (*Фигура 3-35*). В сравнение с надеждността на системи при $\lambda_p=10^{-4}$ 1/h (*Фигура 3-33*) надеждността при $\lambda_p=10^{-3}$ 1/h е подобна и изследваните системи са подредени по същия начин според тяхната надеждност (*Фигура 3-35*).



Фигура 3-35. Надеждност на системи с различно разпределение на структурния излишък, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

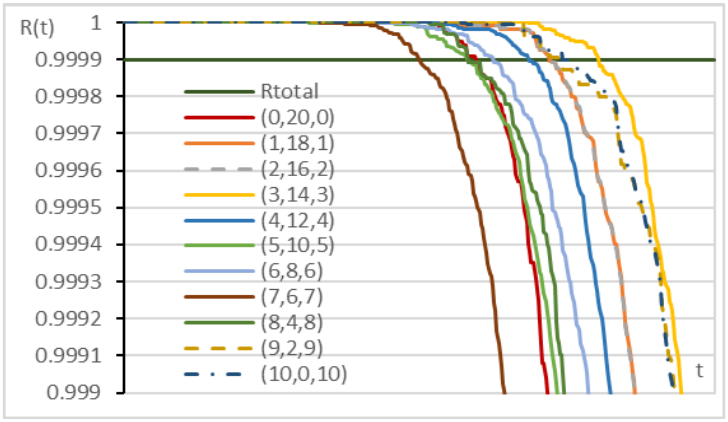
3.3 Подход на настройваема надеждност

Критичните за безопасността приложения изискват много висока надеждност, за да предоставят гарантоспособната услуга, за която са предназначени. При проектирането им се задава желаната системна надеждност и останалите ѝ характеристики се съобразяват с това изискване. Изследването на отказоустойчивата система с настройваема надеждност е разширено, за да може в повече дълбочина да се проследи нейното поведение и да се предложат възможности за постигане на висока желана надеждност. В представения дисертационен труд тази надеждност се нарича *обща надеждност* и се означава с R_{total}. Въз основа на изследванията, представени в т. 3.2.2 и 3.2.3 и [75], [76], е разработен подход на настройваема надеждност за определяне на системите, които постигат R_{total}.

R_{total} се определя при задаването на спецификациите на проектираната система според изискванията на приложението. По време на проектирането се дефинират режимите на неизправност и отказ, коефициентите на покритие на средствата за самопроверка, *MTTF*, *MTTR* и т.н. Определят се λ_p, μ_p, μ_{sys}, време на живот/мисия и R_{total}. При дадена R_{total} се определят и изследват всички възможни разпределения на модулния излишък, *система (i, j, k)*, за *N* компонента и *M* модула. Системите (i, j, k), т.е. системните конфигурации, се симулират, както е описано в т. 3.1, и се получават техните графики на надеждността във функция от времето. Надеждността на всяка конфигурация R_d се сравнява с R_{total}. След това се определят системите с $R_d(t) \geq R_{total}$. За всяка система се определя и периодът на висока надеждност.

Резултатите за системите, описани в т. 3.2.2 и 3.2.3, са показани на *Фигура 3-36* за R_{total}=0.9999 за система с N=20. Всички изследвани разпределения на структурния излишък постигат R_{total}, но поддържат тази надеждност за различни периоди. Резултатите от симулирането показват взаимоотношението между общата надеждност и разпределението на структурния излишък и илюстрират подхода на настройваема надеждност.

Система (3,14,3) има най-висока надеждност (жълтата крива на *Фигура 3-36*), следвана от система (10,0,10) (тъмно синята крива на *Фигура 3-36*) и система (1,18,1) (оранжевата крива на *Фигура 3-36*). Системата, изградена само от дублирани компоненти, система (0,20,0), има най-ниска надеждност (червената крива на *Фигура 3-36*). Разпределението на излишъка в компонентите на системата влияе върху системната надеждност (*Фигура 3-33, Фигура 3-35* и *Фигура 3-36*). Общата надеждност е по-висока за някои разпределения на структурния излишък, например система (3,14,3) (жълтата крива на *Фигура 3-36*), система (1,18,1) (оранжевата крива) и система (10,0,10) (тъмно синята крива), и е по-ниска за други, като система (7,6,7) (кафявата крива), система (5,10,5) (светло зелената крива) и (6,8,6) (светло синята крива на *Фигура 3-36*).



Фигура 3-36. Постигане на надеждност R_{total}=0.9999, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}$=0.1 1/h

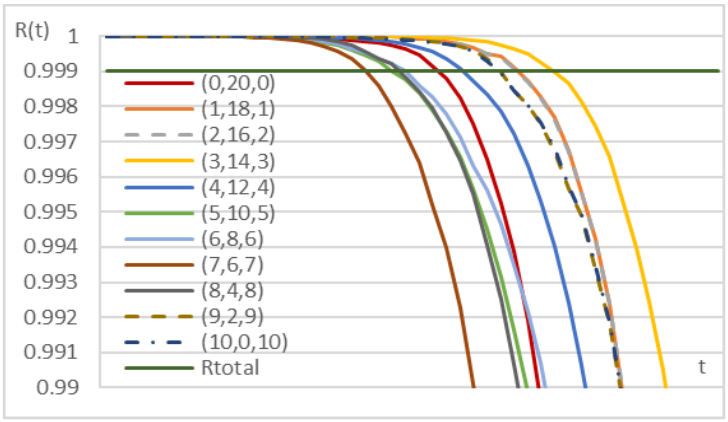
Не може да се изведе ясна зависимост между разпределението на излишъка и системната надеждност. Ако броят на компонентите с коефициент на покритие C_3 (т.е. с ТМИ) е по-голям от броя на компонентите с коефициент на покритие C_2 (т.е. с ДМИ), това не означава непременно, че системната надеждност ще се повиши. Въвеждането на единични компоненти, от друга страна, не води до значително намаляване на системната надеждност. В някои случаи, например система (10,0,10) (тъмно синята крива на *Фигура 3-36*), надеждността е по-добра отколкото при системи с по-малък брой единични компоненти, като система (6,8,6) (светло синята крива на *Фигура 3-36*).

Таблица 3-3 показва периодите, през които надеждността R_d на всяка от системите с настройваема надеждност надвишава R_{total}=0.9999, като се започва от системата с най-дълъг период. Системата (3,14,3) поддържа своята надеждност над R_{total} за най-дълъг период от време в сравнение с останалите системи. Система (0,20,0) без настройваема надеждност има сравнително по-кратък период на надеждност над R_{total}=0.9999.

Таблица 3-3. Периоди на работа на системи (i, j, k) с надеждност $R_d \geq R_{total}=0.9999$, $\lambda_p=10^{-4}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h, N=20

Система	$R_d \geq R_{total}$	Време [h]
(3,14,3)	0.999902	32300
(9,2,9)	0.999904	29800
(10,0,10)	0.999922	29800
(1,18,1)	0.999905	28900
(2,16,2)	0.999909	28900
(4,12,4)	0.999902	27500
(6,8,6)	0.999907	25100
(0,20,0)	0.9999	24000
(8,4,8)	0.999912	23400
(5,10,5)	0.999902	23400
(7,6,7)	0.999903	20100

При симулиране на системите за $\lambda_p=10^{-3}$ 1/h (*Фигура 3-37*) подреждането на графиките на надеждността на различните конфигурации на системата е приблизително същото като при интензивност на неизправностите $\lambda_p=10^{-4}$ 1/h (*Фигура 3-36*). Отново най-висока надеждност има система (3,14,3) (жълтата крива на *Фигура 3-37*), а най-ниска – система (7,6,7) (кафявата крива на *Фигура 3-37*). Системата без настройваема надеждност (0,20,0) (червената крива на *Фигура 3-37*) показва средна надеждност.



Фигура 3-37. Постигане на надеждност $R_{total}=0.999$, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h

Периодите на работа на конфигурациите с надеждност $R_{total} \geq 0.999$ за $\lambda_p=10^{-3}$ 1/h са показани в *Таблица 3-4*. Както личи и от графиките на *Фигура 3-37*, система (3,14,3) най-дълго поддържа желаната надеждност R_{total}, а най-кратък е периодът за система (7,6,7). Система (0,20,0) без настройваема надеждност има сравнително по-кратък период на поддържане на R_{total} в сравнение с повечето от останалите системи.

Таблица 3-4. Периоди на работа на системи *(i, j, k)* с надеждност $R_d \geq R_{total}=0.999$, $\lambda_p=10^{-3}$ 1/h, $\mu_p=\mu_{sys}=0.1$ 1/h, *N*=20

Система	$R_d \geq R_{total}$	Време [h]
(3,14,3)	0.999242	3300
(1,18,1)	0.9991	3100
(2,16,2)	0.99908	3100

(9,2,9)	0.999357	2900
(10,0,10)	0.999295	2900
(4,12,4)	0.999098	2700
(0,20,0)	0.99914	2500
(6,8,6)	0.999004	2300
(5,10,5)	0.999022	2200
(8,4,8)	0.999212	2200
(7,6,7)	0.999035	2000

Резултатите от симулирането показват, че разпределянето на системните ресурси в зависимост от тяхната важност за приложението може да даде предимство за системната надеждност. Например, един съвременен автомобил е оборудван с реалновременни разпределени системи, които управляват различни блокове, като двигател, окачване, скоростна кутия, врати, седалки и др. Тези блокове на свой ред са подсистеми, състоящи се от други модули, които работят заедно в изпълнение на конкретна задача. Една такава подсистема може да използва подхода на настройваема надеждност, за да постигне надеждността, диктувана от приложението. Определяйки R_{total} и знаейки броя на компонентите в подсистемата и техните надеждностни характеристики, могат да бъдат изведени и симулирани разпределенията на структурния излишък, за да се сравни тяхната надеждност. По този начин може по-нататък да се изследва и разработи модулното разпределение с най-висока надеждност, отчитайки особеностите на проектираната подсистема.

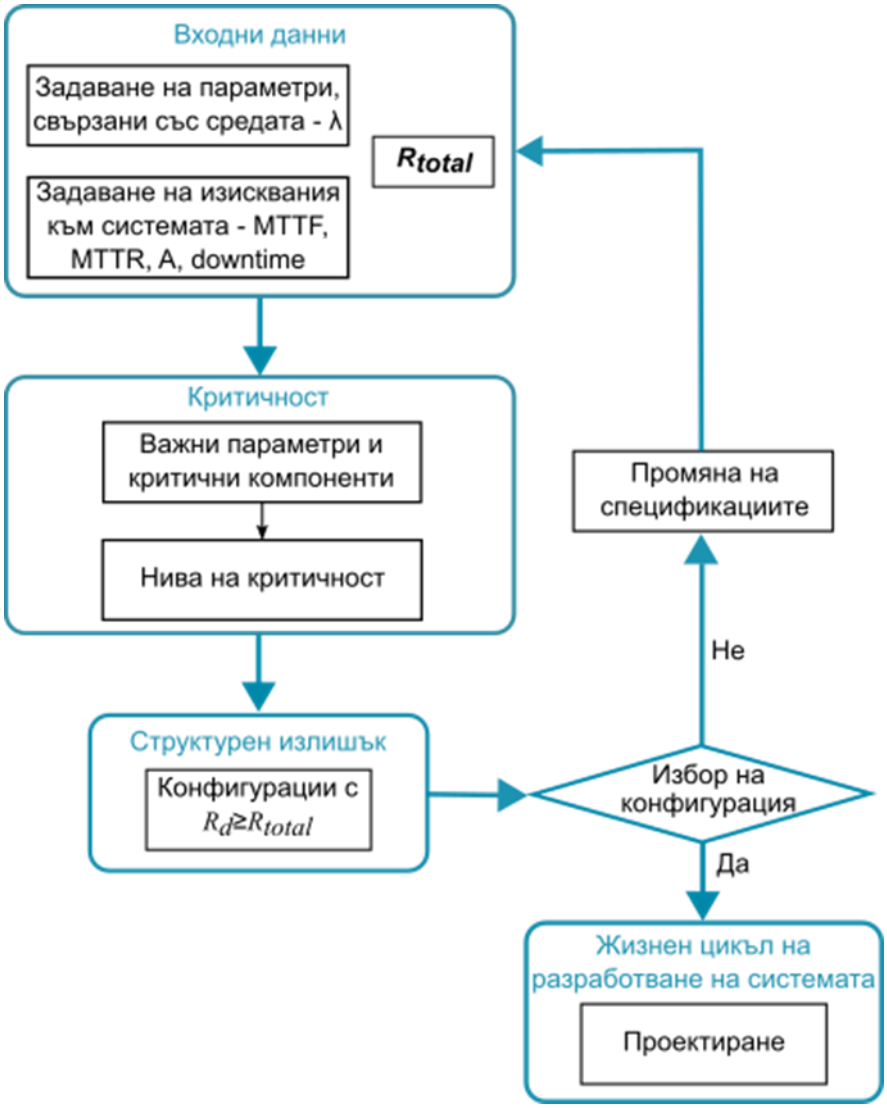
Представените резултати от симулационното моделиране (т. 3.2) показват, че има разпределения на структурния излишък, при които системата с настройваема надеждност постига по-висока надеждност R_{total} и я поддържа за по-дълъг период от време в сравнение със система без настройване на надеждността (*Фигура 3-36* и *Таблица 3-3, Фигура 3-37* и *Таблица 3-4*). При какви условия се случва това обаче е трудно да се установи, тъй като няма ясна зависимост между системната надеждност и разпределението на излишъка. Затова в дисертационния труд се предлага *подход на настройваема надеждност*, чрез който да се определят конфигурациите на структурния излишък, удовлетворяващи изискването за системна надеждност на приложението.

Подходът на настройваема надеждност може да се опише със следните действия:

1. Задаване на R_{total},
2. Задаване на параметрите, описващи средата – интензивност на неизправностите,
3. Задаване на изискванията към системата – средно време до отказ, средно време до ремонт, готовност, средно време на престой, възможности за локален и системен ремонт и съответно интензивности на локалните и системните ремонти,
4. Определяне на важните контролирани параметри и на критичните компоненти,

5. Определяне на нивата на критичност,
6. Извеждане на системните конфигурации, при които настройваемата надеждност е равна или по-голяма от изискваната обща надеждност R_{total},
7. Проверка коя от възможните конфигурации отговаря най-добре на изискванията на приложението,
8. При липса на подходяща конфигурация се променят входните спецификации и процедурата се повтаря.

Описаните действия са онагледени на *Фигура 3-38*.



Фигура 3-38. Описание на подхода на настройваема надеждност

Ако повече от възможните конфигурации на системата с настройваема надеждност изпълняват изискването за системна надеждност при зададените спецификации, подходящата за приложението конфигурация може да се избере според допълнителни критерии, като брой единични, дублирани или триплирани компоненти, желани нива на критичност, най-висока обща надеждност, най-голям период с висока обща надеждност и т.н. Ако нито една

конфигурация на системата с настройваема надеждност не удовлетворява изискването за R_{total} на приложението, е необходимо да се преразгледат системните спецификации, включително и изискването за обща надеждност.

3.4 Изводи и резултати

В *Глава 3* е представена симулационната програма, разработена според изискванията в т. 3.1.1. Представени са основната структура и блоковата схема на програмата.

Изследван е компонент на отказоустойчивата система с настройваема надеждност в зависимост от коефициента на покритие на блока за самопроверка C и коефициента на възстановяване от случайна неизправност C_r. Симулирани са компоненти с двоен и троен модулен излишък при работа с и без локален ремонт. Оценено е влиянието на C и C_r върху надеждността на компонентите, тяхната готовност, *MTTF, MTTS, MTBF, MTBS* и средното време за престой.

Според предвидения изследователски протокол са проведени експерименти за системи с различен брой компоненти (N=10 и N=20), различна интензивност на постоянните неизправности λ_p и различни стойности на коефициентите на покритие C_1, C_2 и C_3. Получени са данни за: $R(t)$, *A, MTTF, MTTR, MTTS, downtime*. Определени са възможните разпределения на структурния излишък при зададените N и M. Изследвано е влиянието на броя компоненти, коефициентите на покритие и интензивността на неизправностите върху надеждностните характеристики на отказоустойчивата система с настройваема надеждност и на системи без разпределение на структурния излишък. Определени са конфигурациите на системата, удовлетворяващи изискването за обща надеждност.

Създаден и представен е авторски подход на настройваема надеждност, чрез който да се определя кои разпределения на излишъка в компонентите удовлетворяват желаната обща системна надеждност. Въз основа на изискванията на приложението подходът намира системните конфигурации, които могат да постигнат общата надеждност.

Налага се изводът, че може да се постигне висока надеждност чрез разпределение на структурния излишък, като в някои случаи тя надвишава надеждността на системи без разпределение на излишъка. Конфигурациите, при които това е изпълнено могат да бъдат определени чрез подхода на настройваема надеждност.

Постигнатите резултати имат научно-приложен и приложен характер. Научно-приложни са разработването на симулационна програма за моделиране на гарантоспособни разпределени системи и формулирането на подход на настройваема надеждност. Приложните резултати са свързани с провеждане на експерименти със симулационната програма с цел да

се изследват надеждностните характеристики на отказоустойчива разпределена система с и без настройваема надеждност.

Чрез изследванията, представени в *Глава 3*, са изпълнени задачи 3 и 4 на дисертацията.

Глава 4. Обсъждане и анализ на резултатите

Гарантоспособните разпределени системи, които са обект на дисертацията, се разработват за приложения, които са критични по отношение на безопасността. Те се изграждат със специализирани или с готови компоненти, като и двата подхода имат своите предимства и недостатъци. Специализираните компоненти отразяват по-адекватно особеностите на приложението, дават възможност за постигане на висока надеждност с методи и техники, съобразени с конкретната работна среда и контекст на системата, и са добре верифицирани и валидирани. Това обаче изисква време и усилия, които имат своята цена. Такива системи се проектират и внедряват по-бавно, което, от една страна, ги прави твърде трудни за адаптиране към промени в средата на функциониране на системата и, от друга страна, оскъпява крайната им реализация.

Прилагането на готови компоненти скъсява периода между проектиране и внедряване на разпределената система и намалява цената. Той има недостатък, че внася допълнителни рискове за надеждността на системата. Готовите компоненти не дават гаранции за изпълнение на изискванията за отказоустойчивост. Затова се търсят методи и средства за компенсиране на ниската собствена надеждност на готовите компоненти.

Анализът на гарантоспособните разпределени системи от гледна точка на структурния излишък, направен в *Глава 1*, показва, че основните подходи за постигане на повече гъвкавост по отношение на изискванията на приложението са промяна на софтуерния структурен излишък (при статично разпределение на хардуерния структурен излишък) и въвеждане на нива на критичност.

Отказоустойчивата разпределена система с настройваема надеждност предлага и изследва подход, който да притежава гъвкавостта на гарантоспособните системи с готови компоненти, да отчита нивата на критичност на системите със смесена критичност, да дава възможности за настройване на надеждностни характеристики и в същото време да отговаря на изискванията за висока надеждност. Всички изброени видове системи реализират отказоустойчивостта си посредством структурен излишък. Те прилагат равномерно разпределен хардуерен излишък на компонентите и съобразяват с приложението разпределението на софтуерния структурен излишък. Предложената система с настройваема надеждност внася гъвкавост чрез разпределение на хардуерния структурен излишък.

При изграждане на идеята за ОРС с настройваема надеждност са взети под внимание концептуалният модел на подход за вземане на решения във връзка с гарантоспособността и класификацията на гарантоспособните разпределени системи според възможностите им за определяне на структурния излишък в зависимост от приложението. Предложената система е изградена от отказоустойчиви компоненти с различна степен на репликиране, която дава възможност да бъдат изследвани надеждностните характеристики на различни конфигурации на структурния излишък. Отказоустойчивостта на компонентите се определя от наличието на блок за самопроверка на всеки модул и средства за сравнение на неговите резултати. Представените Марковски вериги на ОРС с настройваема надеждност моделират поведението на системата при отсъствие или наличие на възможности за възстановяване на компонент и ремонт на системата. Тези модели стоят в основата на симулационната програма, чрез която са проведени експериментите в дисертацията. Избраният изследователски подход на симулационно моделиране предлага възможност за представяне на поведението на системата по отношение на неизправностите и отказите и изследване на нейните надеждностни характеристики, дефинирани в *Глава 2*, т. 2.1.2. Симулацията позволява моделиране на система с много компоненти и състояния и задаване на различни параметри за изследване на тяхното влияние върху системната надеждност.

Представените в *Глава 3* резултати от симулационното моделиране на отказоустойчивата система с настройваема надеждност показват, че изследваната система има добри надеждностни характеристики. Направен е анализ на резултатите, за да се провери дали се потвърждава хипотезата на дисертационния труд, а именно постига ли се висока надеждност и гъвкавост на системата чрез настройване на надеждността според изискванията на приложението.

При симулирането на компонент на системата са разгледани варианти на компонент с двоен и троен модулен излишък. Изследвано е влиянието на коефициента на покритие на блока за самопроверка и коефициента на възстановяване след случайна неизправност. Резултатите за надеждността, готовността, *MTTF, MTTR, MTTS, MTBF*, *MTBS* и времето за престой показват, че добавянето на блокове за самопроверка към всеки модул от компонента подобрява значително надеждностните характеристики на системата, особено когато тя работи без възможност за локален ремонт.

Симулационното моделиране на ОРС с настройваема надеждност с 10 компонента не очертава ясна зависимост между системната надеждност и разпределението на структурния излишък. От една страна, системата без настройваема надеждност (0,10,0) показва най-висока надеждност. От друга страна, при по-нисък коефициент на покритие C_2 някои конфигурации с разпределение на структурния излишък имат по-висока или близка до нейната надеждност.

Влиянието на C_1 върху надеждността е незначително. Коефициентите на покритие C_2 и C_3 подобряват значително общата надеждност на системата, което е логично, предвид по-голямата им стойност.

При ОРС с настройваема надеждност с 20 компонента най-висока надеждност показва системата (3,14,3). Най-ниска надеждност има система (7,6,7). Конфигурациите с малко единични и малко триплирани компоненти, като (1,8,1), (2,16,2) и (3,14,3), имат сравнително висока надеждност. Увеличаването на броя на триплираните компоненти може да повиши надеждността, но това не е валидно във всички случаи.

Изследванията при по-висока интензивност на неизправностите $\lambda_p=10^{-3}$ 1/h показват, че някои системи с настройваема надеждност са по-подходящи за работа при такива условия. Системи (1,18,1) и (2,16,2) имат втората по големина надеждност, докато при интензивност $\lambda_p=10^{-4}$ 1/h имат по-ниска надеждност. По-добре работи при висока интензивност и системата без настройваема надеждност (0,20,0). Това поведение на изследваните системи предполага гъвкавост при избора на подходяща система за конкретно приложение.

Системите с най-висока обща надеждност имат и най-дълги периоди, през които я поддържат. Това е мярка за тяхната готовност. Ако този показател е важен за приложението, той трябва да се вземе под внимание при избора на конфигурация с настройваема надеждност.

При проведените симулационни изследвания за N=10 и N=20 различните конфигурации на системата с настройваема надеждност не показват постоянно поведение. Надеждността им се влияе от броя на компонентите, интензивността на постоянните неизправности, коефициентите на покритие на средствата за самопроверка. При някои конфигурации общата надеждност е по-висока от тази на система без настройваема надеждност, при други не е. За да се определи подходящата конфигурация на ОРС с настройваема надеждност според изискванията на приложението, е създаден подход на настройваема надеждност. Той предвижда последователност от действия за избор на разпределение на структурния излишък в зависимост от изискването за обща системна надеждност на приложението. Подходът определя всички системни конфигурации, които постигат желаната надеждност, и представя възможност за избор на онази, която в най-голяма степен удовлетворява зададените системни спецификации.

От направените експерименти със симулационната програма могат да се направят няколко извода. Конфигурациите с настройваема надеждност постигат висока системна надеждност, съпоставима и в някои случаи по-висока от тази на системи без разпределение на структурния излишък. Подходът на настройваема надеждност определя системните конфигурации, които най-добре изпълняват изискването за обща системна надеждност на приложението. Това дава гъвкавост при проектирането на отказоустойчиви разпределени

системи да бъде избрано разпределение на структурния излишък, което най-добре отразява нуждите на конкретната реализация.

Тези изводи потвърждават хипотезата на дисертационния труд, че може да се постигне гъвкавост и висока надеждност на отказоустойчивите разпределени системи чрез разпределение на хардуерния структурен излишък според изискванията на приложението.

4.1 Изводи и резултати

Направено е обсъждане и анализ на резултатите, представени в дисертационния труд и на тази основа те са групирани, както следва:

Научни резултати:

1. Представен е нов архитектурен модел на отказоустойчива разпределена система с настройваема надеждност, като са дефинирани изискванията към нейните компоненти и системата като цяло;
2. Създаден е симулационен модел на предложената отказоустойчива разпределена система с настройваема надеждност;
3. Предложен е синтез на класификация и класификация на гарантоспособни разпределени системи със структурен излишък.

Научно-приложни резултати:

1. Създаден е концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност;
2. Формулиран е подход на настройваема надеждност;
3. Разработена е симулационна програма, реализираща метода за симулационно моделиране на гарантоспособни разпределени системи.

Приложни резултати:

1. Създадената симулационна програма може да се използва за моделиране и изследване на надеждностните характеристики и на други отказоустойчиви системи. С нея може да се изследва влиянието и на случайни хардуерни неизправности.

Получените в дисертационното изследване резултати показват, че поставените задачи са изпълнени.

Приложните резултати доказват твърденията, поддържащи научната хипотеза на дисертацията: Може да се постигне висока надеждност и гъвкавост на разпределението на системните ресурси посредством настройваема надеждност, реализирана с разпределение на хардуерния структурен излишък. Това се доказва със следните резултати:

1. Представената отказоустойчива разпределена система с настройваема надеждност постига висока обща надеждност, съпоставима с надеждността на системи без разпределение на структурния излишък.
2. Отказоустойчивата разпределена система с настройваема надеждност има конфигурации на разпределението на структурния излишък, които притежават по-добри надеждностни характеристики от тези на системи без разпределение на структурния излишък.
3. Подходът на настройваема надеждност дава възможност за определяне на конфигурациите на структурния излишък, които удовлетворяват изискването за обща надеждност на приложението.

Заключение и бъдеща работа

В дисертационния труд са изследвани надеждностните характеристики на отказоустойчива разпределена система с настройваема надеждност. Системата е предложена като възможност за постигане на гъвкавост в проектирането на гарантоспособни разпределени системи. При направения обзор на гарантоспособни разпределени системи за работа в реално време са очертани две основни направления на изграждане на такива системи – с използване на специализирани компоненти и с използване на готови компоненти. Системите и от двата вида постигат отказоустойчивост посредством разнообразни начини за въвеждане на излишък. Прилагат се структурен, времеви и функционален излишък. Структурният излишък добавя хардуерни и софтуерни елементи към системната архитектура. Най-често той се реализира като еднакво репликирани хардуерни компоненти, които изпълняват различно репликирани софтуерни задачи.

В дисертационния труд е разработен концептуален модел на подход за вземане на решение при осигуряване на гарантоспособност и е направен синтез на класификацията на гарантоспособни разпределени системи на базата на модела за разработване на системи.

Предложени са авторска архитектура и модел на отказоустойчива разпределена система за работа в реално време, наречена от автора система с настройваема надеждност. Тя предлага настройване на хардуерния структурен излишък за постигане на обща надеждност според изискванията на приложението. Системата е изследвана посредством метода на симулационно моделиране.

Проектиран и създаден е програмен продукт за симулационно моделиране на отказоустойчиви системи. Той реализира създадения модел на системата с настройваема надеждност. В резултат от изпълнението му се получава функция на надеждността, както и

данни за надеждностните характеристики на системата. Симулационният продукт е написан на език за програмиране C++ и с него могат да се изследват отказоустойчиви системи с и без разпределение на структурния излишък.

Резултатите от проведените експерименти показват добра обща надеждност на системата с настройваема надеждност. Съществуват разпределения на структурния излишък, при които системната надеждност е по-висока от тази на система с равномерно разпределен излишък. При някои от конфигурациите се наблюдава стохастично подреждане, т.е. кривите на надеждността не се пресичат, което означава, че изборът на архитектурно решение не зависи от съответните стойности на коефициентите на покритие. Има случаи, при които различните архитектурни решения са неразличими, и други, при които не се наблюдава стохастично подреждане. Това прави избора на конкретно инженерно решение не очевиден и зависим от по-задълбоченото познаване на стойностите на коефициентите на покритие. Разликите във функцията на надеждността на изследваните конфигурации показват, че при проектиране на системата трябва да се използват средства, които да дадат количествена оценка на вариантите на разпределение на структурния излишък, за да бъде избрано най-подходящото за приложението решение.

Това мотивира и създаването от автора на подход, наречен подход на настройваема надеждност, който определя при какви конфигурации на структурния излишък системата постига надеждността, изисквана от приложението.

Получените при моделирането на отказоустойчивата разпределена система с настройваема надеждност резултати показват, че системата има предимства по отношение на разпределянето на структурния излишък според изискванията на приложението, които могат да се използват при проектирането на гарантоспособни разпределени системи. Настройваемата надеждност е подходяща за използване в системи със смесена критичност на компонентите, в компактни системи, където множество възли са разположени в ограничено пространство, в системи с високи изисквания за надеждност, които позволяват работа с готови компоненти и др. под. Програмният продукт за симулационно моделиране на отказоустойчиви системи с разпределение на структурния излишък може да се използва и за моделиране на други гарантоспособни разпределени системи с добавяне на модули, които описват техните характеристики.

Насоки за бъдеща работа

Отказоустойчивата система с настройваема надеждност може да се изследва за различни приложения, изискващи нива на критичност, висока надеждност и разпределение на структурния излишък. Подходът на настройваема надеждност може да се усъвършенства, за да включва съобразяване и на други изисквания на приложението на гарантоспособни

разпределени системи. Моделът на отказоустойчивата разпределена система с настройваема надеждност може да се разшири за моделиране на софтуерна надеждност и изследване на ефекта на софтуерните неизправности върху отказоустойчивостта на системата. Подходът и моделът на настройваема надеждност могат да се приложат за конкретни системи.

Симулационната програма подлежи на усъвършенстване, като се ускори нейното изпълнение чрез прилагане на техники за паралелна обработка. В нея могат да се включат още блокове за изследване на влиянието на други фактори върху надеждностните характеристики на дадена система. Програмният продукт може да се развие и за изследване на други видове разпределени системи.

Списък на публикациите по дисертацията

1. Djambazova, E., & Andreev, R. (2023). Redundancy management in dependable distributed real-time systems. *Problems Of Engineering Cybernetics And Robotics*. (под печат)
2. Djambazova, E. (2022). Achieving system reliability using reliability adjustment. International Conference on Computer Systems and Technologies 2022 (CompSysTech ’22), Ruse, Bulgaria. ACM, NewYork, NY, USA, pp. 64-68. DOI: 10.1145/3546118.3546129. SJR(SCOPUS) 2020: 0,18
3. Djambazova, E. (2012). Adjusting reliability of a fault-tolerant distributed process control system – Preliminary results. International Conference “Automatics and Informatics 2012”, Sofia, Bulgaria, pp. 175-178.
4. Djambazova, E. (2009). Node reliability of a fault-tolerant distributed process control system – Simulation results. International Conference “Automatics and Informatics’ 2009”, Sofia, Bulgaria, pp. I-131 – I-134.
5. Джамбазов, К., & Ананиева, Е. (1995). Управляващи системи с модулно настройване на отказоустойчивостта. Национална конференция с международно участие „Автоматика и информатика ‘95”, София, стр. 247-250.

Участие в проекти

Част от разработките са включени в работата по два национални проекта:

1. Моделиране и изследване на интелигентни системи за обучение и сензорни мрежи“ (ИСОСеМ) – Договор № КП-06-Н 47/4 от 2020 г., финансиран от ФНИ (текущ).
2. Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТ в НОС) – Д01-205/2018 г., финансиран от МОН.

Основни научни и научно-приложни резултати

Научни резултати:

1. Предложен е нов архитектурен модел на отказоустойчива разпределена система с настройваема надеждност.
2. Създаден е симулационен модел на отказоустойчива разпределена система с настройваема надеждност.
3. Синтезирана е класификация на гарантоспособни разпределени системи според възможностите им за определяне на структурния излишък в зависимост от приложението.

Научно-приложни резултати:

4. Направен е критичен анализ на гарантоспособни разпределени системи, на базата на който е разработен концептуален модел на подход за вземане на решения при осигуряване на гарантоспособност.
5. Идентифицирани са основните направления на управление на структурния излишък в гарантоспособни разпределени системи и са очертани изследователски възможности.
6. Проектиран и реализаран е софтуерен продукт за симулационно моделиране на изследваната система.
7. След сравнителен анализ на отказоустойчивата система с настройваема надеждност със системи без разпределение на структурния излишък е разработен и приложен подход на настройваема надеждност.

Приложни резултати:

8. Създадената симулационна програма може да се използва за моделиране и изследване на надеждностните характеристики и на други отказоустойчиви системи. С нея може да се изследва влиянието и на случайни хардуерни неизправности.