РЕЦЕНЗИЯ НА ДОКТОРСКА ДИСЕРТАЦИЯ

Автор: **Едита Джамбазова**
Тема: **Изследване на надеждностните характеристики на отказоустойчива разпределена система за работа в реално време с настройваема надеждност**

Професионално направление: 5.3 Комуникационна и компютърна техника
Докторска програма: „Компютърни системи, комплекси и мрежи“
Консултант: доц. д-р Румен Андреев

Рецензент: доц. д-р Петър Попов
Месторабота: катедра „Computer Science“,
City, University of London, United Kingdom

Основание: Заповед No. 191 / 20.07.2023 на директора на ИИКТ – БАН.

1. ОБЩО ОПИСАНИЕ НА ДИСЕРТАЦИЯТА

1.1. Структура и обем

Дисертацията се състои от 134 страници текст, 6 страници библиография и 2 приложения с общ обем от 20 страници и съдържа: увод, 4 глави, заключение с резюме на получените резултати и дискусия на бъдещите изследвания, декларация за оригиналност и библиография.

Структурата и обемът да дисертацията представят много ясно идеите и търсенията на автора. Текстът логично преминава от детайлно представяне на гарантоспособността и системите за реално време, като две свързани и добре установени научни дисциплини, през обосновка на целите на изследване, резултатите от изследванията, които включват нов подход за създаване на отказоустойчива разпределена система за управление в реално време с настройваема надеждност и методика за количествена оценка на надеждността на разпределени системи за управление в реално време, изградени с компоненти с различни нива на структурен излишък.

Структурата на дисертационния труд съответства на изискванията на Закона за развитие на академичния състав в Република България (ЗРАСРБ) и Правилника за неговото прилагане (ППЗ) а също така на изискванията към такива документи във Великобритания и няколко европейски страни (напр. Испания, Норвегия, Италия), с които съм запознат.

Уводът на дисертацията представя:

- Мотивацията за проведеното изследване. Многоканалните отказоустойчиви системи за обработка се изграждат с помощта на излишък (дублиране/триплиране и т.н.), което води до допълнителни закъснения, необходими за синхронизацията на каналите на отказоустойчивата система. Изискванията за обработка в реално време, от друга страна, налагат ограничения на времето за обработка и генериране на управляващо въздействие към обекта за управление. Разрешаването на тези две изисквания едновременно – отказоустойчивост, която не води до нарушаване на времевите ограничения – е сериозно предизвикателство, и е основна мотивация за проведените изследвания.
- Научна постановка на изследването, което включва:
    - Предмет на изследване

- Цел на изследването
- Работна хипотеза, която е прецизирана в няколко твърдения (research questions), за които се търси потвърждение с проведените изследвания.
- Методология за изследване
- Основни задачи на изследване.

В *първа глава* се прави обзор на терминологията, използвана в специализираната литература, посветена на гарантоспособността на компютърните системи за управление в реално време на индустриални системи. Значителна част в главата е отделена на различните методи за повишаване надеждността чрез въвеждане на излишък – структурен/функционален и времеви – и създаване на отказоустойчиви системи за управление.

Втората глава е посветена на детайлно моделиране на отказоустойчива разпределена система за управление в реално време. Представен е подробен модел на разпределената система, мотивирани са модел на компоненти с излишък и са описани надеждностните характеристики на системата. Представени са и допусканията, направени при моделирането.

Третата глава е централна в дисертацията и представя резултатите, получени чрез симулиране работата на система с помощта на специализиран софтуер за симулационно моделиране, разработен от кандидата. Ползата от предложения метод за настройваема надеждност е илюстрирана убедително (повече подробности са предоставени по-долу).

Четвъртата глава обобщава резултатите от проведените изследвания.

1.2. Актуалност на темата

Актуалността на темата не буди никакви съмнения. Разпределените системи за обработка в реално време се използват много широко в различни индустриални приложения. Системите за критични приложения (safety-critical applications) в атомната енергетика, критичните инфраструктури (енергетика, телекомуникации и т.н.), интелигентните системи (роботика, автономни автомобили и т.н.) са примери, където се изисква висока надеждност на управление в реално време. Не всички функции в такива системи за управление обаче са еднакво критични. При тези условия става възможно да се търси висока надеждност чрез отказоустойчивост само за онези "критични функции", които влияят съществено на системната надеждност. За системи със съществена сложност (напр. с много компоненти), определянето на критичните функции може да *не е очевидно*, особено в случаите, когато излишък може да бъде присвоен само на някои компоненти на системата. В такива случаи разработчиците се сблъскват със сериозен проблем как да разпределят наличните ресурси (т.е. наличните модули) по начин, който води до най-висока системна надеждност. Този проблем не може да бъде решен без използване на методи за количествена оценка на алтернативите. Предложената методика за количествена оценка на надеждността и разработеният софтуер за симулационно моделиране и оценка на системната надеждност са съществени приноси към решаването на проблема за оптимално разпределение на излишъка между компонентите на системата.

Дисертацията съдържа 49 фигури и 4 таблици, които представят резултатите на проведените изследвания.

1.3. Метод на изследване

Дисертацията показва убедително, че г-жа Джамбазова има траен интерес към гарантоспособните системи за управление в реално време, демонстрира умение да формулира съществен изследователски проблем, да разработва и използва стохастични модели при оценка надеждността на системи за управление със сложна структура.

1.4. Използвана литература

102 литературни източника са използвани в дисертацията[1]. Те покриват добре темите гарантоспособност, отказоустойчивост и системи за реално време. Цитираните източници, свързани със стохастичното моделиране, са също достатъчни.

Повечето от литературните източници са на английски език, което показва отлично познаване на водещия международен опит.

Около половината от цитираните литературни източниците са публикувани през новия век, съществена част са от последните 5 години.

Всички източници са описани според официалните изисквания и са цитирани в текста коректно и според правилата.

2. РЕЗУЛТАТИ И ПРИНОСИ

Дисертацията е изцяло теоретично ориентирана. Оригиналните резултати са представени в Глава 2 и Глава 3.

Авторефератът представя работата и постигнатите резултати добре.

Най-съществените резултати от работата са представени в Глава 3. Например, Фигура 3-37 (на стр. 90 на дисертацията) и следващите графики, показващи резултатите от изследванията на система с 20 модула, илюстрират убедително полезността на предложената методика за количествена оценка на различни конфигурации при зададен общ брой модули, което позволява адекватно сравнение на алтернативните конфигурации. Графиките на системната надеждност показват, че отсъства "стохастично подреждане" (stochastic ordering) между надеждността на различните конфигурации, което пък свидетелства за това, че коя от възможните конфигурации предлага най-добра надеждност зависи не само от конфигурацията и как излишъкът е разпределен между компонентите на системата, но също така и от времевия интервал, за който се оценява системната надеждност и се прави сравнение на възможните конфигурации.

Г-жа Джамбазова посочва, че дисертацията е довела до 3 научни резултата, 4 научно-приложни резултата и 1 приложен резултат (симулационна програма), твърдения които приемам.

Бих желал да подчертая като особено съществена демонстрацията, че отсъства стохастично подреждане между различните конфигурации, създадени при зададен брой модули. Този резултат изключва възможността да се определи "оптимална конфигурация", която би гарантирала най-добра системна надеждност при зададен общ брой модули и компоненти, *независимо от времевия интервал, за който се оценява надеждността*. На практика този резултат показва, че проектиране на разпределена система за управление при зададено ниво на системен излишък трябва да включва анализ, подобен на този който е предложен в дисертацията,

3. ОЦЕНКА НА ПУБЛИКАЦИИТЕ И АВТОРЕФЕРАТА

Изследванията на г-жа Джамбазова са довели до 5 публикации и включване на резултатите в 2 научни отчета (по проекти с външно финансиране).

Прави впечатление, че публикациите са направени в продължение на продължителен период от време, което демонстрира, че авторът има дълготрайни изследователски интереси по

[1] [40] и [41] изглеждат идентични.

темата[2].

40% от публикациите са написани от двама автори, от които една е съвместна работа на докторанта с д-р Джамбазов и една – с научния ръководител/консултант доц. д-р Андреев.

Авторефератът обобщава точно и ясно (в рамките на 49 страници) основните идеи на автора. Постиженията на дисертацията, а също и насоките за работа в бъдеще, са представени точно.

4. БЕЛЕЖКИ, ВЪПРОСИ И ПРЕПОРЪКИ

Като се има предвид, че изследването е фокусирано върху настройваема *хардуерна гарантоспособност*, би било интересно предложената методика да бъде разширена и да отчете влиянието на софтуерните откази. Тази възможност се сочи в дисертацията като едно от направленията за бъдещи изследвания.

4.1. Необходими корекции

Смятам, че следните корекции на текста на дисертацията са ***необходими***:

1. (p.66) "Допуска се, че .... времената до отказ са нормално разпределени".

   С: Смятам, че това допускане не е необходимо и би следвало текстът да се коригира.

   > Стохастичният модел е напълно дефиниран от структурата на модела и параметрите (интензивности на отказ и възстановяване). Времената то настъпване на системен отказ (т.е. достигане на абсорбиращото състояние на системен отказ) може да бъде изчислено чрез "решаване" на модела, например с използване на симулиране или на подходящи числени методи. Асимптотично разпределението на това време е *експоненциално* (see Littlewood's work from 1979[3] for the class of models semi-Markov models).

2. (p. 71) "Тъй като размерът ѝ е голям (над 40 според изискванията на статистическите пресмятания; в нашия случай размерът на генералната съвкупност е 10^5), според централната гранична теорема [37], [100], [101] може да се допусне нормално разпределение на генералната съвкупност [99]".

   С: това твърдение се нуждае от пояснение. Не става ясно как се формира "генералната съвкупност". От времена до системен отказ или от нещо друго? Уточненията са необходими, за да стане ясно към какво се прилага централната пределна теорема.

   > Централната пределна теорема (ЦПТ) се прилага към разпределението на средното значение на случайна величина, за която съществува статистическа извадка. ЦПТ е приложима към случайни величини с произволно разпределение.

3. (p. 71) "Надеждността се изчислява в зависимост от времената до отказ и можем да допуснем..."

   С: Това твърдение създава впечатление, че системната надеждност зависи от MTBF and MTTR, но не става ясно дали това са параметрите на компонентите.

   > Системната надеждност разбира се зависи от MTBF and MTTR на компонентите, но би могла да се изчисли директно, например като се използват ефективни числени методи при дефинирана матрица на преходите на Марковска верига с непрекъснато време (continuous-time Markov chain). Предполагам, че текстът е опит да се покаже, че

[2] В потвърждение на това твърдение бих желал да посоча и това, че списъкът на литературни източници включва и други публикации на г-жа Джамбазова, направени през годините в съавторство или самостоятелно.

[3] B. Littlewood, *Software reliability model for modular program structure.* IEEE Trans Reliability, 1979. **28**(3): p. 241-246.

параметрите на модела са всъщност свързани с MTBF and MTTR на модулите/компонентите използвани в модела.

4. (p. 80+) Координатите на фигурите в секция 3.2.2 не са напълно дефинирани. Трябва да се добавят значенията, за които са изчислени значенията на системната надеждност, показани на графиките.

   С: Пропуснатите етикети на оста X трябва да се добавят. Предполагам, че интервалът на значенията ще бъде [0, 10^5] часа.

4.2. Въпроси по дисертацията

Бих искал, по време на защитата да чуя отговори на следните ***въпроси***:

1. (p. 19) Дисертацията включва следните две твърдения:
   a. "Коректна услуга (correct service) се предоставя, когато услугата прилага системната функция". ...
   b. "Отказ в услугата настъпва или поради отклонението ѝ от функционалните спецификации, или защото спецификациите не описват адекватно системната функция".

   *Q. Бихте ли обяснили какво е **correct service**? Защо в дефиницията има препратка към **системна функция**? Не би ли било по-уместно да се използва препратка към (функционалните) изисквания (requirements)? Струва ми се, че има противоречие между двете твърдения цитирани по-горе. Бихте ли потвърдили, че това е наистина така?*

   Моите съмнения се свеждат до следните два аспекта:

   - отклонение на поведението на системата от функционалната спецификация (functional requirements) е наистина системен отказ, който би трябвало да бъде уставен чрез *верификация* на системата (напр. чрез тестиране) или чрез мониторинг по време на работата.

   - неправилно функциониране, което се дължи на неправилна функционална спецификация не би трябвало да се третира като системен отказ а като отказ в спецификацията, който би трябвало да бъде открит и отстранен чрез *валидиране* на спецификацията.

2. (p. 21) Дискутира се Fault – forecasting. В дисертацията се твърди, че фокусът на изследването е fault-tolerance.

   Q. Бих желал да чуя мнението на докторанта за връзката между fault-tolerance и fault-forecasting? По-специално, необходима ли е fault-forecasting при проектиране на системи с използване на fault-tolerance? Ако това е така, бих желал да чуя мнението на докторанта за характера на тази връзка/зависимост?

   Връзката между fault-tolerance и fault-forecasting присъстваха (неявно) на Fig. 1-3 (p.29) където forecasting (или по-общо assessment) е показана като интегрална част на fault tolerance. Би ли се съгласил кандидатът, че фокусът на предложената дисертация включва и "fault forecasting"?

3. (p.23) "Възлите са ***независими*** елементи, които комуникират помежду си по обща съобщителна среда".

Q: Би ли пояснил кандидатът в какъв смисъл възлите са независими? За стохастична независимост ли става въпрос (т.е. отказите възникват независимо) или за нещо друго?

4. (p.57) "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".

   Q: На какво се базира това допускане кога системата отказва? В теорията на надеждността, (напр., при използването на Reliability Block Diagrams, RBD), се използва понятието "structure function", която е булева функция определяща системното състояние ("работоспособно/отказ") като функция на състоянията ("работоспособно/отказ") на компонентите на системата. Не смята ли докторантът, че подобен подход бе бил уместен в дисертационния труд?

   > Structure function очевидно влияе на резултатите на оценка надеждността. "Structure function" на системи без излишък е булева функция AND, т.е. системата работи коректносамо когато всички компоненти са работоспособни. Когато се използват компоненти с резервиране, както е направено в дисертацията, structure function ще включва булеви OR(s).

5. (p. 61) "На изходите се поддържа безопасно управляващо въздействие (fail safe) ... Предимството на стоповото състояние е във възможността да се диагностицира по-лесно и бързо причината за отказ чрез информацията от средствата за самопроверка, което намалява времето за престой ".

   Q1: Би ли дал кандидатът примери за "fail safe" състояние на компонентно ниво?

   > Fail-safe състояние обикновено се дефинира на СИСТЕМНО ниво, напр. автономен автомобил (autonomous vehicle) спира. В дисертацията се предлага fail-stop състояние на ниво компонент. Това предполага, че в процеса на работа някои компоненти могат да спрат да изпращат управляващи въздействия към устройствата (actuators), които те управляват, докато останалите компоненти могат да продължат да изпращат управляващи сигнали. Би било полезно да се даде пример на система, в която такъв подход би бил полезен.

   Q2: Би ли дал кандидатът пример илюстриращ как self-checking би бил полезен във fail-safe състояние?

4.3. Препоръчителни корекции на текста на дисертацията

При рецензирането на работата си водих бележки за възможни подобрения на текста на дисертацията, които са представени по-долу като ***препоръки*** към г-жа Джамбазова. Не очаквам отговор на тези препоръки по време на защитата и оставям на нея да прецени дали да ги отчете при нова редакция на текста на дисертацията.

1. (p. 46) "Настройваемост е свойството на гарантоспособната разпределена система за реално време да разпределя структурния излишък ***според изискванията за надеждност на приложението***"

   R. Очевидно е, че на различните компоненти могат да бъдат реализирани с различен излишък. Остава неясно, обаче, как нуждите на приложението за повишена надеждност ще бъдат отчетени. Би било добре този аспект да бъде пояснен.

2. (p. 65) "Единичните компоненти имат най-малък коефициента на покритие – C1. Компонентите с двоен модулен излишък имат коефициент на покритие C2 > C1, а триплираните компоненти имат коефициент на покритие C3 > C2 > C1".

   R: Би било полезно да се поясни, че неравенствата посочени по-горе са просто допускания. Още по-добре би било, ако се добави и обосновка за правдоподобността на тези допускания.

3. (p.66) "...Определяне на времената до отказ (one of the outcomes from the studies)".

   R: Би било добре да се посочи, че се използва вероятностното разпределение (e.g., cumulative distribution function) на времето до настъпване на системен отказ.

   Би било също любопитно да се провери дали асимптотичния резултат на Littlewood (the time to failure is exponentially distributed) е в сила за проведените изследвания.

4. (p. 75) "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...."

   R: Възприетите значения на интензивностите на отказите/неизправностите са нереалистично високи. Това е направено са "удобство" – да се съкрати времето за симулация. Би било добре да се дискутират възможните side-effects, напр. някои от характеристиките на модела като неговата "stiffness" могат да бъдат засегнати.

5. Бих препоръчал списъкът на литературните източниците да бъде разделен на традиционните категории монографии, статии, доклади, и др.

5. ЗАКЛЮЧЕНИЕ

Дисертацията на тема "Изследване на надеждностните характеристики на отказоустойчива разпределена система за работа в реално време с настройваема надеждност", разработена от Едита Джамбазова под научното ръководство на доц. д-р Румен Андреев **отговаря на изискванията за присъждане на образователната и научна степен "доктор".**

Поради това изразявам положително становище и препоръчвам настойчиво на уважаемите членове на научното жури да гласуват „за".

На основание ЗЗЛД

5 септември 2023 г
Лондон

Рецензент:
доц.