НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Малиновський Михайло Леонідович

УДК 681.5:004.43

МЕТОДИ ТА ЗАСОБИ ПРОЕКТУВАННЯ ТЕХНІЧНИХ І ПРОГРАМНИХ КОМПОНЕНТІВ БЕЗПЕЧНИХ ПЛІС-КОНТРОЛЕРІВ З ПАРАЛЕЛЬНОЮ АРХІТЕКТУРОЮ

Спеціальність 05.13.05 – комп'ютерні системи та компоненти

Автореферат дисертації на здобуття наукового ступеня
доктора технічних наук

Харків – 2010

Дисертацією є рукопис.

Роботу виконано на кафедрі автоматизації та комп'ютерних технологій Харківського національного технічного університету сільського господарства ім. П. Василенка Міністерства аграрної політики України.

Науковий консультант – доктор технічних наук, професор
Фурман Ілля Олександрович,
Харківський національний технічний університет сільського господарства, завідувач кафедри автоматизації та комп'ютерних технологій

Офіційні опоненти: доктор технічних наук, професор
Дербунович Леонід Вікторович,
Національний технічний університет «Харківський політехнічний інститут», професор кафедри автоматики і управління в технічних системах

доктор технічних наук, професор
Ястребенецький Михайло Онисимович,
Державний науково-технічний центр з ядерної та радіаційної безпеки, м. Харків, начальник відділу аналізу безпеки керуючих та інформаційних систем АЕС

доктор технічних наук, професор
Романкевич Олексій Михайлович,
Національний технічний університет України «Київський політехнічний інститут», професор кафедри спеціалізованих комп'ютерних систем

Захист відбудеться "_24_" __червня__ 2010 р. о _14^{30}_ годині на засіданні спеціалізованої вченої ради Д 64.050.14 у Національному технічному університеті "Харківський політехнічний інститут" за адресою: 61002, м. Харків-2, вул. Фрунзе, 21.

З дисертацією можна ознайомитись у бібліотеці Національного технічного університету «Харківський політехнічний інститут» за адресою: 61002, м. Харків, вул. Фрунзе, 21.

Автореферат розісланий "_27_" ___квітня___ 2010 р.

Вчений секретар
спеціалізованої вченої ради _____ І. Г. Ліберг

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Запобігання техногенних катастроф є однією із глобальних проблем сучасності. Рішення даної проблеми в значній мірі залежить від досягнутого рівня функціональної безпеки технічних і програмних компонентів (ТПК), які використовуються у комп'ютерних системах критичного застосування (СКЗ). Сучасні концепції і підходи до створення ТПК СКЗ передбачають наявність трьох основних ознак, по яких можна класифікувати ці системи. До цих ознак відносяться: тип елементної бази (релейна або мікроелектронна), принцип дії (послідовний або паралельний), принцип досягнення безпеки (із застосуванням компонентів із симетричними або несиметричними відмовами).

Для побудови СКЗ широко використовуються релейно-контактні елементи з несиметричними відмовами, які, як показав багаторічний досвід їхньої експлуатації, дозволяють досягти надзвичайно високих показників безпеки (з імовірністю небезпечної відмови 10^{-13} 1/ч). З розвитком мікроелектронних технологій з'явилися СКЗ на основі мікропроцесорної (МП) техніки. Перші зразки мікропроцесорних СКЗ будувалися на МП-компонентах із симетричними відмовами - стандартних промислових контролерах. Безпека при цьому досягалася резервуванням на системному рівні. Наступним етапом розвитку теорії побудови СКЗ стала розробка методів і засобів побудови нового класу МП-компонентів, якім властиві несиметричні відмови, - безпечних промислових контролерів, що дозволило спростити структурну організацію і підвищити ефективність проектування програмного забезпечення для СКЗ.

Досвід масового використання МП-компонентів СКЗ виявив не тільки їхні явні переваги в порівнянні з релейними, але й істотні недоліки. Причинами низької ефективності МП-систем критичного застосування є складність методів синхронізації каналів, що резервуються, сполучення мікроелектронних структур з виконавчими механізмами, а також послідовний принцип обробки інформації, що обмежує можливості в частині підвищення швидкодії та вірогідності обробки інформації.

В останні роки спостерігається розвиток і усе більш широке застосування методів і засобів створення СКЗ на основі мікроелектронних компонентів паралельної дії із застосуванням програмованих логічних інтегральних схем (ПЛІС). Використання ПЛІС дало можливість підвищити швидкодію, надійність, вірогідність обробки інформації в СКЗ, але, так само як і у випадку використання МП-компонентів, не дозволило вирішити основну задачу: забезпечити функціональну безпеку на рівні релейних систем, у зв'язку із чим сучасні мікроелектронні системи в найбільш відповідальних вузлах дублюються релейно-контактними схемами, що гарантують реалізацію умов безпеки СКЗ.

Таким чином, сучасний етап розвитку теорії побудови комп'ютерних систем критичного застосування характеризується протиріччям, що складається у тому, що релейні системи, які масово застосовуються, морально і фізично застаріли та вимагають заміни, при цьому методи та ідеологія побудови

мікроелектронних і МП-компонентів і систем по багатьом важливим показникам, у тому числі показникам безпеки, уступають релейним.

У зв'язку з цим актуальним є вирішення науково-прикладної проблеми розробки та реалізації методів і засобів проектування технічних і програмних компонентів безпечних ПЛІС-контролерів з паралельною архітектурою та розв’язання таким чином протиріччя між існуючими методами побудови систем критичного застосування на елементах з симетричними та несиметричними відмовами, що визначило напрямок дисертаційних досліджень.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконувалися на кафедрі автоматизації та комп’ютерних технологій Харківського національного технічного університету сільського господарства імені Петра Василенка. Як науковий керівник здобувач очолював виконання господарського договору "Розробка, виготовлення та поставка дослідного зразку мікроелектронної системи централізації депо Московське Харківського метрополітену" (НПП Хартрон-Енерго, м. Харків), а також пошукових НДР за ініціативою Харківського національного технічного університету сільського господарства імені Петра Василенка: АіКТ-2 "Дослідження та розробка високоефективних мікроелектронних обчислювальних і керуючих пристроїв з нетрадиційною архітектурою" (ДР № 0104U005149), АіКТ-3 "Розробка програми та інтерфейсу технологічного візуального програмування мікропроцесорних керуючих засобів промислового призначення" (ДР № 0104U005151), АіКТ-5 "Розробка та дослідження логічних керуючих автоматів паралельної дії" (ДР № 0107U001629) і АіКТ-8 "Розробка трансляторів технологічних мов у стандартні мови програмування ПЛК" (ДР № 0107U001632).

Мета і задачі дослідження. Метою дослідження є підвищення показників безпеки систем критичного застосування шляхом розробки методів і засобів проектування технічних і програмних компонентів обробки інформації та формування керуючих впливів на основі безпечних ПЛІС-контролерів з паралельною архітектурою. Відповідно до зазначеної мети поставлено наступні задачі:

1. Провести аналіз існуючих методів і засобів проектування систем і компонентів критичного застосування; сформувати стратегію досліджень.

2. Розробити методологію синтезу абстрактних, структурних і HDL-моделей безпечних логічних автоматів для ПЛІС-контролерів з паралельною архітектурою.

3. Розробити мову, технологію та інструментальні засоби проектування програмного забезпечення (ПЗ) для безпечних ПЛІС-контролерів з паралельною архітектурою.

4. Запропонувати та виконати дослідження методів проектування та моделей пристроїв безпечного формування керуючих впливів.

5. Провести експериментальні дослідження і промислові випробування безпечних ПЛІС-контролерів з паралельною архітектурою в складі комп’ютерної системи критичного застосування.

6. Виконати порівняльну оцінку показників функціональної безпеки відомих і розроблених методів і засобів проектування ТПК СКП.

Об'єкт дослідження - процес проектування технічних і програмних компонентів систем критичного застосування.

Предмет дослідження - методи та засоби проектування технічних і програмних компонентів безпечних ПЛІС-контролерів з паралельною архітектурою для систем критичного застосування.

Методи досліджень. Основні теоретичні положення дисертації базуються на узагальнених засадах теорії синтезу цифрових автоматів, яка була використана при розробці методології абстрактного і структурного синтезу безпечних логічних автоматів паралельної дії з функціональною деградацією і математичних моделей пристроїв безпечного формування керуючих впливів. При розробці абстрактних і структурних моделей безпечних логічних автоматів циклічної дії використано методи синтезу та формального опису паралельних програмованих логічних автоматів. При побудові абстрактних моделей безпечних логічних автоматів паралельної дії використано математичний апарат мереж Петрі. При розробці табличної мови опису апаратури для ПЛІС використано методи формального опису мов програмування. Методи математичного, імітаційного та фізичного моделювання використано при дослідженні та аналізі функціонування безпечних ПЛІС-контролерів з паралельною архітектурою і пристроїв безпечного формування керуючих впливів. Методи метричної оцінки складності ПЗ (Холстеда, Чепіна) використано при виконанні порівняльної оцінки показників функціональної безпеки відомих і розроблених мов програмування ПЛІС. При виконанні оцінки функціональної безпеки використано теорію надійності, графо-аналітичний метод розрахунку показників функціональної безпеки. Теорію ймовірностей і методи статистичного аналізу використано при оцінці функціональної безпеки програмного забезпечення, розробленого на запропонованій табличній мові опису апаратури THDL.

Наукова новизна отриманих результатів. У результаті виконання дисертаційної роботи були запропоновані перспективні методи та нові засоби проектування технічних і програмних компонентів безпечних ПЛІС-контролерів з паралельною архітектурою, що дозволяє підвищити безпеку систем критичного застосування за рахунок реалізації процедури керування функціональною деградацією, застосування спрощеної технології програмування і формування вихідних керуючих впливів шляхом послідовного перетворення параметрів сигналів, що динамічно змінюються у часі.

- Уперше запропонована сукупність математичних моделей і методів синтезу безпечних логічних автоматів паралельної дії (БЛП-автоматів), які не вимагають надлишкового безпечного кодування внутрішніх станів і, за рахунок використання розроблених процедур перетворення графів χ-автоматів, забезпечують керування функціональною деградацією і збереження реалізуємих відповідальних функцій при відмовах.

- Одержали подальший розвиток методи завдання безпечних автоматів, які, на відміну від відомих, базуються на формальному описі вимог до безпеки

χ-автоматними моделями М- і Р-типу, а також на формуванні множин відповідальних операцій, що реалізуються автоматом, що дозволяє використовувати кон'юнктиву функцію керування деградацією.

- Удосконалений метод опису цифрових пристроїв на ПЛІС: розроблені мова, технологія та інструментальні засоби програмування, які, на відміну від відомих, базуються на використанні спрощених табличних конструкцій для опису процедур обробки інформації, настройки функцій забезпечення безпеки та кодування вхідних і вихідних сигналів, що дозволяє зменшити кількість помилок і за рахунок цього підвищити безпеку програмного забезпечення.

- Одержали подальший розвиток методи проектування пристроїв безпечного формування керуючих впливів за рахунок використання принципу послідовного перетворення параметрів сигналів, що динамічно змінюються в часі, що виключає можливість формування небезпечного керуючого впливу при відмові контрольних засобів і наявності хоча б одного працездатного каналу.

- Уперше запропоновані математичні та HDL-моделі *n*-канальних пристроїв безпечного формування гармонічних сигналів, які, на відміну від відомих, здійснюють формування ШІМ-сигналу за рахунок застосування логічної операції "нееквівалентності" для двох сигналів із близькими частотами та виключають можливість генерації небезпечних керуючих впливів при наявності (*n* - 1)-кратних відмов.

- Одержав подальший розвиток метод Чепіна оцінки складності ПЗ, що дозволяє розраховувати складність HDL-описів з урахуванням використання верифікованих програмних компонентів і ієрархічного принципу опису цифрових пристроїв на основі ПЛІС.

Практичне значення отриманих результатів полягає в тому, що вони дозволяють вирішити комплекс задач, пов'язаних з розробкою та проектуванням безпечних ПЛІС-контролерів з паралельною архітектурою для СКЗ в області енергетики, залізничної автоматики, авіації тощо. На основі отриманих методів та моделей розроблено безпечні модулі логічної обробки інформації з керуванням функціональною деградацією на основі ПЛІС, безпечні модулі формування вихідних керуючих впливів, запропоновано інструментальні засоби та мову проектування програмного забезпечення для безпечних ПЛІС-контролерів і створено програмно-апаратні комплекси на їхній основі.

Отримані в дисертації результати використані при розробці, виготовленні та промислових випробуваннях мікроелектронної системи централізації Харківського метрополітену на основі безпечних ПЛІС-контролерів з паралельною архітектурою а також компонентів систем автоматизації залізниць і метрополітенів, що підтверджується відповідними актами впровадження, а саме: безконтактних модулів керування стрілками БМК-С; безконтактних модулів керування сигналами світлофорів БМК-СС; генераторів автоматичного регулювання швидкості Г-АРС-М.

Запропонована архітектура та створені експериментальні зразки безпечних ПЛІС-контролерів з паралельною архітектурою є оригінальними, захищені патентами України і аналогів у світовій практиці не мають.

Особистий внесок здобувача. Положення і результати, що виносяться на захист дисертаційної роботи, отримані здобувачем особисто. Серед них: методологія, математичні моделі та методи синтезу безпечних автоматів, методи, технологія та інструментальні засоби табличного HDL-синтезу цифрових пристроїв на ПЛІС, методи проектування та моделі безпечних пристроїв формування керуючих впливів для об’єктів критичного застосування, метод оцінки складності HDL-описів з урахуванням використання верифікованих програмних компонентів і ієрархічного принципу опису цифрових пристроїв на основі ПЛІС.

Апробація результатів дисертації. Положення дисертації та результати досліджень доповідалися і обговорювалися на: Міжнародних науково-практичних конференціях "Dependable Systems, Services And Technologies" (Полтава – 2006 р., Кіровоград – 2007 – 2009 рр.); Міжнародній науково-практичній конференції "Перспективні комп'ютерні, керуючі та телекомунікаційні системи для залізничного транспорту України" (Алушта – 2008 р.); Науково-технічному семінарі "Критичні комп'ютерні технології та системи" (Харків – 2007, 2009 рр.); Міжнародній науково-практичній конференції "Задоволення потреб населення в пасажирських перевезеннях - невід'ємна частина соціально-економічного розвитку великих міст" (Харків – 2005 р.); Конференції головних інженерів Асоціації "Метро" (Харків – 2008 р.); Міжнародних науково-технічних конференціях "Проблеми енергопостачання і енергозбереження в АПК України" (Харків – 2005 – 2008 р); Міжнародній науково-технічній конференції "Енергетика в АПК" (Мелітополь – 2006, 2008 р.); III міжнародному науково-практичному семінарі кафедри автоматизації виробничих процесів Харківського державного технічного університету будівництва і архітектури (Харків – 2007 р.); Міжнародній науково-практичній конференції "Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2007" (Харків – 2007 р.); Міжнародному молодіжному форумі "Радіоелектроніка і молодь у XXI столітті" (Харків – 2009 р.); Міжнародній науково-практичній конференції "Автомобільний транспорт в XXI столітті" (Харків – 2005 р.); XI міжнародній науково-практичній конференції "Електромеханічні системи, методи моделювання та оптимізації" (Кременчук – 2009 р.).

У повному обсязі дисертація доповідалася і обговорювалася на науково-технічному семінарі "Критичні комп'ютерні технології і системи" (Національний аерокосмічний університет ім. М. Є. Жуковського "ХАІ") (2009 р.); розширеному засіданні кафедри автоматизації та комп'ютерних технологій Харківського національного технічного університету сільського господарства ім. П. Василенка (2009 р.), в Інституті кібернетики ім. В. М. Глушкова НАН України (2009 р.).

Публікації. Основні наукові положення дисертації опубліковані в 37 друкованих працях, з них 5 монографій, 21 статей у наукових фахових виданнях ВАК України та 6 патентів України.

Структура та обсяг роботи. Дисертація складається із вступу, семи розділів, висновків, 7 додатків та списку літератури. Повний обсяг дисертації містить 379 сторінок; з них 59 рисунок по тексту, 51 рисунок на 33 окремих сторінках, 35 таблиць по тексту, 19 таблиць на 9 окремих сторінках, 7 додатків на 52 сторінках і 159 найменувань використаних джерел на 18 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовується актуальність, сформульовані мета і завдання дослідження, наукова новизна та практична цінність.

У першому розділі розглянуті основні поняття і термінологія, що використовуються при оцінці якісних характеристик ТПК СКЗ. Виконано аналіз еволюційного розвитку методів забезпечення безпеки ТПК СКЗ, що застосовувалися в різних системах, починаючи від механічних і релейних і закінчуючи сучасними мікропроцесорними і мікроелектронними на основі ПЛІС. Розглянуто методи забезпечення безпеки апаратних і програмних засобів, а також відомі автоматні моделі ТПК СКЗ.

Виконано аналіз перспективних методів алгоритмізації та програмування систем логічного керування на основі ПЛІС. Показано, що на сьогоднішній день, поряд із традиційними методами та засобами програмування ПЛІС, активно розвиваються нові напрямки, що утворюють два перспективних підходи, орієнтованих на архітектуру керуючих автоматів і на способи представлення алгоритмів керування.

Аналіз стану проблеми показав, що основними причинами, які стримують впровадження мікроелектронних і мікропроцесорних ТПК СКЗ, є висока вартість, необхідність підготовки фахівців, які могли б успішно обслуговувати дані системи, а також недоліки, які властиві відомим методам і засобам побудови СКЗ. Зокрема, відомі методи синтезу безпечних автоматів не охоплюють ряд важливих задач, у тому числі: формалізації вимог до безпеки автоматів, синтезу автоматів за формалізованими вимогами до безпеки, синтезу безпечних автоматів з функціональною деградацією. Програмування ТПК СКЗ виконується з використанням технологій, орієнтованих на користувачів з високою кваліфікацією, що мають професійні навики в програмуванні, що ускладнює підготовку і налагодження ПЗ та приводить до появи помилок у програмних продуктах. Методи побудови пристроїв узгодження мікроелектронних структур з виконавчими механізмами орієнтовані на двоканальну реалізацію мікроелектронних структур, вимагають синхронізації резервованих каналів і виконання спеціальних діагностичних процедур для контролю справного стану каналів шляхом введення різних видів надмірності.

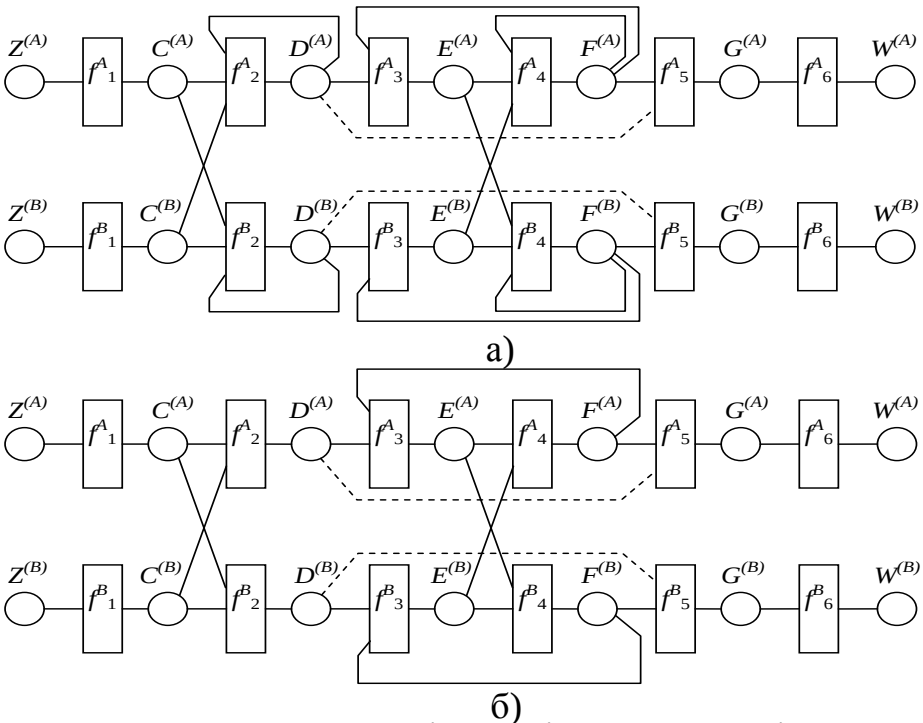
Таким чином, сучасний етап розвитку теорії побудови систем критичного застосування характеризується наявністю науково-прикладної проблеми, що полягає у необхідності ліквідації протиріччя між властивостями елементної бази з симетричними та несиметричними відмовами.

Сформульовано і обґрунтовано концепцію та етапи проведення дисертаційних досліджень.

У другому розділі розроблена методологія абстрактного синтезу безпечних логічних автоматів паралельної дії (БЛП-автоматов) для ПЛІС-контролерів. Розроблено класифікацію БЛП-автоматів, що містить шість їхніх різновидів.

Розроблені математичні моделі БЛП-автоматів Мілі та Мура М- і Р-типу (рис. 1), представлені у вигляді мереж Петрі, що містять функціональні переходи (f-переходи) $f^{(A)}_1$ - $f^{(A)}_6$ і $f^{(B)}_1$ - $f^{(B)}_6$. Як видно з моделей, БЛП-автомати містять вхідні сигнали $Z^{(A)}$ і $Z^{(B)}$, вихідні сигнали $W^{(A)}$ і $W^{(B)}$, а також стани, які можна розділити на підмножини $C^{(A)}$, $C^{(B)}$, $D^{(A)}$, $D^{(B)}$, $E^{(A)}$, $E^{(B)}$, $F^{(A)}$, $F^{(B)}$, $G^{(A)}$, $G^{(B)}$, що відповідають однойменним місцям мережі Петрі.

Властивості абстрактних моделей БЛП-автоматів здійснювати безпечні переходи з урахуванням попереднього стану (для М-типу) або без урахування попереднього стану (для Р-типу) визначаються наявністю дуг, що з'єднують місця $D^{(A)}$ з f-переходом $f^{(A)}_2$, $D^{(B)}$ з f-переходом $f^{(B)}_2$, $F^{(A)}$ з f-переходом $f^{(A)}_4$, $F^{(B)}$ з f-переходом $f^{(B)}_4$. Абстрактні моделі БЛП-автоматів М- і Р-типів містять дуги, які відзначені пунктиром і з'єднують місця $D^{(A)}$ з переходом $f^{(A)}_5$ і $D^{(B)}$ з переходом $f^{(B)}_5$. Зазначені дуги містять БЛП-автомати Мілі, тоді як у БЛП-автоматів Мура ці дуги відсутні.



а)

б)

Рис. 1. Абстрактні моделі БЛП-автоматів:
а) – М-типу,
б) – Р-типу.

Таким чином, БЛП-автомат описується кортежем

$$\text{БЛП} = [Z, C, D, E, F, G, H, W, \varphi, \omega, \delta, \chi, \lambda, \psi], \qquad (1)$$

де $Z = \{Z^{(A)}, Z^{(B)}\}$ – вхідні сигнали, яким відповідає алфавіт $z^{(A)}_1, \dots, z^{(A)}_n, \dots, z^{(A)}_N$, $z^{(B)}_1, \dots, z^{(B)}_n, \dots, z^{(B)}_N$;

$W = \{W^{(A)}, W^{(B)}\}$ – вихідні сигнали, яким відповідає алфавіт $w^{(A)}_1, \dots, w^{(A)}_k, \dots, w^{(A)}_K, w^{(B)}_1, \dots, w^{(B)}_k, \dots, w^{(B)}_K$;

$C = \{C^{(A)}, C^{(B)}\}$ – множина станів, яким відповідає алфавіт $c^{(A)}_1, \dots, c^{(A)}_n, \dots, c^{(A)}_N, c^{(B)}_1, \dots, c^{(B)}_n, \dots, c^{(B)}_N$;

$D = \{D^{(A)}, D^{(B)}\}$ – множина станів, яким відповідає алфавіт $d^{(A)}_1, \dots, d^{(A)}_n, \dots, d^{(A)}_N, d^{(B)}_1, \dots, d^{(B)}_n, \dots, d^{(B)}_N$;

$E = \{E^{(A)}, E^{(B)}\}$ – множина станів, яким відповідає алфавіт $e^{(A)}_1, \dots, e^{(A)}_l, \dots, e^{(A)}_L, e^{(B)}_1, \dots, e^{(B)}_l, \dots, e^{(B)}_L$;

$F = \{F^{(A)}, F^{(B)}\}$ – множина станів, яким відповідає алфавіт $f^{(A)}_1, \dots, f^{(A)}_l, \dots, f^{(A)}_L, f^{(B)}_1, \dots, f^{(B)}_l, \dots, f^{(B)}_L$;

$G = \{G^{(A)}, G^{(B)}\}$ – множина станів, яким відповідає алфавіт $g^{(A)}_1, \dots, g^{(A)}_k, \dots, g^{(A)}_K, g^{(B)}_1, \dots, g^{(B)}_k, \dots, g^{(B)}_K$;

φ – функція переходів, яка визначає стани $C^{(A)}$, $C^{(B)}$ автомата в залежності від вхідних сигналів $Z^{(A)}$ і $Z^{(B)}$;

ω – функція переходів, яка визначає стани $D^{(A)}$, $D^{(B)}$ автомата в момент часу t в залежності від станів $C^{(A)}$, $C^{(B)}$, а також станів $D^{(A)}$ і $D^{(B)}$ (для автоматів М-типу) в момент часу $t - 1$;

δ – функція переходів, яка визначає стани $E^{(A)}$, $E^{(B)}$ автомата в момент часу t в залежності від станів $D^{(A)}$, $D^{(B)}$ і $F^{(A)}$, $F^{(B)}$ в момент часу $t - 1$;

χ – функція переходів, яка визначає стани $F^{(A)}$, $F^{(B)}$ автомата в момент часу t в залежності від станів $E^{(A)}$, $E^{(B)}$, а також станів $F^{(A)}$ і $F^{(B)}$ (для автоматів М-типу) в момент часу $t - 1$;

λ – функція переходів, яка визначає стани $G^{(A)}$, $G^{(B)}$ автомата в момент часу t в залежності від станів $F^{(A)}$, $F^{(B)}$, а також станів $D^{(A)}$ і $D^{(B)}$ (для автоматів Мілі) в момент часу $t - 1$;

ψ – функція переходів, яка визначає вихідні сигнали $W^{(A)}$, $W^{(B)}$ автомата в залежності від станів $G^{(A)}$ и $G^{(B)}$.

Для опису зв'язків між станами різних видів БЛП-автоматів використовуються наступні залежності (на прикладі автомата Мілі М-типу):

$$\begin{cases} C^{(A)}_t = \varphi\,(Z^{(A)}_t); \\ C^{(B)}_t = \varphi\,(Z^{(B)}_t); \\ D^{(A)}_t = \omega\,(C^{(A)}_t, C^{(B)}_t, D^{(A)}_{(t\text{-}1)}); \\ D^{(B)}_t = \omega\,(C^{(A)}_t, C^{(B)}_t, D^{(B)}_{(t\text{-}1)}); \\ E^{(A)}_t = \delta\,(F^{(A)}_{t\text{-}1}, D^{(A)}_{(t\text{-}1)}); \\ E^{(B)}_t = \delta\,(F^{(B)}_{t\text{-}1}, D^{(B)}_{(t\text{-}1)}); \\ F^{(A)}_t = \chi\,(E^{(A)}_t, E^{(B)}_t, F^{(A)}_{(t\text{-}1)}); \\ F^{(B)}_t = \chi\,(E^{(A)}_t, E^{(B)}_t, F^{(B)}_{(t\text{-}1)}); \\ G^{(A)}_t = \lambda\,(F^{(A)}_{t\text{-}1}, D^{(A)}_{(t\text{-}1)}); \\ G^{(B)}_t = \lambda\,(F^{(B)}_{t\text{-}1}, D^{(B)}_{(t\text{-}1)}); \\ W^{(A)}_t = \psi\,(G^{(A)}_t); \\ W^{(B)}_t = \psi\,(G^{(B)}_t). \end{cases} \qquad (2)$$

Етапи завдання БЛП-автоматів включають: завдання функцій переходів δ і λ традиційного цифрового автомата; завдання функції φ перетворення вхідного сигналу $z \in Z$ у сигнал $c \in C$; завдання функції виходів ψ перетворення сигналу $g \in G$ у сигнал $w \in W$; завдання функцій ω и χ - перетворення станів (визначаються вимогами до безпеки автомата).

Розроблено методи завдання функцій ω і χ безпечних автоматів М- і Р-типу табличними формами: таблицею відповідності, квадратною таблицею, таблицею переходів χ-автомата, а також графічними формами: графом безпечних переходів з відміченими дугами та графом переходів χ-автомата.

Розроблено методи завдання функцій ω і χ безпечних автоматів симетричними та усіченими графами. Запропоновано наступну формальну ознаку, що підтверджує, що два графи є симетричними один одному:

Нехай дані графи G_i і G_j; виконаємо перетворення графа G_i в граф G_i' у відповідності з наступним правилом: для кожної стрілки, що має відмітку k і спрямована від вершини з номером r до вершини з номером s, побудуємо вершину з номером k і направимо від неї стрілку до вершини з номером s; біля побудованої стрілки поставимо відмітку r; якщо графи G_i' та G_j еквівалентні, то граф G_i симетричний графу G_j.

Симетричність графа G_i відносно G_j запропоновано позначати виразом $G_i \,\%\, G_j$. Установлено, що якщо існує χ-автомат A, який описується усіченим графом G_i, і χ-автомат B, який описується усіченим графом G_j, причому $G_i \,\%\, G_j$, то автомати A і B відповідають однієї і тієї ж функції χ.

Установлено зв'язок між графом χ-автомата та графом безпечних переходів, що визначається розробленою процедурою перетворення графа безпечних переходів у граф переходів χ-автомата.

Запропоновано процедуру, що застосовується до графу безпечних переходів з відміченими ребрами, яка дозволяє одержати відповідні даному графові таблицю і граф переходів χ-автомата:

1. Граф безпечних переходів з відміченими ребрами описується таблицею з L стовпцями та L' рядками, де L - кількість вершин графа безпечних переходів, L' - кількість букв вхідного алфавіту χ-автомата, кожному стовпцю якої ставиться у відповідність стан і кожному рядку - буква e_{ij} вхідного алфавіту χ-автомата.

2. Таблиця заповнюється такий чином: для кожного рядка, що відповідає букві e_{ii} вхідного алфавіту (у якій індекси збігаються), у всіх стовпцях проставляються номери i; правила заповнення інших елементів таблиці наступні: для кожного елементу, що розташовується на перетинанні i-го стовпця і рядка, що відповідає букві e_{jk} вхідного алфавіту, встановлюється номер: j, якщо існує стрілка, відзначена номером i та спрямована від j-ої до k-ої вершини графа безпечних переходів; k, якщо існує стрілка, відзначена номером i та спрямована від k-ої до j-ої вершини графа безпечних переходів; r, якщо одночасно існують стрілки, відзначені номером i та спрямовані від j-ої до r-ої вершини та від k-ої до r-ої вершини.

3. По отриманій таблиці будується граф переходів автомата Мура, що є графом χ-автомата.

Розроблено метод формального опису вимог до безпеки БЛП-автоматів, що дозволяє реалізувати наступну процедуру завдання χ-автомата:

1. Формується множина відповідальних операцій $\Phi = \{\phi_1, \phi_2, \ldots, \phi_n\}$, які повинен реалізувати автомат;

2. Кожному *i*-му стану автомата ставиться у відповідність підмножина $\Phi_i \in \Phi$ функцій, які реалізуються автоматом в *i*-му стані;

3. Будується граф, кожна *i*-а вершина якого відповідає *i*-му стану автомата; стрілки, що з'єднують вершини, будуються за наступним правилом: стрілка, спрямована від *i*-ї вершини до *j*-ї вершини існує тоді й тільки тоді, коли $\Phi_j \in \Phi_i$, де Φ_j та Φ_i - підмножини з множини Φ відповідальних функцій, реалізуємих автоматом в *j*-му та *i*-му станах відповідно.

4. Отриманий граф є графом безпечних переходів і однозначно визначає функцію χ БЛП-автомата.

Проблема синтезу БЛП-автоматів з функціональною деградацією сформульована наступним чином: потрібно побудувати процедуру, що дозволяла б по відомому алгоритму, описаному канонічною моделлю автомата М у виді графа або таблиці переходів і виходів, знаходити граф або таблицю переходів χ-автомата, таку, для якої будь-яке спотворення або послідовна серія спотворень одного із вхідних сигналів $e_i \sim e_j$ викликає такі спотворення вихідного сигналу $f_i \sim f_r$, при яких відсутня деградація безпеки та має місце можливо менший рівень деградації працездатності БЛП-автомата.

Запропоновано розв’язання проблеми синтезу БЛП-автоматів з функціональною деградацією шляхом побудови, аналізу та перетворення χ-автоматів. Процедура синтезу БЛП-автоматів, у яких функція χ описується графом безпечних переходів, зводиться до виконання наступних етапів:

1. Відповідно до традиційної теорії абстрактного синтезу кінцевих автоматів будується граф переходів *G* з *L* вершинами, що задає канонічну модель автомата Мілі або Мура.

2. Будується граф *Gs* безпечних переходів з *L* вершинами.

3. Якщо будь-яка пара вершин отриманого графа *Gs* зв'язана ребром безпосередньо або через третю вершину, до якої спрямовані стрілки безпечних помилкових переходів (надалі будемо називати такі графи β-зв'язаними), то переходимо до завдання таблиці переходів для функції χ (п. 8 процедури).

4. (Якщо граф *Gs* не β-зв'язний), для кожної пари (групи) не β-зв'язних вершин створюються нові вершини, до яких з кожної з незв'язних вершин даної групи будуються дуги безпечних переходів, забезпечуючи таким чином β-зв’язність розглянутої пари (групи).

5. Вихідний граф *G* доповнюється вершинами, уведеними в граф *Gs*, виходячи з аналізу алгоритму керування будуються дуги й описуються умови переходів з нових вершин до початкових.

6. Граф *Gs* доповнюється новими стрілками, що відповідають безпечним переходам, що зв'язують нові вершини з початковими.

7. Повертаємося до п. 3.

8. Будується таблиця переходів відповідно запропонованої процедури перетворення графа безпечних переходів у граф переходів χ-автомата.

9. Будується таблиця виходів для всієї сукупності станів, отриманих у результаті виконаних перетворень.

Якщо БЛП-автомат М-типу, то операції 2-8 виконуються для кожного стану, що відповідає вершині графа *G*.

Процедура синтезу БЛП-автоматів, у яких функція χ описується автоматом Мура, відрізняється від наведеної тим, що граф *Gs* будується як усічений граф переходів χ-автомата, а також пунктами 3, 4 і 8, які для цього випадку мають наступне формулювання:

3. Якщо для кожної *i*-й вершини існує повний набір вихідних стрілок з відмітками (*i*+1, *i*+2, ... *L*), де *L* - кількість вершин графа *Gs*, то переходимо до пункту 8.

4. Для кожної вершини (або групи вершин), для якої відсутній повний набір вихідних стрілок з відмітками (*i*+1, *i*+2, ... *L*), будується нова вершина.

8. Відповідно до отриманого графа *Gs* будується таблиця переходів.

Розроблено абстрактні моделі БЛП-автоматів циклічної дії. При цьому запропонована модель автомата циклічної дії, що представляє собою два взаємодіючих компонентних автомати S і T. Автомат T = {*A, Z, ENDmc,* λ} (*Transition*), де λ – функція переходів, що визначає стан *Z* у залежності від попереднього стану *Z*, вхідного сигналу *A* і сигналу *ENDmc*, є автоматом переходів між станами та описується таблицею переходів.

Автомат S = {*Z, B, B', W, ENDmc, C,* χ, δ, δ'} (*State*), де δ – функція переходів, що визначає стан *B'* в залежності від стану *Z* і номера поточної операції *W*, δ' – функція яка визначає стан сигналу *ENDmc* в залежності від стану *Z* і номера поточної операції *W*, χ – функція переходів, що визначає вихідний стан *C* у залежності від стану *Z* і номера поточної операції *W*, являє собою автомат станів (описує простір станів об'єкта керування відповідно до таблиці станів).

Зв’язок між станами автоматів S і T, що входять до складу автомата циклічної дії, описуються часовими залежностями:

$$\begin{cases} Z_t = \lambda\{A_t, Z_{(t-1)}, ENDmc_t\}; \\ B'_t = \delta\{Z_{(t-1)}, W_t\}; \\ ENDmc_t = \delta'\{Z_{(t-1)}, W_t\}; \\ C_t = \chi\{Z_{(t-1)}, W_t\}; \\ W_t = \begin{cases} W_{(t-1)} & \text{при } B'_t \neq B_t; \\ W_{(t-1)} + 1 & \text{при } B'_t = B_t \text{ и } ENDmc_t = 0. \end{cases} \end{cases} \qquad (3)$$

Абстрактні моделі БЛП-автоматів циклічної дії представлені у вигляді двох взаємодіючих мереж Петрі, одна з яких описує функціонування безпечного автомата T* (переходів між станами), а друга - безпечного автомата S* (простору станів). Автомат T* містить вхідні сигнали $A^{(A)}$, $A^{(B)}$, вихідні

сигнали $Z^{(A)}$, $Z^{(B)}$, множини станів $T^{(A)}_1$ ... $T^{(A)}_3$ і $T^{(B)}_1$ ... $T^{(B)}_3$. Стани $S^{(A)}_5$ та $S^{(B)}_5$ належать автомату S^* і для автомата T^* є вхідними сигналами.

Автомат S* містить вхідні сигнали $B^{(A)}$, $B^{(B)}$, вихідні сигнали $C^{(A)}$, $C^{(B)}$, стани $S^{(A)}_1$ ... $S^{(A)}_7$ та $S^{(B)}_1$ ... $S^{(B)}_7$. Стани $Z^{(A)}$ и $Z^{(B)}$ належать автомату T*.

Взаємодія автоматів S* і T* забезпечується наявністю дуг, що з'єднують місця $Z^{(A)}$ і $Z^{(B)}$ автомата T* з переходами $f^{(A)}_3$, $f^{(A)}_4$ та $f^{(B)}_3$, $f^{(B)}_4$ автомата S*, а також місця $S^{(A)}_4$ и $S^{(B)}_4$ автомата S* з переходами $f^{(A)}_3$ и $f^{(B)}_3$ автомата T*.

Розроблено методи опису компонентів БЛП-автоматів, які містять форми (табличні або графічні) і процедури їхнього настройки на реалізацію функцій перетворення вхідних і вихідних сигналів, логічної обробки інформації і вибору безпечних станів.

Виконані в другому розділі дослідження і аналіз показують, що розроблена методологія абстрактного синтезу та моделі БЛП-автоматів є універсальним апаратом для опису дискретних пристроїв і систем з реалізацією функцій забезпечення безпеки керування та можуть використовуватися на різних стадіях проектування ТПК СКЗ, таких як абстрактний синтез БЛП-автоматів, розробка і формальний опис процедур керування СКЗ і їхня верифікація.

У третьому розділі розроблена методологія структурного синтезу БЛП-автоматів. Отримано структурні моделі БЛП-автоматів Мілі і Мура М- і Р-типу. Структура БЛП-автомата Мілі М-типу (рис. 2) складається з компонентних автоматів А і В та містить набір функціональних перетворювачів $ФП^{(A)}_{\varphi}$, $ФП^{(B)}_{\varphi}$ і $ФП^{(A)}_{\psi}$, $ФП^{(B)}_{\psi}$, комбінаційних схем $КС^{(A)}_{\omega}$, $КС^{(B)}_{\omega}$, $КС^{(A)}_{\delta}$, $КС^{(B)}_{\delta}$, $КС^{(A)}_{\chi}$, $КС^{(B)}_{\chi}$, $КС^{(A)}_{\lambda}$, $КС^{(B)}_{\lambda}$ і блоків пам'яті $БП^{(A)}_1$, $БП^{(B)}_1$, $БП^{(A)}_2$, $БП^{(B)}_2$. Інформація про поточний стан об'єкта керування надходить на входи компонентних автоматів А і В у вигляді сигналів, у яких у якості ознаки використовуються їхні часові параметри. Вхідні функціональні перетворювачі $ФП^{(A)}_{\varphi}$, $ФП^{(B)}_{\varphi}$ забезпечують перетворення цих сигналів у сигнали, у яких ознакою стану є логічний рівень (0 або 1). Функція перетворення φ реалізується функціональними перетворювачами $ФП^{(A)}_{\varphi}$, $ФП^{(B)}_{\varphi}$.

Комбінаційні схеми $КС^{(A)}_{\omega}$, $КС^{(B)}_{\omega}$ забезпечують порівняння результатів перетворення вхідних сигналів компонентними автоматами А і В відповідно до заданих умов забезпечення безпеки функціонування СКЗ. У тому випадку, якщо застосовуються методи кодування інформації, при яких один із станів вхідних сигналів використовуються в якості захисного, комбінаційні схеми $КС^{(A)}_{\omega}$, $КС^{(B)}_{\omega}$ реалізують логічну функцію порозрядного множення (кон'юнкції) якщо захисним є логічний 0, або логічну функцію порозрядного додавання (диз'юнкції) якщо захисною є логічна 1.

Формування сигналів на виходах комбінаційних схем $КС^{(A)}_{\omega}$, $КС^{(B)}_{\omega}$ відповідно до логічної функції ω для БЛП-автоматів М-типу виконується з урахуванням стану $d_{(t-1)} \in D$, що забезпечується наявністю сигналів $q_{1(t-1)}$ ... $q_{N''(t-1)}$ на входах $КС^{(A)}_{\omega}$, $КС^{(B)}_{\omega}$. З виходів комбінаційних схем $КС^{(A)}_{\omega}$, $КС^{(B)}_{\omega}$ сигнали надходять на входи блоків пам'яті $БП^{(A)}_1$, $БП^{(B)}_1$ які виконують функцію зберігання інформації про поточний стан $d \in D$. З виходів блоків пам'яті $БП^{(A)}_1$, $БП^{(B)}_1$ сигнали надходять на входи комбінаційних схем $КС^{(A)}_{\delta}$, $КС^{(B)}_{\delta}$, які

реалізують логічну функцію δ, що відповідає однойменної логічної функції традиційного автомата, що описує вихідний алгоритм керування технологічним об'єктом. Результати реалізації логічної функції δ компонентними автоматами A і B порівнюються комбінаційними схемами $КС^{(A)}_{\chi}$, $КС^{(B)}_{\chi}$, які реалізують логічну функцію χ. Формування сигналів y_1 ... $y_{L'}$ комбінаційними схемами $КС^{(A)}_{\chi}$, $КС^{(B)}_{\chi}$ для БЛП-автоматів М-типу здійснюється як на підставі порівняння результатів реалізації функції δ компонентними автоматами A і B, так і з урахуванням стану $f_{(t-1)} \in F$. З виходів комбінаційних схем $КС^{(A)}_{\chi}$, $КС^{(B)}_{\chi}$ сигнали надходять на входи блоків пам'яті $БП^{(A)}_2$, $БП^{(B)}_2$ які виконують функцію зберігання інформації про поточний стан $f \in F$. З виходів блоків пам'яті $БП^{(A)}_2$, $БП^{(B)}_2$ сигнали надходять на входи комбінаційних схем $КС^{(A)}_{\lambda}$, $КС^{(B)}_{\lambda}$, які реалізують логічну функцію λ, що відповідає однойменної логічної функції традиційного автомата, що описує вихідний алгоритм керування технологічним об'єктом. Вихідні функціональні перетворювачі $ФП^{(A)}_{\psi}$, $ФП^{(B)}_{\psi}$ забезпечують перетворення сигналів u_1 ... $u_{K''}$, у яких ознакою стану є логічний рівень, у сигнали v_1 ... $v_{K'}$, у яких ознакою стану є часові параметри цих сигналів.

Також виконаний структурний синтез БЛП-автоматів циклічної дії М- і Р-типу, у яких для реалізації функцій λ_1, φ_1, φ_7 використані функціональні перетворювачі $ФП^{(A)}_{\lambda 1}$, $ФП^{(B)}_{\lambda 1}$, $ФП^{(A)}_{\varphi 1}$, $ФП^{(B)}_{\varphi 1}$, $ФП^{(A)}_{\varphi 7}$, $ФП^{(B)}_{\varphi 7}$; для реалізації функцій λ_2, λ_3, λ_4, φ_2, φ_3, φ_4, φ_5, φ_6, φ_8 використані комбінаційні схеми $КС^{(A)}_{\lambda 2}$, $КС^{(B)}_{\lambda 2}$, $КС^{(A)}_{\lambda 3}$, $КС^{(B)}_{\lambda 3}$, $КС^{(A)}_{\lambda 4}$, $КС^{(B)}_{\lambda 4}$, $КС^{(A)}_{\varphi 2}$, $КС^{(B)}_{\varphi 2}$, $КС^{(A)}_{\varphi 3}$, $КС^{(B)}_{\varphi 3}$, $КС^{(A)}_{\varphi 4}$, $КС^{(B)}_{\varphi 4}$, $КС^{(A)}_{\varphi 5}$, $КС^{(B)}_{\varphi 5}$, $КС^{(A)}_{\varphi 6}$, $КС^{(B)}_{\varphi 6}$, $КС^{(A)}_{\varphi 8}$, $КС^{(B)}_{\varphi 8}$; для формування внутрішніх станів автомата $z^{(A)}_{(t-1)}$, $z^{(B)}_{(t-1)}$, $t^{(A)}_{2\,(t-1)}$, $t^{(A)}_{2\,(t-1)}$, $s^{(A)}_{2\,(t-1)}$, $s^{(B)}_{2\,(t-1)}$, $s^{(A)}_{7\,(t-1)}$, $s^{(B)}_{7\,(t-1)}$, використані блоки пам'яті $БП^{(A)}_1$, $БП^{(B)}_1$, $БП^{(A)}_2$, $БП^{(B)}_2$, $БП^{(A)}_3$, $БП^{(B)}_3$, $БП^{(A)}_4$, $БП^{(B)}_4$.

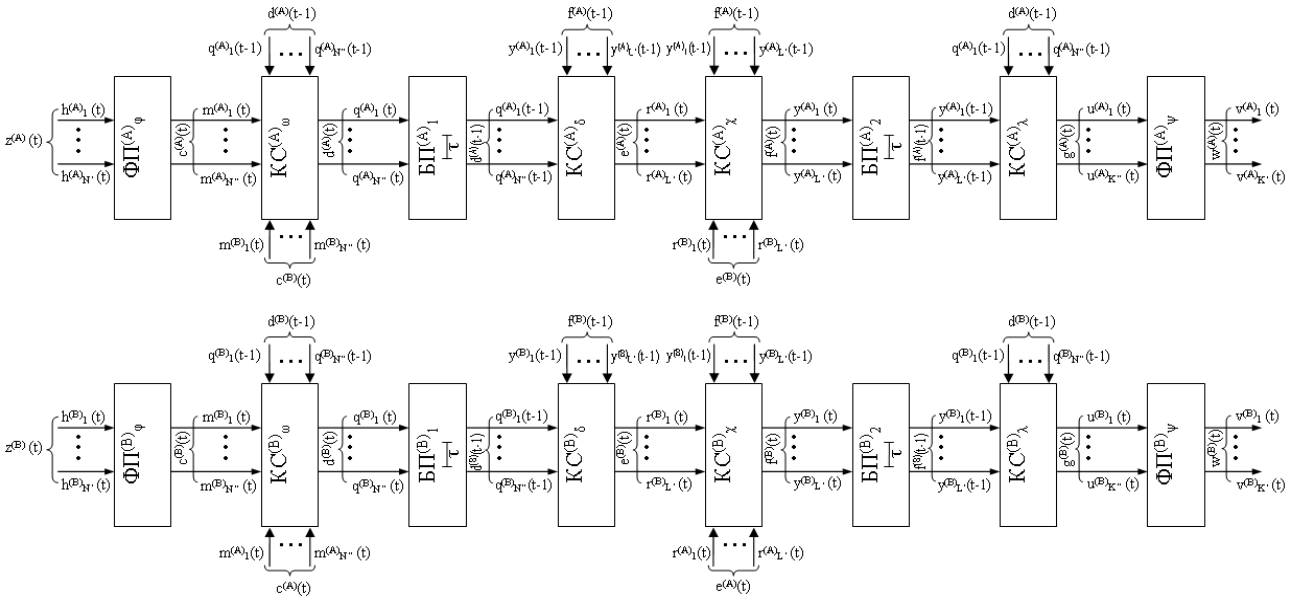


Рис. 2. Структурна модель БЛП-автомата Мілі М-типу

У результаті об'єднання функціональних блоків ($ФП^{(A)}_{\lambda 1}$, $ФП^{(B)}_{\lambda 1}$, $ФП^{(A)}_{\varphi 1}$, $ФП^{(B)}_{\varphi 1}$, $ФП^{(A)}_{\varphi 7}$, $ФП^{(B)}_{\varphi 7}$, $КС^{(A)}_{\lambda 2}$, $КС^{(B)}_{\lambda 2}$, $КС^{(A)}_{\lambda 3}$, $КС^{(B)}_{\lambda 3}$, $КС^{(A)}_{\lambda 4}$, $КС^{(B)}_{\lambda 4}$, $КС^{(A)}_{\varphi 2}$, $КС^{(B)}_{\varphi 2}$, $КС^{(A)}_{\varphi 3}$, $КС^{(B)}_{\varphi 3}$, $КС^{(A)}_{\varphi 4}$, $КС^{(B)}_{\varphi 4}$, $КС^{(A)}_{\varphi 5}$, $КС^{(B)}_{\varphi 5}$, $КС^{(A)}_{\varphi 6}$, $КС^{(B)}_{\varphi 6}$, $КС^{(A)}_{\varphi 8}$,

$КС^{(B)}{}_{\varphi 8}$, $БП^{(A)}{}_1$, $БП^{(B)}{}_1$, $БП^{(A)}{}_2$, $БП^{(B)}{}_2$, $БП^{(A)}{}_3$, $БП^{(B)}{}_3$, $БП^{(A)}{}_4$, $БП^{(B)}{}_4$) синтезовані структури БЛП-автоматів циклічної дії, які містять компонентні автомати T* і S* і представлені на рис. 3-4.

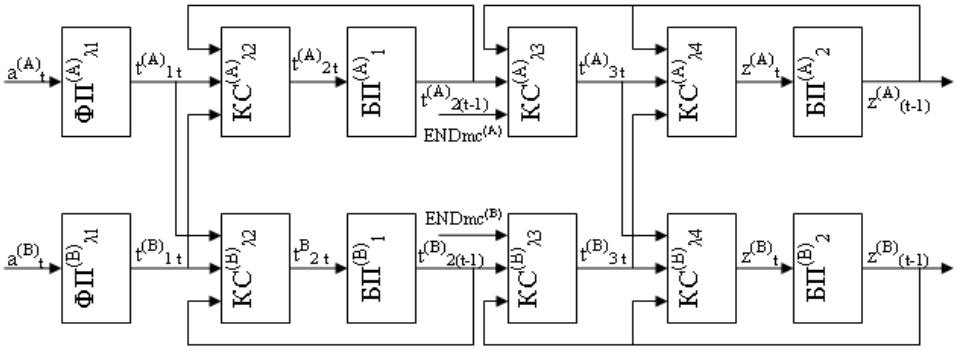


Рис. 3. Структурна модель автомата T*, що входить до складу БЛП-автомата циклічної дії

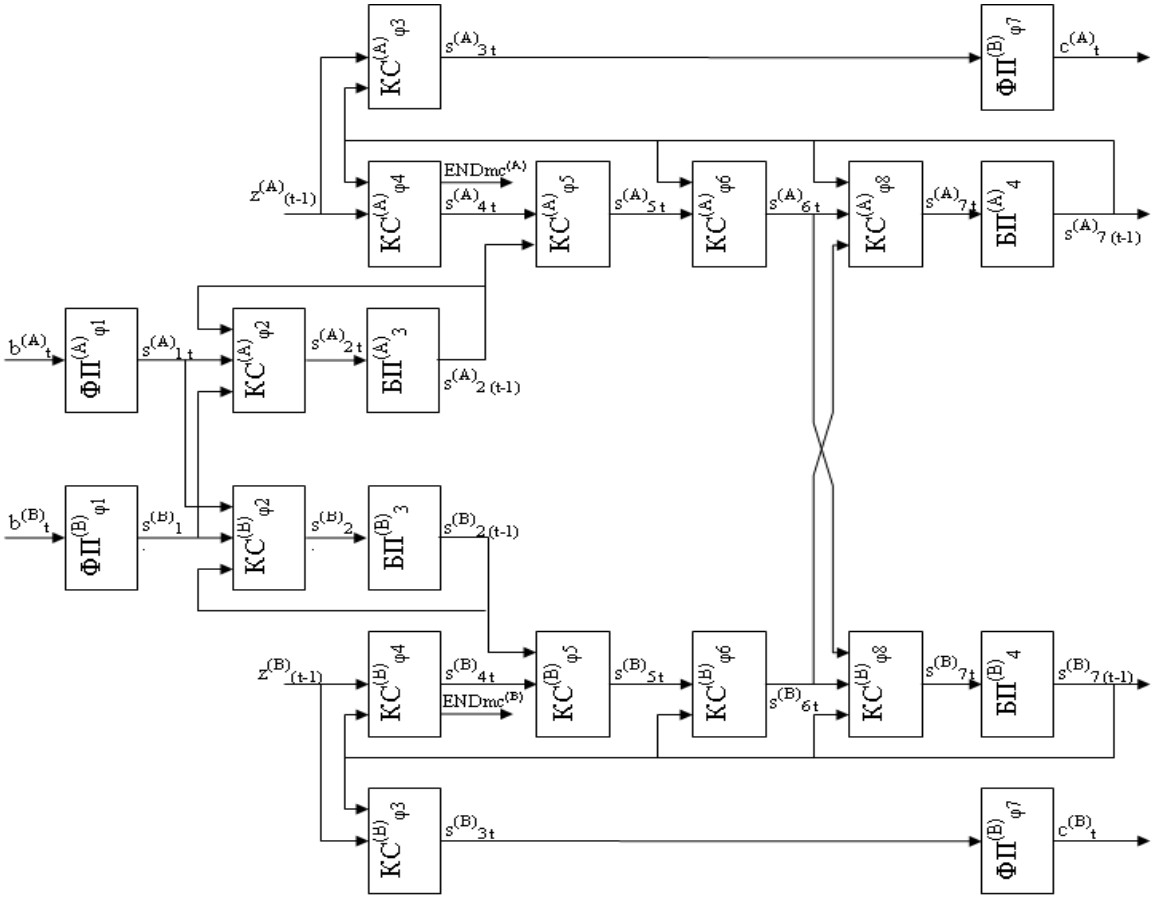


Рис. 4. Структурна модель автомата S*, що входить до складу БЛП-автомата циклічної дії

Аналіз функціонування БЛП-автоматів циклічної дії показав, що вони забезпечують коректну реалізацію алгоритмів, що описуються таблицями переходів і станів при відсутності спотворення станів та сигналів, і не формують небезпечних керуючих впливів при будь-яких одиночних спотвореннях станів та сигналів.

Розроблено і досліджено логічні структури функціональних блоків БЛП-автоматів: вхідних і вихідних функціональних перетворювачів і блоків пам'яті, що реалізують функцію багаторазового контролю правильності реалізації функцій логічного керування СКЗ. Крім того, запропоновані HDL-моделі БЛП-автоматов і їхніх компонентів, які дозволяють значно скоротити трудовитрати програмістів при проектуванні ПЗ для безпечних ПЛІС-контролерів. При цьому розроблювач ПЗ одержує можливість використання готових налагоджених конструкцій, а процес програмування зводиться до їхньої настройки на реалізацію заданих алгоритмів, опису умов кодування вхідних і вихідних сигналів і умов забезпечення безпеки відповідно до методу завдання БЛП-автоматів, розробленому у розд. 2.

Розроблений у розд. 2 метод синтезу БЛП-автоматів по формальному опису вимог до безпеки, заснованому на формуванні множин відповідальних операцій, дозволяє на етапі структурного синтезу використати наступний принцип кодування станів: розрядність коду повинна відповідати кількості реалізованих елементарних операцій; код i-го стану автомата формується з елементів i-го стовпця таблиці, що описують множини відповідальних операцій, починаючи від першого та закінчуючи останнім рядком. Функція χ при такому кодуванні описується як порозрядна кон’юнкція вхідних сигналів $E^{(A)}$, $E^{(B)}$. Побудований таким чином автомат при спотвореннях сигналів e_i, e_j завжди буде здійснювати перехід до деякого стану f_{ij}, код якого буде містити одиниці для елементарних операцій з множини Φ_{ij}, що утворюється на пересіченні множин Φ_i та Φ_j. У результаті цього код стану точно визначає перелік відповідальних операцій, які можуть бути реалізовані автоматом в умовах спотворень, виходячи із чого будується функція виходів.

Таким чином, розроблена методологія структурного синтезу БЛП-автоматів дозволяє виконувати синтез технічних і програмних компонентів ПЛІС-контролерів з функціональною деградацією, які захищені від небезпечних спотворень сигналів і станів, з урахуванням вимог, пропонованих до безпеки їхнього функціонування, а також особливостей структурної організації та взаємозв'язків між окремими компонентами.

У четвертому розділі розроблені мова, технологія та інструментальні засоби програмування безпечних ПЛІС-контролерів з паралельною архітектурою. Сформульовано концепцію створення мови і технології проектування програмного забезпечення для ПЛІС-контролерів, що заснована на трьох найважливіших положеннях: простота і наочність, психологічна природність, мінімум конструкцій і елементів. Для опису алгоритмів логічного керування запропоновано використовувати три блоки-оператори і відповідні їм табличні форми, яким одночасно властиві і типові конструкції, що застосовуються при реалізації цифрових пристроїв на ПЛІС, і зручні, природні форми подання алгоритмів логічного керування. Таким чином, вони становлять точку перетинання підходів "від архітектури" і "від первинних форм опису", які були позначені в базовій концепції даних досліджень.

Розроблено табличну мову опису апаратури THDL (Table Hardware Description Language), алфавіт і синтаксис якого формально описується наступними формулами:

<letter> :: = a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z;

<digit> :: = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F;

<number> :: = <digit> | <number> <digit> ;

<binary_number> :: b"<number>";

<octal_number> :: o"<number>";

<decimal_number> :: <number>;

<hexadecimal_number> :: h"<number>";

<number> :: = <binary_number> | <octal_number> | <decimal_number> | <hexadecimal_number>;

<word> :: = <letter> | <word> <letter>;

<name> :: = <word> | <word> <decimal_number>;

<group> :: = <name>[<decimal_number>..<decimal_number>];

<component_name> :: = <name> | <group>;

<node_name> :: = <name> | <group>;

<parametr_name> :: = <name>;

<state_name> :: = <name> | <group>;

<value> :: = <number>;

<input_value> :: = <value>;

<state_value> :: = <value>;

<verification_period_value> :: = <decimal_number>;

<verification_rate_value> :: = <decimal_number>;

<address> :: = <decimal_number>;

<operation_symbol> :: = & | AND | # | OR | ! | NOT | !& | NAND | !# | NOR | $ | XOR | !$ | XNOR | + | - | ^ | MOD | DIV | LOG2 | == | != | > | >= | < | <= ;

<expression> :: = (<node_name> | <parametr_name> | <state_name> | <number>) | <expression> <operation_symbol> <expression> ;

<statement> :: = <expression> | <value>;

<table_construction> :: = <CLT> | <TT> | <McT> | <CT>;

<program> :: = <table_construction> | <program> <table_construction>.

Розроблено семантику табличної мови THDL, що розкриває призначення чотирьох його конструкцій (таблиць логічних перетворень, переходів, мікроциклів і з'єднань) і встановлює загальні правила їх використання.

Запропоновано моделі програмування ПЛІС мовою THDL, які утворюють квадранти моделей (рис. 5) і відповідають стилям програмування: "від подій" (I), структурному (II), "від станів" (III), сентенціальному (IV).

Розроблено процедуру і інструментальні засоби програмування безпечних ПЛІС-контролерів з паралельною архітектурою, що представляють собою надбудову над існуючими САПР проектування цифрових пристроїв на основі ПЛІС. При цьому розроблений редактор введення описів - табличний редактор

Table Editor; редактор завдання умов забезпечення функціональної безпеки Safe-providing Editor; редактор настроювання функцій обміну даними і кодування вхідних і вихідних сигналів Interface Editor; автоматичний транслятор.

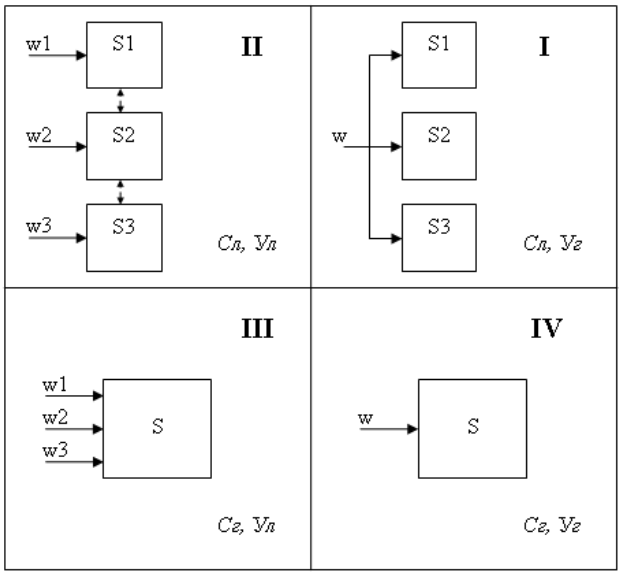


Рис. 5. Моделі програмування ПЛІС-контролерів

Запропоновані мова, технологія та інструментальні засоби програмування безпечних ПЛІС-контролерів з паралельною архітектурою дозволяють підвищити безпеку ПЗ при підготовці програм шляхом використання спрощених табличних конструкцій для опису алгоритмів, настройки функцій забезпечення безпеки і кодування вхідних і вихідних сигналів.

У п'ятому розділі розроблені та досліджені методи проектування і моделі пристроїв безпечного формування керуючих впливів. Запропоновані методи засновані на використанні принципу послідовного перетворення параметрів моделі пристрою формування керуючого впливу, які динамічно змінюються у часі. Запропоновано математичні моделі пристроїв безпечного формування вихідних керуючих впливів (ПБФ КВ) з послідовним, паралельним і змішаним з'єднанням каналів. Розроблено і досліджено математичну модель однофазних пристроїв безпечного формування гармонічного вихідного сигналу (ПБФ ГС), що описується кортежем

$$H = \{z, p_{11}, p_{12}, fg, f_1, f_2, n, l, s_1, s_2, \varphi, \chi\}, \qquad (4)$$

де p_{11} и p_{12} – параметри сигналів, що надходять з виходів першого та другого каналів ПБФ ГС, f_1, f_2 – частоти сигналів p_{11}, p_{12}, Гц; T_1, T_2 – періоди сигналів p_{11}, p_{12}, с; n – коефіцієнт, який визначає відношення періоду сигналу з меншим періодом на різницю періодів T_1 і T_2; s_1, s_2 – скважність сигналів p_1, p_2, %; φ – зсув фази між сигналами p_{11}, p_{12}, %; z – сигнал, отриманий у результаті застосування функції "Виключне АБО"для p_1 і p_2: $z = p_{11} \oplus p_{12}$; g – сигнал, що отриманий у результаті фільтрації високих частот сигналу z; fg – частота

сигналу g; l – співвідношення сумарної тривалості імпульсів і пауз сигналу z за обраний інтервал часу t (характеризує скважність сигналу z, що динамічно змінюється), %.

Зв'язок між компонентами кортежу визначається залежностями:

$$\begin{cases} z = p_{11} \oplus p_{12}; \\ f_1 = fg * (n+1); \\ f_2 = fg * n; \\ l = \chi(\varphi, s_1, s_2). \end{cases} \quad (5)$$

Розглянемо діаграму і графік залежності, наведені на рис. 6. Тут представлені результати математичного аналізу моделі при $s_1 = s_2 = 50$ %. На рис. 6 а наведені значення сигналів p_{11}, p_{12}, z при зміні зсув фаз φ, а на рис. 6 б представлена залежність $l = \chi(\varphi, s_1, s_2)$ при $s_1 = s_2 = 50$ %. Як видно з рисунка, форма залежності $l = \chi(\varphi, s_1, s_2)$ має вигляд трикутника, а функція χ описується залежностями:

$$l = \begin{cases} 2\varphi, & \text{при } \varphi < 50\ \%; \\ 2(100 - \varphi), & \text{при } \varphi > 50\ \%. \end{cases} \quad (6)$$

Аналогічну форму буде мати і формований вихідний сигнал.

Шляхом зміни параметрів s_1 і s_2, отримана така форма залежності $l = \chi(\varphi, s_1, s_2)$, при якій коефіцієнт нелінійних спотворень Ku є найменшим. При цьому встановлено, що оптимальним значенням параметра s_1 є 50 %. Для визначення оптимального значення параметра s_2 отримана залежність коефіцієнта Ku від s_2 при $s_1 = 50$ %

$$Ku = \frac{\sqrt{\left(\frac{\sin 3\pi s_2}{9}\right)^2 + \left(\frac{\sin 5\pi s_2}{25}\right)^2 + \left(\frac{\sin 7\pi s_2}{49}\right)^2}}{\sin \pi s_2}. \quad (7)$$

Чисельний метод розрахунку дозволив одержати криву залежності Ku від s_2 для значень s_2 у діапазоні від 0 до 50 % для 3, 5 і 7 гармонік, що наведена на рис. 7. Дослідження залежності $Ku = f(s_2)$ на екстремум дозволило визначити значення скважності s_2, при якому Ku досягає мінімального значення: $Ku_{min} = 4{,}3$ % при $s_2 = 34{,}5$ %.

Розроблено і досліджено математичну модель n-фазних ПБФ ГС. Математична модель трифазного ПБФ ГС описується кортежем

$$H^{(3)} = \{X, op, k_1, k_2, k_3, z_1, z_2, z_3, fg, fk, fop, n, l_1, l_2, l_3, \varphi_1, \varphi_2, \varphi_3, \chi\}, \quad (8)$$

де $X = \{L, R, N\}$ – множина вхідних станів (команд); L - вхідний стан, що відповідає команді на обертання фаз уліво; R - вхідний стан, що відповідає

команді на обертання фаз вправо; *N* - вхідний стан, що відповідає команді на відключення вихідного сигналу; *op* - опорний дискретний імпульсний сигнал; k_1 - вихідний дискретний імпульсний сигнал першого каналу; k_2 - вихідний дискретний імпульсний сигнал другого каналу; k_3 - вихідний дискретний імпульсний сигнал третього каналу; z_1 - вихідний ШІМ-сигнал першого каналу; z_2 - вихідний ШІМ-сигнал другого каналу; z_3 - вихідний ШІМ-сигнал третього каналу; *fg* - частота вихідного трифазного гармонічного сигналу; *fk* - частота вихідних дискретних імпульсних сигналів першого, другого і третього каналів; *fop* - частота опорного дискретного імпульсного сигналу; *n* - коефіцієнт, що визначає відношення періоду опорного сигналу на різницю періодів вихідного дискретного імпульсного сигналу і опорного сигналу, або кількість рівнів апроксимації вихідного трифазного гармонічного сигналу; l_1 - співвідношення сумарної тривалості імпульсів і пауз сигналу z_1 за обраний інтервал часу *t*; l_2 - співвідношення сумарної тривалості імпульсів і пауз сигналу z_2 за обраний інтервал часу *t*; l_3 - співвідношення сумарної тривалості імпульсів і пауз сигналу z_3 за обраний інтервал часу *t*; φ_1 - зсув фази між сигналами *op* і k_1; φ_2 - зсув фази між сигналами *op* і k_2; φ_3 - зсув фази між сигналами *op* і k_3; χ - функція, що описує залежність l_1, l_2, l_3 від φ_1, φ_2, φ_3 відповідно при заданих значеннях скважності $s_1 = 50$ % і $s_2 = 33$ %.

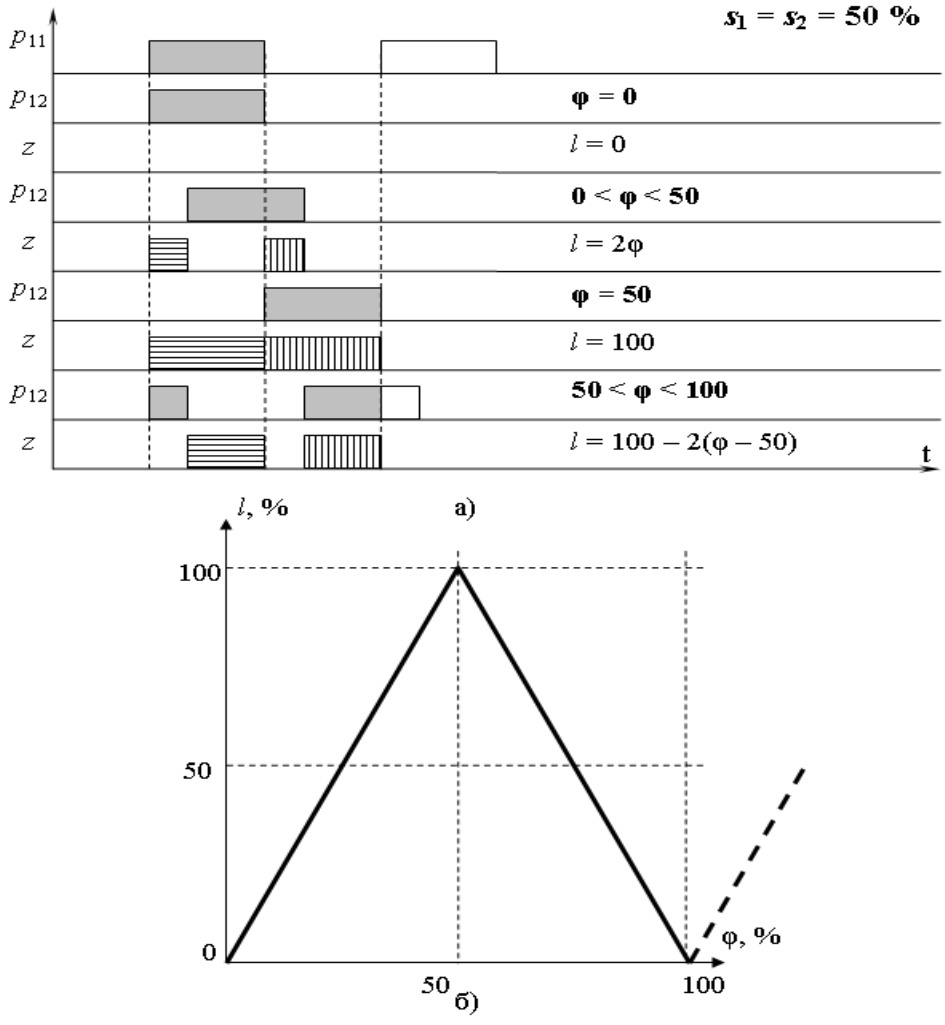


Рис. 6. Залежність $l = \chi(\varphi, s_1, s_2)$ при $s_1 = s_2 = 50$ %

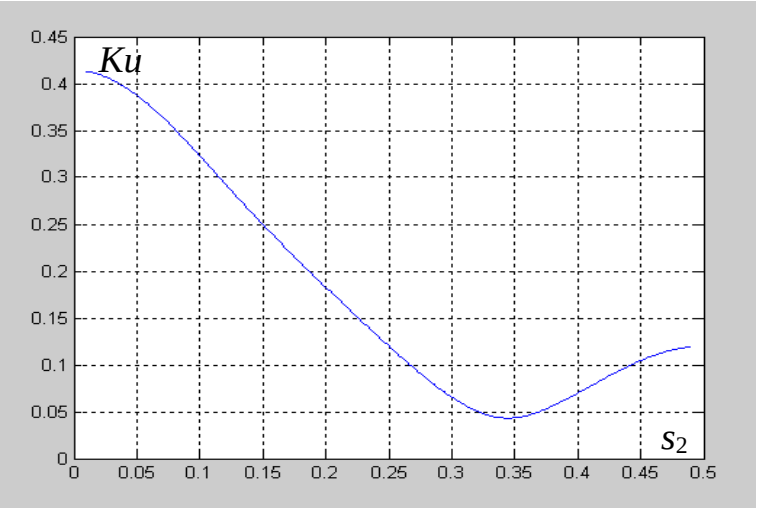


Рис. 7. Залежність коефіцієнта нелінійних спотворень *Ku* формованого сигналу від скважності s_2

Зв’язок між компонентами кортежу визначається залежностями:

$$\begin{cases} k_1(t-1) = k_3(t)\ \&\ L + k_2(t)\ \&\ R; \\ k_2(t-1) = k_1(t)\ \&\ L + k_3(t)\ \&\ R; \\ k_3(t) = \overline{k_1(t)\ \&\ k_2(t)\ \&\ N}; \\ z_1 = (k_1(t) \oplus op)\ \&\ \overline{N}; \\ z_2 = (k_2(t) \oplus op)\ \&\ \overline{N}; \\ z_3 = (k_3(t) \oplus op)\ \&\ \overline{N}; \\ fop = fg * (n+1); \\ fk = fg * n; \\ l_1 = \chi(\varphi_1); \\ l_2 = \chi(\varphi_2); \\ l_3 = \chi(\varphi_3). \end{cases} \qquad (9)$$

Розроблено методику розрахунку параметрів моделі *n*-фазних ПБФ ГС, що дозволяє визначити значення параметрів моделі для формування *n*-фазних гармонічних керуючих сигналів із заданими частотою і кількістю рівнів апроксимації.

Розроблено і досліджено HDL-моделі *n*-фазних ПБФ ГС. При цьому HDL-опис ПБФ ГС виконано на запропонованій в розд. 4 мові THDL. Аналіз результатів комп'ютерного моделювання моделей показав, що запропонований метод реалізації і моделі ПБВ КВ з використанням принципу послідовного перетворення параметрів сигналів, що динамічно змінюються у часі, дозволяє виконувати безпечне сполучення виконавчих механізмів і мікроелектронних структур з асинхронно функціонуючими каналами, причому відключення хоча б одного з каналів приводить до принципової неможливості формування на виході небезпечного керуючого впливу.

У шостому розділі представлені результати практичної реалізації розроблених методів і засобів проектування технічних і програмних

компонентів безпечних ПЛІС-контролерів з паралельною архітектурою. При цьому використані наступні моделі, методи і інструментальні засоби: моделі і методи синтезу БЛП-автоматів - при розробці та проектуванні безпечних модулів логічної обробки інформації на основі ПЛІС; мова, технологія і інструментальні засоби програмування безпечних ПЛІС-контролерів - при проектуванні ПЗ для безпечних логічних ПЛІС-контролерів (БЛК) і розробці безконтактного модуля керування стрілкою (БМК-С); методи проектування і моделі ПБФ КВ - при розробці генератора автоматичного регулювання швидкості (Г-АРС), безконтактного модуля керування стрілкою (БМК-С), безконтактного модуля керування сигналами світлофора (БМК-СС)

Отримані результати лабораторних досліджень і виробничих випробувань безпечних ПЛІС-контролерів у складі мікроелектронної системи централізації (МСЦ) підтверджують відповідність розроблених у дисертації теоретичних положень і технічних рішень вимогам українських та міжнародних стандартів до функціональної безпеки та електромагнітної сумісності.

Сьомий розділ присвячений оцінці ефективності виконаних досліджень. Виконано оцінку безпеки БЛП-автоматів з керуванням функціональною деградацією. При цьому показано, що останов або часткова втрата працездатності пов'язані із введенням певних ризиків, обумовлених збільшенням ролі людського фактора в процесах керування об'єктами критичного застосування, що необхідно враховувати при інтегральній оцінці функціональної безпеки ТПК СКЗ. Запропоновано розглядати деградацію ТПК СКЗ як процес перерозподілу елементів множини відповідальних функцій $\Phi_r = \{ \Phi_{r(cs)}, \Phi_{r(dm)}, \Phi_{r(u)} \}$ між його підмножинами: відповідальних функцій, реалізуємих системою керування (СК) $\Phi_{r(cs)} = \{\phi_{r(cs)1}, \phi_{r(cs)2}, \ldots, \phi_{r(cs)Nr(cs)}\}$, відповідальних функцій, реалізуємих особою, що приймає рішення (ОПР) $\Phi_{r(dm)} = \{\phi_{r(dm)1}, \phi_{r(dm)2}, \ldots, \phi_{r(dm)Nr(dm)}\}\}$, і функцій, які не можуть бути реалізовані на даному рівні деградації $\Phi_s = \{\phi_{s1}, \phi_{s2}, \ldots, \phi_{sNs}\}$. Розглянуто клас задач, що описуються графом безпечних переходів, які мають ієрархічну структуру. У рамках задач даного класу відповідальні функції з множини $\Phi_{r(cs)}$, які не можуть бути реалізовані СК в умовах деградації, покладають на ОПР і переходять у множину $\Phi_{r(dm)}$. Отримано аналітичну залежність для оцінки підвищення безпеки при реалізації алгоритму керування деградацією

$$\frac{\lambda_{1df}}{\lambda_{1df}'} = \frac{1 + P_{1(dm)}\, j}{1 + \dfrac{P_{1(dm)}}{z}\, j}, \qquad (10)$$

де λ_{1df} - інтенсивність небезпечних відмов (dangerous failure) при реалізації однієї відповідальної функції; λ_{1df}' - інтенсивність небезпечних відмов при реалізації однієї відповідальної функції при реалізації процедури керування функціональною деградацією; $P_{1(dm)}$ – імовірність приналежності даної відповідальної функції множині $\Phi_{r(dm)}$ у деякий довільний момент часу; z –

коефіцієнт, що враховує зменшення інтенсивності переходів відповідальної функції з підмножини $\Phi_{r(cs)}$ в $\Phi_{r(dm)}$ $\lambda_{1(cs\text{-}dm)}$ за рахунок реалізації процедури керування функціональною деградацією

$$z = \frac{\lambda_{1(cs-dm)}}{\lambda_{1(cs-dm)}'}; \qquad (11)$$

j – коефіцієнт, що визначає відношення інтенсивності небезпечних відмов ОПР $\lambda_{1df(dm)}$ і СК $\lambda_{1df(cs)}$ при реалізації однієї відповідальної функції

$$j = \lambda_{1df(dm)} / \lambda_{1df(cs)}. \qquad (12)$$

Розрахунки показали, що застосування для задач розглянутого класу процедури синтезу БЛП-автоматів з керуванням деградацією, запропонованої в розд. 2, дозволяє зменшити інтенсивність небезпечних відмов в 1,2 - 1,38 разів залежно від кількості рівнів деградації.

Виконано порівняльну оцінку безпеки ПЗ, реалізованого на табличній і текстовій мовах опису апаратури. Запропоновано вдосконалений метод оцінки складності ПЗ, який представляє собою розширення методу Чепіна, що враховує ієрархічний принцип опису цифрових пристроїв на ПЛІС і можливість використання готових компонентів (мегафункцій).

Для прогнозної оцінки ефективності використання мови THDL як альтернативи відомим текстовим мовам опису апаратури при розв'язанні типових задач використана наступна методика:

1. Обрано n типових задач із різним рівнем складності.

2. Розраховано складність обраних задач $Q = \{Q1, Q2, \ldots Qn\}$ відповідно до запропонованого розширення метрики Чепіна.

3. Розраховано прогнозну кількість помилок для обраних задач $B = \{B1, B2, \ldots Bn\}$ відповідно до метрики Холстеда при розробці HDL-описів на мовах AHDL ($B^{(A)} = \{B^{(A)}1, B^{(A)}2, \ldots B^{(A)}n\}$) і THDL ($B^{(T)} = \{B^{(T)}1, B^{(T)}2, \ldots B^{(T)}n\}$).

4. Отримані за результатами статистичних досліджень експериментальні значення кількості помилок при розробці HDL-описів на мовах AHDL ($B^{(A)}_э = \{B^{(A)}_э1, B^{(A)}_э2, \ldots B^{(A)}_эn\}$) і THDL ($B^{(T)}_э = \{B^{(T)}_э1, B^{(T)}_э2, \ldots B^{(T)}_эn\}$).

5. Розраховано відносні значення метрики $Boi = B^{(A)}i / B^{(T)}i$.

6. Розраховано відносні значення метрики $Bo_эi = B^{(A)}_эi / B^{(T)}_эi$.

7. Розраховано значення коефіцієнтів $Vpi = (Boi - 1)/(Bo_эi - 1)$.

8. Побудовано залежності $Vp = f1(Q)$ та $Boэ = f2(Q)$.

Графік залежності кількості помилок у програмі $Boэ$ від складності Q $Boэ = f2(Q)$ наведений на рис. 8. Як показують експериментальні дослідження, значення $Boэ$ може коливатися в межах 2 - 5, при цьому закономірності в зміні $Boэ$ залежно від складності Q не спостерігається.

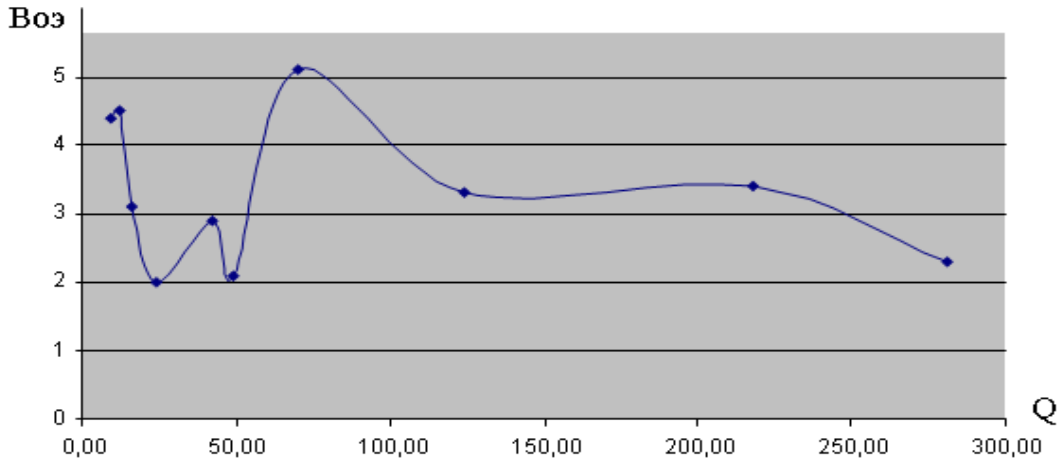


Рис. 8. Залежність кількості помилок у програмі *Воэ* від складності *Q*

Аналіз графіка залежності вагового коефіцієнта *Vp* від складності *Q* *Vp* = *f*1*(Q)* (рис. 9) показує, що коефіцієнт *Vp* змінюється в діапазоні 0,57 - 0,86, причому він має тенденцію знижуватися при зростанні значення складності *Q*. При *Q* > *40* діапазон змін коефіцієнта *Vp* зменшується і обмежується значеннями 0,57 - 0,7.

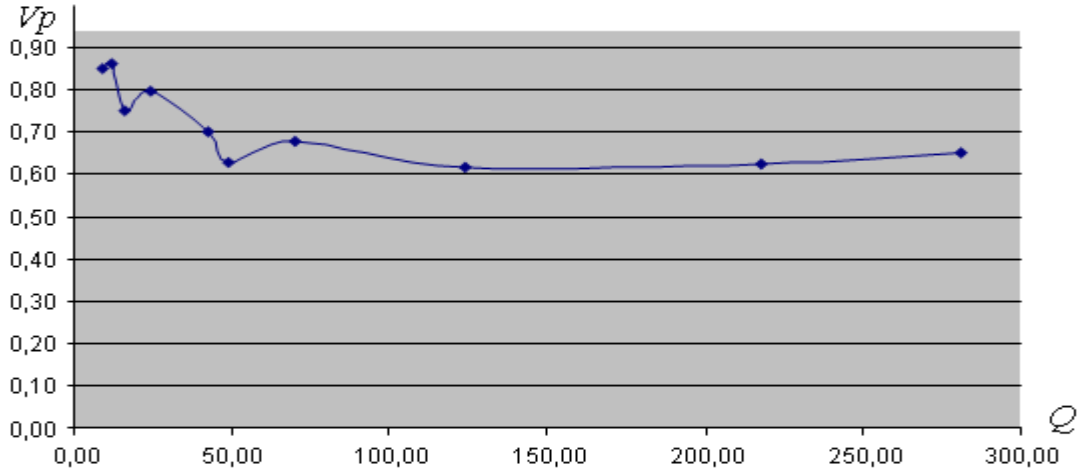


Рис. 9. Залежність вагового коефіцієнта *Vp* від складності *Q*

Таким чином, для оцінки зниження ймовірності появи помилок у програмі при використанні мови THDL як альтернативи відомим текстовим мовам опису апаратури, доцільно використовувати коефіцієнт *Vp*. При цьому необхідно виконати розрахунок метрики складності *Q* відповідно до запропонованого вище розширення методу Чепіна та метрики кількості помилок (відносного значення) відповідно до методу Холстеда. Якщо складність програми *Q* < *40*, то діапазон значень *Vp* повинен становити 0,7 - 0,86; якщо *Q* > *40*, то діапазон значень *Vp* повинен становити 0,57 - 0,7.

Виконано порівняльну оцінку функціональної безпеки розроблених і відомих пристроїв формування керуючих впливів. На рис. 10, який ілюструє модель відомого пристрою формування керуючих впливів, Ар Вр – стан із працездатними каналами А і В; Ар Во - стан із працездатним каналом А та

несправним каналом В; Ао Вр - стан із працездатним каналом В та несправним каналом А (із захисною відмовою); Ао Во - стан з несправними каналами А і В (небезпечне); λ_a – інтенсивність відмов, пов'язаних з порушенням функцій формування керуючих впливів; $\lambda_к$ - інтенсивність відмов, пов'язаних з порушенням контрольних функцій; μ - інтенсивність відновлень.

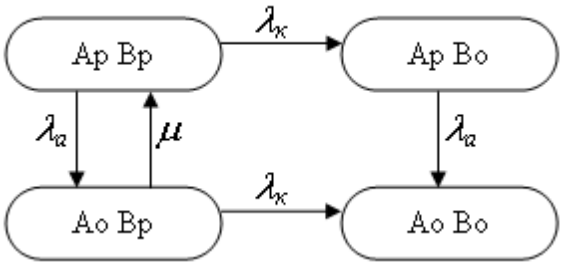


Рис. 10. Діаграма станів відомого пристрою формування керуючих впливів

Рис. 11 ілюструє модель розробленого пристрою формування керуючих впливів.

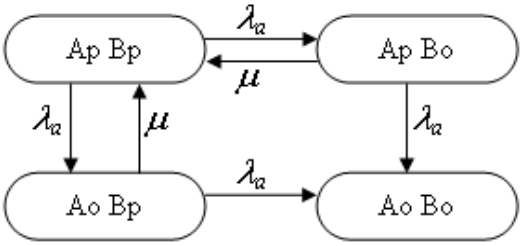


Рис. 11. Діаграма станів розробленого пристрою формування керуючих впливів

У логарифмічній шкалі залежність $P3(\lambda_к, \lambda_a)$ для відомого варіанта описується площиною (див. рис. 12) та має вигляд

$$\lg P3 = \lg \lambda_к + \lg \lambda_a + 9{,}6. \qquad (13)$$

У логарифмічній шкалі залежність $P3(\mu, \lambda_a)$ для відомого варіанта також описується площиною (див. рис. 13) та має вигляд

$$\lg P3 = 2\lg\lambda_a - \lg \mu + 5{,}2. \qquad (14)$$

Оскільки обидві залежності в логарифмічній шкалі описуються площинами, їхнє подання в чотирьохмірному просторі з осями (-lg P3), (-lg $\lambda_к$), (-lg λ_a) і (-lg μ) дасть дві чотирьохмірних поверхні, причому тривимірна поверхня, що утвориться при перетинанні чотирьохмірних площин буде відповідати границі ефективної області використання нового методу.

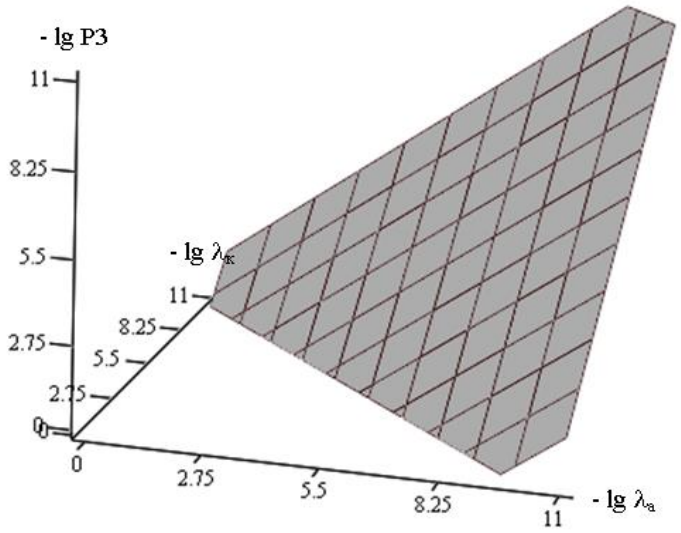


Рис. 12. Залежність $РЗ(\lambda_к, \lambda_a)$ у логарифмічній шкалі для відомого варіанта

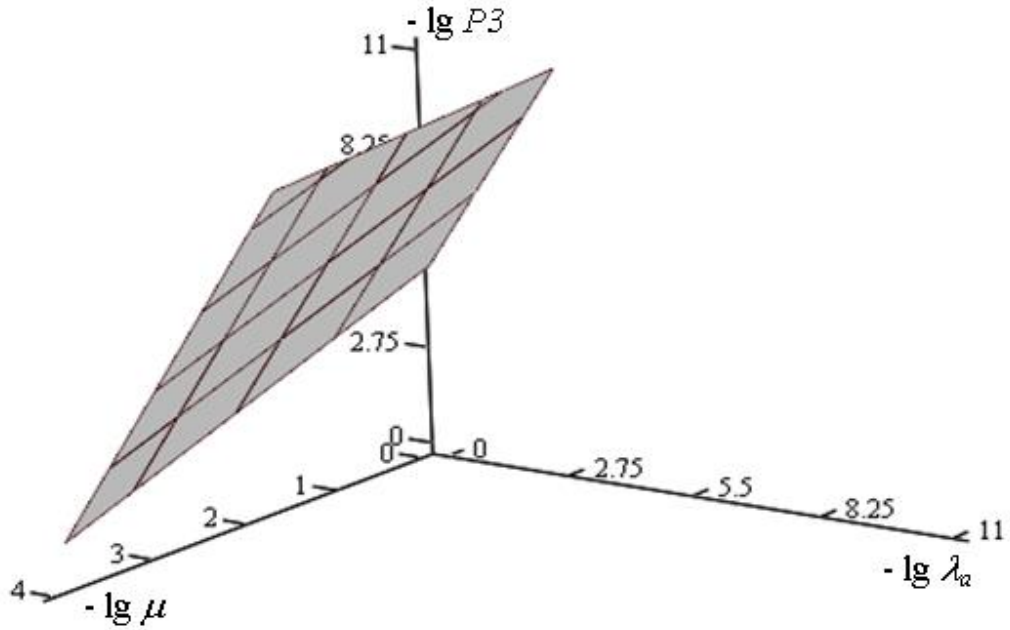


Рис. 13. Залежність $РЗ(\mu, \lambda_a)$ у логарифмічній шкалі для нового варіанта

Рівняння для тривимірної площини перетинання має вигляд

$$\mu = (\lambda_a \ / \ \lambda_к) * 10^{-4,4}. \qquad (15)$$

Таким чином, область, розташована над поверхнею $\mu = f(\lambda_a, \lambda_к)$ (рис. 14) є областю ефективного використання розробленого в розд. 5 методу формування керуючих впливів для об'єктів критичного застосування (ОКЗ). Для того, щоб визначити, у скільки разів знижується ймовірність при використанні

розробленого методу $РЗ_H$ у порівнянні з відомим $РЗ_U$, необхідно скористатися вираженням

$$\frac{РЗ_U}{РЗ_H} = \frac{\lambda_k \cdot \mu}{\lambda_a \cdot 10^{-4,4}} \cdot \qquad (16)$$

Таким чином, використання розроблених моделей і методів побудови пристроїв формування *n*-фазних гармонічних сигналів дозволяє істотно підвищити показники функціональної безпеки для широкого діапазону значень інтенсивностей відмов і відновлень.

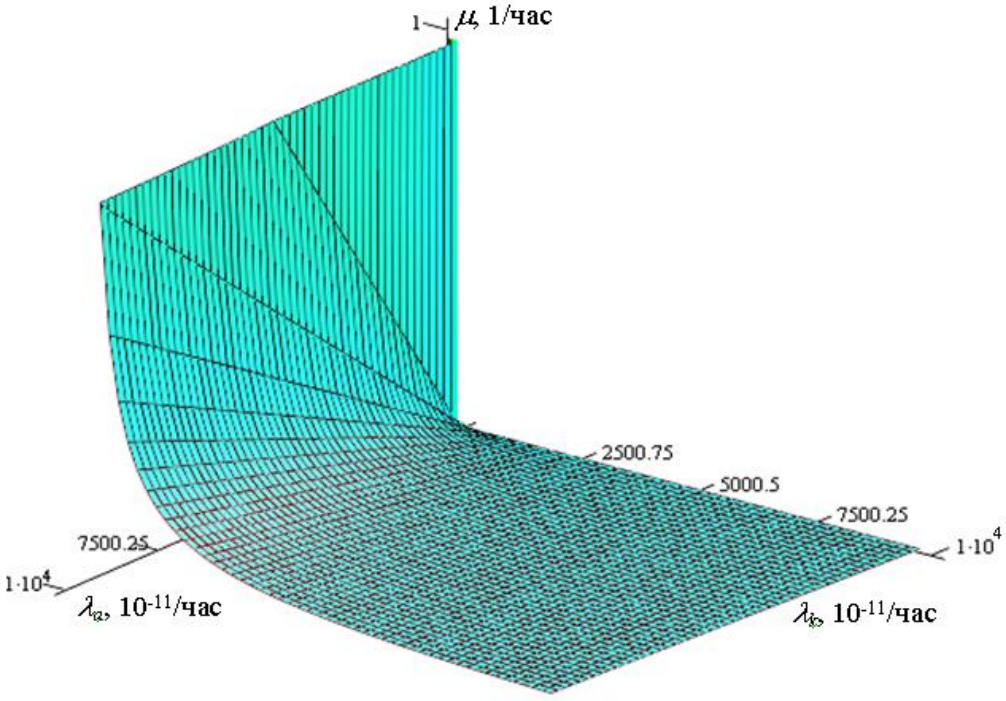


Рис. 14. Залежність $\mu = f(\lambda_a, \lambda_к)$, яка визначає область ефективного використання розробленого методу

У додатках наведено результати математичного та комп'ютерного моделювання розроблених безпечних автоматів з функціональною деградацією, HDL-моделі БЛП-автоматів та пристроїв безпечного формування керуючих впливів, акти впроваджень та розрахунки якісних показників програмного забезпечення на мові THDL.

ВИСНОВКИ

У дисертації запропоновано узагальнення і розв'язання науково-прикладної проблеми розробки та реалізації методів і засобів проектування технічних і програмних компонентів безпечних ПЛІС-контролерів з паралельною архітектурою з метою підвищення показників безпеки систем критичного застосування.

Основні наукові і практичні результати роботи полягають у наступному:

1. Виконано аналіз методів і засобів проектування комп'ютерних систем і компонентів критичного застосування і тенденцій їхнього розвитку, на основі якого сформульована проблема і задачі дослідження, обґрунтовані концепція та методика проведення досліджень.

2. Розроблено методологію синтезу, розроблені та досліджені абстрактні, структурні та HDL-моделі безпечних логічних автоматів для ПЛІС-контролерів з паралельною архітектурою, аналіз яких показав, що синтезовані формальні моделі та методи є універсальним апаратом для опису дискретних пристроїв і систем з реалізацією функцій забезпечення безпеки керування, що забезпечує можливість формалізованого проектування безпечних ПЛІС-контролерів з паралельною архітектурою, у тому числі: розробки і формального опису процедур керування ОКЗ, їхньої верифікації, синтезу архітектури і HDL-описів програмних і технічних компонентів.

3. Запропоновано процедури абстрактного синтезу БЛП-автоматів з функціональною деградацією забезпечують збереження максимально можливої кількості реалізованих автоматом відповідальних функцій в умовах наявності спотворень при безумовному забезпеченні безпеки.

4. Розроблено мову, технологію та інструментальні засоби проектування програмного забезпечення для безпечних ПЛІС-контролерів з паралельною архітектурою з використанням спрощених табличних конструкцій для опису алгоритмів, настройки функцій забезпечення безпеки та кодування вхідних і вихідних сигналів, що дозволяє зменшити кількість помилок і за рахунок цього підвищити безпеку ПЗ.

5. Отримано метод реалізації та моделі безконтактних модулів безпечного формування керуючих впливів, які, на відміну від відомих, базуються на використанні принципу послідовного перетворення параметрів сигналів, що динамічно змінюються у часі, що дозволяє виконувати безпечне сполучення виконавчих механізмів і мікроелектронних структур з асинхронно функціонуючими каналами, які резервуються, причому відключення хоча б одного з каналів приводить до принципової неможливості формування на виході небезпечного керуючого впливу.

6. Дослідження залежності коефіцієнта нелінійних спотворень вихідного сигналу розробленого *n*-фазного пристрою безпечного формування гармонічних сигналів від скважності ВЧ-сигналу на виході одного з перетворювачів $Ku = f(s_2)$ на экстремум дозволило визначити значення скважності (s_2 = 34,5 % або s_2 = 65,5 %), при яких Ku досягає мінімального значення ($Ku_{\min}$ = 4,3 %), і за рахунок цього забезпечити підвищення якості керування ОКЗ.

7. Дослідження математичної моделі *n*-фазних ПБФ ГС показали, що: зсув фаз між вихідними гармонічними сигналами, формуємими шляхом фільтрації ВЧ-складової сигналів, z_1, z_2, ... z_n, відповідає зрушенню фаз між дискретними імпульсними сигналами керування k_1, k_2, ... k_n, що дозволяє забезпечити безпеку керування *n*-фазними виконавчими механізмами; реалізація рівнянь моделі забезпечує можливість керування напрямком

обертання фаз або відключення вихідного сигналу шляхом зміни вхідного стану моделі; перехід у захисний стан одного з каналів, а також відключення опорного сигналу приводить до принципової неможливості формування вихідного сигналу, що дозволяє використовувати опорний сигнал для переводу ПБФ ГС у захисний стан при виявленні відмов.

8. Запропоновано метод розрахунку параметрів моделі безпечних *n*-фазних ПБФ ГС, що дозволяє визначити значення параметрів моделі для заданих значень частоти формуємого *n*-фазного сигналу, кількість рівнів апроксимації і частоти сигналу тактування.

9. Розроблено HDL-модель *n*-фазних ПБФ ГС, що реалізована на запропонованій мові опису апаратури THDL, яка являє собою функціонально-завершений програмний компонент безпечних ПЛІС-контролерів з паралельною архітектурою та дозволяє використовувати формальну процедуру проектування ПЗ шляхом програмної настройки параметрів даного компонента.

10. Створено систему керування ОКЗ на основі безпечних ПЛІС-контролерів з паралельною архітектурою - мікроелектронну систему централізації (МСЦ) для залізничного транспорту і метрополітенів. При розробці системи керування ОКЗ на базі безпечних ПЛІС-контролерів з паралельною архітектурою були використані: математичні моделі та методи синтезу БЛП-автоматів – при розробці та проектуванні безпечних модулів логічної обробки інформації на основі ПЛІС; мова, технологія та інструментальні засоби програмування безпечних ПЛІС-контролерів – при проектуванні ПЗ для безпечних логічних ПЛІС-контролерів (БЛК) і розробці безконтактного модуля керування стрілкою (БМК-С); методи проектування і моделі ПБФ КВ - при розробці генератора автоматичного регулювання швидкості (Г-АРС), безконтактного модуля керування стрілкою (БМК-С), безконтактного модуля керування сигналами світлофора (БМК-СС).

11. Отримані результати лабораторних досліджень і виробничих випробувань безпечних ПЛІС-контролерів у складі мікроелектронної системи централізації (МСЦ) підтверджують відповідність розроблених у дисертації теоретичних положень і технічних рішень вимогам українських та міжнародних стандартів до функціональної безпеки та електромагнітної сумісності.

12. Аналіз і розрахунок показників безпеки ТПК СКЗ із урахуванням ризиків, обумовлених збільшенням ролі людського фактора в процесах керування об'єктами критичного застосування в умовах деградації показав, що застосування для задач розглянутого класу методів синтезу БЛП-автоматів з функціональною деградацією, запропонованих у розд. 2, 3, дозволяє зменшити інтенсивність небезпечних відмов в 1,2 - 1,38 разів.

13. Виконаний розрахунок і проведені експериментальні дослідження показують, що використання мови THDL як альтернативи відомим мовам опису апаратури, дозволяє підвищити функціональну безпеку програмного забезпечення за рахунок зниження кількості помилок у програмі в 2 - 5 разів для задач різних класів і рівнів складності.

14. Запропоновано розширення метрики Чепіна, що дозволяє оцінювати складність HDL-описів *Q* з урахуванням можливості використання

верифікованих програмних компонентів і ієрархічного принципу опису цифрових пристроїв на основі ПЛІС.

15. Порівняльна оцінка функціональної безпеки безконтактних модулів безпечного формування керуючих впливів показала, що використання розроблених методів проектування і моделей пристроїв безпечного формування гармонічних сигналів дозволяє істотно підвищити показники функціональної безпеки для широкого діапазону значень інтенсивностей відмов і відновлень. Зокрема, при інтенсивності відмов пристроїв формування сигналів $\lambda_a = 10^{-7}$ 1/годину, контрольних засобів $\lambda_к = 10^{-10}$ 1/годину, відновлень $\mu = 0{,}5$ 1/годину ймовірність небезпечної відмови $P3(t)$ за 10 років експлуатації знижується в 12,56 разів.

16. Результати дисертаційних досліджень впроваджені на Харківському метрополітені, що підтверджується відповідними актами.

СПИСОК ОПУБЛІКОВАНИХ РОБІТ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Малиновский М. Л. Проектирование цифровых устройств на ПЛИС / М. Л. Малиновский, И. А. Фурман, С. Я. Бовчалюк ; под ред. И. А. Фурмана. – Харків: Факт, 2006. – 164 с.

Здобувачем розроблено структурні та HDL-моделі цифрових автоматів з несиметричними відмовами.

2. Малиновский М. Л. Контроллеры и процессоры с параллельной архитектурой / И. А. Фурман, В. А. Краснобаев, М. Л. Малиновский, С. В. Панченко ; под ред. Г. И. Загария. – Харків: УкрГАЖТ, 2006. – 416 с.

Здобувачем розроблено методи синтезу та досліджено моделі безпечних автоматів.

3. Малиновский М. Л. Управление объектами критического применения на основе ПЛИС : моногр. / М. Л. Малиновский. – Харків: Факт, 2008. – 224 с., 67 ил.

4. Малиновский М. Л. Система обработки информации и управления АСУ ТП на основе применения кодов модулярной арифметики: моногр. / В. И. Барсов, В. А. Краснобаев, И. А. Фурман, М. Л. Малиновский, В. В. Шевченко. – Харків: УИПА, 2009. – 160 с.

Здобувачем запропоновано методи введення несиметричності відмов цифрових пристроїв шляхом корекції помилок систем, що функціонують у медулярній арифметиці.

5. Малиновский М. Л. Модели и методы параллельной реализации логических операций в АСУ ТП: моногр. / В. И. Барсов, И. А. Фурман, М. Л. Малиновский, В. А. Краснобаев, В. В. Шевченко. – Харків: УИПА, 2009. – 140 с.

Здобувачем розроблено методи безпечної паралельної реалізації логічних операцій в АСКТП.

6. Малиновский М. Л. Новая концепция и перспективные средства реализации микроэлектронных систем автоматизированного управления

движением поездов на метрополитенах / М. Л. Малиновский // Інформаційно-керуючі системи на залізничному транспорті. – 2005. – № 4. – С. 44–48.

7. Малиновський М. Л. Вдосконалення архітектури програмованих логічних контролерів паралельної дії / І. О. Фурман, С. Я. Бовчалюк, М. Л. Малиновський // Вісник Харківського національного технічного університету сільського господарства – 2005. – т. 2 – С. 164–168.

Здобувачем запропоновано архітектуру паралельного логічного контролера, яка є захищеною від небезпечних відмов при наявності одиночних дефектів.

8. Малиновский М. Л. Концепция, методы и средства моделирования на ПЛИС контроллеров и процессоров с параллельной архитектурой / И. А. Фурман, В. А. Краснобаев, М. Л. Малиновский, С. А. Кошман, С. Я. Бовчалюк // Сборник научных трудов Харьковского национального автодорожного университета. – Харьков, 2005. – Вып. 16 – С. 338–341.

Здобувачем розроблено HDL-моделі безпечних автоматів з паралельною архітектурою.

9. Малиновский М. Л. Новая концепция разработки и структурная организация безопасной системы автоматизированного управления движением поездов на метрополитенах / Фурман І. О., Малиновский М. Л. // Радіоелектронні і комп'ютерні системи. – 2006. №5. - С. 97 – 102.

Здобувачем запропоновано концепцію розробки системи керування рухом поїздів.

10. Малиновський М. Л. Оптимізація архітектури та схемотехніки каналів обміну даними між безпечними ПЛІС-контролерами паралельної дії / М. Л. Малиновский // Вісник Харківського національного технічного університету сільського господарства. – 2006. – Вип. 43, т. 2 – С. 123–127.

11. Малиновський М. Л. Удосконалення методів проектування програмного забезпечення для мікроелектронних систем керування технологічним обладнанням / М. Л. Малиновський, І. О. Фурман, О. Ю. Аллашев // Вісник Харківського національного технічного університету сільського господарства. – 2006. – Вип. 43, т. 1 – С. 202–206.

Здобувачем запропоновано технологію проектування програмного забезпечення для систем критичного застосування.

12. Малиновський М. Л. Методы, схемотехника и протоколы передачи информации в сетях ПЛИС-контроллеров параллельного действия / І. О. Фурман, М. Л. Малиновський, А. В. Святобатько, С. Я. Бовчалюк, С. М. Тихонравов // Праці / Таврійська держ. агротехн. акад. – Мелітополь, 2006. – Вип. 43. – С. 3–10.

Здобувачем розроблено HDL-модель пристрою обміну інформацією між паралельними ПЛІС-контролерами.

13. Малиновський М. Л. Синтез керуючих автоматів циклічної дії (цикломатів) / М. Л. Малиновський, І. О. Фурман, О. Ю. Аллашев, С. М. Тихонравов // Вісник Харківського національного технічного університету сільського господарства – 2007. – Вип. 57, т. 2 – С. 92–99.

Здобувачем розроблено математичну модель автомата циклічної дії.

14. Малиновский М. Л. Математические модели безопасных ПЛИС-контроллеров с параллельной архитектурой / М. Л. Малиновский // Радіоелектронні і комп'ютерні системи. – 2007. – №7. – С. 105–113.

15. Малиновский М. Л. Методы проектирования программного обеспечения для ПЛИС-контроллеров на табличном языке CycloGraF / М. Л. Малиновский // Радіоелектронні і комп'ютерні системи. – 2008. – №5 (32). – С. 168–172.

16. Малиновський М. Л. Опыт и перспективы параллельной реализации алгоритмов логического управления объектами критического применения / И. А. Фурман, М. Л. Малиновский, А. Ю. Аллашев, С. Я. Бовчалюк // Радіоелектронні і комп'ютерні системи. – 2008. – № 6 (33). – С. 245–250.

Здобувачем досліджено історію розвитку систем паралельного керування об'єктами критичного застосування.

17. Малиновский М. Л. Абстрактный синтез безопасных параллельных логических автоматов циклического действия / М. Л. Малиновский // Праці / Таврійська держ. агротехн. акад. – Мелітополь, 2008. – Вип. 8, том 2. – С. 63–71.

18. Малиновський М. Л. Проблемно-орієнтована таблична мова алгоритмів логічного керування технологічним обладнанням / М. Л. Малиновський, І. О. Фурман, С. Я. Бовчалюк, О. Ю. Аллашев // Вісник Харківського національного технічного університету сільського господарства. – 2008. – Вип. 73, т. 2 – С. 52–54.

Здобувачем запропоновано табличні конструкції для програмування пристроїв автоматизації виробничих процесів.

19. Малиновський М. Л. Концепція розробки промислового зразка ПЛІС-контролера паралельної дії / І. О. Фурман, М. Л. Малиновський, С. Я. Бовчалюк // Вісник Харківського національного технічного університету сільського господарства. – 2008. – Вип. 73, т. 2 – С. 96 – 97.

Здобувачем розроблено структурні моделі та програмне забезпечення для універсального ПЛІС-контролера промислового призначення.

20. Малиновський М. Л. Підвищення ефективності побудови систем керування аварійним захистом АЕС на основі безпечних ПЛІС-контролерів з паралельною архітектурою / Кощей Л. Д., Тертишний С. М., Борисенко В. А., Фурман І. О., Малиновський М. Л. // Вісник Харківського національного технічного університету сільського господарства. – 2008. – Вип. 73, т. 2 – С. 35 – 38.

Здобувачем запропоновано архітектуру ПЛІС-контролера для системи керування аварійним захистом АЕС.

21. Малиновський М. Л. Методи абстрактного синтезу безпечних автоматів / Малиновський М. Л., Алєнін Д. О. // Вісник Харківського національного технічного університету сільського господарства. – 2009. – Вип. 87 – С. 74 – 76.

Здобувачем розроблено методи абстрактного синтезу автоматів з несиметричними відмовами різних класів.

22. Малиновський М. Л. Розробка абстрактних, структурних та HDL-

моделей автоматів циклічної дії / Фурман І. О., Барсов В. І., Малиновський М. Л., Аллашев О. Ю., Тихонравов С. М., Алєнін Д. О. // Вісник Харківського національного технічного університету сільського господарства. – 2009. – Вип. 87 – С. 77 – 80.

Здобувачем розроблено абстрактні і HDL-моделі автоматів циклічної дії.

23. Малиновский М. Л. Метод безопасного формирования гармонических управляющих сигналов / М. Л. Малиновский // Інформаційно-керуючі системи на залізничному транспорті. – 2009. - № 1. С. 22 – 26.

24. Малиновский М. Л. Оценка сложности HDL-описаний цифровых устройств / М. Л. Малиновский // Радіоелектронні і комп'ютерні системи. – 2009. – № 5 (39). – С. 171 – 175.

25. Малиновский М. Л. Программирование безопасных ПЛИС-контроллеров на табличном языке THDL / М. Л. Малиновский // Інформаційно-керуючі системи на залізничному транспорті. – 2009. - № 2. С. 18 – 23.

26. Малиновский М. Л. Модели и методы управления объектами критического применения на основе безопасных ПЛИС-контроллеров с параллельной архитектурой / М. Л. Малиновский // Радіоелектронні і комп'ютерні системи. – 2009. – № 6 (40). – С. 36 – 40.

27. Пат. 71200 Україна, МПК (2006) G 05 B 19/05, G 06 F 9/00. Програмований логічний контролер / Фурман І. О., Бовчалюк С. Я., Малиновський М. Л. (Україна).; заявители и патентообладатели Фурман І. О., Бовчалюк С. Я., Малиновський М. Л. – № 20031210864 ; заявл. 01.12.03; опубл. 15.05.06, Бюл. № 5. – 4 с. : ил.

Здобувачем удосконалено архітектуру програмованого логічного контролера шляхом введення блоку пам'яті заборонених станів.

28. Пат. 77886 Україна, МПК (2006) G 05 B 19/18, G 05 B 19/05. Програмований логічний контролер. Фурман І. О., Бовчалюк С. Я., Малиновський М. Л. (Україна) ; заявители и патентообладатели Фурман І. О., Бовчалюк С. Я., Малиновський М. Л. – № a200506855 ; заявл. 11.07.05 ; опубл. 15.01.07, Бюл. №1. – 4 с. : ил.

Здобувачем удосконалено архітектуру програмованого логічного контролера шляхом введення блоку вибору логічних операцій.

29. Пат. 82759 Україна, МПК (2006) G 05 B 19/18. Програмований логічний контролер / Малиновський М. Л., Кулик П. Д., Філіппович В. П., Фурман І. О. (Україна) ; заявитель и патентообладатель ТОВ НКП Укртрассигнал. – № a200608437 ; заявл. 27.07.06 ; опубл. 12.05.08, Бюл. №9. – 4 с. : ил.

Здобувачем удосконалено архітектуру програмованого логічного контролера шляхом введення блоків, що забезпечують динамічне перетворення інформації за забезпечують таким чином несиметричність відмов.

30. Пат. 33091 Україна, МПК (2006) G 05 B 19/18. Спосіб автоматичного перетворення технологічної циклограми у програмний код логічних контролерів / Фурман І. О., Малиновський М. Л., Бовчалюк С. Я., Аллашев О. Ю. (Україна) ; заявители и патентообладатели Фурман І. О., Малиновський М. Л., Бовчалюк С. Я., Аллашев О. Ю. – № u200801479 ; заявл.

05.02.08 ; опубл. 10.06.08, Бюл. №11. – 1 с.:ил.

Здобувачем розроблено форму технологічної циклограми, що одночасно є конструкцією програмування засобів автоматизації.

31. Пат. 37285 Україна, МПК (2006) G 05 B 19/18. Спосіб автоматичного синтезу ПЛІС-контролера по технологічній циклограмі. Фурман І. О., Малиновський М. Л., Бовчалюк С. Я., Аллашев О. Ю. (Україна) ; заявители и патентообладатели Фурман І. О., Малиновський М. Л., Бовчалюк С. Я., Аллашев О. Ю. – № u200806966 ; заявл. 20.05.08 ; опубл. 25.11.08, Бюл. №22. – 2 с.: ил.

Здобувачем запропоновано табличний процесор, який автоматично перетворює технологічну циклограму в HDL-код.

32. Пат. 39228 Україна, G05B19/18/. Спосіб безпечного формування гармонічного сигналу з використанням широтно-імпульсної модуляції (ШІМ) / Аллашев А. Ю., Бовчалюк С. Я., Борисенко В. А., Бутов А. С., Кощей Л. Д., Малиновский М. Л., Тертышный С. Н., Фурман И. А. ; заявители и патентообладатели Аллашев А. Ю., Бовчалюк С. Я., Борисенко В. А., Бутов А. С., Кощей Л. Д., Малиновский М. Л., Тертышный С. Н., Фурман И. А. – № u200812423 ; опубл. 10.02.09, Бюл. № 3.

Здобувачем запропоновано принцип утворення сигналу з широтно-імпульсною модуляцією шляхом використання функції нееквівалентності для двох сигналів з близькими частотами.

33. Фурман І. О., Малиновський М. Л., Джулгаков В. Г. та ін. Мікроелектронні засоби програмного керування. Підручник для студентів ВНЗ. – Харків: Факт, 2007. – 486 с.

Здобувачем розроблено класифікацію, моделі та методи HDL-синтезу безпечних автоматів.

34. Малиновский М. Л. Оценка эффективности информационной технологии параллельного логического управления объектами критического применения / И. А. Фурман, М. Л. Малиновский, С. Я. Бовчалюк, А. Ю. Аллашев // Міжнародна наук.-техн. конф. «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2007» / Нац. аерокосм. ун-т ім. М. Є. Жуковського «ХАИ». – Х., 2007. – С. 388 – 390.

Здобувачем запропоновано метод оцінки складності HDL-описів цифрових пристроїв.

35. Малиновський М. Л. Программирование микропроцессорных средств промышленной автоматизации / И. А. Фурман, М. Л. Малиновский, А. Ю. Аллашев // Матеріали IV міжнар. наук.-практ. семінару «Методичні аспекти застосування електротехнічного обладнання фірми «LENZE» у навчальному процесі і виробництві», – Харьков, 2008. – С. 50–56.

Здобувачем розроблено табличну мову програмування THDL.

36. Совершенствование методов и средств программирования безопасных ПЛИС-контроллеров с параллельной архитектурой / В. А. Борисенко, Л. Д. Кощей, С. Н. Тертышный, М. Л. Малиновский, И. А. Фурман // Інформаційно-керуючі системи на залізничному транспорті. – 2008. – Додаток до журн. – № 4 (72). – С. 3–4.

Здобувачем розроблено мову та інструментальні засоби технологічного програмування безпечних ПЛІС-контролерів.

37. Малиновский М. Л. Модели и стили программирования ПЛИС на табличном языке THDL // 13-й міжнародний молодіжний форум «Радіоелектроніка і молодь в XXI сторіччі»: Зб. матеріалів форуму. Ч.2.- Харків: ХНУРЕ, 2009. – С. 12.

АНОТАЦІЇ

Малиновський М. Л. Методи та засоби проектування технічних і програмних компонентів безпечних ПЛІС-контролерів з паралельною архітектурою. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 - комп'ютерні системи і компоненти. – Національний технічний університет «Харківський політехнічний інститут», Харків, 2010.

Дисертація присвячена проблемі розробки та реалізації методів і засобів проектування технічних і програмних компонентів безпечних ПЛІС-контролерів з паралельною архітектурою для систем критичного застосування.

Розроблено методологію абстрактного та структурного синтезу безпечних логічних автоматів паралельної дії. Запропоновано моделі та виділено класи безпечних автоматів; табличні та графічні методи завдання безпечних автоматів; методи синтезу безпечних автоматів з функціональною деградацією; методи кодування станів з кон’юнктивною функцією керування деградацією. Розроблено мову та технологію програмування безпечних ПЛІС-контролерів. Запропоновано формальний опис алфавіту та синтаксису розробленої мови THDL (Table Hardware Description Language). Розроблено процедуру і інструментальні засоби програмування безпечних ПЛІС-контролерів. Розроблено та досліджено методи проектування і моделі пристроїв безпечного формування керуючих впливів, що засновані на використанні принципу послідовного перетворення параметрів сигналів, які динамічно змінюються у часі. На основі отриманих у дисертації теоретичних результатів розроблено та впроваджено мікроелектронну систему централізації на основі безпечних ПЛІС-контролерів з паралельною архітектурою для залізниць та метрополітенів.

Ключові слова: комп’ютерні системи та компоненти, мовно-програмні засоби HDL-синтезу, системи критичного застосування, ПЛІС-контролер, БЛП-автомат, функціональна безпечність, безпечний автомат з функціональною деградацією, несиметричні відмови.

Малиновский М. Л. Методы и средства проектирования технических и программных компонентов безопасных ПЛИС-контроллеров с параллельной архитектурой. - Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.05 - компьютерные системы и компоненты. –

Национальный технический университет «Харьковский политехнический институт», Харьков, 2010.

Диссертация посвящена проблеме разработки и реализации методов и средств проектирования технических и программных компонентов безопасных ПЛИС-контроллеров с параллельной архитектурой для систем критического применения.

Разработана методология абстрактного и структурного синтеза безопасных логических автоматов параллельного действия (БЛП-автоматов). Предложены абстрактные модели и выделены классы безопасных автоматов. Разработаны табличные и графические методы задания безопасных автоматов; методы синтеза безопасных автоматов с функциональной деградацией, основанные на формировании множеств ответственных операций и построении, анализе и преобразовании χ-автоматов.

Разработаны методы кодирования состояний, которые позволяют реализовать конъюнктивную функцию управления деградацией безопасных автоматов. Предложены абстрактные и структурные модели безопасных автоматов циклического действия. Выполнено исследование и компьютерное моделирование безопасных автоматов различных классов. Рассмотрены и исследованы типовые модели безопасного функционирования систем и компонентов критического применения.

Сформулирована концепция создания языка и инструментальных средств табличного HDL-синтеза цифровых систем на основе ПЛИС. В соответствии с предложенной концепцией разработаны язык, инструментальные средства и технология проектирования программного обеспечения для безопасных ПЛИС-контроллеров с параллельной архитектурой. Предложено формальное описание алфавита и синтаксиса разработанного языка описания аппаратур THDL (Table Hardware Description Language). Разработана семантика табличного языка THDL, раскрывающая назначение четырех его конструкций (таблиц логических преобразований, переходов, микроциклов и соединений) и устанавливающая общие правила их использования.

Предложены модели программирования ПЛИС на языке THDL, которые образуют квадранты и отвечают стилям программирования: "от событий", структурному, "от состояний", сентенциальному. Разработана процедура и инструментальные средства программирования безопасных ПЛИС-контроллеров с параллельной архитектурой, которые представляют собой надстройку над существующими САПР проектирование цифровых устройств на основе ПЛИС.

Предложены формальные модели THDL-конструкций и шаблоны HDL-описаний в поведенческом и структурном стилях, которые положены в основу создания методов и инструментальных средств трансляции THDL-описаний в традиционные языки описания аппаратуры цифровых систем.

Разработаны и исследованы методы проектирования и модели устройств безопасного формирования управляющих воздействий. Предложенные методы основаны на использовании принципа последовательного преобразования параметров сигналов устройства формирования управляющих воздействий,

которые динамично изменяются во времени. Предложены математические модели устройств безопасного формирования управляющих воздействий с последовательным, параллельным и смешанным соединением каналов. Разработана и исследована математическая модель однофазных и n-фазных устройств безопасного формирования гармоничного сигнала. Разработана методика расчета параметров моделей безопасных устройств формирования управляющих воздействий.

Выполнен расчет показателей безопасности автоматов с функциональной деградацией и устройств формирования управляющих воздействий. Предложена сравнительная оценка качественных показателей программного обеспечения на табличном языке THDL и известных текстовых языках описания аппаратуры цифровых систем.

На основе полученных в диссертации теоретических результатов разработана и внедрена микроэлектронная система централизации на основе безопасных ПЛИС-контроллеров с параллельной архитектурой для железных дорог и метрополитенов.

Ключевые слова: компьютерные системы и компоненты, языково-программные средства HDL-синтеза, системы критического применения, ПЛИС-контроллер, БЛП-автомат, функциональная безопасность, безопасный автомат с функциональной деградацией, несимметричные отказы.

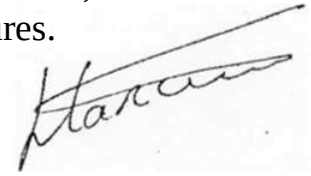
Malinovskiy M. L. Methods and means of designing of technical and program components of safe FPGA-controllers with parallel architecture. - Manuscript.

The thesis for a doctor of the technical science degree by speciality 05.13.05 - Computer Systems and Components. - National Technical University “Kharkov Polytechnic Institute”, Kharkov, 2010.

The dissertation is devoted to a problem of development and realization of methods and means of designing of technical and program components of safe FPGA-controllers with parallel architecture for safe-critical systems.

The methodology of abstract and structural synthesis of safe State Machines of parallel action (SP-machines) is developed. The models and the classes of safe State Machines, tabular and graphic methods of the description of safe State Machines, methods of synthesis of safe State Machines with functional degradation, methods of coding of states are offered. Language, tools and technology of designing of the software for safe FPGA-controllers are developed. The formal description of the alphabet and syntax of the developed Table Hardware Description Language (THDL) and its semantics is offered. The procedure and tools of programming of safe FPGA-controllers with parallel architecture are developed. Methods of designing and models of devices of safe formation of control influences are developed. On the basis of the theoretical results, received in the dissertation, the microelectronic system of centralization on the basis of safe PLD-controllers with parallel architecture for railway transport is developed and installed.

Keywords: computer systems and components, languages and tools of HDL-synthesis, critical applications, FPGA-based controllers, SP-machines, functional safety, safe machine with functional degradation, asymmetrical failures.



Відповідальний за випуск Фурман І. О.

Підписано до друку 21.04.2010 р. Формат 60х84/16
Папір офсетний Гарнітура «Times New Roman» Друк - різограф
Друк. арк. – 2,25 Наклад 100 прим.
Ціна договірна Зам. № 2/31-10

Видавництво Харківського університету Повітряних Сил імені Івана Кожедуба
Свідоцтво про державну реєстрацію ДК № 2535 від 22.06.2006 р.

Друкарня Харківського університету Повітряних Сил імені Івана Кожедуба
61023, Харків – 23, вул. Сумська, 77/79