МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

В. І. Мойсеєнко, В. М. Бутенко

БЕЗПЕЧНІСТЬ СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Навчальний посібник

Харків 2021

УДК 614.8:656.25
М 748

Рекомендовано вченою радою Українського державного університету залізничного транспорту як навчальний посібник (витяг з протоколу № 13 від 24 грудня 2020 р.)

Рецензенти:

д-р техн. наук, професор Сергій БУРЯКОВСЬКИЙ (директор НДПКІ «Молнія» НТУ «ХПІ»),

д-р техн. наук, професор Георгій КУЧУК (НТУ «ХПІ»)

Мойсеєнко В. І., Бутенко В. М. Безпечність
М 748 спеціалізованих комп'ютерних систем: навч. посібник. – Харків: УкрДУЗТ, 2021. – 133 с., рис. 50, табл. 13.

ISBN

Навчальний посібник призначено для студентів усіх форм навчання спеціальності 123 «Комп'ютерна інженерія» другого рівня вищої освіти – «магістр», з можливим застосуванням для споріднених курсів.

У навчальному посібнику сформульовано основні положення безпечності систем залізничного транспорту критичного призначення, визначено термінологію та розглянуто принципи аналізу причин і наслідків порушень.

Наведено приклади побудови програмних та апаратних рішень, включно з інтерфейсом безпечної взаємодії з об'єктами залізничної автоматики.

Значну увагу приділено висвітленню питань ризик-менеджменту, сучасній концепції керування ризиками, методам аналізу та формування кількісних оцінок небезпек з використанням апарату дерев подій та пошкоджень.

Насамперед посібник призначений для студентів, аспірантів, інженерів та викладачів комп'ютерних спеціальностей, навчання і професійна діяльність яких пов'язана із залізничним транспортом.

УДК 614.8:656.25

ISBN

ЗМІСТ

ВСТУП

Основою комп'ютерної інженерії сучасних підприємств промисловості та всіх видів транспорту є спеціалізовані комп'ютерні системи (СКС). Вони забезпечують захист людей та довкілля від дії небезпечних факторів, які виникають унаслідок пошкоджень у системах керування виробництв з підвищеним ризиком.

Дисципліна «Безпечність спеціалізованих комп'ютерних систем» відповідає на запит суспільства про забезпечення безпечного використання систем з підвищеним ризиком. Вона базується на сучасних уявленнях про керування безпекою на основі процедур ризик-менеджменту, які були сформовані наприкінці 20 сторіччя.

Посібник призначений для студентів та магістрантів спеціальності «Комп'ютерна інженерія». Також його матеріал може бути корисним для підготовки фахівців спеціальностей, які розглядають технології, що пов'язані з ризиками для персоналу та навколишнього середовища. Тому його можна вважати деякою мірою універсальним.

У процесі створення посібника використаний багаторічний науковий досвід авторів, результати наукових праць професорів В. М. Самсонкіна, Я. М. Миколайчука, В. С. Харченка. У роботі розглядаються регулюючі документи Міжнародної електротехнічної комісії, європейські та національні відомчі нормативні документи з питань функціональної безпеки на залізничному транспорті.

У навчальному посібнику подано інформацію про новітні розробки з моделювання та оцінювання ризиків провідних університетів Америки та Великобританії, фахівців лабораторії Белл Телефоун (Х. А. Уотсон), фірми Боїнг, а також наведені сучасні уявлення про методи аналізу ризиків, які відображено у роботах професора Кембриджського університету Х. Хусімо, Джона Фусселя, Є. Хенлі, Х. Куммамото та інших фахівців світового рівня.

У посібнику надано визначення та характеристику СКС, розглянуто принципи безпечності програмних та апаратних

рішень. Матеріал, присвячений аналізу та оцінюванню ризиків, містить конкретні приклади реалізації на залізничному транспорті при впровадженні комп'ютерних інформаційно-керуючих систем керування рухом поїздів.

Навчальний посібник містить матеріали для виконання практичних завдань та самостійної роботи, які орієнтовані на формування у студентів, магістрантів та слухачів відповідних фахових компетентностей. Виконання завдань потребує не тільки знань та вмінь, а й креативних підходів, необхідності належної комунікації на підготовчому етапі та під час обговорення результатів розробки.

Мойсеєнко В. І. склав структуру посібника та частково написав розділи два, три та чотири (загальним обсягом 60 %).

Бутенко В. М. розробив вступ, перший розділ, частину другого розділу та частину контрольних запитань і завдання до розділів навчального посібника (загальним обсягом 40 %).

Автори висловлюють подяку Міроновій Н. С. за допомогу у створенні посібника.

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО СПЕЦІАЛІЗОВАНІ КОМП'ЮТЕРНІ СИСТЕМИ

1.1. Історична довідка

Для кращого розуміння матеріалу, який розглянуто у посібнику, звернемося до історичного досвіду та еволюції уявлень про ризики небезпечної діяльності у суспільстві. Вказана проблематика достатньо повно відображена у роботі Дж. Хенлі та Х. Куммамото «Надійність технічних систем та оцінка ризиків». Нижче наведена квінтесенція цих уявлень.

З очевидних причин початковий імпульс до створення числових методів оцінювання надійності дала авіаційна промисловість. Після Першої світової війни з огляду на збільшення інтенсивності польотів та авіаційних катастроф було вироблено критерії надійності для літаків і вимоги до рівня безпеки. Зокрема проведено порівняльний аналіз одномоторних і багатомоторних літаків з погляду успішного завершення польоту і вироблено вимоги за частотою аварій, віднесених до першої години польотного часу. До 1960 року, наприклад, було встановлено, що одна катастрофа припадає в середньому на 1 млн посадок. Отже, для автоматичних систем посадки літаків можна було б установити вимоги за рівнем ризику, що не перевищує однієї катастрофи на 10^7 посадок.

Р. Х. Дженнінгс наводить хронологію розвитку теорії і техніки надійності в 40–70-х роках. Математик Р. Луссер визначив, що старий закон «що ланцюг не міцніший, ніж найслабша його ланка» непридатний до систем послідовного типу. Потім Р. Луссер отримав закон відтворення для послідовних елементів, а саме: надійність системи з послідовно з'єднаних елементів дорівнює відтворенню надійності цих елементів. Отже, у системі послідовного типу надійність окремих елементів має бути значно вищою для задовільного функціонування системи.

У США в 40-х роках основні зусилля для підвищення надійності було сконцентровано на всебічному поліпшенні якості. Покращені конструкції, міцні матеріали, підвищені твердість і якість обробки поверхонь, що швидко зношуються,

досконалі вимірювальні інструменти тощо – все це було спрямовано на збільшення активної довговічності вузлів і агрегатів. Електротехнічне відділення фірми «Дженерал моторс» (General Motors), наприклад, збільшило активний ресурс приводних двигунів локомотивів з 400 тис. до 1,6 млн км за рахунок використання поліпшеної ізоляції і застосування вдосконалених конічних та сферичних роликових підшипників, а також проведення випробувань за високої температури. Довговічність дизелів була набагато збільшена завдяки розробленню фірмою «Токко» (Tocco) технології підвищення твердості опорних поверхонь цанг і кулачків. Було досягнуто прогрес у розробці ремонтопридатних конструкцій і в забезпеченні підприємств устаткуванням, інструментом і документацією для виконання операцій з технічного обслуговування і профілактичних робіт.

Інша форма прогресу була продемонстрована в 40-х роках завдяки підвищеному інтересу керівників промислових підприємств до складання і затвердження типових графіків періодичних перевірок, карт контролю високопродуктивного верстатного устаткування, вироблення рівнів оцінювання та економічно обґрунтованого підходу до якості продукції. Ці заходи ознаменували вступ інженерів, що працюють у промисловості, в цю галузь, і, як результат, більшість інструкцій і навчальних курсів з надійності приділяли увагу забезпеченню і контролю якості та статистичним методам, які до них належать.

50-ті роки. Велике значення надавалося безпеці, особливо в аерокосмічній і атомній галузях. Це десятиріччя відзначено початком використання основних понять з надійності елементів, а саме: інтенсивність відмов, очікувана довговічність, відповідність конструкції заданим вимогам і прогнозування якості. Міністерство оборони США виявило, що ненадійне обладнання потребувало величезного обсягу робіт з технічного обслуговування і ремонту. Підрахували, що річна вартість обслуговування озброєння становить 2 дол. на кожен долар вартості самого устаткування електронного типу. Отже, при десятирічному терміні експлуатації необхідно 20 млн дол.., для утримання обладнання закупівельною вартістю в 1 млн дол. Ці факти продемонстрували уряду, що набагато розумніше

закладати основи надійності конструкції під час проектування, ніж очікувати, поки обладнання відмовить, і після цього його ремонтувати.

Саме на початку 50-х років було витрачено значні зусилля на те, щоб зрозуміти і навчитися виправляти помилки людини, що призводять до відмов систем. Одна з перших кількісних оцінок можливостей людини була виконана в 1952 році в лабораторії «Сандіа». Було досліджено систему ядерної зброї на літаках з використанням методу, що базується на експериментальних оцінках середньої кількості помилок оператора на виконувану операцію. Завдання оператора були поділені на дві категорії залежно від умов, у яких вони виконувалися: частота виникнення помилок приймалася рівною 0,01 для операцій, що виконуються на землі, і 0,02 – у повітрі. Ці значення були введені в рівняння, що описують надійність роботи системи, поряд з іншими подіями, що належать до системи.

У **60-ті роки** стала очевидною гостра необхідність нових методів забезпечення надійності та більш широкого їх застосування в різних додатках. Центр уваги перемістився від аналізу поведінки окремих елементів різного типу (механічних, електричних або гідравлічних) на наслідки, спричинені відмовою цих елементів у відповідній системі. Вступ в еру міжконтинентальних балістичних ракет (МБР) і подальша розробка пілотованих ракетно-космічних кораблів, як-от: «Меркурій» і «Джеміні» – прискорили реалізацію девізу «успіх за будь-яку ціну». Ці обставини поглиблювалися вимогою ураження цілі «з одного пострілу», кульмінація якого досягається при передстартовому відліку перед запуском реактивних двигунів та інших систем ракети на пусковому столі. Значні зусилля були витрачені на випробування систем і окремих елементів протягом перших років космічної ери. Усі дані щодо кожної відмови і результати аналізу ретельно реєструвалися поряд з інформацією з інших технічних недоліків, розкритих під час аналізу. Вид, механізм та причина кожної відмови будь-якого елемента їх вплив на систему оцінювалися для внесення змін, що виключають їх повторення. Аналіз систем з використанням блок-схем як основних моделей набув бурхливого розвитку і великого

поширення для досягнення високого ступеня надійності і безпеки.

Зі збільшенням складності більш витончено складених блок-схем виникла необхідність іншого підходу. У 1961 році вперше Х. А. Уотсон з лабораторії фірми «Белл телефон» (Bell Telephone) запропонував новий принцип аналізу за допомогою дерева відмов як програми для оцінювання надійності системи управління запуском ракет «Мінітмен». Пізніше фірма «Боїнг» (Boeing) модифікувала цей принцип для моделювання на ЕОМ.

У 1965 році Д. Ф. Хаасль розвинув методику побудови дерева відмов стосовно широкого кола різних технічних проблем, що стосуються надійності і безпеки.

Вивчення безпеки систем як окремої незалежної діяльності було офіційно введено в практику в 1962 році після катастрофічних аварій на чотирьох підземних комплексах запуску МБР. У 1966 році міністерство оборони США запровадило стандарти ВВС і ввело вимогу проводити аналіз надійності на всіх етапах розроблення всіх видів озброєння. Ці стандарти безперервно доповнювалися і перероблялися, а в 1969 році було прийнято стандарт MIL-STD-882 «Програма щодо забезпечення надійності систем, підсистем і устаткування. Вимоги» як основний стандарт для всіх промислових підрядників з військових поставок.

Паралельно розроблялися вимоги з надійності, працездатності і ремонтопридатності промислових виробів. Такі стандарти, як, наприклад, MIL-STD-471 «Ремонтопридатність (перевірка, підтвердження, оцінка)» і MIL-STD-781 «Випробування на надійність (експоненціальний розподіл)» є документами, які зокрема визначають високий ступінь завантаженості інженерів і консультантів з надійності серед військових і цивільних фахівців.

60-ті роки також відзначені початком широкого видання книг і журналів в описуваній галузі. Монографію І. Базовські «Надійність: теорія і практика» опублікувало видавництво «Прентіс-хол» (Prentice-Hall) у 1961 році, а до кінця десятиріччя з'явилося щонайменше ще 15 книг (бібліографія наведена в кінці цього посібника). У цей період побачив світ журнал IEEE «Transactions on Reliability», який під керівництвом д-ра Р. Еванса став провідним періодичним виданням у цій галузі.

Такі видатні математики, як З. У. Бірнбаум, Р. Барлоу, Ф. Прошан, Д. Ж. Цезарі та У. Вейбулл, почали розробляти статистичні методи, що стосуються проблем надійності і ремонтопридатності.

Кампанія, що почалася в 50-х і прискорилася в 60-х роках, привела до накопичення і систематизації даних за параметрами елементів, систем і помилок людини-оператора. Розробки в цій галузі є предметом інших досліджень.

70-ті роки. Інтенсивна робота з оцінювання ризику, що пов'язана з експлуатацією атомних електростанцій, була організована Комісією з атомної енергії США і завершилася в 1977 році випуском звіту «WASH-1400. Аналіз безпеки реактора». Проф. Н. Расмуссен і керована ним група дослідників з багатомільйонним бюджетом проаналізували широкий спектр аварій, що сталися на підприємствах атомної енергетики, чисельно класифікували їх у порядку ймовірності появи, а потім оцінили потенційні наслідки для населення. Дерево подій, дерево відмов і техніка оцінювання ризику й наслідків, використані в цьому звіті, були потім застосовані в хімічній та інших галузях промисловості. Дослідження «за Расмуссеном» набули поширення в країнах Європи, Азії та в США.

Зростаюча стурбованість громадськості щодо індустріальних небезпек у поєднанні зі зростаючим ступенем споживання і впливом на довкілля спричинили значний вплив протягом цього десятиріччя. У Західній Європі услід за серйозними промисловими аваріями у Фліксборо (Великобританія) і Червеза (Італія) було ухвалено ряд законів, які передбачали проведення досліджень основних джерел ризику перед початком будівництва будь-якого підприємства. Новий закон щодо токсичних матеріалів, ухвалений у Великобританії, може вплинути на будь-яке підприємство, що має хоча б одну ємність зі стисненим газом. У США введено закони про охорону здоров'я на виробництві та про відповідальність за якість продукції; цікаво зазначити, що витрати підприємств хімічної промисловості з огляду на ці закони оцінено у 1977 році у 2 млрд дол.

1.2. Визначення спеціалізованих комп’ютерних систем

Сучасні інформаційно-керуючі системи (ІКС) значною мірою є уніфікованими та стандартизованими. Це стосується як окремих компонентів (корпуси, рознімання, плати, окремі елементи схем), так і компонування системи у цілому та побудови її програмного забезпечення. Людині, яка не є фахівцем у конкретній галузі, дуже складно визначити сферу застосування конкретної ІКС за її зовнішніми ознаками. Насамперед це пов’язано з уніфікацією елементної бази, способів введення команд керування, відображення інформації тощо. Такий підхід дає змогу:

- суттєво зменшити час та фінансові витрати на процеси проектування, виготовлення та монтаж обладнання;
- спростити пошук пошкоджень та зменшити витрати часу персоналу на процес відновлення;
- суттєво скоротити процес навчання фахівців, що мають обслуговувати ІКС.

Тенденції до уніфікації існували достатньо давно, ще з кінця 19 сторіччя, але їх інтенсивний розвиток став можливий з появою контролерів та комп’ютерів. Цей процес набув широкого розмаху наприкінці 20 сторіччя з появою надійних та високопродуктивних засобів мікропроцесорної техніки.

Сучасну ІКС можна зобразити у вигляді спрощеної структурної схеми (рис. 1.1).

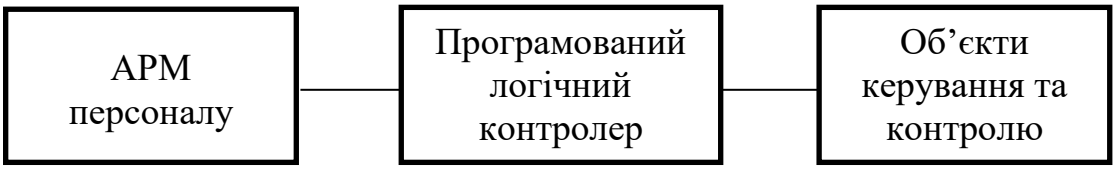


Рис. 1.1. Структурна схема ІКС

Автоматизоване робоче місце (АРМ) персоналу забезпечує формування команд керування у відповідь на дії оператора й дає змогу інформувати його про стан об’єктів контролю.

Програмований логічний контролер (ПЛК) у свою чергу забезпечує підтримку логіки роботи системи, формування команд

керування відповідним об’єктам та знімання інформації про їх стан. Також однією з важливих функцій ПЛК є зв'язок з АРМ персоналу.

Та при всіх згаданих вище тенденціях окремі ІКС можуть дуже суттєво відрізнятися від інших. Ми не беремо до уваги їх логіку функціонування, яка прописана у програмному забезпеченні.

Основні відмінності спостерігаються у підходах до побудови структури системи та організації її програмного забезпечення. Крім того, іноді системи виконують однакові функції, але мають принципові відмінності у структурній та програмній організації.

Розглянемо системи керування кондиціонуванням повітря у супермаркеті, метрополітені або підводному човні. Формально вони виконують однакові функції, але водночас технічна та програмні реалізації суттєво відрізняються. З**амислімося, чому?** Відповідь можливо знайти, якщо проаналізувати вимоги до ІКС та зміст основних функцій.

Система кондиціонування повітря у супермаркеті здебільшого має забезпечувати комфортні умови перебування людей у приміщенні. На відміну від розглянутої, на системи кондиціонування повітря у підводному човні чи метрополітені покладаються додаткові функції забезпечення здоров’я та збереження життя людей. Системи керування рухом поїздів забезпечують не тільки ефективність перевізного процесу, а й його безпечність для людей, інфраструктури та довкілля. Зважаючи на зростаючі швидкості руху та перевезення залізницею небезпечних вантажів, ціна аварії може бути дуже високою.

З огляду на це, незважаючи на близькість призначення та переліку основних функцій, наведені вище системи, а саме: і система кондиціонування повітря супермаркету, підводного човна чи метрополітену, повинні мати суттєві відмінності.

Отже, ми дійшли висновку, що деякі ІКС мають специфічні, притаманні тільки їм, вимоги до реалізації технологічних процесів роботи системи керування. І в цьому сенсі вони є унікальними, відмінними від аналогічних.

Безумовно, ми розглядаємо тільки функції, що мають принципове значення з точки зору захисту людей, довкілля, уникнення значної шкоди об'єктам інфраструктури тощо. У цьому сенсі будемо вживати термін «спеціалізовані комп'ютерні системи» (СКС) як ті, що мають реалізовувати специфічні, важливі для суспільства або техніки функції, не притаманні аналогічним ІКС [7, 8, 13, 16, 17].

Такі системи забезпечують функціонування атомних електростанцій, авіаційної та космічної техніки, залізничного транспорту в частині керування рухом поїздів та інших галузях економіки.

Залізничні СКС розглядаються як системи, що є критичними до безпеки [17, 39–42], тому їх іноді називають системами критичного призначення. Однак слід зауважити, що до таких систем належать не всі залізничні ІКС. Наприклад, інформаційна система для сповіщення пасажирів на вокзалах або автоматизована система продажу квитків не можуть бути критичними до безпеки. Їх можна розглянути як спеціалізовані за галузевою ознакою щодо алгоритмів функціонування.

Комп'ютерні системи (КС) увійшли у всі види людської діяльності: промисловість, управління, навчання, бізнес, дозвілля тощо. За своєю природою вони є універсальними, тому звичайній людині, не фахівцю, дуже важко розрізнити, які саме завдання вирішує окрема КС. Насамперед це пояснюється уніфікацією апаратних засобів, починаючи від шафи, корпусів, системних блоків ПЕОМ і закінчуючи розніманнями, пристроями для монтажу та іншими компонентами. Такий підхід суттєво спрощує процеси розроблення, проектування, монтажу та подальшого технічного обслуговування системи. Однак нарівні з тенденцією уніфікації існує й розвивається тенденція спеціалізації КС. Необхідність створення СКС обумовлена специфічними умовами їх використання, за яких використання звичайних, тобто уніфікованих або універсальних КС є недоцільним.

За визначенням професора Я. М. Миколайчука, СКС належать до класу проблемно-орієнтованих суперфункціональних систем. Вони можуть бути централізованими або розподіленими, вмонтованими в окремі елементи технічних засобів. Професори А. О. Мельник та В. П. Тарасенко визначають три групи основних причин появи спеціалізації КС.

Першою групою причин є суперечність між формальними математичними методами та алгоритмічними і технічними можливостями стандартних КС та проблемами реалізації функцій системи, що потребують нестандартного математичного апарату, нестандартних алгоритмів і відповідно нестандартних підходів до практичної реалізації отриманих результатів.

Друга група причин обумовлена специфічністю предметної галузі, для якої розробляється СКС. Водночас слід зазначити, що вказані специфічні умови, як правило, є надто принциповими і не враховувати їх без втрати сутності просто неможливо.

Наприклад, якщо взяти систему керування кондиціонуванням у великому супермаркеті та метрополітені, то при збіжності багатьох параметрів та однаковому призначенні СКС кондиціонування метрополітену має суттєву специфічну особливість – її робота пов'язана із забезпеченням здоров'я та життя пасажирів. Саме тоді, як система кондиціонування повітря для супермаркету забезпечує комфортні умови для покупців і персоналу. Крім цього, є галузі з дуже специфічними умовами і технологічними алгоритмами функціонування, які характерні саме для неї, при чому використання традиційних підходів і алгоритмів дуже часто є просто неможливим.

До третьої групи належать причини, що обумовлені окремими дуже жорсткими вимогами до окремих показників функціонування. Як правило, реалізація таких вимог стандартними методами та підходами є неефективною або взагалі неможливою. Найчастіше це системи керування ядерними реакторами, залізничні системи керування рухом, авіаційні або космічні комплекси. Найчастіше підвищені умови висуваються до показників функціональної безпеки, відмовостійкості, безвідмовності чи ремонтопридатності.

Отже, СКС – це окремий клас КС, які призначені для реалізації специфічних завдань та вимог, оптимізованих за спеціальними критеріями.

Графічно сутність основних складових СКС наведено на рис. 1.2.

Необхідно зазначити, що конкретні СКС можуть мати від однієї до трьох складових, що зображені на рис. 1.2. Як правило, специфіка галузі формує відповідні вимоги до окремих

показників функціонування, наприклад, дуже високий, критичний рівень надійності. Поява екстремальних вимог, що наближені до теоретично-можливої границі якості реалізації окремих функцій СКС, унеможливлює використання традиційного математичного та алгебраїчного апарату й потребує нових, проривних підходів.

Рис. 1.2. Основні складові визначення СКС

Серед предметних галузей, у яких застосовується СКС, є такі, що безпосередньо пов’язані із забезпеченням суверенності та державності України, а саме: комп’ютеризоване обладнання і системи військово-оборонного призначення; автоматизовані системи керування рухом транспорту; системи автоматизації в енергетиці; засоби забезпечення конфіденційності інформації у державному секторі та сфері бізнесу тощо.

Отже, СКС відрізняються від універсальних КС вимогами критичності системних характеристик (максимізації або мінімізації). Модель СКС можна подати у вигляді деякого узагальненого функціонала]

$$E = F(T, V, M, S),$$

де T – час виконання операції над деяким ресурсом;

V – швидкість виконання операції;

M – обсяг ресурсу, що використовується (наприклад пам’яті);

S – системні функції.

Зазвичай наведеним функціоналом може бути будь-яка КС, однак до спеціалізованих систем, як було зазначено раніше, на відміну від універсальних, висуваються критичні вимоги:

T = min V max;
V = min V max;
M = min V max;
S = min V max.

Слід зазначити, що одночасне досягнення вказаних вище вимог технічно неможливе. Це пояснюється власне змістом вимог. Так, наприклад, якщо необхідно мінімізувати час обробки деякого сигналу, то очевидно, що цього можна досягти втрачаючи деякі інші показники, наприклад захист від завад. Тому слід наголосити, що процес створення будь-якої СКС завжди базується на системному підході з використанням багатоваріантних, часто компромісних рішень.

Що на практиці означає системний підхід? *Спробуємо пояснити це на невеликому, досить простому прикладі. Припустимо, що ми отримали завдання виточити на токарному верстаті циліндр з дуже міцного матеріалу з дуже малим значенням похибки у розмірах. Зазвичай обираємо відповідний верстат та знаходимо необхідний інструмент для різання заготовки. Чи зможемо успішно виконати замовлення? Ні! Тому що в процесі різання інструмент буде нагріватися й унаслідок цього втратить не тільки твердість, а й змінить геометричні розміри. Далі починаємо охолоджувати різець і заготовку, подаючи на неї охолоджувальну рідину. Діло пішло, але чи отримаємо в кінці саме ті розміри, що потрібні? Найймовірніше, ні. Чому? Тому що в процесі виготовлення заготовки температура повітря у цеху може змінюватися. Відповідно до цього вироби також будуть відрізнятися за геометричними розмірами один від одного. Тому на виробництві при виготовленні особливих деталей підтримується постійно однакова температура, що дорівнює 20 ˚С. Якщо похибка у розмірах циліндра зі звичайної сталі не має суттєвого значення, то, очевидно, його можна виготовити на будь-якому обладнанні, за будь якої температури звичайним інструментом.*

Отже, необхідно враховувати не тільки всі можливі фактори, що впливають на кінцевий результат чи процес, а й брати до уваги, як ці фактори можуть взаємодіяти між собою. Наприклад, якщо один з чотирьох транзисторних ключів мікросхеми нагрівається і виходить з ладу внаслідок перевантаження, то найімовірніше станеться і тепловий пробій інших, бо всі вони містяться в одному корпусі, який уже нагрівся.

1.3. Класифікація спеціалізованих комп'ютерних систем

На теперішній час є велика кількість типів СКС, а саме: концентровані та розподілені системи, архітектура з мультипрограмним та мультипроцесорним опрацюванням даних.

Бувають однорівневі архітектури та багаторівневі розподілені СКС. Окремим класом є радіотехнічні інформаційні системи та комп'ютерні мережі з ретрансляторами, з оптичними каналами зв'язку тощо. Розвиток КС та інформаційних технологій привів до стирання меж між традиційними системами автоматики та зв'язку. На теперішній час таких меж фактично не існує, особливо якщо це стосується КС і мереж для обміну даними між абонентами. Насамперед це пояснюється єдиною природою сигналів, що передають інформацію від А до В: це можуть бути телеметричні дані чи музика.

Дуже поширеними в промисловості є інформаційно-керуючі СКС. До інформаційних СКС можна віднести:

- інформаційні корпоративні СКС, зокрема залізничні;
- системи обліку витрат енергетичних та інших ресурсів різного виду (електроенергії, дизельного пального, матеріалів тощо);
- охоронні системи, системи відеомоніторингу;
- геоінформаційні системи та багато інших.

Не менш затребуваними є ІКС, які набули великого поширення на підприємствах. Найбільш характерними представниками таких СКС є:

- ІКС керування повітряним рухом (цивільного та військового призначення);
- автоматизовані системи керування (АСК) в енергетиці, особливо атомній;

- системи керування рухом поїздів на залізничному транспорті;
- системи керування міським транспортом.

Сучасний залізничний транспорт порівняно з іншими галузями економіки має найбільшу кількість інформаційних та інформаційно-керуючих СКС. Інформаційні системи здебільшого виконують функції збору, обробки та передачі інформації, а також забезпечують підтримку прийняття рішень відповідним персоналом (рис. 1.3).

До систем загальнодержавного рівня можна віднести комплекс, що забезпечує проведення виборів та деякі інші загальнодержавні функції. Галузеві системи також можуть мати загальнодержавне значення: це інформаційні системи ДСНС, військові, метеорологічні та ін. Вони виконують конкретні галузеві завдання у загальнодержавному масштабі.

Більшість галузевих КС мають дво- або трирівневу структуру. Найбільш характерними представниками є системи в енергетиці, які забезпечують розподіл електроенергії, комплекси керування газо- і нафтопроводами та транспортні інформаційно-керуючі системи.

Рис. 1.3. Класифікація СКС

СКС залізничного транспорту забезпечують функціонування перевізного процесу на залізниці, яка за своєю природою є унікальною. З огляду на те, що такі системи забезпечують безпечність перевезень, тобто життя і здоров’я

людей, до їх основних функцій висуваються надзвичайно жорсткі вимоги, критичні до функціональної безпеки. Відповідно алгоритми, за якими функціонують такі СКС, також є специфічними й деякою мірою унікальними.

З огляду на це системи мають назву «системи критичного призначення», або «відповідальні системи» [8, 9, 11–13]. Класичним прикладом критичних до безпеки СКС є системи керування рухом поїздів на перегонах та станціях. Перегінні СКС керують рухом поїздів на перегоні, а станційні – відповідно на станції, крім того, є мобільні пристрої, що встановлюються на локомотивах, та системи диспетчерського керування, які належать до верхнього рівня. Крім перегінних та станційних СКС, до класу відповідальних або критичних до безпеки можна віднести автоматичну систему переїзної сигналізації, яка встановлюється для керування переїзною сигналізацією та автошлагбаумами. Також необхідно вказати на систему локомотивної сигналізації та безпеки, яка інформує машиніста про встановлену швидкість руху поїзда та перевіряє безпечність його дій.

Усі перераховані СКС, а саме: перегінні, станційні, переїзні та локомотивні або мобільні – відносять до систем нижнього рівня. До їх основних функцій висуваються найбільш жорсткі критичні вимоги щодо показників функціонування. На верхньому рівні, стосовно вказаних СКС, перебуває система диспетчерської централізації. Вона призначена для керування рухом поїздів на окремих ділянках (диспетчерських колах) досить великої довжини 100 км і більше. Мікропроцесорна система диспетчерської централізації накладається на системи нижнього рівня, перегінні та станційні. Останнім часом саме мікропроцесорні системи диспетчерської централізації або диспетчерського керування демонструють найбільшу динаміку розвитку.

Розглянуті вище системи належать до інформаційно-керуючих, їх об’єктами керування та контролю є залізничні пристрої. Однак не меншу вагу мають ІКС для підтримки прийняття рішень оперативного персоналу залізниці. За своєю кількістю вони переважають усі інші і будуються за галузевою ознакою. Загальногалузеві системи забезпечують функціонування залізничного комплексу України, а галузеві прив’язані до

конкретної галузі. Прикладом галузевих АСК є системи планування перевезень, забезпечення роботи залізничних станцій обліку вагонів та роботи локомотивів, розподіл електричної енергії тощо. Також слід вказати на АСК для комерційної та фінансової роботи, матеріально-технічного постачання і багато інших.

Основними складовими загальної автоматизована система керування (АСК) АТ «Укрзалізниця» (УЗ) є:

– АСК ВП УЗ – автоматизована система керування вантажними перевезеннями УЗ;

– АСК ПП УЗ – автоматизована система керування пасажирськими перевезеннями УЗ;

– АСК РС УЗ – автоматизована система керування рухомим складом (локомотивами та вагонами);

– АСК ЕФ УЗ – АСК економіка, фінанси та матеріально-технічне забезпечення УЗ.

За попередніми приблизними підрахунками загальна кількість видів АРМ персоналу на залізничному транспорті нашої держави становить декілька сотень.

1.4. Концепція безпеки спеціалізованих комп'ютерних систем

Концепція, тобто загальна ідея, головна думка, набір загальних принципів убезпечення процесу функціонування КС потребує деяких пояснень. Очевидно, що розробники та споживачі потребують отримувати лаконічне і вкрай однозначне визначення цієї ідеї. Такий підхід забезпечить можливість уникнення непорозумінь та можливостей існування інших трактувань головних понять.

Формування концепції завжди починається з визначення мети існування системи, її призначення та переліку основних функцій. Логічно припустити, що чим простішою за конструкцією та функціями є КС, тим більш однозначною буде її концепція безпеки. Для складної системи керування завжди важко сформулювати просту та однозначну ідею убезпечення функціонування. Насамперед це пояснюється численними

робочими функціями, що часто мають внутрішні протиріччя. Так, встановлення нових засобів технічної діагностики або автоконтролю розширює можливості системи щодо виявлення передаварійних станів, але одночасно зменшує її безвідмовність.

Зважаючи на це, приходимо до висновку, що чим складніша СКС, тим більш різноманітними будуть методи та підходи до її функціональної безпеки у цілому. Як учинити інженеру-розробнику у такій складній ситуації, сповненій численними протиріччями? Однак наука і практика давно мають надійну підказку – це застосування комплексного підходу під час формування концепції безпеки. Тобто сучасна концепція безпеки СКС передбачає одночасне застосування багатьох підходів, навіть якщо вони формально можуть мати внутрішні протиріччя. Такий підхід подано у документі Європейського комітету з електротехнічної стандартизації CENELEC EN50126 для використання на залізниці[17]. Власне сама абревіатура RAMS у назві стандарту означає одночасне використання показників безвідмовності, експлуатаційної готовності, ремонтопридатності та безпеки. Цей документ формує концепцію СКС як поєднання цілей якості, продуктивності та безпечності. Саме такий підхід повною мірою відповідає вимогам міжнародних стандартів ISO 900. На практиці це означає комплекс поєднання різних стратегій досягнення безпечності системи. Європейський стандарт EN 50126 CENELEC надає в розпорядження залізничним підприємствам, розробникам та постачальникам залізничної продукції спосіб послідовного використання керування надійністю, експлуатаційною готовністю, ремонто-придатністю та безпекою (RAMS) для залізничного транспорту.

Поняття RAMS – це характеристика поведінки системи при тривалому функціонуванні, яка досягається застосуванням технічних планів, процесів, інструментів і техніки під час усього життєвого циклу системи. RAMS для системи можна описати як кількісне і якісне зазначення ступеня, до якого може система, підсистема або компоненти, з яких система складається, функ-ціонувати згідно зі специфікацією. Під RAMS у рамках цього стандарту розуміють комбінацію надійності (**Reliability**), експлуатаційної готовності (**Availability**), ремонтопридатності (**Maintainability**) і безпеки (**Safety**).

Безпека й експлуатаційна готовність пов'язані за змістом одна з одною, причому конфлікт, викликаний неузгодженістю між вимогами безпеки й експлуатаційної готовності, може перешкодити досягненню необхідної надійності системи.

Зв'язок між елементами RAMS вказує на існуючу взаємозалежність між показниками безпечності й експлуатаційної готовності (рис. 1.4).

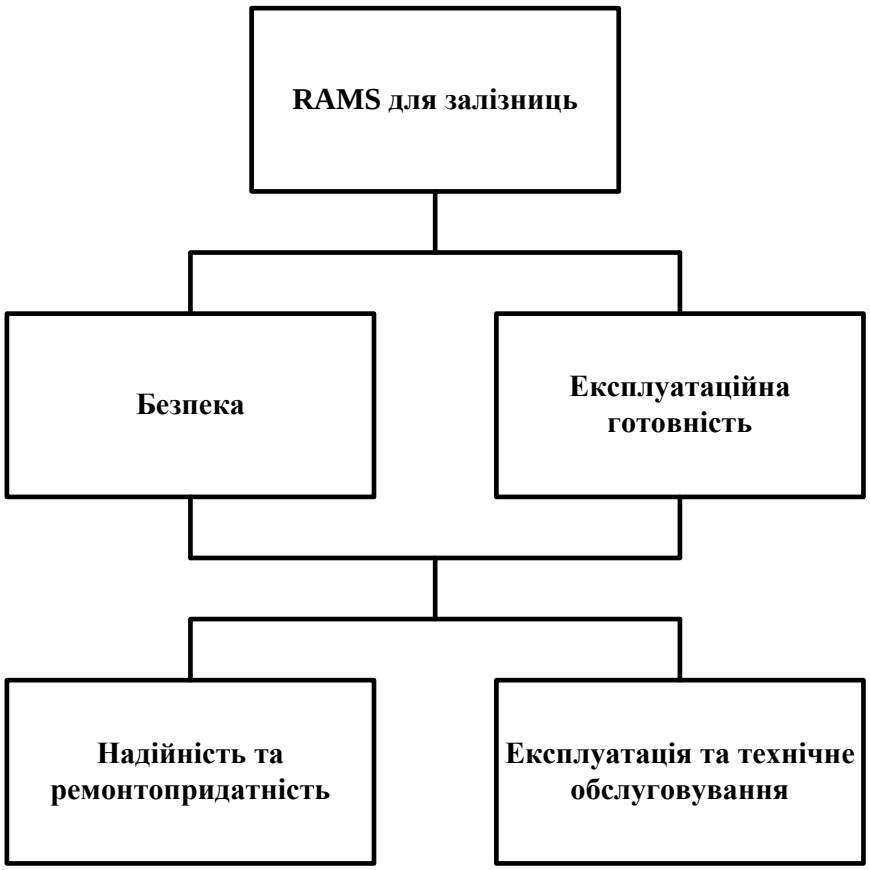


Рис. 1.4. Зв'язок між елементами RAMS залізниці

Цілі безпеки й експлуатаційної готовності можуть бути досягнуті тільки тоді, коли постійно виконуються вимоги надійності і ремонтопридатності та здійснюються поточні основні роботи з технічного обслуговування.

Технічні принципи для експлуатаційної готовності ґрунтуються на відомостях:

– про надійність;

– ремонтопридатність;

– експлуатацію й технічне обслуговування.

Технічні принципи для безпеки ґрунтуються на відомостях:

– про всі можливі небезпечні стани в системі при всіх режимах експлуатації, технічного обслуговування і станах довкілля;

– показники кожного небезпечного стану, що виражається в тяжкості їх наслідків;

– імовірність виникнення відмов, що пов’язані з безпекою; послідовність виникнення подій, які можуть призвести до відмови і навіть аварії; імовірність, з якою відбувається кожна з цих подій або відмов;

– ремонтопридатність усіх пов'язаних з безпекою частин системи;

– процес експлуатації системи і технічного обслуговування пов'язаних з безпекою частин системи з урахуванням впливу людського фактора на ефективне технічне обслуговування; засоби та методи ефективного його проведення;

– ефективний контроль і заходи щодо уникнення небезпечних станів і зменшення їх наслідків.

Характеристики RAMS залізничної системи схильні до потрійного впливу, а саме: джерел помилок (пошкоджень) і відмов, які проявляють себе всередині системи на будь-якому етапі життєвого циклу системи (системні умови); заважаючих впливів, яких зазнає система під час експлуатації (умови експлуатації); джерел помилок (пошкоджень), яких зазнає система під час робіт з технічного обслуговування (умови обслуговування). Ці джерела помилок (пошкоджень), відмови і заважаючі впливи, тобто дестабілізуючі фактори можуть також взаємодіяти одне з одним.

Як указано у RAMS, функціонування залізничної системи забезпечується внаслідок комплексного підходу, який ураховує системні умови, умови експлуатації й технічного обслуговування (рис. 1.5). Такий підхід має принципове значення для розроблення організаційних заходів і технічних засобів, що спрямовані на підвищення функціональної безпеки [54].

На підставі аналізу даних і статистики RAMS з'являється можливість розроблення та впровадженні нових методів експлуатації і підтримки систем залізничної автоматики у штатному, безпечному стані [17].

Рис. 1.5. Ілюстрація системного підходу RAMS залізниці

Згідно з [46] при створенні сучасних ІКС залізничної автоматики основним напрямком є принцип виключення можливості появи потенційно небезпечної ситуації (або зведення ймовірності появи цієї події до мінімально допустимої величини).

Тому досягнення безпеки функціонування пристроїв і систем керування рухом поїздів повинно базуватися на таких основоположних принципах:

– гарантування безпечного функціонування системи керування;

– забезпечення якісного виготовлення пристроїв системи і її програмного забезпечення;

– принцип допущення гіршого випадку, при якому система навіть при малоймовірному поєднанні вражаючих факторів повинна виключати появу потенційно небезпечної ситуації;

– організація безперервного контролю функціонування об’єктів керування в процесі експлуатації;

– здійснення моніторингу стану пристроїв системи методами діагностики.

Для цього використовуються контролюючі і діагностуючі пристрої, які оцінюють значення вихідних параметрів системи і значення спеціальних діагностичних ознак, а в необхідних випадках і навколишнього середовища (вібрації, температура, електромагнітний стан та ін.).

Другою складовою концепції безпечності СКС є застосування принципу однієї відмови. Тобто система або пристрій, що мають безпечні властивості, повинні блокувати будь-яку одноразову відмову технічних засобів, одноразовий збій у роботі програмного забезпечення чи одну помилкову дію персоналу.

Стратегії та принципи. Зважаючи на складність та багатофункціональність залізничних систем критичного призначення, всі вони тією чи іншою мірою використовують усі стратегії: безвідмовності; безпечної поведінки при відмові; відмовостійкості та ремонтопридатності.

Розробники релейних систем приділяли основну увагу стратегіям безвідмовності та безпечної поведінки при відмові. Показники безвідмовності забезпечувались якісними матеріалами й технологіями виготовлення апаратури (є випадки роботи релейних систем протягом 70 років і більше, реле першого класу перевіряється один раз на 10 років). Відмовостійкість забезпечувалась переважно для джерел живлення апаратури: джерело живлення підключалось до дубльованої електричної мережі (два незалежних фідери), якщо пошкоджено обидва фідери, система переходила на резервне джерело від акумуляторної батареї або резервного генератора.

Перші релейні системи потребували значних витрат часу для проведення ремонтних або відновлювальних робіт. Крім того, саме поняття технічного обслуговування для пристроїв сигналізації, централізації та блокування практично виключало виконання ремонтних робіт, застосовуючи профілактику та заміну. Тільки у 60-х роках двадцятого сторіччя почали впроваджуватися релейні системи керування рухом поїздів блокового типу. Це дало змогу суттєво зменшити час на пошук відмови та її усунення.

Зміна елементної бази залізничних СКС привела до перерозподілу ваги стратегій; на відміну від унікальних, характерних тільки для залізничного транспорту методів досягнення показників функційної безпеки, почали використовуватися більш уніфіковані підходи, які характерні для СКС промисловості (рис. 1.6, а). Розробники сучасних КС використовують повною мірою всі стратегії, віддаючи деяку перевагу стратегії безпечної поведінки при відмові, як показано на рис. 1.6, б.

Європейський стандарт EN 50126 визначає концепцію залізничних систем керування також у вигляді симбіозу стратегій безпечності, експлуатаційної готовності та ремонтопридатності (рис. 1.5) [17].

А – релейні системи

В – мікропроцесорні системи

Рис. 1.6. Стратегії безпечності СКС:
А – релейні системи, В – мікропроцесорні системи

Мається на увазі, що процеси експлуатації залізниці й технічного обслуговування компонентів її інфраструктури повинні відбуватися за особливими процедурами, які гарантують безпечність.

Надалі звернемося до поняття «**захисний стан**». Безпечна поведінка при відмовах або збоях програмного забезпечення

досягається завдяки використанню так званого «захисного стану», захисної та небезпечної відмови.

Спробуємо більш докладно розібратися у цьому, використовуючи ситуацію, яка знайома кожному. Коли людина захворіла, то її життєва активність зменшується, вона лежить та приймає ліки, тобто її життєва активність суттєво обмежується доти, поки вона не одужає. Що буде, якщо хворий продовжуватиме повноцінно працювати? Лікарі і життєвий досвід показують, що нічим хорошим така безглузда поведінка, як правило, не закінчується.

Аналогічний підхід маємо і в техніці: очевидно, при пошкодженні пристрою або системи вони не можуть у повному обсязі виконувати покладені на них функції, й, очевидно, не в змозі забезпечити належний рівень безпеки (читайте вищенаведений приклад). З цієї причини система переходить від штатного стану до нештатного стану захисної відмови і далі до нештатного захищеного стану, у якому можливості виконувати покладені на неї функції штучно обмежуються до гарантованого безпечного рівня (рис. 1.7).

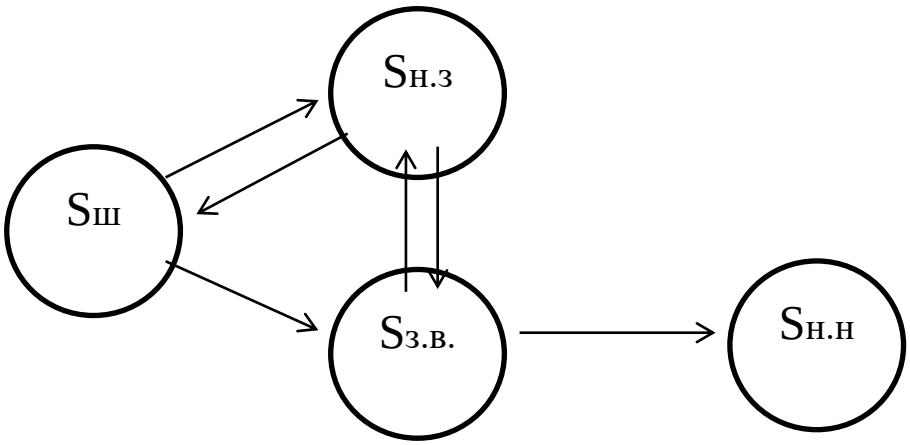


Рис. 1.7. Граф станів залізничних систем критичного призначення

Згідно з наведеним графом при пошкодженні система переходить зі штатного до нештатного стану. У КС загального призначення при пошкодженні системи вона може перебувати достатньо довго, поки персонал не ідентифікує порушення й почне процедуру відновлення. При цьому він самостійно виключає обладнання для проведення ремонту, але може цього і не робити.

Для залізничних систем, які є критичними до безпеки, такий підхід категорично не можна використовувати, але ЧОМУ?

Головною причиною є те, що при перебуванні у нештатному стані захисної відмови не гарантується безпечність виконання основних робочих функцій. До того ж, чим довше система буде перебувати у нештатному стані, тим більша ймовірність появи ще одного порушення та відповідно виникнення небезпечної події.

Таким чином, на відміну від так званих універсальних, звичайних СКС, спеціалізовані залізничні КС мають важливу характерну особливість їх використання. Ця особливість пояснюється введенням стану захисної відмови (рис. 1.7), і надалі здійснюється перехід до захищеного стану, у який система переводиться при появі будь-якої загрози для безпечного функціонування.

Стан захисної відмови відрізняється від захищеного стану тим, що у захищеному стані здійснюється локалізація небезпеки. На відміну від стану захисної відмови переведення до захищеного стану відбувається за участю персоналу.

Усі технічні засоби залізничної автоматики будуються за таким принципом. Виникнення одного будь-якого пошкодження, одного будь-якого елемента або одноразовий збій програмного забезпечення не повинні призводити до небезпечної події. Вказані події ***автоматично*** приводять до переведення у стан захисної відмови Sз.в., після чого за командами персоналу система переводиться у нештатний захищений стану Sн.з.

$$S\text{Ш} \rightarrow S_{\text{З. В.}} \rightarrow S_{\text{Н. З}}$$

Після проведення відновлювальних робіт відбудеться перехід до

$$S_{\text{н. з}} \rightarrow S_{\text{ш.}}$$

Під час проведення профілактичних робіт з технічного обслуговування доводиться штучно обмежувати функціонування системи, переводячи її у захищений стан, а після завершення роботи повертати у штатний:

$$S_{\text{ш}} \rightarrow S_{\text{З}} \rightarrow S_{\text{ш}}.$$

На перший погляд такий підхід надто ускладнює роботу системи керування, але це пояснюється специфічними умовами експлуатації:

– необхідність забезпечити безперервне функціонування залізничної транспортної системи за будь-яких можливих ускладнень;

– необхідність дотримання вимог безпеки.

Ці дві вимоги дуже часто є взаємовиключальними, тому саме введення такого додаткового стану $S_{н.з.}$ забезпечує можливість існування компромісу між указаними вимогами.

У КС загального призначення таких протиріч, як правило, не існує або вони не є категоричними, тому вони не мають захисного стану, переходячи від штатного працездатного до нештатного непрацездатного, і навпаки.

Для гарантування безпечної поведінки СКС та блокування подальшого розвитку небезпеки необхідно локалізувати її негативні наслідки.

Указана локалізація саме і забезпечується ***введенням захисного стану,*** у якому й відбуваються ремонтні роботи.

Другою важливою властивістю залізничних КС є те, що переведення з нештатного у захисний стан повинно відбуватися ***АВТОМАТИЧНО***, без втручання людини-оператора.

Третьою безпечною властивістю є особливості процедури повернення у штатний стан. На відміну від попереднього переходу цей відбувається ***ТІЛЬКИ ЗА УЧАСТЮ ЛЮДИНИ-ОПЕРАТОРА*** після проведення необхідних перевірок.

Окремо необхідно наголосити на ролі людини-оператора в убезпеченні роботи СКС. Персонал припускається помилок у процесі експлуатації й технічного обслуговування. Тому, очевидно, що технічні та програмні засоби КС повинні блокувати такі небезпечні дії. І навпаки, при появі апаратного чи програмного збою у роботі системи людина-оператор оперативно локалізує подальший розвиток небезпечної події. У цьому сенсі можна вважати, що людина інтегрована у технологічний процес функціональної безпеки [56].

1.5. Принципи безпеки спеціалізованих комп'ютерних систем

У попередньому підрозділі була дана характеристика СКС та критерії, за якими вони визначаються. Одним з таких критеріїв є властивість автоматичного переведення до так званого захисного стану. Розглянемо більш докладно цю та інші властивості функціональної безпечності СКС.

Кожен з нас може згадати приклади таких систем: це засоби автоматизації атомних електростанцій, системи керування літаками, охоронні системи військових складів, хімічних підприємств і багато інших. Їх загальною рисою є загрози для життя і здоров'я людей, довкілля, які виникають у процесі функціонування вказаних галузей.

Тоді не зрозуміло, чому системи, що виконують ідентичні по своїй суті завдання, можуть дуже суттєво відрізняти за принципами побудови? Порівняймо системи керування повітряними суднами, залізничні засоби автоматизації та системи керування атомними станціями.

У подібних ситуаціях необхідно відповісти на питання, яке є головним: ***як повинен поводитися об'єкт керування при появі окремих пошкоджень?*** Відповідь на це ключове питання й визначить концепцію побудови СКС.

1. Для повітряних суден головним завданням усіх систем літака є забезпечення продовження його польоту й гарантування безпечної посадки на землю.

2. Для систем керування атомним реактором при появі пошкодження, що загрожує безпеці, робота реактора повинна бути переведена на режим зі зменшеною потужністю або зупинена.

3. Залізничні системи керування рухом поїздів: при появі пошкодження функціонування системи повинно бути обмежено, тобто поїзд повинен зменшити швидкість або зупинитися, маршрути для руху не встановлюються тощо.

Аналіз наведених вище прикладів показує спільність принципів для систем залізничної автоматики та атомних електростанцій.

Що є спільним у їх поведінці при відмові? Спільним є обмеження, що автоматично накладається на роботу об'єкта керування.

Яка мета цих обмежень? Очевидно, що метою є приведення об'єкта керування до безпечного стану, при якому він не створює загроз для людей та довкілля.

У цьому сенсі головним і надважливим питанням є те, яким чином об'єкт буде приводитися до безпечного стану? *Знову звернемося до виробничої ситуації. Наприклад, на виробництві сталося пошкодження верстата. Очевидно, що у цьому випадку робітник вимикає його й викликає майстра для подальшого ремонту. У ситуації, що розглядається, робітник:* ***ідентифікує пошкодження, приймає рішення, вимикає обладнання.***

Таким чином, фактично все залежить від поведінки людини, яка, як відомо, не тільки відрізняється чіткістю виконання функцій, а й дуже часто помиляється. Очевидно, що довірити людині переводити об'єкт керування у безпечний стан є дуже невдалою ідеєю.

Який має бути вихід із цієї ситуації? Очевидно, слід по можливості виключити людину-оператора з цього ланцюга та забезпечити ***автоматичний перехід об'єктів керування у безпечний стан при появі пошкодження.*** Автоматичне переведення системи керування й відповідно об'єкта керування у безпечний, так званий «захисний стан», є ключовою умовою безпеки СКС. Тобто при появі пошкодження система керування повинна автоматично (без участі людини) перейти до захисного, безпечного стану.

Та не все так просто. Існують деякі пошкодження, які можуть з'являтися, а потім зникати. Наприклад, контакт в електричному колі. Він може зникнути і коло розірветься, а потім відновитися і протікання струму знову відновиться.

Якщо це важливе, тобто відповідальне коло з критичними вимогами до функціональної безпеки, то це не означає, що система автоматично повинна відновити функціонування у повному обсязі.

З позиції економічної ефективності, ми почуємо логічну відповідь: «так, система повинна автоматично відновити функціонування, бо при цьому втрати від простою будуть

мінімальними». Так можна чи ні автоматично відновлювати роботу об’єкта керування при появі так званого короткотермінового пошкодження?

Знову повертаємося до головного принципу – аналізу поведінки об’єкта дослідження при пошкодженні.

Спробуємо відповісти на такі питання:

– Чи відома нам причина пошкодження?

– Чи відомі нам наслідки пошкодження?

– Чи можемо ми гарантувати, що після відновлення роботи об’єкта керування його функціонування буде безпечним?

Очевидно, що не встановивши причину пошкодження і не визначивши його наслідки, зокрема й на функціональну безпеку, ми не можемо гарантувати, що після автоматичного відновлення робота об’єкта буде безпечною. **Тоді постає питання, що робити?** А тепер настає черга людини. *Вона повинна:*

– знати причину пошкодження;

– виконати роботи з відновлення системи або об’єкта керування;

– перевірити безпечність роботи.

І тільки після виконання всіх перевірок можна відновити функціонування системи або об’єкта керування.

Висновки до першого розділу та практичні завдання

1. При появі пошкодження будь-якого компонента СКС або виникнення збою програмного забезпечення система керування повинна АВТОМАТИЧНО перейти до захисного (безпечного) стану.

2. Виведення системи із захисного стану здійснюється людиною-оператором після процедури перевірки функціональної безпеки.

3. Система або пристрій, що мають безпечні властивості, повинні блокувати будь-яку одноразову відмову технічних засобів, одноразовий збій у роботі програмного забезпечення чи одну помилкову дію персоналу.

4. Досягнення безпеки функціонування пристроїв і систем керування рухом поїздів повинно базуватися на таких основоположних принципах:

– гарантування безпечного функціонування системи керування;

– забезпечення якісного виготовлення пристроїв системи і її програмного забезпечення;

– принцип допущення гіршого випадку, при якому система навіть при малоймовірному поєднанні факторів враження повинна виключати появу потенційно небезпечної ситуації;

– організація безперервного контролю функціонування об'єктів керування в процесі експлуатації;

– моніторинг стану пристроїв системи методами автоконтролю та діагностики.

5. Європейський стандарт RAMS визначає концепцію функціональної безпеки залізничних СКС у вигляді комбінації надійності (Reliability), експлуатаційної готовності (Availability), ремонтопридатності (Maintainability) і безпеки (Safety).

Практичні завдання

Мета: набуття практичних навичок щодо принципів побудови і забезпечення безпеки СКС та закріплення теоретичних знань, отриманих при вивченні розд. 1.

Завдання

1. З наведеного переліку оберіть системи керування критичної інфраструктури:

– система керування роботою двигунів літака – система керування рухом поїздів;

– система керування роботою енергоблока атомної станції – система керування роботою силового обладнання морського судна;

– система керування роботою ескалатора метрополітену – система керування роботою тунельної вентиляції;

– система керування рухом поїздів – система керування силовим обладнанням гелікоптера;

– система керування роботою обладнання хімічного підприємства – система керування роботою аеропорту;

– система керування роботою обладнання теплоелектростанції – система керування ракети Джавелін;

– система керування повітряним рухом – система керування атомним реактором.

2. Для кожної обраної пари визначте стратегії та концепції безпеки, охарактеризуйте вказані показники для кожної системи у парі.

3. Порівняйте стратегії та концепції безпеки визначеної пари, зробіть висновки щодо спільних показників та розбіжностей, наведіть пояснення.

Ситуації для проведення дискусій та обговорення

1. Чому системи керування літаками та регулювання рухом поїздів, вирішуючи загалом дуже близькі за змістом завдання, мають досить різні стратегії безпечності?

2. Які, на вашу думку, відбулися зміни у підходах до безпеки функціонування систем залізничного транспорту за останні 50 років?

Контрольні питання для самостійної роботи до розд. 1

1. Чим спеціалізовані КС відрізняються від систем загального призначення?
2. Визначте галузі застосування СКС.
3. Що означає термін «безпечність СКС»?
4. Які стратегії використовуються для гарантування функціональної безпеки СКС?
5. Що означає підхід RAMS до безпеки СКС залізниці:
6. У чому різниця між концепціями безпеки авіаційного та залізничного транспорту?
7. Концепція безпеки яких галузей промисловості є найбільш близькою до залізничної?
8. Що таке «захисний стан»?
9. Для чого системи безпеки залізничного транспорту мають «захисний стан»?
10. Які властивості захисного стану?
11. Визначте поняття захисної відмови.

2. БЕЗПЕЧНІСТЬ ТЕХНІЧНИХ ТА ПРОГРАМНИХ РІШЕНЬ

2.1. Загальні принципи

Принципи побудови апаратних засобів з безпечною властивістю. У попередньому розділі було сформульовано принцип «поодинокої відмови», який базується на тому, що будь-яке пошкодження одного елемента схеми не призводить до появи небезпечного стану. Він є захисним і переводить систему у безпечний стан. *Проілюструємо це твердження ситуативним прикладом. Наприклад, якщо стрілка або інший об'єкт керування втрачають контроль, то, очевидно, немає впевненості у їхньому стані, тому формування команд керування для них припиняється до відновлення контролю.*

Зокрема є очевидним, що виконання будь-якої керівної дії, яка спрямована на зміну стану об'єкта, може підвищити ризик небезпеки. Команди, виконання яких супроводжується більшим ризиком небезпеки, наведені у табл. 2.1.

Таблиця 2.1

Приклади команд керування з підвищеним ризиком

Команди збільшення ризику небезпеки	Команди зменшення ризику небезпеки
Увімкнення на світлофорі більш дозвільного показання	Увімкнення на світлофорі менш дозвільного показання
Переведення стрілки	Заборона на переведення стрілки
Відкриття сигналу	Заборона на відкриття сигналу
Розмикання маршруту	Замикання маршруту

Аналогічно для контрольної інформації більш відповідальною є та, при появі якої з'являється можливість формувати команди керування з підвищеним ризиком.

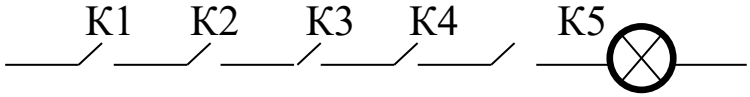
Звичайно, що наведена вище таблиця не дає повного уявлення про всі можливі команди керування, але дає змогу

визначити головну закономірність. Якщо комбінація «0» «1» призводить до збільшення ризику небезпеки, то очевидно, «1» «0», навпаки, має менший ризик. Такий саме підхід може бути використано і для комбінації «1» «0» як більш ризикованої та «0» «1» відповідно як менш ризикованої.

Вибір типу комбінацій залежить від характеру роботи об'єкта керування, який є головним при виборі. Зважаючи на це, небезпечним є спотворення, що призводить до формування саме більш ризикованої комбінації, тобто формування команди з підвищеним ризиком для безпеки.

Слід наголосити на умовності значень логічно змінних «1» та «0». Усе залежить від того, що розуміє під цими символами сам розробник.

Розглянемо критерії оцінювання роботи схемних рішень на прикладі електричного кола з п'ятьма контактами К1–К5 та лампочкою.



Замкнений стан контакту Кі позначимо через Хі, а розімкнений – як $\overline{Xi}$, тоді, якщо К1–К5 перевіряють п'ять логічних умов, то критерієм успішної роботи схеми буде функція

F1 (x) =X1 ∩ X2 ∩ X3 ∩ X4 ∩ X5 → лампа горить.

Тоді, очевидно, при неуспішній роботі наведеної схеми лампа не горить, якщо хоча б один з контактів незамкнений

$$F2(x) = \overline{X1} \cup \overline{X2} \cup \overline{X3} \cup \overline{X4} \cup \overline{X5} \rightarrow \text{лампа не горить.}$$

Припустимо, що контакт К3 пошкоджено. Розглянемо два варіанти пошкодження:

– замикання контакту (забезпечує проходження струму після вимкнення);

– незамикання контакту (струм не проходить при будь-якому стані).

Також визначено, якщо контакт Кі замкнений, то $\overline{K_i}$ – це умова безпеки.

Вважається виконаю:

Xi = 1 – контакт замкнений, умова виконана;

Xi = 0 – контакт розімкнений, умова не виконана.

Розглянемо поведінку попередньої схеми при замиканні контакту X3 = 1. Це автоматично призводить до появи небезпечної трансформації, третьої логічної змінної «0» → «1», якщо X3 = 0. Якщо виникає пошкодження, що призводить до незамикання К3, не формуються умови для проходження струму, тобто трансформація «1» → «0» для такого кола є захисною. Це пояснюється тим, що об’єкт керування не змінює свого стану, якщо виникає пошкодження електричної схеми (рис. 2.1).

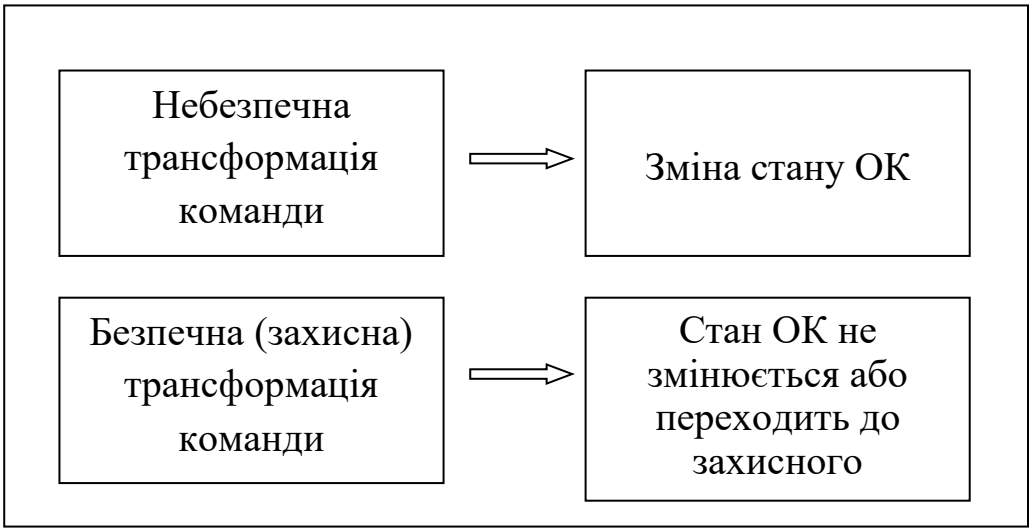


Рис. 2.1. Пояснення трансформації команд керування

Перейдемо до аналізу роботи вихідних елементів модулів виведення ПЛК. Дослідимо поведінку електронного транзисторного ключа, який є комутуючим елементом електронного модуля виведення ПЛК (рис. 2.2, табл. 2.2).

Штатний режим роботи:

– вихідний транзистор закритий, опір переходу емітер – колектор високий, струм у колі навантаження мінімальний, об’єкт керування не змінює стану;

– вихідний транзистор відкритий, опір переходу емітер – колектор мінімальний, струм у колі навантаження максимальний, об’єкт керування змінює стані.

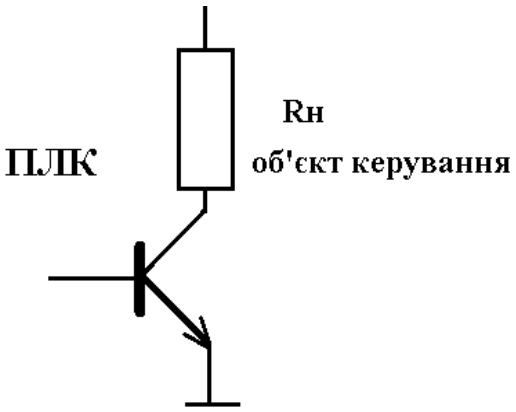


Рис. 2.2. Схема вихідного кола електронного модуля виведення

Таблиця 2.2

Характеристика станів вихідного транзистора модуля виведення

Стан вихідного транзистора модуля виведення	Стан
1. Транзистор закритий	Вимкнено
2. Транзистор відкритий	Увімкнено
3. Тепловий пробій переходу Е – К	Вимкнено
4. Електричний пробій переходу Е – К	Увімкнено

Нештатний режим (пошкодження):

– тепловий пробій, опір переходу емітер – колектор високий, струм у колі навантаження мінімальний;

– електричний пробій переходу емітер – колектор вихідного транзистора, струм у колі навантаження якого мінімальний а струм у колі навантаження максимальний.

Отже, стани 1 і 3 та 2 і 4 є тотожними за наслідками. У 1 і 3 ситуаціях об’єкт контролю (ОК) вимкнений, а у 2 та 4 – увімкнений. Отже, головною небезпекою розглянутої електричної схеми електронного кола є неможливість у статичному режимі відрізнити робочий стан транзистора від пошкодженого.

Аналогічні ситуації виникають і при організації контролю стану об’єктів керування. Тут також слід підходити диференційно до характеру створення контрольної інформації. Якщо інформація після створення вказує на появу більшого ризику, ніж той, що існує, це можна вважати відносно безпечним або, як було визначено у попередньому розділі, – захисною

трансформацією. Якщо інформація, що надається модулем введення при появі пошкодження, вказує на зменшення рівня ризику небезпеки, ніж той, що фактично існує, – це небезпечна трансформація.

Тобто, якщо активний і відповідно більш небезпечний стан ОК описується логічною одиницею, а більш безпечний – логічним нулем, тоді трансформації контрольних сигналів:

1→0 – небезпечна трансформація;

0→1 – заважаюча трансформація.

Це пояснюється тим, що при появі спотворення виду 1→0 у контролер вводиться хибна інформація про більш безпечний стан ОК. Наприклад, якщо колія зайнята поїздом, що позначається змінною Xi = 1, програмне забезпечення системи блокує встановлення маршруту. При небезпечній трансформації контрольного сигналу 1→0 це сприймається як звільнення колії поїздом і поява можливості для встановлення іншого маршруту.

2.2. Розроблення технічних рішень систем критичного призначення

Розроблення структури системи. Перед розглядом цього питання відзначимо. По-перше, розглядаючи ту чи іншу структурну схему, ми будемо мати справу тільки з функціонально завершеними елементами (модулями). Ними будуть: модуль живлення, процесорний модуль, модулі введення-виведення, комунікації і т. ін. Кожен з модулів буде розглядатися як «чорний ящик». З огляду на це можна навести аналогію з елементами конструктора, з яких збираються різні вироби [57].

По-друге, структуру однозначно визначити досить важко. Необхідно брати до уваги не тільки взаємодію процесорних блоків, але й електричних кіл введення-виведення. Наприклад, при двоканальному режимі вмикання процесорних модулів пристрої введення-виведення в каналах можуть підключатися за одноканальною схемою (рис. 2.3).

Датчик Д1 та виконавчий пристрій ВП1 увімкнуті за одноканальною схемою (кожен тільки від одного модуля).

Датчик Д2 та виконавчий пристрій ВП2 увімкнуті від двох модулів.

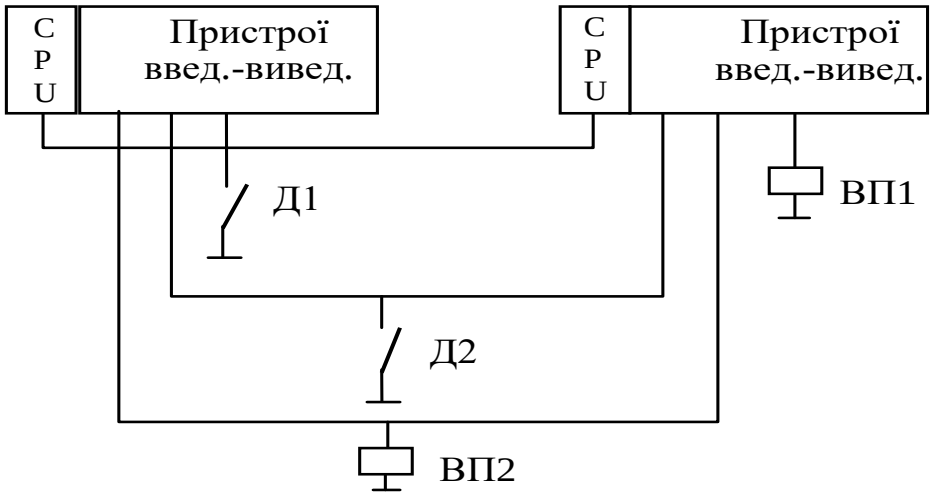


Рис. 2.3. Приклад підключення об’єктів у двоканальній конфігурації процесорних модулів

Слід звернути увагу, що двоканальна конфігурація підключення датчиків може реалізувати операцію «І» (рис. 2.4), а також операцію «АБО» (рис. 2.5).

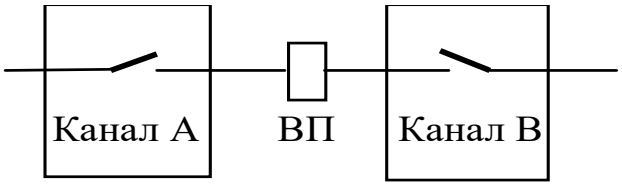


Рис. 2.4. Підключення виконавчого пристрою (ВП) при підвищених вимогах безпеки

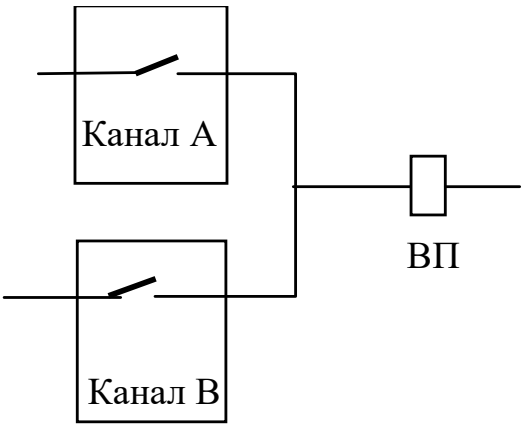


Рис. 2.5. Підключення виконавчого пристрою (ВП) при підвищених вимогах надійності

Розглянемо спочатку конфігурації систем, а потім підключення електричних кіл до модулів введення-виведення.

Одноканальна конфігурація (рис. 2.6) має один канал логічної обробки даних, пристрої введення-виведення можуть підключатися за змішаною схемою, водночас природно ми ніколи не отримаємо повною мірою всі можливості такого ж підключення при двоканальній системі. Тут можлива тільки дубльована або подвійна перевірка пристроїв введення-виведення. Вихід з ладу процесорного модуля призводить до зупинки системи, бо всі модулі як основного блока, так і модулів розширення, якщо вони є, управляються одним контролером. Такою конфігурацією важко забезпечити високі показники надійності й безпеки.

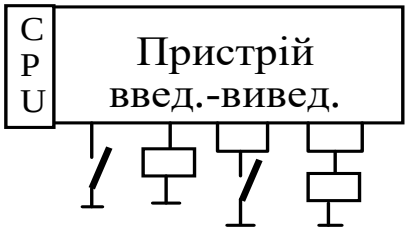


Рис. 2.6. Одноканальна конфігурація

Для поліпшення цих показників можна застосувати односторонню конфігурацію. «Одностороння» з назви означає, що блоки розширення можуть підключатися тільки до одного CPU і при виході його з ладу вони також не працюють. Система може працювати за схемою «ведений-ведучий». У наведеній схемі канал А є провідним, він здійснює виконання прикладної логіки і формує команди керування. Канал В може виконувати прикладну логіку, але самостійно в нормальному режимі команд керування не продукує. При пошкодженні каналу А функції керування може взяти на себе канал В. Іноді його використовують для задач тестування, контролю, діагностики з метою дещо розвантажити основний канал А (рис. 2.7).

Конфігурація, що перемикається, (рис. 2.8) повною мірою не може бути названа двоканальною, тому що в ній пристрій введення-виведення (ПВВ) модуля розширення може керувати тільки одним з каналів. Між собою канали А і В включаються за схемою «ведений-ведучий». При виході з ладу каналу А керування модулями розширення бере на себе канал В. У цьому

випадку пристрої введення-виведення каналу А не функціонують, а в каналі В і модулі розширення працюють.

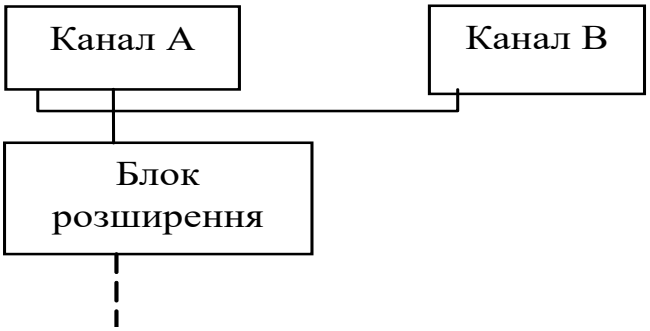


Рис. 2.7. Одностороння конфігурація

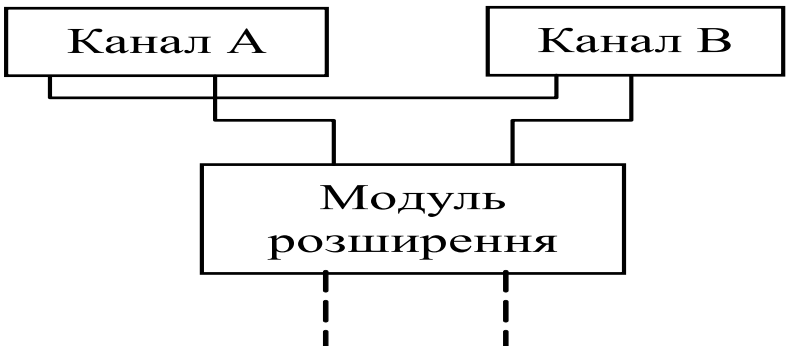


Рис. 2.8. Конфігурація, що перемикається

Як випливає з опису, така конфігурація може забезпечити досить надійну роботу системи, особливо тієї її частини, яка підключена до модуля розширення. Показники безпеки конфігурації, що перемикається, мало відрізняються від розглянутих раніше.

У класичному двоканальному режимі модулі розширення з'єднані тільки з блоком свого каналу. Це одна з найбільш простих, але водночас досить ефективних структур для вирішення завдань, пов'язаних з безпекою. У цей час світова практика має дві концепції безпеки, що досить чітко проглядається на ідеології контролерів Siemens і Schneider. Ідеологія Siemens ґрунтується на спеціалізованих технічних засобах, архітектурі й програмному забезпеченні. Такий підхід дає змогу вирішувати найвідповідальніші завдання, пов’язані з вимогами забезпечення безпеки. Його недоліком є дуже висока вартість розробки. Особливо це помітно в тих ситуаціях, коли

замовник не виставляє жорстких вимог щодо забезпечення умов безпеки, наприклад, станції промислового транспорту.

У таких умовах більш ефективною є ідеологія Schneider, що використовує принцип апаратного виділення відповідальних функцій. Для цього у звичайному промисловому контролері, наприклад, Micro або Premium, установлюється модуль безпеки, де є входи і виходи для підключення більш відповідальних об'єктів. Модуль безпеки, як правило, забезпечує перевірку виконання програми і справний стан кнопок керування і блокування.

Структура системи керування повинна реалізовуватися на певному типі контролера. Тому, визначивши у загальному вигляді структуру, переходять до вибору типу контролера. Може виявитися так, мікроконтролер що «сподобався», не в змозі забезпечити висунуті вимоги щодо структури, тоді доведеться переходити до іншого типу або знаходити компромісні варіанти.

Актуалізуються питання зв'язку між каналами і в самому каналі, між основним блоком і блоком розширення. Треба відповісти на питання: «Якими технічними засобами в запропонованій структурі буде забезпечуватися інформаційна взаємодія?».

Слід також пам'ятати, що проектована система має кимось управлятися, а для цього необхідний АРМ, тобто ЕОМ з монітором. І знову питання: «Як підключити ЕОМ до контролера?».

Як забезпечити обмін даними з автоматизованою системою управління (АСУ) або АСК вищого рівня?

Для отримання детальної інформації необхідно користуватися каталогом обраного раніше контролера.

Коли вирішено питання загальної структури системи, можна переходити і до питань конфігурації підключення кіл введення-виведення.

Конфігурації та підключення кіл введення-виведення

У реальній системі керування датчики і виконавчі пристрої вирішують різні за ступенем відповідальності завдання і тому до них висуваються різні вимоги щодо надійності і безпеки.

Для реалізації цих вимог використовуються різні типи конфігурації введення-виведення. Необхідно вказати, що всі ці модулі не є спеціалізованими. Завдання полягає в тому, щоб, використовуючи типові загальнопромислові модулі, забезпечити показники надійності і безпеки. На рис. 2.9 подано деякі можливі

варіанти конфігурації введення. Власне кажучи, їх може бути як завгодно багато. Конфігурація *а* найбільш проста без контролю стану датчика і модуля введення, у *б* та *в* показана її реалізація для двоканальної структури з одним датчиком і з двома Д1 і Д2. Це можуть бути контакти одного реле або кнопки в різних групах. За рахунок цього можна виявити злипання одного з контактів Д1 або Д2. Однак у всіх розглянутих конфігураціях пошкодження всіх датчиків або сигнал перешкоди виявити неможливо. У відповідних завданнях, коли необхідно з високим ступенем достовірності мати інформацію про стан контрольованого параметра, через контакти датчика на вхід модуля введення подається певна імпульсна послідовність (рис. 2.9, г–ж). У цьому випадку корисний сигнал відрізняється від перешкоди, крім того, остаточне рішення про стан датчика можна приймати не відразу, а після надходження декількох сигналів. Наприклад, фактом спрацювання датчика можна вважати надходження поспіль трьох імпульсів на відповідний вхід модуля введення. Зазвичай формується кілька імпульсивних полюсів живлення, як на схемі рис. 2.9, ж.

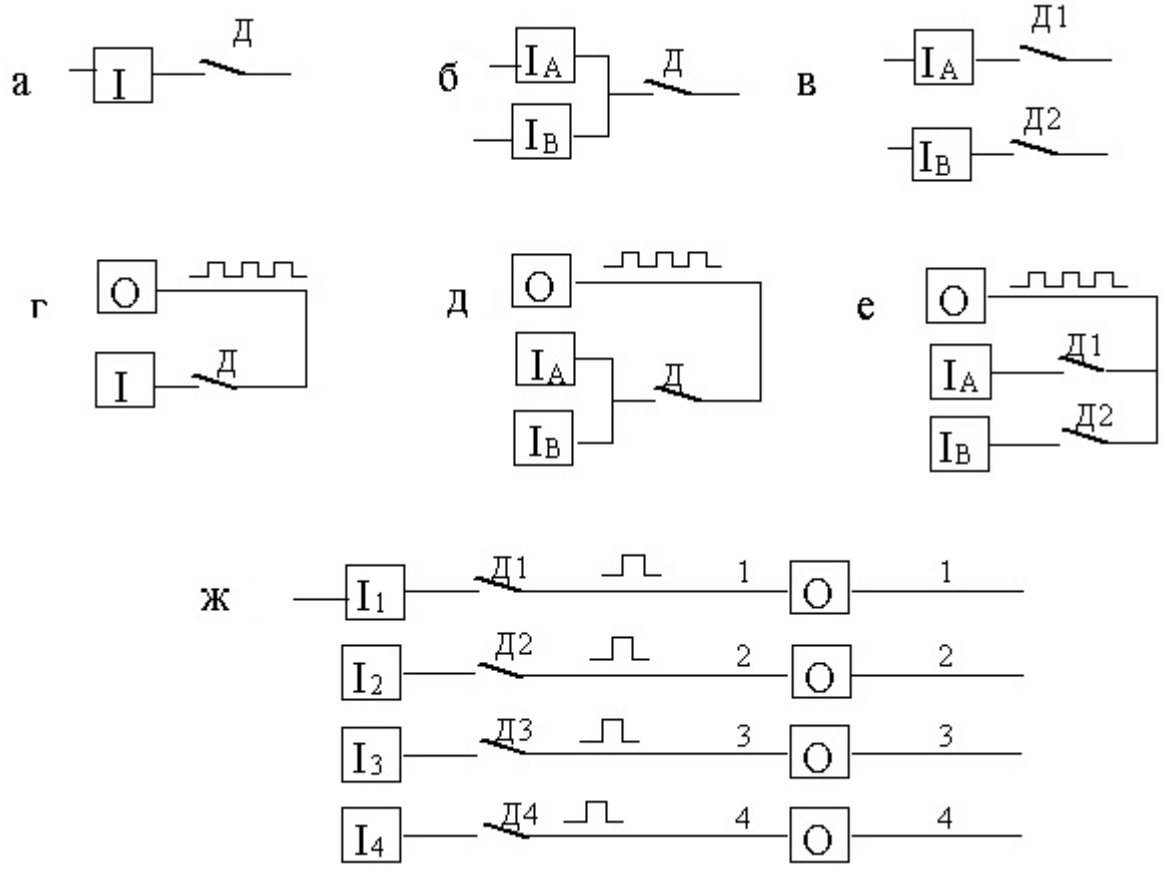


Рис. 2.9. Варіанти конфігурації введення

Зверніть увагу: конфігурації *г*, *д*, *е* відрізняються від *а*, *б*, *в* наявністю модуля виведення, який виробляє імпульсне живлення, що надходить через контакти датчиків на модулі введення.

Конфігурації виведення також можуть бути досить різноманітними, (рис. 2.10). Варіант *1* найбільш простий, без перевірки працездатності виходу з однополюсною комутацією. У *2* застосована двополюсна комутація. У цьому випадку пошкодження одного виходу не призводить до помилкового вмикання ОК, однак, контролю стану схеми немає. Варіанти *3* та *4* є розвитком схем *1* і *2*, із з'єднанням виходів за схемою «І».

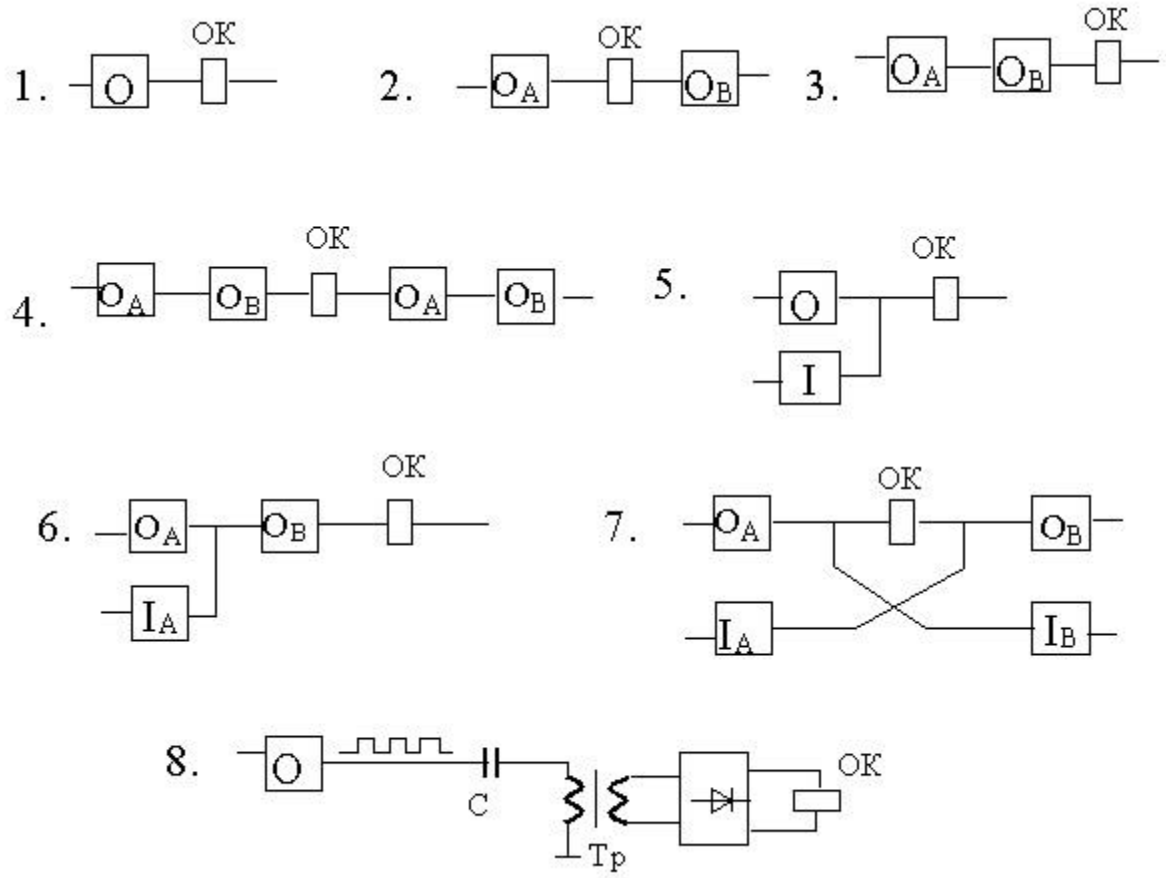


Рис. 2.10. Варіанти конфігурації кіл виведення

Конфігурації *2–4* можна використовувати в багатоканальних структурах, проте стани $О_А$ і $О_В$ не контролюються. У схемах *5*, *6*, *7* передбачений контроль стану виходу, причому в конфігурації *6* вихід $О_В$ може виконувати захисну функцію: при пошкодженні $О_А$ (електричний пробій вихідного транзистора або зварювання контактів реле) з його допомогою відбувається вимикання

виконавчого пристрою. Схема *7* у цьому сенсі більш досконала за рахунок перехресного контролю виходів по каналах А і В. Вихід каналу А контролюється входом каналу В і навпаки, крім того, двополюсна комутація покращує показники безпеки схеми.

Очевидно, що варіантів конфігурацій вихідних кіл можна запропонувати досить багато залежно від характеру конкретного завдання і висунутих обмежень за вартістю. Цей фактор часто є визначальним, тому що вартість одного входу або виходу досить велика. Слід також зазначити, що незважаючи на всілякі хитрощі при електричному пробої виходів у схемах *1–7* створюються умови для вмикання виконавчого елемента.

Для усунення цього недоліку використовується динамічний режим роботи виходу. Якщо пошкоджено елементи вихідного кола, схема втрачає динамічні властивості, і умов для спрацювання ВП немає. На схемі 8 показано вмикання реле постійного струму при імпульсному сигналі виходу. Пошкодження модуля виведення в будь-якому випадку призводить до знеструмлення реле. Такі схеми завжди досить складні і тому виконуються, як правило, у вигляді окремого конструктиву.

Схемна надмірність істотно здорожує розробку, особливо при значній кількості об'єктів керування. Однак саме по собі збільшення кількості комутуючих і контрольних елементів у відповідальному колі проблему не вирішує, оскільки в статичному режимі дуже важко виявити пошкодження (зруйнованого пристрою або хибний стан виходу).

У цьому плані становить інтерес квазіімпульсний режим роботи вихідного каскаду, зібраного за схемою 5 або 6. Якщо немає вихідного сигналу, формується послідовність імпульсів малої тривалості.

Контроль працездатності виходу при увімкненому стані забезпечується шляхом його періодичного закриття. Тривалості імпульсів і пауз підбираються таким чином, щоб вони не впливали на роботу виконавчого пристрою.

Другим, досить ефективним способом захисту схем від небезпечної відмови є комутація полюсів живлення модулів виведення контактами аварійного реле. Якщо пошкоджено вихід, аварійне реле знеструмлюється, знімаючи напругу живлення (ПА, МА) з клем модулів.

При цьому вмикання самого аварійного реле повинно проводитися від окремої схеми з безпечними властивостями.

Надалі більш детально розглянемо питання безпеки структур програмно-апаратних комплексів мікропроцесорної централізації (МПЦ), які будуються з урахуванням особливостей функціонування системи керування рухом поїздів. Існуючі структури систем мікропроцесорної централізації, як правило, мають одно- або двоканальну структуру, рідше багатоканальну структуру програмно-технічних засобів. Їх структура орієнтована на виконання функцій безпеки чи надійності (відмовостійкість, ремонтопридатність тощо). Традиційно зусилля розробників спрямовані на забезпечення реалізації функцій системи традиційними методами структурного синтезу на основі математичного апарату теорії надійності. При такому підході станція як об'єкт керування розглядається без урахування особливостей її технологічного процесу. Тим часом аналіз експлуатаційної роботи станції вказує на наявність дублюючих елементів у колійному розвитку, які забезпечують виконання поїзної роботи при пошкодженнях окремих елементів колійного розвитку. Як правило, при пошкодженні окремого елемента втрачається тільки частина функцій, що виконуються. Наприклад пошкодження стрілки парної горловини призводить до неможливості встановлення маршрутів парного приймання або непарного відправлення. Враховуючи вказані особливості технології роботи конкретної станції при побудові структури програмно-апаратних засобів систем МПЦ можна підвищити її показники надійності й функціональної безпеки.

Розглянемо роботу станції двоколійної ділянки. Якщо абстрагуватися від окремих деталей, то технологічний процес з приймання, відправлення поїздів та маневрову роботу можливо розділити на окремі технологічні зони, які спеціалізуються на виконанні експлуатаційної роботи за відповідними напрямками, (рис. 2.11).

Технологічна зона 1 забезпечує організацію непарного приймання поїздів та маневрову роботу вказаного напрямку. Технологічна зона 2 забезпечує відправлення поїздів непарного напрямку та відповідну маневрову роботу. Технологічна зона 3 забезпечує відправлення поїздів у парному напрямку та

відповідну маневрову роботу. Технологічна зона 4 забезпечує організацію парного приймання поїздів та маневрову роботу.

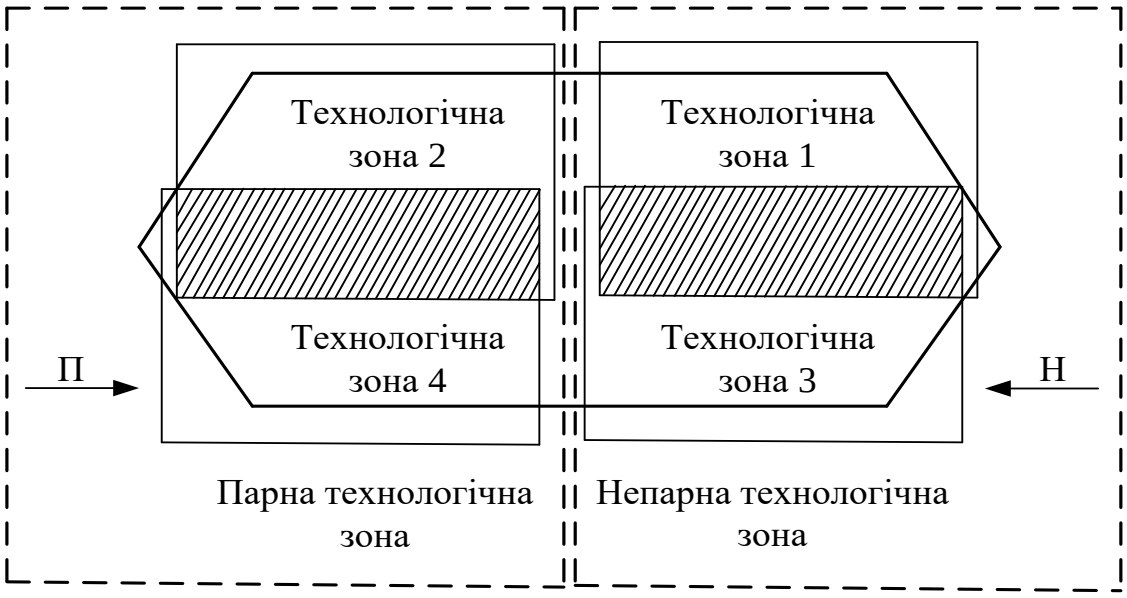


Рис. 2.11. Схема технологічних зон станції двоколійної ділянки

Кожна з технологічних зон охоплює головні колії й ділянки наближення чи віддалення, які примикають до станції. Їх функції частково дублюються: зона 1 дублює зону 3, а зона 2 дублює зону 4 навпаки. Прикладом такого дублювання є приймання поїзда по неправильній колії при нештатних ситуаціях на одній з колій перегону. Внаслідок дублювання основних маршрутів зонами 1, 3 та 2, 4 забезпечується стійке функціонування станції при окремих пошкодженнях елементів колійного розвитку.

На першому етапі розглянемо найбільш загальну ситуацію з двома технологічними зонами Н та П (непарне приймання, парне відправлення, парне приймання, непарне відправлення). Будемо вважати, що система керування має найбільш просту одноканальну структуру програмно-апаратних засобів (рис. 2.12). Структура має два однакових комплекти з ідентичним програмним забезпеченням, які орієнтовані на об'єкти керування і контролю парної й непарної горловини. Програмна логіка кожного програмованого логічного контролера має дві складові.

Отже, кожен комплект виконує всі необхідні логічні залежності станції в цілому. У штатному режимі роботи

активною є тільки складова, що забезпечує функціонування власної горловини. Інша забезпечує перевірку умов безпеки станції, але команд керування не формує.

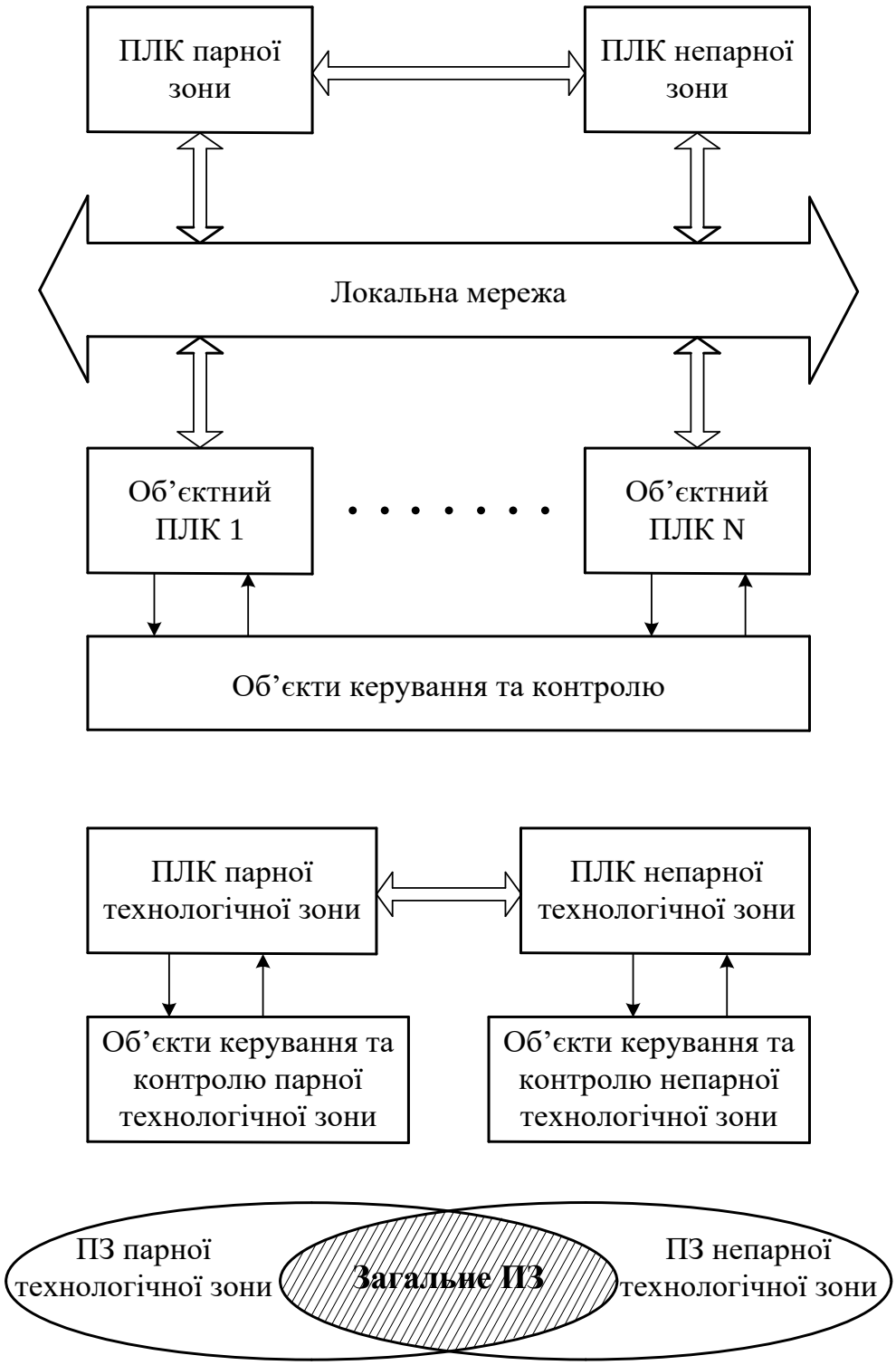


Рис. 2.12. Структура програмно-апаратних засобів МПЦ, побудованої за горловинами станцій

Введення і виведення відповідної інформації відбувається тільки після успішного порівняння результатів роботи двох програм (першої парної – другої непарної або другої парної – першої непарної). При появі збою в роботі програмного забезпечення парної (ПарЗони) чи непарної (НепарЗони) зон вихідний сигнал не формується внаслідок розбіжності результатів роботи логіки ПЛК ПарЗони та ПЛК НепарЗони. Завдяки дублюванню технологічних функцій, які реалізуються в одноканальній структурі, виконується перевірка функцій безпеки технологічних зон аналогічно у двоканальній структурі.

Розглянемо більш докладно роботу системи при пошкодженні одного з ПЛК. У такому випадку за санкцією чергового по станції система переходить у режим роботи з одним ПЛК. Функції пошкодженого елемента передаються оператору, який підтверджує можливість реалізації команди. Внаслідок використання об'єктних контролерів основні ПЛК безпосередньо не прив'язані до груп об’єктів керування, а наслідки відмов локалізуються.

Логічним продовженням попередньої структури є схема з чотирма ПЛК, що орієнтовані до раніше визначених технологічних зон. Кожний ПЛК має спеціалізацію, відповідну своїй технологічній зоні. Прикладна програмна логіка головних контролерів складається з чотирьох підпрограм відповідно до кількості технологічних зон на станції. Активною є тільки програма власної технологічної зони. Вона забезпечує керування об'єктними контролерами. При формуванні команд відбувається попарна перевірка результатів роботи головних контролерів за такою схемою: [ПЛК НепарЗони 1 – ПЛК НепарЗони 3] – [ПЛК ПарЗони 2 – ПЛК ПарЗони 4], (рис. 2.12, 2.13).

Наявність у кожному з ПЛК інших програм забезпечує стійкість систем до відмов: МПЦ продовжує функціонування навіть за умов виходу з ладу трьох контролерів логіки централізації.

На базі розглянутої структури можливо організувати двоканальне введення-виведення шляхом використання ресурсів інших ПЛК без втрати основних показників функціонування.

Подальшим розвитком запропонованих структур є поєднання їх з, класичними методами теорії надійності для вирішення завдань, пов’язаних зі створенням вітчизняної системи мікропроцесорної централізації для ділянок з напруженим пасажирським рухом.

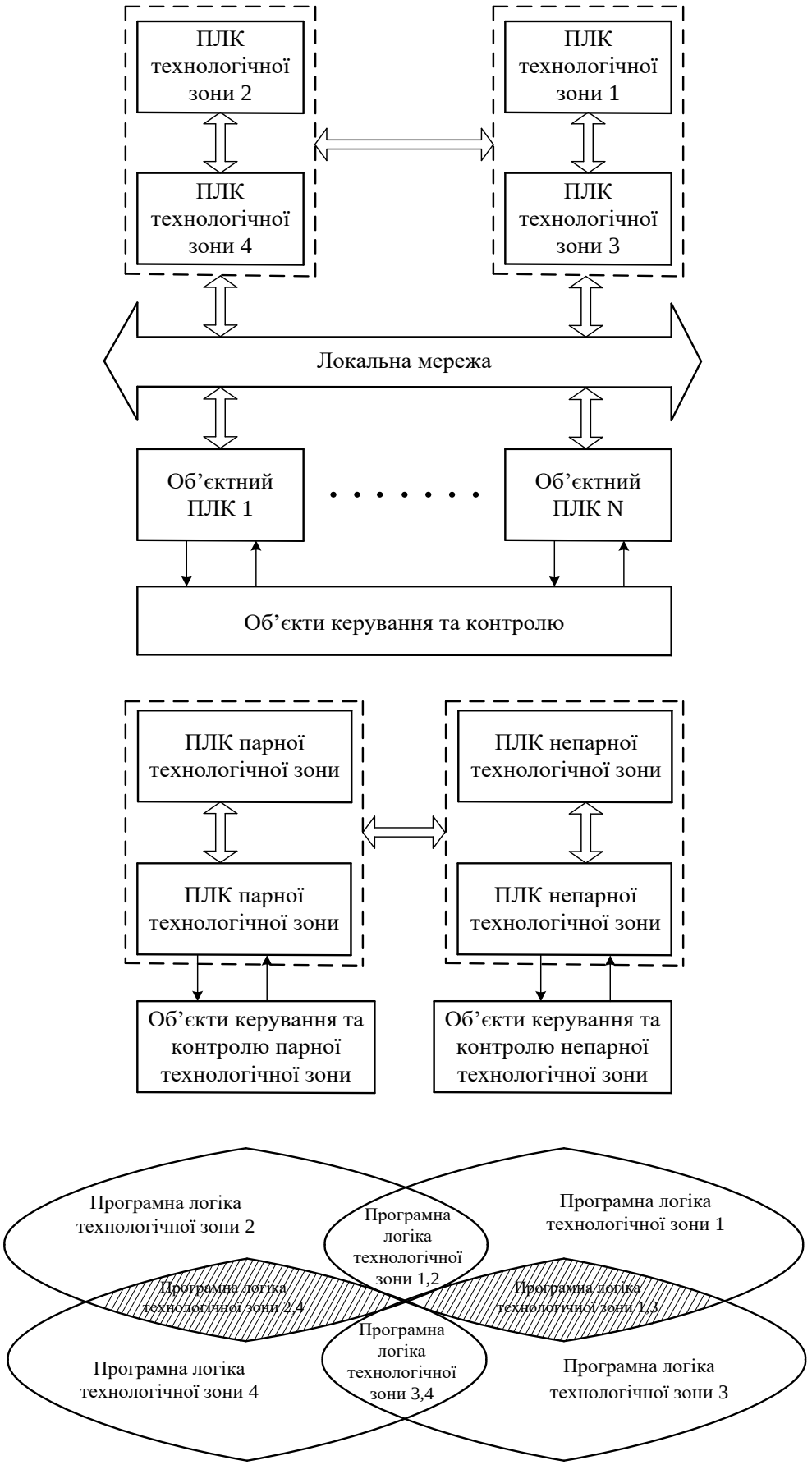


Рис. 2.13. Структура програмно-апаратних засобів МПЦ, побудованої за технологічними зонами станції

2.3. Безпечність прикладного програмного забезпечення систем критичного призначення

2.3.1. Аналіз причин та характеристика основних видів небезпечних збоїв приладного програмного забезпечення

Насамперед слід указати на деяку принципову відмінність у поведінці апаратних та програмних засобів.

На відміну від апаратних програмні засоби:

– є віртуальним продуктом, їх неможливо побачити;

– їх існування можливе тільки за умови апаратних засобів;

– програмний продукт не має терміну зберігання, він не старіє і не втрачає своїх можливостей у часі;

– збої у роботі програмного продукту можливі тільки в процесі його функціонування, він не може бути пошкоджений у неробочому стані апаратних засобів.

Нижче наведено деякі найбільш поширені причини збоїв програмного забезпечення (ПЗ) СКС

1. Збої ПЗ, що обумовлені помилками людини:

– помилки фахівців, що допущені в процесі розроблення ПЗ системи;

– помилки фахівців у процесі проектування;

– помилки фахівців у процесі експлуатації ПЗ.

2. Збої ПЗ, що обумовлені дією дестабілізуючих факторів:

– атмосферна електрика;

– електромагнітні та електростатичні завади;

– завади, що надходять від джерел живлення;

– внутрішні завади, які генеруються власними елементами системи.

Слід зазначити, що робота програмного забезпечення системи і, зокрема прикладного ПЗ, завжди перевіряється на всіх етапах життєвого циклу. Тому критерієм небезпечної трансформації команди завжди є збіг у часі двох помилок: **збій у роботі робочого ПЗ + збій тестування ПЗ.**

Найбільш характерними помилками програмістів у процесі створення прикладного ПЗ є невідповідний або не досить коректний опис алгоритму роботи об’єкта керування або систем у цілому. У процесі проектування найчастіше припускаються помилок у конфігурації системи (помилкова адресація об’єктів керування або контролю).

Помилки в процесі експлуатації не досить поширені. Вони можуть виникати при внесенні змін до робочого ПЗ. У зв'язку з чим це повинен робити тільки підготовлений фахівець з відповідним дозволом.

Особливістю помилок програмістів є те, що їх дуже складно виявити за допомогою тестової програми. Вплив зовнішніх і внутрішніх дестабілізуючих факторів зменшують відомими методами (фільтрація, екранування, заземлення тощо).

Практика впровадження мікропроцесорних систем, зокрема і на залізничному транспорті, показала ефективність багатоканальних і багатопрограмних структур. Найпростішою і найдешевшою є одноканальна, однопрограмна система з тестування. Найефективнішими за критерієм безпечності є двоканальні структури з різними програмами у каналах.

Для запобігання впливу помилок людини на якість прикладного ПЗ системи є застосування так званого програмного диверситету. Вони дають змогу виявити так звані d-відмови, обумовлені ідентичністю технічної документації обох каналів. Це пояснюється тим, що технічну документацію обох каналів готують ті самі фахівці. Тому для виявлення цих помилок і використовується метод програмного диверситету (тобто відмінності).

Програмна відмінність досягається залученням до написання ПЗ різних команд із наперед відомими різними підходами до реалізації завдання. Головною умовою є відсутність інформаційної взаємодії між командами-розробниками ПЗ.

Програмний диверситет досягається за допомогою використання:

– бригад програмістів з різним баченням реалізації завдань;

– різних мов програмування;

– різних програмістів для каналів без їх взаємодії.

Диверситетний метод є дуже ефективним для одноканальних структур, де апаратні засоби є спільними для обох програм.

Найбільш ефективними формами програмної диверситетної надмірності є:

– інверсне повторення;

– надмірне кодування;

– багатоінверсне програмування.

На теперішній час поширеним і бюджетним варіантом є інверсне повторення основної програми транслятором кодів за принципом $0 \to 1;\ 1 \to 0$.

Принцип інверсного повторення полягає у повторному розв'язанні задачі за зворотним алгоритмом. Такий підхід досить давно використовується при фінансових ревізіях та перевірці монтажних схем проектувальниками за принципом: з початку – до кінця, з кінця – до початку.

Для всіх багатопрограмних структур актуальним є питання процедури порівняння результатів. Вона може здійснюватися за результатом або покроково. Очевидно, порівняння результатів роботи різних програм можливе тільки за кінцевим результатом. Водночас не потрібно синхронізувати роботу каналів. Це спрощує систему, але ускладнює процес пошуку конкретної помилки чи збою. При покроковому порівнянні роботи програм легше виявити місце збою, але для реалізації необхідно синхронізувати роботу програм.

2.3.2. Програмне забезпечення мікропроцесорних систем залізничної автоматики

Розглянемо основні принципи підвищення безпечних властивостей мікропроцесорних систем керування рухом поїздів на станції. Спочатку доцільно розглянути питання, пов'язані зі структурним синтезом систем керування з властивостями безпеки. Вибір тієї чи іншої структури обумовлюється технічними вимогами та економічними показниками системи, що розробляється.

Для завдань з «нежорсткими» вимогами до показників безпеки може бути запропонована одноканальна двопрограмна система з безпечним введенням, виведенням та індикацією (рис. 2.14). Вона в цілому задовольняє мінімальні вимоги магістрального транспорту, але є критичною до відмов. При пошкодженні хоча б одного з компонентів структури (процесорного блока, елементів введення чи виведення) система повністю втрачає функціонування й переходить у захисний стан.

Особливістю цієї МПЦ є наявність безпечної індикації стану об’єктів керування та контролю, що відповідає вимогам вітчизняних правил технічної експлуатації залізниць.

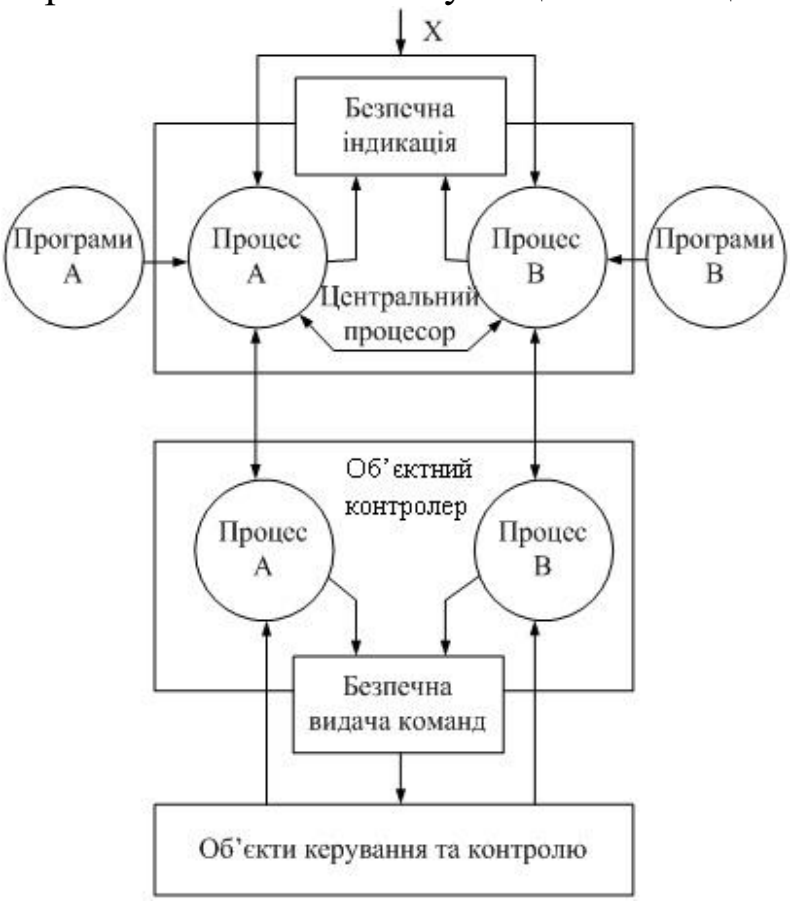


Рис. 2.14. Одноканальна двопрограмна система

Безпека функціонування забезпечується двома незалежними програмними процесами А та В, видача інформації на індикацію або на об’єктивні контролери може відбуватися тільки після порівняння та збігу результатів роботи обох каналів.

Слід зауважити, що формування відеограми станції також можливе тільки при наявності збігу сигналів від програм А та В. Аналогічно відбувається і формування команди на зміну стану польового обладнання, що контролюється програмним модулем безпечного виведення команд. Критеріями небезпечної відмови є:

– небезпечне перетворення сигналів А і В;

– формування несанкціонованої команди безпечного введення або індикації.

Для підвищення показників відмовостійкості може бути запропоновано апаратне резервування на верхньому та нижньому рівнях.

Логічним продовженням розглянутої структури є система з програмним порівнянням функціонування обох каналів (рис. 2.15).

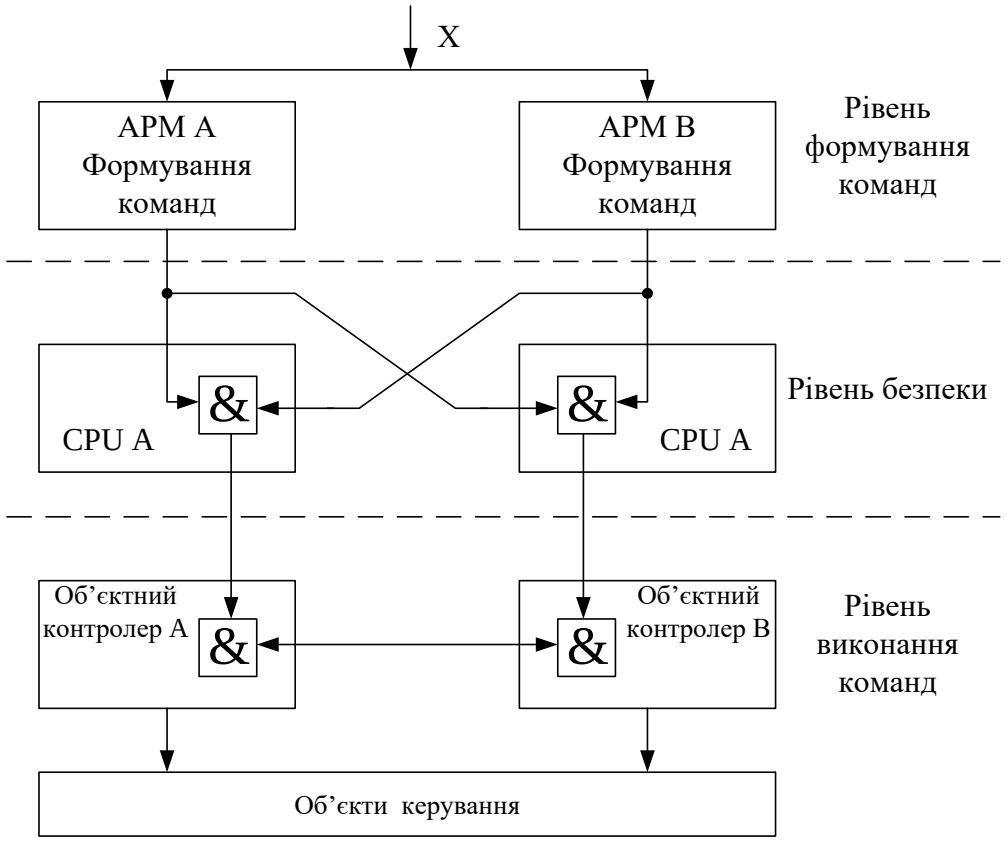


Рис. 2.15. Двоканальна структура з програмним порівнянням

Особливістю програмного забезпечення АРМ персоналу є наявність у них двох прикладних програмних оболонок: АРМ А має власну програму та програму В і навпаки. Внаслідок такого підходу АРМ А та АРМ В можуть виконувати різні функції, наприклад АРМ А використовується черговим по станції, а АРМ В – технічним персоналом.

Інформація з верхнього рівня формування команд паралельно надається на процесори логіки централізації А і В. Кожен з процесорів забезпечується даними з двох АРМ і після перевірки умов безпеки інформація передається на нижній рівень виконання команд. Формування вихідного сигналу модулями виведення об'єктивних контролерів стає можливим тільки за умови збігу результатів роботи програм у каналах А та В.

Проблемним питанням системи є безпека схем узгодження з об’єктами керування. Складнощі можуть бути частково вирішені при застосуванні двоканальної структури з апаратним порівнянням (рис. 2.16).

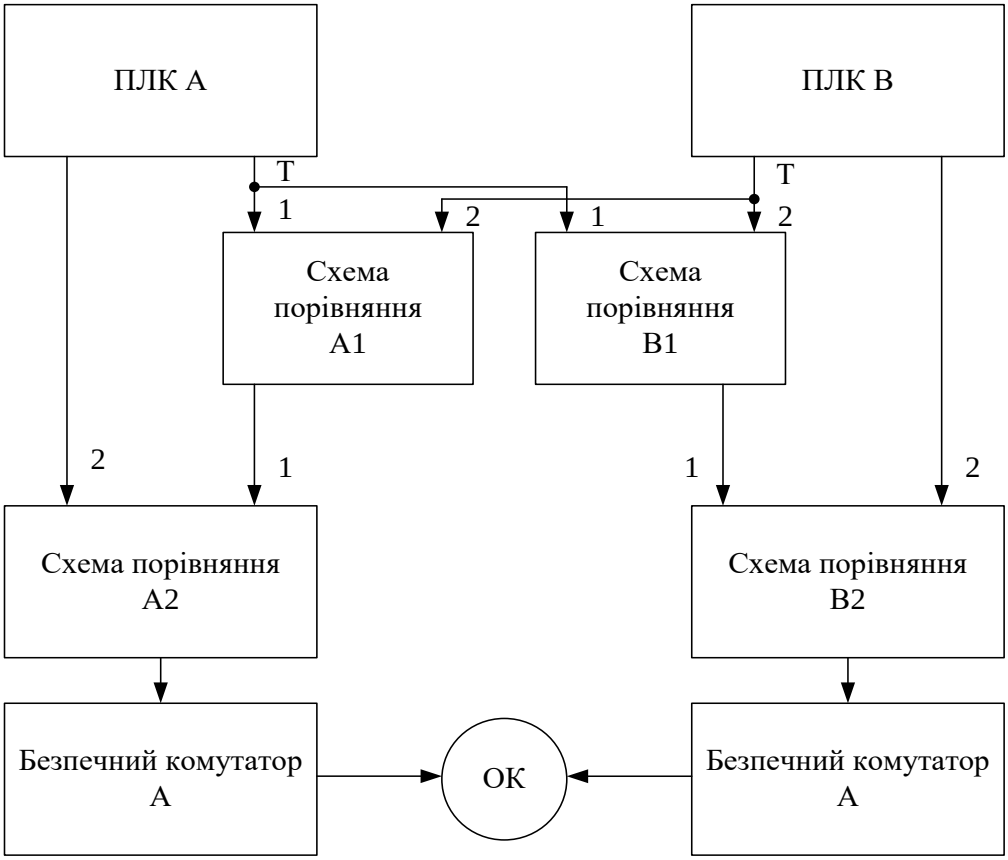


Рис. 2.16. Двоканальна двопрограмна структура з апаратним порівнянням

Система має по дві схеми порівняння в кожному каналі: A_1, A_2, B_1, B_2. Програмовані логічні контролери обох каналів ПЛК А та ПЛК В мають по два виходи для даних Д та результатів тестування Т. Схеми порівняння A_1, B_1 забезпечують перевірку робочого стану (коректності виконання програм) шляхом порівняння тестових сигналів Т обох ПЛК. При успішному результаті перевірки вони формують одиночний сигнал на тестові входи 1 схеми порівняння A_2, B_2.

Відключення об’єкта керування (ОК) відбувається при успішному результаті порівняння схем A_2, та B_2, на зворотні входи яких надходять інформаційні сигнали ПЛК А та ПЛК В. Для активізації об’єкта керування необхідно мати два безпечні

комутатори, які вмикають прямий та зворотний полюси живлення, забезпечуючи необхідний рівень безпеки [ ].

Критеріями небезпечної відмови є несанкціонована трансформація сигналів в обох каналах або збої в роботі схем порівняння A_1, B_1; A_2, B_2; A_1, B_2.

Використання безпечних комутаторів вирішує значну частину проблем виведення інформації, однак самі по собі вони є нестандартним обладнанням, що ускладнює процес упровадження та обслуговування.

Указану проблему достатньо ефективно, з технічної точки зору, вирішує гарантоване відключення живлення від об'єктів керування при пошкодженні типових модулів виведення. Модуль безпеки контролює стан виходів і у разі їх пошкодження робота системи припиняється (рис. 2.17). Окремі типи ПЛК мають подібні модулі, наприклад ПЛК Premium Schneider Electric [н].

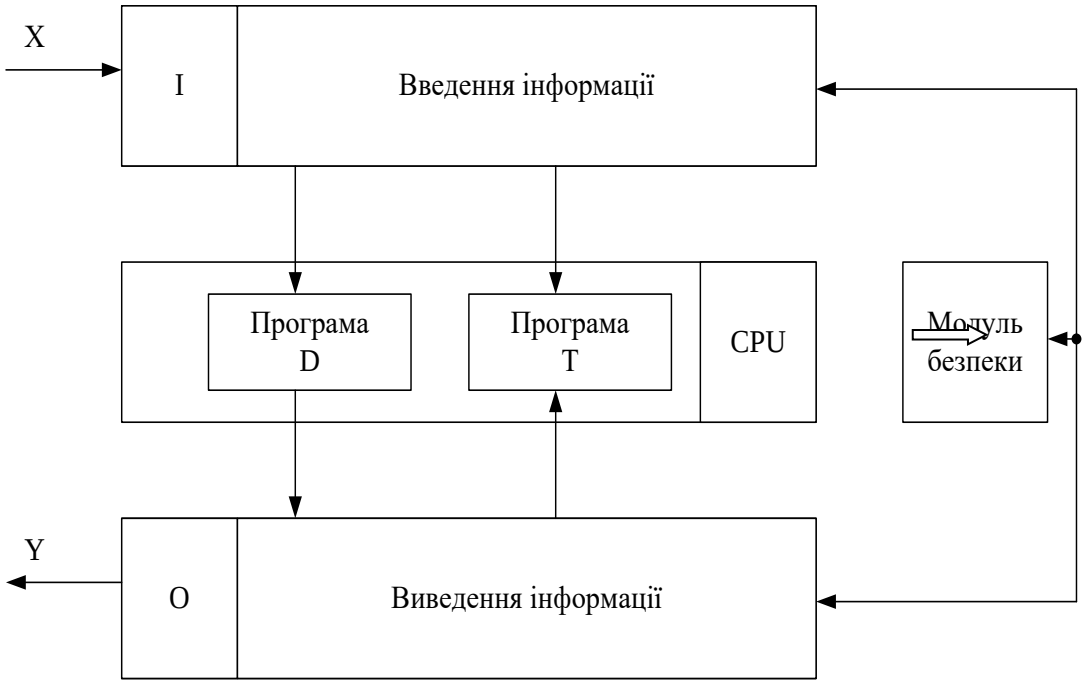


Рис. 2.17. Схема з тестовим каналом та модулем безпеки

Фактично це окремий процесор, який здійснює моніторинг стану модулів виведення і у разі незбігу фактичного значення виходу з нормованим на виході з'являється сигнал тривоги. Організація схемних рішень за цим методом досить докладно наведена у роботах [46, 57] та використана у системах МПЦ на

Південно-Західній залізниці АТ «Укрзалізниця» та Київському метрополітені.

Розглянемо реалізацію методу при вмиканні ОК. Для комутації напруги в робочих колах модулів виведення застосовуються окремі блоки комутації живлення (БКЖ).

Кожен з таких блоків забезпечує вмикання групи об’єктів керування. З позиції відмовостійкості в ідеалі кількість БКЖ має дорівнювати кількості об’єктів, однак це негативно впливає на економічні показники системи. Тому було запропоновано групувати об’єкти за технологічними ознаками. Це забезпечило підвищення стійкості системи до відмов, зменшило затримки поїздів і тому запропоновані заходи можна вважати компромісними для технічних та економічних показників (рис. 2.18).

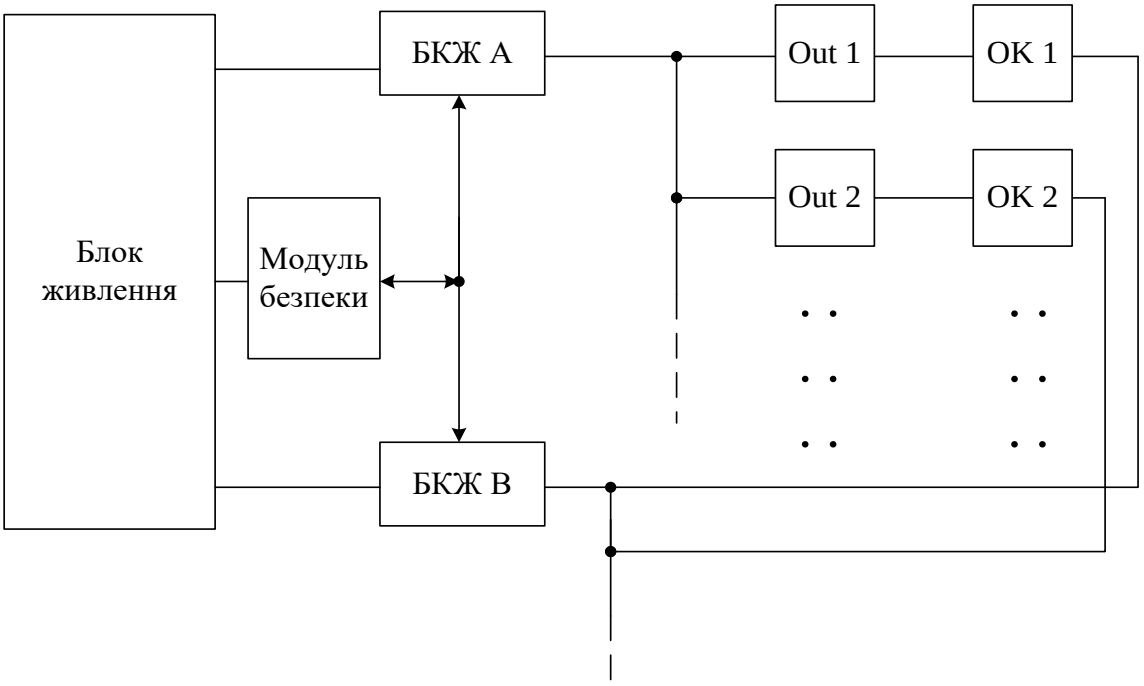


Рис. 2.18. Організація виведення інформації з безпечними комутаторами живлення

Система може функціонувати без окремого модуля безпеки, використовуючи модулі виведення для керування роботою БКЖ, за які доцільно використовувати реле першого класу. Однак водночас необхідно гарантувати безпечне вмикання керуючих реле від модулів виведення відповідно до рекомендацій, наведених у [31, 39, 40–42, 46, 57]. У вказаних роботах також сформульовано методи організації безпечного введення

відповідальної інформації. Принцип дії методу полягає у подачі на вхід модуля введення меандру стандартних імпульсів, який формує контролер на виході одного з модулів виведення (рис. 2.19). Формування вхідного сигналу відбувається за умови збігу прийнятої послідовності зі зразковим сигналом для об'єктів цієї групи. Частотне, або фазове розділення зразкових сигналів об'єктів контролю забезпечує підвищення захищеності системи МПЦ від сторонніх електромагнітних завад та сигналів інших датчиків.

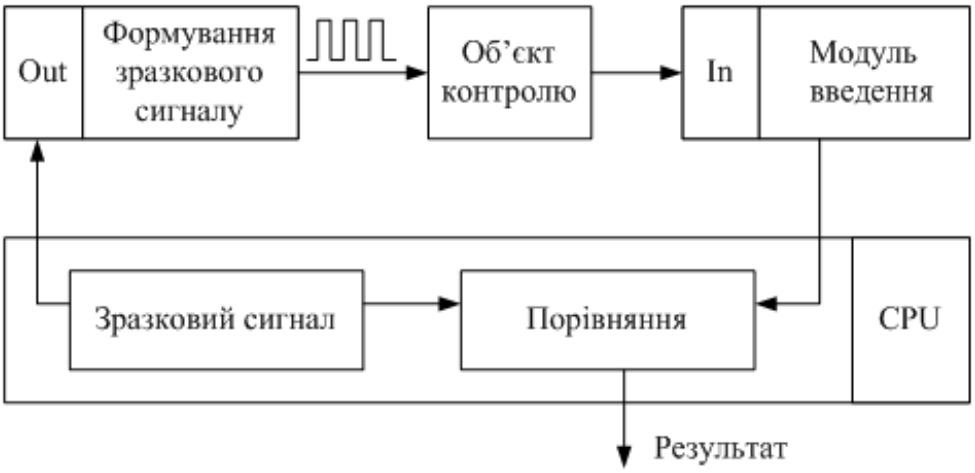


Рис. 2.19. Організація безпечного введення команд

Розвитком цього напрямку є процедура попереднього діагностування стану елементів системи, які стосуються маршруту, що встановлюється. Тестові сигнали не змінюють стан об'єкта керування, але забезпечують контроль працездатності модуля виведення перед зміною його стану.

Діагностування модуля з вимкненим ОК здійснюється сигналом ***A***, відповідно для активного виходу застосовується сигнал ***B***. Умовою формування цих сигналі є вимоги незмінності стану реле при появі імпульсної послідовності. Якщо модуль виведення не реагує на тестові сигнали, його функціонування блокується і команда не виконується.

Розглянуті методи безпечного узгодження реалізовані в системі МПЦ-М метрополітену. Вона має три рівні керування: рівень формування команд, рівень логіки централізації та рівень виконання команд. Показники безпеки та надійності

забезпечуються двоканальною двопрограмною структурою з гарячим резервуванням у кожному каналі. Усі інформаційні потоки дублюються, також дублюються всі відповідальні функції системи. Черговий по станції має основний та резервний АРМи з однаковим програмним забезпеченням. Вони функціонують паралельно, але активним може бути тільки один. У разі виникнення аварійної ситуації, пов’язаної з пошкодженням електронної компоненти, виконання основних функцій системи, пов’язаних з рухом поїздів, забезпечується пультом аварійного керування та релейними схемами вмикання польового обладнання. Описані структури були використані і на магістральному транспорті з деякими незначними змінами.

2.3.3. Приклади реалізації програмного забезпечення систем мікропроцесорної централізації

Нижче наведено опис ПЗ мікропроцесорної централізації Стріла-10 виробництва ТОВ «НВП СТАЛЬЕНЕРГО».

Структура комплексу програмно-технічних засобів (КПТЗ) побудована із використанням резервування на всіх рівнях системи, що забезпечує роботу підсистем за принципом «2oo2D».

Вона має модульну розподілену структуру, що допускає гнучку зміну конфігурації з урахуванням об'єкта проектування. До КПТЗ (рис. 2.20) входять такі складові частини:

– комплект засобів інтерфейсу користувача (КЗІК);
– центральний обчислювальний модуль (ЦОМ);
– цифровий модуль керування об’єктами автоматики (ЦМА);
– автоматизована система сповіщення та інформування (АССІ);
– установка живлення модульна суміщена (УЖМС);
– засоби технічної діагностики і моніторингу (СТДМ);
– пристрій ввідно-захисний постів ЕЦ (ПВЗ-ЕЦ);
– пульт ключів-жезлів (ПКЖ);
– пульт запрошувальних сигналів (ПЗС).

До складу КСПІ входять:

– автоматизоване робоче місце чергового по станції АРМ-Ц ДСП;

– автоматизоване робоче місце чергового електромеханіка АРМ ШН;

– автоматизоване робоче місце чергового диспетчера дистанції СЦБ АРМ ШЧД.

Рис. 2.20. Структурна схема «КПТЗ Стріла-10»

Сервери, які входять до КСПІ, – сервер КПТЗ основний та сервер КПТЗ резервний; – працюють у режимі загального резервування та забезпечують тривале збереження архіву КПТЗ: дані про минулий стан КПТЗ та польового обладнання, про дії оператора АРМ-Ц ДСП.

До складу ЦВМ входить: апаратура ядер логіки (ЯЛ) й обміну даними (АЯЛ ОД), яка містить у собі чотири ТЕЗ ядер логіки та два ТЕЗ концентраторів зв’язку верхнього рівня (КСв).

АЯЛ ОД виконує такі функції:

– зберігає в енергонезалежній пам’яті програму функціонування КПТЗ, яка складається з постійної частини (основа логіки залежностей СЦБ) і змінної частини, яка визначається конфігурацією станції;

– зберігає в енергонезалежній пам’яті уставки для параметрів ОК;

– функціонує у двоканальному режимі у справному стані (канал 1 і канал 2), а також в одноканальному режимі (канал 1 чи канал 2) при пошкодженні в одному з каналів;

– приймає дані з ОК з перевіркою відсутності їх спотворення.

АЯЛ ОД має двоканальну структуру – «постійне резервування» з використанням способу резервування «дублювання» – основний та резервний канали.

Кожен з каналів складається:

– з двох однакових ТЕЗ ядер логіки (ЯЛ А і ЯЛ В), які працюють в режимі дублювання за схемою «1оо2»;

– з ТЕЗ концентратора зв'язку верхнього рівня КСв.

Кожен з каналів АЯЛ ОД має окремі канали обміну (16 портів) для зв'язку з апаратурою ЦМА.

Програмне забезпечення ЯЛ А і ЯЛ В ідентичне, тому буде розглянуто тільки ЯЛ А (рис. 2.21).

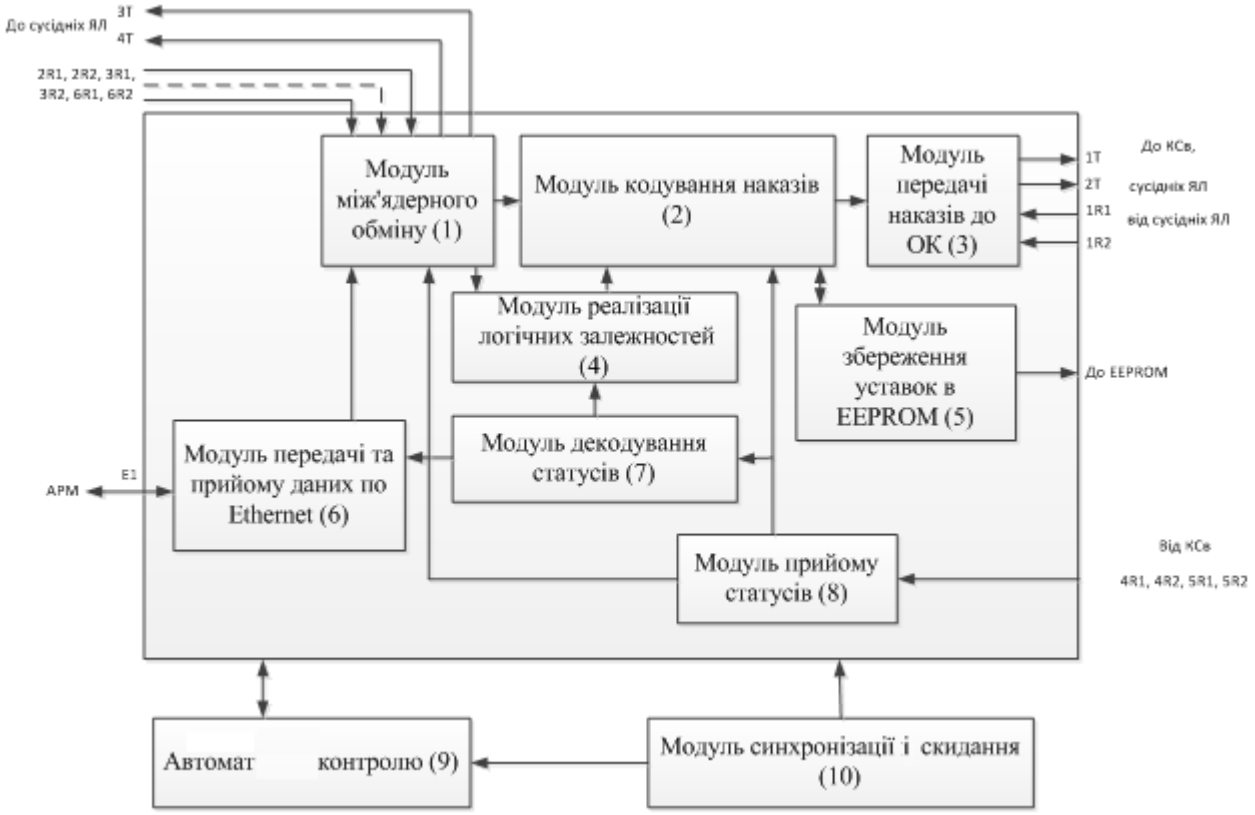


Рис. 2.21. Структура ПЗ ЯЛ

Структура ПЗ ЯЛ, наведена на рис. 2.21, та містить такі програмні модулі:

– модуль між'ядерного обміну (1) – забезпечує синхронізацію компонентів й обмін лічильниками циклів, контрольними сумами даних, ідентифікаторами статусів ОК, сигнатурами самотестування і сервісними даними між ЯЛ, вирівнювання команд, отриманих від АРМ;

– модуль кодування наказів (2) – кодує накази для передачі на ОК;

– модуль передачі наказів на ОК (3) – формує телеграми наказів, порівнює їх з телеграмами, які надходять від сусіднього ЯЛ, і передає на ОК;

– модуль реалізації логічних залежностей (4) – формує накази для ОК на основі статусів ОК і внутрішньої логіки;

– модуль збереження уставок в EEPROM (5) – зберігає у незалежну пам'ять уставки об'єктних контролерів і ознаку переходу ЯЛ в захисний стан;

– модуль передачі та прийому даних по каналах Ethernet (6) – забезпечує передачу діагностичних даних і даних блока реалізації логічних залежностей в АРМ, а також прийом команд від АРМ;

– модуль декодування статусів (7) – забезпечує декодування статусів, отриманих від ОК, і формування вихідних даних для модуля реалізації логічних залежностей;

– модуль прийому статусів (8) – забезпечує прийом телеграм статусів, а також порівняння телеграм, отриманих через КСв1 і КСв2;

– автомат контролю (9) – забезпечує синхронізацію всіх ЯЛ, що входять до складу АЯЛ ОД, керування компонентами ЯЛ і контроль їх функціонування;

– модуль (далі по тексту – модуль) синхронізації і скидання (10) – забезпечує синхронізацію роботи всіх модулів ЯЛ, а також формує частоти для взаємодії із зовнішніми системами. Забезпечує синхронне скидання всіх компонентів ЯЛ.

У структурі ЯЛ, (рис. 2.22) можна виділити функціональні вузли:

– блоки драйверів RS-422 (1, 5) – забезпечують обмін інформацією між КСв та суміжними ЯЛ. Усі блоки драйверів RS-422 обслуговуються програмовані логічні інтегральні схеми (ПЛІС) незалежно;

– блоки гальванічної розв'язки (2, 4) – призначені для захисту ПЛІС (9) від електромагнітних впливів на інтерфейсних лініях RS-422;

– блоки живлення (3) 1,2; 2,5; 3,3; 5 В зі схемою плавного пуску і фільтрації – формують стабілізовану напругу для живлення ЯЛ;

– блоки вхідних (6) і вихідних (8) дискретних сигналів – взаємодіють з відповідними блоками інших ЯЛ для синхронізації роботи;

– супервізор живлення (7). При виході рівня напруги живлення за робочий діапазон супервізор живлення видає команду в ЯЛ про необхідність переходу в початковий стан. Команда супервізора транслюється на обидва ядра в каналі, тобто при порушенні живлення в одному ядрі таку команду отримає і сусіднє ядро. При отриманні такої команди в ЯЛ запускається лічильник допустимого часу відновлення живлення. Якщо протягом цього часу живлення відновилося, ЯЛ продовжує нормальну роботу. Якщо рівень живлення не повернувся в робочий діапазон, ЯЛ виконують усі необхідні для завершення циклу і гарантування безпечної роботи системи дії, скидають усі дані і переходять у стан «Initial»;

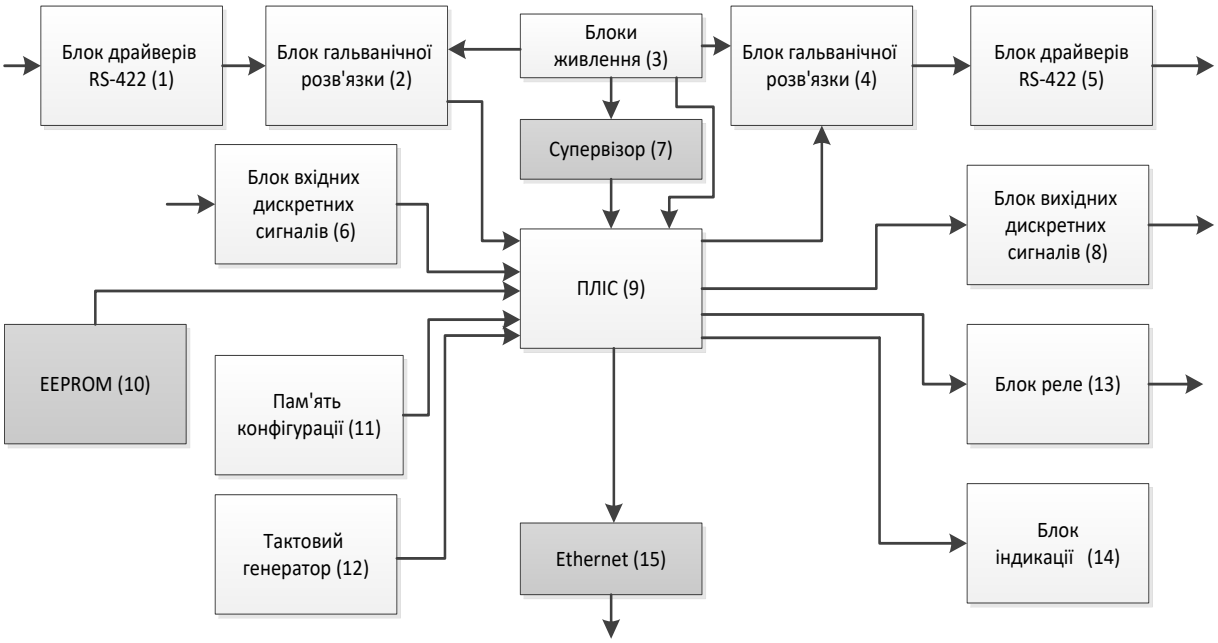


Рис. 2.22. Структурна схема ЯЛ

– програмована логічна інтегральна схема ПЛІС (9) – реалізує основні функції ЯЛ;

– незалежна пам'ять EEPROM (10), у якій зберігаються дані і ознаки переходу ОК в захисний стан;

– пам'ять конфігурації (11) – незалежна пам'ять ініціалізації ядра логіки. У ній зберігається конфігурація ПЛІС, яка захищена

контрольною сумою. При подачі живлення конфігурація перевантажується в ПЛІС, а контрольна сума за цих умов гарантує цілісність цієї конфігурації;

– тактовий генератор (12) – генератор опорної частоти 100 МГц;

– блок реле (13) – забезпечує передачу сигналу працездатності ЯЛ у систему автоматизованого диспетчерського контролю;

– блок індикації (14) – відображає поточний стан ЯЛ;

– Ethernet (15) – модуль швидкісного інтерфейсу Ethernet.

Робота програмного забезпечення ЯЛ складається з двох частин: стартової та основної.

Старт системи. При вмиканні ЯЛ в роботу запускається автомат FSM_Start_A_ea (входить до складу автомата керування та контролю 9 на рис. 2.21. Діаграма його станів наведена на рис. 2.23.

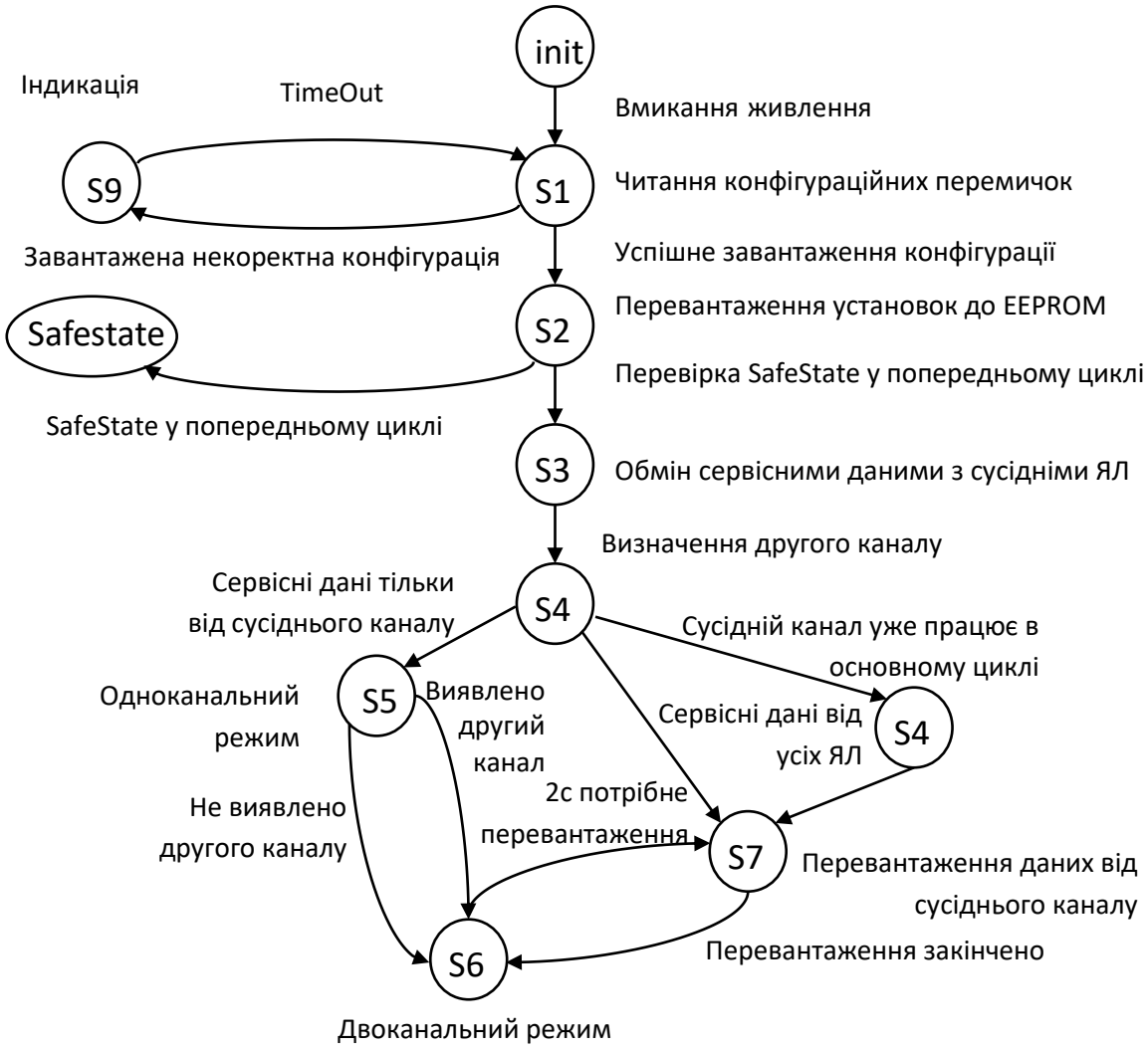


Рис. 2.23. Діаграма станів автомата FSM_Start_A_ea

У ЯЛ завантажується конфігурація, яка задається зовнішніми перемичками – тип ядра (A або B) і код станції, на якій це ЯЛ буде використовуватися (стан S1). Якщо отримана конфігурація некоректна, формується відповідна світлодіодна індикація і ядро очікує коректної конфігурації (стан S9).

Якщо отримано коректну конфігурацію, перевіряється факт входження ЯЛ у захисний стан у попередньому циклі роботи (стан S2). Якщо цей факт виявлено, робота ЯЛ блокується. Якщо в попередньому циклі роботи не було переходу в захисний стан, вставки з незалежної пам'яті EEPROM перевантажуються в модуль кодування через модуль збереження вставок в EEPROM (5) на (рис. 2.21). Коли всі вставки перевантажені, запускається обмін сервісними байтами початку роботи із сусіднім ядром (стан S3). Після отримання байта початку роботи від сусіднього ядра автомат переходить у стан визначення наявності другого каналу (стан S4).

Якщо байт початку роботи від сусіднього каналу не отриманий, ЯЛ переходить в одноканальний режим роботи (стан S5). Якщо отриманий – перевантажуються вставки між каналами (стан S7). Коли від ядер сусіднього каналу отримані дані, що вони вже працюють в одноканальному режимі, а не перебувають у стартовій перевірці, ядро переходить у двоканальний обмежений режим (стан S8). Водночас воно не формує ніяких керуючих впливів. Через 2 с в нього завантажуються необхідні дані від сусіднього каналу (стан S7) і ядро переходить у двоканальний режим роботи (стан S6).

Якщо ЯЛ в одноканальному режимі (стан S5) виявляє сервісні байти другого каналу, воно переходить у двоканальний режим (стан S6) на 2 с. Після цього перевантажує необхідні дані до ядер каналу, вмикається стан S7 та продовжує роботу у двоканальному режимі.

Основний цикл роботи. Після вибору одноканального або двоканального режиму роботи запускається автомат керування та контролю. Діаграму станів автомата наведено на рис. 2.24.

Ядро логіки видає діагностичні дані для АРМ і накази для об'єктних контролерів, сформовані в минулому циклі роботи (стан S1). При видачі накази, сформовані в сусідніх ЯЛ, порівнюються. Якщо вони не збіглися, ядро переходить у захисний стан.

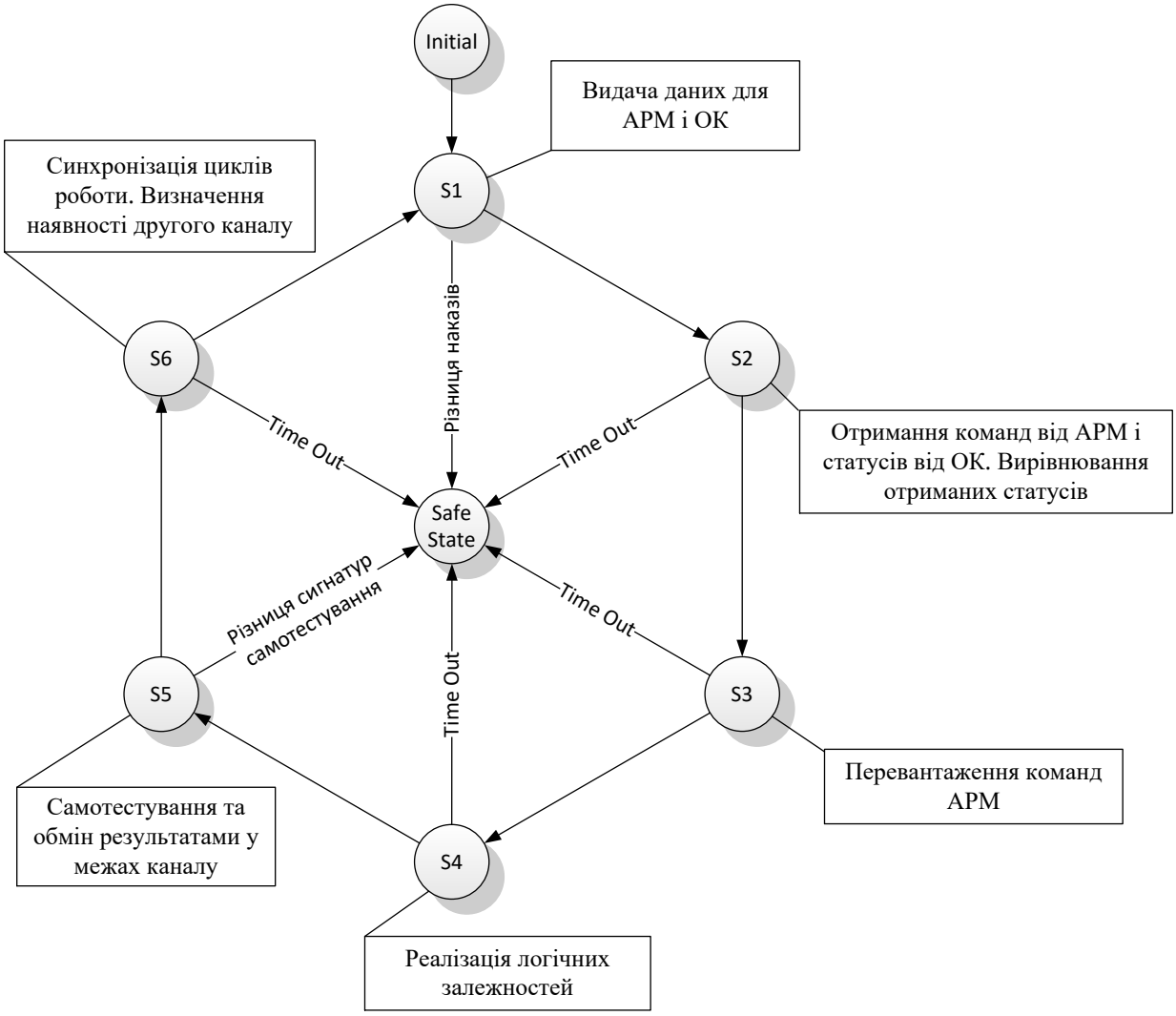


Рис. 2.24. Діаграма станів автомата керування та контролю

Після видачі всіх даних ядро переходить до отримання команд від АРМ і статусів від ОК (стан S2). Отримані статуси вирівнюються із сусіднім ЯЛ. Після закінчення вирівнювання ядра формують відповідний сигнал. Коли такий сигнал не отримано від сусіднього ЯЛ, ядро переходить у захисний стан.

Команди, отримані від АРМ, перевантажуються у внутрішній буфер і вирівнюються з усіма ядрами системи (стан S3). Після закінчення перевантаження ядра формують відповідний сигнал. Якщо такий сигнал не отримано від сусіднього ЯЛ, ядро переходить у захисний стан.

На основі статусів, отриманих від ОК, команд, отриманих від АРМ, і внутрішньої логіки формуються накази для ОК (стан S4). Після закінчення формування наказів ядра видають відповідний

сигнал. Якщо такий сигнал не отримано від сусіднього ЯЛ, ядро переходить у захисний стан. У стані S5 в кожному автоматі, що впливає на безпеку, підраховується сигнатура самотестування. Сигнатура передається в сусіднє ЯЛ, де порівнюється з обчисленою. Якщо вони не збіглися, ЯЛ переходить у захисний стан.

У стані S6 ЯЛ видає сервісні байти синхронізації циклу й очікує відповідний байт від сусіднього ядра. Його отримання означає, що обидва ядра перебувають у стані S6. При неотриманні байта ЯЛ переходить у захисний стан.

Після синхронізації циклів із сусіднім ЯЛ починається обмін з ЯЛ сусіднього каналу. Якщо цей обмін сервісними даними пройшов успішно й отримано сигнали синхронізації від сусіднього каналу, ЯЛ переходить у новий цикл роботи у двоканальному режимі. Якщо сервісне повідомлення від сусіднього каналу не отримано, ЯЛ переходить у новий цикл роботи в одноканальному режимі.

Розглянемо розрахунок інтенсивності появи небезпечної відмови в повідомленнях наказів, які передаються елементами мережевої комунікації від компонентів верхнього до об'єктних контролерів нижнього рівня системи (рис. 2.25).

Інтенсивність появи небезпечної відмови АЯЛ ОД $\lambda_{АЯЛОД}$, 1/год, складається з інтенсивностей небезпечних відмов ЯЛ ($\lambda_{ЯЛ}$, 1/год), лінії зв'язку ($\lambda_{Л}$, 1/год) та КСв ($\lambda_{КСв}$, 1/год):

$$\lambda_{АЯЛОД} = \lambda_{ЯЛ} + \lambda_{Л} + \lambda_{КСв}. \qquad (2.1)$$

Небезпечною відмовою КСв є спотворення повідомлень (телеграм) А і В таким чином, щоб вони були ідентичні та сприйняті ЦМА як коректні.

Інтенсивність небезпечної відмови розраховується як

$$\lambda_{КСв} = \frac{p_{КСв} \cdot p_{оп.и}}{\Delta t}, \qquad (2.2)$$

де $p_{КСв}$ – імовірність виходу з ладу елементів КСв, які можуть призвести до небезпечного спотворення телеграм;

$p_{оп.и}$ – імовірність сприйняття спотворених телеграм ЦМА;

Δt – цикл передачі, Δt = 100 мс.

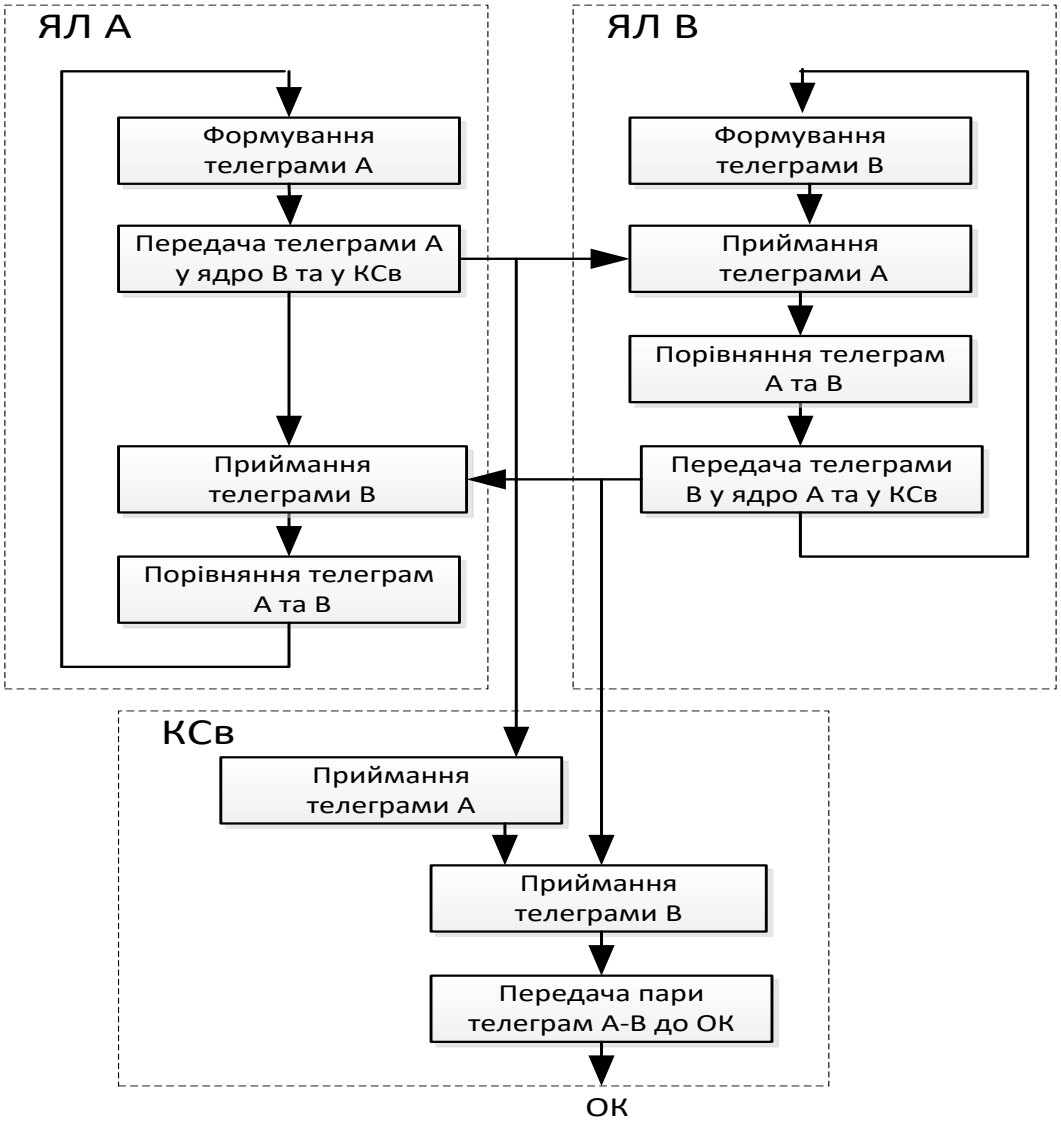


Рис. 2.25. Структурна схема безпечного формування команд керування

До спотворення телеграм А і В може призвести некоректна робота ПЛІС у КСв. Імовірність відмови ПЛІС розраховуємо за формулою

$$p_{КСв} = \frac{\lambda_{пліс}}{\lambda_{пліс} + \mu} = 9{,}0 \cdot 10^{-8}, \qquad (2.3)$$

де $\lambda_{пліс}$ – інтенсивність відмов ПЛІС, $\lambda_{пліс} = 9{,}0 \cdot 10^{-9}$ 1/год;

μ = 1/10, – інтенсивність відновлення працездатності ПЛІС (з урахуванням того, що час відновлення дорівнює 10 год), 1/год.

Для виникнення ситуації, коли ЯЛ або ЦМА сприймуть телеграму, спотворену в результаті передачі через КСв як правильну, необхідно, щоб одночасно були виконані умови:

– збіглися контрольні суми телеграм А і В;
– була правильна довжина телеграм А і В;
– був правильний тип телеграм (статус) відповідно для А і В;
– телеграми А і В були відповідними одна одній;
– збігся лічильник телеграм А і В;
– збіглася адреса об'єктного контролера в телеграмах А і В.

Збіг контрольної суми.

Наявність у форматі контрольної суми CRC-8 забезпечує виявлення помилок даних з кратністю не більше 3.

Нехай імовірність того, що в результаті некоректної роботи ПЛІС в одному кодовому символі (біті) з'явиться спотворення, дорівнює 0,5. Тоді поява «0» і «1» в будь-якому кодовому символі рівноймовірна.

Розглянемо структуру інформаційного пакета наказу (рис. 2.26), довжиною 48 біт (6 байт). Пакет містить поле адреси (2 байта), службової інформації (1 байт), поле даних (2 байта) і циклічну контрольну суму CRC-8:

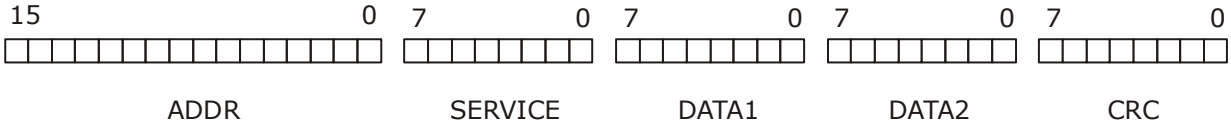


Рис. 2.26. Структура інформаційного пакета наказу

Теоретично доведено, що вибір полінома з парною кількістю елементів дає змогу виявляти всі помилки непарної кратності. Також вважається, що CRC-8 має кодову відстань $d = 4$, і може виявляти всі 1-, 2- і 3-кратні помилки. Аналітично імовірність переходу з одного дозволеного стану в інший при помилках 4, 6, 8 і т. д. кратності, для інформаційного пакета довжиною 48 біт і ймовірності помилки приймання 1 біт (Р):

$$P_{48} = \sum_{t=2}^{24} C_{48}^{2t} \cdot p^{2t} \cdot (1-p)^{48-2t} . \qquad (2.4)$$

Для перевірки та уточнення аналітичної залежності необхідно провести експерименти, де імітуються помилки при передачі цього інформаційного пакета. Очевидно, що перебір усієї сукупності можливих варіантів поєднань помилок кратності 1...48 становить певну складність і дорівнює

$$N_{48} = \sum_{t=1}^{48} C_{48}^{t} = 2.8 \cdot 10^{14} \text{ варіантам.} \qquad (2.5)$$

Для вирішення такого класу задач використовується метод Монте-Карло, суть якого полягає в багаторазових, випадкових випробуваннях математичної моделі явища. Для цієї задачі алгоритм роботи подано на рис. 2.27.

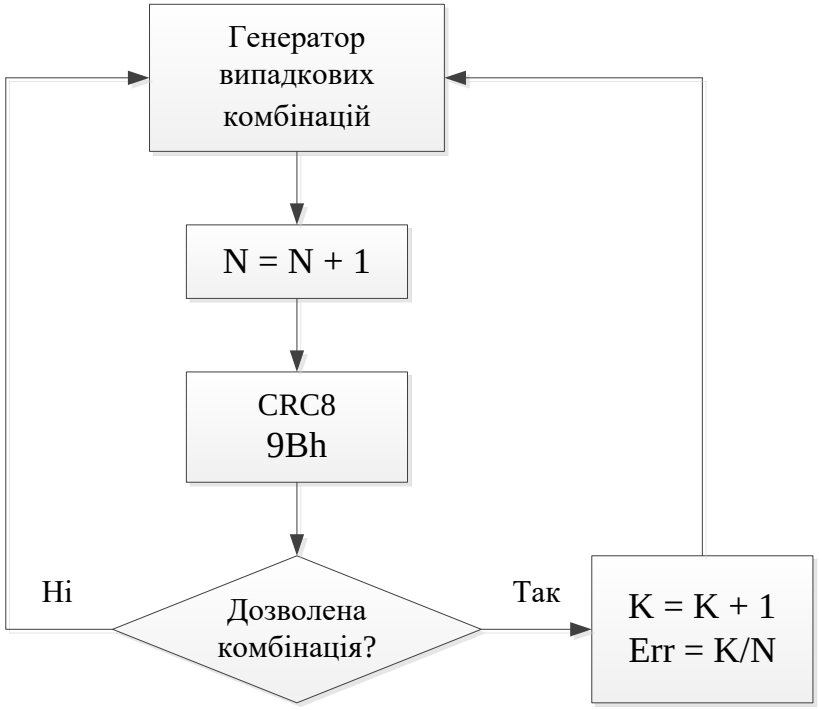


Рис. 2.27. Алгоритм перевірки можливості виявлення спотворення наказів

У процесі роботи, генератор, видає випадкові комбінації біт по всій довжині «посилки», і обчислює загальну кількість варіантів N. Якщо випадкова комбінація для полінома CRC-8 дає в залишку 0, отже така комбінація біт операцією XOR може призвести до переходу від однієї дозволеної команди до іншої, отже, є помилкою, що не виявляється.

Підрахунок відношення комбінацій, які не виявляються, K до загальної кількості випадкових комбінацій N дає оцінку завадостійкості обраного полінома ($x^8 + x^7 + x^2 + 1$) і дає змогу уточнити теоретичну формулу визначення помилок. Результат роботи наведено в табл. 2.3.

Таблиця 2.3

Результати перевірки можливості виявлення спотворення наказів

Крат-ність	1	2	3	4	5	6	7	…	44	45	46	47	48
Err	0	0	0	0,077	0	0,077	0	…	0,077	0	0,062	0	0

Значення Err показує частку комбінацій, які не виявляються у загальній кількості сполучень для помилок цієї кратності. Як видно, захист пакета циклічної контрольної суми CRC-8 справді дає змогу виявляти всі помилки кратності до третьої і всі непарні помилки. Отже, імовірність приймання спотвореного повідомлення, що не виявляється:

$$P_{err} = \frac{1}{130}\sum_{t=2}^{22} C_{48}^{2t} \cdot p^{2t} \cdot (1-p)^{44-2t} + \frac{1}{160} C_{48}^{46} \cdot p^{46} \cdot (1-p)^4 = 3{,}85 \cdot 10^{-3}. \quad (2.6)$$

Імовірність одночасного невиявлення спотворених телеграм A і B

$P_{\text{errAB}} = (P_{\text{err}})^2 = 1{,}48 \cdot 10^{-5}$.

Результати розрахунків показують, що ймовірність спотворення наказів перебуває у межах нормативного показника [46, 76].

Висновки до другого розділу та практичні завдання

1. Одноканальні структури доцільно використовувати для завдань, не критичних до безпеки, дещо поліпшити характеристики функційної безпеки можливо завдяки двопрограмній системі.

2. Двоканальна структура з порівнянням за схемою I виграє в безпечності, але програє у відмовостійкості, покращити її характеристики можна резервуванням у кожному каналі.

3. Мажоритарна структура може забезпечити більш високі показники функціонування порівняно з класичною двоканальною, але має проблеми з вмиканням виконавчих пристроїв.

4. Для безпечного вмикання датчиків та виконавчих пристроїв необхідно контролювати не тільки стан об'єкта керування, а й стан модуля до якого він підключений.

5. Найбільш ефективним з точки зору безпечності інтерфейсу є застосування динамічного режиму роботи кіл введення – виведення.

6. Програмне забезпечення є віртуальним продуктом. Воно не змінює своїх властивостей у часі, а збої проявляються тільки в процесі функціонування.

7. Найбільш ефективним методом досягнення безпечних властивостей прикладного програмного забезпечення СКС є програмний диверситет, оснований на відмінностях програм у каналах.

Практичні заняття

Мета: набуття практичних навичок щодо побудови архітектури СКС та організації безпечного вмикання пристроїв керування і контролю, закріплення теоретичних знань, отриманих при вивченні розд. 2.

Завдання

1. Проаналізуйте функціональну безпечність апаратних та програмних рішень обраної автоматизованої системи керування.

2. Для заданого об'єкта керування розробіть технічні рішення з безпечними властивостями.

3. Розробіть технічні рішення для контролю стану об'єкта, який виконує функції, що безпосередньо пов'язані з безпекою.

4. Проаналізуйте функціональну безпечність варіантів конфігурації кіл введення-виведення, які зображені на рис. 2.18, 2.19.

Ситуації для проведення дискусій та обговорення

1. Проаналізуйте можливі відмови та їх наслідки:

- вихідного елемента безконтактного модуля виведення;
- вихідного елемента модуля виведення з релейним виходом;
- модуля введення;
- модуля зв’язку;
- процесорного модуля.

2. Проаналізуйте можливі наслідки збоїв у роботі програмного забезпечення:

- збій у роботі файла, де прописана конфігурація системи;
- збій від спотворення даних оперативної підсистеми;
- які наслідки від реалізації різних програмних стратегій оновлення оперативних даних про стан об’єктів (циклічна та спорадична);

Контрольні питання для самостійної роботи до розд. 2

1. Наведіть приклади відповідальних команд.
2. Яка трансформація команди керування є небезпечною?
3. Визначте головну проблему забезпечення функціональної безпеки електронних схем.
4. Наведіть приклади небезпечних пошкоджень електронного ключа.
5. Наведіть приклади небезпечних пошкоджень вихідного реле модуля виведення.
6. Наведіть приклади небезпечних пошкоджень вихідного діода.
7. Визначте критерії небезпечної відмови одноканальної двопрограмної системи.
8. Які структури алгоритмів та секцій програмного забезпечення мають більшу безпечність?
9. Охарактеризуйте поняття програмного диверситету, його види та принцип роботи.
10. Які структурні відмінності між мовами програмування програмного забезпечення?
11. Які мови програмування більш підходять для створення безпечнішого програмного забезпечення?

3. ПРОЦЕДУРИ РИЗИК-МЕНЕДЖМЕНТУ СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

3.1. Концепція та принципи оцінювання ризику

Зазвичай у техніці при проведенні досліджень явищ, що мають негативний характер, використовують математичний апарат теорій імовірностей, який є досить ефективним і дає змогу фахівцям визначити можливість появи тих чи інших подій. Основою для застосування теорій імовірностей є наявність у розпорядженні дослідника деякого обсягу статистичних даних, які характеризують об'єкт дослідження. Очевидно, чим більший розмір вибірки та час спостереження, тим більшою буде достовірність отриманих результатів.

Однак цей підхід не завжди можливо застосувати на практиці. Справа у тому, що найбільш резонансні аварії на залізничному транспорті і у промисловості стаються дуже рідко. Відповідно їх кількість є дуже обмеженою, а термін повторення дуже великий (іноді десятки років). У цій ситуації класичний підхід до визначення частот небезпечних подій не може бути застосованим, неможливо сформувати статистичну вибірку та скористатися класичним апаратом теорії ймовірності [6–11].

Альтернативний підхід базується на теорії ризиків, яка застосовує суб'єктивну логіку. Імовірність появи рідкісних явищ сприймається як міра суб'єктивних оцінок окремих найбільш досвідчених фахівців, які виконують роль експертів.

Класичне визначення ризику як можливості втрат дає Дж. Хенлі [64]

$$\text{Ризик} = \left\{\frac{\text{Наслідки}}{\text{Час}}\right\}; \text{Частота} = \left\{\frac{\text{Подія}}{\text{Одн. Часу}}\right\}; \text{Величина} = \left\{\frac{\text{Наслідки}}{\text{Подія}}\right\}$$

Ризик є комплексним показником і може бути визначений як міра ймовірності небезпеки й ступеня тяжкості наслідків (шкоди) від порушення безпеки. Отже, ***безпека може визначатися як уявлення про допустимість ризику***. Граничний рівень ризику не має якогось певного кількісного виразу. Межа між безпекою та ризиком не є стійкою й визначається загальними та індивідуальними масштабами оцінювання різних факторів.

Ризик обмежений не тільки фізико-технічними рамками, а й тим, що зі зростанням рівня безпеки витрати на подальше його зниження збільшуються прогресивно. Унаслідок чого з'являються економічні межі, з яких випливає потреба вживати необхідних заходів з підтримання безпечного перевізного процесу шляхом компромісу між прагненням громадськості до максимального рівня безпеки на транспорті та дотриманням економічних інтересів залізниць.

Для ризиків масштабних подій вирішальне значення має розмір втрат. Чим більшими є втрати від аварії чи катастрофи, тим довше вона буде в пам'яті людей і відповідно впливати не на формування загальних настроїв. У цьому сенсі більш резонансною буде одна катастрофа з 10 загиблими за 100 років, ніж загибель однієї людини за 10 років, хоча в обох випадках ризик дорівнює 0,1 фатальних наслідків за рік.

Ризики небезпек для людей можна класифікувати на індивідуальні, колективні та соціальні. Індивідуальний ризик стосується окремої людини, колективний – групи людей (наприклад, пасажири у літаку або поїзді). Соціальний ризик – це найбільш загальна категорія, яка застосовується для оцінювання явища у цілому. Прикладом може бути ризик нещасного випадку при користуванні літаком або поїздом.

Необхідно зазначити, що надане вище визначення ризику через частоту подій та розмір втрат не є вичерпним. Іноді доводиться мати справу з подіями, що не мають визначення у часі. Можливе застосування інших показників, а саме: кількості транспортних подій, віднесених до сумарного обсягу перевезень. Очевидно, що перший та другий показник й потрібно брати за той самий проміжок часу.

Показник частоти подій у визначенні ризику дає змогу при проведенні розрахунків застосовувати ймовірні дані, якщо такі можливо визначити. Якщо у 10 000 поїздках було травмовано 10 пасажирів, то, очевидно, ризик травмування пасажира при користуванні цим засобом транспорту буде R = 10 травмованих / 10 000 поїздок, тобто ризик травмування буде визначатися як один випадок на 1000 поїздок. На відміну від класичної ймовірності результат не є безрозмірним, а вказує на оцінку втрат.

На залізничному транспорті кількісні оцінки ризику базуються на комбінаціях показників частоти подій та її наслідків. RAMS для залізниці [17] встановлює 6 категорій ризиків (табл. 3.1).

Таблиця 3.1

Частоти ризиків небезпек

Категорія	Визначення
Часто	Постійна небезпека
Імовірно	Відбувається багаторазово, можна очікувати часте виникнення небезпеки
Випадково	Може відбуватися неодноразово, очікування небезпеки також неодноразове
Рідко	Іноді трапляється, але небезпеку слід урахувати
Малоймовірно	Виникає дуже рідко, але існування можливе, небезпека у виняткових випадках
Вкрай малоймовірно	Можна вважати, що небезпеки не існує

Можливі наслідки небезпеки для різних рівнів дає змогу оцінити табл. 3.2. Кількість рівнів небезпек та наслідки для кожного рівня повинні бути адаптовані для кожної залізничної галузі (табл. 3.2).

Таблиця 3.2

Рівні небезпек та їх наслідки

Рівень небезпеки	Наслідки для людей та довкілля	Наслідки для роботи залізничної підсистеми
Катастрофіч-ний	Загиблі та/або поранені, та/або значна шкода довкіллю	Зупинка роботи
Критичний	Поодинокі випадки загибелі чи поранення людей, та/або суттєва загроза довкіллю	Суттєві зупинки у роботі
Граничний	Травмовані люди та/або суттєва загроза довкіллю	Затримки у роботі
Незначний	Незначні травмування	Можливі затримки роботи

Якісні категорії ризиків та заходи, що повинні вживатися для них, наведені у табл. 3.3.

Таблиця 3.3

Якісні категорії ризику

Категорія ризику	Заходи
Неприйнятний	Повинен виключатися
Небажаний	Можна застосовувати за відсутності альтернативних, більш безпечних підходів та якщо зниження ризику практично неможливе або економічно недоцільне
Прийнятний	При наявності відповідних заходів
Такий, що можна не брати до уваги	Не потребує впровадження спеціальних обмежувальних та інших заходів

На заключному етапі аналізу розроблено матрицю частоти та наслідків, яка поєднує частоту виникнення ризику та можливі негативні наслідки (табл. 3.4). Вона дає змогу визначити рівень ризику для конкретної транспортної події. У табл. 3.5 наведено приклад оцінювання ризику.

Зазначена матриця фактично поєднує частоту та рівень ризику й дає змогу визначити межі допусків для розробників та дослідників СКС.

Таблиця 3.4

Матриця «Частота – наслідки»

Частота	Рівні ризику			
Часто				
Імовірно				
Рідко				
Малоймовірно				
Практично неймовірно				
	Незначний	Граничний	Критичний	Катастрофічний
	Рівні небезпеки			

Таблиця 3.5

Приклад оцінювання ризику

Частота	Рівні ризику			
Часто	Небажано	Неприйнятно	Неприйнятно	Неприйнятно
Імовірно	Прийнятно	Небажано	Неприйнятно	Неприйнятно
Рідко	Зневажливо	Прийнятно	Небажано	Небажано
Малоймо-вірно	Зневажливо	Зневажливо	Прийнятно	Прийнятно
Практично неймовірно	Зневажливо	Зневажливо	Зневажливо	Зневажливо
	Незначний	Граничний	Критичний	Катастрофіч-ний
	Рівні небезпеки			

Наведені вище таблиці дають змогу здійснити ранжування небезпек та оцінити їх використовуючи метод експертних оцінок при недостатній кількості статистичних даних.

3.2. Методи дослідження ризиків на основі аналізу причин та наслідків порушень

Діаграма причин-наслідків уперше була запропонована в Данії лабораторією RISO [1–5], де було складено діаграму з вибору критичної події, тобто події, яка запускає ланцюгову реакцію аварійної ситуації. Власне процедура починається з першої (ініціювальної) події, за якою йдуть інші. Після цього необхідно відповісти на запитання: «За яких умов подія, що розглядається, може бути причиною появи інших подій?». По суті це розгляд умов для так званої «ланцюгової реакції небезпеки». Наприклад, виникнення пожежі в окремому приміщенні може бути локалізовано або вона може поширитися і знищити всю споруду тощо.

Подальшим розвитком аналізу відмов та наслідків є вивчення небезпек і працездатності. Фактично це є розширений варіант попереднього методу з включенням показників працездатності. Автором методу є Робінсон, який уперше описав ці прийоми для фірми «Кемікл індастріз». Ця методика за

прийнятою в ній термінологією ймовірно належить до стадії «Вивчення небезпек» і відповідає етапу «Вивчення ризику» та виконується за допомогою дерева відмов.

Визнання множинності причин транспортних пригод призводить до того, що на практиці під час розслідування причин пригод визначити будь-яку основну причину, що належить до тієї чи іншої галузі залізничного господарства, у більшості випадків принципово неможливо й неплідно [2].

У роботі [17] запропоновано підхід до оцінювання безпечності перевезень та ризиків втрат, оснований на керівних вказівках з аналізу технологічних ризиків, які розроблені Технічним комітетом № 56 «Надійність» Міжнародної електротехнічної комісії (МЕК). Мета цієї методики – кількісно визначити вірогідність переходу процесу руху за розрахунковий інтервал часу в одне з можливих нештатних небезпечних станів та можливі втрати. Розв'язання поставлених задач виконується через частотний аналіз нештатних небезпечних станів, який у свою чергу застосовує такі три підходи:

– використання та оброблення статистичних початкових даних;

– розрахунок частоти подій за допомогою методів аналізу дерев подій або відмов (згідно з стандартом МЕК 1025);

– застосування експертних оцінок.

Показник безпечності процесу руху визначається через показники безпечності: технічних засобів, дій технічного персоналу й зовнішнього середовища. Методика має теоретичний характер, у ній не обумовлено процедуру, що дає змогу наявні дані статистичного обліку щодо порушень безпеки привести до частотних характеристик відмов за групами. Не показано також принципи використання цієї методики в керуванні безпекою.

Загальний методологічний підхід до вдосконалення системи обліку та аналізу даних про транспортні пригоди, прийнятий у комітеті з безпеки перевезень США [5], базується на таких основних положеннях:

– кожна подія – це дефект у роботі транспортної системи;

– завдяки правильному аналізу кожної події можна знайти шлях усунення цього дефекту;

– необхідно знати не тільки, що відбувалося під час порушення, але й чому це сталося, і що можна зробити для того, щоб унеможливити повторення такого випадку;

– події розглядаються не як ізольовані випадки: аналіз відображає постійний пошук зв'язків та тенденцій у їх настанні.

Для здійснення такого пошуку необхідно мати уявлення не тільки про специфічні обставини кожної події, а й про загальні закономірності, що діють у розглянутій галузі транспорту.

Крім того, дослідження рівня безпечності залізничної техніки слід проводити відносно кожного типу технічних засобів декількома інстанціями незалежно: виробником, користувачем і, якщо можливо, міжвідомчими експертами.

Для реалізації кількісних підходів до оцінювання безпеки велике значення має моделювання аварійних ситуацій. Водночас обсяг та форма емпіричної інформації мають забезпечувати вивчення причин виникнення аварійних ситуацій, характер розвитку в часі та інших обставин, здатних вплинути на безпеку, тобто можливість фіксування й аналізу причинно-наслідкових зв'язків між різними факторами аварійності. Отже, необхідне використання великого обсягу статистичної інформації (баз даних), яка може бути основою для проведення ймовірнісних оцінювань інформації, що характеризує стан безпеки, та аналізу потенційних ризиків.

Використання кількісного аналізу та ймовірнісних оцінювань статистичних даних потребує розроблення науково обґрунтованих методів і є предметом спеціальних досліджень.

Зважаючи на широту й досить високу складність аналізованої проблеми останнім часом під час аналізу факторів, пов'язаних з порушеннями безпеки, дедалі більше набувають поширення сучасні методи, що базуються на спеціальній методології та широкому використанні теорії інформації та математичної логіки. Це стосується методів аналізу дерев відмов/подій та аналізу наслідків відмов. В основі цих методів лежить логіко-аналітичний метод установлення причинно-наслідкових зв'язків між окремими подіями й можливими станами залізничної транспортної системи.

Загальною основою для вирішення завдань такої високої складності є різні аналітичні та імітаційні методи, методи аналізу

систем, системотехніки, дослідження операцій та ін. Серед кількісних аналітичних груп методів найпоширенішими є різні матричні методи.

Існує також ряд додаткових вимог, без урахування яких неможливе ефективне використання інформації, що характеризує стан безпеки:

– забезпечення повноти та достовірності масиву початкових даних;

– оперативність оброблення інформації;

– отримання інформації в систематизованому вигляді, зручному для керівної роботи;

– адекватна поставленим цілям систематизація початкових даних про порушення безпеки руху – це необхідний етап аналізу, який дає змогу провести розрахунки щодо кількісного оцінювання рівня безпеки та вироблення керівних заходів.

Складність цієї проблеми передбачає використання спеціалізованих автоматизованих систем збирання, оброблення, зберігання та аналізу інформації про події, які характеризують рівень безпеки на залізницях.

Проведення системного аналізу, створення автоматизованої системи обліку та оброблення статистичної інформації про порушення безпеки та проведення на цій основі цілеспрямованих заходів щодо зниження аварійності дало змогу різко скоротити кількість сходжень рухомого складу з рейок та зіткнень, що припадають на 1 млн поїзд.км на залізницях Німеччини у 80-х роках.

Законодавство більшості країн Європейської Співдружності потребує проведення аналізу ризиків упровадження об’єктів з підвищеною небезпекою. Насамперед його потребують підприємства хімічної та ядерної промисловості, швидкісний транспорт та ін. Такий аналіз може виконуватися й на стадії використання систем, особливо за наявності «нештатних» ситуацій. Ці заходи спрямовані на задоволення потреб держави та населення у безпеці й можуть сприяти зменшенню рівня ризиків. Однак останнє можливо за умови, якщо такий аналіз здійснюється для зменшення аварійності, а не для зняття персональної відповідальності окремих робітників за негативні наслідки небезпечних подій.

Процедура аналізу містить три основні етапи:
- ***попередній аналіз небезпек;***
- ***установлення послідовності небезпечних подій;***
- ***аналіз їх наслідків.***

Порівняльна характеристика методів аналізу ризиків наведена у табл. 3.6.

Таблиця 3.6

Методи аналізу ризиків

Метод	Характеристика	Переваги	Недоліки
1	2	3	4
Попередній аналіз небезпек	Призначений для виявлення небезпек та елементів системи для подальшого аналізу відмов та наслідків	Дає змогу формалізувати уявлення про можливі небезпеки та визначити елементи системи, що пошкоджуються	Може застосовуватися тільки на етапі попереднього розгляду
Аналіз наслідків відмов за їх видами	Розглядає всі можливі відмови елементів апаратури та для кожної встановлює можливі наслідки під час роботи системи в цілому й елемента окремо	Достатньо простий, процедура регламентована, не потребує математичного апарату	Не враховує дію людського фактора у відмовах техніки. Не враховує взаємну дію відмов. Потребує значних витрат часу
Аналіз критичності	Визначає й класифікує елементи системи за ступенем їх впливу на кінцевий результат функціювання системи	Достатньо простий, процедура регламентована, не потребує особливого математичного апарату	Часто не враховує відмови із загальної причини, ергономіку та взаємодію окремих компонентів системи між собою

Продовження табл. 3.6

1	2	3	4
Дерева подій	На підставі базової дії визначаються й оцінюються альтернативні послідовності розвитку подій у системі	Дає змогу визначити послідовність реалізації результатів відмов та альтернативні шляхи їх розвитку	Не може бути застосований у разі паралельної послідовності подій, відсутня деталізація
Аналіз небезпек та працездатності	Розширений вид, аналіз причин та наслідків за умови зміни окремих параметрів	Ефективний для підприємств, що мають багато параметрів, які змінюються у часі	Недостатньо формалізований та описаний у літературі

На жаль, їх застосування на залізничному транспорті перебуває в початковій стадії. Проводячи попередній аналіз, спочатку виявляють джерела небезпеки (відповідальні функції системи, процеси, види діяльності, технології тощо). Надалі визначаються підсистеми (частки системи), пристрої, окремі вузли та їхні елементи, які можуть бути причиною нештатної небезпечної ситуації.

Засобами досягнення розуміння ступеня небезпеки є інженерний аналіз системи, розгляд впливів зовнішнього та внутрішнього середовища, технологічних процесів роботи підприємства й самого обладнання. Особливої уваги варті події з великими масштабами втрат навіть за умови дуже малої ймовірності їх появи.

У такому випадку, виконуючи аналіз, застосовують класифікацію небезпек. Наприклад, у аерокосмічній промисловості використовують чотири класи небезпек, які розділяють за тяжкістю наслідків. У табл. 3.7 наведено форму запису результатів попереднього аналізу небезпек (ПАН) та зовнішній вигляд дерева рішень (рис. 3.1).

Таблиця 3.7

Форма запису результатів ПАН

Підсистема (операція)	Ситуація	Небезпечний елемент	Небезпечний стан	Умови появи небезпечного стану	Подія, що ініціює небезпеку	Характеристика потенційної небезпечної події	Наслідки	Клас небезпеки	Заходи щодо запобігання небезпекам	Попередня оцінка
1	2	3	4	5	6	7	8	9	10	11

Рис. 3.1. Дерево рішень для ПАН

На другій стадії встановлюють послідовність небезпечних ситуацій за допомогою дерев відмов та подій. Перелік основних завдань, що вирішуються на цьому етапі, наведено на рис. 3.2.

На кінцевій стадії дослідження ризиків проводять аналіз наслідків та оцінюють їх вплив на техніку, людей та довкілля. Як правило, результати надаються у вигляді гістограм частот небезпечних подій. Ця гістограма є не що інше, як крива Фармера, яка є основою для моделі послідовного розвитку небезпечної події.

До інших видів можна віднести аналіз видів та наслідків (АВН). На основі послідовного розгляду всіх елементів системи аналізують їх можливі відмови, встановлюють аварійні ситуації та їх результуючу дію на роботу системи.

Рис. 3.2. Завдання, що вирішуються на стадії виявлення небезпечних послідовностей нештатних ситуацій

Основним завданням є встановлення впливу відмови одного елемента на інші відповідно до вимог документа IEE 279./97/.IOCFP50.

На відміну від дерева відмов ця процедура є детальнішою, вона охоплює всі види пошкоджень, які властиві конкретному елементу. Після аналізу складається перелік необхідних перевірок, які слід виконати під час перевіряння.

Результуючим документом є карта перевірки, можлива форма якої надана у табл. 3.8.

Таблиця 3.8

Результати аналізу видів пошкоджень та їх наслідків

Назва блока чи елемента системи	Вид відмови	Причина відмови	Ознаки відмови	Наслідки відмови, включно із залежними відмовами	Метод розпізнання	Методи локалізації відмов	Результат дії на систему

Форма подання таблиці є довільною, у разі потреби можна вводити дані щодо ймовірності відмов.

Розвитком описаного вище методу є аналіз критичності. У його основі лежить схема класифікації за класами та категоріями. У [17] наведено схему класифікації з чотирма градаціями:

клас 1 – ефекти, якими можна знехтувати,

клас 2 – граничні ефекти,

клас 3 – критичні ситуації,

клас 4 – катастрофічні наслідки.

Товариство автотранспортних інженерів (SAE) також пропонує чотири категорії (методика, яку рекомендовано для аерокосмічної техніки (ARD-926)):

– категорія 1 – відмова, що потенційно призводить до жертв;

– категорія 2 – відмова, що потенційно призводить до невиконання основного завдання;

– категорія 3 – відмова, що призводить до затримань у роботі або втрати працездатності;

– категорія 4 – відмова, що призводить до додаткового незапланованого обслуговування.

Елементи можна класифікувати на основі коефіцієнта критичності Cr

$$C_r = \sum_{i=1}^{N} \beta \, \alpha \, K_E \, K_D \, \lambda_G \, t \cdot 10^6, \; n = 1,2,\ldots,N,$$

де Cr – коефіцієнт критичності у втратах на мільйон спроб;

n – кількість критичних відмов;

N – сумарна кількість відмов, які відповідають конкретному виду втрат;

λ_G – частота відмов;

K_D – коефіцієнт, що враховує різницю між розрахунковим та фактичним навантаженням елемента;

K_E – коефіцієнт, що враховує різницю між умовами роботи елемента під час заміни та очікуваними умовами експлуатації;

α – коефіцієнт, що враховує частку цієї відмови в критичному стані системи;

β – умовна ймовірність появи наслідків критичної відмови;

t – час роботи системи в процесі виконування заданої функції.

Розглянутий метод не дає повного уявлення про кількісну оцінку масштабів втрат. Його головним завданням є поліпшення

якості системи й зменшення можливих негативних наслідків у результаті пошкоджень. Окремі фахівці обмежуються дослідженням небезпек та працездатності системи.

3.3. Застосування принципів ризик-менеджменту впродовж життєвого циклу спеціалізованих комп'ютерних систем

Більшість досліджень у галузі управління ризиками підприємств залізничного транспорту розглядають різні аспекти оцінювання ризиків небажаних подій у транспортних процесах, що безпосередньо пов'язані з управлінням ризиками та спрямовані на побудову корпоративних систем управління ризиком на практиці. Але, з іншого боку, замало досліджень проводиться в напрямку посилення контролю над незапланованими матеріальними і фінансовими витратами при експлуатації обладнання, а також зниження збитку від виходу його з ладу. У цьому сенсі управління ризиками потрібно розглядати як логічний і систематичний процес, який можна застосовувати для вибору методів подальшого вдосконалення діяльності не підприємств, а підвищення ефективності функціонування систем керування в процесі експлуатації і ТО та Р та має на увазі ретельний аналіз умов для прийняття рішень.

На стадії аналізу безпеки функціонування СКС передбачається можливість виникнення відмов, тому доцільно проведення аналізу ризику, тобто наскільки часто відбуваються порушення елементів системи через порушення в роботі системи керування та іншого пов'язаного з ним устаткування, а також помилок людини-оператора.

Згідно з EN 50126 усі залізничні системи протягом життєвого циклу зазнають різноманітних ризиків, аналіз яких має такі цілі:

– ідентифікація загроз, які пов'язані із системою;
– ідентифікація подій, які викликають ці загрози;
– визначення ризику, пов'язаного із загрозами;
– розробка процесу безперервного управління ризиком.

Вимоги аналізу ризиків полягають у такому:

– систематичний пошук і класифікація всіх ризиків, можливих за нормальних умов;

– ідентифікація прихованих загроз;

– виявлення частоти виникнення подій, пов'язаних з наявними загрозами;

– виявлення / оцінювання розміру впливів наявних загроз;

– виявлення ризику для системи, пов'язаного з кожною загрозою;

– визначення та класифікація допустимості ризиків, що відповідають кожній відомій загрозі її виникнення;

– розробка протоколу загроз як базису для управління ризиком.

Будь-яка ІКС має визначені стадії життєвого циклу від розробки до утилізації, тому на кожному етапі можливо застосовувати різні методи оцінювання. Розділимо цей період на декілька стадій, які наведемо нижче.

Перша стадія роботи (стадія 1) має на меті визначення самої системи і виявлення в загальних рисах потенційних небезпек, тобто:

– виявити джерела небезпеки;

– визначити частини системи, які можуть викликати ці небезпечні стани;

– ввести обмеження на аналіз, властиві саме цій системі.

Нерідко стадія 1 включає не тільки попереднє виявлення елементів системи, а ще й подій, які спричиняють виникнення небезпечних ситуацій. Якщо завдання аналізу розширюються з використанням більш формалізованих (кількісних) прийомів, зокрема з включенням до розгляду послідовності подій, що перетворюють небезпеку в подію (у нашому випадку – транспортну подію), то проводиться більш точна процедура попереднього аналізу небезпек (ПАН) яка є першою спробою виявити обладнання (елементи) технічної системи й окремі події, які можуть спричинити виникнення небезпеки. Можливі рішення можна подати як дерево рішень. Цей аналіз доцільно проводити на початковому етапі розробки системи, де можливо намітити запобіжні заходи, щоб виключити або знизити ці небезпеки.

Другою стадією (стадія 2) є виявлення послідовності небезпечних ситуацій з використанням для оцінювання

ймовірності таких аналітичних методів прогнозування, як дерево подій та дерево відмов ця стадія починається після того, як вибрано обладнання та визначено конфігурацію системи.

Дерево рішень, як різновид дерева подій, можливо застосовувати тоді, коли всі можливі стани системи виражаються через стани елементів, тобто їхні стани взаємно ув'язані, і їх вірогідність у сумі дорівнює 1 і якщо відмови всіх елементів незалежні або якщо є елементи з кількома можливими станами і є односторонні залежності.

Третя стадія (стадія 3) – аналіз наслідків, один із прийомів аналізу рішень – аналіз видів відмов і наслідків (АВВН): на основі послідовного розгляду одного елемента за одним аналізуються всі можливі види відмови чи аварійні ситуації та вдається виявити їх результуючий вплив на систему.

Окремі аварійні ситуації і види відмов елементів проявляються й аналізуються для того, щоб визначити їх вплив на інші сусідні елементи і системи в цілому.

Далі надамо короткий перелік та характеристики можливих видів проведення аналізу, які також доцільно використовувати на етапі експлуатації й технічного обслуговування та ремонту ІКС.

Аналіз критичності – вивчення небезпек і працездатності – розширений варіант АВВН за рахунок включення в аналіз показників працездатності на додаток до розгляду різних видів відмов обладнання.

Аналіз причин – наслідків – вибір ініціювальної події, за якою йдуть інші події і знаходяться відповіді на такі питання:

– за яких умов ця подія приводить до розвитку подальших подій;

– на які інші елементи діє ця подія;

– яку наступну подію викликає ця подія.

Доцільно використовувати комбіновані методи дерева відмов (виявити причини) і дерева подій (показати наслідки), причому всі явища розглядаються в природній послідовності їх появи.

Усі відмови ІКС так чи інакше пов’язані з людською діяльністю: помилки оператора, дефекти конструкції, помилки при технічному обслуговуванні; або які стосуються обладнання: неправильні сигнали відповідальних елементів; фізичний знос і

старіння. Також впливають події, пов'язані з довкіллям: повені, урагани, зсуви тощо.

Небезпеки в системах досить часто викликаються поєднанням відразу кількох типів відмов, тобто відмовами обладнання плюс помилка людини і (або) стихійного лиха [30, 43].

Згідно зі стандартами IEC/ISO 31010:2009, IDT та ДСТУ IEC/ISO 31010:2013 Risk management — Risk assessment techniques (Керування ризиком. Методи загального оцінювання ризику) визначено, що процес управління ризиком допомагає приймати рішення з урахуванням невизначеності та можливості настання майбутніх подій чи обставин (навмисних або ненавмисних) і їхніх впливів на узгоджені цілі.

Управління ризиком передбачає застосування логічних і систематичних методів:

– щодо обміну інформацією та консультування протягом цього процесу;

– установлення оточення для ідентифікації, аналізування, оцінювання, обробки ризику, пов'язаного з будь-якими діяльністю, процесом, функціонуванням та ін.;

– моніторингу та критичного аналізу ризиків;

– належного звітування про результати та їх протоколювання.

Загальне оцінювання ризику – це та частина управління ризиком, яка дає можливість мати структурований процес, у ході якого визначають, що може вплинути на досягнення цілей, а також аналізують ризик стосовно наслідків та їхніх імовірностей.

Під час загального оцінювання ризику намагаються відповісти на такі запитання:

– що може трапитися й чому (через ідентифікування ризику);

– якими можуть бути наслідки;

– якою є ймовірність виникнення їх у майбутньому;

– чи є якісь фактори, що пом'якшують наслідок ризику або знижують імовірність ризику;

– чи є рівень ризику допустимим або прийнятним і чи треба буде його обробляти у подальшому.

Організація ризик-менеджменту являє собою систему заходів, спрямованих на раціональне поєднання всіх його елементів у єдиній технології процесу управління ризиком.

Як система управління ризик-менеджмент містить у собі: процес вироблення мети ризику, визначення ймовірності настання події, виявлення ступеня і величини ризику, аналіз довкілля, вибір стратегії управління ризиком і необхідних для цієї стратегії прийомів управління ризиком, здійснення цілеспрямованого впливу на ризик. Зазначені процеси в сукупності становлять етапи організації ризик-менеджменту, що подані на рис. 3.3.

Рис. 3.3. Процедури ризик-менеджменту

Для визначення цих етапів насамперед необхідна оцінка ступеня ризику, тобто кількісний аналіз, що передбачає числове визначення окремих ризиків і ризику управлінського рішення в цілому. Для цього визначаються числові значення ймовірності настання ризикових подій та їх наслідків, здійснюється кількісна оцінка ступеня ризику, визначається допустимий у цій конкретній обстановці рівень ризику.

Отже, основною функцією ризик-менеджменту є забезпечення прийняття скоригованих на ризик управлінських рішень і створення умов для їх успішної реалізації.

Усіма наявними ІКС залізничної автоматики безпосередньо управляє людина, тому є можливість помилкових дій операторів, які можуть призвести до негативних наслідків різного ступеня тяжкості.

Загальний підхід, описаний у стандартах та джерелах [35, 38, 59, 60], відображає принципи та заходи для управління будь-якою формою ризиків систематичним і прозорим способом для будь-якої галузі і будь-якої сфери застосування. Ці стандарти можуть застосовуватись протягом усього життєвого циклу організації або системи. Отже, необхідно використати й адаптувати вимоги та підходи цих стандартів для застосування в подальшій роботі з удосконалення методів та моделей експлуатації технічних засобів керування рухом поїздів та оперативного визначення технічного стану пристроїв залізничної автоматики.

Для цього встановимо основну умову, що ключові вимоги стандартів адаптуються для вдосконалення ІКС керування рухом поїздів, а саме технологій експлуатації й технічного обслуговування та ремонту.

Класичне формулювання поняття ***«Ризик» – це можлива небезпека будь-якого несприятливого результату, можливість того, що все відбуватиметься не так, як очікується, можливість припуститися помилки.***

Ризик-менеджмент, управління ризиками – процес прийняття і виконання управлінських рішень, спрямованих на зниження ймовірності виникнення несприятливого результату і мінімізацію можливих втрат, спричинених його реалізацією.

Оцінювання ризику – це аналіз причин його виникнення і масштабів прояву в конкретній ситуації. У міжнародній практиці поширеним підходом до оцінювання професійних ризиків є так звана «п’ятикрокова система» [17].

Після адаптації вищезазначеної системи ці етапи можливо викласти так:

1. Ідентифікація небезпек, що призводять до ризику – потенційно можливі місця заподіяння шкоди та визначення персоналу, що задіяний у цьому процесі;

2. Оцінювання та «ранжирування» ризиків (їх серйозність, їх імовірність та ін.), розподіл за важливістю;

3. Визначення превентивних заходів – ідентифікація заходів для виключення ризиків та управління ними;

4. Вживання заходів – складання плану (процедури) реалізації захисних та превентивних заходів;

5. Моніторинг та перевірка – оцінка, яка проводиться на регулярній основі з оформленням результатів, що будуть застосовані при модернізації системи, змінах технології керування, технології обслуговування й ремонту та ін.

Структурна схема процесу ризик-менеджменту (рис. 3.4) ілюструє процес загального оцінювання процедур ризик-менеджменту.

Основною метою оцінювання ризику є подання на основі об’єктивних свідчень інформації, необхідної для прийняття обґрунтованого рішення щодо способів обробки ризику.

Оцінка ризику забезпечує:

– розуміння потенційних небезпек і впливу їх наслідків на досягнення встановлених цілей;

– отримання інформації, необхідної для прийняття рішень;

– розуміння небезпеки і її джерел;

– ідентифікацію ключових факторів, що формують ризик, вразливих місць організації та її систем;

– можливість порівняння ризику з ризиком альтернативних технологій, методів і процесів;

– обмін інформацією про ризик і невизначеності;

– інформацію, необхідну для ранжирування ризику.

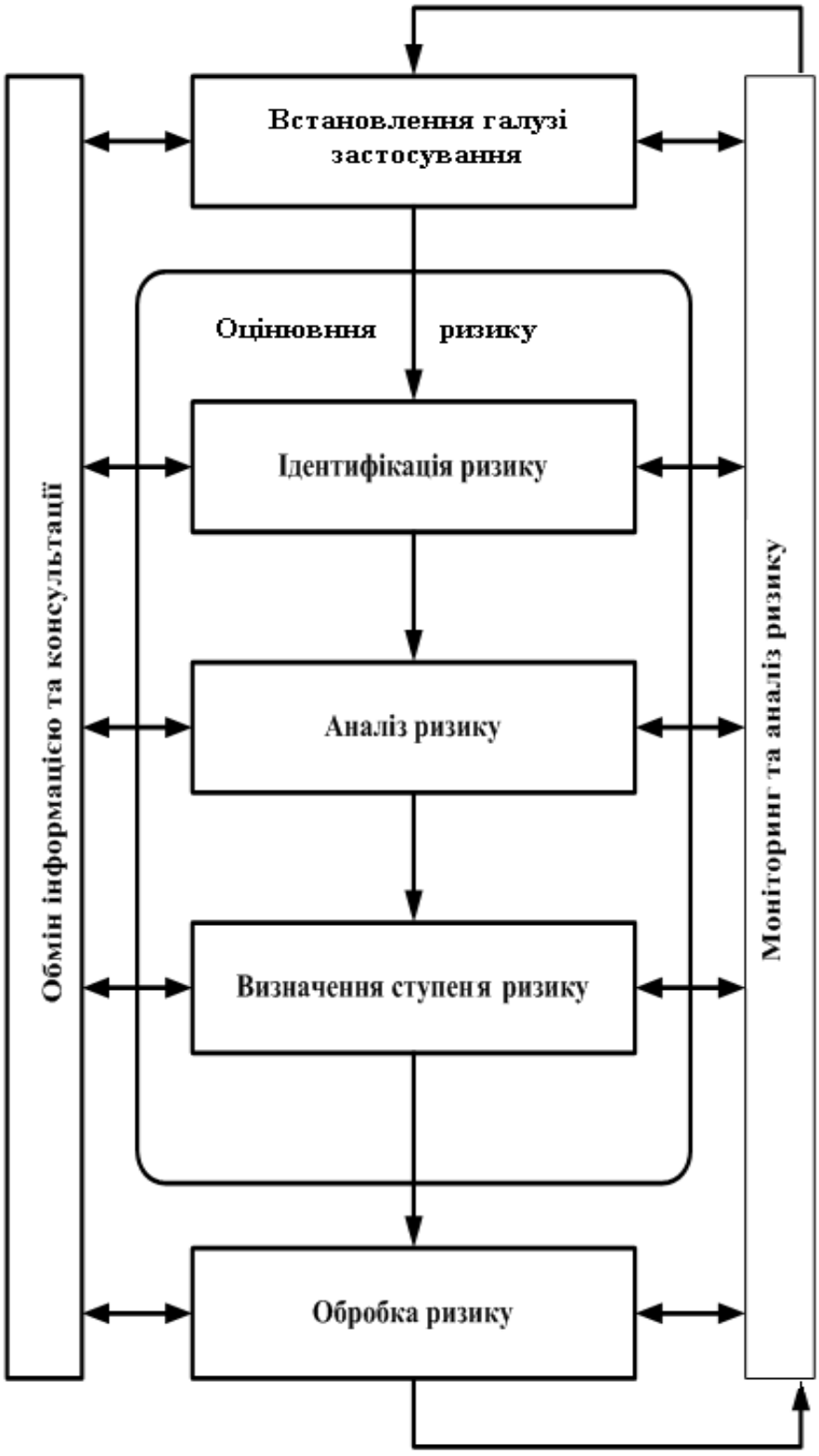


Рис. 3.4. Структурна схема процесу загального оцінювання ризиків процедур ризик-менеджменту

Оцінювання ризику – це процес, що поєднує ідентифікацію, аналіз і порівняльну оцінку ризику для всієї системи, окремих її компонентів або конкретної небезпечної події. Тому в різних

ситуаціях можуть бути застосовані різні методи оцінювання. Оцінка ризику забезпечує розуміння можливих небезпечних подій, їх причин та наслідків, імовірності їх виникнення та прийняття рішень:

– про необхідність робити відповідні дії;

– способи максимальної реалізації всіх можливостей зниження ризику;

– необхідність обробки ризику;

– вибір між різними видами ризику;

– пріоритетність дій з обробки ризику;

– вибір стратегії обробки ризику, що дає змогу знизити ризик до прийнятного рівня.

Після завершення оцінювання ризику приймається і виконується одне або декілька рішень про обробку ризику, що дають змогу змінити ймовірність виникнення небезпечної події та/або її вплив. Обробка ризику зазвичай є адаптивним процесом перевірки ризику на його прийнятність і відповідність раніше встановленим критеріям для визначення необхідності подальшої обробки ризику.

Моніторинг та аналіз ризику є складовою частиною процесу ризик-менеджменту. Вони спрямовані на перевірку:

– достовірності припущень про ризик;

– достовірності припущень, на яких основана оцінка ризику, включно із зовнішніми та внутрішніми сферами застосування;

– досяжності очікуваних результатів;

– відповідності результатів оцінювання ризику фактичній інформації про ризик;

– правильності застосування методів оцінювання ризику;

– ефективності обробки ризику.

Процеси моніторингу та аналізу ризику мають бути задокументовані, а результати моніторингу та аналізу ризику – зафіксовані у відповідних звітах.

Для різних стадій життєвого циклу встановлені різні вимоги і застосовні різні методи оцінювання ризику і зазвичай їх багаторазово використовують із різними рівнями деталізації на кожній стадії для прийняття рішень.

Одним із найважливіших етапів процесу управління ризиками при розробці та проектуванні ІКС є створення

концепції управління де визначаються ризики та готується детальний опис загроз і ризиків. На цьому етапі життєвого циклу можливо виділити дві категорії ризиків:

– апаратні ризики – ризики, пов'язані з використанням нового апаратного забезпечення або доопрацюванням вже наявного для підвищення продуктивності або досягнення принципово нової функціональності;

– програмні ризики – ризики, пов'язані з придбанням або використанням складного програмного забезпечення або систем, розроблених за індивідуальним замовленням.

На цьому етапі якість програмного коду має великий вплив на якість проектованої системи на всіх наступних етапах життєвого циклу, що є причиною появи певних небезпек (ризиків), які можуть перейти в серйозні відхилення або невідповідності. Сучасні методики оцінювання ризиків не дають змогу у повному обсязі виявити і належно оцінити їх під час проектування, розроблення, впровадження та експлуатації СКС [32].

На сьогоднішній день існує достатня кількість методів оцінювання ризику, які можливо використовувати для дослідження в предметній галузі з урахуванням різних етапів життєвого циклу системи.

На стадії розробки та проектування можливо використовувати: метод попереднього аналізу небезпек (PHA) (Preliminary Hazard Analysis); аналіз видів і наслідків відмов та аналіз видів, наслідків та критичності відмов (FMEA – Failure Mode Effect Analysis); аналіз дерева несправностей (FTA); аналіз дерева рішень; аналіз прихованих дефектів і аналіз паразитних кіл (SA – Sneak Analysis).

У процесі постійної експлуатації доцільно використовувати: дослідження HAZOP – дослідження небезпеки і працездатності (Hazard and Operability Study); метод SWIFT (Structured what-if technique); аналіз видів і наслідків відмов та аналіз видів, наслідків та критичності відмов (FMEA – Failure Mode Effect Analysis); аналіз дерева несправностей (FTA) – Fault Tree Analysis; аналіз дерева подій (ETA) – Event Tree Analysis; метод «Аналіз причин і наслідків»; причинно-наслідковий аналіз (діаграма Ісікави); метод LOPA – Layers of Protection Analysis;

аналіз впливу людського фактора (HRA) – Human Reliability Assessment; аналіз «краватка-метелик»; технічне обслуговування, спрямоване на забезпечення надійності (RCM); «марківський аналіз».

Висновки до третього розділу та практичні завдання

1. Ризик – це можлива небезпека будь-якого несприятливого результату, можливість того, що все відбуватиметься не так, як очікується, можливість припуститися помилки.

2. Ризик-менеджмент, управління ризиками – процес прийняття і виконання управлінських рішень, спрямованих на зниження ймовірності виникнення несприятливого результату і мінімізацію можливих втрат, спричинених його реалізацією.

3. Основною функцією ризик-менеджменту є забезпечення прийняття скоригованих на ризик управлінських рішень і створення умов для їх успішної реалізації.

4. Етапи оцінювання ризику:

- ідентифікація небезпек, що призводять до ризику, – потенційно можливі місця заподіяння шкоди та визначення персоналу, що задіяний у цьому процесі;
- оцінювання та ранжирування ризиків (їх серйозність, їх імовірність та ін.), розподіл за важливістю;
- визначення превентивних заходів – ідентифікація заходів для виключення ризиків та управління ними;
- вживання заходів – складання плану (процедури) реалізації захисних та превентивних заходів;
- моніторинг та перевірка – оцінювання, що проводиться на регулярній основі, з оформленням результатів, що будуть застосовані при модернізації системи, змінах технології керування, технології обслуговування й ремонту та ін.

5. Оцінювання ризику забезпечує:

– розуміння потенційних небезпек і впливу їх наслідків на досягнення встановлених цілей;

– отримання інформації, необхідної для прийняття рішень;

– розуміння небезпеки і її джерел;

– ідентифікацію ключових факторів, за якими вираховують ризики, вразливі місця організації та її систем;

– можливість порівняння ризику з ризиком альтернативних технологій, методів і процесів;

– обмін інформацією про ризик і невизначеності;

– інформацію, необхідну для ранжирування ризику.

Практичні заняття

Мета: набуття практичних навичок щодо визначення, аналізу та формування оцінок ризиків небезпек, закріплення теоретичних знань, отриманих при вивченні розд. 3.

Завдання

1. Розрахуйте ризики окремих небезпечних подій, обраних самостійно або сформульованих викладачем.

2. Сформулюйте концепцію ризик-менеджменту для обраної системи керування протягом життєвого циклу.

3. Для обраної схеми об’єкта керування проведіть аналіз причин та наслідків відмов. Результати дослідження занесіть у табл. 3.8.

4. Заповніть табл. 3.7, використовуючи результати табл. 3.8.

5. Проаналізуйте рівень ризиків для обраних систем керування на залізничному транспорті.

Ситуації для проведення дискусій та обговорення

1. Функціонування об’єкта пов’язане зі значним ризиком. Які фактори необхідно враховувати при розробленні заходів зі зменшення ризику?

2. Як ви розумієте термін «приймальний рівень ризику»?

3. Проаналізуйте ризики небезпек для власного здоров’я протягом цього року, які види вашої діяльності є найбільш ризикованими?

4. Які базові категорії ризик-менеджменту?

Контрольні питання для самостійної роботи до розд. 3

1. Визначте ризик травмування пасажирів, якщо з 1000 поїздок за рік двоє пасажирів отримали ушкодження.

2. Що означає масштаб втрат?

3. Що таке приймальний рівень ризику?

4. За сучасними уявленнями безпека – це... (дайте визначення через ризик).

5. Які відмінності наслідків катастрофічного та граничного рівня ризиків?

6. Для чого проводиться аналіз причин та наслідків порушень?

7. Для чого проводиться аналіз критичності?

8. Які базові категорії ризик-менеджменту?

9. Якими величинами безпечності оперують СКС?

10. Якими величинами характеризується ризик?

11. Яка розмірність ризиків?

4. МОДЕЛЮВАННЯ ВІДМОВ ТА ОЦІНЮВАННЯ НЕБЕЗПЕКИ

4.1. Побудова дерев подій та відмов

Діаграма причин-наслідків уперше була запропонована в Данії лабораторією RISO [9]. Складання діаграми з вибору критичної події, тобто події, яка запускає ланцюгову реакцію аварійної ситуації. Власне процедура починається з першої (ініціювальної) події, за якою йдуть інші. Після цього необхідно відповісти на запитання: «За яких умов подія, що розглядається, може бути причиною появи інших подій?». По суті це розгляд умов для так званої «ланцюгової реакції небезпеки». Наприклад виникнення пожежі в окремому приміщенні може бути локалізовано або пожежа може поширитися і спричинити знищення всієї споруди тощо.

На відміну від дерева відмов дерево подій (рис. 4.1) розглядає можливі варіанти розвитку подій при виникненні початкового пошкодження. На кожному етапі аналізу розглядаються тільки два можливих результати його розвитку: «успіх» або «відмова» з відповідними значеннями ймовірностей для кожного випадку.

З погляду на зовнішній вигляд конструкція, що зображена на рис. 4.1, нагадує дерево з гілками. Одна з них іде нагору, інша донизу й вони символізують напрям розвитку подій A, B, C, D по горизонталі. Наприклад, подія спрацювання схеми захисту це – «успіх» і, навпаки, її не спрацювання або пошкодження розуміється як відмова. Залежно від комбінацій результатів реалізації подій A–D отримаємо деяку кількість можливих варіантів наслідків, які відбуваються з визначеною ймовірністю. Слід зазначити, що подія A є ініціювального, саме з неї починається реалізація небезпечного сценарію, який може завершитися аварією або іншою небажаною подією.

У результаті аналізу маємо можливі варіанти розвитку ініціювальної події. При наявності числових значень імовірностей успіху або відмови є можливість також і кількісно оцінити визначені варіанти та обрати найбільш імовірний сценарій розвитку подій.

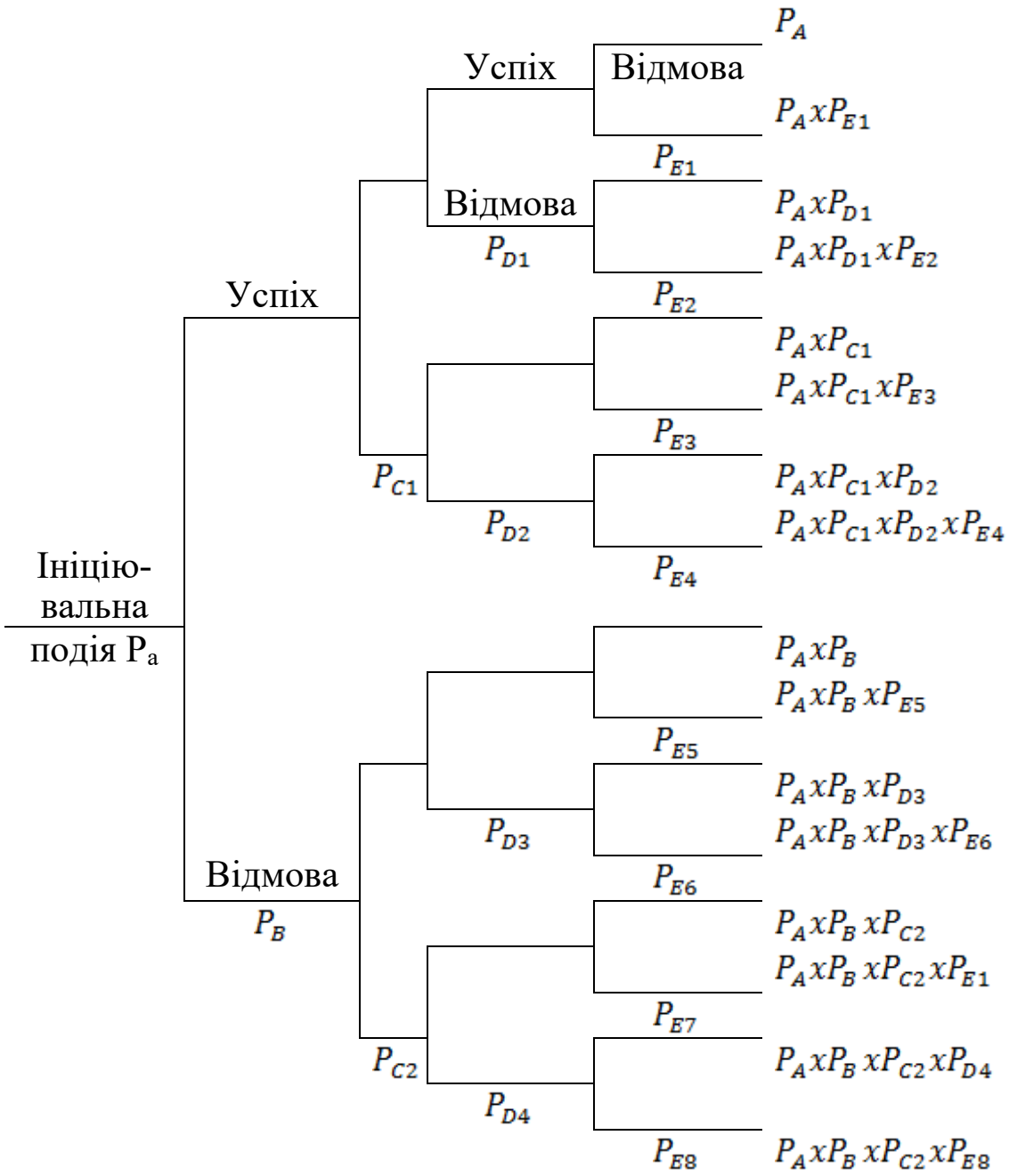


Рис. 4.1. Зовнішній вигляд дерева подій

Метод аналізу за допомогою дерева відмов розробив Х. А. Уотсон на початку 60-х років 20 сторіччя. Він розробив систему керування пуском ракети «Мінітмен» у лабораторії «Белл телефоун». Завдяки працям Хаасля, Лумберта та Фусселя цей метод набув поширення. На думку Фусселя, він забезпечує:

– пошук відмов;

– виявляє саме такі аспекти, які мають значення для відмови;

– високий рівень наочності;

– можливість проведення як якісного, так і кількісного аналізу відмов;

– глибокий детальний аналіз роботи системи.

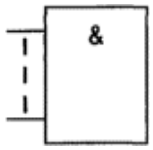
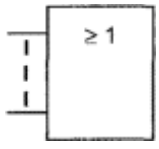
Основні обмеження визначаються бінарною природою подій, а також можливостями булевої логіки з операторами «І», «АБО». Крім цього, суттєве значення для коректності отриманих результатів є вимога незалежності первинних подій.

Також необхідно зробити деякі зауваження що до побудови та аналізу дерев небезпечних подій (відмов). У роботі [45] для логічних конструкцій «І-АБО» та «АБО-І» визначені мінімальні аварійні та мінімальні прохідні сполучення. Вони функціонують таким чином, що при видаленні хоча б однієї первинної події кінцева не може настати. Тобто це в масштабі дерева буде мінімальний збіг небезпечних подій, яких у сукупності мінімально достатньо для появи кінцевої події. Це означає, що непоява хоча б однієї події з базового переліку унеможливлює існування кінцевої події дерева.

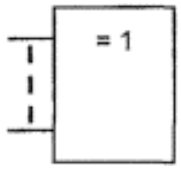
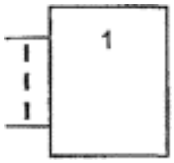
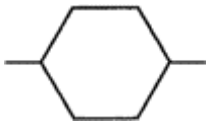
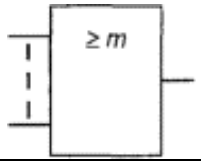
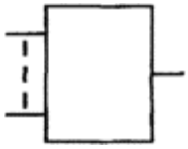
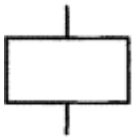
Основні конструкції дерева становлять логічні символи І, АБО, кінцева подія відображає характер пошкодження, а як первинні події приймаються початкові прояви можливого пошкодження, як правило це елементарні події, які не розкладаються на складові (табл. 4.1).

Таблиця 4.1

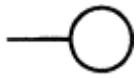
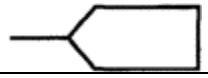
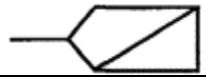
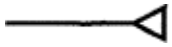
Характеристика символів дерева відмов

Символ IEC	Символ ANSI	Функція	Опис
1	2	3	4
		Клапан «ТА»	Подія відбувається, якщо всі вхідні події відбуваються одночасно
		Клапан «АБО»	Подія відбувається, якщо відбувається будь-яка з вхідних подій (або одна, або в будь-якій комбінації)

Продовження табл. 4.1

1	2	3	4
		Клапан «виключне АБО»	Подія відбувається, якщо відбувається одна з вхідних подій (використовується зазвичай з двома вхідними подіями)
		Клапан «НІ»	Подія являє собою стан, який є інверсією стану певної вхідної події (подія, протилежна вхідній події)
	-	Клапан «ЗАБОРОНА»	Подія відбувається, якщо відбувається вхідна подія, прикладена справа, тоді як подія, вказана всередині символу і яка формує умови, виконується. Якщо умову викликано появою іншої події, клапан «ЗАБОРОНИ» здійснює синхронізацію подій
		Надлишкова структура	Подія відбувається, якщо відбувається щонайменше *m* з *n* вхідних подій
	-	Клапан (загальна форма)	Загальний символ клапана, функція якого вказується всередині символу
	-	Блок опису події	Назва або опис події, код події і ймовірності появи (за необхідності) повинні бути вказані всередині символу

Продовження табл. 4.1

1	2	3	4
	-	Основна подія	Подія, яка не може бути поділена на складові події
	-	Нерозроб-лена подія	Подія, подальша розробка якої не була проведена (зазвичай тому, що це було недоцільним)
	-	Аналізува-ти подію в іншому місці	Подія, яка аналізується в іншому дереві несправностей
	-	Зупинка	Подія, що сталася або станеться обов'язково
	-	Нульова подія	Подія, яка не може відбутися
	-	«Перехід в»	Подія, визначена в іншому місці дерева несправностей
	-	«Перехід з»	Подія, що переходить з іншого місця дерева несправностей

Як видно з наведеної таблиці, крім згаданих вище можуть використовуватися й інші символи, які необхідні для моделювання того чи іншого пошкодження системи.

Далі наведемо процедуру розроблення дерева відмов.

Крок 1. Аналіз роботи об’єкта дослідження.

На самому початку необхідно детально розібратися з тим, як функціонує об’єкт чи система, для яких розробляється дерево. Найкраще для цього процесу підходить структурна схема або електрична принципова схема при нескладних технічних рішеннях. На початку необхідно чітко визначити функції, що виконує кожен блок чи елемент схеми, як він пов'язаний з іншими компонентами. Необхідно проаналізувати шляхи

проходження сигналів керування та контролю в схемі, а також провести аналіз причин та наслідків порушень. Для цього кожному компоненту схеми складають перелік можливих пошкоджень або порушень режимів експлуатації, визначають можливу причину та її наслідки. Фактично це є класична процедура дослідження причин та наслідків порушень, яка була описана раніше.

Крок 2. Визначення кінцевої та початкової подій.

Кінцева подія визначає власне мету дослідження, тому її необхідно формулювати відповідно до можливих станів системи, яка досліджується, з урахуванням термінології відповідних регулюючих документів. Відповідно до держстандартів для систем залізничної автоматики такими подіями можуть бути: катастрофа, аварія, інцидент, транспортна подія, порушення або формування небезпечної несанкціонованої команди.

Після визначення кінцевої події приступають до формування переліку первинних подій. Фактично це первинні причини можливості існування кінцевої події. Ця процедура досить складна і відповідальна, тому потребує чіткого уявлення про технологію роботи пристрою чи системи, для яких будується дерево. Тому у нагоді може стати структурна схема об’єкта дослідження, яка дає уявлення про послідовність проходження сигналів керування та контролю в процесі функціонування.

Тож зображуємо структурну схему й детально аналізуємо її роботу у різних режимах. Після того, як ви будете мати чітке уявлення про побудову і роботу об’єкта дослідження, стане можливим визначити перелік первинних подій. Водночас слід пам’ятати про системне уявлення процесів, що відбуваються. Це означає необхідність ураховувати ймовірну поведінку та можливі помилки людини-оператора і дестабілізуючі фактори середовища.

Для того, щоб визначити перелік можливих помилок людини-оператора, необхідно мати чітке уявлення про те, які функції вона виконує. Власне кажучи, якщо не вдаватися в конкретні подробиці роботи оператора, достатньо знати його функції у штатних та нештатних ситуаціях. При такому підході іноді буває достатньо визначення первинної події як «небезпечна помилка» (дії оператора). Аналогічно можна визначити і чинники

впливу дестабілізуючих факторів. Первинні події доцільно позначити буквами a, b, c, d…… або при їх великій кількості у вигляді X1, X2, X3…

Крок 3. Визначення проміжних подій дерева та формування критеріїв їх існування.

Указані події виникають у результаті дії логічних операцій дерева. Вони фактично пояснюють процедуру розробки та спрощують його побудову. Особливо це важливо для складних, багатоформатних дерев, що містять велику кількість логічних змінних. Фактично проміжні події дуже часто виступають у ролі критеріїв існування кінцевої події. Завдяки такому підходу розробнику стає легше рухатися до кінцевої мети, маючи опис того, що відбувалося раніше. Знаючи проміжні події (критерії існування кінцевої події дерева), можна в процесі розроблення дерева рухатися зверху вниз, переходячи від кінцевої події до проміжних, і надалі вийти на первинні події, які фактично зумовлюють їх існування. Проміжні події можна визначати конкретно, наприклад «пошкодження схеми керування електропривода», або у абстрактному вигляді як «подія k, j, m, n…». У кожному випадку проміжні події необхідно позначати деякими змінними тому, що вони можуть бути включені до функції дерева.

Крок 4. Розроблення структурної функції дерева.

Власне структурна функція може бути записана як до, так і після розробки дерева. Це залежить від особливостей об’єкта дослідження, його масштабності, складності, уподобання і можливостей власне дослідника та інших факторів.

Крок 5. Побудова дерева відмов.

Розглянемо схему вмикання лампи зеленого вогню залізничного світлофора. Принцип дії схеми основується на двоканальній комутації ланцюгів живлення об’єкта керування за допомогою різних каналів А та В, а також перехресним контролем цих дій (рис. 4.2).

Концепція безпеки наведеної схеми основується на двоканальній комутації полюсів живлення двома незалежними каналами та перехресним контролем сигналів керування, тобто наявність (відсутність) сигналу А контролює канал В, і навпаки.

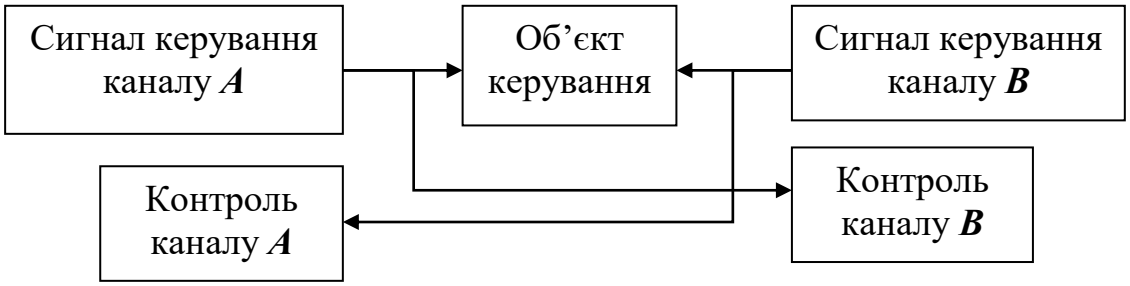


Рис. 4.2. Структурна схема увімкнення об'єкта керування критичної інфраструктури

Небезпечні стани об'єкта керування:

– несанкціоноване вмикання об'єкта керування, тобто лампи зеленого вогню світлофора;

– несанкціоноване не вимикання об'єкта керування (на світлофорі продовжує горіти зелений вогонь, тоді як повинен увімкнутися інший).

Можливі причини появи цих небезпечних подій та їх наслідки наведені у табл. 4.2. Будемо вважати, що використовується електронний модуль виведення з вихідним транзистором.

Зосередимося на чотирьох визначених у табл. 4.2 пошкодженнях, хоча при більш детальному розгляді їх може бути значно більше. Отже, аналіз даних дає змогу сформулювати кінцеву подію. Небезпечним алгоритмом функціонування є несанкціоноване вмикання лампи світлофора або невмикання її у разі необхідності.

Таблиця 4.2

Аналіз причин та наслідків пошкоджень

Характер пошкодження	Можливі причини	Характер відмови	Наслідки
1	2	3	4
Поява несанкціонованого сигналу А	Тепловий пробій вихідного транзистора	Захисна відмова	Лампа не горить
	Електричний пробій вихідного транзистора	Небезпечна відмова	Лампа горить

Продовження табл. 4.2

1	2	3	4
Поява несанкціонованого сигналу В	Тепловий пробій вихідного транзистора	Захисна відмова	Лампа не горить
	Електричний пробій вихідного транзистора	Небезпечна відмова	Лампа горить
Несанкціонована трансформація сигналу контролю в каналі А	Пошкодження схеми або програмний збій у роботі модуля	Небезпечна відмова	Лампа не горить, але надходить сигнал про її горіння
Несанкціонована трансформація сигналу контролю в каналі В	Пошкодження схеми або програмний збій у роботі модуля	Небезпечна відмова	Лампа не горить, але надходить сигнал про її горіння

Визначимо перелік вхідних подій та можливі наслідки їх збігів.

Первинні події:

– електричний пробій вихідного транзистора модуля А – X1;

– електричний пробій вихідного транзистора модуля В – X2;

– небезпечні трансформації сигналу в модулі А

(0 ... 1; 1 ... 0) – X3;

– небезпечні трансформації сигналу в модулі В

(0 ... 1; 1 ... 0) – X4.

Далі визначимо критерії (умови) існування небезпечного алгоритму функціонування світлофора:

1. Електричний пробій модулів виведення А та В одночасно.

2. Пробій виходу А та небезпечна трансформація у вихідному модулі В.

3. Пробій виходу В та небезпечна трансформація у сигналі вихідного модуля А.

4. Одночасне спотворення контрольних сигналів у каналах А та В.

З урахуванням визначених небезпечних збігів побудуємо дерево, зовнішній вигляд якого можна спостерігати на рис. 4.3.

Наведене дерево досить наочно ілюструє поведінку схеми, яка досліджується, і дає змогу визначити найбільш уразливі місця.

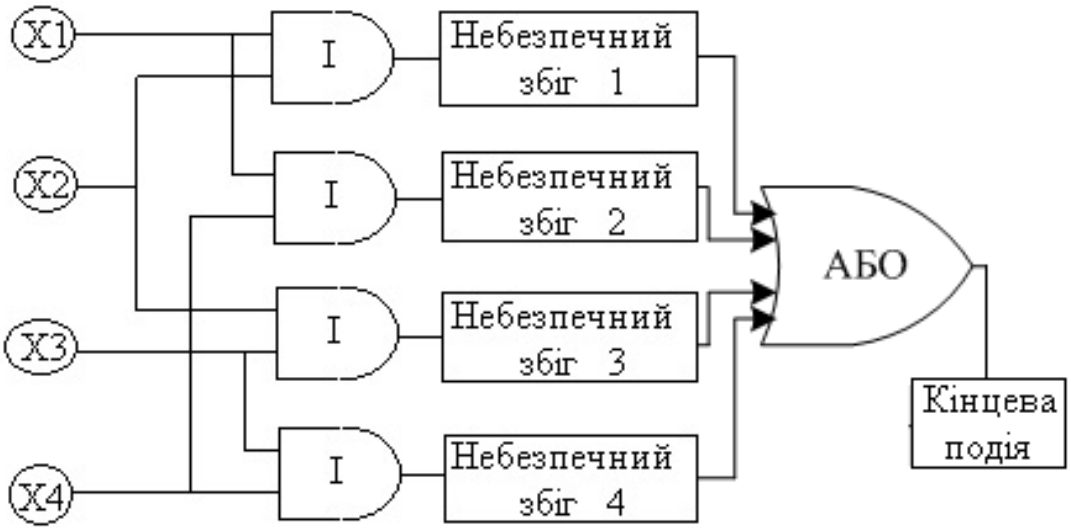


Рис. 4.3. Дерево небезпечних подій

4.2. Приклади дерев небезпечних відмов

4.2.1. Дерево безпечності виконання відповідальної функції для системи мікропроцесорної централізації

Розглянемо дерево безпечності виконання відповідальної функції для системи мікропроцесорної централізації Стріла-10, структурна схема якої була розглянута у другому розділі (рис. 2.20).

Відповідно до неї на першому етапі була синтезована структурна схема реалізації відповідальної функції (рис. 4.4).

Реалізація відповідальних функцій у КПТЗ виконується за програмою, яка зберігається у ЦВМ, і містить послідовний циклічний обмін, а саме:

– цикл видачі команд:

а) послідовний аналіз наявності команд від АРМо-Ц ДСП (АРМр-Ц ДСП) та їх приймання до ЦВМ;

б) перевірка у ЦВМ прийнятої команди на коректність;

в) перевірка у ЦВМ прийнятих команд на відповідність умовам безпеки руху поїздів, що закладені у логіці залежностей СЦБ;

г) видача цих команд з ЦВМ до об’єктних контролерів ЦМА за відповідності умовам безпеки;

д) формування об’єктними контролерами ЦМА керуючих впливів для польових об’єктів керування;

– цикл контролю стану польових об’єктів:

а) приймання об’єктними контролерами ЦМА даних про стан польових об’єктів до апаратури ЦМА;

б) обробка прийнятих даних у об’єктних контролерів ЦМА та трансляція їх, а також даних про стан самих контролерів до ЦВМ;

в) обробка у ЦВМ прийнятих з ЦМА даних та збереження поточного стану польового обладнання й об’єктних контролерів ЦМА.

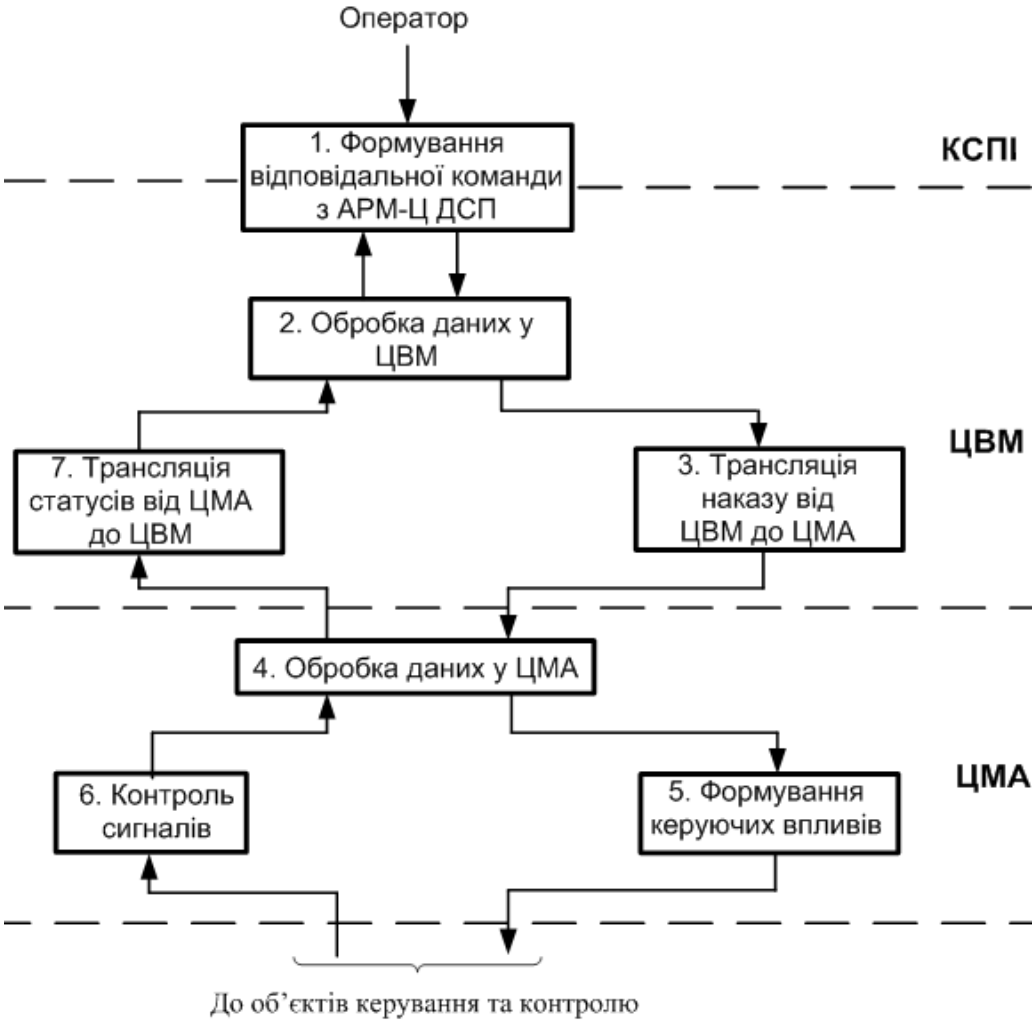


Рис. 4.4. Загальна схема реалізації відповідальної функції

Наступний цикл роботи починається знову з опитування наявності команд з АРМ-Ц ДСП.

АРМ, що входять до КСПІ, послідовно зчитують із сервера КПТЗ дані про поточний стан польового обладнання та апаратури КПТЗ для можливості відображення цього стану на своїх моніторах.

Для проведення розрахунків інтенсивності небезпечних відмов обираємо функцію, під час виконання якої задіяна найбільша кількість обладнання. Такою функцією є «Встановлення маршруту Ч-2П». Структурна схема виконання цієї функції наведена на рис. 4.5, дерево відмов та розрахунок інтенсивності небезпечних відмов під час виконання цієї функції наведені нижче.

Дерево відмов виконання функції «Встановлення маршруту Ч-2П» (рис. 4.6) розроблено з урахуванням нижченаведених обмежень.

Підчас виконання цієї функції з періодом 100 мс до ЯЛ надходять статуси про стани пристроїв керування, в ОК виконується самодіагностика елементів, які відповідають за функціональну безпечність, з періодом 20 с, тому всі ймовірності відмов елементів ураховуємо за час 20 с.

До небезпечних відмов під час виконання функції «Встановлення маршруту Ч-2П» може призвести:

- небезпечна відмова ЦВМ;
- небезпечна відмова ОКД;
- небезпечна відмова ОКС;
- небезпечна відмова ОКПС;
- небезпечна відмова у лінії.

Небезпечна відмова ЦВМ може бути викликана такими відмовами:

- небезпечна відмова ЯЛ, яка настає при небезпечній відмові в одному з каналів;
- небезпечна відмова одного з каналів ЯЛ;
- небезпечна відмова у лінії;
- небезпечна відмова КСв.

Небезпечна відмова ОКД виникає при небезпечній відмові в одному з чотирьох ОКД-Е-В, задіяних при виконанні цієї функції.

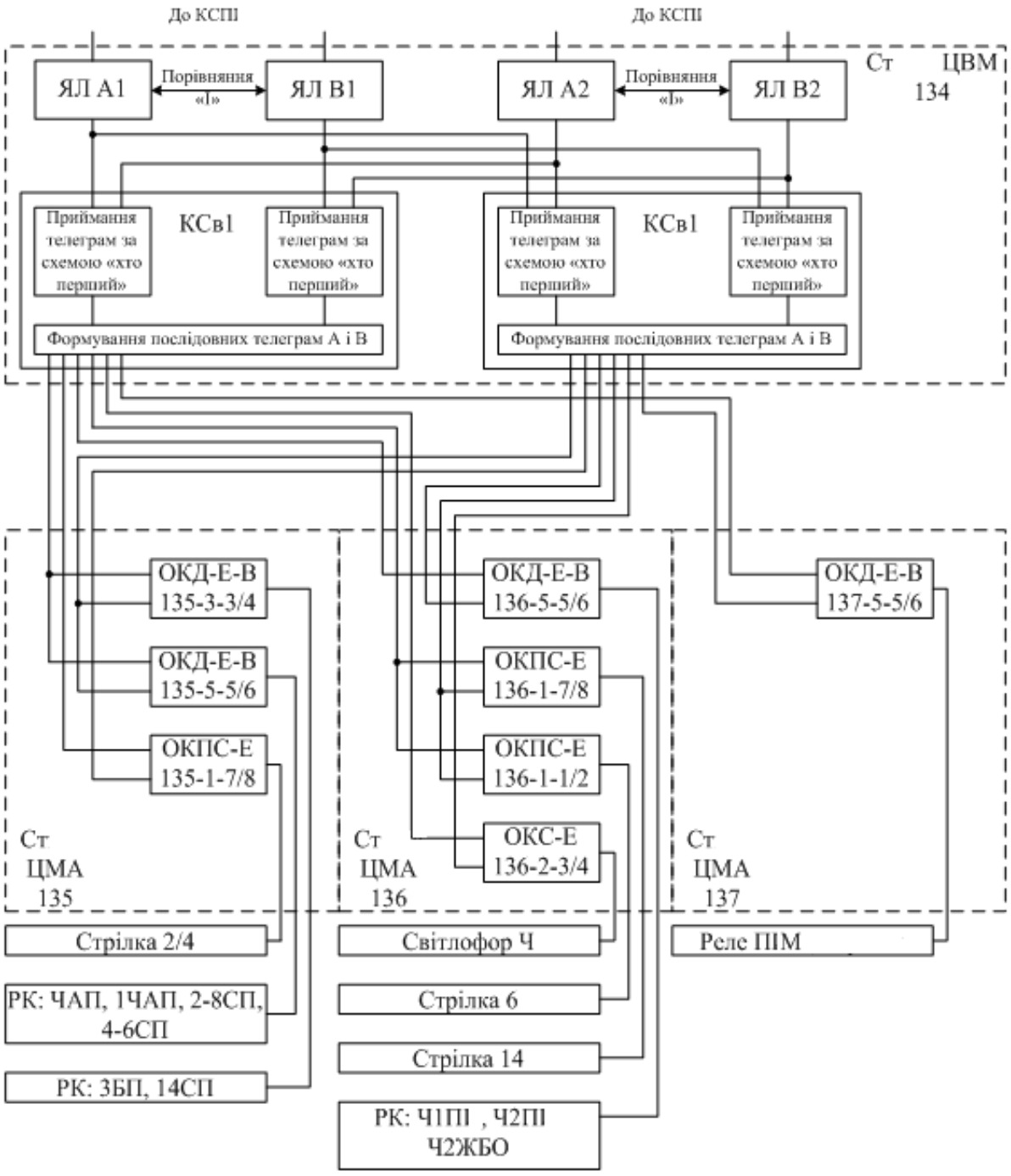


Рис. 4.5. Структурна схема виконання функції «Встановлення маршруту Ч-2П»

Небезпечна відмова ОКС виникає при небезпечній відмові в ОКС-Е, який задіяний при виконанні цієї функції.

Небезпечна відмова ОКПС виникає при небезпечній відмові в одному з трьох ОКПС-Е, задіяних при виконанні цієї функції.

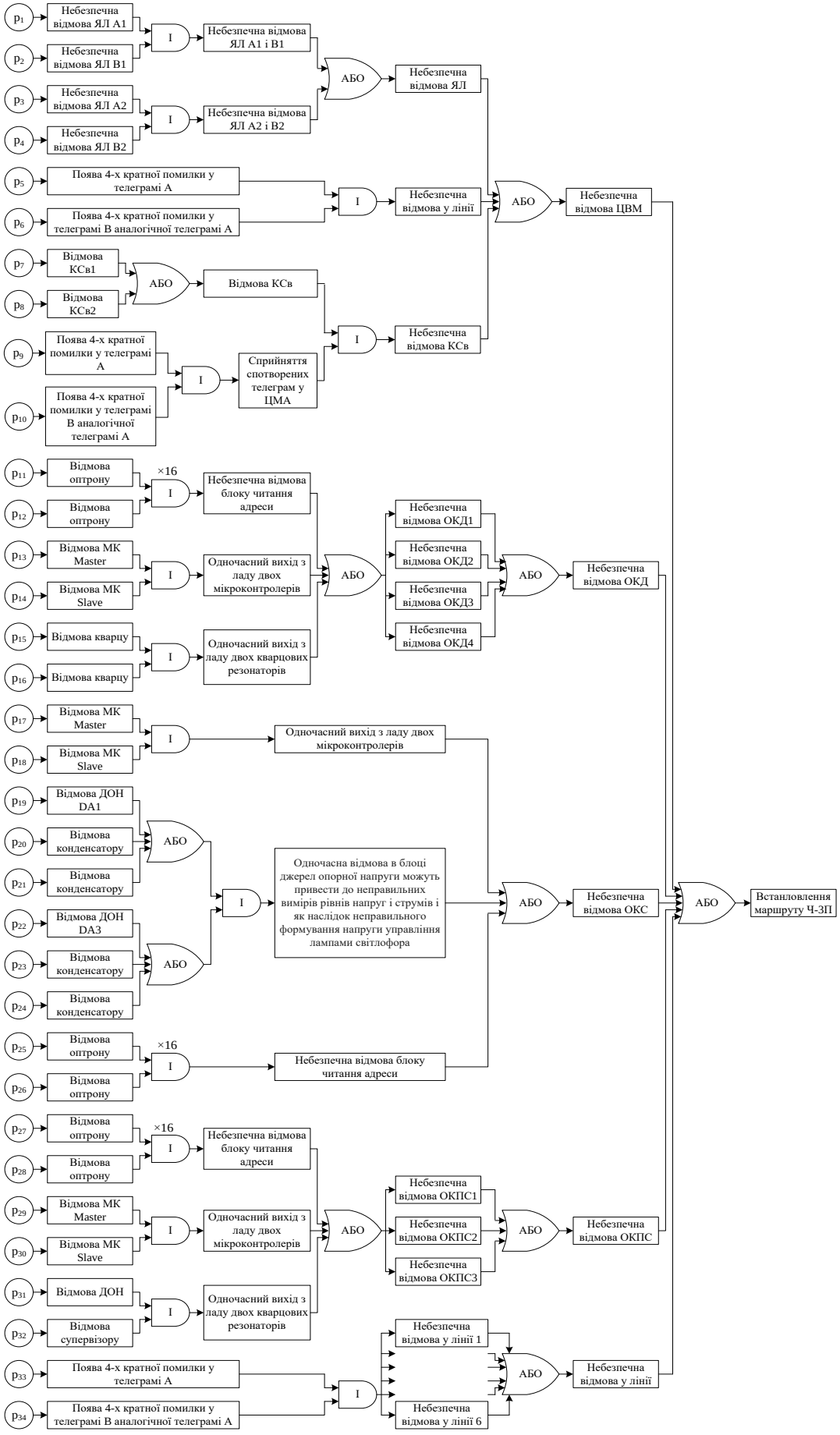


Рис. 4.6. Дерево відмов відповідальної функції

Небезпечна відмова у лінії виникає при небезпечній відмові в однієї з дванадцяти ліній, які зв'язують ЦВМ з об'єктними контролерами.

Розрахунок імовірності небезпечних відмов під час виконання функції «Встановлення маршруту Ч-2П» виконується за формулою

$$p_{нв} = \{[(p_1 \cdot p_2) + (p_3 \cdot p_4)] + (p_5 \cdot p_6) + [(p_7 + p_8) \cdot (p_9 \cdot p_{10})]\} +$$
$$+ [(p_{11} \cdot p_{12}) \cdot 16 + (p_{13} \cdot p_{14}) + (p_{15} \cdot p_{16})] \cdot 8 +$$
$$+ \{(p_{17} \cdot p_{18}) + [(p_{19} + p_{20} + p_{21}) \cdot (p_{22} + p_{23} + p_{24})] + (p_{25} \cdot p_{26}) \cdot 16\} \cdot 2 +$$
$$+ [(p_{27} \cdot p_{28}) \cdot 16 + (p_{29} \cdot p_{30}) + (p_{31} \cdot p_{32})] \cdot 6 + (p_{33} \cdot p_{34}) \cdot 12 = 1{,}77 \cdot 10^{-14}, \quad (5.1)$$

де p_1, p_2, p_3, p_4 – імовірність виходу з ладу ПЛІС у ЯЛ А1, В1, А2, В2 відповідно ($p_1 = p_2 = p_3 = p_4 = 5 \cdot 10^{-11}$);

p_5 – імовірність появи 4-кратної помилки у телеграмі А ($p_5 = 1{,}61 \cdot 10^{-7}$);

p_6 – імовірність появи 4-кратної помилки у телеграмі В, такої, як у телеграмі А ($p_6 = 6{,}62 \cdot 10^{-12}$);

p_7, p_8 – імовірність виходу з ладу ПЛІС у КСв1 і КСв2 відповідно $p_7 = p_8 = 9 \cdot 10^{-8}$);

p_9 – імовірність невиявлення помилок у телеграмі А за рахунок CRC-8 ($p_9 = 0{,}77$);

p_{10} – імовірність появи помилок у телеграмі В, аналогічних помилкам у телеграмі А ($p_{10} = 1{,}24 \cdot 10^{-7}$);

p_{11}, p_{12} – імовірність виходу з ладу оптрона у блоці читання адреси ОКД-Е ($p_{11} = p_{12} = 1{,}35 \cdot 10^{-9}$);

p_{13}, p_{14} – імовірність виходу з ладу мікроконтролерів у ОКД-Е ($p_{13} = p_{14} = 1{,}06 \cdot 10^{-10}$);

p_{15}, p_{16} – імовірність виходу з ладу кварцу у ОКД-Е ($p_{15} = p_{16} = 1{,}17 \cdot 10^{-10}$);

p_{17}, p_{18} – імовірність виходу з ладу мікроконтролерів у ОКС-Е ($p_{17} = p_{18} = 1{,}06 \cdot 10^{-10}$);

p_{19}, p_{22} – імовірність виходу з ладу мікросхем DA1, DA3 відповідно у блоках ДОН ОКД-Е ($p_{19} = p_{22} = 3{,}95 \cdot 10^{-11}$);

p_{20}, p_{23} – імовірність виходу з ладу конденсаторів С8, С25 відповідно у блоках ДОН ОКД-Е ($p_{20} = p_{23} = 1{,}01 \cdot 10^{-11}$);

p_{21}, p_{24} – імовірність виходу з ладу конденсаторів С9, С26 відповідно у блоках ДОН ОКД-Е ($p_{21} = p_{24} = 2{,}87 \cdot 10^{-11}$);

p_{25}, p_{26} – імовірність виходу з ладу оптрона у блоці читання адреси ОКС-Е ($p_{25} = p_{26} = 1{,}35 \cdot 10^{-9}$);

p_{27}, p_{28} – імовірність виходу з ладу оптрона у блоці читання адреси ОКПС-Е ($p_{27} = p_{28} = 1{,}35 \cdot 10^{-9}$);

p_{29}, p_{30} – імовірність виходу з ладу мікроконтролерів у ОКПС ($p_{29} = p_{30} = 1{,}06 \cdot 10^{-10}$);

p_{31} – імовірність виходу з ладу мікросхеми DA2 у блоку ДОН ОКПС-Е ($p_{31} = 4{,}96 \cdot 10^{-9}$);

p_{32} – імовірність виходу з ладу супервізору DA23 у ОКПС-Е ($p_{32} = 3{,}95 \cdot 10^{-11}$);

p_{33} – імовірність появи 4-кратної помилки у телеграмі А при передачі по лінії зв'язку ($p_{33} = 1{,}61 \cdot 10^{-7}$);

p_{34} – імовірність появи 4-кратної помилки у телеграмі В, такої, як у телеграмі А при передачі по лінії зв'язку ($p_{34} = 6{,}62 \cdot 10^{-12}$).

З урахуванням того, що ймовірність небезпечної відмови під час виконання відповідальної функції дорівнює (5.1) – $1{,}77 \cdot 10^{-14}$ за час 20 с, інтенсивність небезпечної відмови на одну відповідальну функцію буде становити – $\lambda_{нв} = 3{,}18 \cdot 10^{-12}$ 1/год.

До КПТЗ у цілому ставиться четвертий рівень вимог функційної безпечності згідно з ДСТУ 4178. Через це інтенсивність небезпечної відмови за кожну годину на одну відповідальну функцію безпечності за проектно-конструкторськими нормативами не повинна перевищувати значення $1{,}4 \cdot 10^{-11}$ 1/год. Отже, отримане значення інтенсивності $3{,}18 \cdot 10^{-12}$ 1/год не перевищує нормативне значення і відповідає вимогам ДСТУ 4178-2003.

4.2.2. Структурні моделі залізничних транспортних подій

Синтезуємо дерево транспортної події за галузевими ознаками, маючи на увазі, що виникаюче порушення безпеки руху може бути віднесено тільки за однією галуззю (рис. 4.7). Функція дерева має вигляд класичної логічної операції «АБО»

$$У_{ТП} = 1-(1-y_1)\cdot(1-y_2)\cdot(1-y_3)\cdot(1-y_4)\ldots,$$

де y_1, y_2, y_3, y_4, … – структурні функції галузевих дерев транспортних подій.

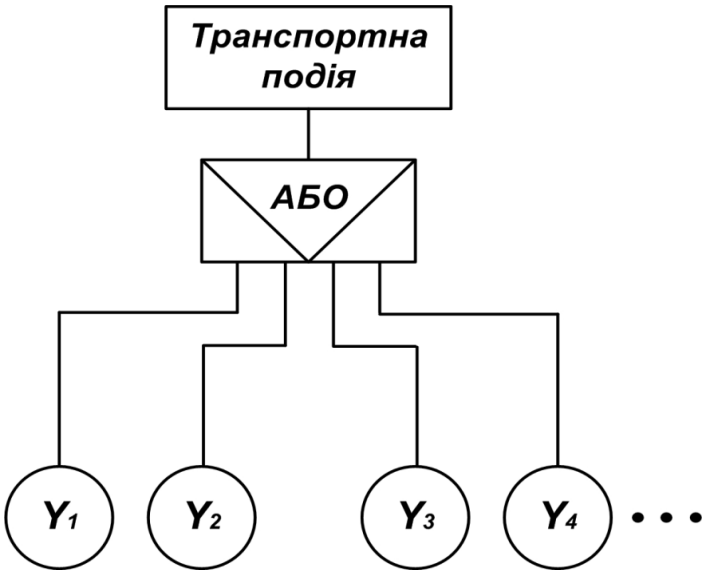


Рис. 4.7. Дерево транспортної події за галузевою ознакою

Специфіку використання засобів транспорту для основних визначених напрямків діяльності залізниці враховують окремі галузеві дерева. До них належать: рухомий склад, залізнична колія, пристрої автоматики, підсистема керування рухом поїздів.

Для рухомого складу критеріями небезпечної події є пошкодження технічних засобів внаслідок внутрішніх причин або помилок людини-оператора.

Дерево транспортної події підсистеми тягового рухомого складу у загальному вигляді може мати такі первинні порушення: x_{11} – небезпечні дії локомотивної бригади, x_{12} – збій у роботі засобів автоконтролю та діагностування, x_{13} – небезпечні помилки технічного персоналу, який здійснює роботи з технічного обслуговування та ремонту рухомого складу (рис. 4.8).

Логічна функція кінцевої події для дерева підсистеми рухомого складу близька до «І-АБО»

$$Y_1 = 1-\left[(1-x_{11})(1-x_{12}\cdot x_{13})\right] = x_{11} + x_{12}\cdot x_{13} - x_{11}\cdot x_{12}\cdot x_{13}.$$

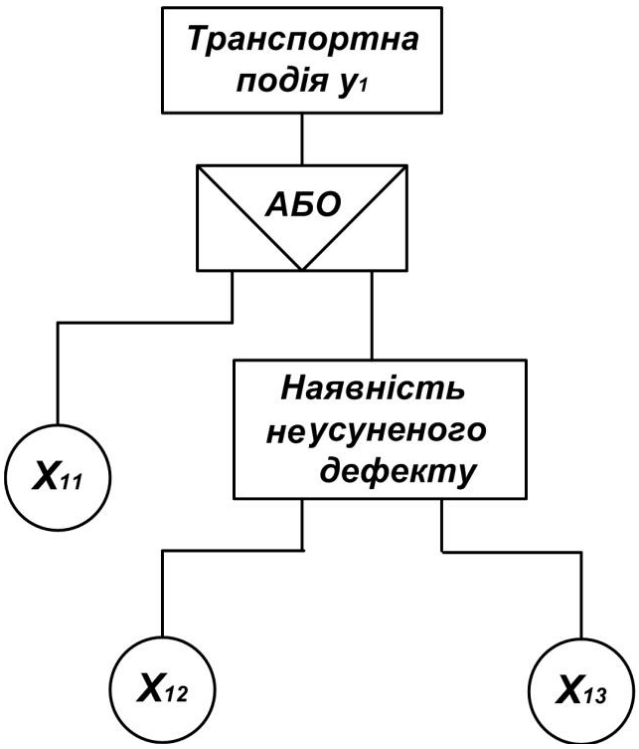


Рис. 4.8. Дерево транспортної події для підсистеми рухомого складу

Поява небезпеки насамперед визначається змінними x_{11} та x_{12} x_{13}, тобто помилками експлуатаційного і технічного штату.

Дерево транспортної події засобів залізничної автоматики має вигляд класичної функції «**І**». Критерієм існування кінцевої події є наявність пошкоджень технічних засобів x_{21} та x_{22}, небезпечні дії персоналу, який повинен виконувати профілактичні роботи з технічного обслуговування, x_{23} та наявність рухомої одиниці в небезпечній зоні x_{24} (рис. 4.9). Структурна функція дерева записується у вигляді

$$Y_2 = x_{21} \cdot x_{22} \cdot x_{23} \cdot x_{24},$$

де x_{21} та x_{22} – захисні відмови технічних засобів, які в сукупності визначають появу небезпечної події;

x_{23} – небезпечні дії технічного персоналу;

x_{24} – наявність рухомого складу в зоні пошкодження.

Визначальною є змінна x_{23}, що характеризує «людський фактор», через те, що ймовірності відмов технічних засобів значно менші, тобто $x_{21} \cdot x_{22} << x_{23}$. Підтвердженням цієї тези можуть бути дані статистичної звітності, згідно з якими з вини

працівників трапляється більш ніж 60 % усіх випадків порушень у роботі галузі [24]. З огляду на відзначене виникає необхідність автоматичного контролю виконання технічним штатом регламентних робіт з технічного обслуговування пристроїв залізничної автоматики. Це потребує деталізації останнього дерева щодо помилок персоналу.

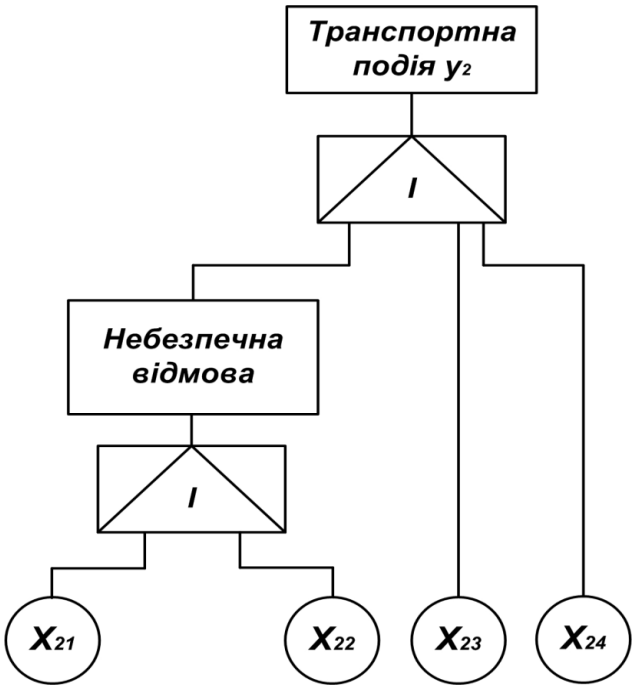


Рис. 4.9. Дерево транспортної події для пристроїв залізничної автоматики

Надалі розглянемо причини виникнення порушень у колійному господарстві. У його складі є залізнична колія та інженерні споруди, які безпосередньо забезпечують рух поїздів (мости, залізничні тунелі тощо). Стале функціонування технічних засобів колійного господарства забезпечується насамперед роботами з ремонту й утримання колії та сучасними засобами технічного діагностування. Пошкодження колії або інженерних споруд, які забезпечують рух поїздів, повинні виявляти персонал або технічні засоби. Через це критерієм небезпеки є поява пошкодження, яке не виявила людина або технічні засоби. Окремі аварії відбуваються внаслідок неякісно виконаних або невиконаних регламентних робіт. Тому дерево для підсистеми колії та інженерних споруд за критеріями існування кінцевої події є близьким до раніше розглянутого (рис. 4.10).

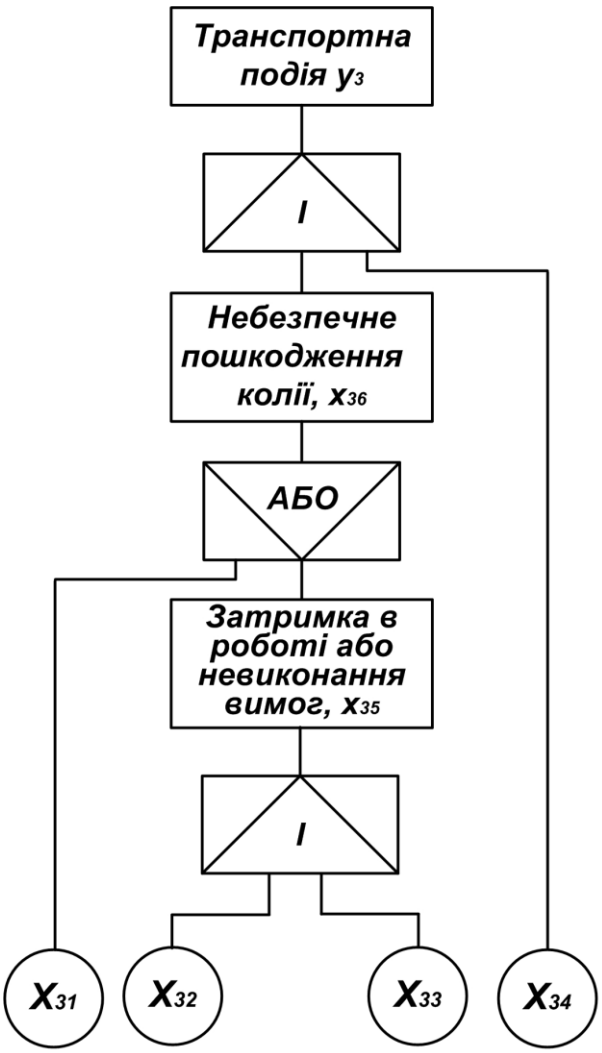


Рис. 4.10. Дерево транспортної події для підсистеми колії та інженерних споруд

Структурна функція дерева будується відповідно до сформованих критеріїв

$$Y_3 = \left[1-\left(1-x_{31}\right)\cdot\left(1-x_{35}\right)\right]\cdot x_{34} = x_{31}\cdot x_{34} + x_{32}\cdot x_{33}\cdot x_{34} + x_{31}\cdot x_{32}\cdot x_{33}\cdot x_{34},$$

де x_{31} – небезпечне пошкодження колії;

x_{32} – помилки або збій засобів діагностування стану колії;

x_{33} – небезпечні дії персоналу;

x_{34} – наявність рухомої одиниці в небезпечній зоні.

На відміну від рухомого складу небезпечна подія може відбутися тільки за умов появи рухомої одиниці в зоні пошкодження. Аналіз функції дерева траєкторії вказує на дуже велике значення засобів діагностування та змінна x_{32} присутня в

двох з трьох збігів. Крім того, принципове значення має інтенсивність руху поїздів на пошкодженій ділянці. Можна припустити, що, на відміну від попереднього дерева, поява пошкодження колії й наявність у небезпечній зоні рухомої одиниці достатньо для появи транспортної події зі значним рівнем імовірності. З указаної причини частота перевірок стану верхньої будови колії повинна бути пропорційна інтенсивності руху на цій ділянці.

Господарство перевезень, у якому основними причинами порушень безпеки руху є помилки оперативного персоналу, що безпосередньо забезпечують управління рухом поїздів.

Як відомо, безпеку перевезень забезпечують системи сигналізації, централізації та блокування і регламентовані дії людини-оператора. В наявних пристроях залізничної автоматики більшість важливих для безпеки функцій оператора виконуються автоматично або дублюються технічними засобами. Тому критерієм небезпеки є пошкодження засобів безпеки і помилка людини-оператора або помилка людини при виконанні відповідальної функції, яка не дублюється пристроями автоматики. При пошкодженні засобів автоматики оператор починає працювати більш інтенсивно, обстановка напружується і тому людина частіше припускається помилок у роботі. Дерево транспортної події для господарства перевезень наведено на рис. 4.11.

Його структурна функція визначає можливі небезпечні дії персоналу

$$Y_4 = x_{44} \cdot x_{45} = x_{44}\left[\left(1-(1-x_{41})\times\left(1-x_{42}\cdot x_{43}\right)\right)\right] = x_{41}\cdot x_{42} + x_{42}\cdot x_{43}\cdot x_{44} + x_{41}\cdot x_{42}\cdot x_{43}\cdot x_{44},$$

де x_{41} – небезпечні дії персоналу, які не блокуються технікою;

x_{42} – небезпечні дії персоналу, які блокуються технікою;

x_{43} – відмова засобів безпеки.

Аналіз рівняння (4.15) вказує на необхідність розширення функцій керування систем безпеки для зменшення впливу «людського фактору» на роботу транспорту. Вказані завдання можливо вирішити тільки шляхом застосування сучасних мікропроцесорних систем керування рухом поїздів з розширеними можливостями.

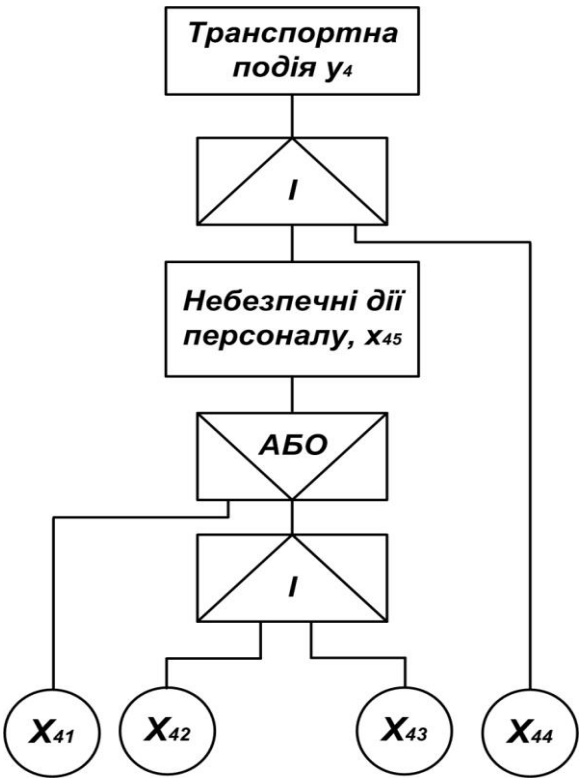


Рис. 4.11. Дерево транспортної події для господарства перевезень

Для визначення транспортної події за галузевим принципом повернемося до базової функції транспортної події. Після підстановки значень функцій $y_1 - y_4$ маємо остаточне рівняння для визначення транспортної події за галузевою ознакою

$$Y_{ТП} = 1 - \left[\begin{array}{l} \left(1 - x_{11} - x_{12}x_{13} + x_{11}x_{12}x_{13}\right) \cdot \left(1 - x_{21}x_{22}x_{23}x_{24}\right) \cdot \\ \cdot \left(1 - x_{31}x_{34} - x_{32}x_{33}x_{34} + x_{31}x_{32}x_{33}x_{34}\right) \cdot \left(1 - x_{41}x_{44} - x_{42}x_{43}x_{44} + x_{41}x_{42}x_{43}x_{44}\right) \end{array} \right].$$

Функція дерева має декілька мінімальних збігів небезпечних подій, а саме: (x_{11}, x_{12}); (x_{21}, x_{22}, x_{23}, x_{24}); (x_{31}, x_{34}); (x_{32}, x_{33}, x_{34}); (x_{41}, x_{42}); (x_{42}, x_{43}, x_{44}).

Цей перелік збігів є найбільш небезпечним для експлуатаційної роботи і через це потребує ретельного контролю.

Очевидно, що синтезовані галузеві дерева можуть розглядатися як базові, що визначають критерії існування небезпечної події для окремої галузі залізничного транспорту в системі оперативної безпеки. Для практичного використовування вони повинні деталізуватися. Крім того, на цей час є певні проблеми із забезпеченням розрахунку структурних функцій необхідними статистичними даними про порушення, що

виникають. За цих обставин для вирішення проблеми забезпечення розрахунковими даними було синтезовано формалізоване дерево транспортної події. В основу дерева покладено таке порушення безпеки руху (рис. 4.12):

– небезпечні відмови засобів транспорту з причин, незалежних від дій персоналу, x_1;

– небезпечні відмови засобів транспорту внаслідок дій (або бездіяльності) персоналу, x_2;

– небезпечні дії персоналу, який забезпечує керування рухом поїздів, x_3;

– небезпечні дії персоналу, який забезпечує експлуатацію рухомого складу, x_4.

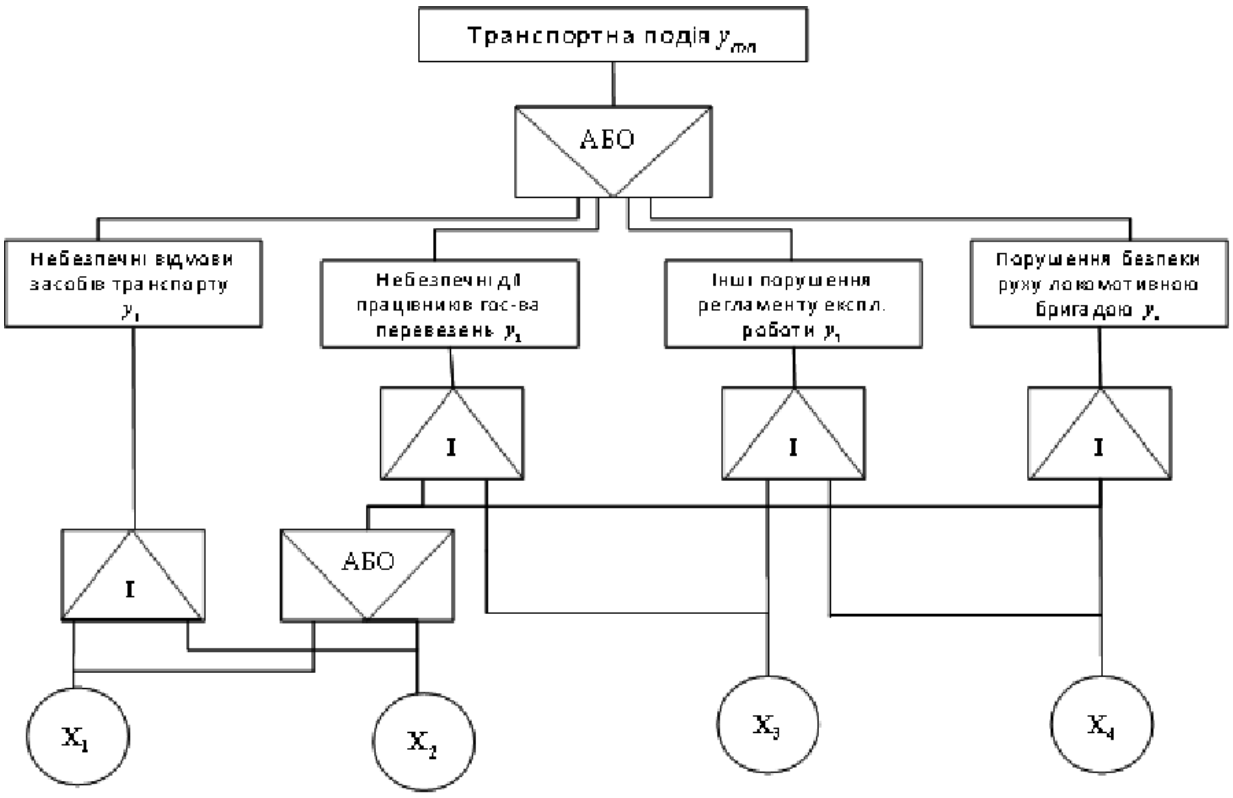


Рис. 4.12. Формалізоване дерево транспортної події

Визначено чотири небезпечних збіги, що призводять до появи кінцевої події:

$y_1=x_1x_2$;

$y_2=(x_1+x_2-x_1 \cdot x_2)\, x_3$;

$y_3=x_3x_4$;

$y_4=(x_1+x_2-x_1 \cdot x_2)\, x_4$.

Формула реалізації кінцевої події формалізованого дерева матиме вигляд

$$У_{ТП}=1–(1–y_1)\cdot(1–y_2)\cdot(1–y_3)\cdot(1–y_4).$$

Після підстановки значень небезпечних збігів y_1 – y_4 отримаємо

$$У_{ТПФ}=1-\left(1-x_1x_2\right)\times\left(1-\left(x_1+x_2-x_1x_2\right)\cdot x_3\right)\times\left(1-x_3x_4\right)\times\left(1-\left(x_1+x_2-x_1x_2\right)\cdot x_4\right).$$

Критерієм існування транспортної події для формалізованого дерева можна вважати такий перелік первинних порушень: *(x_1 і x_2)*; *(x_3 і x_4)*; [(x_1 *або* x_2) *і* x_3]; [(x_1 *або* x_2) *і* x_4]. Подія x_1 фігурує у всіх збігах, але остаточне визначення її значення та значень інших порушень можливо зробити тільки при проведенні кількісного аналізу отриманих функцій дерев небезпечних подій.

Висновки до четвертого розділу та практичні завдання

Послідовність етапів розроблення дерева відмов:

- крок 1 – аналіз роботи об’єкта дослідження;
- крок 2 – визначення кінцевої та початкової подій;
- крок 3 – визначення проміжних подій дерева та формування критеріїв їх існування;
- крок 4 – розроблення структурної функції дерева;
- крок 5 – побудова дерева відмов.

Практичні заняття

Мета: набуття практичних навичок щодо розроблення та аналізу дерев подій і відмов, закріплення теоретичних знань, отриманих при вивченні розд. 4.

Завдання

1. Проаналізуйте найпростіші види дерев подій та відмов, визначте їхні структурні функції.

2. Для обраної нештатної події СКС розробіть дерево подій. Визначте найбільш небезпечний та безпечний перебіг подій. Яка подія має найбільш важливе значення?

3. Для обраної структурної або електричної схеми розробіть дерево відмов, користуючись методикою, яка викладенна у п. 4.2.

4. Проведіть розрахунок кінцевої події дерева, що було розроблене, та визначте ймовірні причини пошкодження.

Ситуації для проведення дискусій та обговорення

1. Проаналізуйте дерева відмов, які наведено у пп. 4.3.2.

2. Порівняйте відомі вам методи аналізу електричних схем (наприклад структурно-логічну схему) з деревами подій та відмов, визначте їхні переваги та недоліки.

Контрольні питання для самостійної роботи до розд. 4

1. Чим відрізняється дерево пошкоджень від дерева подій?
2. Для чого розробляється дерево пошкоджень?
3. Чим відрізняється первинна подія дерева пошкоджень від інших?
4. Яке обмеження накладається на первинні події дерева?
5. Які переваги для проведення аналізу систем надає дерево пошкоджень?
6. Що таке мінімальний збіг подій дерева?
7. Кінцева подія дерева визначає ... (продовжити).
8. Що визначає дерево подій системи?
9. Як формуються дерева подій?
10. Як при формуванні дерева подій ураховуються програмні засоби?
11. Як впливають на розрахунок програмних засобів структури алгоритмів?
12. Які фактори створення програмного забезпечення впливають на швидкісні, які на вартісні, а які на безпекові якості системи?

Бібліографічний список

1. Artificial Neural Networks: Concepts and Theory. *IEEE Computer Society Press*. 1992. P. 12–17.
2. Back Propagation Neural Net Engine v1.33u for C programmers by Patrick Ko Shu-pui. No.11, 14 ST., Hong Lok Yuen Tai Po, Hong Kong.
3. Berry M. V. Catastrophes and semiclassical mechanics. *In Rencontrre de Cargiese sur les Singularities et leur Applications* (F. Pham,ed.). Institute d'Etudes Scientifiopees de Cargese, Publ.Math. Dept., Univ. Nice, 1975. P. 133–136.
4. Berry M. V. Waves and Thom's theorem. *Adv. Phys*. 25, 1976. P. 1–25.
5. Bowen I. P. Safety – critical systems Elservier. 1994. 406 p.
6. Bowles J. B., Chi Wan. Software failure modes and effects analysis for a small embedded control system. *Proc. of annu reliability and maintainability symp*. Philadelphia, 2001. P. 137–155.
7. Brummer J., Kersken M., Marlz J. Tools for software safety analysis, reliability engineering and System I Safety, Elsevier 46, 1994. P. 123–138.
8. Bush S. A review of Nuclear Piping Falures at their use in Establishing the reliability of Piping Sistems. *Service Experience in Fossil and Nuclear Power Plants*. ASME 1999. PVP Vol. 392. P. 137–155.
9. Chen X., Wang D., Huang H. & Wang Z. Verification and Validation in Railway Signalling Engineering – An Application of Enterprise Systems Techniques. *Enterprise Information Systems* 8 (4): 490–511. 2014. doi:10.1080/17517575.2013.835071.
10. Chatterjee P. Fault tree analyses Reliability theory and systems safety analysis. Nowember. 1994.
11. David Brown. Systems analysis and Design for Safety. Prenlice Hatt Incorporation, Engtewood Gtiffs, New Jercy. 2003.
12. Dickson D., Thom R. Was Newton's apple a cusp or a swallowtail. *Times Higher Education Supplement*, 5th December 1975. P. 13.
13. DIN V 19 250, Measurement and control, fundamental safety aspects for measuring and control protective equipment.

14. EEMUA Guidelines – Publication No 160, Safety related instrument for the process industry (including programmable electronic systems). 1989.

15. EN 50129 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signaling (Залізничні застосування – Електронні залізничні системи управління і захисту, пов'язані з безпекою).

16. EN 50128 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. (Залізничні застосування – ПЗ для залізничних систем управління і захисту).

17. EN 50126 RAMS CENELEC Европейский стандарт. Спецификация и доказательство надежности, эксплуатационной готовности, ремонтопригодности и безопасности для использования на железнодорожном транспорте. 1999. 74 с.

18. Everline C. Probabilistic Risk Assessment Examples from the South Ukraine NPP In – Depth Safety Assessment. 1998.

19. Factures of their use in Establishing the reliability of Piping Systems. *Service Experience in Fossil and Nuclear Power Prants*. ASSME 1999. PVP Vol. 392 p.

20. Fussel I. B. Fault free analysis concepts and techniques Aerojekt Nucfear Company Idaho Falls. Idaho USA.

21. Fussel I. B. and Wessely W. E. Anew methodology for obtnining cut sets for fault free. *Trans Amer Nuct Sos Vol.* 15. June, 1972.

22. Fusssel I. B. Fault free analyses concepts and techniques Acrojekt Nucfear Company Idaho Falls. Idaho USA.

23. Ganti T. A theory of Biochemical super systems and its application to problems of natural and artificial biogenesis. Budapest; *Akademiai*, 1979. 136 p.

24. Gluchkov V. M., Ivanov V. V., Janenko V. One class of nonlinear dynamic models and its applications. *Physika.* 1981. 2D. P. 61–72.

25. Gosselin S., Fleming K. Evaluation of Pipe Failure Potential via Degradation Mechanism Assessment. *Proceedings of ICON5*: 5th International Conference on Nuclear Engineering. Poster 2641. 1997. P. 10.

26. Grosette P. A. Computer Programs for Fault Tree Analyses. DUN – 5508. HSE, Regulating higher hazards: exploring

the issues (2000). *HSE Publication, Guidance on the use of programmable electronic systems in safety-related applications*. 1989.

27. Hughes P. J. Instrumentation and control systems important to safety: a new IAEA safety guide / Inter. topical meet. On nuclear plant instrumentation, control and human- machine interface technologies [Hughes P. J., Johnson G. L., Pauksens J., Pachner J.] ANS, Washington DS, 2000.

28. IEC 61508-3-2010 Function safety of electrical/electronic/programmable electronic electronic safety related systems – Part 3: Software requirements (Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою. Вимоги до програмного забезпечення).

29. IEC 61508-2-2010 Function safety of electrical/electronic/programmable electronic electronic safety related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety related systems (Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою. Вимоги до систем).

30. Petersen D. Techniques of Safety Menagement. N. Y.: McCraw Hill Group Comp., 1988. P. 22–28.

31. Удосконалення організаційно-управлінської роботи на підприємствах залізничного транспорту в сучасних умовах: навч. посіб. / Г. Ф. Арбузов, В. М. Бутенко, О. Г. Дайнека, А. О. Каграманян та ін.; за заг. ред. М. І. Данька. Харків: УкрДАЗТ, 2007. 178 с.

32. ДСТУ 44 96:2005. Безпечність руху залізничного транспорту. Терміни та визначення понять. Київ: Держспоживстандарт України, 2006. С. 1–8.

33. Кількісний аналіз показників надійності систем автоматики з використанням моделювання дерев небезпечних відмов. / В. М. Бутенко, Д. О. Зубрицький, С. В. Сіроштан, Є. С. Строєв. *Зб. наук. праць*. Харків: УкрДАЗТ, 2008. Вип. 92. С. 133–138.

34. Дрейнс Ю. О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи

об’єктів критичної інфраструктури. *Захист інформації.* Київ: НАУ, 2017. Т. 19. С. 15–29.

35. ДСТУ 2827-94. Комплекси мікропроцесорних засобів диспетчеризації, автоматики, телемеханіки. Правила приймання і методи випробувань. Київ: Держстандарт України, 1995. 78 с.

36. ДСТУ 2862-94. Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги. Київ: Держстандарт України, 1995. 78 с.

37. ДСТУ 3004-95. Надійність техніки. Методи оцінки показників надійності за експериментальними даними. Київ: Держстандарт України, 1995. 78 с.

38. ДСТУ 3413-96. Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції. Київ: Держстандарт України, 1995. 78 с.

39. ДСТУ 3433-96 (ГОСТ 27.005-97). Надійність техніки. Моделі відмов. Основні положення. Київ: Держстандарт України, 1995. 78 с.

40. ДСТУ 3681-98 (ГОСТ 30585-98). Сумісність технічних засобів електромагнітна. Стійкість до дії грозових розрядів. Технічні вимоги та методи. Київ: Держстандарт України, 1995. 78 с.

41. ДСТУ 4178-2003. Комплекси технічних засобів систем керування та регулювання руху поїздів. Функціональна безпечність і надійність. Вимоги та методи випробування. Київ: Держстандарт України, 1995. 78 с.

42. Жуковицький І. В., Косолапов А. А. Концептуальне проектування комп’ютерних систем реального часу. Дніпро: ДНУЗТ ім. акад. В. Лазаряна, 2018. 215 с.

43. Про залізничний транспорт: Закон України від 4 липня 1996 р. № 273/96-ВР, зі змінами та доповненнями.

44. Роїна О. М. Залізничний транспорт в Україні. Нормативна база. Київ: КНТ, 2005. 480 с.

45. Інструкція з організації технічного обслуговування та ремонту програмно-апаратних комплексів залізничної автоматики, телемеханіки та зв'язку ЦШ-0057: наказ від 18.05.2009 № 291-Ц. 36 с.

46. Математичне моделювання в розподілених інформаційно-керуючих системах залізничного транспорту:

монографія / С. В. Лістровий, С. В. Панченко, В. І. Мойсеєнко, В. М. Бутенко. Харків: ФОП Бровін О. В., 2017. 220 с.

47. Методика доказу безпеки функціонування мікроелектронних комплексів систем управління та регулювання рухом поїздів: наказ УЗ від 17.08.2001 № 452-Ц.

48. Мойсеєнко В. І. Локалізація небезпечних подій процесу використання засобів залізничного транспорту. *Зб. наук. праць Укр. держ. акад. залізнич. трансп.* Харків: УкрДАЗТ, 2010. Вип. 114. С. 22–24.

49. Мойсеєнко В. І. Мікропроцесорні системи залізничної автоматики: навч. посіб. для студ. вищ. навч. закл. Харків: Регіон-інформ, 1999. 147 с.

50. Мойсеєнко В. І. Функції ризиків втрат для оцінки безпеки залізничного транспорту. *Зб. наук. праць.* Харків: УкрДАЗТ, 2005. Вип. 69. С. 26–32.

51. ДСТУ ISO/IES 27005:2015. Національний стандарт України. Управління ризиками інформаційної безпеки. Київ: Держстандарт України, 2015. 135 с.

52. ДСТУ ISO/IES 27005:2015. Національний стандарт України. Управління ризиками інформаційної безпеки. Київ: Держстандарт України, 2015. 135 с.

53. Нормативні акти з безпеки руху поїздів. Київ: Транспорт України, 2002. 142 с.

54. Положення про класифікацію транспортних подій на залізничному транспорті України. №800 від 16.10.2003 наказ МТУ. С. 2–5.

55. Правила безпечної експлуатації пристроїв автоматики, телемеханіки та зв'язку на залізницях України ЦШ/0030: наказ від 17.11.2003 № 288-Ц.

56. Правила ядерной безопасности реакторных установок атомных станций. ПБЯРУ АС – 8911 *Атомная энергия*. 1990. Т. 69, вып. 6. С. 409–422.

57. Рішення Ради національної безпеки і оборони України від 16 лютого 2017 року Про невідкладні заходи з загроз енергетичній безпеці України та посилення захисту критичної інфраструктури

58. Самсонкин В. Н., Шалаева Т. А Системный подход в проблеме управления безопасностью движения. *Вісник*

Дніпропетр. нац. ун-ту ім. акад. В. Лазаряна. Дніпропетровськ, 2005. Вип. 8. С. 101–106.

59. Самсонкин В. Н. Теоретические основы автоматизированного контроля человеческого фактора в человеко-машинных системах на железнодорожном транспорте: дис. … д-ра техн. наук. Харьков, 1997. 440 с.

60. Сокол Э. Н. Железнодорожно-транспортное происшествие и его механизм (Судебная экспертиза. Элементы теории и практики): монография. Львів: *ПАІС*, 2011. 376 с.

61. Самсонкін В. М., Мойсеєнко В. І Теорія безпеки на залізничному транспорті: монографія Київ: Каравелла, 2014. 248 с.

62. Смит Дэвид Дж., Симпсон Кеннет Дж. Л. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов. Москва: Издательский дом “Технология”, 2004. 208 с.

63. Харченко В. С., Ястребенецкий М. А., Васильченко В. Н Нормирование и оценка безопасности информационных и управляющих систем АЭС: Регулирующие требования к программному обеспечению *Ядерная и радиационная безопасность*. 2002. № 1. С. 18–33.

64. Хенли Э. Д. Надежность технических систем и оценка риска: пер. с англ. В. С. Сыромятова, Г. С. Деминой; под общ. ред. В. С. Сыромятова. Москва: Машиностроение, 1984. 528 с.

Навчальний посібник

Мойсеєнко Валентин Іванович,
Бутенко Володимир Михайлович

БЕЗПЕЧНІСТЬ СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Відповідальний за випуск Бутенко В. М.

Редактор Еткало О. О.

Підписано до друку 07.07.20 р.

Формат паперу 60х84 1/16. Папір писальний.

Умовн.-друк. арк. 7,25. Тираж 50. Замовлення №

Видавець та виготовлювач Український державний університет
залізничного транспорту,
61050, Харків-50, майдан Фейєрбаха, 7.
Свідоцтво суб'єкта видавничої справи ДК № 6100 від 21.03.2018 р.