УДК 656.25

ФОРМУВАННЯ ОЦІНОК ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ЦИФРОВИХ СИСТЕМ ЗАЛІЗНИЧНОЇ АВТОМАТИКИ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Мойсеєнко Валентин Іванович
д. т. н., професор
Каменєв Олександр Юрійович
к. т. н., доцент
Дученко Павло Юрійович,
Сафін Вадим Талгатович
аспіранти
Український державний університет
залізничного транспорту, м. Харків, Україна

Вступ. Всі системи керування об’єктами критичної інфраструктури потребують процедур оцінювання показників функціонального призначення. У переважній більшості система оцінок формується на стадії розроблення та процедур сертифікації. На залізничному транспорті регулюючими документами [ДСТУ] визначений порядок та показники оцінювання. Зокрема це показники функціональної безпечності, які є найбільш важливими для систем керування рухом поїздів.

У подальшому на етапі технічного використання такі розрахунки можуть проводитися як правило, при розгляді питань подовження терміну експлуатації. Подібні дослідження більш характерні для системи керування ядерним устаткуванням. На залізничному транспорті процедури формування on-line оцінок показників функціональної безпеки обмежуються поки-що періодичними оглядами з визначенням технічного стану шляхом експертного оцінювання. Такий стан питання обумовлений електромеханічною елементною базою систем керування, яка унеможливлює застосування моніторингу та оперативного діагностування стану технічних засобів.

Впровадження мікропроцесорних систем знімає існуючі раніше обмеження, але недостатня наукова підтримка проблем оперативного оцінювання показників функціонування технічних засобів залізничної автоматики дещо гальмує цей процес. Тому проблема формування методів та моделей оперативного оцінювання показників функціонування залізничних систем керування критичного призначення є актуальною та практично необхідною.

Метою роботи є розроблення методу та моделей оперативного оцінювання функціональної безпеки мікропроцесорних систем критичного призначення для потреб залізничного транспорту в режимі реального часу.

Матеріали та методи. Більш адаптованим під механізми оперативного оцінювання показників функціонування людино-машинних систем є математичний апарат теорії катастроф. Він дозволяє відслідковувати поведінку системи й заздалегідь визначати критичні моменти у функціонуванні системи. Головним недоліком цього методу моделювання небезпек є прив'язка до обраного виду поверхні катастрофи. Дослідження авторів показали складність вибору поверхні, яка достатньо адекватно описує поведінку залізничних систем керування, які мають широкий спектр дестабілізуючих факторів, природа яких не завжди добре досліджена.

Результати і обговорення. Як було показано раніше, всі існуючі методи і моделі формування системи оцінювання функціональної безпеки систем залізничної автоматики базуються на концепції одного виміру. Як правило це здійснюється на етапі розроблення та впровадження системи. Крім того оцінюється робота всієї системи в комплексі. На практиці користувачам доцільно мати інформацію про безпечність конкретного маршруту і конкретної дії, і бажано в режимі реального часу. Це дозволить обрати більш безпечний маршрут, або завчасно запобігти розвитку небезпечної ситуації. Для об'єкту дослідження обираємо станційні системи керування рухом поїздів, алгоритми функціонування яких є найбільш складними. Значною мірою це пояснюється наявністю у колі керування людини-оператора.

На думку авторів для подальших досліджень доцільно обрати метод, який орієнтований на технологію функціонування об’єкта дослідження, а саме станції. Для цього обираємо основну функцію станційних систем – завдання маршрутів для руху поїзда.

Накопичуючи пошкодження технічних засобів, збоїв програмного забезпечення та помилок персоналу можливо підрахувати їх інтенсивності і відповідно імовірність відмови, порушення або безвідмовної (успішної) роботи.

У цьому сенсі принцип моделювання за ознакою "команда" на думку авторів є більш універсальним та значно простішим у реалізації. Крім того цей підхід дозволяє врахувати помилки людини-оператора.

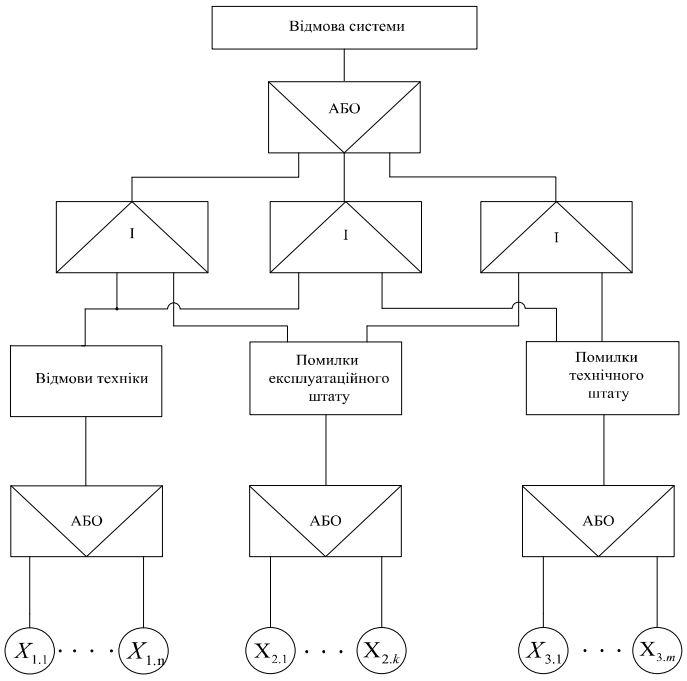

Рис. 1. Дерево безпеки команд керування

Будемо вважати за первинні події характеристики змінних, що визначають безпеку технічних засобів системи: $X_{1.1},\ldots X_{1.n}$; безпеку реалізації команд керування експлуатаційним штатом $X_{2.1},\ldots X_{2.k}$; та безпечну поведінку технічного штату при виконанні робіт з технічного обслуговування $X_{3.1},\ldots X_{3.m}$. Це помилки при виконанні регламентних робіт, порушення термінів виконання, тощо.

Структурна функція безпеки моделі на рисунку 1 матиме вигляд:

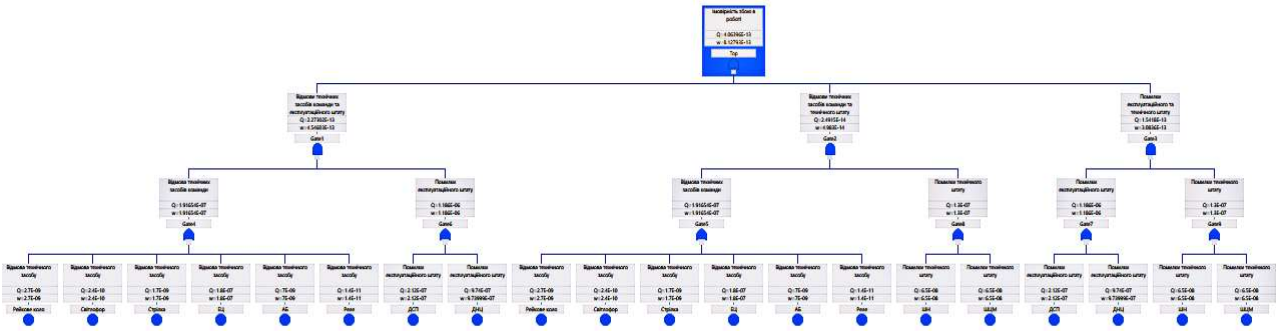

Рис. 2. Структурна функція безпеки моделі, що досліджується

Для проведення дослідження моделі команд використовувалась комп'ютерна програма TopEvent FTA.

При цьому введені такі припущення та обмеження:

– вважається, що потік події є незалежними у сукупності;

– будемо вважати, що поведінка первинних подій дерева описується бінарною логікою за схемою (x_i=1 – подія відбувається; x_i=0 – подія не відбувається).

Результати розрахунків показників надійності та функціональної безпеки, при появі відмови технічного засобу та/або помилки експлуатаційного, технічного штату наведено в таблиці 1.

Таблиця 1

Імовірність настання кінцевої події при відмовах

Характер пошкодження	**Імовірність настання відмови (сумісної відмови)**
Відмова технічних засобів системи	$1.32 \cdot 10^{-6}$
Помилка експлуатаційного штату	$3.22 \cdot 10^{-7}$
Помилка технічного штату	$1.38 \cdot 10^{-6}$

Чисельні значення імовірності настання кінцевої події при помилках технічного штату або відмовах техніки корелюються, у той час як помилка експлуатаційного персоналу має на порядок меншу вагу.

Висновки. Запропонований авторами підхід базується на системному підході до оцінювання стану та ресурсу системи, або окремого компонента при якому для кожного функціонального вузла, або елемента системи синтезується окрема модель його поведінки, й формується статистика відмов на основі об'єктивних даних чорної скриньки та суб'єктивних оцінок експертів. Головним завданням подальшого дослідження є розроблення математичного апарату для формування статистик та вирішення проблеми інтеграції результатів спостережень по кожному компоненту в загальну оцінку.

Література:

1. Голинкевич Т. А. Прикладная теория надежности: учебник для вузов по спец. "Автоматизированные системы управления" / Т. А. Голинкевич. – 2-е изд. перераб. и доп. – М.: Высш. шк., 1985. – 168 с.
2. Хенлі Е.Дж. Надійнісне проектування технічних систем і оцінка ризику / Е.Дж. Хенлі, Х. Кумамато / пер. з англ. за ред. Ю.Г. Зареніна. – К.: Вища школа, гол. вид-во, 1987. – 544 с.
3. ДСТУ 4178-2003. Комплекси технічних засобів систем керування та регулювання руху поїздів. Функційна безпечність і надійність. Вимоги та методи випробовування. – К.: Держспоживстандарт України, 2003. – 32 с.
4. Abd-El-barr M. Design And Analysis of Reliable and Fault-tolerant Computer Systems. – Imperial Collegdge Press, 2006.
5. Lin Huang. Lifetime Reliability for Load-Sharing Redundant Systems with Arbitrary Failure Distributions / Lin Huang, Qiang Xu // Reliability, IEEE Trans. on. – 2010. – Vol. 59, № 2. – P. 319–330