УДК 656.212.5: 681. 3

МОЙСЕЄНКО В.І. професор (УкрДАЗТ);
БУРЯКОВСЬКИЙ С.Г. доцент (УкрДАЗТ).

Інтеграція програмного забезпечення розгалужених телекомунікаційних та інформаційно-керуючих систем

Вступ

На протязі останнього десятиріччя спостерігається значний прогрес у розвитку закордонних і вітчизняних телекомунікаційних та інформаційно-керуючих систем на залізничному транспорті. Прикладом можуть бути мікропроцесорні централізації, сучасні телекомунікаційні системи та системи диспетчерського керування. В цілому визначені напрямки їх структурного, апаратного та програмного синтезу, методи досягнення заданих показників функціонування. Найбільше поширення мають одно, двох, або багатоканальні (мажоритарні) структури. В основі їх побудови знаходяться класичні методи теорії надійності та безпеки.

При створенні апаратних, чи програмних засобів інформаційно-керуючих систем переважна більшість розробників вважає, що виникаючі пошкодження чи збої по своїй природі мають властивості стаціонарності й ординарності, тобто їх можна вважати незалежними. Виходячи з цього припущення формується система кількісних оцінок показників функціонування та методи забезпечення показників надійності й безпеки.

Однак чи можливо у повній мірі вважати незалежними відмови компонентів програмно-апаратних комплексів сучасних систем? Це питання до теперішнього часу знаходиться у дискусійній площині.

Аналіз досліджень та публікацій

Відповідно до [1-4] системи та їх елементи можна віднести до незалежних, якщо відмова одного модуля, чи елемента не приводить до відмови іншого модуля (елемента). Для забезпечення принципу незалежності розробники використовують екранування, заземлення, гальванічне розділення електричних кіл та фізичне розділення елементів і систем, що відносяться до різних каналів, або до різних систем. Слід також зазначити, що фізичне розділення суттєво зменшує вплив так званого «людського чиннику» на показники функціонування.

Аналіз інформаційних та керуючих систем, які у теперішній час експлуатуються на залізничному транспорті безпосередньо вказує на існуючі недоліки. Зокрема переважна більшість апаратних і програмних засобів виконана на одній і тій-же елементній чи програмній базі [4,7,8]. Апаратура каналів знаходиться не тільки у одному приміщенні, а й у одній шафі, тобто у безпосередній близькості.

Слід зазначити, що використання різних типів контролерів, обчислювальних машин, мережевого обладнання від різних виробників ще не є гарантією незалежності їх роботи. Справа у тому, що їх елементна база, способи монтажу є дуже уніфікованими і виробляються, як правило, одними й тими ж фірмами.

Крім того більшість електронної апаратури має практично однаковий строк служби і можна припустити, що інтенсивності відмов їх елементів також буде однаково змінюватися у часі.

Спільність датчиків та виконавчих пристроїв, що територіально концентровані спільною кабельною мережею та технічне обслуговування всіх компонентів електронних виробів одним штатом посилює вплив «людського чинника» й залежність всіх компонентів системи від зо-

внішніх впливів[6, 9]. Тому у науковому плані можна говорити про існування значної кількості відмов з загальної причини.

Ціллю статті

Теоретичне обґрунтування поліпшення експлуатаційних властивостей телекомунікаційних та інформаційно-керуючих систем.

Викладення основного матеріалу

Введення фізичного розділення програмно-апаратних засобів різних каналів та зміна системи їх технічного обслуговування може стати суттєвим невикористаним резервом для підвищення функціональної безпеки системи керування та контролю на залізничному транспорті. Однак виконати ці вимоги при стандартному підході до системного синтезу дуже складно і у переважній більшості випадків неможливо.

Звернемося до технології роботи залізничного транспорту, яка представляє собою єдиний комплекс технологічних операцій, що використовуються на станціях і перегонах. Рух поїздів по ділянках перегону залежить від роботи станцій й відповідно до цього функціонування всіх пристроїв залізничної автоматики також повинно здійснюватися у постійній взаємодії.

Нажаль релейні системи сигналізації, централізації та блокування функціонують здебільше автономно, а їх взаємодія з іншими обмежується тільки самими необхідними зв'язками. У роботах фахівців з безпеки залізничного транспорту, розробників сучасних автоматизованих систем керування, безпосередньо вказується на роль загальної поїзної моделі, що функціонує у масштабі реального часу, для альтернативного визначення місця знаходження рухомої одиниці. Це може суттєво підвищити рівень безпеки руху. Дуже перспективним у цьому класі є використання альтернативних систем і методів визначення ординати рухомого складу на полігоні на основі засобів супутникової навігації.

Традиційно завдання керування рухом поїздів на ділянці залізниці покладались на пристрої диспетчерської централізації (ДЦ). Сучасні системи ДЦ, маючи необмежені інформаційні можливості, можуть створювати й забезпечувати функціонування динамічної поїзної моделі, враховувати всі особливості технологічного процесу (роботи з ремонту, технічного обслуговування, обмеження швидкості, виникаючі пошкодження тощо).

Слід зазначити, що система диспетчерського контролю може фіксувати не тільки пошкодження автоматики, але й пристроїв електроживлення, контактної мережі тощо.

У зв'язку з цим, для зменшення ступеню залежності апаратних і програмних компонентів систем пропонується наступний підхід. У складі технічного, а особливо програмного забезпечення системи керування, передбачається дві основних компоненти: локальну і глобальну. Локальна компонента – це програмно-апаратний комплекс конкретної станції, або іншої системи, що не має принципового значення. Його технічні та програмні модулі вирішують стандартні завдання керування та контролю.

Глобальна компонента системи представлена програмно-апаратним комплексом системи верхнього рівня – глобальна компонента, яка враховує процеси, що відбуваються на всій ділянці керування, рис.1. Система у своєму складі безпосередньо може мати два програмних, або програмно-апаратних модуля: технологічний і модуль безпеки. Технологічний модуль забезпечує реалізацію функцій системи, а модуль безпеки контролює стан безпеки у режимі реального часу.

Рис. 1. Графічна ілюстрація взаємодії програмно-апаратних модулів

Глобальний програмно-апаратний модуль знаходиться у складі системи верхнього рівня. До нього надходить вся необхідна інформація про процеси, що відбуваються на станції, перегоні, переїзді, у пристроях зв'язку, електроживлення, електропостачання, тощо. Формування команд керування відбувається за принципом 2 з 3^x з можливими пріоритетами у разі необхідності. За рахунок такого підходу система набуває деякі ознаки мажоритарності й створюються умови для зменшення залежності компонентів від впливу зовнішніх чинників та людського фактору.

Позначимо через A_1, A_2, A_3 події, що характеризують появу небезпечного створення програм у технологічному програмно-апаратному модулі безпеки. Критерієм небезпечного функціонування є поява небезпечної помилки одночасно у двох програмних каналах, тобто

$$(A_1 \cap A_2) \cup (A_2 \cap A_3) \cup (A_3 \cap A_1). \quad (1)$$

Для подальших перетворень (1) звернемося до структурних функцій виду ($P(A_i) = 1$) – подія існує; ($P(A_i) = 0$) – подія не існує, докладно поданих у [5], тоді рівняння (1) набуде вигляду

$$У_н = 1 - (1 - У_а)(1 - У_в)(1 - У_с), \quad (2)$$

де $У_а, У_в, У_с$ –структурні функції, що характеризують події *A_1, A_2, A_3:*

$$У_а = (У_1 \cdot У_2);\ У_в = (У_2 \cdot У_3);$$
$$У_с = (У_3 \cdot У_1).$$

Після підставлення у (2) значень $У_1, У_2, У_3$ та деяких очевидних перетворень

$$У_н = У_1У_2 + У_2У_3 + У_3У_1 - У_1^2У_2У_3 - У_1У_2^2У_3 - У_1У_2У_{з3}^2 + У_1^2У_2^2У_3^2; \quad (3)$$

Повернувшись до ймовірностей початковий подій *$P(A_1)$, $P(A_2)$, $P(A_3)$* останнє рівняння можна подати так:

$$P_н(A) = P(A_1) \cdot P(A_2) + P(A_2) \cdot P(A_3) + P(A_3)P(A_1) - P^2(A_1)P(A_2)P(A_3) - \quad (4)$$
$$-P(A_1)P^2(A_2)P(A_3) - P(A_1)P(A_2)P^2(A_3) + P^2(A_1)P^2(A_2)P^2(A_3).$$

Складові рівняння (4) фактично відображають всі можливі небезпечні нештатні ситуації, причому $P(A_1) \cdot P(A_2) \cdot P(A_3)$ характеризує появу небезпечного спотворення у всіх трьох каналах.

Глобальний програмний модуль формується на основі віртуальних локальних програмних модулів окремих підсистем керування та контролю диспетчерської дільниці, рис. 2. За рахунок інформаційного поєднання локальних модулів 1, 2, 3,

4 …n з'являються нові якості глобального модуля, які у сукупності були не притаманні первинній інформації. При такому підході отримаємо реальну модель функціонування диспетчерської дільниці, яка потім використовується у роботі окремої підсистеми нижнього рівня (рис. 1 та рис. 2.).

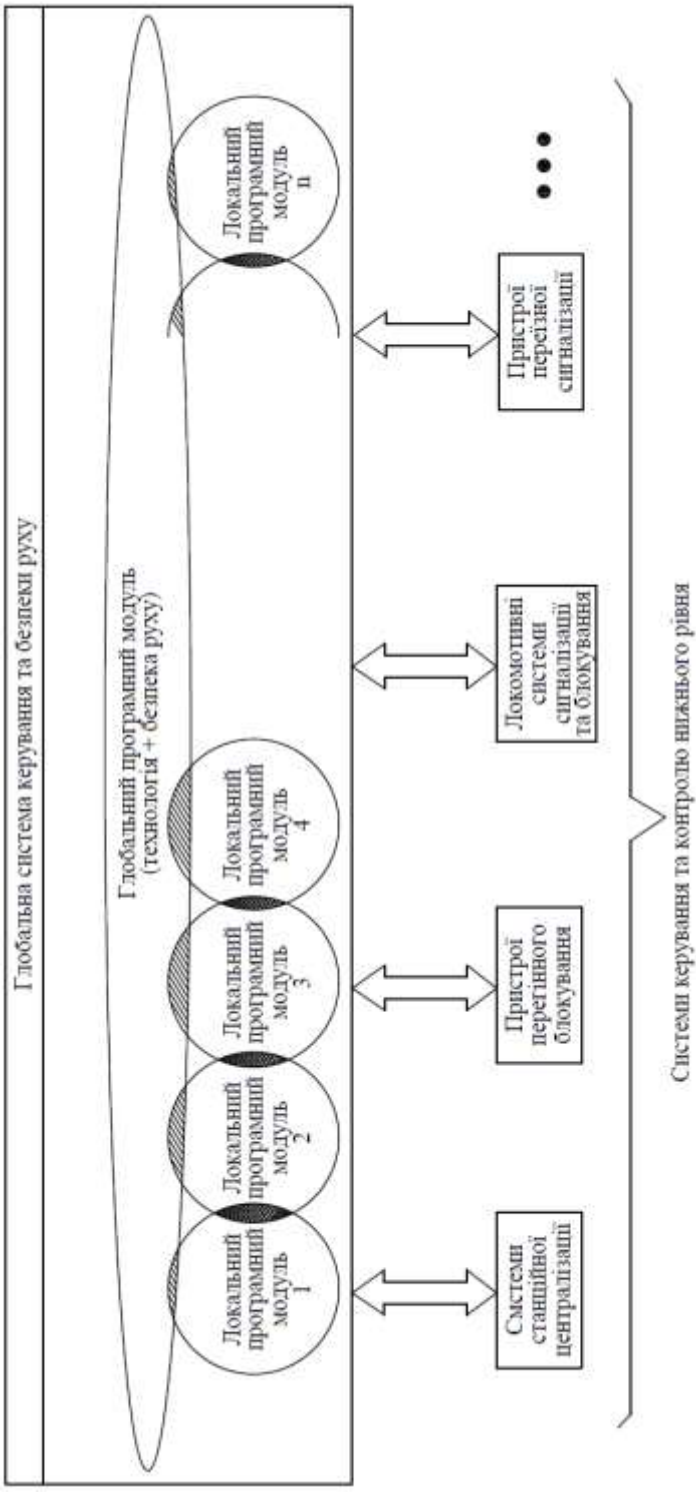

Рис. 2. Структура інформаційної взаємодії глобального модулю з системами нижнього рівня

Основою для прийняття рішення є технологічний модуль та модуль безпеки нижнього рівня. У разі виникнення невизначеності у результатах роботи програмних модулів нижнього рівня, рішення приймаються за схемою порівняння 2 з 3^x. Розглянемо більш докладно змістову частину цих модулів. Технологічний програмно-апаратний модуль забезпечує виконання тільки основних функцій системи керування. Ідентифікуються тільки ті пошкодження та події, які мають відносно простий алгоритм реалізації і не допускають невизначеності у трактуванні їх кінцевих результатів. Таке обмеження у першу чергу пов'язано з вимогами безпеки. Відомо, що всіляке ускладнення алгоритму функціонування збільшує ступінь невизначеності інформації, збільшує витрати на процес аналізу й, відповідно, зменшує рівень безпеки.

З іншого боку без ідентифікації складних подій, якими і є порушення, неможливо забезпечити сучасний рівень вимог до показників функціональної безпечності. Для усунення визначеного протиріччя сформовано програмний модуль безпеки, рис. 3. Він забезпечує ідентифікацію саме складних подій, до яких у першу чергу відносяться такі.

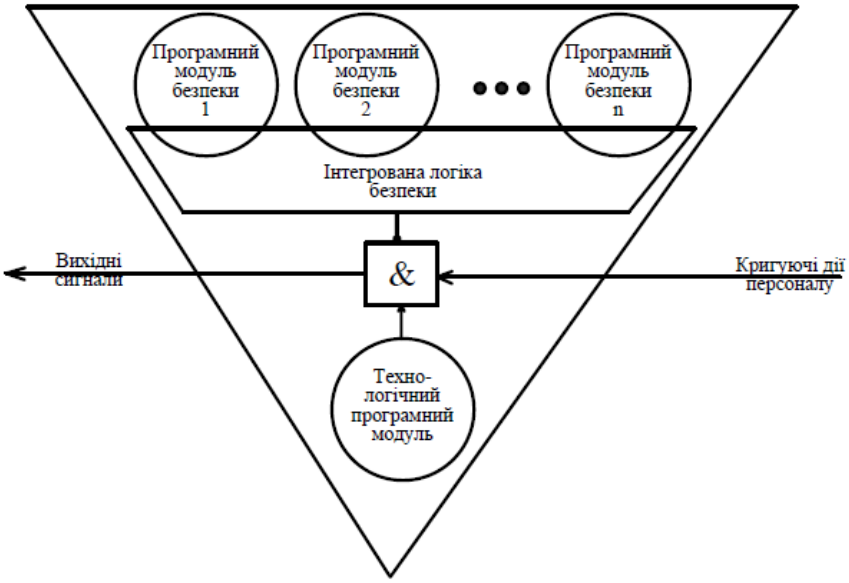

Рис. 3. Структурна організація програмного модулю безпеки

1. Контроль безпеки роботи експлуатаційного штату (чергових по станції, операторів, тощо) та формування сигналів блокування при порушенні регламенту.

2. Контроль роботи технічного штату, а саме:

– контроль регламенту виконання робіт з технічного обслуговування;

– контроль безпеки при виконанні робіт з виключенням пристроїв із залежності;

– контроль безпеки при виконанні відновлювальних робіт;

– контроль безпеки при виконанні ремонтних робіт, особливо робіт у «вікно»;

– забезпечення безпечного ведення робіт на колії, виконання регламентних профілактичних робіт на ділянках з рухом поїздів.

3. Ідентифікацію складних пошкоджень у пристроях та системах керування рухом поїздів, енергопостачання, інших засобах залізничної автоматики.

4. Ідентифікація порушень та окремих транспортних пригод (проїзд черво-

ного вогню світлофора, розріз стрілки, перекриття сигналу з проїздом).

5. Оперативна оцінка стану безпеки руху й видача відповідних рекомендацій персоналу та команд блокування.

Перераховані вище функції позначені у вигляді локальних програмних модулів безпеки 1, 2, …, n. Інтегрована логіка забезпечує оцінку виявлених підсистемами 1-n порушень й формування у разі необхідності блокувальних сигналів. У разі виникнення невизначеної ситуації, або при збоях у роботі локальних програмних модулів, чи інтегрованої логіки застосовується коригуючи дія персоналу. Вона є дуже відповідальною, тому повинна виконуватися як особлива команда, що потребує найбільшої уваги персоналу.

Висновок

Застосування інтегрованої логіки при синтезі територіально розгалужених систем керування та контролю створює принципово нові можливості для покращення показників їх безпеки та експлуатаційної надійності. Крім того з'являється можливість розширення переліку та змісту функцій у системах нижнього рівня за рахунок інтелектуальної підтримки їх рішень на верхньому рівні. Наявність територіального розгалуження окремих компонентів системи дозволить зменшити ступінь їх взаємної залежності.

Список літератури.

1. Александровская Л.Н. Современные методы обеспечения безотказности сложных технических систем / Л.Н. Александровская, А.П. Афанасьев, А.А. Лисов; Учебник. – М.: Логос, 2003. – С. 74–100.

2. Аронов И.З. Обеспечение безопасности сложных технических систем на примере энергоблоков атомных станций / И.З. Аронов, Г.И. Грозовский, Г.В. Маливинский // Надежность и контроль качества. – 1994. – №5. – С.43–49.

3. Вироби електронної техніки. Методи розрахунку надійності: ДСТУ 2992-95. – Введ. 01.01.96. – К.: Вид – во стандартів. 1995. – 78 с.

4. Харченко В. С. Нормирование и оценка безопасности информационных и управляющих систем АЭС (7): Регулирующие требования к программному обеспечению / В. С. Харченко, М. А. Ястребенецкий, В. Н. Васильченко // Ядерная и радиационная безопасность. – 2002. – №1. –С. 18 – 33.

5. Хенли Э. Д. Надежность технических систем и оценка риска / Э. Д. Хенли, Х. Кумамото Пер. с англ. В. С. Сыромятова, Г. С. Деминой под общ. ред. В. С. Сыромятова. – М. : Машиностроение, 1984. – 528 с.

6. Ястребенецкий М. А. Безопасность атомных электростанций. Информационные и управляющие системы / М. А. Ястребенецкий, Васильченко, Ю. В. Розен, С. В. Виноградская и др. Под ред. М. А.Ястребенецкого. – К.: Техніка. – 472 с.

7. Ястребенецкий М. А. Нормирование и оценка безопасности информационных и управляющих систем: Процедура оценки и их информационное обеспечение / М. А. Ястребенецкий, Ю. В. Розен, В. Н. Васильченко // Ядерная и радиационная безопасность. – 2002. – №3. – С. 40 – 57.

8.Стандарт МЭК. Анализ деревьев отказов (Метод вероятностного оценивания риска.) Публикация 1025. – 1-е изд. – М. , 1990. – С 4 – 15.

9. Стандарт EN 50126 CENELEC Спецификация и доказательство надежности, эксплуатационной готовности, ремонтопригодности и безопасности (RAMS) для использования на железных дорогах, 1999. – 73с.

Аннотации:

В статті розглянуті питання захисту програмного забезпечення інформаційно-керуючих систем від збоїв, що мають загальну причину. Зокрема запропоновано підхід при якому окремі програмні модулі виконуються різними технічними засобами загальної інформаційної систем з послідуючим порівнянням результатів їх функціонування.

В статье рассмотрены вопросы защиты программного обеспечения информационно-управляющих систем от искажений, возникающих по общей причине. В частности предложен подход, при котором программные модули системы реализуются разными техническими средствами, разнесенными в пространстве с последующим сравнением полученных результатов.

The article considers the protection of software information management systems of the distortions that arise due to common cause. In particular, a method in which software modules are implemented by various technical means, separated in space and then comparing the results obtained.

УДК 656.212.5:681.3

ПАХОМОВА В.М., к.т.н, доцент (ДНУЗТ);
ПОВОД В.В., студент (ДНУЗТ).

Логічна структуризація інформаційних мереж залізничного транспорту на основі комутаторів ETHERNET

Постановка проблеми

Стратегія інформатизації залізничного транспорту України на сучасному етапі передбачає створення єдиного інформаційного простору при забезпеченні інтеграції автоматизованих систем управління залізничною галуззю [1]. Цілий ряд лінійних підприємств використовує технологію ETHERNET, тому цілком обгрунтованим є подальша масштабованість відповідних мереж. Загальна структура такої гіпотетичної мережі представлена на рис. 1 і припускає поєднання використання двох базових структур - стягнуту в точку магістраль, перевагами якої є висока продуктивність магістралі, а також її протокольна незалежність, і розподілену магістраль, яка скорочує вартість кабельної системи і долає обмеження на відстані [2]. Для з' єднання рівня лінійних підприємств (рівень 1) з рівнем залізниці (рівень 2) використовується FAST ETHER-?ET, для з' єднання рівня залізниці з рівнем Укрзалізниці (рівень 3) - GIGABIT ETHERNET.