УДК 621.396.66

ОЦІНКА ПОКАЗНИКІВ НАДІЙНОСТІ ТА БЕЗПЕЧНОСТІ ІНФОРМАЦІЙНО-КЕРУЮЧОЇ СИСТЕМИ RTP 3000 З ВИКОРИСТАННЯМ RAM COMMANDER

Л.Д. Озірковський
Кандидат технічних наук, доцент*
Контактний тел.: 067-673-34-45
E-mail: l.ozirkovsky@gmail.com
Т.І. Панський*
Контактний тел.: 097-914-37-59
E-mail: panskyy@gmail.com
О.В. Сидорчук*
Контактний тел.: 096-113-88-50
E-mail: sydorchuk90@gmail.com
І.В. Кулик
Аспірант*
Контактний тел.: 098-919-47-70
E-mail: kulyk.ew@gmail.com
*Кафедра теоретичної радіотехніки та радіовимірювання
Національний університет «Львівська політехніка»
вул. С. Бандери, 12, м. Львів, Україна, 79000

В статті приведена методологія оцінки показників безпечності та надійності системи відповідального призначення RTP 3000 за допомогою програмного забезпечення RAM Commander та ASNA

Ключові слова: надійність, безпечність, FMEA/FMECA-аналіз, структурна схема надійності, дерево відмов

В статье приведена методология оценки показателей отказобезопасности и надежности системы ответственного назначения RTP 3000 с помощью программного обеспечения RAM Commander и ASNA

Ключевые слова: надежность, отказобезопасность, FMEA/FMECA-анализ, структурна схема надежности, деревья отказов

1. Постановка задачі

При застосуванні інформаційно-керуючих систем відповідального призначення важливим є забезпечення заданого рівня їх надійності. Однак, особливістю таких систем є те, що необхідно мінімізувати наслідки їх виходу з ладу, що кількісно характеризується показником безпечності (safety – англ., отказобезопасность – рос.). Безпечність – така властивість системи, коли в ній при виході з ладу окремих підсистем чи системи в цілому, не допускається ситуація небезпечна для життя і здоров'я людей та навколишнього середовища. В більшості випадків при оцінці надійності складних систем кількісною оцінкою безпечності (safety) нехтують. Це пояснюється тим, що з одного боку в стандартах з надійності країн СНД моделей і методів для оцінки безпечності немає, а з іншого – забезпечення заданого рівня безпечності потребує зниження, а в окремих випадках і суттєвого, рівня надійності систем. Тому необхідно розробити методологію, яка дає змогу оцінити комплексно як показники безпечності так і надійності. Оскільки задача такої оцінки є трудомісткою і потребує багатократного виконання при проведенні багатоваріантного аналізу складної системи на етапі її системо-технічного проектування, то необхідно також вибрати спеціалізоване програмне забезпечення для такої оцінки.

2. Опис досліджуваної системи

Інформаційно-керуюча система (ІКС) відповідального призначення RTP 3000 призначена для управління процесами та системами безпеки атомних електростанцій, небезпечних виробництв, газо- та нафтотранспортування тощо [1]. Вона може бути використана як в якості автономного контролера безпеки, так і в якості елемента системи управління для ІКС відповідального призначення.

Структурна схема ІКС RTP 3000 приведена на (1) і включає node-процесори, chassis-процесор, модулі вводу/виводу. Ця система реалізована як відмовостійка система з дубльованими модулями вводу та node-процесорами.

Така конфігурація повинна забезпечувати, згідно специфікацій виробника, заданий рівень безпечності та надійності з мінімальним числом модулів. Однак кількісних оцінок безпечності в специфікаціях ІКС, представлених в [1] не виявлено.

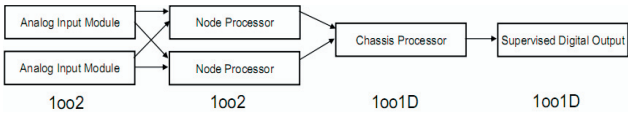

Рис. 1. Структура системи RTP 3000

3. Вибір програмних засобів для оцінки надійності та безпечності

Переважна більшість спеціалізованих програмних засобів (ПЗ) дає змогу здійснити лише оцінку надійності систем [2]. Комплексну оцінку можна отримати за допомогою ПЗ Relex (ReliaSoft) та RAM Commander (A.L.D.), виробники якого є світовими лідерами в цій галузі. Крім цього дане ПЗ враховує моделі та рекомендації з оцінки надійності і безпечності і відповідає вимогам таких стандартів як: MIL-217, MIL-HDBK-217, Telcordia, FIDES, NPRD-95, MIL-STD-1629, CNET 2000, TR332-Bellcore Issue 6, Prism, NSWC-98, GJB299. Ще одним обмеженням при виборі спеціалізованого ПЗ, яке дає можливість оцінити безпечність, є його висока ціна. Ліцензія на продукти фірм ReliaSoft чи A.L.D. становить 12-20 тис. доларів за шт. Оскільки Національний університет «Львівська політехніка» веде співпрацю з A.L.D. [3] і цією фірмою для проведення наукових досліджень і навчального процесу надано 30 ліцензій ПЗ RAM Commander, то в якості інструмента вибрано програмне забезпечення RAM Commander.

4. Формування методології оцінки надійності і безпечності складної системи на основі ПЗ RAM Commander

Оцінка показників надійності та безпечності здійснюється за допомогою методології, яка враховує вимоги міжнародних стандартів і в першу чергу MIL-217, MIL-HDBK-217, Telcordia та FIDES. Згідно їх вимог, на першому етапі, здійснюється побудова дерева системи та попередня оцінка її надійності (Reliability Prediction) без урахування засобів забезпечення відмовостійкості. Необхідність цього кроку викликана потребою оцінки затрат на подальше технічне обслуговування системи. Крім цього, дерево системи є вхідними даними для всіх наступних етапів оцінки надійності та безпечності.

На основі дерева системи будують структурну схему надійності - RBD (Reliability Block Diagram), що дає змогу оцінити середній час між критичними відмовами (MTBCF) та середній час роботи до катастрофічної відмови (MTTF). Структурна схема надійності дає змогу врахувати засоби забезпечення відмовостійкості, зокрема резервування, і відобразити це графічно.

Наступним кроком - здійснюється побудова дерева відмов - FTA (Fault Tree Analysis). На відміну від структурної схеми надійності, яка показує при якій конфігурації система буде працездатною і є аналізом системи знизу догори, дерево відмов дає змогу оцінити кількісно ймовірність виникнення кожної відмови та прослідкувати причину її виникнення, і є дедуктивним методом аналізу надійності. Це один з найбільш розповсюджених методів аналізу надійності складних систем [4], застосування якого не регламентується вітчизняними стандартами, але є обов'язковим згідно вимог, усіх без винятку, міжнародних стандартів з надійності. Аналіз дерева відмов дає змогу визначити різні комбінації відмов, які спричиняють ризик чи відмову системи та оцінити кількісно їх чутливість.

Для оцінки безпечності доцільно використати методи FMEA/FMECA (Failure Mode and Effects Analysis/ Failure Mode Effects and Criticality Analysis)-аналізу, який є систематичною групою методів спрямованих на розпізнавання й оцінку потенційної відмови системи чи процесу і наслідків цієї відмови, ідентифікацію дій, які можуть усунути чи знизити імовірність виникнення потенційної відмови. В результаті аналізу отримують показник ризику – RPN (Risk Priority Number), який характеризує безпечність системи. Якщо показник ризику не перевищує 80, згідно рекомендацій більшості стандартів, то рівень безпечності є задовільним. Якщо значення показника є більше 80, то необхідно здійснити заходи по зменшенню ризику - повторно здійснити аналіз дерев відмов та FMEA/FMECA-аналіз. Цей процес є ітеративним і може потребувати значних часових затрат.

5. Оцінка надійності та безпечності ІКС RTP 3000 на основі розробленої методології з використанням RAM Commander

Розрахунок показників надійності за допомогою структурної схеми надійності. Для визначення імовірності безвідмовної роботи та середнього часу напрацювання до відмови необхідно побудувати графічну модель надійності - структурну схему надійності (ССН) [6]. У відповідності до структури (1) вона буде складатися з двох паралельно з'єднаних вхідних модулів, двох паралельно з'єднаних процесорів вузла, шасі процесора та вихідного модуля. Структурну схему надійності ІКС RTP 3000, розроблену в середовищі RAM Commander приведено на рис. 2.

На основі створеної ССН в RAM Commander можна отримати наступні показники надійності: залежність імовірності безвідмовної роботи від часу та середнє напрацювання до критичної відмови (MTBCF).

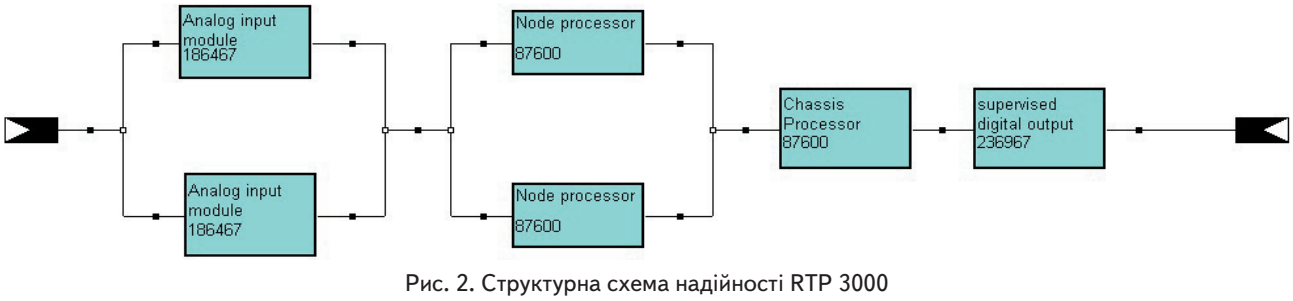

Рис. 2. Структурна схема надійності RTP 3000

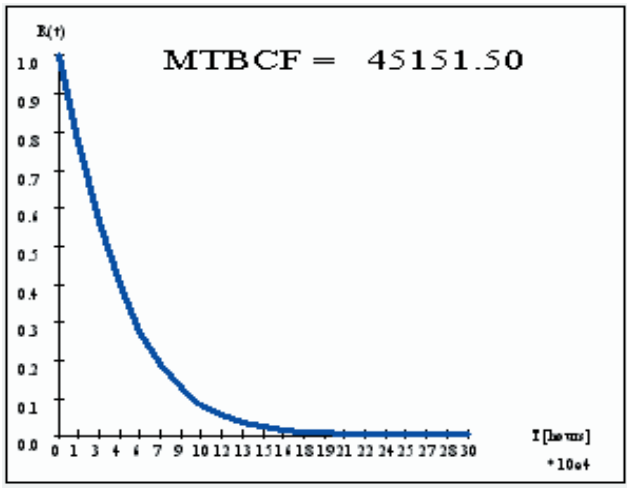

Рис. 3. Залежність імовірності безвідмовної роботи від часу

Для верифікації отриманих результатів розроблено структурно-автоматну модель (САМ) системи RTP 3000 за технологією [5]. Побудова структурно-автоматної моделі здійснюється на основі вербальної моделі, яка задає вхідні дані у вигляді переліку базових подій, умов і обставин, при яких ці події відбуваються. При розробці структурно-автоматної моделі необхідно вирішити наступні задачі: сформувати вектор станів; визначити множину формальних параметрів моделі; описати поведінку системи у вигляді базових подій, які відбуваються у системі, а також умов і обставин при яких відбуваються ці події; сформувати формули розрахунку інтенсивностей переходів із стану в стан; сформувати формули розрахунку ймовірностей альтернативних переходів; встановити правила модифікації компонент вектора станів.

Наступним кроком є побудова моделі системи у вигляді графа станів і переходів. Інструментом для отримання показників надійності, а саме: залежності імовірності безвідмовної роботи від часу та середнього часу напрацювання системи до відмови, є програмне забезпечення ASNA. Це програмне забезпечення використовує САМ як вхідні дані і автоматизовано формує граф станів і переходів, складає систему диференційних рівнянь Колмогорова-Чепмена (Марковська модель), здійснює її розв'язок і на основі отриманого розподілу ймовірностей перебування у станах, формує показники надійності досліджуваної системи [6], які представлені в рис. 4.

Побудована модель системи RTP 3000 в програмному модулі ASNA дає змогу зробити висновок про адекватність моделі в цілому.

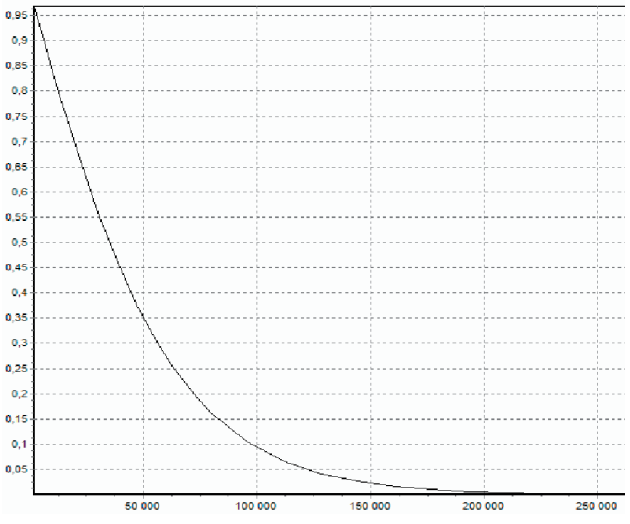

Рис. 4. Залежність імовірності безвідмовної роботи від часу

Розрахунок показників надійності за допомогою дерева відмов. Дерево відмов – це графічне представлення подій в ієрархічній структурі типу дерева. Воно використовується для визначення різних комбінацій відмов апаратного та програмного забезпечення і помилок, викликаних «людським чинником», які виливаються в певний ризик або відмову системи. На вершині дерева знаходиться відмова системи [4]. Решта частина дерева представляє собою паралельні або послідовні події, які потенційно можуть призвести колізії або відмови.

В найнижчих елементах дерева вказується їхня імовірність відмови і далі програмне забезпечення RAM Commander розраховує загальну імовірність відмови системи.

Дерево відмов ІКС RTP 3000 представлено на рис. 5.

Аналізуючи дерево відмов, визначено такі мінімальні перерізи, які показують послідовність відмов яких елементів найбільше впливає на надійність всієї системи.

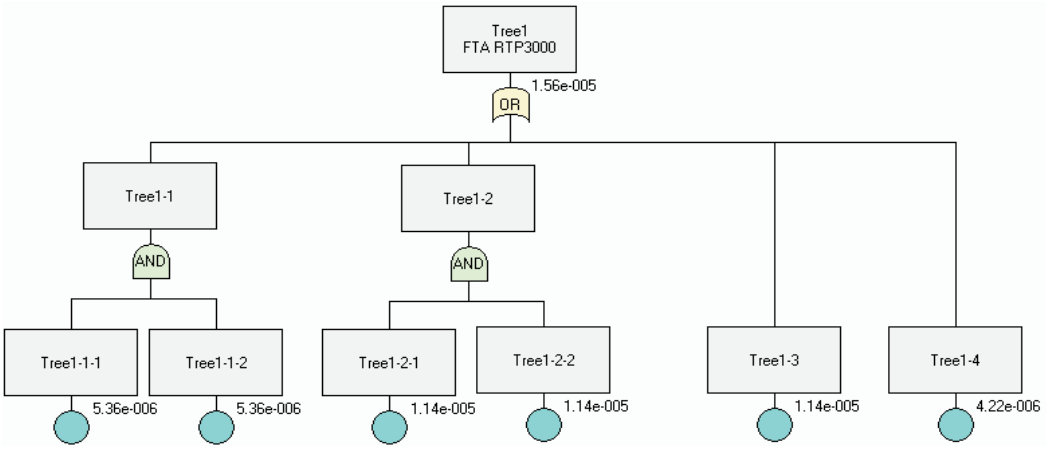

Рис. 5. Дерево відмов (FTA)

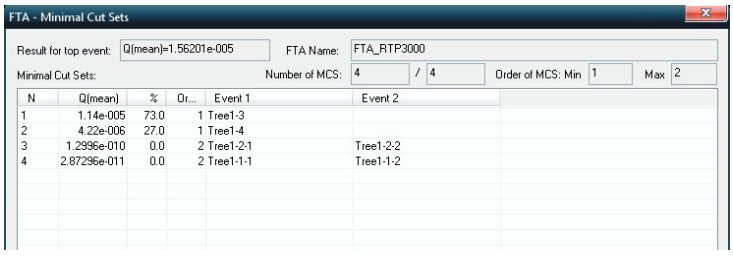

Рис. 6. Мінімальні перерізи

Розрахунок показників надійності за допомогою FMEA/FMECA. На основі дерева відмов проводиться FMEA/FMECA-аналіз [7]. Він дозволяє розрахувати показник безпечності. Для оцінки безпечності системи визначається показник Risk Priority Number (RPN):

RPN = S·O·D,

де S – Severity (оцінка серйозності наслідку потенційного виду відмови), O – Occurrence (оцінка імовірності того, що окрема причина виникає і виливається у відмову), D – Detection (це оцінка імовірності того, що дані засоби управління виявляють відмову). Кількісно RPN має бути менше 80, а для системи відповідального призначення не більше 60. Результати FMEA/ FMECA аналізу, проведеного в RAM Commander представлено в табл. 1

6. Висновки

Представлена методологія дає змогу оцінити показники ефективності складних радіоелектронних систем з використанням спеціалізованого програмного забезпечення RAM Commander та ASNA. На відміну від існуючих, розроблена методологія, дозволяє отримати як показники надійності, так і показники безпечності складної системи.

Для здійснення такої оцінки необхідно вирішити наступну послідовність задач:

- побудувати дерево складної системи для попередньої оцінки надійності;
- розробити модель надійності у вигляді структурної схеми надійності;
- розробити модель надійності у вигляді дерева відмов;
- здійснити верифікацію розроблених моделей за допомогою структурно-автоматної моделі;
- на основі розроблених моделей провести оцінку безпечності складної системи з використанням FMEA/FMECA-аналізу.

Розроблена методологія була апробована на прикладі оцінки показників безпечності та надійності системи відповідального призначення RTP 3000.

Таблиця 1

Результати FMEA/FMECA аналізу

№	Potential FM	End Effect of Failure	Result Severity	Result Occurrence	Result Detection	Result RPN
1	Failure supervised digital output	System failure	10	1	3	30
2	Failure chassis processors	System failure	10	2	2	40
3	Failure 2 node processors	System failure	10	2	2	40
4	Failure 2 analog input moduls	System failure	10	1	2	20

Література

1. RTP corporation [Електронний ресурс] – Режим доступу: \www/ URL: http://www.rtpcorp.com/.
2. А. Строганов. Обзор программных комплексов по расчёту надёжности сложных технических систем. / А. Строганов, В. Жаднов, С. Полесский. // «Компоненты и технологии», № 5 (70), 2007. - с. 74-81.
3. A.L.D. Advanced logistics development [Електронний ресурс] – Режим доступу: \www/ URL: http://www.aldservise.com/en/reliability-products/rams-software.html.
4. Henley E., and H. Kumamoto. 1981. Reliability Engineering and Risk Assessment. Englewood Cliffs, N.J.: Prentice Hall.
5. Волочій Б.Ю. Технологія моделювання алгоритмів поведінки інформаційних систем/ Б.Ю. Волочій. -Львів: Вид-во НУ"Львівська політехніка", 2004. - 220с.
6. Половко, А.М. Основы теории надежности [Текст] / А.М. Половко, С.В. Гуров. - СПб.: БХВ-Петербург, 2006. - 702 с.
7. Николаева Н.Г. FMEA – анализ видов и последствий отказов [Текст]: учеб, пособие/ Н.Г. Николаева, С.М. Горюнова – К.: КГТУ, 2007. – 96с.

Abstract

The article includes the methodology for estimation of safety indexes and reliability responsible destination system RTP 3000. Was selected the appropriate software. Estimation of reliability and safety indexes was performed using software RAM Commander. This software takes into account the model and recommendations for estimation of reliability and safety and meets the requirements such standards as: MIL-217, MIL-HDBK-217, Telcordia, FIDES, NPRD-95, MIL-STD-1629, CNET 2000, TR332-Bellcore Issue 6, Prism, NSWC-98, GJB299. Verification of the system was carried out in the software module ASNA. The article includes the description of object and application in different industrial areas. Step by step methodology was selected for estimation the system safety index, starting from reliability block diagram (RBD), fault tree analysis (FTA), which gives the opportunity to build Failure Mode and Effects Analysis (FMEA). Calculated RPN value satisfies the boundary conditions

Keywords: *reliability, safety, FMEA, realiability block diagram, fault tree*