УДК 656.25

ВИБІР НАПРЯМІВ ГАРМОНІЗАЦІЇ НОРМАТИВНОЇ БАЗИ З МІЖНАРОДНИМИ СТАНДАРТАМИ З ПИТАНЬ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ

Клюєв С.О.

DIRECTIONS CHOICE OF NORMATIVE BASE HARMONIZATION WITH INTERNATIONAL STANDARDS ON FUNCTIONAL SAFETY PROBLEMS

Kliuiev S.

У статті розглянуто параметри безпеки в ході всього циклу існування системи, включаючи етапи розробки, підтвердження безпеки, монтажу, експлуатації та виведення з експлуатації. В якості технічної основи для підтримки забезпечення функціональної безпеки міжнародними та європейськими стандартами розглянуто використання поетапної структури, заснованої на життєвому циклі аналізованої системи. В загальному вигляді визначені рекомендації по використанню певних методів і заходів для методологічної підтримки функціональної безпеки в нормативних документах галузі, і стосуються в основному доказу безпеки систем.

Ключові слова: *нормативні документи, функціональна безпека, міжнародні стандарти, життєвий цикл, поетапна структура, гармонізація.*

Вступ. Збільшення обсягів використання мікропроцесорів в поєднанні зі зміною принципів обробки і передачі даних призводить до значних змін систем управління і забезпечення безпеки залізничних перевезень. Досягти високих вимог з безпеки стислі можна тільки при наявності сучасної нормативної бази, яка регламентує: обсяг організаційно-технічних заходів і порядок їх виконання; структуру і обсяг документації необхідної для відображення достатньої інформації; коло осіб і організацій, що беруть участь в прийнятті рішень про функціональну безпеки, порядок їх взаємодії і взаємної відповідальності [1, 2].

Постановка проблеми. Під керівництвом IEC (International Electrotechnical Commission) були розроблені нормативні документи IEC 61508 [3], що встановлюють загальний підхід до всіх видів діяльності і спрямовані на досягнення функціональної безпеки для систем містять електричні, електронні, програмовані електронні компоненти, які використовуються для виконання функцій безпеки. До таких компонентів можна віднести компоненти входять до складу існуючих і розроблюваних стислі. Розроблені нормативні документи дають можливість зрозуміти в якому напрямку і за допомогою яких кроків можна створювати безпечні складні системи для великого числа практичних застосувань. Однак їх не можна використовувати як однозначне керівництво до дії в застосуванні до питань безпеки залізничних перевезень. Нормативні документи, розроблені IEC, носять рекомендаційний характер.

Аналіз останніх досліджень і публікацій. Розробку норм по функціональної безпеки на міжнародному рівні здійснює IEC, а в межах країн Європейського союзу, стосовно безпеки руху, зв'язку та інших пристроїв сигналізації - CENELEC (European Committee for Electrotechnical Standardization).

Для визначення умов ефективного досягнення безпеки систем управління рухом, зв'язку та інших пристроїв сигналізації, під керівництвом CENELEC були створені такі основні норми:

- застосування на залізничному транспорті - Специфікація і демонстрація надійності, експлуатаційної готовності, ремонтопридатності і безпеки (RAMS) (EN 50126) [4];
- застосування на залізничному транспорті – Програмне забезпечення для систем управління і забезпечення безпеки на залізничному транспорті (EN 50128) [5];
- застосування на залізничному транспорті - Електронні системи, пов'язані із забезпеченням безпеки, призначені для сигналізації (EN 50129) [6];
- застосування на залізничному транспорті - Системи зв'язку сигналізації та обробки даних (EN 50159) [7].

Перераховані стандарти засновані на міжнародних нормах IEC 61508 [3], а також національних директивах в області безпеки, таких як MIL-STD-882 (військовий стандарт США) [8], Def Stan 00-55 (00-56) (військові стандарти Великобританії) [9, 10], Mü 8004 [11] (керівні вказівки Німецьких залізниць)

і вимагають обов'язкового виконання своїх положень.

Мета статті. Аналіз стану та визначення напрямів гармонізації міжнародної та галузевої нормативної бази з функціональної безпеки систем залізничної автоматики і телемеханіки.

Основний зміст. Для проведення порівняльного аналізу підходів до функціональної безпеки сучасних міжнародних нормативних документів та існуючих галузевих стандартів виділимо актуальні, з власної точки зору, напрямки:

- існуючі принципові відмінності в підходах;
- структура організації процесу забезпечення функціональної безпеки;
- методологічна підтримка заходів для досягнення функціональної безпеки;
- технологічна підтримка розробки безпечних систем;
- документальний супровід процесу розробки.

Перш за все, необхідно відзначити, що міжнародні та європейські нормативні документи IEC 61508 [3], CENELEC вперше пропонують використовувати для аналізу систем критичних до безпеки заснований на ризиках підхід. Це означає, що критерії безпеки встановлюються в залежності від відповідних ризиків. Заснований на ризики підхід або концепція ризику - це комбінація двох елементів: ймовірності, з якою відбувається подія або група подій, що призводять до небезпеки і наслідків небезпечних подій. Залежно від імовірності відмов системи або її елемента і категорії ризику стандартами для досягнення економічної доцільності, при якій витрати на забезпечення безпеки не повинні перевищувати вимоги поставленого завдання, введені чотири класи безпеки. Найбільш високі вимоги пред'являє клас 4, до якого відносяться, наприклад, системи централізації. Нижчий клас 1 виділений для найпростіших додатків з відповідальними функціями. Додатки, які не впливають на безпеку, віднесені до класу 0. Належність до того чи іншого класу безпеки залежить від того, наскільки важкими можуть бути пов'язані з керованим процесом виникненню небезпечних ситуацій, як часто вони можуть виникати, а також від бажаного рівня безпеки [12].

В якості технічної основи для підтримки забезпечення функціональної безпеки міжнародними та європейськими стандартами рекомендується використовувати поетапну структуру, засновану на життєвому циклі аналізованої системи.

Для кожного етапу нормативні документи визначають цілі і завдання, вимоги, які є необхідною умовою досягнення цілей і завдань етапу, способи і методи виконання вимог етапу.

Доказом того, що процес забезпечення функціональної безпеки йде відповідно до певних вимог, служать процедури верифікації, атестації та експертизи, що розробляється. Процедура верифікації виконується на кожному етапі життєвого циклу розроблюваної системи. Вона призначена для доказу виконання завдань, визначених на попередньому етапі, і дозволяє при будь-деталізації завдання дотримуватися основної концепції безпеки. Процедура експертизи проводиться для визначення правильності завдання рівня безпеки аналізованої системі.

Важливою особливістю такого підходу, є те, що він вимагає розгляду параметрів безпеки в ході всього циклу існування системи, включаючи етапи розробки, підтвердження безпеки, монтажу, експлуатації та виведення з експлуатації.

Такий підхід, при якому для досягнення безпеки розроблюваної системи використовується не тільки тестування кінцевого продукту на відповідність вимогам, що пред'являються, а й перевірка самого процесу розробки, дозволяє отримувати більш ефективні результати при створенні систем критичних до безпеки, що підтверджується реальним практичним досвідом зарубіжних фахівців (Японія, Німеччина).

Прийнятий в даний час в галузі підхід до структури розробки систем критичних до безпеки заснований на порядку формування документації супроводу створюваних систем. Концепція безпеки в цьому випадку полягає в доказі безпеки аналізованої системи методами тестування (аналітичного, експериментального, імітаційного і т.д.). гармонізації з міжнародними стандартами в цьому напрямку можна досягти шляхом поетапного переходу до рекомендованої міжнародними нормами структурі процесу забезпечення функціональної безпеки. Вимоги щодо формування додаткової документації, яка визначається процесом, вводяться в існуючу структуру. На наступному етапі здійснюється повний перехід до порядку і обсягом формування регламентованої міжнародними стандартами документації.

Відповідно до заданого класом безпеки методи і заходи, що застосовуються на різних рівнях життєвого циклу системи, в цих документах поетапно посилюються для різних додатків - від щодо некритичних систем до систем з високими вимогами до безпеки. Допустимі процедури і критерії, організовані таким чином, що для перевірки пропонується кілька рівноцінних технологій і методів.

Рекомендації по використанню певних методів і заходів для методологічної підтримки функціональної безпеки в нормативних документах галузі визначені в загальному вигляді, і стосуються в основному доказу безпеки систем. Крім цього застосовуються в галузі методи докази функціональної безпеки на основі схематичного аналізу відмов апаратури, стендових випробувань, імітаційного моделювання відмов складових пристроїв, розрахунків імовірності небезпечного відмови апаратури, широко апробовані для стиснення на релейних компонентах, і недостатньо орієнтовані на доказ безпеки складних програмованих систем. Напрямок вдосконалення і гармонізації методологічної підтримки процесу забезпечення функціональної безпеки полягає, з нашої точки зору, по-перше, в прийнятті структури формування рекомендацій щодо використання методів і заходів, в залежності від пропонованих до системи

вимог безпеки, по-друге, в прийнятті до використання сучасних методів аналізу, розробки та перевірки правильного функціонування, як апаратури, так і, в першу чергу, програмного забезпечення, і, потретє, використання власних напрацювань в цій галузі, наприклад, розроблені під ВНІІАС України: методи аналізу систем на основі напівмарковських методів; методи прискорених натурних випробувань; методи імітаційного моделювання на безпеку складних мікропроцесорних систем з використанням прикладного математичного пакету MATLAB [13].

У плані технологічної підтримки міжнародні та європейські стандарти не пропонують конкретних рішень виконання поставлених вимог безпеки. Тому в рамках технологічної підтримки функціональної безпеки при розробці нових нормативних документів слід орієнтуватися на багатий досвід фахівців галузі з розробки ефективних, оригінальних схематичних рішень забезпечення функціональної безпеки.

Однією з основних проблем при гармонізації є питання про необхідність переходу до нового підходу до формування документації супроводу створюваної системи. Обсяг необхідної документації суттєво збільшується, тому що на кожному етапі життєвого циклу формується вихідна документація етапу, і крім цього формується документ «Доказ безпеки». За оцінками зарубіжних фахівців процес переходу є досить трудомістким, вимагає великих затрат часу, але в кінцевому підсумку виправдовує такі витрати.

Таким чином в порівнянні з колишніми інструкціями по розробці критичних до безпеки систем в стандартах IEC, CENELEC з'явився ряд змін серед яких такі: - введення нового підходу заснованого на оцінці ризиків; - регламентація ієрархічно структурованих заходів на кожному етапі процесу розробки для різних рівнів вимог до безпеки; - визнання недостатності тестування для повного підтвердження безпечної роботи; - не тільки регламентація процесу розробки (від постановки завдання до результуючого продукту, включаючи тестування), але і його перевірка на основі результатів окремих етапів.

Для ефективного вирішення завдання гармонізації з міжнародними стандартами при розробці нового покоління галузевих нормативних документів, необхідно: регламентувати поетапний перехід до структури процесу забезпечення функціональної безпеки; прийняти форму рекомендацій використання методів і заходів в залежності від вимог безпеки до системи; використовувати досвід зарубіжних і вітчизняних фахівців в методичній підтримці досягнення безпеки; при виборі рекомендації по використанню технологічних рішень орієнтуватися на напрацювання фахівців галузі в цій області.

В якості практичного прикладу вирішення завдання гармонізації з міжнародними стандартами, можна навести досвід зі створення нових керівних принципів для залізничних систем Японії [14].

Керівні принципи об'єднують умови управління безпекою та технічні заходи протягом усього терміну служби. Регулювання при цьому не передбачається.

Керівні принципи включають в себе необхідні технічні умови, розроблені в рамках залізничних систем Японії на основі IEC 61508 [3].

Основний текст принципів не встановлює будь-яких конкретних, заходів або цілей, виражених цифровими показниками, але для пояснення вони даються в таблицях відповідно до IEC 61508 [3].

Керівні принципи, відповідно до положень, зазначених вище, узгоджуються з IEC 61508 [3], що визначають правила для комп'ютеризованих систем безпеки загального призначення і стосуються необхідних умов забезпечення роботи систем захисту залізничних перевезень.

Висновок. Аналіз стану міжнародної та галузевої нормативної бази з функціональної безпеки систем залізничної автоматики і телемеханіки показав необхідність створення нового покоління галузевих нормативних документів, які гармонізують з міжнародними стандартами і забезпечують безпечну експлуатацію і конкурентоспроможність вітчизняних систем залізничної автоматики.

Для ефективного вирішення завдання гармонізації з міжнародними стандартами при розробці нового покоління галузевих нормативних документів, необхідно:

- регламентувати поетапний перехід до структури процесу забезпечення функціональної безпеки;

- прийняти форму рекомендацій використання методів і заходів в залежності від вимог безпеки до системи;

- використовувати досвід зарубіжних і вітчизняних фахівців в методичній підтримці досягнення безпеки;

- при виборі рекомендації по використанню технологічних рішень орієнтуватися на напрацювання фахівців галузі в цій області.

Література

1. Клюєв С.О. Підвищення безпеки руху на залізниці. Вісник СНУ ім. В. Даля. Сєвєродонецьк, 2016. № 1 (225). С. 104–107.
2. Клюєв С.О. Підвищення безпеки систем залізничної автоматики і телемеханіки / С.О. Клюєв // Збірник наукових праць державного університету інфраструктури та технологій. Серія "Транспортні системи і технології". – Київ: ДУІТ. – 2018. – Вип. № 32 (Т.2). – С. 32–40.
3. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 2000.
4. CENELEC EN 50126: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 1998.
5. CENELEC EN 50128: Railway Applications - Communications, signaling and processing systems - Software for Railway Control and Protection Systems. 2000.
6. CENELEC EN 50129: Railway Applications - Safety-related Elec-tronic Systems for Signalling. 2000.

7. CENELEC 50159-1/-2: Railway Applications - Communications, signaling and processing systems - Safety-related communication in open/closed communication systems. 2001.
8. MIL-STD-882: System Safety Program Requirements. Department of Defense (US). 1993 (version C). 2000 (version D).
9. Def Stan 00-55: Safety Management Requirements for Defence System. Ministry of Defence (UK). 1996.
10. Def Stan 00-56: Requirements for Safety Related Software in De-fence Equipment. Ministry of Defence (UK). 1997.
11. Mü 8004: Anweisung zu den technischen Anforderungen fur die Zulassung von Sicherungsanlagen (Principles of Technical Approval for Signalling and Communications Technology; in German). Federal German Railways Office (EBA). 1988.
12. Braband J., Lennartz A.; Systematic Process for the Definition of Safety Targets for Railway Signalling Applications/ Signal + Draht. - 1999. - №9.
13. Розенберг Е.Н., Шубинский И.Б. Методы и модели анализа функциональной безопасности технических систем. - М.: ВНИИАС, 2004.
14. RTRI: Safety guidelines for computerized train control and protection systems (in Japanese). 1996.

R e f e r e n c e s

1. Kliuiev, S. O. (2016). Pidvyshchennia bezpeky rukhu na zaliznytsi. Visnyk SNU im. V. Dalia. Sievierodonetsk, 1 (225), 104–107.
2. Kliuiev, S. O. (2018). Pidvischennya bezpeki sistem zaliznichnoyi avtomatiki i telemehaniki. Zbirnik naukovih prats derzhavnogo universitetu Infrastrukturi ta tehnologiy. Seriya "Transportni sistemi i tehnologiyi". Kiyiv, DUIT, 32 (T.2), 32–40.
3. IEC 61508 (2000): Functional safety of electrical/electronic/programmable electronic safety-related systems.
4. CENELEC EN 50126 (1998): Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
5. CENELEC EN 50128 (2000): Railway Applications - Communications, signaling and processing systems - Software for Railway Control and Protection Systems.
6. CENELEC EN 50129 (2000): Railway Applications - Safety-related Elec-tronic Systems for Signalling.
7. CENELEC 50159-1/-2 (2001): Railway Applications - Communications, signaling and processing systems - Safety-related communication in open/closed communication systems.
8. MIL-STD-882 (2000): System Safety Program Requirements. Department of Defense (US), version D.
9. Def Stan 00-55 (1996): Safety Management Requirements for Defence System. Ministry of Defence (UK).
10. Def Stan 00-56 (1997): Requirements for Safety Related Software in Defence Equipment. Ministry of Defence (UK).
11. Mü 8004 (1988): Anweisung zu den technischen Anforderungen fur die Zulassung von Sicherungsanlagen (Principles of Technical Approval for Signalling and Communications Technology; in German). Federal German Railways Office (EBA).
12. Braband J., Lennartz A. (1999). Systematic Process for the Definition of Safety Targets for Railway Signalling Applications / Signal + Draht, 9.
13. Rozenberg E.N., Shubinskiy I.B. (2004). Metodyi i modeli analiza funktsionalnoy bezopasnosti tehnicheskih sistem. M, VNIIAS.
14. RTRI (1996): Safety guidelines for computerized train control and protection systems (in Japanese).

Клюев С.О. С Выбор направлений гармонизации нормативной базы с международными стандартами по вопросам функциональной безопасности.

В статье рассмотрены параметры безопасности в ходе всего цикла существования системы, включая этапы разработки, подтверждения безопасности, монтажа, эксплуатации и вывода из эксплуатации. В качестве технической основы для поддержки обеспечения функциональной безопасности международными и европейскими стандартами рассмотрено использование поэтапной структуры, основанной на жизненном цикле рассматриваемой системы. В общем виде определены рекомендации по использованию определенных методов и мер по методологической поддержки функциональной безопасности в нормативных документах отрасли, и касаются в основном доказательства безопасности систем.

Ключевые слова: *нормативные документы, функциональная безопасность, международные стандарты, жизненный цикл, поэтапная структура, гармонизация.*

Kliuiev S. Directions choice of normative base harmonization with international standards on functional safety problems.

The article discusses the safety parameters during the entire life cycle of the system, including the stages of development, confirmation of safety, installation, operation and decommissioning. As a technical basis for supporting the provision of functional safety by international and European standards, the use of a phased structure based on the life cycle of the system under consideration has been considered. In general, recommendations on the use of certain methods and measures for the methodological support of functional safety in the industry regulatory documents are defined, and mainly relate to evidence of system safety.

Analysis of the international and sectoral regulatory framework for the functional safety of railway automation and remote control systems has shown the need to create a new generation of industry regulatory documents that harmonize with international standards and ensure the safe operation and competitiveness of domestic railway automation systems.

To effectively address the task of harmonization with international standards in the development of a new generation of industry regulatory documents, it is necessary to regulate a phased transition to the structure of the process of ensuring functional safety.

Keywords: *regulatory documents, functional safety, international standards, life cycle, phased structure, harmonization.*

Клюєв С.О. – к.т.н., доц. кафедри «Логістичне управління та безпека руху на транспорті» СНУ ім. В. Даля, м. Сєвєродонецьк, e-mail: sergistreet@gmail.com.

Рецензент: д.т.н., проф. ***Чернецька-Білецька Н.Б.***

Стаття подана 15.04.2019