УДК 004.942:827

Лифар В. О., Лифар О. К., Рязанцев А. О., Герасименко К.Є.

МЕТОДИ ОЦІНКИ РІВНІВ SIL ПРИ РОЗРОБЦІ ВИМОГ ДО ПОВНОТИ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ЕЛЕКТРИЧНИХ /ЕЛЕКТРОННИХ/ ПРОГРАМОВАНИХ ЕЛЕКТРОННИХ СИСТЕМ

Представлені методи визначення інтегральних рівнів безпеки при розробці вимог до електричних, електронних, і програмованих електронних систем автоматизованих систем управління, які використовуються в безперервних виробництвах підвищеної небезпеки. Пропонується використовувати метод визначення типів наслідків відмов елементів при проведенні FMEA аналізу, який дозволяє консервативно і уніфіковано провести поділ частот відмов окремих елементів досліджуваних блоків і модулів обладнання, для якого проводиться сертифікація, за типами відмов і отримати інтегральні показники рівня повноти безпеки.
***Ключові слова**: Safety integrity level, рівень повноти безпеки, електронні програмовані пристрої, надійність, безпека.*

1. Актуальність досліджень.

Проблеми забезпечення функціональної безпеки в безперервних керованих виробництвах вирішуються різними методами управління рівнем безпеки, які регламентовані і представлені різними стандартами [1-4].

В основі стандартів закладено припущення про існування процесів, що створюють загрозу безпеці, що виявляється при поєднанні відмов або поломок в технологічному процесі. Таким чином, стандарт дозволяє аналізувати порушення в процесах і відмови системи і здійснювати системне і засноване на рівнях ризики управління рівнем безпеки.

Незважаючи на докладний опис в стандартах процесів оцінки рівня повноти безпеки автоматизованих систем управління технологічних процесів (АСУТП), центральною частиною яких є комп'ютерні інтегровані апаратні засоби, забезпечені спеціалізованим програмним забезпеченням, значні труднощі відчувають розробники таких систем при оцінці ризику і оцінки повноти інтегрального рівня безпеки (SIL - Safety integrity level) з метою приведення розробок керуючих систем до нормативних вимог і сертифікації апаратно-програмних засобів, що виготовляються і просуваються на ринках автоматизованих систем управління технологічними процесами.

2. Постановка проблеми.

Стандарти передбачають необхідність розробки функцій безпеки, які знижують рівень ризику. Функції безпеки в сукупності утворюють «інструментальну систему безпеки» (Safety Instrumented Systems - SIS). Однак для розробників різних електричних / електронних / програмованих електронних (Е/Е/ПЕ) систем, які лежать в основі АСУТП суттєвою проблемою є саме визначення функцій безпеки, так як функціональні можливості Е/Е/ПЕ систем не мають очевидного зв'язку з небезпечними наслідками відмов елементів таких систем. У даній роботі пропонується метод і критерії визначення небезпечних, безпечних і таких, що не впливають на безпеку відмов, а також методи визначення рівня діагностування відмов і кількісних показників надійності елементів обладнання Е/Е/ПЕ систем.

Другорядною метою стандарту [1-3] є створення умов для розробки електричних, електронних і програмованих електронних систем забезпечення безпеки для галузей, в яких відповідні стандарти відсутні. Такі вказівки другого рівня в безперервних виробництвах розглядаються в міжнародному стандарті [4]. У стандарті [4], 3.2.25 наводиться таке визначення: «Функціональна безпека є частиною загальної безпеки, що стосується системи забезпечення безпеки процесу і основної системи управління безперервним процесом, що залежить від коректної роботи SIS і інших рівнів захисту». Іншими словами, функціональна безпека - це зниження рівня ризику шляхом впровадження функцій забезпечення безпечного управління процесами. На жаль, стандарт містить загальні вимоги і рекомендації по розробці функціональної безпеки SIS, не пропонуючи конкретних методів аналізу і прикладів документального оформлення «Керівництва по функціональної безпеки» (РФБ).

У даній роботі на прикладі розробки РФБ для модулів керуючого комплексу МСКУ з резервованою структурою представлені методи аналізу видів, наслідків та критичності відмов (Failure Mode and Effects Analysis - FMEA) та визначення показників рівня повноти інтегральної безпеки.

3. Аналіз даних, методи проведення FMEA-аналізу.

Для того, щоб оцінити характер відмов модулів і компонентів Е / Е / ПЕ систем, використовуються такі визначення:

- Стан при безпечному відмову (Failure-Safe State) - стан, при якому вихідний сигнал досягає порогу, заданого користувачем, або вихід відключається (або включається);
- Безпечна відмова (Failure Safe) - відмова, при якому модуль / (суб) система переходить в вказаний вище безпечний стан без запиту з боку контрольованого процесу;

- Небезпечна відмова (Failure Dangerous) - відмова, при якому система не відповідає на запит з боку контрольованого процесу (тобто не здатна перейти в заданий безпечний стан);
- Небезпечна недіагностована відмова (Failure Dangerous Undetected) - небезпечна відмова, яка не виявляється засобами внутрішньої діагностики;
- Небезпечна відмова, що виявляється (Failure Dangerous Detected) - небезпечна відмова, яка виявляється засобами внутрішньої діагностики (при таких відмовах система може переводитися в заданий безпечний стан);
- Відмова з високим рівнем (Failure High) - відмова, при якій вихідний сигнал досягає максимально допустимого верхнього значення;
- Відмова з низьким рівнем (Failure Low) - відмова, при якій вихідний сигнал досягає мінімально допустимого нижнього значення;
- Відмова, що не виявляє ефекту (Failure No Effect) - відмова компонента, яка є частиною функції безпеки, але не впливає на функцію безпеки, і який не виявляється засобами внутрішньої діагностики. При розрахунку SFF вона розглядається як недіагностована безпечна відмова.

Категорії «Відмова, що не виявляє ефекту» (FailNoeffect) і «незафіксована сигналізація» (Noannunciation) використовуються в тих випадках, коли існує необхідність аналізу надійності більш детального, ніж вимагає стандарт [1]. Категорії «Відмова що не виявляє ефекту» і «незафіксована сигналізація» визначаються як безпечна недіагностована відмова, навіть якщо вони не змушують функцію безпеки переходити в безпечний стан. Тому їх необхідно враховувати при розрахунку функціоналу безпечних відмов (Safe Failure Functional - SFF);

- Відмова компоненти, яка не є частиною функції безпеки (Failure Not Part) - відмова компоненти, яка не є частиною функції безпеки, але в той же час є частиною електричної схеми та зображена для її повноти. При розрахунку SFF ця категорія відмов не враховується;
- Стан при безпечній відмові (Failure-SafeState) - в залежності від застосування, стан при безпечній відмові визначається як перехід виходу в стан з низьким рівнем (Failure Low) або в стан з високим рівнем (Failure High). Значення низького і високого рівнів можуть програмуватися користувачем.

Згідно таблиці 3 зі стандарту МЕК 61508-1, середня частота відмови на запит виконання функції безпеки (Average probability of dangerous failure on demand per hour- середня ймовірність небезпечних відмов за годину) PFH для систем, що працюють в режимі високого рівня запитів, повинна бути в діапазоні від> = 1.00 E-08 до <1.00 E-07 для рівня SIL 3 функцій безпеки.

Відповідно до таблиці 3 стандарту МЕК 61508-2, для компонентів типу B значення SFF має бути:

- ≥ 99% для SIL 3 (суб-) систем зі стійкістю до відмов апаратної частини 0;
- ≥90% для SIL 3 (суб-) систем зі стійкістю до відмов апаратної частини 1;
- ≥60% для SIL 3 (суб-) систем зі стійкістю до відмов апаратної частини 2.

Якщо вимоги розділу 11.4.4 стандарту [4] (редакція 2003-01), виконані, стійкість до відмов апаратної частини 1 достатня для рівня SIL 3 (суб) для компонентів типу B з стійкістю 1 необхідно SFF> 90%. Стійкість до апаратних відмов N означає, що N + 1 відмову може привести до порушення функції безпеки пристрою.

Вважаючи, що логічний пристрій може фіксувати вихід сигналу як за верхні (відмова "Fail-high"), так і за нижні межі діапазону (відмова "Fail-low"), відмови цих обох типів можуть класифікуватися як безпечні виявлені відмови або як небезпечні виявлені відмови, в залежності від конкретного застосування.

Так як інтегральні апаратні комплекси, що розробляються, і які є центральною частиною АСУТП не виконують функцій, які безпосередньо можуть бути визначені як функції безпеки, то, взявши за основу наведені вище визначники і показники, пропонується наступний метод проведення FMEA-аналізу:

1. Приймається важливе обов'язкове твердження про те, що при будь-яких діагностуємих функціональних відмовах елементів і блоків програмно-апаратної Е/Е/ПЕ системи, центральна (керуюча) її частина переводить всю систему в безпечний стан. До таких відмов відноситься і повне припинення функцій центральної частини. Це означає, що приймаючи в розробку, впровадження та експлуатацію програмно-апаратні комплекси АСУТП необхідно створити таку архітектуру і засоби управління, які при переході в нормально вимкнений (неробочий) стан здійснювали функцію аварійної зупинки або перемикання на резервні засоби управління таким чином, щоб такий перехід не міг привести до небезпечних наслідків. Неприйняття або невизначеність такого положення виключає будь-яку можливість підтверджувати будь-який рівень повноти безпеки.
2. Приймається консервативний підхід до визначення типу відмови елемента (небезпечний, безпечний, що не діагностується, діагностується). Це означає, що якщо неможливо довести, що відмова елемента призводить до безпечних наслідків, то він автоматично вважається небезпечним. Аналогічно приймається рішення щодо діагностування.
3. Застосовується узагальнений підхід до всіх типів елементів. Це означає, наприклад, що відмова резистора може розглядатися як «розрив» і «дрейф 50%» для всіх резисторів з долями 0,5 і при цьому «розрив» вважається «безпечним діагностуються». Для мікросхем, наприклад, приймається також уніфікована структура відмов:

Приклад таблиці заповнення частот відмов

Таблиця 1.

		λ	λdd, FIT	λdu, FIT	λsd, FIT	λsu, FIT	вид	доля
D80	Мікросхема LP2992IM5-1.5 National Semiconductor	15	1.455	0	0	0	Втрата контакту	0.1
			1.455	0	0	0	КЗ	0.1
			2.91	0	0	0	Зміна значення	0.2
			0	0	3	0		0.2
			2.91	0	0	0	Функціональні відмови	0.2
			0	0	3	0		0.2

4. Підсумкові інтегральні показники оформляються в таблиці і приймаються як вхідні дані для подальших розрахунків показників надійності, представлених в розділі 5 даної статті.

4. Цель и задачі розробки

Об'єкт дослідження – процес інформаційної підтримки генерації вимог до рівня повноти функціональної безпеки керуючого обладнання автоматизованих систем управління.

Дана розробка проводиться з метою створення методів визначення відповідності показників надійності програмно-апаратних комплексів АСУТП необхідному рівню SIL. Рішення задач визначення рівня інтегральної безпеки для систем, що містять електронні/електричні/програмовані елементи і вузли можливо шляхом розробки методів аналізу видів відмов і їх наслідків з метою визначення кількісних показників надійності і їх зіставлення з нормативними вимогами.

5. Методи представлення й обробки даних при визначенні рівня SIL.

Основні позначки:

- DC (Diagnostic coverage): рівень діагностики (небезпечних або безпечних відмов), який забезпечувався б логічним пристроєм системи безпеки для розглянутого модуля.

- DCs (Diagnostic coverage for safe failures): рівень діагностики для безпечних відмов = $\frac{\lambda_{sd}}{\lambda_{sd}+\lambda_{su}}$

- DCd (Diagnostic coverage for dangerous failures): рівень діагностики для небезпечних відмов = $\frac{\lambda_{dd}}{\lambda_{dd}+\lambda_{du}}$

- FIT (Failure In Time): Кількість відмов в одиницю часу (1E-9 відмов в годину).
- Failure Rates (Інтенсивності відмов):

Дані про інтенсивність відмов, використані в аналізі FMEA, це базові інтенсивності відмов, взяті з бази даних по відмовах стандарту Siemens SN 29500. Ці інтенсивності відмов підходять для розрахунків при оцінці рівня повноти безпеки і відповідають граничним (стресовим) умовам експлуатації, типовим для промислового середовища, подібним описаним у стандарті МЕК 60654-1, клас С. Передбачається, що реальна кількість відмов буде менше, ніж кількість, розрахована на основі цих інтенсивностей відмов.

Режим, коли частота запитів на виконання системою безпеки функцій захисту не більше, ніж один раз на рік і не перевищує частоту проведення перевірочних тестів більш, ніж в два рази.

- MTBF (MeanTimeBeforeFailure): Середній час напрацювання між відмовами (середній час напрацювання на відмову по ГОСТ 2702-89, може бути застосовано для ремонтованих приладів).
- MTTF (MeanTimeToFailure): Середній час напрацювання до відмови.
- MTTFS (MeanTimeToSafeFailure): Середній час напрацювання до безпечної відмови.
- MTTFD: (MeanTimeToDangerousFailure): Середній час напрацювання до небезпечної відмови.
- MTTR (MeanTimeToRepair): Середній час відновлення системи.
- PFDavg: Середня ймовірність відмови на запит виконання необхідної функції безпеки.
- SFF (Safe Failure Fraction):

Частка безпечних відмов відповідно до стандарту МЕК 61508 (представляє суму частки відмов, які призводять до переходу в безпечний стан, і частки відмов, які виявляються діагностичними засобами, і в результаті також завершуються переходом в безпечний стан.

$$SFF = \frac{\sum\lambda_{dd}+\sum\lambda_{sd}+\sum\lambda_{su}}{\sum\lambda_{dd}+\sum\lambda_{du}+\sum\lambda_{sd}+\sum\lambda_{su}} = 1-\frac{\sum\lambda_{du}}{\sum\lambda_{dd}+\sum\lambda_{du}+\sum\lambda_{sd}+\sum\lambda_{su}}$$

де: λ_{dd} : інтенсивність небезпечних відмов, що виявляються;

λ_{du} : інтенсивність небезпечних відмов, що не виявляються;

λ_{sd} : інтенсивність безпечних відмов, що виявляються;

λ_{su} : інтенсивність небезпечних відмов, що не виявляються.

- SIF (Safety Instrumented Function): інструментальна функція забезпечення безпеки.
- SIS (Safety Instrumented System): інструментальна система забезпечення безпеки (система протиаварійного захисту).
- SIL (Safety Integrity Level): рівень повноти безпеки.
- T ProofTest&Maintenance (TI): Міжповірочний інтервал періодичного автономного (off-line) функціонального тестування, який служить для виявлення відмов, що не виявляються діагностикою, з метою перевірки і відновлення вихідного рівня функціональної безпеки (наприклад, 1 - 5 - 10 років, 1 рік = 8760 годин.). Час обслуговування приймається рівним 8 години.

Методика розрахунків показників надійності полягає в наступному:

В результаті проведення FMEA для блоків і пристроїв керуючого комплексу проводиться поділ частот відмов елементів комплексу, які представлені в технічній документації або паспортах на елементи. Основне завдання аналізу - отримати обґрунтовані дані та значення λ_{dd}, λ_{du}, λ_{sd}, λ_{su}.

Приймається регламентоване значення, зазвичай: MTTR=8 годин, T_1=8760 год.

При цьому у відповідності зі стандартом [1-3] (зокрема його розділів 6 B.3.3.1):

$$\lambda_d = \lambda_{du} + \lambda_{dd} \tag{1}$$

$$t_{CE} = \frac{\lambda_{du}}{\lambda_d}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{dd}}{\lambda_d} MTTR \tag{2}$$

MRT=MTTR=8 годин. β приймаєм = 0,05 (5% відмова за загальними причинами); β_D =0,025.

Якщо припустити, що система, пов'язана з безпекою при виявленні будь-якого відмови дає змогу встановити в безпечний стан, то:

- для архітектури 1oo1 $PFH_G = \lambda_{du}$ (3)

- для архітектури 1oo2 $PFH_G = 2\left(\left(1-\beta_D\right)\lambda_{dd} + \left(1-\beta\right)\lambda_{du}\right)\left(\left(1-\beta\right)\lambda_{du} t_{CE}\right) + \beta\lambda_{du}$ (4)

- для архітектури 2oo2 $PFH_G = 2\lambda_{du}$ (5)

- для архітектури 1oo2D $t_{CE} = \dfrac{\lambda_{du}\left(\frac{T_1}{2} + MRT\right) + \left(\lambda_{dd} + \lambda_{sd}\right)MTTR}{\lambda_{du}\left(\lambda_{dd} + \lambda_{sd}\right)}$ (6)

$$PFH_G = 2\left(1-\beta\right)\lambda_{du}\left(\left(1-\beta\right)\lambda_{du} + \left(1-\beta_D\right)\lambda_{dd} + \lambda_{sd}\right)t_{CE} + 2\left(1-K\right)\lambda_{dd} + \beta\lambda_{du} \tag{7}$$

- для архітектури 2oo3 $t_{CE} = \frac{\lambda_{du}}{\lambda_d}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{dd}}{\lambda_d} MTTR$ (8)

$$PFH_G = 6\left(\left(1-\beta_D\right)\lambda_{dd} + \left(1-\beta\right)\lambda_{du}\right)\left(1-\beta\right)\lambda_{du} t_{CE} + \beta\lambda_{du} \tag{9}$$

- для архітектури 1oo3 (10)

$$t_{GE} = \frac{\lambda_{du}}{\lambda_d}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{dd}}{\lambda_d} MTTR \tag{11}$$

$$PFH_G = 6\left(\left(1-\beta_D\right)\lambda_{dd} + \left(1-\beta\right)\lambda_{du}\right)^2\left(\left(1-\beta\right)\lambda_{du} t_{CE} t_{GE}\right) + \beta\lambda_{du} \tag{12}$$

При заповненні таблиць підрозділів розділу 6 використовуються наступні дані:
- код модуля відповідає коду, що представлений в малюнку аналізованої структури;
- кількість - вказується кількість структурних елементів використовуваних в даному модулі;
- конфігурація - архітектура резервування, використовувана в аналізованій структурі;

λ_{dd}, FIT – частота небезпечних діагностуємих відмов 10-9 / час;

λ_{dd} *к-во, FIT – добуток частоти небезпечних діагностуємих відмов на кількість структурних елементів;

λ_{du}, FIT - частота небезпечних недіагностуємих відмов 10-9 / час;

λ_{du} *к-во - добуток частоти небезпечних недіагностуємих відмов на кількість структурних елементів;

λ_s – частота безпечних діагностуємих відмов 10-9 / час;

У рядку «Разом для гілки, 1 / год» - наводиться сума даних в колонках λ *к-во в розмірності «1/год».

У рядку «CCF, 1/час» наводиться значення добутку β на значення в «Всього для гілки, 1/год».

Підсумкові значення λ_{dd}; λ_{du}; λ_s обчислюються на підставі даних про конфігурацію:

Визначення інтегральних показників ризику з урахуванням зміни резервування.

Таблиця 2.

Конфігурація	Виявлені	Невиявлені	Безпечні
1oo1	λ_{dd}	λ_{du}	λ_s
1oo2	$2\lambda_{dd}^{\ 2}MDT$	$\lambda_{du}^{\ 2}T_1$	$2\lambda_s$
2oo2	$2\lambda_{dd}$	$2\lambda_{du}$	$2\lambda_s^{\ 2}MDT$
1oo3	$3\lambda_{dd}^{\ 3}MDT^2$	$\lambda_{du}^{\ 3}T_1^2$	$3\lambda_s$
2oo3	$6\lambda_{dd}^{\ 2}MDT$	$3\lambda_{du}^{\ 2}T_1$	$6\lambda_s^{\ 2}MDT$
3oo3	$3\lambda_{dd}$	$3\lambda_{du}$	$3\lambda_s^{\ 3}MDT^{\ 2}$
1oo4	$\lambda_{dd}^{\ 4}MDT^{\ 3}$	$\lambda_{du}^{\ 4}T_1^3$	$4\lambda_s$
2oo4	$12\lambda_{dd}^{\ 3}MDT^{\ 2}$	$4\lambda_{du}^{\ 3}T_1^2$	$12\lambda_s^{\ 2}MDT$
3oo4	$12\lambda_{dd}^{\ 2}MDT$	$6\lambda_{du}^{\ 2}T_1$	$12\lambda_s^{\ 3}MDT^{\ 2}$
4oo4	$4\lambda_{dd}$	$4\lambda_{du}$	$\lambda_s^{\ 4}MDT^{\ 3}$

Підсумкові значення λ_{dd}; λ_{du}; λ_s для аналізованої структури обчислюються як суми значень «CCF» і «Всього λ_* » відповідних колонок.

Доля безпечних відмов аналізованої структури обчислюється на основі підсумкових значень λ_{dd}; λ_{du}; λ_S:

$$SFF = \frac{\lambda_{dd} + \lambda_s}{\lambda_{dd} + \lambda_{du} + \lambda_s} \tag{13}$$

Підсумкові значення показників надійності наводиться в таблиці 3. Наприклад, для модуля зв'язку МСКУ:

Приклад показників надійності для МСКУ.

Таблиця 3.

Σλ, FIT	1852,8
$\Sigma\lambda_{dd}$, FIT	14,9
$\Sigma\lambda_{du}$, FIT	4,4
$\Sigma\lambda_{sd}$, FIT	949,8
$\Sigma\lambda_{su}$, FIT	826,6
DC, %	77
SFF, %	99,7
PFDavg(T_1)	9,77 E-06
PFH, 1/h	1,72E-12

Проводиться підсумкове порівняння рівня повноти безпеки з даними [1] і робиться висновок про значення SIL для обладнання, щодо якого проводиться сертифікація. В даному прикладі рівень повноти безпеки модуля зв'язок не гірше SIL 4.

Цього достатньо, щоб переконатися в можливості застосування досліджуваних керуючих комплексів в системах з рівнем повноти безпеки на гірше, ніж заявлений рівень SIL.

Висновки.

Пропонований в роботі метод визначення типів наслідків відмов елементів досліджуваних апаратних блоків і модулів частин АСУТП дозволяє консервативно розділити функціональні відмови, що виникають в результаті відмов окремих електронних елементів і отримати інтегральні показники надійності досліджуваних блоків.

Використання запропонованих методів визначення інтегрального рівня повноти безпеки дозволяє в повній мірі відповідно до вимог стандартів [1-4] підготувати матеріал для проходження процедури сертифікації центральних частин програмно-апаратних комплексів автоматизованих систем управління без визначення безпосередніх функцій безпеки.

При використанні описаних методів можливо зняти протиріччя і невизначеність, що виникають при розгляді програмно-апаратних комплексів центральних частин АСУТП поза їхнім зв'язком з блоками і модулями датчиків, засобів отримання вхідної інформації, а також виконавчими пристроями.

Література

1. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью = Ч. 1. Общие требования : Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements: национальный стандарт Российской Федерации ГОСТ Р МЭК 61508-1-2007 / Федеральное агентство по техническому регулированию и метрологии. – М.: Стандартинформ, 2008. - V, 44 с.
2. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью = Ч. 2. Требования к системам : Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2. Requirements for systems: национальный стандарт Российской Федерации ГОСТ Р МЭК 61508-2-2007 / Федеральное агентство по техническому регулированию и метрологии. – М.: Стандартинформ, 2008. - V, 58 с.
3. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью = Ч. 6. Руководство по применению ГОСТ Р МЭК 61508-2-2007 и ГОСТ Р МЭК 61508-3-2007 : Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 6. Guidelines on the application of GOST R IEC 61508-2-2007 and GOST R IEC 61508-3-2007 : национальный стандарт Российской Федерации ГОСТ Р МЭК 61508-6-2007 / Федеральное агентство по техническому регулированию и метрологии. - Москва : Стандартинформ, 2008. - V, 62 с.
4. Функциональная безопасность в непрерывных производствах. Руководство по безопасности процессов / IEC 61511:2004 Functional Safety – Safety Instrumented Systems for the Process Industry Sector/ национальный стандарт Российской Федерации ГОСТ Р МЭК 61511-1-2011 / Федеральное агентство по техническому регулированию и метрологии. – М.: Стандартинформ, 2013. – V, 66 с.
5. Руководство по функциональной безопасности для систем, связанных с безопасностью, и других применений с уровнем SIL2, SIL3 в соответствии со стандартами МЭК 61508 и МЭК 61511 / GM International Technology for safety / Via San Fiorano 70, 20058 Villasanta (MI) Italy, 2013. – D100, 77 p.

References

1. Funkcional'naya bezopasnost' sistem ehlektricheskih, ehlektronnyh, programmiruemyh ehlektronnyh, svyazannyh s bezopasnost'yu = CH. 1. Obshchie trebovaniya : Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements: nacional'nyj standart Rossijskoj Federacii GOST R MEHK 61508-1-2007 / Federal'noe agentstvo po tekhnicheskomu regulirovaniyu i metrologii. – M.: Standartinform, 2008. - V, 44 s.
2. Funkcional'naya bezopasnost' sistem ehlektricheskih, ehlektronnyh, programmiruemyh ehlektronnyh, svyazannyh s bezopasnost'yu = CH. 2. Trebovaniya k sistemam : Functional safety of electrical, electronic, pro-grammable electronic safety-related systems. Part 2. Requirements for systems: nacional'nyj standart Rossijskoj Federacii GOST R MEHK 61508-2-2007 / Federal'noe agentstvo po tekhnicheskomu regulirovaniyu i metrologii. – M.: Standartinform, 2008. - V, 58 s.
3. Funkcional'naya bezopasnost' sistem ehlektricheskih, ehlektronnyh, programmiruemyh ehlektronnyh, svyazannyh s bezopasnost'yu = CH. 6. Rukovodstvo po primeneniyu GOST R MEHK 61508-2-2007 i GOST R MEHK 61508-3-2007 : Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 6. Guidelines on the application of GOST R IEC 61508-2-2007 and GOST R IEC 61508-3-2007 : nacional'nyj stan-dart Rossijskoj Federacii GOST R MEHK 61508-6-2007 / Federal'noe agentstvo po tekhnicheskomu regulirova-niyu i metrologii. - Moskva : Standartinform, 2008. - V, 62 s.
4. Funkcional'naya bezopasnost' v nepreryvnyh proizvodstvah. Rukovodstvo po bezopasnosti processov / IEC 61511:2004 Functional Safety – Safety Instrumented Systems for the Process Industry Sector/ nacional'nyj standart Rossijskoj Federacii GOST R MEHK 61511-1-2011 / Federal'noe agentstvo po tekhnicheskomu regulirovaniyu i metrologii. – M.: Standartinform, 2013. – V, 66 s.
5. Rukovodstvo po funkcional'noj bezopasnosti dlya sistem, svyazannyh s bezopasnost'yu, i drugih primenenij s urovnem SIL2, SIL3 v sootvetstvii so standartami MEHK 61508 i MEHK 61511 / GM International Technology for safety / Via San Fiorano 70, 20058 Villasanta (MI) Italy, 2013. – D100, 77 r.

Представлены методы определения интегральных уровней безопасности при выработке требований к электрическим, электронным, и программируемым электронным системам автоматизированных систем управления, которые используются в непрерывных производствах повышенной опасности. Предлагается использовать метод определения типов последствий отказов элементов при проведении FMEA анализа, который позволяет консервативно и унифицировано провести разделение частот отказов отдельных элементов исследуемых блоков и модулей оборудования, для которого проводится сертификация, по типам отказов и получить интегральные показатели уровня полноты безопасности.

Ключевые слова: *Safety integrity level, уровень полноты безопасности, электронные программируемые устройства, надежность, безопасность.*

Methods for determining integral safety levels are presented in the development of requirements for electrical, electronic and programmable electronic systems of automated control systems that are used in continuous production with a high level of risk. It is proposed to use the method for determining the types of consequences of failures of elements during the FMEA analysis, which allows conservatively and unify the spread of failures of individual elements of the investigated blocks and equipment modules for which certification is performed, according to the type of failure and obtain integrated indicators of the safety integrity level.
Key words*: Safety integrity level, level of safety integrity, electronic programmable devices, reliability, safety.*

Довідка про авторів:

Лифар Володимир Олексійович
Доктор технічних наук, доцент, зав. кафедри програмування та математики
Східноукраїнський національний університет ім. Володимира Даля
моб. 097-547-03-97, тел. 70-40-60
E-mail: lyfarva61@ukr.net

Лифар Олена Костянтинівна
Старший викладач
Східноукраїнський національний університет ім. Володимира Даля
моб. 097-335-51-29, тел. 70-40-60
E-mail: lyfarva61@ukr.net

Рязанцев Андрій Олександрович
Студент інституту транспорту і логістики
Східноукраїнський національний університет ім. Володимира Даля
моб. 050-102-73-26,
E-mail: drew.ryazancev@gmail.com

Герасименко Костянтин Євгенович
Заступник директора по системам автоматизації в енергетиці НВО «Імпульс»
+38 (06452) 6-01-94
E-mail: gerasymenko_ke@imp.lg.ua