Міністерство освіти і науки України
Національний технічний університет
«Харківський політехнічний інститут»

МЕТОДИЧНІ ВКАЗІВКИ ТА ЗАВДАННЯ

щодо самостійної роботи студентів

з дисципліни «Теорія ризиків»

для студентів спеціальності «Цивільна безпека»,

спеціалізації – Охорона праці

Затверджено
редакційно-видавничою радою
університету
протокол №2 від 24.05. 2018 р.

Харків
НТУ «ХПІ»
2018

Методичні вказівки та завдання щодо самостійної роботи студентів з дисципліни « Теорія ризиків » Для студентів спеціальності «Цивільна безпека», спеціалізації – охорона праці / Уклад. Березуцький В.В., - Харків : НТУ «ХПІ», 2018. – 38 с.

Укладач : В.В. Березуцький

Рецензент: Т.С. Бондаренко

Кафедра «Охорона праці та навколишнього середовища»

Вступ

Мета - забезпечити майбутніх фахівців з охорони праці теоретичними знаннями, необхідними для визначення ризиків та управління ними відповідно до спеціальності та завдань з охорони праці, щодо створення безпечних і нешкідливих умов праці, проектуванню безпечної техніки та технологічних процесів.

В результаті вивчення курсу “ Теорія ризиків ” студенти повинні знати:

- ✓ основні етапи розвитку науки про ризики;
- ✓ стан ризиків на сучасному етапі у державі та у світі;
- ✓ концептуальні основи припустимого та неприпустимого ризиків;
- ✓ теоретичні основи системи управління ризиками на виробництві.

Відповідність фахової підготовки в Україні, відповідає підготовці європейських фахівців за напрямом – професійна безпека та здоров’я (Occupational Safety and Health – OSH).

Дисципліна вивчається за змішаною формою навчання, в якої використовуються денна (очна) та Інтернет ресурс.

Вивчення дисципліни сплановано на **16** тижнів, щотижня по 2 години аудиторних (лекції) – **32** години та **40** годин самостійної роботи. Разом – **72** години.

Для успішного опанування лекційного матеріалу, запропоновані завдання та спілкування на форумах в Інтернеті за вище вказаною адресою. Лекційний матеріал запропоновано у дистанційному курсі. Завдання виконуються студентом із використанням лекційного матеріалу із дисципліни «Теорія ризиків».

Відповіді на індивідуальні завдання готувати у наступному вигляді:

1. Текст, до 2-х сторінок у форматі Word, кегель 14.
2. Висновок.
3. Джерела інформації (література, електроні ресурси тощо).
4. Викладачу надсилати у електронному вигляді

САМОСТІЙНА РОБОТА

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	32
2	Підготовка до практичних(лабораторних, семінарських) занять	16
3	Самостійне вивчення тем та питань, які не викладаються на лекційних заняттях	28
4	***Виконання індивідуального завдання:***	21
5	Інші види самостійної роботи	-
	Разом	72

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Реферат та тези доповіді на конференцію враховується, як виконання індивідуального завдання.

№ з/п	Назва індивідуального завдання та (або) його розділів	Терміни виконання (на якому тижні)
1	Методи оцінки ризику. Структуровані або частково структуровані інтерв'ю	4 тиждень
2	Методи оцінки ризику. Контрольні листи	5 тиждень
3	Методи оцінки ризику. Аналіз сценаріїв.	6 тиждень
4	Методи оцінки ризику. Аналіз впливу на бізнес.	7 тиждень
5	Методи оцінки ризику. Аналіз першопричини (RCA).	8 тиждень
6	Методи оцінки ризику. Аналіз рівнів захисту. Метод LOPA	9 тиждень
7	Методи оцінки ризику. Аналіз дерева рішень.	10 тиждень
8	Методи оцінки ризику. Аналіз впливу людського фактора. Метод HRA	11 тиждень
9	Методи оцінки ризику. Аналіз «краватка-метелик»	12 тиждень
10	Методи оцінки ризику. Аналіз прихованих дефектів і аналіз паразитних ланцюгів (SA - Sneak Analysis).	13 тиждень

ЗАВДАННЯ

Завдання1. Структуровані або частково структуровані інтерв'ю

Короткий огляд

У структурованому інтерв’ю опитуваному задають питання із заздалегідь підготовленого переліку, що заохочують всебічний аналіз ситуації і, таким чином, більш повну ідентифікацію небезпек і ризику. Частково структуроване інтерв’ю аналогічно структурованого, однак воно забезпечує більшу свободу при обговоренні досліджуваної проблеми.

Область застосування

Структуровані і частково структуровані інтерв’ю корисні в ситуаціях, коли важко зібрати людей для обговорення або коли вільне обговорення в групі неможливо. Дані види інтерв’ю найчастіше використовують як частина процесу аналізу ризику для ідентифікації небезпек або оцінки ефективності засобів управління. Вони можуть бути застосовані на всіх стадіях проекту або процесу. Структуровані і частково структуровані інтерв’ю можуть бути використані при зборі вхідних даних для оцінки ризику причетними сторонами.

Вхідні дані

Вхідні дані включають в себе:

– Точне визначення цілей інтерв’ю;

– Список опитуваних, який повинен бути складений з урахуванням інтересів залучених причетних сторін;

– Перелік питань.

Процес виконання методу

Спочатку необхідно скласти перелік питань, що направляють роздуми опитуваного. Питання повинні бути, наскільки можливо, простими, викладені зрозумілою для опитуваного мовою і охоплювати тільки одну проблему. Відповіді на питання не повинні бути обмежені за часом. Питання, що спрямовані на роз’яснення відповідей, повинні бути підготовлені заздалегідь.

Потім питання повинні бути запропоновані опитуваної особі. При уточнені відповіді повинні бути обмеження за часом. Необхідно стежити за тим, щоб постановка питання не підказувала опитуваному певну відповідь.

При аналізі відповідей необхідно проявляти гнучкість і забезпечити можливість дослідження областей, пропонованих опитуваними у своїх відповідях.

Вихідні дані

Вихідними даними є інформація про сприйняття причетними сторонами проблем, які є предметом інтерв'ю.

Порядок виконання завдання.

1. Скласти лист опитування (інтерв'ю) за одною із нижче наведених тем (кількість запитань до 10):

Небезпеки на робочому місці студента в аудиторії 1206;

Шкідливі фактори у лабораторії 1206а;

Небезпеки при проїзду із місця проживання до університету.

Завдання 2. Контрольні листи

Короткий огляд

Контрольні листи являють собою переліки небезпек, ризику або відмов засобів управління, які зазвичай розробляють на основі отриманого раніше досвіду, результатів попередньої оцінки ризику або результатів відмов, що сталися в минулому.

Область застосування

Контрольний лист може бути використаний для ідентифікації небезпек і ризику або оцінки ефективності засобів управління. Контрольні листи можуть бути використані на всіх стадіях життєвого циклу продукції, процесу або системи. Контрольні листи можуть бути використані як частина інших методів оцінки ризику, проте вони найбільш корисні для перевірки повноти розгляду досліджуваної проблеми після застосування більш образних і творчих методів при ідентифікації нових проблем.

Вхідні дані

Попередня інформація та експертні оцінки з проблеми, що забезпечують вибір питань та розробку значимого контрольного листа (бажано затвердженого).

Процес виконання методу

Повинна бути виконана наступна процедура:

- Визначення області застосування;

➢ Складання контрольного листа таким чином, щоб він охоплював всю область застосування. Контрольні листи повинні бути ретельно складені для досягнення поставленої мети. Наприклад, складений раніше контрольний лист не може бути використаний при ідентифікації нових небезпек або ризику;

➢ Особа або група осіб повинні застосовувати контрольний лист послідовно до кожного елементу процесу або системи для визначення того, представлений чи цей елемент в контрольному листі.

Вихідні дані

Вихідні дані залежать від стадії процесу менеджменту ризику, на якій застосовані контрольні листи. Наприклад, вихідними даними можуть бути переліки неадекватних засобів управління або переліки небезпек.

Порядок виконання завдання.

1. Необхідно скласти контрольний лист небезпек до одного із наступних об'єктів :

- Ліфт у навчальному корпусі У\1;
- Спортивна кафедра;
- Лабораторні роботи на фізичної кафедрі;
- Лабораторні роботи на хімічної кафедрі.

Завдання 3. Аналіз сценаріїв.

Короткий огляд

Найменування методу «аналіз сценаріїв» дано процесу розробки описових моделей розвитку подій. Метод може бути використаний для ідентифікації ризику шляхом розгляду можливих подій у майбутньому і дослідження їх значимості та наслідків. Набори сценаріїв, що відображають, наприклад, «кращий випадок», «найгірший випадок» і «очікуваний випадок», можуть бути використані для аналізу можливих наслідків і їх ймовірності для кожного сценарію.

Можливості методу аналізу сценаріїв можна проілюструвати, розглядаючи основні зміни за минулі 50 років у технологіях, переваги споживачів, соціальних відносинах і т. п. У процесі аналізу сценаріїв важко прогнозувати ймовірність таких змін в майбутньому, проте можна аналізувати наслідки, допомогти організаціям використовувати переваги і забезпечити стійкість до прогнозованих змін.

Область застосування

Аналіз сценаріїв може бути корисний у прийнятті політичних рішень і плануванні майбутніх стратегій, а також при розгляді існуючих видів діяльності.

Даний метод може бути використаний для всіх трьох елементів оцінки ризику. На етапах ідентифікації та аналізу ризику набори сценаріїв, що відображають, наприклад, кращий, гірший і найбільш вірогідний випадок, можуть бути використані для встановлення того, що може статися в конкретних обставинах, а також для аналізу потенційних наслідків і їх ймовірності для кожного сценарію.

Метод аналізу сценаріїв може бути використаний для прогнозування можливих загроз і їх розвитку в часі і може бути застосований для всіх типів ризику в короткостроковій і довгостроковій перспективі.

У короткостроковій перспективі при наявності достовірних даних ймовірні сценарії можуть бути екстрапольовані на основі існуючих даних. У довгостроковій перспективі з урахуванням низької достовірності даних аналіз сценаріїв дозволяє визначити загальний характер розвитку подій.

Вхідні дані

Необхідною умовою застосування методу аналізу сценаріїв є наявність групи фахівців, що володіють розумінням характеру змін що досліджуються (наприклад, можливих досягнень у технологіях).

Ці фахівці повинні бути здатні спрогнозувати ситуацію в майбутньому, не вдаючись до екстраполяції на основі даних минулих подій. Корисно також використання даних літературних джерел і даних, що відносяться до змін.

Процес виконання методу

Структура методу аналізу сценаріїв може бути формалізованою або довільною. Після формування групи, встановлення каналів обміну інформацією, визначення досліджуваних проблем та області застосування методу необхідно ідентифікувати характер можливих змін. Слід також дослідити основні тенденції та оцінити ймовірний час змін на основі експертного прогнозу.

Досліджувані зміни можуть включати в себе:

– Зовнішні зміни (такі як зміни технологій);

– Рішення, які необхідно прийняти в найближчому майбутньому і які можуть призвести до різних результатів;

– Потреби причетних сторін і можливі зміни;

– Зміни в макросередовищі (обов'язкових вимог, демографії та інші), деякі з яких неминучі, інші можливі.

Іноді зміни можуть статися внаслідок іншого небезпечного події. Наприклад, зміна клімату призводить до змін споживчого попиту на продукти харчування, що впливає на те, які продукти харчування вигідно експортувати, а які – вирощувати в своєму регіоні.

Потім слід скласти перелік локальних факторів і макрофакторів або тенденцій і аранжувати спочатку за значимістю, потім по невизначеності. Особливу увагу слід приділяти факторам, які є найбільш значущими і більш невизначеними.

Ключові фактори або тенденції наносять на карту навпроти один одного, щоб показати і виявити області розробки сценаріїв. Зазвичай пропонують набір сценаріїв, кожен з яких відповідає ймовірного зміни параметрів. Потім для кожного сценарію складають опис переходу від вихідної ситуації до розглянутого сценарієм. Опис може включати ймовірні деталі, які можуть бути дуже корисні для сценарію.

Далі сценарії можуть бути використані для дослідження або оцінки вихідної проблеми. При проведенні досліджень необхідно враховувати всі суттєві, але прогнозовані чинники (наприклад, шаблони, що використовують). Потім слід досліджувати виконання політики або діяльності при реалізації цього сценарію і оцінити результати попереднього дослідження сценарію з використанням запитань «що, як що», заснованих на припущеннях моделей.

Після проведення оцінки питань або припущень щодо кожного сценарію може стати очевидним, що саме необхідно змінити і як це зробити найбільш доцільним і безпечним чином. Можуть бути також визначені основні індикатори, що вказують на появу можливих змін.

Моніторинг основних індикаторів і вжиті відповідні заходи дозволяють забезпечити можливість внесення змін в заплановані стратегії. Так як сценарії охоплюють тільки окремі частини можливого розвитку майбутніх подій, важливо упевнитися, що враховані ймовірності появи конкретних сценаріїв, тобто – визначити структуру ризику. Наприклад, якщо використовують сценарії кращого випадку, гіршого випадку і найбільш ймовірного випадку, необхідно зробити декілька спроб для їх класифікації та оцінити ймовірність появи кожного сценарію.

Вихідні дані

Найбільш відповідного сценарію може не бути, однак аналіз дозволяє отримати більш чітке розуміння варіантів розвитку подій і способів зміни дій при зміні індикаторів.

Порядок виконання завдання.

Використовуючи вище зазначений метод, зробити сценарій подій виходячи із наступних вхідних даних:

Є джерело небезпеки, яке із ймовірністю 0,8 може вибухнути та із ймовірністю 0,3 може уразити 3-х працівників, а із ймовірністю 0,8 уразити 1 працівника. Сценарій може бути змінено, якщо ввести системи захисту.

Завдання 4. Аналіз впливу на бізнес.

Короткий огляд

Метод аналізу впливу на бізнес BIA (Business Impact Analysis), також відомий як оцінка впливу на бізнес, дозволяє досліджувати, як ключові види відмов/порушень/руйнувань, які можуть вплинути на ключові види діяльності і процеси організації, а також ідентифікувати і кількісно визначити необхідні можливості для управління організацією в цих умовах. Процес методу BIA забезпечує узгодження і розуміння:

– Ідентифікації та критичності ключових бізнес-процесів, функцій, пов'язаних ресурсів та ключових взаємозв'язків, існуючих в організації;

– Впливу відмов/порушень/руйнувань на можливості організації досягати встановлених критичних цілей бізнесу;

– Необхідних можливостей управління впливом відмов / порушень / руйнувань і відновленням нормального ходу діяльності організації.

Область застосування

Метод BIA використовують при визначенні критичності процесів організації, часу їх відновлення (RTO – Recovery Time Objective) і необхідних ресурсів (активи, персонал, навички, технології, виробничі площі та інформація) для забезпечення досягнення встановлених цілей. Крім того, метод BIA допомагає при визначенні взаємозв'язків між процесами, внутрішніми і зовнішніми сторонами і всіма ланцюгами поставок організації.

Вхідні дані

Для застосування методу необхідні:

– Група аналізу та розробки плану безперервності бізнесу;

– Інформація про цілі, навколишнє середовище, види діяльності та взаємозв’язки організації;

– Докладний опис видів діяльності та функціонування організації, що включають процеси, допоміжні ресурси, взаємозв’язки з іншими організаціями, угоди про аутсорсинг, причетні сторони;

– Економічні та виробничі наслідки, викликані порушенням критичних процесів;

– Підготовлені анкети;

– Список опитуваних осіб у відповідних областях діяльності організації та/або причетних сторін.

Процес виконання методу

У процесі BIA зазвичай використовують анкетування, інтерв’ю, структуровані наради або їх комбінацію, що дозволяє досягти розуміння функціонування критичних процесів, впливу порушень цих процесів і необхідного часу відновлення RTO і ресурсів.

Ключові етапи методу BIA:

– Визначення критичності ключових процесів і ключових видів продукції, робіт, послуг організації на основі оцінки для них небезпек, загроз і вразливості;

– Визначення економічних і виробничих наслідків відмов / порушень / руйнувань ідентифікованих критичних процесів за певні періоди часу;

– Ідентифікація взаємозв’язків з ключовими внутрішніми і зовнішніми причетними сторонами. На цьому етапі може бути корисно складання карт взаємозв’язків у системі і в ланцюзі постачань;

– Визначення наявних необхідних ресурсів для забезпечення безперервності робіт після відмов/порушень/руйнувань на мінімальному припустимому для організації рівні;

– Ідентифікація альтернативних способів виконання робіт і процесів, що існують або запланованих до розробки. Альтернативні способи виконання робіт та процесів можуть бути застосовані в ситуації нестачі або відсутності необхідних ресурсів або можливостей під час відмов/порушень/руйнувань;

– Визначення максимально допустимого періоду простою при відмовах / порушеннях / руйнуваннях (MAO – Maximum Acceptable Outage Time) для кожного процесу, заснованого на ідентифікованих наслідках і критичних факторах виконуваних видів діяльності. MAO являє собою період часу, після закінчення якого існує загроза остаточної втрати життєздатності організації, в

тому випадку, якщо поставка продукції та/або надання послуг не будуть відновлені;

– Визначення цільового часу відновлення (RTO) для будь-якого спеціалізованого обладнання, інформаційних технологій та інших активів організації. RTO являє собою час, запланований для відновлення виробництва продукції та надання послуг після відмов/порушень/руйнування, відновлення діяльності організації і відновлення спеціалізованого обладнання, інформаційних технологій або інших активів;

– Встановлення рівня підготовленості критичних процесів для управління в умовах порушень, яке може включати оцінку рівня резервування процесу (наприклад, наявності запасного обладнання) або існування альтернативних постачальників.

Вихідні дані

Вихідними даними є:

– Перелік ранжируваних за пріоритетами критичних процесів і відповідних взаємно залежностей;

– Зареєстровані економічні та виробничі впливи, викликані порушенням критичних процесів;

– Допоміжні ресурси, необхідні для ідентифікованих критичних процесів;

– Можливі терміни простою та відновлення критичних процесів і взаємопов’язаних інформаційних технологій.

Порядок виконання завдання.

Успішне підприємство визначається стабільністю доходів та передбаченням подій. Але небезпечні та шкідливі фактори, у поєднанні із непередбаченим людським фактором, можуть зруйнувати кар’єру керівників або навіть підприємство.

Вам необхідно запропонувати технологію, метод або щось інше що дозволить виявити вплив людського фактору (каталізатора) розвитку небезпечних факторів на робочому місці. Ідеї повинні бути оригінальними та реалістичними.

Завдання 5. Аналіз першопричини (RCA).

Короткий огляд

Аналіз втрат, що становлять основну частку збитку, спрямований на запобігання їх повторного виникнення, зазвичай називають аналізом

першопричини (RCA – Root Cause Analysis), аналізом першопричини відмови (RCFA – Root Cause Failure Analysis) або аналізом втрат. Метод RCA використовують для дослідження втрат внаслідок різних видів відмов, у той час як аналіз втрат головним чином застосовують для дослідження фінансових або економічних втрат від зовнішніх факторів або катастроф. Метод RCA спрямований на виявлення первинних причин відмови без розгляду їх зовнішніх проявів. Очевидно, що коригувальні дії не завжди ефективні і часто вимагають їх постійного поліпшення. Метод RCA зазвичай застосовують для оцінки основної складової втрат, однак його можна застосовувати для аналізу більш загальних втрат з метою виявлення можливостей постійного поліпшення.

Область застосування

Метод RCA має багато напрямів застосування:

– В галузі безпеки метод RCA використовують для дослідження нещасних випадків в галузі охорони праці та виробничої безпеки;

– В технологічних системах для аналізу надійності та технічного обслуговування використовують аналіз відмов;

– RCA виробництва застосовують для контролю якості виробничих процесів;

– RCA процесів застосовують для дослідження бізнес-процесів;

– RCA систем, що представляє собою комбінацію перерахованих видів RCA, застосовують при аналізі складних систем в системах управління змінами менеджменту ризику і в системному аналізі.

Вхідні дані

Основними вхідними даними методу RCA є всі об’єктивні дані про відмови або втрати. Дані про аналогічні відмовах також можуть бути розглянуті в процесі аналізу. Іншими вхідними даними можуть бути дані, отримані при перевірці конкретних гіпотез.

Процес виконання методу

Після прийняття рішення про застосування методу RCA формують групу експертів для проведення аналізу та розробки рекомендацій. Спеціалізація експертів головним чином залежить від цілей аналізу і особливостей відмови.

Методи проведення аналізу можуть істотно відрізнятися, однак основні етапи методу RCA аналогічні і включають:

– Формування групи;

– Встановлення області застосування і цілей методу RCA;

– Збір даних та об’єктивних свідчень про відмову або втрати;

– Проведення структурованого аналізу для визначення першопричини;

– Вироблення рішень і рекомендацій;

– Виконання рекомендацій;

– Верифікацію позитивного результату від впровадження рекомендацій.

Застосовують такі структуровані методи аналізу:

– Метод «5 чому», що складається в багаторазовому повторенні питання «чому?», Для дослідження п’яти рівнів глибини причини відмови;

– Аналіз видів і наслідків відмов;

– Аналіз дерева несправностей;

– Діаграма Ісікави або «риб’ячий скелет»;

– Аналіз Парето;

– Складання карти першопричини.

Оцінку причин часто починають з дослідження спочатку очевидних фізичних причин, далі вивчають причини, пов’язані з людським фактором, і вже потім переходять до вивчення прихованих причин управління або основних причин. Для того щоб застосування коригувальних дій було ефективним, залучені сторони повинні мати можливість керувати виявленими в процесі аналізу причинними факторами або усунути їх.

Вихідні дані

Вихідні дані методу RCA включають в себе:

– Документацію щодо зібраних даних та об’єктивних свідченнях;

– Розглянуті гіпотези;

– Висновок про найбільш ймовірні першопричини відмов і втрат;

– Рекомендовані та коригувальні дії.

Переваги та недоліки

Перевагами методу є можливість:

– Залучення до робочої групи технічних експертів;

– Використання структурованого аналізу;

– Розгляду всіх імовірних гіпотез;

– Документування отриманих результатів;

– Обов’язкового впровадження заключних рекомендацій.

Недоліки методу RCA полягають у наступному:

– Відсутня можливість залучення необхідних технічних експертів.

– Критичні об’єктивні свідчення можуть бути втрачені в момент відмови або під час прибирання.

– Обмеження за часом і ресурсами можуть не дозволити робочій групі провести всебічну оцінку ситуації.

– Іноді неможливо впровадити розроблені рекомендації.

Завдання 6. Методи оцінки ризику. Аналіз рівнів захисту. Метод LOPA

Короткий огляд

Метод LOPA – Layers of Protection Analysis – метод змішаної оцінки ризику, пов’язаного з небажаною подією або сценарієм. Метод спрямований на аналіз достатності заходів по управлінню або зниження ризику.

Метод LOPA заснований на виборі пар причин і наслідків та ідентифікації рівнів захисту, які можуть запобігти причині, що приводить до небажаного наслідку. Для визначення адекватності заходів зниження ризику до допустимого рівня необхідно провести розрахунок наслідків.

Область застосування

Метод LOPA може бути використаний як якісний метод дослідження рівнів захисту між небезпекою або причинним подією і результатом. Зазвичай змішаний підхід застосовують для досягнення більшої точності після HAZOP або PHA.

Метод LOPA забезпечує основу для визначення вимог до незалежних рівнів захисту (IPL – Independent Protection Layers) і рівням повноти безпеки (рівні SIL – Safety Integrity Levels) для автоматизованих систем, як встановлено в серії стандартів МЕК 61508 та 61511, а також при визначенні вимог до рівнів повноти безпеки SIL для автоматизованих систем безпеки. Метод LOPA може бути корисний для ефективного розподілу ресурсів, спрямованих на зниження ризику, шляхом застосування аналізу зниження ризику при впровадженні кожного рівня захисту.

Вхідні дані

Вхідними даними методу LOPA є:

– Основна інформація про ризик, включаючи небезпеки, причини і наслідки, аналогічно вхідним даним методу PHA;

– Інформація про фактичних і планових засобах управління;

– Частота причинних подій, оцінки імовірності відмови рівнів захисту, оцінки наслідків і допустимого ризику;

– Частота ініціюючих причин, оцінки ймовірності відмови рівнів захисту, оцінки наслідків і допустимого ризику.

Процес виконання методу

Метод LOPA зазвичай виконує група експертів із застосуванням такої процедури:

– Ідентифікація початкових причин виникнення небажаного результату і збір даних про їх частоту та наслідки;

– Вибір однієї пари причина-наслідок;

– Ідентифікація рівнів захисту, що запобігають причині, що приводить до небажаного наслідку, та аналіз їх ефективності;

– Ідентифікація незалежних рівнів захисту (IPL) (не всі рівні захисту є незалежними);

– Оцінка ймовірності відмови кожного IPL;

– Дослідження частоти початкових причин спільно з вірогідністю відмови кожного IPL і ймовірностями реалізації всіх умовних параметрів (прикладом умовного параметра є присутність або відсутність людини в зоні небезпечного впливу) для визначення частоти виникнення небажаного наслідки.

При дослідженні враховують порядок значень частот і ймовірностей;

– Порівняння розрахункового рівня ризику з допустимим для визначення необхідності у подальшому захисті.

Незалежний рівень захисту IPL – система пристроїв або дій, які здатні попередити реалізацію сценарію, який приводить до небажаного наслідку, і забезпечити незалежність причин подій чи рівнів захисту, пов’язаних зі сценарієм. Незалежними рівнями захисту IPLs є:

– Конструктивні особливості проекту;

– Фізичні пристрої захисту;

– Системи блокування і відключення;

– Аварійна сигналізація і можливості ручного втручання оператора;

– Фізичний захист при реалізації події;

– Системи аварійного реагування (процедури і перевірки, які не відносяться до IPLs).

Вихідні дані

Вихідними даними методу є рекомендації щодо подальшого застосування засобів управління та їх ефективності для зниження ризику. Метод LOPA є одним

з методів, використовуваних при оцінці SIL для систем безпеки і автоматизованих систем.

Переваги та недоліки

Перевагами методу LOPA є наступні:

– Метод вимагає для застосування меншого часу і ресурсів, ніж метод аналізу дерева несправностей або повної кількісної оцінки ризику і є більш точним, ніж якісний метод експертних оцінок.

– Метод LOPA допомагає ідентифікувати найбільш критичні рівні захисту і забезпечити їх ресурсами.

– Даний метод допомагає ідентифікувати операції, системи та процеси з недостатнім рівнем захисних заходів.

– Метод спрямований на найбільш серйозні небажані наслідки.

Недоліками методу є наступні:

– Метод LOPA дозволяє розглядати одну пару причина-наслідок і один відповідний сценарій при одноразовому до нього зверненні. Даний метод не охоплює складні взаємодії між ризиками або засобами управління.

– Кількісна оцінка ризику не завжди може бути отримана для загальних видів відмов.

– Метод LOPA не застосовується до складних сценаріїв в ситуаціях з великою кількістю пар причин-наслідків або з наслідками, що зачіпають різні причетні сторони.

Посилання на стандарти

МЕК 61508 (всі частини) Функціональна безпека систем електричних, електронних, програмованих електронних, пов’язаних з безпекою [23].

МЕК 61511 Безпека функціональна. Система безпеки, що забезпечується приладами для сектора обробної галузі промисловості[24].

Стандарт IEC 61508.

Функціональна безпека електричних, електронних і програмованих електронних систем, пов’язаних з безпекою "(Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems).

Стандарт Міжнародної Електротехнічної Комісії (International Electrotechnical Commission) IEC 61508 – "Функціональна безпеку електричних, електронних і програмованих електронних систем, пов’язаних з безпекою" – це міжнародний стандарт, розроблений для визначення систем безпеки (Safety Related Systems – SRS) загального вигляду.

Стандарт може використовуватися для будь-яких галузей промисловості, де є необхідність у використанні програмованих систем безпеки. Дата офіційного затвердження стандарту – 2000 рік. В цілому стандарт досить складний для сприйняття не тільки з-за свого величезного обсягу (більше 400 сторінок густого тексту двома мовами – англійською і французькою), але й надзвичайно ускладненою і заплутаною термінології. Стандарт визначає концепцію Моделі життєвого циклу системи безпеки, аналогічну ISA 84.01–96 (див. рис. 1 – 3). Загальна схема моделі життєвого циклу, яку відтворює і структура самого стандарту IEC 61508, наведена в першому розділі цієї роботи "Постановка задач автоматизації", рис. 1. Модель життєвого циклу системи встановлює, що рівень допуску системи не обмежується початковим рівнем допуску до якого входять пристрої, включаючи датчики і виконавчі механізми.

IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511 Functional safety – Safety instrumented systems for the process industry sector

Рівень допуску системи, точно так само, як і рівень допуску людини, повинен визначатися і підтверджуватися для всіх стадій і етапів на всьому життєвому шляху:

- Зародження ідеї;
- Попереднє обстеження і оцінка;
- Проектування;
- Експлуатація;
- Випробування, перевірка і техобслуговування.

Стандарт є безпекою від "неприпустимого ризику". Іншими словами, абсолютної безпеки досягти неможливо, можна тільки знизити ризик до припустимого рівня. Стандарт визначає 4 рівня інтегральної безпеки (Safety Integrity Level – SIL) залежно від конкретної імовірності відмови виконання необхідної функції (Probability of Failure on Demand – PFD):

Рівні безпечного допуску SIL за стандартом IEC 61508

4 – Захист від загальної катастрофи

3 – Захист обслуговуючого персоналу і населення

2 – Захист устаткування та продукції, захист від травматизму

1 – Захист устаткування та продукції

Модель життєвого циклу електричної, електронної, програмованої електронної системи безпеки (E / E / PES) наведено на рис.1.

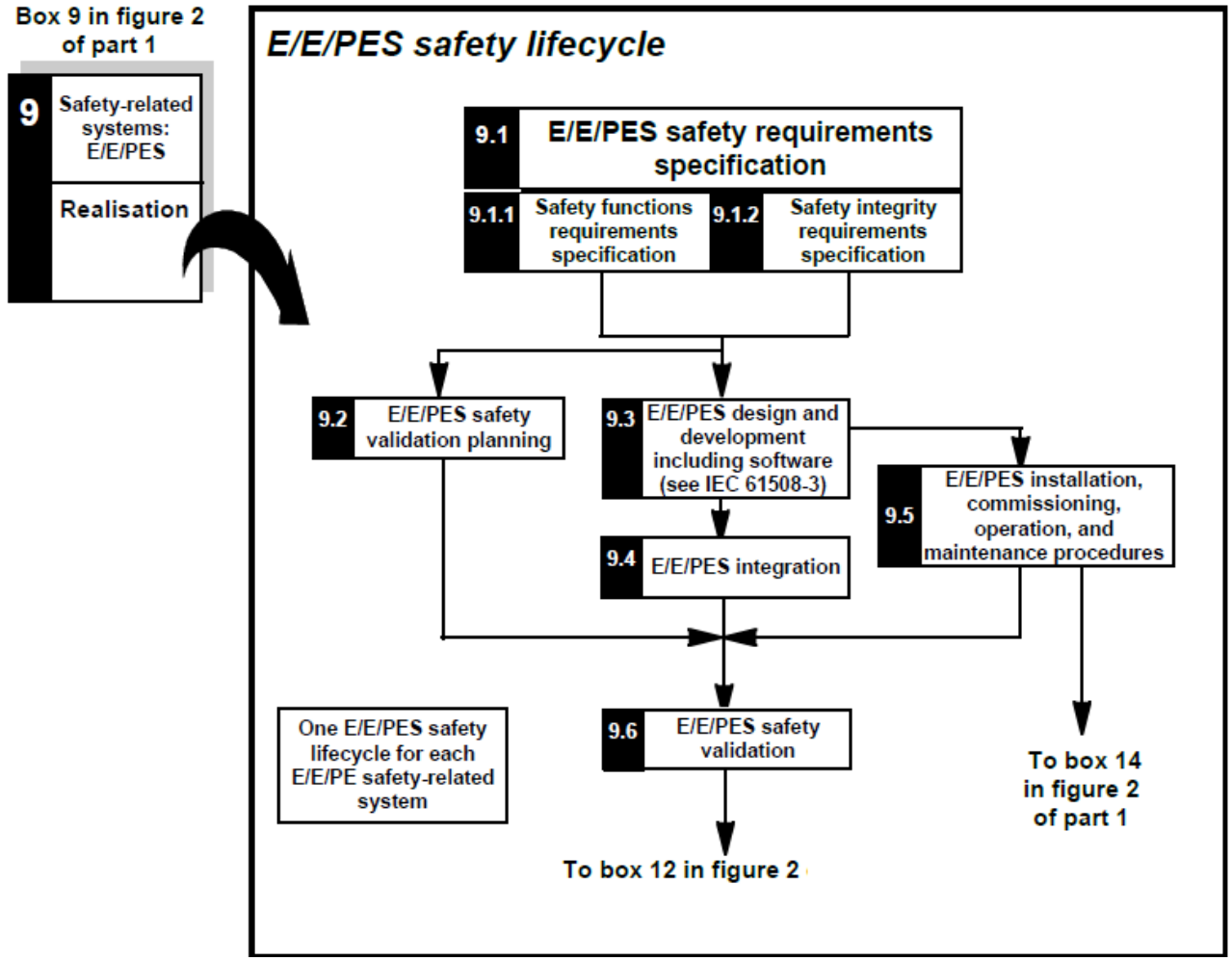

Рисунок 1 – Модель життєвого циклу програмного забезпечення

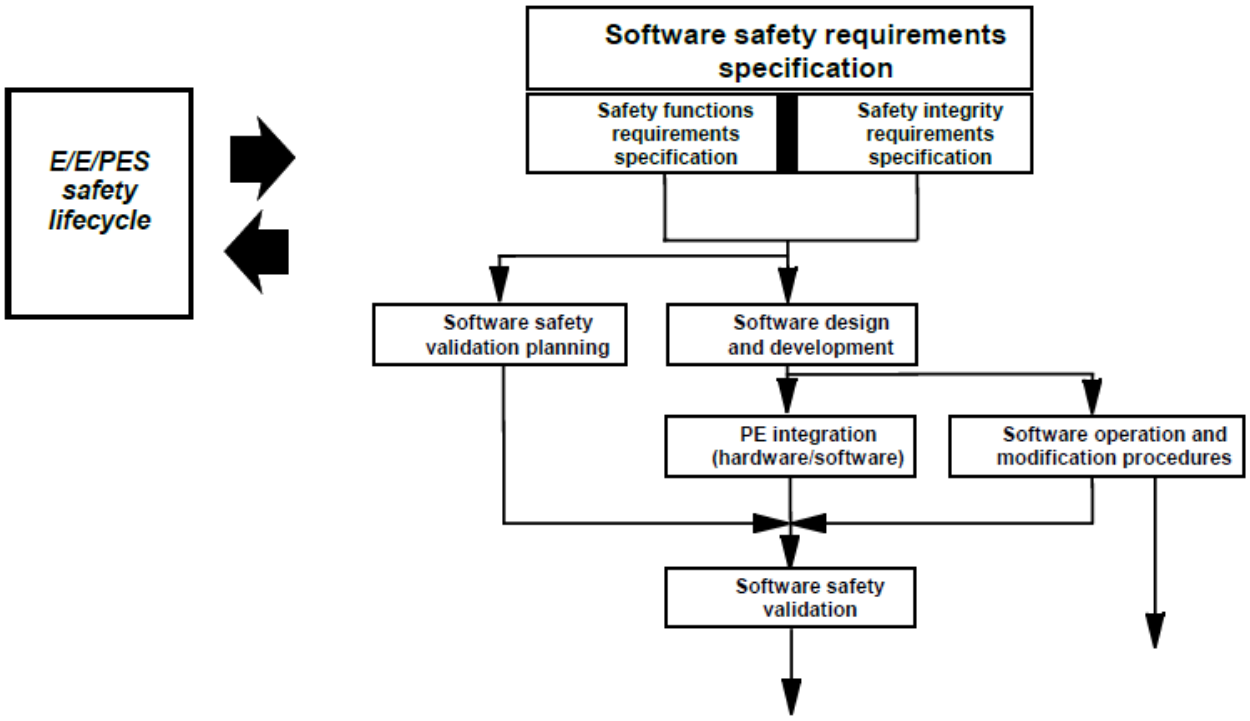

Рисунок 2 – Взаємодія моделей життєвого циклу електричної, електронної, програмованої електронної системи безпеки (E / E / PES) і програмного забезпечення

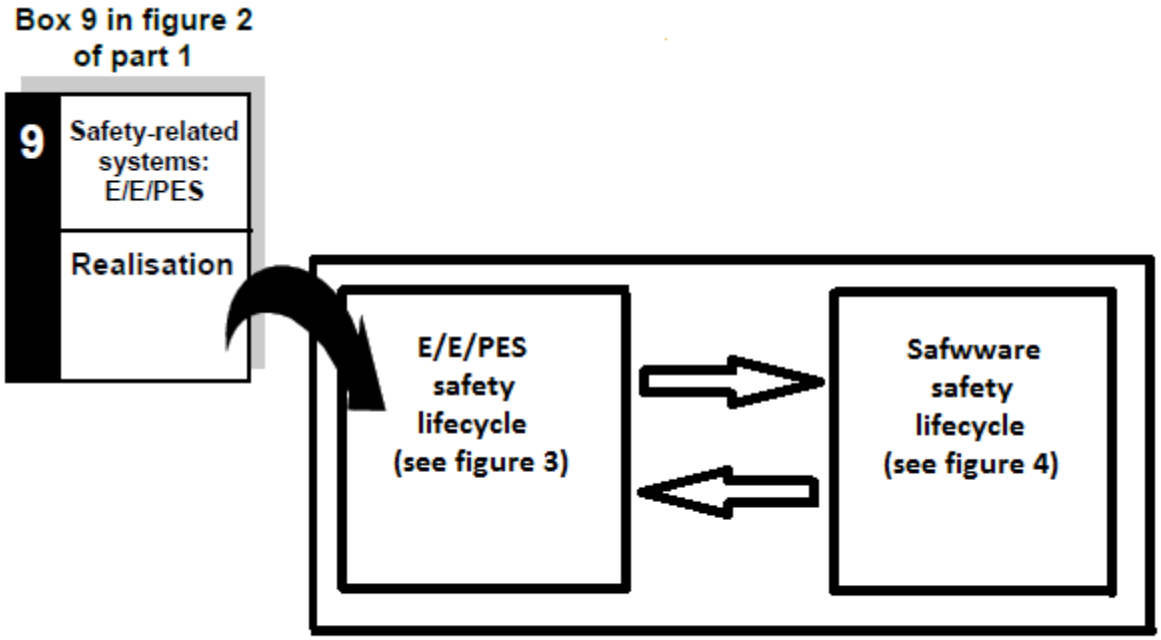

Рисунок 3 – Взаємодія моделей життєвого системи безпеки (E / E / PES) і програмного забезпечення

При цьому необхідно розуміти, що, наприклад, прийняття рівня допуску SIL1 означає, що рівень небезпеки процесу та обмеження на економічні втрати при відмові системи захисту низькі настільки, що системі дозволяється 10% відмов виконання функцій захисту. Відповідно, 90% надійність означатиме, що з кожних десяти випадків перевищення, наприклад, рівня в ємності, в одному випадку з цих десяти відбудеться переповнення ємності. Фактор зниження ризику також потребує правильної інтерпретації. Наприклад, збільшення фактора зниження ризику до 100 і більше років при рівні допуску SIL2 зовсім не означає, що дана конкретна система здатна пропрацювати без небезпечних відмов і помилкових спрацьовувань цю саму сотню років. Це значення означає, що із сотні одночасно працюючих систем одна система протягом одного року призведе процес до небезпечної відмови.

Зрештою, завдання рівня допуску SIL ґрунтується на необхідній величині зниження ризику, яка визначається в ході аналізу небезпеки процесу.

Звичайно, кожне підприємство вільно самостійно приймати рішення, і встановлювати свої вимоги до систем безпеки на основі власної технічної політики. Однак сучасні стандарти безпеки встановлюють і вимагають від підприємств відповідності розпорядженням, виробленим на основі досвіду експлуатації та аналізу причин аварій великого числа вибухопожежонебезпечних виробництв. Сказане означає, що в будь-якому випадку вибір рівня інтегральної безпеки і відповідної йому системи захисту повинен бути ретельно проаналізований, обґрунтований і точно документований. Діаграма ризиків і рівні допуску стандарту IEC 61508 представлені на рис. 4.

Стандарт визначає вимоги до професійної підготовки та кваліфікації фахівців, що визначають рівень вимог до систем безпеки для конкретного процесу. На відміну від усіх попередніх стандартів безпеки, стандарт IEC 61508 передбачає безпосередню участь технологічного персоналу в забезпеченні функцій безпеки. Разом з тим, у стандарті робиться застереження, що конкретні вимоги до технологічного та обслуговуючого персоналу повинні встановлюватися в галузевих стандартах (і в стандартах підприємства), які повинні розроблятися з урахуванням загальної методології безпеки, яка визначається даним стандартом.

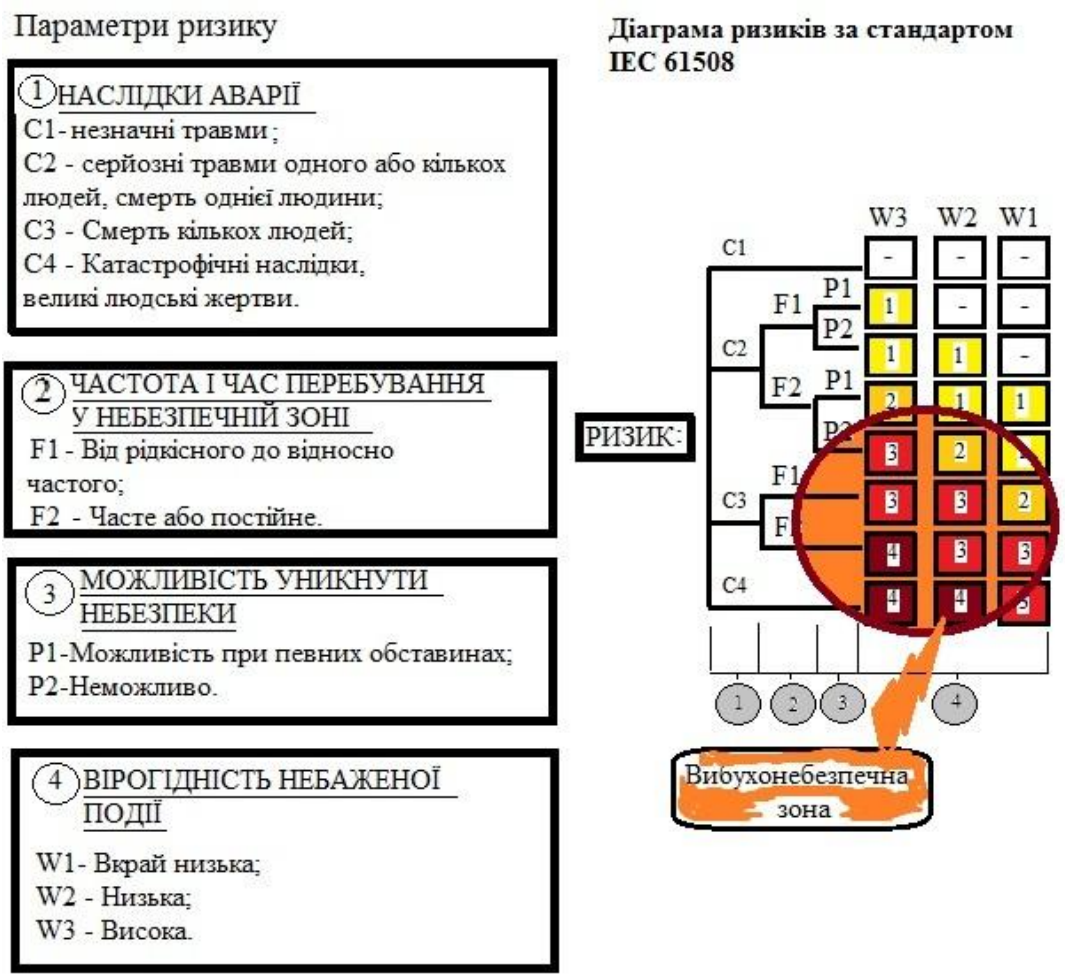

Рисунок 4 – Діаграма ризиків і рівні допуску стандарту IEC 61508

У найзагальнішому вигляді, стандарт IEC 61508:

1. Визначає Модель розвитку системи безпеки.

2. Визначає два підходи до систем безпеки:

– Системи, яка забезпечує захист і безперервність контролю за середній частоті небезпечних відмов;

– Системи, що забезпечує захист і контроль за середньою імовірністю небезпечної відмови протягом зумовленого інтервалу часу.

3. Визначає концепцію безпечного допуску.

4. Встановлює 4 рівня безпечного допуску (SIL).

Структура і параметри ризику стандарту IEC 61508 запозичені запросто і без церемоній з німецького стандарту DIN 19250. При цьому структури діаграм параметрів ризику для DIN і IEC повністю збігаються. Параметри ризику за стандартом IEC 61508 (див. рис. 4).

Травматизм

C1 – Незначні травми

C2 – Серйозні травми одного або кількох людей, смерть однієї людини

C3 – Смерть кількох людей

C4 – Катастрофічні наслідки, великі людські втрати.

Тривалість перебування в небезпечній зоні

F1 – Від рідкісного до відносно частого

F2 – Часте або постійне.

Запобігання небезпеки

P1 – Можливо при певних обставинах

P2 – Неможливо.

Імовірність небажаної події

W1 – Вкрай низька

W2 – Низька

W3 – Висока.

Стандарт IEC 61511 Функціональна безпека: Обладнані під безпеку системи для переробного сектора промисловості ". Стандарт IEC 61511 "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" – це міжнародний стандарт, розроблений для спільного використання з IEC 61508. На додаток до стандарту IEC 61508, який визначає загальні вимоги безпеки, в 2004 році МЕК прийняла стандарт безпеки технологічних процесів IEC 61511.

Стандарт IEC 61508 спочатку призначався для виробників і постачальників устаткування. Стандарт IEC 61511 призначений для проектувальників систем безпеки, фахівців з їх інтегруванню в процес – розробників, і користувачів систем управління виробничими і технологічними процесами.

Стандарту IEC 61511 повинні відповідати системи безпеки, призначені для захисту технологічних процесів в нафтовій, газовій, хімічній, нафтохімічній та інших галузях промисловості. Сенсори, логічні пристрої та виконавчі елементи стандартом IEC 61511 також розглядаються як складові елементи системи безпеки. Стандарт також розглядає інтерфейси з іншими рівнями контролю та управління на відповідність загальним вимогам безпеки виробництва і навіть людської спільноти (рис. 5).

Аналогічно стандарту IEC 61508, стандарт IEC 61511 визначає дві головні концепції, які лежать в основі його практичного застосування:

1. Життєвий цикл системи безпеки;

2. Інтегральний рівень безпеки.

<u>Концепція рівнів захисту згідно IEC 61511</u>

Стандарт охоплює повний життєвий цикл системи:

1. Проектування;
2. Складання;
3. Впровадження;
4. Експлуатація;
5. Обслуговування;
6. Модифікація;
7. Списання системи.

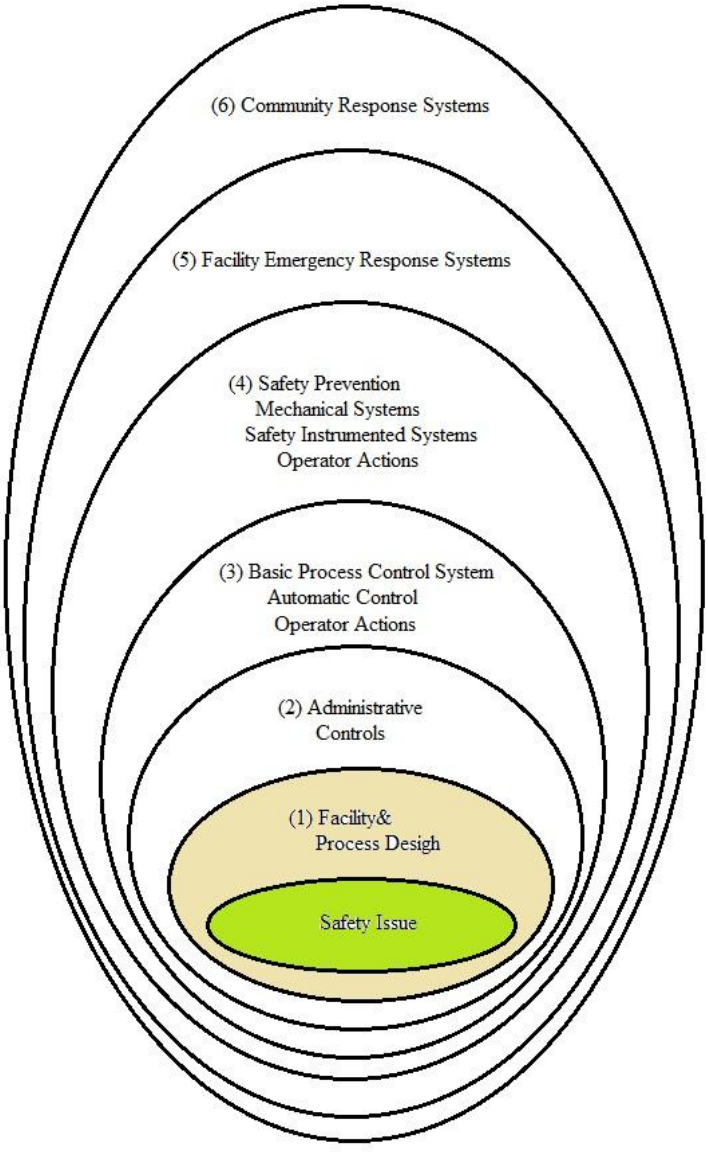

Рисунок 5 – Рівні контролю та управління на відповідність загальним вимогам безпеки виробництва (людської спільноти)

При розгляді життєвого циклу системи:

- Кількісно оцінюються ризики технологічного процесу,
- Визначаються вимоги до системи безпеки, що включає сенсори і виконавчі елементи,
- Розглядаються і проектуються рівні управління і захисту,
- Визначається архітектура системи безпеки, що забезпечує захист від ризиків процесу.

Так само, як і стандарт IEC 61508, стандарт IEC 61511 має 4 рівня інтегрального допуску. Але на відміну від стандарту загального призначення IEC 61508, стандарт IEC 61511 не рекомендує розглядати катастрофічні процеси, відповідні найвищим рівню вимог SIL4, як області застосування програмованих електронних систем.

Ідентифікація інтегрального рівня безпеки SIL.

Рівень допуску системи безпеки може розглядатися як статистичне уявлення відповідності системи заданому інтегральному рівню безпеки. При цьому необхідно ясно розуміти, що дані вимоги ставляться спочатку до кожної окремої функції, що включає в себе і сенсори, і логічні пристрої, і виконавчі елементи. Некоректно стверджувати, що окрема одиниця обладнання має якийсь власний інтегральний рівень безпеки.

Деякий компонент обладнання системи може бути схвалений на застосування по певному рівню SIL, але наявність сертифікату складає всього лише незначну частину загальних зусиль з безпеки, оскільки на відповідність необхідному рівню повинні бути перевірені значення ймовірностей відмови всіх комплексних критичних функцій в конкретному додатку. І тільки потім можуть бути визначені значення інтегральних показників надійності всього програмно-технічного комплексу системи.

Система тільки тоді здатна досягти необхідного рівня інтегральної безпеки, коли весь технологічний цикл було розглянуто на відповідність даному рівню.

Необхідно впевнитися і закріпити документально, що:

- Архітектура системи відповідає специфікації;
- Всі компоненти системи знаходяться на своїх місцях і правильно працюють;
- Функції системи реалізовані відповідно до Технічного завдання;
- Документація розроблена відповідно до проекту.

Тільки в такому випадку може з’явитися впевненість, що SIL дійсно є інтегральним показником створеної системи, і враховує всі життєво необхідні фактори:

- Рівень допуску та окремих пристроїв, і системи в цілому;
- Опис та ідентифікація можливих відмов, і відмов спільного походження;
- Процедури попередніх і періодичних випробувань;
- Вимоги до експлуатації;
- Метрологічне забезпечення;
- Діагностика та технічне обслуговування;
- Навчання та кваліфікація персоналу.

Завдання 7. Методи оцінки ризику. Аналіз дерева рішень.

Короткий огляд

Метод аналізу дерева рішень дозволяє послідовно представити альтернативні варіанти рішень з їх вихідними даними і відповідної невизначеністю. Як і при виконанні аналізу дерева подій, побудова слід починати з початкової події або рішення що прийнято. Далі необхідно побудувати шляхи розвитку подій, визначити результати, які можуть бути отримані при реалізації подій, і різні рішення, які можуть бути прийняті.

Область застосування

Метод дерева рішень зазвичай застосовують в управлінні ризиком проектних рішень та в інших випадках, коли необхідно вибрати найкращий спосіб дій в ситуації невизначеності. Графічне представлення може бути обґрунтуванням прийнятих рішень.

Вхідні дані

Вхідними даними є план проекту із зазначенням пунктів, по яких необхідно прийняти рішення, інформація про можливі результати прийнятих рішень і події, що впливають на ці рішення.

Процес виконання методу

Побудова дерева рішень починають з початкового рішення, наприклад рішення про відновлення проекту А або проекту В. Оскільки можуть бути реалізовані два гіпотетичних проекту, то далі можуть відбутися відповідні події і можуть бути прийняті різні рішення. Цей процес представляють у формі дерева за аналогією з деревом подій. Імовірність подій може бути оцінена разом з оцінкою витрат та/або ефективності остаточного результату обраного шляху розвитку подій.

Інформація, що стосується найкращого шляху прийняття рішень, має логічну форму, отже, можливий розрахунок найбільшого середнього значення, розрахованого як добуток всіх умовних ймовірностей на даному шляху прийняття рішень на значення отриманого результату.

Вихідні дані

Вихідними даними методу є:

– Логічний аналіз ризику, що відображає різні варіанти можливих рішень;

– Очікуване значення ризику для кожного можливого шляху рішень.

Переваги та недоліки

Перевагами методу є наступні:

– Метод забезпечує точне графічне представлення всіх деталей вирішення проблеми.

– Метод дозволяє розрахувати кращі шляхи вирішення проблеми.

Недоліками методу є наступні:

– Великі дерева рішень занадто складні для обміну інформацією із зацікавленими сторонами.

– Застосування діаграми дерева рішень може привести до зайвого спрощення ситуації.

Завдання 8. Методи оцінки ризику. Аналіз впливу людського фактора. Метод HRA

Короткий огляд

Метод HRA – Human Reliability Assessment, застосовують для оцінки впливу дій людини, в тому числі помилок оператора, на роботу системи.

У багатьох процесах існує можливість помилки оператора, особливо у випадку якщо у оператора недостатньо часу для прийняття рішень. Імовірність того, що події розвиватимуться таким чином, що приведуть до серйозних проблем, повинна бути мала. Проте в деяких випадках дія оператора може бути єдиним захистом, що запобігає катастрофічні наслідки відмови.

Значимість оцінки дій оператора підтверджується подіями, в яких критичні помилки оператора сприяли катастрофічного розвитку подій. Ці події показують неприйнятність оцінок ризику, які враховують лише технічні та програмні засоби системи. Вони показують небезпеку ігнорування помилок оператора. Більш того, оцінка дій оператора дозволяє виявити помилки, які можуть негативно впливати

на продуктивність, і визначити способи усунення даних помилок та інших відмов (технічних і програмних засобів).

Область застосування

Метод HRA може бути використаний як в якісному, так і в кількісному вигляді. Якісна оцінка дій оператора може бути використана для ідентифікації його можливих помилок і їх причин, що дозволяє знизити ймовірність таких помилок. Крім того, метод HRA може бути використаний для отримання кількісних даних про відмови, пов'язаних з помилками оператора, для застосування FTA або інших методів.

Вхідні дані

Вхідними даними методу HRA є:

– Інформація для визначення завдань, що виконуються операторами;

– Дані про типові помилки, що зустрічаються на практиці, і їх причини;

– Експертні оцінки помилок оператора (людини) та їх кількісне вираження.

Процес виконання методу

Процес HRA включає наступні етапи:

– Постановка завдання. Визначення типів дій оператора (людини), які повинні бути досліджені і оцінені.

– Аналіз завдання. Визначення способів виконання завдання і допоміжних засобів, необхідних для її виконання.

– Аналіз помилки оператора. Визначення відмов, що виникають у процесі виконання завдання, можливих помилок оператора і способів їх усунення.

– Подання. Визначення того, як ці помилки при виконанні завдання в поєднанні з іншими подіями, пов'язаними з устаткуванням, програмним забезпеченням і впливають факторами, можуть бути використані для розрахунку ймовірності відмови системи в цілому.

– Попередня перевірка. Визначення помилок або завдань, що вимагають детальної кількісної оцінки.

– Кількісна оцінка. Визначення ймовірності помилок оператора і відмов при виконанні завдання.

– Оцінка впливу. Визначення значущості помилок або завдань, тобто помилок і завдань, які більшою мірою впливають на забезпечення надійності або прийнятного рівня ризику.

– Скорочення помилок. Визначення способів скорочення кількісних помилок оператора.

– Документування. Визначення інформації та деталей аналізу HRA, які повинні бути зареєстровані.

На практиці процес HRA найчастіше виконують поетапно, хоча іноді деякі його частини (наприклад, аналіз завдань та ідентифікацію помилок) проводять паралельно.

Вихідні дані

Вихідними даними методу є:

– Перелік помилок, які можуть відбутися, і методи їх скорочення (переважно через модернізацію системи);

– Види помилок, причини і наслідки типових помилок;

– Якісна чи кількісна оцінка ризику розглянутих помилок.

Переваги та недоліки

Перевагами методу HRA є наступні:

– Метод HRA забезпечує формалізований спосіб дослідження помилок оператора при оцінці ризику для систем, в яких персонал відіграє важливу роль.

– Формалізоване дослідження видів і помилок оператора і способів дозволяє зменшити ймовірність відмов, викликаних цими помилками.

Недоліками методу є наступні:

– Складність і різноманіття способів поведінки операторів створює значні труднощі при визначенні простих видів відмови та оцінки їх ймовірності.

– Неможливо описати багато дій операторів за допомогою понять «працездатний» і «непрацездатний» стан. Метод HRA важко застосувати в ситуації з частковими відмовами або відмовами по причині прийняття невідповідних рішень (див. приклад на рис. 6).

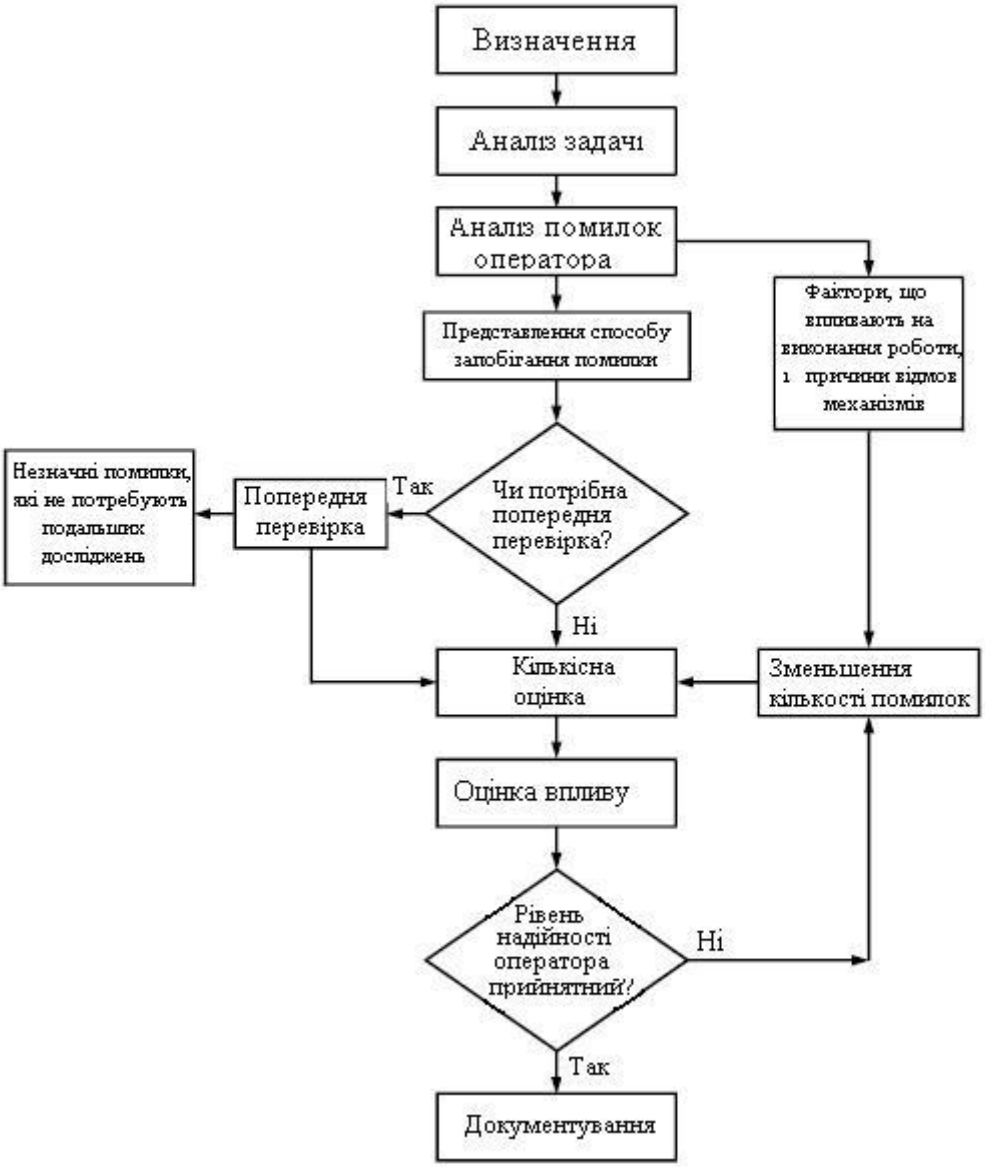

Рисунок 6 – Приклад аналізу впливу людського фактору

Завдання 9. Методи оцінки ризику. Аналіз «краватка-метелик»

Короткий огляд

Аналіз «краватка-метелик» являє собою схематичний спосіб опису та аналізу шляху розвитку небезпечної події від причин до наслідків. Даний метод поєднує дослідження причин події за допомогою дерева несправностей і аналіз наслідків за допомогою дерева подій. Однак основна увага методу «краватка-метелик» сфокусовано на бар'єрах між причинами і небезпечними подіями і небезпечними подіями та наслідками. Діаграми «краватка-метелик» можуть бути побудовані на основі виявлених несправностей і дерев подій, але частіше їх будують безпосередньо в процесі проведення мозкового штурму.

Область застосування

Аналіз «краватка-метелик» використовують для дослідження ризику на основі демонстрації діапазону можливих причин і наслідків. Метод слід застосовувати в ситуації, коли складно провести повний аналіз дерева несправностей або коли дослідження в більшій мірі спрямоване на створення бар'єрів або засобів управління для кожного шляху відмови. Метод може бути корисний у ситуації, коли існують точно встановлені незалежні шляхи, що призводять до відмови. Аналіз «краватка-метелик» часто значно більше простий для розуміння, ніж аналіз дерева подій або дерева несправностей, і, отже, він може бути корисний для обміну інформацією при використанні більш складних методів.

Вхідні дані

Вхідними даними методу є інформація про причини та наслідки небезпечних подій, ризиків, бар'єрів та засобах управління, які можуть їм запобігти, пом'якшити або стимулювати.

Процес виконання методу

Аналіз «краватка-метелик» слід будувати у відповідності з наступною процедурою:

a) Визначення небезпечної події, обраного для аналізу, і відображення його в якості центрального вузла «краватки-метелика»;

b) Складання переліку причин події за допомогою дослідження джерел ризику (або небезпеки);

c) Ідентифікація механізму розвитку небезпеки до критичного події;

d) Проведення лінії, що відокремлює причину від події, що дозволяє сформувати ліву сторону метелика. Додатково можуть бути ідентифіковані і включені в діаграму фактори, які можуть призвести до ескалації небезпечної події та її наслідків;

e) Нанесення поперек лінії вертикальних перешкод, відповідних бар'єрам, які запобігають небажаним наслідкам. Якщо визначені фактори, які можуть викликати ескалацію небезпечної події, то додатково можуть бути представлені бар'єри, що попереджають подібну ескалацію. Даний підхід може бути використаний для позитивних наслідків, коли перепони відображають засоби управління, що стимулюють появу і розвиток події;

f) Ідентифікація в правій стороні метелика різних наслідків небезпечної події і проведення ліній, що з’єднують центральну подію з кожним можливим наслідком;

g) Зображення бар’єрів в якості перешкод у напрямку до наслідку. Даний підхід може бути використаний для позитивних наслідків, коли перепони відображають засоби управління, що забезпечують появу сприятливих наслідків;

h) Відображення під діаграмою «краватка-метелик» допоміжних функцій управління, що відносяться до засобів управління (таких як навчання і перевірка), і з’єднання їх з відповідним засобом управління;

У діаграмі «краватка-метелик» можуть бути застосовані деякі види кількісної оцінки, наприклад, в ситуації, коли незалежні шляхи і відома ймовірність конкретних наслідків або результатів (рис.7). Подібна кількісна оцінка необхідна для забезпечення ефективності управління. Однак необхідно враховувати, що в багатьох ситуаціях шляхи та бар’єри взаємозалежні, і засоби управління можуть бути пов’язані з обраним методом оцінки, отже, ефективність управління є невизначеною. Кількісну оцінку для аналізу «краватка-метелик» часто виконують за допомогою методів FTA і ETA.

Вихідні дані

Вихідними даними методу є проста діаграма, що показує основні шляхи небезпечних подій і встановлені бар’єри, спрямовані на запобігання або пом’якшення небажаних наслідків та/або посилення і прискорення очікуваних наслідків.

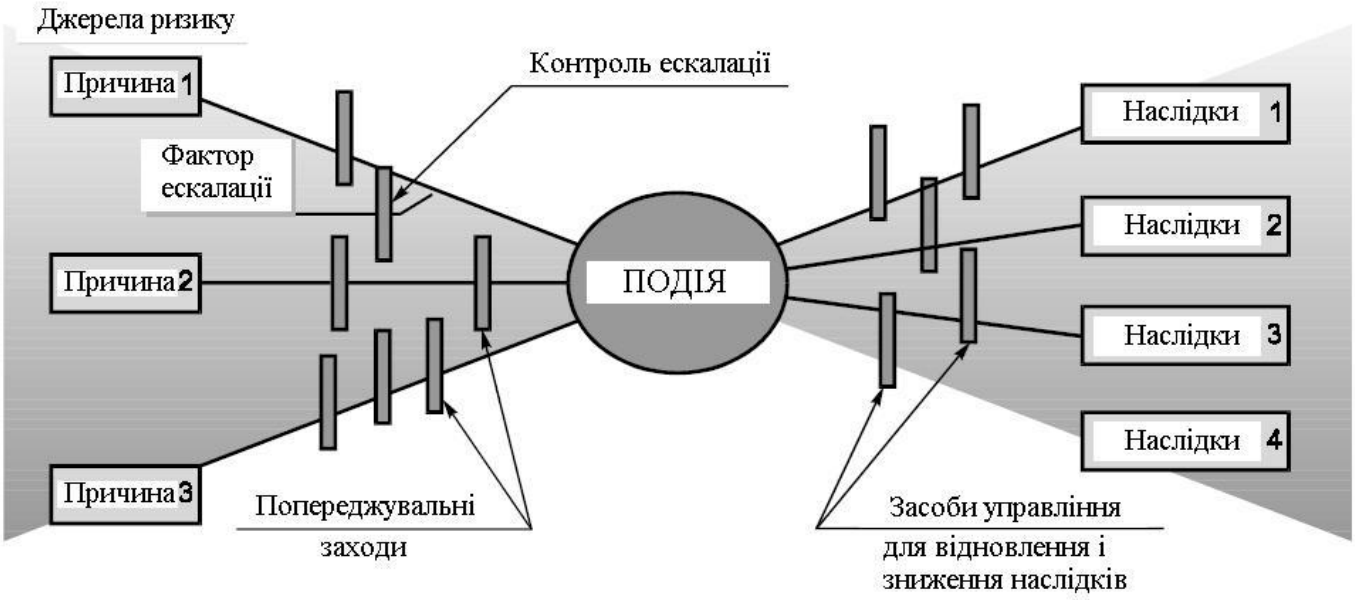

Рисунок 7 – Приклад діаграми «краватка-метелик» для небажаних наслідків

Переваги та недоліки

Перевагами методу аналізу «краватка-метелик» є наступні:

– Метод забезпечує наочне, просте і ясне графічне представлення проблеми.

– Метод орієнтований на засоби управління, які спрямовані на попередження та/або зменшення наслідків небезпечних подій, і оцінку їх ефективності.

– Метод може бути застосований у відношенні сприятливих наслідків.

– Застосування методу не потребує залучення висококваліфікованих експертів.

Недоліками методу є наступні:

– Метод не дозволяє відображати сукупності причин, що виникають одночасно і викликають наслідки (випадок, коли в дереві несправностей, що відбиває ліву сторону діаграми, знаходиться логічний елемент «І»).

– Метод може представити складні ситуації в надмірно спрощеному вигляді, особливо при застосуванні кількісної оцінки.

Завдання 10. Методи оцінки ризику. Аналіз прихованих дефектів і аналіз паразитних ланцюгів (SA - Sneak Analysis).

Короткий огляд

Аналіз прихованих дефектів (SA – Sneak Analysis) є методом ідентифікації помилок проектування. До прихованих дефектів можуть бути віднесені неявні дефекти комп'ютерного обладнання, програмного забезпечення або їх поєднання, що можуть спричинити подію або перешкоджати реалізації очікуваної події і не є наслідком відмови компонентів. Ці дефекти мають випадковий характер і можуть бути не виявлені під час випробувань і тестування. Приховані дефекти можуть призвести до невідповідного виконання технологічних операцій, відмови системи, затримок у роботі програм і навіть травмування або загибелі персоналу.

Область застосування

Аналіз паразитних ланцюгів (SCA – Sneak Circuit Analysis) був розроблений в кінці 1960–х років для НАСА з метою перевірки функціональних можливостей проекту. Даний метод був використаний для виявлення паразитних електричних ланцюгів, а також для розробки рішень з ізолювання кожної функції. У міру технологічного прогресу методи аналізу паразитних ланцюгів також удосконалювалися. Аналіз прихованих дефектів включає і значно перевершує за обсягами аналіз паразитних ланцюгів. Він дозволяє виявляти проблеми як у технічних, так і в програмних засобах. Методи аналізу прихованих дефектів можуть об'єднувати різні типи аналізу, наприклад аналіз дерева несправностей, аналіз видів і наслідків відмов (FMEA), оцінку надійності тощо, в один аналіз, менш витрат за часом і коштами.

Вхідні дані

Для аналізу прихованих дефектів характерне застосування різних методів (деревовидні схеми, схеми типу «ліс», допоміжні фрази або питання, що допомагають фахівцеві, що проводить аналіз, ідентифікувати наявність прихованих дефектів) для виявлення конкретного типу проблеми. Деревовидні схеми і схеми типу «ліс» – це топологічні угруповання досліджуваної системи. Кожна деревоподібна схема являє собою під функцію і показує все вхідні дані, які можуть вплинути на вихідні дані розглянутої функції системи. Схеми типу «ліс» будують шляхом об'єднання деревовидних схем, які беруть участь у формуванні вихідних даних конкретної системи. Належним чином побудована схема тип «ліс» відображає вихідні дані системи з урахуванням всіх пов'язаних з

ними вхідних даних. Поряд з іншими вхідними даними вони стають вхідними даними для аналізу.

Процес виконання методу

Виконання методу передбачає наступні етапи:

– Підготовка даних;

– Побудова деревовидної схеми;

– Оцінка шляхів схеми;

– Складання заключних рекомендацій та звіту.

Вихідні дані

Паразитний ланцюг – це непередбачений спосіб або логіка функціонування системи, які за певних умов можуть ініціювати несприятливу функцію або пригнічувати сприятливу функцію.

Паразитний ланцюг може бути присутнім у технічних засобах, програмному забезпеченні, дії оператора або їх поєднаннях. Паразитний ланцюг не є результатом відмови технічних засобів, а є прихованим станом, ненавмисно включеним в систему, програмний продукт або наслідком помилки оператора. Існує чотири категорії паразитних ланцюгів:

a) Паразитні канали: непередбачені канали, по яких струм, енергія або логічні послідовності проходять в непередбаченому напрямку;

b) Паразитний хронометраж: виникнення подій в непередбаченій або суперечливою послідовності;

c) Паразитні показання: невизначена або помилкова індикація режиму функціонування системи, яка може призвести до збою системи або стати причиною небажаної дії оператора;

d) Паразитні позначення: невідповідні або неточні позначення функцій системи, наприклад вводів системи, органів управління, каналів передачі інформації, які можуть викликати введення оператором невірних керуючих команд в систему.

Переваги та недоліки

Перевагами методу є наступні:

– Аналіз прихованих дефектів дозволяє ідентифікувати помилки проектування.

– При спільному використанні з дослідженням HAZOP метод дає можливість отримати найкращі результати.

– Метод може бути застосований до систем, які мають різні стани, наприклад, таким як виробництва безперервного або полу неперервної дії.

Метод має такі недоліки:

– Процес аналізу може відрізнятися в залежності від того, застосовується він до електричних ланцюгів, технологічних установок, механічного обладнання або програмним засобам.

– Метод залежить від правильності побудови деревовидних схем.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1	Березуцький В.В. , Адаменко М.І. Небезпечні виробничі ризики та надійність: навчальний посібник для студентів за напрямком підготовки 6.170202 «Цивільна безпека»/ В.В. Березуцький, М.І. Адаменко – Харків. : НТУ «ХПІ», 2016. – 385 с.

Допоміжна література

2	Методика визначення ризиків Міністерства праці та соціальної політики України 04.12.2002 №637
3	ISO 31000:2009 - Принципи та Керівництво з впровадження
4	ISO / IEC 31010:2009 - Управління ризиками - методи оцінки ризику
5	План ліквідації аварійних ситуацій (ПЛАС). Затверджено наказом Комітету по нагляду за охороною праці України 17.06.99 N 112, та було зареєстровано в Міністерстві юстиції України 30 червня 1999 р. за N 424/3717

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1.Видання кафедри «Охорони праці та навколишнього середовища» НТУ «ХПІ» - Доступ до ресурсу:

http://sites.kpi.kharkov.ua/SafetyOfLiving/Htm/metrazr-2.php

Методичні вказівки та завдання

до виконання самостійної роботи студентів

з дисципліни «Теорія ризиків»

для студентів спеціальності «Цивільна безпека»,

спеціалізації – Охорона праці

Укладач: БЕРЕЗУЦЬКИЙ Вячеслав Володимирович

Відповідальний за випуск проф. Березуцький В.В.

Роботу до видання рекомендувала проф. Пономаренко О.І.

В авторській редакції

План 2018 р., поз. 113
Підп. До друку 15.06.2018. Формат 60х84 1/12. Папір офсет.
Друк – різографія. Гарнітура Times New Roman. Ум. друк. арк. 1,95.
Наклад 50 прим. Зам. № Ціна договірна.

Видавничий центр НТУ «ХПІ».
Свідоцтво про державну реєстрацію ДК №5478 від 21.08.2017 р.
61002, Харків, вул. Кирпичова, 2

Надруковано у ФОП

Свідоцтво про державну реєстрацію фіз. особи - підприємця