

Винахід стосується способу та пристрою для експлуатації багаторозрядного лічильника у одному напрямку лічби.

На сьогодні відома безліч галузей застосування, де потрібно здійснювати підрахунок подій. Такими подіями можуть бути: частота застосування якогось приладу, проходження людей, транспортних засобів або предметів, реєстрація телефонних тактових імпульсів, а також реєстрація довжини пробігу, тобто кілометраж у легкових автомобілях або підрахунок годин роботи будь-якого приладу і, не в останню чергу, реєстрація часу роботи або присутності працівника на своєму робочому місці. Всі ці випадки відрізняються тим, що реєстрація мусить бути проведена з якомога більшою точністю, тобто, як правило, має місце великий діапазон числових значень. Крім того, у згаданих випадках зазвичай є потреба у тому, щоб результат лічильника не був придатний до маніпулювання, тобто щоб його не можна було скинути. Подібну вимогу можна, звичайно, виконати за допомогою однорозрядного лічильника, який здатен робити відлік вперед або назад лише від свого дотеперішнього стану. Це, наприклад, можна легко реалізувати за допомогою програмованого постійного запам'ятовуючого пристрою з електричним стиранням (ЕСПЗП=EEPROM), причому для кожного значення лічильника передбачають комірку ЕСПЗП, а ЕСПЗП допускає або тільки запис, або тільки стирання, залежно від того, підсумовує лічильник чи віднімає.

Згадана вимога щодо спроможності лічильника визначати якомога більший діапазон чисел приводить до того, що при такій реалізації запам'ятовуючий пристрій ЕСПЗП мусить мати відповідно багато комірок пам'яті. У цифровому вираженні це означає, що для досягнення, наприклад, максимального стану лічильника 225 потрібно мати точно 255 комірок пам'яті. Однак у наші дні більш звичною є тенденція надавати таким пристроям якомога меншу конструкцію. Застосування багаторозрядного лічильника на 8 розрядів, тобто на 8 комірок, приводить також до максимального стану лічби 255. Але такий багаторозрядний лічильник (8-розрядний двійковий лічильник) має той недолік, що при зміні наступного розряду попередній розряд відновлює свій початковий стан. Внаслідок цього реалізація багаторозрядного лічильника, який веде підрахунок лише у одному напрямку і одночасно не допускає маніпулювання, може бути здійснена з великими труднощами.

У документі EP 0321727 описано пристрій, у якому послідовно розміщені численні комірки ЕСПЗП. При цьому у свою чергу кілька рядів з'єднані між собою. Комірки пам'яті кожного ряду являють собою єдиний рівень коефіцієнтів значимості, причому зміст пам'яті одного ряду може бути стертим за допомогою логічної схеми контролю лише у тому випадку, коли відбувається перенесення у наступний вищий ряд. Описаний у цьому документі пристрій має такі ж недоліки, як зазначено вище, причому внаслідок впливу на логічну схему не можна гарантувати лічбу у одному напрямку. Подібний, але дещо більш високотратний пристрій описано у EP 0618591, причому для перезапису до кожного наступного більш високого ряду передбачено допоміжну комірку пам'яті, яка може бути запрограмованою, а потім знову стертою, і ця схема також є легко маніпульованою, оскільки допоміжні комірки пам'яті придатні як для запису, так і для стирання.

Із US 5264689 відома здатна до підзаряджування телефонна картка, яка має кредиторний лічильник та дебіторний лічильник. У кредиторному лічильнику при заряджуванні картки встановлюють максимальне числове значення. З кожною використаною одиницею комірка пам'яті перепрограмується, а дебіторний лічильник зростає. Як тільки числові значення дебіторного і кредиторного лічильників стають однаковими, карта вважається "порожньою". Тепер для заряджування картки спочатку треба збільшити кредиторний лічильник. Задля виключення недобросовісного використання обидва лічильники не можна повернути у первинне положення. Внаслідок цього при досягненні максимального значення лічильника картку більше не можна використовувати. Таким чином, перед винаходом стоїть задача створення способу та пристрою для експлуатації багаторозрядного лічильника, у якому простим шляхом був би підвищений захист від маніпулювання.

Згідно з винаходом цю задачу вирішують шляхом заходів, наведених у пунктах 1 та 5 формули винаходу.

Внаслідок одночасної експлуатації однорозрядного лічильника, який може лічити лише або вперед, або назад, та багаторозрядного лічильника, який здійснює лічбу власне кількості подій, та їх порівняння було встановлено, що пороховане значення багаторозрядного лічильника принаймні за порядком величин відповідає порохованому значенню однорозрядного лічильника. Шляхом поєднання порохованого значення однорозрядного лічильника з додатковими даними та перших автентифікаційних даних при обробці переданих далі автентифікаційних даних пороховане значення однорозрядного лічильника непомітно для спостерігача стає готовим до користування і може служити для визначення автентичності. Такими нескладними засобами виключається можливість маніпулювання, оскільки для перевірки на автентичність служить не лише встановлене ключове слово і/або випадкове число, передане заздалегідь контрольним пристроєм, а також і пороховане значення допоміжного лічильника, яке змінюється відповідно до можливостей цього допоміжного лічильника.

Подальше удосконалення здійснюють шляхом додаткового з'єднання з порохованим значенням багаторозрядного лічильника.

Наступна перевага виникає внаслідок того, що частина додаткових даних являє собою випадкове число, передане заздалегідь контрольним пристроєм.

Далі винахід описано за допомогою фігури, причому приклад виконання зображено у формі блок-схеми.

Зображений на фігурі приклад виконання має m-розрядний лічильник 11, де m=8. На зображенні його треба сприймати як 8-розрядний двійковий лічильник. Таким чином, лічильник може лічити від 0 до 255, тобто має 256 лічильних станів. Лічильник 11 з'єднаний із блоком 3 управління, який подає на лічильник 11 лічильний сигнал S11. З кожним надходженням лічильного сигналу S11 вміст лічильника 11 змінюється на одиницю, причому зміна відбувається у тому ж напрямку, що і попередня зміна. Це означає, що символічно зображений на фігурі лічильник 11 виконаний таким чином, що він може здійснювати лічбу або лише вперед, або назад. Поточний лічильний стан багаторозрядного лічильника 11 у вигляді сигналу Z11 порохованого значення надходять до логічної схеми контролю 4. Окрім того передбачено однорозрядний лічильник 1, який уданому прикладі виконання має "n" комірок, де "n"=16. Цей символічно зображений на

фігурі лічильник має таку конструкцію, що також може робити відлік лише у одному напрямку, а саме від 0 до 15, тобто має 16 лічильних станів. Однорозрядний лічильник 1 отримує від блоку 3 управління лічильний сигнал S1, після чого його пороховане значення змінюється на одиницю. Поточний лічильний стан однорозрядного лічильника 1 надходять до блоку 3 управління і у вигляді контрольного сигналу Z1 - до логічної схеми контролю 4. Логічна схема контролю 4 порівнює сигнал Z1 порохованого значення з контрольним сигналом Z1 і через контактний вивід Р надсилає до управління лічильником 5 сигнал, визначений залежно від порівняння.

Обидва лічильники 11 та 1 виконані як комірки ЕСППЗП. При цьому передбачено, що відповідно до відомого принципу роботи двійкового лічильника окремі комірки пам'яті можуть бути записані або стерті згідно з правилами відліку вперед або назад. Точно таким чином однорозрядний контрольний лічильник 1 складається із комірок ЕСППЗП, причому окремі комірки від 1 до "n" можуть або лише записуватись, або стиратися послідовно одна за одною. Логічна схема контролю 4 з'єднана з пам'яттю даних D, у якій накопичуються додаткові дані. При автентифікації пристрою логічна схема контролю 4 поєднує додаткові дані з порохованим значенням однорозрядного лічильника 1 і таким чином створює перші показання автентичності. Додаткові дані ідеально складаються із ключового слова та випадкового числа, переданого перед тим не зображеним контрольним пристроєм.

Коли пристрій отримує від контрольного пристрою через вхід Е запрошення до автентифікації, то автентифікаційні дані утворюються шляхом поєднання порохованого значення допоміжного лічильника 1 з додатковими даними і надходять із блоку 3 управління через вихід А. Одночасно блок 3 управління отримує пороховане значення багаторозрядного лічильника 11 і передає його також через вихід А до контрольного пристрою. Для контролю автентичності пороховане значення допоміжного лічильника реєструється або відновлюється у не зображеному контрольному пристрої, який має перевірити автентичність, і звідси утворюються другі автентифікаційні дані. Автентичність має місце, коли другі автентифікаційні дані співпадають із першими. Якщо автентичність є наявною, то обмін даними з пристроєм припиняється. Другі автентифікаційні дані виникають шляхом поєднання відновленого порохованого значення допоміжного лічильника 1 з допоміжними даними, якщо вони невідомі контрольному пристроєві і також передаються через вихід А. Як варіант можливо, щоб випадкове число було задане не контрольним пристроєм, а схемою, яку він перевіряє. Однак у такому разі випадкове число може бути частиною додаткових даних, які пересилаються, що не має місця у наведеному вище прикладі, оскільки тут другі автентифікаційні дані утворюються за допомогою заздалегідь заданого випадкового числа та додаткових даних, що передаються, якщо вони невідомі контрольному пристроєві.

Як інший варіант виконання можна також поєднувати пороховане значення багаторозрядного лічильника 11 з першими автентифікаційними даними. Аналогічно з вищезазначеним, це мусить також відбуватися в контрольному пристрої для створення других автентифікаційних даних, причому пороховане значення багаторозрядного лічильника не відновлюється, оскільки воно переноситься на контрольний пристрій як відоме.

Коли автентичність точно встановлена, відбувається подальший процес із зображених на фігурі. Принципово передбачено, що з кожним вхідним сигналом на вході Е від блоку управління 3 виходить лічильний сигнал S11. При цьому логічна схема контролю 4 перевіряє лічильні стани обох лічильників 1 та 11 за допомогою сигналу Z11 порохованого значення та контрольного сигналу Z1. Якщо обидва, наприклад, дорівнюють 0, то логічна схема контролю 4 визначає, що існує співпадіння, і контрольним сигналом Р дозволяє блоку 5 управління лічильником видати лічильний сигнал S11.

Крім того передбачено, що обидва лічильники можуть лічити від 0 до 255. Це означає, що однорозрядний контрольний лічильник 1 при кожному шістнадцятому лічильному сигналі S11, який надходить на багаторозрядний лічильник 11, отримує також від управління 5 у блоці 3 контрольний лічильний сигнал S1. З метою неманіпульованого функціонування логічна схема контролю виконана таким чином, що вона слідує за тим, щоб пороховане значення лічильника 11 відповідало якраз отриманому порохованому значенню контрольного лічильника 1. Тобто, у зображеному прикладі виконання пороховане значення лічильника 11 не може бути меншим за $(ix16)-1$. Це стосується і схеми зі зворотним відліком; тут також дані лічильника згідно з логічною схемою лічби мусять знаходитися у діапазоні, що відповідає порохованому значенню контрольному лічильника 1.

Якщо логічна схема контролю 4 не визначає співпадіння, через контакт Р виходить сигнал помилки.

Однак винахід не обмежується варіантом виконання, зображеним на фігурі. Більше того, може мати місце варіант, коли зокрема при дуже великому діапазоні значень лічильника 11 з метою заощадження комірок однорозрядного лічильника застосовують не лінійний, а, наприклад, декадний лічильник. Тобто, однорозрядний лічильник може отримувати від управління 5 контрольний лічильний сигнал S1, наприклад, з кожним 10-м, 100-м, 1000-м і т.д. лічильним сигналом. Для забезпечення неманіпульованої експлуатації логічна схема контролю 4 мусить бути виконана відповідним чином, тобто у такому разі пороховане значення лічильника 11 повинне відповідати порядку величин, що має відповідність із поточним порохованим значенням контрольному лічильника 1. Так само легко можна уявити, що взаємозв'язок між порохованими значеннями лічильника 11 та контрольного лічильника 1 відповідає логарифмічній, експоненціальній або будь-якій іншій придатній або бажаній функції. Цей принцип може бути застосованим для лічильників як з прямим, так і зворотним напрямком лічби.

Наприкінці слід зауважити, що лічильник 11 і контрольний лічильник 1 не повинні примусово робити лічбу у одному напрямку. Скоріше можна також передбачити, що один із лічильників лічить вперед, а інший назад. Єдиною умовою неманіпульованої експлуатації є те, що контрольний лічильник працює лише у одному напрямку, і логічна схема контролю 4 побудована таким чином, щоб пороховані значення лічильника 11 мали логічний взаємозв'язок із порохованими значеннями контрольного лічильника 1.

