(19) C2 (11) 72342 (13) UA

(98) "Пахаренко і партнери", вул. Пушкінська, 9, кв. 11, м. Київ, 01034
(85) 2003-04-11
(74) Пахаренко Олександр Володимирович, (UA)
(45) [2005-02-15]
(43) [2003-06-16]
(24) 2005-02-15
(22) 2001-08-30
(12) null
(21) 2003032024
(46) 2005-02-15

(86) 2001-08-30 PCT/DE01/03335
(30) 100 44 837.2 2000-09-11 DE
(54) СХЕМНИЙ ПРИСТРІЙ І СПОСІБ ВИЯВЛЕННЯ НЕБАЖАНОГО ВТРУЧАННЯ В ІНТЕГРАЛЬНУ МІКРОСХЕМУ СПОСОБ И УСТРОЙСТВО ДЛЯ ОБНАРУЖЕНИЯ НЕЖЕЛАТЕЛЬНОГО ДОСТУПА К ИНТЕГРАЛЬНОЙ СХЕМЕ METHOD AND DEVICE FOR DETECTING UNDESIRED ACCESS TO AN INTEGRATED CIRCUIT
(56) WO/EP99/08456б , G 06 F 1/00, 04.11.1999 2
(71)
(72) DE Гаммель Берндт DE Гаммель Берндт DE Гаммель Берндт
(73) DE ІНФІНЕОН ТЕКНОЛОДЖІС АГ DE ИНФИНЕОН ТЕКНОЛОДЖИС АГ DE INFINEON TECHNOLOGIES AG

Настоящее изобретение относится к устройству для предотвращения нежелательного доступа к интегральной схеме. Предлагаемое устройство содержит сигнальную шину для передачи импульсного синхронизирующего сигнала и две шины управления, каждая из которых обеспечивает, по меньшей мере, передачу одного бита данных. Сигнальная шина и шины управления расположены между первым и вторым схемными элементами интегральной схемы. Сигнальная шина и шины управления подключены к устройству контроля, который изменяет последовательность выполнения функций интегральной схемы в соответствии с сигналами на сигнальной шине и шинах управления. Устройство контроля может быть также использовано для диагностики интегральной схемы с целью обнаружения неисправностей в процессе работы.

Винахід пропонує схемний пристрій для виявлення небажаного втручання в інтегральну мікросхему, що містить сигнальний провідник, на який подається тактовий сигнал, а також щонайменше одну пару провідників, призначену для кодування одного біта, причому сигнальний провідник і щонайменше одна пара провідників під'єднані між першим і другим функціональними блоками інтегральної мікросхеми. Сигнальний провідник і щонайменше одна пара провідників зв'язані з детекторною схемою, яка в залежності від сигналів на сигнальному провіднику і на провідниках щонайменше однієї пари провідників може змінювати режим роботи інтегральної мікросхеми. Детекторна схема такою ж мірою може бути використана для виявлення дефектів виробництва інтегральних мікросхем.

The invention relates to a circuit arrangement for detecting an undesired attack on an integrated circuit. Said circuit arrangement comprises a signal line, which is subjected to a clock pulse signal and at least one pair of lines, each pair being responsible for encoding one bit. The signal line and the pair(s) of lines run between a first and a second circuit block of the integrated circuit The signal line and the pair(s) of lines are connected to a detector circuit, which modifies the sequence of functions of the integrated circuit, in accordance with the signals from the signal line and the pair(s) of lines. The detector circuit can likewise be used to test for production errors.

1. Схемний пристрій для виявлення небажаного втручання в інтегральну мікросхему (A, B), що містить сигнальний провідник (1), на який подано тактовий сигнал, щонайменше одну пару провідників (2, 3; 4, 5), призначену для кодування одного біта, причому сигнальний провідник (1) і щонайменше одна пара провідників (2, 3; 4, 5), призначена для кодування одного біта, під'єднані між першим і другим функціональними блоками (A, B) інтегральної мікросхеми, який **відрізняється** тим, що сигнальний провідник (1) і щонайменше одна пара провідників (2, 3; 4, 5), призначена для кодування одного біта, зв'язані з детекторною схемою (11), виконаною з можливістю зміни режиму роботи інтегральної мікросхеми в залежності від сигналів сигнального провідника (1) і щонайменше однієї пари провідників (2, 3; 4, 5), призначеної для кодування одного біта.
2. Схемний пристрій за п. 1, який **відрізняється** тим, що кожен провідник щонайменше однієї пари провідників (2, 3; 4, 5) безпосередньо зв'язаний з детекторною схемою (11).
3. Схемний пристрій за п. 1, який **відрізняється** тим, що пари провідників (2, 3; 4, 5) зв'язані з детекторною схемою (11) через мультиплексор.
4. Спосіб виявлення небажаного втручання в інтегральну мікросхему, яка для передачі кожного біта між першим і другим функціональними вузлами містить пару провідників (2, 3; 4, 5), призначену для кодування одного біта, і сигнальний провідник (1) , на який подано тактовий сигнал, який включає такі стадії:
a) при першому значенні сигналу на сигнальному провіднику (1) виявляють однакові рівні сигналу на обох провідниках пари провідників (2, 3; 4, 5), призначеної для кодування одного біта,
b) при другому значенні сигналу на сигнальному провіднику (1) виявляють різні рівні сигналу на обох провідниках пари провідників (2, 3; 4, 5), призначеної для кодування одного біта, причому в разі відхилення від результату, очікуваного в стадіях a) і/або b), змінюють режим роботи інтегральної мікросхеми.
5. Спосіб за п. 4, який **відрізняється** тим, що першим значенням сигналу на сигнальному провіднику (1) є логічний 0 або логічна 1.
6. Спосіб за п. 5, який **відрізняється** тим, що рівень сигналу на обох провідниках пари провідників (2, 3; 4, 5) дорівнює логічному 0 або логічній 1.
7. Спосіб за одним із пп. 4-6, який **відрізняється** тим, що другим значенням сигналу на сигнальному провіднику (1) є логічна 1 або логічний 0.
8. Спосіб за п. 7, який **відрізняється** тим, що рівень сигналу на першому провіднику пари провідників (2, 3; 4, 5) дорівнює логічному 0 або логічній 1, тоді як рівень сигналу на другому провіднику дорівнює логічній 1 або логічному 0.

Винахід стосується схемного пристрою для виявлення небажаного втручання в інтегральну мікросхему, що містить сигнальний провідник, на який подається тактовий сигнал, а також щонайменше одну пару провідників, призначену для кодування одного біта, причому сигнальний провідник і щонайменше одна пара провідників під'єднані між першим і другим функціональними блоками інтегральної мікросхеми.

Багато схем, використовуваних, наприклад, в мікропроцесорах, маркерах безпеки та інших пристроях для обробки даних, потребують високого рівня захисту оброблюваних даних від фізичного втручання і перехоплення. Таке втручання можливе шляхом аналізу інтегральної мікросхеми з використанням методу "переконструювання" (інженерного аналізу з метою розкриття). За допомогою такого аналізу можливе як виявлення принципу роботи інтегральної мікросхеми, так і вплив на принцип роботи з метою маніпулювання даними чи процесом обробки даних.

На практиці уже існують різні способи, за допомогою яких такий аналіз може бути принаймні утруднений.

Наприклад, відоме накривання інтегральної мікросхеми так званим "щитом". При цьому щит складається із щонайменше двох розміщених над інтегральною мікросхемою - як правило у формі меандру - електропровідних доріжок. Розривання або коротке замикання цих доріжок виявляє схема оцінки, яка потім переводить інтегральну мікросхему у захищений стан. Це може бути здійснено, наприклад, шляхом формування команди скидання (reset) або стирання вмісту пам'яті.

Крім того, відомий спосіб, згідно з яким може бути виявлене видалення пластмасового корпусу, виготовленого із прес-маси. При цьому виявляють зміну ємності між двома доріжками при видаленні прес-маси. Для цього в пластмасовому корпусі розміщено велику кількість датчиків.

Крім того, відомий спосіб виявлення видалення пасивувального шару над поверхнею чіпа.

Для захисту від криптоаналітичного втручання інтегральні мікросхеми для областей застосування, критичних з точки зору безпеки, виконують у схемотехніці, відомій як "подвійний канал з попереднім заряджанням" (Dual-Rail with Precharge). При цьому один біт кодується за допомогою двох комплементарних провідників. У фазі першого такту - так званій "фазі попереднього заряджання" (precharge phase) - здійснюють попереднє заряджання обох комплементарних провідників (логічна 1 чи високий рівень), внаслідок чого попередньо записана інформація стирається. У фазі другого такту, так званій "фазі оцінки" (evaluation phase), обидва провідники розряджають (логічний 0 чи низький рівень) і на фронті наступного такту здійснюють оцінку.

Всі названі вище способи виявлення служать для перешкоджання доступу до доріжок інтегральної мікросхеми. В разі подолання цього бар'єра дані, що передаються через доріжки інтегральної мікросхеми, можуть бути проаналізовані або можуть зазнати маніпуляцій. Останнє може бути здійснене шляхом прикладення напруги чи розривання доріжок.

Тому задача цього винаходу полягає в розробці схемного пристрою, а також способу виявлення небажаного втручання в інтегральну мікросхему, який забезпечує покращений захист.

Ця задача вирішена ознаками пункту 1 формули винаходу, який стосується схемного пристрою, а також ознаками пункту 4 формули винаходу, який стосується способу. Вигідні форми виконання винаходу відображені в додаткових пунктах формули винаходу.

При цьому в інтегральній мікросхемі застосована згадана вище технологія "подвійного каналу з попереднім заряджанням" (Dual-Rail with Precharge), тобто для кодування одного біта використовують пару провідників. При цьому інтегральна мікросхема може містити велику кількість пар провідників. Відповідно до винаходу передбачено, що сигнальний провідник, на який поданий тактовий сигнал, і щонайменше одна пара провідників з'єднані з детекторною схемою, яка в залежності від сигналів сигнального провідника і щонайменше однієї пари провідників може змінювати стан інтегральної мікросхеми.

У першому варіанті виконання пристрою кожен провідник щонайменше однієї пари зв'язаний з детекторною схемою безпосередньо. Альтернативно пари провідників можуть бути зв'язані з детекторною схемою через мультиплексор. Сигнальний провідник, на який подається тактовий сигнал, в кожному із цих варіантів з'єднаний з детекторною схемою.

Відповідний винаходові схемний пристрій використовує ту обставину, що при технології "подвійного каналу з попереднім заряджанням" дійсним логічним станам протипоставлені п'ять заборонених станів. Вони визначаються детекторною схемою і в разі потреби послідовність функціонування інтегральної мікросхеми може бути змінена.

Поряд із забороненими станами в роботі захищеної інтегральної мікросхеми, які вказують на спробу фізичного втручання (наприклад, за допомогою голок, сфокусованого пучка іонів, шляхом маніпулювання зі світлом, температурою, напругою), відповідний винаходові схемний пристрій може бути активізований уже при технологічному тестуванні, тобто при самотестуванні схеми. Таким чином можуть бути виявлені дефекти виробництва, наприклад, дефекти типу "константний нуль" чи "константна одиниця". Оскільки на етапі виробництва інтегральної мікросхеми можна виходити із того, що втручання не відбувається, несприятливі результати аналізу пар провідників вказують на дефект виробництва, наприклад, коротке замикання.

Відповідний винаходові пристрій дуже простий, оскільки додатково він потребує лише детекторної схеми, з'єднаної з парами провідників і з сигнальним провідником, на який поданий тактовий сигнал.

Принцип дії відповідного винаходові схемного пристрою детальніше пояснюється далі в ході опису способу.

При першому значенні сигналу на сигнальному провіднікові перевіряють провідники першої пари на наявність однакового рівня сигналу. При другому значенні сигналу на сигнальному провіднікові перевіряють провідники першої пари на наявність різних рівнів сигналу, причому в разі відхилення від очікуваного результату змінюють режим роботи інтегральної схеми.

Іншими словами це означає, що при одному із заборонених станів, які далі будуть пояснені детальніше, режим роботи інтегральної схеми змінюється. У відповідному винаходові способі здійснюють контроль зарядного стану (рівня сигналу) обох провідників пари, причому перевірка заборонених станів може бути представлена за допомогою таблиці станів чи таблиці істинності. Схемотехнічна реалізація таблиці істинності є стандартною задачею і тому тут детальніше не пояснюється.

Принципово фаза заряджання може бути здійснена на вибір при першому значенні сигналу, відповідному логічному 0 чи логічній 1.

Перевагу має перше значення сигналу на сигнальному провіднику, яке дорівнює логічному 0. В цьому разі таблиця станів відповідає звичайному підходові при технології "подвійного каналу з попереднім заряджанням" (Dual-Rail with Precharge).

Коли до сигнального провідника прикладений сигнал, що має перше значення, рівень сигналу на двох провідниках певної пари дорівнює логічному 0 або логічній 1. Таким чином цими двома станами задається істинне "заряджання" ("Precharge"). Інші стани визначаються як заборонені.

Відповідно другим значенням сигналу на сигнальному провідникові є логічна 1 чи логічний 0. Друге значення сигналу принципово має бути комплементарним першому значенню.

Під час дії другого значення сигналу на сигнальному провідникові значення сигналу на першому провідникові пари провідників має бути логічним 0 чи логічною 1, а на другому провідникові даної пари має бути логічною 1 чи логічним 0, тобто комплементарним.

Як наслідок, заборонений стан виникає тоді, коли під час дії другого значення сигналу на сигнальному провідникові на обох провідниках однієї пари присутні ідентичні значення. Таким чином загалом може бути п'ять заборонених станів.

Нижче відповідний винаходові підхід докладніше пояснюється з використанням фігур. На них схематично зображено:

Фіг.1 - перший приклад виконання відповідного винаходові схемного пристрою,

Фіг.2 - другий приклад виконання відповідного винаходові схемного пристрою,

Фіг.3 - приклад епюр сигналів на сигнальному провіднику і на двох парах провідників,

Фіг.4-7 - чотири таблиці станів.

На фіг.1 зображений перший приклад виконання відповідного винаходові схемного пристрою для виявлення небажаного втручання в інтегральну мікросхему. Інтегральна мікросхема для прикладу представлена функціональними блоками A, B, між якими знаходяться електропровідні доріжки 1-5. При цьому доріжка 1 представляє сигнальний провідник "Синхр", на який подано тактовий сигнал. Крім того, для прикладу представлені дві пари провідників L1.1, L2.1 і L1.n, L2.n. Таким чином, між функціональними блоками A, B можуть бути передані два біти. Звичайно ж, в принципі між функціональними блоками A, B може бути під'єднана довільна кількість пар провідників.

Відповідно до винаходу для контролю електропровідних доріжок передбачена детекторна схема 11. Кожна із доріжок 1-5 між функціональними блоками A, B з'єднана з детекторною схемою 11. Це показано провідниками 6-10. В разі забороненого стану детекторна схема формує на провіднику 12 сигнал тривоги, яким інтегральна схема може бути запущена знову або можуть бути зітерті дані, суттєві з точки зору безпеки.

Крім того, може бути передбачена можливість селективного активування чи дезактивування детекторної схеми з використанням сигнального провідника 13.

В першому прикладі виконання згідно з Фіг.1 кожен із провідників 1-5 безпосередньо з'єднаний з детекторною схемою 11. В прикладі виконання згідно з Фіг.2 лише сигнальний провідник 1, на який поданий тактовий сигнал, провідником 6 безпосередньо з'єднаний з детекторною схемою 11. Пари провідників L1.1, L2.1, а також L1.n, L2.n зв'язані з детекторною схемою через мультиплексор 14.

Тоді як пристроєм згідно з Фіг.1 може бути здійснений контроль одночасно усіх пар провідників, пари провідників згідно з Фіг.2 перевіряють на наявність заборонених станів по черзі. Оскільки принцип дії мультиплексора досить відомий із рівня техніки, його детальний опис не наводиться.

За допомогою таблиць станів на Фіг.4-7 можна краще зрозуміти принцип дії відповідного винаходові схемного пристрою. В першій колонці наведені номери можливих станів. В колонках 2-4 вказані можливі стани сигнального провідника Синхр, а також двох провідників пари, в даному разі L1.k, L2.k. При цьому індекс k представляє пари провідників 1-n. В останній колонці наведене логічне значення, що контролюється детекторною схемою 11.

Під час перших чотирьох станів (номери 1-4) сигнальний провідник Синхр перебуває в так званій фазі попереднього заряджання. Під час цієї фази зарядні стани двох провідників пари L1.k, L2.k повинні мати однакові значення. На Фіг.4 і 6 ця умова виконується, коли L1.k, L2.k мають значення логічної 1, тоді як на Фіг.5 і 7 умова виконується при значенні логічного 0.

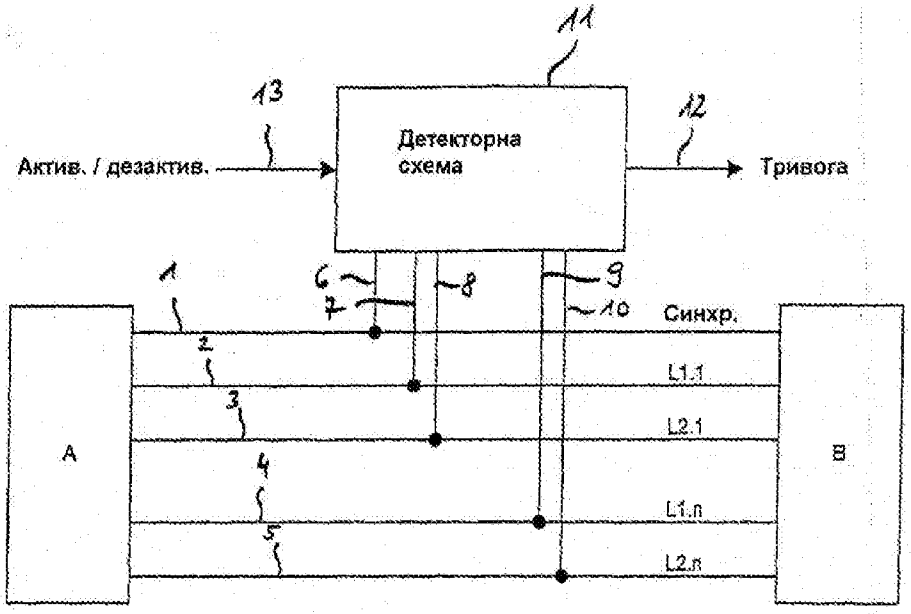
У так званій "фазі оцінки" (evaluation phase) (номери станів 5-8) провідники L1.k, L2.k не можуть мати ідентичного зарядного стану. В цьому разі йдеться про дефект або про втручання. Номеру стану 6 на вибір може бути поставлене у відповідність логічне значення 0 або 1. Відповідно до цього логічне значення стану 7 має бути 1 або 0, тобто бути комплементарним до логічного значення стану 6.

Використання таблиць станів, зображених на Фіг.4 і 5, для відповідного винаходові способу виявлення має перевагу, бо фаза заряджання здійснюється при логічному значенні 0 сигнального провідника Синхр. Звичайно ж, альтернативно можна здійснювати фазу заряджання при значенні логічної 1, а фазу оцінки - при значенні логічного 0. Це відображено в таблицях станів 6 і 7.

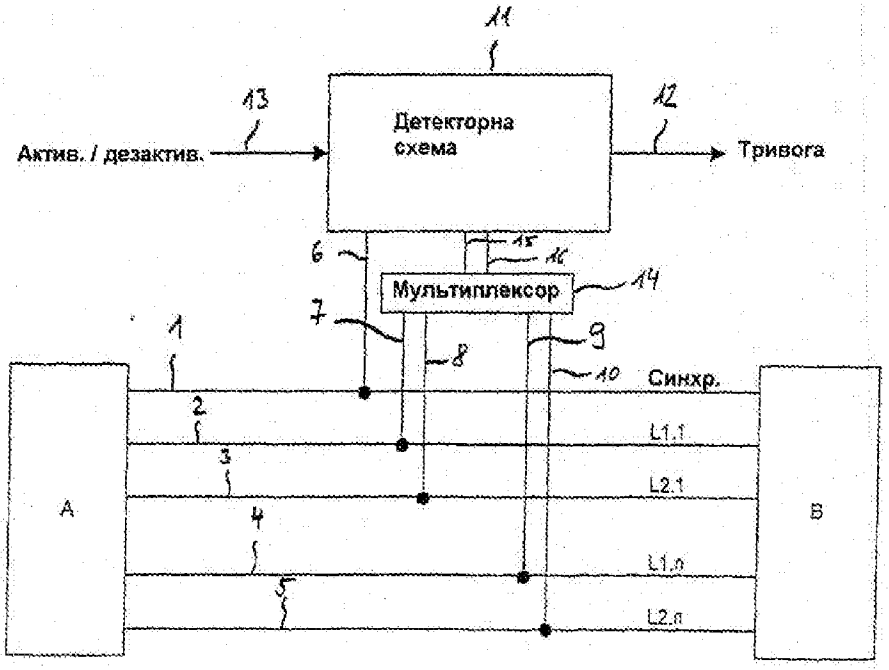
На Фіг.3 для прикладу наведені епюри сигналів на сигнальному провіднику "Синхр", а також двох парах провідників L.1.1, L.2.1 і L1.n, L2.n. Для контролю забороненого стану, наприклад, виявлення наявності дефекту чи втручання, в принципі слід порівняти між собою сигнали сигнального провідника і провідників пар. Зображені на Фіг.3 епюри сигналів оцінювалися за таблицею станів згідно з Фіг.4. Таким чином, уже під час першого значення на сигнальному провіднику "Синхр" (фаза T_0 тактового сигналу) виявлений дефект в першій парі провідників, оскільки другий провідник L.2.1 під час фази "попереднього заряджання" не прийняв ідентичного значення. Під час фаз T_0 і T_9 тактового сигналу також виявлений дефект у фазі оцінки, оскільки сигнальні стани обох провідників пари 1 мають ідентичний зарядний стан, що заборонено згідно з таблицею станів Фіг.4. Ще один дефект виявлено під час фази T_{10} тактового сигналу.

На противагу цьому, епюри сигналів n-ої пари провідників - як показує порівняння з таблицею станів згідно з Фіг.4 - свідчать про їх нормальний стан.

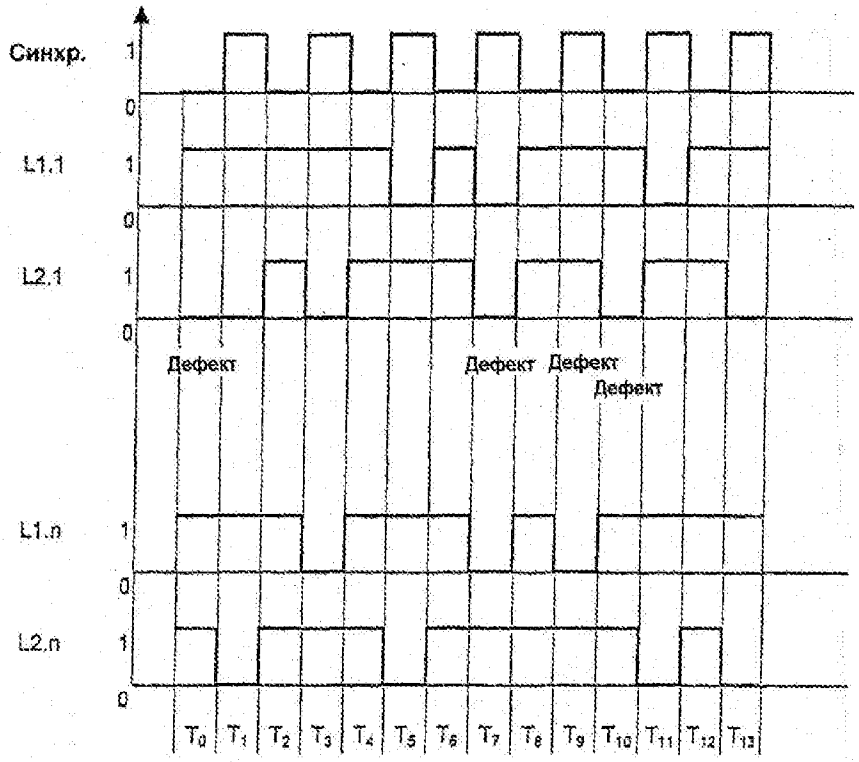
Перелік позиційних позначень
1-5 Електропровідна доріжка
6-10 Електропровідна доріжка
11 Детекторна схема
12 Сигнальний провідник
13 Сигнальний провідник
14 Мультиплексор
A, B Функціональний блок



ФІГ. 1



ФІГ. 2



ФИГ. 3

Номер стану	Синхр.	L1.k	L2.k	Логічне значення	
1	0	1	1	О.К.	
2	0	1	0	Заборонений стан	
3	0	0	1	Заборонений стан	
4	0	0	0	Заборонений стан	
5	1	1	1	Заборонений стан	
6	1	1	0	0	1
7	1	0	1	1	0
8	1	0	0	Заборонений стан	

k = 1 – n

ФІГ. 4

Номер стану	Синхр.	L1.k	L2.k	Логічне значення	
1	0	1	1	Заборонений стан	
2	0	1	0	Заборонений стан	
3	0	0	1	Заборонений стан	
4	0	0	0	О.К.	
5	1	1	1	Заборонений стан	
6	1	1	0	0	1
7	1	0	1	1	0
8	1	0	0	Заборонений стан	

k = 1 – n

ФІГ. 5

Номер стану	Синхр.	L1.R	L2.k	Логічне значення	
1	1	1	1	О.К.	
2	1	1	0	Заборонений стан	
3	1	0	1	Заборонений стан	
4	1	0	0	Заборонений стан	
5	0	1	1	Заборонений стан	
6	0	1	0	0	1
7	0	0	1	1	0
8	0	0	0	Заборонений стан	

k = 1 – n

ФІГ. 6

Номер стану	Синхр.	U.k	L2.k	Логічне значення	
1	1	1	1	Заборонений стан	
2	1	1	0	Заборонений стан	
3	1	0	1	Заборонений стан	
4	1	0	0	О.К.	
5	0	1	1	Заборонений стан	
6	0	1	0	0	1
7	0	0	1	1	0
8	0	0	0	Заборонений стан	

k = 1 – n

ФІГ. 7