УДК 681.5:004.056

М.Л. Малиновский

Синтез безопасных автоматов с функциональной деградацией

Разработаны абстрактные модели и выделены классы безопасных автоматов. Предложены табличные и графические методы задания таких автоматов и методы синтеза безопасных автоматов с функциональной деградацией, основанные на формировании множеств ответственных операций и построении, анализе и преобразовании χ-автоматов.

The abstract models are developed and the classes of secure automatic machines are singled out. The tabular and graphic methods of specifying such machines and the methods of synthesis of such machines with functional degradation are suggested based on the formation of sets of crucial operations and the construction, analysis and transformation of χ-machines.

Розроблено абстрактні моделі та виділено класи безпечних автоматів. Запропоновано табличні та графічні методи завдання таких автоматів, а також методи синтезу безпечних автоматів з функціональною деградацією, засновані на формуванні множин відповідальних операцій і побудові, аналізі та перетворенні χ-автоматів.

Введение. С развитием и массовым внедрением микроэлектронных систем и компонентов критического применения (СКП) проблема повышения безопасности (функциональной и информационной) становится все более актуальной. Важнейшая роль в ее решении принадлежит теории синтеза цифровых автоматов [1]. В настоящее время данная теория интенсивно развивается и охватывает все более широкий диапазон областей человеческой деятельности. Вместе с тем многие важные задачи, связанные с построением СКП в промышленности, на транспорте, в информационных системах остаются неохваченными существующими методами, в результате чего достижение необходимого уровня безопасности становится чрезвычайно сложной, а иногда и неразрешимой проблемой.

Наибольший вклад в развитие теории синтеза безопасных автоматов внесли В.В. и Вл.В. Сапожниковы, которые ввели понятия безопасного автомата, опасного и неопасного ложного перехода, разработав методы абстрактного и структурного синтеза безопасных автоматов, реализованных на элементах с несимметричными отказами [2]. При этом неохваченными теорией остаются следующие задачи:

- разработка и выделение классов безопасных автоматов и методов их задания;
- разработка методов формализации требований, предъявляемых к безопасности автоматов;
- разработка методов синтеза безопасных автоматов с функциональной деградацией, реакция которых на искажения функций и сигналов обеспечивает сохранение максимально возможного количества реализуемых ответственных функций управления при безусловном обеспечении безопасности.

Цель статьи – повышение безопасности СКП путем решения перечисленных задач.

Понятие о безопасном автомате и опасных и безопасных искажениях сигналов и функций

Как известно, каноническая модель цифрового автомата представляет собой шестиэлементный кортеж $M = \{Z, W, S, s_0, \delta, \lambda\}$, где Z – конечное множество входных сигналов, называемое входным алфавитом автомата, W – конечное множество выходных сигналов, называемое выходным алфавитом автомата, S – конечное множество состояний автомата, s_0 – элемент из множества Z, называемый начальным состоянием автомата, δ – функция переходов, задающая однозначные отображения множества пар (s, z), где $s \in S$ и $z \in Z$, в множество S, и λ – функция выходов, задающая однозначные отображения множества пар (s, z) в множество W [1].

Очевидно, что имеет место цепочка связанных событий: неисправность вызывает искажение входных и выходных сигналов, а также функций переходов δ и выходов λ автомата; в свою очередь, искажения, достигнув интерфейса с внешним миром, приводят к отказу (или сбою) цифрового компонента. При этом к сбою приводят кратковременные самоустраняющиеся неисправности, а к отказу – действующие дли-

тельное время и устраняющие, как правило, вмешательством человека.

Условимся считать, что искажения сигналов и функций вызывают отображение исправного автомата M в неисправный автомат M', и обозначать такое отображение $M \sim M'$.

Следовательно, искажение функции переходов δ может стать причиной выполнения ложного перехода автомата. Обозначим такие ложные переходы $s_i \delta' s_j$ или $s_i \sim s_j$, где $s_i \in S$ – состояние, в которое переходит автомат под воздействием (неискаженной) функции δ, δ′ – функция переходов, которую индуцирует искажение функции δ, s_j – состояние (в общем случае, s_j может не принадлежать множеству S), в которое переходит автомат под воздействием функции δ′. Искажение функции выходов λ приводит к искажению выходного сигнала, обозначим их $w_i \lambda' w_j$ или $w_i \sim w_j$. Искажения входного сигнала обозначим $z_i \sim z_j$.

В [2] предложено разделять переходы и отказы на безопасные и опасные. Аналогичным образом разделим искажения сигналов и функций δ, λ, являющихся причиной возникновения этих отказов, на два класса: безопасных искажений, приводящих к частичной или полной потере работоспособности, и опасных, что приводят к нарушению безопасности цифрового компонента.

Под функциональной безопасностью (ФБ) модели M будем понимать свойство модели исключать (с некоторой заданной вероятностью) опасные искажения сигналов и функций.

Для дальнейшего анализа важны понятия зависимых и независимых, одиночных и кратных, а также константных искажений сигналов и функций. Под зависимыми понимаем искажения, обусловленные общей причиной. Независимые искажения такой обусловленности не имеют. Под одиночными будем понимать одно или несколько зависимых искажений. Под кратными – два и более независимых искажений. Термин «константные искажения» имеет смысл по отношению к входным и выходным сигналам с динамическим кодированием, при котором состояние сигнала определяется его временными параметрами (фазой, частотой, скважностью и т.д.). При наличии константных искажений временные параметры сигналов приобретают некоторые предельные значения (0 Гц, если речь идет о частоте, 0 или 100%, если речь идет о скважности, ∞, если речь идет о сдвиге фаз).

Важно также понятие деградации безопасного автомата, под которым понимается снижение работоспособности или безопасности автомата при наличии искажений сигналов и функций. Деградация может быть частичной, при которой автоматом не реализуется часть функций управления, предусмотренных алгоритмом, или полной, когда не реализуется ни одна из функций управления. Для систем критического применения деградацию следует описывать двумерной поверхностью как функцию от двух переменных, одна из которых соответствует поддерживаемому уровню работоспособности, а другая – поддерживаемому уровню безопасности. На практике встречаются задачи, в которых деградация согласно первому измерению может принимать несколько дискретных значений, и только два дискретных значения согласно второму измерению: при первом из них безопасность обеспечивается, а при втором – не обеспечивается. В дальнейшем будем разделять деградацию автомата на деградации работоспособности и безопасности. Уровню деградации работоспособности для данного класса искажений соответствует разность между единицей и количеством функций, реализуемых автоматом в условиях этих искажений, отнесенному к полному количеству функций, предусмотренных алгоритмом, задающим автомат.

Предложенное ранее [2] определение: безопасным автоматом называется автомат, у которого исключается реализация опасных событий при всех отказах его логической сети, вероятность которых надо учитывать, ориентировано на построение логической сети на элементах с несимметричными отказами. Ориентируясь на использование элементов с симметричными отказами, сформулируем следующее определение:

Безопасным назовем автомат, у которого исключается реализация опасных событий (деградация безопасности) при любых одиночных искажениях функций и сигналов, а также одиночных и кратных константных искажениях входных и выходных сигналов.

Разработка абстрактных моделей безопасных автоматов

Каноническая модель M не отражает свойств ФБ цифровых компонентов. С целью наделить данную модель свойствами ФБ, выполним ее преобразование.

1. Множество входных сигналов Z представим в виде подмножеств $Z = \{Z^{(A)}, Z^{(B)}\}$, которым соответствуют входные алфавиты $z^{(A)}_1, \ldots z^{(A)}_n, \ldots, z^{(A)}_N, z^{(B)}_1, \ldots, z^{(B)}_n, \ldots, z^{(B)}_N$;

2. Множество выходных сигналов W представим в виде подмножеств $W = \{W^{(A)}, W^{(B)}\}$, которым соответствуют выходные алфавиты $w^{(A)}_1, \ldots, w^{(A)}_k, \ldots, w^{(A)}_K, w^{(B)}_1, \ldots, w^{(B)}_k, \ldots, w^{(B)}_K$;

3. Множество состояний S представим в виде подмножеств $S = \{ C = \{C^{(A)}, C^{(B)}\}, D = \{D^{(A)}, D^{(B)}\}, E = \{E^{(A)}, E^{(B)}\}, F = \{F^{(A)}, F^{(B)}\}, G = \{G^{(A)}, G^{(B)}\} \}$, которым соответствуют алфавиты состояний $c^{(A)}_1, \ldots, c^{(A)}_n, \ldots, c^{(A)}_N, c^{(B)}_1, \ldots, c^{(B)}_n, \ldots, c^{(B)}_N$; $d^{(A)}_1, \ldots, d^{(A)}_n, \ldots, d^{(A)}_N, d^{(B)}_1, \ldots, d^{(B)}_n, \ldots, d^{(B)}_N$; $e^{(A)}_1, \ldots, e^{(A)}_l, \ldots, e^{(A)}_L, e^{(B)}_1, \ldots, e^{(B)}_l, \ldots, e^{(B)}_L$; $f^{(A)}_1, \ldots, f^{(A)}_l, \ldots, f^{(A)}_L, f^{(B)}_1, \ldots, f^{(B)}_l, \ldots, f^{(B)}_L$; $g^{(A)}_1, \ldots, g^{(A)}_k, \ldots, g^{(A)}_K, g^{(B)}_1, \ldots, g^{(B)}_k, \ldots, g^{(B)}_K$.

4. Введем следующие функции:

φ – функция переходов, определяющая состояния $C^{(A)}$, $C^{(B)}$ автомата в зависимости от входных состояний $Z^{(A)}$ и $Z^{(B)}$;

ω – функция переходов, которая определяет состояния $D^{(A)}$, $D^{(B)}$ автомата в момент времени t в зависимости от внутренних состояний $C^{(A)}$, $C^{(B)}$, а также состояний $D^{(A)}$ и $D^{(B)}$ в момент времени $t-1$;

δ – функция переходов, определяющая состояния $E^{(A)}$, $E^{(B)}$ автомата в момент времени t в зависимости от внутренних состояний $D^{(A)}$, $D^{(B)}$ и $F^{(A)}$, $F^{(B)}$ в момент времени $t-1$;

χ – функция переходов, которая определяет состояния $F^{(A)}$, $F^{(B)}$ автомата в момент времени t в зависимости от внутренних состояний $E^{(A)}$, $E^{(B)}$, а также состояний $F^{(A)}$ и $F^{(B)}$ в момент времени $t-1$;

λ – функция переходов, определяющая состояния $G^{(A)}$, $G^{(B)}$ автомата в момент времени t в зависимости от внутренних состояний $F^{(A)}$, $F^{(B)}$, а также состояний $D^{(A)}$ и $D^{(B)}$ в момент времени $t-1$;

ψ – функция выходов, которая определяет выходные состояния $W^{(A)}$, $W^{(B)}$ автомата в зависимости от внутренних состояний $G^{(A)}$ и $G^{(B)}$.

Таким образом, полученный автомат, названный в дальнейшем безопасным логическим автоматом параллельного действия или БЛП-автоматом, описывается кортежем:

$$\text{БЛП} = [Z, C, D, E, F, G, H, W, \varphi, \omega, \delta, \chi, \lambda, \psi]. \quad (1)$$

Временные зависимости между компонентами кортежа определяются уравнениями:

$$\begin{cases} C^{(A)}_t = \varphi\,(Z^{(A)}_t); \\ C^{(B)}_t = \varphi\,(Z^{(B)}_t); \\ D^{(A)}_t = \omega\,(C^{(A)}_t, C^{(B)}_t, D^{(A)}_{(t-1)}); \\ D^{(B)}_t = \omega\,(C^{(A)}_t, C^{(B)}_t, D^{(B)}_{(t-1)}); \\ E^{(A)}_t = \delta\,(F^{(A)}_{(t-1)}, D^{(A)}_{(t-1)}); \\ E^{(B)}_t = \delta\,(F^{(B)}_{(t-1)}, D^{(B)}_{(t-1)}); \\ F^{(A)}_t = \chi\,(E^{(A)}_t, E^{(B)}_t, F^{(A)}_{(t-1)}); \\ F^{(B)}_t = \chi\,(E^{(A)}_t, E^{(B)}_t, F^{(B)}_{(t-1)}); \\ G^{(A)}_t = \lambda\,(F^{(A)}_{(t-1)}, D^{(A)}_{(t-1)}); \\ G^{(B)}_t = \lambda\,(F^{(B)}_{(t-1)}, D^{(B)}_{(t-1)}); \\ W^{(A)}_t = \psi\,(G^{(A)}_t); \\ W^{(B)}_t = \psi\,(G^{(B)}_t). \end{cases} \quad (2)$$

Условимся различать БЛП-автоматы Мили, в которых состояние G описывается функцией $G_t = \lambda\,(F_{(t-1)}, D_{(t-1)})$, и БЛП-автоматы Мура, где оно же описывается функцией $G_t = \lambda\,(F_{(t-1)})$. Также будем различать БЛП-автоматы P-типа, в которых состояние D_t описывается функцией $D_t = \omega\,(C^{(A)}_t, C^{(B)}_t)$ и состояние F_t описывается функцией $F_t = \chi\,(E^{(A)}_t, E^{(B)}_t)$, и БЛП-автоматы M-типа, в которых состояние D_t описывается функцией $D_t = \omega\,(C^{(A)}_t, C^{(B)}_t, D_{(t-1)})$ и состояние F_t описывается функцией $F_t = \chi\,(E^{(A)}_t, E^{(B)}_t, F_{(t-1)})$.

Методы задания БЛП-автоматов

К этапам задания БЛП-автоматов относятся задания функций:

– переходов δ и λ канонического автомата M;

– φ преобразования входного сигнала $z \in Z$ c в сигнал $c \in C$;

– выходов ψ преобразования сигнала $g \in G$ в сигнал $w \in W$;

– ω и χ – преобразования внутренних состояний (задаются в соответствии с условиями, определяющими безопасность функционирования БЛП-автомата).

Методы задания функций переходов δ и λ известны [1], а методы задания функций φ и ψ определяются используемыми методами динамического кодирования входных и выходных сигналов, что учитывается на этапе структурного синтеза. На этапе абстрактного синтеза интерес представляют методы задания функций ω и χ, поэтому сосредоточим усилия на их разработке. Поскольку данные методы идентичны, рассмотрим только одну из функций – χ.

Для БЛП-автоматов P-типа функция χ описывает некоторую комбинационную схему с двумя входами $E^{(A)}$, $E^{(B)}$ и одним выходом $F^{(A)}$, алфавиты которых имеют одинаковое количество букв L. Входной алфавит данной комбинационной схемы составляют всевозможные пары $(e_i\ e_j)$, где i и j пробегают все значения натурального ряда 1, 2, … , L. Таким образом, входной алфавит комбинационной схемы содержит L^2 букв, каждая из которых составляет пару букв входных сигналов $E^{(A)}$, $E^{(B)}$. Обозначим каждую такую букву символом e_{ij}.

Очевидный способ задания функции χ БЛП-автоматов P-типа – нахождение соответствия буквам входного алфавита e_{ij} букв выходного алфавита f_k. Для сокращения количества букв входного алфавита совместим пары (e_{ij}, e_{ji}), которым соответствует одна и та же буква выходного алфавита f_k, в одну букву e_{ij}. В результате этого количество букв входного алфавита составит $L' = 0{,}5\ (L^2 + L)$.

Для БЛП-автоматов М-типа функция χ описывает автомат Мура, в котором обозначения состояний и отмечающих их выходных сигналов совпадают. Таким образом, функция χ для БЛП-автоматов М-типа задается таблицей переходов с L столбцами, соответствующими номерам состояний и одновременно буквам выходного сигнала, и L' строками, каждой из которых соответствует буква e_{ij} входного алфавита.

Другой (более компактный) способ задания функции χ – ее описание при помощи квадратной таблицы, каждому столбцу и каждой строке которой соответствует та или иная буква входного алфавита сигналов $E^{(A)}$, $E^{(B)}$. Причем для БЛП-автоматов P-типа строится одна такая таблица, а для M-типа – L таблиц для каждой из L букв выходного алфавита. Таблица имеет следующие особенности:

– равенство количества строк и столбцов;

– наличие диагонали соответствий, которая начинается в верхнем левом и заканчивается в нижнем правом углу;

– симметричность относительно диагонали соответствий. Исходя из этого, ячейки таблицы, расположенные над (или под) диагональю соответствий, можно не заполнять.

Заметим, что предложенная квадратная таблица (назовем ее χ-таблицей) может рассматриваться как таблица переходов автомата Мура, в которой строки соответствуют буквам входного алфавита, а столбцы – состояниям автомата. Автомат Мура реализует функцию χ БЛП-автомата, если χ-таблица совпадает с таблицей переходов данного автомата Мура. Автоматы Мура, реализующие функцию χ БЛП-автомата, обозначим χ-автоматами.

Очевидно, χ-автомат может быть описан в виде графа переходов с L вершинами и ребрами, соответствующими буквам входного алфавита. Такие графы в дальнейшем назовем χ-графами.

Установим связь между графом χ-автомата и графом безопасных переходов, предложенным в [2]. Данная связь определяется следующими правилами (процедурой) преобразования графа безопасных переходов в граф переходов χ-автомата.

Процедура 1.

• Граф безопасных переходов описывается таблицей, каждый столбец и каждая строка которой нумеруются от 1 до L, где L – количество вершин.

• Таблица заполняется следующим образом: на диагонали соответствий, ячейки которой рас-

полагаются на пересечении строк и столбцов с одинаковыми номерами, проставляются номера вершин, соответствующих номерам строк и столбцов, на пересечении которых они располагаются. Правила заполнения остальных ячеек следующие: если стрелка направлена от i-й вершины к j-й, то на пересечении i-го столбца и j-й строки, а также j-го столбца и i-й строки, устанавливается номер j-й вершины; если i-я и j-я вершины не соединены ребрами, но существует k-я вершина, к которой направлены стрелки от i-й и j-й вершин, то на пересечении i-го столбца и j-й строки, а также j-го столбца и i-й строки, устанавливается номер k-й вершины; если i-я и j-я вершины не соединены ребрами, а также не существует k-я вершина, к которой направлены стрелки от i-й и j-й вершин, то на пересечении i-го столбца и j-й строки, а также j-го столбца и i-й строки, устанавливается прочерк.

• По полученной таблице строится граф переходов автомата Мура.

Обратное преобразование (графа переходов χ-автомата в граф безопасных переходов) не всегда возможно. Существует следующий формальный признак, свидетельствующий о невозможности такого преобразования: для χ-автомата с L состояниями, описываемого таблицей переходов, имеется пара (i, j), где $i = 1, 2, \ldots, L$, $j = 1, 2, \ldots, L$, для которой: пересечение i-го столбца и j-й строки таблицы переходов обозначено k ($k \neq i$, $k \neq j$); пересечение i-го столбца и k-й строки таблицы переходов обозначено $r \neq k$ или пересечение k-го столбца и j-й строки таблицы переходов обозначено $s \neq k$.

Поскольку преобразование графа безопасных переходов в граф переходов χ-автомата возможно всегда, функция χ БЛП-автомата может задаваться графом безопасных переходов, если такой граф существует.

Из сказанного следует, что предлагаемые методы задания безопасных автоматов позволяют решить более широкий класс задач по сравнению с методами, основанными на применении графов безопасных переходов.

Граф переходов χ-автомата может быть построен как для БЛП-автоматов P-типа (о чем сказано выше), так и для БЛП-автоматов M-типа. Для последнего случая граф содержит L вершин, символизирующих состояния автомата, где L – количество букв выходного алфавита, и L' стрелок, каждой из которых соответствует буква e_{ij} входного алфавита (одинаково направленные стрелки, соединяющие любую пару вершин, могут объединяться и изображаться в виде одной стрелки, подписанной несколькими буквами e_{ij}). Если для описания χ-автомата используются графы безопасных переходов, то таких графов для задания одного автомата необходимо L – по одному на каждое состояние. Очевидно, для некоторых состояний такие графы могут оказаться эквивалентными.

Для компактного описания χ-автоматов M-типа графами безопасных переходов метод их построения следует дополнить следующим правилом: каждая стрелка графа, соединяющая вершины i и j, должна иметь отметку и соответствовать некоторому текущему состоянию k, для которого переход из i-й в j-ю вершину безопасен. Пользуясь этим правилом можно описать χ-автомат M-типа одним графом безопасных переходов. Назовем такие графы безопасными графами переходов с отмеченными ребрами.

Следующая процедура, применяемая к графам безопасных переходов с отмеченными ребрами, позволяет получить соответствующие данному графу таблицу и граф переходов χ-автомата.

Процедура 2.

• Граф безопасных переходов с отмеченными ребрами описывается таблицей с L столбцами и L' строками, где L – количество вершин графа безопасных переходов, L' – количество букв входного алфавита χ-автомата, каждому столбцу которой соответствует состояние и каждой строке – буква e_{ij} входного алфавита χ-автомата.

• Таблица заполняется следующим образом: для каждой строки, соответствующей букве e_{ii} входного алфавита (в которой индексы совпадают), во всех столбцах проставляются номера i; правила заполнения остальных ячеек следующие: для каждой ячейки, расположенной

на пересечении i-го столбца и строки, соответствующей букве e_{jk} входного алфавита, устанавливается номер:

– j, если существует стрелка, отмеченная номером i и направленная от j-й к k-й вершине графа безопасных переходов;

– k, если существует стрелка, отмеченная номером i и направленная от k-й к j-й вершине графа безопасных переходов;

– r, если одновременно существуют стрелки, отмеченные номером i и направленные от j-й к r-й вершине и от k-й к r-й вершине.

• По полученной таблице строится граф переходов автомата Мура.

Метод синтеза БЛП-автоматов по формальному описанию требований к безопасности, основанному на формировании множеств ответственных функций

Многие практические задачи управления системами критического применения удается представить в виде множества элементарных операций $\Phi = \{\phi_1, \phi_2, \ldots, \phi_n\}$, реализующих автомат. Все множество Ф может быть разделено на два подмножества: ответственных операций, неправильное выполнение которых может привести к аварии, и штатных, что приводят лишь к снижению некоторых качественных характеристик системы управления, например производительности. Для упрощения дальнейших рассуждений считаем, что все операции из множества Ф для данного автомата являются ответственными. В этом случае каждому i-му состоянию автомата соответствует подмножество $\Phi_i \in \Phi$ операций, которые могут быть реализованы автоматом в этом состоянии. Тогда формальное описание требований к безопасности БЛП-автоматов сводится к заполнению таблицы, каждая строка которой соответствует элементу из множества Ф, а каждый столбец – состоянию автомата. Единица на пересечении j-й строки и i-го столбца ставится, если функция ϕ_j может быть реализована автоматом, находящимся в i-м состоянии. Остальные клетки таблицы заполняются нулями. Множества ответственных операций для каждого i-го состояния формируются из операций, отмеченных единицей для данного состояния.

Представленный метод формального описания требований к безопасности БЛП-автоматов позволяет реализовать следующую процедуру задания χ-автомата на этапе абстрактного и структурного синтеза. На этапе абстрактного синтеза данная процедура основывается на построении графа безопасных переходов.

Процедура 3.

• Формируется множество ответственных функций $\Phi = \{\phi_1, \phi_2, \ldots, \phi_n\}$, которые должен реализовать автомат.

• Каждому i-му состоянию автомата соответствует подмножество $\Phi_i \in \Phi$ функций, реализуемое автоматом в i-м состоянии.

• Строится граф, каждая i-я вершина которого соответствует i-му состоянию автомата; стрелки, соединяющие вершины, строятся по следующему правилу: стрелка, направленная от i-й к j-й вершине, существует тогда и только тогда, когда $\Phi_j \in \Phi_i$, где Φ_j и Φ_i – подмножества из множества Ф ответственных функций, реализуемых автоматом в j-м и i-м состояниях соответственно.

• Полученный граф является графом безопасных переходов и однозначно определяет функцию χ БЛП-автомата.

На этапе структурного синтеза достаточно использовать следующий принцип кодирования состояний: разрядность кода должна соответствовать количеству реализуемых элементарных операций; код i-го состояния автомата формируется из элементов i-го столбца таблицы, начиная от первой и заканчивая последней строкой. Функция χ при таком кодировании описывается как поразрядная конъюнкция входных сигналов $E^{(A)}$, $E^{(B)}$. Построенный таким образом автомат при формировании в результате искажений сигналов e_i, e_j всегда осуществляет переход к некоторому состоянию f_{ij}, код которого содержит единицы для элементарных операций из множества Φ_{ij}, образующихся на пересечении множеств Φ_i и Φ_j. В результате этого код состояния точно определяет перечень ответственных функций, которые могут быть реализованы автоматом в условиях искажений, исходя из чего строится функция выходов.

Процедура синтеза БЛП-автоматов с функциональной деградацией

Большинство современных подходов к решению проблемы синтеза автоматных моделей систем и компонентов критического применения базируются на переводе автомата в защитное состояние при наличии искажений функций и сигналов. При этом среди множества внутренних состояний автомата выделяется безопасное состояние s_0, которое, как правило, также соответствует начальному. При обнаружении несоответствий в результатах обработки информации резервируемыми каналами автомат переводится в состояние s_0.

В работе [2] для безопасного поведения при искажениях функций и сигналов предлагается метод избыточного безопасного кодирования состояний, обеспечивающий реализацию безопасных переходов при любых искажениях сигналов заданного класса, кодирующих внутренние состояния.

Процедура синтеза БЛП-автоматов с функциональной деградацией, предлагаемая в статье, предполагает такое поведение автомата, при котором его реакция на искажения функций и сигналов обеспечивает сохранение максимально возможного количества реализуемых ответственных функций управления при безусловном обеспечении безопасности. Таким образом обеспечивается поддержание работоспособности автомата и его многоступенчатая деградация в условиях потока искажений.

Проблему синтеза БЛП-автоматов с функциональной деградацией сформулируем следующим образом: *требуется создать процедуру, которая позволяла бы по известному алгоритму, описанному канонической моделью автомата M в виде графа или таблицы переходов и выходов, находить граф или таблицу переходов χ-автомата, такую, для которой любое искажение или последовательная серия искажений одного из входных сигналов $e_i \sim e_j$ вызывает такие искажения выходного сигнала $f_i \sim f_r$, при которых отсутствует деградация безопасности и имеет место возможно меньший уровень деградации работоспособности БЛП-автомата*.

Проблема синтеза БЛП-автоматов с функциональной деградацией может быть решена путем построения, анализа и преобразования χ-автоматов. С учетом сказанного следует, χ-автоматы могут быть заданы таблицей переходов, графом переходов автомата Мура или графом безопасных переходов.

Ниже приведена процедура синтеза БЛП-автоматов, в которых функция χ описывается графом безопасных переходов.

Процедура 4.

1. В соответствии с традиционной теорией абстрактного синтеза конечных автоматов строится граф переходов G с L вершинами, задающий каноническую модель автомата Мили или Мура (без учета требований, предъявляемых к безопасности).

2. Строится граф Gs безопасных переходов с L вершинами.

3. Если любая пара вершин полученного графа Gs связана ребром непосредственно либо через третью вершину, к которой направлены стрелки безопасных ложных переходов (назовем такие графы β-связными), то переходим к заданию таблицы переходов для функции χ (п. 8 процедуры).

4. Если граф Gs не β-связный, то для каждой пары (группы) не β-связных вершин создаются новые вершины, к которым из каждой из несвязных вершин данной группы строятся дуги безопасных переходов, обеспечивая таким образом β-связность рассматриваемой пары (группы).

5. Исходный граф G дополняется вершинами, введенными в граф Gs, исходя из анализа алгоритма управления, строятся дуги и описываются условия переходов из новых вершин к исходным.

6. Граф Gs дополняется новыми стрелками, соответствующими безопасным переходам, связывающим новые вершины с исходными.

7. Возвращаемся к п. 3.

8. Строится таблица переходов в соответствии с 1 и 2-м правилами (этапами) процедуры 1 преобразования графа безопасных переходов в граф переходов χ-автомата, рассмотренными выше.

9. Строится таблица выходов для всей совокупности состояний, полученных в результате выполненных преобразований.

Если БЛП-автомат *M*-типа, то операции 2–8 выполняются для каждого состояния, соответствующего вершине графа *G*.

Процедура синтеза БЛП-автоматов, в которых функция χ описывается автоматом Мура, отличается от приведенной тем, что граф *Gs* строится как граф переходов χ-автомата, а также пунктами 3, 4 и 8, которые для этого случая имеют следующую формулировку:

• Если количество исходящих стрелок каждой вершины соответствует количеству вершин графа *Gs* (при этом стрелки изображаются раздельно для каждого условия, по которому осуществляется переход), то переходим к пункту 8.

• Для каждой вершины (или группы вершин), количество исходящих стрелок которых меньше количества вершин графа *Gs*, строятся новые вершины.

• В соответствии с полученным графом *Gs* строится таблица переходов, которая не должна содержать прочерков.

Заключение. В статье предложено обобщение и новое решение научно-прикладной проблемы разработки моделей и методов синтеза безопасных автоматов с функциональной деградацией с целью повышения показателей безопасности систем критического применения.

Основные научные и практические результаты состоят в следующем:

• Даны понятия безопасного автомата и двумерной деградации безопасного автомата.

• Разработаны:

– модели безопасных логических автоматов параллельного действия (БЛП-автоматов); выделены классы БЛП-автоматов Мили, Мура, *M*-типа и *P*-типа;

– методы задания БЛП-автоматов *M*- и *P*-типа табличными формами: таблицей соответствия, квадратной таблицей, таблицей переходов χ-автомата, а также графическими формами: графом безопасных переходов с отмеченными дугами и графом переходов χ-автомата;

– метод формализации требований, предъявляемых к безопасности автоматов, основанный на формировании множеств ответственных операций, реализуемых автоматом;

– процедуры абстрактного и структурного синтеза безопасных автоматов по формальному описанию требований к безопасности, основанному на формировании множеств ответственных функций;

– процедуры синтеза безопасных автоматов с функциональной деградацией, основанные на построении, анализе и преобразовании χ-автоматов.

1. *Глушков В.М.* Синтез цифровых автоматов. – М. : Физматгиз, 1962. – 476 с.
2. *Методы* построения безопасных микроэлектронных систем железнодорожной автоматики / В.В. Сапожников, Вл.В. Сапожников, Х.А. Христов и др. – М.: Транспорт, 1995. – 272 с.
3. *Малиновский М.Л.* Управление объектами критического применения на основе ПЛИС: моногр. – Харьков: Факт, 2008. – 224 с.

Поступила 08.11.2009
Тел. для справок: (61052) 712-3537 (Харьков)
E-mail: w818w@mail.ru