УДК 681.5:004.056

М.Л. МАЛИНОВСКИЙ

Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Украина

СИНТЕЗ ЦИФРОВЫХ АВТОМАТОВ С НЕСИММЕТРИЧНЫМИ ОТКАЗАМИ

Разработаны модели безопасных логических автоматов параллельного действия (БЛП-автоматов); выделены классы БЛП-автоматов Мили, Мура, М-типа и Р-типа. Разработаны методы задания БЛП-автоматов М- и Р-типа табличными и графическими формами. Разработан метод формализации требований, предъявляемых к безопасности автоматов, основанный на формировании множеств ответственных операций, реализуемых автоматом. Разработаны процедуры синтеза безопасных автоматов с функциональной деградацией.

Ключевые слова: *несимметричные отказы, безопасные автоматы, функциональная деградация, безопасность, системы критического применения*

Введение

Предотвращение техногенных катастроф является одной из глобальных проблем современности. Решение данной проблемы в значительной степени зависит от достигнутого уровня функциональной безопасности технических и программных компонентов систем критического применения (СКП). 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.

Безопасное функционирование цифровых компонентов СКП выражается в свойствах несимметричности их отказов. При этом отказы разделяются на классы (в известных автору случаях - на два класса: опасных и безопасных), после чего определяются требования в части вероятностных показателей отказов каждого из классов. Очевидно, вероятность так называемых опасных отказов должна быть значительно ниже, чем вероятность защитных отказов, – в этом и состоит проявление несимметричности.

Для формального описания цифровых устройств, в том числе с учетом требований к безопасности, широко используется инструментарий теории автоматов [1]. Автоматы с несимметричными отказами, так же, как в работе [2], будем называть безопасными.

Заметим, что англоязычный термин «Safe Finite State Machine» не является аналогом термину «Безопасный автомат», который мы будем использовать в рамках данной статьи.

Анализ публикаций показывает, что неохваченными теорией синтеза безопасных автоматов 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.

Целью статьи является повышение безопасности СКП путем решения перечисленных выше задач.

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

Традиционно модель цифрового автомата представляет собой шестиэлементный кортеж $M = \{Z, W, S, s_0, \delta, \lambda\}$, где Z – множество входных сигналов (входной алфавит), W –множество выходных сигналов (выходной алфавит), S – множество состояний автомата, s_0 – элемент из множества Z, называемый начальным состоянием, 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].

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 – такие неисправности, которые действуют длительное время и устраняются, как правило, вмешательством человека.

Искажения сигналов и функций вызывают отображение исправного автомата M в неисправный автомат M', которое символизируется как $M \sim M'$.

Очевидно, искажение функции переходов δ может стать причиной выполнения ложного перехода автомата. Условимся обозначать 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.

Будем обозначать такие искажения $w_i \lambda' w_j$ или $w_i \sim w_j$. Искажения входного сигнала будем обозначать $z_i \sim z_j$.

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

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

Для дальнейшего важны понятия зависимых и независимых, одиночных и кратных, а также константных искажений сигналов и функций. Под зависимыми будем понимать искажения, которые обусловлены общей причиной. Независимые искажения такой обусловленности не имеют.

Под одиночными будем понимать одно или несколько зависимых искажений.

Под кратными будем понимать 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).

Также будет важным 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, при которой не реализуется ни одна из функций управления. Для систем критического применения деградацию следует описывать поверхностью как функцию от двух переменных, одна из которых соответствует поддерживаемому уровню работоспособности, а другая – поддерживаемому уровню безопасности. На практике часто 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 и при втором – не обеспечивается. В дальнейшем будем разделять деградацию автомата на деградацию работоспособности и деградацию безопасности. Уровню деградации работоспособности для данного класса искажений поставим в соответствие разность между единицей и количеством функций, реализуемых автоматом в условиях этих искажений, отнесенному к полному количеству функций, предусмотренных алгоритмом, задающим автомат.

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

Безопасным будем называть автомат, у которого исключается реализация опасных событий при любых одиночных искажениях функций и сигналов, а также одиночных и кратных константных искажениях входных и выходных сигналов.

2. Разработка абстрактных моделей безопасных автоматов

Каноническая модель M не отражает свойств ФБ цифровых компонентов. С целью наделения данной модели свойствами ФБ, выполним её преобразование.

1. Множество входных сигналов Z представим в виде подмножеств

$$Z = \{Z^{(A)}, Z^{(B)}\},$$

которым соответствуют входные алфавиты

$$z_1^{(A)},...,z_n^{(A)},...,z_N^{(A)},\ z_1^{(B)},...,z_n^{(B)},...,z_N^{(B)};$$

2. Множество выходных сигналов W представим в виде подмножеств

$$W = \{W^{(A)}, W^{(B)}\},$$

которым соответствуют выходные алфавиты

$$w_1^{(A)},...,w_k^{(A)},...,w_K^{(A)},\ w_1^{(B)},...,w_k^{(B)},...,w_K^{(B)};$$

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

$$c_1^{(A)},...,c_n^{(A)},...,c_N^{(A)},\ c_1^{(B)},...,c_n^{(B)},...,c_N^{(B)};$$

$$d_1^{(A)},...,d_n^{(A)},...,d_N^{(A)},\ d_1^{(B)},...,d_n^{(B)},...,d_N^{(B)};$$

$$e_1^{(A)},...,e_l^{(A)},...,e_L^{(A)},\ e_1^{(B)},...,e_l^{(B)},...,e_L^{(B)};$$

$$f_1^{(A)},...,f_l^{(A)},...,f_L^{(A)},\ f_1^{(B)},...,f_l^{(B)},...,f_L^{(B)};$$

$$g_1^{(A)},...,g_k^{(A)},...,g_K^{(A)},\ g_1^{(B)},...,g_k^{(B)},...,g_K^{(B)}.$$

4. Введем следующие функции:

– φ – функция переходов, которая определяет 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, которая определяет 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, которая определяет 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, который в дальнейшем будем называть 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:

Условимся различать БЛП-автоматы Мили, в которых состояние G описывается функцией

$$G_t = \lambda(F_{(t-1)}, D_{(t-1)}),$$

и БЛП-автоматы Мура, в которых состояние G описывается функцией

$$G_t = \lambda(F_{(t-1)}).$$

Также будем различать БЛП-автоматы P-типа, в которых состояние D_t описывается функцией

$$D_t = \omega(C_t^{(A)}, C_t^{(B)})$$

и состояние F_t описывается функцией

$$F_t = \chi(E_t^{(A)}, E_t^{(B)}),$$

и БЛП-автоматы M-типа, в которых состояние D_t описывается функцией

$$D_t = \omega(C_t^{(A)}, C_t^{(B)}, D_{(t-1)})$$

и состояние F_t описывается функцией

$$F_t = \chi(E_t^{(A)}, E_t^{(B)}, F_{(t-1)}):$$

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

3. Методы задания БЛП-автоматов

К этапам задания БЛП-автоматов относятся:

1. задание функций переходов δ и λ канонического автомата M;

2. задание функции φ преобразования входного сигнала $z \in Z$ c в сигнал $c \in C$;

3. задание функции выходов ψ преобразования сигнала $g \in G$ в сигнал $w \in W$;

4. задание функций 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]. 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, будем рассматривать только одну из функций – χ.

Для БЛП-автоматов Р-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 $E^{(A)}$, $E^{(B)}$. Будем обозначать каждую такую букву символом e_{ii}.

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

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

Другим (более компактным) способом задания функции χ является её 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 Р-типа строится одна такая таблица, а для M-типа – L таблиц для каждой из L букв выходного алфавита. Данная 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.

Нетрудно видеть, что предложенная выше квадратная таблица (в дальнейшем условимся называть её χ-таблицей) может рассматриваться как таблица переходов автомата Мура, в которой строки соответствуют буквам входного алфавита, а столбцы – состояниям автомата. Будем говорить, что автомат Мура реализует функцию χ БЛП-автомата, если χ-таблица совпадает с таблицей переходов данного автомата Мура. Автоматы Мура, реализующие функцию χ БЛП-автомата, будем обозначать 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 будем называть 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.

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

2. Таблица заполняется следующим образом: на диагонали соответствий (ячейки которой располагаются 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 столб-

ца 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 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.

3. 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 $i = 1,2,...,L$, $j = 1,2,...,L$, для которой 1) пересечение i-го столбца и j-й строки таблицы переходов обозначено $k(k \neq i, k \neq j)$; 2) 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 (как было показано выше) преобразование графа безопасных переходов в граф переходов χ-автомата возможно всегда, функция χ БЛП-автомата может задаваться графом безопасных переходов, если такой граф существует.

Граф переходов χ-автомата может быть построен как для БЛП-автоматов Р-типа (что было показано 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 является безопасным. Пользуясь этим правилом можно описать χ-автомат М-типа одним графом безопасных переходов. В дальнейшем будем называть 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.

1. 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 ставится в соответствие состояние и каждой строке – буква e_{ij} входного алфавита χ-автомата.

2. 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-ой к k-ой вершине графа безопасных переходов;

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

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

3. По полученной таблице строится граф переходов автомата Мура.

4. 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 $\Phi = \{\phi_1, \phi_2, ..., \phi_n\}$, которые реализует автомат. Все множество Φ может быть разделено на два подмножества – ответственных операций, неправильное

выполнение которых может привести к аварии, и штатных, неправильное выполнение которых приводит лишь к снижению некоторых качественных характеристик системы управления, например производительности. Для упрощения дальнейших рассуждений будем считать, что все операции из множества Φ для данного автомата являются ответственными. В этом случае каждому i-му состоянию автомата можно поставить в соответствие 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 Φ, 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 тех операций, которые отмечены единицей для данного состояния.

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

Процедура 3.

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

2. Каждому i-му состоянию автомата ставится в соответствие подмножество $\Phi_i \in \Phi$ функций, которые реализуются автоматом в i-м состоянии;

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

4. 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 будет осуществлять переход к некоторому состоянию f_{ij}, код которого будет содержать единицы для элементарных операций из множества Φ_{ij}, которое образуется 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.

5. 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 [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.

Проблему синтеза БЛП-автоматов с функциональной деградацией сформулируем следующим образом: *требуется построить 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.

Как было показано выше, 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 (в дальнейшем будем называть 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) 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 М-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:

3. 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.

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

5. В соответствии с полученным графом Gs строится таблица переходов (которая не должна содержать прочерков).

Выводы

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

Основные научные и практические результаты работы состоят в следующем:

1. Разработаны модели безопасных логических автоматов параллельного действия (БЛП-автоматов); выделены классы БЛП-автоматов Мили, Мура, М-типа и Р-типа.

2. Разработаны методы задания БЛП-автоматов М- и Р-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.

3. Разработан метод формализации требований, предъявляемых к безопасности автоматов, основанный на формировании множеств ответственных операций, реализуемых автоматом.

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

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

Литература

1. Глушков В.М. Синтез цифровых автоматов / В.М. Глушков. – М. : Физматгиз, 1962. – 476 с.

2. Сапожников В.В. Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В.В. Сапожников, Вл.В. Сапожников, Х.А. Христов, Д.В. Гавзов; под ред. Вл.В. Сапожникова. – М.: Транспорт, 1995. – 272 с.

3. Малиновский М.Л. Управление объектами критического применения на основе ПЛИС: моногр. / М.Л. Малиновский. – Х.: Факт, 2008. – 224 с.

Поступила в редакцию 14.02.2010

Рецензент: д-р техн. наук, проф. Л.В. Дербунович, Национальный технический университет "Харьковский политехнический институт", Харьков, Украина.

СИНТЕЗ ЦИФРОВИХ АВТОМАТІВ С НЕСИМЕТРИЧНИМИ ВІДМОВАМИ

М.Л. Малиновський

Розроблено моделі безпечних логічних автоматів паралельної дії (БЛП-автоматів); виділені класи БЛП-автоматів Мілі, Мура, М- і Р-типу. Розроблено методи завдання БЛП-автоматів М- і Р-типу табличними і графічними формами. Розроблено метод формалізації вимог, що пред'являються до безпеки автоматів, заснований на формуванні множини відповідальних операцій, що реалізуються автоматом. Розроблені процедури синтезу безпечних автоматів з функціональною деградацією.

Ключові слова: несиметричні відмови, безпечні автомати, функціональна деградація, безпека, системи критичного застосування.

FINITE STATE MACHINES WITH ASYMMETRICAL FAILURES SYNTHESIS

M.L. Malynovskiy

The models of Safe Finite State Machines (SFSM) of parallel action; the classes of Mealy and Moore, M- and P-type SFSM; the methods of describing of M- and P-type SFSM by table and graphic forms; the method of formalization of requirements, produced to safety of automats based on forming of plural of responsible operations, realized by FSM; procedures of SFSM with functional degradation synthesis are offered.

Keywords: asymmetrical failures, Safe Finite State Machines, functional degradation, safety, safe-critical systems.

Малиновский Михаил Леонидович – канд. техн. наук, доцент, Харьковский национальный технический университет сельского хозяйства имени Петра Василенко, Харьков, Украина, e-mail: w8l8w@mail.ru.