УДК 681.5
ББК 30.17

ПОДХОД К ОБЕСПЕЧЕНИЮ И ПОДДЕРЖАНИЮ БЕЗОПАСНОСТИ СЛОЖНЫХ СИСТЕМ НА ОСНОВЕ АВТОМАТНЫХ МОДЕЛЕЙ[1]

Резчиков А. Ф. [2], **Богомолов А. С.**[3], **Иващенко В. А.**[4], **Филимонюк Л. Ю.**[5]
(*ФГБУН Институт проблем точной механики и управления РАН, Саратов*)

Предложен подход к обеспечению и поддержанию безопасности функционирования авиационно-транспортных систем на основе согласования взаимодействия их компонентов. На базе причинно-следственного подхода построена автоматная модель процесса функционирования этих систем, позволяющая представить синхронное взаимодействие входящих в них компонентов. Данная модель может найти применение в учебно-авиационных центрах, занимающихся периодической наземной подготовкой, повышением квалификации и переподготовкой авиационных специалистов.

Ключевые слова: сложная система, авиационно-транспортная система, конечный автомат, синхронизация, безопасность, аварии.

---

[1] *Работа поддержана грантом РФФИ 12-08-00490*

[2]*Резчиков Александр Федорович, член-корреспондент РАН, директор ИПТМУ РАН (iptmuran@san.ru).*

[3]*Богомолов Алексей Сергеевич, кандидат физико-математических наук, доцент (alexbogomolov@ya.ru).*

[4] *Иващенко Владимир Андреевич, доктор технических наук, ученый секретарь (iptmuran@san.ru).*

[5] *Филимонюк Леонид Юрьевич, кандидат технических наук (filimonyukleonid@mail.ru).*

1. Введение

Проблема обеспечения и поддержания безопасности авиационно-транспортных систем (АТС) на основе согласования (синхронизации) взаимодействия их компонентов приобретает все большую актуальность [3, 6, 9]. Это обусловлено рядом обстоятельств, в том числе правильным распределением потоков воздушных судов (ВС) в районе аэропортов – загруженность крупных воздушных гаваней настолько велика, что взлетно-посадочные полосы вынуждены принимать или отправлять ВС каждые 40-45 секунд. При этом лицам, принимающим решения (ЛПР), необходимо за короткое время выполнять анализ воздушной обстановки и оперативно принимать правильные решения, обеспечивающие штатную работу аэропортов.

На сегодняшний день синхронизация взаимодействия отдельных компонентов человеко-машинных систем, к которым относятся и АТС, наиболее просто может быть организована в агрегативных системах [1], сетях Петри [7] и автоматных моделях [2]. Отдельные аспекты такой организации представлены, например, в работах [4, 8].

В статье предложен подход, обеспечивающий наиболее полное решение данной проблемы на формальной основе. В качестве формального аппарата использована теория конечных детерминированных автоматов [2], обеспечивающая высокий уровень доказательности и простоты объяснений решений, принимаемых ЛПР, а также эффективность по времени и объему вычислительных операций.

2. Постановка задачи

Пусть в системе выделен набор подсистем $a_1, \ldots, a_n$, работоспособность которых определяет безопасность ее функционирования. Под состоянием безопасности системы будем понимать вектор, координата которого $[s]_i$ с номером i равна 1, если подсистема a_i исправна и 0 – в противном случае, $i \in \{1, \ldots, n\}$. Управляющее воздействие (УВ) из некоторого множества X

допустимых УВ переводит при наличии соответствующих ресурсов и их требуемого сочетания систему из состояния безопасности $s(t)$ в некоторое состояние безопасности $s'(t)$, определяемое УВ, состоянием $s(t)$ и воздействием внешней среды.

Пусть для исследуемой системы выделены $S_{ав}$ и $S_{шт}$ – множества аварийных и штатных состояний безопасности, соответственно. Например, в качестве аварийных состояний могут выступать состояния, характеризующиеся критическими сочетаниями отказов [3] подсистем $a_1, a_2, \ldots, a_n$, а штатных – не отнесенные к таковым.

Необходимо построить алгоритм определения кратчайшей (безопасной) последовательности p^* УВ, переводящих систему из любого состояния $s \in S$ в некоторое безопасное состояние $s' \in S_{шт}$.

3. Метод решения задачи

В качестве формального аппарата решения поставленной задачи используем конечный детерминированный автомат Мили $(S, X, Y, \delta, \lambda)$, состояния которого – элементы множества S отожествляются с состояниями безопасности системы, а входные сигналы – элементы X – с УВ, подаваемыми на нее. Ввиду того, что для парирования неблагоприятных событий в системе УВ может оказаться недостаточно, то каждый элемент множества X представляется тройкой $(x_{упр}, x_{кон}, x_{пар})$, где $x_{упр} \in X_{упр}$ – множество управляющих сигналов, $x_{кон} \in X_{кон}$ – множество специальных контрольных и диагностических сигналов, $x_{пар} \in X_{пар}$ – множество сигналов парирования неблагоприятных событий. Также предполагается наличие в алфавите $X_{пар}$ пустого символа ε для случая, когда реакция на контрольный сигнал означает штатное функционирование, и приложение парирующих сигналов не требуется.

Решение задачи сводится к нахождению такой входной последовательности $p = x_1, \ldots, x_m$, которая переводит автомат из множества заданных начальных состояний $S_0 \subseteq S$ в некоторое конечное состояние $s \in S$, зависящее от p. Любая последовательность с таким свойством называется синхронизирующей для автомата. Множество всех таких последовательностей и всех синхросостояний

$P_{синх} = \{p \in X^* |\ (\exists s \in S)(\forall s \in S_0)(\delta(s, p) = s)\}$, $S_{синх} = \{s \in S |\ (\exists p \in P_{синх})(\forall s \in S_0)(\delta(s, p) = s)\}$.

Если автомат синхронизирован и имеет место $S_{шт} \cap S_{синх} \neq \varnothing$, т.е. существуют синхросостояния, являющиеся штатными, то соответствующие синхронизирующие последовательности позволяют привести систему в безопасное состояние. Если осуществлять поиск по возрастанию длины последовательности, то первая найденная последовательность будет кратчайшей.

Решение задачи определения синхронизирующих последовательностей сводится к поиску решений по синхронизирующим деревьям, что требует значительных вычислительных ресурсов. Для линейных автоматов (ЛА) получены результаты, позволяющие значительно ускорить определение синхронизирующих последовательностей и свести решение задачи к решению систем линейных алгебраических уравнений.

Наряду с традиционным понятием состояний ЛА рассматриваются обобщенные состояния. Обобщенным состоянием (ОС) называется вектор

$$\bar{s}(t) = (s_1(t), \ldots, s_v(t), x, \ldots, x)^{\mathrm{T}}.$$

Переменная x в $\bar{s}(t)$ повторяется n-v ($0 \leq v \leq n$) раз и может принимать любое значение из множества $\{0, \ldots, p\text{-}1\}$. Таким образом, ОС – это множество состояний ЛА, у которых первые v координат зафиксированы.

Входная последовательность называется обобщенной синхронизирующей последовательностью (ОСП) для ЛА, если после подачи этой последовательности на вход автомата он переходит в одно и то же заключительное ОС независимо от начального состояния. При v=n ОСП является классической по Гиллу [2].

В случае существования ОСП ЛА называется обобщенно синхронизируемым. Обобщенную синхронизирующую последовательность наименьшей длины будем называть «минимальной» и обозначать ее длину через $k_{\min}$. Каждое из заключительных ОС, в которое можно перевести ЛА подачей ОСП длины k, будем называть обобщенным синхросостоянием. Множество обобщенных синхросостояний обозначим через S_{syn} (k). Известен критерий существования ОСП [2].

Теорема 1. Для ЛА с главной характеристической матрицей A ОСП длины k существует тогда и только тогда, когда $[A^k]_v = [0]$.

При выполнении данного условия входные последовательности длины k или более являются ОСП. Кроме того, в большинстве случаев имеются несколько ОСП, переводящих ЛА в одно и тоже ОС. Введем меру, по которой будут сравниваться такие ОСП. Каждому входному символу **u** поставим в соответствие его вес $W(\mathbf{u})$, а весом входной последовательности назовем сумму весов всех ее членов.

Содержательно вес $W(\bar{U})$ последовательности $\bar{U}$ представляет собой суммарные затраты ресурсов на ее реализацию.

Как показывает теорема 2, все обобщенные синхросостояния достигаются ОСП минимальной длины и таким образом это множество (далее – $S_{yn}(\overline{A})$) не зависит от k.

Теорема 2. Для обобщенно синхронизируемого ЛА множество $S_{yn}(\overline{A}, k)$ при любом $k \geq k_{\min}$ совпадает с множеством всех линейных комбинаций линейно независимых столбцов матрицы $[A^{kmin\text{-}1}B, \ldots, B]_v$.

Теорема 3 показывает, что ОСП минимального может быть найдена среди ОСП минимальной длины.

Теорема 3. Если $W(\mathbf{u}) \geq 0$ для любого входного сигнала **u**, то для любой ОСП $\bar{\mathbf{U}}$ длины $k \geq k_{\min}$ существует ОСП $\bar{\mathbf{U}}_{\min}$ длины $k_{\min}$, переводящая ЛА в то же обобщенное синхросостояние, что и ОСП $\bar{\mathbf{U}}$, причем $W(\bar{\mathbf{U}}_{\min}) \leq W(\bar{\mathbf{U}})$.

Показано, что в случае $W(\mathbf{u})<0$ при некотором **u** задача нахождения ОСП минимального веса не имеет решения, поскольку всегда можно указать достаточно длинные ОСП с неограниченным по модулю отрицательным весом.

Теорема 4. Построение ОСП минимального веса, переводящей обобщенно синхронизируемый ЛА в заданное обобщенное синхросостояние $\overline{S}$, всегда может быть сведено к задаче целочисленного программирования с линейными ограничениями и $lk_{min}+v$ переменными, где $k_{\min}$ – длина минимальной ОСП для данного ЛА, l – размерность входных векторов, v – характеристика ОС.

Доказательство теорем 1-4 проводится по схеме, рассмотренной в [10].

Теорема 5. Если для ЛА над полем GF(2) существуют ОСП, то их минимальная длина не превосходит величины $(n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$, где n – порядок главной характеристической матрицы A.

Доказательство. Пусть в условиях теоремы минимальная длина ОСП равна k, где $k > (n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$. Согласно теореме 1 это означает, что для данного k выполнено условие $[A^k]_v = [0]$. По теореме Шварца [12] степени любой булевой матрицы порядка n периодичны, начиная со степени $(n\text{-}1)^2+1$. Длина периода этой последовательности определяется [11] как наименьшее общее кратное наибольших общих делителей длин минимальных циклов в сильно связных компонентах соответствующего данной матрице графа. Так как наибольшие общие делители длин минимальных циклов не больше числа вершин сильно связной компоненты, а наименьшее общее кратное натуральных чисел не больше их произведения, то длина периода не превосходит максимума произведения чисел, сумма которых равна n. Согласно [13] такой максимум равен $2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}$, поэтому период последовательности степеней A^k, начиная со степени $k = (n\text{-}1)^2+1$, не превосходит величины $2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}$. Это справедливо и для последовательности подматриц $[A^k]_v$, т.е. для каждого $k > (n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$ существует $k' \le (n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$ такое, что $[A^k]_v = [A^{k'}]_v$. Следовательно, если при некотором $k > (n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$ выполняется условие $[A^k]_v = [0]$, то оно выполняется и при некотором $k' \le (n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$. Это означает по теореме 1 существование ОСП длины k' и противоречит изначальному предположению о минимальности длины k. Теорема доказана.

Замечание. Отдельно рассмотрим случай, когда в определении ОС полагается $v = n$, т.е. ОС совпадает с состоянием в обычном смысле и решается классическая задача синхронизации. В этом случае оценка из теоремы 5 может быть существенно улучшена: правая часть заменяется на n, так как выполнение условия (1) при некотором k означает нильпотентность главной характеристической матрицы, откуда следует [11], что $A^k = [0]$ уже при некотором $k \le n$.

Как следует из теоремы 5, проверку условия $[A^k]_v = [0]$ имеет смысл осуществлять для значений $k \le (n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$. Первое значение степени, при котором выполнится условие

$[A^k]_v = [0]$ будет число $k_{\min}$, которое фигурирует в теореме 2. Все последовательности длины $k_{\min}$ и более будут являться обобщенно синхронизирующими, однако, как следует из теоремы 2, для вычисления всех синхросостояний достаточно найти $S_{yn}(\overline{A}, k_{\min})$.

На основе доказанных теорем разработан алгоритм нахождения УВ для перевода системы в безопасное состояние независимо от ее начального состояния, который состоит из следующих шагов:

1. Проверять условие теоремы 1 последовательно при $k = 1, \ldots, (n\text{-}1)^2+2^{2\text{-}(n\text{-}1)\mathrm{mod}3}3^{n\text{-}2\text{-}2[(n\text{-}1)/3]}+1$.

2. Проверять выполнение условия $[A^k]_v = [0]$. Если это условие не выполняется, то синхронизирующей последовательности не существует. Закончить выполнение алгоритма. При достижении некоторого $k_{\min}$, при котором условие $[A^k]_v = [0]$ выполняется, перейти к шагу 3.

3. Вычислить элементы множества синхросостояний $S_{yn}(\overline{A}, k_{\min})$ как линейные комбинации линейно независимых столбцов матрицы $[A^{kmin\text{-}1}B, \ldots, B]_v$ согласно утверждению теоремы 2.

4. В случае выполнения условия $S_{\text{шт}} \cap S_{yn}(\overline{A}, k_{\min}) \ne \varnothing$ существуют штатные состояния, в которые система может быть

переведена обобщенно синхронизирующими входными последовательностями длины $k_{\min}$. В этом случае перейти к шагу 5, а противном – закончить алгоритм, так как среди элементов множества $S_{шт}$ нет синхросостояний.

5. Для каждого штатного синхросостояния $s \in S_{шт} \cap S_{yn}(\overline{A}, k_{\min})$ существует ОСП, переводящая систему из любого ее состояния в состояние s. Согласно теореме 2 в качестве такой последовательности может быть взято любое решение системы линейных алгебраических уравнений вида $[A^{kmin\text{-}1}B, \ldots, B]_v\, p^{\mathrm{T}} = s$. Для этого нужно разбить полученное решение на входные вектора соответствующей размерности. Решение у данной системы существует согласно теореме 2. Таким образом, на этом шаге существует возможность:

а) выбрать штатное синхросостояние и определить соответствующую ОСП;

б) решая задачи целочисленного программирования, упомянутые в теореме 4, выбрать ОСП, соответствующую некоторому синхросостоянию; в качестве линейных ограничений при этом будет выступать упомянутая в данном пункте система линейных алгебраический уравнений;

в) комбинировать пункты а) и б); при этом при последовательной проверке, как это предписывается в пункте 1 данного алгоритма, гарантируется минимальная длина ОСП и её минимальный вес в случае неотрицательных весов входных сигналов (теорема 3).

Таким образом, приведенный выше алгоритм может быть использован для синхронизации системы в штатное состояние.

4. Пример решения задачи

Для решения задачи выбраны следующие классы объектов, характеризующих состояния системы управления воздушным движением [5]: «заданный эшелон» – «$Э_1$», «$Э_2$», «$Э_3$», …, «$Э_m$»; ВС – «$ВС_1$», «$ВС_2$», «$ВС_3$», …, «$ВС_k$»; «диспетчер» – {«команда $ВС_i$ занять $Э_j$»}, $i = \{1, 2, ..., k\}$, $j = \{1, 2, ..., m\}$.

Будем полагать, что условия безопасности выполнены, если на каждом эшелоне находится не более одного ВС. Рассмотрим случай m=k=3. Тогда имеем $S = \{S_1, S_2, \ldots, S_{27}\}$, $S_{\text{шт}} = \{S_1, S_2, \ldots, S_6\}$, $S_{\text{ав}} = \{S_7, S_8, \ldots, S_{27}\}$, $X = \{x_1, x_2, \ldots, x_9\}$: x_1 – ВС$_1$ занять эшелон Э$_1$, x_2 – ВС$_1$ занять эшелон Э$_2$, x_3 – ВС$_1$ занять эшелон Э$_3$, x_4 – ВС$_2$ занять эшелон Э$_1$, x_5 – ВС$_2$ занять эшелон Э$_2$, x_6 – ВС$_2$ занять эшелон Э$_3$, x_7 – ВС$_3$ занять эшелон Э$_1$, x_8 – ВС$_3$ занять эшелон Э$_2$ и x_9 – ВС$_3$ занять эшелон Э$_3$.

На рис. 1а показано, что в результате приложения последовательности $p_1 = x_4\ x_8\ x_2$ (неверная команда на занятие ВС$_2$ 1-го эшелона, ВС$_1$ и ВС$_3$ 2-го эшелона) система перешла в критическое состояние s_{14}, означающее опасное сближение ВС$_1$ и ВС$_3$. На рис. 1б представлен вариант перехода из критического состояния s_{14} в состояние s_1, соответствующее штатному расположению всех ВС по эшелонам зоны ожидания, который обеспечивается реализацией синхронизирующей последовательности $p = x_3\ x_8\ x_4$ (команда на занятие ВС$_1$ 3-го эшелона, ВС$_2$ 1-го эшелона, ВС$_3$ 2-го эшелона).

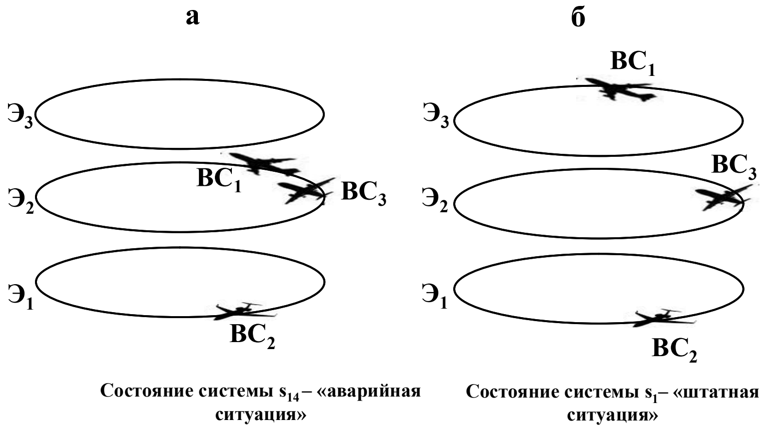

Рис. 1. Нарушенная (а) и штатная (б) синхронизация процессов в авиационно-транспортной системе

5. Заключение

Предложен подход, обеспечивающий эффективное по времени и объему вычислительных операций решение задачи по обеспечению и поддержанию безопасности авиационно-транспортных систем за счет формирования минимальной по длине последовательности управляющих воздействий на систему, приводящих ее в безопасное состояние. Формирование такой последовательности осуществляется на основе использования математической модели, в качестве которой выступает конечный автомат.

Данная модель может быть использована для обучения персонала авиационно-транспортных систем, а в дальнейшем – для оперативного управления потоками воздушных судов в реальных условиях. Результаты работы нашли применение в ОАО «Ил» и могут быть использованы как составная часть общегосударственной системы обеспечения и подержания авиационной безопасности полетов.

Литература

1. БУСЛЕНКО Н. П. *Моделирование сложных систем.* – М.: Наука, 1968. – 356 с.
2. ГИЛЛ А. *Введение в теорию конечных автоматов*. – М.: Наука, 1966. – 272 с.
3. КЛЮЕВ В.В, РЕЗЧИКОВ А.Ф., КУШНИКОВ В.А., ТВЕРДОХЛЕБОВ В.А., ИВАЩЕНКО В.А., БОГОМОЛОВ А.С., ФИЛИМОНЮК Л.Ю. *Анализ критических ситуаций, вызванных неблагоприятным стечением обстоятельств* // Контроль. Диагностика. – 2014. – №7. – С. 12-16.
4. ЛАПКОВСКИЙ Р.Ю., ИВАНОВ А.С., ИВАЩЕНКО В.А. *Причинно-следственный подход к моделированию движения на сложных участках дорожно-транспортной сети* // Управление

большими системами. Выпуск 35. – М.: ИПУ РАН. – 2011. – С. 283-303.

5. НЕЙМАРК М.С., ЦЕСАРСКИЙ Л.Г., ФИЛИМОНЮК Л.Ю. *Модель поддержки принятия решений при входе воздушных судов в зону ответственности аэропорта* // Общероссийский научно-технический журнал "Полет". – 2013. №3. – С. 31-37.
6. НОВОЖИЛОВ Г.В., РЕЗЧИКОВ А.Ф., НЕЙМАРК М.С., ТВЕРДОХЛЕБОВ В.А., ЦЕСАРСКИЙ Л.Г., ФИЛИМОНЮК Л.Ю. *Причинно-следственный подход к анализу авиационно-транспортных систем* // Общероссийский научно-технический журнал "Полет". – 2011. №7. – С. 3-8.
7. ПИТЕРСОН ДЖ. *Теория сетей Петри и моделирование систем.* – М: Мир, 1984. – 264 с.
8. ЦУКАНОВ М.А. *Координация работы технологических звеньев сложноструктурированного производства как экономическая мера* // Управление большими системами: материалы Всеросс. школы-конф. молодых ученых. Т. 3. – Уфа, 1913. – С. 318-321.
9. ШАРОВ В.Д. Применение байесовского подхода для уточнения вероятностей событий в автоматизированной системе прогнозирования и предотвращения авиационных происшествий // Управление большими системами. Выпуск 43. – М.: ИПУ РАН. – 2013. – С. 240-253.
10. BOGOMOLOV A.S., SPERANSKII D.V. *On an optimal synchronizing experiment with linear automata* // Journal of Computer and Systems Sciences International. – 2002. – V. 41. – № 3. – P. 397-403.
11. ROSENBLATT D. // Naval Res.Log. Quart. – 1957. – V. 4. – P. 151.
12. SCHWARZ S. // Czech. Math. Jour. – 1970. – V .20. – P. 632–679.
13. SLOANE N.J.A. // The On-Line Encyclopaedia of Integer Sequences. – 1996 – V. 38. – P. 333-337.

AN APPROACH TO SUPPORT AND MAINTENANCE OF COMPLEX SYSTEMS' SAFETY ON THE BASIS OF AUTOMATION MODELS

Alexander Rezchikov, *Institute of Precision Mechanics and Control of RAS, Saratov, Doctor of Science, Director (iptmuran@san.ru).*
Aleksey Bogomolov, *Institute of Precision Mechanics and Control of RAS, Saratov, Candidate of Science, Scientist (alexbogomolov@ya.ru).*
Vladimir Ivaschenko, *Institute of Precision Mechanics and Control of RAS, Saratov, Doctor of Science, Scientific Secretary (iptmuran@san.ru).*
Leonid Filimonyuk, *Institute of Precision Mechanics and Control of RAS, Saratov, Candidate of Science, Scientist (filimonyukleonid@mail.ru).*

Abstract: An approach to safety support of aviation-transport systems' functioning on a basis of interaction's matching of its components is offered. An automaton model of functioning process of this system, which lets represent a synchronous interaction of their components, based on cause-effect approach is developed. The model can be applied in air-training centers, which arrange retraining and further training of specialist in aviation area.

Keywords: complex system, aviation transport system, finite-state machine, synchronization, safety, accidents.

Статья представлена к публикации членом редакционной коллегии ...

Поступила в редакцию ...
Дата опубликования ...