КІБЕРНЕТИКА

А.А. ЛЕТИЧЕВСКИЙ, А.А. ЛЕТИЧЕВСКИЙ мл., В.Г. СКОБЕЛЕВ, В.А. ВОЛКОВ

УДК 519.68

КИБЕР-ФИЗИЧЕСКИЕ СИСТЕМЫ

Аннотация. Приведен ретроспективный анализ теории кибер-физических систем и охарактеризовано ее современное состояние. Исследован ряд проблем, возникающих в теории гибридных автоматов. Рассмотрена полугрупповая система переходов, являющаяся основой распространения алгебраической теории взаимодействия размеченных транзиционных систем на кибер-физические системы.

Ключевые слова: кибер-физические системы, гибридные автоматы, верификация.

ВВЕДЕНИЕ

Современные информационные технологии инициировали фундаментальные изменения практически во всех сферах жизнедеятельности человека. В частности, в настоящее время широко применяются кибер-физические системы — Cyber-Physical Systems (CPS). Они характеризуются тем, что компьютерные сети и встроенные контроллеры управляют (возможно, при участии человека) физическими процессами посредством обратных связей, т.е. физические процессы влияют на вычисления, а вычисления — на выбор и ход физических процессов [1]. На сегодняшний день CPS используются при исследовании космоса, управлении транспортом, производством, в энергетической и военной сферах, медицине, при построении современной инфраструктуры, для бесконтактного управления бытовой электроникой и т.д.

Как правило, CPS являются системами с критической областью применения. Поэтому при проектировании таких систем предъявляются повышенные требования к их надежности и безопасности. С учетом этого правительство США с 2007 г. рассматривает разработки в области CPS как одну из основных стратегий развития [2] (термин CPS предложен Х. Гилл в 2006 г. Национальному научному фонду США — National Science Foundation). В течение короткого промежутка времени интенсивные исследования в этой области стали проводить во многих странах. В [3–5] охарактеризовано современное состояние теоретических исследований CPS и их приложений на практике. Перспективность и значимость этого направления обосновывается разработкой дорожных карт развития данной научной области в США [6, 7] и Европе [8, 9].

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ

Отправной точкой изучения непрерывно-дискретных систем, по-видимому, можно считать классическую работу Н. Винера [10].

В 50-е годы XX в., в основном в рамках теории дифференциальных уравнений, начала формироваться теория управления. Исходя из этой теории, исследовалась устойчивость трех классов непрерывных систем с переключениями:

1) системы со структурными изменениями — переключения выполняются под действием внешней среды, сбоев, отказов элементов или подсистем; 2) системы с переменной структурой — переключения осуществляются только в контуре обратной связи; 3) импульсные системы — состояние системы может изменяться скачкообразно. Обзор результатов, полученных при исследовании устойчивости непрерывных систем с переключениями, содержится в [11].

Отметим значительный вклад ученых ИК АН УССР в развитие данного направления. Исследования А.И. Кухтенко посвящены анализу и построению сложных многомерных систем управления [12], построению аксиоматической теории динамических управляемых систем [13], разработке теории инвариантности [14], анализу внутренних связей между кибернетикой и фундаментальными науками, в частности с физикой [15]. Результатом исследований В.М. Кунцевича стала разработка основ теории нелинейных систем управления с частотно-импульсной модуляцией [16]. Исследования А.Г. Ивахненко ориентированы на разработку методов автоматического построения моделей по экспериментальным данным на основе группового учета аргументов [17–19].

С учетом математической теории систем построен ряд различных математических моделей непрерывно-дискретных систем. Наиболее известными из них являются следующие три модели.

• Агрегативная система Н.П. Бусленко [20], представляющая собой динамическую систему с фиксированной структурой и выделенными состояниями, в которых возможно мгновенное изменение значений как параметров, так и поведения. Предполагается, что анализ такой модели осуществляется численным моделированием.

• Разработанная В.М. Глушковым непрерывно-дискретная модель, в которой заложена возможность изменения структуры системы за счет порождения, удаления, активации и деактивации элементов в процессе их параллельной эволюции. На основе этой модели в ИК АН УССР была реализована программная система НЕДИС [21], моделирующая поведение системы последовательным выбором событий из календаря планирования и использующая при необходимости подпрограммы непрерывных численных методов (интеграторов).

• Гибридная система [22], в основе которой лежит предположение о том, что непрерывным объектом управляет дискретное устройство (контроллер). Это означает, что непрерывная динамика, порождаемая одной из заданных непрерывных систем, перемежается с дискретными командами либо на мгновенное переключение с этой системы на другую, либо на мгновенную перестройку с заданных текущих координат на другие координаты, либо на то и другое одновременно. Непрерывная и дискретная составляющие системы могут включать параметры, влияющие на поведение системы. Некоторыми из таких параметров можно управлять. Математической моделью гибридной системы является гибридный автомат [23–25]. Эта модель основана на достижениях теории символьных вычислений [26, 27] и теории реактивных систем [28, 29]. Гибридный автомат представляет собой конечную размеченную систему переходов, дуги которой соответствуют событиям, приводящим к изменению поведения, а вершины — динамическим системам, реализующим непрерывное поведение между событиями.

Рассмотренные три модели непрерывно-дискретных систем отличаются базовыми понятиями, выбранными в качестве основных. Различия являются внешними в том смысле, что эти модели определяют один и тот же класс систем, что доказано в [30] методом сведения одной модели к другой.

Начиная с конца XX в. гибридный автомат становится одной из основных математических моделей для кибер-физических систем. Из-за проблем, связан-

ных с разрешимостью задач, в теоретических исследованиях ограничиваются классом гибридных автоматов, у которых непрерывная динамика линейная или кусочно-линейная, а условия, определяющие дискретные переходы, являются линейными неравенствами.

Хотя в теоретических исследованиях, как правило, фигурируют гибридные автоматы, построенные для достаточно простых модельных задач, известны интересные применения таких автоматов при решении прикладных задач. Отметим некоторые из них. В [31, 32] рассмотрена задача построения системы температурного контроля атомного реактора. Показано, что символьная верификация (с использованием системы HyTech) соответствующего гибридного автомата применима при параметрическом синтезе нижней границы значения времени допустимого повторного использования стержня для охлаждения котла. В [33] предложен подход к анализу жизнеспособности многоканальных сенсорных сетей на основе представления компонентов TinyOS линейными гибридными автоматами, символьный анализ которых осуществлялся с помощью системы HyTech. В [34] на основе представления реакций возбудимых клеток кусочно-линейными гибридными автоматами получены аналитические решения в различных фазах цикла возбуждения. Такие автоматы можно использовать как основу для символьного моделирования сложных биологических систем. В [35] электрическая активность возбудимой сердечной ткани моделируется сетью нелинейных гибридных автоматов, представляющей собой $n \times n$-массив. Предложенную модель можно использовать для анализа диапазонов параметра и сетевого соединения, связанных с опасными болезнями сердца, а также для проверки функциональности таких вживляемых сердечных устройств, как кардиостимуляторы и дефибрилляторы. В [36] предложен символьный масштабируемый метод автоматического синтеза гибридных автоматов, моделирующих электрические сети с переключениями, т.е. состоящие из физических компонентов, соединенных в соответствии с некоторой реконфигурируемой топологией сети. В [37] исследуется структура подсистемы, встроенной в производственную CPS и предназначенной для автоматического обнаружения износа и отказов оборудования. Сформулированы задачи, решение которых необходимо для построения такой подсистемы. Следует отметить предложенный авторами подход к организации автоматического on-line обнаружения аномалий в компонентах объекта. В его основе лежит изучение поведения гибридных автоматов при корректном функционировании моделируемого объекта на экспериментальных данных.

В последнее время большое внимание уделяется разработке моделей, абстракций и архитектуры, ориентированных на интеграцию в единую систему потоков информации, генерируемой на различных уровнях проектирования CPS [38], а также моделей и методов, предназначенных для обеспечения безопасности CPS [39]. Проблемы моделирования, проектирования и анализа CPS изложены с единых позиций в [40].

Отметим, что с 70-х годов XX в. начались разработки программных комплексов, предназначенных для моделирования и анализа непрерывно-дискретных систем. Существенный прорыв в этом направлении связан с появлением техники символьных вычислений [41] и автоматизированных методов анализа реактивных систем [42]. В 1992 г. создана программная система Kronos [43], в которой оценки значений непрерывных переменных в локальных поведениях использовались в математической модели для применения методов символьной верификации при анализе поведения гибридной системы. В 1995 г. была разработана программная система HyTech [31] для автоматической верификации гибридных систем на основе символьных методов. На рубеже XX и XXI вв. появи-

лись языки, претендующие на универсальность: язык UML [44], предназначенный для построения модели исследуемого объекта практически любого вида, и язык Modelica [45] для моделирования объектов, представляемых системами алгебро-дифференциальных уравнений. В [46] приведен сравнительный анализ базовой семантики, выразительной силы и решающих механизмов наиболее распространенных языков, формализмов и инструментариев, предназначенных для проектирования и верификации гибридных систем.

ГИБРИДНЫЕ АВТОМАТЫ

Следуя [23, 25], рассмотрим гибридный автомат (ГА) как систему $\mathsf{H} = (V, E, \Sigma, X, Init, Inv, Flow, Jump)$. Здесь:

V — конечное множество вершин, соответствующих непрерывным режимам работы;

Σ — конечное множество имен дискретных событий;

$E \subseteq V \times \Sigma \times V$ — множество дискретных переходов (переход из вершины v_1 в вершину v_2 под действием события σ обозначается $v_1 \xrightarrow{\sigma} v_2$);

$X = \{x_1, \ldots, x_n\}$ — конечное множество действительных переменных, где число n — размерность ГА H (множество производных по времени переменных из множества X обозначается $\dot{X} = \{\dot{x}_1, \ldots, \dot{x}_n\}$, а множество значений переменных из множества X, передаваемых при дискретных переходах, — $X' = \{x_1', \ldots, x_n'\}$);

$Init$, Inv, $Flow$ — отображения множества V во множества таких предикатов, что для каждой вершины $v \in V$ свободные переменные предикатов $Init(v)$ и $Inv(v)$ принадлежат множеству X, а свободные переменные предиката $Flow(v)$ — множеству $X \cup \dot{X}$ ($Init(v)$ определяет значения переменных, из которых ГА H может стартовать в вершине v, $Inv(v)$ — ограничения на значения переменных, при которых реализуется непрерывная динамика ГА H в вершине v, а $Flow(v)$ — уравнения динамики ГА H в вершине v);

$Jump$ — отображение множества E во множество предикатов, свободные переменные которых принадлежат множеству $X \cup X'$ (для каждого перехода $e = v_1 \xrightarrow{\sigma} v_2$ предикат $Jump(e)$ определяет, когда возможен дискретный переход, соответствующий событию σ, а также какие значения переменных и как изменяются при этом переходе).

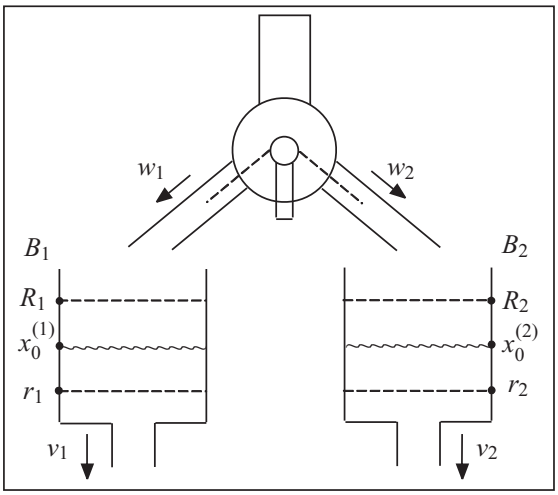

Рис. 1. Система резервуаров, наполняемых водой

Пример 1. Проиллюстрируем возможность применения ГА при построении системы управления для обобщения модельной задачи наполнения двух резервуаров водой [47].

Имеются цилиндрические резервуары B_i $(i = 1, 2)$ с отверстиями в дне, которые могут наполняться водой с помощью переключаемого крана (рис. 1). Технические характеристики резервуара B_i $(i = 1, 2)$ следующие: s_i — площадь поперечного сечения, r_i — нижняя граница допустимого уровня воды, R_i — верхняя граница допустимого

уровня воды, w_i — скорость наполнения водой, v_i — скорость стока воды. Предполагается, что первоначально кран отключен, а уровень воды в резервуаре B_i $(i=1,2)$ равен $x_0^{(i)}$, где $r_i < x_0^{(i)} < R_i$.

Требуется построить систему управления переключениями крана, обеспечивающую уровень воды в резервуарах в допустимых границах.

Построим ГА, являющийся математической моделью системы управления переключениями крана. Множество вершин, соответствующих непрерывным режимам управления, имеет вид $Q = \{q_0, q_1, q_2\}$, где q_0 — режим, при котором кран закрыт, а q_i $(i=1,2)$ — режим, при котором наполняется резервуар B_i.

Из физических соображений вытекает, что динамика (т.е. потоковые условия) изменения уровня воды в резервуаре B_i $(i=1,2)$ описывается дифференциальными уравнениями:

- $\dot{x}^{(i)} = s_i^{-1}(w_i - v_i)$, если поток воды направлен в данный резервуар;
- $\dot{x}^{(i)} = -s_i^{-1} v_i$, если поток воды не направлен в данный резервуар.

Из формулировки задачи вытекает, что:

— инвариантные условия, при которых осуществляется наполнение водой резервуара, имеют вид

- $x^{(2)} > r_2 \,\&\, x^{(1)} < R_1$ для резервуара B_1;
- $x^{(1)} > r_1 \,\&\, x^{(2)} < R_2$ для резервуара B_2;

— условия переходов имеют вид

- $x^{(1)} = r_1 \,\&\, x^{(2)} > r_2$ для перехода от вершины q_0 к вершине q_1;
- $x^{(2)} = r_2 \,\&\, x^{(1)} > r_1$ для перехода от вершины q_0 к вершине q_2;
- $x^{(2)} = r_2 \vee x^{(1)} = R_1$ для перехода от вершины q_1 к вершине q_2;
- $x^{(1)} = r_1 \vee x^{(2)} = R_2$ для перехода от вершины q_2 к вершине q_1;

— начальными условиями, передаваемыми при каждом переходе $q_0 \to q_1$, $q_0 \to q_2$, $q_1 \to q_2$ и $q_2 \to q_1$, являются финальные значения переменных $x^{(1)}$ и $x^{(2)}$ в вершине, из которой осуществляется переход.

Таким образом, получаем ГА, изображенный на рис. 2.

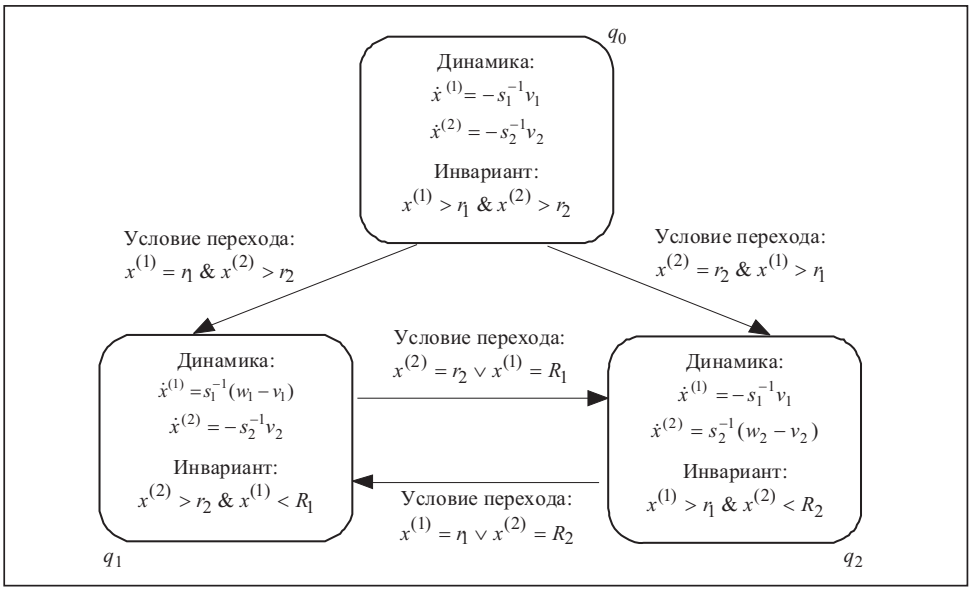

Рис. 2. Схема ГА, управляющего системой резервуаров, наполняемых водой

При моделировании ГА осуществляется переход от дифференциальных уравнений к следующим конечно-разностным уравнениям с заданным положительным шагом Δt:

- $x_{n+1}^{(i)} = x_n^{(i)} + s_i^{-1}(w_i - v_i)\Delta t$ $(n = 0, 1, \dots)$ для уравнения $\dot{x}^{(i)} = s_i^{-1}(w_i - v_i)$;
- $x_{n+1}^{(i)} = x_n^{(i)} - s_i^{-1} v_i \Delta t$ $(n = 0, 1, \dots)$ для уравнения $\dot{x}^{(i)} = -s_i^{-1} v_i$.

Согласно условию задачи считаем, что первоначально кран отключен, уровень воды в резервуаре B_i $(i = 1, 2)$ равен $x_0^{(i)}$, где $r_i < x_0^{(i)} < R_i$, а при инициализации процесса управления для каждого резервуара B_i $(i = 1, 2)$ вычисления осуществляются в соответствии с формулами $x_{n+1}^{(i)} = x_n^{(i)} - s_i^{-1} v_i \Delta t$ $(n = 0, 1, \dots)$. При достижении критического уровня воды в некотором резервуаре кран включается и начинает подавать в него воду. Далее кран может только переключаться с одного резервуара на другой.

Основная цель моделирования построенного ГА состоит в проверке корректности системы управления, выявлении допустимых диапазонов значений параметров и т.д.

Для каждого ГА H могут быть определены следующие две размеченные транзиционные системы (РТС).

Временна́я РТС (ВРТС) имеет вид $S_{\mathsf{H}}^t = (Q, Q_0, A, T_A)$, где $Q \subseteq V \times \mathsf{R}^n$ — пространство состояний (любое подмножество множества Q называется регионом), удовлетворяющее условию $(v, \mathbf{x}) \in Q \Leftrightarrow Inv(v)[X := \mathbf{x}] = true$, $Q_0 \subseteq Q$ — такой регион начальных состояний, что $(v, \mathbf{x}) \in Q_0 \Leftrightarrow Init(v)[X := \mathbf{x}] = true \,\&$ $\& \; Inv(v)[X := \mathbf{x}] = true$, $A = \Sigma \cup \mathsf{R}_{\geq 0}$ — множество отметок переходов, а $T_A \subseteq$ $\subseteq Q \times A \times Q$ — множество таких переходов, что

$$(\forall \sigma \in \Sigma)((v, \mathbf{x}) \xrightarrow{\sigma} (v', \mathbf{x}') \in T_A \Leftrightarrow (\exists e \in E)(e = v \xrightarrow{\sigma} v' \&$$

$$\& \; Jump(e)[X := \mathbf{x}, X' := \mathbf{x}'] = true)),$$

$$(\forall \delta \in \mathsf{R}_{\geq 0})((v, \mathbf{x}) \xrightarrow{\delta} (v, \mathbf{x}') \in T_A \Leftrightarrow (\exists (f : [0, \delta] \to \mathsf{R}^n \&$$

$$\& \; \dot{f} : (0, \delta) \to \mathsf{R}^n))(f(0) = \mathbf{x} \,\&\, f(\delta) = \mathbf{x}' \&$$

$$\& \; (\forall \varepsilon \in (0, \delta))(Inv(v)[X := f(\varepsilon)] = true \&$$

$$\& \; Flow(v)[X := f(\varepsilon), \dot{X} := \dot{f}(\varepsilon)] = true))).$$

Из последней формулы вытекает $q \xrightarrow{0} q$ для всех $q \in Q$.

Абстрактная по времени РТС (АРТС) имеет вид $S_{\mathsf{H}}^a = (Q, Q_0, B, T_B)$, где Q и Q_0 — такие же, как и для ВРТС, $B = \Sigma \cup \{\tau\}$ $(\tau \notin \Sigma)$, а $T_B \subseteq Q \times B \times Q$ — множество переходов, где $(v, \mathbf{x}) \xrightarrow{\sigma} (v', \mathbf{x}') \in T_B$ $(\sigma \in \Sigma)$ определяется так же, как и для ВРТС, $(v, \mathbf{x}) \xrightarrow{\tau} (v', \mathbf{x}') \in T_B \Leftrightarrow (\exists \delta \in \mathsf{R}_{\geq 0})((v, \mathbf{x}) \xrightarrow{\delta} (v', \mathbf{x}') \in T_A)$.

Каждому переходу $q \xrightarrow{a} q'$ $(a \in A)$ ВРТС S_{H}^t сопоставлена его продолжительность δ, где $\delta = 0$ для $a \in \Sigma$ и $\delta = a$ для $a \in \mathsf{R}_{\geq 0}$. Бесконечная траектория (при анализе РТС вместо термина «траектория» используется термин «история») $\langle a_i q_i \rangle_{i \geq 1}$ ВРТС S_{H}^t расходится, если расходится ряд $\sum_{i \geq 1} \delta_i$, где δ_i — продолжительность перехода $q_{i-1} \xrightarrow{a_i} q_i$. Бесконечная траектория $\langle a_i q_i \rangle_{i \geq 1}$ АРТС S_{H}^a расхо-

дится, если существует такая расходящаяся траектория $\langle b_i q_i \rangle_{i\geq 1}$ ВРТС S^t_{H}, что для каждого $i \geq 1$ выполнено условие $a_i = b_i$ или $a_i, b_i \notin \Sigma$.

Для систем реального времени реализация осуществляется только в виде ГА, у которых бесконечные траектории расходятся. Это единственное предположение о жизнеспособности ГА. Такие ГА называются незеноновскими (nonzeno).

Из-за сложности анализа и проблем разрешимости ВРТС S^t_{H} используется только при решении задач достижимости того или иного региона (такие задачи возникают при верификации требований безопасности) и задач включения множеств временны́х трасс. Во всех остальных случаях используется АРТС S^a_{H}.

Отметим, что в терминах ВРТС S^t_{H} для заданной вершины ГА можно осуществить качественный анализ региона ее начальных состояний и региона, из которого в ней происходит дискретный переход. Действительно, в [48] предложен непрерывный подход (on-the-fly approach) для построения покрывающей аппроксимации достижимого региона состояний ГА, автоматически генерируемой и запускающейся с текстового схемного файла нелинейной аналоговой схемы с переключениями. Такой же подход можно применить и для построения покрывающей аппроксимации региона начальных состояний. Используя двустороннее построение этих аппроксимаций, получаем классификацию пар фрагментов рассматриваемых регионов по времени соответствующей динамики. Также могут быть выделены фрагменты регионов, лишние при корректном функционировании ГА.

Для АРТС S^a_{H} множество трасс с операцией их сочленения является частичной полугруппой, аналогичной тем, которые исследованы в [49]. В то же время для ВРТС S^t_{H} ситуация значительно сложнее из-за наличия переходов вида $q \xrightarrow{a} q'$ $(a \in \mathsf{R}_{\geq 0})$.

ПОЛУГРУППОВЫЕ ТРАНЗИЦИОННЫЕ СИСТЕМЫ

Понятие полугрупповой транзиционной системы, предложенное в [50], обобщает модели, основанные на понятиях временны́х и гибридных автоматов. Основной целью его введения является распространение алгебраической теории взаимодействия и технологии инсерционного моделирования на кибер-физические системы.

Зафиксируем множество T моментов времени, которое предполагается подмножеством множества R вещественных чисел, множество состояний S, полугруппу трасс H и параметрическое отношение переходов $G = \{g_t \subseteq S \times H \times S | \, t \in T\}$. Элементы множеств g_t называются переходами. По аналогии с тем, как это сделано для РТС, положим: $s \xrightarrow{h}_t s' \Leftrightarrow (s,h,s') \in g_t$, $s \xrightarrow{h} s' \Leftrightarrow \exists\, (t \in T)((s,h,s') \in g_t)$. Выражение вида $s \xrightarrow{h}_t s'$ будем использовать не только как высказывание, но и как обозначение перехода. При этом t называется длительностью этого перехода. Конечная или бесконечная последовательность переходов вида

$$s_0 \xrightarrow{h_1}_{t_1} s_1 \ldots s_{n-1} \xrightarrow{h_n}_{t_n} s_n \xrightarrow{h_{n+1}}_{t_n} s_{n+1} \ldots$$

называется историей, а сумма длительностей переходов конечной истории — длительностью этой истории. Таким образом, трассы на переходах используются в истории как действия.

Полугрупповой транзиционной системой (ПТС) называется тройка $\mathsf{S} = (S, H, G)$, удовлетворяющая следующим аксиомам:

$$\forall\, (t, t' \in T)(t + t' \in T), \tag{1}$$

$$\forall (s \in S) \exists (h \in H,\ s' \in S)(s \xrightarrow{h} s'), \tag{2}$$

$$\forall (t, t' \in T,\ s, s', s'' \in S,\ h, h' \in H)(s \xrightarrow{h}_{t} s' \xrightarrow{h'}_{t'} s'' \Rightarrow s \xrightarrow{hh'}_{t+t'} s''), \tag{3}$$

$$\forall (t, t' \in T,\ s, s' \in S,\ h \in H)(s \xrightarrow{h}_{t+t'} s' \Rightarrow$$

$$\Rightarrow (\exists\, h', h'' \in H,\ s'' \in S)(h = h'h'',\ s \xrightarrow{h'}_{t} s'' \xrightarrow{h''}_{t'} s')). \tag{4}$$

Аксиома (1) называется аксиомой полугруппы и выражает тот факт, что T — полугруппа, а время направлено в сторону увеличения, если в T нет отрицательных чисел.

Аксиома (2) называется аксиомой продолжения и означает, что в ПТС (в отличие от РТС) нет тупиков.

Аксиома (3) называется аксиомой свертывания и показывает, что любую конечную историю можно свернуть до одного перехода.

Аксиома (4) называется аксиомой развертывания и показывает, что любой достаточно длинный переход можно развернуть в историю из нескольких переходов.

В работе [50] приведены примеры полугрупп моментов времени, полугрупповых систем и полугрупп трасс, которые могут встретиться на практике. В частности, показано, что ГА Хенцингера можно представить в виде ПТС определенного вида, а РТС получаются, когда множество моментов времени совпадает с множеством положительных целых чисел и полугруппа трасс — свободная полугруппа.

Для дальнейшего необходимо уточнить понятие эквивалентности состояний и построить алгебру поведений полугрупповых систем.

Эквивалентность. Полугрупповая система может рассматриваться как обычная РТС, действия которой — элементы полугруппы H, а переходы размечены временны́ми параметрами так, что выполняются аксиомы полугрупповой системы. Если длительности переходов включить в действия, т.е. рассматривать в качестве действий пары (h, t), $h \in H$, $t \in T$, то получим дискретную систему, а эквивалентность состояний дискретной системы можно перенести на исходную полугрупповую систему. Понятия трассовой и бисимуляционной эквивалентности, а также алгебра поведений определены для дискретных систем. Остается распространить эти понятия на полугрупповые системы.

Сначала рассмотрим трассовую эквивалентность. Пусть

$$s_0 \xrightarrow{h_1}_{t_1} \ldots \xrightarrow{h_n}_{t_n} s_n$$

является конечной историей функционирования полугрупповой системы. Нормированной трассой, порожденной этой историей, назовем пару $(h_1 \ldots h_n, t_1 + \ldots + t_n)$.

Пусть $L(s)$ — множество всех нормированных трасс, порожденных историями, которые начинаются в состоянии s. Состояния s и s' называются трассово эквивалентными, если $L(s) = L(s')$. Любую конечную историю полугрупповой системы можно свернуть в один переход, длительность которого равна сумме длительностей переходов этой истории.

Таким образом, рассматривая состояния полугрупповой системы с точностью до трассовой эквивалентности, абстрагируемся от состояний и представления элементов полугруппы трасс на историях с сохранением временны́х характеристик трасс.

Бисимуляционная эквивалентность определяется прямым перенесением этого понятия с дискретных транзиционных систем. Именно, бинарное отношение R на множестве состояний полугрупповой системы назовем отношением бисимуляции (bisimulation), если для любой пары (s, s') состояний имеют место следующие утверждения:

$$(s, s') \in R \wedge s \xrightarrow{h}_t r \Rightarrow \exists r'((r, r') \in R \wedge s' \xrightarrow{h}_t r'),$$

$$(s, s') \in R \wedge s' \xrightarrow{h}_t r' \Rightarrow \exists r((r, r') \in R \wedge s \xrightarrow{h}_t r).$$

Состояния s и s' полугрупповой системы называются бисимуляционно эквивалентными (bisimilar), если существует отношение бисимуляции R такое, что $(s, s') \in R$.

Поведение РТС является инвариантом эквивалентности состояний. Для конструктивного определения поведений строится алгебра поведений и поведения рассматриваются как решения систем уравнений вида $x = F(x)$ в этой алгебре, $x = (x_1, x_2, \ldots)$ (допускается и бесконечное множество уравнений и неизвестных).

Полугрупповая алгебра поведений. Такая алгебра строится для ПТС так же, как и алгебра поведений для их дискретных моделей: двухосновная алгебра, основное множество — поведения, другое множество — действия. Две операции: префиксинг $a.u$ и недетерминированный выбор $u + v$ (a — действие, u и v — поведения); три константы: Δ (завершение поведения), 0 (тупиковое поведение) и $\perp$ (неопределенное поведение). На алгебре поведений определяется частичный порядок с наименьшим элементом $\perp$. Недетерминированный выбор — это ассоциативная коммутативная и идемпотентная операция. Единственным отличием полугрупповой алгебры поведений является то, что на множестве действий определена полугрупповая операция. В связи с этим в полугрупповой алгебре поведений возникает еще одно тождество: $a.b.u = (ab).u$.

Для вычисления поведений необходима полная алгебра поведений (каждое направленное множество имеет наименьшую верхнюю грань). Конструкция полной полугрупповой алгебры поведений повторяет конструкцию, описанную в работе [51] для РТС. Теперь можно решать уравнения в алгебре поведений и определить поведение системы в заданном состоянии.

Пусть задана некоторая полугрупповая система. Сопоставим каждому состоянию s поведение $beh(s)$ системы в данном состоянии. Поведения — это элементы полугрупповой алгебры поведений. Поведения удовлетворяют системе уравнений

$$beh(s) = \sum_{t \in T} \sum_{s \xrightarrow{h}_t s'} (h, t).beh(s').$$

Данная система бесконечная, однако при достаточно конструктивном задании переходов ее можно использовать для последовательного порождения историй и трасс.

Для полугрупповой алгебры поведений может быть доказана следующая теорема о связи поведений с бисимуляционной эквивалентностью состояний.

Теорема 1. Два состояния полугрупповой системы бисимуляционно эквивалентны тогда и только тогда, когда их поведения совпадают.

Для решения некоторых задач вместо бисимуляционной эквивалентности целесообразнее использовать более сильную трассовую эквивалентность. Важнейшим примером такой задачи является задача распознавания достижимости некоторого свойства состояний транзиционной системы. Для трассовой эквивалентности в качестве алгебры поведений используется алгебра, которая получается из алгебры поведений добавлением тождества правой дистрибутивности:

$$a.(u + v) = a.u + a.v.$$

Если заменить операцию префиксинга последовательной композицией поведений, то получим известную полугрупповую алгебру Клини. Выражения этой алгебры определяют множества нормированных трасс, порождаемых состояниями транзиционных систем.

Алгебру поведений обычно обогащают, добавляя новые операции, которые определяются с помощью систем уравнений. К стандартным обогащениям относятся последовательная и параллельная композиции.

ПОЛУГРУППОВЫЕ СРЕДЫ

Полугрупповые транзиционные системы, так же, как временны́е автоматы или ГА, удобно использовать для моделирования простейших систем, состоящих из небольшого числа управляемых (непрерывных) и управляющих (дискретных) компонентов. Для моделирования более сложных распределенных многоуровневых систем с большим числом взаимодействующих компонентов необходимо использовать дополнительные средства, позволяющие моделировать структурные свойства этих систем. В технологии инсерционного моделирования такими средствами являются средства описания взаимодействия агентов и сред [52].

Основная модель кибер-физической системы в инсерционном моделировании — многоуровневая среда с погруженными в нее агентами. Естественным образом возникает задача адаптации системы инсерционного моделирования IMS для работы с моделями кибер-физических систем (CPS-моделями). Для этой цели строим CPS-модель в виде композиции среды и агентов, погруженных в эту среду, причем среда и агенты представлены в виде ПТС.

Атрибутная полугрупповая среда. Такая среда строится так же, как и атрибутная среда в инсерционном моделировании, но с некоторыми отличиями. Среда и агенты суть ПТС, а их композиция определяется с помощью функции погружения. Эта функция должна быть построена так, чтобы выполнялись аксиомы полугрупповых систем. Описание среды определяет ее тип и представляет собой набор функциональных символов (сигнатура) многосортного языка исчисления предикатов, который используется для описания свойств системы (базовый логический язык).

Функциональные символы делятся на интерпретированные и неинтерпретированные (атрибуты). Интерпретация атрибутов определяет состояние системы. В дискретных системах (с дискретным временем) переходы выполняются скачкообразно: один переход, одно изменение состояния. При моделировании кибер-физических систем удобно различать непрерывные и дискретные атрибуты. Непрерывные атрибуты меняют свои значения непрерывно с течением времени, дискретные — только в моменты выполнения действий, которые эти значения изменяют. В остальные моменты времени они сохраняют значения, полученные при последнем изменении.

Для определенности будем считать, что состояние непрерывного атрибута представлено простым атрибутом типа real (одномерная система) или массивом элементов типа real (многомерная система). Для каждого непрерывного атрибута задан закон его эволюции и в любой момент времени можно получить точное или приближенное значение его состояния. Это означает следующее. При моделировании системы, представляющей собой среду с погруженными в нее агентами, строится история функционирования системы, начинающаяся в определенный момент модельного времени. Моменты времени, в которые выполняются переходы системы, выбираются инсерционной машиной.

Операторы, выполняющие переход, могут получить текущее время (время начала перехода) с помощью непрерывного атрибута current time, а значение непрерывного атрибута в момент t — с помощью атрибутного выражения $\mathrm{state}(x, t)$,

где x — имя непрерывного атрибута, t — момент времени. Изменение закона эволюции непрерывного атрибута получают различными средствами. Примером является оператор $z{:=}\,\text{evolution}(z0,\ F(z))\text{while}(u(z))$ со следующей семантикой. Пусть $f: T \to \mathsf{R}$ — решение уравнения $\dot{z} = F(z)$ с начальным условием $z(0) = z0$. Тогда предыдущий закон эволюционирования атрибута z заменяется новым законом $z(t) = f(t)$. При этом новый закон определен на максимальном интервале, на котором во всех точках выполняется условие $u(z)$ (инвариант режима в автомате Хенцингера).

Для системы должна быть истинной аксиома продолжения. Поэтому все непрерывные атрибуты определяются на всем множестве T. Это можно выполнить с помощью законов эволюции, которые действуют по умолчанию. Например, непрерывный атрибут сохраняет некоторое постоянное значение или может приобретать любое значение из некоторого интервала.

Локальные описания и базовые протоколы. Для описания функции погружения (взаимодействие агентов и сред) используются локальные описания (по другой терминологии — базовые протоколы). Общая форма локального описания остается традиционной:

$$B = \forall x(\alpha(x) \to < P(x) > \beta(x)).$$

Локальные описания можно рассматривать двояко. С одной стороны, это формула, определяющая некоторое свойство системы, с другой — локальное описание определяет множество переходов системы для некоторого класса ее состояний или недетерминированный оператор на множестве состояний среды. Когда локальное описание используется в таком качестве, оно называется базовым протоколом.

Пред- и постусловия базового протокола — это формулы базового логического языка. Процесс в полугрупповой системе, как и в дискретном случае, определяется конечным выражением алгебры поведений. Пользуясь эквивалентными преобразованиями выражений алгебры поведений, один протокол можно свести к множеству протоколов, в каждом из которых процесс будет нормированной трассой (h, t), а базовый протокол определяет один переход длительности t.

Базовые протоколы используются для порождения историй и трасс атрибутной среды. Возможны два подхода для решения данной задачи. Первый называется конкретным, второй — символьным моделированием. В первом случае имеются в виду конкретные состояния атрибутной среды, в которых все атрибуты, необходимые для вычисления предусловия, заданы точно. Новое состояние также должно быть конкретным. Переход вычисляется для конкретного набора значений параметров. Для вычисления перехода задаются алгоритмы решения двух задач: вычисление предусловия и выбор конкретных значений атрибутов среды таким образом, чтобы постусловие было истинным на новом состоянии среды. Переход возможен только при истинном значении предусловия и существовании состояния, на котором истинно постусловие.

При символьном моделировании состояние среды определяется ее свойствами, выраженными на базовом логическом языке. Условием применимости перехода является выполнимость конъюнкции формулы текущего состояния среды и предусловия локального описания. Для выполнения перехода используется предикатный трансформер — преобразование формулы исходного состояния в формулу, определяющую возможные новые состояния. Подробные описания предикатных трансформеров для дискретных сред и достаточно широкого класса формул приведены в работе [53].

Если операторы изменения законов эволюции непрерывных атрибутов можно представить в виде присваиваний, то эти формулы можно использовать и для полугрупповых сред. Требуется только настроить дедуктивную систему на проверку выполнимости формул, содержащих такие функции, как решение системы дифференциальных уравнений или неравенства с трансцендентными функциями. Стандартным подходом может служить аппроксимация сложных функций полиномами и использование алгоритмов компьютерной алгебры.

Описание моделей в системе IMS. Инсерционная машина системы IMS, разработанная для моделирования, генерации трасс и тестирования многоагентных распределенных систем, использует двухуровневую систему управления генерацией трасс. Нижний уровень, или базовая система, состоит из базовых протоколов, определяющих функцию погружения атрибутной среды. Локальных описаний может быть недостаточно для полного задания модели. На базовых протоколах не определены ограничения на последовательности их применения, что может привести к рассмотрению нежелательных историй и трасс.

В системе IMS верхним уровнем описания модели служит управляющая система, определяющая порядок применения локальных определений базовой системы. Она может быть задана системой уравнений в расширенной алгебре поведений, т.е. алгебре поведений, в которой помимо основных операций и функций используются функции погружения для различных сред. Особенность этой системы в том, что в множество ее действий входят локальные определения для базовой системы. Состояние всей системы определяется выражением $U[S]$, где U — состояние управляющей системы, S — состояние базовой системы, определенной множеством локальных описаний Q. Отношение переходов для системы с управлением определяется правилами

$$\frac{U \xrightarrow{a} U'}{U[S] \xrightarrow{a} U'[S]}\ a \notin Q, \qquad \frac{U \xrightarrow{a} U',\ S \xrightarrow{a} S'}{U[S] \xrightarrow{a} U'[S']}\ a \in Q.$$

Допустим, что скрыли переходы с действиями, отличными от локальных описаний базовой системы, т.е. первое правило заменили правилом

$$\frac{U \xrightarrow{a} U'}{U[S] \to U'[S]}\ a \notin Q.$$

Тогда для внешнего наблюдателя не будет разницы между функционированием базовой системы без управления и с управлением. Он видит только трассы, которые относятся к той же самой базовой системе. Правда, с управляющей системой их может быть меньше, а также возможны тупиковые состояния, которых нет у базовой системы. Управляющая система как среда имеет доступ к состоянию базовой системы и может анализировать ее состояния так, как это выполняет инсерционная машина реального времени. Эти машины могут использоваться как управляющие системы. Однако для генерации трасс нужен еще один уровень управления — аналитическая инсерционная машина. Такая машина рассмотрена в [54]. Для верхнего уровня управления в ней используется язык UCM [55], предназначенный для графического представления требований с возможностью описывать параллельные вычисления.

ПРИМЕР ОПИСАНИЯ CPS В СИСТЕМЕ IMS

Рассмотрим систему управления наполнением двух резервуаров водой, представленную ранее с помощью ГА. Среда включает атрибут перечислимого

типа $\mathrm{tap} = 0,1,2$, характеризующий состояние крана: отключен, направлен в первый резервуар, направлен во второй резервуар, и два непрерывных атрибута $x1$ и $x2$, определяющих уровень воды в двух резервуарах. По умолчанию доступен атрибут current time. Остальные символы — это переменные (параметры базовых протоколов) и вещественные константы. Семантика оператора evolution описана выше. Функции Fon и Foff соответствуют правым частям уравнений: $\mathrm{Fon}(\mathrm{i}) = (\mathrm{w}(\mathrm{i}) - \mathrm{v}(\mathrm{i}))/\mathrm{s}(\mathrm{i})$, $\mathrm{Foff}(\mathrm{i}) = -(\mathrm{v}(\mathrm{i})/\mathrm{s}(\mathrm{i}))$. Начальные состояния определяются формулой (запятая используется вместо конъюнкции)

$$\mathrm{init}: (\mathrm{tap} = 0,\ \mathrm{x1} = \mathrm{x10},\ \mathrm{x2} = \mathrm{x20},\ \mathrm{r1} < \mathrm{x10} < \mathrm{R1},\ \mathrm{r2} < \mathrm{x20} < \mathrm{R2});$$

Полугруппа трасс — свободная полугруппа с единицей, порожденная символами S0, S1 и S2. Следующие базовые протоколы определяют функционирование базовой системы без управления верхнего уровня:

```
BP0: (
        1 -> <S0>
        (
                x1:=evolution(state(x1,0),Foff(1))while(x1>r1),
                x2:=evolution(state(x2,0),Foff(2))while(x2>r2)
        )
);
BP1: Forall (t,tau) (
        t=current time,
        delta<=tau<=delta1&
        (x1=r1&x2>r2)&(tap=0)| /((x1=r1)|/(x2=R2))&(tap=2)
                -> <after tau S1>
        (
                tap:=1,
                x1:=evolution(state(x1,t+tau),Fon(1))while(x1<R1),
                x2:=evolution(state(x2,t+tau),Foff(2))while(x2>r2)
        )
);
BP2: Forall (t,tau) (
        t=current time,
        delta<=tau<=delta1&
        (x2=r2&x1>r1)&(tap=0)|/((x2=r2)|/(x1=R1))&(tap=1)
                -> <after tau S2>
        (
                tap:=2,
                x1:=evolution(state(x1,t+tau),Foff(1))while(x1>r1),
                x2:=evolution(state(x2,t+tau),Fon(2))while(x2<R2)
        )
);
```

Базовая система, определенная протоколами BPi, эквивалентна ГА Хенцингера при $\mathrm{delta} = \mathrm{delta1} = \mathrm{tau} = 0$. Для ее нормального функционирования всегда должно выполняться условие безопасности $\mathrm{x1} < \mathrm{R1}\ \&\ \mathrm{x2} > \mathrm{r2} |/\ \mathrm{x1} > \mathrm{r1}\ \&\ \mathrm{x2} < \mathrm{R2}$. Нарушение этого условия эквивалентно формуле

$$\mathrm{x2} >= \mathrm{R2}\ \&\ \mathrm{x1} >= \mathrm{R1} |/\ \mathrm{x2} <= \mathrm{r2}\ \&\ \mathrm{x1} <= \mathrm{r1},$$

полученной приведением к дизъюнктивной нормальной форме отрицания условия безопасности и отбрасыванием тождественно ложных дизъюнктов. Данная формула достижима.

В случае достижимого состояния, близкого к состоянию (x1 = r1) & (x2 = r2), возможны истории, содержащие явление зеноновских парадоксов (бесконечная смена режимов в течение конечного времени). Для автомата Хенцингера такие истории запрещаются. Но физически они остаются. Их можно исключить, вводя конечное время переключения, т.е. полагая delta > 0.

Обеспечить выполнение условия безопасности можно, заменив строгие равенства подходящими неравенствами. Например,

```
BP1: Forall (t,tau) (
        t=current time,
        delta<=tau<=delta1&
        (x1<=r1+epsilon)&(tap=0)|/((x1<=r1+epsilon)|/(x2>=
                                        R2-epsilon))&(tap=2)
                -> <after tau S1>
        (
                tap:=1,
                x1:=evolution(state(x1,t+tau),Fon(1))while(x1<R1),
                x2:=evolution(state(x2,t+tau),Foff(2))while(x2>r2)
        )
);
```

Здесь константа epsilon выбирается таким образом, чтобы за время delta1 уровень воды в первом сосуде не мог опуститься ниже r1, а во втором не мог подняться выше R2. Аналогично корректируется базовый протокол BP2.

На рис. 3 приведена UCM-карта, отображающая поток управления. От начальной точки до разветвления идет непрерывный процесс стекания воды из резервуаров. Затем выбирается тот из двух протоколов, который раньше будет готов к выполнению (предусловие станет истинным). Если оба протокола готовы одновременно, происходит недетерминированный выбор одного из них.

Ромбы (Stub) скрывают вычисления момента модельного времени, в который следующий протокол будет готов к выполнению. Эти вычисления осуществляет среда. Таким образом, истории функционирования системы имеют вид

$$s_0 \xrightarrow{S0} tau_1\ s_1 \xrightarrow{\varepsilon} t_1\ s_1' \xrightarrow{S1(S2)} tau_2\ s_2 \xrightarrow{\varepsilon} t_2\ s_2' \ldots$$

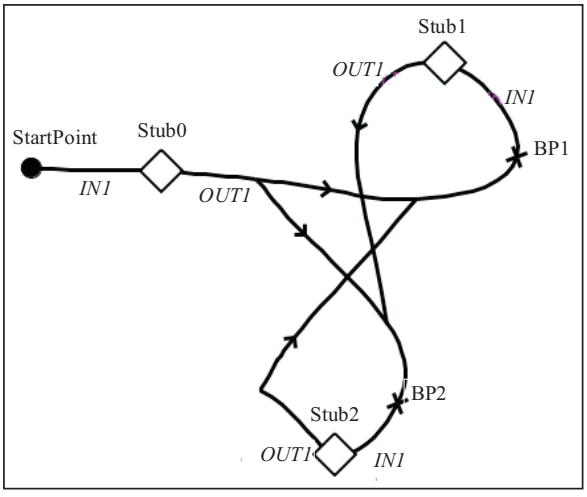

Рис. 3. UCM-карта потока управления переключениями крана

Посредством прямого символьного моделирования с произвольными допустимыми начальными условиями можно получить формулу состояния, которая будет проверяться на выполнимость пересечения с заданным свойством безопасности. Возможен также метод обратного символьного моделирования, когда начальным условием является свойство нарушения безопасности, а результатом — формула начальных условий, при которых это нарушение безопасности возможно.

ЗАКЛЮЧЕНИЕ

В настоящей работе дан ретроспективный обзор исследований, предшествующих современному состоянию теории кибер-физических систем. Подробно рассмотрено понятие гибридного автомата Хенцингера. Показаны пути использования алгебраической теории взаимодействия и технологии инсерционного моделирования для решения задач анализа и синтеза кибер-физических систем. Рассмотрена новая модель CPS, полугрупповая атрибутная среда, предназначенная для распространения алгебраической теории взаимодействия РТС на CPS. При этом важное значение имеет детальная проработка моделей полугрупповых атрибутных сред и алгоритмов их символьной верификации, ориентированных на решение прикладных задач. В частности, большое значение имеет исследование ряда задач, непосредственно связанных с решением для CPS проблемы достижимости за ограниченное время.

СПИСОК ЛИТЕРАТУРЫ

1. Lee E.A. Cyber physical systems: Design challenges. *Proc. of the 11th IEEE Int. Symp. on Object Oriented Real-Time Distributed Computing* (*ISORC*) (May 6, 2008, Orlando, FL., USA). 2008. P. 363–369.
2. Leadership under change: Information technology R&D in a competitive world. 2007. URL: http://www.nitrd.gov/Pcast/reports/PCAST-NIT-FINAL.pdf.
3. Shi J., Wan J., Yan H., Suo H. A survey of cyber-physical systems. *Proc. of the Int. Conf. on Wireless Communications and Signal Processing* (Nanjing, China, Nov. 9–11, 2011). URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.397.4496&rep=rep1&type=pdf.
4. Cyber-physical systems: Situation analysis of current trends. Technologies and Challenges. 2012. URL: http://events.energetics.com/NIST-CPSWorkshop/pdfs/CPS_Situation_Analysis.pdf.
5. Gunes V., Peter S., Givargis T., Vahid F. A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet and Information Systems*. 2014. Vol. 8, N 12. P. 4242–4268.
6. Foundations for innovation in cyber-physical systems. Workshop summary report. 2013. URL: www.nist.gov/sites/default/files/documents/el/CPS-WorkshopReport-1-30-13-Final.pdf.
7. Foundations for innovation. Strategic R&D opportunities for 21st century cyber-physical systems. 2016. URL: http://bookprem.com/gd-ebooks/B00U37SUBG.
8. Cyber-Physical European Roadmap&Strategy, 2015. URL: www.cyphers.eu.
9. sCorPiuS-project.eu: European Roadmap for cyber-physical systems in manufacturing deliverable D1.1. State of the art on cyber-physical systems. 2015. URL: http://www.scorpius.drupal.Pulsartecnalia.com/files/documents/sCorPiuS_D1.1_SotA_v1.2.pdf.
10. Wiener N. Cybernetics, or control and communication in the animal and the machine. New York: John Wiley and Sons, Inc., 1948. 194 p.
11. Васильев С.Н., Маликов А.И. О некоторых результатах по устойчивости переключаемых и гибридных систем. *Актуальные проблемы механики сплошной среды*. 2011. Т. 1. С. 23–81.
12. Кухтенко А.И. Основные задачи теории управления сложными системами. *Сложные системы управления*. 1968. Вып. 1. С. 3–40.
13. Кухтенко А.И. Об аксиоматическом построении математической теории систем. *Кибернетика и вычислительная техника*: *Сложные системы управления*. 1976. Вып. 31. С. 3–25.
14. Кухтенко А.И. Основные этапы формирования теории инвариантности: Ч.1. Основополагающие работы. *Автоматика*. 1984. № 2. С. 3–13; Ч. 2. Расширение тематики исследований. 1985. № 2. С. 3–14; Ч. 3. Нелинейные инвариантные системы. 1985. № 6. С. 3–14.
15. Кухтенко А.И. Кибернетика и фундаментальные науки. Киев: Наук. думка, 1987. 142 с.
16. Кунцевич В.М. Импульсные самонастраивающиеся и экстремальные системы автоматического управления. Киев: Техніка, 1966. 284 с.
17. Ивахненко А.Г. Индуктивный метод самоорганизации моделей сложных систем. К.: Наук. думка, 1982. 296 с.
18. Ивахненко А.Г., Мюллер Й.А. Самоорганизация прогнозирующих моделей. Киев: Техніка, 1985. 225 с.
19. Ивахненко А.Г., Степашко В.С. Помехоустойчивость моделирования. Киев: Наук. думка, 1985. 216 с.

20. Бусленко Н.П. Моделирование сложных систем. Москва: Наука, 1968. 356 с.
21. Программное обеспечение моделирования непрерывно-дискретных систем. Под ред. В.М. Глушкова. Москва: Наука. 1975. 280 с.
22. Maler O., Manna Z., Pnueli A. From timed to hybrid systems. Real-time: Theory in Practice. *LNCS*. 1991. Vol. 600. P. 447–484.
23. Henzinger T.A. The theory of hybrid automata. *Proc. of the 11th Ann. IEEE Symp. on Logic in Computer Science* (*LICS* 96). 1996. P. 278–292.
24. Lynch N., Segala R., Vaandrager F. Hybrid I/O automata. *Information and Computation*. 2003. Vol. 185, Iss. 1. P. 105–157.
25. Raskin J.F. An introduction to hybrid automata. Handbook of Networked and Embedded Control Systems. NY: Springer-Verlag, 2005. P. 491–518.
26. Symbolic computation: applications to scientific computing. Ed. R. Grossman. Philadelphia: SIAM, 1989. 185 p.
27. Advances in the design of symbolic computation systems. Eds. A. Miola, M. Temperini. Wien: Springer-Verlag, 1997. 259 p.
28. Abadi M., Lamport L., Wolper P. Realizable and unrealizable specifications of reactive systems. *LNCS*. 1989. Vol. 372. P. 1–17.
29. Aceto L., Ingolfsdottir A., Larsen K.G., Srba J. Reactive systems: Modelling, specification and verification. Cambridge: Cambridge University Press, 2007. 300 p.
30. Парийская Е.Ю. Сравнительный анализ математических моделей и подходов к моделированию и анализу непрерывно-дискретных систем. *Дифференциальные уравнения и процессы управления. Электронный журнал*. 1997. № 1. 30 с. URL: http://www.math.spbu.ru/diffjournal/RU/numbers/1997.1/issue.html.
31. Henzinger T., Ho P.T. HyTech: The cornell hybrid technology tool. Hybrid systems II. *LNCS*. 1995. Vol. 999. P. 265–293.
32. Saeedloei N., Gupta G. A logic-based modeling and verification of CPS. *ACM SIGBED Review*. 2011. Vol. 8, Iss. 2. P. 31–34.
33. Coleri S., Ergen M., Koo T.K.J. Lifetime analysis of a sensor network with hybrid automata modelling. *Proc. of the 1st ACM International Workshop on Wireless Sensor Networks and Applications* (*WSNA'02*) (Sept. 28, 2002, Atlanta, Ga., USA). 2002. P. 98–104.
34. Ye P., Entcheva E., Grosu R., Smolka S.A. Efficient modeling of excitable cells using hybrid automata. *IET Systems Biology*. 2008. Vol. 2, Iss. 1. P. 24–32.
35. Abbas H., Jang K.J., Mangharam R. Benchmark: Nonlinear hybrid automata model of excitable cardiac tissue. URL: http://repository.upenn.edu/mlab sub papers/90.
36. Cimatti A., Mover S., Sessa M. From electrical switched networks to hybrid automata (Extended version). *LNCS*. 2016. Vol. 9995. P. 164–181.
37. Niggemann J., Lohweg V. On the diagnosis of cyber-physical production systems: State-of-the-art and research. *Agenda Proc. of the 29th AAAI Conference on Artificial Intelligence* (*AAAI'15*) (Austin, Tex., Jan. 25–30, 2015). 2015. P. 4119–4126.
38. Balaji B., Al Faruque M.A., Dutt N., Gupta R., Agarwal Y. Models, abstractions, and architectures: The missing links in cyber-physical systems. *Proc. of the 52nd Annual Design Automation Conference* (*DAC'15*) (San Francisco, Ca., June 07–11, 2015). NY: ACM, 2015. URL: http: dx.doi.org/10.1145/2744769.2747936.
39. Nguen P.H., Ali S., Yue T. Model-based security engineering for cyber-physical systems. *Journal of Information and Software Technology*. 2017. Vol. 83, Iss. C. P. 116–135.
40. Lee E.A., Seshia S.A. Introduction to embedded systems: A cyber-physical systems approach. Sec. Ed. Cambridge, Mass.: MIT Press, 2017. 568 p.
41. Wolfram S.: Mathematica: A system for doing mathematics by computer. Boston, Mass.: Addison-Wesley Longman Publishing Co., Inc., 1988. 767 p.
42. Alur R., Courcoubetis C., Dill D.L. Model-checking for real-time systems. *Proc. of the 5th IEEE Symposium* "*Logic in Computer Science*" (Philadelphia, Pa.) 1990. P. 414–425.
43. Olivero A., Yovine S. Kronos: A tool for verifying real-time systems. User's guide and reference manual. Grenoble: VERIMAG, 1992.
44. Booch G., Rumbaugh J., Jacobson I. Unified modeling language user guide. Boston, Mass.: Addison-Wesley Longman Publishing Co., Inc., 1998. 512 p.
45. Introduction to physical modeling with Modelica. Edited by M. Tiller. *The Kluwer International Series in Engineering and Computer Science*. Boston; Dordrecht; London: Kluwer Academic Publishers, 2001. Vol. 615. 368 p.

46. Carloni L.P., Passerone R., Pinto A., Sangiovanni-Vincentelli A.L. Languages and tools for hybrid systems design foundations and trends in electronic. *Design Automation*. 2005. Vol. 1, Iss. 1/2. P. 1–193.
47. Lygeros J. Lecture notes on hybrid systems. Cambridge: University of Cambridge, 2003. URL: https://fenix.tecnico.ulisboa.pt/downloadFile/3779579688470/lygeros.pdf.
48. Lee H.S.L., Althoff M., Hoelldampf S., Olbrich M., Barke E. Automated generation of hybrid system models for reachability analysis of nonlinear analog circuits. *Proc. of the 20th Asia and South Pacific Design Automation Conference* (*ASP-DAC-2015*). Chiba; Tokyo: IEEE, 2015. P. 725–730.
49. Скобелев В.В. Анализ структуры атрибутных транзиционных систем без скрытых переходов *Кибернетика и системный анализ*. 2017. Т. 53, № 2. С. 3–15.
50. Летичевский А.А. Алгебраическая теория взаимодействия и кибер-физические системы. *Проблемы управления и информатики*. 2017. № 5. С. 37–55.
51. Letichevsky A. Algebra of behavior transformations and its applications, in V.B. Kudryavtsev and I.G. Rosenberg eds. Structural theory of Automata, Semigroups, and Universal Algebra, NATO Science Series II. Mathematics, Physics and Chemistry. Dordrecht: Springer, 2005. Vol. 207. P. 241–272.
52. Летичевский А.А. Инсерционное моделирование. *Управляющие машины и системы*. 2012. № 6. P. 1–21.
53. Letichevsky A.A., Letychevskyi O.A., Peschanenko V.S., Weigert T. Insertion modeling and symbolic verification of large systems. *LNCS.* 2015. Vol. 9369. P. 3–18.
54. Летичевский А.А., Летичевский А.Ал., Песчаненко В.С., Губа А.А. Генерация трасс в системе инсерционного моделирования. *Кибернетика и системный анализ*. 2015. Т. 51, № 1. С. 7–19.
55. Recommendation Z.151, User Requirements Notation (URN). J.: International Telecommunication Union. 2008. 208 p.

Надійшла до редакції 10.07.2017

О.А. Летичевський, О.О. Летичевський, В.Г. Скобелєв, В.А. Волков
КІБЕР-ФІЗИЧНІ СИСТЕМИ

Анотація. Наведено ретроспективний аналіз теорії кібер-фізичних систем та характеристику її сучасного стану. Досліджено низку проблем, які виникають у теорії гібридних автоматів. Розглянуто напівгрупову систему переходів, яка є основою для розповсюдження алгебраїчної теорії взаємодії розмічених транзиційних систем на кібер-фізичні системи.

Ключові слова: кібер-фізичні системи, гібридні автомати, верифікація.

A.A. Letichevsky, O.O. Letychevskyi, V.G. Skobelev, V.A. Volkov
CYBER-PHYSICAL SYSTEMS

Abstract. The authors perform retrospective analysis of cyber-physical systems theory and its state of the art and investigate some problems inherent in hybrid automata theory. A semigroup transition system is presented, which underlies the propagation of algebraic interaction theory for cyber-physical systems.

Keywords: cyber-physical systems, hybrid automata, verification.

Летичевский Александр Адольфович,
академик НАН Украины, доктор физ.-мат. наук, профессор, заведующий отделом Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: aaletichevsky78@gmail.com.

Летичевский Александр Александрович,
доктор физ.-мат. наук, старший научный сотрудник Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: lit@issukraine.com.

Скобелев Владимир Геннадиевич,
доктор физ.-мат. наук, профессор, ведущий научный сотрудник Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: skobelevvg@gmail.com.

Волков Владислав Анатольевич,
кандидат физ.-мат. наук, старший научный сотрудник Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: vlad@issukraine.com.