Проектный институт
АвтоПромТермоОбработка

Опыт верификации автоматных программ на платформе Rodin (на примере задачи управления генератором эндогаза)

Максим Нейзов
(neyzov.max@gmail.com)

Презентация сделана на базе материалов статьи:

[1] Нейзов М. Формальный дедуктивный анализ автоматного алгоритма управления генератором эндогаза с помощью платформы Rodin. Часть 1. Определение требований надёжности и безопасности работы генератора эндогаза. Современная электроника. 2020. №9. с.62-63.

[2] Нейзов М. Формальный дедуктивный анализ автоматного алгоритма управления генератором эндогаза с помощью платформы Rodin. Часть 2. Алгоритм управления и платформа Rodin. Современная электроника. 2021. №1. с.44-46.

[3] Нейзов М. Формальный дедуктивный анализ автоматного алгоритма управления генератором эндогаза с помощью платформы Rodin. Часть 3. Построение формальной теории для алгоритма управления. Современная электроника. 2021. №2. с.40-43.

Идея дедуктивной верификации реактивных систем:

1. Формализовать поведение реактивной системы и её окружения с помощью аксиом;
2. Формализовать требуемые свойства системы в виде утверждений;
3. Доказать требуемые свойства как теоремы.

Теорема – гарантия выполнения требования

Причины перехода к дедуктивной верификации:

- Проектирование взрывоопасных промышленных объектов;
- Повышенные требования безопасности технологических процессов;
- Невозможность верификации бесконечных систем методом model checking;
- Верификация систем с параметрами (доказать корректность для произвольного n).

Используемые функции платформы Rodin:

- Задание/редактирование формальной модели поведения (логика предикатов первого порядка и теория множеств);
- Моделирование работы с целью валидации и тестирования;
- Проверка модели (model checking);
- Автоматизация доказательства теорем.

Платформа Rodin – инструмент для поддержки метода Event-B

Event-B – формальный метод моделирования и анализа систем

Компоненты Event-B

Контекст
(статика модели)

Машина
(динамика модели)

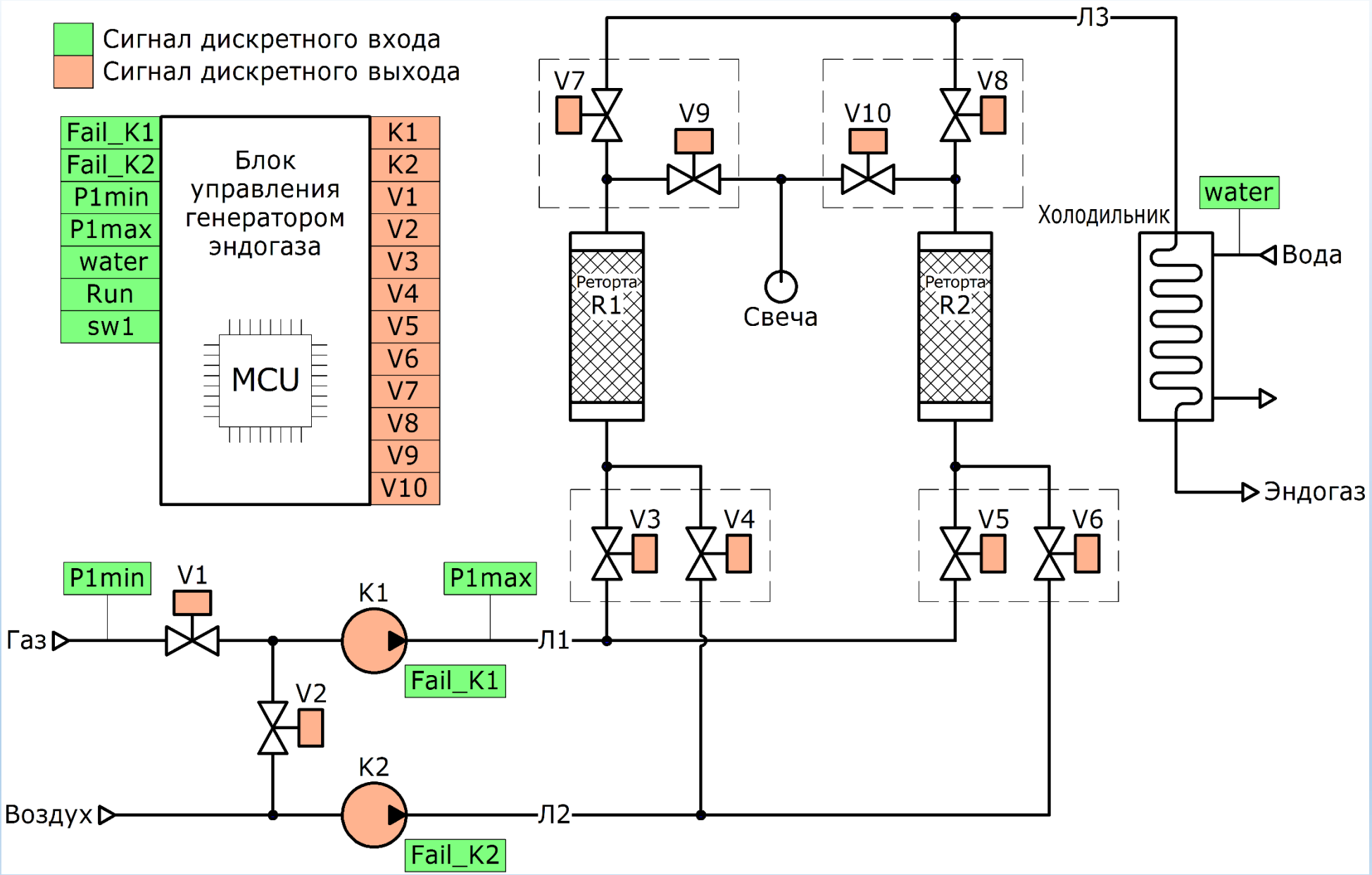
Машина содержит

Переменные
(хранят состояние машины)

События
(изменяют состояние машины)

Модель Event-B – дискретная система переходов

Схема генератора эндогаза



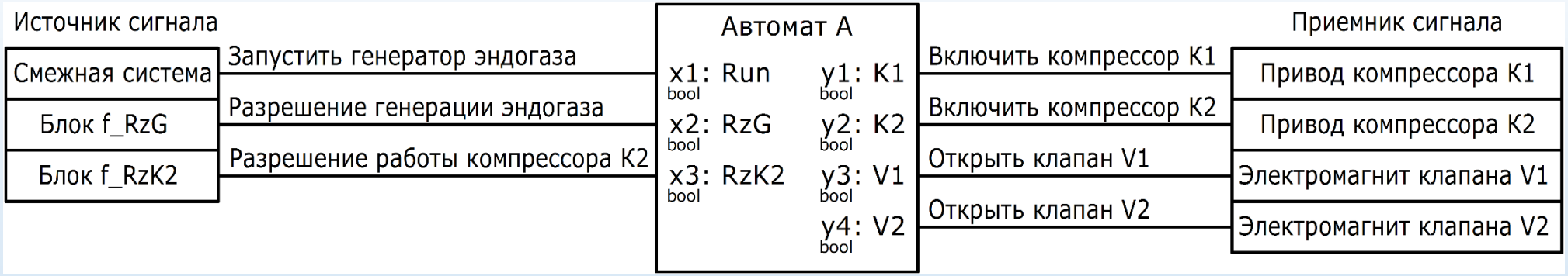
Требования безопасности

REQ1: Клапаны V1 и V2 никогда не открыты одновременно.
REQ2: Клапаны V3 и V4 никогда не открыты одновременно.
REQ3: Клапаны V5 и V6 никогда не открыты одновременно.
REQ4: Клапаны V7 и V9 никогда не открыты одновременно.
REQ5: Клапаны V8 и V10 никогда не открыты одновременно.
REQ6: Снятие сигнала Run закрывает все клапаны.
REQ7: Компрессор K1 работает только при наличии разрешения генерации эндогаза.
REQ8: Компрессор K2 работает только при наличии разрешения его работы.
REQ9: Воздушный компрессор K2 перекачивает только воздух.
REQ10: Компрессор K1 перекачивает или газ, или воздух, но не их вместе.
REQ11: Компрессоры K1 и K2 никогда не перекачивают одно и то же вещество.
REQ12: Снятие сигнала Run отключает компрессоры.
REQ13: Эндогаз не может подаваться в холодильник из двух реторт одновременно.
REQ14: В линии Л3 никогда нет воздуха.
REQ15: При подаче газа всегда открыт газовый тракт через реторту.
REQ16: Газ подаётся на две реторты и одна из них работает на холодильник тогда и только тогда, когда первая реторта находится в рабочем режиме, а вторая – в режиме продувки газом.

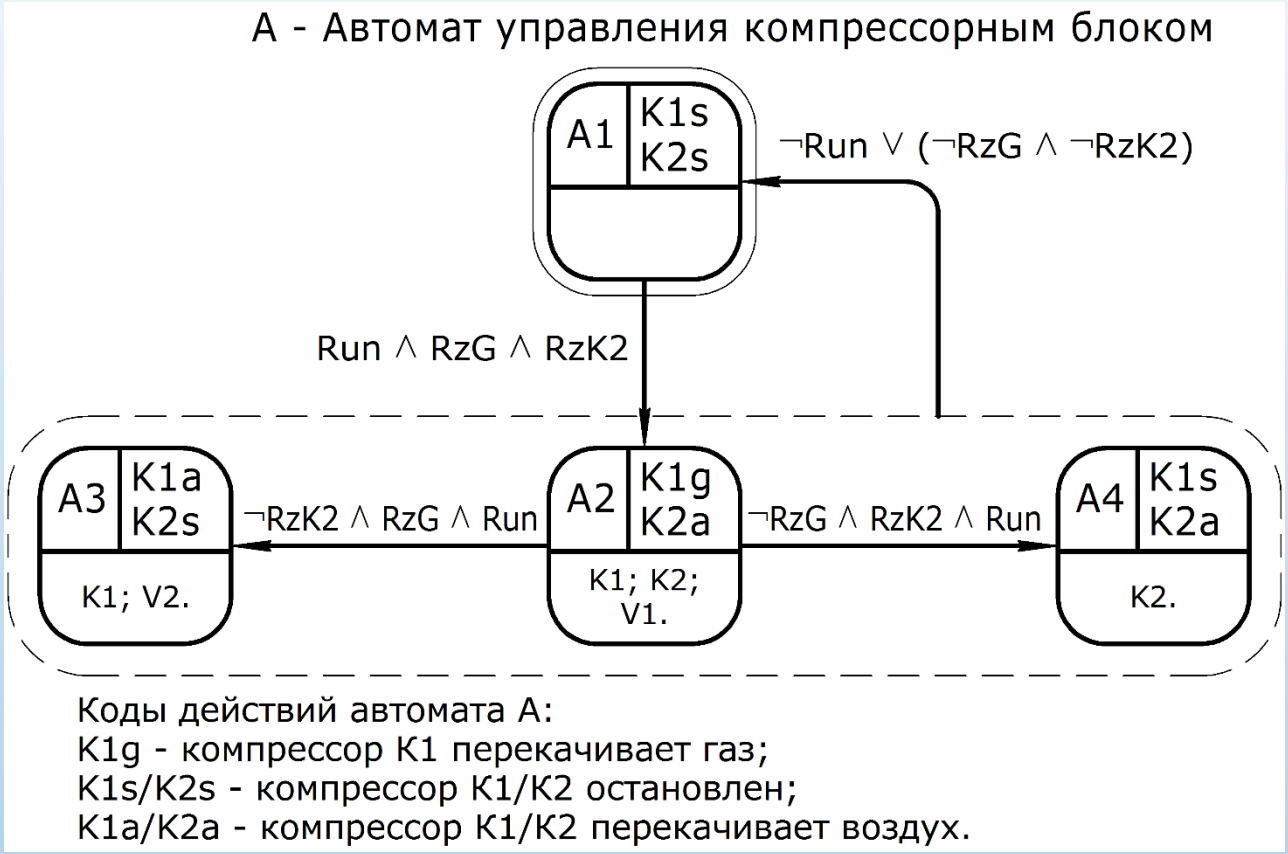
Формализация требований безопасности

T1: ¬ (V1=TRUE ∧ V2=TRUE)
T2: ¬ (V3=TRUE ∧ V4=TRUE)
T3: ¬ (V5=TRUE ∧ V6=TRUE)
T4: ¬ (V7=TRUE ∧ V9=TRUE)
T5: ¬ (V8=TRUE ∧ V10=TRUE)
T6: ∀v·(v∈Valve ∧ Run=FALSE) ⇒ closed(v)=TRUE
T7: K1=TRUE ⇒ RzG=TRUE
T8: K2=TRUE ⇒ RzK2=TRUE
T9: K2=TRUE ⇒ V2=FALSE
T10: K1=TRUE ⇒ ((V1=TRUE ∧ V2=FALSE) ∨ (V2=TRUE ∧ V1=FALSE))
T11: (K1=TRUE ∧ K2=TRUE) ⇒ V2=FALSE
T12: (Run=FALSE) ⇒ (K1=FALSE ∧ K2=FALSE)
T13: ¬ (V7=TRUE ∧ V8=TRUE)
T14: ¬ ((V7=TRUE ∧ V9=TRUE) ∨ (V7=TRUE ∧ V4=TRUE) ∨ (V7=TRUE ∧ V3=TRUE ∧ V2=TRUE))
T15: (K1=TRUE ∧ V1=TRUE) ⇒ ((V3=TRUE ∧ (V7=TRUE ∨ V9=TRUE)) ∨ (V5=TRUE ∧ (V8=TRUE ∨ V10=TRUE)))
T16: (V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE)) ⇔ (b=B6 ∨ b=B8)

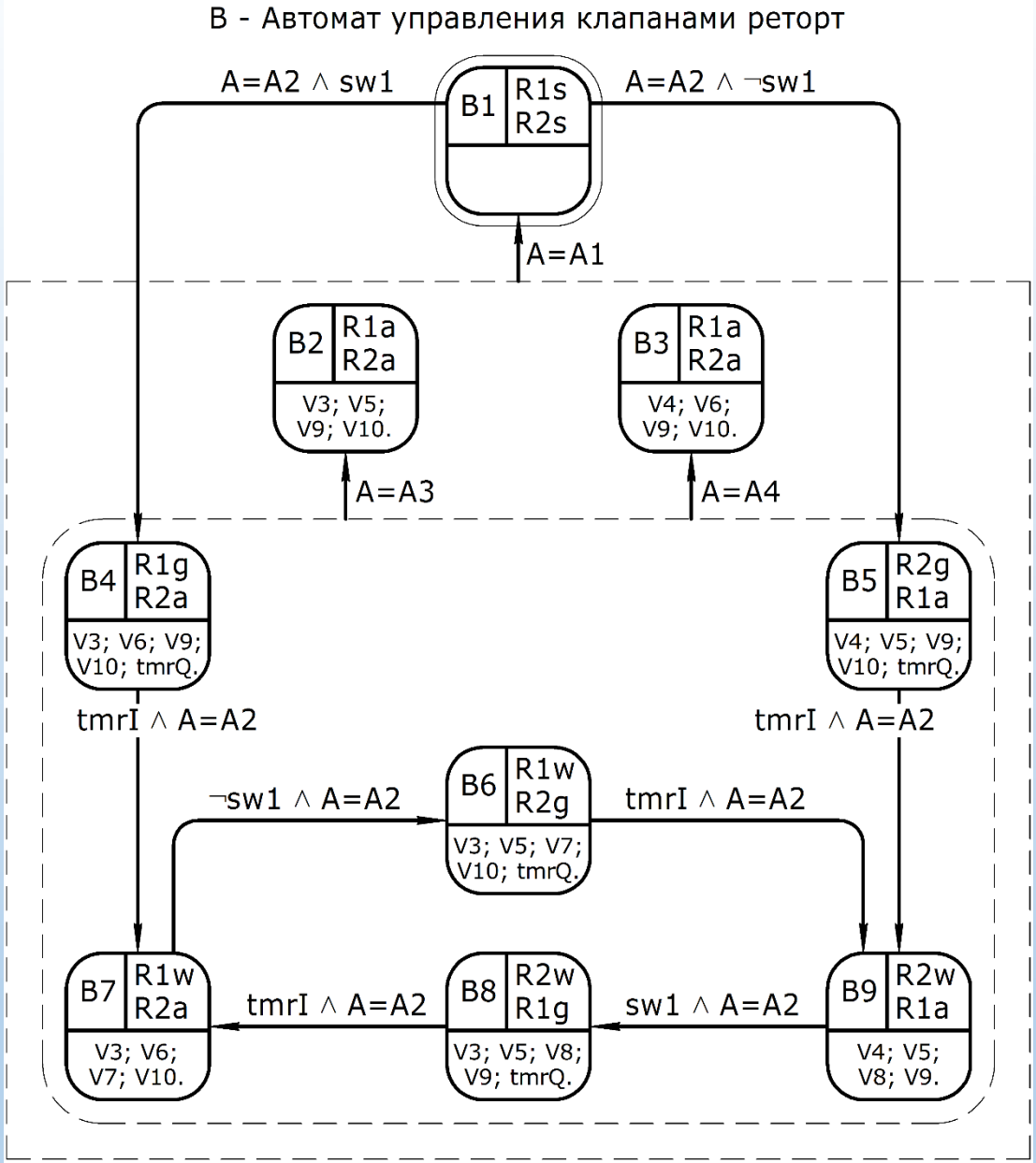
Алгоритм управления в виде системы автоматов S = A*B



Графы переходов автоматов A и B

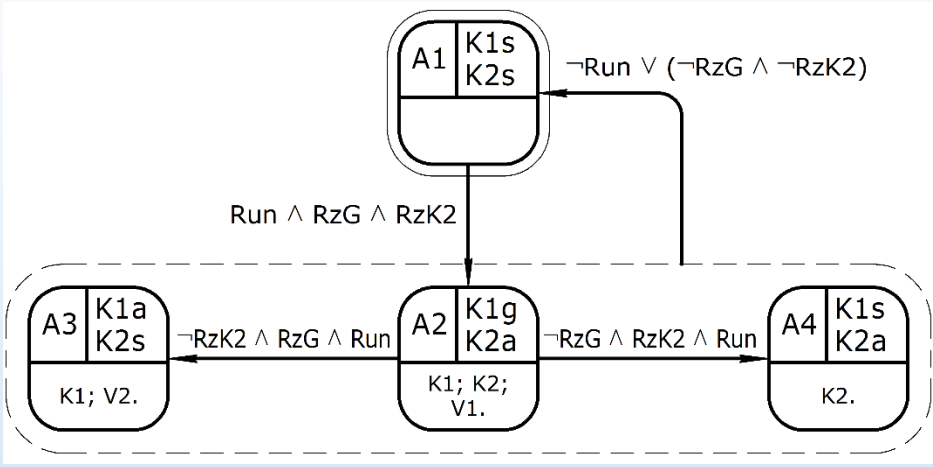


Коды действий автомата A:
K1g - компрессор K1 перекачивает газ;
K1s/K2s - компрессор K1/K2 остановлен;
K1a/K2a - компрессор K1/K2 перекачивает воздух.



Коды действий автомата B:
R1s/R2s - работа реторты R1/R2 остановлена (нет протока через реторту);
R1a/R2a - продувка реторты R1/R2 воздухом;
R1g/R2g - продувка реторты R1/R2 газом;
R1w/R2w - работа реторты R1/R2 (генерация эндогаза).

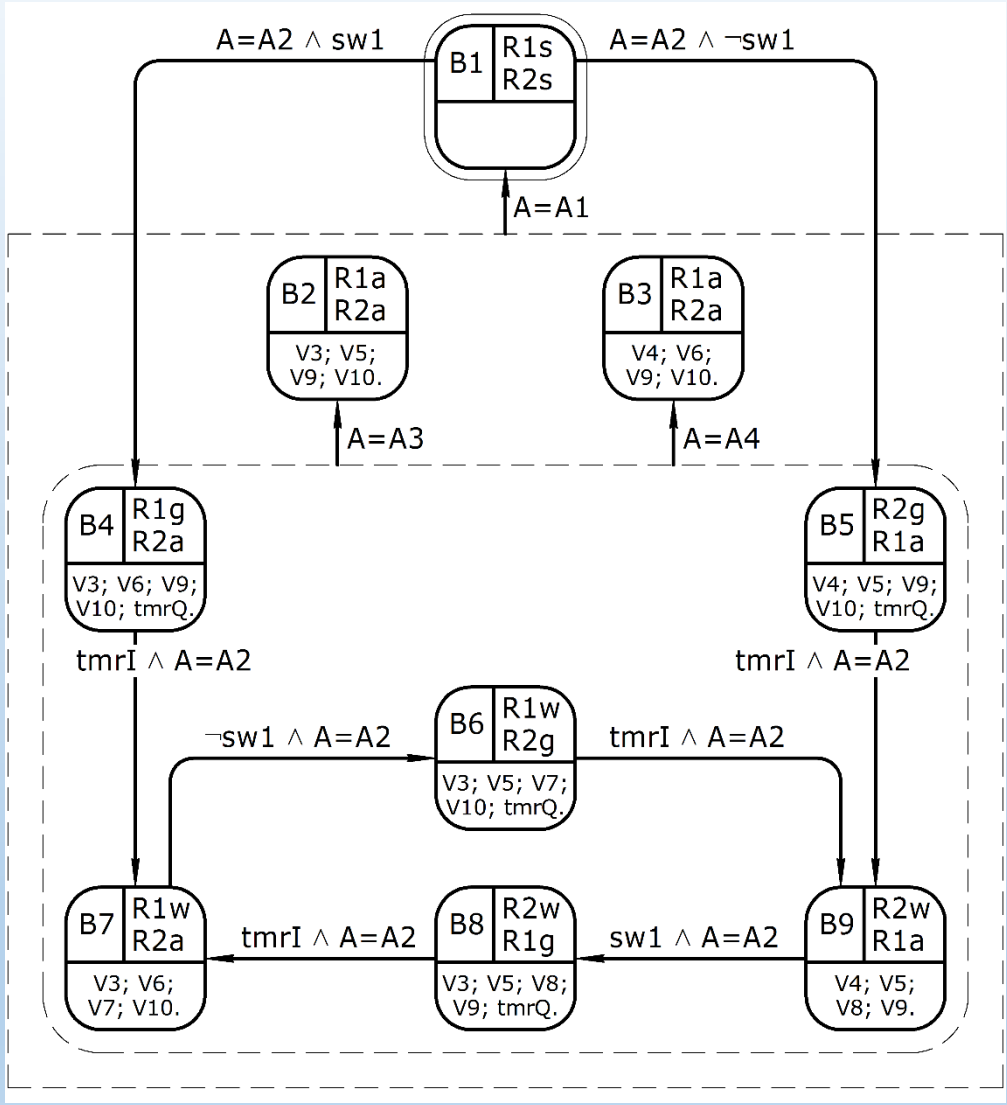
Аксиоматика автомата A



axm1: partition(A, {A1},{A2},{A3},{A4})
axm2: InA = (BOOL × BOOL × BOOL)
axm3: a_1_2 = {x1 ↦ x2 ↦ x3 | x1=TRUE ∧ x2=TRUE ∧ x3=TRUE}
axm4: a_2_3 = {x1 ↦ x2 ↦ x3 | x1=TRUE ∧ x2=TRUE ∧ x3=FALSE}
axm5: a_2_4 = {x1 ↦ x2 ↦ x3 | x1=TRUE ∧ x2=FALSE ∧ x3=TRUE}
axm6: a_234_1 = {x1 ↦ x2 ↦ x3 | (x1=FALSE ∧ x2∈BOOL ∧ x3∈BOOL)
∨ (x1∈BOOL ∧ x2=FALSE ∧ x3=FALSE)}
axm7: a_1_1 = InA\(a_1_2)
axm8: a_2_2 = InA\(a_2_3 ∪ a_2_4 ∪ a_234_1)
axm9: a_3_3 = InA\(a_234_1)
axm10: a_4_4 = InA\(a_234_1)
axm11: dta ∈ (A × InA) → A
axm12: ∀s,i·((s=A1 ∧ i∈a_1_1) ∨ (s∈{A2,A3,A4} ∧ i∈a_234_1)) ⇔ dta(s ↦ i) = A1
axm13: ∀s,i·((s=A1 ∧ i∈a_1_2) ∨ (s=A2 ∧ i∈a_2_2)) ⇔ dta(s ↦ i) = A2
axm14: ∀s,i·((s=A2 ∧ i∈a_2_3) ∨ (s=A3 ∧ i∈a_3_3)) ⇔ dta(s ↦ i) = A3
axm15: ∀s,i·((s=A2 ∧ i∈a_2_4) ∨ (s=A4 ∧ i∈a_4_4)) ⇔ dta(s ↦ i) = A4
axm16: LA_y1 ∈ A → BOOL
axm17: LA_y2 ∈ A → BOOL
axm18: LA_y3 ∈ A → BOOL
axm19: LA_y4 ∈ A → BOOL
axm20: ∀s·(s=A2 ∨ s=A3) ⇔ LA_y1(s) = TRUE
axm21: ∀s·(s=A2 ∨ s=A4) ⇔ LA_y2(s) = TRUE
axm22: ∀s·(s=A2) ⇔ LA_y3(s) = TRUE
axm23: ∀s·(s=A3) ⇔ LA_y4(s) = TRUE

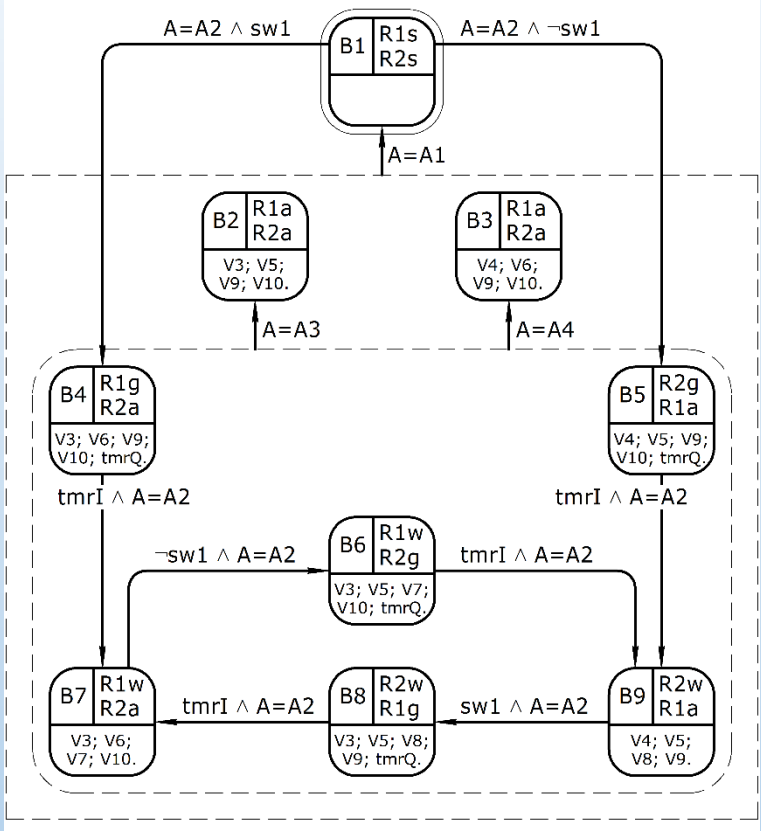
Аксиоматика автомата B

axm24: partition(B, {B1},{B2},{B3},{B4},{B5},{B6},{B7},{B8},{B9})
axm25: InB = (A × BOOL × BOOL)
axm26: b_1_4 = {x1 ↦ x2 ↦ x3 | x1=A2 ∧ x2=TRUE ∧ x3∈BOOL}
axm27: b_9_8 = b_1_4
axm28: b_1_5 = {x1 ↦ x2 ↦ x3 | x1=A2 ∧ x2=FALSE ∧ x3∈BOOL}
axm29: b_7_6 = b_1_5
axm30: b_4_7 = {x1 ↦ x2 ↦ x3 | x1=A2 ∧ x2∈BOOL ∧ x3=TRUE}
axm31: b_5_9 = b_4_7
axm32: b_6_9 = b_4_7
axm33: b_8_7 = b_4_7
axm34: b_x_1 = {x1 ↦ x2 ↦ x3 | x1=A1 ∧ x2∈BOOL ∧ x3∈BOOL}
axm35: b_x_2 = {x1 ↦ x2 ↦ x3 | x1=A3 ∧ x2∈BOOL ∧ x3∈BOOL}
axm36: b_x_3 = {x1 ↦ x2 ↦ x3 | x1=A4 ∧ x2∈BOOL ∧ x3∈BOOL}
axm37: b_1_1 = InB\(b_1_4 ∪ b_1_5)
axm38: b_2_2 = InB\(b_x_1)
axm39: b_3_3 = InB\(b_x_1)
axm40: b_4_4 = InB\(b_x_1 ∪ b_x_2 ∪ b_x_3 ∪ b_4_7)
axm41: b_5_5 = InB\(b_x_1 ∪ b_x_2 ∪ b_x_3 ∪ b_5_9)
axm42: b_6_6 = InB\(b_x_1 ∪ b_x_2 ∪ b_x_3 ∪ b_6_9)
axm43: b_7_7 = InB\(b_x_1 ∪ b_x_2 ∪ b_x_3 ∪ b_7_6)
axm44: b_8_8 = InB\(b_x_1 ∪ b_x_2 ∪ b_x_3 ∪ b_8_7)
axm45: b_9_9 = InB\(b_x_1 ∪ b_x_2 ∪ b_x_3 ∪ b_9_8)
axm46: dtb ∈ (B × InB) → B
axm47: ∀s,i·((s=B1 ∧ i∈b_1_1) ∨ (s∈B\{B1} ∧ i∈b_x_1)) ⇔ dtb(s ↦ i) = B1



Аксиоматика автомата B (продолжение)

axm48: ∀s,i·((s=B2 ∧ i∈b_2_2) ∨ (s∈B\{B1,B2,B3} ∧ i∈b_x_2)) ⇔
dtb(s ↦ i) = B2
axm49: ∀s,i·((s=B3 ∧ i∈b_3_3) ∨ (s∈B\{B1,B2,B3} ∧ i∈b_x_3)) ⇔
dtb(s ↦ i) = B3
axm50: ∀s,i·((s=B4 ∧ i∈b_4_4) ∨ (s=B1 ∧ i∈b_1_4)) ⇔ dtb(s ↦ i) = B4
axm51: ∀s,i·((s=B5 ∧ i∈b_5_5) ∨ (s=B1 ∧ i∈b_1_5)) ⇔ dtb(s ↦ i) = B5
axm52: ∀s,i·((s=B6 ∧ i∈b_6_6) ∨ (s=B7 ∧ i∈b_7_6)) ⇔ dtb(s ↦ i) = B6
axm53: ∀s,i·((s=B7 ∧ i∈b_7_7) ∨ (s=B4 ∧ i∈b_4_7) ∨ (s=B8 ∧ i∈b_8_7))
⇔ dtb(s ↦ i) = B7
axm54: ∀s,i·((s=B8 ∧ i∈b_8_8) ∨ (s=B9 ∧ i∈b_9_8)) ⇔ dtb(s ↦ i) = B8
axm55: ∀s,i·((s=B9 ∧ i∈b_9_9) ∨ (s=B5 ∧ i∈b_5_9) ∨ (s=B6 ∧ i∈b_6_9))
⇔ dtb(s ↦ i) = B9
axm56: LB_y1 ∈ B → BOOL
...
axm64: LB_y9 ∈ B → BOOL
axm65: ∀s·s∈{B2,B4,B6,B7,B8} ⇔ LB_y1(s) = TRUE
axm66: ∀s·s∈{B3,B5,B9} ⇔ LB_y2(s) = TRUE
axm67: ∀s·s∈{B2,B5,B6,B8,B9} ⇔ LB_y3(s) = TRUE
axm68: ∀s·s∈{B3,B4,B7} ⇔ LB_y4(s) = TRUE
axm69: ∀s·s∈{B6,B7} ⇔ LB_y5(s) = TRUE
axm70: ∀s·s∈{B8,B9} ⇔ LB_y6(s) = TRUE
axm71: ∀s·s∈{B2,B3,B4,B5,B8,B9} ⇔ LB_y7(s) = TRUE
axm72: ∀s·s∈{B2,B3,B4,B5,B6,B7} ⇔ LB_y8(s) = TRUE
axm73: ∀s·s∈{B4,B5,B6,B8} ⇔ LB_y9(s) = TRUE



Динамическая модель алгоритма и окружения: переменные машины

```
VARIABLES
 a      // Текущее состояние автомата A
 b      // Текущее состояние автомата B
 Run    // Запуск работы (внешний сигнал)
 RzG    // Разрешение генерации (внешний сигнал)
 RzK2   // Разрешение работы K2 (внешний сигнал)
 sw1    // Переключить на реторту 1 (внешний сигнал)
 tmrI   // Время продувки реторты вышло
 K1     // Включить компрессор K1
 K2     // Включить компрессор K2
 V1     // Открыть клапан V1
 V2     // Открыть клапан V2
 V3     // Открыть клапан V3
 V4     // Открыть клапан V4
 V5     // Открыть клапан V5
 V6     // Открыть клапан V6
 V7     // Открыть клапан V7
 V8     // Открыть клапан V8
 V9     // Открыть клапан V9
 V10    // Открыть клапан V10
 tmrQ   // Запустить таймер продувки реторты
```

Динамическая модель алгоритма и окружения: событие инициализации машины

```
INITIALISATION
 a := A1
 b := B1
 Run := FALSE
 RzG := FALSE
 RzK2 := FALSE
 sw1 := FALSE
 tmrI := FALSE
 K1 := FALSE
 K2 := FALSE
 V1 := FALSE
 V2 := FALSE
 V3 := FALSE
 V4 := FALSE
 V5 := FALSE
 V6 := FALSE
 V7 := FALSE
 V8 := FALSE
 V9 := FALSE
 V10 := FALSE
 tmrQ := FALSE
```

Динамическая модель алгоритма и окружения: итерация работы машины

```
iter
ANY
  x1
  x2
  x3
  x4
  x5
WHERE
  grd1: x1 ∈ BOOL
  grd2: x2 ∈ BOOL
  grd3: x3 ∈ BOOL
  grd4: x4 ∈ BOOL
  grd5: x5 ∈ BOOL
  grd6: (a = A3) ⇒ (x2 = TRUE ∧ x3 = FALSE)
  grd7: (a = A4) ⇒ (x2 = FALSE ∧ x3 = TRUE)
THEN
  act1: a ≔ dta(a ↦ (x1 ↦ x2 ↦ x3))
  act2: K1 ≔ LA_y1(dta(a ↦ (x1 ↦ x2 ↦ x3)))
  act3: K2 ≔ LA_y2(dta(a ↦ (x1 ↦ x2 ↦ x3)))
  act4: V1 ≔ LA_y3(dta(a ↦ (x1 ↦ x2 ↦ x3)))
  act5: V2 ≔ LA_y4(dta(a ↦ (x1 ↦ x2 ↦ x3)))
  ...
```

Динамическая модель алгоритма и окружения: итерация работы машины - продолжение

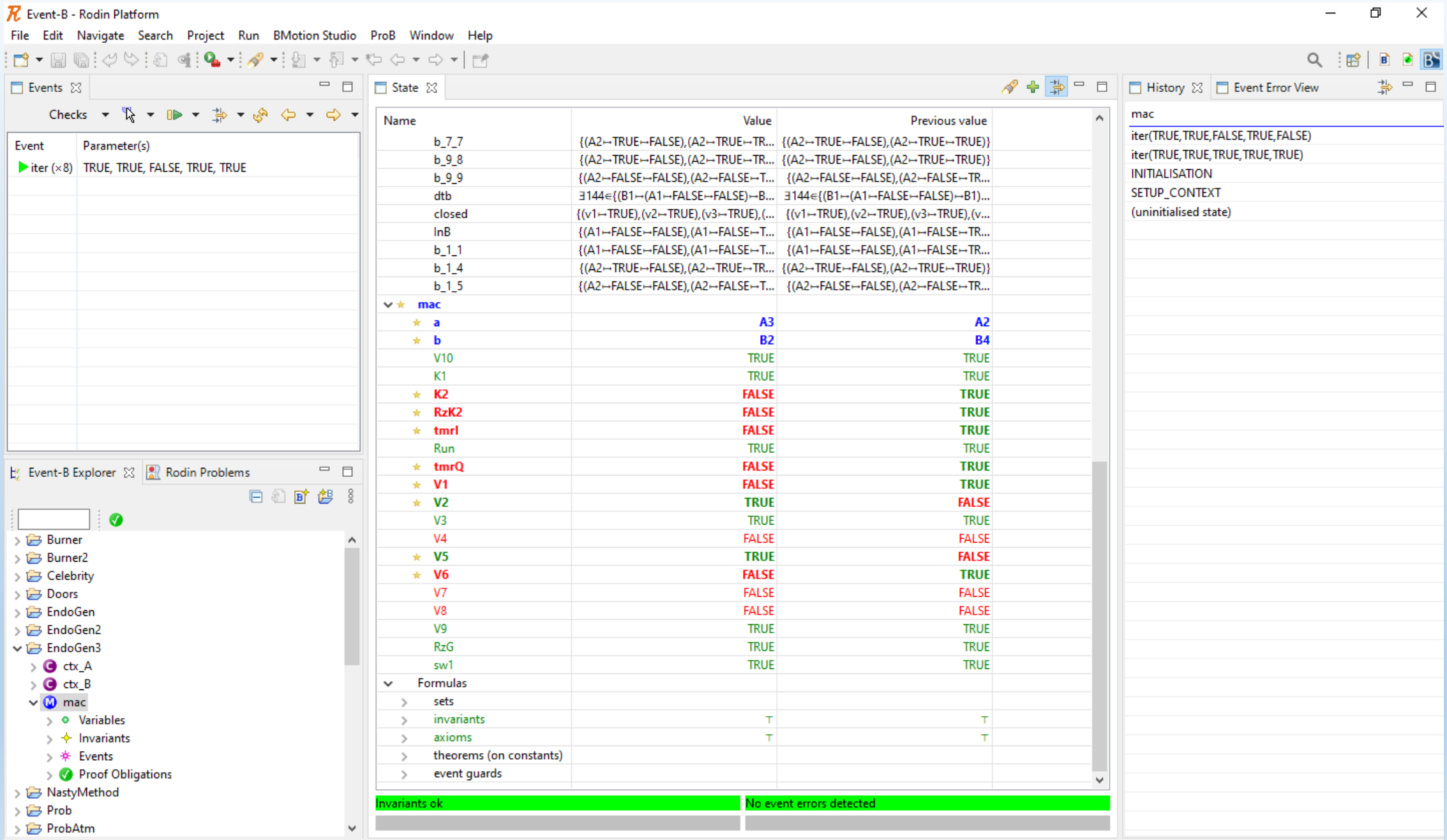
```
...
  act6: b ≔ dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))
  act7: V3 ≔ LB_y1(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act8: V4 ≔ LB_y2(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act9: V5 ≔ LB_y3(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act10: V6 ≔ LB_y4(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act11: V7 ≔ LB_y5(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act12: V8 ≔ LB_y6(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act13: V9 ≔ LB_y7(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act14: V10 ≔ LB_y8(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act15: tmrQ ≔ LB_y9(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))
  act16: Run ≔ x1
  act17: RzG ≔ x2
  act18: RzK2 ≔ x3
  act19: sw1 ≔ x4
  act20: tmrI ≔ x5
END
```

Процедуры верификации:

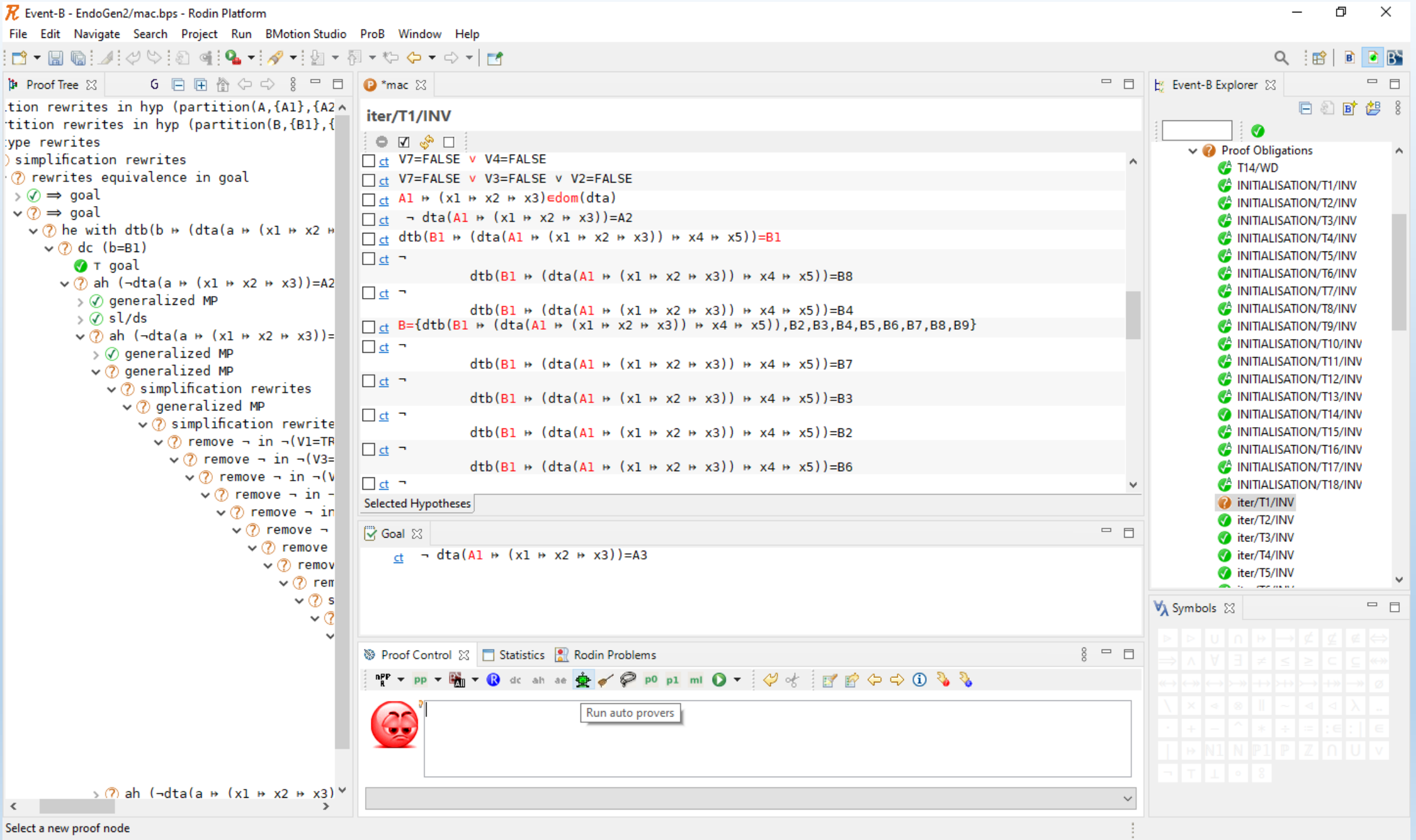
1. Моделирование работы машины (тестирование по сценарию);
2. Проверка модели (model checking);
3. Доказательство теорем.

Совместное использование!

Моделирование работы машины и model checking (плагин ProB)



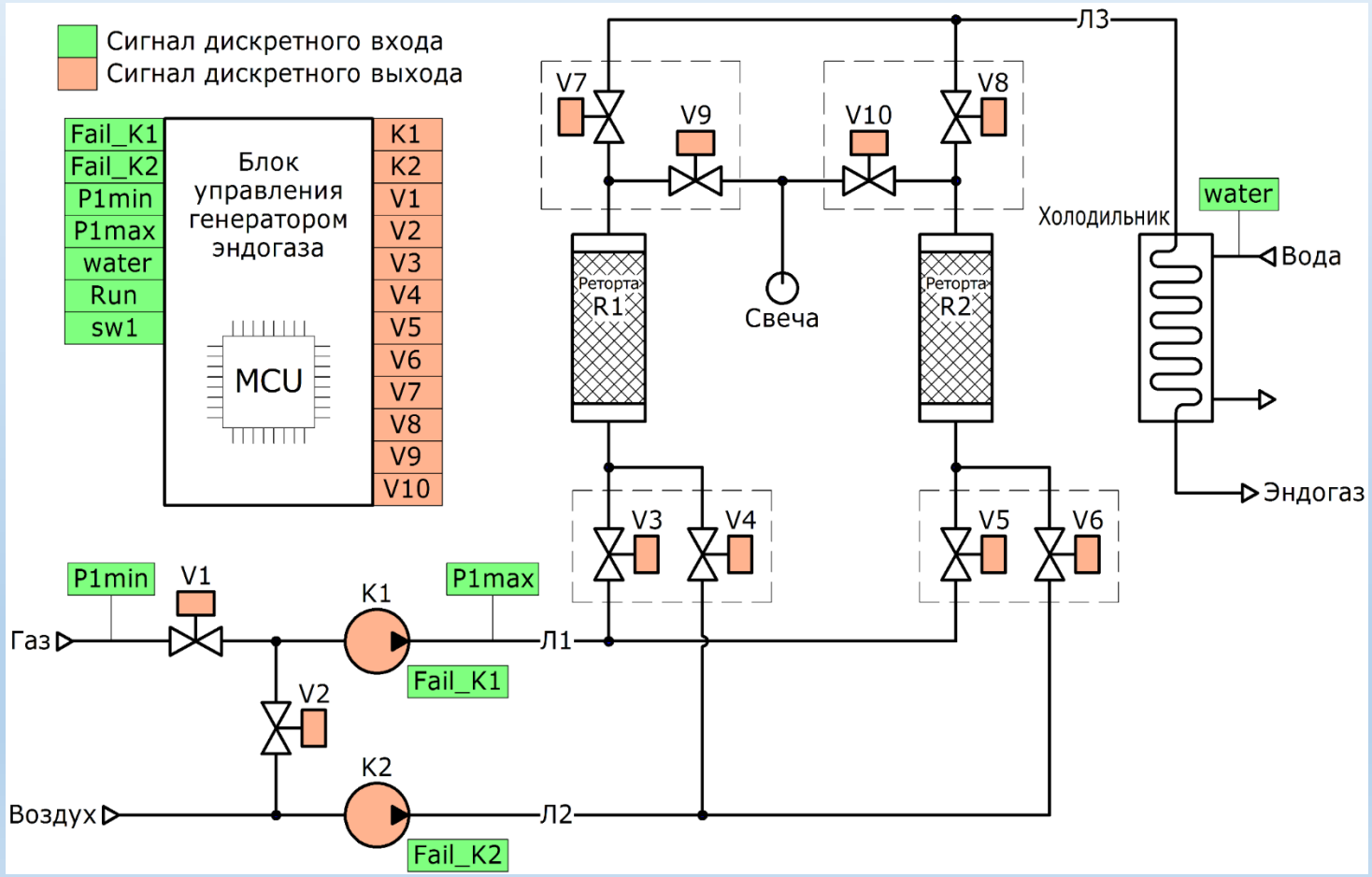
Интерактивное доказательство теорем

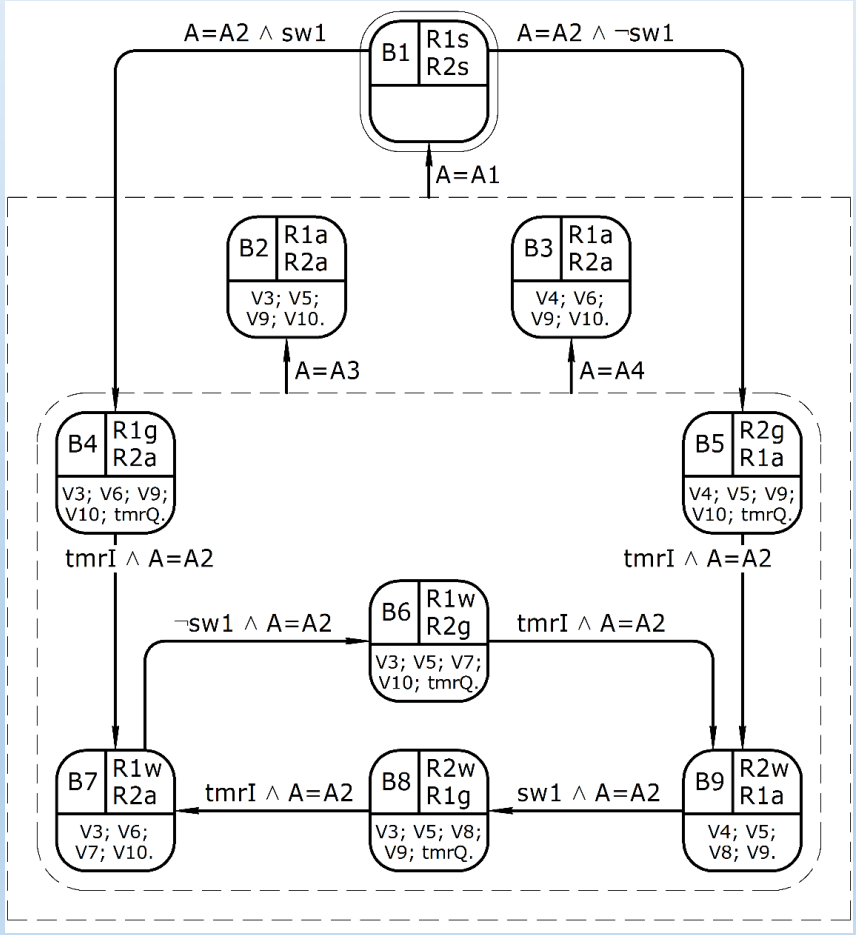


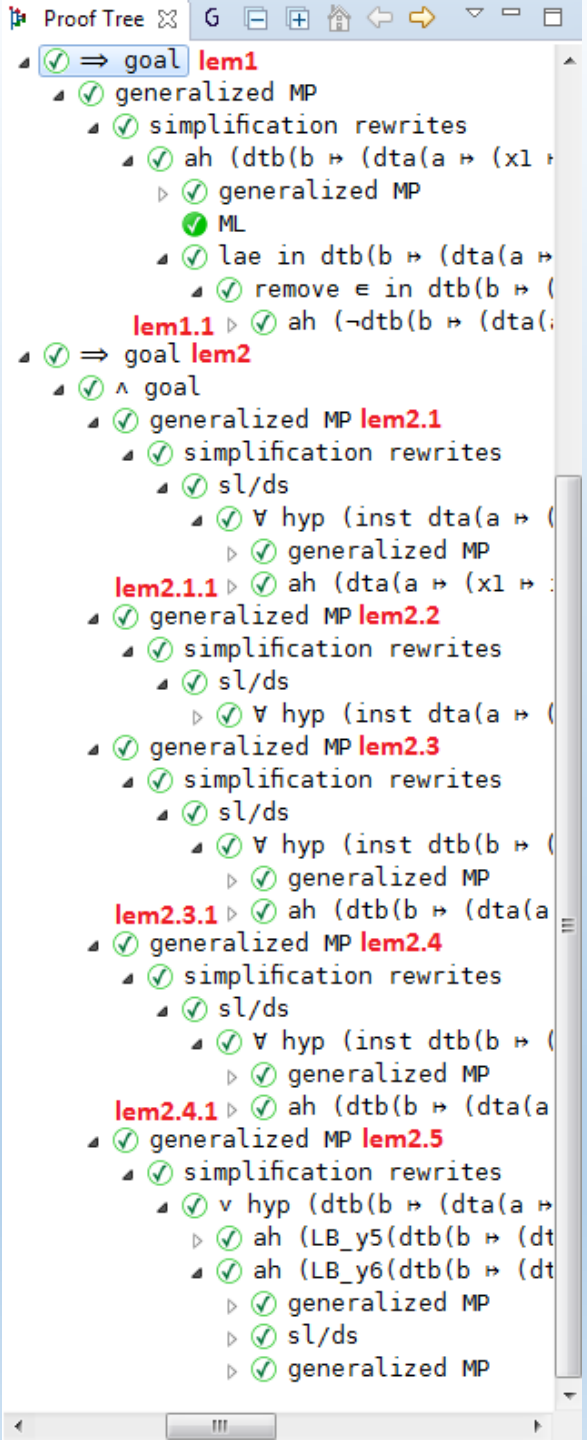
Доказательство выполнения требования REQ16

REQ16: Газ подаётся на две реторты и одна из них работает на холодильник тогда и только тогда, когда первая реторта находится в рабочем режиме, а вторая – в режиме продувки газом.

T16: (V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE)) ⇔ (b=B6 ∨ b=B8)







Основные леммы теоремы T16

T16 = (lem1 ∧ lem2)

Лемма	Утверждение
lem1	LA_y3(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE ∧ LA_y1(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE ∧ LB_y1(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∧ LB_y3(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∧ (LB_y5(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∨ LB_y6(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE) ⇒ (dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))=B6 ∨ dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))=B8) Интерпретация: V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE) ⇒ (b=B6 ∨ b=B8)
lem1.1	¬dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))∈{B1,B2,B3,B4,B5,B7,B9}
lem2	(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))=B6 ∨ dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))=B8) ⇒ LA_y3(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE ∧ LA_y1(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE ∧ LB_y1(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∧ LB_y3(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∧ (LB_y5(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∨ LB_y6(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE) Интерпретация: (b=B6 ∨ b=B8) ⇒ V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE)

Основные леммы теоремы T16 (продолжение)

Лемма	Утверждение
lem2	(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))=B6 ∨ dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))=B8) ⇒ LA_y3(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE ∧ LA_y1(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE ∧ LB_y1(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∧ LB_y3(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∧ (LB_y5(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∨ LB_y6(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE) Интерпретация: (b=B6 ∨ b=B8) ⇒ V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE)
lem2.1	LA_y3(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE Интерпретация: V1=TRUE
lem2.2	LA_y1(dta(a ↦ (x1 ↦ x2 ↦ x3)))=TRUE Интерпретация: K1=TRUE
lem2.3	LB_y1(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE Интерпретация: V3=TRUE
lem2.3.1	dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))∈{B2,B4,B6,B7,B8}
lem2.4	LB_y3(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE Интерпретация: V5=TRUE
lem2.4.1	dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))∈{B2,B5,B6,B8,B9}
lem2.5	(LB_y5(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE ∨ LB_y6(dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5)))=TRUE) Интерпретация: (V7=TRUE ∨ V8=TRUE)

Доказательство леммы lem1

lem1: V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE) ⇒ (b=B6 ∨ b=B8)

Теорема дедукции: если (Hyp,x) ⊢ y, то Hyp ⊢ (x ⇒ y).

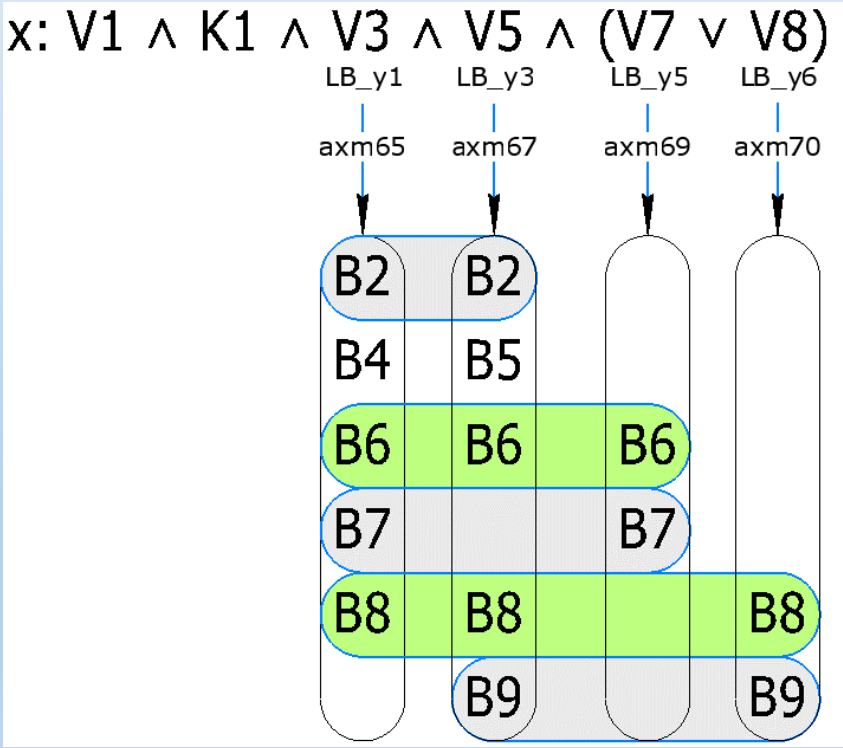
Hyp, (V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE)) ⊢ (b=B6 ∨ b=B8)
x y

lem1.1: ¬dtb(b ↦ (dta(a ↦ (x1 ↦ x2 ↦ x3)) ↦ x4 ↦ x5))∈{B1,B2,B3,B4,B5,B7,B9}

lem1.1 ⊢ (b=B6 ∨ b=B8)

¬dtb(…)=B1,
¬dtb(…)=B2,
¬dtb(…)=B3,
¬dtb(…)=B4,
¬dtb(…)=B5,
¬dtb(…)=B7,
¬dtb(…)=B9
⊢ lem1.1

Метод от противного:
Пусть dtb(…)=B2, тогда ¬x.
Противоречие.
Следовательно ¬dtb(…)=B2.



Доказательство леммы lem2

lem2: (b=B6 ∨ b=B8) ⇒ V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE)

Теорема дедукции: если (Hyp,x) ⊢ y, то Hyp ⊢ (x ⇒ y).

x y

Hyp, (b=B6 ∨ b=B8) ⊢ V1=TRUE ∧ K1=TRUE ∧ V3=TRUE ∧ V5=TRUE ∧ (V7=TRUE ∨ V8=TRUE)

lem2.1: V1=TRUE
lem2.2: K1=TRUE
lem2.3: V3=TRUE
lem2.4: V5=TRUE
lem2.5: V7=TRUE ∨ V8=TRUE

⊢ y

dta(…)=A2 ⊢ lem2.1, lem2.2

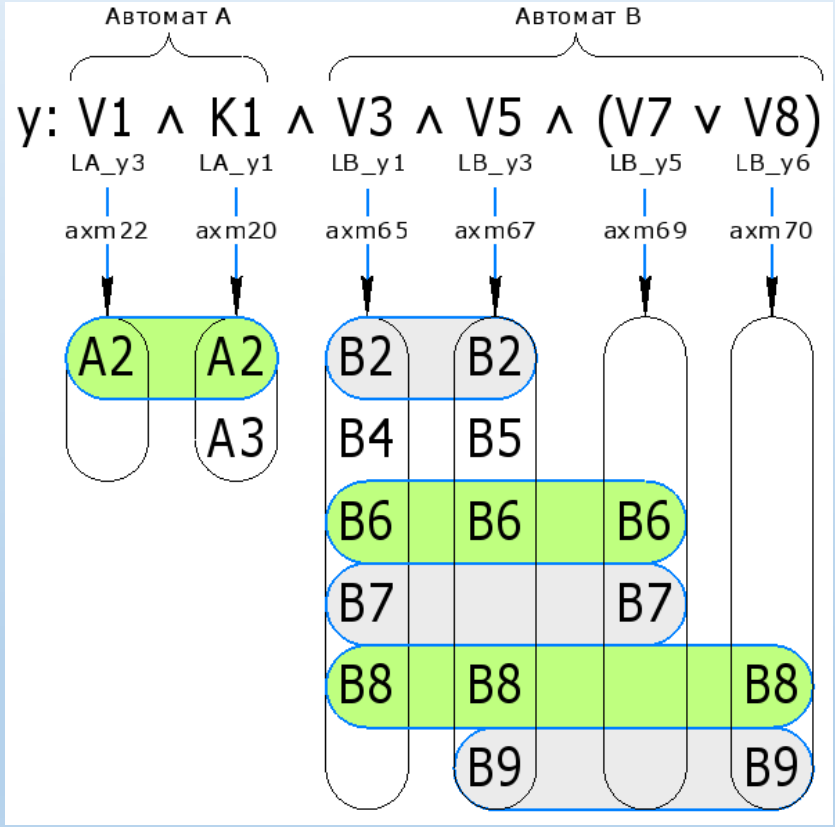
Метод от противного:

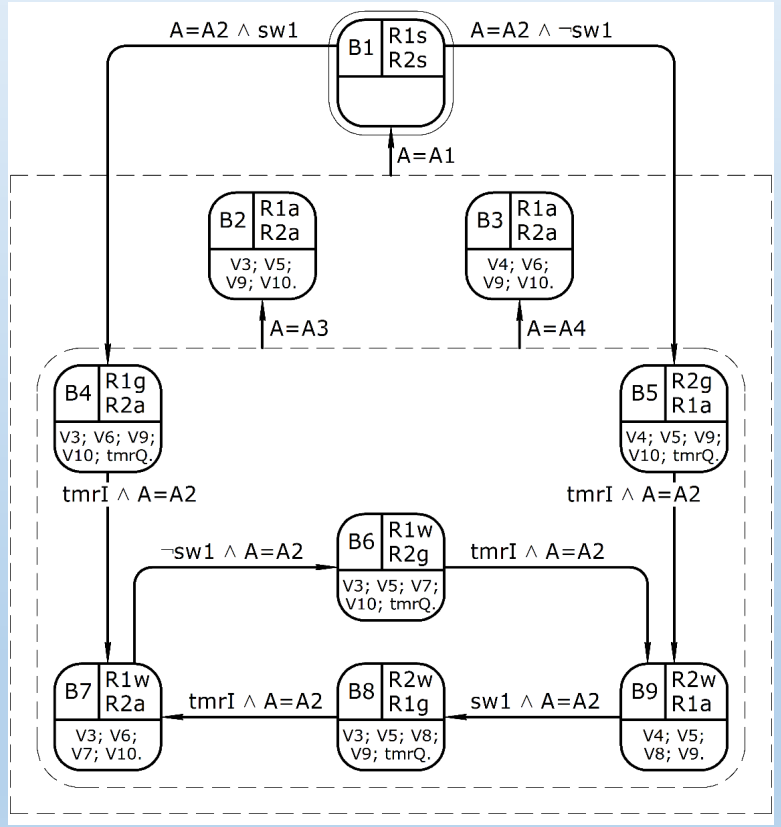
¬dta(…)=A2 ⊢ ¬x

¬x = ¬(b=B6) ∧ ¬(b=B8)

dta(…)=A1 ⊢ dtb(…)=B1
dta(…)=A3 ⊢ dtb(…)=B2(B1,B3)
dta(…)=A4 ⊢ dtb(…)=B3(B1,B2)

⊢ ¬x





x ⊢ lem2.3, lem2.4, lem2.5

Плюсы использования Rodin:

- Строгая спецификация поведения проектируемой системы;
- Моделирование работы системы;
- Проверка модели (model checking);
- Автоматизация доказательства теорем.

Минусы использования Rodin:

- Высокая трудоемкость доказательства сложных теорем.

Будущие задачи:

- Исследование различных аксиоматик (для упрощения доказательств);
- Доказательство свойств живости (liveness properties);
- Верификация систем с параметрами;
- Последовательная разработка больших систем методом Event-B (через уточнение - refines);
- Использование автоматической кодогенерации.

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ.

Целесообразность использования дедуктивной верификации для конечных систем (i > c)