И.Б.Бурдонов, А.С.Косачев.
Эквивалентные семантики взаимодействия.
Труды Института системного программирования РАН, N 14.1, 2008, стр.55-72.
18 стр.

Бурдонов И.Б., Косачев А.С.

Эквивалентные семантики взаимодействия

Введение

Тестирование существенно зависит от имеющегося набора тестовых возможностей по управлению и наблюдению за поведением тестируемой системы. Эти тестовые возможности формализуются в виде семантики взаимодействия. Поэтому представляет интерес сравнение различных семантик по мощности тестирования. В данной статье исследуется вопрос о том, когда одна семантика «не сильнее», чем другая семантика, и когда семантики эквивалентны по мощности тестирования. Мы используем определения семантики взаимодействия, безопасности и конформности, которые даны в первом разделе нашей статьи «Системы с приоритетами: конформность, тестирование, композиция» (см. данный сборник). Эти определения можно также найти в [1,3]. Повторим здесь кратко основные определения.

Говорят, что задана $\mathfrak{R}/\mathfrak{Q}$-семантика, если задан алфавит внешних действий L и два семейства его подмножеств: семейство кнопок $\mathfrak{R}\subseteq\mathcal{P}(L)$, которым соответствуют наблюдаемые отказы, и семейство кнопок $\mathfrak{Q}\subseteq\mathcal{P}(L)$, которым соответствуют ненаблюдаемые отказы. Предполагается, что $\mathfrak{R}\cap\mathfrak{Q}=\varnothing$ и $\cup\mathfrak{R}\cup\cup\mathfrak{Q}=L$. Внутреннее действие обозначается символом τ, дивергенция (бесконечная последовательность τ-действий) – символом Δ, разрушение – символом γ. $\mathfrak{R}$-трасса – последовательность внешних действий и $\mathfrak{R}$-отказов, быть может, завершающаяся дивергенцией или разрушением. $\boldsymbol{F}$-трасса – $\mathfrak{R}$-трасса для $\mathfrak{R}=\mathcal{P}(L)$. Примеры таких семантик можно найти в [3-6].

LTS – это совокупность $\mathbf{S}=\mathrm{LTS}(V_S,L,E_S,s_0)$, где V_S – непустое множество состояний, L – алфавит внешних действий, $E_S\subseteq V_S\times(L\cup\{\tau,\gamma\})\times V_S$ – множество переходов, $s_0\in V_S$ – начальное состояние. Множество $\boldsymbol{F}$-трасс LTS $\mathbf{S}$ обозначается $\boldsymbol{F}(\mathbf{S})$. Множество состояний, достижимых из состояния s по трассе σ обозначается s ***after*** σ; $\mathbf{S}$ ***after*** σ $=_{\text{def}}$ s_0 ***after*** σ.

Отношение безопасности кнопки после $\mathfrak{R}$-трассы в реализации:

P ***safe in*** $\mathbf{I}$ ***after*** σ

$=_{\text{def}}\ \sigma\cdot\langle\Delta\rangle\notin\boldsymbol{F}(\mathbf{I})\ \&\ \forall u{\in}P\ \sigma\cdot\langle u,\gamma\rangle\notin\boldsymbol{F}(\mathbf{I})\ \&\ (P{\in}\mathfrak{R}\ \vee\ \sigma\cdot\langle P\rangle\notin\boldsymbol{F}(\mathbf{I}))$.

Безопасность кнопки после $\mathfrak{R}$-трассы в спецификации – отношение ***safe by***, удовлетворяющее следующим трём требованиям:

1) R ***safe by*** $\mathbf{S}$ ***after*** $\sigma\ \Leftrightarrow\ \sigma\cdot\langle\Delta\rangle\notin\boldsymbol{F}(\mathbf{S})\ \&\ \forall u{\in}R\ \sigma\cdot\langle u,\gamma\rangle\notin\boldsymbol{F}(\mathbf{S})$,

2) $\sigma\cdot\langle z\rangle\in\boldsymbol{F}(\mathbf{S})\ \&\ \sigma\cdot\langle\Delta\rangle\notin\boldsymbol{F}(\mathbf{S})\ \&\ \exists T{\in}\mathfrak{R}\cup\mathfrak{Q}\ z{\in}T\ \&\ \forall u{\in}T\ \sigma\cdot\langle u,\gamma\rangle\notin\boldsymbol{F}(\mathbf{S})$
$\Rightarrow\ \exists P{\in}\mathfrak{R}\cup\mathfrak{Q}\ z{\in}P\ \&\ P$ ***safe by*** $\mathbf{S}$ ***after*** σ,

3) Q ***safe by*** $\mathbf{S}$ ***after*** σ
$\Rightarrow\ \sigma\cdot\langle\Delta\rangle\notin\boldsymbol{F}(\mathbf{S})\ \&\ \forall u{\in}Q\ \sigma\cdot\langle u,\gamma\rangle\notin\boldsymbol{F}(\mathbf{S})\ \&\ \exists v{\in}Q\ \sigma\cdot\langle v\rangle\in\boldsymbol{F}(\mathbf{S})$.

$\mathfrak{R}$-отказ R безопасен после трассы, если после трассы безопасна кнопка R. Действие z безопасно после трассы, если оно разрешается некоторой кнопкой $z{\in}P$, безопасной после трассы. $\mathfrak{R}$-трасса безопасна, если в модели нет трассы $\langle\gamma\rangle$, и каждый символ трассы безопасен после непосредственно предшествующего ему префикса трассы. Множества безопасных трасс реализации $\mathbf{I}$ и спецификации $\mathbf{S}$ обозначаются $\boldsymbol{SafeIn}(\mathbf{I})$ и $\boldsymbol{SafeBy}(\mathbf{S})$.

Гипотеза о безопасности (безопасно-тестируемости) реализации для заданной спецификации:

$\mathbf{I}$ ***safe for*** $\mathbf{S}\ =_{\text{def}}\ (\langle\gamma\rangle\notin\boldsymbol{F}(\mathbf{S})\ \Rightarrow\ \langle\gamma\rangle\notin\boldsymbol{F}(\mathbf{I}))$
$\&\ \forall\sigma{\in}\boldsymbol{SafeBy}(\mathbf{S})\cap\boldsymbol{SafeIn}(\mathbf{I})\ \forall P{\in}\mathfrak{R}\cup\mathfrak{Q}$
$(P$ ***safe by*** $\mathbf{S}$ ***after*** $\sigma\ \Rightarrow\ P$ ***safe in*** $\mathbf{I}$ ***after*** $\sigma)$.

Множество безопасных реализаций $\boldsymbol{safe}\mathfrak{I}(\mathbf{S})=\{\mathbf{I}\,|\,\mathbf{I}$ ***safe for*** $\mathbf{S}\}$.

Отношение безопасной конформности:

$\mathbf{I}$ ***saco*** $\mathbf{S}\ =_{\text{def}}$ $\mathbf{I}$ ***safe for*** $\mathbf{S}$
$\&\ \forall\sigma{\in}\boldsymbol{SafeBy}(\mathbf{S})\cap\boldsymbol{SafeIn}(\mathbf{I})\ \forall P$ ***safe by*** $\mathbf{S}$ ***after*** σ
$\boldsymbol{obs}(\sigma,P,\mathbf{I})\subseteq\boldsymbol{obs}(\sigma,P,\mathbf{S})$,

где $\boldsymbol{obs}(\sigma,P,\mathbf{T})\ =_{\text{def}}\ \{u\,|\,\sigma\cdot\langle u\rangle\in\mathbf{T}\ \&\ (u{\in}P\ \vee\ u{=}P\ \&\ P{\in}\mathfrak{R})\}$.

Множество конформных реализаций $\mathfrak{I}(\mathbf{S})=\{\mathbf{I}\,|\,\mathbf{I}$ ***saco*** $\mathbf{S}\}$.

И.Б.Бурдонов, А.С.Косачев.
Эквивалентные семантики взаимодействия.
Труды Института системного программирования РАН, N 14.1, 2008, стр.55-72.
18 стр.

1. Квазипорядок и эквивалентность семантик

Пусть в алфавите внешних действий L заданы две семантики $\mathfrak{R}_1/\mathfrak{Q}_1$ и $\mathfrak{R}_2/\mathfrak{Q}_2$: $\cup(\mathfrak{R}_1\cup\mathfrak{Q}_1)=\cup(\mathfrak{R}_2\cup\mathfrak{Q}_2)=\mathsf{L}$. Будем говорить, что $\mathfrak{R}_1/\mathfrak{Q}_1$-семантика *не сильнее* $\mathfrak{R}_2/\mathfrak{Q}_2$-семантики и обозначать $\mathfrak{R}_1/\mathfrak{Q}_1\le\mathfrak{R}_2/\mathfrak{Q}_2$, если для каждой спецификации $\mathbf{S}$ с отношением $\mathit{safe}\,\mathfrak{I}_1$ в $\mathfrak{R}_1/\mathfrak{Q}_1$-семантике существует отношение $\mathit{safe}\,\mathfrak{I}_2$ в $\mathfrak{R}_2/\mathfrak{Q}_2$-семантике, сохраняющее классы безопасных и конформных реализаций: $\mathit{safe}\mathfrak{I}_1(\mathbf{S})=\mathit{safe}\mathfrak{I}_2(\mathbf{S})\ \&\ \mathfrak{I}_1(\mathbf{S})=\mathfrak{I}_2(\mathbf{S})$. Определим также: $\mathfrak{R}_1/\mathfrak{Q}_1\ge\mathfrak{R}_2/\mathfrak{Q}_2 =_{\text{def}} \mathfrak{R}_2/\mathfrak{Q}_2\le\mathfrak{R}_1/\mathfrak{Q}_1$.

Лемма 1: Отношение «не сильнее» для семантик является квазипорядком: рефлексивно и транзитивно.
Доказательство:
Рефлексивность: $\forall\mathbf{S}\ \forall\mathit{safe}\,\mathfrak{I}_1\ \ \mathit{safe}\mathfrak{I}_1(\mathbf{S})=\mathit{safe}\mathfrak{I}_1(\mathbf{S})\ \&\ \mathfrak{I}_1(\mathbf{S})=\mathfrak{I}_1(\mathbf{S})$.
Транзитивность:
если $\forall\mathbf{S}\ \forall\mathit{safe}\,\mathfrak{I}_1\ \exists\mathit{safe}\,\mathfrak{I}_2\ \ \mathit{safe}\mathfrak{I}_1(\mathbf{S})=\mathit{safe}\mathfrak{I}_2(\mathbf{S})\ \&\ \mathfrak{I}_1(\mathbf{S})=\mathfrak{I}_2(\mathbf{S})$
и $\forall\mathbf{S}\ \forall\mathit{safe}\,\mathfrak{I}_2\ \exists\mathit{safe}\,\mathfrak{I}_3\ \ \mathit{safe}\mathfrak{I}_2(\mathbf{S})=\mathit{safe}\mathfrak{I}_3(\mathbf{S})\ \&\ \mathfrak{I}_2(\mathbf{S})=\mathfrak{I}_3(\mathbf{S}))$,
то $\forall\mathbf{S}\ \forall\mathit{safe}\,\mathfrak{I}_1\ \exists\mathit{safe}\,\mathfrak{I}_3\ \ \mathit{safe}\mathfrak{I}_1(\mathbf{S})=\mathit{safe}\mathfrak{I}_3(\mathbf{S})\ \&\ \mathfrak{I}_1(\mathbf{S})=\mathfrak{I}_3(\mathbf{S})$.
Лемма доказана.

Будем говорить, что $\mathfrak{R}_1/\mathfrak{Q}_1$- и $\mathfrak{R}_2/\mathfrak{Q}_2$-семантики эквивалентны и обозначать $\mathfrak{R}_1/\mathfrak{Q}_1\sim\mathfrak{R}_2/\mathfrak{Q}_2$, если они не сильнее друг друга: $\mathfrak{R}_1/\mathfrak{Q}_1\le\mathfrak{R}_2/\mathfrak{Q}_2$ и $\mathfrak{R}_2/\mathfrak{Q}_2\le\mathfrak{R}_1/\mathfrak{Q}_1$. Очевидно, это отношение является эквивалентностью: рефлексивно, симметрично и транзитивно.

2. Необходимые условия квазипорядка

Сначала исследуем вопрос о необходимых условиях отношения «не сильнее». Эти условия будут сформулированы и доказаны в следующих четырёх леммах, использующих примеры на Рис.1.

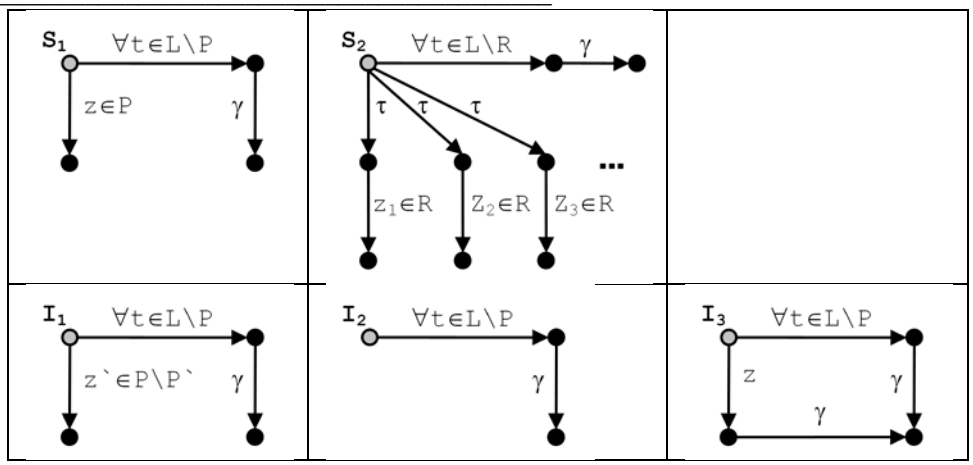

Рис.1.

Лемма 2: Если $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$, то каждая $\mathfrak{Q}_1$-кнопка является также $\mathfrak{Q}_2$-кнопкой: $\mathfrak{Q}_1 \subseteq \mathfrak{Q}_2$.

Доказательство: Допустим утверждение не верно: существует кнопка $P \in \mathfrak{Q}_1 \setminus \mathfrak{Q}_2$. Рассмотрим LTS-спецификацию $\mathbf{S_1}$, в которой в начальном состоянии определены разрушающие переходы по каждому действию $t \in L \setminus P$, и один переход по некоторому действию $z \in P$. Выберем отношение ***safe by*$_1$**, объявляющее кнопку P безопасной (после пустой трассы), а все остальные $\mathfrak{Q}_1$-кнопки опасными. Возможны два случая в зависимости от того, разрешается ли действие z какой-нибудь $\mathfrak{Q}_2$-кнопкой, безопасной по отношению ***safe by*$_2$**.

1. По отношению ***safe by*$_2$** действие z разрешается некоторой безопасной кнопкой $P` \in \mathfrak{Q}_2$.

   По допущению, $P` \ne P$. Поскольку каждое действие $t \in L \setminus P$ разрушающее, а кнопка $P`$ безопасна в спецификации, должно быть $t \notin P`$. Следовательно, $P` \subset P$. Тогда найдётся действие $z` \in P \setminus P`$. Для реализации $\mathbf{I_1}$, в которой есть ненаблюдаемый в $\mathfrak{R}_2/\mathfrak{Q}_2$-семантике отказ $P`$, имеем $\mathbf{I_1}$ ***safe for*$_2$** $\mathbf{S_1}$. Поскольку по отношению ***safe by*$_1$** единственная $\mathfrak{Q}_1$-кнопка, безопасная после пустой трассы, это кнопка P, имеем $\mathbf{I_1}$ ***safe for*$_1$** $\mathbf{S_1}$. Но это противоречит $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$.
2. По отношению ***safe by*$_2$** действие z не разрешается безопасными $\mathfrak{Q}_2$-кнопками.

   Тогда по отношению ***safe by*$_2$** после пустой трассы вообще нет безопасных $\mathfrak{Q}_2$-кнопок: $\mathfrak{Q}_2$-кнопка, вложенная в P, не содержит действие z и, следовательно, не разрешает ни одного действия в спецификации, а такая

$\mathfrak{Q}_2$-кнопка опасна; $\mathfrak{Q}_2$-кнопка, не вложенная в P, разрушающая по некоторому действию $t \in L \setminus P$. А тогда $\mathbf{I_2}$ ***safe for***$_2$ $\mathbf{S_1}$. В то же время, поскольку по отношению ***safe by***$_1$ $\mathfrak{Q}_1$-кнопка P безопасна после пустой трассы, имеем $\mathbf{I_2}$ ~~***safe for***~~$_1$ $\mathbf{S_1}$. Но это противоречит $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$.

В обоих случаях мы пришли к противоречию, следовательно, наше допущение не верно, а утверждение Леммы верно.

Лемма 3: Если $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$, то каждая $\mathfrak{Q}_2$-кнопка представима в виде объединения $\mathfrak{R}_1$- и $\mathfrak{Q}_1$-кнопок: $\forall P \in \mathfrak{Q}_2 \ \exists \mathfrak{U} \subseteq \mathfrak{R}_1 \cup \mathfrak{Q}_1 \ P = \cup \mathfrak{U}$.

Доказательство: Допустим утверждение не верно: существует кнопка $P \in \mathfrak{Q}_2$, которую нельзя представить в виде объединения $\mathfrak{R}_1$- и $\mathfrak{Q}_1$-кнопок. Тогда найдётся такое действие $z \in P$, которое не разрешается ни одной $\mathfrak{R}_1$- или $\mathfrak{Q}_1$-кнопкой, вложенной в P. Рассмотрим LTS-спецификацию $\mathbf{S_1}$, в которой в начальном состоянии определены разрушающие переходы по каждому действию $t \in L \setminus Q$, и один переход по действию z. Для любого отношения ***safe by***$_1$ нет безопасной $\mathfrak{R}_1$- или $\mathfrak{Q}_1$-кнопки, разрешающей действие z. В $\mathfrak{R}_2/\mathfrak{Q}_2$-семантике есть неразрушающая кнопка P, разрешающая действие z. Поэтому для любого отношения ***safe by***$_2$ должна найтись безопасная кнопка, разрешающая действие z. Но в таком случае реализация $\mathbf{I_3}$ ***safe for***$_1$ $\mathbf{S_1}$, но $\mathbf{I_3}$ ~~***safe for***~~$_2$ $\mathbf{S_1}$, что противоречит $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$. Мы пришли к противоречию, следовательно, наше допущение не верно, а утверждение Леммы верно.

Лемма 4: Если $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$, то каждая $\mathfrak{R}_1$-кнопка представима в виде объединения конечного числа $\mathfrak{R}_2$-кнопок: $\forall P \in \mathfrak{R}_1 \ \exists \mathfrak{U} \subseteq \mathfrak{R}_2 \ P = \cup \mathfrak{U}$ & $\mathfrak{U}$-конечно.

Доказательство: Допустим утверждение не верно: некоторая кнопка $P \in \mathfrak{R}_1$ не представима в виде объединения конечного числа $\mathfrak{R}_2$-кнопок. Рассмотрим LTS-спецификацию $\mathbf{S_2}$, в которой в начальном состоянии определены разрушающие переходы по каждому действию $t \in L \setminus P$, а для каждого действия $z \in P$ определён τ-переход в состояние, из которого выходит только переход по действию z. По отношению ***safe by***$_1$ после пустой трассы кнопка P безопасна, но отказ P отсутствует. В реализации $\mathbf{I_2}$ в этой ситуации имеется отказ P. Следовательно, $\mathbf{I_2}$ ~~***saco***~~$_1$ $\mathbf{S_2}$. По отношению ***safe by***$_2$ после пустой трассы безопасна такая и только такая $\mathfrak{R}_2$-кнопка, которая вложена в P. Более

того, после любой конечной трассы таких $\mathfrak{R}_2$-отказов безопасна тоже такая и только такая $\mathfrak{R}_2$-кнопка, которая вложена в P. Любая конечная последовательность $\mathfrak{R}_2$-отказов, вложенных в P, конформна: она реализуется в состоянии после τ-перехода, соответствующего действию z, которое не принадлежит объединению этих $\mathfrak{R}_2$-кнопок, а такое действие всегда найдётся, поскольку P не представимо в виде объединения конечного числа $\mathfrak{R}_2$-кнопок. Тем самым, $\mathbf{I}_2$ $\boldsymbol{saco}_2$ $\mathbf{S}_2$. Но это противоречит $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$. Мы пришли к противоречию, следовательно, наше допущение не верно, а утверждение Леммы верно.

Лемма 5: Если $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$, то каждая $\mathfrak{R}_2$-кнопка представима в виде объединения конечного числа $\mathfrak{R}_1$-кнопок: $\forall R \in \mathfrak{R}_2 \ \exists \mathfrak{U} \subseteq \mathfrak{R}_1 \ R = \cup\mathfrak{U}$ & $\mathfrak{U}$-конечно.

Доказательство аналогично доказательству Леммы 4.

3. Нормализация отношения *safe by*

Требования к отношению ***safe by*** однозначно определяют безопасность $\mathfrak{R}$-кнопок, но оставляют достаточно много свободы в объявлении безопасных и опасных $\mathfrak{Q}$-кнопок. В некоторых случаях можно говорить о «несогласованности» отношения ***safe by*** в следующем смысле: хотя некоторая $\mathfrak{Q}$-кнопка объявлена безопасной после одной $\mathfrak{R}$-трассы спецификации и опасной – после другой $\mathfrak{R}$-трассы, в любой реализации после этих $\mathfrak{R}$-трасс эта кнопка одинаково опасна или безопасна по отношению ***safe in***. Это происходит тогда, когда в любой реализации эти две $\mathfrak{R}$-трассы заканчиваются в одном и том же множестве состояний. А это, в свою очередь, происходит тогда, когда $\mathfrak{R}$-трассы *эквивалентны*: в этих $\mathfrak{R}$-трассах на соответствующих местах стоят одинаковые внешние действия или последовательности $\mathfrak{R}$-отказов с одинаковым множеством отвергаемых внешних действий. Этим последовательностям $\mathfrak{R}$-отказов соответствуют стабильные состояния, в которых нет переходов по всем действиям, принадлежащим каким-нибудь отказам в последовательности. Эквивалентность $\mathfrak{R}$-трасс формально определяется так:

$\mu_1 \sim \mu_2 =_{def} \mu_1=\rho_1^1\cdot\langle z_1^1\rangle\cdot\ldots\cdot\rho_1^n\cdot\langle z_1^n\rangle\cdot\rho_1^{n+1}$ & $\mu_2=\rho_2^1\cdot\langle z_2^1\rangle\cdot\ldots\cdot\rho_2^n\cdot\langle z_1^n\rangle\cdot\rho_2^{n+1}$ & $\forall i=1..n\ z_1^i=z_2^i$ & $\forall j=1..n+1\ \cup\mathit{Im}(\rho_1^j)=\cup\mathit{Im}(\rho_2^j)$, где z_k^i – внешнее действие, а ρ_k^j – трасса отказов.

Лемма 6: Необходимым и достаточным условием того, что две $\mathfrak{R}$-трассы в любой модели заканчиваются в одном и том же множестве состояний, является их эквивалентность.

Доказательство:

1. Сначала докажем достаточность.

Доказательство будем вести по индукции. В любой модели пустые трассы эквивалентны и заканчиваются в одном множестве состояний, поскольку равны. Пусть в некоторой модели $\mathbf{S}$ с начальным состоянием s_0 трассы μ_1 и μ_2 эквивалентны и заканчиваются в одном и том же множестве состояний: $s_0\ \mathit{after}\ \mu_1 = s_0\ \mathit{after}\ \mu_2$.

Рассмотрим их продолжение одним и тем же внешним действием z:

$s_0\ \mathit{after}\ \mu_1\cdot\langle z\rangle = \cup\{s\ \mathit{after}\ \langle z\rangle \mid s\in(\mathbf{S}\ \mathit{after}\ \mu_1)\}$

$= \cup\{s\ \mathit{after}\ \langle z\rangle \mid s\in(\mathbf{S}\ \mathit{after}\ \mu_2)\} = \mathbf{S}\ \mathit{after}\ \mu_2\cdot\langle z\rangle$.

Теперь рассмотрим продолжение трасс последовательностями отказов ρ_1 и ρ_2 с одним и тем же множеством отвергаемых внешних действий $\cup\mathit{Im}(\rho_1)=\cup\mathit{Im}(\rho_2)$:

$s_0\ \mathit{after}\ \mu_1\cdot\rho_1 = \{s\in(\mathbf{S}\ \mathit{after}\ \mu_1) \mid \forall z\in\{\tau,\gamma\}\cup\cup\mathit{Im}(\rho_1)\ s\text{—}z\not\rightarrow\}$

$= \{s\in(\mathbf{S}\ \mathit{after}\ \mu_2) \mid \forall z\in\{\tau,\gamma\}\cup\cup\mathit{Im}(\rho_1)\ s\text{—}z\not\rightarrow\} = s_0\ \mathit{after}\ \mu_2\cdot\rho_2$.

Достаточность доказана.

2. Теперь докажем необходимость.

Вместо исходной LTS-спецификации $\mathbf{S}$, в которой есть трассы μ_1 и μ_2, возьмём соответствующую ей «расплетённую» LTS $\boldsymbol{T}(\mathbf{S})$. Её состояниями будут $\mathfrak{R}$-трассы исходной LTS, начальное состояние – пустая трасса. Переход $\mu\text{—}u\rightarrow\mu'$ по внешнему действию или разрушению u проводится тогда и только тогда, когда $\mu'=\mu\cdot\langle u\rangle$. Переход $\mu\text{—}\tau\rightarrow\mu'$ проводится тогда и только тогда, когда трасса μ не заканчивается отказом, а $\mu'=\mu\cdot\rho$, где ρ непустая трасса отказов. Нетрудно показать, что множества $\mathfrak{R}$-трасс LTS $\mathbf{S}$ и $\boldsymbol{T}(\mathbf{S})$ совпадают.

Допустим трассы μ_1 и μ_2 не эквивалентны. Рассмотрим первое место в этих трассах, где нарушается их эквивалентность. Здесь возможны два случая.

2.1. Несовпадение действий: $\mu_1=\lambda_1\cdot\langle z_1\rangle\cdot\kappa_1$, $\mu_2=\lambda_2\cdot\langle z_2\rangle\cdot\kappa_2$, $\lambda_1\sim\lambda_2$, $z_1\neq z_2$,.

Поскольку $\lambda_1\sim\lambda_2$, имеем $\boldsymbol{P}(\mathbf{S})$ ***after*** λ_1 = $\boldsymbol{P}(\mathbf{S})$ ***after*** λ_2. Граф LTS $\boldsymbol{T}(\mathbf{S})$ является деревом: в начальном состоянии не заканчивается ни один переход, а в каждое другое состояние ведёт только один переход. Поэтому в этой LTS трассы $\lambda_1\cdot\langle z_1\rangle$ и $\lambda_2\cdot\langle z_2\rangle$ заканчиваются в двух множествах состояний таких, что ни одно состояние одного множества не достижимо из состояния другого множества. Отсюда следует, что трассы μ_1 и μ_2 заканчивается в разных (даже не пересекающихся) множествах состояний LTS $\boldsymbol{P}(\mathbf{S})$.

2.2. Несовпадение множеств отвергаемых внешних действий: $\mu_1=\lambda_1\cdot\rho_1\cdot\kappa_1$, $\mu_2=\lambda_2\cdot\rho_2\cdot\kappa_2$, $\lambda_1\sim\lambda_2$, $\cup\boldsymbol{Im}(\rho_1)\neq\cup\boldsymbol{Im}(\rho_2)$, λ_1 и λ_2 не заканчиваются отказами, а κ_1 и κ_2 не начинаются с отказов.

Поскольку $\lambda_1\sim\lambda_2$, имеем $\boldsymbol{P}(\mathbf{S})$ ***after*** λ_1 = $\boldsymbol{P}(\mathbf{S})$ ***after*** λ_2. Эти множества содержат состояния λ_1 и λ_2, из которых ведут переходы $\lambda_1\text{—}\tau\rightarrow\lambda_1\cdot\rho_1$ и $\lambda_2\text{—}\tau\rightarrow\lambda_2\cdot\rho_2$. Добавим новое терминальное состояние, в которое для i=1,2 проведём из состояния $\lambda_i\cdot\rho_i$ все переходы по действиям $z\notin\{z_i\}\cup\cup\boldsymbol{Im}(\rho_i)$, если трасса κ_i начинается с внешнего действия z_i, или $z\notin\cup\boldsymbol{Im}(\rho_i)$, если трасса κ_i пуста. После такого добавления, очевидно, трассы μ_1 и μ_2 сохраняются в LTS. Но теперь либо трасса $\lambda_1\cdot\rho_1$ не заканчивается в состоянии $\lambda_2\cdot\rho_2$, либо трасса $\lambda_2\cdot\rho_2$ не заканчивается в состоянии $\lambda_1\cdot\rho_1$ (либо и то и другое). Какими бы ни были продолжения κ_1 и κ_2, теперь трассы μ_1 и μ_2 заканчиваются в разных множествах состояний.

Необходимость доказана.

Лемма доказана.

Отношение ***safe by*** будем называть *нормальным*, если оно определяет одинаковые безопасные кнопки после эквивалентных $\mathfrak{R}$-трасс. Любое отношение ***safe by*** можно *нормализовать*, если после каждой $\mathfrak{R}$-трассы μ объявить безопасными те и только те кнопки, которые исходным отношением объявлены безопасными после *какой-нибудь* $\mathfrak{R}$-трассы, эквивалентной $\mathfrak{R}$-трассе μ.

Лемма 7: Нормализованное отношение ***safe by*** удовлетворяет всем трём требованиям, предъявляемым к такому отношению. При нормализации сохраняются класс безопасных и класс конформных реализаций.

Доказательство: Оба утверждения Леммы непосредственно следуют из Леммы 6, поскольку эквивалентные трассы заканчиваются в одном и том же множестве состояний как в спецификации, так и в любой реализации, в которой такие трассы есть.

4. Достаточные условия квазипорядка

Мы покажем, что совокупность условий Лемм 2÷5 является не только необходимым, но и достаточным условием $\mathfrak{R}_1/\mathfrak{Q}_1 \le \mathfrak{R}_2/\mathfrak{Q}_2$. Будем считать, что эти условия выполнены. Поскольку нормализация сохраняет безопасные и конформные реализации (Лемма 7), а отношение «не сильнее» является квазипорядком (Лемма 1), нам достаточно рассматривать только нормализованные отношения ***safe by***.

Сначала введём отображение $\mathfrak{R}_1$-трасс в $\mathfrak{R}_2$-трассы и обратно. Мы будем обозначать: $\mathbf{1+}=\mathbf{2}$ и $\mathbf{2+}=\mathbf{1}$. Для i=1,2 отображение f_i каждую $\mathfrak{R}_i$-трассу превращает в $\mathfrak{R}_{i+}$-трассу, заменяя каждый $\mathfrak{R}_i$-отказ R_i на конечную последовательность $\mathfrak{R}_{i+}$-отказов $R_{i1}, R_{i2}, \ldots, R_{in}$, объединение которых совпадает с ним: $R_i = R_{i1} \cup R_{i2} \cup \ldots \cup R_{in}$.

Заметим, что отображение f_i переводит трассу в эквивалентную ей. Поэтому множество состояний после любой $\mathfrak{R}_i$-трассы μ совпадает с множеством состояний после $\mathfrak{R}_{i+}$-трассы $f_i(\mu)$.

Также отметим, что разрушаемость или неразрушаемость кнопки после любой трассы модели не зависит от семантики и определяется только самой моделью.

Определим отношение ***safe by***$_2$ в $\mathfrak{R}_2/\mathfrak{Q}_2$-семантике. Безопасность $\mathfrak{R}_2$-кнопок определяется однозначно требованием 1): $\mathfrak{R}_2$-кнопка безопасна тогда и только тогда, когда она неразрушающая после $\mathfrak{R}_2$-трассы, а трасса не продолжается дивергенцией. $\mathfrak{Q}_2$-кнопку, являющуюся также $\mathfrak{Q}_1$-кнопкой, объявим безопасной после $\mathfrak{R}_2$-трассы μ тогда и только тогда, когда она безопасна после $\mathfrak{R}_1$-трассы $f_2(\mu)$. В силу нормализации отношения ***safe by***$_2$, это означает, что кнопка безопасна после каждой $\mathfrak{R}_1$-трассы, эквивалентной трассе $f_2(\mu)$. Остальные $\mathfrak{Q}_2$-кнопки объявим опасными после любых $\mathfrak{R}_2$-трасс.

Лемма 8: Определённое таким образом отношение ***safe by***$_2$ удовлетворяет всем трём требованиям, предъявляемым к такого рода отношению. Если отношение ***safe by***$_1$ нормально, то отношение ***safe by***$_2$ также нормально.

Доказательство:

1. Требование 1) выполнено по определению.

2. Докажем выполнение требования 2). Пусть $\mathfrak{R}_2$-трасса μ продолжается в спецификации действием z, которое разрешается некоторой неразрушающей кнопкой P_2. Если это $\mathfrak{R}_2$-кнопка, то она же и безопасна. Если это $\mathfrak{Q}_2$-кнопка, то она совпадает с объединением $\mathfrak{R}_1$- и $\mathfrak{Q}_1$-кнопок $P_2=P_{21}\cup P_{22}\cup\ldots\cup P_{2n}$, каждая из которых неразрушающая после $\mathfrak{R}_2$-трассы μ. Для некоторого i имеет место $z\in P_{2i}$ и кнопка P_{2i} неразрушающая после $\mathfrak{R}_2$-трассы μ. А тогда кнопка P_{2i} неразрушающая после $\mathfrak{R}_1$-трассы $f_2(\mu)$. В таком случае в $\mathfrak{R}_1/\mathfrak{Q}_1$-семантике существует кнопка P_1, которая разрешает действие z и безопасна после $\mathfrak{R}_1$-трассы $f_2(\mu)$. Если это $\mathfrak{Q}_1$-кнопка, то она же является $\mathfrak{Q}_2$-кнопкой и безопасна после $\mathfrak{R}_2$-трассы μ. Если это $\mathfrak{R}_1$-кнопка, то она представима в виде объединения $\mathfrak{R}_2$-кнопок $P_1=P_{11}\cup P_{12}\cup\ldots\cup P_{1n}$, каждая из которых неразрушающая после $\mathfrak{R}_1$-трассы $f_2(\mu)$. Тогда найдётся такое j, что $z\in P_{1j}$ и $\mathfrak{R}_2$-кнопка P_{1j} неразрушающая после $\mathfrak{R}_2$-трассы μ. А тогда $\mathfrak{R}_2$-кнопка P_{1j} безопасна после $\mathfrak{R}_2$-трассы μ. Выполнение требования 2) доказано.

3. Выполнение требования 3) следует из того, что из $\mathfrak{Q}_2$-кнопок безопасной после $\mathfrak{R}_2$-трассы μ может быть только $\mathfrak{Q}_1$-кнопка Q_1. А тогда она безопасна после $\mathfrak{R}_1$-трассы $f_2(\mu)$. Следовательно, она разрешает некоторое действие, которым продолжается $\mathfrak{R}_1$-трасса $f_2(\mu)$. А тогда этим же действием продолжается $\mathfrak{R}_2$-трассы μ, поскольку она заканчивается в том же множестве состояний.

4. Покажем, что отношение ***safe by***$_2$ нормально, если нормально отношение ***safe by***$_1$.

Пусть есть две эквивалентные $\mathfrak{R}_2$-трассы $\mu_1\sim\mu_2$. Поскольку они заканчиваются в одном и том же множестве состояний спецификации, неразрушающие $\mathfrak{R}_2$-кнопки после этих трасс одинаковые, следовательно, одинаковые безопасные $\mathfrak{R}_2$-кнопки. Также имеем $f_2(\mu_1)\sim f_2(\mu_2)$. Отсюда следует, что после $\mathfrak{R}_1$-трасс $f_2(\mu_1)$ и $f_2(\mu_2)$ одинаковые безопасные $\mathfrak{Q}_1$-

кнопки. А тогда после $\mathfrak{R}_2$-трасс μ_1 и μ_2 одинаковые безопасные $\mathfrak{Q}_2$-кнопки (совпадающие с этими безопасными $\mathfrak{Q}_1$-кнопками).

Лемма доказана.

Теперь исследуем вопрос о соотношении безопасных $\mathfrak{R}_1$- и $\mathfrak{R}_2$-трасс, связанных отображениями f_2 и f_1, и о безопасности кнопок после таких трасс.

Лемма 9: Если $\mathfrak{R}_i$-трасса μ безопасна по ***safe by***$_i$, то $\mathfrak{R}_{i+}$-трасса $f_i(\mu)$ безопасная по ***safe by***$_{i+}$. Пусть $\mathfrak{R}_i$-кнопка R_i безопасна по ***safe by***$_i$ после $\mathfrak{R}_i$-трассы μ и совпадает с объединением $\mathfrak{R}_{i+}$-кнопок $R_i=R_{i1}\cup R_{i2}\cup...\cup R_{in}$. Тогда после $\mathfrak{R}_{i+}$-трассы $f_i(\mu)$ все эти $\mathfrak{R}_{i+}$-кнопки безопасны по ***safe by***$_{i+}$. Пусть $\mathfrak{Q}_i$-кнопка Q_i безопасна после $\mathfrak{R}_i$-трассы μ по ***safe by***$_i$. Тогда она является также $\mathfrak{Q}_{i+}$-кнопкой и безопасна после $f_{i+}(\mu)$ по ***safe by***$_{i+}$.

Доказательство: Пусть после $\mathfrak{R}_i$-трассы μ $\mathfrak{R}_i$-кнопка R_i безопасна по ***safe by***$_i$ и совпадает с объединением $\mathfrak{R}_{i+}$-кнопок $R_i=R_{i1}\cup R_{i2}\cup...\cup R_{in}$. Трассы μ и $f_i(\mu)$ заканчиваются в одном и том же множестве состояний, а кнопки с наблюдаемым отказом безопасны тогда и только тогда, когда они неразрушаемые. Поэтому после $\mathfrak{R}_{i+}$-трассы $f_i(\mu)$ все эти $\mathfrak{R}_{i+}$-кнопки безопасны по ***safe by***$_{i+}$.

Из этого утверждения следует, что, если $\mathfrak{R}_i$-трасса μ безопасна по ***safe by***$_i$, то $\mathfrak{R}_{i+}$-трасса $f_i(\mu)$ безопасная по ***safe by***$_{i+}$.

Пусть $\mathfrak{Q}_i$-кнопка безопасна после $\mathfrak{R}_i$-трассы μ по ***safe by***$_i$. Если i=2, то $\mathfrak{Q}_2$-кнопка объявляется безопасной после μ по ***safe by***$_2$, если она является $\mathfrak{Q}_1$-кнопкой, безопасной по ***safe by***$_1$ после $f_2(\mu)$, что и требовалось показать. Если i=1, то $\mathfrak{Q}_1$-кнопка является также $\mathfrak{Q}_2$-кнопкой, которая объявляется безопасной по ***safe by***$_2$ после $f_1(\mu)$, если, как $\mathfrak{Q}_1$-кнопка, она безопасна по ***safe by***$_1$ после $f_2(f_1(\mu))$. Трассы μ и $f_2(f_1(\mu))$ эквивалентны, следовательно, для нормализованного отношения ***safe by***$_1$ безопасность кнопок после них одинаковая: если кнопка безопасна после μ, то она также безопасна после $f_2(f_1(\mu))$. А тогда эта кнопка, как $\mathfrak{Q}_2$-кнопка, безопасна по ***safe by***$_2$ после $f_1(\mu)$, что и требовалось показать.

Теорема 1: Совокупность условий Лемм 2÷5 является не только необходимым, но и достаточным условием $\mathfrak{R}_1/\mathfrak{Q}_1\le\mathfrak{R}_2/\mathfrak{Q}_2$.

Доказательство: Необходимость условий доказана в Леммах 2÷5. Докажем достаточность совокупности этих условий.

1. Докажем, что, если реализация безопасна для спецификации с отношением ***safe by*$_2$**, то она безопасна этой же спецификации с отношением ***safe by*$_1$**. Допустим, это не так. Тогда найдётся такая реализация безопасная для спецификации с отношением ***safe by*$_2$**, такая безопасная в спецификации по ***safe by*$_1$** $\mathfrak{R}_1$-трасса μ, которая имеется также в реализации, и найдётся такая $\mathfrak{R}_1$- или $\mathfrak{Q}_1$-кнопка P_1, которая безопасна после μ в спецификации по ***safe by*$_1$**, но опасна в реализации после этой трассы. По доказанному, $\mathfrak{R}_2$-трасса $f_1(\mu)$ безопасная по ***safe by*$_2$**.

1.1. Пусть P_1 $\mathfrak{R}_1$-кнопка. Тогда она совпадает с объединением $\mathfrak{R}_2$-кнопок $P_1=P_{11}\cup P_{12}\cup\ldots\cup P_{1n}$, и все эти $\mathfrak{R}_2$-кнопки безопасны по ***safe by*$_2$** после $\mathfrak{R}_2$-трассы $f_1(\mu)$. Но тогда все они безопасны после $\mathfrak{R}_2$-трассы $f_1(\mu)$ в реализации. А отсюда следует, что $\mathfrak{R}_1$-кнопка P_1 безопасна после $\mathfrak{R}_1$-трассы μ в реализации, что не верно по допущению.

1.2. Пусть P_1 $\mathfrak{Q}_1$-кнопка. Тогда она также $\mathfrak{Q}_2$-кнопка и безопасна по ***safe by*$_2$** после $\mathfrak{R}_2$-трассы $f_1(\mu)$. А тогда она безопасна после $\mathfrak{R}_2$-трассы $f_1(\mu)$ в реализации. Следовательно, она безопасна в реализации после $\mathfrak{R}_1$-трассы μ, что противоречит допущению.

Итак, мы пришли к противоречию, следовательно, наше допущение не верно, и утверждение доказано: если реализация безопасна для спецификации с отношением ***safe by*$_2$**, то она безопасна этой же спецификации с отношением ***safe by*$_1$**.

2. Докажем, что, если реализация конформна для спецификации с отношением ***safe by*$_2$**, то она конформна этой же спецификации с отношением ***safe by*$_1$**. Допустим, это не так. Тогда найдётся такая реализация конформная для спецификации с отношением ***safe by*$_2$**, такая безопасная в спецификации по ***safe by*$_1$** $\mathfrak{R}_1$-трасса μ, которая имеется также в реализации, и найдётся такая $\mathfrak{R}_1$- или $\mathfrak{Q}_1$-кнопка P_1, которая безопасна после μ в спецификации по ***safe by*$_1$**, и, по доказанному, безопасная в реализации после этой трассы, что в реализации трасса μ продолжается символом u, которое либо a) является действием $u=z\in P_1$, либо b) отказом $u=P_1$, если $P_1\in\mathfrak{R}_1$, а в спецификации трасса не продолжается символом u. По доказанному, $\mathfrak{R}_2$-трасса $f_1(\mu)$ безопасная по ***safe by*$_2$**. Очевидно также, что $\mathfrak{R}_2$-трасса $f_1(\mu)$ в реализации продолжается символом u, а в спецификации – нет.

2.1. Пусть P_1 $\mathfrak{Q}_1$-кнопка. Тогда она является также $\mathfrak{Q}_2$-кнопкой и безопасна по ***safe by***$_2$ после $\mathfrak{R}_1$-трассы $f_1(\mu)$. Тем самым $\mathfrak{R}_2$-трасса $f_1(\mu)$ безопасна в спецификации по ***safe by***$_2$, после неё безопасна по ***safe by***$_2$ $\mathfrak{Q}_2$-кнопка P_1, $u{=}z{\in}P_1$, в реализации трасса продолжается действием $u{=}z$, а в спецификации – нет. Но это противоречит конформности реализации для спецификации с отношением ***safe by***$_2$.

2.2. Пусть P_1 $\mathfrak{R}_1$-кнопка. Тогда она совпадает с объединением $\mathfrak{R}_2$-кнопок $P_1{=}P_{11}{\cup}P_{12}{\cup}\ldots{\cup}P_{1n}$, и все эти $\mathfrak{R}_2$-кнопки безопасны по ***safe by***$_2$ после $\mathfrak{R}_2$-трассы $f_1(\mu)$.

2.2.1. Пусть $u{=}z{\in}P_1$. Тогда для некоторого i имеем $u{=}z{\in}P_{1i}$. Тем самым $\mathfrak{R}_2$-трасса $f_1(\mu)$ безопасна в спецификации по ***safe by***$_2$, после неё безопасна по ***safe by***$_2$ $\mathfrak{R}_2$-кнопка P_{1i}, $u{=}z{\in}P_{1i}$, в реализации трасса продолжается действием $u{=}z$, а в спецификации – нет. Но это противоречит конформности реализации для спецификации с отношением ***safe by***$_2$.

2.2.2. Пусть $u{=}P_1$. Тогда $\mathfrak{R}_2$-трасса $f_1(\mu)$ безопасна в спецификации по ***safe by***$_2$, после неё безопасны по ***safe by***$_2$ все $\mathfrak{R}_2$-кнопки P_{1i}, и в реализации трасса продолжается трассой отказов $\langle P_{11}, P_{12}, \ldots, P_{1n}\rangle$. Но тогда в спецификации $\mathfrak{R}_2$-трасса $f_1(\mu)$ также должна продолжаться этой трассой отказов. А в таком случае $\mathfrak{R}_2$-трасса $f_1(\mu)$ продолжается отказом P_1. Следовательно, $\mathfrak{R}_1$-трасса μ также продолжается отказом P_1, что не верно.

Мы пришли к противоречию, и, значит, наше допущение не верно, а доказываемое утверждение верно: если реализация конформна для спецификации с отношением ***safe by***$_2$, то она конформна этой же спецификации с отношением ***safe by***$_1$.

3. Докажем, что, если реализация безопасна для спецификации с отношением ***safe by***$_1$, то она безопасна этой же спецификации с отношением ***safe by***$_2$. Допустим, это не так. Тогда найдётся такая реализация безопасная для спецификации с отношением ***safe by***$_1$, такая безопасная в спецификации по ***safe by***$_2$ $\mathfrak{R}_2$-трасса μ, которая имеется также в реализации, и найдётся такая $\mathfrak{R}_2$- или $\mathfrak{Q}_2$-кнопка P_2, которая безопасна после μ в спецификации по ***safe by***$_2$, но опасна в реализации после этой трассы. По доказанному, $\mathfrak{R}_1$-трасса $f_2(\mu)$ безопасная по ***safe by***$_1$.

3.1. Пусть P_2 $\mathfrak{R}_2$-кнопка. Тогда, по доказанному, она совпадает с объединением $\mathfrak{R}_1$-кнопок $P_2=P_{21}\cup P_{22}\cup\ldots\cup P_{2n}$, и все эти $\mathfrak{R}_1$-кнопки безопасны по ***safe by***$_1$ после $\mathfrak{R}_1$-трассы $f_2(\mu)$. Но тогда все они безопасны после $\mathfrak{R}_1$-трассы $f_2(\mu)$ в реализации. А отсюда следует, что $\mathfrak{R}_2$-кнопка P_2 безопасна после $\mathfrak{R}_2$-трассы μ в реализации, что не верно по допущению.

3.2. Пусть P_2 $\mathfrak{Q}_2$-кнопка. Тогда она должна быть также $\mathfrak{Q}_1$-кнопкой, безопасной по отношению ***safe by***$_1$ после $\mathfrak{R}_1$-трассы $f_2(\mu)$. Но тогда в реализации эта кнопка безопасна после $\mathfrak{R}_1$-трассы $f_2(\mu)$, следовательно, безопасна после $\mathfrak{R}_2$-трассы μ, что противоречит допущению.

Итак, мы пришли к противоречию, следовательно, наше допущение не верно, и утверждение доказано: если реализация безопасна для спецификации с отношением ***safe by***$_1$, то она безопасна этой же спецификации с отношением ***safe by***$_2$.

4. Докажем, что, если реализация конформна для спецификации с отношением ***safe by***$_1$, то она конформна этой же спецификации с отношением ***safe by***$_2$. Допустим, это не так. Тогда найдётся такая реализация конформная для спецификации с отношением ***safe by***$_1$, такая безопасная в спецификации по ***safe by***$_2$ $\mathfrak{R}_2$-трасса μ, которая имеется также в реализации, и найдётся такая $\mathfrak{R}_2$- или $\mathfrak{Q}_2$-кнопка P_2, которая безопасна после μ в спецификации по ***safe by***$_2$, и, по доказанному, безопасная в реализации после этой трассы, что в реализации трасса μ продолжается символом u, которое либо a) является действием $u=z\in P_2$, либо b) отказом $u=P_2$, если $P_2\in\mathfrak{R}_2$, а в спецификации трасса не продолжается символом u. По доказанному, $\mathfrak{R}_1$-трасса $f_2(\mu)$ безопасная по ***safe by***$_1$. Очевидно также, что $\mathfrak{R}_1$-трасса $f_2(\mu)$ в реализации продолжается символом u, а в спецификации – нет.

4.1. Пусть P_2 $\mathfrak{Q}_2$-кнопка. Тогда, поскольку она безопасна, она является также $\mathfrak{Q}_1$-кнопкой и безопасна по ***safe by***$_1$ после $\mathfrak{R}_1$-трассы $f_2(\mu)$. Тем самым $\mathfrak{R}_1$-трасса $f_2(\mu)$ безопасна в спецификации по ***safe by***$_1$, после неё безопасна по ***safe by***$_1$ $\mathfrak{Q}_1$-кнопка P_2, $u=z\in P_2$, в реализации трасса продолжается действием $u=z$, а в спецификации – нет. Но это противоречит конформности реализации для спецификации с отношением ***safe by***$_1$.

4.2. Пусть P_2 $\mathfrak{R}_2$-кнопка. Тогда она совпадает с объединением $\mathfrak{R}_1$-кнопок $P_2=P_{21}\cup P_{22}\cup\ldots\cup P_{2n}$, и все эти $\mathfrak{R}_1$-кнопки безопасны по ***safe by*$_1$** после $\mathfrak{R}_1$-трассы $f_2(\mu)$.

4.2.1. Пусть $u=z\in P_2$. Тогда для некоторого i имеем $u=z\in P_{2i}$. Тем самым $\mathfrak{R}_1$-трасса $f_2(\mu)$ безопасна в спецификации по ***safe by*$_1$**, после неё безопасна по ***safe by*$_1$** $\mathfrak{R}_1$-кнопка P_{2i}, $u=z\in P_{2i}$, в реализации трасса продолжается действием $u=z$, а в спецификации – нет. Но это противоречит конформности реализации для спецификации с отношением ***safe by*$_1$**.

4.2.2. Пусть $u=P_2$. Тогда $\mathfrak{R}_1$-трасса $f_2(\mu)$ безопасна в спецификации по ***safe by*$_1$**, после неё безопасны по ***safe by*$_1$** все $\mathfrak{R}_1$-кнопки P_{2i}, и в реализации трасса продолжается трассой отказов $\langle P_{21}, P_{22}, \ldots, P_{2n}\rangle$. Но тогда в спецификации $\mathfrak{R}_1$-трасса $f_2(\mu)$ также должна продолжаться этой трассой отказов. А в таком случае $\mathfrak{R}_1$-трасса $f_2(\mu)$ продолжается отказом P_2. Следовательно, $\mathfrak{R}_2$-трасса μ также продолжается отказом P_2, что не верно.

Мы пришли к противоречию, и, значит, наше допущение не верно, а доказываемое утверждение верно: если реализация конформна для спецификации с отношением ***safe by*$_1$**, то она конформна этой же спецификации с отношением ***safe by*$_2$**.

Теорема доказана.

5. Эквивалентные и минимальные семантики

Из Теоремы 1 непосредственно следует следующая теорема.

Теорема 2: Необходимым и достаточным условием эквивалентности двух семантик является совпадение семейств $\mathfrak{Q}$-кнопок и представимость каждой $\mathfrak{R}$-кнопки одной семантики в виде объединения конечного числа $\mathfrak{R}$-кнопок другой семантики.

Представляет интерес определение минимальной (по вложенности семейств кнопок) эквивалентной семантики. Иными словами, какие кнопки можно удалить из заданной $\mathfrak{R}/\mathfrak{Q}$-семантики так, чтобы получилась семантика, эквивалентная исходной. По Теореме 2, $\mathfrak{Q}$-кнопки удалять нельзя, а $\mathfrak{R}$-кнопку можно удалить в том случае, когда она равна объединению конечного числа

остающихся $\mathfrak{R}$-кнопок. $\mathfrak{R}$-кнопку будем называть *разложимой*, если её можно представить в виде объединения конечного числа $\mathfrak{R}$-кнопок, отличных от неё самой.

Теорема 3: В минимальной эквивалентной $\mathfrak{R}_0/\mathfrak{Q}$-семантике, если она существует, семейство $\mathfrak{R}_0$ совпадает с множеством неразложимых $\mathfrak{R}$-кнопок из $\mathfrak{R}$.

Доказательство: Если кнопка $P\in\mathfrak{R}$, то, в силу эквивалентности семантик, она может быть представлена в виде объединения конечного числа $\mathfrak{R}_0$-кнопок. Но тогда, если кнопка P неразложима, она просто должна быть $\mathfrak{R}_0$-кнопкой. Наоборот, если бы кнопка $P\in\mathfrak{R}_0$ была разложима, то её можно было бы представить в виде объединения конечного числа $\mathfrak{R}$-кнопок, отличных от неё самой $P=P_1\cup P_2\cup...\cup P_n$. В силу эквивалентности семантик, каждая кнопка P_i, в свою очередь, может быть представлена в виде объединения конечного числа $\mathfrak{R}_0$-кнопок $P_i=P_{i1}\cup P_{i2}\cup...\cup P_{in_i}$, которые очевидно, тоже отличны от P. А тогда кнопку P можно представить в виде объединения конечного числа $\mathfrak{R}_0$-кнопок P_{ij}, отличных от неё самой, что противоречит минимальности $\mathfrak{R}_0/\mathfrak{Q}$-семантики.

Однако минимальная эквивалентная семантика не обязательно существует. Примером может служить семантика, в которой $\mathfrak{R}$-кнопки – это все бесконечные подмножества бесконечного алфавита: все $\mathfrak{R}$-кнопки разложимы.

Теорема 4: Для существования минимальной эквивалентной $\mathfrak{R}_0/\mathfrak{Q}$-семантики необходимо и достаточно, чтобы любая разложимая $\mathfrak{R}$-кнопка разлагалась в объединение конечного числа неразложимых $\mathfrak{R}$-кнопок.

Доказательство: Необходимость условия следует из эквивалентности (любая $\mathfrak{R}$-кнопка представима в виде объединения конечного числа $\mathfrak{R}_0$-кнопок) и Теоремы 3: в минимальной эквивалентной $\mathfrak{R}_0/\mathfrak{Q}$-семантике семейство $\mathfrak{R}_0$ совпадает с множеством неразложимых $\mathfrak{R}$-кнопок из $\mathfrak{R}$. Покажем достаточность: если условие выполнено, то $\mathfrak{R}_0/\mathfrak{Q}$-семантика эквивалентна и минимальна, где $\mathfrak{R}_0$ – это множество неразложимых $\mathfrak{R}$-кнопок из $\mathfrak{R}$. Эта семантика эквивалентна по условию. Если бы семантика не была минимальной,

то какую-то кнопку можно было бы удалить из неё. А это возможно лишь тогда, когда эта кнопка разлагается в объединение конечного числа $\mathfrak{R}_0$-кнопкой, следовательно, является разложимой, что не верно.

Теорема 5: Если конечно число бесконечных $\mathfrak{R}$-кнопок (в частности, конечно семейство $\mathfrak{R}$), то минимальная эквивалентная семантика существует.

Доказательство: Процесс разложения любой конечной разложимой $\mathfrak{R}$-кнопки заканчивается через конечное число шагов (на каждом шаге разлагаем все получившиеся разложимые кнопки) в силу конечности самой кнопки (на каждом шаге получаются конечные множества меньшей мощности). В силу этого, процесс разложения бесконечной $\mathfrak{R}$-кнопки также заканчивается через конечное число шагов, поскольку конечно число бесконечных $\mathfrak{R}$-кнопок (на каждом шаге получаем кнопки, каждая из которых либо строго вложенная бесконечная кнопка, а число бесконечных кнопок конечно, либо конечна).

Теорема 6: Если минимальная эквивалентная семантика существует, то она же является наименьшей.

Доказательство: Это непосредственно следует из Теоремы 3.

6. Пример: семантики отношений *ioco* и $ioco_{\beta\gamma\delta}$

Отношение конформности ***ioco*** (Input-Output Conformance) было предложено Яном Тритмансом [7,8] для реактивных систем. Взаимодействие с такими системами сводится к обмену сообщениями между реализацией и тестом. Алфавит L внешних действий разбивается на множество $?L$ стимулов – сообщений, передаваемых из теста в реализацию (обозначаются с префиксом "?"), и множество $!L$ реакций – сообщений, передаваемых из реализации в тест (обозначаются с префиксом "!"). Единственный наблюдаемый отказ – отсутствие реакций, называемый стационарностью (*quiescence*) и обозначаемый символом $\delta=!L$.

Генерация тестов для отношения ***ioco*** предполагает, что, кроме единственной $\mathfrak{R}$-кнопки "δ", для каждого стимула $?x$ существует $\mathfrak{Q}$-кнопка "$\{?x\}$", с помощью которой в реализацию можно послать этот стимул. Отказ, возникающий при посылке одного стимула, называется блокировкой этого стимула и ненаблюдаем. Обозначим семейства этой семантики $\mathfrak{R}_0=\{\delta\}=\{!L\}$ и $\mathfrak{Q}_0=\{\{?x\}|?x\in?L\}$. По Теореме 2, не существует другой семантики, эквивалентной данной. В то же время Тритманс заявляет, что использование

таких дополнительных тестовых возможностей, как посылка нескольких стимулов или совмещение посылки стимулов с приёмом всех реакций, не увеличивает мощность тестирования и приводит только к излишнему недетерминизму теста. Иными словами, семантика, получаемая добавлением $\mathfrak{Q}_1$-кнопок вида $\{\{?x_1\},\{?x_2\},\ldots\}$ или $\{\delta\}\cup\{\{?x_1\},\{?x_2\},\ldots\}$, эквивалентна исходной.

Причина расхождения в том, что Тритманс определяет отношение конформности не на всём классе реализаций, а на его подклассе. Требуется, чтобы реализация была, во-первых, строго-конвергентной, а, во-вторых, всюду-определённой по стимулам (*input-enabled*). Такая реализация в каждом своём достижимом состоянии не имеет дивергенции, а в каждом достижимом стабильном состоянии принимает все стимулы. Кроме того, Тритманс рассматривает модели без разрушения. На таком подклассе реализаций, действительно, добавление в исходную семантику указанных $\mathfrak{Q}_1$-кнопок даёт эквивалентную семантику, поскольку в реализации не возникает ненаблюдаемых отказов, а весь алфавит внешних действий покрывается кнопками исходной семантики.

Этот пример показывает, что эквивалентность семантик может существенно изменяться, если её рассматривать на подклассах реализаций. Разумеется, для того, чтобы опираться на такую модифицированную эквивалентность, нужны обоснованные гипотезы о возможных классах тестируемых реализаций.

В [2] нами предложена семантика для реактивных систем с разрушением и дивергенцией, допускающая наблюдение блокировок стимулов: $\mathfrak{R}_2=\mathfrak{R}_0\cup\mathfrak{Q}_0$ и $\mathfrak{Q}_2=\varnothing$, и соответствующее отношение конформности $\boldsymbol{ioco}_{\beta\gamma\delta}$. В отличие от ***ioco***, для такой семантики, по Теореме 2, эквивалентные семантики существуют на классе всех реализаций. Эквивалентной будет любая семантика, получающаяся добавлением любых $\mathfrak{R}$-кнопок, каждая из которых разрешает конечное число стимулов и, быть может, все реакции. Это почти те же самые кнопки, которые для отношения ***ioco*** можно добавлять на подклассе строго-конвергентных и всюду-определённых по стимулам реализаций. Отличие в том, что, во-первых, для ***ioco*** эти кнопки добавляются как $\mathfrak{Q}$-кнопки, а для $\boldsymbol{ioco}_{\beta\gamma\delta}$ – как $\mathfrak{R}$-кнопки, и, во-вторых, для $\boldsymbol{ioco}_{\beta\gamma\delta}$ требуется конечность числа стимулов, которые могут посылаться нажатием одной кнопки. Последнее объясняется тем, что наблюдение отказа при попытке послать бесконечное число стимулов, не эквивалентно наблюдению конечной последовательности блокировок стимулов.

Литература

1. Бурдонов И.Б., Косачев А.С., Кулямин В.В. Формализация тестового эксперимента. «Программирование», 2007, No. 5.
2. Бурдонов И.Б., Косачев А.С., Кулямин В.В. Теория соответствия для систем с блокировками и разрушением. «Наука», 2008.
3. Бурдонов И.Б. Теория конформности для функционального тестирования программных систем на основе формальных моделей. Диссертация на соискание учёной степени д.ф.-м.н., Москва, 2007. http://www.ispras.ru/~RedVerst/RedVerst/Publications/TR-01-2007.pdf
4. Heerink L. Ins and Outs in Refusal Testing. PhD thesis, University of Twente, Enschede, The Netherlands, 1998.
5. Lestiennes G., Gaudel M.-C. Test de systemes reactifs non receptifs. Journal Europeen des Systemes Automatises, Modelisation des Systemes Reactifs, pp. 255–270. Hermes, 2005.
6. Petrenko A., Yevtushenko N., Huo J.L. Testing Transition Systems with Input and Output Testers. Proc. IFIP TC6/WG6.1 15th Int. Conf. Testing of Communicating Systems, TestCom'2003, pp. 129-145. Sophia Antipolis, France, May 26-29, 2003.
7. Tretmans J. Conformance testing with labelled transition systems: implementation relations and test generation. Computer Networks and ISDN Systems, v.29 n.1, p.49-79, Dec. 1996.
8. Tretmans J. Test Generation with Inputs, Outputs and Repetitive Quiescence. In: Software-Concepts and Tools, Vol. 17, Issue 3, 1996.