УДК 004.052

О.М. Тарасюк, А.В. Горбенко, В.С. Харченко, Ю.В. Мотора

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

ПРИМЕР КОМПЛЕКСНОГО ИСПОЛЬЗОВАНИЯ ФОРМАЛЬНЫХ МЕТОДОВ СПЕЦИФИКАЦИИ ТРЕБОВАНИЙ И АНАЛИЗА НАДЕЖНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ УПРАВЛЕНИЯ

Представлены результаты совместного использования формального метода спецификации требований Event-B, метода анализа видов и последствий критических отказов FME(C)A, а также метода анализа деревьев отказов FTA на примере системы управления движением автотранспорта по однонаправленному мосту.

Ключевые слова: *формальные методы, Event-B, FME(C)A, FTA, надежность компьютерных систем.*

Введение

Обеспечение высокой гарантированной надежности компьютерных систем управления является чрезвычайно актуальной задачей в условиях повсеместного внедрения информационных компьютерных технологий. Отказы систем управления транспортом, энергетических комплексов, вредных химических производств и других комплексов критического применения могут приводить не только к значительным финансовым потерям, но и к человеческим жертвам и экологическому ущербу. Например, одной из вероятных причин крупной железнодорожной катастрофы в Бельгии, произошедшей 15 февраля 2010 г. и унёсшей жизни более чем 25 человек, указывается сбой системы управления, вследствие чего два поезда оказались на одном пути [1].

Для построения высоконадежных (гарантоспособных) систем управления корректность спецификации и её аппаратно-программная реализация является необходимым, но недостаточным условием. Корректность предполагает отсутствие отказов, обусловленных дефектами проектирования (design faults), что может достаточно эффективно обеспечиваться на основе применения формальных методов разработки и верификации, например Ebent-B, VDM, Model Checking и др. В то же время компьютерные системы комплексов критического применения должны быть устойчивы и к отказам, обусловленным физическими отказами элементов (physical faults), а также внешними воздействиями, в том числе информационными (intrusions). Реализация данного свойства возможна при наличии средств отказоустойчивости (fault- and intrusion-tolerance), т.е. средств, обеспечивающих реализацию всех составляющих операционного цикла обнаружения, локализации, парирования отказов и восстановления вычислительного (управляющего) процесса [2]. Необходимым условием построения эффективных отказоустойчивых систем является анализ возможных видов, причин и последствий отказов, вызванных различными причинами.

В этом контексте актуальным представляется совместное применение формальных методов разработки систем и формальных методов анализа их надежности. Особый интерес представляет совместное применение метода спецификации требований Event-B [3], метода анализа видов и последствий критических отказов FME(C)A [4] и деревьев отказов FTA [5]. Такой вывод логичен с учетом понятий полноты и минимальности множеств инвариантов [6], поскольку FME(C)A-таблицы (FTA-деревья) представляют собой систематизированную информацию о возможных отказах.

Целью данной статьи является исследование и практическая иллюстрация возможности совместного использования формального метода Event-B, а также таблично-графовых методов анализа надежности FME(C)A и FTA на классическом примере системы управления движением автотранспорта по однонаправленному мосту [7].

1. Формальные методы разработки и анализа надежности

1.1. Сущность и основные принципы Event-B

Метод Event-B основан на использовании нотации абстрактной машины AMN (Abstract Machine Notation) для формальной разработки программного обеспечения. Данный метод формализует процесс описания свойств и динамического поведения систем, обеспечивает контроль за соблюдением этих свойств в процессе функционирования на основе механизма предусловий, а также позволяет получить программный код путем разработки и поэтапной детализации формальной спецификации системы. При использовании формального метода Event-B спецификация системы представляется в виде её формальной модели, основными элементами которой являются:

– набор системных переменных (variables), конкретное значение которых отражает определенное состояние системы (state);

– контекст (context), представленный в виде набора системных констант;

– инварианты (invariants) – набор свойств (условий), истинность которых должна всегда соблюдаться в процессе функционирования системы;

– события (events), возникающие внутри системы или за её пределами и переводящие систему из одного состояния в другое путем выполнения системой определенных операций, изменяющих значения системных переменных в качестве реакции на каждое конкретное событие;

– набор предусловий (guards) для каждого события, запрещающих его возникновение, если в результате реакции системы на это событие произойдет нарушение инвариантов.

Ключевыми особенностями Event-B являются поэтапная детализация (step-wise refinement) модели системы и автоматическое доказательство её корректности. Детализация предполагает поэтапный переход от более абстрактной модели системы к более конкретной на основе добавления новых событий или изменения существующих, добавления новых операций, переменных, пред- и пост-условий, инвариантов и/или констант. Доказательство корректности выполняется путем перебора всех событий и инвариантов, и автоматически-выполняемого математического доказательства того, что при возникновении каждого события с учетом механизма предусловий не происходит нарушения ни одного инварианта. На каждом новом этапе детализации выполняется доказательство только новых теорем. Применение Event-B позволяет повысить качество требований к системе (снизить вероятность дефектов в требованиях), а также значительно сократить или исключить полностью дефекты проектирования, гарантируя корректное поведение системы в рамках используемой системы инвариантов.

1.2. Сущность и основные принципы FTA

Практика показывает, что возникновение и развитие крупных аварий, как правило, характеризуется комбинацией случайных локальных событий, возникающих с различной частотой на разных стадиях аварии (отказы оборудования, человеческие ошибки, внешние воздействия, разрушения, интоксикация и т.д.).

Для выявления причинно-следственных связей между этими событиями используют логико-графические методы анализа деревьев отказов и событий FTA (fault tree analysis). При анализе деревьев отказов FTA выявляются комбинации отказов элементов системы, ошибок персонала и внешних (техногенных, природных, информационных) воздействий, приводящих к основному событию (аварийной ситуации). Метод FTA используется для анализа возможных причин возникновения аварийной ситуации и расчета ее частоты (на основе знания частот исходных событий). Его целью является:

– выявление всех путей, которые приводят к главному нежелательному событию при определенном стечении обстоятельств;

– определение минимального числа комбинаций событий, которые могут привести к главному событию;

– качественное определение основных причин нежелательного события;

– анализ чувствительности отдельных событий к отклонениям параметров системы.

Ключевой теоретической основой FTA является предположение о том, что компоненты в системе либо работают успешно, либо отказывают полностью. Дерево отказов представляет собой дедуктивное логическое построение, которое использует концепцию одного финального события (как правило, авария или отказ блока, всей системы) с целью нахождения всех возможных путей, при реализации которых оно может произойти. Для графического изображения простейшего дерева событий используют базовый набор символических изображений, которые представлены на рис. 1.

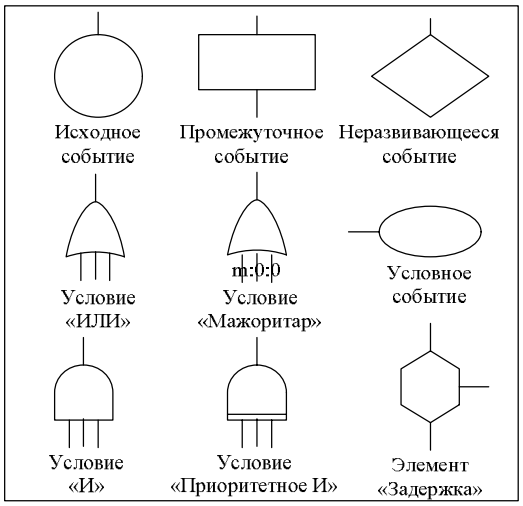

Рис. 1. Символы FTA

1.3. Сущность и основные принципы FME(C)A

Метод анализа видов, причин и последствий отказов и их критичности FME(C)A (failure modes and effect criticality analysis) состоит в:

– формировании иерархии элемент-система и определении множества элементов, отказы которых анализируются с точки зрения влияния на работоспособность системы;

– определении видов отказов каждого из элементов;

– анализе последствий отказов каждого из них для работоспособности системы;

– определении критичности этих отказов как интегральной характеристики, включающей, прежде всего, вероятность и тяжесть последствий отказов (по качественной или количественной шкале оценивания);

– определении наиболее критических отказов на основе построения и анализа построении двух- («вероятность» – «тяжесть последствий»), а в общем случае – N-мерной матрицы критичности, в которой

каждый из элементов размещается в определенной ячейке матрицы в соответствии с его критичностью.

Выявление отказов, анализ их причин и последствия, а также их ранжирование по степени критичности позволяет решать задачу оптимального повышения надежности систем.

2. Подход к совместному использованию Event-B, FMECA и FTA

Иерархический подход к анализу видов причин и последствий отказов и анализу деревьев отказов FTA может быть совмещен с процедурой детализации (refinement), являющейся основой Event-B метода. В этом случае для начальной абстрактной модели Event-B формируется абстрактная FMEA-таблица и абстрактное дерево отказов FTA.

В процессе выполнения процедуры детализации, когда выполняется очередной переход от более абстрактной к более конкретной модели системы, соответственно выполняется и детализация FMEA-таблицы и дерева отказов FTA [8].

Таким образом, в конечном счете, имеем иерархию FMEA-таблиц и FTA-деревьев соответствующих иерархии моделей Event-B системы. В свою очередь, операции декомпозиции (decomposition) модели Event-B будет соответствовать операция разбиения более абстрактной FMEA-таблицы на несколько FMEA-таблиц следующего уровня детализации, а также более абстрактного FTA-дерева на несколько FTA-деревьев следующего уровня. При этом на каждом этапе детализации происходит оценка критичности отказов и наименее критические могут быть исключены из дальнейшего анализа. Такой подход позволяет решить проблему размерности и сложности FMEA- и FTA-анализа для многокомпонентных иерархических систем, а также рассматривать дополнительное свойство прослеживаемости (трассируемости) FMEA- и FTA-анализа, что особенно важно для независимой экспертизы и верификации.

3. Пример комплексного использования Event-B, FMECA и FTA

3.1. Система управления движением по одностороннему мосту

В качестве примера, демонстрирующего возможности комплексирования формального метода Event-B, FMECA и FTA, рассмотрим разработку спецификации для системы управления движением автотранспорта по одностороннему мосту, связывающему остров с материком.

Вербальные требования к разрабатываемой системе систематизированы в табл. 1, а её визуальное представление показано на рис. 2. Полный пример разработки модели Event-B системы управления движением подробно рассмотрен в [7, 9].

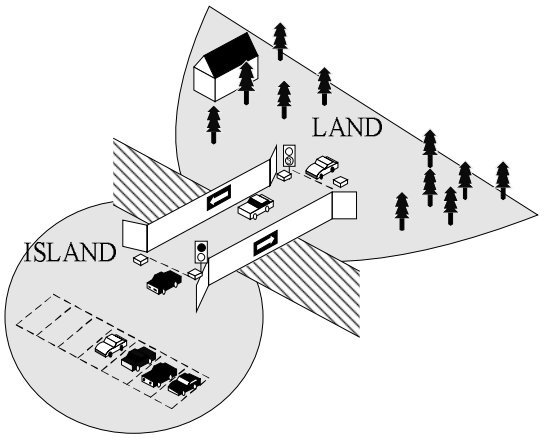

Рис. 2. Однонаправленное движение по мосту

Таблица 1

Требования к системе управления движением автотранспорта по однонаправленному мосту

№	Требование	Условное обозначение
1.	Система управляет движением по мосту, соединяющему остров с материком	FUN-1
2.	Количество машин на острове ограниченно количеством мест на стоянке, *d*	FUN-2
3.	Мост является однонаправленным, т.е. в один момент времени по нему могут двигаться машины только либо по направлению к острову, либо к материку	FUN-3
4.	Однажды запущенная, система должна работать без остановок (т.е. без блокировок)	FUN-4
5.	Система оснащена двумя светофорами которые имеют два света: зеленый и красный. В один момент времени горит только один свет	EQP-1
6.	Светофоры расположены по обе стороны моста	EQP-2
7.	Машинам разрешается двигаться только на зеленый свет	EQP-3
8.	Система оснащена четырьмя бинарными датчиками движения, каждый из которых принимает значение 0 или 1	EQP-4
9.	С каждой стороны моста расположено по два датчика, которые определяют наличие подъезжающей машины, а также направление движения	EQP-5

3.2. Абстрактная модель Event-B

Рассмотрим построение модели Event-B системы управления с некоторого абстрактного уровня детализации, на котором реализуются базовые требования FUN-1, FUN-2, FUN-3, а также логика работы со светофорами (функции EQP-1, EQP-2, EQP-3). Модель Event-B системы, реализующая данные требования (рис. 3), использует следующие переменные:

a – счетчик машин, въехавших на мост и двигающихся по направлению к острову; b – счетчик машин, уже находящихся на острове; c – счетчик машин, въехавших на мост и двигающихся по направлению к материку; *ml_tl* – светофор перед мостом со стороны материка; *il_tl* – светофор перед мостом со стороны острова; (переменные могут принимать одно из двух значений: 0 – соответствует красному цвету светофора; 1 – зеленому цвету); $ml\_pass \in \{0, 1\}$, $il\_pass \in \{0, 1\}$ – переменные, предназначенные для индикации того факта, что по мосту уже проехала хотя бы одна машина в направлении острова (*ml_pass*) или материка (*il_pass*).

В модели определены следующие события:

– ML_out_1, ML_out_2 – въезд на мост очередной машины со стороны материка, причем ML_out_2 соответствует ситуации, когда с материка на мост заезжает машина, занимающая последнее свободное место на стоянке острова. В этом случае светофор на стороне материка должен переключиться в красный цвет до тех пор, пока с острова не выедет хоть одна машина. Предусловиями, разрешающими возникновение данных событий являются: 1) «зеленый» светофор со стороны материка (*ml_tl*=1); 2) наличие на стоянке острова свободных мест (ровно одно свободное место – в случае события ML_out_2);

– L_out_1, IL_out_2 – выезд машины с острова на мост, причем IL_out_2 активизируется при выезде с острова последней машины, что переключает в зеленый свет светофор на стороне материка. В качестве предусловий данных событий определены: 1) «зеленый» светофор со стороны острова (*il_tl*=1); 2) наличие машин на острове (последней машины – в случае события IL_out_2);

– ML_in, IL_in – выезд машины с моста на материк (ML_in) или на остров (IL_in);

– ML_tl_green, IL_tl_green – переключение светофора в зеленый свет, разрешающий въезд машин на мост со стороны материка (ML_tl_green) или острова (IL_tl_green). Для события ML_tl_green определены следующие предусловия: 1) светофор на стороне материка установлен в красный цвет (*ml_tl*=0); 2) количество машин на острове и двигающихся по мосту в сторону острова меньше количества мест на стоянке острова ($a+b<d$); 3) на мосту нет машин, двигающихся в сторону материка (c=0); 4) в направлении материка по мосту уже проехала как минимум одна машина (*il_pass*=1). Соответствующие предусловиями определены и для события IL_tl_green: 1) *il_tl*=0; 2) $b>0$; 3) a=0; 4) *ml_pass*=1.

Ключевыми инвариантами модели являются:

– ***inv1_5*:** $(a = 0) \vee (c = 0)$ – по мосту возможно только одностороннее движение;

– ***inv2_3*:** $ml\_tl = 1 \Rightarrow ((a + b) < d) \wedge (c = 0)$ – зеленый цвет светофора со стороны материка разрешен только при условии, что на стоянке острова еще есть свободные места, а также на мосту нет машин, двигающихся в сторону материка;

– ***inv2_4*:** $il\_tl = 1 \Rightarrow (b > 0) \wedge (a = 0)$ – имеет аналогичный смысл, что и ***inv2_3***, но по отношению к светофору на стороне острове;

– ***inv2_5*:** $(ml\_tl = 0) \vee (il\_tl = 0)$ – в один момент времени оба светофора не могут быть установлены в зеленый цвет;

– ***inv2_8*:** $ml\_tl = 0 \Rightarrow ml\_pass = 1$ – светофор со стороны материка может быть переключен в красный цвет, при условии, что до этого хотя бы одна машина уже проехала по мосту в сторону острова;

– ***inv2_9*:** $il\_tl = 0 \Rightarrow il\_pass = 1$ – аналогично *inv2_8* по отношению к светофору со стороны острова.

Представленная модель обладает очевидным недостатком – для переключения светофора с зеленого цвета на красный необходимо, чтоб хотя бы одна машина въехала на мост. До этого момента выезд машин с противоположного конца моста будет запрещен.

CONTEXT *Bridge*
CONSTANTS *d*
AXIOMS
  axm1: $d \in \mathbf{N}$
  axm1: $d > 0$
END
MACHINE *Car_control2*
SEES *Bridge*
VARIABLES
ml_tl, *il_tl*,
ml_pass, *il_pass*
INVARIANTS
 inv1_1: $a \in N$;
 inv1_2: $b \in N$;
 inv1_3: $c \in N$;
 inv1_5: $(a = 0) \vee (c = 0)$.
 inv2_1: $ml\_tl \in \{0, 1\}$
 inv2_2: $il\_tl \in \{0, 1\}$
 inv2_3: $ml\_tl=1$
  $\Rightarrow((a + b) < d) \wedge (c = 0)$
 inv2_4: $il\_tl = 1$
  $\Rightarrow (b > 0) \wedge (a = 0)$
 inv2_5: $(ml\_tl=0)\vee(il\_tl=0)$
 inv2_6: $ml\_pass \in \{0, 1\}$
 inv2_7: $il\_pass \in \{0, 1\}$
 inv2_8: $ml\_tl = 0$
  $\Rightarrow ml\_pass = 1$
 inv2_9: $il\_tl = 0$
  $\Rightarrow il\_pass = 1$
EVENTS
 ML_out_1
  where
   grd1: $ml\_tl = 1$
   grd2: $a + b + 1 \neq d$
  then
   act1: $a := a + 1$
   act2: $ml\_pass := 1$
 END
 ML_out_2
  where
   grd1: $ml\_tl = 1$
   grd2: $a + b + 1 = d$
  then
   act1: $a := a + 1$
   act2: $ml\_tl := 0$
   act3: $ml\_pass := 1$
 END
 IL_out_1
  where
   grd1: $il\_tl = 1$
   grd2: $b \neq 1$
  then
   act1: $b := b - 1$
   act2: $c := c + 1$
   act3: $il\_pass := 1$
 END
 IL_out_2
  where
   grd1: $il\_tl = 1$
   grd2: $b = 1$
  then
   act1: $b := b - 1$
   act2: $c := c + 1$
   act3: $il\_tl := 0$
   act4: $il\_pass := 1$
 END
 ML_in
  where
   grd1: $c > 0$
  then
   act1: $c := c - 1$
 END
 IL_in
  where
   grd1: $a > 0$
  then
   act1: $a := a - 1$
   act2: $b := b + 1$
 END
 ML_tl_green
  where
   grd1: $ml\_tl = 0$
   grd2: $a + b < d$
   grd3: $c = 0$
   grd4: $il\_pass = 1$
  then
   act1: $ml\_tl := 1$
   act2: $il\_tl := 0$
   act3: $ml\_pass := 0$
 END
 IL_tl_green
  where
   grd1: $il\_tl = 0$
   grd2: $b > 0$
   grd3: $a = 0$
   grd4: $ml\_pass = 1$
  then
   act1: $il\_tl := 1$
   act2: $ml\_tl := 0$
   act3: $il\_pass := 0$
 END
END

Рис. 3. Модель Event-B системы управления движением по однонаправленному мосту

3.3. FTA-анализ модели Event-B

На рис. 4 представлено дерево событий/отказов, сочетание которых приводит к возникновению аварийной ситуации (столкновению машин, их скоплению и нарушению движения).

Детальный анализ отказов F1 и F5 позволяет сделать вывод о том, что их проявление может быть обусловлено как отказом системы управления, так и нормальным алгоритмом работы, реализуемым абстрактной моделью Event-B. Как было отмечено выше, ограничением этой модели является то, что переключение светофора с зеленого на красный цвет происходит только после проезда машины по мосту в соответствующем направлении.

Машины, находящиеся с другой стороны моста и ожидающие разрешения на выезд, должны дождаться проезда встречной машины, что следует из инвариантов inv2_8 и inv2_9. Очевидно, что данная модель системы не может быть использована в качестве спецификации и должна быть детализирована на основе уточнения реализации требований EQP-4 и EQP-5 и пересмотра инвариантов inv2_8 и inv2_9.

В то же время, необходимо уделить внимание правильной инициализации переменных системы, т.к. даже в рамках описанной модели Event-B запрещение въезда на остров при отсутствии машин, находящихся на острове или двигающихся по мосту в сторону материка, является явной ошибкой.

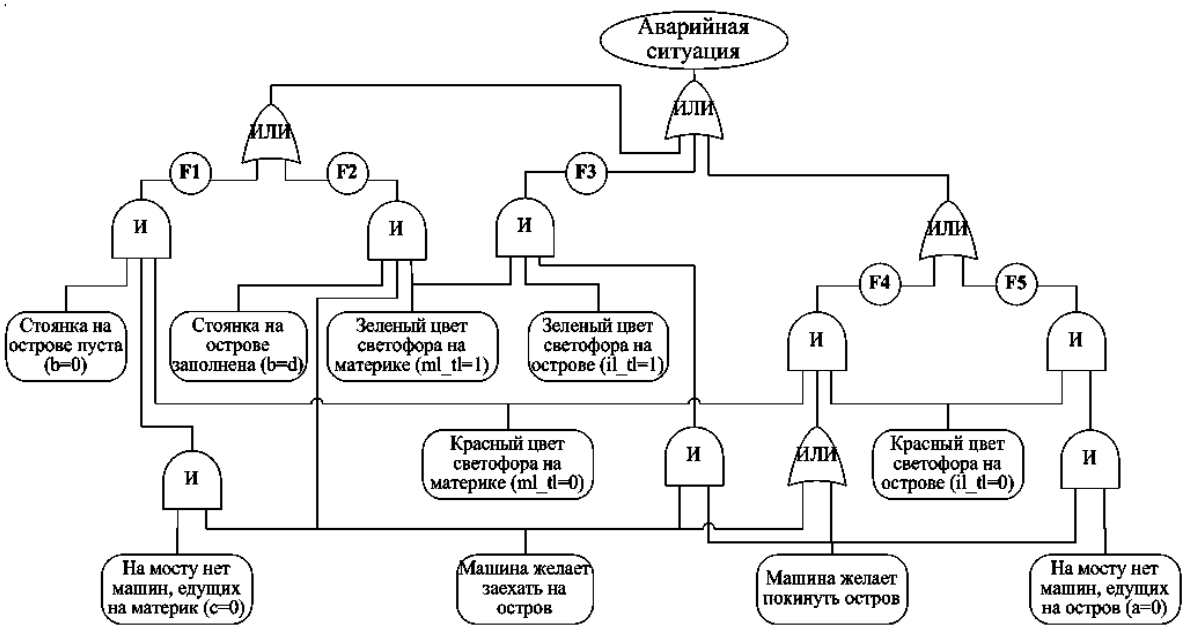

Рис. 4. Дерево отказов системы управления движением автотранспорта по однонаправленному мосту

Отказы F2-F4 связаны с явным нарушением инвариантов в случаях: 1) въезда машин на остров при заполненной стоянке; 2) разрешении встречного движения машин по мосту; 3) блокировки въезда/выезда машин на остров. Для более детального исследования и понимания причин и последствий этих отказов, оценке степени их критичности и определении методов или средств парирования или недопущения аварии целесообразным является проведение FMECA-анализа.

3.4. FMECA-анализ модели Event-B

Результаты анализа вида, причин и последствий отказов систематизированы в табл. 2.

По каждому из отказов, выявленному в результате FTA-анализа, определён нарушаемый инвариант модели Event-B, а также определены следующие возможные причины (которые необходимо уточнить с учетом особенностей реализации аппаратных средств и элементов оборудования):

1) повреждение линий связи, по которой передается команда на переключение светофора;

2) искажение команды на переключение светофора при её передаче;

3) сбой аппаратных средств (АС) системы управления (СУ) движением;

4) отказ АС СУ или средств автоматики.

Степень критичности отказов определяется последствиями, в то время как вероятность возникновения – на основе анализа причин отказов.

Как видно, наибольшую степень критичности имеет отказ F3, возникновение которого может спровоцировать столкновение машин. Возникновение отказа F3 непосредственно нарушает инвариант inv2_5, а при одновременном наличии машин, желающих заехать на остров и покинуть его, – инвариант inv1_5, т.е. инварианты, соблюдение которых является ключевым условием безопасной работы данной системы управления.

В качестве средств обеспечения отказоустойчивости определены: 1) резервирование аппаратных средств и автоматики; 2) использование протокола обмена информацией с контролем целостности сообщений, подтверждением и повторной передачей в случае искажения; 3) использование сторожевого таймера для обнаружения сбоев АС, приводящих к зависанию системы управления, и автоматического перезапуска СУ.

Таблица 2

FMEA-таблица анализа видов, причин и последствий отказов элементов системы управления движением автотранспорта по однонаправленному мосту

Вид отказа	Нарушаемый инвариант	Последствия отказа	Причина отказа	Средства отказоустойчивости	Средства отказобезопасности	Критичность	
						Тяжесть последствий	Вероятность отказа
F1: На острове нет машин, но светофор на стороне материка не разрешает въезд машин на мост	*inv2_8*	Скопление машин перед мостом, нарушение движения	Повреждение линий связи	Резервирование	Диагностика отказа и индикация аварийного режима	Низкая	Низкая
			Искажение команды на переключение	Использование контрольной суммы и протокола передачи с подтверждением	-	Низкая	Средняя
			Сбой АС СУ	Использование сторожевого таймера, резервирование	Запрещение движения на время перезагрузки системы	Низкая	Высокая
			Отказ АС СУ или автоматики	Резервирование	Диагностика отказа и индикация аварийного режима	Низкая	Средняя
F2: Все места на стоянке острова заняты, но светофор со стороны метрика разрешает заезд машин	*inv2_3*	Скопление машин на острове, нарушение движения	-//-	-//-	-//-	Средняя	-//-
F3: Два светофора одновременно разрешают движение машин навстречу друг другу	*inv2_5, inv1_5*	Аварийная ситуация	-//-	-//-	-//-	Высокая	-//-
F4: Два светофора одновременно запрещают движение машин	*inv2_5*	Скопление машин, нарушение движения	-//-	-//-	-//-	Средняя	-//-
F5: Светофор со стороны острова не разрешает машинам покинуть остров	*inv2_9*	Нарушение движения	-//-	-//-	-//-	Низкая	-//-

Для систем критического применения необходимо также определить средства обеспечения отказобезопасности (fail-safety), т.е. средства, позволяющие не допустить возникновение аварии даже в случае возникновения какого-либо отказа, несмотря на используемые средства отказоустойчивости (перевести систему в состояние защищенного отказа). В случае повреждения линий связи светофоров с контроллером системы управления, а также при отказе аппаратных средств СУ и автоматики светофоров для реализации свойства отказо-безопасности можно выключить систему управления и светофоры (fail-stop). Более целесообразным является переключение светофоров в режим явной индикации об ошибке (например, включение режима «мигающий красный»).

Очевидно, что необходимым условием реализации отказобезопасности является наличие средств диагностирования. Для обнаружения отказов в [8] предложено реализовать выполнение Event-B модели системы параллельно с работой самой системы. В этом случае, любое отклонение в состоянии одноименных переменных модели и системы, а также возникновение событий, нарушающих инварианты модели, будет свидетельствовать о возникновении отказов или других исключительных ситуаций. Например, нарушение инварианта *inv1_5* может сигнализировать о нарушении водителем правил дорожного движения – проезде на красный цвет светофора. Примером других исключительных ситуаций, не вошедших в табл. 2, является транспортировка на остров машины на эвакуаторе или же ошибочное принятие датчиками двух машин, следующих друг за другом с коротким интервалом, за одну.

Заключение

Совместное использование формального метода разработки систем Event-B и анализа их надежности (FMECA, FTA), позволяет расширить практическое применение Event-B, распространив его возможности на системы, критичные к отказам, обусловленным как проектными дефектами, так и физическими дефектами, а также при соответствующем анализе и дополнении модели на основе FIMEA [10], дефектами взаимодействия (информационного и физического).

Более того, при определенных условиях такое комплексирование может быть использовано для создания систем, устойчивых не только к отказам, а и к изменениям требований и параметров внешней среды (системам, способным эволюционировать в реальном времени – real-time evolvable systems [11, 12]). В этом случае расширяется множество допустимых событий и соответствующих им инвариантов. Однако при этом возникает проблема модификации существующих и генерации новых инвариантов, для решения которой могут быть применены средства искусственного интеллекта, например, нейромодели.

Другой актуальной задачей является анализ и классификация существующих формальных и формализованных методов и инженерных методик, их систематизация по этапам жизненного цикла, областям применения, классам систем и др., а также исследование возможности их совместного использования в целях обеспечения гарантоспособности (надежности и безопасности) систем критического применения. Прежде всего, внимание следует обратить на формальные методы спецификации и автоматического доказательства теорем (B, Event-B, VDM), формальные методы моделирования и верификации свойств систем (сети Петри, системы массового обслуживания, Model Checking), формализованные методики анализа надежности (FMECA, FTA, HAZOP), метод оценки надежности на основе построения и анализа марковских моделей.

Таким образом, следует сделать вывод о необходимости систематизации формальных методов с целью выбора одного или нескольких для решения конкретных практических задач, их комплексирования в случае, когда они дополняют друг друга и позволяют получить синергетический эффект от совместного применения. В любом случае проекты для критических приложений, в которых применяются формальные методы разработки, должны быть верифицированы с использованием диверсного инструментария, обеспечивающего требуемый доказуемый уровень достоверности оценки.

Список литературы

1. Причиной аварии поездов был сбой системы [Электронный ресурс] / Интернет газета «Дни.ру». – Режим доступа к газете: http://www.dni.ru/news/2010/2/15/185583.html.

2. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2006. – № 5. – С. 7-19.

3. Abrial J.-R. Modeling in Event-B: System and Software Engineering / J.-R. Abrial. – Cambridge University Press, 2009. – 586 p.

4. Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis (FMEA), IEC 60812. – 2006. – 41 p.

5. Fault tree analysis (FTA), IEC 61025. – 2006. – 103 p.

6. Tarasyuk O. Practical aspects of applying the Invariant-based approach to the formal system development and verification / O. Tarasyuk, A. Gorbenko, V. Kharchenko // In T. Walkowiak, J. Ma-zurkiewicz, J. Sugier and W. Zamojski (Eds.). Mono-graph of System Depend-ability. Vol. 2. Dependabil-ity of Networks. – Wroclaw: Oficyna Wydawnicza Politechnki Wroclawskiej, 2010. – P. 129-141.

7. Abrial J.-R. Formal Method Course. Example II: Controlling Cars on a Bridge / J.-R. Abrial. – Zürich: ETHZ, 2005. – 27 p.

8. Тарасюк О.М. Комплексирование формальных методов разработки и анализа надежности Event-B и FME(C)A / О.М. Тарасюк, А.В. Горбенко, В.С. Харченко // Математические машины и системы. – 2010. – № 2. – С. 166-177.

9. Тарасюк О.М. Формальные методы разработки критического программного обеспечения: Лекционный материал; Учеб. пособие; под ред. В.С. Харченко / О.М. Тарасюк, А.В. Горбенко. – Х.: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2008. – 214 с.

10. Gorbenko A.V. F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring / A.V. Gorbenko, V.S. Kharchenko, O.M. Tarasyuk, A.A. Furmanov. – In Butler M. et al. (eds.). Rigorous Development of Complex Fault-Tolerant Systems, LNCS 4157. – Springer. – 2006. – P. 153-168.

11. TR 026764: Resilience-Building Technologies: State of Knowledge, Deliverable D12. – ReSIST: Resilience for Survivability in IST. – 2006. – 345 p.

12. Sterritt R. Self- properties in NASA missions / R. Sterritt, C.A. Rouff, J.L. Rash et al. // Proc. 4th Int. Workshop on System/Software Architectures (IWSSA'05) at Int. Conf. on Software Engineering Research and Practice (SERP'05), Las-Vegas, Nevada (USA), 2005. – P. 66-72.*

Поступила в редколлегию 28.10.2010

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ПРИКЛАД КОМПЛЕКСНОГО ЗАСТОСУВАННЯ ФОРМАЛЬНИХ МЕТОДІВ СПЕЦИФІКАЦІЇ ВИМОГ ТА АНАЛІЗУ НАДІЙНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ УПРАВЛІННЯ

О.М. Тарасюк, А.В. Горбенко, В.С. Харченко, Ю.В. Мотора

У статті представлено результати сумісного використання формального методу Event-B, методу аналізу видів та наслідків критичних відмов FME(C)A, а також методу аналізу дерев відмов FTA на прикладі системи керування рухом автотранспорту по мосту з одностороннім рухом.

Ключові слова: *формальні методи, Event-B, FME(C)A, FTA, надійність комп'ютерних систем.*

EXAMPLE OF COMPLEX APPLICATION OF FORMAL METHODS OF REQUIREMENTS SPECIFICATION AND DEPENDABILITY ANALYSIS OF COMPUTER-BASED CONTROL SYSTEMS

O.M. Tarasyuk, A.V. Gorbenko, V.S. Kharchenko, Ju.V. Motora

Results of complex application of formal specification method Event-B, failure modes and effect analysis techniques and method of fault-tree analysis are reported in the paper by the example of car controlling system for one-way bridge.

Keywords: *formal methods, Event-B, FME(C)A, FTA, dependability of computer systems.*