УДК 629.7.05 + 004.05

В.С. Харченко[1], Н.В. Замирец[2], С.А. Засуха[3]

[1] *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков*
[2] *Научно-исследовательский технологический институт приборостроения, Харьков*
[3] *Государственное космическое агентство Украины, Киев*

ОПЕРАТИВНАЯ ВЕРИФИКАЦИЯ И КОРРЕКЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИУС КОСМИЧЕСКИХ СИСТЕМ. ЦЕЛИ, СЦЕНАРИИ И МОДЕЛИ

Дано формальное описание целей верификации программного обеспечения (ПО) информационно-управляющих систем (ИУС) космических систем (КС). Уточнены цели оперативной корректирующей верификации (ОКВ) ПО в полете, и предложено теоретико-множественное описание функций с учетом их критичности и целей ОКВ. Описаны сценарии и показатели для оценки готовности ИУС КС при реализации ОКВ. Дано краткое описание моделей готовности для разных сценариев ОКВ. Определены понятие стратегии ОКВ и особенности ее формирования.

Ключевые слова: *ИУС космических систем, программное обеспечение, оперативная верификация, коррекция ПО.*

Введение. Постановка задачи

В работе [1] был проведен анализ программного обеспечения (ПО) информационно-управляющих систем космических систем (ИУС КС) как объекта верификации, нормативной базы и существующих методов верификации ПО КС. Введено понятие оперативной корректирующей верификации (ОКВ), которая может проводиться по разным сценариям для функций разного уровня критичности. ОКВ проводится в условиях полета, когда не может быть обеспечена требуемая достоверность проверки, или для тех функций, проверка которых в наземных условиях невозможна или нецелесообразна по экономическим соображениям при обеспечении требований по надежности и безопасности. Определены этапы и операции по верификации ПО ИУС КС на разных этапах. Дано детальное описание операций этапа разработки ПО ИУС КС.

Актуальность проблем верификации ПО для критических приложений подтверждается проведение специальных конференций, посвященных этой тематике [2]. Данная статья является продолжением работы [1]. Ее целью является разработки элементов методологии ОКВ, в частности, формальное описание целей верификации программного обеспечения (ПО) информационно-управляющих систем (ИУС) космических систем (КС), сценариев, моделей готовности и стратегий ОКВ. Статья структурирована следующим образом. В первом разделе уточняются цели ОКВ ПО в полете и предлагается теоретико-множественное описание функций с учетом их критичности и целей ОКВ. Второй раздел посвящен описанию сценариев и показателей для оценки готовности ИУС КС при реализации ОКВ; дается характеристика моделей готовности для разных сценариев ОКВ; определяются понятие стратегии ОКВ и особенности ее формирования.

В последнем разделе сделаны выводы и намечены направления дальнейших исследований.

1. Цели верификации

1.1. Общее множество целей верификации

Основной целью верификации является подтверждение соответствия результатов разработки на соответствующем этапе сформулированным в его начале или ранее требованиям. Учитывая многоэтапность жизненного цикла ИУС КС, повторяемость этапов при пусках, общая цель верификации разделяется на множество подцелей.

Множество функций ИУС космических систем различаются по уровню критичности, определяемой ущербом, который может иметь место в результате возникновения соответствующего события (критической ситуации).

Они получили обозначение по мер снижения критичности A, B, C, U. Набор функций MF по критичности делятся на четыре множества:

$$MF = FA \cup FB \cup FC \cup FU,$$

каждое из которых описывается набором функций:

$$FA = \{f_{Ai}, i = 1,\ldots, b_A\},$$
$$FB = \{f_{Bj}, j = 1,\ldots, b_B\},$$
$$FC = \{f_{Ck}, k = 1,\ldots, b_C\},$$
$$FU = \{f_{Ul}, l = 1,\ldots, b_U\}.$$

Множество целей верификации может быть представлено в виде выражения:

МЦ = {МЦD, МЦК, МЦА, МЦS, МЦО, МЦР},

в котором каждое из множеств целей может быть

декомпозировано на подмножества в соответствии с двумя признаками:

– уровнем критичности верифицируемых функций, u_{cr} (A,B,C,U);

– задачей верификации, решаемой на данном этапе исходя из целевого назначения, a_{cr}, и др.

1.2. Множество целей верификации в полете

Нормативная база, возможности реализуемости и соображения экономической эффективности для коммерческих пусков допускают (при условии полного и строгого выполнения требований по безопасности) допускают, что часть функций системы может быть верифицировано в полете. С учетом этого проведем декомпозицию целей верификации ИУС КС для этапа полета:

МЦО ={ЦОА, ЦОВ1, ЦОВ2, ЦОВ3, ЦОС2, ЦОС3},

где ЦА1 – повышение (подтверждение) достоверности верификации функций А для снижения уровня приемлемого риска (дальнейшее повышение стандартов безопасности);

ЦВ1 – повышение (подтверждение) достоверности верификации функций В для снижения уровня приемлемого риска (дальнейшее повышение стандартов безопасности);

ЦВ2 – проведение верификации функций В, которые невозможно проверить в наземных условиях или невозможно обеспечить требуемый уровень достоверности оценки;

ЦВ3 – проведение верификации функций В в случае, если это допустимо по соображениям безопасности и требует меньших затрат, чем в наземных условиях;

ЦС2 – проведение верификации функций С, которые невозможно проверить в наземных условиях или невозможно обеспечить требуемый уровень достоверности оценки;

ЦС3 – проведение верификации функций С в случае, если это допустимо по соображениям безопасности и требует меньших затрат, чем в наземных условиях.

Исходя из этого, имеем:

$$МЦ = \{\Delta МЦ_Д, \Delta МЦ_Н, \Delta МЦ_З\},$$

где $\Delta МЦ_Д = \{ЦА1, ЦВ1\}$ – множество целей, связанных с повышением (подтверждением) достоверности верификации функций А, В для снижения уровня приемлемого риска (дальнейшее повышение стандартов безопасности);

$\Delta МЦ_Н = \{ЦВ2, ЦС2\}$ – множество целей, связанных с верификацией функций В,С, которые невозможно проверить в наземных условиях или невозможно обеспечить требуемый уровень достоверности оценки;

$\Delta МЦ_З = \{ЦВ3, ЦС3\}$ – множество целей, связанных с верификацией функций В, С в случае, если это допустимо по соображениям безопасности и требует меньших затрат, чем в наземных условиях. Соответствие целей верификации функций в полете и критичности отражается табл. 1.

Таблица 1

Соответствие целей верификации функций в полете и их критичности

Критичность	$\Delta МЦ_Д/F$		$\Delta МЦ_Н/F$		$\Delta МЦ_З/F$	
A	ЦА1	$FA_Д$ / $FA_{\overline{Д}}$				
B	ЦВ1	$FB_Д$ / $FB_{\overline{Д}}$	ЦВ2	$FB_Н$ / $FB_{\overline{Н}}$	ЦВ3	$FB_З$ / $FB_{\overline{З}}$
C			ЦС2	$FC_Н$ / $FC_{\overline{Н}}$	ЦС3	$FC_З$ / $FC_{\overline{З}}$
U						

В табл. 1 индексы при функциях соответствуют целям и условиям верификации (повышение или подтверждение достоверности верификации – индекс «д», в противном случае «$\overline{д}$»; проведение верификации функций, которые невозможно проверить в наземных условиях или невозможно обеспечить требуемый уровень достоверности оценки – индекс «$\overline{н}$», в противном случае – индекс «н»; проведением верификации функций в полете в случае, если это допустимо по соображениям безопасности и требует меньших затрат, чем в наземных условиях – индекс «з», в противном случае «$\overline{з}$»).

1.3. Графическая интерпретация функций с учетом целей верификации и их теоретико-множественное описание

С учетом декомпозиции целей верификации функций ИУС КС в полете их графическая интерпретация для разных уровней критичности представлена на рис. 1. На этом рисунке линии разного типа разделяют функции FA (а), FB (б), FC (в), FU (г) в соответствии с возможными целями верификации. С учетом целей верификации для функций с разной критичностью справедливы следующие выражения:

а) для функций FA:

$FA = \{FA_Д, FA_{\overline{Д}}\}, \quad FA_Д \cap FA_{\overline{Д}} = \varnothing;$

б) для функций FB:

$FB = \{FB_Д, FB_Н, FB_З, FA_{\overline{Д}}, FB_{\overline{Н}}, FB_{\overline{З}}\}$

$FB = FB_Д \cup FB_{\overline{Д}} = FB_Н \cup FB_{\overline{Н}} = FB_З \cup FB_{\overline{З}}$

$FB_Д \cap FB_{\overline{Д}} = FB_Н \cap FB_{\overline{Н}} = FB_З \cap FB_{\overline{З}} = \varnothing$

$FB_Н \subset FB_{\overline{Д}}, FB_З \cap FB_Н = \varnothing \quad (FB_З \subset FB \setminus FB_Н)$

$FB_З = FB_{ДЗ} \cup FB_{\overline{Д}З}, \quad FB_{ДЗ} \cap FB_{\overline{Д}З} = \varnothing$

$FB_{ДЗ} = FB_Д \cap FB_З, \quad FB_{\overline{Д}З} = FB_{\overline{Д}} \cap FB_З$

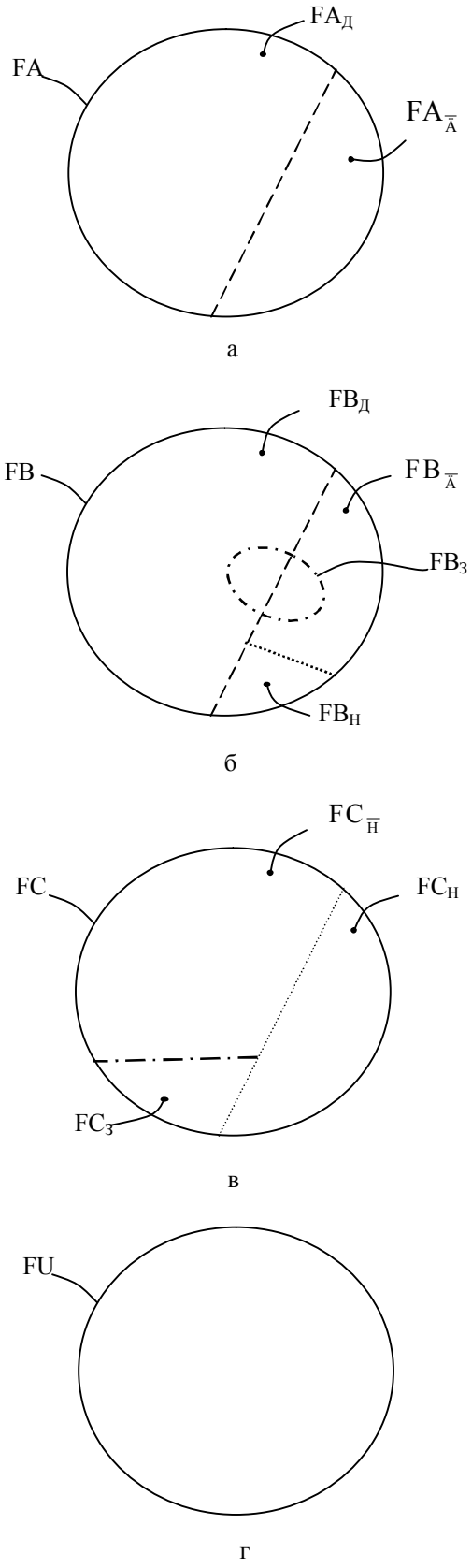

Рис. 1. Графическая интерпретация функций ИУС КС разной критичности с учетом целей верификации (для функций FA(а), FB(б), FC(в), FU(г))

в) для функций FC:

$FC = \{FC_Н,\ FC_{\bar{Н}},\ FC_З,\ FC_{\bar{З}}\}$

$FC = FC_Н \cup FC_{\bar{Н}} = FC_З \cup FC_{\bar{З}}$

$FC_Н \cap FC_{\bar{Н}} = FC_З \cap FC_{\bar{З}} = \varnothing$

$FC_З \subset FC_{\bar{Н}},\ \ FC_З \cap FC_Н = \varnothing$

$FC_{\bar{Н}} = FC_{\bar{Н}З} \cup FC_{\bar{Н}\bar{З}},\ \ FC_{\bar{Н}З} \cap FC_{\bar{Н}\bar{З}} = \varnothing$

$FC_{\bar{Н}З} = FC_{\bar{Н}} \cap FC_З,\ \ FC_{\bar{Н}\bar{З}} = FC_{\bar{Н}} \cap FC_{\bar{З}}.$

2. Модели готовности ИУС КС с ОКВ ПО

С учетом проведенного анализа и описания процессов верификации необходимо разработать возможные сценарии реакции на выявленные в полете дефекты и описать базовое множество моделей готовности ИУС КС.

2.1. Сценарии верификации и работы при выявлении дефекта

Множество сценариев может декомпозироваться в зависимости от множества $H=\{h_i, i=1,\ldots,4\}$ следующих признаков:

– возможность проведения ОВ для функций, полная верификация которых в наземных условиях невыполнима, h_1 (h_{11} – без возможности коррекции при обнаружении дефектов, h_{12} – с возможностью коррекции дефектов по результатам ОВ при сохранении полной функциональности – случай ОКВ; коррекция может быть выполнена путем скользящей замены дефектного участка, модуля новым (частичная замена) или введения новой версии (полная замена));

– возможность проведения ОВ для функций с ограниченной критичностью, верификация которых в наземных условиях более затратна, h_2 (h_{21} – без возможности коррекции, h_{22} – с возможностью коррекции – случай ОКВ);

– возможность проведения обновления ПСр в полете, h_3 (h_{31} – профилактического, связанного с устранением дефектов, h_{32} –функционального, связанного с изменением набора функций);

– возможность парирования выявленных дефектов путем блокирования функций и потерей качества, h_4 (управляемая деградация).

Признаки h_i (а также подпризнаки h_{ij}) являются булевыми переменными и принимают значения 0 или 1 в зависимости от возможности (1) или невозможности (0) проведения соответствующего вида ОВ или ОКВ.

Исходя из значений признаков $h_i \in H$ формируется множество сценариев $MSC = \{SC_q, q = 1,\ldots,w\}$, описываемые вектором значений $SC_q \sim < h_{iq} >$. Далее описываются некоторые из возможных сценариев:

SC1 – все возможные (для наземных условий) виды верификации выполняются; ОВ и коррекция дефектов в полете невозможна; этому сценарию соответствует набор признаков $H_{SC1} = \{\forall\ i = 1,\ldots,4: h_i = 0\}$;

SC2 – все возможные (для наземных условий) виды верификации выполняются; ОВ в полете не проводится; возможна коррекция (части) дефектов, проявившихся в полете; коррекция производится только при обнаружении/проявлении дефекта; этому сценарию соответствует набор при1знаков $H_{SC1} = \{h_1 = h_2 = h_4 = 0, h_{31} = 1\}$;

SC3 – все возможные для наземных условий виды верификации выполняются; в полете проводится верификация всех функций, верификация которых невозможна в наземных условиях и по ее результатам проводится коррекция обнаруженных дефектов (случай ОКВ); этому сценарию соответствует набор признаков $H_{SC1}=\{h_{12}=1, h_2=h_3=h_4=0\}$;

SC4 – все возможные для наземных условий виды верификации выполняются; в полете проводится верификация всех функций, верификация которых невозможна в наземных условиях и по ее результатам проводится коррекция обнаруженных дефектов (случай ОКВ); при этом возможно блокирование части функций и деградация системы при обнаружении дефектов; этому сценарию соответствует набор признаков $H_{SC1}=\{h_{12}=h_4=1, h_2=h_3=0\}$ и др.

2.2. Показатели

Для оценки ИУС КС с учетом возможностей проведения ОКВ предлагается использовать следующие показатели.

1. Показатели готовности, а именно:

– функция готовности $К_г(t)$,

– функция оперативной готовности $К_{ог}(t)$ и их стационарные значения (для систем с установившимся режимом).

2. Показатели для оценки риска аварии $R=[1–К_г(t)]\cdot У$, где У – ущерб.

3. Показатели деградации:

– число уровней d и величина допустимой деградации ΔП;

– коэффициент выполнения функций k_F, определяемый долей числа выполняемых функций с учетом их критичности, которая может быть оценена весовым коэффициентом.

4. Показатели затрат на верификацию $З_В$ и коррекцию $З_К$.

2.3. Основные типы моделей

Для оценки готовности и других показателей систем в зависимости от множества сценариев MCS необходимо разработать модели. Они могут базироваться на одно- или многофрагментных марковских моделях [3]. Приведем в общем виде примеры таких моделей.

Модель 1 (сценарий SC1). Граф состояний для этой модели показан на рис. 2, а.

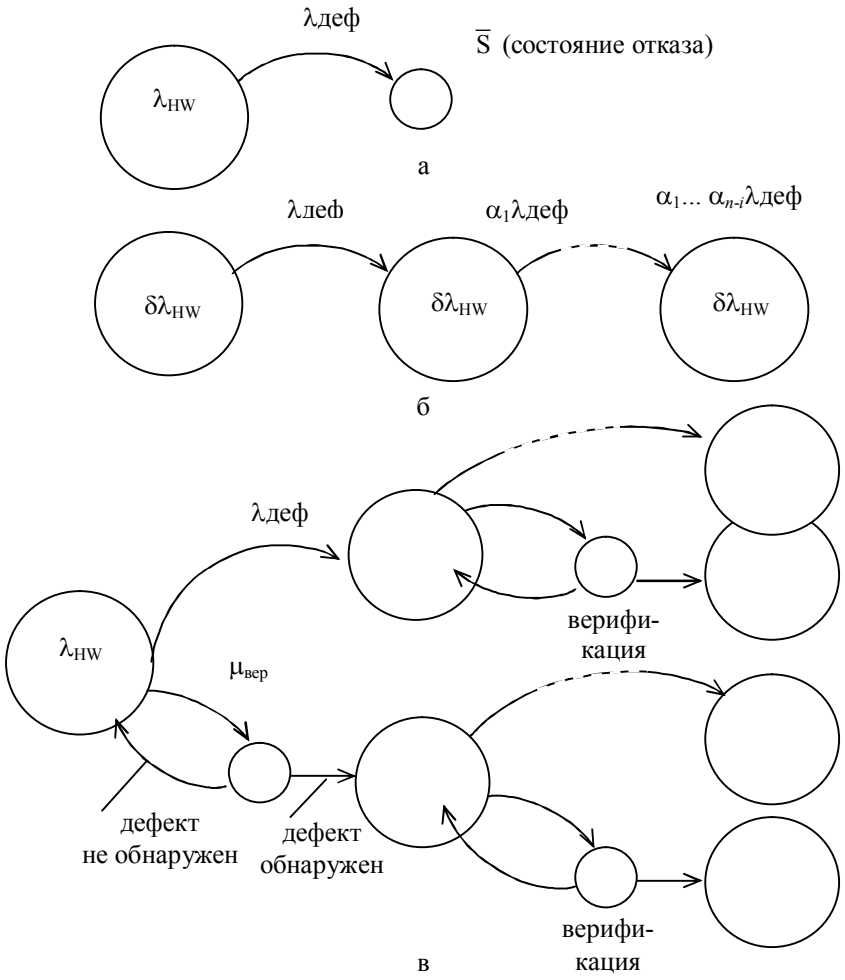

Рис. 2. Модели готовности ИУС с ОВ (а – модель 1; б – модель 2; в – модели 3, 4)

Она характеризуется некоторым множеством состояний и переходов, обусловленных потоками отказов аппаратных средств и восстановлений с учетом архитектуры системы и возможностей обнаружения отказов и восстановления работоспособности. Один из определяющих параметров – интенсивность отказов аппаратных средств, λ_{HW}. С интенсивностью λдеф система переходит в состояние отказа.

Модель 2 (сценарий SC2, рис. 2, б). Отличие состоит в том, что возможно обнаружение и частичное устранение или парирование дефектов программных средств. Уменьшение их интенсивности учитывается с помощью коэффициента α, $\alpha < 1$. Кроме того, в модель вводится коэффициент δ ($\delta > 1$), учитывающий усложнение аппаратных средств для обеспечения оперативной коррекции в полете.

Модель 3 (сценарии SC3, SC4, рис. 2, в). Для данной модели характерна древовидная структура графа переходов, в котором есть расходящиеся ветви в зависимости от того, какое событие наступает: обнаружение дефекта или начало процесса верификации. Отличие модели для разных сценариев определяется только значением параметров. Для сценария SC4 интенсивность перехода в состояние верификации (как и проявления дефектов) может быть выше.

2.4. Стратегии верификации

Стратегия верификации характеризуется набором управляющих параметров и сценарием верификации. Стратегия верификация выбирается исходя из требований к системе и имеющихся ограничений. Формирование стратегии верификации включает:

– определение параметров доверификации тех функций, верификация которых невозможна в наземных условиях;

– определение целесообразности и параметров доверификации тех функций, которые м.б. проверены и в наземных условиях и в полете.

Выводы

В статье дано теоретико-множественное описание функций по уровням критичности, целей и операций ОКВ, предложено множество сценариев, показателей и математических моделей для систем с корректируемым программным обеспечением. Эти элементы совместно с представленным в [1] описанием критичности функций и операций верификации формируют методологическую базу ОКВ.

С практической точки зрения следует использовать ее для разработки более детальных требований, методик и программно-аппаратных средств для проведения верификации и коррекции ПО ИУС КС, допускающих оперативное обновление. В теоретическом плане целесообразно разработать и исследовать модели готовности для различных сценариев, а также процедур выбора стратегий верификации, минимизирующих ресурсы при заданном уровне безопасности.

Список литературы

1. Харченко В.С. Оперативная верификация и коррекция программного обеспечения ИУС космических систем. Критичность функций и этапы верификации / В.С. Харченко, Н.В. Замирец, С.А. Засуха // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ НіУ», 2011. – С. 124-130.

2. Bender Marc. Positioning Verification in the Context of Software / System Certification / Marc Bender, Tom Maibaum, Mark Lawford, Alan Wassyng // Proceedings of the 11th International Workshop on Automated Verification of Critical Systems (AVoCS 2011). – Necastle-upon-Tyne. – 2011. – 15 p.

3. Безопасность критических инфраструктур: математические и инженерные методы оценки и обеспечения / под ред. В.С. Харченко. – Х.: Нац. аэрокосм. ун-т «ХАИ», 2011. – 603 с.

Поступила в редколлегию 10.11.2011

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

ОПЕРАТИВНА ВЕРИФІКАЦІЯ І КОРЕКЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІКС КОСМІЧНИХ СИСТЕМ. ЦІЛІ, СЦЕНАРІЇ Й МОДЕЛІ

В.С. Харченко, М.В. Замирець, С.О. Засуха

Наведено формальний опис цілей верифікації програмного забезпечення (ПЗ) інформаційно-керуючих систем (ІКС) космічних систем (КС). Уточнені цілі оперативної коригувальної верифікації (ОКВ) ПЗ в польоті й запропонований теоретико-множинний опис функцій з урахуванням їхньої критичності й цілей ОКВ. Описані сценарії й показники для оцінки готовності ІКС КС при реалізації ОКВ. Дано короткий опис моделей готовності для різних сценаріїв ОКВ. Визначені поняття стратегії ОКВ і особливості її формування.

Ключові слова: *ІКС космічних систем, програмне забезпечення, оперативна верифікація, корекція ПО.*

ON-LINE VERIFICATION AND CORRECTION OF SPACE I&C SYSTEMS SOFTWARE. THE PURPOSES, SCENARIOS AND MODELS

V.S. Kharchenko, M.V. Zamyrets, S.O. Zasukha

The formal description of the Space Instrumentation and Control systems (SICS) software (SW) verification purposes is given. The purposes of operative correcting verification (OCV) of SW in flight are specified, and the theoretical-set description of functions in view of their criticality and OCV purposes is offered. Scenarios and indicators for an estimation of SICS availability are proposed taking into account OCV features. The brief description of SICS availability models for different OCV scenarios is given. Concept of OCV strategy and features of its formation are defined.

Keywords: *space instrumentation and control system, software, on-line verification, correction of software.*