

О ТЕХНОЛОГИИ ТЕСТИРОВАНИЯ НАДЕЖНОСТИ ПРОГРАММНЫХ СРЕДСТВ АСУ СЛОЖНЫМИ СИСТЕМАМИ В ЭКСТРЕМАЛЬНЫХ УСЛОВИЯХ

В. А. Балыбердин

*ВАЛЕРИЙ АЛЕКСЕЕВИЧ БАЛЫБЕРДИН – д.т.н., профессор 3 ЦНИИ Минобороны РФ.
E-mail: baliberdinv@yandex.ru.*

107564 г. Москва, Погонный проезд, 10, Федеральное государственное бюджетное учреждение «3 Центральный научно-исследовательский институт» Министерства обороны Российской Федерации.

Рассматриваются технологические вопросы организации тестирования надежности программных средств (ПС) АСУ сложными системами в экстремальных условиях (АСУ СС). При этом внимание уделяется таким факторам надежности ПС как завершенность и отказоустойчивость, которые имеют существенное значение для эффективности функционирования АСУ СС. Факторы восстанавливаемости и готовности ПС не рассматриваются как не критичные в условиях специфики АСУ СС. Тестирование завершенности ПС предлагается осуществлять на основе оригинальной технологии, основанной на методологии анализа событий с малой вероятностью их проявления. Такая технология обеспечивает наиболее широкую сферу практического применения. Технология тестирования отказоустойчивости ПС реализуется с помощью оценочных показателей отказоустойчивости ПС, отображающих возможные факторы нарушения работоспособности ПС.

Ключевые слова: программные средства (ПС), технология тестирования завершенности ПС, технология тестирования отказоустойчивости ПС; оценочные показатели.

ABOUT THE TECHNOLOGY OF TESTING THE RELIABILITY OF SOFTWARE TOOLS OF ACS COMPLEX SYSTEMS IN EXTREME CONDITIONS

V.A. Balyberdin

10, Pogonny proezd, Moscow, 107564, Russia Federal State Budget Institution "3 Central Research Institute" of the Ministry of Defense of the Russian Federation.

The technological issues of the organization of testing the reliability of software tools (ST) of ACS complex systems in extreme conditions (ACS CS) are considered. At the same time, attention is paid to such reliability factors of ST as completeness and fault tolerance, which are essential for the efficiency of the automated control system. Recovery and readiness factors of ST are not considered as not critical in the context of the specifics of ACS CS. It is proposed to test the completeness of ST based on an original technology based on a methodology for analyzing events with a low probability of their occurrence. This technology provides the widest scope of practical application. The technology for testing the fault tolerance of ST is implemented using the estimated indicators of fault tolerance of ST, reflecting possible factors of disruption in the performance of the substation.

Keywords: software tools (ST), technology for testing the completeness of the ST, technology for testing the fault tolerance of the ST, estimated indicators.

Характеристика общего подхода к построению технологии тестирования надежности программных средств (ПС) АСУ сложными системами в экстремальных условиях (АСУ СС)

Решение вопросов обеспечения надёжности ПС АСУ СС представляет важную научно-техническую проблему, которая до настоящего времени не нашла должного решения. Особенно мало исследованы вопросы разработки практических технологий проверки надежности ПС АСУ СС.

В данной работе предполагается рассмотреть некоторые вопросы в отношении построения технологии тестирования надежности ПС. При этом внимание уделяется таким факторам надежности ПС как завершенность и отказоустойчивость, которые имеют существенное влияние на эффективность функционирования АСУ СС, как это показано в работах [1–3].

Общепризнано, что в основе проверки надежности разработанного ПС лежат процессы верификации и валидации ПС, основанные на реализации процедур установления соответствия ПС заданным требованиям и реальным потребностям прикладного использования ПС [4, 6]. В основу этих процедур положены процессы тестирования ПС.

В настоящее время понятие тестирование ПС включает два аспекта: *статическое* тестирование и *динамическое* тестирование. При одинаковой целевой установке статическое тестирование основывается на анализе всей доступной документации ПС, а динамическое тестирование – на проведение прогонов ПС (исполнения) на реальных исходных данных.

Технология тестирования завершенности ПС

Целью испытаний является оценка фактора завершенности ПС (ГОСТ ИСО/МЭК 25010), характеризующего частоту отказов, обусловленных дефектами ПС (т.е. ошибками, внесёнными в ПС в процессе его создания или модификации).

При статическом тестировании ПС осуществляется анализ всей имеющейся документации на ПС. При этом целевая установка заключается в поиске различного рода несоответствий и дефектов (ошибок) ПС, допущенных на различных этапах создания ПС.

При этом главное внимание следует обращать на возможные дефекты ПС, допущенные на этапах постановки и алгоритмизации решаемой проблемы, поскольку эти дефекты труднее обнаружить и исправить при динамическом тестировании ПС.

Процедура проведения динамического тестирования ПС для оценки *завершенности* ПС заключается в осуществлении совокупности прогонов испытуемых ПС. Каждый такой прогон проводится на собственном оригинальном наборе исходных данных.

Существующие методы оценки завершенности ПС базируются на получении и обработке статистики обнаружения дефектов (ошибок) ПС. Однако в ряде ситуаций (например, в условиях приемо-сдаточных испытаний ПС) такую статистику получить достаточно сложно или даже невозможно ввиду того, что на испытания предъявляются уже протестированные ПС. Поэтому предлагается иной подход к тестированию ПС, основанный на следующих соображениях.

Вместо анализа отказов ПС предлагается перейти к анализу положительных исходов прогонов ПС. Испытания проводятся до тех пор, пока не появится серия из n подряд проведённых прогонов ПС, ни в одном из которых не возникло программной ошибки. Величина n определяется на основе известных соотношений [1, 4, 6]. При этом важно соблюсти условие, что каждый отдельный прогон ПС осуществляется на своем индивидуальном «фоне», т.е. на оригинальном наборе исходных данных. При обнаружении отказа до получения зачетной серии прогонов ПС осуществляется устранение программной ошибки и испытания начинаются вновь «с чистого листа».

Проверяемые характеристики:

- среднее время T_{cp} до проявления очередного дефекта (ошибки) в ПС в процессе проведения тестирования (эксплуатации) ПС;
- вероятность безошибочного функционирования ПС за время $T - P(T)$.

Для проверки характеристики T_{cp} число бездефектных испытаний определяется по формуле [1, 6]:

$$n = \ln(1 - \beta) / \ln(1 - 1/T_0 \lambda), \quad (1)$$

где: T_0 – задаваемое предельное значение T_{cp} , λ – средняя интенсивность запросов к ПС, β – доверительная вероятность.

Соответственно, для проверки характеристики $P(T)$ число бездефектных испытаний определяется по формуле [1, 6]:

$$n = \ln(1 - \beta) / \ln((P_0(T))^{1/N}), \quad (2)$$

где: $P_0(T)$ – задаваемое предельное значение вероятности $P(T)$, N – среднее число обращений к ПС за время T , β – доверительная вероятность.

Получение серии из n бездефектных прогонов свидетельствует о том, что при доверительной

вероятности β среднее значение времени между проявлениями дефекта ПС не менее заданного T_0 (формула 1), либо заданная вероятность бездефектного функционирования ПС – не менее $P_0(T)$ (формула 2).

Технология тестирования отказоустойчивости ПС

Целью испытаний является оценка фактора отказоустойчивости ПС характеризующего способность ПС поддерживать необходимый уровень пригодности при проявлении дефектов ПС, сбоев и отказов технических средств или нарушении установленных интерфейсов [5, 7].

Способность ПС поддерживать необходимый уровень пригодности обеспечивается введением избыточности на различных уровнях рассмотрения прикладной системы. Различаются следующие основные виды избыточности:

(1) Временная избыточность. Заключается в использовании некоторой части производительности ЭВМ для контроля исполнения программ

и восстановления вычислительного процесса после отработки нештатных ситуаций.

(2) Информационная избыточность. Состоит в дублировании накопленных исходных и промежуточных данных и используется для повышения сохранности данных, в наибольшей степени влияющих на нормальное функционирование ПС и требующих значительного времени для восстановления.

(3) Программная избыточность. Используется для контроля и обеспечения достоверности наиболее важных результатов обработки информации, а также обеспечения работы системы при обнаружении дефекта ПС (программной ошибки).

Оценка отказоустойчивости ПС проводится с помощью оценочных показателей отказоустойчивости ПС.

Оценочные показатели для проверки реализации контроля данных ПС (компонентов ПС), а также для проверки работоспособности ПС при сбоях и отказах технических средств и ОС, нарушениях интерфейса и при обнаружении дефектов ПС представлены в таблице.

Таблица

Оценочные показатели для проверки отказоустойчивости ПС

Код показателя	Наименование показателя	Оценка показателя
<i>Раздел 1. Проверка реализации контроля данных</i>		
П101	Наличие контроля допустимых значений данных	0–1
П102	Наличие контроля полноты данных	0–1
П103	Наличие контроля непротиворечивости (соответствия) данных	0–1
П104	Наличие контроля актуальности данных	0–1
П105	Наличие контроля степени доверия к данным	0–1
П106	Наличие средств диагностики и устранения ошибочных значений данных	0–1
<i>Раздел 2. Проверка сохранения работоспособности ПС и информации при сбоях и отказах технических средств и ОС</i>		
П201	Наличие возможности восстановления результатов работы при отказах оборудования	0/1
П202	Наличие средств восстановления процесса в случае сбоя операционной системы	0/1
П203	Наличие средств диагностики сбоев и отказов ТС и ОС	0/1
<i>Раздел 3. Проверка работоспособности ПС при обнаружении дефектов (ошибок) в компонентах ПС</i>		
П301	Наличие средств обработки ошибочных ситуаций	0/1
П302	Полнота обработки ошибочных ситуаций	0–1
П303	Наличие резервных копий компонентов ПС	0/1
П304	Наличие средств диагностики и устранения ошибочных ситуаций	0/1
<i>Раздел 4. Обобщенная оценка отказоустойчивости ПС</i>		
П401	Доля успешно обработанных ситуаций отказа	A/B

Оценка реализации контроля входных данных ПС (показатели П101-П106) осуществляется, в основном, экспертным методом на основе анализа представленной документации (статическое тестирование ПС). Каждому показателю присваивается оценка в диапазоне 0–1 в зависимости от степени реализации соответствующего вида контроля.

Оценка сохранения работоспособности ПС при сбоях и отказах технических средств и ОС (показатели П201 – П203) осуществляется экспериментальным методом с имитацией соответствующих ситуаций для ТС и ОС. Каждому показателю присваивается значение 1, при положительном исходе испытаний (наличие соответствующих средств) и 0 – в противном случае.

Оценка работоспособности ПС при обнаружении дефектов (ошибок) в компонентах ПС (показатели П301 – П304) осуществляется экспериментальным методом с имитацией соответствующих ситуаций наличия ошибки в ПС. Каждому показателю присваивается значение 1 при положительном исходе испытаний (наличие соответствующих программных средств) и 0 – в противном случае.

Выводы

1. С учетом специфики АСУ СС основное внимание при анализе надежности ПС следует уделять таким факторам надежности ПС как завершенность и отказоустойчивость, которые имеют существенное значение для эффективности функционирования АСУ СС.

2. Предлагаемый метод проведения динамического тестирования ПС для оценки *завершенности* ПС заключается в обеспечении появления серии из n подряд проведенных прогонов ПС, ни в одном

из которых не возникло программной ошибки. Такой подход обеспечивает возможность построения необходимых оценок завершенности ПС даже в ситуациях, когда методы, основанные на анализе статистики отказов ПС, не работают.

3. Оценка отказоустойчивости ПС проводится с помощью представленных оценочных показателей отказоустойчивости ПС. Оценочные показатели соотносятся с формами действий, направленных на обеспечение необходимой отказоустойчивости ПС.

Литература

1. Балыбердин В.А., Степанов О.А. Методы оценки и обеспечения надёжности программных средств АСУВ. – М.: 3 ЦНИИ МО РФ, 2014. 136 с.
2. Балыбердин В.А., Белевцев А.М., Степанов О.А. Известия ЮФУ. Технические науки. 2015. №3. С. 62–70.
3. Балыбердин В.А., Степанов О.А., Шумило Д.А. Об оценке надежности программных средств АСУ в условиях приемосдаточных испытаний. М.: Избранные труды. XVI Международная научно-практическая конференция «Управление качеством». М.: МАИ, 2017. С. 69–73.
4. Балыбердин В.А., Маркелов Е.Б., Степанов О.А., Морозов О.С., Шумило Д.А. Изв. Рос. Акад. Ракет. и Артил. наук. 2016. №3. С. 23–28.
5. Systems and Software Engineering – Software Testing – ISO/IEC 29119-Part 1–4. 2013.
6. Балыбердин В.А., Белевцев А.М., Степанов О.А. Известия ЮФУ. Технические науки. 2018. №3. С. 209–220.
7. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality – ISO/IEC 25023. 2016.