УДК 621

Вестник СибГАУ
Т. 16, № 1. С. 86–90

ЗАВИСИМЫЕ ОТКАЗЫ В МНОГОФУНКЦИОНАЛЬНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

П. А. Кузнецов

Сибирский государственный технологический университет
Российская Федерация, 660049, г. Красноярск, просп. Мира, 82
E-mail: forubox@yandex.ru

Рассматривается вопрос взаимовлияния элементов автоматизированной системы управления (АСУ). Изучается безопасность и живучесть. Приводится градация отказов. Освещаются последствия отказов элементов и модулей системы, вызывающих отказы других элементов и модулей, возможности предотвращения этих отказов. Приводятся варианты возможных зависимых отказов. Показывается, что возможным источником опасности могут быть как отказы модулей, так и отказы резервных элементов в этих модулях. Постулируется, что повышение числа резервных элементов как минимум, не понижает до нуля потенциальную опасность. Рассматриваются различные логические структуры соединения элементов в АСУ. Приводится типичная надежностная структура автоматизированной системы управления, выполняющей несколько функций, древовидная структура. Выводится, что одна система АСУ ТП выполняет несколько функций. Один КА зачастую исполняет несколько функций. Также у самой АСУ имеются функции, не влияющие на управление, и для определения надежности системы необходимо определять, какие элементы участвуют в выполнении каких функций. Необходимо определять последовательности элементов, выполняющие ту или иную функциональную задачу. Иллюстрируется процесс развития отказов в многофункциональных системах, взаимное влияние элементов в них в случае простой линейной и разветвленной резервированной структур. Рассматриваются негативные последствия применения резервирования. Приводится пример расчёта надёжности системы с параллельным соединением элементов и учётом зависимых отказов, вызываемых элементами. Сделан вывод о необходимости нерезервирующих методов повышения надежности и предотвращения опасных воздействий.

Ключевые слова: безопасность, отказ, зависимый отказ.

Vestnik SibGAU
Vol. 16, No. 1, P. 86–90

DEPENDENT FAILURES IN MULTIFUNCTIONAL ACS

P. A. Kuznetsov

Siberian State Technological University
82, Mira Av., Krasnoyarsk, 660049, Russian Federation
E-mail: forubox@yandex.ru

The article discusses the interference of elements of the automated control system. We study the safety and survivability. Gradation failure is given. The consequences of failure cells and modules of the system, causing failures of other cells and modules, the possibility of preventing these failures are highlighted. A range of possible dependent failures is provided. It is shown that a possible source of danger can be as module failure, and failure of backup elements in these modules. It is postulated that the increase in the number of redundant elements at least does not reduce to zero the potential danger. The various logical structures of the compound elements in ACS are discussed. A typical structure of reliability of automated control system that performs several functions, the tree structure is shown. It is deduced that one system APCS performs several functions. One spacecraft often performs several functions. Also there are functions of the ACS which do not affect the operation. And to determine the reliability of the system we must determine which elements involved in performing any functions. It is necessary to determine the sequence of elements to perform a functional task. It is illustrated by the development of failures in multi-functional systems, the mutual influence of elements in them in case of simple linear and branched redundant structures. We consider the negative effects of redundancy. An example of calculating the reliability of the system with a parallel connection of elements into account and dependent failures caused by the elements is given. The conclusion of necessity of non-redundant methods to improve reliability and hazard prevention was made.

Keywords: safety, failure, dependent failure.

Введение. Надёжность систем автоматизированного сбора данных и управления является одним из важнейших показателей. От их правильной работы зависит успешность выполнения аппаратом своей миссии. Организация IEEE определяет надежность как «способность системы или компонента выполнять требуемые функции при определенных условиях за определенный период времени». Это определение дал А. Н. Авиженис, и оно считается классическим [1; 2].

Безотказностью называется свойство системы сохранять работоспособность в течение определённого времени при нормальных условиях. Живучесть – способность технического устройства, сооружения, средства или системы выполнять основные свои функции, несмотря на полученные повреждения. Ввиду расплывчатости понятия неисправности и ущерба, их конкретизация привела к выделению двух подмножеств их состояний: «большая» неисправность – отказ, «допустимая» неисправность – дефект. Уровень тестируемости дефекта определяется как вероятность обнаружения сбоя на случайно выбранном выходе [3].

Безопасностью же называется способность системы не переходить в опасное состояние, в состояние, при котором возникает ущерб «большого масштаба». Именно для сложных систем характерной является возможность весьма сложных, многократных комбинаций отказов, каждая из которых невероятно мала, а в сумме таких невероятных состояний накапливается достаточно, чтобы система попала в опасное состояние [4–6].

Подобными последствиями отказа может быть возникновение аварии, выброс энергии или материи, причиняющей вред окружающим объектам и персоналу. Переход системы в опасное состояние вызывается отказами её функциональных модулей или их резервных элементов. Выход из строя как всего модуля, так и его элемента может привести к возникновению опасного воздействия [7].

Вероятность выхода систем, а значит, и их модулей из строя, следует уменьшать. Для создания систем с высокой надежностью применяют множество принципов: принцип упрощения, принцип контроля, принцип резервирования. Последний принцип рассмотрим более подробно. Под резервированием понимается применение определённых технических средств с целью обеспечения работоспособности объекта при отказе. В системах с резервированием выделяют основной и резервный элементы [8].

Отказ может произойти как в модуле, так и в отдельном резервном элементе. И аналогично, за неисправностью элемента может последовать выброс энергии или материи, авария. Следовательно, опасность несёт как модуль, так и его резервные элементы. Данные опасности следует разделять на опасности, возникающие из-за выхода из строя модуля и выхода из строя элемента. В случае горячего резервирования количество отказов элементов увеличивается соответственно самому количеству элементов. В случае холодного – число отказов элементов остаётся не меньшим, чем без резервирования, в то время как число отказов модуля уменьшается.

Таким образом, повышение числа резервных элементов, как минимум, не понижает до нуля потенциальную опасность. Опасные воздействия могут быть направлены на персонал и инфраструктуру предприятия, в рамках которого действует АСУ ТП, и в таком случае данными воздействиями будет причиняться ущерб [9; 10].

Зависимые отказы в однофункциональных системах. Наряду с воздействием на персонал и инфраструктуру, опасное воздействие, возникшее в результате отказа одного модуля системы, может повлиять на другие модули системы и вызвать их отказ – так называемый зависимый отказ [11–13].

АСУ имеют различную логическую структуру. В случае, когда все модули системы связаны последовательно, отказ хотя бы одного модуля приводит к отказу всей системы и зависимые отказы никак не изменяют её состояние (рис. 1).

В приведённой на рис.1 системе отказ модуля 2 вызывает зависимый отказ модуля 3, но вне зависимости от этого система будет неисправна из-за отказа модуля 2.

Более сложный случай возникает, когда система имеет разветвленную структуру, в случае, когда система выполняет несколько функций, но не все элементы участвуют в выполнении любой из функций. Тогда выход из строя одного модуля приведёт к неисправности только тех функций, в выполнении которых он участвует.

Зависимые отказы в многофункциональных системах. Как правило, одна система АСУ ТП выполняет несколько функций. Один и тот же технологический процесс (ТП), хоть и рассматривается как единое целое, зачастую исполняет несколько функций. Также у самой АСУ имеются функции, не влияющие на процесс. И для определения надежности системы необходимо определять, какие элементы участвуют в выполнении каких функций. Необходимо определять последовательности элементов, выполняющие ту или иную функциональную задачу. Данная процедура разделения имеющейся системы на подсистемы (компоненты) называется декомпозицией [14].

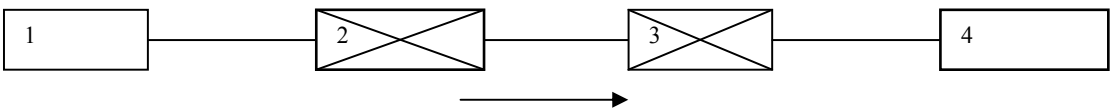

Рис. 1. Зависимый отказ в системе последовательно соединённых модулей

Декомпозиция как процесс расчленения позволяет рассматривать любую исследуемую систему как сложную, состоящую из отдельных взаимосвязанных подсистем, которые, в свою очередь, также могут быть расчленены на части. При декомпозиции каждое расчленение образует свой уровень. На этапе декомпозиции, обеспечивающем общее представление системы, осуществляются определение и декомпозиция общей цели исследования и основной функции системы как ограничение траектории в пространстве состояний системы или в области допустимых ситуаций. Наиболее часто декомпозиция проводится путем построения дерева целей и дерева функций.

Глубина декомпозиции ограничивается [15]. Декомпозиция должна прекращаться, если необходимо изменить уровень абстракции – представить элемент как подсистему. Если при декомпозиции выясняется, что модель начинает описывать внутренний алгоритм функционирования элемента вместо закона его функционирования в виде «черного ящика», то в этом случае произошло изменение уровня абстракции. Это означает выход за пределы цели исследования системы и, следовательно, вызывает прекращение декомпозиции.

Функциональная декомпозиция базируется на анализе функций системы. При этом ставится вопрос, что делает система, независимо от того, как она работает. Основанием разбиения на функциональные подсистемы служит общность функций, выполняемых группами элементов. С целью получения более полного представления о системе и её связях в структуру включают надсистему и составляющие её части [14; 15].

Чаще всего АСУ имеет древовидную структуру, когда из одной функциональной последовательности, выполняющей функцию получения конечного продукта, ответвляются иные функции, преимущественно функции контроля параметров системы [16].

В некоторых ситуациях выход из строя элемента, находящегося в горячем резерве, может повлиять на основной элемент.

Многократно зарезервированный «коренной» модуль при выходе из строя его элемента может как выводить из строя надёжностно, логически не связанную с ним последовательность, так и нести повышенную опасность в общем.

Рис. 2 иллюстрирует вышесказанное. Имеется система, выполняющая две функции. Первую функцию выполняют модули 1 и 2, вторую – 1 и 3. Причём модуль 2 дублирован.

Собственный отказ резервного элемента 2.2 модуля 2 не приводит к прекращению выполнения первой функции. Но этот отказ вызывает зависимый отказ модуля 3, и из-за него прекращается выполнение второй функции.

Таким образом, избыточность одного модуля предотвращает его отказ, но одновременно вызывает отказ других модулей системы и, следовательно, выводит другие функции из строя. Следовательно, при расчёте безотказности необходимо учитывать вероятность выхода системы из строя из-за зависимых отказов.

Расчёт надежности с учётом зависимых отказов. Учёт зависимых отказов весьма серьёзно изменяет модель надежности системы. К примеру, если учитывать возможность вызова зависимого отказа элементом модуля, в том числе и резервным, у нас появляется способ учесть вероятность того, что повышение степени резервирования будет уменьшать надежность системы, с определённой вероятностью при отказе разрушая другие модули. Рассмотрим иллюстрирующий это пример (рис. 3).

Возьмём систему, состоящую из двух последовательно соединённых модулей, причём второй модуль имеет n-кратное резервирование. Положим, что P_1 – вероятность безотказной работы элемента первого модуля; P_2 – вероятность безотказной работы элемента второго модуля.

Без учета зависимых отказов вероятность безотказной работы

$$P = P_1(1 - (1 - P_2)^n).$$

Теперь предположим, что каждый элемент второго модуля имеет вероятность вызвать отказ первого модуля. Положим, что P_d – вероятность вызова отказом второго модуля отказа первого.

Система будет исправна при следующих событиях:

S_1 – первый модуль собственно исправен;

S_2 – исправен хотя бы один из элементов второго модуля;

S_3 – не произошёл зависимый отказ первого модуля, вызванный элементом второго.

Следовательно, для безотказности системы должно быть верным следующее выражение:

$$S_1 \wedge S_2 \wedge S_3 .$$

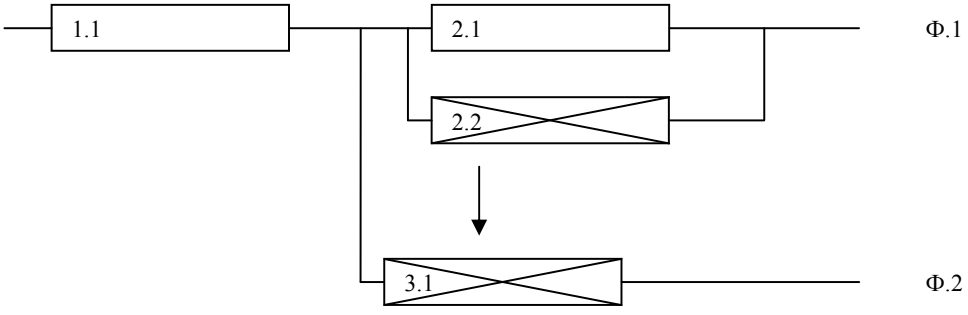

Рис. 2. Зависимый отказ в многофункциональной АСУ

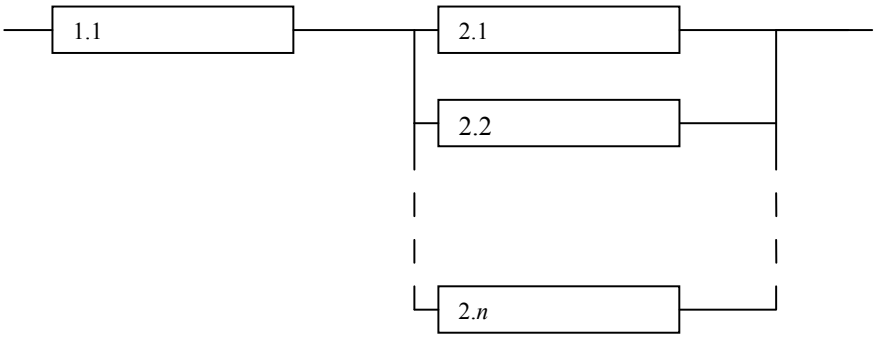

Рис. 3. Система с избыточностью и зависимыми отказами

Вероятность S_1 равна P_1, а вероятность события S_2 определяется по формуле

$$P_{s_2} = 1 - (1 - P_2)^n.$$

Вероятность события S_3 находится как обратная вероятность наступления двух событий одновременно (отказ элемента второго модуля и вызов им зависимого отказа):

$$P_{s_3} = 1 - (1 - P_2^n)P_d.$$

Вероятность безотказной работы с учетом этого вычисляется как

$$P = P_1(1 - (1 - P_2)^n)\cdot(1 - (1 - P_2^n)\, P_d). \qquad (1)$$

Заключение. Выражение (1) показывает, что при увеличении избыточности резервирования надежность системы с учётом зависимых отказов одновременно и растёт из-за резервирования, и убывает из-за наличия зависимых отказов. Следовательно, для повышения надежности систем следует применять иные, чем введение избыточных элементов, методы повышения надежности и вводить меры предотвращения опасных воздействий.

Таким образом, представленная формализация подхода к оценке надежности АСУ с зависимыми отказами позволяет построить модель, которая будет обладать большей гибкостью, учитывать влияние опасных ситуаций на безотказность многофункциональных АСУ.

Библиографические ссылки

1. Авиженис А. Н., Лапри Ж. К. Гарантоспособные вычисления: от идей до реализации в проектах // ТИИЭР. 1986. Т. 74, № 5. С. 8–21.

2. Курочкин Ю. А., Смирнов А. С., Степанов В. А. Надежность и диагностирование цифровых устройств и систем. СПб. : Изд-во Санкт-Петербургского ун-та, 1993. 320 с.

3. Ковалев И. В. Анализ проблем в области исследования надежности программного обеспечения: многоэтапность и архитектурный аспект // Вестник СибГАУ. 2014. № 3 (55). С. 78–92.

4. Рябинин И. А. Надежность и безопасность структурно-сложных систем. СПб. : Изд-во Санкт-Петербургского ун-та, 2007. 276 с.

5. Надежность технических систем : учеб. пособие / под общ. ред. Е. В. Сугака и Н. В. Василенко. Красноярск : НИИ СУВПТ, 2000. 608 с.

6. Охтилев М. Ю., Соколов Б. В. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М. : Наука, 2006. 410 с.

7. К вопросу оценки надежности АСУ с блокирующими модулями защиты / И. В. Ковалев [и др.] // Приборы. 2013. Вып. 6. С. 20–24.

8. Кузнецов П. А., Бесчастная Н. А., Бахмарева К. К. Модификация метода Волковича–Михалевича с целью оптимизации затрат при синтезе отказоустойчивых информационно-вычислительных систем // Вестник СибГАУ. 2012. № 6(46). С. 97–100.

9. ГОСТ Р 22.10.01–2001. Безопасность в чрезвычайных ситуациях. Оценка ущерба. Термины и определения [Электронный ресурс]. URL: http://vsegost.com/Catalog/64/6474.shtml (дата обращения: 12.02.2015).

10. Безопасность и надежность технических систем : учеб. пособие / Л. Н. Александровская [и др.] М. : Логос, 2004. 280 с.

11. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения [Электронный ресурс]. URL: http://vsegost.com/Catalog/11/11290.shtml (дата обращения: 12.02.2015).

12. Общие положения обеспечения безопасности ядерных энергетических установок судов : федер. нормы и правила в области использования атомной энергии НП-022-2000 (утв. постановлением Госатомнадзора РФ от 27 сентября 2000 г. № 5).

13. IAEA-TECDOC-probabilistic safety assessment [Электронный ресурс]. Vienna, Austria, 1992, 36 p. URL: http://www-pub.iaea.org/books/IAEABooks/908/Procedures-for-Conducting-Common-Cause-Failure-Analysis-in-Probabilistic-Safety-Assessment (дата обращения: 12.02.2015).

14. Родионов М. Г. Информационно-измерительные системы: теория систем и системный анализ : учеб. пособие. Омск : Изд-во ОмГТУ, 2011. 83 с.

15. Хорошев А. Н. Введение в управление проектированием механических систем : учеб. пособие. Белгород, 1999. 372 с.

16. Васильев А. А. Электрическая часть станций и подстанций : учебник для вузов / под ред. А. А. Васильева. 2-е изд. М. : Энергоатомиздат, 1991. 600 с.

References

1. Avizhenis A. N., Lapri Zh. K. [Guarantee-able calculations: from the idea to realization in projects]. *TIIER*. 1986, vol. 5, p. 8–21 (In Russ.).

2. Kurochkin Yu. A., Smirnov A. S., Stepanov V. A. *Nadezhnost' i diagnostirovanie tsifrovykh ustroystv i sistem* [Reliability and diagnostics of digital systems]. St.Petersburg, St.Petersburg University Publ., 1993, 320 p.

3. Kovalev I. V. [Analysis of the problems in the study of the reliability of the software: multi-stage and architectural aspects]. *Vestnik SibGAU*. 2014, No. 3(55), p. 78–92 (In Russ.).

4. Ryabinin I. A. *Nadezhnost' i bezopasnost' strukturno-slozhnykh sistem* [Reliability and safety of structural complex systems]. St.Petersburg, St.Petersburg University Publ., 2007, 276 p.

5. Sugak E. V, Vasilenko N. V. *Nadezhnost' tekhnicheskikh sistem. Uchebnoe posobie dlya vysshikh uchebnykh zavedeniy* [Reliability of technical systems. Study guide]. Krasnoyarsk, NII SUVPT Publ., 2000, 608 p.

6. Okhtilev M. Yu. Sokolov B. V. *Intellektual'nye tekhnologii monitoringa i upravleniya strukturnoy dinamikoy slozhnykh tekhnicheskikh ob"ektov* [Intelligent technologies for monitoring and management of the structural dynamics of complex technical objects]. Moscow, Nauka Publ. 2006, 410 p.

7. Kovalev I. V., Kuznetsov P. A., Zelenkov P. V., Shaydurov V. V., Bakhmareva K. K. [To the question of the reliability of automated control systems with blocking protection modules]. *Pribory*. 2013, vol. 6, p. 20–24 (In Russ.).

8. Kuznetsov P. A., Beschastnaya N. A., Bakhmareva K. K., Antamoshkin O. A., Antamoshkin A. N. [Modification of the Volkovich`s-Michalevi`c method to optimize costs in the synthesis of fault-tolerant information systems]. *Vestnik SibGAU*. 2012, No. 6(46), p. 97–100 (In Russ.).

9. *GOST R 22.10.01–2001. Bezopasnost' v chrezvychaynykh situatsiyakh. Otsenka ushcherba. Terminy i opredeleniya* [State Standart R 22.10.01–2001. Safety in emergencies. Damage assessment. Terms and definitions.] (In Russ.) Available at: http://vsegost.com/Catalog/64/6474.shtml (accessed 12.02.2015).

10. Aleksandrovskaya L. N., Aronov I. Z., Kruglov V. I., Kuznetsov A. G., Patrakov N. N., Sholom A. M. *Bezopasnost' i nadezhnost' tekhnicheskikh sistem. Uchebnoe posobie* [Safety and reliability of technical systems. Study guide]. Moscow, Logos Publ., 2004, 280 p.

11. *GOST 27.002–89. Nadezhnost' v tekhnike. Osnovnye ponyatiya. Terminy i opredeleniya* [State Standart 27.002–89. Reliability in the technology. Basic concepts. Terms and Definitions] (In Russ.) Available at: http://vsegost.com/Catalog/11/11290.shtml (accessed 12.02.2015).

12. RF Federal Standards and Rules in the Field of Nuclear Energy NP-022-2000 “General provisions to ensure the safety of nuclear powered vessels” 27.09.2000 (In Russ.) Available at: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=424308 (accessed 12.05.2015).

13. IAEA-TECDOC-probabilistic safety assessment, Vienna, Austria, 1992, 36 p. Available at http://www-pub.iaea.org/books/IAEABooks/908/Procedures-for-Conducting-Common-Cause-Failure-Analysis-in-Probabilistic-Safety-Assessment (accessed 12.02.2015).

14. Rodionov M. G. *Informatsionno-izmeritel'nye sistemy: teoriya sistem i sistemnyy analiz: uchebnoe posobie* [Information-measuring system: systems theory and systems analysis: a study guide] Omsk, OmGU Publ., 2011, 83 p.

15. Khoroshev A. N. *Vvedenie v upravlenie proektirovaniem mekhanicheskikh sistem: Uchebnoe posobie.* [Introduction to the management of designing mechanical systems: Study guide]. Belgorod, 1999, 372 p.

16. Vasil'ev A. A. *Elektricheskaya chast' stantsiy i podstantsiy Uchebnik dlya vuzov.* [Electric part of stations and substations. Study guide for high schools]. Moscow, Energoatomizdat Pabl., 1991, 600 p.