DOI: 10.25728/mlsd.2023.0197

МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

Лепешкин О.М., Остроумов О.А.
Военная орденов Ленина и Жукова краснознаменная академия связи имени С.М. Буденного, Санкт-Петербург, Россия
lepechkin1@yandex.ru, oleg-26stav@mail.ru

Аннотация. Для современных сложных технических систем критично нарушение их устойчивого функционирования. В работе предлагается подход обеспечения функциональной устойчивости такой системы, основанный на использовании процессного подхода и закона сохранения целостности системы. Полученная методология описывает процесс обеспечения функциональной устойчивости сложной технической системы.

Ключевые слова: функциональная устойчивость, процессный подход, закон сохранения целостности, критичность.

Введение

Современные сложные технические системы (СТС) функционируют в условиях неопределенности их состояния и воздействующих на них факторов, которые могут приводить к снижению функциональной устойчивости системы. Нарушение функционирования такой системы может привести к невозможности выполнения системой, объектом, в интересах которых функционирует сложная техническая система, требуемого перечня функций и задач. Такие системы становятся критичными. На критичность влияет также развитие систем, появление у них и их элементов новых функций. Возникает проблема обеспечения функциональной устойчивости СТС [1-4].

Под функциональной устойчивостью системы будем понимать ее свойство, характеризующее способность выполнять заданный перечень функций и задач системы в течении требуемого времени, в условиях воздействия на СТС различных факторов [5, 6].

К критически важным (критичным) СТС можно отнести объекты информационной инфраструктуры, химической, ядерной промышленности, военно-промышленного комплекса, объекты, влияющие на обеспечение правопорядка и т.д. Критичность обусловлена последствиями нарушения функционирования таких системы, объектов, поэтому при рассмотрении таких объектов необходимо учитывать риски и минимизировать их [7, 8].

СТС должна работать на гарантированное выполнение требуемого перечня функций и задач, своего предназначения, а также обеспечения отсутствия возникновения в системе конфликтов, обусловленных потребностями вышестоящей системы и невозможности выполнить эти потребности СТС, что определяет актуальность исследования.

Вопросами исследования устойчивости сложных систем занимаются давно. Традиционно устойчивость рассматривается с позиции надежности [9, 10], живучести [11-14], помехоустойчивости [15-17] и киберустойчивости [18-20]. Показатели оценки устойчивости, как правило, носят вероятностный характер и не показывают способность системы в любой момент выполнить требуемый набор функций и задач.

1. Структура СТС

Основой любой СТС, системы связи, системы управления, информационной системы и т.д. является ее структура, определяемая элементами системы, связями между ними и характеристиками этих связей (рис. 1) [1, 5, 21]. На основании структуры системы строится процесс функционирования. Физическая структура системы является основой функциональной структуры. Характер выполняемых задач, качество их выполнения, взаимовлияние друг на друга, а также целевое предназначение системы определяет функциональную структуру системы.

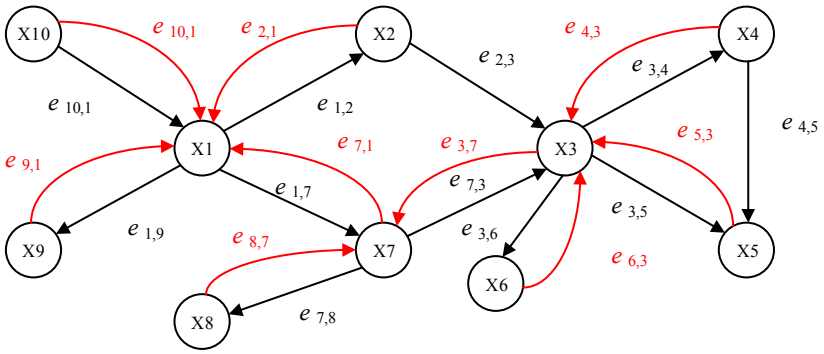

Рис. 1. Пример графического представления структуры СС G(X, L)

Функциональную структуру СТС представим в виде модели процесса функционирования системы, включающей цели, требования, функции, задачи и ресурсы (рис. 2). В работе под ресурсами понимается сами физические средства системы, а также производные их функционирования. Симбиоз человека и технических средств позволяет системе выполнять свое целевое предназначение.

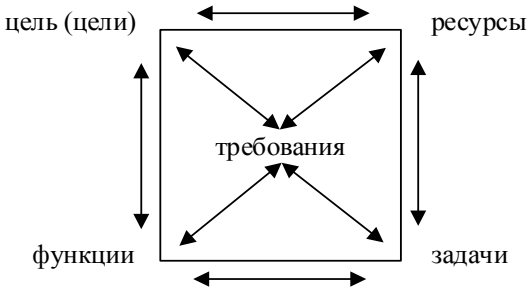

Рис. 2. Концептуальная модель процесса функционирования системы

Современные СТС, их элементы функционируют в условиях неопределенности их состояния, на которое оказывают влияние различные дестабилизирующие факторы, как внешние, так и внутренние. Быстрота процессов в системе, необходимость обеспечения выполнения целевого предназначения СТС, а также потребности вышестоящей системы и лиц, принимающих решение, в знаниях о системе и процессах в ней в режиме реального времени определяют необходимость выявления и устранения конфликтов.

2. Выявление конфликтов

В процессе функционирования СТС выполняется определенный ограниченный набор функций и задач. Могут возникать нештатные ситуации, обусловленные усложнением обстановки, воздействием какого-либо фактора, появлением новых задач в системе, выходом из строя элементов системы и необходимости перераспределения задач. Необходимо своевременно выявлять такие ситуации и реагировать на них, отсутствие которого может привести к саморазрушению системы [22, 23]. Возникновение конфликта в системе обусловлено невозможностью или снижением качества выполнения функции, задачи. В первую очередь на это влияет наличие ресурса и поддержание его работоспособности на требуемом уровне. Могут возникать конфликты, обусловленные отсутствием ресурса, возможности доступа к нему, не готовности его к использованию, использованию его для выполнения других задач.

Задачи, невыполнение которых приведет к невыполнению целевого предназначения СТС являются критическими для системы.

Под конфликтом понимается дефицит ресурсов при выполнении регламентов СТС, возникающий в случае изменения обстановки и приводящий (могущий привести) к нарушению ее функционирования и приводящий (могущий привести) к срыву выполнения целевого предназначения СТС.

Основным способом выявления конфликтов в СТС является реализация обратной связи в процессе управления и контроля функционирования системы. В качестве инструмента контроля предлагается

использовать профиль функционирования СТС. Несоответствие профиля, заданного планом и профиля, формируемого при функционировании СТС будет определять конфликт в системе.

Профиль функционирования системы совокупность взаимосвязанных характеристик системы (сети) связи, правил, описывающих процесс функционирования системы (сети) и характеризующих ее целевое предназначение на ограниченном отрезке времени [24].

Для построения профиля функционирования СТС требуется формализация системы с точки зрения процессного подхода и рассмотрения каждого элемента методологии Деминга-Шухарта с точки зрения рассматриваемого объекта исследования. Наряду с этим, возникает потребность определения связи между целевым предназначением системы с его структурой и процессом функционирования, для чего предлагается использовать закон сохранения целостности, предложенный Бурловым В.Г. [23, 25], и включающий три элемента: объект, действие и предназначение.

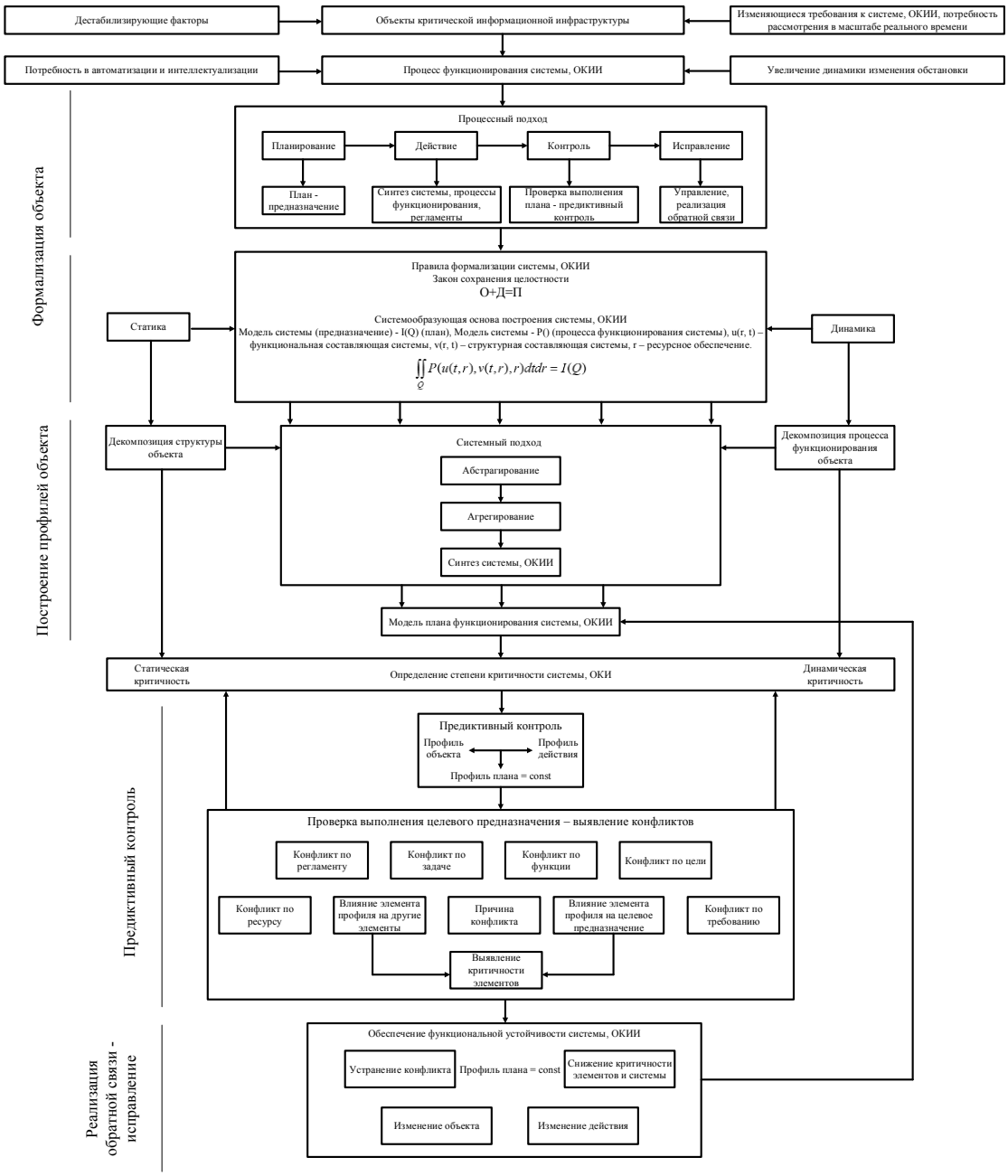

Рис. 3. Структура методологии обеспечения функциональной устойчивости СТС

Для выполнения требуемого целевого предназначения объекта необходимо на основе системного подхода провести декомпозицию объекта, декомпозицию действия, абстрагирование и агрегирование, а также синтез объекта для выполнения целевого предназначения за счет имеющего ресурса системы**.**

Контроль процесса функционирования СТС осуществляется с использованием сканера и запросов в БД, а также оценки выполнения плана системой. Через систему контроля реализуется обратная связь путем предоставления информации и состоянии системы, а также выполнении плана лицам, принимающим решение.

Процесс контроля функционирования СТС осуществляется через последовательные проверки ресурсов, задач, функций, требований, целей СТС, а также анализа критичности самой системы и ее элементов с помощью запросов в систему [5, 6, 26].

3. Методология обеспечения функциональной устойчивости

Структурная схема базовых элементов методологии обеспечения функциональной устойчивости СТС показана на рисунке 3.

Основой методологии является математический аппарат теории иерархических систем, теории графов, теории множеств и теории матриц, позволяющих формализовать функциональную составляющую системы связи, алгебры логики предикатов, позволяющей определить операции над элементами СТС и теории управления рисками, позволяющей производить синтез СТС на основе ее функционального предназначения для обеспечения функциональной устойчивости и гарантированного выполнения целевого предназначения.

Системообразующей основой методологии является интеграл функции от векторов структурной и функциональной составляющей СТС, зависящие от множества задач, реализующих процесс функционирования системы, потенциала поля плана, через пространственно-разнесенные ресурсы и время.

Формализация проблемы представляет собой функцию зависимости совокупности модели объекта и модели действия, необходимых для реализации выполнения целевой функции системы, за счет ее ресурсов, которая представляет собой план функционирования системы.

5. Заключение

Проблема обеспечения функциональной устойчивости сложных системы является актуальной. Актуальность обусловлена потребностями и зависимостью других систем, лиц, предприятий, отраслей промышленности, государства от выполняемых ими функций и задач. Нарушение функциональной устойчивости из-за воздействия различных дестабилизирующих факторов может привести к невыполнению функций вышестоящей системы. Формализация объекта исследования в рамках процессного подхода позволяет гарантированно достигать целевое предназначение системы за счет контроля и реализации обратной связи в процессе функционирования СТС. Использование в методологии закона сохранения целостности позволяет объединить в единое целое действие и объект, операции над которыми позволяют выполнять заданное планом целевое предназначение. Для формализации целевого предназначения – плана функционирования СТС, предлагается использовать профиль функционирования системы, который выступает в качестве основного средства контроля процесса функционирования СТС. Выявление и устранение конфликтов в системе в любой момент времени позволит выполнить системе целевое предназначение и обеспечить ее функциональную устойчивость.

Литература

1. *Иванов С. А.* Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. №9. с. 86-90.

2. *Дурняк Б.В., Машков О.А., Усаченко Л.М., Сабат В.И.* Методология обеспечения функциональной устойчивости иерархических организационных систем управления // Сборник научных статей: Институт проблем моделирования в энергетике, НАН Украины. В. 48. 2008. – с. 3-21.

3. *Королев А.Н.* Функциональная устойчивость навигационно-информационных систем // Известия вузов. Приборостроение. 2018. Т. 61. № 7. С. 559-565. DOI: 10.17586/0021-3454-2018-61-7-559-565.

4. *Тарасов А.А.* Функциональная реконфигурация отказоустойчивых систем: монография. – М.: Логос, 2012. – 152 с.

5. *Остроумов О. А.* Проблема обеспечения функциональной устойчивости систем критически важных объектов // Электросвязь. № 1. 2022. с. 14-18.

6. *Кондрашов Ю. В., Сатдинов А. И., Синюк А. Д., Остроумов О. А.* Концептуальная модель контроля функций системы связи для выявления конфликтных ситуаций // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16. №5. с. 21-27.

7. *Lepeshkin O.M., Ostroumov O.A., Sinyuk A.D.* The communication system functional stability with critical objects // В сборнике: Проблемы управления безопасностью сложных систем. Материалы XXIX международной научно-практической конференции. Москва, 2021. – с. 80-85.

8. *Петренко С. А.* Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН. Т. 41. 2009. с. 175-193.

9. *El-Mowafy Ahmed* (2019). On detection of observation faults in the observation and position domains for positioning of intelligent transport systems. Journal of Geodesy. p. 93. doi: 10.1007/s00190-019-01306-1.

10. *Falahati B., Fu Y.* Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies. in IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1677-1685, July 2014. doi: 10.1109/TSG.2014.2310742.

11. *Аллакин В. В.* Модель идентификации технического состояния устройств информационно-телекоммуникационных сетей общего пользования подсистемой сетевого мониторинга. Системы управления, связи и безопасности. 2021. № 5. С. 40-64. doi: 10.24412/2410-9916-2021-5-40-64.

12. *Грудинин И. В., Суровикин С. В.* Управление ресурсами информационно-управляющей подсистемы АСУ огнем в интересах обеспечения ее живучести // Известия Института инженерной физики. 2016. № 3 (41). С. 57-62.

13. *Brauner F., Claßen M., Fiedrich F.* (2018) Competence as Enabler of Urban Critical Infrastructure Resilience Assessment. In: Fekete A., Fiedrich F. (eds) Urban Disaster Resilience and Security, The Urban Book Series Springer, Cham. doi: doi.org/10.1007/978-3-319-68606-6_11.

14. *Haring I., Ebenhoch S., Stolz A.* Quantifying Resilience for Resilience Engineering of Socij Technical Systems. Springer International Publishing. 2016. pp. 21-58. doi: 10.1007/s41125-015-0001-x.

15. *Савищенко Н. В. Остроумов О. А.* Расчет оптимального и рационального числа ветвей разнесения в каналах связи с аддитивным белым гауссовым шумом и общими замираниями Райса-Накагами // Информационно-управляющие системы. №6 (79). 2015. С. 71-80.

16. *Pashintsev V.P., Chipigs A.F., Koval S.A., Skorik A.D.* Analytical method for determining the interval of spatial correlation of fading in single-beam decameter radio line. Telecommunications and Radio Engineering. 2021. Т. 80. № 2. pp. 89-104.

17. *Макаренко С. И.* Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.

18. *Haque M. A., Shetty S., Krishnappa B.* ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems, 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 2019, pp. 273-281, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.

19. *Haque M. A., De Teyou G. Shetty K., S., Krishnappa B.* Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights, 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 2018, pp. 25-30, doi: 10.1109/ISI.2018.8587398.

20. *Kotenko I., Saenko I., Lauta O., Karpov M.* Methodology for management of the protection system of smart power supply networks in the context of cyberattacks. Energies, Vol. 14, № 18, 2021. doi: 10.3390/en14185963.

21. *Одоевский С. М., Лебедев П. В.* Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой // Системы управления, связи и безопасности. 2021. № 1. С. 152-189. DOI: 10.24411/2410-9916-2021-10107.

22. *Коцыняк М.А., Лаута О.С., Нечепуренко А.П.* Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1-2 (127-128). С. 58-62.

23. *Burlov V., Uzun O., Grachev M., Faustov S., Sipovich D.* Web-based power management and use model (2021). Advances in Intelligent Systems and Computing, 1258 AISC, pp. 629-641. doi: 10.1007/978-3-030-57450-5_54.

24. *Лаута О. С, Баленко Е. Г., Федоров В. Х., Лепешкин О. М., Остроумов О. А.* Метод построения профиля функционирования сложной технической системы // Инженерный вестник Дона. 2023. №2. URL: ivdon.ru/ru/magazine/archive/n1y2023/8183 (дата обращения: 10.05.2023).

25. *Бурлов В.Г.* Теоретические основы управления риском. – СПб.: НПО «Стратегия будущего», 2009. – 270 с.

26. *Davliatova M., Brechko A., Lvova N., Sorokin M.* Enterprise functioning quality management under conditions of destructive program actions // In: IOP Conference Series: Materials Science and Engineering. 2019. p. 012131.