Проблема автоматизации анализа функциональной стабильности критичных систем управления в промышленности

П.В. Сундеев (КГТУ)

Предложен подход к автоматизации анализа свойств функциональной стабильности информационных систем, используемых при управлении критичными промышленными объектами, на основе интеграции методов системного анализа и современных технологий.

В результате повсеместной информатизации критичные функции управления передаются под контроль автоматизированных систем (АС). Этот процесс порождает проблему обеспечения функциональной стабильности (ФС) критичных систем управления (КСУ) таких, как системы управления: опасными производствами и объектами атомной энергетики; космическими полетами, воздушным или железнодорожным движением; военного назначения; органов государственной власти и др. Большинство систем этого класса характеризуются критичностью решаемых функциональных задач, территориальной и информационной распределенностью, концентрацией информации ограниченного доступа, использованием биологических и электронных технологий обработки информации, семантической доступностью для информационного воздействия, временными ограничениями цикла управления и другими свойствами, которые определяют сложность ТП обработки информации и потенциальную опасность при нарушении их ФС.

Границы управляемости свойств ФС КСУ

КСУ можно отнести к сложноорганизованным эргатическим информационным системам, использующим биологические и компьютерные технологии обработки информации, для которых характерно наличие технологических участков с автоматическим, автоматизированным и интеллектуальным управлением (рис. 1).

Область возможного управления ФС сложной системы определяется на основе иерархической стратификации структуры сложных систем и целевых функций ее подсистем (рис. 2).

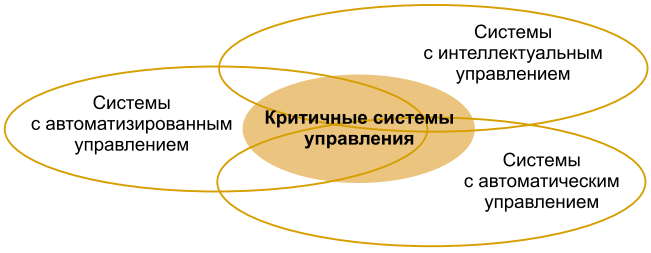

Рис. 1. Критичные информационные системы в иерархии сложности эргатических систем

Иерархическая стратификация целевых функций подсистем сложной системы с управлением представлена в табл. 1.

Анализ возможных дестабилизирующих факторов, структуры и целевых функций сложных информационных систем позволяет сделать заключение о том, что ФС для исследуемого класса систем зависит от трех аспектов: состояния функциональной безопасности, уровня технологической надежности и функциональности элементов и подсистем.

Вопросы надежности и функциональности технических систем достаточно полно исследованы, изложены в теории надежности, прикладных теориях и учитываются на практике при проектировании АС. Влияние аспекта функциональной безопасности на ФС менее изучено и наиболее актуально для анализа в конфликтных средах, поскольку он связан с целенаправленным воздействием конкурирующих систем. Поэтому анализ ФС КСУ целесообразно ограничить аспектами функциональной безопасности с учетом требований по функциональности и надежности.

Повышение адекватности моделирования информационных процессов и систем

Одной из трудноразрешимых задач системного анализа сложных КСУ является повышение адекватности моделей информационных процессов и систем их реальным прототипам.

Предлагается три метода решения этой задачи: трехуровневое описание взаимодействия информационных

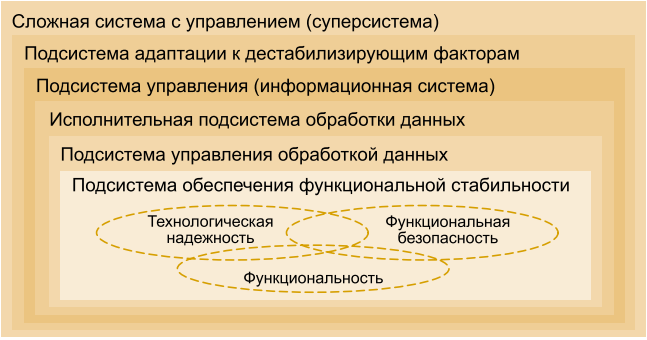

Рис. 2. Иерархическая стратификация структуры сложной системы с управлением

Таблица 1. Иерархическая стратификация подсистем и целевых функций

Элементы иерархической структуры сложной системы с управлением	Иерархия целевых функций	Иерархия информационных функций	Результат (цель)
Сложная система с управлением (суперсистема)	Обеспечение структурной стабильности системы	–	Целостность системы в течение жизненного цикла
Подсистема адаптации к дестабилизирующим факторам	Адаптация системы к новым условиям с минимальными структурными изменениями	Управление свойствами суперсистемы	Суперсистема с новыми свойствами, обеспечивающими целостность
Подсистема управления (информационная система)	Моделирование суперсистемы и внешней среды	Управление информационными моделями суперсистемы и внешней среды (реализация функциональных алгоритмов)	Модель структуры суперсистемы с новыми свойствами
Исполнительная подсистема обработки данных	Реализация процедур по обработке информационных моделей (данных)	Управление обработкой данных (реализация исполнительных алгоритмов)	Хранение, передача, интерпретация на физическом уровне и трансляция данных
Подсистема управления обработкой данных	Моделирование процессов обработки данных	Управление исполнительной подсистемой обработки данных	Согласование процедур информационного процесса
Подсистема обеспечения функциональной стабильности информационной системы	Обеспечение обработки данных при дестабилизирующих информационных воздействиях	Управление состоянием информационной подсистемы	Функциональная стабильность информационной подсистемы
Подсистема обеспечения технологической надежности	Обеспечение технологической надежности элементов и подсистем	Управление надежностью информационной технологии	Работоспособность элементов и подсистем
Подсистема обеспечения функциональности	Обеспечение функциональности элементов и подсистем	Управление информационными функциями	Доступность информационных сервисов
Подсистема обеспечения функциональной безопасности	Обеспечение функциональной безопасности	Управление функциональной безопасностью	Конфиденциальность и целостность информации

систем; визуализация процесса декомпозиции исследуемых систем на основе использования современных компьютерных технологий; автоматизация процесса синтеза математических моделей информационных процессов и систем из объектно-ориентированных диаграмм на основе разработанного математического аппарата формального описания состояний системы.

Первый метод основан на предположении, что любое информационное взаимодействие между сложными системами реализуется последовательно на физическом, синтаксическом и семантическом уровнях взаимодействия (рис. 3). Причем, системы должны иметь соответствующие интерфейсы для взаимодействия на каждом из уровней[1]. Разделив систему на информационные объекты (функциональные модули), и описав все их интерфейсы взаимодействия, можно декларировать относительную полноту множества учитываемых отношений между элементами системы, которые определяют ее поведение и являются предметом анализа функциональной стабильности.

Второй метод повышения достоверности моделирования основан на визуализации процесса построения моделей системы в виде объектно-ориентированных

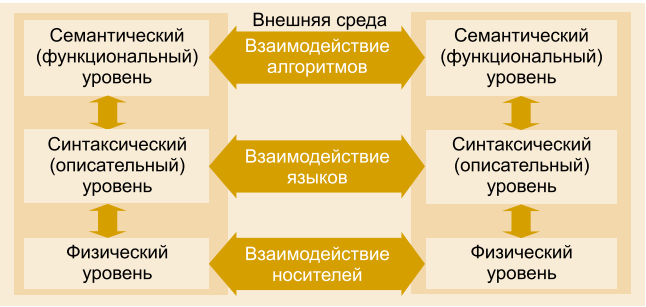

Рис. 3. Модель информационного взаимодействия сложных систем

диаграмм. Использование универсального языка моделирования UML и поддерживающих его программных инструментальных средств анализа и проектирования сложных систем позволяют формализовать и автоматизировать процесс синтеза интегрированных моделей системы, снизить зависимость от субъективности аналитика и его ошибок, и, как следствие, повысить адекватность моделей. Для возможности декомпозиции информационных систем на информационные объекты и модули необходимо использовать метод классификации элементов системы и связей между ними по информационно-функциональному принципу.

Третий метод повышения достоверности моделирования основан на генерации математических моделей информационной системы из объектно-ориентированных диаграмм. Для его реализации предлагается использовать разработанный математический аппарат формального описания состояний информационной системы[1].

Основные положения теории функциональной стабильности

Модель реализации угроз ФС при информационном взаимодействии систем демонстрирует отношения на трех уровнях взаимодействия, через которые возможна дестабилизация системы (рис. 4).

Существенным фактором, представленным в модели, является выделение в структуре информационной системы функциональных алгоритмов, предназначенных для интерпретации семантики объектов управления, и исполнительной подсистемы обработки данных, которая предназначена для реализации информационных услуг по хранению, передаче и преобразованию данных по запросам функциональных алгоритмов. Реализация угроз возможна на любом уровне взаимодействия. Кроме того, возможно взаимодействие функцио-

[1] Симанков В.С., Сундеев П.В. Системный анализ функциональной стабильности критичных информационных систем. Монография / Под ред. В.С. Симанкова. Институт современных технологий и экономики. Краснодар, 2003.

нальных алгоритмов, если они имеют интерфейсы и функции, характерные для исполнительной подсистемы по обработке данных. Представленная модель позволяет говорить о системе воздействия дестабилизирующих факторов для анализа ФС КСУ.

На ФС КСУ оказывают существенное влияние особенности используемых технологий обработки информации. В КСУ используются две полнофункциональные технологии обработки информации: биологическая и электронная. Однако существенным различием между ними с точки зрения обеспечения ФС является не вид носителя информации, а синтаксический метод представления знаний и данных. Рассмотренная ранее интерпретация модели угроз ФС характерна для технологий обработки информации, представленной на контекстно-независимых языках. В этом случае в системе существуют отдельные информационные объекты, с которыми возможно взаимодействие через несанкционированные информационные каналы. К таким объектам относятся технологические участки КСУ, использующие компьютерные технологии обработки данных. Для систем с контекстно-зависимым представлением информации, к которым относится человек и перспективные интеллектуальные компьютерные системы, основанные на "нейросетевых" технологиях, внешнее дестабилизирующее информационное воздействие можно реализовать только через штатные входы/выходы системы. Угрозы, направленные на дестабилизацию исполнительной подсистемы обработки данных, для этого случая не актуальны, если она реализована по принципу иерархического предоставления информационных услуг и выполнены требования по информационной безопасности. Очевидно, что функциональная стабильность системы может быть обеспечена при учете парадигмы трехуровневого информационного взаимодействия, системы дестабилизирующих факторов и реализации угроз, а также положений теории ФС.

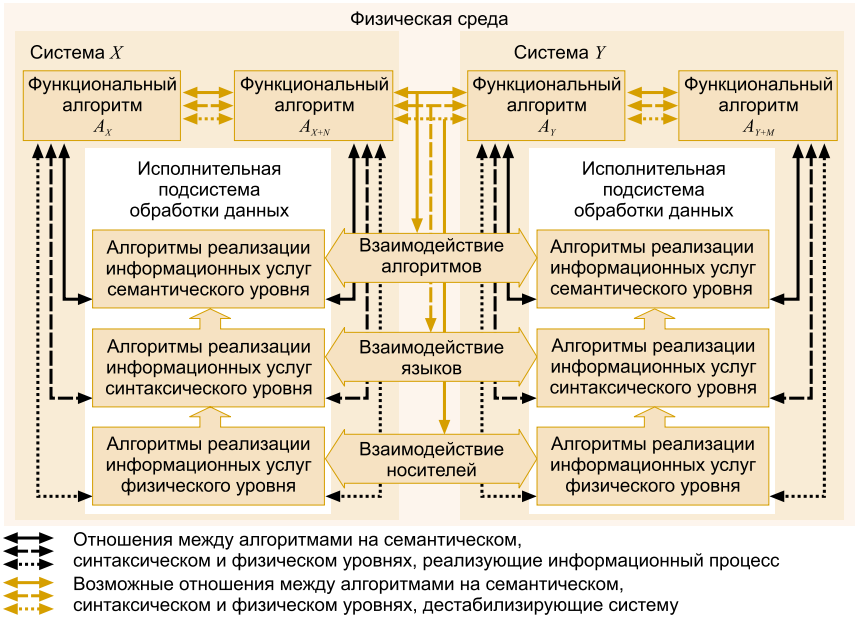

Рис. 4. Модель реализации угроз функциональной стабильности при информационном взаимодействии систем

Принципы построения архитектуры и организации информационного процесса для функционально стабильных систем должны определяться стратегией контроля информационного доступа к функциональным интерфейсам информационных объектов. В системе выделяются информационные объекты, способные выполнять стандартные функции по обработке информации на трех уровнях информационного взаимодействия. Функциональность объектов определяется наличием у них открытых интерфейсов для каждого из уровней. Возможность взаимодействия определяется нахождением объектов в одной зоне информационного доступа и наличием у них парных интерфейсов. Поскольку уровни взаимодействия иерархичны, то возможность взаимодействия на вышестоящем уровне определяется наличием его на всех нижестоящих уровнях. Зоны физического, синтаксического или семантического доступа определяются архитектурой системы и средствами разграничения доступа на соответствующих уровнях.

Система считается функционально стабильной, если в ходе информационного процесса ее информационные объекты находятся в разрешенных для них зонах информационного доступа. Система считается функционально нестабильной, если в ходе информационного процесса в зону возможного взаимодействия попадают объекты, отношения между которыми считаются опасными для функционирования системы на данном уровне. Эти положения являются критерием оценки ФС КСУ, основанными на регламентации логики информационно-функционального взаимодействия элементов и подсистем.

Анализ ФС на системном уровне заключается в поиске траекторий перехода системы в опасные состояния, что является основной проблемой при проектировании, эксплуатации и модернизации КСУ, которые должны иметь определенный уровень ФС. Для определения всех или почти всех (т.е. относительно полного множества) траекторий перехода системы в опасные состояния необходима методология, позволяющая моделировать архитектуру и информационные процессы систем, формализовать состояния любых информационных систем, проводить анализ ФС.

Методологический подход к автоматизации анализа ФС КСУ

Методология построения моделей и анализа ФС КСУ включает несколько этапов (рис. 5).

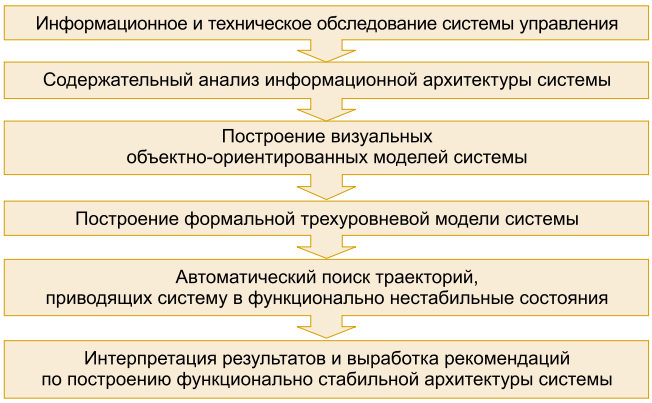

Рис. 5. Последовательность анализа ФС КСУ

На первом этапе проводится информационное и техническое обследование системы управления с целью выявления информационных объектов и отношений между ними, описания информационных интерфейсов на трех уровнях взаимодействия.

Содержательный анализ информационной архитектуры системы проводится с целью структуризации исходных данных для последующего моделирования.

Сложность объекта исследования и размерность модели требуют применения специальных методов моделирования. Наиболее перспективным для данного случая является применение методологии объектно-ориентированного анализа и проектирования сложных систем, поддерживаемого CASE-средствами, которые позволяют визуализировать и автоматизировать процесс построения модели.

Построение интегрированных визуальных моделей информационной системы основано на возможности представления архитектуры системы в виде мультиграфа, который изображается в виде объектно-ориентированных диаграмм. Вершинами графа являются информационные объекты и классы системы, дуги нагружаются информационными отношениями. Взаимодействие объектов и классов в ходе информационного процесса ограничивается архитектурой системы, интерфейсами объектов и средствами разграничения доступа, которые логически или физически разделяют систему на физические, синтаксические и семантические зоны. Нахождение информационных объектов в одной зоне информационного доступа при совпадении соответствующих интерфейсов предполагает возможность их взаимодействия и, следовательно, возможность изменения состояния системы.

Задачей анализа ФС КСУ является нахождение всех возможных траекторий информационного процесса, способных привести систему в опасные состояния. Для ее решения необходимо перевести визуальные диаграммы КСУ на язык математической логики, описав объекты, их интерфейсы, опасные и безопасные состояния и правила перехода состояний в виде предложений формальной логики исчисления предикатов первого порядка. Граф состояний модели КСУ представляет собой направленный граф переходов, отображающий изменения состояния исследуемой КСУ, т.е. ее поведение, определяемое архитектурой системы и технологией обработки данных (рис. 6). Вершинами этого графа являются элементы из множества состояний, а ребрами – из множества событий.

Решение прямой задачи анализа ФС КСУ состоит в определении отсутствия траекторий, приводящих систему в опасные состояния, при установлении конкретных типов информационных отношений между информационными объектами.

Генерация теорем и аксиом в виде формальных высказываний математической логики исчисления предикатов может осуществляться автоматически из объектных диаграмм и диаграмм классов на основе

Рис. 6. Граф возможных состояний критичной информационной системы

исходных данных о структуре ориентированного графа, свойствах его вершин и дуг, полученных на этапе объектно-ориентированного анализа КСУ, при наличии совместимого с CASE-средством (например, Rational Rose) компилятора для языка типа Пролог.

Рассмотренный подход к автоматизации анализа свойств критичных систем управления применялся в ходе проектирования функционально стабильных информационных систем предприятий связи и органов государственной власти. Предложенный научно-методический аппарат может быть использован для разработки или проверки функциональной стабильности информационных систем любых промышленных объектов, на которых необходимо контролировать информационные риски с целью обеспечения стабильности критичных производственных процессов.

Сундеев Павел Викторович *– канд. техн. наук, доцент кафедры компьютерных технологий и информационной безопасности Кубанского государственного технологического университета.*

Контактный телефон (8612) 40-16-07. E-mail: sundeev@kuban.mts.ru