УДК 004.9

СИТУАЦИОННОЕ МОДЕЛИРОВАНИЕ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ПРОМЫШЛЕННО-ПРИРОДНЫХ СИСТЕМ

А. Я. Фридман[а], *доктор техн. наук, профессор*
В. Г. Курбанов[б], *канд. физ.-мат. наук, старший научный сотрудник*
[а]*Институт информатики и математического моделирования технологических процессов Кольского научного центра РАН, Апатиты, РФ*
[б]*Институт проблем машиноведения РАН, Санкт-Петербург, РФ*

Введение: *ранее развитый одним из авторов ситуационный подход к моделированию состояния промышленно-природных систем и сопоставлению альтернативных структур их реализации обобщен на задачи разработки логических моделей структурной надежности и безопасности функционирования подобных систем. Цель исследования состоит в разработке методики построения логических моделей структурной надежности и безопасности функционирования промышленно-природных систем на основе модели их нормального функционирования.* ***Результаты:*** *моделирование опасных и критических ситуаций выполняется как «расширение» моделей нормального функционирования и использует ту же программную среду. Принципиальное отличие предложенного подхода от известных методов создания логических моделей надежности и безопасности сложных систем с опорой на структурную схему состоит в том, что детальность моделирования повышена до отдельного материального или информационного сигнала, которым могут обмениваться элементы системы. Существенно повышена достоверность результатов анализа логической модели за счет более полного учета взаимосвязей элементов системы, особенно в части выявления сложных (многократных) комбинаций отказов этих элементов, которые приводят к наиболее тяжелым последствиям.* ***Практическая значимость:*** *использование единой инструментальной среды и методологии для моделирования как нормальных, так и критических режимов функционирования промышленно-природных систем позволяет аккумулировать разнородные знания об объекте исследования в целях их комплексного применения.*

Ключевые слова *— ситуационное моделирование, логическая модель надежности, логическая модель безопасности, инициирующее событие, логико-вероятностный метод.*

Введение

Большинство крупных действующих и проектируемых технических комплексов и производств представляют собой сложные промышленно-природные системы (ППС). При этом вопросы выбора рациональной структуры такого объекта (или структур составных частей) актуальны на всех этапах его жизненного цикла. Для оценки вариантов, альтернатив реализации (управления структурой) ППС ранее была разработана ситуационная система моделирования [1, 2], ядро которой — ситуационная концептуальная модель (СКМ).

Надежность и безопасность функционирования ППС относятся к важным критериям оценки эффективности систем такого класса. Существуют различные подходы к формализации этих критериев. Одно из плодотворных направлений — логико-вероятностный метод [3–6]. В данной статье рассматривается способ интеграции ситуационного моделирования и логико-вероятностного метода в целях формирования ситуационной системы для исследования надежности и безопасности ППС.

Основы логико-вероятностного метода

Структурно-сложными системами (ССС) считаются [3] такие системы, которые при формализации не сводятся к последовательным, параллельным или древовидным структурам, а описываются сценариями сетевого типа с циклами.

Построение логической модели надежности (ЛМН) ССС начинается с описания условия работоспособности системы. Это описание выполняется графически, в виде структурной схемы системы (элементов и связей).

В ЛМН используются логические (двоичные) переменные:

$x_i = 1$ ($x_i' = 0$), если элемент x_i работоспособен, и $x_i = 0$ ($x_i' = 1$), если этот элемент отказал. В настоящем разделе штрих обозначает операцию отрицания.

Соответственно определяются:

$P\{x_i = 1\} = R_i$ — вероятность безотказной работы элемента x_i;

$P\{x_i' = 1\} = Q_i$ — вероятность отказа элемента x_i.

Конкретные значения логических переменных формируют вектор состояния системы: $\mathbf{x} = (x_1, x_2, ..., x_m)$.

На основе структурной схемы составляется функция алгебры логики (ФАЛ), связывающая состояние элементов с состоянием системы и называемая функцией работоспособности системы (ФРС) или структурной функцией системы: $y = y(x_1, x_2, ..., x_m)$.

Предполагается, что ССС находится только в двух состояниях: состоянии полной работоспособности ($y = 1$) или состоянии полного отказа ($y = 0$).

Для систем, у которых замена отказавшего элемента на исправный не приводит к отказу системы, ФРС монотонна. Всякая ФАЛ, включающая только операции конъюнкции и дизъюнкции (без отрицания), задает некоторую монотонную функцию. Для монотонных структур ФРС можно записать в виде дизъюнкции кратчайших путей успешного функционирования (конъюнкций минимально необходимых наборов работоспособных элементов) или в виде конъюнкции минимальных сечений отказов системы (конъюнкций минимально необходимых наборов неработоспособных элементов).

В начале построения логической модели безопасности (ЛМБ) ССС описывается сценарий опасного состояния в терминологии работы [3] или, в более употребительной терминологии, сценарий аварии. Элементы сценария — это инициирующие (опасные) события или инициирующие условия (ИС или ИУ), а также связи (причинно-следственные) между ними. Ниже для краткости используется только термин «ИС». Сценарий в ЛМБ, как и структурная схема в ЛМН, разрабатывается в графической форме. Отмечается, что «описание сценария представляет наибольшую трудность и является творческим процессом, который не имеет алгоритма» [3]. При построении ЛМБ принимается:

$z_i = 1$, если ИС z_i произошло, и $z_i = 0$, если не произошло.

Соответственно:

$P\{z_i = 1\} = \text{О}_i$ — вероятность опасности от ИС z_i;

$P\{z_i' = 1\} = \text{Б}_i$ — вероятность безопасности от ИС z_i.

На основе графического описания (сценария) составляется аналитическое описание (ФАЛ) в форме логической функции опасности системы, аргументами которой выступают инициирующие события z_i, приводящие к чрезвычайной ситуации: $y = y(z_1, z_2, ..., z_m)$.

Инвертируя функцию опасности системы, получаем функцию безопасности системы: $y' = y'(z_1', z_2', ..., z_m')$.

Монотонная функция опасности системы содержит дизъюнкции кратчайших путей опасного функционирования (конъюнкций минимально необходимых наборов ИС) либо конъюнкции отрицаний минимальных сечений предотвращения опасности (конъюнкций минимально необходимых наборов отрицаний ИС).

Таким образом, ЛМН и ЛМБ записываются в форме ФАЛ. Затем полученные ФАЛ преобразуются в вероятностные функции надежности и безопасности системы [3].

Итак, необходимым условием построения ЛМН или ЛМБ ССС является описание структуры системы или выявление сценария аварии. Этап формирования этих исходных структур и особенно сценариев — как для действующих, так и (тем более) для проектируемых систем — наиболее сложный, творческий и, как следствие, наименее автоматизированный и обоснованный. Поскольку построение указанных структур осуществляется «вручную», эвристически, детальность и достоверность полученных схем ограничены возможностями экспертов. Трудности многократно возрастают, когда надо сгенерировать и исследовать различные варианты построения системы.

По мнению авторов, остроту этих проблем можно снизить в рамках представленного далее ситуационного подхода к моделированию и управлению структурой ППС.

Ситуационная концептуальная модель ППС

Ситуационная концептуальная модель включает в себя три множества элементов: объекты, процессы и ресурсы (данные), — на которых определены связи и отношения. Иерархия объектов отражает их организационные взаимоотношения. Каждому объекту может приписываться набор процессов, моделирующих преобразование входных ресурсов в выходные. В качестве ресурса в СКМ рассматривается любой материальный или информационный сигнал, которым обмениваются элементы модели. Ресурсы атрибутированы списками допустимых значений. Списки используются и для числовых, и для ранжированных переменных с целью избежать вычислительных проблем, связанных с малыми изменениями данных, и обеспечить их совместную расчетно-логическую обработку. Последняя реализуется посредством встроенной экспертной системы, которая может быть назначена исполнителем любого ресурса или процесса СКМ. Подлежащие сопоставлению альтернативы реализации ППС вносятся в СКМ на этапе ее конструирования путем декомпозиции некоторого объекта на подобъекты по типу «или» либо заданием альтернативных наборов ресурсов на входе некоторого процесса. С помощью отношений иерархии любой составной объект СКМ однозначно сопоставляется с некоторым подмножеством элементов, отображаемых геоинформационной системой (ГИС) и формирующих его графическое представление, что позволяет автоматически измерять графические характеристики для использования в расчетах.

Наряду с экспертной системой, СКМ интегрирует и ГИС, что позволяет равноправно обрабатывать результаты математических расчетов, графические данные и знания экспертов. Для СКМ разработаны методы и алгоритмы контроля данных, обработки ситуаций, управления структурой моделируемого объекта.

По аналогии с работой [3] далее предлагается строить ЛМН и ЛМБ на основе ФАЛ, описывающих

причинно-следственные связи между работоспособными и неработоспособными, безопасными и опасными состояниями элементов СКМ. Поскольку именно информационные связи отражают взаимовлияние элементов СКМ, характеристики надежности и безопасности определяются, прежде всего, для ресурсов (данных).

Моделирование надежности ППС

Свяжем с каждым ресурсом СКМ res_m логическую переменную $x(res_m)$, отражающую структурную надежность его получения. Для расчета надежности выработки выходных ресурсов структурными элементами ППС, т. е. процессами и объектами, необходимо выделить надежность самого элемента и надежность его обеспечения входными ресурсами, тогда для любого выходного ресурса некоторого объекта o_i или процесса p_j получаем

$$\forall(res_m \in list\_out(o_j))x(res_m) = \\ = x(o_i) \wedge \left(\begin{matrix} \wedge\ x(res_l) \\ res_l \in list\_in(o_i) \end{matrix} \right); \quad (1)$$

$$\forall(res_m \in list\_out(o_j))x(res_m) = \\ = x(p_j) \wedge \left(\begin{matrix} \wedge\ x(res_l) \\ res_l \in list\_in(p_j) \end{matrix} \right), \quad (2)$$

где $list\_in(*)$ и $list\_out(*)$ — списки входных и выходных ресурсов некоторого элемента СКМ, условно обозначенного *.

Ситуационная концептуальная модель дает возможность исследовать надежность на уровне объектов непосредственно по соотношениям (1), но тогда необходимо задавать $x(o_i)$ вручную. Более логично учитывать надежность преобразований ресурсов внутри объекта, в таком случае следует использовать соотношения (2) для всех категорий процессов СКМ, включая внутренние процессы (все их входные и выходные ресурсы принадлежат одному объекту). При таком методе расчета можно оценить структурную надежность каждого объекта o_i по формулам (1), (2) как надежность выработки его выходных ресурсов в предположении гарантированной выработки его входных ресурсов, т. е. положив

$$\forall(res_m \in list\_in(o_i))\ x(res_m) = 1. \quad (3)$$

Поскольку СКМ допускает избыточность модели по номенклатуре выходных ресурсов, то при оценке надежности объекта следует учитывать только ту часть списка выходных ресурсов (назовем их существенными выходными ресурсами $ess\_out(o_i)$), которая потребляется другими объектами:

$$\forall(res_m \in ess\_out(o_i))\ res_m \in list\_in(o_j),\ i \neq j. \quad (4)$$

Тогда для ФАЛ, описывающей надежность объекта, из (1), (2) получим

$$x(o_i) = x_{in}(o_i) \wedge \\ \wedge \left(\begin{matrix} \wedge x(res_l) \\ res_l \in ess\_out(o_i) \ \subseteq list\_out(o_i) \end{matrix} \right) \quad (5)$$

при выполнении (3). В (5) первый конъюнкт позволяет учесть отказы, которые нельзя связать ни с одним из процессов, приписанных данному объекту. Аналогично (5) описывается надежность любого связного фрагмента модели ППС, тогда условие (3) должно выполняться для всех ресурсов, внешних по отношению к анализируемому фрагменту.

При необходимости легко учесть возможность отказов при передаче ресурсов между объектами, поскольку последние, по определению, имеют в СКМ географическую привязку. В общем случае надежность некоторого входного ресурса объекта вычисляется как конъюнкция надежности его выработки порождающим объектом и надежности передачи между объектами, зависящей от взаимного расположения последних:

$$\forall((res_m \in list\_in(o_i) \wedge (res_m \in list\_out(o_k))\ x_{in}(res_m) = \\ = x_{out}(res_m) \wedge x_{tr}(res_m), \quad (6)$$

причем показатель надежности передачи ресурса $x_{tr}(res_m)$ целесообразно формировать в функции от графических характеристик ГИС-представлений объектов o_i и o_k:

$$x_{tr}(res_m) = x_{tr}\ \underline{\underline{h}}^{\alpha}(o_j) \cup \underline{\underline{h}}^{\alpha}(o_k), \quad (7)$$

где $\underline{\underline{h}}^{\alpha}(o_j)$ — множество ГИС-элементов, подчиненных объекту o_i [1].

С помощью встроенного набора ГИС-операций [1] над ГИС-элементами, заданными в (7), можно автоматизировать измерение требуемых графических характеристик (координат, расстояний, площадей и т. п.) элементов моделируемого объекта и их ввод в расчетные модули.

Получение ФАЛ для расчета надежности любого выбранного фрагмента СКМ производится автоматически по формулам (1), (2), (6), (7) с учетом следующих очевидных правил.

При наличии альтернатив реализации ППС на уровне объектов (декомпозиции некоторого объекта o_i на подобъекты o_{ij}, $j = 1, 2, ..., n$, по типу «или») из формулы (1) имеем

$$\forall(res_m \in list\_out(o_j)),\ x(res_m) = \\ = \bigvee_{j=1}^{n} \left[x(o_{ij}) \wedge \left(\begin{matrix} \wedge\ x(res_l) \\ res_l \in list\_in(o_{ij}) \end{matrix} \right) \right]. \quad (8)$$

Для альтернативных реализаций ППС на уровне ресурсов (при задании альтернативного набора

ресурсов $set\_alt(p_j) \subset list\_in(p_j)$ на входе некоторого процесса p_j) надежность выработки входных ресурсов в формуле (2) для ресурсов, входящих в альтернативный набор, вычисляется как дизъюнкция по всем m имеющимся альтернативам выработки этих ресурсов:

$$\forall(res_m \in set\_alt(p_j)), \quad x(res_m) = \bigvee_{k=1}^{m} x(res_{mk}). \quad (9)$$

При агрегировании (суммировании значений) наборов ресурсов на входе некоторого процесса (спецификации набора входных ресурсов $set\_agr(p_j)$ по типу «сумма» или «итерация») аналогично (9) получаем

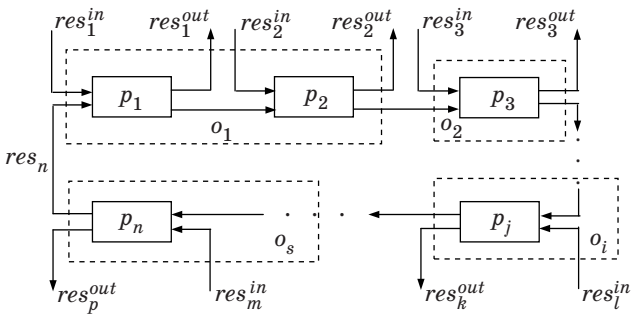
$$\forall(res_m \in set\_agr(p_j)), x(res_m) = \bigwedge_{k=1}^{m} x(res_{mk}). \quad (10)$$

Рекуррентное применение соотношений (1), (2), (6), (8)–(10), начиная от листьевых ресурсов, позволяет автоматически синтезировать ФРС для всего объекта моделирования в целом или для любой его части, которой соответствует связный фрагмент СКМ [1]. При наличии циклов по ресурсам это выявляется специальным алгоритмом, предотвращающим зацикливание алгоритма построения ФРС по описанным выше соотношениям. Если цикл образован некоторой последовательностью из n процессов p_j, связанных n внутренними (по отношению к данному циклу) ресурсами res_j и приписанных s объектам o_i, причем на входы процессов поступает m внешних (относительно этого цикла) ресурсов res_i^m, а из цикла выходят вовне p ресурсов res_k^{out} (рис. 1), то структурную надежность функционирования такого цикла (назовем его *элементарным циклом*), естественно охарактеризовать величиной

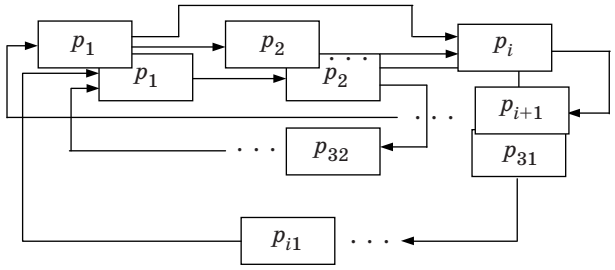
$$x(cycle1) = \left(\bigwedge_{l=1}^{m} x_{in}(rec_l^{in})\right) \wedge \left(\bigwedge_{j=1}^{n} x(p_j)\right) \wedge$$
$$\wedge \left(\bigwedge_{i=1}^{s} x_{in}(o_i)\right) \wedge \left(\bigwedge_{i=1}^{s} x_{tr}(res_j)\right), \quad (11)$$

где в последнем сомножителе в конъюнкцию согласно (6) включаются только ресурсы, передаваемые между объектами. При определении ФРС всей системы для всех выходных ресурсов цикла следует принять

$$x_{out}(res_k^{out}) = x(cycle1). \quad (12)$$



■ ***Рис. 1.*** Структура элементарного цикла



■ ***Рис. 2.*** Структуры кратных циклов

Не составляет принципиальных трудностей обобщить соотношение (11) для более сложных структур, допустимых в СКМ и показанных на рис. 2. Для этого следует учесть в соответствующих конъюнкциях из (11) кратность вхождения того или иного элемента СКМ (объекта, процесса, ресурса) в данную структуру. Явные соотношения здесь не выписываются ввиду их громоздкости.

Построенная описанным способом ФРС, очевидно, относится к монотонным ФАЛ, что позволяет применять к ней все предложенные [3] методы канонического представления для конструирования кратчайших путей успешного функционирования и (или) минимальных сечений отказов ППС. Более того, предложенное здесь использование понятия надежности выработки каждого ресурса как основы разработки ЛМН ППС в принципе позволяет оценивать частичную работоспособность фрагментов ППС при отказе тех или иных элементов, учитывая уже имеющиеся в модели значения текущих количеств всех материальных ресурсов [1] и скорость их расходования для расчета допустимого времени восстановления отказавших элементов. В частности, при этом уже не для всех выходов циклов будет справедливо соотношение (12). Однако в общем случае подобные вопросы требуют дополнительного обоснования.

Моделирование безопасности ППС

При разработке ЛМБ ППС в рамках СКМ можно, аналогично работе [3], считать, что ЛМБ должны разрабатываться прямыми методами, в частности, что они принципиально отличны от ЛМН, и только язык их формального описания одинаков. Однако из-за уже отмеченной существенно большей детальности СКМ по сравнению с сценарием опасного состояния по логико-вероятностному методу кажется разумным использовать СКМ также и в качестве ядра ЛМБ. Это дает

возможность автоматизировать формализацию достаточно распространенных на практике функционально-зависимых ИС (обозначение — ИС1), возникающих без явных дополнительных причин при выходе тех или иных ресурсов за пределы ограничений, соответствующих режимам нормальной работы (внутренняя или технологическая безопасность). Таким образом, для расчетов безопасного функционирования ППС следует выделить и (или) дополнительно специфицировать в каждом элементе ППС те его выходные ресурсы, которые целесообразно атрибутировать диапазонами безопасного функционирования *SR* (*Safety Range*) и рассматривать как возникновение ИС1 отрицание события

$$res_m \in SR(res_m). \qquad (13)$$

Принятое в СКМ представление диапазонов значений переменных величин в виде списков [1] позволяет моделировать в форме (13) и «двоичные» (да–нет, 1–0 и т. д.) ресурсы, назначая им $SR = \{0\}$.

В принципе, можно выделить два подтипа ИС1:

— ИС11, когда условие (13) нарушается для некоторого выходного ресурса элемента ППС и свидетельствует о его переходе в опасное состояние;

— ИС12, когда нарушение условия (13) для некоторого выходного ресурса элемента ППС расценивается как показатель опасного функционирования других элементов, для которых этот ресурс является входным.

Специфицированы еще две категории ИС, появление и развитие которых зависит от пространственных и (или) временных характеристик элементов СКМ. Они названы пространственно-порожденными (ИС2) и время-порожденными (ИС3), возможны и их комбинации (ИС4). К таким ИС относятся процессы, связанные с переносом (распространением) воздействующей субстанции (вещества, поля) в различных средах и (или) зависящие от рельефа местности, на которой размещена моделируемая ППС (например, зоны затопления при различных объемах прорвавшейся воды). Условия возникновения подобных ИС формируются экспертным путем в функции от времени и доступных в СКМ графических характеристик элементов.

В отличие от ЛМН ППС, основанной на надежности выработки ресурсов, атомарными единицами ЛМБ ППС являются объекты СКМ, поскольку они имеют географическую привязку. ЛМБ каждого объекта должна учитывать возможность возникновения на нем ИС всех введенных выше типов. Обозначая, аналогично работе [3], индикаторы появления ИС символами z с соответствующими индексами, ФАЛ для описания опасного состояния объектов СКМ будем строить в виде

$$y(o_i) = z_1(o_i) \vee z_2(o_i) \vee z_3(o_i) \vee z_4(o_i), \qquad (14)$$

где

$$z_1(o_i) = \left(\underset{res_l \in list\_out(o_i)}{\vee z(res_l)} \right) \vee \left(\underset{res_l \in list\_in(o_i)}{\vee z(res_l)} \right),$$

аналогично (1) описывает ИС11 и ИС12 соответственно, причем в дизъюнкцию включаются только те ресурсы из списков входных и выходных ресурсов объекта, которые влияют на его безопасность, а появление «элементарных» ИС $z(res_l)$ диагностируется по нарушению соотношения (13);

$z_2(o_i) = z_2(\underline{\underline{h}}^{\alpha}(o_i))$ описывает ИС2 и формируется аналогично (7) в функции от графических характеристик ГИС-представления объекта o_i.

При описании ИС3 и ИС4 требуется уметь учитывать достаточно широкий класс пространственно-временных соотношений между характеристиками объекта, что может в общем случае потребовать включения в СКМ объекта дополнительных процессов, описывающих эти соотношения и формирующих $z_3(o_i) \vee z_4(o_i)$. Возможно также использовать для этих целей встроенные в экспертную систему СКМ пространственно-временные функции. В настоящее время разработаны два вида пространственных функций и один вид временных функций [1]. Временная функция поддерживает выборку ретроспективных данных за некоторый промежуток времени, ее синтаксис имеет вид

в_течение (<условие>, <начало>,

<конец>, <доля>), (15)

где **<условие>** — логическая функция значений ресурсов некоторого элемента ППС, оно определяет критерий опасного функционирования этого элемента;

<начало> и **<конец>** задают соответственно начальный и конечный моменты интервала проверки (их отстояние в прошлое от текущего момента времени), они могут задаваться либо в абсолютных единицах времени, либо в количестве интервалов дискретности модели по времени;

<доля> определяет минимальный допустимый процент элементов среди всех анализируемых, которые должны удовлетворять **<условию>**, чтобы функция (15) дала утвердительный ответ на запрос; этот параметр используется интерпретатором пространственно-временных функций.

Если введено нулевое значение параметра **<начало>**, проводится анализ всей имеющейся информации до момента времени **<конец>**. Аналогично при нулевом значении параметра **<конец>** анализируются данные от момента **<начало>** до текущего момента времени. При совпадении величин **<начало>** и **<конец>** рассматривается только один момент времени в прошлом.

Пространственные функции записываются в форме **соседние (<условие>, <доля>)** и **сходные (<условие>, <доля>, <параметры_сходства>).**

Параметры **<условие>** и **<доля>** имеют тот же смысл, что и в функции (15), различие между видами пространственных функций заключается в критерии отбора элементов для совместного анализа: в первой функции анализируются элементы, примыкающие к текущему геометрически, а во второй отбираются элементы, имеющие одинаковые с текущим элементом значения **<параметров_сходства>**, принадлежащих списку имен ресурсов текущего элемента.

Поскольку все пространственно-временные функции имеют выход логического типа, допускается однократная вложенность различных функций друг в друга, т. е. запросы вида **соседние (сходные (<условие>, <доля1>, <параметры_сходства>), <доля2>).**

Таким образом, в отличие от ЛМН, СКМ не обеспечивает полной автоматизации разработки ЛМБ, но, по мнению авторов, позволяет существенно облегчить их создание за счет гибкой алгоритмической поддержки процедур описания ИС и получить в результате функцию опасного состояния всей ППС или ее связной подсистемы, пригодную для построения кратчайших путей опасного функционирования и (или) минимальных сечений предотвращения опасности [3].

Вопросы количественной оценки надежности и безопасности ППС на базе представленных выше методов генерации их логических моделей выходят за рамки настоящей работы и заслуживают отдельного рассмотрения. В принципе, для этого применимы и логико-вероятностные методы [3]. Однако из-за известной проблемы недостаточности доступных исходных данных о ППС для применения вероятностной парадигмы в некоторых случаях представляется целесообразным применять представленный ниже метод оценки степени опасности ситуации, использующий экспертные оценки опасности тех или иных значений переменных состояния ППС.

Формализация пространства состояний объекта моделирования

В СКМ критерий качества работы каждого объекта или процесса имеет вид

$$\Phi ::= \left(\frac{1}{m} \sum_{i=1}^{m} \left(\frac{a_i - a_{i0}}{\Delta a_i} \right)^2 \right)^{1/2} ::= \left(\frac{1}{m} \sum_{i=1}^{m} \delta a_i^2 \right)^{1/2}, \quad (16)$$

где a_i — сигналы из списка выходных параметров данного объекта, их общее количество равно m; a_{i0} и $\Delta a_i > 0$ — настроечные параметры, отражающие требования вышестоящего объекта к номинальному значению a_i и допустимому отклонению Δa_i от этого значения соответственно; $\delta a_i ::= \frac{a_i - a_{i0}}{\Delta a_i}$ — относительное отклонение фактического значения сигнала a_i от его номинального значения a_{i0}.

Если считать a_i скалярными критериями качества работы элемента модели, номинальные значения которых определяются величинами a_{i0}, то (16) есть обобщенный критерий [7] с коэффициентами важности, обратно пропорциональными допустимым отклонениям скалярных критериев, что не противоречит здравому смыслу. Его значение равно единице в том случае, если значения всех его аргументов находятся на грани допусков:

$$\Phi = 1, \text{ если } |a_i - a_{i0}| = \Delta a_i,\ i = \overline{1, m}, \quad (17)$$

и не превосходит единицы, если все аргументы находятся в пределах допусков.

Перечисленные свойства обеспечивают естественную нормировку сигналов и облегчают поиск элементов модели, чьи характеристики существенно отличаются от желаемых.

Применение критерия (16) обеспечивает статический сопоставительный анализ ситуаций и их экстраполяцию в имитационном режиме [1], а также используется при решении задач координации подсистем ППС [8], но не позволяет оценивать управление моделируемым объектом во времени, для чего традиционно применяется концепция состояния объекта как временного среза траектории изменения его характеристик в некотором абстрактном многомерном пространстве [9]. Для решения задач динамического управления ППС необходимо ввести метрику в пространстве состояний, она и предлагается далее.

Поскольку, как отмечено выше, вычисление критерия (16) и на его основе — удельных обобщенных затрат [1] позволяет однозначно сопоставлять текущие варианты состояния ППС между собой, представляется естественным строить метрику пространства состояний на основе этого же критерия.

Если применение соотношения (16) для задания метрики числовых переменных проблем не вызывает, то его использование для подпространства строковых переменных требует некоторого ужесточения правил формирования списков допустимых значений таких переменных. В настоящем разделе предлагается процедура метризации пространства строковых переменных, позволяющая сконструировать для них критерий, аналогичный (16) и удовлетворяющий ограничению (17).

Вначале необходимо выделить одно (любое, включая граничные) из допустимых значений как номинальное (идеальное для реализации управления) значение. Затем следует упорядочить остальные допустимые значения по степени их отклонения от идеального значения (чем больше это отклонение для данного допустимого

значения, тем дальше от идеального должно быть оно в списке), причем все значения, помещенные в список до идеального, должны отличаться «направлением» отклонения от всех значений, находящихся в списке после идеального (рис. 3, *а*).

Минимальное допустимое значение параметра, имя которого обозначим $<\text{зн}^{inf}_{\text{доп}}>$, имеет порядковый номер (целое неотрицательное число) $k^{inf}_{\text{доп}} = 0$, максимальное допустимое значение параметра $<\text{зн}^{sup}_{\text{доп}}>$ имеет порядковый номер n, идеальное допустимое значение параметра $<\text{зн}_{\text{ид}}>$ имеет порядковый номер m, а остальные значения пронумерованы возрастающими натуральными числами в порядке расположения слева направо (см. рис. 3, *а*). Направление упорядочения (для конкретности примем, что это увеличение) показано на рисунке стрелками. Например, допустимыми значениями параметра «рост» могут быть следующие (перечислены в порядке «возрастания», в скобках даны их порядковые номера в списке значений): $<\text{зн}^{inf}_{\text{доп}}>$ = «*значительно ниже среднего*» ($k = k^{inf}_{\text{доп}} = 0$), «*ниже среднего*» ($k = 1$), «*несколько ниже среднего*» ($k = 2$), «*средний*» ($k = k_{\text{ид}} = m = 3$), «*несколько выше среднего*» ($k = 4$); $<\text{зн}^{sup}_{\text{доп}}>$ = «значительно выше среднего» ($k = k^{sup}_{\text{доп}} = n = 5$).

В предположении о равноправии и «равноудаленности» соседних значений некоторого параметра друг от друга в качестве меры расстояния между двумя значениями этого параметра можно, по аналогии с расстоянием в теории ориентированных графов, выбрать длину маршрута между значениями, если рассматривать сами значения как вершины графа.

Из определения критерия (16) имеем, что граничные (минимальное и максимальное) допустимые значения числовой переменной достигаются, когда модуль относительной погрешности δa_i равен единице:

$$\delta a_i = \frac{a_i - a_{i0}}{\Delta a_i} = \pm 1, \Rightarrow \begin{matrix} a_{i\max} = a_{i0} + \Delta a_i \\ a_{i\min} = a_{i0} - \Delta a_i \end{matrix}. \qquad (18)$$

Из-за возможной асимметрии количества значений строковых параметров относительно идеального значения допустимые отклонения от него вправо и влево различны. Тогда условия нормировки (18) сохранятся, если определить допустимые отклонения параметра от идеального значения в виде

$$\Delta a^{inf}_i \overset{\Delta}{=} k_{\text{ид}} - k^{inf}_{\text{доп}} = m; \quad \Delta a^{sup}_i \overset{\Delta}{=} k^{sup}_{\text{доп}} - k_{\text{ид}},$$

а относительное отклонение фактического значения параметра от его номинального значения задать соотношением

$$\delta a_i \overset{\Delta}{=} \begin{cases} \dfrac{k - k_{\text{ид}}}{\Delta a^{inf}_i};\ k < k_{\text{ид}} \\ \dfrac{k - k_{\text{ид}}}{\Delta a^{sup}_i};\ k \geq k_{\text{ид}} \end{cases} \qquad (19)$$

или для случая, когда индекс идеального значения есть m (см. рис. 3):

$$\delta a_i \overset{\Delta}{=} \begin{cases} \dfrac{k - m}{\Delta a^{inf}_i};\ k < m \\ \dfrac{k - m}{\Delta a^{sup}_i};\ k \geq m \end{cases}. \qquad (20)$$

Если идеальное значение некоторого параметра совпадает с одним из его граничных значений, то для этого значения принимаем $\delta a_i = 0$.

В целях моделирования нештатных и аварийных ситуаций в ППС нежелательные и недопустимые значения параметров должны «расширять» упорядоченный список допустимых значений (они образуют диапазон безопасного функционирования *SR*) в соответствующие стороны (рис. 3, *б*). Более жирной линией показаны подмножества недопустимых значений параметра, которые на рис. 3, *а* отсутствуют. Без потери общности можно принять, что все внутренние значения параметра, выходящие за допуск, соответствуют нежелательным, но не критическим режимам функционирования ППК, а крайние значения — критические.

Например, нежелательными значениями параметра «рост» могут быть выбраны, с одной стороны, $<\text{зн}^{sup}_{\text{крит}}>$ = «*карлик*» ($k = k^{inf}_{\text{доп}} = 0$) а с другой — $<\text{зн}^{sup}_{\text{крит}}>$ = «*гигант*» ($k = k^{sup}_{\text{доп}} = n$).

Если предположение о равноудаленности значений параметра неприемлемо, то вышеприведенные определения расстояния нетрудно обобщить, вводя положительные веса дуг между соседними значениями параметра (на рис. 3 обозначены символами β с индексами). Тогда аналогично получим

$$\Delta a^{inf}_i \overset{\Delta}{=} \sum_{k=1}^{k_{\text{ид}}} \beta_k; \qquad \Delta a^{sup}_i \overset{\Delta}{=} \sum_{k=k_{\text{ид}}+1}^{k_{\text{доп}}} \beta_k; \qquad (21)$$

■ ***Рис. 3.*** Допустимые (*а*) и все возможные (*б*) значения строкового параметра

$$\delta a_i = \begin{cases} \dfrac{-\sum_{j=k}^{k_{\text{ид}}} \beta_j}{\Delta a_i^{inf}}; \; k < k_{\text{ид}} \\ \dfrac{-\sum_{j=k}^{k_{\text{ид}}} \beta_j}{\Delta a_i^{sup}}; \; k \geq k_{\text{ид}} \end{cases}. \qquad (22)$$

Очевидно, для соотношений (21), (22) условие равенства единице модуля δa_i для граничных допустимых значений параметра также сохраняется.

Для отображения повышенной степени нежелательности и (или) опасности некоторых значений параметров веса этих значений следует выбирать много больше единицы, тогда соответствующее состояние ППС будет отбраковано в ходе решения задачи классификации ситуаций [1].

После выполнения описанной выше модификации строковые параметры могут включаться в пространство состояний ППС наравне с числовыми переменными, поскольку их метрика имеет аналогичные свойства, что позволяет рассматривать интегральные характеристики поведения ППК в этом пространстве. Следует отметить, что и для числовых переменных может оказаться полезным переход от вычисления относительной погрешности по формуле (16) к формулам типа (21), допускающим асимметрию диапазона возможных значений относительно номинального (идеального) значения.

Заключение

В настоящей работе ситуационный подход к моделированию состояния ППС и сопоставлению альтернативных структур реализации таких объектов обобщен на задачи разработки логических моделей структурной надежности и безопасности функционирования ППС.

В ЛМН каждому ресурсу приписывается логическая переменная, отражающая структурную надежность его получения. Для ресурсов, поступающих извне, она задается априорно, а для ресурсов, формируемых элементами СКМ, вычисляется в ходе моделирования. При этом соответствующая ФАЛ учитывает надежность элемента СКМ, вырабатывающего этот ресурс, надежность обеспечения самого элемента входными ресурсами и возможность отказов при передаче ресурсов между объектами, которые по определению имеют в СКМ географическую привязку.

При разработке ЛМБ влияющие на безопасность ресурсы атрибутированы диапазонами безопасного функционирования *SR*. Выход за пределы соответствующего диапазона интерпретируется как *функционально-порожденное* инициирующее событие (ИС1). Таким образом, модели ИС1 в СКМ рассматриваются как расширение моделей нормального функционирования элементов ППС, что представляется рациональным. Специфицированы еще две категории ИС, появление и развитие которых зависит от пространственных и (или) временных характеристик элементов СКМ. Они названы *пространственно-порожденными* (ИС2) и *время-порожденными* (ИС3), возможны и их комбинации (ИС4). Условия их возникновения формируются экспертным путем в функции от времени и доступных в СКМ графических характеристик элементов.

Основное отличие предложенного подхода от известных методов создания логических моделей надежности и безопасности ССС с опорой на структурную схему [3] состоит в том, что детальность моделирования ССС (ППС) повышена до отдельного ресурса, т. е. любого материального или информационного сигнала, которым могут обмениваться элементы ССС. Это, по мнению авторов, позволяет существенно повысить достоверность результатов анализа логической модели за счет более полного учета взаимосвязей элементов ППС, особенно в части выявления сложных (многократных) комбинаций отказов этих элементов.

К преимуществам представленного выше подхода можно отнести:

— возможность спецификации и формализованного описания типичных для ППС классов функционально-, пространственно- и время-порожденных отказов, инициирующих событий и инициирующих условий, появление и развитие которых зависит от пространственно-временных характеристик элементов ППС;

— принципиальную возможность оценки частичной работоспособности фрагментов ППС при отказе тех или иных элементов с учетом текущих количеств материальных ресурсов и скорости их расходования для расчета допустимого времени восстановления отказавших элементов и анализа последствий отказов;

— поддержку формирования и исследования альтернативных логических моделей, что актуально при проектировании ППС, а также при создании систем управления надежностью и безопасностью ППС;

— в практическом аспекте — использование единой инструментальной среды и методологии для моделирования как нормальных, так и критических режимов функционирования ППС, что позволяет аккумулировать разнородные знания об объекте исследования в целях их комплексного применения.

Следует отметить, что вопросы оценки вычислительной сложности описанных методов

построения логических моделей надежности и безопасности ППС требуют более детального анализа, хотя доказана [1] полиномиальная (квадратичная) сложность основных алгоритмов анализа ситуаций в СКМ.

Работа выполнена при финансовой поддержке РФФИ (проекты № 14-07-00256-а, 14-07-00257-а, 14-07-00205-а, 13-07-00318-а, 12-07-00689-а, 12-07-000550-а, 12-07-00302-а) и Президиума РАН (проект 4.3 Программы № 16).

Литература

1. **Фридман А. Я., Фридман О. В., Зуенко А. А.** Ситуационное моделирование природно-технических комплексов. — СПб.: Изд-во Политехнического ун-та, 2010. — 436 с.
2. **Фридман А. Я.** Ситуационный подход к моделированию промышленно-природных комплексов и управлению их структурой // Идентификация систем и задачи управления: тр. IV Междунар. конф., Москва, 25–28 января 2005 г./ ИПУ РАН. — М., 2005. С. 1075–1108.
3. **Рябинин И. А.** Надежность и безопасность структурно-сложных систем. — СПб.: Политехника, 2000. — 248 с.
4. **Городецкий А. Е., Курбанов В. Г., Тарасова И. Л.** Экспертная система анализа и прогнозирования аварийных ситуаций в энергетических установках // Информационно-управляющие системы. 2012. № 4. С. 59–63.
5. **Городецкий А. Е., Дубаренко В. В., Курбанов В. Г., Тарасова И. Л.** Логико-вероятностные методы моделирования плохо формализуемых процессов и систем // Изв. ЮФУ. Технические науки. 2012. № 6(131). С. 255–257.
6. **Городецкий А. Е., Курбанов В. Г., Тарасова И. Л.** Имитационное моделирование развития аварийных ситуаций в энергетических установках // Информационно-управляющие системы. 2013. № 2. С. 38–42.
7. **Салуквадзе М. Е.** Задачи векторной оптимизации в теории управления. — Тбилиси: Мецниереба, 1975. — 202 с.
8. **Фридман А. Я., Фридман О. В.** Градиентный метод координации управлений иерархическими и сетевыми структурами // Информационно-управляющие системы. 2010. № 6. С. 13–20.
9. **Деруссо П., Рой Р., Клоуз М.** Пространство состояний в теории управления. — М.: Наука, 1970. — 620 с.

UDC 004.9

Situational Modelling of Reliability and Safety for Industrial-Natural Systems

Fridman A. Ya.[a], Dr. Sc., Tech., Professor, fridman@iimm.ru
Kurbanov V. G.[b], PhD, Phys.-Math., Senior Researcher, vugar_borchali@yahoo.com
[a]Institute for Informatics and Mathematical Modelling of Technological Processes of RAS, 24A, Fersman St., 184209, Apatity, Murmansk Region, Russian Federation
[b]Institute of Problems in Mechanical Engineering, 61, Bol'shoi St., V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: The situational approach to modelling the state of industrial-natural systems (INS) and to comparing alternative structures of their realization proposed earlier by one of the authors is generalized for the problems of developing logical models of structural reliability and safety of such systems. The research is aimed at developing the technique to build logical models of structural reliability and safety of INS functioning on basis of their normal functioning model. **Results:** Dangerous and critical situations are modeled as an "extension" of normal performance models, using the same software environment. The modelling process is detailed down to a single material or informational signal transferred between the system elements. This is the main difference of the proposed technique from the conventional ways of modeling safety/reliability of complex systems on basis of their structure charts. It provides the following advantages: the opportunity to specify and formalize descriptions of functionally, spatially and temporally generated failures typical for INS as well as triggering events and conditions whose appearance and development depends on spatial-temporal attributes of INS elements; the principle possibility to estimate partial operability of an INS at failures of certain elements taking into account the current quantity of the resources and rates of their spending in order to calculate acceptable restoration times for failed elements and analyze the consequences of their failures; the support of building and studying alternative logical models during INS construction, as well as the systems to control its safety and reliability. **Practical relevance:** This technique can raise the validity of logical models of safety and reliability by more complete consideration of interconnections between INS elements, thus revealing the most dangerous situations and scenarios caused by combined and multiple failures within the system. A common modeling environment for both normal and emergency modes of INS functioning provides accumulation of diverse kinds of knowledge about the investigated object for their integration.

Keywords — Situational Modelling, Logic Model of Reliability, Logic Model of Safety, Triggering Event, Logic Probabilistic Method.

References

1. Fridman A. Ya., Fridman O. V., Zuenko A. A. *Situacionnoe modelirovanie prirodno-tehnicheskih kompleksov* [Situational Modelling of Nature-Technical Complexes]. Saint-Petersburg, Politekhnicheskii universitet Publ., 2010. 436 p. (In Russian).
2. Fridman A. Ya. Situational Approach to Modelling of Nature-Technical Complexes and Their Structure Control. *Trudy IV Mezhdunarodnoj konferencii "Identifikacija sistem i zadachi upravlenija"* [Proc. IV Intl. Conf. "Identification of Systems and Control Problems"]. Moscow, 2005, pp. 1075–1108 (In Russian).
3. Ryabinin I. A. *Nadezhnost' i bezopasnost' strukturno-slozhnyh sistem* [Reliability and Safety of Structurally Complex Systems]. Saint-Petersburg, Polytechnica Publ., 2000. 248 p. (In Russian).
4. Gorodetsky A. E., Kurbanov V. G., Tarasova I. L. Expert System of Analysis and Forecasting Emergencies in Power Generating Systems. *Informatsionno-upravliaiushchie sistemy*, 2012, no. 4, pp. 59–63 (In Russian).
5. Gorodetsky A. E., Dubarenko V. V., Kurbanov V. G., Tarasova I. L. Logical-and-Probabilistic Methods for Modelling of Poorly Formalizable Processes and Systems. *Izvestiia IuFU. Tekhnicheskie nauki*, 2012, no. 6, pp. 255–257 (In Russian).
6. Gorodetsky A. E., Kurbanov V. G., Tarasova I. L. Simulation Modeling of Emergencies Development in Power Installations. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 2, pp. 38–42 (In Russian).
7. Salukvadze M. E. *Zadachi vektornoj optimizacii v teorii upravlenija* [Vector Optimization Problems in Control Theory]. Tbilisi, Metsniereba Publ., 1975. 202 p. (In Russian).
8. Fridman A. Ya., Fridman O. V. Gradient Coordination Technique to Control Hierarchical and Network Structures. *Informatsionno-upravliaiushchie sistemy,* 2010, no. 6, pp. 13–20 (In Russian).
9. Derusso P., Roy R., Close M. *Prostranstvo sostojanij v teorii upravlenija* [State Space in Control Theory]. Moscow, Nauka Publ., 1970. 620 p. (In Russian).