УДК 004.75 DOI: 10.26102/2310-6018/2020.29.2.018

Информационная поддержка проактивного управления функциональной безопасностью компонентов киберфизических систем

В.Е. Гвоздев, М.Б. Гузаиров, О.Я. Бежаева, Р.Р. Курунова, Р.А. Насырова
Уфимский государственный авиационный технический университет,
Уфа, Российская Федерация

Резюме: Обеспечение функциональной безопасности киберфизических систем является необходимым условием их внедрения в области, в которых надежное и предсказуемое поведение узлов распределенных систем киберфизического управления является критическим требованием. В литературе с начала 90-х годов прошлого столетия в рамках теории управления рисками обсуждается подход к обеспечению функциональной безопасности субъектоцентрических систем. Концептуальную основу этого подхода составляет положение о неизбежности наличия в сложных технических системах латентных дефектов разной природы, условия активизации которых предсказать невозможно. Из этого вытекает необходимость создания барьеров, препятствующих преобразованию опасности в инцидент. Предлагаемый в настоящей работе подход к построению системы структурных моделей на основе аппарата схем сопряжения и таблиц истинности функциональных компонентов следует рассматривать с позиций информационной поддержки формирования барьеров. Основу рассматриваемого подхода к построению структурных моделей, позволяющих выполнять сценарный анализ показателей функциональной безопасности узлов киберфизических систем, составляет аппарат схем сопряжения и таблиц истинности. Показано, что предлагаемый подход позволяет в качестве частных решений получать модели, соответствующие Failure Tree Analysis, Root Cause Analysis, а также совокупность моделей, получаемых в рамках концепции профилей.

Ключевые слова: функциональная безопасность, киберфизические системы, надежность, информационный сервис, профиль.

Для цитирования: Гвоздев В.Е., Гузаиров М.Б., Бежаева О.Я., Курунова Р.Р., Насырова Р.А. Информационная поддержка проактивного управления функциональной безопасностью компонентов киберфизических систем. *Моделирование, оптимизация и информационные технологии.* 2020;8(2). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/05/GvozdevSoavtors_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.018

Information support for proactive management of functional safety of components of cyber-physical systems

V.E. Gvozdev, M.B. Guzairov, O.Y. Bezhayeva, R.R. Kurunova, R.A. Nasyrova
Ufa State Aviation Technical University,
Ufa, Russian Federation

Abstract: Ensuring the functional safety of cyber-physical systems is a prerequisite for their implementation in areas in which reliable and predictable behavior of nodes of distributed cyber-physical control systems is a critical requirement. In the literature from the beginning of the 90s of the last century, within the framework of the theory of risk management, an approach to ensuring the functional safety of subject-centric systems is discussed. The conceptual basis of this approach is the provision on the inevitability of the presence of latent defects of different nature in complex technical systems, the activation conditions of which cannot be predicted. This implies the need to create barriers

to the conversion of danger into an incident. The approach proposed in this paper to constructing a system of structural models based on the apparatus of conjugation schemes and truth tables of functional components should be considered from the perspective of information support for the formation of barriers. The basis of the approach to constructing structural models that allow performing a scenario analysis of the functional safety indicators of the nodes of cyber-physical systems is the apparatus of conjugation schemes and truth tables. It is shown that the proposed approach allows one to obtain models corresponding to Failure Tree Analysis, Root Cause Analysis, as well as a set of models obtained as part of the concept of profiles as particular solutions.

Keywords: functional safety, cyber-physical systems, reliability, information service, profile.

For citation: Gvozdev V.E., Guzairov M.B., Bezhaeva O.Y., Kurunova R.R., Nasyrova R.A. Information support for proactive management of functional safety of components of cyber-physical systems. *Modeling, optimization and information technology*. 2020;8(2). Available from: https://moit.vivt.ru/wp-content/uploads/2020/05/GvozdevSoavtors_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.018 (In Russ).

Введение

К числу ключевых компонент, обеспечивающих реализацию положений доктрины Industry 4.0, помимо интернета вещей (IoT), интернета сервисов (IoS), «умных производств» (Smart Factory), интероперабельности информационных систем, относятся киберфизические системы (Cyber-Physical Systems – CPS) [1]. Обеспечение надежного и предсказуемого поведения CPS является необходимым условием их внедрения в области, в которых безопасное функционирование является критическим требованием (управление дорожным движением; управление воздушными судами; здравоохранение [1-5].) Особенностью CPS являются территориальная распределенность, гетерогенность функциональных компонент (физических устройств, программных продуктов), входящих в состав распределенной динамической сети, а также разные типы процессов (непрерывные и дискретные, протекающие в физических и программных компонентах узлов сети соответственно). В силу этого для решения задач, связанных с анализом функциональной безопасности узлов киберфизических систем, необходимо разрабатывать методы, позволяющие рассматривать с единых позиций свойства физических устройств (функционирование которых определяется объективными законами природы) и программных продуктов (функциональные и нефункциональные характеристики которых определяются субъективными решениями разработчиков).

В настоящей работе рассматривается подход к построению структурных моделей узлов CPS, основу которой составляет совместное использование аппарата схем сопряжения [6] и таблиц истинности, характеризующих логическую связь между сигналами на входах и выходах функциональных компонент в составе узлов CPS. Использование схем сопряжения позволяет, во-первых, в единой форме отобразить взаимное влияние процессов, имеющих место в физических и программных компонентах узлов CPS. Это обеспечивается за счет того, что описание взаимодействия осуществляется посредством абстрактного понятия «сигнал». Во-вторых, включает в себя в качестве частных случаев известные сценарные подходы к изучению отказов (FTA[7], ETA[8], RCA[9, 10]). В-третьих, позволяет сформировать в рамках концепции профилей [11, 12] совокупность моделей для разноаспектного анализа причин и последствий отказов (в том числе частичных) в компонентах, входящих в состав CPS.

Краткая характеристика методов проактивного управления функциональной безопасностью субъектоцентрических систем

«Модель швейцарского сыра». Авторами «модели швейцарского сыра» (англ. – Swiss Cheese Model – SCM) являются John Wreathall и J. Reason. SCM является

метафорой, получившей широкое распространение при исследовании инцидентов, имеющих место в субъекто-центрических технических системах (к числу которых относятся медицинские системы; системы управления летательными аппаратами; аппаратно-программные комплексы. Следуя результатам, изложенным в [13], одним из подходов к изучению CPS следует выделить тот, который основан на рассмотрении киберфизических систем как разновидности субъекто-центрических систем).

Концептуальную основу CPS составляет положение о том, что инцидент является результатом совмещения на одной линии источника опасности (hazard) и латентных дефектов (именуемых «дырами» – holes), присутствующих в слоях иерархически организованной системы. Результатом такого совмещения является возникновение пути преобразования опасности в инцидент.

Предотвращение преобразования опасности в инцидент основано на формировании в каждом слое защитных барьеров, именуемых hard defences (к ним относятся проектные и конструкторские решения) и soft defences (к ним относятся процедуры, правила, инструкции, обучение). В литературе описаны три модификации системных моделей (Mark-I, Mark-II, Mark-III), разработанных в рамках метафоры SCM. SCM выполняет следующие роли:

1) SCM как концепция. Фокусом концепции является положение о том, что никакой инцидент не может быть обусловлен единственной причиной. Инцидент является результатом непредсказуемого сочетания нескольких факторов, истоки которых разнесены в пространстве и во времени. Выделяется системная составляющая инцидента, обусловленная нерациональными организационными, проектными и технологическими решениями, и являющаяся причиной возникновения латентных дефектов. Случайные, непредсказуемые внешние воздействия приводят к активизации латентных дефектов («дыр» в слоях системы).
2) SCM как коммуникационная основа. Фокусом этой роли является то, что SCM позволяет на систематической основе обеспечить коммуникации специалистов в различных предметных областях при расследовании причин инцидентов.
3) SCM как база для анализа. Инцидент объясняется возникающей во времени каузальной цепочкой различного рода недостатков (англ. – deficiencies). Наличие недостатков не означает, что инцидент обязательно произойдет. При формировании каузальных цепочек исходят из того, что одно негативное событие может породить другое негативное событие, что в итоге может привести к инциденту. Однако в рамках этой роли не представляется возможным объяснить инциденты, имеющие место в случае, когда нет видимых причин инцидентов, т.е. в случае, когда все контролируемые параметры компонентов CPS лежат в допустимых границах.
4) SCM как основа построения прогностических моделей. SCM ориентирует на выделение ограниченного набора «показателей здоровья» технических систем, исследование изменения которых во времени создает основу для решения задач краткосрочного прогнозирования. Результатом решения задачи прогнозирования является оценка возможности возникновения разных инцидентов (областью применимости моделей является ограниченное число (10-12) классов отказов). При этом точность оценивания времени и места возникновения инцидентов достаточно низкая.

Прогностические модели, реализованные в рамках SCM, позволяют получить достаточно грубые (но устойчивые) результаты, обладающие низкой разрешающей способностью. Эти модели ориентированы на выделение в системе функций, повреждение которых может послужить причиной различного рода инцидентов.

Ограничениями SCM являются следующие:

1) Предполагается линейная схема преобразования источника опасности в инцидент. Не учитывается то обстоятельство, что латентные дефекты в вышестоящих слоях иерархической системы могут быть обусловлены ошибочным реагированием на отказы, ранее имевшие место в нижележащих слоях.

2) Предполагается, что каузальные цепочки возникают хаотично. Отсутствуют подходы к ранжированию возможности реализации инцидентов, обусловленных различными каузальными цепочками.

3) Не предусмотрена возможность одновременного возникновения инцидентов разной природы.

4) Постулируется линейная упорядоченность событий во времени. Однако из того, что событие А предшествовало событию В, не следует, что А является причиной В. В рамках SCM не представляется возможным указать события – коренные причины инцидентов, разнесенные в пространстве и во времени.

5) Не определен подход для оценивания вклада субъективной, организационной и технологической составляющих в возникновение латентных дефектов.

Методы диверсионного анализа. В [14] описан подход Anticipatory Failure Determination – AFD, в отечественной литературе известный как «диверсионный анализ».

Концептуальную основу AFD составляет положение: обнаружение и идентификация отказов есть творчество, которое, тем не менее, может реализовываться в рамках системного подхода.

Областью применимости AFD являются все виды деятельности, в которых:

- Необходимо обнаружить коренные причины ошибок; неудачных действий; отказов или инцидентов, имеющих место в технических системах;
- Предупредить возникновение проблемных ситуаций и ошибок;
- Разработать эффективные подходы, обеспечивающие предупреждение возникновения проблемных ситуаций.

Методическую основу AFD составляет решение системы задач: во-первых, выявление и идентификация сценариев событий, во-вторых, квантификация возможности реализации различных сценариев; в-третьих, квантификация ущерба, соответствующая каждому из сценариев. Формально этому соответствует модель вида (1).

$$R = \{< S_i, L_i, X_i >\}_c, \quad (1)$$

где S_i – i-ый сценарий событий, L_i – квантификация возможности реализации i-го сценария, X_i – квантификация ожидаемого ущерба от реализации i-го сценария.

AFD является обобщением известных методов сценарного анализа: Failure Tree Analysis (FTA); Fault and Event Trees; Hazard and Operations Analysis (HAZOP).

Основными задачами построения сценариев отказов являются:

а) Построение сценария штатного функционирования объекта S_0.

б) Определение множества инициирующих событий $\{IE\}$ (Initiating Events), нарушающих S_0. Инициирующие события могут быть как внешними, так и происходящими внутри самой системы.

в) Построение в виде ориентированного помеченного графа $G_i = (v_i, e_i)$ сети событий, вызываемых IE_i. Каждый путь в этой сети соответствует сценарию преобразования IE_i в X_i. Последствия реализации сценария могут быть позитивными (benign end state - BES), либо негативными (harmful end state - HES). Каждый узел сети представляет собой «слово в сценарии», т.е. одно из событий в казуальной цепи преобразования IE_i в X_i.

г) Построение на основе G_i надграфа G, соответствующего всем элементам множества $\{IE\}$.

Сценарии событий строятся для каждой из выделенных компонент системы. Иными словами, конечные результаты сценариев в одном компоненте системы могут являться инициирующими событиями сценариев в другом компоненте.

Выделяют три типа структурных моделей:

1) Построение каузальных цепочек для оценки множества последствий $\{X_i\}$ инициирующего события IE_i , соответствующего отклонению от режима штатного функционирования S_0 («нисходящий» подход к оценке последствий инициирующих событий).

2) Выделение множества каузальных цепочек для оценки инициирующих событий $\{IE_i\}$, способных оказаться причиной исхода X_i («восходящий» подход к оценке причин наблюдаемых исходов).

3) Объединение «нисходящего» и «восходящего» подходов. Инициирующее событие рассматривается как исход элемента множества предыдущих инициирующих событий. Узлам каузальных цепочек, соответствующих сценариям HES, ставятся в соответствие «деревья событий» (event trees), дающие формальное описание условий реализации звена цепочки.

В рамках AFD различают два подхода: AFD-1 и AFD-2. Первый ориентирован на выявление причин отказов, которые уже имели место. Второй ориентирован на установление возможных причин еще не произошедших отказов.

Концептуальную основу AFD-1 составляет переход от вопроса «Почему произошел наблюдавшийся отказ» к вопросу «Какими способами можно обеспечить отказ, который имел место?». С точки зрения сценарного анализа AFD-1 имеет целью поиск каузальных цепочек $S_i^{(k)}$ в k-м слое изучаемой системы $IE_i^{(k)} \to X_i^{(k)}$.

Концептуальную основу AFD-2 составляет переход от вопроса «Что в системе может пойти неправильно?» (главный вопрос задачи оценивания рисков – Quantative Risk Assessment – QRA) к вопросу «Если необходимо нанесение ущерба требуемого масштаба, какой способ вызвать отказ требуемого вида является наиболее эффективным». С точки зрения сценарного анализа AFD-2 имеет целью установить все возможные цепочки $IE_i^{(k)} \to \{X^{(k)}\}_i$, $X_i^{(k)} \to \{IE^{(k)}\}_i$; а также все возможные каузальные цепочки $X_i^{(k-1)} \to \{IE^{(k)}\}_i$, $X_i^{(k)} \to \{IE^{(k+1)}\}_i$. Из анализа особенностей AFD-1, AFD-2 можно сделать заключение, что их формальную основу составляют модели, с разных сторон характеризующие влияние компонент системы на ее функциональную безопасность в рамках выбранной структуры системы.

Научная идея подхода к построению моделей отказов

В работе [15] показано, что свойства системы определяются ее устройством, а также свойствами окружающей ее среды. Устройство системы можно описать посредством описания свойств компонент системы и связей между компонентами.

На ранних стадиях проектирования в силу необходимости обеспечения рассмотрения физических и программных компонент узлов CPS на одном уровне абстракции компоненты целесообразно представлять в виде «черного ящика», а связь входных и выходных параметров компонентов описывать посредством таблиц истинности.

Для унификации описания связей между физическими и программными компонентами узла CPS целесообразно использовать некое абстрактное понятие, инвариантное к физической природе связей. Известен подход к описанию структуры

системы посредством аппарата схем сопряжения [6]. Особенностью этого подхода является, во-первых, многомерность представления функциональных возможностей компонент системы. Во-вторых, возможность унифицированного описания различных по физической природе связей посредством понятия «сигнал». В-третьих, возможность унифицированной формы описания связей между компонентами системы и внешней средой.

В качестве базы для сопоставления свойств физических устройств и программных компонентов выступает понятие «отказ», являющийся проявлением скрытых латентных дефектов. Конкретное содержание этого понятия определяется назначением функциональных компонент узлов CPS.

В качестве технологической основы для построения различных статических структурных моделей отказов и их последствий предлагается совместно использовать схемы сопряжения и таблицы истинности. Предлагаемый подход является реализацией одного из принципов построения моделей сложных систем – принципа полиморфизма.

Примеры структурного моделирования отказов

Совместное использование схем сопряжения и таблиц истинности создает основу для построения структурных моделей, обеспечивающих моделирование отказов в рамках как нисходящего, так и восходящего подходов к исследованию отказов. Также создает основу для исследования (в рамках реализации концепции профилей) последствий нарушения функционирования разных компонентов, входящих в состав системы, на функционирование других компонентов.

Проиллюстрируем реализацию предлагаемого подхода следующим примером. Предположим, известен возможный сценарий S_0 функционирования узла CPS [14]. Этот сценарий представляет собой упорядоченную во времени последовательность реализации логически завершенных этапов. Каждый из этапов представляет собой совокупность взаимосвязанных функциональных компонентов, взаимодействие которых представлено на Рисунке 1.

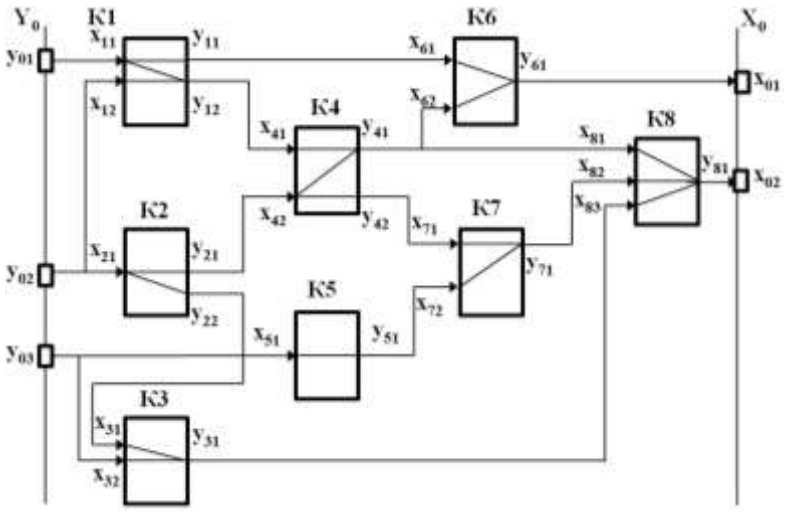

Рисунок 1 – Схема сопряжения компонентов системы
Figure 1 – Scheme of interfacing of system components

На Рисунке 1 обозначено:

x_{km} – входные контакты компонентов и внешней среды;

y_{km} – выходные контакты компонентов и внешней среды;

k – признак компонента (для внешней среды k=0);

m – признак входа/выхода компонента.

В свою очередь, каждому из компонентов ставится в соответствие таблица истинности (примеры таблиц истинности, соответствующих компонентам K1 и K8, представленных на Рисунке 1, представлены на Рисунке 2). В таблицах «0» соответствует ошибке, «1» корректному состоянию.

K1

inputs		outputs	
x_{11}	x_{12}	y_{11}	y_{12}
0	0	0	0
0	1	0	0
1	0	1	0
1	1	1	1

K8

inputs			outputs
x_{81}	x_{82}	x_{83}	y_{81}
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Рисунок 2 – Таблицы истинности

Figure 2 – Truth tables

На Рисунке 3 представлена структурная модель, составляющая основу моделирования отказов в рамках нисходящего подхода FTA [7].

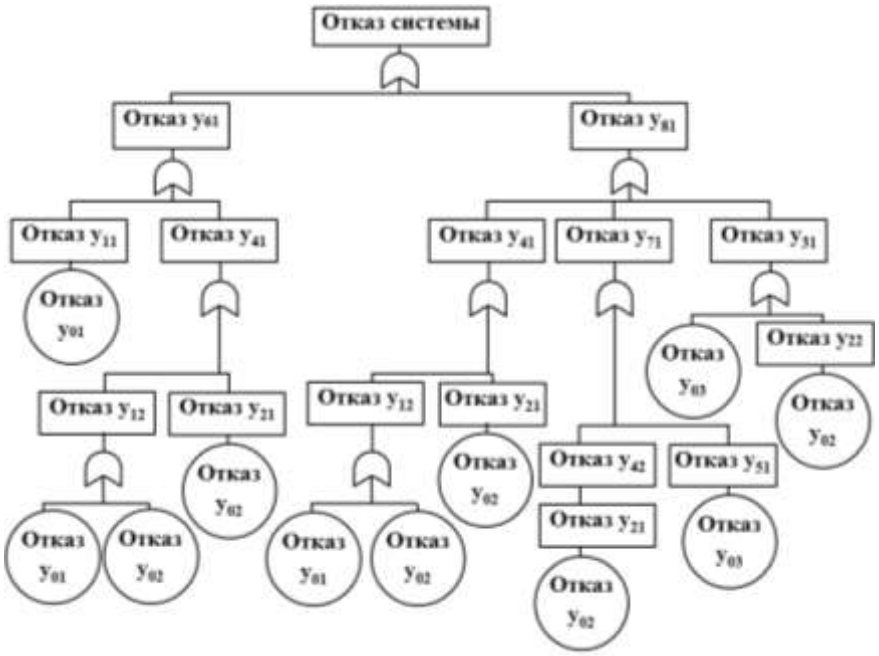

Рисунок 3 – Дерево отказов, соответствующее схеме сопряжения (Рисунок 1) с учетом характера таблиц истинности

Figure 3 – The fault tree corresponding to the interface circuit (Figure 1), taking into account the nature of the truth tables

На Рисунке 4 представлена структурная модель, составляющая основу моделирования отказов в рамках восходящего подхода ETA.

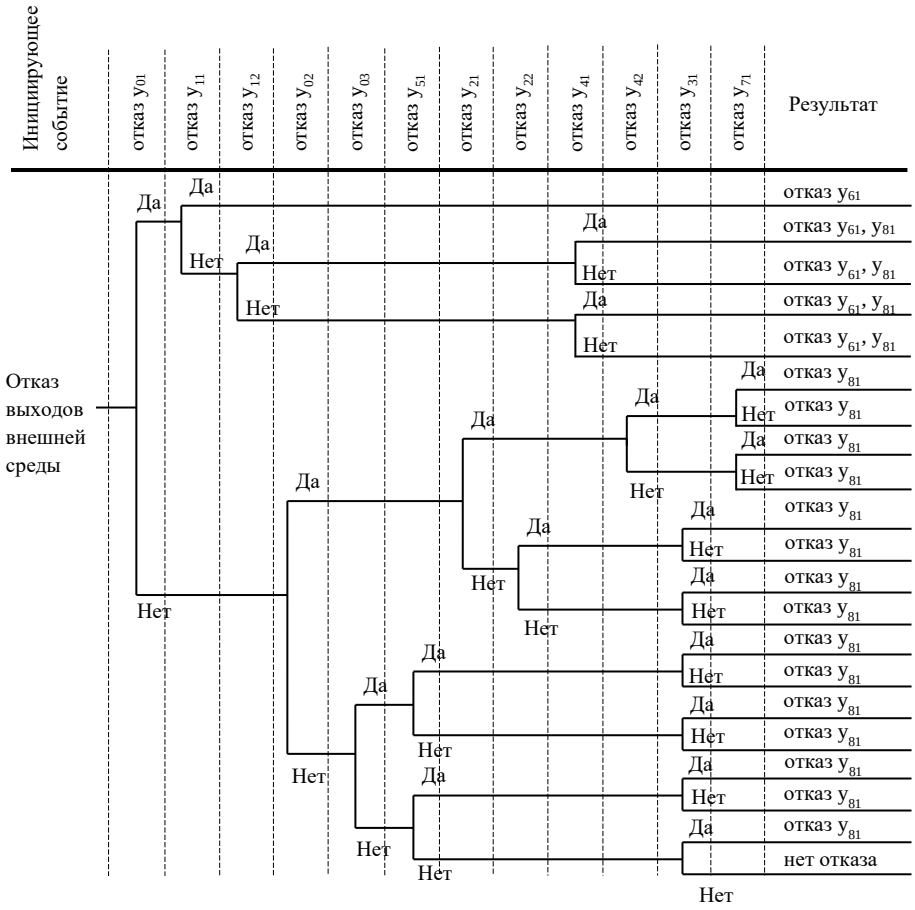

Рисунок 4 – Дерево событий, соответствующее схеме сопряжения (Рисунок 1) с учетом характера таблиц истинности

Figure 4 – The event tree corresponding to the conjugation scheme (Figure 1), taking into account the nature of the truth tables

На Рисунке 5 представлена структурная модель, составляющая основу выявления возможных коренных причин отказов на основе подхода RCA.

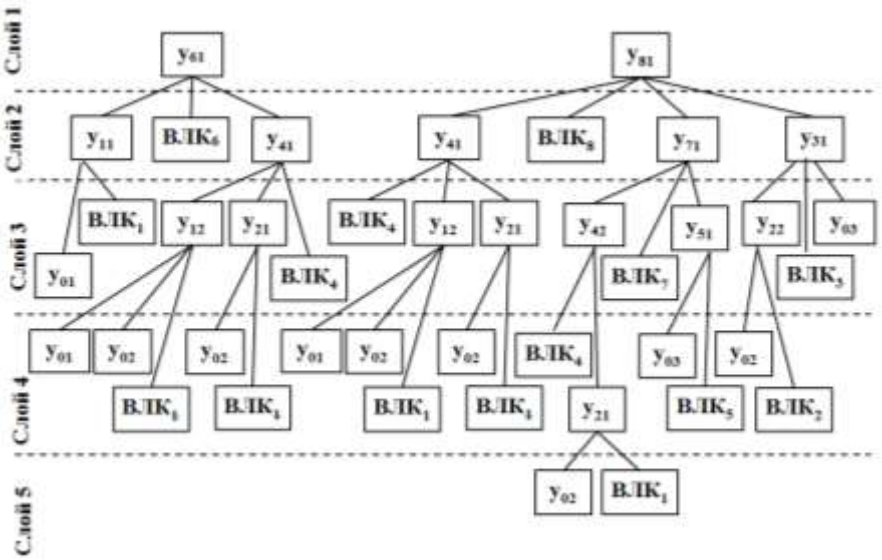

Рисунок 5 – Выявление коренных причин отказов методом RCA

Figure 5 – Identification of the root causes of failures by RCA

Выделенные на Рисунке 5 слои имеют следующий смысл: слой 1 – слой симптомов, слой 2 – слой непосредственных причин, слой 3 – слой причин первого порядка, слой 4 – слой причин второго порядка, слой 5 – слой причин третьего порядка. В рамках этой модели отражено то обстоятельство, что симптомы отказов, наблюдаемые на выходах этапа (y_{61} и/или y_{81}) могут быть обусловлены не только неверными значениями сигналов на входах компонентов системы, но и нарушением внутренней логики компонентов ВЛК$_i$ ($i = \overline{1;8}$) из-за активизации латентных дефектов, имеющихся в компонентах.

На Рисунке 6 представлены FishBone – диаграммы, являющиеся иной формой представления модели, представленной на Рисунке 5.

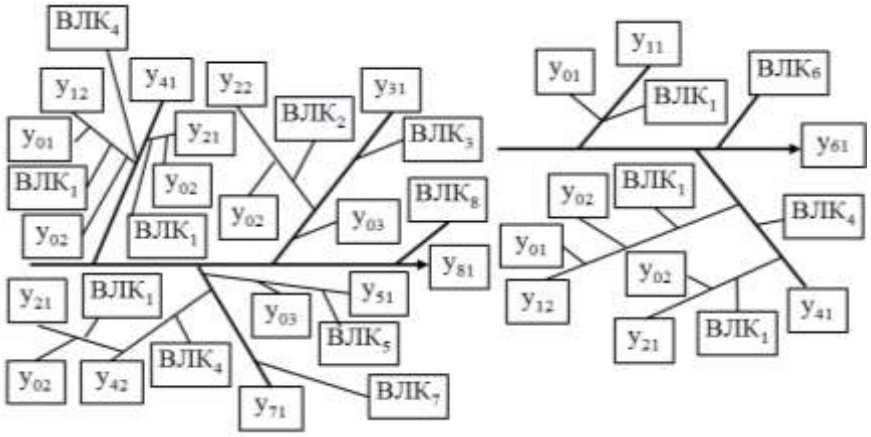

Рисунок 6 – Модели причинно-следственных связей, соответствующие модели анализа коренных причин

Figure 6 – Model of cause-effect relationships corresponding to the RCA

На Рисунке 7 и Рисунке 10 представлены модели, построенные в рамках известной концепции профилей [11, 12].

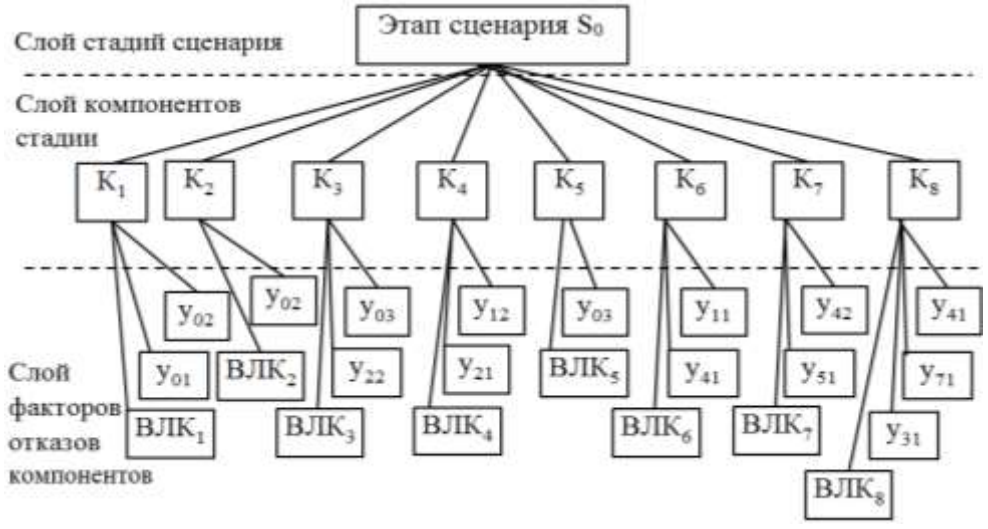

Рисунок 7 – Профиль непосредственных причин отказов компонентов

Figure 7 – Profile of the immediate causes of component failures

Профиль, представленный на Рисунке 8, характеризует количество факторов, определяющих безопасное функционирование каждого из компонент системы, представленной на Рисунке 1.

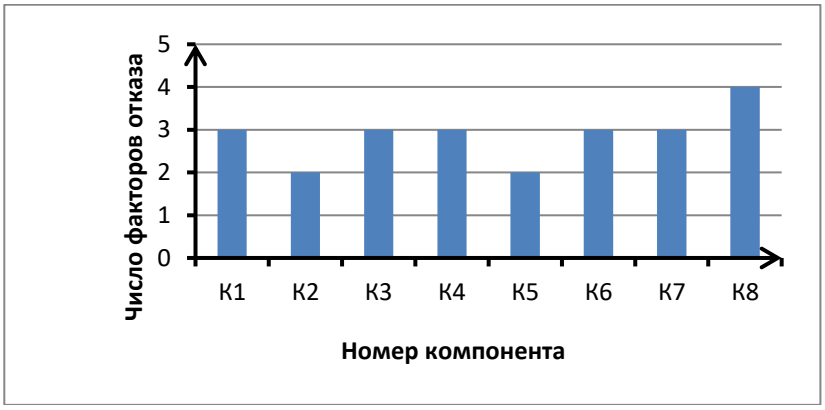

Рисунок 8 – Профиль числа факторов, определяющих безопасное функционирование каждого из компонентов
Figure 8 – Profile of the number of factors determining the safe functioning of each component

Профиль, представленный на Рисунке 9, характеризует число компонентов, на которые передаются сигналы с l-го выхода k-ой компоненты (l,k).

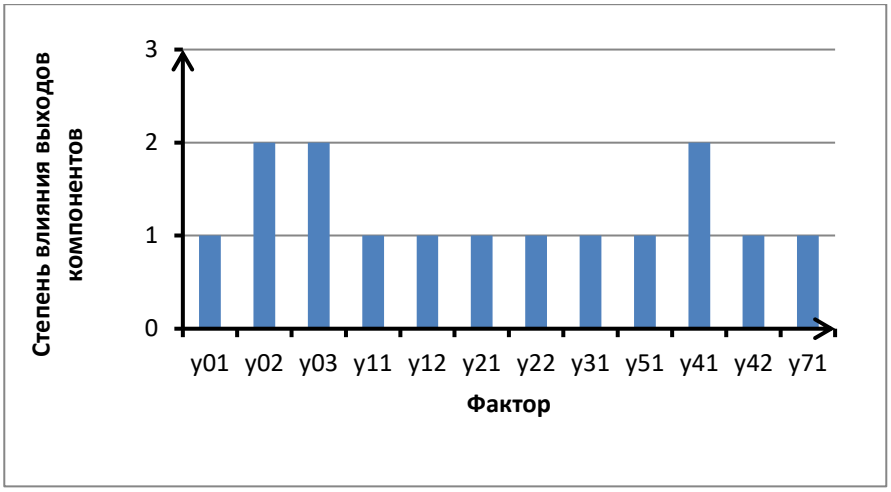

Рисунок 9 – Профиль числа компонентов, которые оказываются под влиянием данного фактора
Figure 9 – Profile of the number of components that are influenced by the factor

На Рисунке 10 представлена модель, позволяющая определить транзитивное влияние каждого из компонентов системы K_i $(i = \overline{1;8})$ на выходы других компонентов.

Рассмотренный пример позволяет заключить, что описание систем посредством совместного использования схем сопряжения и таблиц истинности создают базу для разноаспектного анализа функциональной безопасности узлов CPS на ранних стадиях проектирования киберфизических систем.

Это, в свою очередь, создает информационную основу для сравнения альтернативных вариантов проектных решений по критерию функциональной безопасности, а также для распределения ресурсов, направленных на обеспечение

функционирования компонентов CPS с учетом их значимости для функциональной безопасности киберфизической системы.

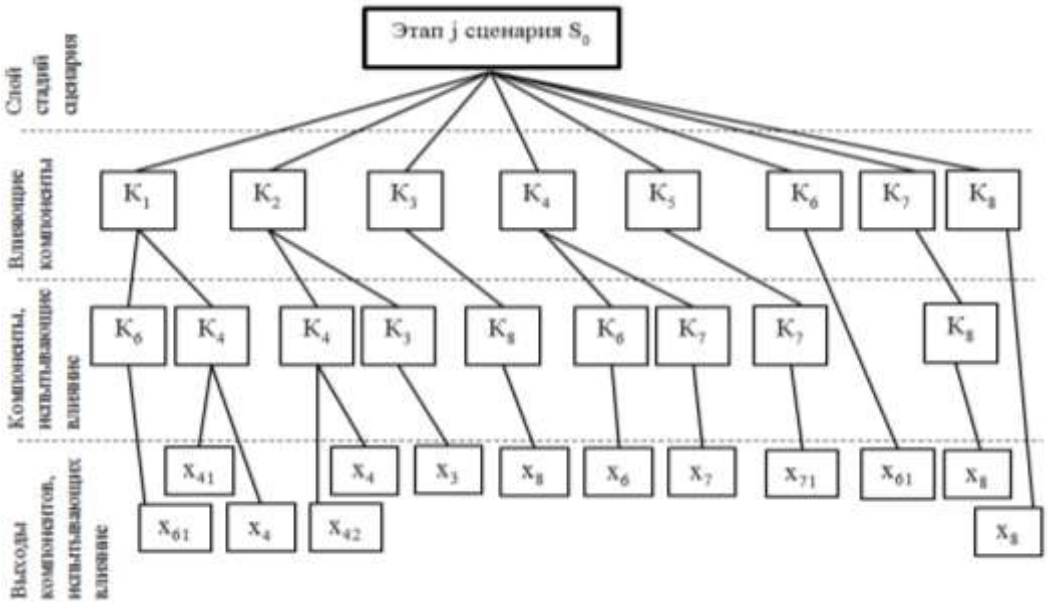

Рисунок 10 – Профиль транзитивного влияния компонентов
Figure 10 – Profile of transitive influence of components

Заключение

Одним из основных требований к CPS является функциональная безопасность [13]. Традиционные методы управления функциональной безопасностью аппаратно-программных комплексов ориентированы на использование объектов в заранее оговоренных условиях. Особенностью CPS является то, что они являются узлами гетерогенной динамической сети, свойства которой меняются случайным образом. В силу этого традиционные методы управления функциональной безопасностью сложных технических систем применительно к CPS имеют ограниченное применение.

В литературе с начала 90-х годов прошлого столетия в рамках теории управления рисками обсуждается подход к обеспечению функциональной безопасности субъектоцентрических систем известный как метафора «Swiss Cheese Model». Концептуальную основу этого подхода составляет положение о неизбежности наличия в сложных технических системах латентных дефектов разной природы, условия активизации которых предсказать невозможно. Из этого вытекает необходимость создания барьеров, препятствующих преобразованию опасности в инцидент [3, 4].

Предлагаемый в настоящей работе подход к построению системы структурных моделей на основе аппарата схем сопряжения и таблиц истинности функциональных компонентов следует рассматривать с позиций информационной поддержки формирования барьеров. В качестве ближайшей задачи дальнейших исследований следует выделить разработку методов исследования свойств многофункциональных объектов (к числу которых относится CPS) при случайных внешних воздействиях и случайных изменениях структуры сигналов в системе.

Благодарности

Работа поддержана грантом 19-08-00177 Методологические, теоретические и модельные основы управления функциональной безопасностью аппаратно-программных комплексов в составе распределенных сложных технических систем.

ЛИТЕРАТУРА

1. Shappell S.A. The Human Factors Analysis and Classification System – HFACS, Final Report, U.S. Department of Transportation, Federal Aviation Administration, 2000.
2. Lee E.A. Cyber Physical Systems: Design Challenges. *Electrical Engineering and Computer Sciences*. 10.1109/ISORC.2008.25. 2008:363-369.
3. Reason J., Hollnagel E., Paries J., *Revisiting the «Swiss Cheese» Model of Accidents, EEC Note No. 13/06. European Organization for the Safety of Air Navigation.* 2006.
4. Perneger T.V. *The Swiss cheese model of safety incidents: Are there holes in the metaphor?* BMC Health Services Research. 5. 71. 10.1186/1472-6963-5-71, 2005. Available at: https://www.researchgate.net/publication/7488318_The_Swiss_cheese_model_of_safety_incidents_Are_there_holes_in_the_metaphor (accessed 20.01.2020).
5. Thorogood J.L., Lauche K., Crichton M., Pollard I., Hviid L.B., Verweijen B., *Getting to Grips with Human Factors in Drilling Operations*. Society of Petroleum Engineers, DOI:10.2118/173104-MS. 2015.
6. Бусленко Н.П. *Моделирование сложных систем.* М.: Наука. 1978.
7. ГОСТ 51901.13-2005. *Менеджмент риска. Анализ дерева неисправностей*. Доступно по: http://docs.cntd.ru/document/gost-r-51901-11-2005 (дата обращения 13.02.2020).
8. ГОСТ 62502-2014. *Менеджмент риска. Анализ дерева событий.* Доступно по: http://docs.cntd.ru/document/1200114221 (дата обращения 13.02.2020).
9. Jucan G., *Root Cause Analysis for IT Incidents Investigation*. Available at: https://docplayer.net/3945984-Root-cause-analysis-for-it-incidents-investigation.html (accessed 15.01.2020)
10. R. Soni, A. Preet, Cognitive Approach to Root Cause Analysis for Improvement Quality of Life: A Case Study for IT industry. *International Journal of Informative and Futuristic Research*. 2013:1(1). Available at: https://pdfs.semanticscholar.org/cd2d/a82fe166bece80319041709e04ab5002129f.pdf (accessed 15.01.2020)
11. Мороз Г., Коваль Г., Коротун Т. Концепция профилей в инженерии надежности программных систем. *Математические машины и системы*. 2004;1:166-182.
12. Cheung R. A User-oriented Software Reliability Model. IEEE Trans. Soft. Eng. 1980;6(2):11-125.
13. Nunes D., Sa Silva J., Boavida F. A Practical Introduction to Human-in-the-Loop Cyber-Physical Systems. John Wiley & Sons Ltd. 2018.
14. Visnepolschi S., Zlotin B., Kaplan S., Zusman A. *New Tools for Failure and Risk Analysis Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*. Ideation Intl Inc. 1999.
15. Медоуз Д. *Азбука системного мышления.* М.: Бином. 2010.

REFERENCES

1. Shappell S.A. *The Human Factors Analysis and Classification System – HFACS*, Final Report, U.S. Department of Transportation, Federal Aviation Administration, 2000.
2. Lee E.A. Cyber Physical Systems: Design Challenges. *Electrical Engineering and Computer Sciences*. 10.1109/ISORC.2008.25. 2008:363-369.
3. Reason J., Hollnagel E., Paries J., *Revisiting the «Swiss Cheese» Model of Accidents, EEC Note No. 13/06. European Organization for the Safety of Air Navigation*. 2006.
4. Perneger T.V. *The Swiss cheese model of safety incidents: Are there holes in the metaphor?* BMC Health Services Research. 5. 71. 10.1186/1472-6963-5-71, 2005. Available at: https://www.researchgate.net/publication/7488318_The_Swiss_cheese_model_of_safety_incidents_Are_there_holes_in_the_metaphor (accessed 20.01.2020).
5. Thorogood J.L., Lauche K., Crichton M., Pollard I., Hviid L.B., Verweijen B., Getting to *Grips with Human Factors in Drilling Operations.* Society of Petroleum Engineers, DOI:10.2118/173104-MS. 2015.
6. Buslenko N.P. *Complex system modeling.* Moscow. 1978.
7. State Standard 51901.13-2005. *Risk management. Fault Tree Analysis*. Available at: http://docs.cntd.ru/document/gost-r-51901-11-2005 (accessed 13.02.2020).
8. State Standard 62502-2014. *Risk management. Event Tree Analysis*. Available at: http://docs.cntd.ru/document/1200114221 (accessed 13.02.2020).
9. Jucan G., *Root Cause Analysis for IT Incidents Investigation.* Available at: https://docplayer.net/3945984-Root-cause-analysis-for-it-incidents-investigation.html. (accessed 15.01.2020)
10. R. Soni, A. Preet, Cognitive Approach to Root Cause Analysis for Improvement Quality of Life: A Case Study for IT industry. *International Journal of Informative and Futuristic Research*. 2013:1(1). Available at: https://pdfs.semanticscholar.org/cd2d/a82fe166bece80319041709e04ab5002129f.pdf (accessed 15.01.2020)
11. Moroz G., Koval G., Korotun T. The concept of profiles in the reliability engineering of software systems. *Mathematical machines and systems*. 2004;1:166-182.
12. Cheung R. A User-oriented Software Reliability Model. IEEE Trans. Soft. Eng. 1980;6(2):11-125.
13. Nunes D., Sa Silva J., *Boavida F. A Practical Introduction to Human-in-the-Loop Cyber-Physical Systems*. John Wiley & Sons Ltd. 2018.
14. Visnepolschi S., Zlotin B., Kaplan S., Zusman A. *New Tools for Failure and Risk Analysis Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*. Ideation Intl Inc. 1999.
15. Meadows D. *Thinking in systems*. Moscow. 2010.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Гузаиров Мурат Бакеевич, д.т.н., профессор, кафедра вычислительной техники и защиты информации, ФГБОУ ВО "Уфимский государственный авиационный технический университет", Уфа, Российская Федерация.
e-mail: mbguzairov@gmail.com

Murat B. Guzairov, Grand PhD in Engineering sciences, Professor, Department of Computer Engineering and Information Protection, Federal State Budgetary Educational Institution of Higher Education "Ufa State Aviation Technical University", Ufa, Russian Federation.

Гвоздев Владимир Ефимович, д.т.н., профессор, кафедра технической кибернетики, ФГБОУ ВО "Уфимский государственный авиационный технический университет", Уфа, Российская Федерация.
e-mail: wega55@mail.ru

Бежаева Оксана Яковлевна, к.т.н., доцент, кафедра технической кибернетики, ФГБОУ ВО "Уфимский государственный авиационный технический университет", Уфа, Российская Федерация.
e-mail: obezhaeva@gmail.com

Курунова Роксана Рафаиловна, к.т.н., старший преподаватель, кафедра технической кибернетики, ФГБОУ ВО "Уфимский государственный авиационный технический университет", Уфа, Российская Федерация.
e-mail: roksana.kurunova@gmail.com

Насырова Рима Айратовна, магистрант, кафедра технической кибернетики, ФГБОУ ВО "Уфимский государственный авиационный технический университет", Уфа, Российская Федерация.
e-mail: nasyrova.rima@yandex.ru

Vladimir E. Gvozdev, Grand PhD in Engineering sciences, Professor, Department of Technical Cybernetics, Federal State Budgetary Educational Institution of Higher Education "Ufa State Aviation Technical University", Ufa, Russian Federation.

Oxana Y. Bezhaeva, PhD in Engineering sciences, Associate Professor, Department of Technical Cybernetics, Federal State Budgetary Educational Institution of Higher Education "Ufa State Aviation Technical University", Ufa, Russian Federation.

Roxana R. Kurunova, PhD in Engineering sciences, senior lecturer, Department of Technical Cybernetics, Federal State Budgetary Educational Institution of Higher Education "Ufa State Aviation Technical University", Ufa, Russian Federation.

Rima A. Nasyrova, Master's Degree student, Department of Technical Cybernetics, Federal State Budgetary Educational Institution of Higher Education "Ufa State Aviation Technical University", Ufa, Russian Federation.