ПОВЫШЕНИЕ ДОСТУПНОСТИ ПРОМЫШЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ НА ОСНОВЕ БИМОДАЛЬНОЙ СЕТИ С ВЕЙРОНАМИ

Полетыкин А.Г., Промыслов В.Г., Семенков К.В., Менгазетдинов Н.Э.
Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
poletik@ipu.ru, vp@ipu.ru, semenkovk@ipu.ru, mengazne@ipu.ru

Аннотация. Предлагается набор решений для повышения доступности цифровой системы управления. Решения включают выбор компонентов системы управления, специальная топология сети со свойствами малого мира и методы диагностики.

Ключевые слова: доступность, вейрон, топология, малый мир, архитектура, безопасность, АСУ ТП.

Введение

Современные цифровые программируемые автоматизированные системы управления технологическими процессами (АСУ ТП) особенно для таких не простых технических объектов, как атомные электростанции (АЭС), имеют сложную структуру. Обычно такие системы создаются по принципу распределенной архитектуры, обеспечивающей обмен информацией между компонентами системы. Обмен информацией является жизненно важной частью способности системы выполнять свои функции.

Необходимость взаимодействия компонентов АСУ ТП для выполнения функций накладывает ограничения на резервирование линий связи, производительность компонентов и объем передаваемой информации. Эти ограничения. в сочетании с другими требуемыми проектными характеристиками, следует учитывать при разработке системы и далее постоянно оценивать их и поддерживать на других этапах жизненного цикла.

В настоящее время в соответствии с принципом безопасного проектирования АСУ ТП [1] все большее значение приобретают ограничения, связанные с информационной безопасностью (ИБ). В информационной безопасности основными свойствами, которые характеризуют качество информации, являются конфиденциальность, целостность и доступность, а совокупность этих основных свойств называется моделью КЦД. Для промышленных АСУ ТП на первый план в модели КЦД выходят свойства, связанные с доступностью [2,3].

Доступность является комплексным свойством [4,5] и в зависимости от дисциплины, контекста задачи, конкретного объекта она может включать в себя элементы связанные с обеспечение надежности, отказоустойчивости системы, управления доступом и временные показатели системы. Выделим далее три основных «измерения доступности» для рассмотрения:

- характеристики компонентов системы АСУ ТП
- топология сети обмена информацией между компонентами АСУ ТП
- методы оценки доступности и диагностирование состояния системы.

В работе рассматриваются несколько решений, обеспечивающие повышенную доступность в каждом из выделенных измерений.

Выбор элементной базы для компонентов системы во многом влияет на систему в целом, включая ее архитектуру и сейчас используются различные вычислительные архитектуры для построения АСУ ТП [6,7]. Для перспективной АСУ ТП с повышенными свойствами доступности был выбраны типовые элементы на основе ARM процессоров с расширенным набором интерфейсов для обмена информацией вейрон [8].

Сетевая топология системы определяется в рамках проектирования системы основываясь на многих, часто взаимоисключающих требований к системе. Очевидно, что на нее влияют коммуникационные возможности компонентов, требования к надёжности и временным характеристикам отдельных компонентов, взаимодействующих при выполнении функции управления системой. Расширенные коммуникационные возможности вейрона, позволяют при необходимости реализовать сложные топологии в отличии от простых регулярные топологии сетей, которые в основном используются сейчас в АСУ ТП [9]. Переход от простой регулярной топологии сети к сетям имеющие сложную топологию, например это может быть например само подлобные сети [10] или сложные регулярные топологии [11], позволяет повысить отказоустойчивость сети АСУ ТП при случайном отказе отдельных компонентов, за счет большого числа альтернативных маршрутов обмена информацией между компонентами системы. В то же время выбор топологией со специальной структурой, например, обладающие свойствами малого мира [12, 13] обеспечивает необходимые

временные характеристики системы и работоспособность сети при целенаправленном на нее воздействие, что важно для обеспечения кибербезопасности АСУ ТП.

Временные показатели системы могут оцениваться как с точки зрения неких усредненных, характеристик, отражающих поведение системы в целом [5], например с применением вероятностных моделей, так и детерминированных моделей [14], или мгновенных показателей, характеризующих поведение системы в определенный момент времени получаемых путем прямых измерений.

В работе рассматривается перспективная АСУ ТП, где реализованы основные меры повышения доступности во всех трех выделенных измерениях доступности. Разработана методология позволяющая осуществить переход от традиционной топологии сети АСУ ТП к топологии с повышенными характеристиками доступности. Приведен пример перехода от простой регулярной топологии сети АСУ ТП, типа кольцо к бимодальной топологии n-star со свойствами малого мира.

1. Вейрон как базовый вычислительный элемент АСУ ТП

Одной из типовых проблем современных АСУ ТП критических объектов является гетерогенность ее компонентов. Такое разнообразие во многом обусловлена с одной стороны специфичностью технических требований, предъявляемых к каждой подсистеме в составе АСУ ТП, с другой стороны сложившимся распределением обязанностей между различными предприятиями разработчиками отдельных подсистем. Унификация компонентов желательна для снижения стоимости разработки, повышения ремонтопригодности и снижения стоимости эксплуатации системы.

Однако, одних только организационных мер по обеспечению унификации недостаточно. Гетерогенность компонентов определяется ориентацией SCADA платформ, используемых в качестве интегрирующей подсистемы в АСУ ТП на клиент-серверную модель, когда относительно маломощные рабочие станции с графическим дисплеем соединялись с мощным вычислителем [15]. В качестве такого вычислителя часто использовалось уникальное серверное оборудование стороннего производителя (например Dell, HewlPackard, Huawei). Такой подход был оправдан, когда доминировало, четкое разделение «персонального компьютера» и «сервера» сложившиеся в конце прошлого века. Однако сейчас, при том, что сохраняется условное разделение на настольные «персональные» компьютеры серверные компьютеры, произошло значительное размытие грани между ними, когда настольные компьютеры стали по мощности сравнимы с серверными решениями начала века. Персональные компьютеры стали многозадачными и многопользовательскими, фактически сравнявшись по программным и коммуникационным возможностям с серверными компьютерами. Все это вместе с удешевлением единицы вычислительно мощности, позволяет осуществить организационные меры внедрения унифицированных компонентов в качестве вычислительных узлов сети АСУ ТП на серверном уровне, рабочих станций оператора и даже в некоторых случаях на коммуникационном уровне и уровне контроллеров.

В частности, предлагается реализовать АСУ ТП на однотипных компонентах «вейрон» [8] обладающие «стандартным» набором коммуникационных возможностей и интерфейсов, что позволяет легко заменять и обслуживать его. Вычислительные мощности однокристальных компьютеров, как показало тестирование, проведенное в ИПУ РАН с применением SCADA Оператор [16] позволяют реализовать все функции АСУ ТП для АЭС с сохранением требуемых временных характеристик. Простоя замена «больших» компьютеров современными малогабаритными решениями, является только первым шагом в концепции будущей архитектуры АСУ ТП. Следующий шагом, является переходом от жёсткой топологии АСУ ТП, к гибкой системе, позволяющей повысить отказоустойчивость системы при множественных отказах, при ограничениях на резервируемых компоненты системы.

2. Гибкая сетевая архитектура АСУ ТП

Коммуникационные возможности вейрона дают возможность объединять отдельные компоненты АСУ ТП в сети с заданной топологией, обеспечивая необходимый уровень резервирования сети. Реализация сети на традиционных проводных технологиях не использует полностью коммуникационных возможностей вейронов, но помехоустойчивость, детерминированность поведения, кибер защищённость проводных каналов во многом будут определять дальнейшее доминирование проводных технологий в системах выполняющие критические функции АСУ ТП важные для безопасности объекта управления.

Однако переход к беспроводным технологиям, ставшими обычными в интернет вещей в некоторых системах АСУ ТП, где требования безопасности не вступает в противоречие с характеристиками

беспроводных сетей имеет большие перспективы. Например, в стандарте Международной Электротехнической Комиссии (МЭК) для АСУ ТП АЭС [17] указаны требования реализация которых позволят применить беспроводную связь в системах не выполняющие критических функций. Такими функциями, например могут быть некоторые функции диагностики, ремонт и обслуживания оборудования, коммуникации и оповещения персонала.

Преимуществами беспроводных линий связи кроме весьма важного свойства отказу от кабельных линий является относительная лёгкость трансформации топологии сети, что обеспечивает гибкость реконфигурации маршрутов при отказе компонента сети если применяется один из протоколов динамической маршрутизации подобный STP [18].

Что бы в полной мере использовать механизм реконфигурации для повышения отказоустойчивости необходимо иметь достаточное количество альтернативных маршрутов. Перспективным направлением может стать переход от классических «простых» топологий сети типа кольцо, звезда или их комбинаций к топологиям, часто возникающим в природе, или социальной среде. Такие топологии могут относиться к типу без масштабных сетей (англ. Scale-free network), которые описываются графом со степенным распределением степени вершин и имеет высокий коэффициент кластеризации, обеспечивающей большое количество маршрутов между компонентами [19]. Произвольная без масштабная сеть не полностью подходит для систем с высокими требованиями к доступности к компонентам, так как пересылка информации между компонентами системы может потребовать значительного количества промежуточных звеньев. От этого недостатка избавлены топологии, удовлетворяющие свойству сетей «Малого мира» (англ. Small World Network), которые с вместе с высоким уровнем резервируемости маршрутов в системе обладают достаточно короткими, порядка логарифма от количества компонентов в системе, средним длинной пути между абонентами системы.

Системы с сетевыми топологиями такого типа могут найти себе применение в вспомогательных подсистемах АСУ ТП позволяя использовать мобильные терминалы для ремонтного персонала или smart датчики, присоединяемые по беспроводным интерфейсам.

Данные топологии не лишена и недостатков. Выделим два из них, которые наиболее важны в контексте промышленных систем:

- «случайность» структуры без масштабных сетей может создать трудности для их применения в подсистемах АСУ ТП с относительно стабильным составом компонентов;
- произвольные сети малого мира, устойчивы к отказу случайных компонентов, но уязвимы для скоординированных атак, которые нацелены на компоненты обеспечивающие «длинные» связи в сети.

Поэтому для АСУ ТП предлагаем применить сети передачи данных с относительно или полностью регулярных топологией, обладающих свойствами сетей малого мира. Возможными топологиями являются, в частности, сети Кэли [13] и n-star [12]. Преимуществом последней является то, что она дополнительно сохраняет свойства малого мира и является устойчивой к целенаправленным атакам.

3. Методология перехода от классической АСУ ТП к регулярным сетям со свойствами малого мира

Рассмотрим основные этапы методологии перехода от АСУ ТП классического типа к АСУ ТП повышенной доступности, использующей решения на основе сети с топологией n-star. Следует учесть, что во основе многих применяемых сетей АСУ ТП лежит топология типа кольцо, сеть типа n-star позволяет относительно легко перейти от сети с топологией типа кольцо к n-star.

В методологии есть три основные этапа:

- Разработать зонную модель основываясь на информационной связанности компонентов выделив основные узлы, обеспечивающие связанность системы [20].
- «Наложить» полученную модель на выбранную топологию n-star расположив основные узлы, обеспечивающие связанность системы в корневых узлах сети с топологией n-star.
- Основываясь на топологии сети настроить основные и дублированные маршруты используя подходящий протокол динамической маршрутизации.

На рисунках (Рис. 1,2) приведен пример перехода от топологии сети АСУ ТП типа кольцо к топологии типа n-star (n=3).

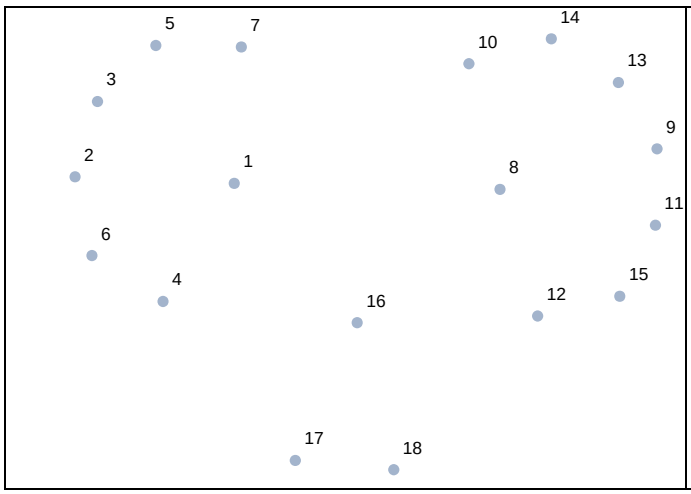

Рис. 1. Топология сети подсистемы типа "кольцо"

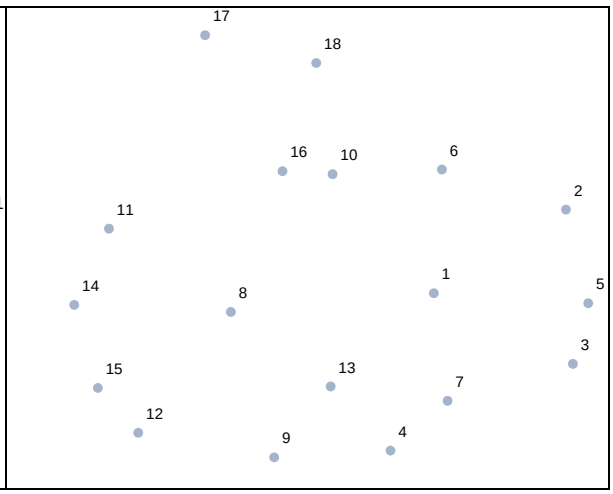

Рис. 2. Топология сети подсистемы типа "3-star" со свойствами малого мира

4. Диагностика временных характеристик на основе детерминированных ограничений

Работоспособность такой системы во многом должна полагаться на своевременное диагностирование отказов и их устранении. Предлагаемая структура сети позволяет во многих случаях осуществить «горячую» замену. Однако без необходимой поддержки со стороны подсистемы диагностики АСУ ТП, отказоустойчивость может привести к тому, что отказы будут накапливаться, до тех пор, пока система исчерпает запас резервируемых компонентов. Поэтому для управления доступностью предлагается расширить функции диагностики АСУ ТП. Отметим, что термин «доступность» используется во многих дисциплинах, связанных с техническими системами, но его интерпретация зависит от области исследования.

Основная отличительная черта доступности при динамической реконфигурации сети, связанной с отказом или ухудшения характеристик ее компонентов заключается в том, что в основном важна «мгновенная» доступность. Это отличается от «общей» системной интерпретации доступности, например, в области надежности, где среднее время между отказами или среднее время доступа обычно рассматриваются как параметры доступности. Для оценки и проверки средних параметров систем были разработаны многочисленные методы, такие как статистические методы или теория массового обслуживания (QST). Для оценки мгновенной доступности предлагается применять метрики и методы оценки, основанные на теории сетевого исчисления, которые позволяют нам получать числовые детерминированные ограничения на временные параметры системы и активно реконфигурировать систему для поддержания доступности до того, как временные характеристики системы выйдут за безопасные пределы [14].

5. Заключение

В работе рассмотрен комплекс решений для повышения доступности АСУ ТП. Решения включают применение:

- однотипных компонентов вейронов с расширенными коммуникационными возможностями;
- специальных топологий сети, объединяющие наличие большого числа альтернативных маршрутов обмена информацией с относительно коротко длинной пути;
- углубленных методы диагностики временных характеристик с применением теории сетевых исчислений.

Данные решения позволяет реализовать АСУ ТП с повышенными требованиями к доступности.

Разработана методология позволяющая перейти от традиционной простой регулярной топологии сети АСУ ТП к топологии, обеспечивающей повышенную доступность, с учетом вышеприведённых решений.

В рамках атомной промышленности, предлагаемые решения могут быть востребованы как в системах управления «классических» АЭС, так и для малых модульных реакторов.

Литература

1. Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series No. NR-T-3.30, IAEA, Vienna (2020).
2. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели.
3. NSS No. 17-T (Rev. 1). IAEA. Computer Security Techniques for Nuclear Facilities. 2021.
4. ГОСТ Р 27.002-2009 Национальный стандарт Российской Федерации, Надежность в технике. Термины и определения.
5. ГОСТ Р ИСО/МЭК 27000-2021Информационные технологии. Методы и средства обеспечения безопасности. Общий обзор и терминология.
6. *Jiang Z. et al.*, "Toward an Analysable, Scalable, Energy-Efficient I/O Virtualization for Mixed-Criticality Systems," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 2, pp. 320-333, Feb. 2022, doi: 10.1109/TCAD.2021.3059566.
7. *Liang Y., Chen L. and Xu B.* Design of multi-channel redundant control system based on DSP and FPGA, 2022 IEEE 6th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Beijing, China, 2022, pp. 76-82, doi: 10.1109/IAEAC54830.2022.9929811.
8. *Полетыкин А.Г., Менгазетдинов Н.Э., Семенков К.В., Жарко Е.Ф., Промыслов В.Г., Бывайков М.Е.* Природоподобные конструкционные узловые компоненты для программно-технические комплексов на основе однокристальных компьютеров // Автоматизация в промышленности. 2023. № 6. С. 12-16.
9. *Didier P.*, Reference Architectures for Industrial Automation and Control Systems. ODVA, 2012 ODVA Industry Conference & 15th Annual Meeting October 16-18, 2012 Stone Mountain, Georgia, USA https://www.odva.org/wp-ontent/uploads/2022/06/2012ODVA_Conference_Didier_FINAL.pdf. (доступ 05/06/2024).
10. *Albert R., Jeong H., and Barabási A.-L.* Error and attack tolerance of complex networks, Nature, vol. 406, no. 6794, pp. 378–382, Jul. 2000, doi: 10.1038/35019019.
11. *Petkov N. and Naumov A*, Overview of Industrial Communication in Process Automation, 2022 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2022, pp. 229-234, doi: 10.1109/ICAI55857.2022.9960067.
12. *Sawai, Hidefumi.* (2013). A Small-World Network Immune from Random Failures and Resilient to Targeted Attacks. Procedia Computer Science. 18. 10.1016/j.procs.2013.05.263.
13. *Xiao W., Parhami B.*, Cayley graphs as models of deterministic small-world networks, Information Processing Letters, Volume 97, Issue 3, 2006, p. 115-117, SSN 0020-0190, https://doi.org/10.1016/j.ipl.2005.10.001.
14. *Промыслов В.Г.* Модель доступности на основе теории сетевого исчисления для потоковой системы обработки данных // Управления большими системами, Выпуск 110, М.: ИПУ РАН, 2024, С. 113-148.
15. Комплекс программ «Программная платформа «SCADA-R» Описание применения. 46865053.00012-01 31https://www.rasu.ru/documents/Scada_description.pdf. (доступ 05/06/2024).
16. *Полетыкин А.Г., Менгазетдинов Н.Э., Жарко Е.Ф., Промыслов В.Г., Бывайков М.Е., Степанов В.Н., Байбулатов А.А., Семенков К.В., Акафьев К.В.* Интеграционная платформ для АСУ ТП - Система Оператор / Труды 16-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD’2023, Москва). М.: ИПУ РАН, 2023. С. 144-148.
17. IEC 62988:2018. Nuclear power plants - Instrumentation and control systems important to safety - Selection and use of wireless devices.
18. *Perlman R.* (2000). Interconnections, Second Edition. USA: Addison-Wesley. ISBN 0-201-63448-1.
19. *Barrat A. and Weigt M.*, “On the properties of small-world network models,” Eur. Phys. J. B, vol. 13, no. 3, pp. 547–560, Jan. 2000, doi: 10.1007/s100510050067.
20. IEC TR 63415. Nuclear Power plants - Instrumentation and control systems - Use of formal security models for I&C security architecture design and assessment. 2023.