Некоторые вопросы безопасности киберфизических корпоративных систем

Тахмасиб Фаталиев[1], Шакир Мехтиев[2]

[1,2]Институт Информационных Технологий НАНА, Баку, Азербайджан

[1]depart3@iit.science.az, [2]depart11@iit.science.az

***Аннотация*— Статья посвящена вопросам обеспечения безопасности киберфизических корпоративных систем. Проанализированы принципы функционирования инфраструктуры э-науки как киберфизической системы, приведена ее концептуальная модель и рассмотрены ключевые вопросы технического обслуживания для поддержания ее безопасности. Информация, генерируемая системой, может использоваться для планирования технического обслуживания и оптимизированного управления для достижения более высокой общей производительности и безопасности.**

Ключевые слова— киберфизические системы, э-наука, функциональная безопасность, надежность, техническое обслуживание.

I. Введение

Киберфизические системы (КФС) — это системы, состоящие из различных физических (природных и промышленных объектов), искусственных подсистем, и управляемые с использованием обратной связи от различных датчиков (сенсоров) [1,2]. В основу функционирования КФС заложен принцип интеграции вычислительных и физических процессов, т.е. физические объекты становятся частью системы [3].

С технической точки зрения КФС имеют много общего со структурами типа грид, реализуемыми посредством интернета вещей (*Internet of Things, IoT*), Индустрии 4.0 *(Industry 4.0*), промышленного интернета вещей (*Industrial Internet*), межмашинного взаимодействия (*Machine-to-Machine, M2M*), туманного и облачного компьютинга (*fog u cloud computing*).

Проведенный анализ функционирования КФС и традиционных корпоративных систем показывает, что они имеют характерные признаки, присущие обеим структурам, такие, как источники первичной информации, передача, хранение, обработка и анализ информации для принятия решений. Исходя из вышеизложенного, в работе исследуются вопросы обеспечения безопасности функционирования инфраструктуры э-науки как КФС.

При рассмотрении информационного пространства Национальной Академии Наук Азербайджана (НАНА) в контексте КФС в ней выделяется инфраструктура э-науки, построенная на сетевой платформе AzScienceNet, объединяющей в настоящее время свыше 6000 единиц компьютерной техники (компьютеры, мобильные устройства и др.), функционирующих в научно-исследовательских институтах и структурах НАНА [4]. AzScienceNet является сложной корпоративной информационной системой, включающей комплекс инженерной инфраструктуры, программно-аппаратное обеспечение серверов обработки данных, устройства хранения информации, коммуникационные каналы и оборудование для предоставления многочисленных услуг э-науки пользователям (хостинг, хранилище данных, облачный сервис, э-почта, э-библиотека, роуминг-сервис академической сети и т.п.) [4,5]. Для обеспечения устойчивого функционирования данной инфраструктуры э-науки необходим комплекс мер по решению возникающих в ней проблем. Для поддержки принятия решений на этом уровне существенную помощь может оказать организация технического обслуживания для поддержания безопасности системы, уменьшения интенсивности сбоев и предупреждения неисправностей.

II. Некоторые Вопросы Обеспечения Безопасности КФС

При увеличении взаимодействия в среде КФС физические системы становятся все более восприимчивы к уязвимостям безопасности. Ключевые проблемы для обеспечения безопасности КФС следующие:

- Понимание угроз и возможных последствий атак;
- Определение уникальных свойств КФС и их отличия от безопасности традиционных информационных технологий;
- Обсуждение механизмов безопасности, применимых к КФС.

Безопасность КФС исследуется по нескольким направлениям [1]:

1. Оценка последствий кибератак.
2. Моделирование уязвимостей и атак.
3. Обнаружение атак.
4. Разработка архитектуры безопасности.

Следствием случайных, несанкционированных или неконтролируемых угроз в КФС могут стать непредвиденные или нежелательные ситуации в их

DOI: 10.25045/NCInfoSec.2017.06

корпоративной среде. Например, злоумышленник может осуществить перехват управления на уровне физических устройств и заставить систему управления выполнять опасные функции. Чтобы уменьшить подобные риски, необходимо обеспечить как информационную, так и функциональную безопасность КФС. Если информационная безопасность предполагает выполнение следующих метрик: конфиденциальность – доступ к информации только авторизованных пользователей; целостность – достоверность и полнота информации и методов ее обработки; доступность – доступ к информации и связанным с ней активам авторизованных пользователей, то функциональная безопасность обеспечивает надежное функционирование системы при оптимальных параметрах ее готовности, сохраняемости, ремонтопригодности, безопасности и живучести.

Функциональная безопасность предполагает организацию технического обслуживания, включающего такие виды деятельности, как мониторинг, настройка, ремонт, замена и модернизация. Техническое обслуживание увеличивает срок службы и надежность систем, уменьшает размер, масштаб и количество непредвиденных перерывов в их работе. Резко снижаются вероятность аварийного ремонта и общие затраты при одновременном повышении уровня безопасности и надежности в широком смысле.

Надежность системы также является важным требованием КФС, поскольку примеры таких систем варьируются от простых до критически важных сложных инфраструктур.

Хотя безопасность отличается от надежности, они взаимозависимы. Хорошо известно, что ненадежная система не может быть в достаточной степени защищена.

Анализ надежности КФС является комплексной задачей. Надежность аппаратной части КФС хорошо изучена. Однако, это, безусловно, недостаточно для оценки общей надежности КФС.

Аппаратные и физические компоненты в КФС тесно сочетаются с программными и вычислительными элементами. В отличие от ухудшения характеристик аппаратных и физических элементов, которые могут быть описаны известными моделями отказов, программное обеспечение не подвержено физическому износу, а его надежность не является функцией времени. Очень часто при внедрении новых поколений современных аппаратных средств предшествующие версии программного обеспечения становятся неработоспособными и требуется их обновление или коррекция [6].

В последнее время область исследований стратегий технического обслуживания значительно расширилась и способствовала развитию интеллектуальных систем технического обслуживания, в том числе и э-техобслуживания [5,7]. Быстрое развитие информационно-коммуникационных технологий способствовало внедрению современных датчиков, а также *IoT* различного назначения, оборудования для сбора данных, беспроводных сетей, коммуникационных устройств и решений для удаленных вычислений. Эта эволюция привела к внедрению прогностической аналитики в рамках структуры КФС, которая позволяет активам производства постоянно отслеживать собственную работоспособность и прогнозировать потенциальные сбои.

Современное прогностическое обслуживание предназначено для применения *IoT* технологий для мониторинга состояний компонентов физической системы в реальном времени и для инициирования необходимых действий по техническому обслуживанию [8]. Оно также предусматривает оснащение систем разумными возможностями для поддержки автоматизированного принятия решений о необходимости технического обслуживания. Например, в компьютерных системах реализуется аппаратно-программный мониторинг состояний отдельных их компонентов через лог-файлы и графики, например, температуры центрального процессора, материнской платы, накопителей на жестких магнитных дисках *HDD*, блока питания; напряжений питания; скорости вращения вентиляторов; сканирование рабочих поверхностей *HDD* на наличие физических неисправностей и логических ошибок (технология *Self Monitoring and Reporting Technology*) и т.п. Или же мониторинг температуры двигателей системы охлаждения в Центре обработки данных (*Data center)* позволит заблаговременно определить проявляющиеся неисправности двигателей, провести упреждающее обслуживание и тем самым предотвратить отказы в их работе.

III. Концептуальная Модель Архитектуры Э-Науки как КФС

Можно предположить, что инфраструктура э-науки является фабрикой по обработке информации, что вписывается в информационно-технологическую концепцию КФС. Это большое количество устройств со встроенными сенсорами, процессорами и средствами хранения данных; интеграция, позволяющая достигнуть наибольшего эффекта путем объединения отдельных компонентов в большую систему; исключение человеческого фактора при принятии решений (*human out of loop*) либо дополнение способностей человека (*human in the loop).* Например, используются способности органов чувств человека, недоступные на сегодняшний день в мире машин, или же привлечены соображения здравого смысла (экспертные системы).

Инфраструктура э-науки состоит из следующих основных компонент, таких как коммуникационная сеть, вычислительные ресурсы, хранение данных, информационные ресурсы, технологии интеллектуального анализа и т.п., которые можно отождествить со структурой КФС.

Исходя из вышеизложенного, предлагаемая концептуальная модель архитектуры э-науки как КФС приведена на рис.1.

Из рис.1 видно, что эта модель состоит из пяти уровней, а именно:

A. Умное соединение

На этом уровне собираются данные со *smart* датчиков различного назначения.

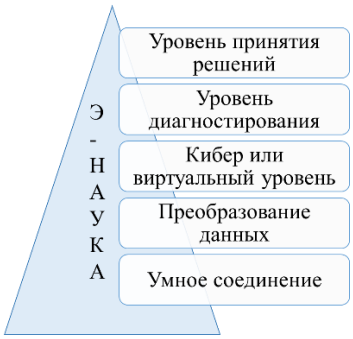

Рис.1. Концептуальная модель э-науки как КФС.

B. Преобразование данных

На этом уровне обрабатываются первичные данные с использованием различных алгоритмов. Например, необработанные данные о температурных режимах или же лог-файлы, которые используют для получения информации о технических и программных средствах. Это уровень локального анализа, например, на отдельных серверах.

C. Кибер или виртуальный уровень

Этот уровень используется как хаб с целью выполнения сложной аналитики для выработки рекомендаций или предпочтений для лучшего использования актива (блоков, узлов, элементов). Методы кибер уровня имеют место в центральном вычислительном узле, таком как ″Облако″ (*Cloud*). Этот уровень можно представить, как некий ″черный ящик″, имеющий входы и выходы, при этом происходящие внутри процессы наблюдателю неизвестны.

D. Уровень диагностирования.

Система использует *on-line* мониторинг, чтобы диагностировать свои собственные потенциальные сбои на основе адаптивного обучения и исходя из истории оценок состояния.

E. Уровень принятия решений

На этом уровне осуществляется обратная связь от киберпространства к физическому пространству для применения корректирующих и превентивных воздействий к диагностируемой системе, которые были приняты на предыдущем уровне.

Как следует из модели, каждый уровень в отдельности, наряду с выполнением своих основных функций, требует обеспечения безопасности. Общая политика безопасности включает в себя как безопасность каждого уровня, так и системы в целом. Подводя итог, отметим, что из комплекса задач по безопасности в работе рассмотрены вопросы технического обслуживания, которое позволит осуществить прогрессивную стратегию технического обслуживания, ориентированную на функциональную надежность и безопасность с минимизацией рисков, и обладает рядом преимуществ по сравнению с традиционными:

- непрерывное *on-line smart* обслуживание;
- прямая связь между потребителями и поставщиками услуг;
- автоматизированный мониторинг физических активов;
- оперативность контроля и профилактики;
- автоматическое проведение ресурсоемкого прогнозирования.

Заключение

Обеспечение безопасности э-науки, как одного из сегментов э-Азербайджана, является одной из составляющих задач в контексте национальной безопасности. Эта задача многопрофильная, сложная и весьма актуальная. Представленная концептуальная модель архитектуры э-науки, как КФС определяет основные направления обеспечения безопасности. Среди этих направлений разработка системы технического обслуживания является актуальной задачей.

Благодарности

Данная работа выполнена при финансовой поддержке Фонда Развития Науки при Президенте Азербайджанской Республики – **Грант № EİF-2014-9(24)-KETPL-14/02/1**

Литература

[1] Р.М. Алигулиев, Я.Н. Имамвердиев, Л.В. Сухостат, “Киберфизические системы: основные понятия и вопросы обеспечения безопасности,” Информационные технологии, Т.23, №7, 517-528, 2017.

[2] E.A. Lee, “Cyber physical systems: Design challenges,” 11th IEEE international symposium on object oriented real-time distributed computing (isorc), pp. 363-369, 2008.

[3] J. Lee, B. Bagheri, H.A. Kao, “A cyber-physical systems architecture for industry 4.0-based manufacturing systems,” Manufacturing Letters, Vol. 3, pp. 18-23, 2015.

[4] Т.Фаталиев, “Электронная наука: состояние и перспективы развития в Азербайджане,” Телекоммуникации, № 8, 41-48, 2016.

[5] T. Fətəliyev, Ş. Mehdiyev, “Şəbəkə mühitində elektron texniki xidmətin təşkili məsələləri,” Proqram mühəndisliyinin aktual elmi-praktiki problemləri‖ I respublika konfransı, Bakı, 17 may 2017-ci il, s.291-293, DOI: 10.25045/NCSoftEng.2017.76

[6] Ш.А. Мехтиев, “Организация технического обслуживания в корпоративной среде,” İnformasiya texnologiyaları problemləri, №1, 92–99, 2017.

[7] E. Levrat, B. Iung, A. Crespo Marquez, “E-maintenance: review and conceptual framework,” Production Planning & Control, Vol. 19, №4, June 2008, pp. 408–429

[8] S. Ruiz-Arenas, I. Horváth, R. Mejía-Gutiérrez, & E. Opiyo, “Towards the maintenance principles of cyber-physical systems,” Strojniški vestnik-Journal of Mechanical Engineering, 60(12), pp. 815-831, 2014.

SOME SECURITY ISSUES OF CYBERPHYSICAL CORPORATE SYSTEMS

Tahmasib Fataliyev[1], Shakir Mehdiyev[2]
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijan
[1]depart3@iit.science.az, [2]depart11@iit.science.az

Abstract – The article is dedicated to the issue of security provision of cyberphysical corporate systems. The principles of functioning of the infrastructure of e-science as a cyber-physical system are analyzed, its conceptual model is presented and the key issues of technical service are considered to maintain its safety. Information generated by the system can be used for planning of technical service and optimized management to achieve higher overall productivity and security

Keywords– cyber-physical systems, e-science, functional security, reliability, technical service.