Применение искусственного интеллекта в киберфизических системах

Д. П. Плахотников[1], Е. Е. Котова[2]
Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина)
Санкт-Петербург, Россия
[1]dimapl21@yandex.ru, [2]apu_kotova@mail.ru

***Аннотация*. Киберфизические системы — это важная составная часть информационной эпохи. В настоящие время для улучшения работы составных частей киберфизических систем, всё чаще используются методы искусственного интеллекта, такие как алгоритмы глубокого обучения. Вместе с развитием области искусственного интеллекта развиваются и киберфизические системы, поскольку качество работы таких систем определяется во многом качеством обработки информации, присутствующей в таких системах. Поэтому использование искусственного интеллекта для киберфизических систем является актуальной на текущей день задачей.**

Ключевые слова: киберфизические системы; алгоритмы глубокого обучения; аналитические платформы

I. Введение

Развитие новейшего технологического уклада на сегодняшний день объединяют с началом наступления четвёртой промышленной революции, которая основывается на массовом внедрении «киберфизических систем» – CPS (Cyber-Physical Systems). Изучение разнообразных свойств информационно-технических систем с позиции взаимодействия их физической и цифровой составляющих – новое и актуальное направление современной науки [1]. Именно с осознанием концепции киберфизических систем и возникновением действующих подобных систем связывают переход к индустрии 4.0 – прогнозируемое событие, массовое внедрение киберфизических систем в производство и обслуживание человеческих потребностей.

II. Что такое киберфизические системы?

Киберфизическая система (Cyber-Physical System, CPS) – это система, состоящая из различных физических сущностей любого вида, искусственных подсистем, таких как различного рода датчики и сенсоры, и управляющих контроллеров, позволяющих представить такое образование как единое целое. В киберфизических системах вычислительная компонента распределена по всей физической системе, которая является её носителем, и синергетически увязана с её составляющими элементами [2]. Говоря иными словами, киберфизические системы – это системы, состоящие из различных объектов (природных, искусственных подсистем) и датчиков, контроллеров, позволяющих представить такую структуру как одно единое целое. В киберфизических системах обеспечивается координация и тесная связь между вычислительными и физическими ресурсами. Вычислительные машины выполняют мониторинг и управление физическими процессами так, что совершающееся процессы в физических системах производят влияние на вычисления и наоборот.

Актуальность вопроса заключается не в создании более крупных автоматизированных систем, где вычислительные машины интегрированы или встроены в какие-либо физические устройства или физические системы, а в гармоничном сосуществовании двух типов этих моделей. С одной стороны – это традиционные инженерные модели (экономические, механические, электрические, химические, биологические и многие другие), а с другой – компьютерные модели.

Предшественниками киберфизических систем считаются встроенные системы реального времени, автоматизированные системы управления техническими процессами и объектами, а также распределенные вычислительные системы [3].

С технической точки зрения киберфизические системы имеют много общего со структурами типа «grid», реализуемыми посредством «Internet of Things» (интернета вещей), «Industrial Internet» (промышленного интернета вещей), «Machine-to-Machine» (межмашинного взаимодействия), «fog и cloud computing» (туманного и облачного компьютинга).

Немецкая академия Acatech (https://www.acatech.de/) уже говорит о перспективах национальных киберфизических платформ, которые складываются из трех типов сетей:

- интернет людей;
- интернет вещей;
- интернет сервисов.

A. Составные части киберфизических систем

Главными составными частями любой киберфизической системы являются:

- физический слой системы (объекты реального физического мира);

- цифровой слой системы (множество данных о системе – алгоритмы управления физическими объектами, алгоритмы обработки информации и другое);
- интерфейс взаимодействия цифрового и физического слоя (различные датчики, управляющие механизмы и другое);
- интерфейс взаимодействия цифрового и физического слоя с человеком (различные технологии расширенной реальности).

Концептуальная схема представлена на рис. 1.

Рис. 1. Концептуальная схема киберфизической системы

Данные составные части взаимодействуют между собой во времени и пространстве, образуя единую экосистему, направленную на решение определённой поставленной задачи. Киберфизические системы являются следующей ступенью эволюции систем с большим масштабом гранулярности. Иными словами, такая система сама состоит из множества других сложных систем.

B. Что является киберфизической системой?

Киберфизической системой считаются как относительно небольшие объекты (например, беспилотный летательный аппарат, система умных устройств помещения), так и масштабные объекты: заводы или даже целые города (системы типа «умный город»).

У киберфизических систем есть очень много общего с другими информационно-техническими концепциями, такими как интернет вещей, умная пыль и туманные вычисления, т.е. со структурами типа «грид». Киберфизические системы – более широкое понятие, чем перечисленные выше, и они могут являться составными частями целой киберфизической системы. Более того, если рассматривать составные устройства киберфизической системы, то по отношению к другим концепциям, в киберфизических системах они находятся на более высоком уровне взаимодействия.

Имеются следующие уровни взаимодействия среди объектов (снизу-вверх):

1. Интеллектуальный уровень связи:

- технология «Plug&Play» («включи и работай»);
- свободная коммуникация;
- сеть датчиков.

2. Уровень преобразования данных в информацию:

- интеллектуальная аналитика для здоровья компонентов машины;
- интеллектуальная аналитика многомерной корреляции данных;
- прогноз деградации и производительности.

3. Киберуровень:

- клонирование моделей для компонентов и машин;
- «машина времени» для вариативной идентификации и памяти;
- кластеризация подобий в интеллектуальном анализе данных.

4. Когнитивный уровень:

- комплексное моделирование и синтез;
- дистанционная визуализация для человека;
- совместная диагностика и принятие решений.

5. Уровень конфигурации:

- самостоятельная настройка для обеспечения устойчивости;
- самостоятельное приспособление к изменениям;
- самооптимизация при нарушении работы.

Графический вид представлен на рис. 2.

Рис. 2. Уровни взаимодействия объектов реального мира внутри цифрового слоя

C. Прототипы киберфизических платформ

Если говорить про прототипы киберфизических платформ, то наиболее удачным примером на сегодняшний день является Сингапур, где на законодательном уровне принята инициатива «Умная нация», которая подразумевает социальное и

экономическое развитие на базе киберфизической платформы.

Для улучшения работы всех составных частей киберфизических систем необходимо прибегнуть к методам искусственного интеллекта, а в частности к алгоритмам глубокого обучения. Данная конвергенция технологий формирует большое количество связей и данных – необходимых для развития искусственного интеллекта.

III. Искусственный интеллект в киберфизических системах

Искусственный интеллект – это свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека [4].

Машинное обучение – подмножество искусственного интеллекта, включающее сложные статистические методы, позволяющие машинам выполнять задачи на основе обучения.

Глубокое обучение – подмножество машинного обучения. Состоит из алгоритмов, позволяющих машинам обучаться для выполнения сложных задач (распознавание объектов на изображении или речи) за счёт обработки нейронными сетями огромных объёмов данных.

Искусственный интеллект включает в себя машинное обучение, которое включает в себя глубокое обучение. Схематически это представлено на рис. 3.

Рис. 3. Подобласти искусственного интеллекта

Вместе с развитием области искусственного интеллекта развиваются и киберфизические системы, поскольку качество работы таких систем определяется во многом качеством обработки данных, присутствующих в системе.

Одной из проблем которую решает искусственный интеллект в киберфизических системах, является обеспечение безопасности, то есть создание систем защиты от киберфизических атак. Основной метод защиты киберфизических систем заключается в обнаружения аномалий в каналах связи между PLC (ПЛК – программируемым логическим контроллером), управляющим технологическими процессами на оборудовании и модулем SCADA (модуль диспетчерского управление и сбора данных). Для поиска аномалий в каналах управления используется рекуррентная нейронная сеть [5]. Данная схема представлена на рис. 4.

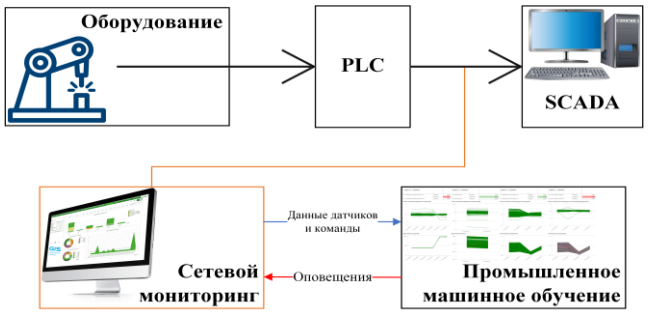

Рис. 4. Применение искусственного интеллекта в киберфизических системах

В качестве данных для обучения такой сети необходимо использовать синтетические данные, получаемые с цифрового «клона» системы. Преимущество такого подхода, по сравнению с традиционным решением, основанным на логических правилах контроля каналов связи, заключается в разнообразии ситуаций, которые система искусственного интеллекта может детектировать. С помощью цифрового клона системы можно предотвратить редко встречающиеся на практике, но потенциально опасные ситуации. И ещё одним важным фактором является скорость, с которой можно получать новые данные для обучения системы.

Иной способ применения искусственного интеллекта в киберфизической системе представлен в следующей главе.

IV. Практическое применение

В процессе работы киберфизических систем образуется множество различных данных. Средствами обработки таких «больших данных» должны заниматься специальные системы. Таким критериям отвечают современные системы класса аналитических платформ, иначе называемые системами интеллектуального анализа данных [6].

В качестве сервера базы данных процессинга киберфизической системы используется СУБД Oracle. С помощью встроенных ETL-инструментов аналитической платформы Qlik данные процессинга загружаются в сервер аналитики [7]. На сервере установлены инструменты данных Python для Qlik, включающие в себя:

- автоматизированное машинное обучение;
- автоматическое машинное обучение;
- глубокое обучение.

Была поставлена задача спрогнозировать нагрузку системы за 2020 г. Из всех имеющихся компонентов наиболее подходящим под эту задачу является Facebook Prophet.

Prophet – это компонент прогнозирования данных временных рядов, основанный на аддитивной модели, в которой нелинейные тренды соответствуют годовой, еженедельной и ежедневной сезонности, а также влиянию выходных дней. Phophet лучше всего работает с временными рядами, которые имеют сильные сезонные эффекты и несколько сезонов исторических данных. Prophet устойчив к отсутствующим данным и изменениям тренда и обычно хорошо справляется с выбросами.

Этот компонент отлично подходит, поскольку нагрузка в используемой киберфизической системе сильно зависит от сезонности и имеются данные за несколько сезонов работы системы. Для использования данного компонента изначально загружаются данные, подключается библиотека и используется специальная формула, представленная на рис. 5.

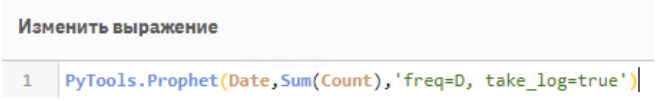

Рис. 5. Формула для прогнозирования нагрузки системы

Выражение представляет собой:

- PyTools – название инструмента;
- Prophet – название компонента;
- Date – дата измерений;
- Sum(Count) – мера по количеству событий;
- freq=D – указание, что частота данных (frequency) соответствует дню (day);
- take_log=true – активируется использование журнала.

В результате был построен график прогноза нагрузки киберфизической системы, представленный на рис. 6. На нём ось x – дата, ось y – ед. нагрузки, одна линия – прогнозируемая нагрузка, а другая – реальные данные.

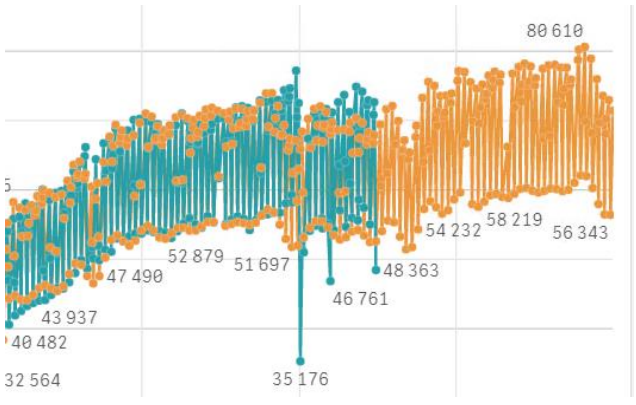

Рис. 6. График прогноза нагрузки киберфизической системы

И построена таблица, содержащая прогнозируемые значения. Часть значений представлена на рис. 7.

Таблица прогнозируемых значений

Дата	Прогнозируемые значения
24.11.2020	77 623
25.11.2020	78 261
26.11.2020	79 363
27.11.2020	80 610
28.11.2020	69 879
29.11.2020	61 918
30.11.2020	74 645
01.12.2020	76 857

Рис. 7. Таблица прогнозируемых значений нагрузки

Благодаря этому, можно сделать следующие выводы:

- ожидается повышение максимальной нагрузки в день с 77164 ед. до 80610 ед.;
- ожидается повышение средней нагрузки с 61029 ед. в день в 2019 г. до 68491 ед. нагрузки в день в 2020 г. (на 12 %).

V. Заключение

Киберфизические системы — важная составная часть информационной эпохи и применение искусственного интеллекта может улучшить работу киберфизических систем на всех уровнях. В статье показано практическое применение в реальной киберфизической системе.

Список литературы

[1] R.G. Sanfelice. Analysis and Design of Cyber-Physical Systems. A Hybrid Control Systems Approach // Cyber-Physical Systems: From Theory to Practice / D. Rawat, J. Rodrigues, I. Stojmenovic. CRC Press, 2016. ISBN 978-1-4822-6333-6.

[2] Allgöwer Frank & Sousa João & Kapinski James & Mosterman Pieter & Oehlerking Jens & Panciatici Patrick & Prandini Maria & Rajhans Akshay & Tabuada Paulo & Wenzelburger Philipp. (2019). Position paper on the challenges posed by modern applications to cyber-physical systems theory. Nonlinear Analysis. 34. 147–165. 10.1016/j.nahs.2019.05.007.

[3] Cheng Albert M. K. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models / EECS Department, University of California, Berkeley, CA 94720-1770, USA, 2015. 15 p.

[4] Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту. М.:Радио и связь, 1992. 256 с.

[5] Filonov Pavel & Kitashov Fedor & Lavrentyev Andrey. (2017). RNN-based Early Cyber-Attack Detection for the Tennessee Eastman Process. ArXiv abs/1709.02232.

[6] Плахотников Д.П. Разработка приложений для анализа данных на базе платформы Qlik Sense[Текст] / Д.П. Плахотников // Сборник статей Международной научно-практической конференции «Концепция «общества знаний» в современной науке» (Челябинск, 11.12.2018 г.). Уфа: OMEGA SCIENCE, 2019. с. 78-80.

[7] Плахотников Д.П., Котова Е.Е. Анализ поведения пользователей на базе платформы бизнес-аналитики // III Международная научная конференция по проблемам управления в технических системах (ПУТС-2019) (Санкт-Петербург, 30 октября - 01 ноября 2019).