БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ: КОММУНИКАЦИОННЫЕ АСПЕКТЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кадушко А.А.

Филатова Д.В. – д.ф.-м.н

В работе рассмотрена концепция фабрики будущего. Показано, что основной проблемой распространения технологии фабрики будущего является кибербезопасность, описана система связи устройство-устройство (D2D). Рассмотрена классификация существующих архитектур систем связи устройства-к-устройству киберфизические систем, а также методов защиты информации.

Концепции фабрики будущего основаны на нескольких принципах: открытость цепочки создания стоимости (понимаемая как адекватность, гибкость, устойчивость и оптимальность по отношению к капитальным затратам, связанных с планированием и управлением предприятием), гибкость производства (по объему, продукту, дизайну, процессу и автоматизации), клиент-ориентированное производство, специфика бизнес-модели (краудсорсинг, AaaS-принцип, симбиотическая экосистема), локальная инициатива («smart»-производство, промышленный интернет, электронная фабрика, Industry 4.0, интеллектуальное производство) [1]. Попытка обобщения концепций привела к появлению понятия «RAMI 4.0», т.е. «модель эталонной архитектуры» [2]. Архитектура отображает фабрику будущего с использованием трехмерной классификации: управление фабрикой - «Layers», иерархия оборудования, материальных и нематериальных ресурсов – «Levels», поток создания стоимости при жизненном цикле – «Life Cycle Value Stream». Отличительной чертой такого восприятия является появление «физической» и «информационной» систем-оболочек, причем вторая воспринимается как клон первой и используется для управления фабрикой в целом [2, 3].

Осуществление управления при помощи информационной оболочки зависит от выбора платформы и ее архитектуры. Одним из решений является архитектура с использованием CPMT (от англ. «cyber-physical machine tools» – киберфизические станки). Идея заключается в представлении CPMT в виде трех подсистем: физические устройства (physical devices), сети (networks) и цифрового близнеца физических устройств, содержащего также алгоритмы обработки информации, диагностики и управления. Очевидно, что между физическими устройствами и их информационными близнецами постоянно происходит передача данных, которые по скорости, объему и структуре характеризуются как Big Data. Но, несмотря на прогресс в области информационных технологий, существуют барьеры, ограничивающие распространение такого решения: связь и взаимодействие физических и информационных уровней предприятия, архитектура системной интеграции, охрана и безопасность хранения и передачи информации между уровнями. Поэтому среди перспективных направлений исследований являются: интернет вещей (IoT) и межмашинное общение (M2M, D2D), облачная инфраструктура приложений и промежуточное ПО, аналитика данных (вычисления в базе данных в памяти, обработка потоков событий, комплексная обработка событий, механизмы принятия решений), умная робототехника (взаимодействие человека и робота, новые парадигмы программирования роботов), интегрированное моделирование производства продукции, аддитивное производство / 3D печать.

Использование интернета вещей связано с проблемой загруженности сети (использование системы связи, построенной на использовании базовых станций, неэффективно, хотя бы из-за отсутствия возможности поддержки неограниченного количество устройств в своей сети без потери качества связи). Альтернативой является 5G технология, т.е. система связи устройство-к-устройству без использования базовых станций [4]. Главная проблема этой технологии - отсутствие формализованных стандартов и методов защиты чувствительных данных. Целью этой работы является изучение и классификация существующих архитектур систем связи устройства-к-устройству киберфизические систем, а также методов защиты информации.

Список использованных источников:

1. Kagermann, H. Securing the future of German manufacturing industry: recommendations for implementing the strategic initiative INDUSTRIE 4.0 / Kagermann H., Wahlster W., Helbig J. // Final report of the Industrie 4.0 Working Group - 2013. – vol. 40, pp. 1 – 84.
2. Lee, J. A cyber-physical systems architecture for industry 4.0-based manufacturing systems / J. Lee, B. Bagheri, H.A. Kao // Manufacturing Letters – January 2015 – vol.3, pp. 18 – 23.
3. Filatova, D. Production process balancing: a two-level optimization approach / D. Filatova, Ch. El-Nouty // International Conference on Information and Digital Technologies (IDT) 2019, – IEEE, 2019 – pp. 123-131.

4. Haus M. Security and Privacy in Device-to-Device (D2D) Communication: A Review / M. Haus, Wagas M., Ding A.Y., Li Y., Tarkoma S., Ott J. // IEEE Communications Surveys & Tutorials, 2017, - IEEE, vol.19 (2) - pp. 1054 - 1079.