«Разработка аппаратных модулей безопасности на платформе ПЛИС для защиты и контроля доступа физических и промышленных установок»

Руководитель темы Коковин Валерий Аркадьевич, к.т.н., ученое звание доцент, доцент кафедры автоматизации технологических процессов и производств, заведующий комплексной лабораторией филиала.

Исторически, сетевые взаимодействия в промышленных управляющих системах были организованы с использованием последовательных сетей полевого уровня RS-485 and RS-422. Протоколы на основе этих интерфейсов, такие как Modbus, Profibus и другие, были разработаны без учета безопасности, поскольку использовались для развертывания в средах с ограниченным доступом.

При организации киберзащиты систем контроля физического доступа (Physical Access Control System, PACS) к технологическим системам основное внимание уделяется проблеме предоставления или блокировке доступа.

Аппаратная безопасность передаваемых сообщений включает набор аппаратных средств, которые защищают конфиденциальность этих сообщений, know-how разработчиков и физическую безопасность оборудования. Кибератаки на разрушение промышленного оборудования чаще всего применяются на вычислительных устройствах и на коммуникационных сетях при организации межмашинных взаимодействий или Интернета вещей (IoT).

В настоящее время большинство PACS имеют в качестве коммуникационного интерфейса RS-485. Это связано в первую очередь с небольшими затратами на реализацию PACS. При этом устройства системы доступа могут подключаться последовательно и на большом расстоянии от основного сервера PACS. Это дает возможность без больших затрат добавлять дополнительные точки доступа к оборудованию. Во-вторых, переход к современным PACS на основе протокола TCP/IP требует значительных вложений и квалифицированный обслуживающий персонал.

В статье V. A. Kokovin, A. N. Sytin and V. V. Skvortsov, "Methods for Increasing the Cybersecurity of FNC Devices on the FPGA-Based Platform in Network Communications" [1] проанализирована опасность кибератак и их последствия с точки зрения критических уязвимостей технологических процессов, управляемых Функциональными Сетевыми Компонентами (Functional Networking Components, FNC). Рассмотрены особенности использования FNC в распределенных системах управления. Представлены алгоритмы формирования криптоидентификаторов для повышения кибербезопасности FNC при взаимодействии по локальным сетям. В качестве уникального идентификатора (Physically Unclonable Function, PUF) использовано значение времени прохождения сигнала через логические элементы ПЛИС, измеренного с помощью TDC7200. Разработана структура FNC с использованием семейства ПЛИС Cyclone 10 LP 10CL025YU256I7G, TDC7200 и контроллера Cortex-A72 ARM для формирования экспериментов по исследованию криптоидентификаторов. Представлены результаты экспериментов. Для увеличения киберзащиты при формировании сообщений использовался алгоритм сжатия данных без потерь [2].

В статье V. A. Kokovin, A. N. Sytin and V. V. Skvortsov "Hardware Cybersecurity on the FPGA Platform During Network Interaction of Distributed Industrial Equipment" [3] обоснована идея защиты данных, передаваемых по RS-485, путем замены отдельных, специально выделенных сегментов сети, имеющих неконтролируемый доступ (открытый для злоумышленника), на сегменты, которые защищены аппаратными средствами. Рассмотрена структурная организация защищенного сегмента сети (Protected Network Segment (PNS) и аппаратные ресурсы, необходимые для решения поставленной задачи.

Основным стандартом, определяющим идеологию PNS, является IEEE Standard 1355. Стандарт представляет собой коммуникационный последовательный интерфейс, предназначенный для соединения точка-точка, использующий среду передачи данных типа витая пара или оптоволокно. Выбор такой среды передачи сообщений определяется необходимой скоростью передачи информации. Способ передачи электрических сигналов в PNS регламентируется стандартом ANSI/TIA/EIA-644-A 2001. Этот стандарт определяет энергоэффективный и высокоскоростной способ передачи сигналов с помощью Low-Voltage Differential Signaling (LVDS**)**. На сигнальном уровне используется DS-кодирование, которое требует две сигнальных линии: D – линия для передачи данных и S – линия для передачи строба (рис.1). DS-кодирование обладает свойством самосинхронизации, поскольку в комбинации DS-сигналов закодирован синхросигнал. Этот сигнал может восстанавливаться на приемной стороне логической операцией XOR над сигналами D и S. Самосинхронизация позволяет произвольно менять скорость передачи, даже в пределах одного сообщения. Это дает хорошее преимущество в безопасности. В интерфейсах RS-485 и RS-422 скорость фиксированная и выбирается из предложенного ряда.

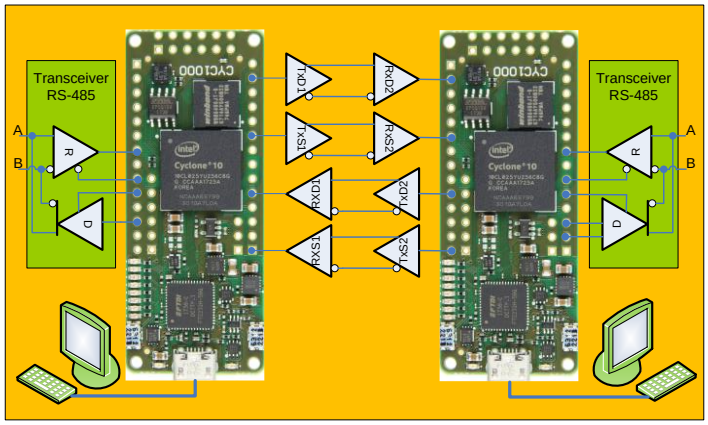

Рис.1. Функциональная схема и ресурсы для реализации PNS.

Использование в составе PNS элементов на платформе ПЛИС дает широкие функциональные возможности: использование сторонних IP-ядер с адаптацией к решаемой задаче, изменение алгоритма "на лету", меняя конфигурацию ПЛИС, и подстраиваясь к изменяющимся условиям работы системы. При проверке работоспособности PNS использовалась ПЛИС семейства Cyclone 10 LP 10CL025YU256C8G фирмы INTEL.

В статье V. A. Kokovin, A. A. Evsikov, A. N. Sytin, V. V. Skvortsov and S. U. Uvaysov, "Development and Research of a Hardware Security Module to Control and Protect Access to Industrial Equipment" [4] рассматриваются методы уменьшения киберугроз при сетевом взаимодействии промышленного оборудования и решение задач киберзащиты систем контроля физического доступа. Предполагается, что в составе управляющих и сетевых контуров оборудования используются решения на платформе ПЛИС. При организации киберзащиты систем контроля физического доступа к производственному оборудованию основное внимание уделяется проблеме предоставления или блокировке доступа. В этом случае реализуется сценарий авторизации лиц, которым разрешен доступ в определенное здание или зону, где находится оборудование. Большие производственные комплексы имеет географически и алгоритмически распределенное промышленное оборудование, что усложняет контроль доступа к оборудованию. Чаще всего для удаленной аутентификации персонала используется коммуникационный интерфейс RS-485.

Разработка тестовой версии Аппаратного Модуля Безопасности для Выделенных Сетевых Сегментов (Hardware Security Module for Dedicated Network Segments,

HSM_DNS), представленная в данной статье, решает задачи киберзащиты отдельных неконтролируемых участков сети связи полевого уровня (RS-485, RS-422), физически доступных злоумышленникам. Киберугроза, называемая атакой типа «человек посередине» (MiTM), возникает для незащищенных сегментов сети. Атака направлена на нарушение контроля доступа, конфиденциальности и целостности данных отправителя в сети, что может привести к подмене вредоносных данных и выводу из строя промышленного оборудования. Для тестирования модуля HSM_DNS была разработана печатная плата в форм-факторе PC/104 (рис.2). В качестве аппаратной платформы управления выбрана программируемая вентильная матрица (ПЛИС). Выбор ПЛИС обоснован необходимостью работы HSM в режиме реального времени, кодируя передаваемые данные по разработанному алгоритму. Кроме того, использование ПЛИС позволяет реализовать нестандартный протокол передачи данных, что повышает защищенность устройства. В статье представлены результаты испытаний и их обсуждение.

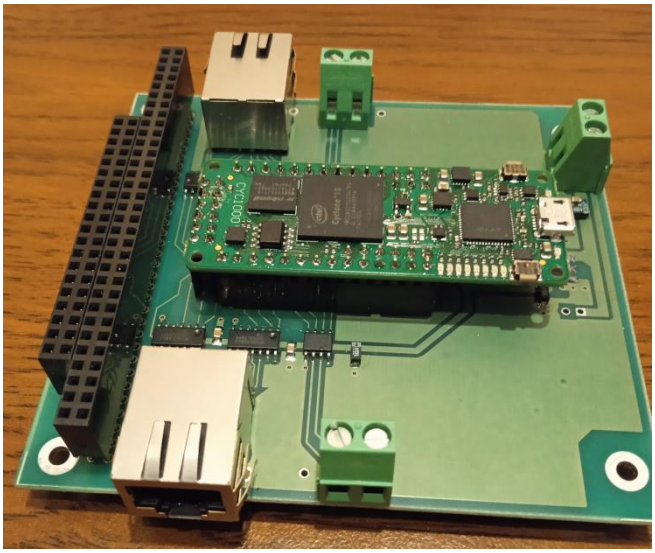

Рис.2. Общий вид тестовой версии HSM_DNS

Исследования разработанного модуля HSM_DNS показали, что решена задача замены отдельных, специально выделенных сегментов сети (RS-485, RS-422) с неконтролируемым доступом (открытых для злоумышленника) на сегменты, защищенные аппаратным шифрованием. Блок управления в ПЛИС анализирует направление передачи данных по RS-485 и настраивает работу блоков в ПЛИС либо на кодирование данных (поток из сети RS-485), либо на декодирование зашифрованного потока данных (поток из DS-Link). Все операции выполняются в режиме реального времени независимо от используемого протокола передачи данных (например, Profibus DP, ModBUS и т. д.) по сети RS-485. Разработка тестового проекта в пакете INTEL Quartus Prime 18.1 для ПЛИС (Cyclone 10 LP 10CL025YU256C8G) показала большой запас как по логическим элементам (используется менее 15%), так и по производительности (ПЛИС может работать на внутренней частоте 300 МГц). Кроме того, большой запас внутренней памяти (M9K, 256x36 блоков) позволяет гибко использовать различные массивы KeyArray [Address][Key], образы которых предварительно записаны в конфигурационную память мини-платы TEI0003-03.

Исследования модулей показали, что при разработке проекта можно использовать ПЛИС с меньшими ресурсами, а значит и более дешевую, либо добавить больше функциональности модулям HSM_DNS.

Разработка печатной платы модуля HSM_DNS в форм-факторе PC/104 позволяет использовать предлагаемое решение в промышленном оборудовании с жесткими условиями эксплуатации, такими как электромагнитные помехи и вибрации.

1. V. A. Kokovin, A. N. Sytin and V. V. Skvortsov, "Methods for Increasing the Cybersecurity of FNC Devices on the FPGA-Based Platform in Network Communications," *2022 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, Sochi, Russian Federation, 2022, pp. 825-830, doi: 10.1109/ICIEAM54945.2022.9787121, https://ieeexplore.ieee.org/document/9787121
2. V. A. Kokovin, S. U. Uvaysov and S. S. Uvaysova, "Real-time sorting and lossless compression of data on FPGA," *2018 Moscow Workshop on Electronic and Networking Technologies (MWENT)*, Moscow, Russia, 2018, pp. 1-5, doi: 10.1109/MWENT.2018.8337187, https://ieeexplore.ieee.org/document/8337187#citations
3. V. A. Kokovin, A. N. Sytin and V. V. Skvortsov, "Hardware Cybersecurity on the FPGA Platform During Network Interaction of Distributed Industrial Equipment," *2024 International Russian Smart Industry Conference (SmartIndustryCon)*, Sochi, Russian Federation, 2024, pp. 568-573, doi: 10.1109/SmartIndustryCon61328.2024.10515711, https://ieeexplore.ieee.org/document/10515711
4. V. A. Kokovin, A. A. Evsikov, A. N. Sytin, V. V. Skvortsov and S. U. Uvaysov, "Development and Research of a Hardware Security Module to Control and Protect Access to Industrial Equipment," *2024 International Seminar on Electron Devices Design and Production (SED)*, Sochi, Russian Federation, 2024, pp. 1-5, doi: 10.1109/SED63331.2024.10741050, https://ieeexplore.ieee.org/document/10741050