Universitatea Tehnică a Moldovei

Dezvoltarea platformei hardware şi software cu un canal de comunicaţie criptat pentru dispecerizarea obiectelor industriale la distanţa (partea Software)

Разработка программно-аппаратной платформы для диспетчеризации удаленных промышленных объектов с зашифрованным каналом связи (программная часть)

Student:

Homenco Andrei

Coordonator:

Şestacova Tatiana

Chişinău, 2020

АННОТАЦИЯ

HOMENCO ANDREI

Тема: Разработка программно-аппаратной платформы для диспетчеризации удаленных промышленных объектов с зашифрованным каналом связи (программная часть).

Структура работы: Введение, 3 Раздела, Заключение, Библиография, Приложения, 47 изображений, 2 таблицы.

Ключевые слова: Диспетчеризация, шифрование AES128, базы данных, Web интерфейс, удаленное управление, промышленные объекты, GPRS, АСУ ТП, SCADA.

Цель работы: Разработка программной части, программно-аппаратной платформы телеметрии/диспетчеризации удаленных промышленных объектов с зашифрованным каналом связи.

Задачи работы: анализ автоматизированных систем управления удаленными объектами, разработать обобщенную структурную схему программно-аппаратной системы и серверного программного обеспечения, разработать структуру базы данных, разработать WEB интерфейс, разработать библиотеку шифрования/дешифровки AES128, разработать сервисную службу обмена данными с удаленным оборудованием, разработать модуль обработки аварийных пределов параметров.

Применяемые методы: В соответствии с процессом разработки SDLC (Software Development Life Cycle) использовался каскадный метод разработки приложений, который включает: анализ, проектирование, разработку, внедрение, тестирование, оценку эффективности приложения.

Полученные результаты: Проведенный анализ автоматизированных систем управления удаленными объектами показал, что большинство существующих систем не приспособлены для работы с удаленным оборудованием. Их безопасность находится на низком уровне. Разработанный подход, к системам диспетчеризации на основе WEB технологий и в частности векторных мнемосхем технологических процессов, выводит данный подход на новую ступень с перспективой стать новым стандартом в АСУ ТП. Разработанный принцип обеспечения безопасности шифрованием по алгоритму AES128, обеспечивает безопасность соединений без использования SSL/TLS. Сервисная служба способна обрабатывать большое количество одновременных безопасных соединений с удаленным оборудованием. Разработанное программное обеспечение рационально использует вычислительные ресурсы, и эффективно функционирует даже в одноплатных промышленных компьютерах.

REZUMAT

HOMENCO ANDREI

Tema: Dezvoltarea platformei hardware şi software cu un canal de comunicaţie criptat pentru dispecerizarea obiectelor industriale la distanţă (partea Software)

Structura lucrării: Introducere, 3 Capitole, Concluzii, Bibliografie, Anexe, 47 de imagini, 2 tabele.

Cuvinte-cheie: Dispecerizare, criptare AES128, baze de date, interfaţă Web, telecomandă, obiecte industriale, GPRS, SCA PT, SCADA.

Scopul lucrării: Dezvoltarea software pentru dispecerizarea obiectelor industriale la distanţă cu un canal de comunicaţie criptat

Obiectivele lucrării: analiza sistemelor automatizate de control pentru obiecte la distanţă, dezvoltare o diagramă bloc generalizată a unui sistem hardware şi software şi a unui software de server, proiectarea structurii bazei de date, dezvoltare o interfaţă WEB, dezvoltare biblioteca de criptare/decriptare AES128, dezvoltare un serviciu de schimb de date cu echipamente la distanţă, dezvoltare un modul de procesare a alarmelor.

Metodele aplicate: Conform procesului de dezvoltare SDLC (Software Development Life Cycle) a fost utilizată metoda cascadă a dezvoltării aplicaţiilor ce include: analiza, proiectarea, dezvoltarea, implementarea, testarea, evaluarea eficienţei aplicaţiei.

Rezultatele obţinute: Analiza sistemelor de control automat al obiectelor la distanţă, a arătat că majoritatea sistemelor existente nu sunt adaptate pentru a funcţiona cu echipamente la distanţă. Securitatea lor este minimă. Abordarea dezvoltată a sistemelor de dispecerizare bazate pe tehnologii WEB şi, în special, bazate pe diagrame mnemonice vectoriale ale proceselor tehnologice, aduce această abordare la un nou nivel, cu perspectiva de a deveni un nou standard în APCS. Principiul de asigurare a securităţii dezvoltat, cu criptare conform algoritmului AES128, asigură securitatea conexiunilor fără utilizarea SSL / TLS. Biroul de servicii este capabil să gestioneze un număr mare de conexiuni simultane securizate al echipamentelor la distanţă. Software-ul dezvoltat foloseşte în mod raţional resursele şi funcţiile de calcul, chiar şi în computerele industriale cu o singură placă.

SUMMARY

HOMENCO ANDREI

Title: Development of a software and hardware platform for dispatching remote industrial objects with an encrypted communication channel (software part).

Thesis structure: Introduction, three chapters, Conclusions, Bibliography , Appendices, 47 pictures, 2 tables.

Keywords: Dispatching, AES128 encrzption, database, Web interface, remote control, industrial facilities, GPRS, APCS, SCADA.

Thesis purpose: Development of a software part for dispatching remote industrial facilities with an encrypted communication channel

Objectives: analysis of automated control systems for remote objects, to develop a generalized block diagram of a hardware and software system and server software, design database structure, develop a WEB interface, develop AES128 encryption/decryption library, develop a service for exchanging data with remote equipment, develop a parameter alarm processing module.

Applied methods: According to the SDLC (Software Development Life Cycle) development process the cascading method of application development which includes: analysis, design, development, implementation, testing, evaluation of application efficiency.

The Obtained Results: The analysis of automated control systems for remote objects showed that most of the existing systems are not adapted to work with remote equipment. Their security is at a low level. The developed approach to dispatching systems based on WEB technologies and, in particular, based on vector mnemonic diagrams of technological processes, brings this approach to a new level with the prospect of becoming a new standard in APCS. The developed principle of ensuring security with encryption using the AES128 algorithm ensures the security of connections without using SSL / TLS. The service desk is capable of handling a large number of concurrent secure connections to remote equipment. The developed software rationally uses computing resources and effectively functions even in single-board industrial computers.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время широкое применение получают системы телеметрии для диспетчеризации и автоматизации технологических процессов.

Системы диспетчеризации – это системы сбора, обработки и визуализации информации. Такие системы позволяют осуществлять централизованный контроль, управление и координацию различных процессов, происходящих на удаленных объектах, с использованием оперативной передачи информации между этими объектами и пунктом управления. Данная система – это эффективное решение для многих сфер, таких как телекоммуникация, водоснабжение, энергетика, нефтяная и газовая промышленность и др.

Использование современных систем учета и контроля позволяет:

осуществлять дистанционное управление и мониторинг технологического оборудования, что дает возможность во многих случаях оперативно установить причину аварийной ситуации, а также предотвратить ее появление в дальнейшем;

получать данные о состоянии всех инженерных систем, а также оптимизировать расходы путём точного учёта потребления энергоресурсов;

принимать сообщения аварийной, охранной и пожарной сигнализации, что даёт возможность быстрой и адекватной реакции на ситуацию;

выполнять более широкие возможности по управлению системами при сокращении штата обслуживающего персонала;

осуществлять протоколирование статистической информации и прогнозирование.

Проблемы передачи информации между удалёнными объектами могут быть решены с применением GSM модемов и концепции M2M.

M2M (Machine-to-Machine или Mobile-to-Machine) – это новая концепция организации сетей, обозначающая передачу телеметрических данных от одного устройства к другому. Система M2M состоит из нескольких элементов: периферийные узлы, коммуникационное оборудование и программное обеспечение. Периферийные узлы это чаще всего датчики, определяющие состояние окружающей среды и условия работы физических устройств. После сбора подробной информации она немедленно преобразовывается в цифровые сигналы, которые передаются потом по сети. Передачу данных к приложениям и другим узлам обеспечивает коммуникационное оборудование. Программное обеспечение на основе анализа данных, полученных от датчиков, принимает решения и посылает команды устройствам. Использование такой беспроводной технологии имеет целый ряд неоспоримых преимуществ. Применение M2M-оборудования позволяет сэкономить на прокладке кабельной инфраструктуры и сохранить драгоценное время, сократить

количество обслуживаемого персонала, сделать бизнес более эффективным и легко управляемым.

Целью проекта является разработка программной части, программно-аппаратной платформы телеметрии/диспетчеризации с зашифрованным каналом связи с удаленными промышленными объектами.

Концепция программно-аппаратной платформы необходима для реализации защищенного канала связи посредством шифрования/дешифрования данных на стороне удаленного оборудования, а также шифрования/дешифрования на стороне сервера.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Провести анализ автоматизированных систем управления удаленными объектами
2. Разработать обобщенную структурную схему программно-аппаратной системы и серверного программного обеспечения.
3. Разработать структуру базы данных
4. Разработать WEB интерфейс
5. Разработать библиотеку шифрования/дешифровки AES128
6. Разработать сервисную службу обмена данными с удаленным оборудованием
7. Разработать модуль обработки аварийных пределов параметров.

Данная платформа должна:

1) Обеспечить возможность мониторинга удаленных промышленных объектов.
2) Обеспечить возможность управления удаленных промышленных объектов
3) Обеспечить надежно зашифрованное соединение сервера с удаленным оборудованием, для предотвращения вмешательства посторонних лиц к управлению технологическими процессами.

БИБЛИОГРАФИЯ

1. В.Скляр «Обеспечение безопасности АСУТП в соответствии с современными стандартами», «Инфа-Инженерия» 2018г., Москва 2018

2. Boico, Vira Shendryk , System Integration and Security of Information Systems, ICTE 2016, December 2016, Riga, Latvia.

3. P. Athreya and P. Tague. Network self-organization in the internet of things. In Proc. of IEEE International Conference on Sensing, Communications and Networking (SECON), June 2013.

4. B. Schoenmakers, Cryptographic protocols, Techinical University of Eindhoven, 2017.

5. А.В. Черемушкин, Криптографические протоколы. Основные свойства и уязвимости, Москва, Академия, 2009.

6. Н. Фергюсон, Б. Шнайер, Практическая криптография, М.: Издательский дом Вильямс, 2005.

7. В. Кангин, Разработка SCADA-систем, LAP Lambert Academic Publishing, 2012

8. G. Clarke, D. Reynders, Practical Modern SCADA Protocols, Newnes, 2004

9. J. Wiles, Techno Security's Guide to Securing SCADA, Syngress, 2008

10. E. D. Knapp, J. T. Langill, Industrial Network Security, Syngress, 2015