ViPNet SIES Core & Pack

криптомодули для интеграции в автоматизированные системы управления и системы межмашинного взаимодействия

Индустриальные криптомодули ViPNet SIES Core & Pack — средства защиты данных, предназначенные для интеграции в автоматизированные системы управления (АСУ) и системы межмашинного взаимодействия (M2M). Индустриальные криптомодули ViPNet SIES Core & Pack организуют выполнение криптографических операций в виде набора простых команд для обработки пользовательских данных. Индустриальные криптомодули ViPNet ViPNet SIES Core & Pack берут на себя задачи по хранению, защите криптографических ключей и поддержанию их жизненного цикла. Для взаимодействия с АСУ индустриальные криптомодули ViPNet SIES Core & Pack используют промышленные или межплатные интерфейсы.

Основные функции безопасности

- Целостность (неискажаемость) данных
- Конфиденциальность данных
- Защита от подмены данных за счет создания и проверки электронной подписи (ЭП)
- Идентификация и аутентификация источника данных

Области применения

- Автоматизированные системы управления технологическим процессом (АСУ ТП)
- Автоматизированные информационно-измерительные системы коммерческого учёта электроэнергии (АИИС КУЭ и АСКУЭ), автоматизированные информационные системы технического учета электроэнергии
- Системы диспетчеризации в зданиях
- Автоматизированные системы управления инженерным оборудованием зданий
- Системы управления на транспорте
- Автоматизированные системы управления в энергетике
- Электронные системы безопасности, системы контроля доступа
- Системы геопозиционирования
- Робототехника
- Системы аварийного управления

Преимущества

- При интеграции индустриальных криптомодулей ViPNet SIES Core & Pack в АСУ информационная безопасность обеспечивается на уровне данных, при этом объем защищаемых данных определяется разработчиком АСУ
- Поддержка промышленных интерфейсов позволяет интегрировать индустриальные криптомодули ViPNet SIES Core & Pack в АСУ без модификации топологии информационных потоков
- Задачи первоначальной инициализации криптографии, обеспечения безопасности ключевой информации и поддержания соответствующей инфраструктуры, необходимые при использовании средств криптографической защиты информации (СКЗИ), не возлагаются на АСУ
- Использование извлекаемого криптографического чипа позволяет минимизировать затраты на изменения технологических и организационных процессов при производстве, установке, хранении и обслуживании АСУ с СКЗИ, необходимые в соответствии с требованиями законодательства РФ

infotecs

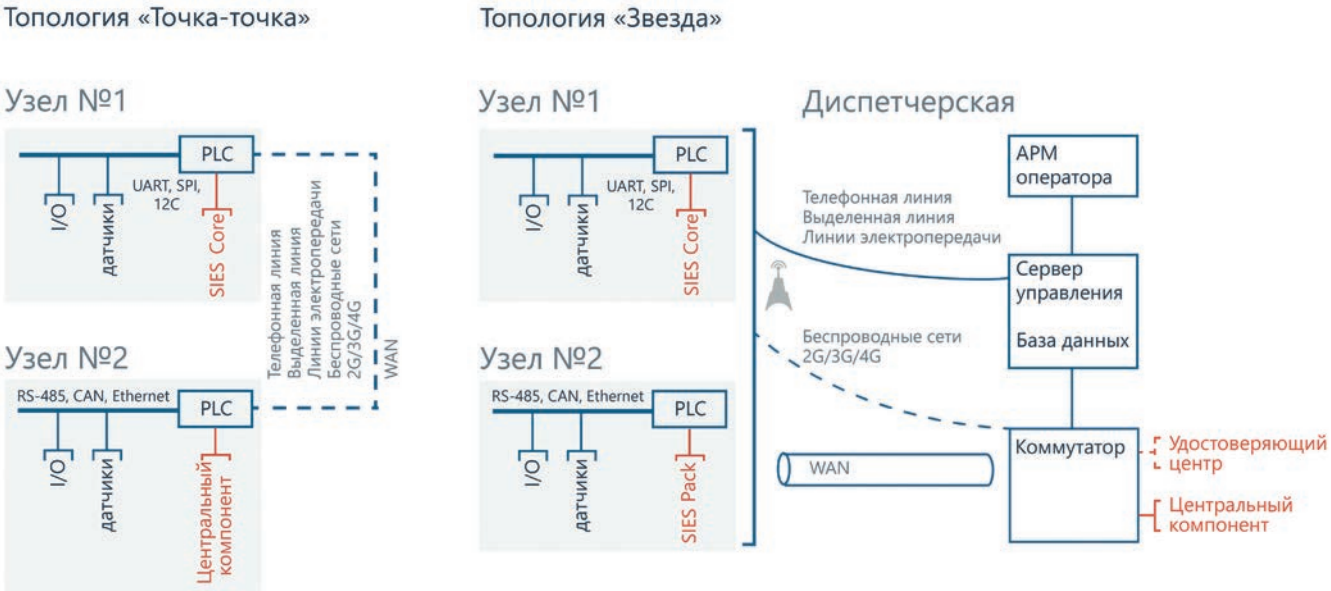
Исполнение и интерфейсы

Криптомодули ViPNet SIES Core & Pack имеют несколько исполнений в зависимости от условий окружающей среды, что позволяет применять решение для различных по архитектуре систем управления.

- **Криптомодуль ViPNet SIES Core** является системой на модуле (SOM) и представляет собой плату для встраивания в электронные устройства автоматизации. ViPNet SIES Core поддерживает работу по интерфейсам UART, SPI, I2C. Криптографический чип может быть установлен в разъем или впаян на плату в зависимости от требований вибропрочности и виброустойчивости.

- **Криптомодуль ViPNet SIES Pack** представляет собой законченное устройство в корпусе и предназначен для интеграции в АСУ без их аппаратной модификации. ViPNet SIES Pack поддерживает ряд промышленных и коммуникационных интерфейсов: RS-232/ RS-485, CAN, Ethernet, USB, GSM/GPRS/EDGE/ UMTS/HSPA, Wi-Fi. Криптомодуль может работать в режиме «точка-точка» с устройством автоматизации или подключаться к уже имеющейся общей шине данных. Исполнение корпуса IP66 и применение разъемов с фиксацией позволяют использовать ViPNet SIES Pack в сложных условиях эксплуатации.

Варианты применения ViPNet SIES в АСУ



infotecs

Интеграция ViPNet SIES Core & Pack в АСУ

При интеграции в АСУ функций информационной безопасности к каждому из управляющих устройств автоматизации, PLC-контроллеров и контроллеров АСУ (далее PLC) подключаются индустриальные криптомодули в подходящем варианте исполнения. Количество индустриальных криптомодулей ViPNet CS определяется количеством PLC в АСУ. Индустриальный криптомодуль является пассивным устройством, подключается к PLC «сбоку» и предоставляет криптографический сервис для АСУ. Физическое подключение криптомодуля к PLC заключается в выборе физического интерфейса передачи данных и реализации вызова набора команд в соответствии с протоколом.

В зависимости от топологии АСУ на одном из Узлов или на Серверной стороне устанавливается Центральный компонент. В зависимости от требований по производительности в роли Центрального компонента могут выступать индустриальные криптомодули ViPNet SIES Core & Pack, криптосервер ViPNet HSM или компьютер, в том числе и промышленный, под управлением ОС Windows, Linux и ОС реального времени с интегрированными криптографическими библиотеками ИнфоТеКС.

Для проведения криптографических операций с ЭП в индустриальном криптомодуле ViPNet SIES Core & Pack и Центральном компоненте к АСУ подключается Удостоверяющий центр (УЦ).

Средства разработчика

Для упрощения интеграции криптомодуля в АСУ компания ИнфоТеКС предлагает набор отладочных средств. Средства разработки предоставляются по запросу.

- **Эмулятор криптомодуля** представляет собой виртуальную машину с набором API. Виртуальная машина реализует все функциональные возможности индустриальных криптомодулей ViPNet SIES Core & Pack , к которым можно подключиться через Ethernet или виртуальный последовательный порт. Эмулятор позволяет производить отладку взаимодействия с ViPNet SIES Core & Pack без физического наличия самого устройства.

- **Отладочная плата ViPNet SIES Kit** представляет собой платформу для независимого использования индустриального криптомодуля ViPNet SIES Core и позволяет работать с платой как с готовым устройством на этапах отладки и тестирования.

Сертификаты

В настоящий момент ведутся работы по сертификации ViPNet SIES в ФСБ России на соответствие требованиям к СКЗИ класса КС3.

infotecs

Характеристики

	ViPNet SIES Core	ViPNet SIES Pack
Функциональные показатели		
Скорость шифрования	1,5 кбайта/с	
Скорость хеширования	2,3 кбайта/с	
Время создания электронной подписи	1 с	
Время проверки электронной подписи	0,55 с	
Технические характеристики		
Процессор	ARM Cortex M	
Операционная система	Free RTOS	
Криптографический чип	Смарт-карта (ISO 7816)	
Хранение данных	Карта microSD	
Протокол	Modbus RTU, Modbus TCP	
Интерфейсы	SPI, UART, I2C, USB 2.0 device	Ethernet, USB 2.0 OTG, GSM, Wi-Fi, RS-232, RS-485, CAN
Габаритные размеры	64 x 36 мм	145 x 120 x 40 мм
Питание	4...17 В DC	9...36 В, 18...36, 36...75 В DC
Условия эксплуатации		
Защита от статического электричества (ESD)	15 кВ для всех интерфейсов	
Рабочая температура	–40 °C... +75 °C	–40 °C... +60 °C
Влагозащита, пылезащита	зависит от конечного решения	IP66
Соответствие стандартам	—	EN 55022, EN 55024 (стандарты электромагнитной совместимости)
Криптографические алгоритмы	ГОСТ Р34.10-2012, ГОСТ Р 34.11-2012 определяется криптографическим чипом	
Вибростойкость	1g в диапазоне частот 5–150 Гц	

* Характеристики ViPNet SIES могут быть модифицированы согласно требованиям конкретного проекта.

ОАО «ИнфоТеКС»
127287, Москва, Старый Петровско-Разумовский проезд, 1/23, стр. 1
Телефон: +7 495 737-6192, 8 800 250-0-260 (бесплатный звонок по России)
Факс: +7 495 737-7278
Email: soft@infotecs.ru, hotline@infotecs.ru
Web: www.infotecs.ru

10017-01 101 01 RUS