

В современных системах автоматизации широко используется сетевой обмен данными между отдельными компонентами автоматизации, между компонентами автоматизации и офисным уровнем предприятия, удаленный доступ к производственным данным через интернет. Использование сетевых технологий повышает открытость и гибкость системы управления производством, упрощает вопросы интеграции новых компонентов, позволяет быстро анализировать поступающие данные, принимать обоснованные решения, повышает конкурентоспособность предприятия.

Однако использования открытых систем связано с рисками кибератак, манипуляции данными, саботажа и промышленного шпионажа. Для надежной защиты от этих негативных воздействий необходимо использовать многоуровневую концепцию защиты производственных данных, которую можно разделить на три уровня:

- Обеспечение защиты на уровне предприятия. Базируется на организационных мерах по мониторингу и контролю доступа, а также внедрению процессов управления безопасностью.
- Обеспечение сетевой безопасности, предполагающей ограничение доступа к производственной сети.
- Обеспечение системной целостности, предполагающей контроль доступа и защиту целостности данных компонентов автоматизации.

Ключевым элементом этой концепции является сетевая безопасность. Она обеспечивается защитой доступа к сетям автоматизации и другим сетям, защитой от удаленного доступа через интернет, сегментацией сетей.

Обеспечение сетевой безопасности в системах автоматизации SIMATIC поддерживается на уровне:

- Аппаратуры серии SCALANCE S.
- Коммуникационных процессоров CP 343-1 Advanced/ CP 443-1 Advanced/ CP 1243-1/ CP 1543-1/ CP 1543SP-1 программируемых контроллеров S7-300/ S7-400/ S7-1200/ S7-1500/ ET 200SP соответственно.
- Коммуникационного процессора CP 1628 для компьютеров.
- Программного обеспечения SOFTNET Security Client для компьютеров.
- UMTS роутера SCALANCE M875.

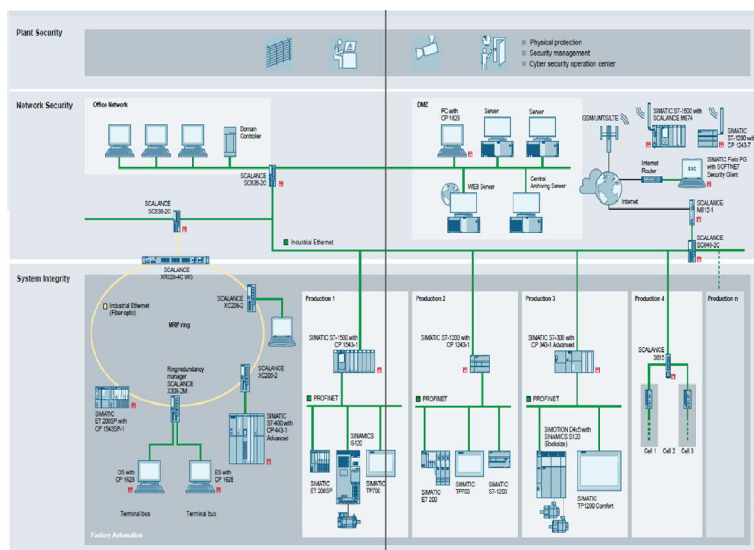
### Модули семейства SCALANCE S

Семейство SCALANCE S объединяет модули защиты данных в производственных и открытых сетях. Они обеспечивают защиту данных, передаваемых между системами автоматизации, защиту от ошибок операторов, от несанкционированного доступа, предотвращают сбой в работе и перегрузку сети. Они способны выполнять аутентификацию партнеров по связи, шифровать данные и передавать их через VPN, защищая от шпионажа и манипуляций. Защищенный обмен данными не зависит от используемых протоколов и может выполняться через интернет.

Конфигурирование всех приборов семейства выполняется с помощью программного обеспечения STC (Security Configuration Tool). Применение аппаратуры SCALANCE S не требует внесения изменений в топологии существующих сетей.

Все модули семейства обеспечивают поддержку функций межсетевого экрана (firewall). Конфигурирование межсетевых экранов выполняется с использованием глобальных правил и символьных имен для IP адресов. В соответствии с этими правилами могут устанавливаться различные уровни прав доступа к сети.

Дополнительный набор поддерживаемых функций зависит от типа используемого модуля.



### SCALANCE SC600

Модуль SCALANCE SC600 может использоваться в сетях со скоростью обмена данными 10/100/1000 Мбит/с. Дополнительно к режиму моста он способен выполнять и функции IP маршрутизатора, присваивать IP адреса внутренним сетевым узлам через встроенный DHCP сервер, обеспечивает поддержку протоколов NAT и NATP.

Он позволяет анализировать содержимое регистрационного журнала с помощью Syslog сервера, обеспечивает поддержку протокола SNMP и может интегрироваться в систему управления сетью, способен работать с динамическими IP адресами.


Поддержка функций VPN шлюза обеспечивает защиту данных от шпионажа и несанкционированных манипуляций.

В сочетании с программным обеспечением SOFTNET Security Client и маршрутизаторами SCALANCE M UMTS модуль позволяет выполнять безопасный удаленный доступ через интернет с поддержкой функций IPsec VPN.

### SCALANCE S615

Модуль SCALANCE S615 может использоваться в сетях со скоростью обмена данными 10/100 Мбит/с и обеспечивает поддержку всех функций модуля S612. Модуль позволяет свободно конфигурировать до пяти защищенных зон и межсетевых экранов между ними на один порт VLAN. Для удаленного доступа через интернет он позволяет использовать не только UMTS, но и GPRS/LTE маршрутизаторы SCALANCE M.

Модуль может быть легко подключен к SINEMA Remote Connect через автоматически конфигурируемый интерфейс (активируется при использовании KEY-PLUG SINEMA Remote Connect) с поддержкой функций OpenVPN.

SCALANCE SC632-2C	SCALANCE SC636-2C	SCALANCE S615	SCALANCE SC642-2C	SCALANCE SC646-2C
				
10/100/1000 Мбит/с	10/100/1000 Мбит/с	10/100 Мбит/с	10/100/1000 Мбит/с	10/100/1000 Мбит/с
Firewall	Firewall	Firewall	Firewall	Firewall
4-порта	6-портов	До 20 VPN туннелей	До 200 VPN туннелей	До 200 VPN туннелей

#### SCALANCE SC632-2C

2x комбинированных порта, электрических или оптических; 10/100/1000 Мбит / с RJ45 или 100 Мбит / с SFP или 1000 Мбит / с SFP, брандмауэр, SINEMA RC (со встроенной лицензией устройства).

#### SCALANCE SC636-2C

4x комбинированных порта, электрических или оптических; 10/100/1000 Мбит / с RJ45 или 100 Мбит / с SFP или 1000 Мбит / с SFP, брандмауэр, SINEMA RC (со встроенной лицензией устройства).

#### SCALANCE SC642-2C

2x комбинированных порта, электрических или оптических, 10/100/1000 Мбит / с RJ45 или 100 Мбит / с SFP или 1000 Мбит / с SFP, брандмауэр, VPN, SINEMA RC (со встроенной лицензией устройства)

#### SCALANCE SC646-2C

4x порта, электрических 10/100/1000 Мбит / с RJ45 и 2x комбинированных портов, электрические или оптические, 10/100/1000

Мбит / с RJ45 или 100 Мбит / с SFP или 1000 Мбит / с SFP, брандмауэр, VPN, SINEMA RC (со встроенной лицензией устройства)

#### Программное обеспечение SOFTNET Security Client

Пакет SOFTNET Security Client является компонентом системы сетевой защиты данных программируемых контроллеров. Он устанавливается на компьютеры/ программаторы и выполняет функции VPN клиента, обеспечивающего защищенный доступ к системам автоматизации через LAN или WAN. Для использования SOFTNET Security Client компьютер/ программатор должен быть оснащен 32-разрядной операционной системой Windows XP Professional SP3, 32- или 64-разрядной операционной системой Windows 7 Professional/ Ultimate.

#### Цены (со склада в Москве без НДС) и заказные номера

Наименование	Заказные номера	Цена,€	
<b>Модули серии SCALANCE S*</b>			
SC632-2C: межсетевой экран, DHCP сервер, Syslog, символьные IP адреса, 10/100/1000 Мбит/с	6GK5632-2GS00-2AC2	1 112	
SC636-2C: межсетевой экран, DHCP сервер, Syslog, символьные IP адреса, 10/100/1000 Мбит/с	6GK5636-2GS00-2AC2	1 316	
S615: межсетевой экран, до 20 VPN соединений 10/100 Мбит/с	6GK5 615-0AA00-2AA2	750	
K-PLUG для активации SINEMA REMOTE CONNECT в модуле SCALANCE S615	6GK5 908-0PB00	117	
SC642-2C: межсетевой экран, до 200 VPN соединений, DHCP сервер, Syslog, 10/100/1000 Мбит/с	6GK5642-2GS00-2AC2	1 367	
SC646-2C: межсетевой экран, до 200 VPN соединений, брандмауэр, DHCP сервер, Syslog, 10/100/1000 Мбит/с	6GK5646-2GS00-2AC2	1 571	
<b>Программное обеспечение</b>			
SOFTNET Security Client V4: для поддержки защищенных VPN соединений между компьютерами/программаторами и сегментами сети PROFINET, модулями SCALANCE S (кроме S615), другими компонентами защиты данных	6GK1 704-1VW04-0AA0	255	
SINEMA REMOTE CONNECT VIRTUAL для поддержки защищенных VPN туннелей между модулями SCALANCE S615, SCALANCE M, компьютерами и программаторами	На 4 VPN соединения	6GK1 720-1AH01-0BV0	270
	На 64 VPN соединения	6GK1 722-1JH01-0BV0	1 005
	На 256 VPN соединений	6GK1 722-1MH01-0BV0	2 009
	На 1024 VPN соединения	6GK1 722-1QH01-0BV0	4 009
SINEMA Remote Connect Client V1.1 клиентское ПО	6GK1 721-1XG01-0AA0	127	
<b>SINEMA Server Basic V13 DL</b> программное обеспечение для мониторинга промышленных сетей, включая PROFINET, с определением топологии сети, с ведением архива событий и автоматическим генерированием отчетов, лицензия на	50 устройств	6GK1 781-1BA14-0AA0	1 479
	100 устройств	6GK1 781-1DA14-0AA0	2 173
	250 устройств	6GK1 781-1JA14-0AA0	3 213
	500 устройств	6GK1 781-1TA14-0AA0	5 141

\* Необходим модуль K-PLUG, заказываемый отдельно

Дополнительную информацию по продуктам Вы можете найти в Интернете по адресу [www.siemens.com/industrial-security](http://www.siemens.com/industrial-security)