SIEMENS
Ingenuity for life

Информационная безопасность в PA

SIMATIC PCS 7 V9.0

Serhii Stepaniuk, RC-UA PD P&S

Промышленная безопасность

SIEMENS
Ingenuity for life

- **Введение**
- Стандарт IEC 62443
- Решение SIEMENS
- Примеры применений
- Преимуществаs работы с Siemens

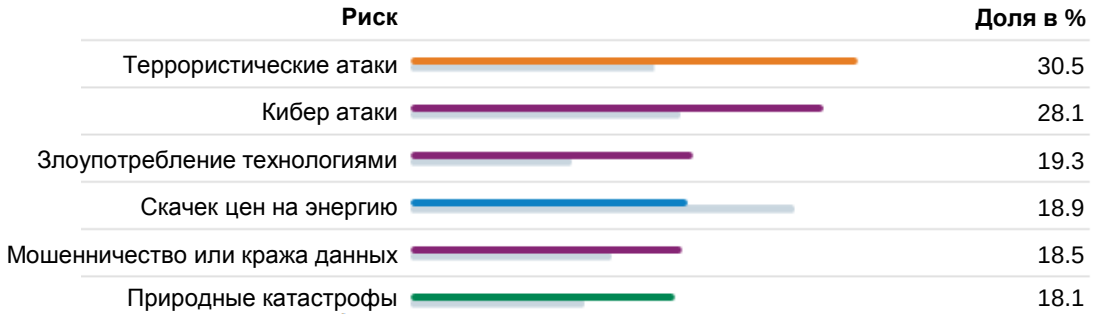
Тренды угроз
Мы видим больше сетевых подключений чем когда либо ранее

SIEMENS
Ingenuity for life

Тенденции влияющие на безопасность

- Подходы облачных вычислений
- Рост использования мобильных устройств
- Беспроводные технологии
- Требования к сокращению персонала
- Умные сети энергоснабжения
- Удаленный доступ к предприятиям, машинам и мобильным приложениям
- “Интернет Вещей”

Рейтинг рисков для бизнеса :



Источник: Международный экономический форум, отчет глобальных рисков 2018, Глобальные риски наибольших проблем для ведения бизнеса – США
http://reports.weforum.org/global-Риски-2018/

Промышленная безопасность
BSI[1]: Top 10 угроз для АСУ

SIEMENS
Ingenuity for life

Обзор топ 10 угроз 2016

1. Социальный инжиниринг и фишинг[2]
2. Введение malware через сменные носители и внешние устройства
3. Malware инфекция через Internet и Intranet
4. Вторжение через удаленны доступ
5. Человеческая ошибка и саботаж
6. Компоненты управления подключенные через Internet
7. Технические неполадки и форс-мажор
8. Компрометирование компонентов внешней сети и облака
9. (Распределенные) атаки «запрет сервиса» ((D)DOS)
10. Компрометирование смартфонов в производственной среде

1 Федеральное ведомство по информационной безопасности Германии
2 Аналитика: BSI анализ по кибер безопасности в 2016

Промышленная безопасность

Кибер-уязвимости могут повлиять на предприятие на разных уровнях

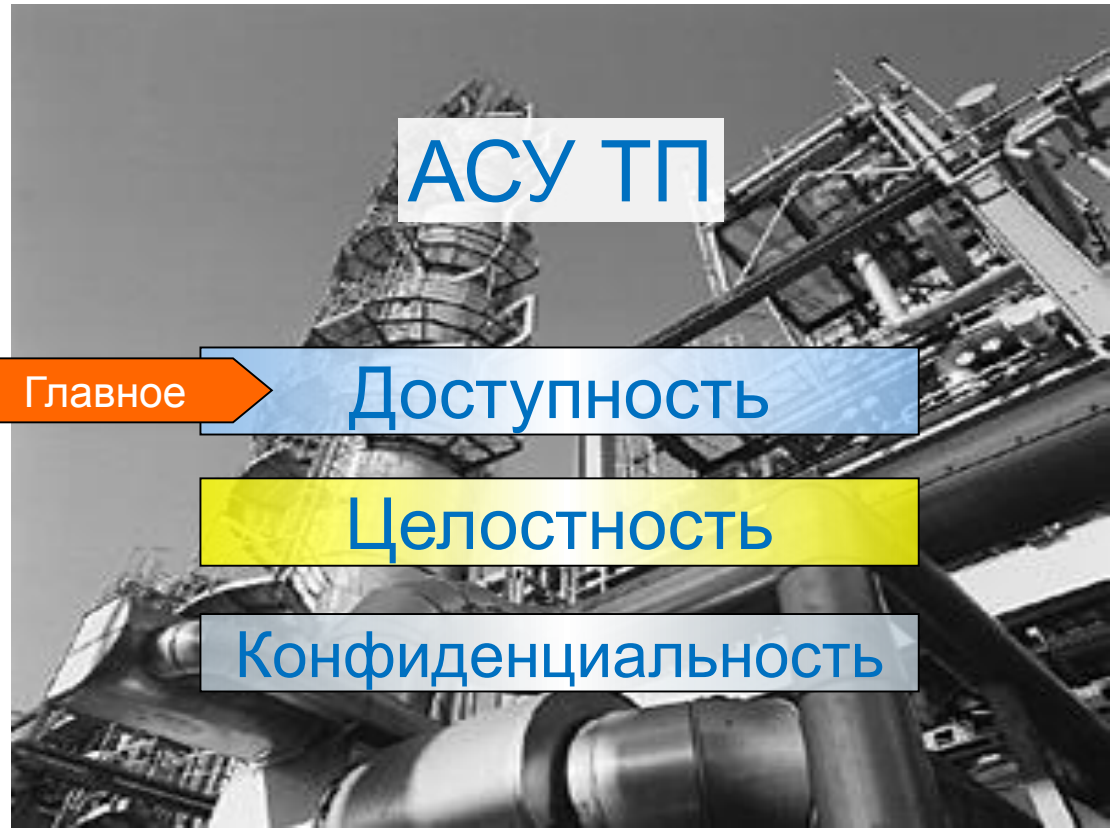
SIEMENS
Ingenuity for life

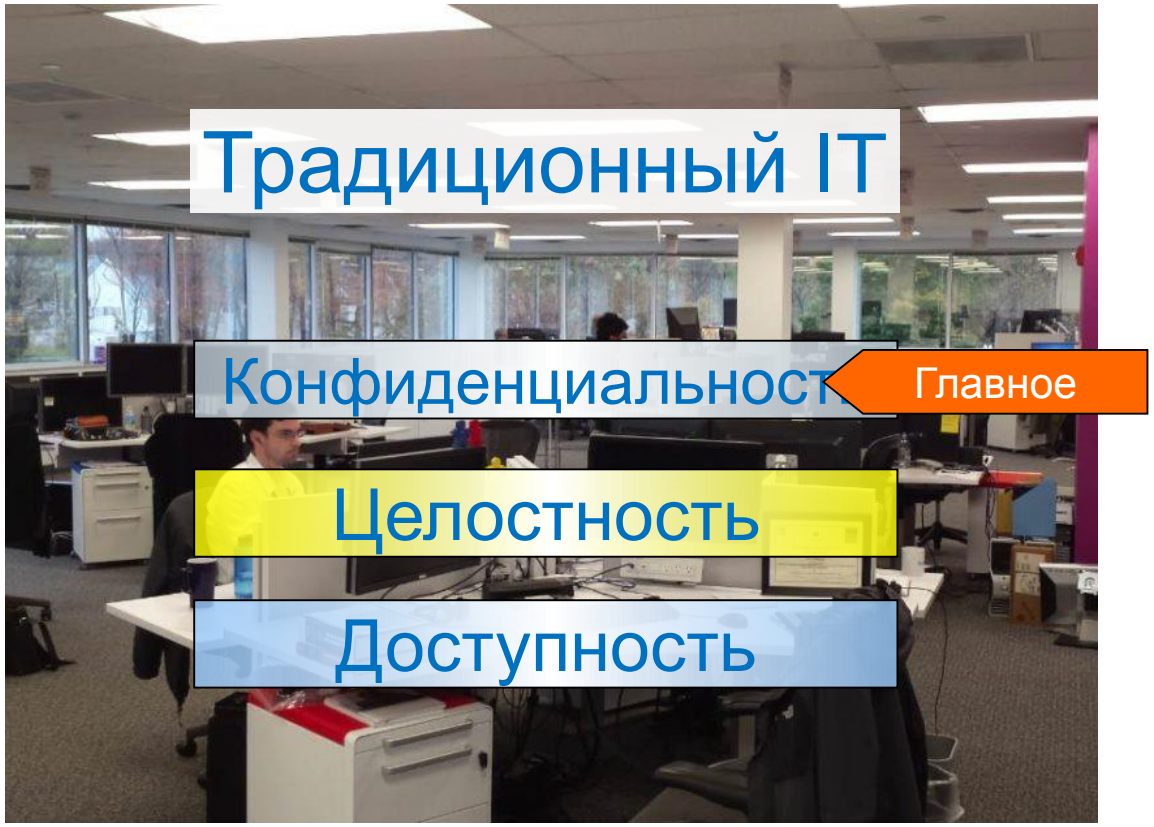
Необходимо действовать из-за уязвимостей в кибер-безопаснсоти

- Потеря интеллектуальной собственности, рецептов,…
- Саботаж производства
- Простои напр. по причине вирусов или malware
- Манипуляция данными или программами
- Неавторизированное использование функций системы
- Соответствие нормам кибер безопасности
  - Нормативные акты:
    FDA, NERC CIP, CFATS, CPNI, KRITIS
  - Стандарты:
    ISA 99, IEC 62443

Среда IT и АСУ ТП имеют разные цели безопасности

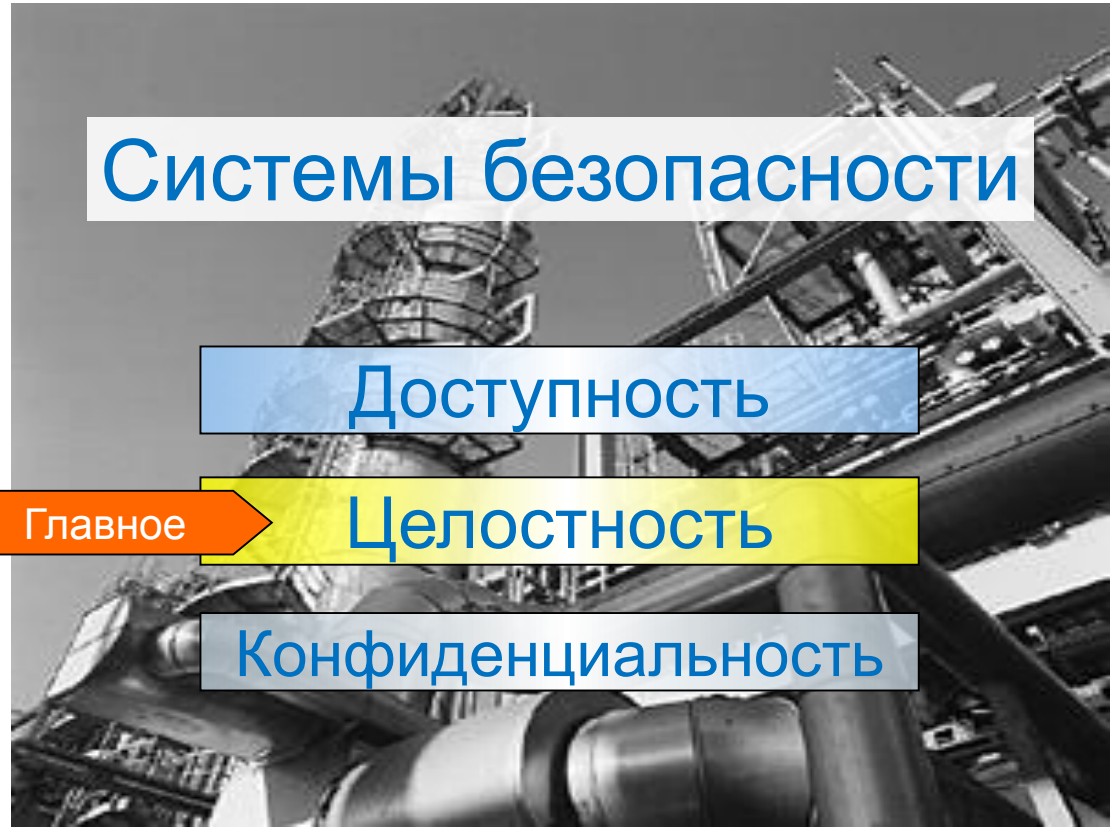
SIEMENS
Ingenuity for life

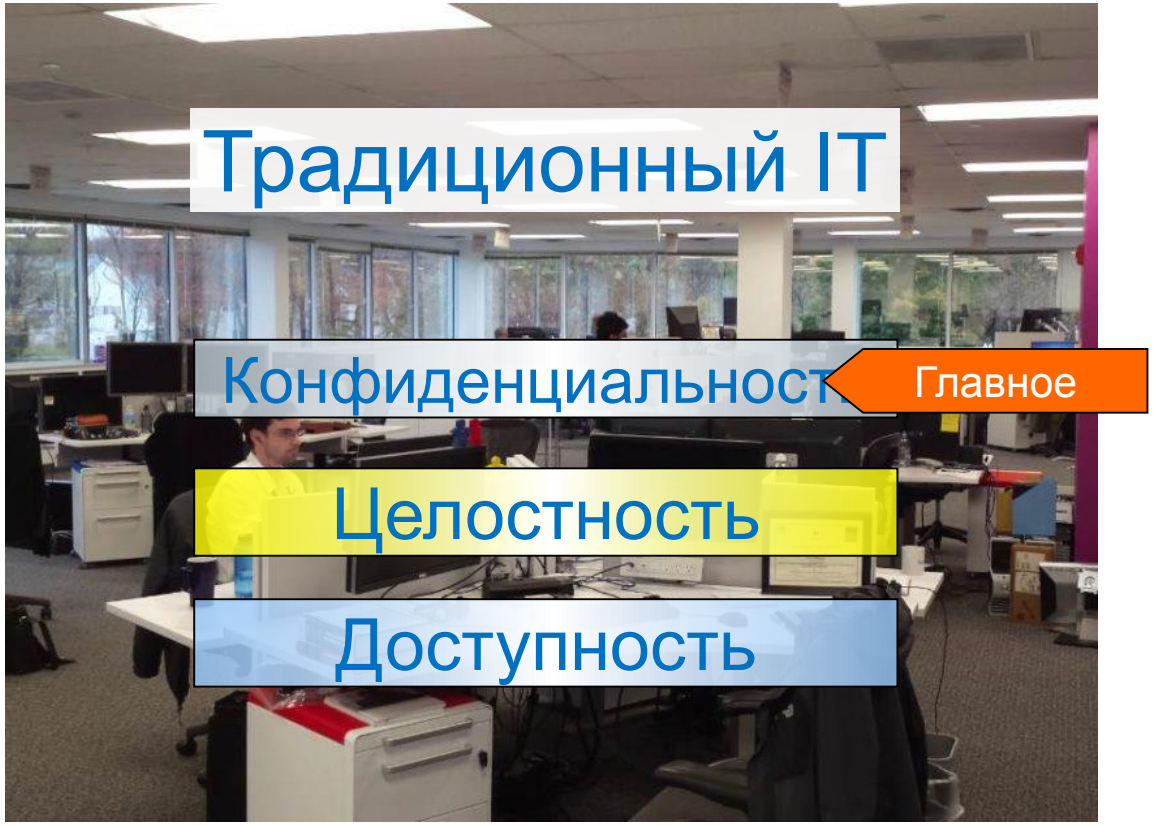




Среда IT и АСУ ТП имеют разные цели безопасности

SIEMENS
Ingenuity for life





Безопасность IT против промышленной безопасности

SIEMENS
Ingenuity for life

„Office Security“ vs. „Industry Security“ …

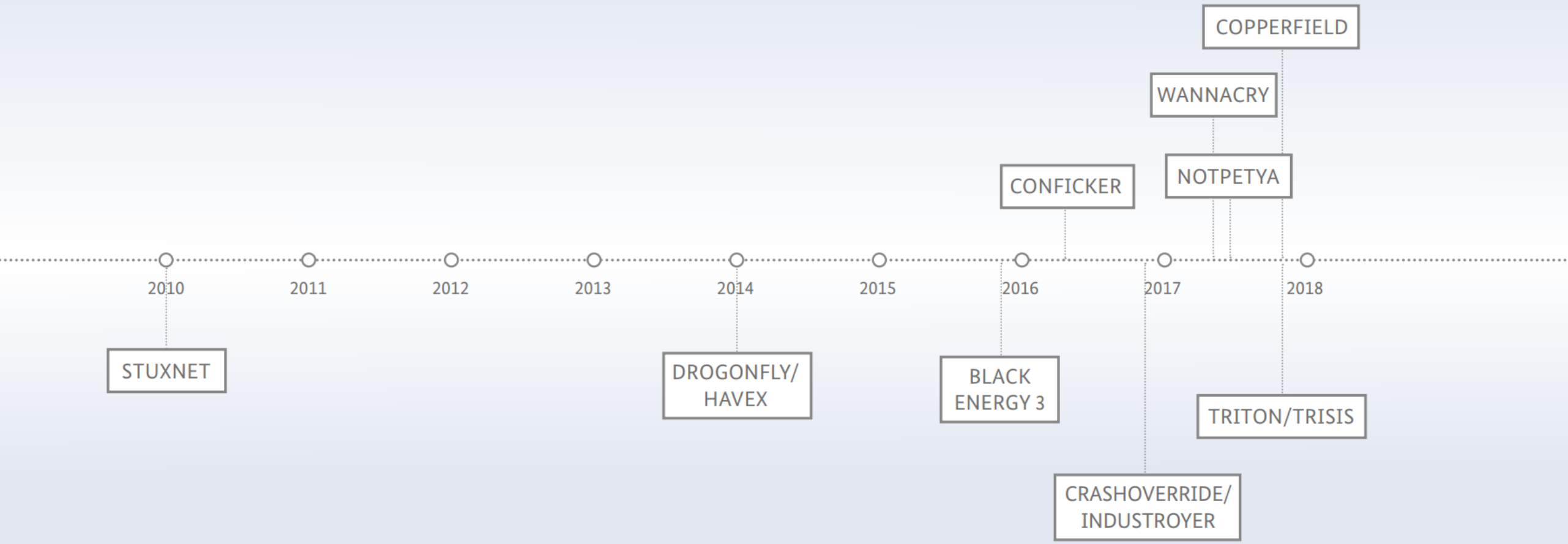
… can‘t we just use „Office Security“ for „Industry Products“?

https://www.cert.siemens.com/

=> Well, YES and NO!

Временная шкала ТОП целевых и не целевых атак, затронувших АСУ

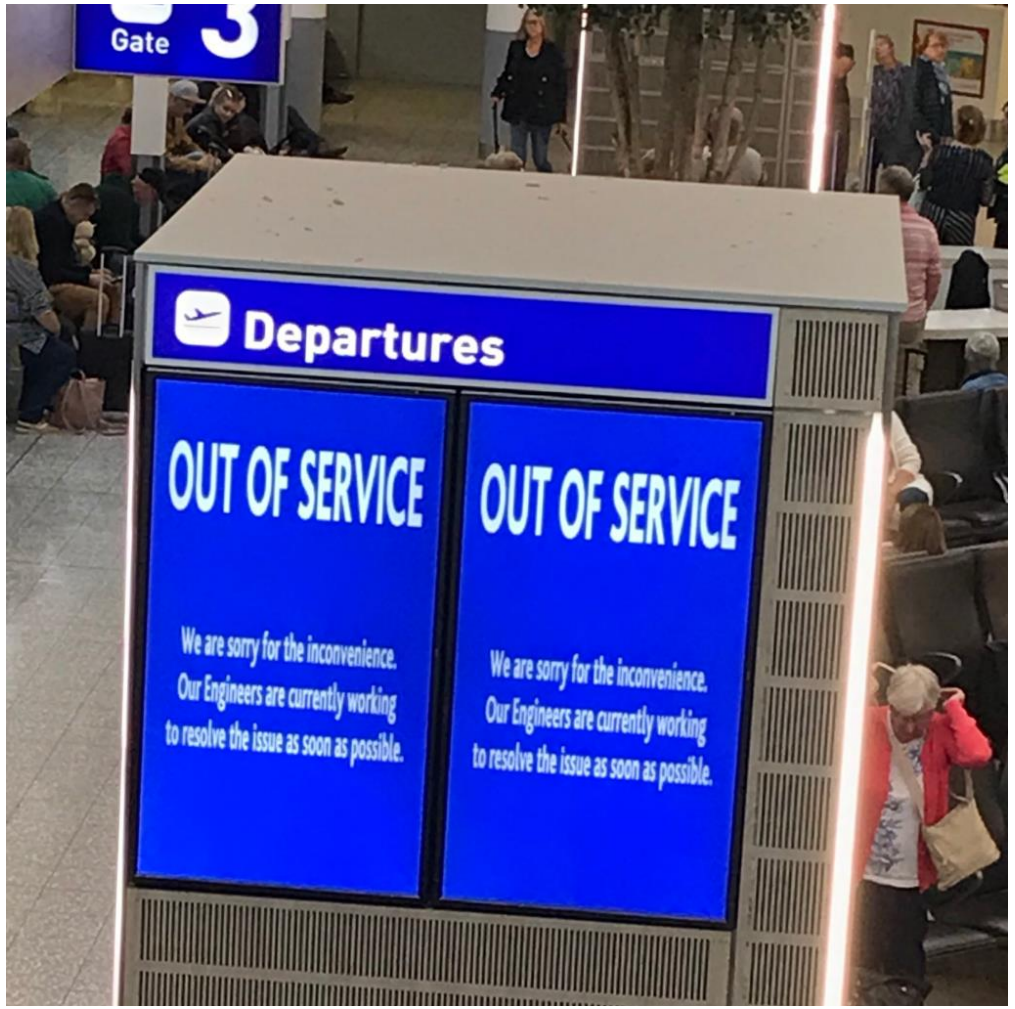
SIEMENS
Ingenuity for life

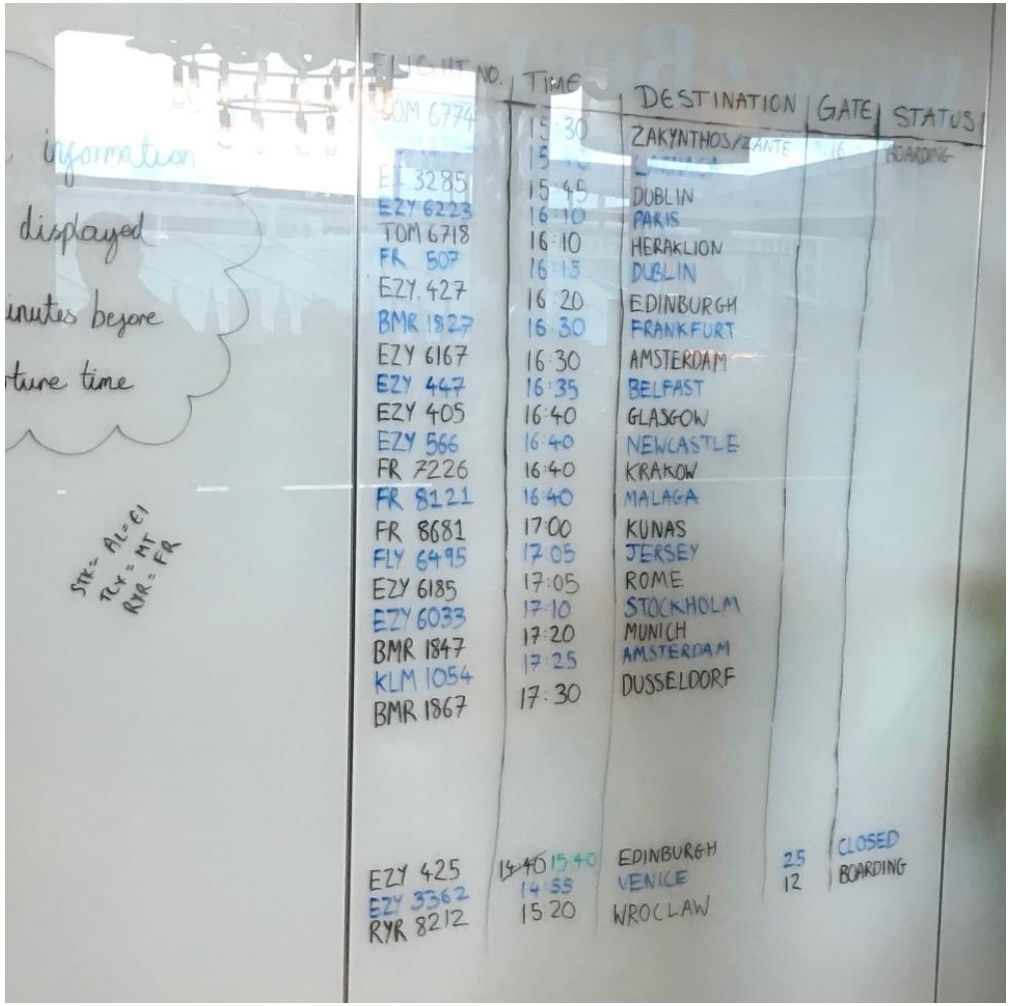


Журнал Безопаснсоть в фокусе. АСУ в Industry 4.0, BSI Magazine 2018/01

14 - 16 сентября 2018 г
Кибер атака на инфраструктуру Бристольского аэропорта

SIEMENS
Ingenuity for life

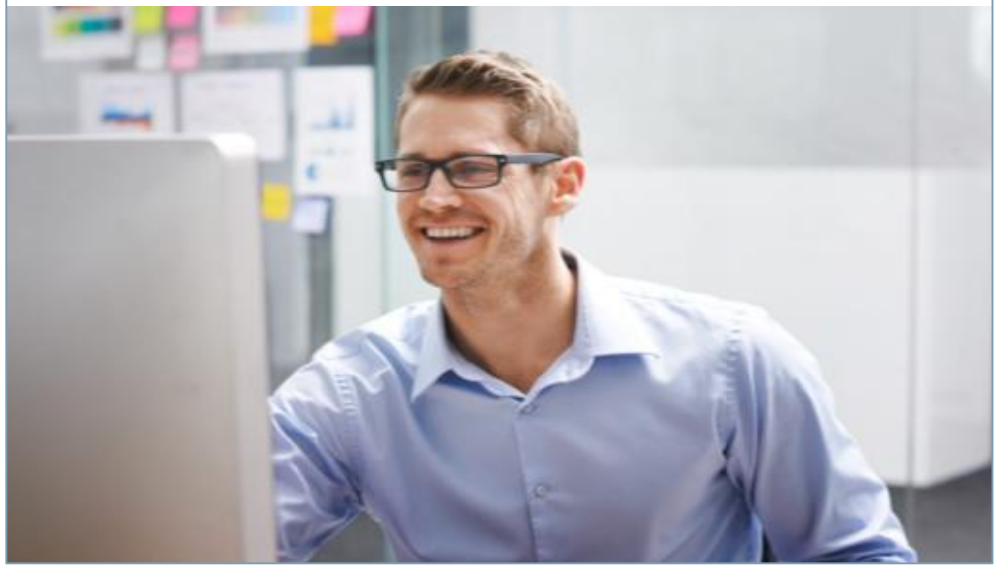




https://www.telegraph.co.uk/news/2018/09/16/bristol-airport/

Кибер атаки возможны «изнутри»

« Зачем беспокоиться?
Моя система не подключена к Интернет»



Управление исправлениями безопасности и другими мерами кибер защиты необходимо даже если Интернет не подключен

Внешние атаки

Атаки через внешниние подключения напр.:

- E-mails (встроенные трояны, инфицированные вложения, гиперссылки на другие системы, …)
- Любые внешние подключения являются потенциальной угрозой, не ограничиваясь только интернетом !

Брандмауэр

Система пользователя

Внутренние атаки

Атака через внутренние системы, например.:

- Инфицированные USB накопители, CD/DVD или другие IT устройства
- Ноутбуки из вне, например принесенные инженером или подрядчиком
- Все вновь установленное ПО или внешние данные

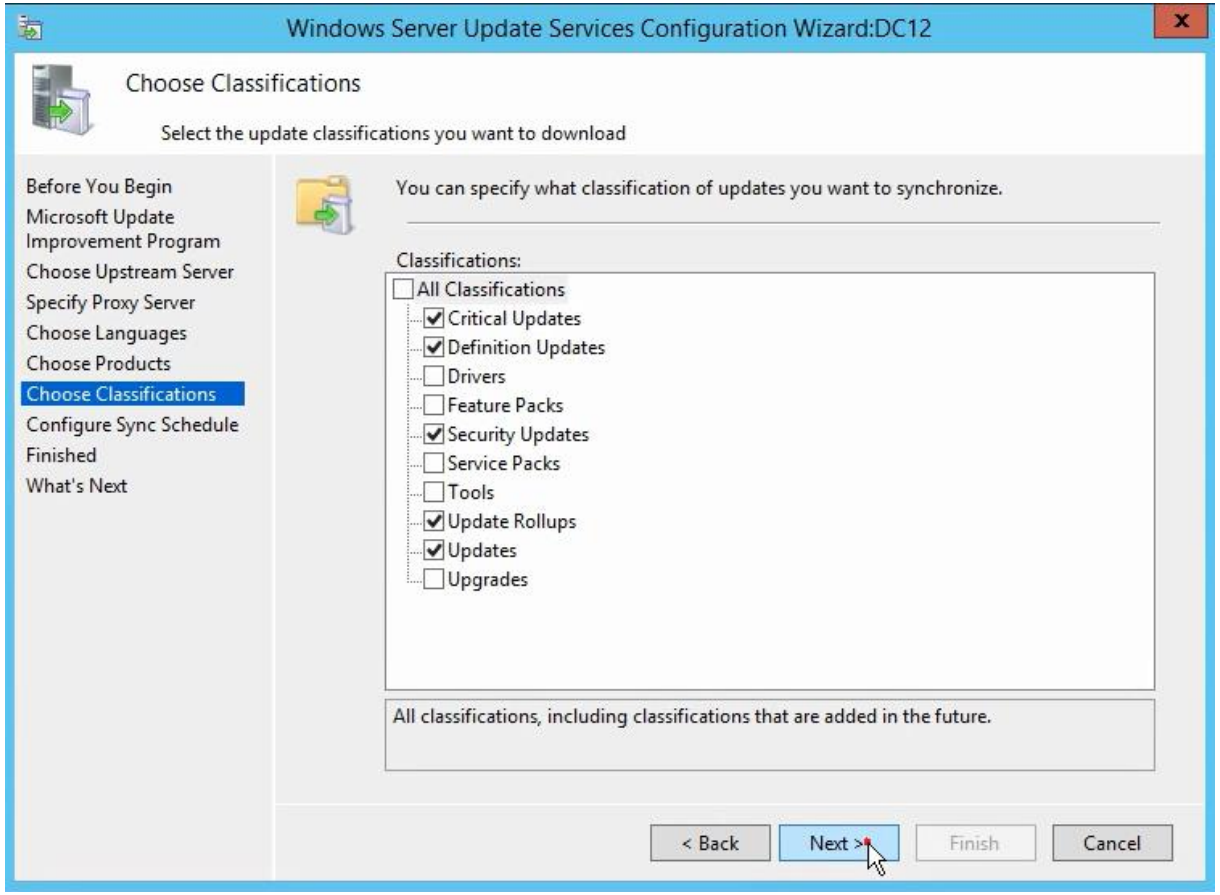
⌧ Даже наилучшие внутренние системы и процедуры могут оставлять возможные риски кибер атак. Люди могут не преднамеренно стать критическими уязвимостям!

Рекомендованная процедура управления изменениями с Microsoft Windows Server Update Service (WSUS)

SIEMENS
Ingenuity for life

WSUS конфиграция

- В диалоге "Products and Classifications" выбрать закладку "Products" и затем все Microsoft продукты имеющие отношение к предприятию.
- В "Products and Classifications" выбрать закладку "Classifications" и отметить :
  - "Definition Updates",
  - "Security Updates",
  - "Update Rollups",
  - "Updates"
  - "Critical Updates"
- Создание группы под проект для распределения обновлений по предприятию.



https://support.industry.siemens.com/cs/document/**18490004**

Windows 10 LTSB (Long Term Servicing Branch – Ветка долгосрочного обслуживания)

SIEMENS
Ingenuity for life

Обновление в версии LTSB (Long Term Servicing Branch)

- Обновление без нового функционала
- Продолжительная основная поддержка - 5 лет
- Расширенная поддержка - 5 лет
- Для сложных процессов проведения изменений или критически важных систем, предусмотрено откладывание обновлений, получение обновлений безопасности и критических исправлений
- Управление обновлениями доступно через Windows Server Update Service (WSUS).

IPC 547G

IPC 647D / 847D

IPC 427E / 477E

IPC 627D / 677D

Производительность

24/7 Готовность и Защита

Жизненный цикл

Гибкость

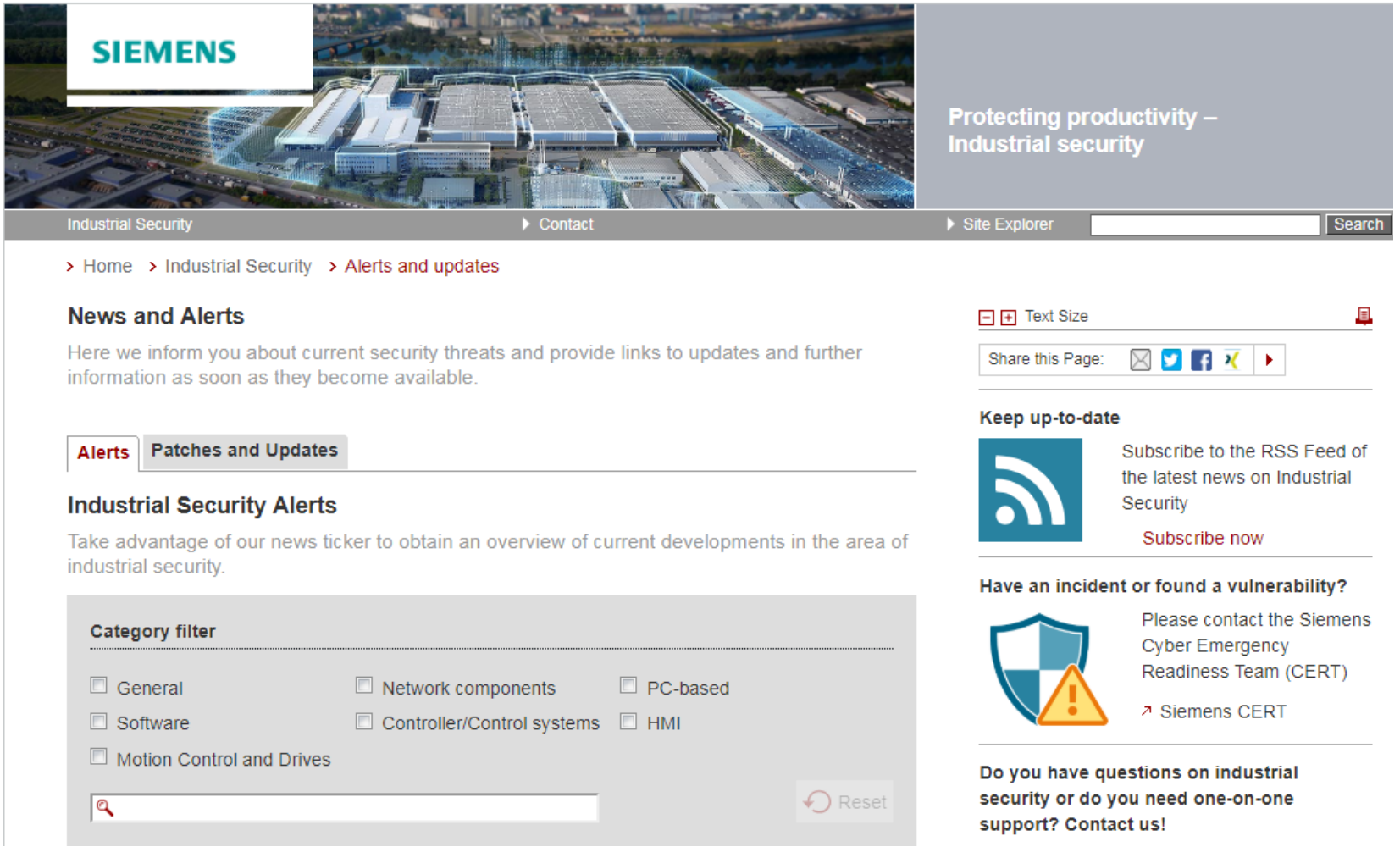
Какие обновления Microsoft Update протестированы на совместимость с SIMATIC PCS 7?

SIEMENS
Ingenuity for life

	A	B	C	D	E	F	G	H	I
1	PatchedProduct	PatchIdentifier1	PatchIdentifier2	ReleaseDate (YYYY-MM-DD)	Description	Patch Status	ReferenceInfo	PassedProduct	FailedProduct
2	2018-08 Security Update for Windows Server 2008 for x86-based Systems (KB4338380)	KB4338380		2018-08-14	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	Current	https://support.microsoft.com/en-us/kb/4338380	PCS7Vxy	-
3	2018-08 Security Update for Windows Server 2008 for x86-based Systems (KB4340937)	KB4340937		2018-08-14	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	Current	https://support.microsoft.com/en-us/kb/4340937	PCS7Vxy	-
4	2018-08 Security Update for Windows Server 2008 for x86-based Systems (KB4340939)	KB4340939		2018-08-14	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	Current	https://support.microsoft.com/en-us/kb/4340939	PCS7Vxy	-
5	2018-08 Security Update for Windows Server 2008 for x86-based Systems (KB4341832)	KB4341832		2018-08-14	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	Current	https://support.microsoft.com/en-us/kb/4341832	PCS7Vxy	-
6	Cumulative Security Update for Internet Explorer 11 for Windows 7 (KB4343205)	KB4343205		2018-08-14	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	Current	https://support.microsoft.com/en-us/kb/4343205	PCS7Vxy	-
7	Cumulative Security Update for Internet Explorer 11 for Windows 7 for x64-based Systems (KB4343205)	KB4343205		2018-08-14	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	Current	https://support.microsoft.com/en-us/kb/4343205	PCS7Vxy	-

https://support.industry.siemens.com/cs/document/**18490004**

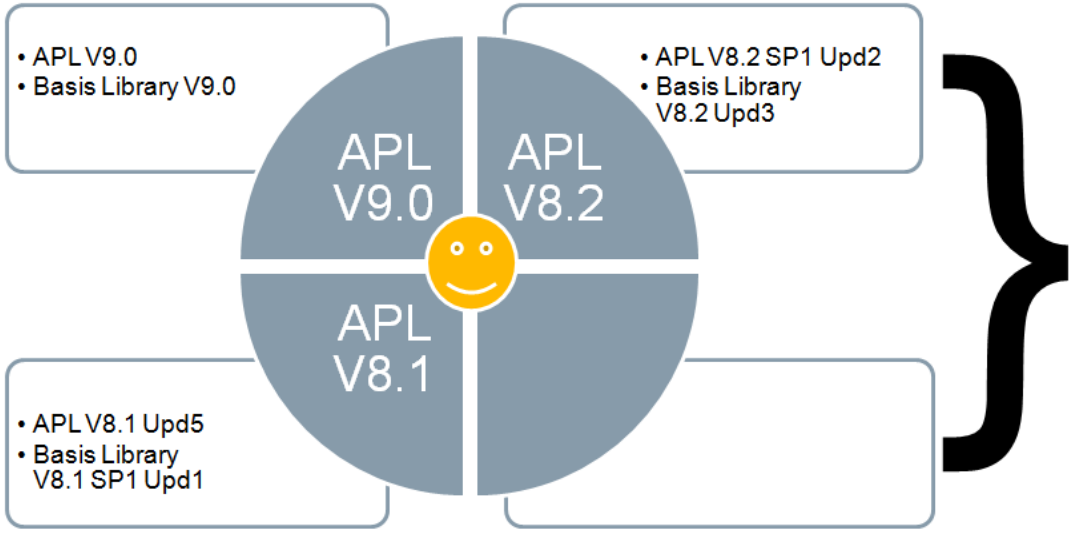
Какие обновления необходимы для продуктов SIEMENS ?
Предупреждения промышленной безопасности

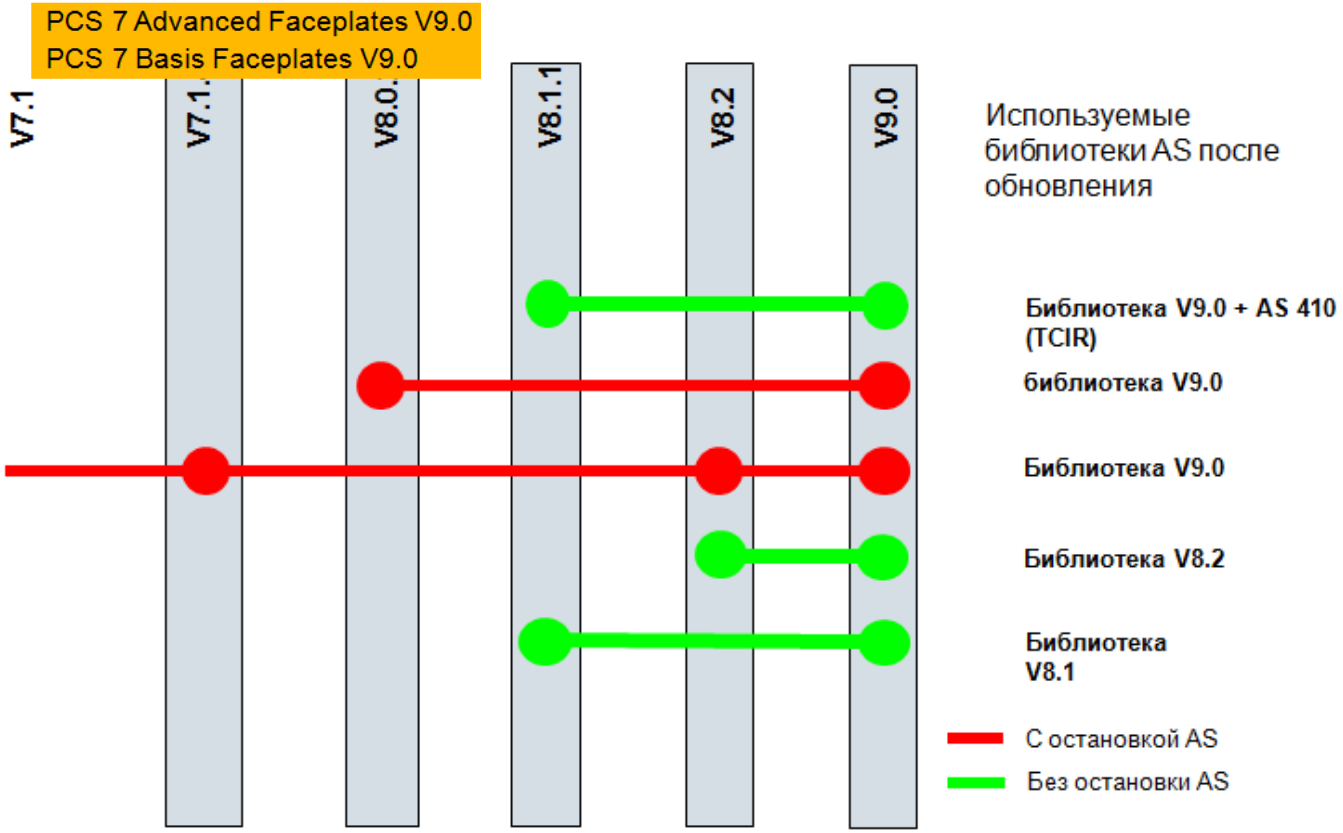


https://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/overview.aspx

Как обновить версию SIMATIC PCS 7 ?
Продуманная процедура перехода но новую версию

SIEMENS
Ingenuity for life





Кибер защита не одноразовое действие, но постоянная задача управления работой системы

SIEMENS
Ingenuity for life

Кибер угрозы

- Атаки через **внешние** подключения и данные (internet, email, проч.)
- Атака через **внутренние** системы (USB память, CD/DVD, сторонние ноутбуки, например **инженеров и проч**.)

Стандарты и законы

- **Примеры:**
  - NERC/CIP: USA
  - ISO 27001: Германия
  - NIS директива: EU
- Критично **наличие системы оценки рисков**

NIS directive

Задачи эксплуатации системы

- Необходима полная **прозрачность** конфигурации и ПО системы
- Требуется хотя бы **ежегодный обзор** изменений конфигурации и ПО
- Оценка потенциальных угроз IT безопасности і**постоянной** основе (например патчей безопасности ПО)
- **Эксплуатация отвечает** за:
  - Сбор информации
  - Определение и оценку риска
  - Определение мер смягчения
  - Выполнение мер

Поддержка и сервис Siemens

- **Концепция глубинной обороны:** Smart комбинация множества уровней системы и дополнительных мер безопасности
- **Мы поддерживаем заказчика:**
  - Выявление технических уязвимостей
  - Рекоммендации
  - Реализация систем у заказчика

Идентиф. | Защита | Обращ

Консультации и Обучение

Multiple system layers and complementing IT security measures enhance IT security

SIEMENS
Ingenuity for life

Безопасность в средние века

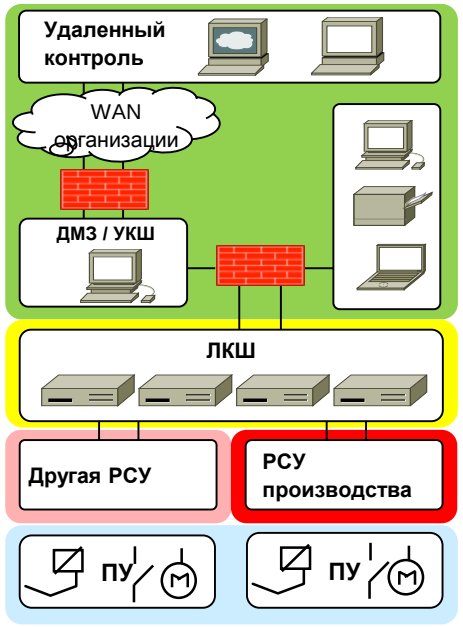
Современная глубоко эшелонированная IT защита

Влияние и вероятность кибер атаки должна быть учтена при оценке риков

SIEMENS
Ingenuity for life

Влияние риска

Влияние риска на функциональность и производительность системы



Система структурирована по зонам:

- **Основная зона критична** для функциональности системы
  → ***Большое влияние***
- **Не основная зона не критична** для функциональности системы
  → ***Малое влияние***

Зоны:

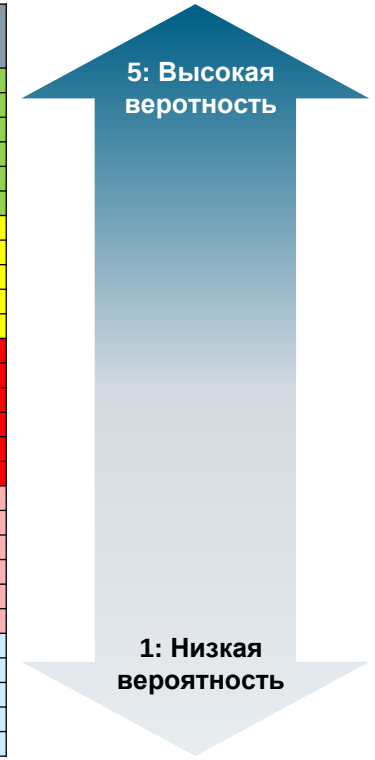
- Не основная зона
- Основная зона
- Основная зона РСУ
- Зона другой РСУ
- Полевой уровень

РСУ	Распределенная система управления
ПУ	Полевые устройства
ЧМИ	Человеко-машинный интерфейс
LAN	Local Area Network
ЛКШ	Локальный коммуникационный шлюз
ДМЗ	Демилитаризованная зона
УКШ	Удаленный коммуникационный шлюз
WAN	Wide Area Network

Вероятность риска

Вероятность что компоненты и зоны систем / подсистем могут стать целью кибер атаки

	Компоненты в поставке системы	Уровень вероятности
IT	Windows клиент	5
	ЧМИ клиент	5
	Cisco коммутатор / Роутер	5
	Ruggedcom коммутатор / Роутер	5
	Брандмауэр	5
	Windows Сервер	4
	ЧМИ Сервер	4
	GPS часы	4
	Сервер Active Directors	4
Распределенная система управления	Simatic контроллеры	3
	Plus Control	3
	Siprotec РЗА	3
	Другие устройства РСУ	3
	Другая РСУ	2
	HVAC	2
	Охлаждение	2
	Автоматика зданий	2
	Пожарная система	2
Полевые устройства	Profibus DP	1
	Интеллектуальные датчики	1
	Интеллектуальные ИМ	1
	Интеллектуальные переключатели	1



Вероятность: 1 Самый низкий, 5 наивысший

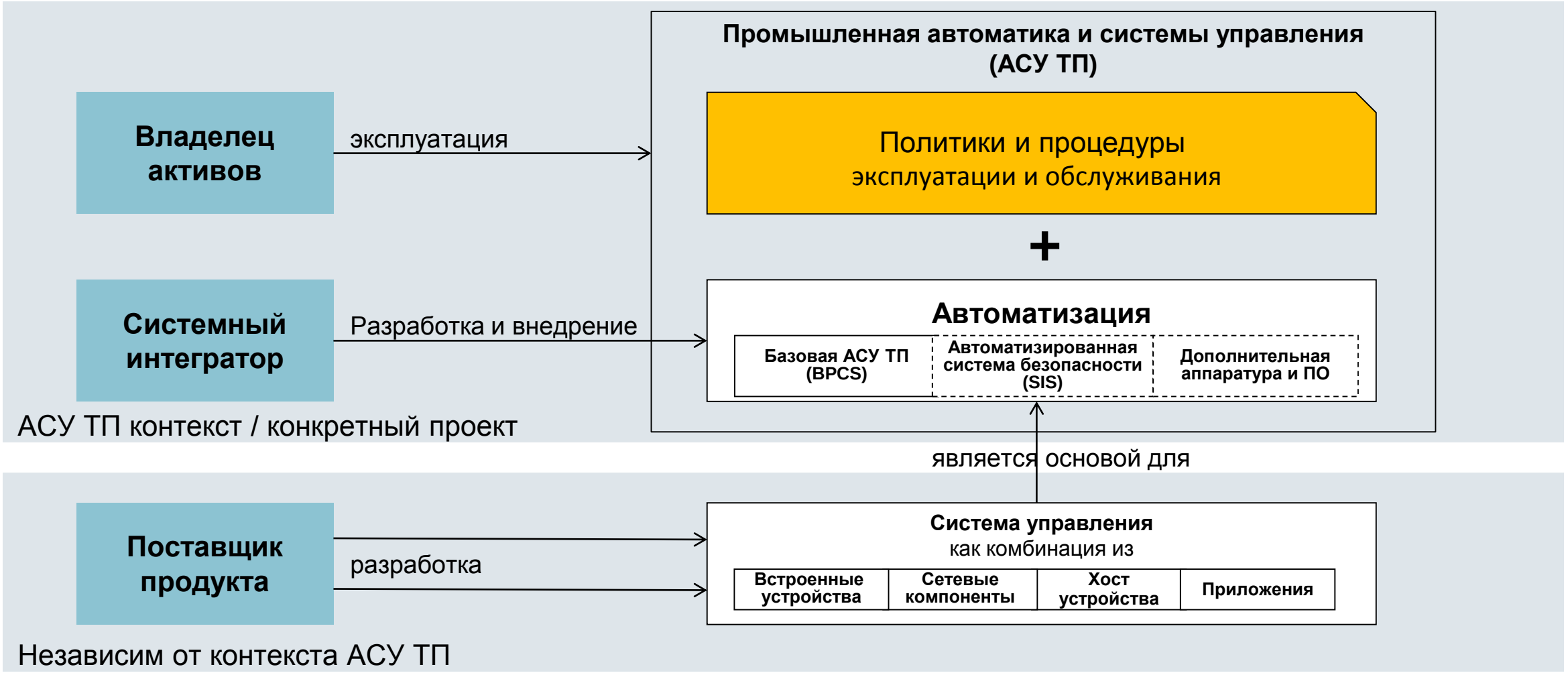
Промышленная безопасность

SIEMENS
Ingenuity for life

- Введение
- **Стандарт IEC 62443**
- Решение SIEMENS
- Примеры применений
- Преимуществаs работы с Siemens

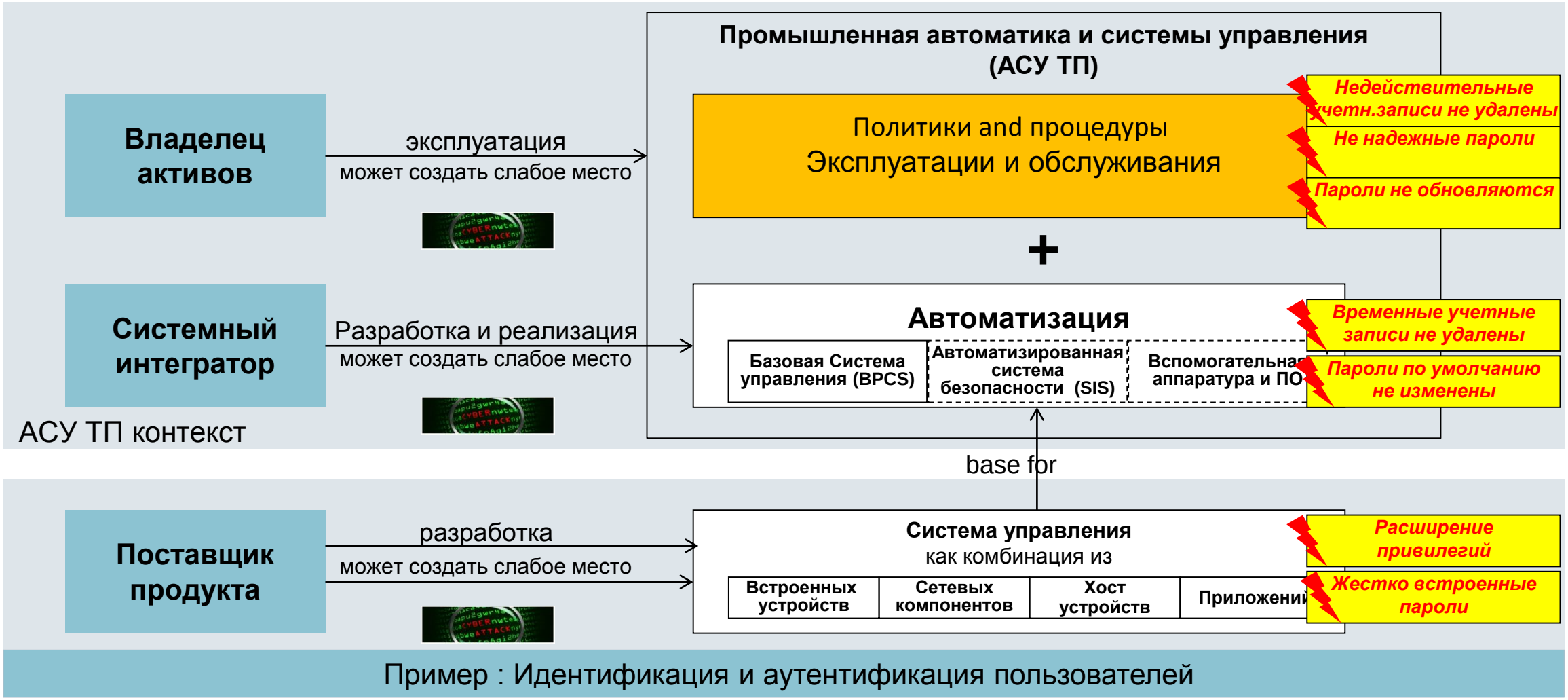
АСУ ТП, автоматизация, системы управления

SIEMENS
Ingenuity for life



Каждая заинтересованная сторона может создавать уязвимости

SIEMENS
Ingenuity for life



Структура IEC / ISA-62443, основные опубликованные документы

SIEMENS
Ingenuity for life

IEC / ISA-62443

Общее	Политики и процедуры	Система	Компоненты
1-1 Терминология, концепции и модели IS* 2009	2-1 Требования для системы управления безопасностью АСУ ТП Ed.2.0 Профиль ISO 27001 / 27002 DC* 10/12	3-1 Технологии безопасности для АСУ ТП TR* 2009	4-1 Требования к разработке продукта DC* 1Q15
1-2 Главный глоссарий терминов и сокращений	2-3 Управление исправлениями в АСУ ТП среде TR* 1Q15	3-2 Оценка риска безопасности и проектирование системы CDV* 2Q15	4-2 Технические требования к безопасности АСУ ТП продуктов DC* 1Q15
1-3 Показатели соответствия безопасности системы DTS* 1Q14 Rejected	2-4 Требования к поставщику решения АСУ ТП IS* 2Q15	3-3 Требования и уровни системы безопасности IS* 08/2013	
Определение показателей	Требования положенные в основу безопасности организации и процессов владельца и поставщиков	Требования достижения безопасности системы	Требования к безопасности продуктов системы

*DC: Draft for Comment
*CDV: Committee Draft for Vote
*IS: International Standard
*TR: Technical Report
*ID: Initial Draft

Функциональные Требования | Процессы / процедуры

Базовые документы IEC / ISA-62443 достаточно установившиеся для применения

SIEMENS
Ingenuity for life

*DC: Draft for Comment
*CDV: Committee Draft for Vote
*IS: International Standard
*TR: Technical Report
*ID: Initial Draft
*** По состоянию на 2015 год

Функциональные Требования | Процессы / процедуры

Различные части IEC / ISA-62443 перекликающиеся с эшелонированной защитой

SIEMENS
Ingenuity for life

Основные части
IEC 62443

Владелец активов

2-1
2-4

Политики и процедуры эксплуатации и обслуживания

Системный интегратор

2-4
3-2
3-3

политики и процедуры

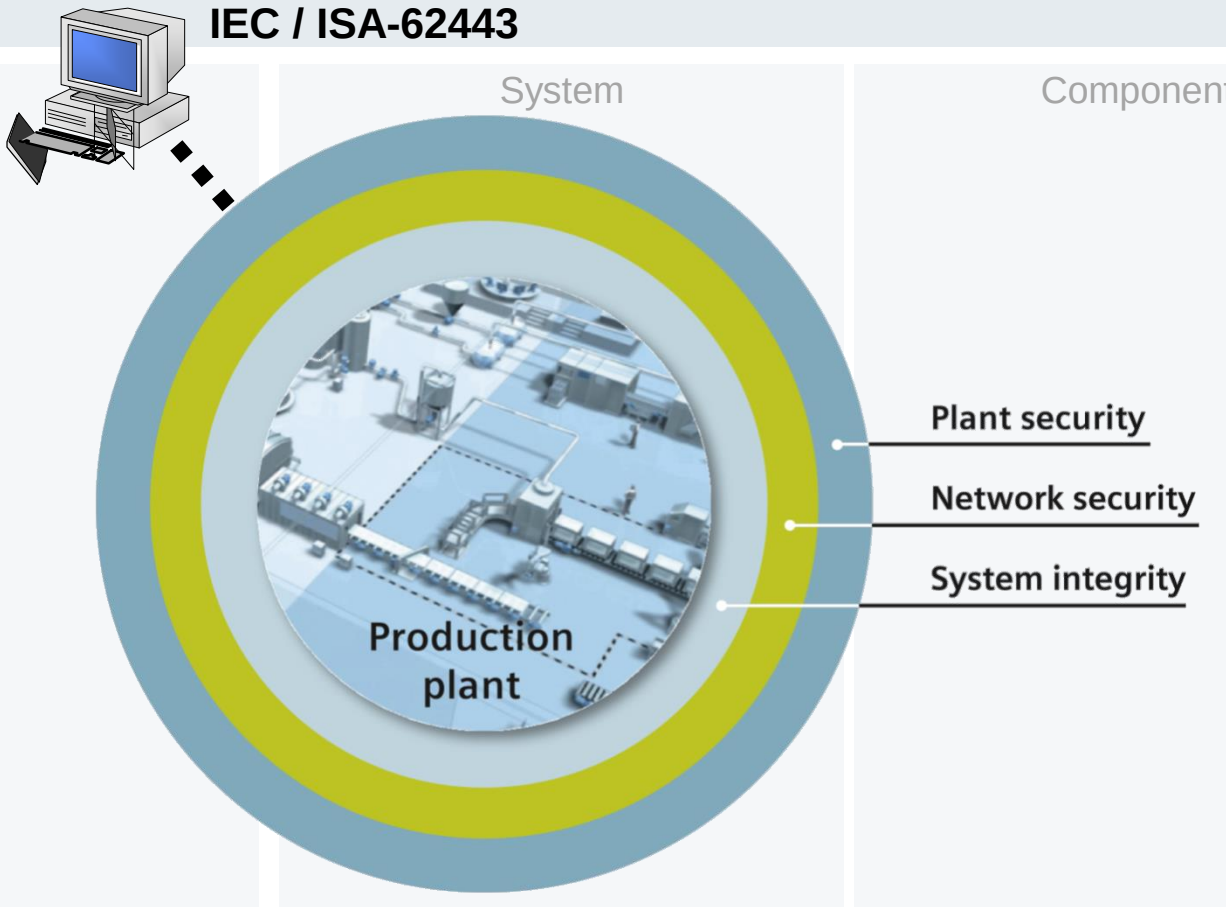
Возможности защиты Автоматизации

Поставщик продукта

3-3
4-2
4-1

Возможности защиты продукта

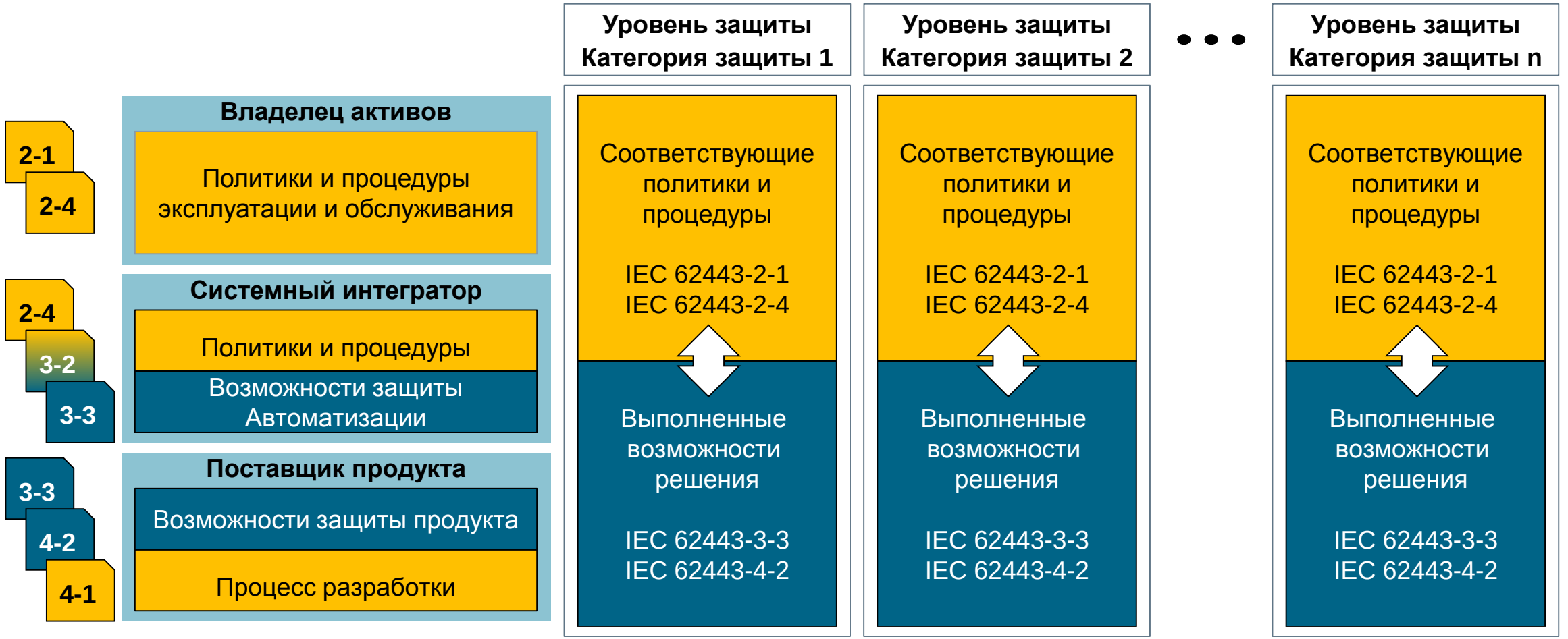
Процесс разработки



‘Эшелонированная защита’ включает все заинтересованные стороны: Владелец активов, Системный интегратор, Поставщик продукта

Требования процесса и функциональные требования взаимосвязаны

SIEMENS
Ingenuity for life



Требования взаимосвязаны.

SIEMENS
Ingenuity for life

Промышленная безопасность

SIEMENS
Ingenuity for life

- Введение
- Стандарт IEC 62443
- **Решение SIEMENS**
- Примеры применений
- Преимуществаs работы с Siemens

Product & Solution Security (PSS)
Web сайт по безопасности - Siemens Industrial Security

Industrial Security

Holistic protection of industrial plants

Industrial Security is based on several lines of defense and a comprehensive approach. To make this complicated topic easier for you to manage, Siemens offers a coordinated portfolio of solutions especially for the security of industrial facilities.

http://www.siemens.com/industrial-security

Концепция промышленной безопасности от Siemens
Глубоко эшелонированная оборона на базе IEC 62443

SIEMENS
Ingenuity for life

Глубоко эшелонированная защита

Угрозы безопасности требуют действовать

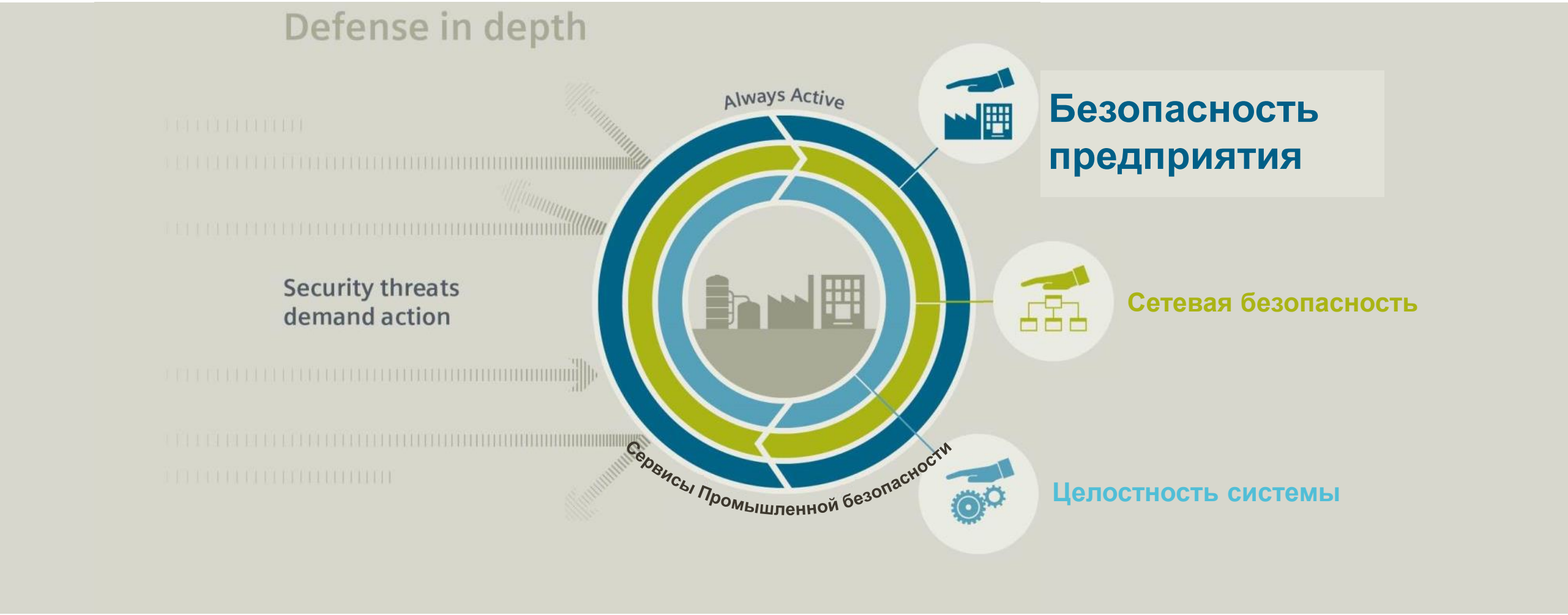
Безопасность предприятия
- Защита физического доступа
- Процессы и руководства
- Комплексный мониторинг безопасности

Безопасность сети
- Защита ячеек и периметра сетей
- Брандмауэри и VPN

Целостность системы
- Усиление системы
- Управление исправлениями
- Обнаружение атак
- Аутентификация и защита доступа

Промышленная безопасность
Решение Siemens для Безопасности предприятия

SIEMENS
Ingenuity for life

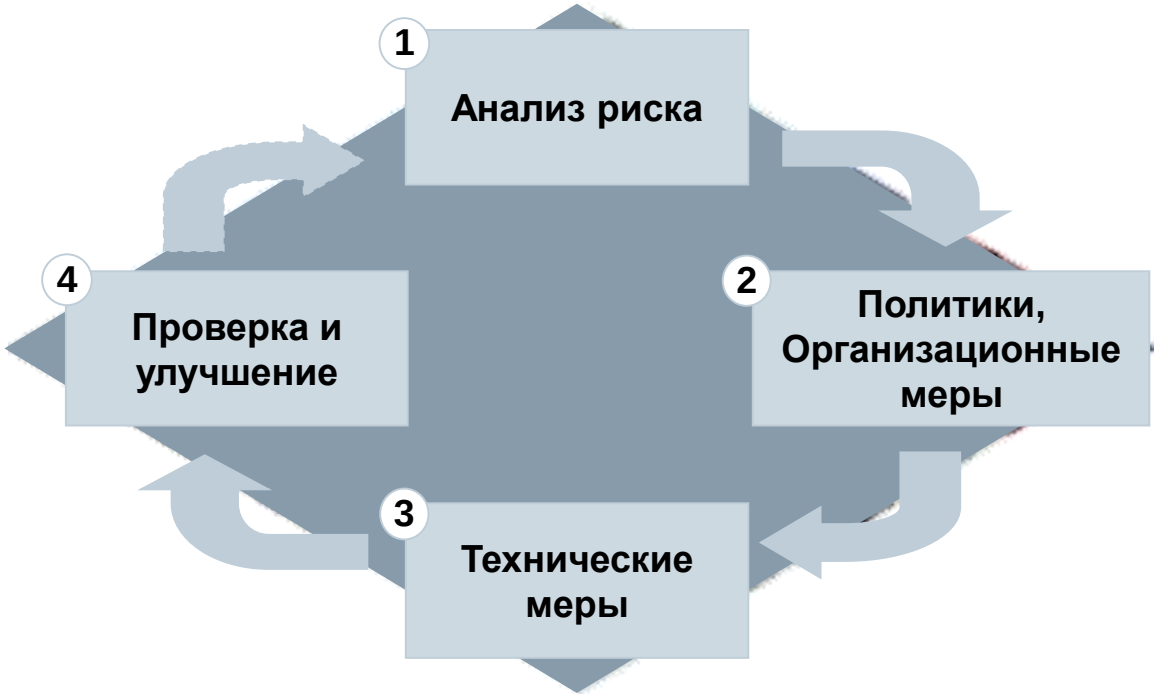


Промышленная безопасность
Управление безопасностью

SIEMENS
Ingenuity for life

Процесс управление безопасностью

- Анализ рисков с определением мер смягчения
- Разработка политик и координация организационных мер
- Координация технических мер
- Регулярный / по событию повторный анализ рисков



Управление безопасность имеет важное значение для хорошо продуманной концепции

Уровень защиты
Введение в методы и анкеты

SIEMENS
Ingenuity for life

Категории защиты должны покрывать все соответствующие критерии безопасности

Уровень защиты оценивается для каждой категории защиты

PL 1	Защита от случайного или не преднамеренного вмешательства
PL 2	Защита от преднамеренного вмешательства с использованием простых методов, малых ресурсов, общих навыков и с низкой мотивацией
PL 3	Защита от преднамеренного вмешательства с использованием сложных методов, умеренных ресурсов, навыками в АСУ ТП и с умеренной мотивацией
PL 4	Защита против преднамеренного вмешательства с использованием сложных методов с расширенными ресурсами, навыками в АСУ ТП и с высокой мотивацией

Подкатегории

- Идентификация и управление доступом
- Удаленный доступ
- Резервирование и восстановление
- Архитектура системы
- Целостность системы
- Конфиденциальность информации
- Управление инцидентами
- Ведение журнала и мониторинг
- Управление изменениями

Требования процесса и функциональные требования взаимосвязаны

SIEMENS
Ingenuity for life

		Уровень защиты Физический доступ	Уровень защиты Безопасность Организации	Уровень защиты Дизайн решения	Уровень защиты Эксплуатация	Уровень защиты Управление жизненным циклом
Владелец активов	**IEC 62443-2-1 ISO/IEC 27001**	Все **процессы для указания безопасного доступа** к автоматике	Все **процессы по построению безопасности организации**	Все **процессы для указания определенных требований и целей** к **дизайну автоматизации** или модификации решения	Все **процессы по безопасной эксплуатации** автоматики	Все **процессы по указанию требований безопасности для безопасного обслуживания** автоматики
Поставщик услуг	**IEC 62443-2-4**	Нет требований к Системному интегратору	Все **процессы поставщика услуг для построения безопасной организации**	Все **процессы Системного интегратора по разработке безопасной автоматики**	Нет требований к поставщику услуг	Все **процессы владельца активов или поставщика услуг для безопасного обслуживания** автоматики
Автоматизация	**IEC 62443-3-3**	**Меры по ограничению физического доступа к Автоматизации** Нет функциональных требований к автоматике	Нет функциональных требований к автоматике	Весь **функционал безопасности** необходимый **для поддержки разработки безопасного решения**	Весь **функционал безопасности** используемый **для поддержки безопасной эксплуатации решения**	Весь **функционал безопасности** используемый **для поддержки безопасное обслуживание** автоматики

Уровни зрелости и Уровни безопасности определенные через анкеты

SIEMENS
Ingenuity for life

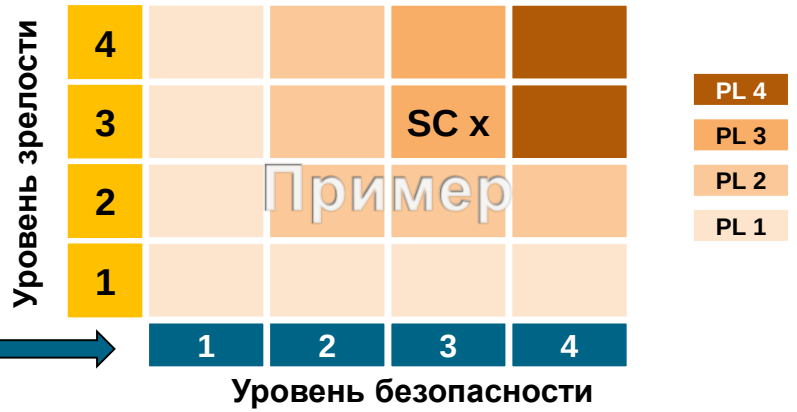
Уровень защиты оценен для каждой Категории защиты

Оценка **требований процесса** по Категории защиты
- IEC 62443-2-1
- IEC 62443-2-4

Control	Maturity Level 1	Maturity Level 2	Maturity Level 3	Maturity Level 4
A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.				
The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.				
All information security responsibilities shall be defined and allocated.				
Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.				
Appropriate contacts with relevant authorities shall be maintained.				
Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.				
Information security shall be addressed in project management, regardless of the type of the project.				
A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.				
A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.				
Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.				
The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.				
Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.				
All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.				
There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.				
Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.				
Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.				
Assets maintained in the inventory shall be owned.				
Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.				
All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.				
Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.				
An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.				
Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.				

Оценка **функциональных возможностей** автоматики согласно Категорий защиты
- IEC 62443-3-3
- IEC 62443-4-2

Control	Security Level 1	Security Level 2	Security Level 3	Security Level 4
The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.				
Unique identification and authentication				
The control system shall provide the capability to uniquely identify and authenticate all human users.				
Multifactor authentication for untrusted networks				
The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).				
Multifactor authentication for all networks				
The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.				
The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.				
Unique identification and authentication				
The control system shall provide the capability to uniquely identify and authenticate all software processes and devices.				
The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.				
Unified account management				
The control system shall provide the capability to support unified account management.				
The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.				
The control system shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon control system installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.				
Hardware security for software process identity credentials				
For software process and device users, the control system shall provide the capability to protect the relevant authenticators via hardware mechanisms.				
The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.				
Unique identification and authentication				
The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.				
For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.				
Password generation and lifetime restrictions for human users				
The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform with commonly accepted security industry practices.				
Password lifetime restrictions for all users				
The control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users.				
Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.				
The control system shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device).				
The control system shall provide the capability to obscure feedback of authentication information during the authentication process.				
The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.				
The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.				
The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.				

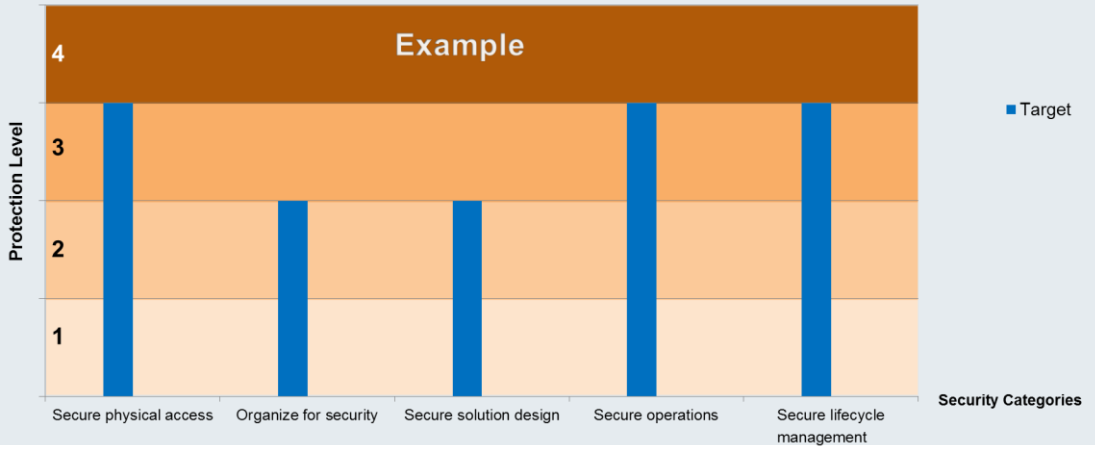


Уровни защиты: Методология

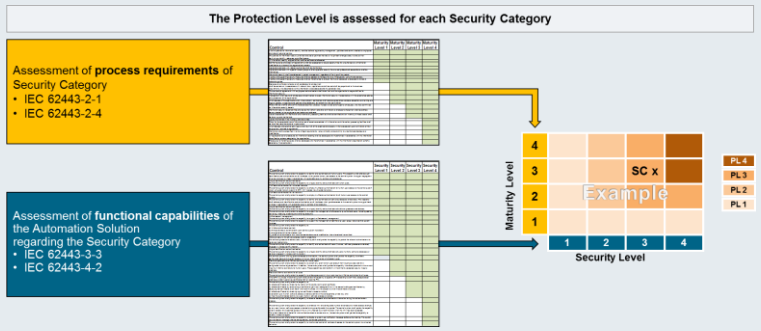
SIEMENS
Ingenuity for life

① Оценка риска для каждой Категории защиты

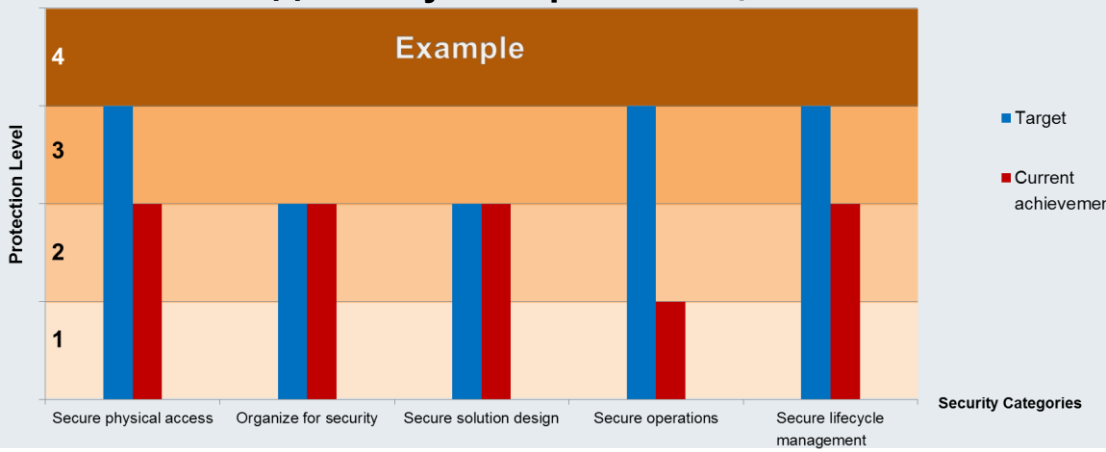
Целевые Уровни защиты



② Оценка Уровня защиты каждой Категории защиты

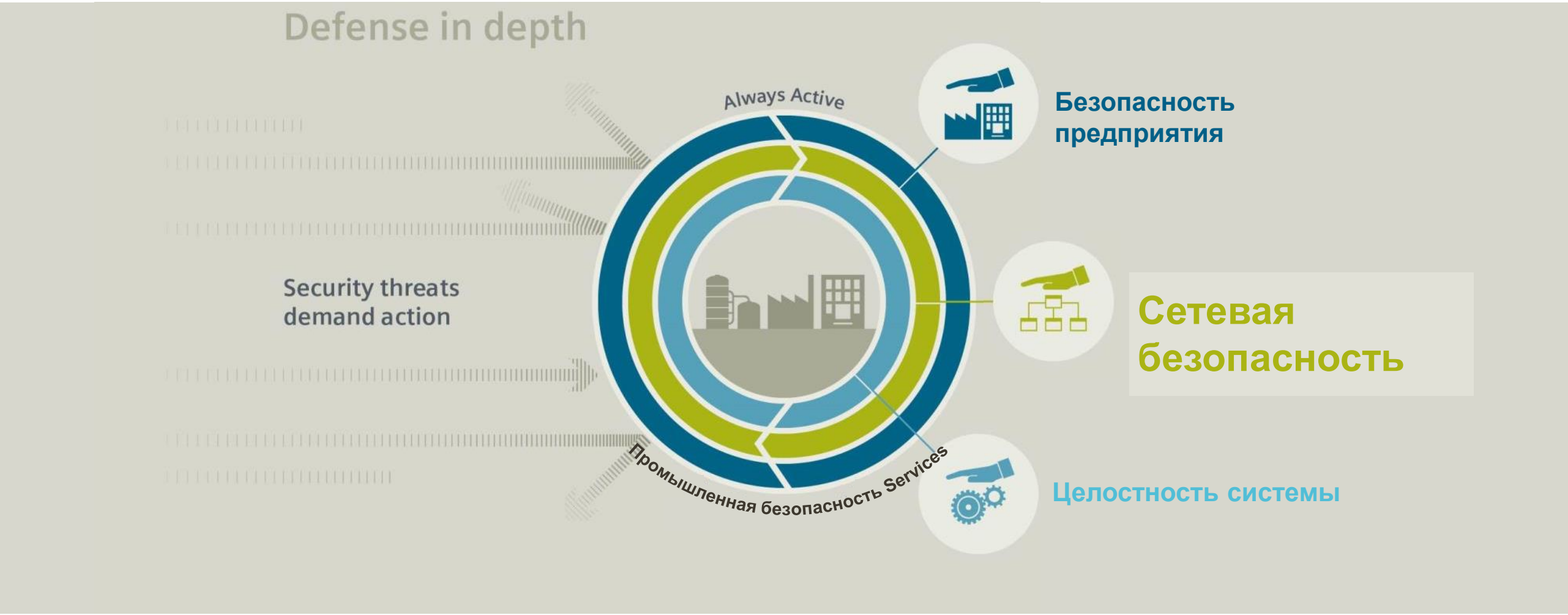


Достигнутые Уровни защит



Промышленная безопасность
Решение Siemens для Сетевой безопасности

SIEMENS
Ingenuity for life

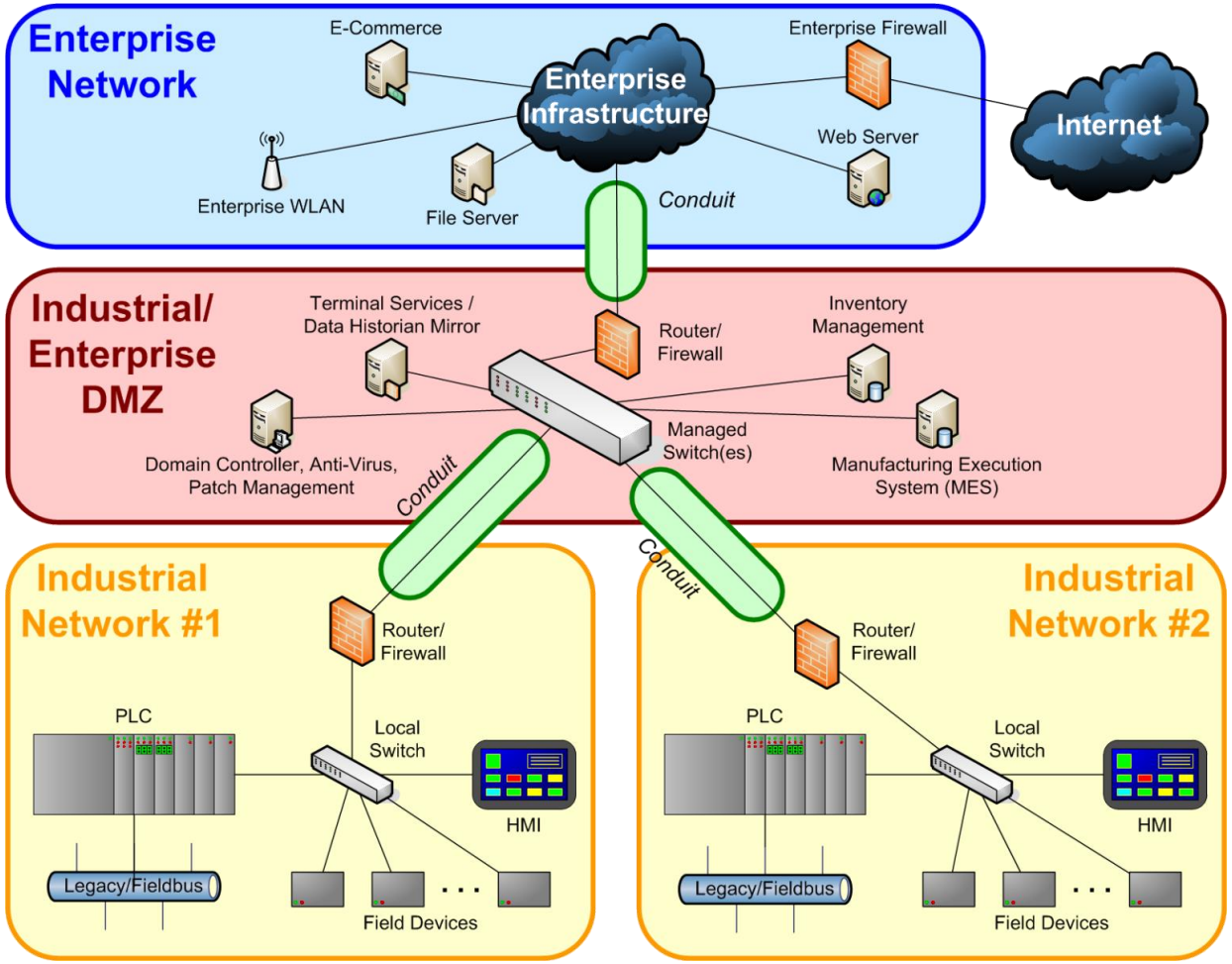


Концепция разделение сети на ячейки безопасности (Зоны)

SIEMENS
Ingenuity for life

Зоны безопасности

- Зона способна работать автономно некоторое время
- Все участники зоны являются доверенными
- Доступ к зоне только через хорошо продуманные точки доступа и
- Ведется журнал сетевой трафика и участников
- Все участники подключены напрямую
- Участники с высокой нагрузкой на сеть интегрированы прямо зону (для предотвращения образования узких мест)



http://isa99.isa.org/Public/Information/ISA99-ISA-62443-Overview.pptx

Промышленная безопасность
Обзор: Сетевая безопасность

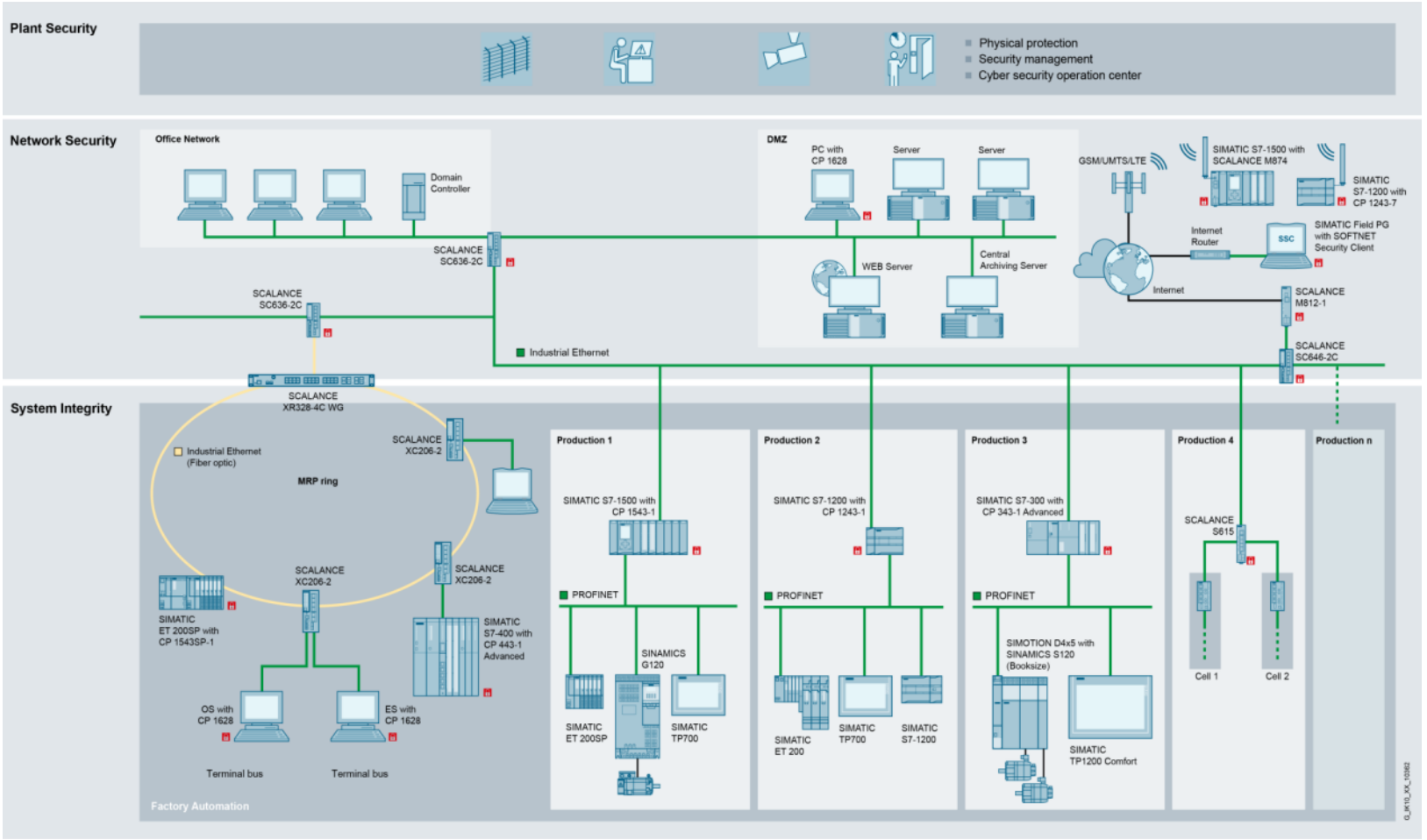
SIEMENS
Ingenuity for life

Меры адаптированные для производства:

Сетевой контроль доступа
- Безопасный интерфейс к IT сетям
- Архитектуры с ДМЗ
- Безопасный удаленный доступ
- Безопасный доступ к локальной сети (безопасность портов) через аутентификацию пользов. и устройств

Резервирование
- Защита резервированных сетевых топологий

Защита ячейки
- Смягчение рисков путем сегментации сети
- Расширение концепции Защиты ячейки:
  - Защищенные коммуникационные процессоры
  - Гибкая конфигурация VLAN



Продукты с функциями брандмауэра или VPN

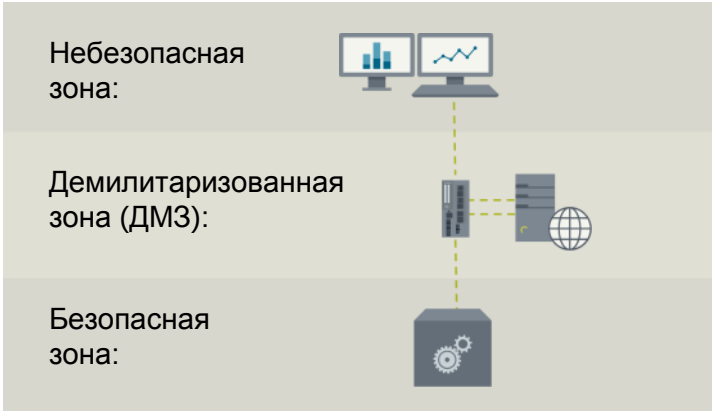
Промышленная безопасность
Сетевая безопасность use cases

SIEMENS
Ingenuity for life

Демилитаризованная зона (ДМЗ)

Больше защита за счет обмена данными через ДМЗ и избегания прямого доступа к сети автоматики.

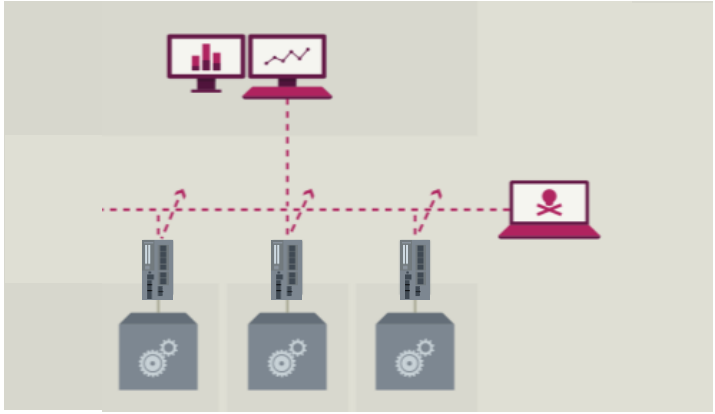
➔ Брандмауэр контролирует все данные между разными сетями и ДМЗ.



Защита ячейки

Устройства без собственной сетевой безопасности могут быть защищены с помощью ячейки безопасности.

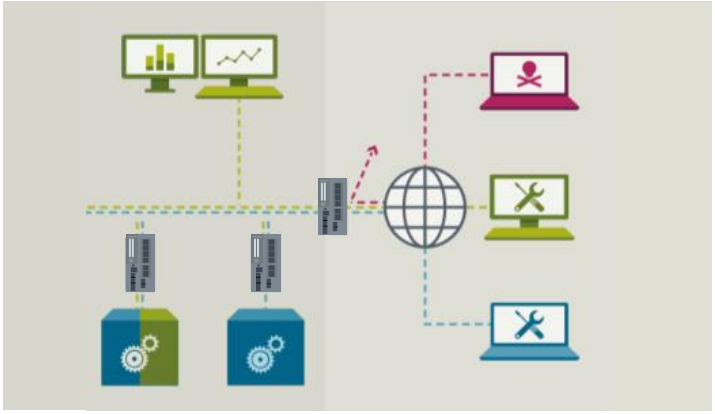
➔ Доступ к ячейке автоматики защищен брандмауэром.



Удаленный доступ

Безопасный удаленный доступ через Internet или мобильную сеть для исключения шпионажа и саботажа.

➔ Шифрование данных и контроль доступа к выделенным конечным устройствам.



Промышленная безопасность

Техничка для промышленная безопасности – SCALANCE S

SIEMENS
Ingenuity for life

SC632-2C SC636-2C S615 SC642-2C SC646-2C

Промышленная безопасность
Защита промышленных сетей со SCALANCE SC-600

SIEMENS
Ingenuity for life

SCALANCE SC646-2C

Возможности / функции		Преимущества
Гибкая конфигурация зон безопасности: • 2 или 6 электрических порта (RJ45), 2 комбо-порта • Свободное назначение портов VLAN	▶	Создание **сегментации сети** включая **ДМЗ:** • Комбо-порты с SFP для ВО тополгий • Защита сетевых топологий
Функциональность защиты: • Брандмауэр с контролем состояния соединений • Virtual Private Network (VPN) • Network Address Translation (NAT)	▶	**Защита критических сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Пропускная способность: • 600 Мбит/с для брандмауэра и маршрутизации • 120 Мбит/с для IPsec-VPN[1)]	▶	Высокая пропускная способность для **высокой доступности** и безопасности данных в сети
Интегрированная разработка: • TIA portal и SINEMA Server • SINEMA Remote Connect	▶	**Централизованная конфигурация и мониторинг** аппаратуры промышленной безопасности

1) Only with SCALANCE SC64x-2C

Промышленная безопасность
Защита промышленных сетей со SCALANCE S615

SCALANCE S615

Возможности / функции		Преимущества
Гибкая конфигурация зон безопасности: • Свободное назначение портов VLAN	▶	Создание **сегментации сети** включая **ДМЗ:** • Защита ячеек сети
Функциональность защиты: • Брандмауэр с контролем состояния соединений • Virtual Private Network (VPN) • Network Address Translation (NAT)	▶	**Защита критических сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Пропускная способность: • 100 Мбит/с для брандмауэра и маршрутизации • 35 Мбит/с для IPsec-VPN	▶	Спрос ориентированная пропускная способность для **производственных машин** и безопасности данных в сетях
Интегрированная разработка: • TIA portal и SINEMA Server • SINEMA Remote Connect	▶	**Централизованная конфигурация и мониторинг** аппаратуры промышленной безопасности

Промышленная безопасность

Промышленные роутеры: Мобильный доступ со SCALANCE M874

M874-3 M874-2

Возможности / функции	Преимущества
Безопасный **подключение через мобильные сети:** • 2G / EDGE • 3G / HSPA+	Безопасное подключение сетей на базе Ethernet к **мобильным сетям 2ro и 3ro поколения:** • Скорость до 14.4 Мбит/с
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • VPN клиент для подключения к SINEMA Remote Connect • Network Address Translation (NAT)	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Полная **интеграция SINEMA Remote Connect**	Удобное **централизованное администрирование и авто конфигурирование** удаленного доступа

Промышленная безопасность

Промышленные роутеры: Мобильный доступ со SCALANCE M876

SIEMENS
Ingenuity for life

M876-3 M876-4

Возможности / функции		Преимущества
Безопасное **подключение через мобильные сети:** • 3G / HSPA+ • 4G / LTE	▶	Безопасный connection of сети на базе Ethernet to **мобильные сети 3ro и 4ro поколения:** • Скорость до 100 Мбит/с
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • VPN клиент для подключения к SINEMA Remote Connect • Network Address Translation (NAT)	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Полная **интеграция в SINEMA Remote Connect**	▶	Удобное **централизованное администрирование и авто конфигурирование** удаленного доступа
Реализация **гибкой концепции зон безопасности**	▶	Интегрирован **4-портовый коммутатор** для простого подключения множества ячеек сети

Промышленная безопасность

Промышленные роутеры: широкополосный доступ with SCALANCE M812 und M816

M812-1 M816-1

Возможности / функции		Преимущества
Безопасный **проводное подключение** to the telephone or **DSL network:** • ADSL2+	▶	Безопасный **широкополосный доступ** для промышленных приложений: • Скорость до 25 Мбит/с
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • VPN клиент для подключения к SINEMA Remote Connect • Network Address Translation (NAT)	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Полная **интеграция в SINEMA Remote Connect**	▶	Удобное **централизованное администрирование и авто конфигурирование** удаленного доступа
Реализация **гибкой концепции зон безопасности**	▶	Встроенный **4-портовый коммутатор** (M816-1) для простого подключения множества ячеек сети

Промышленная безопасность

Промышленные роутеры: широкополосный доступ SCALANCE M826

SIEMENS
Ingenuity for life

M826-2

Возможности / функции		Преимущества
Безопасное **проводное подключение** удаленных устройств автоматики: • SHDSL	▶	Безопасный **2-проводный или 4-проводныйEthernet подключение** для дистанций до 10 км : • Скорость до 15.3 Мбит/с
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • VPN клиент для подключения к SINEMA Remote Connect • Network Address Translation (NAT)	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Полная **интеграция в SINEMA Remote Connect**	▶	Удобное **централизованное администрирование и авто конфигурирование** удаленного доступа
Реализация **гибкой концепции зон безопасности**	▶	Встроенный **4-портовый коммутатор** для простого подключения множества ячеек сети

Промышленная безопасность
коммуникационный процессоps: Безопасный Ethernet с CP 1243-1

SIEMENS
Ingenuity for life

CP 1243-1

Возможности / функции		Преимущества
Безопасное **Ethernet подключение SIMATIC S7-1200**	▶	**Защита сетей** и **сегментация** без дополнительных компонентов безопасности и безопасное подключение к **Telecontrol control center** с TeleControl Server Basic
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • Синхронизация времени (NTP secure) • Безопасный доступ к web серверу(HTTPS) • Передача информации сетевой диагностики с SNMP V3	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Полная **интеграция в SINEMA Remote Connect**	▶	Удобное **централизованное администрирование и авто конфигурирование** удаленного доступа
Встроенный инжиниринг : • STEP 7 в TIA Portal	▶	**Централизованное конфигурирование** коммуникационного процессора

Промышленная безопасность

коммуникационный процессорs: Мобильный доступ со CP 1243-7 LTE

SIEMENS
Ingenuity for life

CP 1243-7 LTE

Возможности / функции		Преимущества
Безопасный **мобильный радио доступ SIMATIC S7-1200:** • 4G / LTE	▶	**Защита сетей** и **сегментация** без дополнительных компонентов безопасности и безопасное подключение к **Telecontrol control center** с TeleControl Server Basic
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • Синхронизация времени (NTP secure) • Безопасный доступ к web серверу(HTTPS) • Передача информации сетевой диагностики с SNMP V3	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Полная **интеграция в SINEMA Remote Connect**	▶	Удобное **централизованное администрирование и авто конфигурирование** удаленного доступа
Встроенный инжиниринг : • STEP 7 в TIA Portal	▶	**Централизованное конфигурирование** коммуникационного процессора

Промышленная безопасность

коммуникационный процессоps: Безопасный to Ethernet with CP 1543-1

SIEMENS Ingenuity for life

CP 1543-1

Возможности / функции		Преимущества
Безопасное подключение **SIMATIC S7-1500** к **Industrial Ethernet**	▶	**Защита сетей** и **сегментация** без дополнительной аппаратуры защиты
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • Синхронизация времени (NTP secure) • Безопасный доступ к web серверу(HTTPS) • Secure file transfers (FTPs) • Передача информации сетевой диагностики с SNMP V3	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Встроенный инжиниринг : • STEP 7 в TIA Portal	▶	**Централизованное конфигурирование** коммуникационного процессора

Промышленная безопасность

коммуникационный процессорs: CP 1543SP-1 for SIMATIC ET 200SP

SIEMENS
Ingenuity for life

CP 1543SP-1

Возможности / функции		Преимущества
Безопасный connection of **SIMATIC ET 200SP** to **Industrial Ethernet**	▶	**Защита сетей** and **сегментация** без дополнительной аппаратуры защиты
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • Синхронизация времени (NTP secure) • Передача информации сетевой диагностики с SNMP V3 • Безопасная аутентификация коммуникационного партнера по сертификату	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Полная **интеграция в SINEMA Remote Connect**	▶	Удобное **централизованное администрирование и авто конфигурирование** удаленного доступа
Встроенный инжиниринг: • STEP 7 в TIA Portal	▶	**Централизованное конфигурирование** коммуникационного процессора

Промышленная безопасность
коммуникационный процессоры: CP 343-1 / CP 443-1 Advanced

SIEMENS
Ingenuity for life

CP 343-1 Advanced

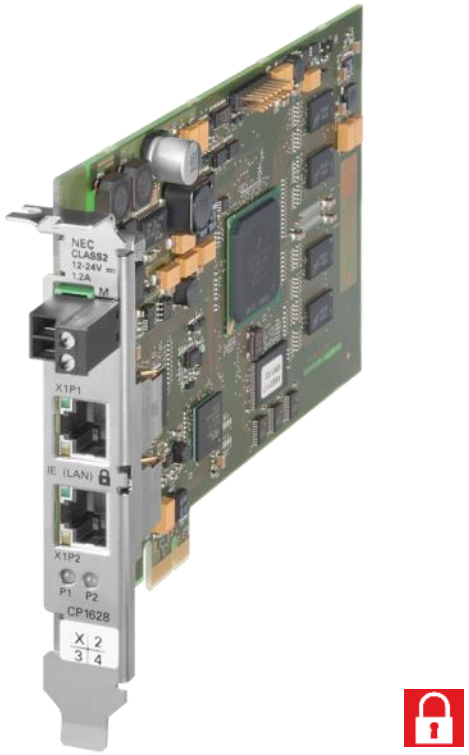
CP 443-1 Advanced

Возможности / функции	Преимущества
Безопасное подключение **SIMATIC S7-400 и S7-300** к **Industrial Ethernet сетям**	▶ **Защита сетей** and **сегментация** без дополнительной аппаратуры защиты
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • Синхронизация времени (NTP secure) • Безопасный доступ к web серверу(HTTPS) • Безопасная передача файлов (FTPs) • Передача информации сетевой диагностики с SNMP V3	▶ **Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Встроенный инжиниринг : • STEP 7 и TIA Portal	▶ **Централизованное конфигурирование** коммуникационного процессора

Промышленная безопасность

коммуникационный процессоры: Безопасное подключение ПК с CP 1628

SIEMENS Ingenuity for life

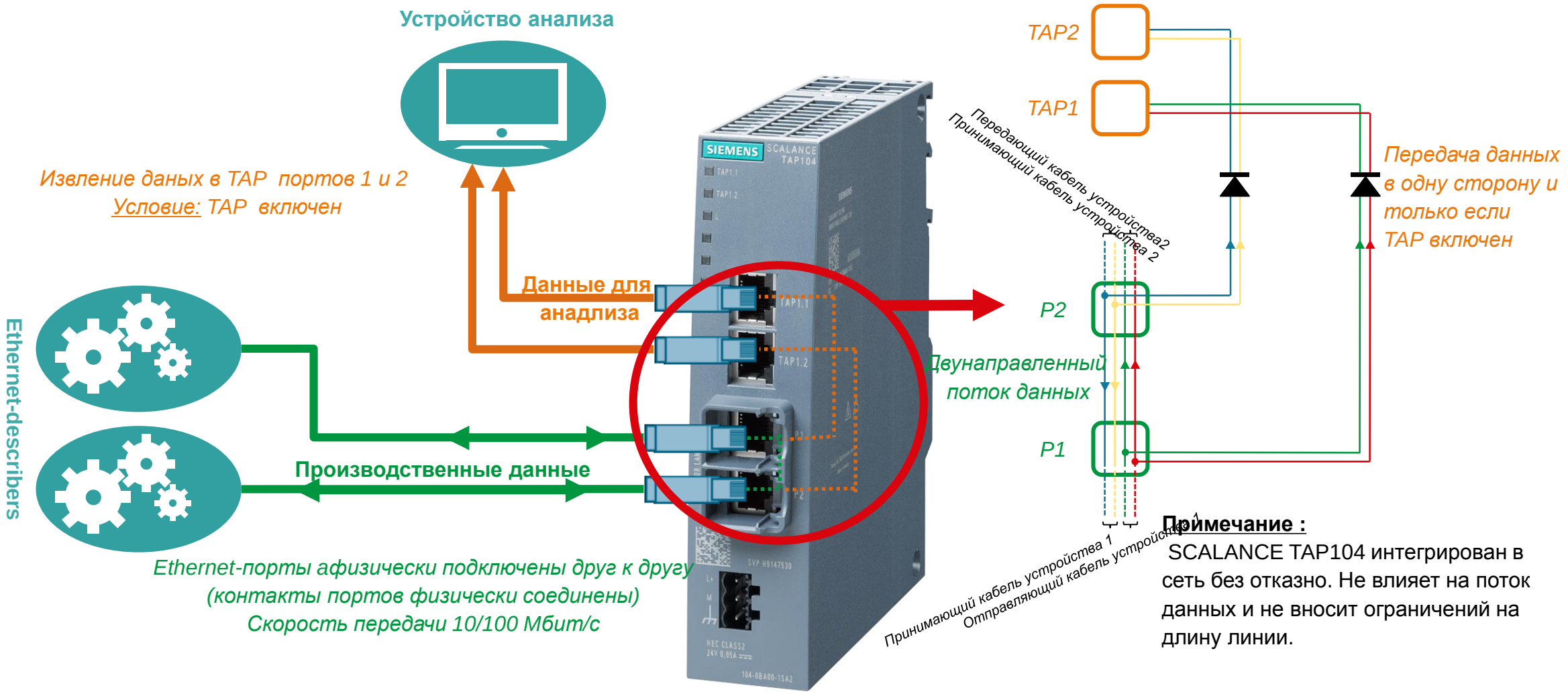


CP 1628

Возможности / функции		Преимущества
Безопасное подключение **PG** или **ПК** к **Industrial Ethernet сетям**	▶	**Безопасная коммуникация** между **PG / ПК** и подключенными **компонентами автоматики**
Функциональность защиты: • сетевой экран с контролем состояния соединений • Virtual Private Network (VPN) • Передача информации сетевой диагностики с SNMP V3	▶	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Встроенный инжиниринг : • STEP 7 в TIA Portal	▶	**Централизованное конфигурирование** коммуникационного процессора

SCALANCE TAP104
Принцип работы

SIEMENS
Ingenuity for life



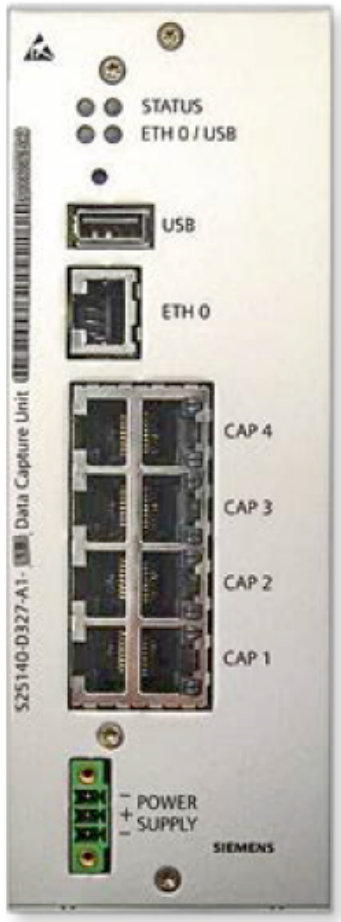
Примечание :

SCALANCE TAP104 интегрирован в сеть без отказно. Не влияет на поток данных и не вносит ограничений на длину линии.

DCU – Data capture unit
Модуль захвата данных

SIEMENS
Ingenuity for life

Возможности и функикции



Придерживается принципа “свобода от вмешательства”: нет прямой связи (гальваническая изоляция); пассивный tap через прямые кабельные подключения; нет подключений передаваемых в обратную сторону. Мониторинг независим от используемого протокола

Поддержка до 4-х 10 или 100 Мбит/с Ethernet линков в полнодуплексном режиме (вывод на Гигабитный Ethernet порт) без прерывания сетевых коммуникаций даже если DCU обесточен или отказал. Фильтрация захваченных данных по протоколам, исходному или конечному IP, порту, модержимому данных. Конфигурирование через web-интерфейс или загрузкой xml файла конфигурации. Поддердивает режимы сетевого tap и одностороннего шлюза с применением приложений шлюза. Разработан для работы в жестких уловиях окружающей среды (промышленное исполнение на рейку). Соответствует требованиям SL3 согласно IEC 62443-4-2

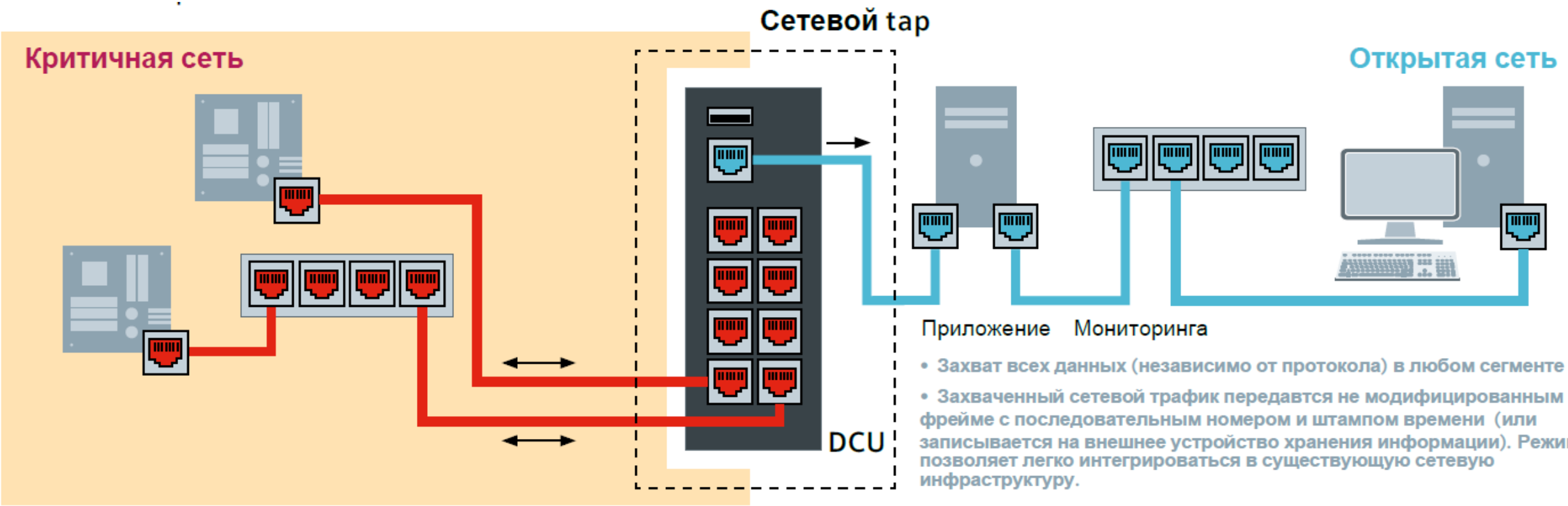
Размеры: 167 x 60.6 x 110.5 мм (В x Ш x Г)

Температурный диапазон: –40 до +85 °C

Номинальное питание : =24 В

DCU – Data capture unit
Модуль захвата данных – режим Tap

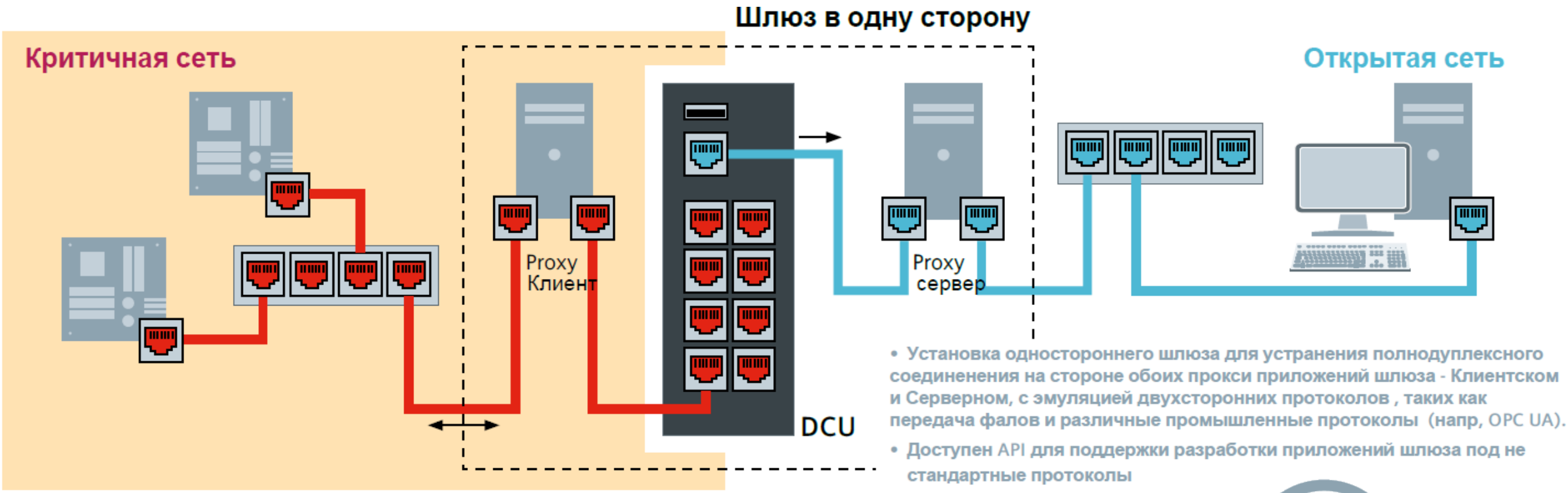
SIEMENS
Ingenuity for life



- Захват всех данных (независимо от протокола) в любом сегменте сети.
- Захваченный сетевой трафик передастся не модифицированным в фрейме с последовательным номером и штампом времени (или записывается на внешнее устройство хранения информации). Режим Tap позволяет легко интегрироваться в существующую сетевую инфраструктуру.

DCU – Data capture unit
Модуль захвата данных – режим Одностороннего шлюза

SIEMENS
Ingenuity for life



- Установка одностороннего шлюза для устранения полнодуплексного соединенения на стороне обоих прокси приложений шлюза - Клиентском и Серверном, с эмуляцией двухсторонних протоколов , таких как передача фалов и различные промышленные протоколы (напр, OPC UA).
- Доступен API для поддержки разработки приложений шлюза под не стандартные протоколы

Промышленная безопасность
Удаленные сети: SOFTNET Security Client

SIEMENS
Ingenuity for life

SOFTNET Security Client

Возможности / функции	Преимущества
Безопасный **доступ из** и **в** инженерные и сервисные ПК	▶ **Безопасные коммуникации** от и к инженерных и сервисных ПК без дополнительной аппаратуры
Функциональность защиты: • Virtual Private Network (VPN)	▶ **Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Встроенная концепция безопасности для технологий автоматики вместе с: • SIMATIC Security CP • Промышленные роутеры SCALANCE M • Промышленная безопасность со SCALANCE S	▶ **Связь** осуществляется исключительно **между аутентифицированными** и **авторизированными** устройствами

Промышленная безопасность

Управление удаленными метями: SINEMA Remote Connect

SIEMENS
Ingenuity for life

SINEMA Remote Connect

Возможности / функции	Преимущества
Безопасное управление туннельными соединениями между центром, сервисными специалистами и установленными системами	**Менеджмент** безопасного **удаленного доступа** к глобально распределенными машинам и системам
Функциональность защиты: • Virtual Private Network (VPN) • Регистрация PKI смарт-карт для менеджмента по Web и SINEMA RC клиента	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными
Встроенная концепция безопасности технологий автоматики совместно с **:** • SIMATIC Security CP • Промышленные роутеры SCALANCE M • Промышленная безопасность со SCALANCE S	**Коммуникация** только через **центральный сервер**. Сервисный работник и машина устанавливают соединение к SINEMA Remote Connect. Далее идентифицируются участники путем обмена сертификатами до установки сокдинения.

Промышленная безопасность
Считыватель карт: Контроль доступа с SIMATIC RF1060R

SIMATIC RF1060R

Возможности / функции	Преимущества
Контроль доступа к компонентам машины или участка	**Гибкие уровни авторизации,** напр. для доступа к машине каждого работника с помощью ID карты
Функциональность защиты: • Идентификация персонала • Отслеживание критических действий • Предотвращение ошибок оператора	**Защита критических компонентов** от: • Неавторизированного доступа к сети и устройствам • Шпионажа или манипуляции данными
Поддерживаемые стандарты: • ISO 14443A/B • ISO 15693	Использование ID карт сотрудников дает **индивидуальный контроль** прав доступа
Для промышленных применений: • IP65 (спереди) • -25 до +55 °C	Для **прямого** использования **на машинах** и системах в жестких условиях окружающей среды

https://support.industry.siemens.com/cs/document/109756169

Промышленная безопасность

Механическое закрытие неиспользуемых портов замком IE RJ45

SIEMENS
Ingenuity for life

IE RJ45 Port Lock

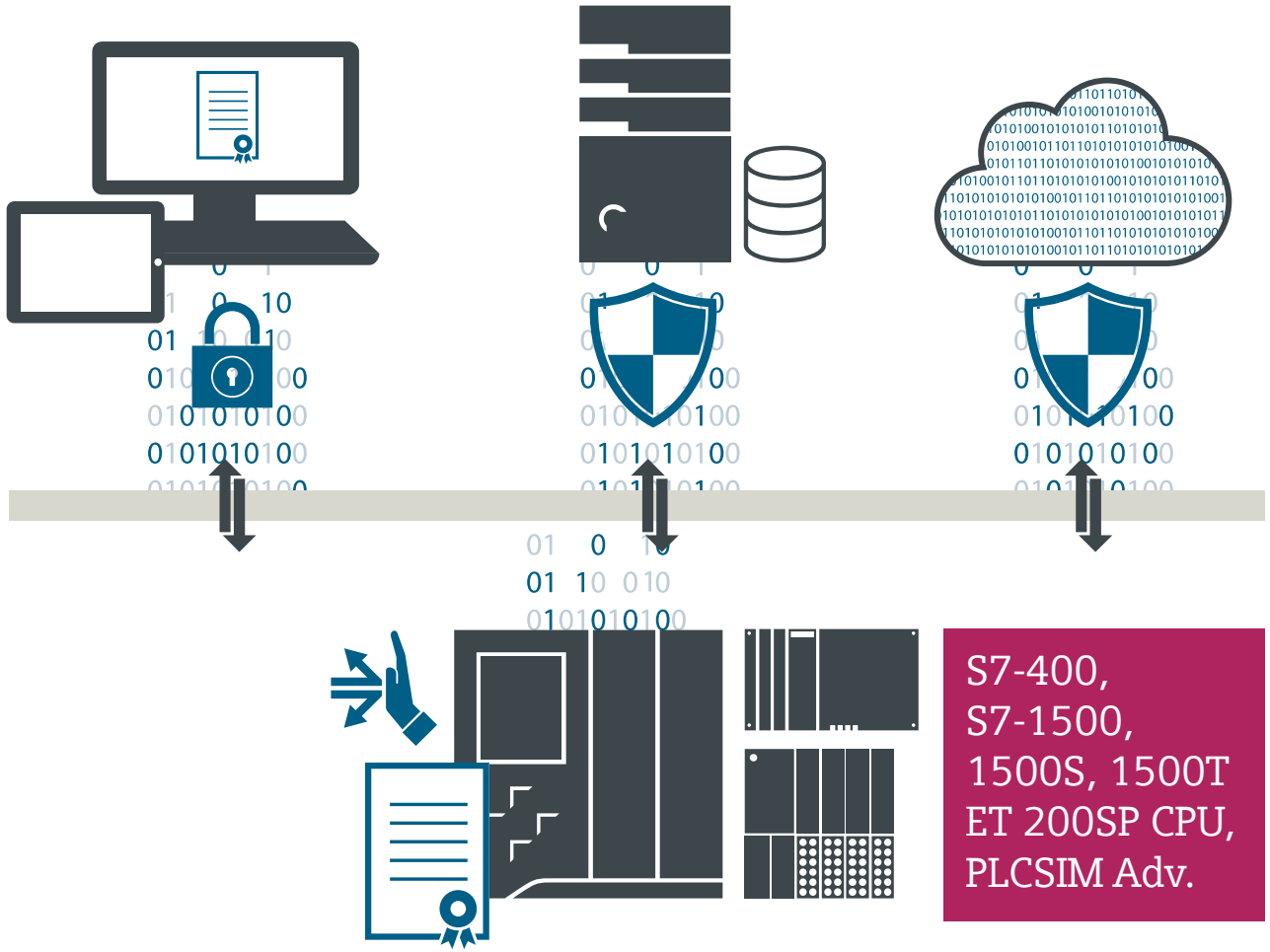
Возможности / функции	Преимущества
Механическое закрытие неиспользуемых интерфейсов RJ45 сетевого оборудования и устройств	**Secures physically** open, unused **RJ45 interfaces** to prevent Неавторизованного доступа Temporary **network disconnections** (plant shutdown for maintenance) can be implemented directly on site
Функциональность : • RJ45 порт может блокировать не сконфигурированные сетевые компоненты • Надежная, промышленная конструкция • Простая установка без инструмента благодаря совместимости с RJ45 • Удаление замка только после размыкания механически ключем	**Защита критичных сетей** против: • Неавторизованного доступа • Шпионажа или манипуляции данными

Промышленная безопасность
Решение Siemens для Целостности системы

SIEMENS
Ingenuity for life

OPC UA
Встроенные механизмы безопасности

SIEMENS
Ingenuity for life



Безопасность OPC UA

- Выбираемые политики безопасности в контроллере и клиенте
- Аутентификация устройства / приложения по сертификату
- Интегрированная защита и шифрованная связь
- Аутентификация пользователя и ограничение доступа к тегам ПЛК

Промышленная безопасность
Безопасность для ЧМИ

SIEMENS
Ingenuity for life

Возможности безопасности

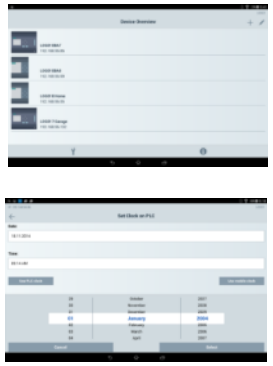
Защита доступа к панели
Назначения пароля для доступа к устройству

Управление пользователями
Защита против не авторизированного доступа с управлением на базе разрешений

Функции усиления системы
Повышенная безопасность с настраиваемыми параметрами жесткости системы, такими как блокировка переключения задач, аутентификация веб-сервера

Промышленная безопасность
SIMATIC Apps

SIEMENS
Ingenuity for life



LOGO! App

S7 App

Sm@rtClient App

Возможности безопасности

SIMATIC Apps предоставляют несколько возможностей защиты:

- **Защита коммуникаций** (для Sm@rtClient App: только для полной версии)
- **Защита данных профиля**
- **Пароль для запуска** (Для Sm@rtClient App: только для iOS)
- **Пароль необходим для подключения**

Промышленная безопасность
Защита IPC

SIEMENS
Ingenuity for life

Требования

Детектирование и предотвращение не авторизированного доступа и malware

Защита против:

- Манипуляций системой / данными
- Вредоносное или нежелательных программ

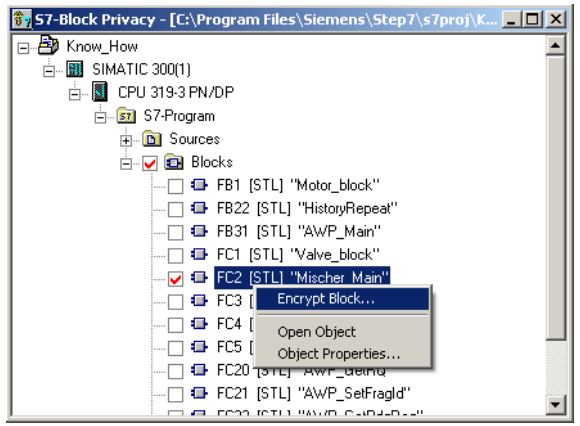
Решение

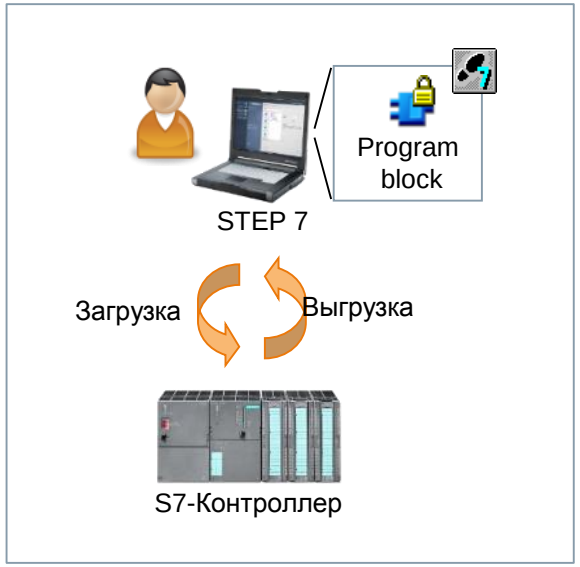
Наши IPC поддерживают разные функции безопасности:

- Защита Загрузки/Конфигурации для BIOS/UEFI
- Управление пользователями ОС (вкл. подключение к центральной Active Directory)
- Поддержка EWF (Enhanced Write Filter)
- Множество возможностей усиления системы → Руководства [Link]
  - Запрещение интерфейсов
  - Блокировка приложений
- Поддержка Антивирусов и решений Вайтлистингов

Промышленная безопасность
STEP 7 V5.5 - Приватность S7 Блоков

SIEMENS
Ingenuity for life





Требования

Защита Know-How и программы

Защита против:

- Шпионажа
- Неавторизированного доступа
- Манипуляция данными

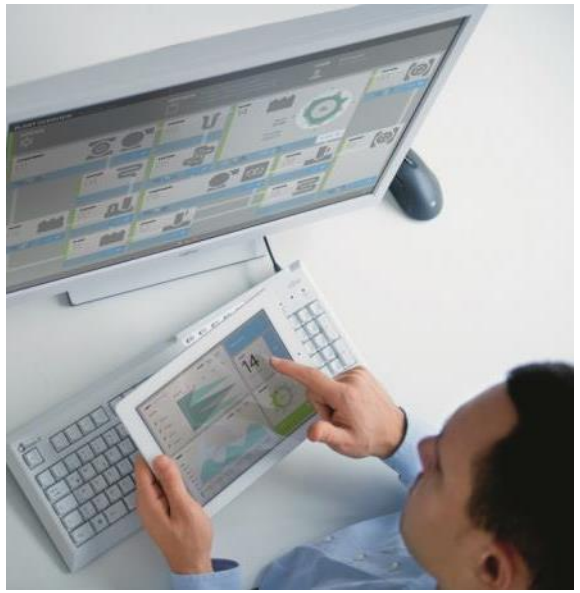
Решение

STEP 7 V5.5 дает следующие возможности защиты:

- **Увеличение защиты Know-how**
  - Защита кода программы паролем и приватность S7-блока
  - Защита блоков от чтения и изменений
  - Только авторизированные пользователи получают доступ к блокам.
- **Программная защита копирования**
  - Защита Know-how программ с защитой копироания
  - Сравнение с заданным серийным номером карты памяти или ЦПУ

Промышленная безопасность
WinCC V7

SIEMENS
Ingenuity for life



Требования

Безопасная SCADA среда

Защита против:

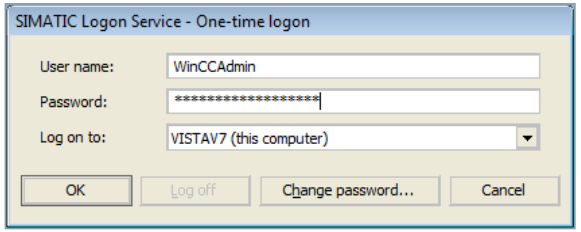
- Шпинажа
- Манипуляции данными
- Системных збоев

Решение

WinCC V7 предлагает широкий спектр средств обеспечения безопасности:

- **Безопасные коммуникации** по **терминальной шине** с **SSL шифрованием** и использование **статических портов** в **коммуникации** (брандмауэры)
- Системные тесты и итоговая документация с текущим **антивирусным сканером** и шаблонами
- **WinCC администрирование пользователей / SIMATIC Logon**
  Только прошедшие проверку пользователи получаю доступ к системе
- **WinCC Runtime**
  Нет или ограниченный доступ к ОС (рабочий стол)
- **WinCC Web Viewer**
  Доступ только к экранам оператора / нет доступа к Internet страницам для предотвращения загрузки malware и проч.
- **WinCC/WebUX**
  Доступ по Web через защищенное соединение (HTTPS)
- **WinCC/Audit, WinCC/Change Control**
  Регистрация действий пользователя, напре. для FDA решений
- **WinCC/Резервирование**
  Выше доступность серверов/подключений к процессу при сбое/ошибке

Промышленная безопасность
SIMATIC Logon



Требования

- Централизованный контроль пользователей по всем системам
- Соответствие требованиям FDA
- Конфигурирование в runtime (добавление / блокирование / удаление пользователей)
- Высокая безопасность на базе ОС MS Windows
- Поддержка концепции доменов и рабочих групп Windows

Решение

Управление безопасным доступом с SIMATIC Logon

Управление пользователями WinCC based в SIMATIC Logon :

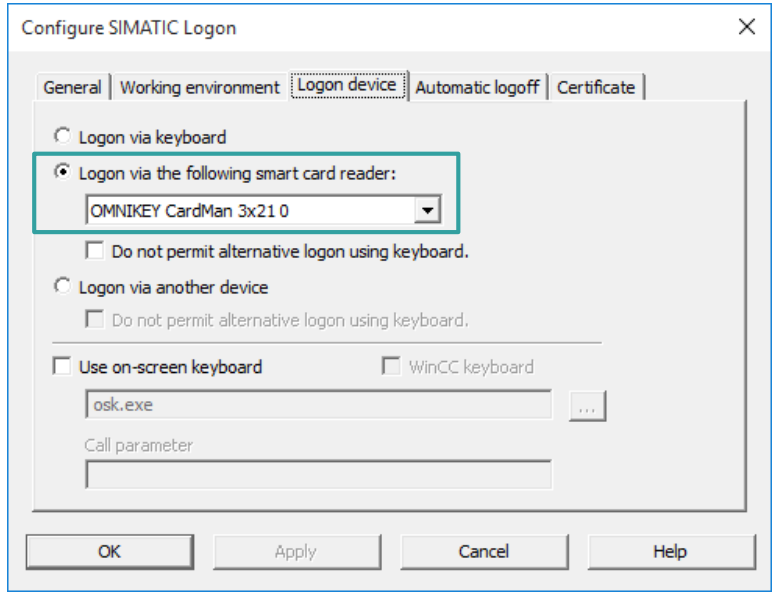
- Центральное администрирование (вкл. устаревание пароля, авто выход по времени, контроль неправильных вводов паролей, блокировка экрана)
- Конфигурация в runtime (добавление / блокирование / удаление пользовательских учетных записей)
- Все конфигурации WinCC поддерживаются включая web
- Поддержка домена и рабочих групп Windows
- Двух факторная авторизация

Управление пользователями и их аутентификацией защищает предприятие

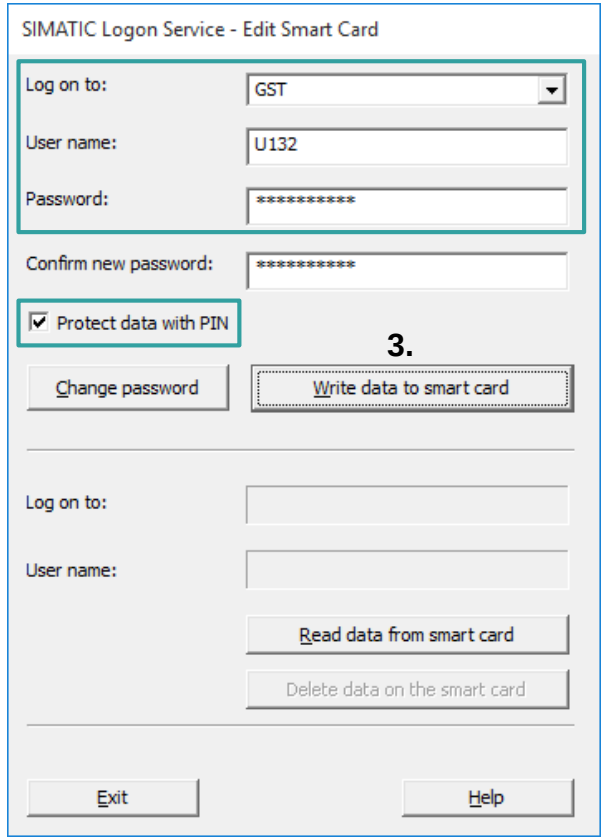
SIMATIC PCS 7 V9.0 – SIMATIC Logon V1.6
Двойная аутентификация (2FA) – Конфигурация

SIEMENS
Ingenuity for life

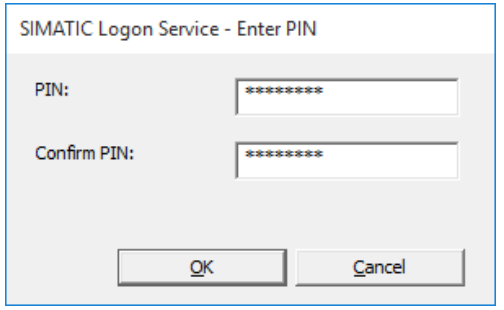
1) Выбор считывателя карт как устройства регистрации



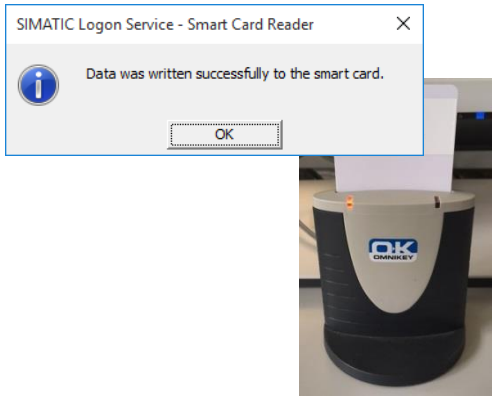
2) Запись учетных данных на смарт-карту



4.



5.

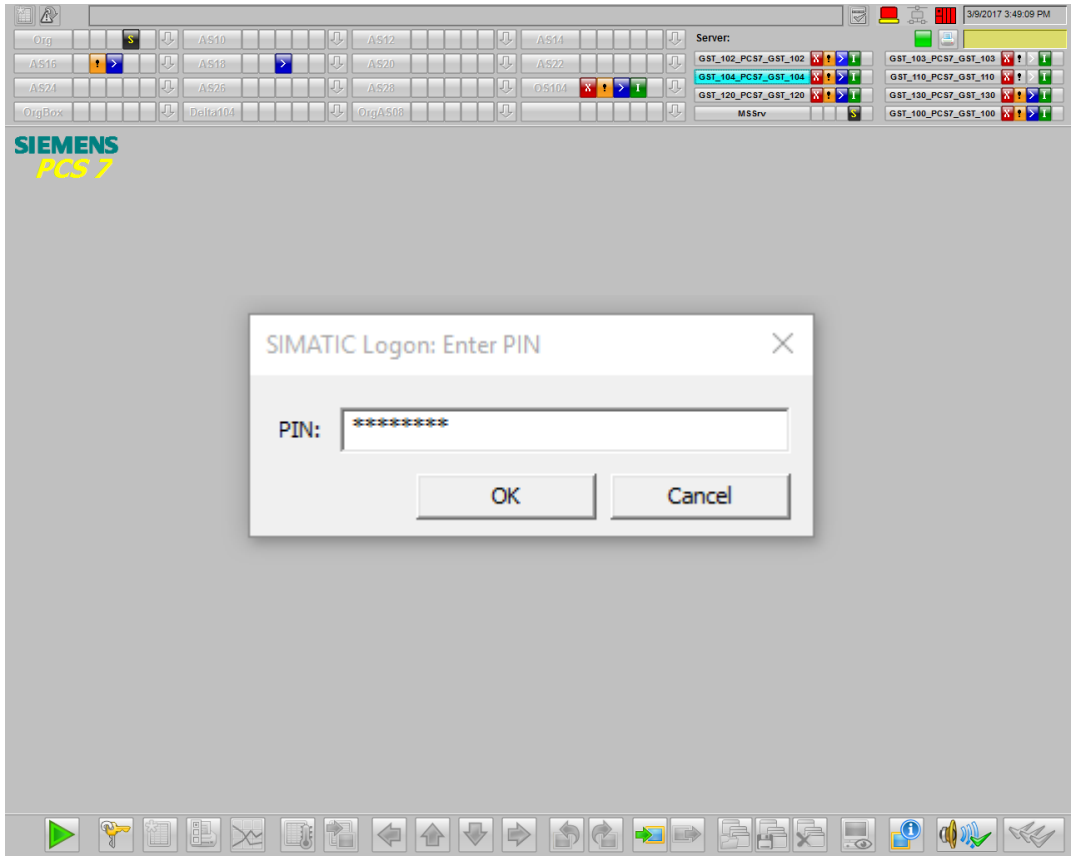


SIMATIC PCS 7 V9.0 – SIMATIC Logon V1.6 – Двух шаговая аутентификация (2FA) – Режим исполнения

SIEMENS
Ingenuity for life

1. Вставить смарт-карту в считыватель

2. Ввести PIN



3. После успешного ввода – Пользователь должен ввести учетные данные

Промышленная безопасность
Антивирусы и вайтлистинг

SIEMENS
Ingenuity for life

Требования

Определение и предупреждение Вирусов, червей и троянов

Защита против:

- Вредоносного или нежелательного ПО
- Манипуляций

Решение

Антивирус и вайтлистинг решения дает различные функции безопасности :

- Защита против вирусов, червей и троянов
- Прекращение неавторизированных приложений и malware

Промышленная безопасность
SIMOTION – Эффективное и безопасное производство

SIEMENS
Ingenuity for life

Требования

Защита интеллектуальной собственности OEM, совместимость с обновлениями и высокая доступность систем

Защита против:

- Шпионажа
- Манипуляции данными
- Неавторизированного доступа
- Воздействия на окружающую среду

Решение

SIMOTION C/D/P имеет несколько встроенных функций безопасности:

- Защита Know-how
- Защита манипуляции исходным кодом с on-/offline сравнением
- Администрирование пользователей и доступ на базе ролей с SIMATIC Logon
- Поддержка антивирусных сканеров*
- Совместимость с заплатками безопасности Windows *

Масштабируемая, модульная, высокопроизводительная система везде где необходимо управление движением. Не имеет значения необходимо реализовать централизованную или распределенную концепцию, либо решение на базе ПК, контроллера или привода

* в платформе SIMOTION на базе ПК-

Промышленная безопасность

SINUMERIK 840D sl – Безопасная инновационная платформа CNC

SIEMENS
Ingenuity for life

Требования

Защита интеллектуальной собственности, выявление вирусов, безопасный доступ и защита сетей для высокой доступности систем

Защита против:

- Шпионажа
- Неавторизированного доступа
- Внешних атак
- Манипуляций

Решение

SINUMERIK 840D sl имеет несколько функций безопасности:

- Защита Know-how для NCK/HMI Open Architecture и PLC-Программы
- Защита цикла CNC
- Аутентификация пользователей на базе ролей
- Поддержка сканера антивирусов*
- Совместимость с исправлениями безопасности Windows *
- Брандмауэр пакетов и проверка надежности интерфейсов

SINUMERIK 840D sl распределенный, масштабируемый, открытый и взаимно подключаемое предложение систем с широким набором функций. Идеально подходит для приложений с различными технологиями.

* для PCU50

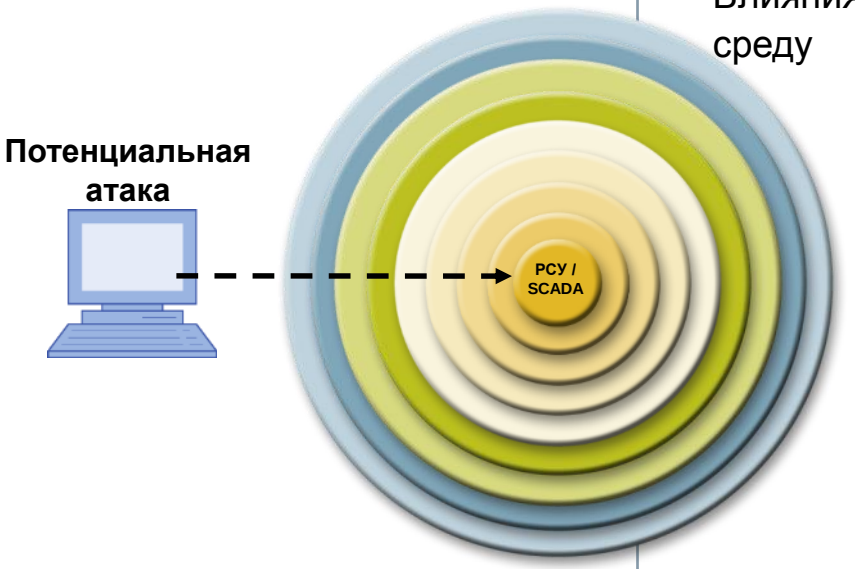
Промышленная безопасность
SIMATIC PCS 7 – Security you trust

SIEMENS
Ingenuity for life

Требования

Защита против:

- Потери управления
- Простоев
- Потери качества продукта
- Влияния нам окружающую среду



Решение

SIMATIC PCS 7 – Снижение риска благодаря стратегии глубоко эшелонированной обороне

- сегментация / безопасность ячеек
- Защита точек доступа
- Аутентификация пользователей
- Безопасная коммуникация
- Защита уязвимой информации
- Управление исправлениями
- Закалка системы
- Сканер вирусов
- Вайтлистинг
- Выявление аномалий

Функциональное руководство безопасности PCS7
PCS 7 Compendium Part F - Industrial Security (V9.0)

SIEMENS
Ingenuity for life

Содержание

- Стратегии безопасности
- Сетевая безопасность
- Усиление системы
- Администрирование пользователей и разрешения пользователей
- Управление исправлениями
- Защита от malware при помощи антивирусов
- Резервное хранение и восстановление данных
- Удаление систем и компонентов
- Удаленный доступ

https://support.industry.siemens.com/cs/document/109756871

Информационные ресурсы

Общая концепция системы безопасности для промышленности
https://www.industry.siemens.com/topics/global/en/industrial-security/Documents/Whitepaper_Security_2016_V10_EN.pdf

Рекомендации по настройке параметров безопасности для ПЛК:
https://support.industry.siemens.com/cs/ww/en/view/77431846

Рекомендации по настройке security для компьютеров SIMATIC IPC
https://support.industry.siemens.com/cs/ww/en/view/109475014

Рекомендации по настройке security для панелей оператора
https://support.industry.siemens.com/cs/ww/de/view/109481300

Конфигурация JumpHost Application с применением SINEMA RC:
https://support.industry.siemens.com/cs/ww/de/view/109746841

Настройка параметров безопасности из Step7 Pro:
https://support.industry.siemens.com/cs/document/109477192

Концепция системы безопасности в PCS7 и WinCC:
https://support.industry.siemens.com/cs/document/60119725

Основы безопасности промышленных сетей:
https://support.industry.siemens.com/cs/document/109747342

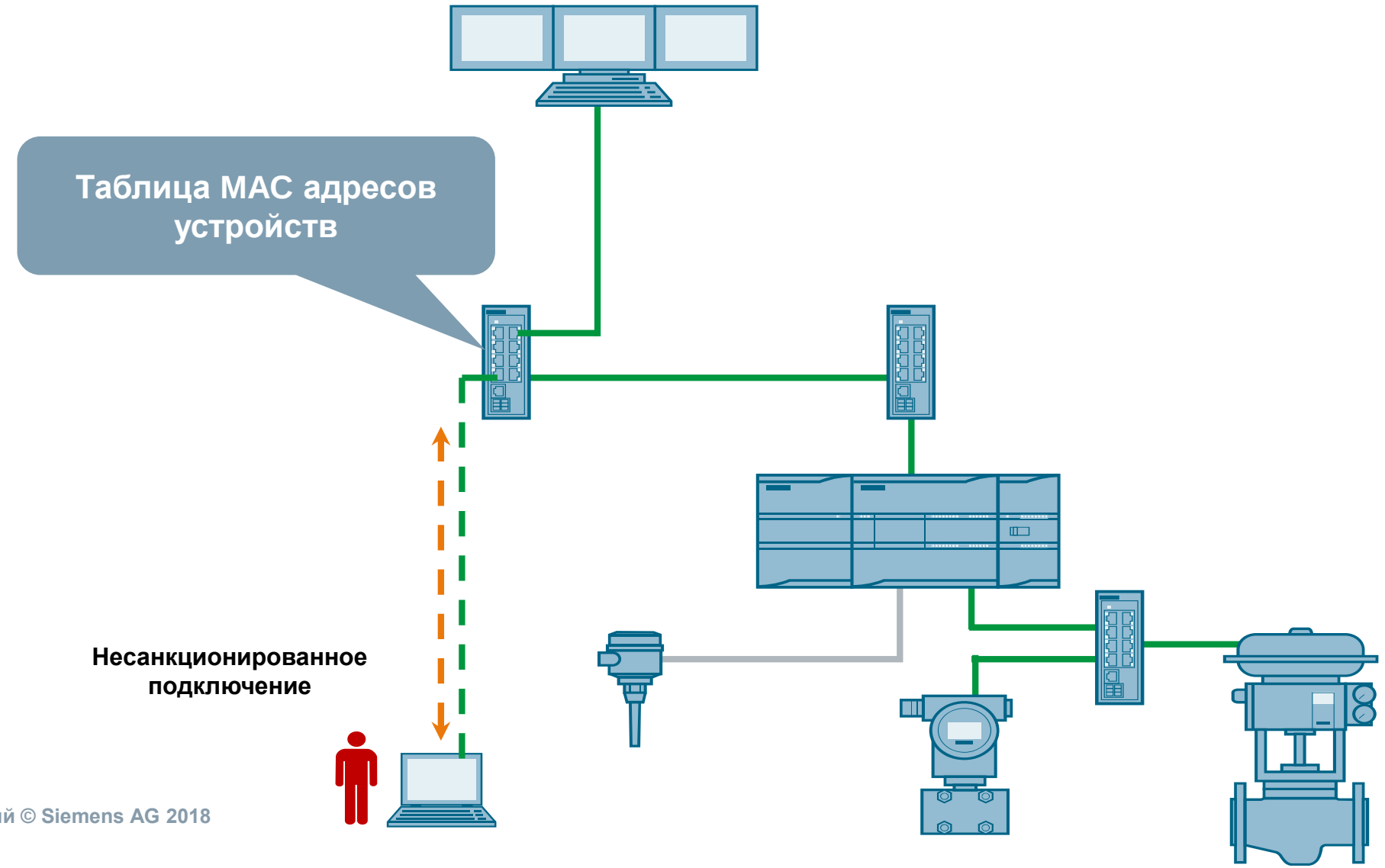
Промышленная безопасность

SIEMENS
Ingenuity for life

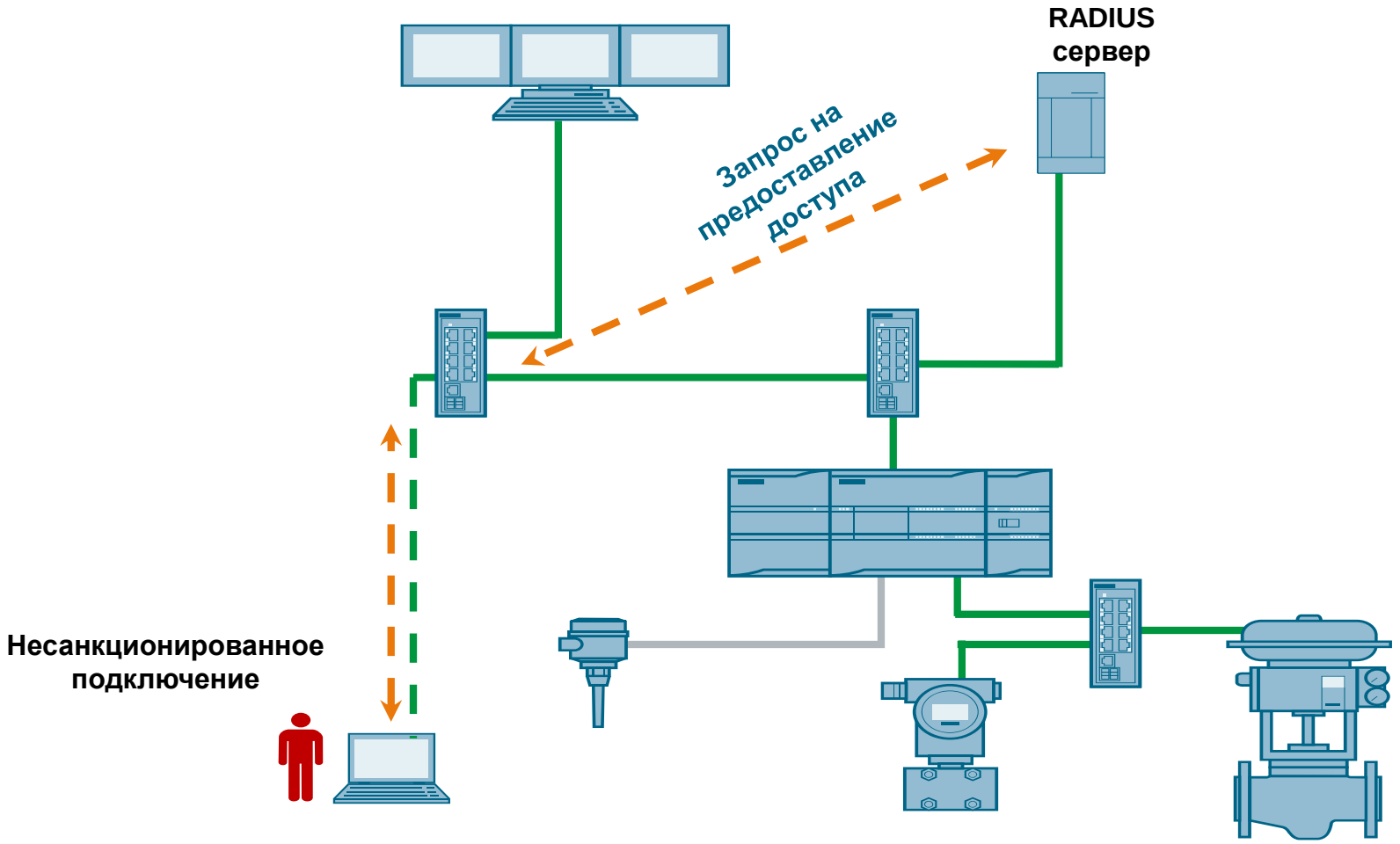
- Введение
- Стандарт IEC 62443
- Решение SIEMENS
- **Примеры применений**
- Преимуществаs работы с Siemens

Защита от несанкционированного подключения с привязкой к MAC адресам устройств

SIEMENS
Ingenuity for life

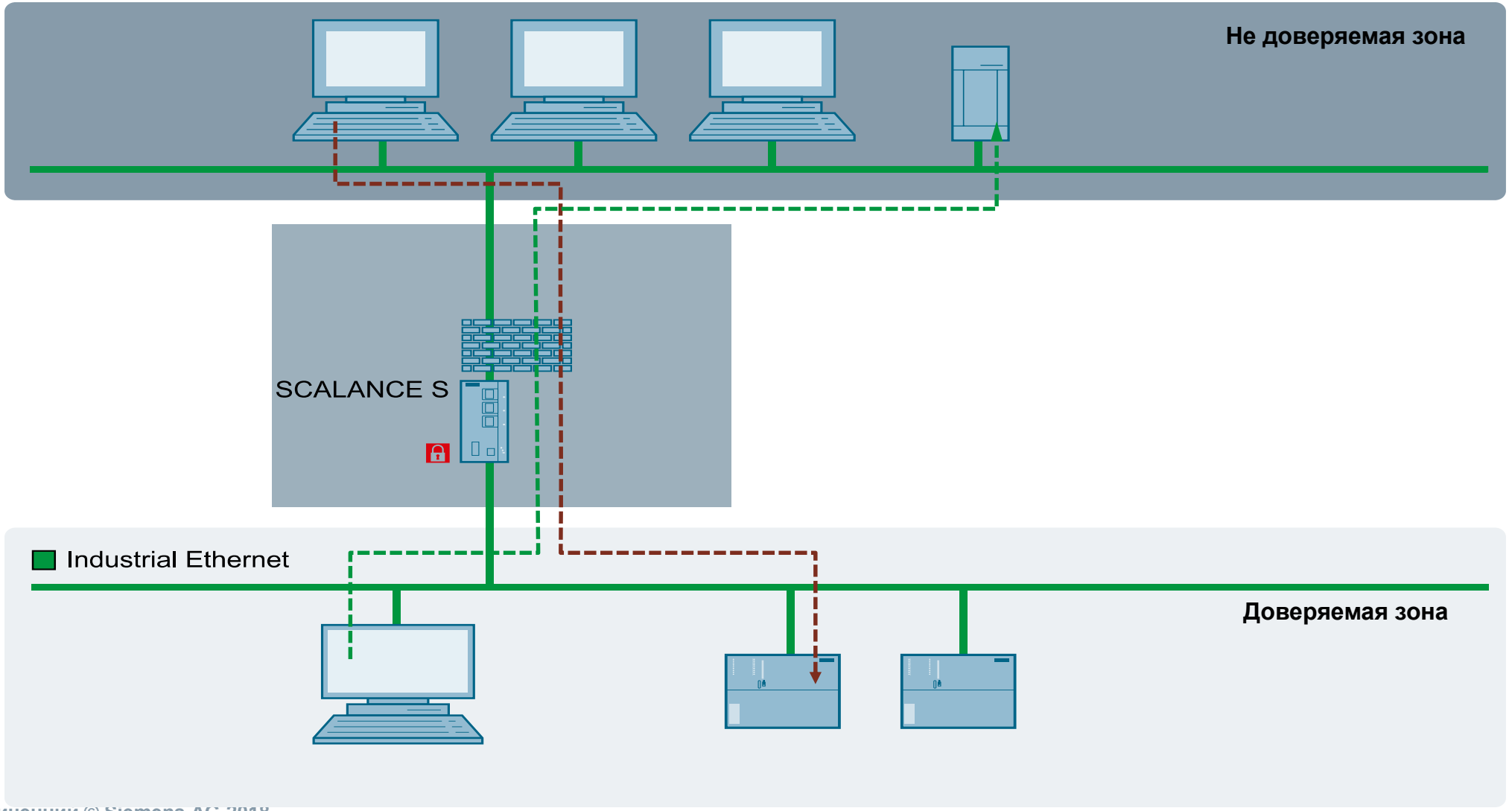


Защита от несанкционированного подключения с использованием протокола 802.1x



Ограничение доступа при помощи межсетевого экрана (Firewall)

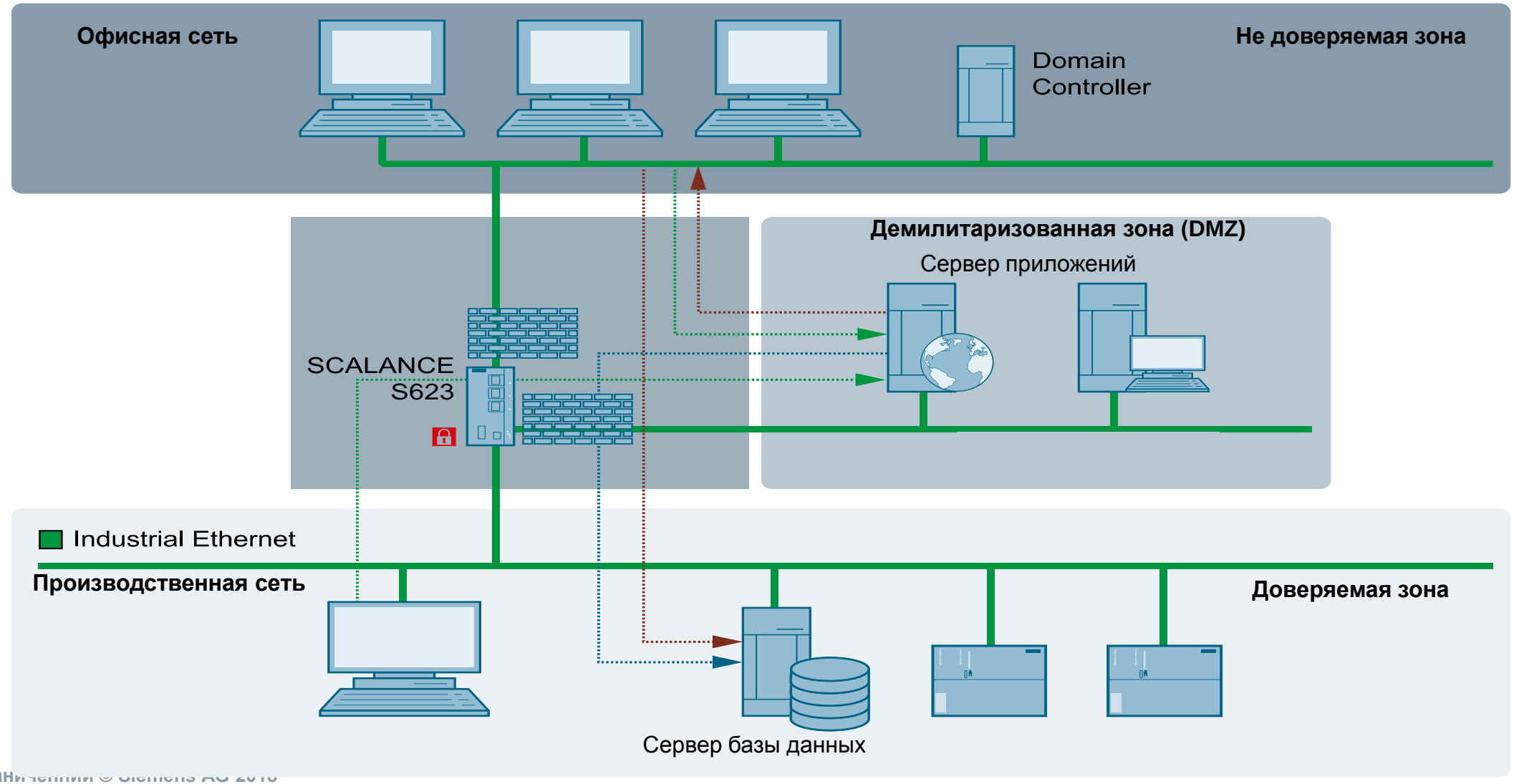
SIEMENS
Ingenuity for life



Разрешённый доступ Неразрешённый доступ Ограниченный доступ

Ограничение доступа при помощи межсетевого экрана (Firewall) с демилитаризованной зоной (DMZ)

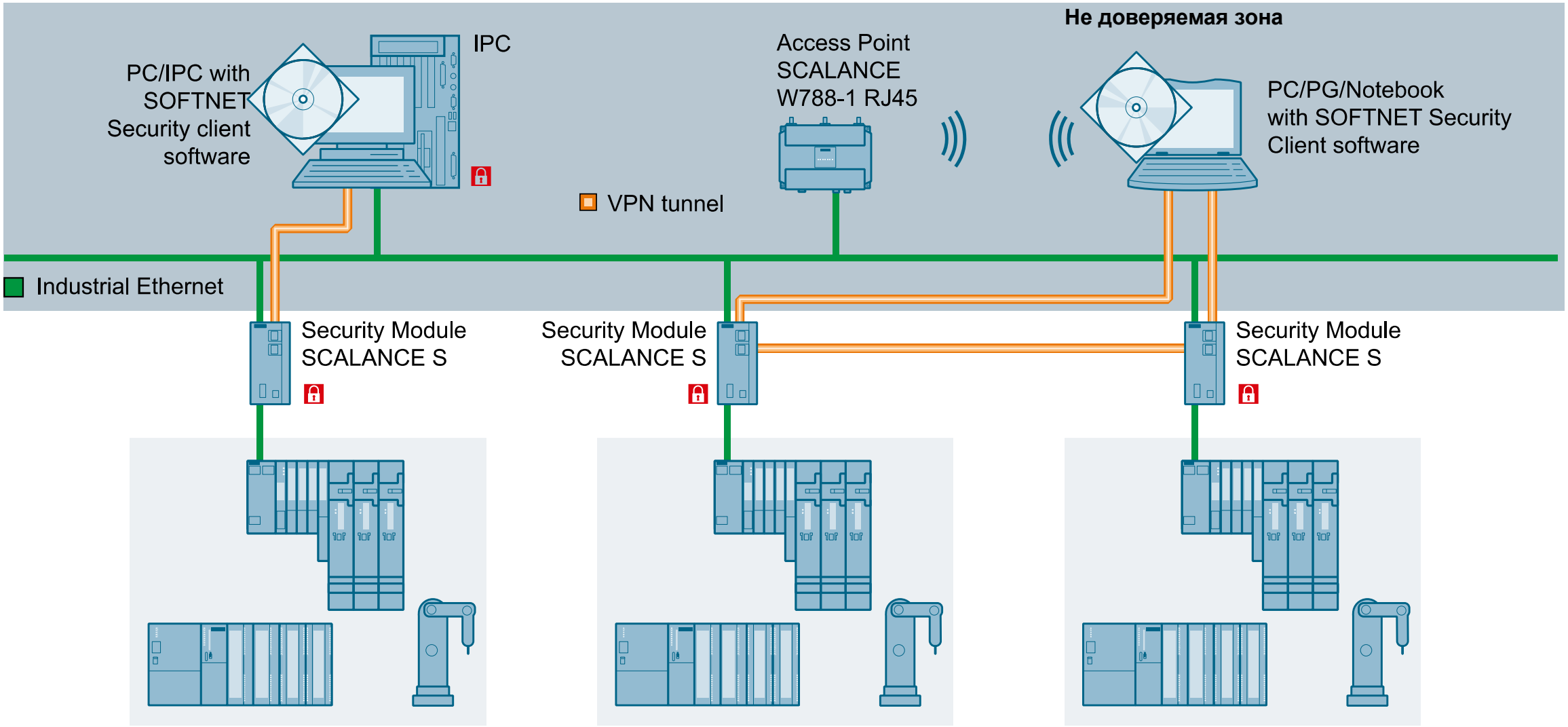
SIEMENS
Ingenuity for life



Разрешённый доступ — Неразрешённый доступ — Ограниченный доступ

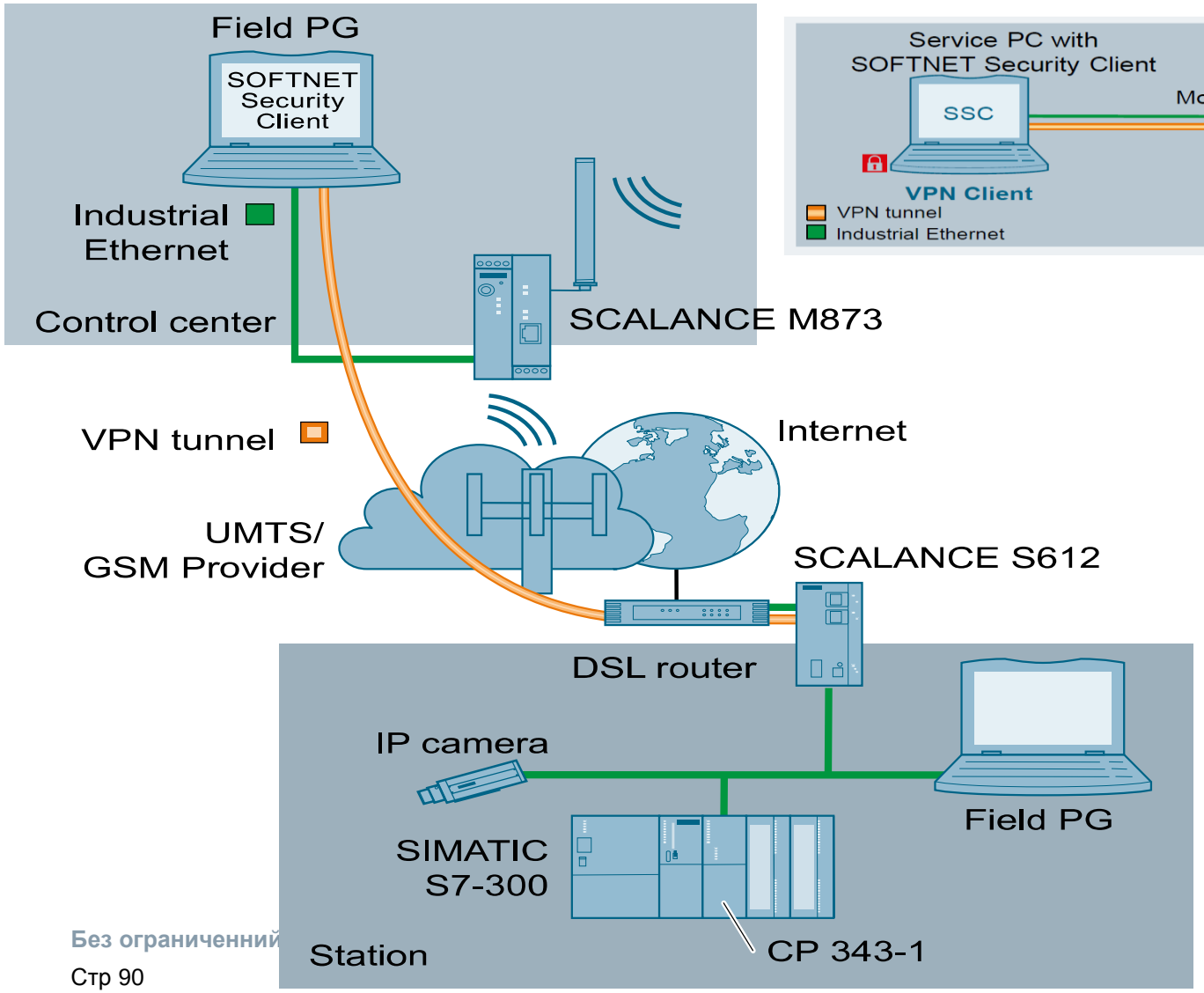
Ограничение доступа при помощи межсетевого экрана (Firewall) с созданием туннелей (VPN tunnel)

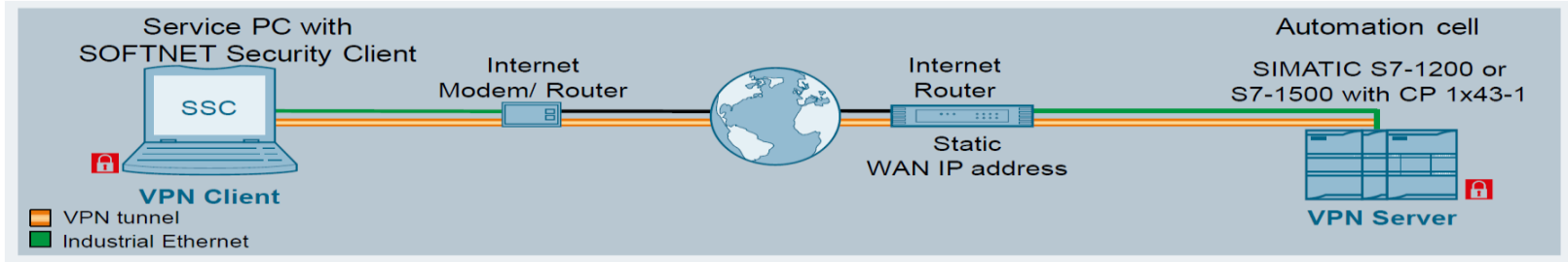
SIEMENS
Ingenuity for life



Шифрованный туннель к удалённой площадке с программным клиентом

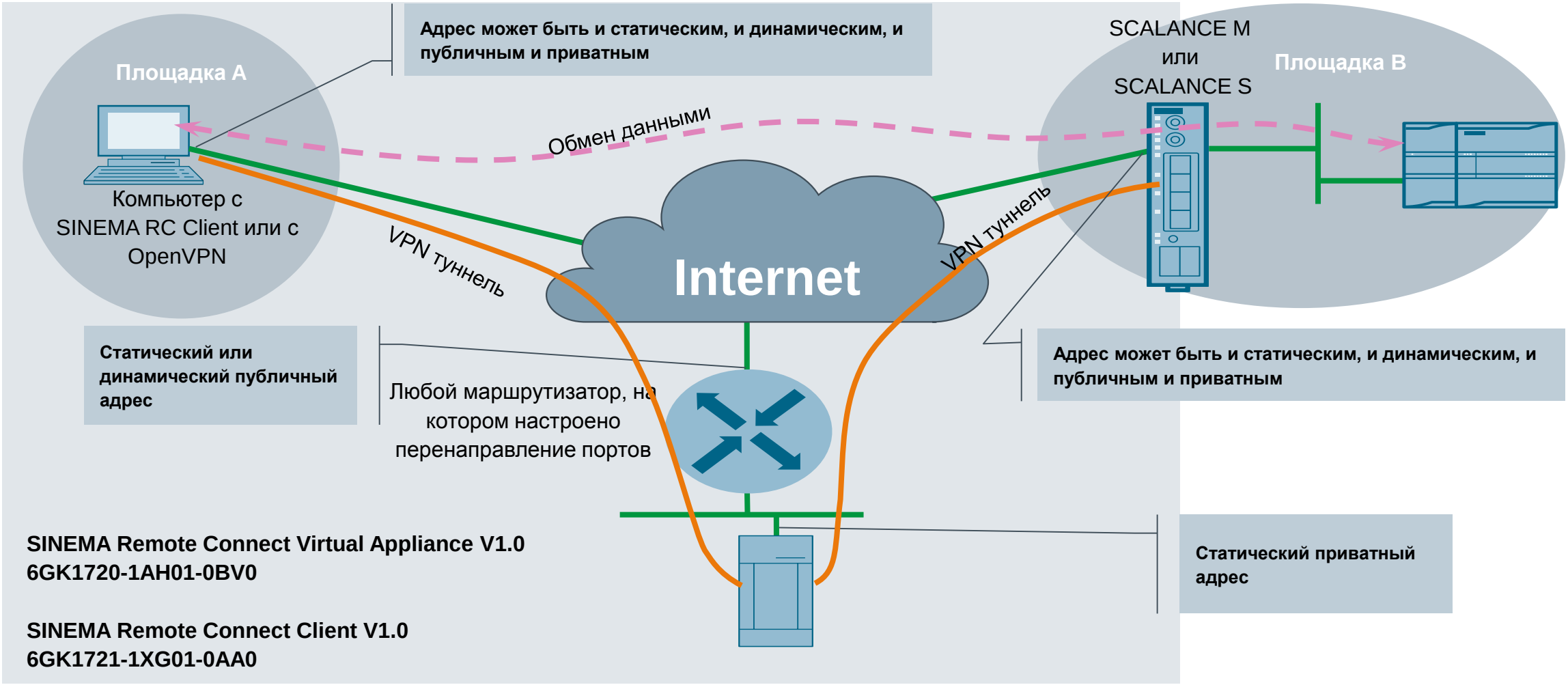
SIEMENS
Ingenuity for life





SINEMA Remote Connect

SIEMENS
Ingenuity for life



SINEMA Remote Connect Virtual Appliance V1.0
6GK1720-1AH01-0BV0

SINEMA Remote Connect Client V1.0
6GK1721-1XG01-0AA0

Примеры сетевой безопасности
Сегментация сети и защита ячейки

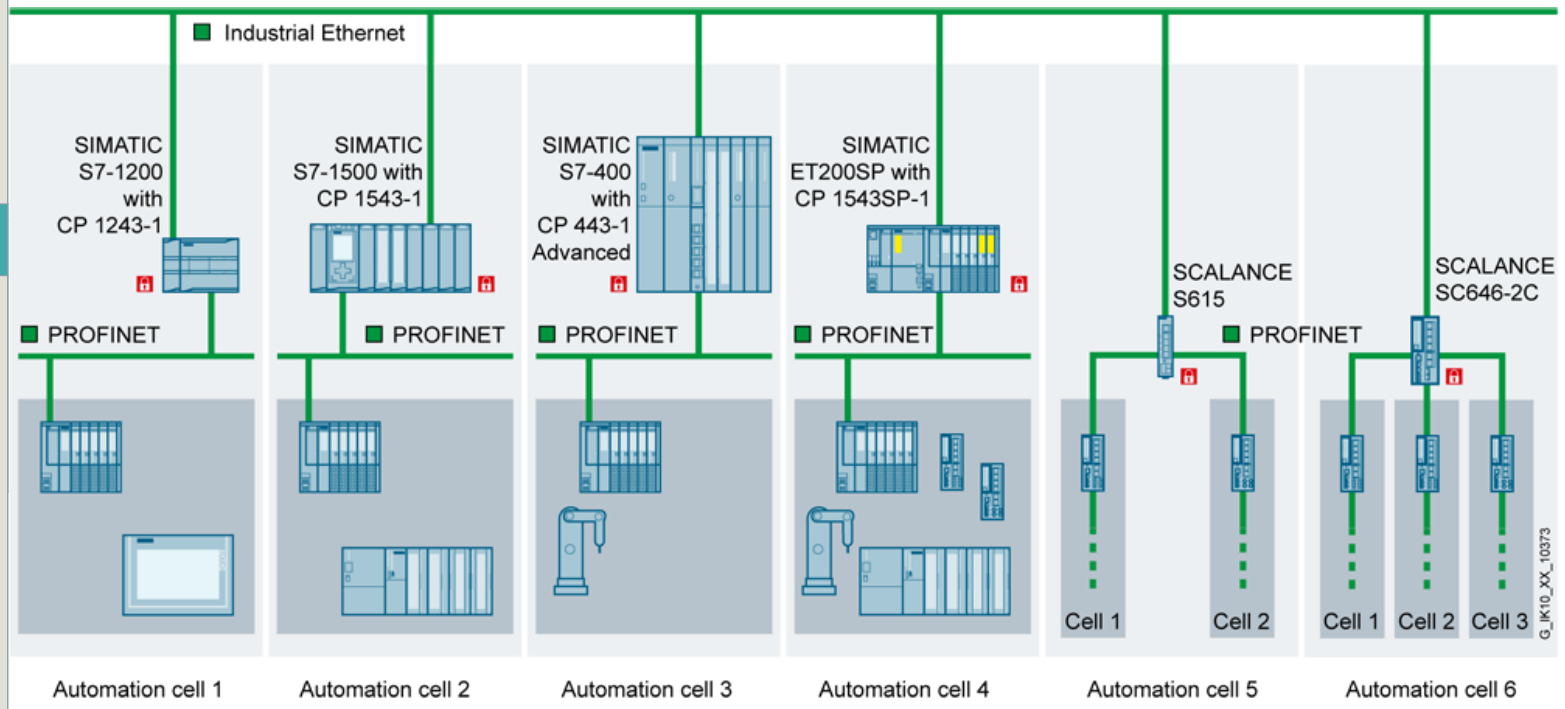
SIEMENS
Ingenuity for life

Задача

С целью уменьшения рисков, большая сеть автоматизации должна быть разделена на несколько зон безопасности. Для каждого сегмента могут быть применены разные требования.

Решение

Отдельные сегменты сети будут защищены с помощью **SCALANCE S** или **защищенных коммуникационных процессоров.** Такие устройства будут контролировать доступ и передачу данных в подчиненном сегменте через их встроенные брандмауэры. С помощью VLAN, **SCALANCE S** могут быть использованы для защиты нескольких ячеек сети одновременно.



Примеры сетевой безопасности

Сегментация сети и защита ячейки для S7-300 и S7-400

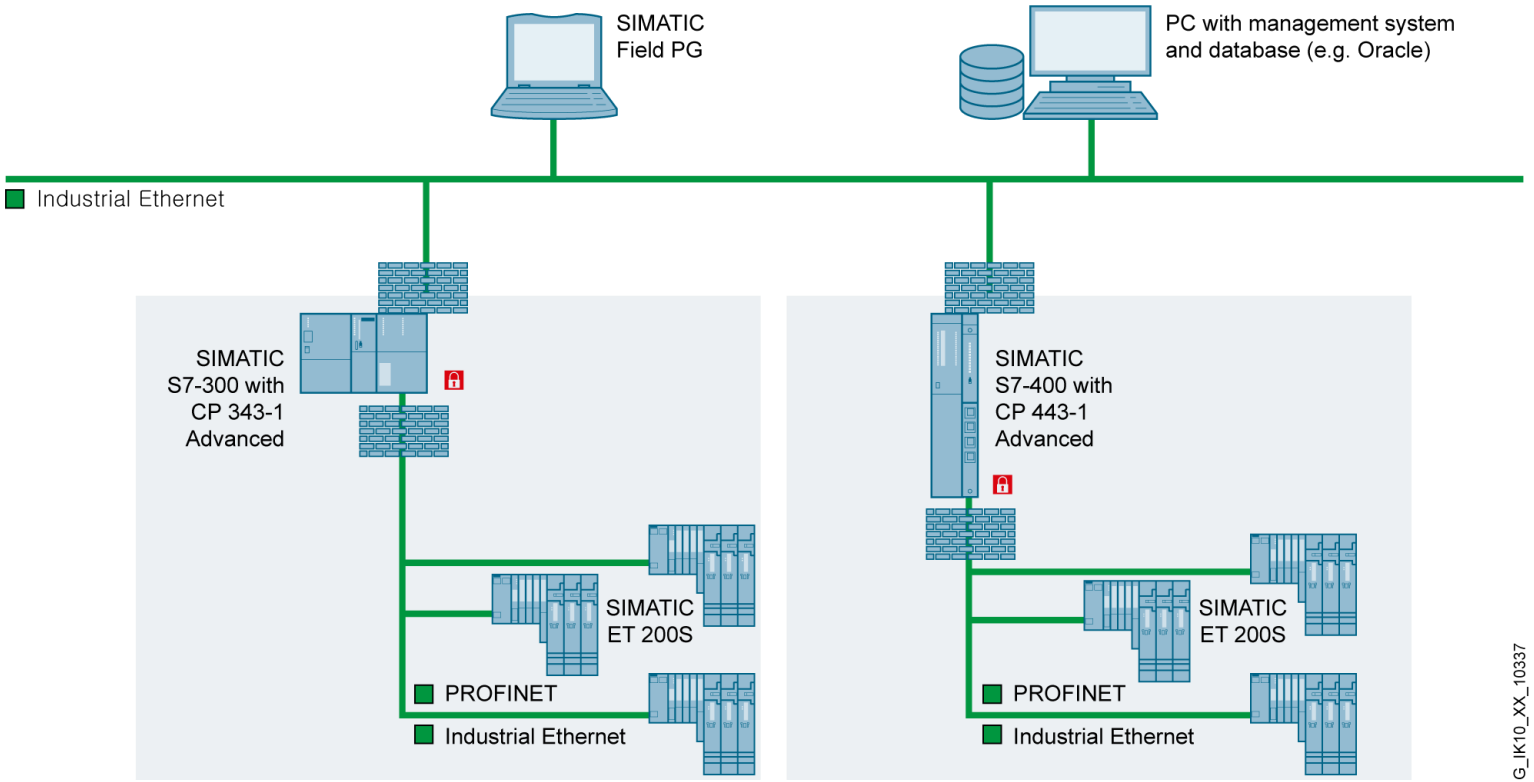
SIEMENS
Ingenuity for life

Задача

Сеть автоматизации и ее коммуникация должны быть разделены на отдельные ячейки, которые контролируются и защищаются контроллером S7-300 или S7-400.

Решение

С помощью встроенных функций безопасности (брандмауэр и VPN) **CP 343-1 Advanced** защищает контроллер S7-300 и **CP 443-1 Advanced** защищает контроллер S7-400. Оба коммуникационных процессора также защищают их подчиненные компоненты от неавторизированного доступа, шпионажа и манипуляция данными.



Примеры сетевой безопасности
Сегментация сети и защита ячейки для S7-1500 станции

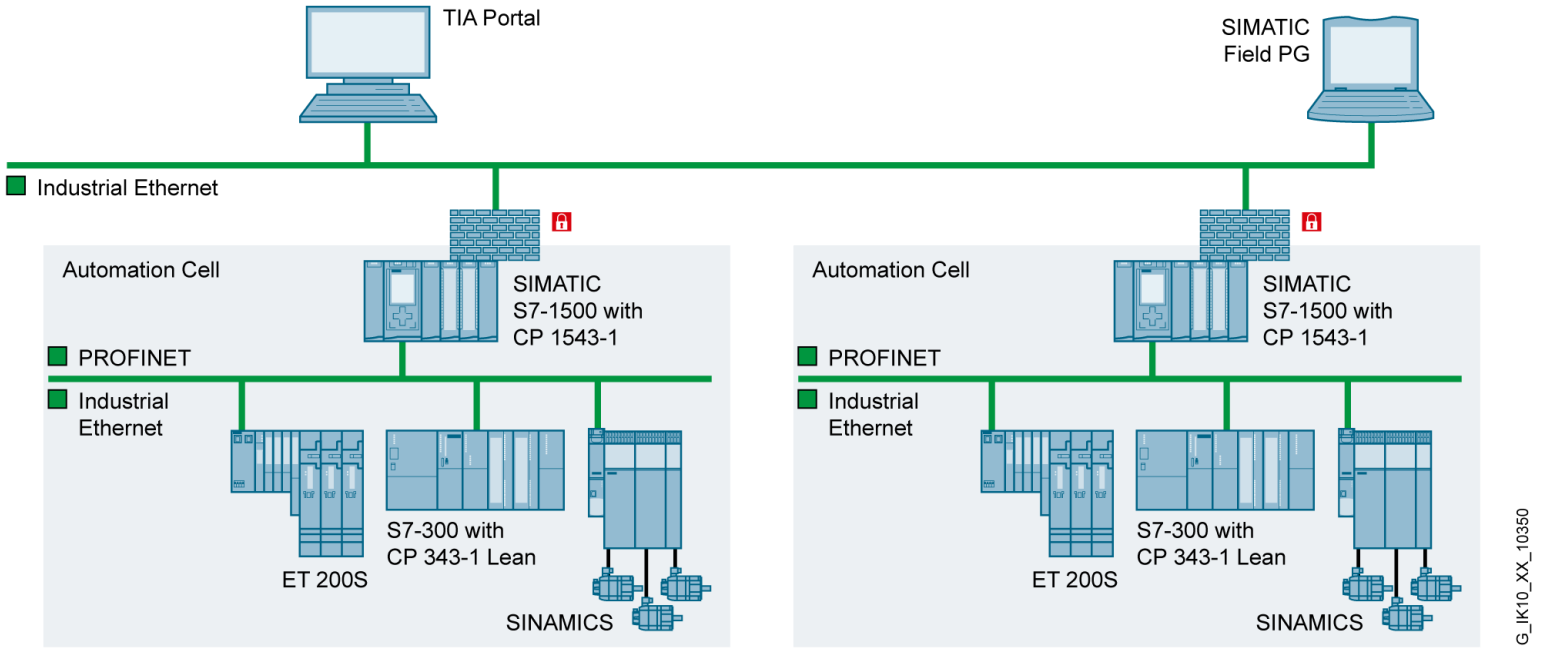
SIEMENS
Ingenuity for life

Задача

Сеть автоматизации и ее коммуникация должны быть разделены на отдельные ячейки, которые контролируются и защищаются контроллером S7-1500.

Решение

С помощью встроенных функций безопасности (брандмауэр и VPN) **CP 1543-1** защищает контроллер S7-1500 и подчиненные компоненты против неавторизированного доступа, шпионажа и манипуляций данными.



Примеры сетевой безопасности

Сегментация сети и защита ячейки для S7-1200 станции

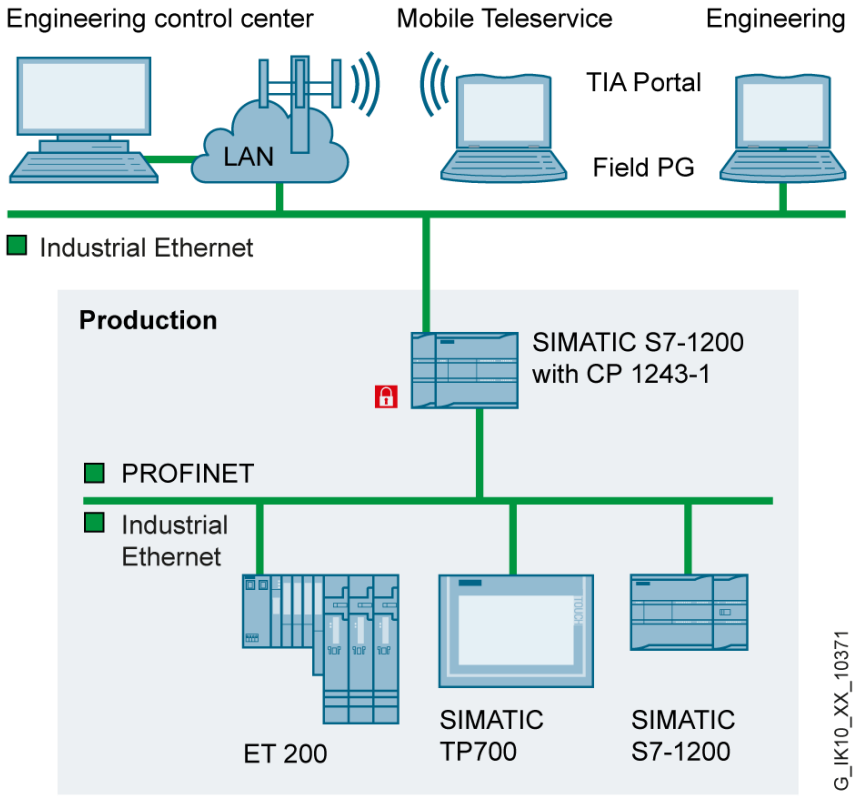
SIEMENS
Ingenuity for life

Задача

Сеть автоматики и ее коммуникации должны быть разделены на отдельные ячейки, которые контролируются и защищаются контроллером S7-1200

Решение

С помощью встроенных функций безопасности (брандмауэр и VPN) **CP 1243-1** защищает контроллер S7-1200 и подчиненные компоненты против неавторизированного доступа, шпионажа и манипуляций данными.



Примеры сетевой безопасности

Сегментация сети и защита ячейки для SIMATIC ET 200SP

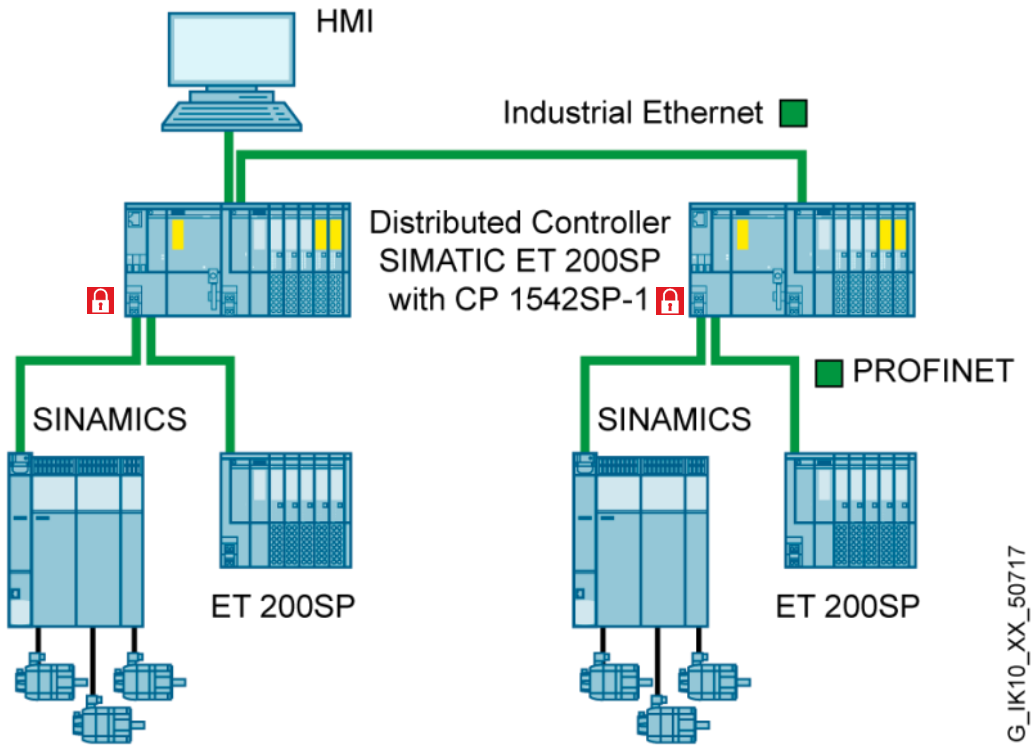
SIEMENS
Ingenuity for life

Задача

Сеть автоматики и ее коммуникации должны быть разделены на отдельные ячейки, которые контролируются и защищаются распределенным контроллером SIMATIC ET 200SP.

Решение

С помощью встроенных функций безопасности (брандмауэр и VPN) **CP 1543SP-1** защищает распределенный контроллер SIMATIC ET 200SP и подчиненные компоненты против неавторизированного доступа, шпионажа и манипуляций данными.



Примеры сетевой безопасности
Безопасная коммуникация между PG / ПК и контроллерами

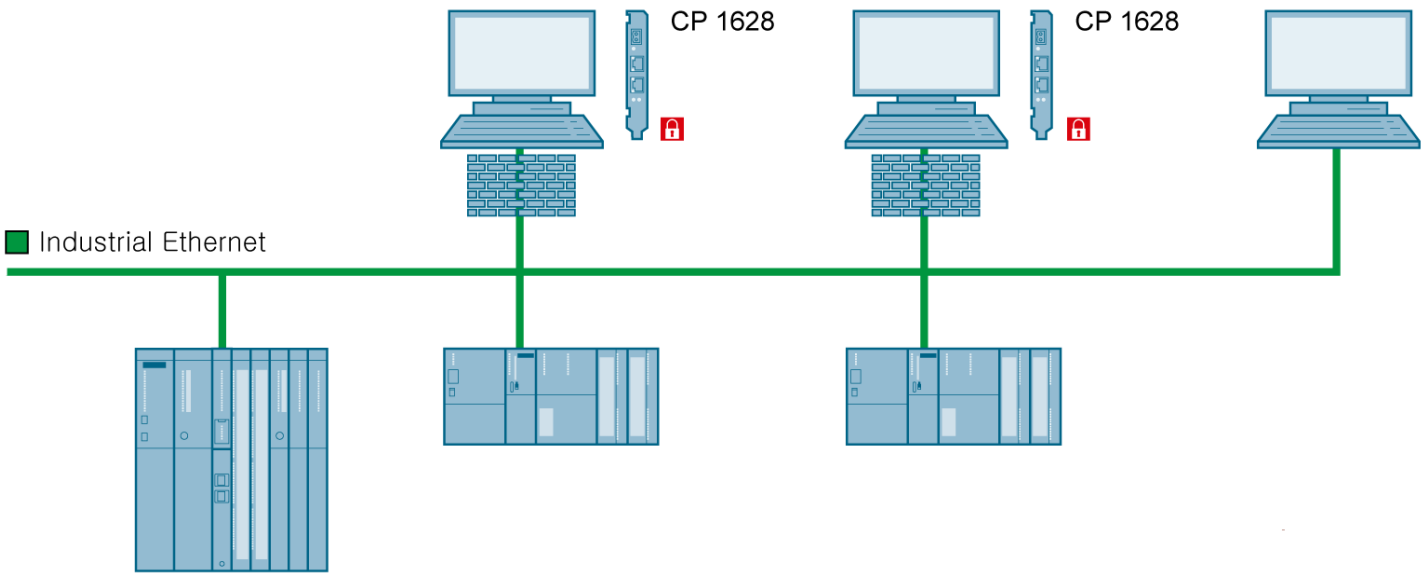
SIEMENS
Ingenuity for life

Задача

Коммуникация из и в ПК системы, такие как OS и ES должны быть контролируемы и защищены.

Решение

С коммуникационным процессорм **CP 1628** (Ethernet PCI карта) и ее встроенными функциями безопасности (брандмауэр и VPN) PG или ПК может быть защищен против неавторизированного доступа, шпионажа и манипуляции данными.



Примеры сетевой безопасности
Безопасное Резервирование для S7-400H контроллеров

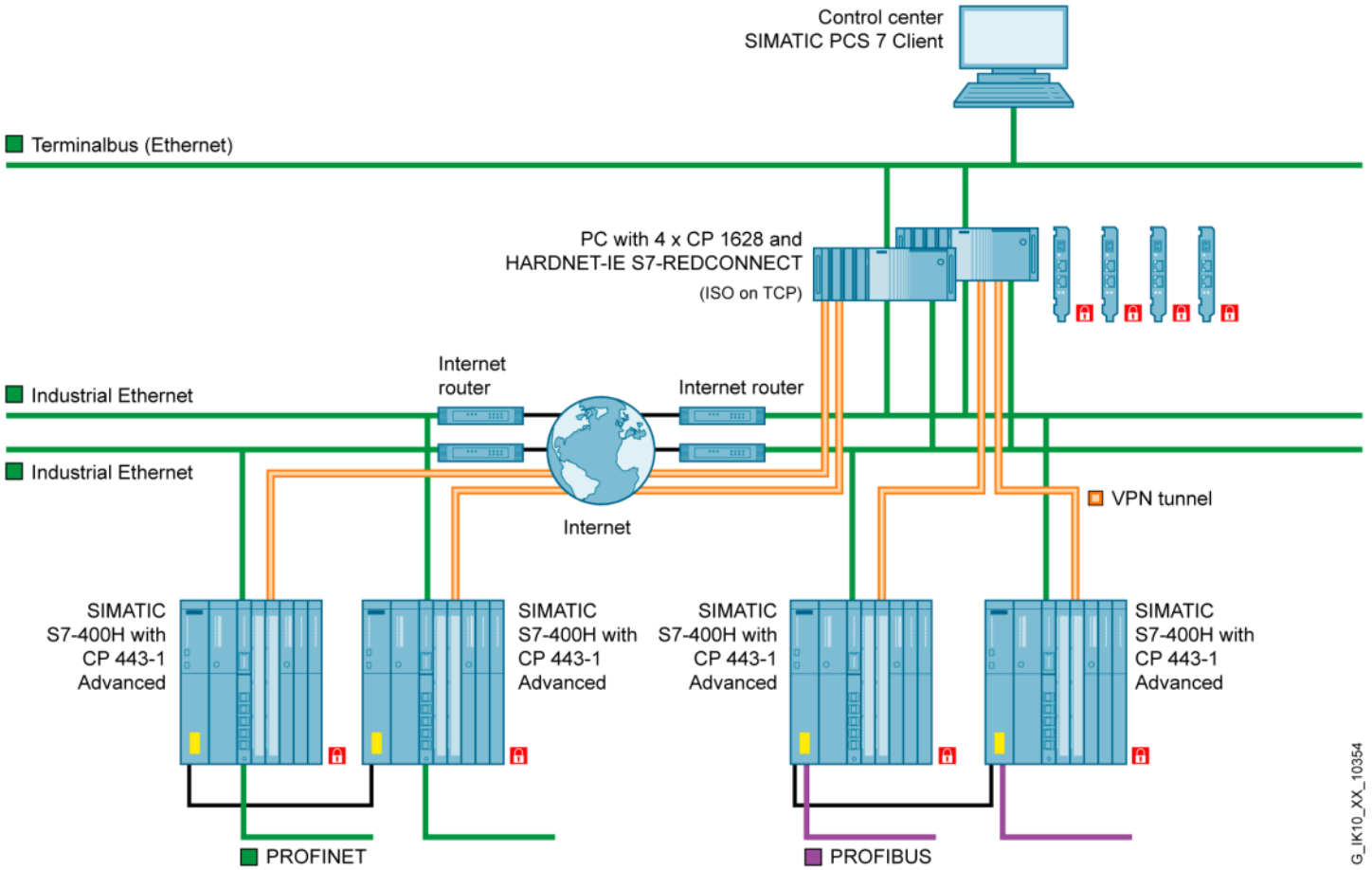
SIEMENS
Ingenuity for life

Задача

Защита резервированных подключений контроллеров между ПК и контроллером S7-400H на участке с требованиями высокой доступности.

Решение

С безопасность коммуникационных процессоров **CP 1628** и **CP 443-1 Advanced** может быть создан VPN туннель, что позволяет безопасную H-коммуникацию.
В дополнение том, что **CP 1628** защищает ПК систему против неавторизированного доступа встроенным брандмауэром.



Примеры сетевой безопасности
Прямой безопасный удаленный доступ к машинам на заводе

SIEMENS
Ingenuity for life

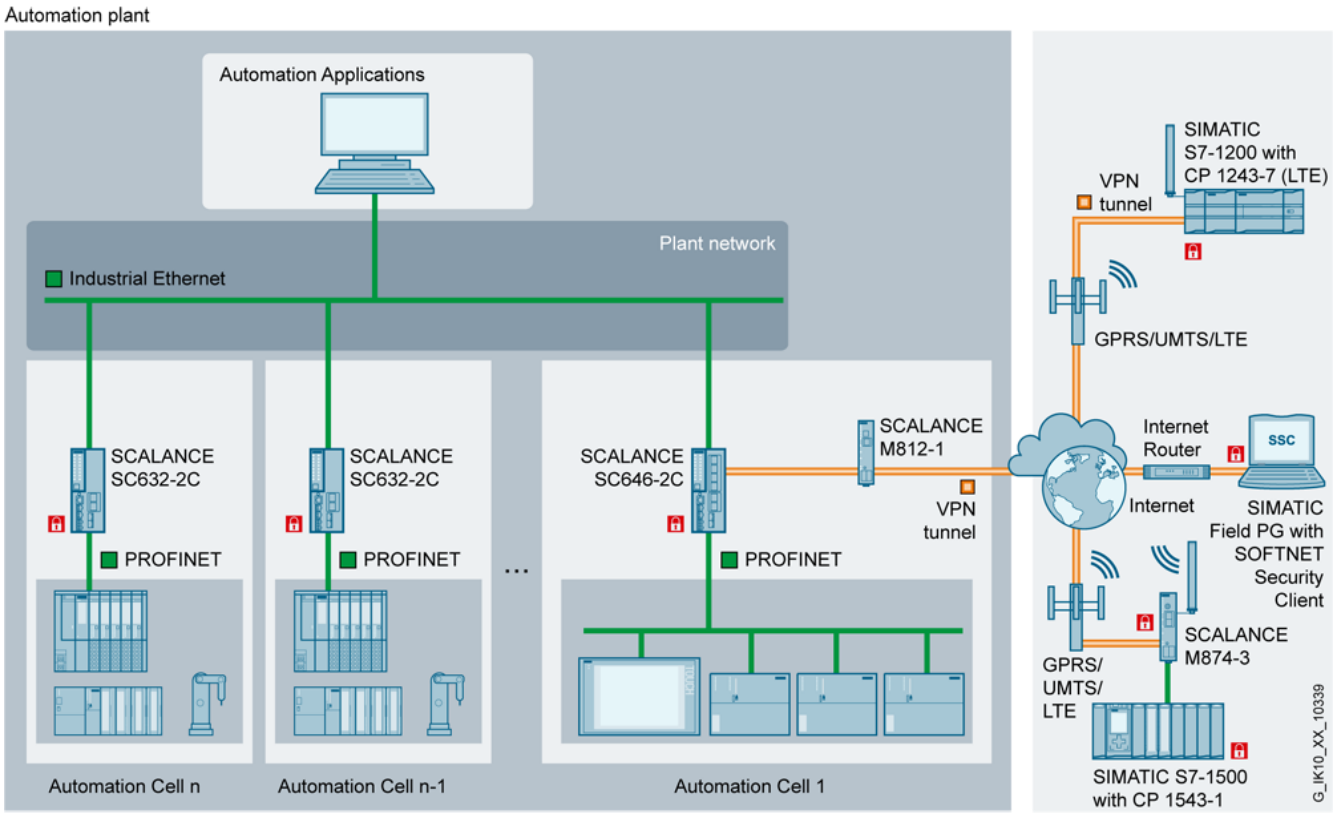
Задача

Должен быть обеспечен прямой безопасный удаленный доступ к машинам и предприятиям.

Решение

С **SOFTNET Security Client** прямой VPN туннель может быть установлен к ячейке автоматики, которая защищена **SCALANCE S**:

- Прямое безопасное подключение устанавливается через клиент-серверное VPN подключение
- брандмауэр с пропуской способностью 600 Мбит/с и VPN с 120 Мбит/с
- Поддержка серийных машин с NAT/NAPT



Примеры сетевой безопасности
Прямой безопасный удаленный доступ по мобильной сети

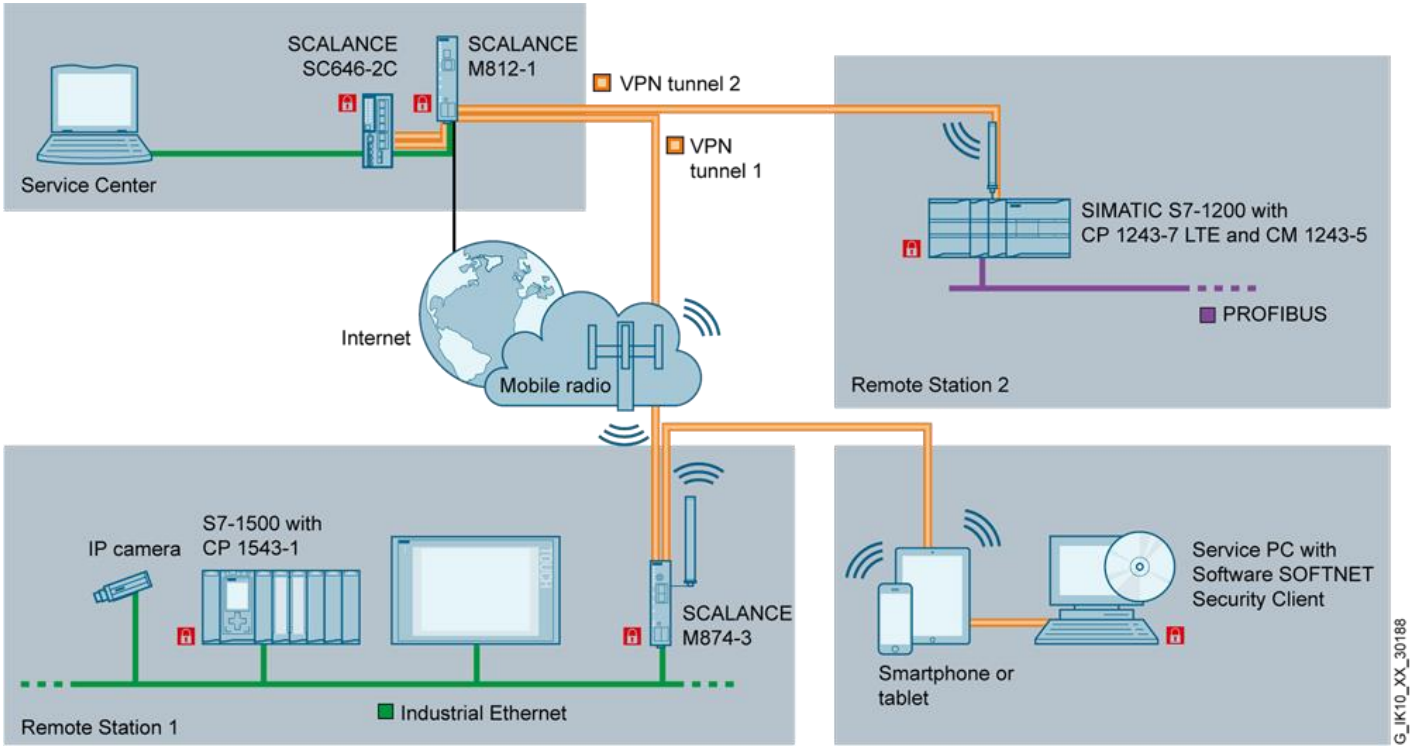
SIEMENS
Ingenuity for life

Задача

Сервисный центр должен подключиться через Internet и получить доступ к глобально распределенным машинам и предприятиям по мобильной связи, что бы выполнить типовые задачи - программирование, назначение параметров, диагностика и мониторинг.

Решение

Все устройства на базе IP защищены промышленными роутерами **SCALANCE M87x** могут быть доступны по мобильной сети. Для распределенных контроллеров SIMATIC S7-1200 может быть применена **CP 1243-7 LTE**. Благодаря встроенной функциональности безопасности также возможно напрямую закрыть VPN туннель на устройстве.



Примеры сетевой безопасности

Безопасный Удаленный доступ через Internet или двухпроводный кабель

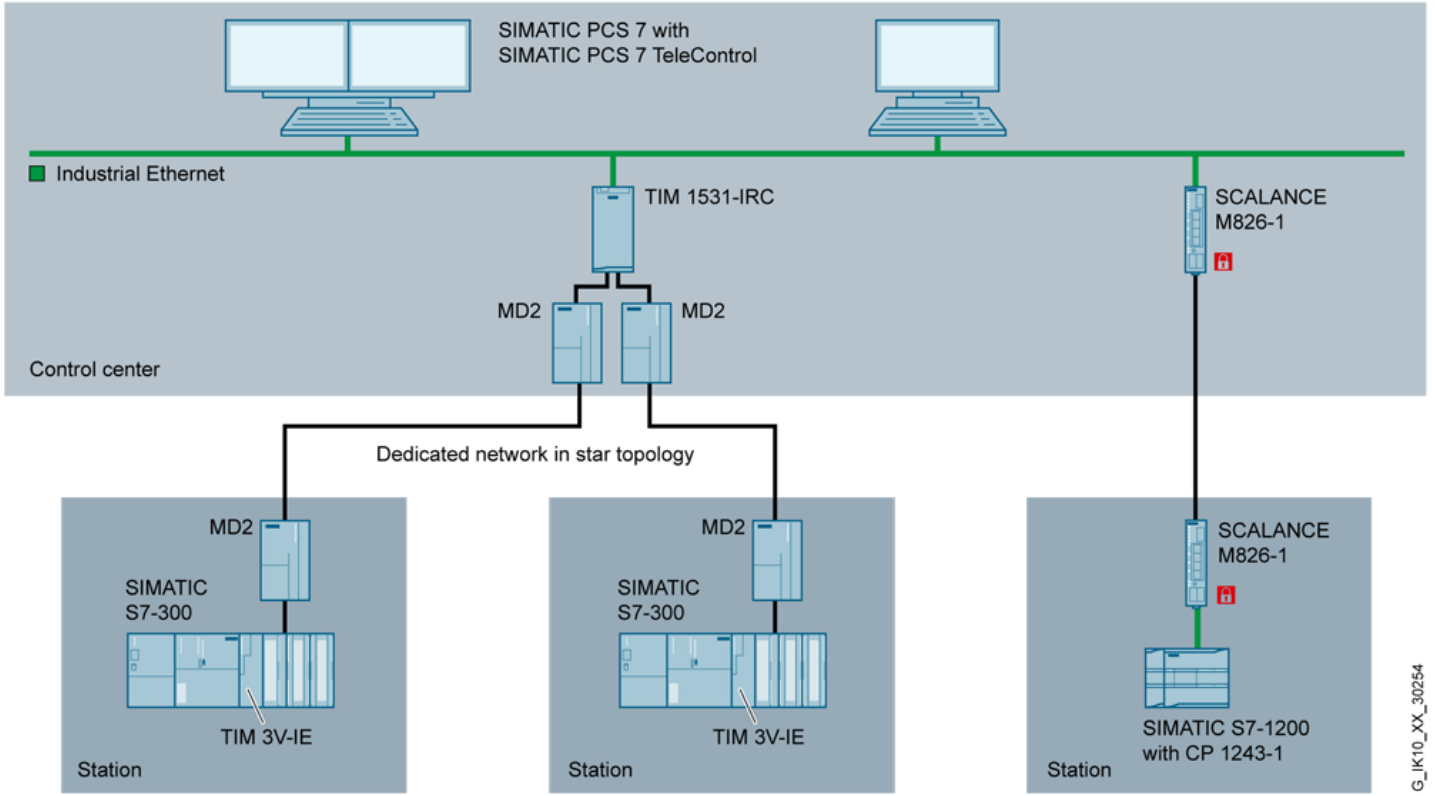
SIEMENS
Ingenuity for life

Задача

Удаленный участок, как станция отбора воды должна быть подключена к центральной диспетчерской через Internet и безопасно передавать команды контроля и мониторинга

Решение

С DSL роутерами **SCALANCE M812-1 / M816-1** или **M826-2** удаленные станции могут быть доступны через Internet или существующие линии. Благодаря встроенному функционалу VPN достигается безопасная передача данных и встроенный брандмауэр предотвращает неавторизированный доступ.



Примеры сетевой безопасности
Безопасный удаленный доступ через сервер рандеву

SIEMENS
Ingenuity for life

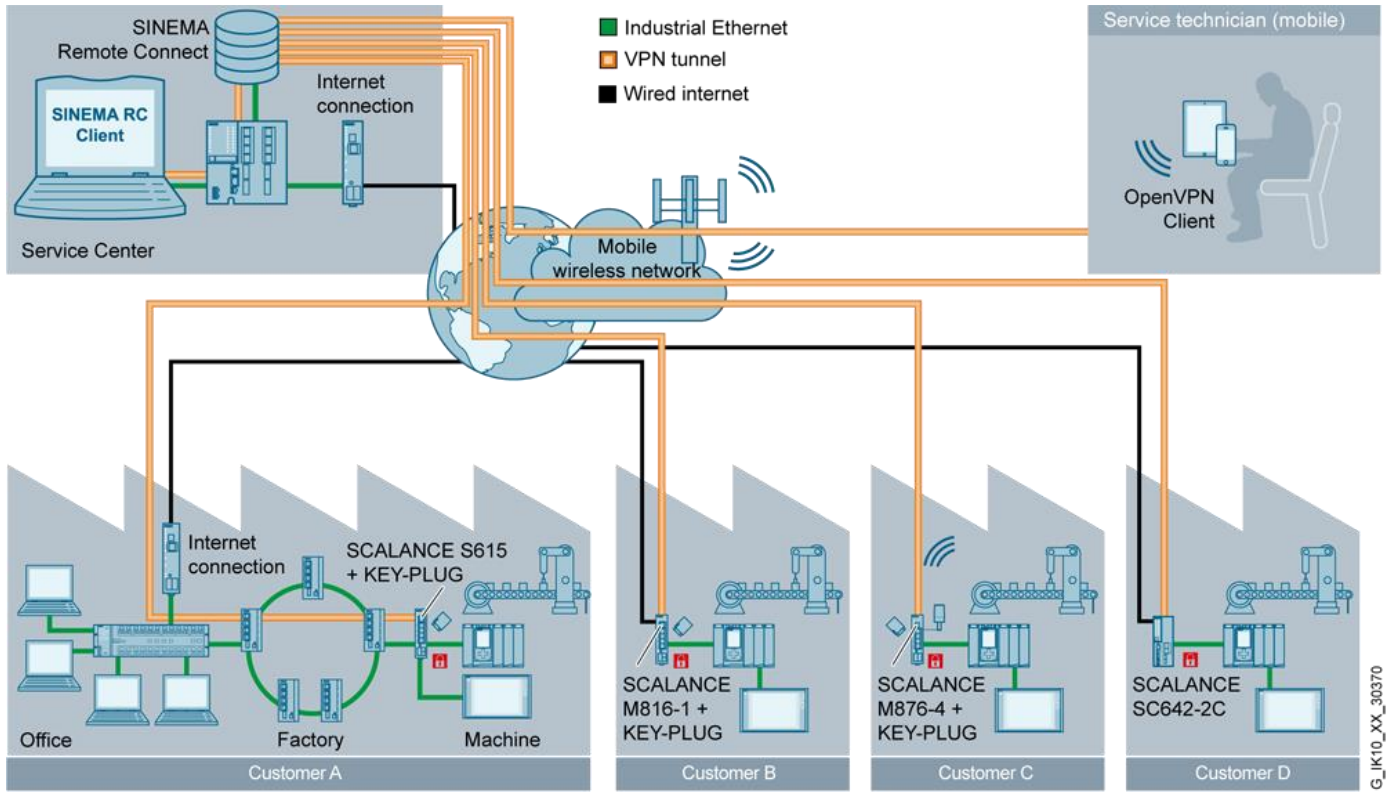
Задача

Безопасный удаленный доступ к производственным предприятиям по всему миру.

Решение

Промышленная **SCALANCE S** встроен в платформу **SINEMA Remote Connect**. Высокая пропускная способность и безопасность данных позволяет сервисному персоналу быстро и безопасно получать доступ к предприятиям и машинам:

- Централизованное и прозрачное управление пользовательскими правами доступа VPN подключений
- Все VPN клиенты подключаются к SINEMA Remote Connect Server (нужет только один публичный статический IP адрес)



Примеры сетевой безопасности

Безопасное удаленное обслуживание специальных и серийных машин

SIEMENS
Ingenuity for life

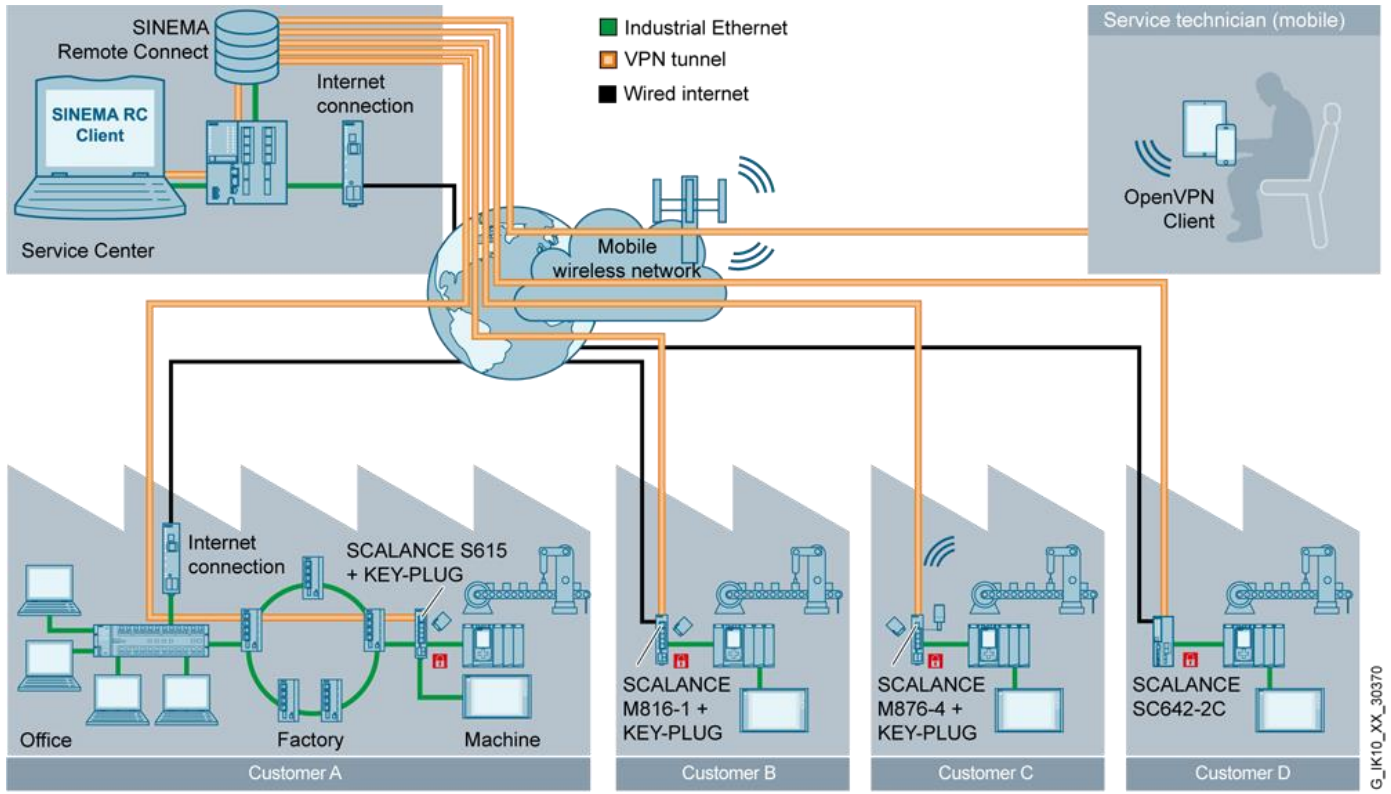
Задача

Безопасное удаленное обслуживание необходимо для специальных и серийных машин также как и для больших предприятий идентичными подсетями. Для всех требуемых подключений данные состояния и обслуживания должны централизованно собираться.

Решение

Централизованное управление подлеченными машинами и авторизированными работниками сервиса в **SINEMA Remote Connect**. Назначение и управление правами пользователя для выделенного доступа:

- Поддержка «серийных машин» путем NAT/NAPT



Примеры сетевой безопасности
Доступ на базе RFID системы идентификации

SIEMENS
Ingenuity for life

Задача

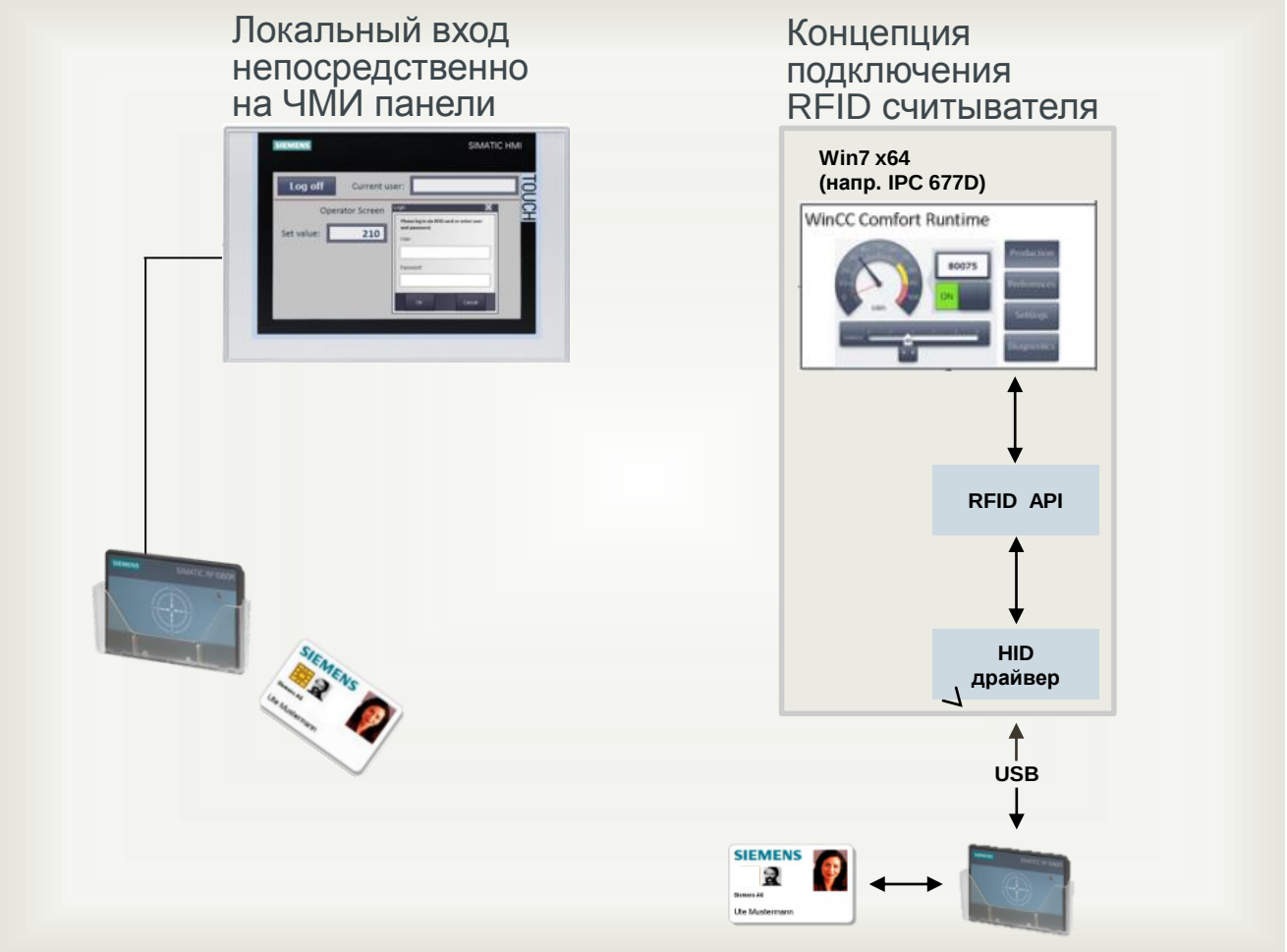
Явная идентификация оперативного персонала машин и участков, включая:

- Контроль доступа
- Аудиторский след

Решение

Доступ к считывателю **SIMATIC RF1060R** поддерживает одноразовый постоянный доступ с RFID картой также как и вход с RFID картой включая четные данные пользователя:

- Вход с RFID картой (одно разово)
- Вход с RFID картой (постоянно)
- Вход с именем пользователя, паролем и RFID картой



Промышленная безопасность
Усиление системы с вайтлистингом

SIEMENS
Ingenuity for life

Пример 1

Обслуживание ОС на важном для производства ПК требует:

- Перезагрузка после установки обновлений.
- Во время обновления необходимо остановка процесса.

Пример 2

Microsoft поддержка Windows XP окончилась в 2014. Для текущей версии mEC контроллеров это обозначает:

- mEC контроллеры не поддерживают новые 64 бит ОС.
- mEC контроллеры - поддержка 64 битной ОС заканчивается в 2014.

Решение

Интервал времени для обслуживания может быть расширен установкой вайтлистинга на ПК:

- Тогда только предопределенное ПО запускается на ПК, патчи безопасности нужно устанавливать не так часто.
- Соответсвтенно, производственный процесс реже требует остановки.

Решение

Жизненный цикл mEC контроллеров может быть расширен настройкой вайтлистинга на этот контроллер:

- Тогда только предопределенное ПО может быть запущено на этом контроллере, который можно использовать определенный период времени после 2014 без дальнейших обновлений безопасности.

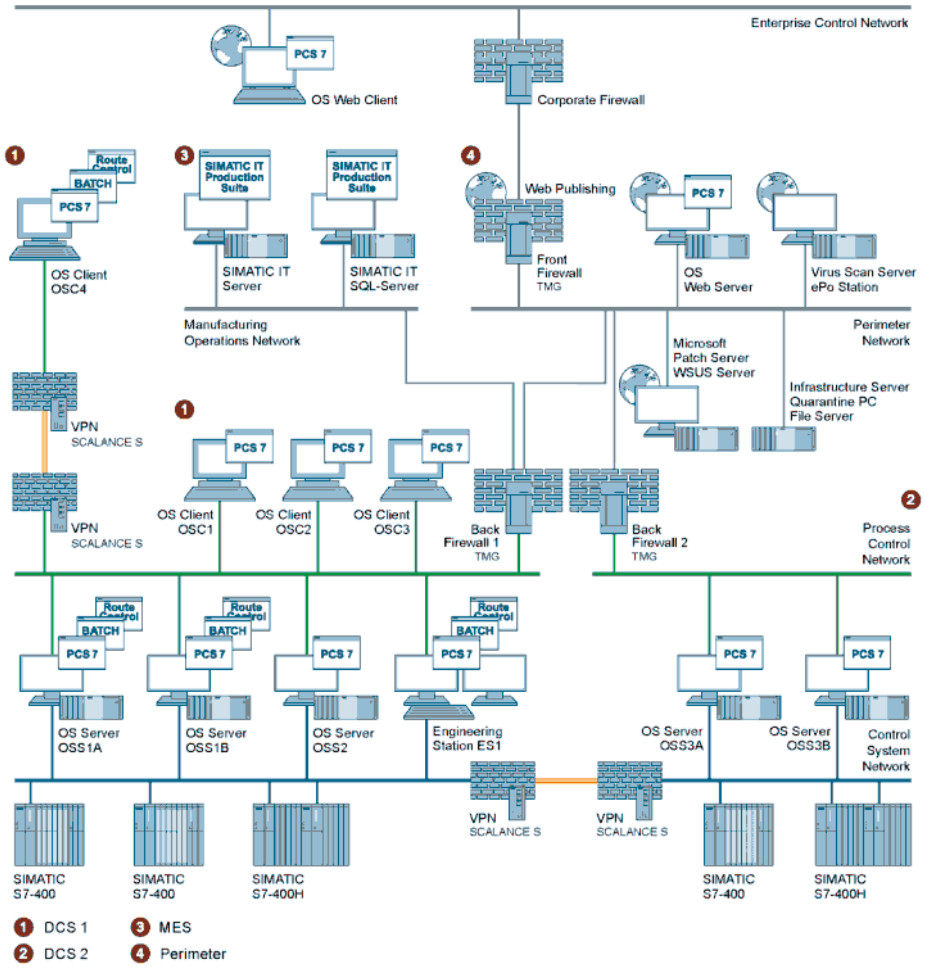
Промышленная безопасность
Пример приложение SIMATIC PCS 7

SIEMENS
Ingenuity for life

SIMATIC PCS 7 *Security You Trust*

Решение Глубоко эшелонированнай оборны

- Аутентификация пользователя
- Сегментация сети
- Демилитаризованные зоны
- Брандмауэры
- VPN туннели
- Антивирусное сканирование
- Управление патчами
- Вайтлистинг приложений



Промышленная безопасность

SIEMENS
Ingenuity for life

- Введение
- Стандарт IEC 62443
- Решение SIEMENS
- Примеры применений
- **Преимуществаs работы с Siemens**

Промышленная безопасность
Гарантировано стандартами

SIEMENS
Ingenuity for life

• **TIA Ethernet устройства** • **Напр. S7-400, S7-300, S7-1500, 1505S, SCALANCE S, …**	• **Процесс разработки**	• **S7- 1500 контроллеры** • **SCALANCE XM408-8C**
• Защит против DoS атак • Защитное поведение в случае атаки • Выше доступность	• Сертификация “Secure Product Development Lifecycle” подразделения DF & PD по стандарту IEC 62443-4-1	• Первый уровень сертификации (CSPN – Certification de Sécurité de Premier Niveau)

Find more information: https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security/certification-standards.html

Find more information:
http://ssi.gouv.fr/certification_cspn/simatic-s7-1518-4-version-du-micrologiciel-1-83/, http://www.ssi.gouv.fr/entreprise/certification_cspn/scalance-xm408-8c/

Промышленная безопасность

Siemens лидирует по сертификации Achilles level 2

SIEMENS
Ingenuity for life

ЦПУ

LOGO!

S7- 300 PN/DP

S7- 400 PN/DP

S7- 1500 and 1505S

S7- 1200

S7- 400 HF CPU V6.0

S7- 410-5H

Распределенные

ET 200 PN/DP ЦПУ

ET 200SP PN ЦПУ

CP

CP343-1 Advanced

CP443-1 & Advanced

CP1243-1

CP1543-1

CP1628

+ Защит против DoS атак
+ Защитное поведение при атаке
  - **Выше доступность**
  - **Международный стандарт**

Промышленная безопасность

Сертификация процесса разработки DF & PD согласно IEC 62443-4-1

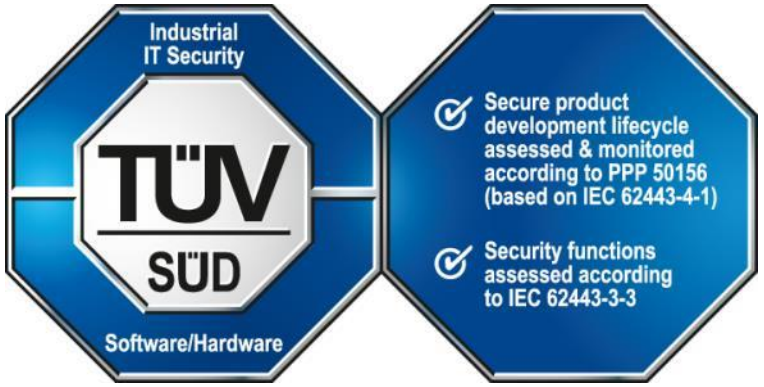
SIEMENS
Ingenuity for life

Заинтересованные стороны по IEC 62443

SIEMENS	Industrial IT Security TÜV SÜD Secure Product Development Lifecycle
Безопасность при разработке	✓
Проверка и аттестация безопасности	✓
Управление обновлениями безопасности	✓

Промышленная безопасность
Сертификация систем SIMATIC PCS 7

SIEMENS
Ingenuity for life

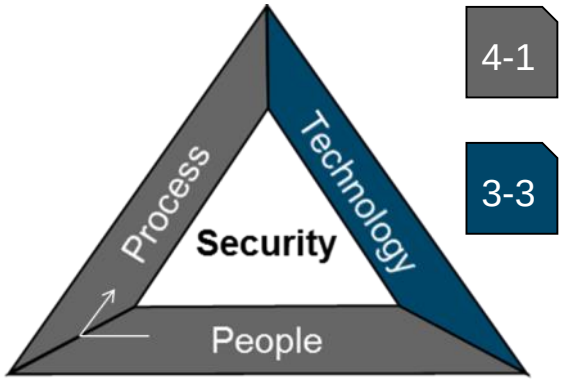


Первая сертификация продукта согласно IEC 62443

- TÜV SÜD сертифицирует, что PCУ SIMATIC PCS 7 соответствует стандарту IEC 62443-4-1 и IEC 62443-3-3

Особенности:

- С этим сертификатом, компания документально подтверждает свой свой подход к безопасности продуктов автоматики и предоставляет интеграторам и операторам прозрачное представление о мерах промышленной безопасности.
- Данная PCУ предлагает исчерпывающие меры безопасности и функции для защиты работы предприятия



4-1 **Жизненный цикл разработки SIMATIC PCS 7**

3-3 **Функциональные возможности безопасности SIMATIC PCS 7**

SIMATIC PCS 7 V9.0
Спасибо за внимание!

SIEMENS
Ingenuity for life

Степанюк Сергей
PCS7 Leading specialist

100% foreign owned subsidiary Siemens Ukraine

RC-UA PD P&S

Ул. Ярославская, 58

04071 Киев, Украина

Тел.: +380 44 392-2322

Моб.: +380 68 538-2322

Эл. почта: serhii.stepaniuk@siemens.com

siemens.com/pcs7-v9